รายงานฉบับสมบูรณ์

โครงการ
ข้อจำกัดของกระบวนการยุติธรรมเพื่อป้องกันและปราบปราม พิศวาสอาชญากรรม (Romance Scam) และแนวทางสร้างความตระหนักรู้ให้กับประชาชน

โดย ผู้ช่วยศาสตราจารย์ ดร.ทศพล ทรรศนกุลพันธ์

ตุลาคม 2562

สัญญาเลขที่ RDG6140057

รายงานฉบับสมบูรณ์
ข้อจำกัดของกระบวนการยุติธรรมเพื่อป้องกันและปราบปราม พิศวาสอาชญากรรม (Romance Scam) และแนวทางสร้างความตระหนักรู้ ให้กับประชาชน

หัวหน้าโครงการและนักวิจัย

ผู้ช่วยศาสตราจารย์ ดร.ทศพล ทรรศนกุลพันธ์ คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่

คณะผู้ช่วยวิจัย

นางสาวปัทชา ศึกษากิจ	คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่
นางสรชา สุเมธวานิชย์	คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่
นางสาววิชญาดา อำพนกิจวิวัฒน์	คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่
นายเขมชาติ ตนบุญ	คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่

สนับสนุนโดย สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.)

(ความเห็นในรายงานนี้เป็นของผู้วิจัย สกสว. ไม่จำเป็นต้องเห็นด้วยเสมอไป)

บทสรุปผู้บริหาร

ผลการศึกษาที่ได้จากการวิจัยสามารถตอบสนองต่อวัตถุประสงค์ทั้ง 3 ประการ อันได้แก่

1. ศึกษาสภาพปัญหา รูปแบบ และวิธีการของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติ

2. พัฒนากฎหมายและมาตรการเฝ้าระวังและเตือนภัยล่วงหน้าเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม

3. สร้างแนวทางเพิ่มความตระหนักให้ประชาชนกลุ่มเสี่ยงตกเป็นเป้าหมายพิศวาสอาชญากรรมให้รู้เท่าทันพิศวาสอาชญากรรม

โดยมีผลการศึกษาดังต่อไปนี้

1. สภาพปัญหา รูปแบบ และวิธีการของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติ

ในหัวข้อนี้จะแสดงให้เห็นผลของการศึกษาใน 2 ส่วนหลัก คือ

1) สถานการณ์ปัจจุบันและสภาพปัญหาพิศวาสอาชญากรรม

2) รูปแบบและวิธีการของพิศวาสอาชญากรรม

1.1. สถานการณ์ปัจจุบันและสภาพปัญหาพิศวาสอาชญากรรม

พิศวาสอาชญากรรม “Romance Scam” คือ การที่นักต้มตุ๋น (Scammer) ได้ใช้เทคนิคทางจิตวิทยาผ่านเครื่องมือทางเทคโนโลยีต่าง ๆ ในการหลอกลวงให้เหยื่อ (Victim) หลงเชื่อจนกระทั่งยินยอมให้ทรัพย์สินที่นักต้มตุ๋นต้องการ ซึ่งวิธีการที่นักต้มตุ๋นมักใช้หลอกลวง คือ การสร้างโปรไฟล์ปลอมๆ ขึ้นมาในโซเชียลมีเดีย หรือเว็บไซต์หาคู่ โดยข้อมูลที่นำมาใช้ทำโปรไฟล์ปลอมก็นำมาจากการขโมยข้อมูลผู้อื่นเช่นกัน เช่น ชื่อ ประวัติ และรูปภาพ แล้วเอามาดัดแปลงเป็นข้อมูลของตนเอง หรืออีกวิธีหนึ่ง คือ จะสร้างข้อมูลเท็จขึ้นมาเองให้ดูสมจริงและน่าดึงดูดที่สุด โดยเหยื่อที่นักต้มตุ๋นเหล่านี้มองหาคนขี้เหงาและเป็นคนอ่อนไหวต้องการใครสักคนมาอยู่เคียงข้างเป็นเหยื่อ

ประเทศไทยมีผู้เสียหายจากพิศวาสอาชญากรรมมากขึ้น และไม่มีแนวโน้มจะลดลง ในปี 2558 มีผู้ร้องเรียนเข้ามาถึง 80 คดี มูลค่าความเสียหาย 150 ล้านบาท และล่าสุดสถิติข้อมูลเมื่อวันที่ 21 มิถุนายน พ.ศ. 2561 ถึง 31 พฤษภาคม พ.ศ. 2562 มีผู้เสียหายหลงเชื่อและโอนเงิน จำนวน 332 ราย รวมมูลค่าความเสียหายประมาณ 193,015,902.11 บาท ยังไม่นับคดีที่ถูกร้องเรียนไปยังสถานีตำรวจท้องที่และเหยื่อที่ไม่กล้าเข้าแจ้งความอีกเป็นจำนวนมาก และผู้ที่ตกเป็นเหยื่อส่วนมากจะเป็นหญิงโสดอายุ 40-60 ปี การศึกษาดี หน้าที่การงานมั่นคง ที่สำคัญคือ “มีทรัพย์สิน” และมีเพียงไม่ถึง 10% เท่านั้นที่มีการแจ้งความ เหตุผลหนึ่งเพราะอับอายและลำบากใจเมื่อทราบว่าตนเองตกเป็นเหยื่อของ

การหลอกลวงนี้ อีกทั้งยังขาดความรู้เกี่ยวกับขั้นตอน และสถานที่ของการแจ้งความเมื่อถูกหลอกลวง และเข้าใจว่าการแจ้งความไม่ได้เกิดประโยชน์อะไรเพราะไม่น่าจะดำเนินคดีกับอาชญากรได้

อาชญากรรมชนิดนี้ไม่มีแนวโน้มที่จะลดลงเมื่อเทียบกับอาชญากรรมที่ใกล้เคียงกันอย่างคอลเซ็นเตอร์ที่ลดจำนวนลงอย่างมากหลังหน่วยงานรัฐที่ถูกอ้างชื่อได้ออกประกาศแจ้งเตือน เนื่องจากพิศวาสอาชญากรรมใช้วิธีการตีสนิทและทำให้ผูกพันเป็นรายบุคคลแตกต่างเรื่องราวกันไป โดยมิได้อ้างอิงกับสถาบันหรือองค์กรที่หน่วยงานจริงจะสามารถออกมาแจ้งเตือนให้ข้อมูลทำลายความน่าเชื่อถือได้ จึงมีความจำเป็นต้องเปิดเผยความจริง “หลังฉาก” เพื่อฉีกหน้ากากที่อาชญากรสร้าง “หน้าฉาก” เพื่อหลอกให้เหยื่อตกลงปลงใจ

อีกสาเหตุที่อาชญากรรมประเภทนี้เกิดขึ้นแพร่หลายในยุคดิจิทัล ก็เพราะ ผู้คนจำนวนมากหันเข้าสู่โลกออนไลน์แทนที่จะออกไปมีปฏิสัมพันธ์กับผู้อื่น และเลือกที่จะสื่อสารเรื่องส่วนตัวกันผ่านสื่อออนไลน์มากกว่า เพราะพวกเขาสามารถระบายหรือได้พูดคุยกับคนที่ไม่รู้จักตัวตนของพวกเขาโดยอาจไม่ต้องเปิดเผยตัวตนที่แท้จริงอันทำให้พวกเขารู้สึกสบายใจกว่า เว็บไซต์และแอพพลิเคชั่นกระตุ้นให้ผู้ใช้สร้างเครือข่ายสังคมออนไลน์เพื่อพบเจอผู้คนที่อาจไม่รู้จัก แต่มีความคิด ความชอบที่เหมือนหรือคล้ายกัน ให้เข้ามาพบเจอกัน โดยเฉพาะเครือข่ายที่เป็นการสร้างชุมชนบนโลกออนไลน์ในลักษณะการใส่ข้อมูลส่วนตัวให้คนอื่นมาสนใจแบบมองมาที่ฉัน (Look at Me) อันเป็นการสร้างความเสี่ยงให้กับผู้ใช้มากขึ้น เนื่องจากผู้ใช้ได้เผยข้อมูลอ่อนไหวของตนให้คนแปลกหน้าซึ่งอาจจะเป็นอาชญากรที่มองหาเหยื่อ

1.2. รูปแบบและวิธีการของพิศวาสอาชญากรรม

กลยุทธ์ที่ใช้หลอกลวงทางอินเตอร์เน็ตมีหลากหลายรูปแบบ อย่างเช่น การหลอกเหยื่อว่าจะส่งของมาให้ โดยนักต้มตุ๋นจะใช้ความไว้เนื้อเชื่อใจของเหยื่อ จากการที่พูดคุยกันมาในระยะเวลาหนึ่ง และมั่นใจว่าเหยื่อให้ความไว้ใจ หรือให้ความสนิทสนมกับตนแล้ว พฤติกรรมการหลอกลวงของสแกมเมอร์มีพัฒนาการตามรูปแบบวิธีการสื่อสาร เมื่อถึงยุคเทคโนโลยีสารสนเทศ 3.0 จะเป็นการหลอกลวงทาง Social Media อย่างเช่น Facebook, Instagram เครือข่ายเหล่านี้เป็นช่องทางที่ถูกอาชญากรใช้มากที่สุด เนื่องจากมีผู้คนเข้าใช้งานเป็นจำนวนมาก อีกทั้งพฤติกรรมของผู้ใช้งานยังถูกเปิดเผยถูกสาธารณะได้ง่าย จึงทำให้อาชญากรสามารถเลือกเหยื่อเป้าหมายได้ไม่ยากนัก

หลักการพื้นฐานทางจิตวิทยาร่วมกับการเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูล การวางแผนและการดำเนินขั้นตอนตามที่วางแผนไว้ หรือเรียกรวมๆ ว่า “วิศวกรรมสังคม” (Social Engineering) โดยกระบวนการล่อลวงนี้สามารถแบ่งได้เป็นขั้นตอนหลัก 6 ขั้นตอน ดังนี้

1) การปลอมโปรไฟล์

สร้างโปรไฟล์ทั้งเพศชาย เพศหญิง และเพศทางเลือกด้วยการขโมยรูปภาพบุคคลอื่นที่มีลักษณะบุคลิกภาพดี หน้าตาดี และดูภูมิฐานจากเว็บไซต์เครือข่ายสังคมออนไลน์ต่างๆ เช่น Facebook, Instagram, twitter หรือเว็บเพจต่างๆ ส่วนใหญ่มักอ้างตัวเป็น “ฝรั่งผิวขาว” ที่เป็นเพศชายมากกว่าเพศหญิง ลักษณะร่วมของคนเหล่านี้มักอ้างว่าโสด หรือหย่าร้าง/หม้าย ต้องการตามหารักแท้และชีวิตรักที่สมบูรณ์ หากปลอมเป็นหญิงก็จะเป็นนางแบบหุ่นดี หน้าตาดี น่าหลงใหล อายุไม่เกิน 35 ปี มีอาชีพ

ทหาร พยาบาล ครู หรืออาชีพที่มีรายได้น้อยเพื่อสร้างความสงสารและน่าเห็นใจ แต่ถ้าเป็นเพศทางเลือกก็จะภาพมักเป็นนายแบบ/นางแบบหุ่นดี แต่งกายดี เจาะกลุ่มรักร่วมเพศ มีอาชีพที่ค่อนข้างมั่นคง

2) เลือกช่องทางในการล่อเป้าหมาย

พื้นที่ในการก่อเหตุที่พบมากที่สุด คือ Facebook รองลงมาคือ Instagram และเว็บไซต์/แอพพลิเคชั่นหาคู่ เช่น Skout, Tinder, Badoo, OkCupid, Twoo, Thai date VIP, Tagged และ Match.com เป็นต้น

3) เลือกเป้าหมาย (เหยื่อ)

หลักการของการเหยื่อคือ การมองหา “คนขี้เหงา” ที่ต้องการหาเพื่อน / คู่ชีวิตในโลกออนไลน์ ต่อมาคือการประเมินศักยภาพทางการเงิน โดยสิ่งเหล่านี้จะถูกประเมินผ่านข้อมูลส่วนบุคคลที่แสดงในเครือข่ายสังคมออนไลน์ เช่น ชื่อ อายุ อาชีพ สถานะทางการเงิน สภาพคู่ครอง และวิถีการดำเนินชีวิต เป็นต้น รวมถึงการแชร์เรื่องราว/รูปภาพ หรือการแสดงความคิดเห็นบนโลกออนไลน์ด้วย ผู้ที่ขาดความรู้ในการอยู่รอดในโลกดิจิทัล เพราะนำข้อมูลส่วนบุคคล หรือวิถีชีวิต (lifestyle) เข้าสู่พื้นที่สาธารณะ อย่างไรก็ตามเพียงแค่การเปิดเผยข้อมูลส่วนบุคคลเป็นประจำ ประกอบกับเป็นคนขี้เหงา/ขี้สงสาร และหลงเชื่อที่จะตอบกลับข้อความจากแชทคนแปลกหน้า ถือว่ามีความเสี่ยงในการตกเป็นเป้าหมาย (เหยื่อ) ของนักหลอกลวงรัก (romance scam) ได้ถึง 70%

4) สร้างบทบาทเพื่อเข้าถึงเป้าหมาย

สร้างความน่าเชื่อถือทางอาชีพ ด้วยวิธีการส่งภาพหนังสือเดินทาง หรือบัตรเจ้าหน้าที่/พนักงาน ที่ผ่านการปลอมแปลงแล้วด้วยการตัดต่อภาพถ่าย และข้อมูลส่วนบุคคล ที่พบมากสุดคือ การแต่งกายด้วยเครื่องแบบทหาร วิศวกรสนาม ภาพถ่ายแท่นขุดเจาะน้ำมันกลางทะเล เว็บไซต์บริษัท/สถานที่ทำงานให้เป้าหมาย เพื่อให้ตรวจสอบได้ว่าตนได้ทำงานอยู่ที่แห่งนั้นจริง ด้วยการสร้างเว็บไซด์ปลอมขึ้นมา

ลักษณะร่วมของการแสดงบทบาทของนักหลอกลวงรักคือการสานสัมพันธ์เชิงชู้สาวจนกลายเป็น “คนรักในอุดมคติ” ด้วยการแสดงออกด้วยวิธีต่างๆ อาทิ การส่งข้อความทักทายและใช้คำพูดที่แสนหวาน ทำให้เป้าหมายรู้สึกว่า “เป็นคนสำคัญ” แสดงความเอาใจใส่ แสดงตัวว่ามีลักษณะของ “คนดี” เช่น การใช้คำพูดและสำนวนในแง่ดีที่จะสื่อนัยยะของการเป็นคนที่ซื่อสัตย์ จริงใจ และพึ่งพาได้ รวมถึงยอมรับข้อเสียและจุดบกพร่องของเป้าหมาย (เหยื่อ) ได้ทุกอย่าง มีการสานสัมพันธ์อย่างรวบรัดและรวดเร็วตั้งแต่ 2-3 วัน หรือไม่ก็เป็นการอดทนยอมใช้เวลาเพื่อสานสัมพันธ์ไปเรื่อยๆ จนกว่าเป้าหมาย (เหยื่อ) จะตกหลุมพราง บางครั้งยาวนานถึง 2 ปี โดยมีการส่งภาพถ่ายกิจกรรมระหว่างวันวิถีชีวิต ให้เหมือนเป็นการสนทนาแบบคู่รัก และแสดงให้เห็นว่ามีตัวตนอยู่จริง

5) การสร้างสถานการณ์

สถานการณ์ที่สร้างความสงสาร ความเห็นใจ และความหวังว่าจะได้พบกันจะถูกสร้างขึ้นเพื่อร้องขอเงินจากเป้าหมาย (เหยื่อ) อันนำไปสู่การสูญเสียทรัพย์สิน ตั้งแต่มีปัญหาทางการเงินเร่งด่วนจากสถานการณ์ฉุกเฉิน ชักชวนให้ร่วมลงทุนสร้างธุรกิจเพื่อใช้ชีวิตบั้นปลายร่วมกัน ส่งสิ่งของ/ทรัพย์สินมาให้แต่ติดปัญหาที่กรมศุลกากร สนามบิน หรือสถานีตำรวจ ต้องจ่ายเงินค่าธรรมเนียมเพื่อรับสิ่งของ/

ทรัพย์สินเหล่านั้น การขอแต่งงาน และส่งทรัพย์สินของหมั้นมาให้ยังประเทศไทย แต่ถูกยึดทรัพย์สิน ต้องจ่ายค่าธรรมเนียมก่อนอาจมีทีมงานแสดงตัวว่าเป็นเจ้าหน้าที่ของรัฐโทรศัพท์มาแจ้งค่าธรรมเนียม และเกิดปัญหาฉุกเฉินระหว่างการเดินทางมาพบกันและต้องการใช้เงินด่วน

เทคนิคการร้องขอเงินหรือผลประโยชน์ มี 2 เทคนิคหลัก คือ 1. Foot in the door technique (FITD) ตัวอย่างเช่น ครั้งแรกนักหลอกลวงรักจะขอให้เป้าหมาย (เหยื่อ) โอนเงินจำนวนไม่มากนักโดยมักอ้างว่าต้องใช้เงินด่วน ขอยืมเงินบางส่วน ซึ่งถ้าเหยื่อหลงเชื่อในครั้งแรก นักหลอกลวงรักก็จะเริ่มขอเงินจำนวนมากขึ้นในครั้งต่อไปด้วยการอ้างสถานการณ์อื่นๆ 2. Door in the face technique (DITF) ตัวอย่างเช่น นักหลอกลวงรักขอให้เหยื่อโอนเงินจำนวนมาก เมื่อเหยื่อปฏิเสธว่าไม่มีเงินมากขนาดนั้น เขาก็ลดจำนวนเงินลง โดยอ้างเหตุผลว่าได้เงินมาบางส่วนแล้วและต้องการอีกแค่บางส่วนเท่านั้น ซึ่งถ้าเหยื่อยอมโอนเงินในครั้งแรกก็จะมีการขอครั้งต่อไปเรื่อยๆ หรือบางครั้งนักหลอกลวงรักก็จะหายตัวไปทันที

6) บรรลุภารกิจทางการเงิน

นักหลอกลวงรักจะร้องขอให้มีการโอนเงินจาก 3 ช่องทางหลัก ดังนี้ 1. โอนเงินไปบัญชีธนาคารภายในประเทศไทย เป็นช่องทางที่จะถูกร้องขอบ่อยที่สุดถึง 90% และส่วนมากชื่อเจ้าของบัญชีเป็นชื่อคนไทย ซึ่งการโอนเงินนี้มักเกิดจากกรณีที่ผู้ร่วมขบวนการอ้างตัวว่าเป็นเจ้าหน้าที่ศุลกากร/เจ้าหน้าที่สนามบิน/เจ้าหน้าที่ส่งพัสดุ/เจ้าหน้าที่ของรัฐอื่นๆ โทรศัพท์แจ้งเป้าหมาย (เหยื่อ) ว่า “มีผู้ส่งพัสดุมูลค่ามหาศาลมาให้ ต้องจ่ายค่าธรรมเนียมเพื่อรับพัสดุดังกล่าว” และอีกกรณีที่พบได้คือนักหลอกลวงอ้างว่าเป็นบัญชีของเพื่อน หรือคนกลางที่สามารถส่งเงินต่อไปยังต่างประเทศได้อย่างรวดเร็ว 2. โอนเงินไปต่างประเทศ ส่วนใหญ่ประเทศปลายทางคือ ไนจีเรีย และมาเลเซีย ผ่านธนาคาร หรือสถาบันทางการเงินระหว่างประเทศโดยมักเป็นกรณีที่อ้างว่าเกิดเหตุฉุกเฉินระหว่างการติดต่อธุรกิจ หรือทำธุรกิจต่างประเทศ 3. มอบเงินด้วยตนเอง ด้วยเหตุผลว่าจะได้พบตัวจริงของคู่สนทนาจากออนไลน์ แต่เมื่อถึงเวลานัดหมายกันมักได้รับการปฏิเสธโดยอ้างเหตุผลว่าโดนกักตัวในสนามบินเพราะพกทรัพย์สินและเงินสดมาเป็นจำนวนมาก จึงให้ตัวแทน (แสดงเป็นเพื่อน นักการทูต เจ้าหน้าที่ศุลกากร) ถือทรัพย์สิน/เงินสดมาให้แทน และต้องมีการจ่ายเงินเพื่อแลกกับสิ่งของเหล่านั้น

เหยื่อหลายรายโดนหลอกซ้ำว่าได้จับตัวอาชญากรคนรักถูกจับแล้วแล้ว โดยผู้หลอกเหยื่อคนใหม่จะแสร้งว่าเป็นผู้มาช่วยเหลือให้อาชญากรหลุดพ้นคดี แต่จริงๆ แล้วก็เป็นอาชญากรด้วยกันเอง ทำให้เหยื่อยังติดกับวงจรของการหลอกลวงนี้ถูกหลอกซ้ำไปซ้ำมาเรื่อยๆ

2. กฎหมายและมาตรการเฝ้าระวังและเตือนภัยล่วงหน้าเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม

ผลการศึกษาสะท้อนให้เห็นถึงอุปสรรคที่เกิดจากข้อจำกัดของกฎหมายและกลไกในการป้องกันและปราบปรามพิศวาสอาชญากรรม เพื่อนำไปสู่การพัฒนากฎหมายและมาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมให้ดียิ่งขึ้น จึงเกิดเป็นผลการศึกษา 2 หัวข้อ คือ

1) กฎหมายและมาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมในปัจจุบัน

2) แนวทางพัฒนากฎหมายและมาตรการเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม

2.1. กฎหมายและมาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมในปัจจุบัน

พิศวาสอาชญากรรมเป็นความผิดที่ใช้ความรักเป็นสาระสำคัญในการหลอกลวง โดยอาศัยหลักการพื้นฐานทางจิตวิทยาร่วมกับการเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูล การวางแผน และการดำเนินขั้นตอนตามที่วางแผนไว้ เป็นการกระทำความผิดที่มีการกระทำผิดเป็นขบวนการ โดยลักษณะของการกระทำผิดเหล่านี้อาจเข้าข่ายความผิดตามกฎหมายได้หลายฐานอยู่แล้ว ไม่ว่าจะเป็นความผิดตามประมวลกฎหมายอาญา ความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ โดยในแต่ละประเด็นมีข้อสังเกตดังต่อไปนี้

1) ข้อกฎหมายที่เกี่ยวข้อง

คดีพิศวาสอาชญากรรมเป็นทั้งคดีที่มีรูปแบบการกระทำความผิดเป็นการเฉพาะตัว คือมีการใช้ “ความรัก” ในการหลอกลวงทรัพย์สินจากผู้เสียหาย ความผิดฐานแรกที่เกี่ยวข้องจึงเป็นความผิดฐานฉ้อโกง ทั้งยังเป็นความผิดต่อแผ่นดินฐานฉ้อโกงประชาชนเมื่อมีการกระทำผิดอย่างเป็นระบบต่อสาธารณชน ทั้งนี้มีการกระทำความผิดในลักษณะร่วมมือกันอย่างเป็นกระบวนการ โดยที่ผู้กระทำความผิดมักเป็นคนต่างชาติที่ร่วมมือกับคนไทยในการกระทำความผิด โดยคนต่างชาติกลุ่มนี้จะเข้ามาในราชอาณาจักร ความผิดที่เกี่ยวข้องประการต่อมาจึงเป็นความผิดตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ และจะใช้วิธีการให้คนไทยผู้ร่วมขบวนการเป็นคนติดต่อกับผู้เสียหาย หรือเป็นเจ้าของบัญชีที่ใช้ในการกระทำความผิดในไทย ดังนี้ก็จะเป็นความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ไม่ว่าจะเป็นฐานมีหรือใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบหรือฐานมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ นอกจากนี้ยังรวมถึงความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในเรื่องการนำข้อมูลที่บิดเบือนหรือปลอมหรือเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ด้วย โดยประการที่น่าจะก่อให้เกิดความเสียหายแก่ประชาชน และความผิดฐานนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น โดยเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง หรือได้รับความอับอายด้วย

2) ผู้เสียหาย

ผู้เสียหายในสังคมไทยไม่ค่อยอยากจะไปยุ่งยากอะไรเกี่ยวกับกระบวนการทางกฎหมายหรือการขึ้นศาลหรือเจอตำรวจซึ่งสร้างยุ่งยากและมีต้นทุนด้านเวลาแก่เหยื่อ ทั้งยังไม่มีความแน่ใจว่าคดีมีความคืบหน้าหรือในท้ายที่สุดจะได้ทรัพย์สินที่เสียไปกลับคืนมาหรือไม่ หากเป็นคนที่มีการศึกษามีหน้าตาในสังคมการเข้าไปแจ้งความแล้วบอกว่าตัวเองโดนหลอกมันทำให้เขาเสื่อมเสียชื่อเสียงเสื่อมเสียสถานะทางสังคมและอาจกระทบต่อหน้าที่การงานไปด้วย จากเงื่อนไขข้างต้นสะท้อนให้เห็นถึงความต้องการกระบวนการเยียวยาร้องทุกข์ที่มีลักษณะปกป้องเกียรติยศชื่อเสียงของเหยื่อ รวมไปถึงมีช่องทางร้องเรียนที่สามารถรักษาความเป็นส่วนตัวและรายงานความคืบหน้าของคดี ไปจนถึงมีประสิทธิผลในการบังคับใช้กฎหมายดำเนินคดีกับผู้กระทำความผิดและติดตามทวงทรัพย์สินกลับมาให้ผู้เสียหายได้

3) กระบวนการยุติธรรม

เมื่อบุคคลซึ่งเป็นผู้เสียหายก็มีสิทธิในการแจ้งความร้องทุกข์ต่อเจ้าหน้าที่ตำรวจ หรืออาจยื่นฟ้องคดีต่อศาล หรืออาจขอเข้าร่วมเป็นโจทก์กับพนักงานอัยการ แต่ในคดีพิศวาสอาชญากรรมขั้นตอนของการดำเนินคดีมักสะดุดและหยุดลงในชั้นของพนักงานสอบสวน เนื่องด้วยลักษณะการกระทำความผิดที่ไม่สามารถระบุได้อย่างแน่ชัดว่าเป็นกระทำผิดในขณะที่ผู้กระทำอยู่ในหรือนอกราชอาณาจักร อีกทั้งยังเป็นกรณีที่ผู้กระทำมักกระทำผิดด้วยการอำพรางตัวตนที่แท้จริงผ่านทางบัญชีปลอม Account หรือไอพี (IP Address) ต่างประเทศ ซึ่งทำให้ยากแก่การตรวจพิสูจน์และยืนยันตัวตนผู้กระทำความผิด

เมื่อผู้กระทำความผิดได้กระทำความผิดทั้งในและนอกราชอาณาจักร และยังเป็นความผิดที่อาจไม่สามารถระบุถึงสถานที่ในการกระทำความผิดได้อย่างชัดเจน ดังนั้น จึงมีมักเกิดปัญหาขึ้นว่าพนักงานสอบสวนท้องที่ใดควรจะเป็นผู้มีอำนาจสอบสวน เพราะการสอบสวนโดยพนักงานสอบสวนที่ไม่มีอำนาจตามกฎหมายจะส่งผลให้การสอบสวนนั้นเป็นการสอบสวนที่ไม่ชอบด้วยกฎหมาย พนักงานอัยการไม่มีอำนาจฟ้อง และศาลต้องยกฟ้องคดีนี้ในที่สุด

4) ขั้นตอนในการสอบสวน

พนักงานสอบสวนเมื่อเริ่มทำการสอบสวนเพื่อให้ได้มาซึ่งตัวผู้กระทำความผิด โดยการรวบรวมพยานหลักฐานเพื่อเอาผิด และการจับกุมตัวผู้กระทำผิดมารับโทษ เมื่อนำมาพิจารณากับกระบวนการพิจารณาคดีอาญาทั้งเรื่องหลักกฎหมายและการปฏิบัติงานของเจ้าหน้าที่ จะเห็นได้ว่าอุปสรรคในการรวบรวมพยานหลักฐานของพนักงานสอบสวน สามารถแบ่งออกเป็น 3 กรณี กล่าวคือ 1) อุปสรรคด้านเวลา 2) อุปสรรคด้านทรัพยากร ไม่ว่าจะเป็นด้านเครื่องมือ กำลังพล หรืองบประมาณ และ 3) อุปสรรคด้านการติดตามตัวผู้กระทำความผิด

นอกจากนี้อุปสรรคสำคัญอย่างหนึ่งในการดำเนินคดี Romance Scam คือ หากเจ้าพนักงานตำรวจตั้งฐานความผิดเป็นคดีฉ้อโกงย่อมส่งผลให้คดี Romance Scam เป็นความผิดที่ยอมความได้ ดังนั้น หากผู้เสียหายตัดสินใจถอนคำร้องทุกข์หรือยุติการดำเนินคดี เจ้าพนักงานตำรวจก็จะไม่สามารถดำเนินคดีนี้ต่อไปได้ ซึ่งสามารถแก้ไขได้ด้วยการดำเนินคดีนี้ต่อในฐานะที่ผู้กระทำความผิดเป็นองค์กรอาชญากรรมข้ามชาติ อันจะทำให้คดี Romance Scam กลายเป็นความผิดอาญาแผ่นดิน และเจ้าพนักงานตำรวจสามารถดำเนินคดีนี้ต่อไปได้แม้ว่าผู้เสียหายจะถอนคำร้องทุกข์หรือยุติการดำเนินคดีก็ตาม

การขอความร่วมมือเพื่อการขยายผลสืบสวนต่างประเทศ (MLAT - Mutual Legal Assistance Treaty) กับรัฐบาลต่างชาติเพื่อขอให้ผู้ดูแลระบบในต่างประเทศช่วยเหลือ กรณีที่มีการกระทำผิดในต่างประเทศเราจะขอให้โครงข่ายสัญญาณโทรศัพท์ในต่างประเทศนั้นทำการพิสูจน์ทราบว่า IP นี้ในวันเวลานั้นใครเป็นคนใช้ แต่ขอความร่วมมือไปสองปียังไม่ได้กลับมาเลยเรื่องพยานหลักฐาน เพราะฉะนั้นอะไรที่เกี่ยวข้องกับเรื่องนี้คาดหวังยากมาก

5) การจับกุม

พนักงานสอบสวนแทบจะไม่สามารถตามผู้กระทำความผิดที่แท้จริงมาลงโทษได้เลย แต่กลับสามารถตามจับได้เฉพาะผู้ร่วมกระทำความผิดที่ได้แต่งงานหรืออยู่กินฉันสามีภรรยากับผู้กระทำความผิดเท่านั้น ทำให้ในการสืบสวนสอบสวน พนักงานสอบสวนจึงทำได้เพียงการสืบทางเส้นทางการเงินของผู้ร่วมกระทำความผิดที่เป็นเจ้าของบัญชี และนำไปขยายผลเพื่อสืบหาตัวผู้กระทำความผิด

แต่ก็มักทำได้ยาก เนื่องจากผู้กระทำความผิดมักอาศัยอยู่นอกราชอาณาจักร หรือไม่สามารถหาหลักฐานมายืนยันได้ว่าผู้กระทำความผิดที่แท้จริงคือใคร เนื่องจากการปลอมแปลงตัวตนและการข้อจำกัดด้านความรู้ความเชี่ยวชาญของเจ้าหน้าที่ ข้อจำกัดด้านอุปกรณ์ และทรัพยากรทั้งหลายรวมถึงเวลา

6) ชั้นกระบวนพิจารณาของศาล

เนื่องจากในคดีอาญามีหลักการ “ต้องพิสูจน์จนสิ้นสงสัย” ทำให้เมื่อพนักงานสอบสวนไม่สามารถหาพยานหลักฐานมายืนยันจนศาล “สิ้นสงสัย” ว่าจำเลยเป็นผู้กระทำความผิดที่แท้จริงตามที่ถูกกล่าวหาได้ ไม่สามารถยืนยันได้ว่าจำเลยเป็นบุคคลที่พูดคุยกับผู้เสียหาย ทำให้ “เมื่อกรณียังเป็นที่สงสัย” ศาลก็ต้องปล่อยตัวจำเลยนั้นไป และส่งผลให้มิอาจมีคำสั่งให้บังคับคดียึดทรัพย์ หรือให้ชดใช้สินไหมทดแทนในทางแพ่งได้

7) การบังคับคดี

การบังคับคดีให้ผู้เสียหายได้รับการคืนเงินต้องสืบทรัพย์ให้เห็นว่ากระจายไปอยู่ที่ใดบ้าง ซึ่งการติดตามหาจะทำได้ยาก ยิ่งส่วนใหญ่ผู้กระทำผิดเป็นต่างชาติจึงยากขึ้นไปอีกว่าจะไปสืบทรัพย์อย่างไร หรือถ้าคนไทยเปิดบัญชีให้จะบังคับคดีได้ไหมก็ไม่แน่ใจเหมือนกันว่าพอตำรวจไปอายัดบัญชีแล้วจะดำเนินการอย่างไรต่อจะมีการดำเนินคดีอาญาฟอกเงินหรืออายัดบัญชีและทรัพย์สินไว้ด้วย หาไม่แล้วทรัพย์สินก็จะถูกยักย้ายถ่ายโอนจนยากจะติดตามกลับมาชดใช้ให้ผู้เสียหาย

8) มาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมโดยอาศัยความร่วมมือระหว่างรัฐกับเอกชน

กฎหมายได้เปิดโอกาสให้รัฐดำเนินการ แต่ยังมีข้อจำกัดในการแก้ไขปัญหา เพราะกฎหมายข้อมูลส่วนบุคคลก็ดี กฎหมายความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติคอมพิวเตอร์ก็ดีต้องสร้างปัจจัยแวดล้อมส่งเสริมให้คนเข้ามาใช้มีความเชื่อถือมั่นใจว่าเข้ามาแล้วปลอดภัย หากสร้างมาตรการให้ผู้ประกอบการผู้ให้บริการต้องโทษทางกฎหมายจากการไม่ให้ความร่วมมือในการสอดส่องและนำข้อมูลปลอมเท็จบิดเบือนออกจากระบบทั้งที่ไม่ได้ทำความผิดอะไรเอง หรือใช้มาตรา 15 ไปจำคุกในฐานะตัวการร่วมกระทำความผิดตามมาตรา 14 หรือมาตรา 19 ไปบีบให้ต้องคอยสอดส่องข้อมูลในระบบและลบทิ้งตลอดเวลา ย่อมไม่เป็นธรรมเพราะว่าในต่างประเทศเองเขาก็ไม่ได้ให้ผู้ให้บริการมารับ ซึ่งจะกระทบต่อการส่งเสริมเศรษฐกิจดิจิทัลเพราะเป็นการสร้างต้นทุนมหาศาลให้ผู้ประกอบการ

2.2. แนวทางพัฒนากฎหมายและมาตรการเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม

ผลการวิจัยที่เป็นแนวทางในการป้องกันและปราบปรามพิศวาสอาชญากรรมมี 2 แนว คือ การพัฒนามาตรการภายในประเทศให้รองรับปัญหาได้ดีมากยิ่งขึ้น และการพัฒนาความร่วมมือระหว่างประเทศ

1) การพัฒนามาตรการภายในประเทศ

การพัฒนามาตรการที่พึงประสงค์ได้แก่

- การสร้างภูมิคุ้มกันในเชิงการรณรงค์ การประชาสัมพันธ์ การสร้างความเชื่อมั่นในกระบวนการยุติธรรม ให้ประชาชนรู้ มีช่องทางเพิ่มมากขึ้นในการแจ้งข่าวสารการร้องทุกข์หรือการเตรียมบุคลากรให้พร้อม
- บุคลากรอาจจะต้องมีทั้งหญิงและชายมีความหลากหลายมากยิ่งขึ้น เพราะบางครั้งเรื่องพวกนี้เป็นความผิดเกี่ยวกับเพศด้วย มันเกี่ยวพันกับทางเพศ การที่ผู้เสียหายจะกล้าเข้ามาแจ้งความร้องทุกข์
- การออกแบบวิธีการร้องทุกข์และดำเนินคดีที่ไม่ต้องเปิดเผยตัวตนหรือเป็นช่องทางร้องเรียนประสานงานออนไลน์
- การพัฒนากระบวนการที่สามารถช่วยเหลือเยียวยาเหยื่อในความเสียหายทางแพ่งและการติดตามทรัพย์สินกลับคืนมาชดใช้สินไหมทดแทน
- การสร้างบุคลากรเพิ่ม มิใช่เพียงสร้างศูนย์ประสานงานแต่บุคลากรไม่เพียงพอ การสร้างบุคลากรที่เข้าใจอาชญากรรมเกี่ยวกับคอมพิวเตอร์ในภาพรวมทั้งหมด สั่งสมความรู้บุคลากรในกระบวนการยุติธรรมและสร้างบุคลากรใหม่ด้วย เข้าใจใน 3-D หนึ่ง Digital Context คือบริบททางเทคโนโลยี สอง คือ Digital Fact รู้ข้อเท็จจริงทางเทคโนโลยี สาม Digital Way คือ วิถีทางทางดิจิตอล
- การทำงานเชิงรุกในหน่วยงานรัฐโดยเฉพาะหน่วยงานที่บังคับใช้กฎหมาย มีการเผยแพร่ข้อมูลในการดำเนินการว่าถ้าตกเป็นเหยื่อหรือมีข้อสงสัยว่าเราจะตกเป็นเหยื่อเราจะดำเนินการยังไงได้บ้าง และมีการรายงานความคืบหน้าว่ารัฐมีการดำเนินการหลังการร้องทุกข์ไปถึงขั้นใดแล้ว
- สร้างมาตรฐานว่าเว็บไหนที่มีมาตรฐานความปลอดภัยเพื่อสร้างความมั่นใจให้ประชาชนเข้าใช้ระบบหรือแอพลิเคชันเหล่านั้น
- มาตรการป้องกันไม่ให้เกิดอาชญากรรมซ้ำอีก คือ การให้ความรู้เผยแพร่ความรู้ความเข้าใจเกี่ยวกับอาชญากรรมไซเบอร์ เตือนภัยเรื่องการล่อลวงรูปแบบต่างๆ หรือทำละครออกมาเป็นข้อคิดให้ประชาชน และการให้กำลังใจเหยื่อเพื่อดำเนินคดีไม่ถอดใจหรือใช้ชีวิตต่อไปได้ไม่สิ้นหวัง

2) การพัฒนาความร่วมมือระหว่างประเทศ

การพัฒนาความร่วมมือระหว่างประเทศ มีศูนย์ประสานงานข้อมูลและความสัมพันธ์ระหว่างประเทศ เรื่องผ่านความร่วมมือระหว่างประเทศทางอาญา (Mutual Legal Assistance Treaty - MLAT) หาเคยได้พยานหลักฐานมาในเชิงสืบสวนนั้น อาจจะเป็นความสัมพันธ์ส่วนบุคคล (connection) ที่ให้มา หากมี connection ติดต่อจากผู้ให้บริการและหน่วยงานบังคับใช้กฎหมายในต่างประเทศหรือระหว่างประเทศได้เลยก็จะรวดเร็วแก้ปัญหาได้ ยิ่งถ้าเกิดมีการรับรองสถานะของพยานหลักฐานที่ได้มาด้วยช่องทางนี้ชัดเจนเข้าสำนวนได้

การเสริมศักยภาพในระดับประเทศเพื่อรองรับภัยคุกคามข้ามชาติแบบบูรณาการกระบวนการยุติธรรมทั้งหมด สามารถเฝ้าระวังติดตามเป็นบุคคลต้องสงสัยสร้างเป็นรายชื่อเฝ้าระวัง (Watch List) ต้องประสาน ตำรวจสากล เพื่อดำเนินคดีหรือจับมาให้ได้ หรือถ้าไม่ได้ก็ต้องขอความร่วมมือให้ เกิดสัมฤทธิ์ผลที่แท้จริง

มาตรการทั้งหลายยังต้องเผชิญกับความท้าทายจากภัยที่มีลักษณะข้ามพรมแดนแต่รัฐทั้งหลายยังมีข้อจำกัดเรื่องเขตอำนาจศาล ความสลับซับซ้อนของกระบวนการยุติธรรม และประสิทธิภาพของการปฏิบัติหน้าที่ของเจ้าพนักงาน ดังนั้น แนวทางในการสร้างความเข้มแข็งให้กับผู้บังคับใช้กฎหมาย ผู้ดูแลระบบ และกลุ่มเสี่ยงที่อาจตกเป็นเหยื่อจึงมีความสำคัญ ดังจะกล่าวถึงต่อไปนี้

3. แนวทางเพิ่มความตระหนักให้ประชาชนกลุ่มเสี่ยงตกเป็นเป้าหมายพิศวาสอาชญากรรม ให้รู้เท่าทันพิศวาสอาชญากรรม

การสร้างความตระหนักถึงภัยคุกคามไซเบอร์ในรูปแบบของพิศวาสอาชญากรรมแก่ผู้บังคับใช้กฎหมาย ผู้ดูแลระบบ และประชาชนโดยเฉพาะกลุ่มเสี่ยงที่มีความรู้ความเข้าใจต่อเทคโนโลยีและการรับรู้ข้อมูลข่าวสาร โดยการรู้เท่าทันกลยุทธ์ของอาชญากรจัดเป็นประเด็นที่สำคัญเนื่องจากอาชญากรรมประเภทนี้มาในรูปแบบการล่อลวงโดยอำพรางและสร้างความผูกพันทางจิตใจโดยอาศัยการสื่อสารผ่านอินเตอร์เน็ต การแสดงให้เห็นถึงกลยุทธ์ที่อาชญากรแสดงออกมาหน้าฉากให้เหยื่อเห็นกับความจริงหลังฉากที่อาชญากรหลบซ่อน จะเป็นการล้างภาพลวงตาและสร้างความเข้มแข็งให้กับกลุ่มเสี่ยงที่จะตกเป็นเหยื่อ

3.1 กลุ่มเป้าหมาย

กลุ่มเสี่ยงที่จะตกเป็นเป้าหมายและต้องเตือนภัยให้เฝ้าระวัง ก็คือ กลุ่มคนที่เข้าไปแสวงหาความรักความสัมพันธ์ในอินเตอร์เน็ตโดยมีการเปิดเผยข้อมูลส่วนตัวในพื้นที่สาธารณะ

เจ้าพนักงานของรัฐที่ทำหน้าที่บังคับใช้กฎหมายเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม อันประกอบไปด้วย เจ้าหน้าที่ตำรวจ เจ้าพนักงานคดีพิเศษ รวมไปถึงพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ

ผู้ดูแลระบบคอมพิวเตอร์ ซึ่งมีความสามารถในการรวบรวมพยานหลักฐานในกรณีเกิดการกระทำความผิดตามนัยของกฎหมาย

3.2 กลยุทธ์ในการสร้างหน้าฉากคนดีเพื่อหลอกลวงอำพรางหลังฉากอาชญากร

การสร้างความตระหนักรู้ผ่านการเผยแพร่งานวิจัยและเปิดเผยตัวตนที่แท้จริงของอาชญากรในแต่ละขั้นตอนเพื่อให้เห็นความจริงหลังฉากของอาชญากรย่อมทำให้ประชาชนสามารถเข้าใจถึงลักษณะของพิศวาสอาชญากรรมและรู้เท่าทันอาชญากรที่มาล่อลวงได้ดียิ่งขึ้น โดยข้อมูลที่จำเป็นที่สุดคือ ตัวตนหน้าฉาก-หลังฉาก ของอาชญากร ดังนี้

	หน้าฉาก	หลังฉาก
1. ภาพถ่ายบนโปรไฟล์	**โปรไฟล์ผู้ชาย** - ลักษณะภาพมักเป็นคนผิวขาวที่ดูมีเสน่ห์ อบอุ่น ภูมิฐาน มีฐานะ และมีท่าทางเป็นคนดี - อายุประมาณ 40 – 50 ปี - เป็นคนอเมริกัน อังกฤษ เยอรมัน หรือแคนาดา จีน สิงคโปร์ หรือเป็นลูกครึ่งไทยกับชาติอื่น	กลุ่ม ‘นักต้มตุ๋น’ อาชญากรจากหลายประเทศ เช่น ไนจีเรีย กานา มาเลเซีย รัสเซีย สหราชอาณาจักร ตุรกี เป็นต้น เริ่มจากการขโมยภาพถ่ายบุคคลที่มีลักษณะตรงตามที่บรรยายใน*หน้าฉาก*จากเว็บไซต์เครือข่ายสังคมออนไลน์ต่างๆ เรียบเรียงคำโปรยแนะนำตนเองให้ดูน่าสนใจ ด้วยการคัดลอกข้อความมาเป็นทอดทอดจากอินเตอร์เน็ต และกลุ่มอาชญากรเดียวกัน
	โปรไฟล์ผู้หญิง *เป้าหมาย – ผู้ชาย* - ภาพมีลักษณะเป็นนางแบบหุ่นดี หน้าตาดี น่าหลงใหล - อายุไม่เกิน 35 ปี - เป็นคนอเมริกัน โรมาเนีย หรือลูกครึ่งไทยกับชาติอื่น *เป้าหมาย – ผู้หญิง* - ภาพถ่ายดูมีอายุ แต่งกายดี ดูมีฐานะและน่าเชื่อถือ เป็นคนไทย เวียดนาม	
	โปรไฟล์เพศทางเลือก - มีลักษณะคล้ายนายแบบหุ่นดี แต่งกายดี	

	หน้าฉาก	หลังฉาก
2.การแนะนำตัวเองอาชีพการงานและสถานะทางสังคม	**โปรไฟล์ผู้ชาย** - มีอาชีพทหาร วิศวกร นักธุรกิจ (โดยเฉพาะเกี่ยวกับน้ำมัน ปิโตรเลียม) แพทย์ หรือเจ้าหน้าที่รัฐ - สถานภาพโสด หรือภรรยาเสียชีวิตแล้ว - อยากมีชีวิตรักที่สมบูรณ์ ตามหารักแท้ **โปรไฟล์ผู้หญิง** <u>*เป้าหมาย – ผู้ชาย*</u> - มีอาชีพทหาร พยาบาล ครู พนักงาน - สถานภาพโสด หรือ หย่าร้าง - อยากมีคู่แท้ ที่เข้าใจและดูแลกันละกัน <u>*เป้าหมาย – ผู้หญิง*</u> - สถานภาพแม่หม้าย ที่เคยมีสามีเป็นคนไทย หรือฝรั่งที่ทิ้งมรดกไว้มหาศาล **โปรไฟล์เพศทางเลือก** - มีอาชีพดีไซน์เนอร์ แพทย์ นักธุรกิจ	นักตุ้มตุ๋น ‘หลอกลวงรัก’ เป็นอาชีพหนึ่งในไนจีเรียที่ทำเงินได้อย่างมหาศาล ซึ่งผู้ที่จะเป็นนักต้มตุ๋นต้องมีทักษะดังนี้ - ทักษะทางคอมพิวเตอร์ และการติดต่อสื่อสารบนโลกออนไลน์ - สามารถสร้างโปรไฟล์ปลอมได้ - ทักษะทางสังคมที่ใช้พูดคุยกับเหยื่อให้ราบรื่น องค์กรอาชญากรรมดังกล่าวแบ่งได้เป็น 3 กลุ่ม ดังนี้ 1. ทำงานคนเดียว (พบค่อนข้างน้อย) 2. ทำเป็นกลุ่มเล็ก 3. ทำเป็นเครือข่ายใหญ่ (แบ่งหน้าที่การทำงานอย่างชัดเจน สามารถเลื่อนขั้นไปตำแหน่งอื่นๆ ได้ มีการแข่งขันเพื่อให้ได้รับสวัสดิการที่ดีในใช้ชีวิต)
3. การสร้างความเชื่อมั่น และความไว้เนื้อเชื่อใจ	ความเอาใจอย่างสม่ำเสมอของคู่สนทนาที่สร้างความผูกพันฉันชู้สาวอย่างรวดเร็ว บางคนใช้เวลาเพียง 2 สัปดาห์ บางคนนานหลายเดือน หรือยาวนานเป็นปี ดังเช่น - ข้อความแสนหวานที่ถูกส่งมาอย่างสม่ำเสมอ เช่น sweetheart, honey, my love, good night เป็นต้น - ความเอาใจใส่ ความเป็นห่วงเป็นใยทุกสถานการณ์ - แสดงตัวว่าเป็น “คนดี”	การกระทำในขั้นนี้มีการแบบแผนมาแล้วระดับหนึ่ง เนื่องจากหน้าที่หลักของนักต้มตุ๋น คือ การส่งความให้เป็นกิจวัตร การรอคอย และการสร้างความไว้วางใจ การสร้างความสัมพันธ์แบบซาบซึ้ง ถูกนำมาใช้ในขั้นตอนนี้เพื่อให้เป้าหมาย (เหยื่อ) เชื่อว่าคู่สนทนาเป็นคนดี ไว้วางใจได้ และมีทรัพย์สิน จริง ซึ่งจะนำไปสู่การชักจูง และโน้มน้าวใจได้ง่ายยิ่งขึ้น ทั้งนี้ปฏิบัติการในขั้นนี้มักเกิดจากการเรียนรู้จากโปรไฟล์ และสิ่ง

	หน้าฉาก	หลังฉาก
	- คำกล่าวอ้างว่าอยากมีรักมั่นคง ร่วมกันสร้างฝัน และใช้บั้นปลายชีวิตร่วมกัน - บางครั้งมีการส่งรูปภาพกิจวัตรในแต่ละวัน มักเป็นกิจกรรมที่มีลักษณะของ ‘กิจกรรมคนรวย’ เช่น ขับรถหรู ใช้สิ่งของแบรนด์เนม เข้าฟิสเนต - บางครั้งมีการส่งสิ่งของให้ เช่น ตุ๊กตา ดอกไม้ พร้อมกับการ์ดข้อความหวานซึ้งที่พร่ำบอกรัก - บางครั้งมีการพูดคุยทางโทรศัพท์	ต่างๆ ที่เป้าหมาย (เหยื่อ) ได้แชร์และโพสต์ลงไปในเครือข่ายสังคมออนไลน์ สิ่งเหล่านั้นจะเป็นประโยชน์อย่างยิ่งสำหรับนักต้มตุ๋นที่จะใช้ในการพิชิตใจเป้าหมาย (เหยื่อ) กลวิธี และเทคนิคต่างๆ ที่เหล่านักต้มตุ๋นใช้แล้วได้ผลลัพธ์ดีจะถูกถ่ายทอดและสอนให้แก่รุ่นสู่รุ่นไปเรื่อยๆ
4. การสร้างสถานการณ์ต่างๆ เพื่อหลอกเอาทรัพย์สิน	จากความสัมพันธ์ที่หอมหวานขยับเข้าสู่ ‘การพิสูจน์รักแท้’ ด้วยการร้องขอให้โอนเงิน หรือจ่ายเงิน เรื่องราวสถานการณ์ที่คู่สนทนาได้พร่ำบอกเพื่อใช้เป็นเหตุผลในการขอทรัพย์สินถูกใช้บ่อยครั้ง ดังนี้ - มีปัญหาทางการเงินเร่งด่วน เช่น ค่ารักษาพยาบาล ค่าเล่าเรียน ธุรกิจถูกโกง/มีปัญหา เกิดอุบัติเหตุ ซื้อตั๋วเครื่องบิน/ทำวีซ่าเพื่อเดินทางมาพบกัน ค่าเช่าห้องพัก เป็นต้น - ชักชวนให้ร่วมลงทุนสร้างธุรกิจ - ส่งสิ่งของ/ทรัพย์สินมาให้ แต่ติดปัญหาที่กรมศุลกากร สนามบิน หรือสถานีตำรวจ ต้องจ่ายเงินค่าธรรมเนียมเพื่อรับสิ่งของ/ทรัพย์สินเหล่านั้น - ขอแต่งงาน และส่งทรัพย์สินของหมั้นมาให้ยังประเทศไทย แต่ถูกยึดทรัพย์สิน ต้องจ่ายค่าธรรมเนียมก่อน (แสดงตัวว่าเป็นเจ้าหน้าที่ของรัฐโทรศัพท์มาแจ้งค่าธรรมเนียมต่างๆ)	ในวงการอาชญากรรมนี้ ‘การทำยอด’ หรือ ‘การปั่นยอด’ เป็นแรงจูงใจสำคัญของนักต้มตุ๋น เพื่อให้ได้รับสวัสดิการที่ดี (ได้เสื้อผ้าใหม่ ห้องพักในโรงแรม และดื่มไวน์สุดหรูใน “VVIP” คลับ) และเลื่อนตำแหน่งงาน ดังนั้นหากได้รับเงินโอนจากเหยื่อมากเท่าใดยิ่งเป็นสิ่งที่ดีมากเท่านั้น เช่น เป้าหมายทั่วไปต้องเงินอย่างน้อย 2-3 ครั้งต่อสัปดาห์ หรือแต่ละเดือนต้องได้เงิน 1,000 ดอลลาร์ เทคนิคที่ถูกนำไปใช่ใน ‘การพิสูจน์รักแท้’ มี 2 เทคนิค คือ 1.Foot in the door technique (FITD) เป็นการร้องขอเงินจำนวนน้อยๆ ได้ถ้ารับเงินครั้งแรกแล้ว จะเพิ่มจำนวนเงินขึ้นเรื่อยๆ ด้วยข้ออ้างต่างๆ 2.Door in the face technique (DITF) เป็นการร้องขอเงินจำนวนมากแบบสุดโต่งในครั้งแรก เมื่อเหยื่อปฏิเสธว่าไม่มีเงินจำนวนนั้น

	หน้าฉาก	หลังฉาก
	- เกิดปัญหาฉุกเฉินระหว่างการเดินทางมาพบกันและต้องการใช้เงินด่วน เช่น ทรัพย์สินจำนวนมากที่นำมาถูกยึด กระเป๋าเงินหาย ถูกกักตัวที่สถานบิน บัตรเครดิตใช้งานไม่ได้ เป็นต้น สถานการณ์ต่างๆ เหล่านี้มักมาพร้อมกับภาพถ่ายที่ว่าเกิดเหตุการณ์นั้นขึ้นจริง รวมทั้งภาพถ่ายทรัพย์สินต่างๆ เพื่อแสดงว่าคนนั้นมีทรัพย์สินที่กล่าวอ้างอยู่จริง	จึงค่อยๆ จำนวนลงตามความเป็นไปได้ของเหยื่อแต่ละคน
5.บรรลุภารกิจทางการเงิน	การร้องขอเงินนั้นเป็นไปได้ 3 วิธีการ ดังนี้ 1. การโอนเงินไปต่างประเทศ ส่วนใหญ่ประเทศปลายทางคือ ไนจีเรีย และมาเลเซีย 2. การโอนเงินไปบัญชีธนาคารภายในประเทศไทย ซึ่งหลายครั้งเจ้าของบัญชีเป็นชื่อคนไทย 3. การมอบเงินด้วยตนเอง ด้วยเหตุผลว่าจะได้พบตัวจริงของคู่สนทนาจากออนไลน์ แต่เมื่อถึงเวลานัดหมายกันมักได้รับการปฏิเสธโดยอ้างเหตุผลว่าโดนกักตัวในสนามบินเพราะพกทรัพย์สินและเงินสดมาเป็นจำนวนมาก จึงให้ตัวแทน (เพื่อน นักการทูต เจ้าหน้าที่ศุลกากร) ถือทรัพย์สิน/เงินสดมาให้แทน และต้องมีการจ่ายเงินเพื่อแลกกับสิ่งของเหล่านั้น	เบื้องหลังกระบวนการ รับเงินนั้นเป็นไปได้ 2 แนวทางหลัก 1. นักต้มตุ๋น ทำงานคนเดียว มักจะให้โอนไปยังต่างประเทศด้วยการส่งภาพถ่ายเป็นหลักฐานของการมีตัวตน มีทรัพย์สินต่างๆ อาจใช้การปลอมแปลงเอกสารใบเสร็จต่างๆ ด้วย 2. นักต้มตุ๋นที่เป็นองค์กร/เครือข่าย มักใช้วิธีการแสดงบทบาทสมมุติหลายบทบาท จากเหล่านักต้มตุ๋นในองค์กร เช่น การอ้างตนว่าเป็นเพื่อน เจ้าหน้าที่รัฐ นักการทูต หรือบุคคลอื่นๆ โดยคนนั้นอาจเป็นชาวต่างชาติ หรือคนไทยก็ได้ไม่มีแบบแผนที่ชัดเจน คนเหล่านั้นมีหน้าที่รับเงินที่ถูกโอนมา หรือบางครั้งต้องเป็นผู้เจราจาต่อรองเพื่อให้เป้าหมาย (เหยื่อ) เชื่อว่าสถานการณ์ที่นักต้มตุ๋นคนหลักได้สร้างไว้เป็นเรื่องจริง ซึ่งที่พบได้บ่อยครั้งคือ การอ้างว่าเป็นเจ้าหน้าที่ศุลกากร แจ้งว่าพัสดุที่ส่งมาเป็นมีมูลค่ามหาศาลต้องจ่ายค่าธรรมเนียมเพื่อรับพัสดุนั้น

	หน้าฉาก	หลังฉาก
		การเปิดบัญชีในประเทศไทยเป็นไปได้ 3 กรณีหลัก คือ 1.ถูกขโมยข้อมูลใช้เปิดบัญชี 2.ถูกหลอกให้เปิดบัญชี 3.สมรู้ร่วมคิดกับเครือข่ายอาชญากร

3.3 แนวทางการป้องกันตนเองของประชาชน

ประชาชนพึงระวังรักษาข้อมูลส่วนบุคคลอ่อนไหวที่ผู้ใช้อินเตอร์เน็ตไว้ไม่เปิดเผยสู่พื้นที่สาธารณะโดยเฉพาะบนโลกไซเบอร์ อันจะนำมาซึ่งความเสี่ยงในการตกเป็นเป้าหมายของเหล่าอาชญากร ได้แก่ ชื่อเต็ม สถานะความสัมพันธ์ รสนิยมทางเพศ ID ที่อยู่จดหมายอิเล็กทรอนิกส์และในเครือข่ายสังคมออนไลน์ หรือบล็อก สิ่งที่สนใจหรือกิจกรรมที่ชื่นชอบ รูปภาพและวิดีโอของตัวเอง หากจะเปิดเผยต้องจำกัดวงในการเข้าถึงเพียงคนที่รู้จักและไว้ใจได้ในชีวิตจริงเท่านั้น

3.4 แนวทางเฝ้าระวังและเตือนภัยโดยผู้ดูแลระบบและผู้บังคับใช้กฎหมาย

แนวทางในการป้องกันพิศวาสอาชญากรรมทางคอมพิวเตอร์ซึ่งเป็นภัยคุกคามทางเทคโนโลยีอันเหมาะแก่การเป็นมาตรการเตือนภัยล่วงหน้าโดยเอกชนผู้ดูแลระบบและหน่วยงานบังคับใช้กฎหมายภาครัฐเพื่อพิทักษ์สิทธิประชาชน โดยข้อมูลที่ควรเผยแพร่ หรือเฝ้าระวังเตือนภัยให้ประชาชนตระหนักรู้มีดังต่อไปนี้

<u>การแจ้งเตือนเมื่อประชาชนเผยข้อมูลส่วนบุคคลอ่อนไหวในอินเตอร์เน็ตอันนำมาซึ่งความเสี่ยง</u> อันได้แก่ ชื่อเต็ม สถานะความสัมพันธ์ รสนิยมทางเพศ ID ที่อยู่จดหมายอิเล็กทรอนิกส์และในเครือข่ายสังคมออนไลน์ หรือบล็อก สิ่งที่สนใจหรือกิจกรรมที่ชื่นชอบ รูปภาพและวิดีโอของตัวเอง โดยปราศจากการบริหารความเป็นส่วนตัวมิให้รั่วไหลสู่คนแปลกหน้า

<u>การเตือนประชาชนให้รู้เท่าทันกลยุทธ์การล่อลวงที่ทำให้เหยื่อเสียทรัพย์</u> กลยุทธ์ที่อาชญากรใช้การเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูล การวางแผน และการดำเนินขั้นตอนตามที่วางแผนไว้หรือเรียกรวมๆ ว่า “วิศวกรรมสังคม” (Social Engineering) โดยกระบวนการล่อลวงนี้สามารถแบ่งได้เป็นขั้นตอนหลัก 5 ขั้นตอน ได้แก่ 1.การอำพรางปลอมโปรไฟล์ 2.การเลือกช่องทางในการล่อเป้าหมาย 3.วิธีการเลือกเหยื่อเป้าหมาย 4.การสร้างบทบาทเพื่อเข้าถึงเป้าหมาย 4.การสร้างสถานการณ์วิกฤติฉุกเฉิน 5.การทำให้เสียทรัพย์สินเงินทอง

4. ข้อเสนอแนะจากการศึกษา

หลังจากได้ศึกษาวิจัยไปจนครบถ้วนแล้วเกิดข้อเสนอแนะในการพัฒนากฎหมายและมาตรการเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรมในโลกไซเบอร์ รวมถึงแนวทางการสร้างความตระหนักรู้ให้กับประชาชนกลุ่มเสี่ยง ดังนี้

4.1 ข้อเสนอแนะเชิงนโยบาย

แม้มาตรการทางกฎหมายและกระบวนการยุติธรรมที่เกี่ยวข้องยังมีข้อจำกัดในการติดตามตัวผู้กระทำความผิดมาดำเนินคดีทางอาญาและชดเชยความเสียหายให้กับเหยื่อ ไม่ว่าจะเป็นความเสียหายทางทรัพย์สินที่ติดตามได้ยากเนื่องจากมักมีการยักย้ายถ่ายโอนไปยังผู้อื่นหรือนอกประเทศไทย ยิ่งถ้าเป็นเสียหายต่อชีวิตและทางเพศย่อมเป็นการยากที่ชดเชยให้กลับมาคืนสภาพเดิม ทั้งยังพบว่าผู้ล่อลวงจำนวนมากปฏิบัติการจากต่างประเทศซึ่งเพิ่มความลำบากให้กับกระบวนการยุติธรรมทางอาญาที่ต้องผสานความร่วมมือไปยังประเทศเจ้าของเขตอำนาจให้ส่งผู้ร้ายข้ามแดนหรือยึดทรัพย์สินกลับมาชดเชยความเสียหายให้กับเหยื่อ การสร้างมาตรการป้องปรามโดยผู้ดูแลระบบและผู้บังคับใช้กฎหมาย และการสร้างความตระหนักรู้ให้กับประชาชนเพื่อให้รู้เท่าทันและไม่ตกเป็นเหยื่อจึงน่าจะเป็นผลดีกว่าการตามดำเนินคดีหลังเกิดความสูญเสียไปแล้ว

แนวทางในการป้องกันและปราบปรามพิศวาสอาชญากรรมทางคอมพิวเตอร์ซึ่งเป็นภัยคุกคามทางเทคโนโลยี ที่เกิดจากบทเรียนของพิศวาสอาชญากรรมทางคอมพิวเตอร์ซึ่งทำลายความไว้วางใจของประชาชนในการใช้เทคโนโลยีในมิติต่างๆ ต้องการข้อเสนอแนะเชิงนโยบายในลักษณะการสร้างความตระหนักรู้ให้กับสังคมดิจิทัล และสามารถนำไปใช้ให้เป็นมาตรการในการป้องกันปราบปรามพิศวาสอาชญากรรมทางคอมพิวเตอร์ด้วยตนเอง ตลอดจนการพัฒนานโยบายแลกเปลี่ยนกระจายข้อมูลเชิงเฝ้าระวังภัยของภาครัฐ และมาตรการเตือนภัยล่วงหน้าโดยเอกชนผู้ดูแลระบบ อันจะฟื้นฟูความไว้วางใจของประชาชนให้ใช้อินเตอร์เน็ตได้อย่างมั่นใจอันเป็นประโยชน์ต่อการพัฒนาเศรษฐกิจดิจิทัลควบคู่ไปกับการคุ้มครองสิทธิประชาชนต่อไป

4.2 ข้อเสนอแนะเชิงปฏิบัติการ

ข้อเสนอแนะเชิงปฏิบัติการประกอบไปด้วย 2 ส่วน คือ ขั้นตอนการร้องทุกข์ของผู้เสียหาย และแนวทางการดำเนินคดีของเจ้าพนักงานบังคับใช้กฎหมาย อันได้แก่

1) ขั้นตอนการการแจ้งความที่เกี่ยวกับคดีพิศวาสอาชญากรรมทางคอมพิวเตอร์

1. ให้ผู้เสียหาย เตรียมเอกสารส่วนตัว และ สำเนาบัตรประจำตัวประชาชน

2. กรณีที่เสียหายต่อชื่อเสียง ให้เตรียมหลักฐาน ที่พบว่ามีการกระทำความผิด เช่น ปริ้นท์เอกสารหน้าจอ หน้าเว็บไซต์ หน้าโปรแกรมไลน์ โปรแกรมเฟซบุ๊ค หรือหน้าเพจที่พบการกระทำความผิด

3. กรณีที่เสียหายต่อทรัพย์ ให้เตรียมหลักฐานที่พบการกระทำความผิด การหลอกลวง เช่น หลักฐานการโอนเงิน โดยปริ้นท์เอกสารออกมาจากระบบคอมพิวเตอร์ให้เรียบร้อย

4. ให้ไปแจ้งความ ณ สถานีตำรวจท้องที่เกิดเหตุ สถานีตำรวจนครบาล หรือสถานีตำรวจภูธร หรือร้องทุกข์ที่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) หรือศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.)

2) แนวทางการดำเนินคดีพิศวาสอาชญากรรม

การล่อลวงให้ผู้เสียหายสูญเสียทรัพย์สินเงินทองมิใช่ “การให้โดยเสน่หา” แต่เป็นความผิดทางอาญา ในคดีพิศวาสอาชญากรรมหลายกรณียังเป็นการกระทำที่เข้าข่ายองค์กรอาชญากรรมข้ามชาติอีกด้วย เนื่องจากเป็นการกระทำที่มีลักษณะของการกระทำผิดแบบข้ามพรมแดน กล่าวคือ เป็นการกระทำความผิดที่ได้กระทำลงมากกว่าในหนึ่งประเทศหรือมีส่วนหนึ่งส่วนใดของการกระทำผิดหรือผลกระทบเกี่ยวข้องตั้งแต่ 2 ประเทศขึ้นไป ซึ่งเป็นการกระทำที่สามารถส่งตัวผู้กระทำผิดที่อยู่นอกราชอาณาจักรกลับมารับโทษในราชอาณาจักรได้

ฐานความผิดที่แตกต่างกันเหล่านี้ส่งผลกับรูปแบบการดำเนินคดี โดยความผิดฐานฉ้อโกงเพียงฐานเดียวเท่านั้นที่เป็นความผิดต่อส่วนตัวหรือเป็นความผิดที่ยอมความได้ ดังนั้น ความผิดฐานนี้จึงจำเป็นต้องมีผู้เสียหาย และผู้เสียหายจะต้องมีการแจ้งความร้องทุกข์ต่อเจ้าพนักงานตำรวจด้วย เจ้าพนักงานตำรวจจึงจะมีอำนาจทำการสืบสวนคดีนั้นต่อไปได้ และหากต่อมาผู้เสียหายตัดสินใจถอนแจ้งความอำนาจในการสืบสวนสอบสวนคดีดังกล่าวก็จะสิ้นสุดลงเช่นกัน ส่วนความผิดฐานอื่นๆ เช่น ความผิดตามเกี่ยวกับการล่อลวง การใช้ภาพโปรไฟล์หรือข้อมูลปลอม อันเป็นความผิดตามพระราชบัญญัติคอมพิวเตอร์ฯ นั้นเป็นความผิดอาญาแผ่นดินผู้เสียหายไม่สามารถยอมความได้ ทำให้เจ้าพนักงานมีอำนาจในการสืบสวนสอบสวนคดีนี้ต่อไปได้โดยไม่จำเป็นต้องมีผู้เสียหาย โดยเฉพาะอย่างยิ่งหากเป็นกรณีองค์กรอาชญากรรมข้ามชาติเจ้าพนักงานยังสามารถนำตัวผู้กระทำผิดที่อยู่นอกราชอาณาจักรมารับโทษในราชอาณาจักรได้อีกด้วย

นอกจากความผิดฐานฉ้อโกง และความผิดตามพระราชบัญญัติคอมพิวเตอร์แล้ว พิศวาสอาชญากรรมยังเป็นความผิดที่เกี่ยวโยงกับความผิดหลายฐานในกฎหมายหลายฉบับด้วยกัน ไม่ว่าจะเป็นความผิดตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 และพระราชบัญญัติคนเข้าเมือง พ.ศ. 2522 อีกด้วย กฎหมายเหล่านี้ได้กำหนดหลักเกณฑ์การได้มาซึ่งพยานหลักฐานไว้แตกต่างจากประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งจะส่งผลต่อการรับฟังพยานหลักฐานของศาลที่มิจำเป็นต้องปฏิบัติตามเงื่อนไขที่ระบุไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา แต่สามารถรับฟังพยานหลักฐานภายใต้เงื่อนไขและหลักเกณฑ์ของกฎหมายต่างๆ เหล่านี้แทนได้ กล่าวคือ

พนักงานเจ้าหน้าที่ตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 นั้น ในกรณีมีเหตุอันควรเชื่อได้ว่าหากเนิ่นช้ากว่าจะรอหมายค้นมาได้ ทรัพย์สินหรือพยานหลักฐานนั้นอาจถูกยักย้าย ซุกซ่อน ทำลาย หรือทำให้เปลี่ยนสภาพไปจากเดิมได้ พนักงานเจ้าหน้าที่มีอำนาจเข้าไปในเคหสถาน สถานที่ หรือยานพาหนะใดๆ ที่มีเหตุอันควรสงสัยว่าจะมีการซุกซ่อนทรัพย์สินที่เกี่ยวกับการกระทำความผิด หรือพยานหลักฐานที่เกี่ยวกับการกระทำความผิดฐานฟอกเงินได้โดยไม่ต้องมีหมายค้น ทั้งมีอำนาจในการเข้าถึงบัญชีของลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ที่ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน และยังมี

อำนาจในการจัดทำเอกสารหลักฐานหรืออำพรางตนเพื่อประโยชน์ในการตรวจสอบและรวบรวมพยานหลักฐานเพื่อดำเนินการกับทรัพย์สินที่เกี่ยวกับการกระทำความผิด หรือดำเนินคดีฐานฟอกเงินด้วย

พนักงานเจ้าหน้าที่ผู้ได้รับมอบหมายตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มีอำนาจในการยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุมัติให้กระทำการใดๆ ให้ได้มาซึ่งเอกสารหรือข้อมูลข่าวสารซึ่งส่งทางคอมพิวเตอร์ เครื่องมือ อุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีใดที่ถูกใช้หรืออาจถูกใช้เพื่อให้ได้รับประโยชน์จากการกระทำความผิดได้ รวมถึงมีอำนาจในการจัดทำเอกสารหรือหลักฐานใดขึ้น หรือปฏิบัติการอำพรางใดเพื่อประโยชน์ในการสืบสวนสอบสวน ซึ่งการกระทำเหล่านี้ถือว่าเป็นการกระทำโดยชอบด้วยกฎหมาย ทั้งยังมีอำนาจในการใช้เครื่องมือสื่อสารโทรคมนาคม เครื่องมืออิเล็กทรอนิกส์ หรือด้วยวิธีการใด ในการสะกดรอยผู้ต้องสงสัยว่ากระทำหรือจะกระทำความผิด เพื่อสืบสวน จับกุม แสวงหา และรวบรวมพยานหลักฐานได้

กรณีอาชญากรเป็นชาวต่างชาติที่พนักงานเจ้าหน้าที่สามารถนำพระราชบัญญัติคนเข้าเมือง พ.ศ. 2522 มาใช้บังคับได้ สำหรับผู้กระทำความผิดชาวต่างชาติที่จะเข้ามาอาศัยอยู่ในราชอาณาจักรนั้น พนักงานเจ้าหน้าที่มีอำนาจตรวจบุคคลที่เดินทางเข้ามาในหรือออกไปนอกราชอาณาจักร โดยมีอำนาจสั่งห้ามมิให้คนต่างด้าวที่มีพฤติการณ์เป็นที่น่าเชื่อว่าเป็นบุคคลที่เป็นภัยต่อสังคม หรือจะก่อเหตุร้ายให้เกิดอันตรายต่อความสงบสุขหรือความปลอดภัยของประชาชน หรือเข้ามาเพื่อประกอบกิจการอื่นที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนเข้ามาในราชอาณาจักรได้ หากอาชญากรเข้ามาในราชอาณาจักรเพื่อการท่องเที่ยว ทำให้ยากต่อการคัดกรองของเจ้าหน้าที่ แต่หากคนต่างด้าวเหล่านั้นมีพฤติการณ์ที่สมควรเพิกถอนการอนุญาตให้อยู่ในราชอาณาจักร พนักงานเจ้าหน้าที่โดยคณะกรรมการพิจารณาคนเข้าเมืองหรืออธิบดีกรมตำรวจมีอำนาจเพิกถอนการอนุญาตให้อยู่ในราชอาณาจักรของคนต่างด้าวเหล่านั้นได้

ส่วนผู้กระทำความผิดที่อยู่นอกราชอาณาจักรก็สามารถนำพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 พระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 มาบังคับใช้ได้ โดยหากผู้กระทำความผิดไม่ได้อาศัยอยู่ในประเทศที่ไทยมีสนธิสัญญาว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา หรือไม่ได้อาศัยอยู่ในประเทศที่ไทยมีสนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างกัน ก็สามารถขอความร่วมมือจากประเทศที่ผู้กระทำความผิดอาศัยอยู่ได้โดยอาศัยวิธีการทางการทูตได้

พนักงานสอบสวนสามารถนำหลักเกณฑ์และวิธีการสืบสวนสอบสวนซึ่งก็คือ การค้นหาพยานหลักฐานในกฎหมายหลากหลายฉบับที่เกี่ยวข้องเหล่านี้มาใช้แทนประมวลกฎหมายวิธีพิจารณาความอาญา รวมถึงขอความร่วมมือกับต่างประเทศได้โดยอาศัยช่องทางทางการทูตหรือสนธิสัญญา ซึ่งจะช่วยลดข้อจำกัดในเรื่องการรับฟังพยานหลักฐานของศาลไปได้ อันจะนำมาซึ่งการนำตัวผู้กระทำความผิดมารับโทษและตรวจสอบยึดทรัพย์สินได้ในที่สุด

บทคัดย่อ

วัตถุประสงค์ในการศึกษาพิศวาสอาชญากรรมที่กระทำผ่านเครือข่ายสังคม (Social Media) และระบบปฏิบัติการในอินเตอร์เน็ต อาทิ เฟซบุ๊ค อินสตาแกรม เว็บบอร์ดในเว็บไซต์หาคู่ และอีเมล ก็เพื่อเข้าใจถึงข้อจำกัดในการดำเนินคดีเพื่อปราบปรามอาชญากรและเยียวยาผู้เสียหาย และนำไปสู่การสร้างแนวทางป้องปรามพิศวาสอาชญากรรมในอนาคต ผู้วิจัยใช้วิธีทบทวนวรรณกรรม ค้นคว้าจากกรณีศึกษาที่เป็นคดีความ และการสัมภาษณ์แหล่งข้อมูลศักยภาพสูง ได้แก่ เหยื่อ ผู้ดูแลระบบ และเจ้าพนักงานของรัฐ ผลการศึกษาวิจัยพบว่า สถานการณ์พิศวาสอาชญากรรมไม่ลดลงและมีแนวโน้มแพร่หลายไปสู่ผู้ใช้อินเตอร์เน็ตมากขึ้นเพราะพลเมืองขาดความรู้ในการระมัดระวังภัยคุกคามจากอาชญากรรมประเภทล่อลวง ทั้งยังทำให้ตนเองตกอยู่ในภาวะเสี่ยงจากการเผยแพร่ข้อมูลส่วนบุคคลอ่อนไหวสู่พื้นที่สาธารณะ ผลการศึกษาเกี่ยวกับมาตรการทางกฎหมายและเฝ้าระวังภัยพบว่า การดำเนินคดีพิศวาสอาชญากรรมมีอุปสรรคสำคัญจากพรมแดนรัฐซึ่งเป็นขอบเขตอำนาจศาลทางกฎหมาย เนื่องจากในหลายกรณีรัฐอาจบ่งชี้ตัวผู้กระทำความผิดได้แต่มิอาจบังคับใช้กฎหมายข้ามรัฐไปจับกุมผู้กระทำผิดในรัฐอื่น รวมถึงมีอุปสรรคในการแสวงหาความร่วมมือจากผู้ให้บริการอินเตอร์เน็ตและระบบปฏิบัติการต่างๆ ทั้งภายในและระหว่างประเทศ ยิ่งไปกว่านั้นข้อจำกัดในแง่ความอับอายของผู้เสียหายที่รัฐก็ต้องคุ้มครองสิทธิในเกียรติยศชื่อเสียงและความเป็นอยู่ส่วนตัวไปจนถึงข้อมูลส่วนบุคคลของเหยื่อ อีกทั้งการป้องกันพิศวาสอาชญากรรมโดยควบคุมการไหลเวียนข้อมูลข่าวสารในลักษณะการเซ็นเซอร์ก็อาจสร้างผลกระทบต่อการไหลเวียนข้อมูลอย่างเสรีในโลกไซเบอร์ด้วย ผลการศึกษาพบแนวทางเพิ่มความตระหนักรู้ให้ประชาชนกลุ่มเสี่ยงที่สอดคล้องกับความก้าวหน้าของเทคโนโลยี คือ การศึกษากลยุทธ์ของอาชญากรและการหาจุดอ่อนที่เหยื่อเปิดเผยข้อมูลส่วนบุคคลในพื้นที่ไซเบอร์จะช่วยทำให้เข้าใจ “รูปแบบ” และ “การพัฒนาเป้าหมาย” ล่อลวงเหยื่อโดยอาชญากร โดยงานวิจัยนี้มีข้อเสนอแนะให้เผยแพร่องค์ความรู้เกี่ยวกับกลยุทธ์ของอาชญากรและความเสี่ยงที่ผู้ใช้อินเตอร์เน็ตเปิดเผยแก่ผู้บังคับใช้กฎหมาย ผู้ดูแลระบบ และประชาชน เพื่อให้สามารถนำความรู้มาสร้างมาตรการเฝ้าระวังและเตือนภัยผู้ใช้อินเตอร์เน็ตให้ดูแลรักษาความปลอดภัยของตนเอง และเป็นแนวทางให้ผู้ประกอบการและรัฐป้องปรามอาชญากรรมได้

คำสำคัญ: พิศวาสอาชญากรรม, การสื่อสารออนไลน์, โลกไซเบอร์

Abstract

The objective for study Romance Scam via Social Media and Internet Operative Systems such as Facebook, Instagram, web board in dating websites and e-mail is understanding the limitations to prosecute criminals and remedy the victims to construct the guideline to prevent further romance scams. This research employ qualitative methodology which collect data from literature reviews, document research from case studies and interviews from high potential informant; victims, system administrators and State officials. The result of research on the problems have shown that the number of romance scam case is increasing and penetrating to diverse Netizen. In term of legal measure and monitoring system analysis, there are the obstacles which come from limitation of State ability to prosecute the criminal due to jurisdiction principle of Modern State. In many cases State official may identify the convicts but unable to enforce the law across border to arrest the criminal in foreign country. Moreover, the cooperation between State and Private Entity is hardly to find either in domestic and international level. The shame of victims is another condition that deter the criminal procedure since there is no specific assurance to protect their privacy or personal data. Furthermore, the strategy to prevent Romance Scam by using censorship tactic might harm to integrity of internet communication and the flow of information in democratic society. This phenomenon reflects that Romance Scam revolts but State still using the same old measure which has many obstacles from the legal principle of Modern State. The research results on guidelines to improve people's realization on romance scam is gained from the studies on criminal tactics and weak points of victim which provide the intelligence to the vulnerable group on how the attack is delivered. Accordingly, the suggestion of this research is to publicize the information about "form" and "target development" strategy which criminal employ to allure victim. These information is suitable for creating preventive measure to protect internet users and the guideline to suppress Romance Scam for State official and system administrator.

Keywords: Romance Scam, Online Communication, Cyberspace

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

ภาคผนวก

สารบัญรูปภาพและแผนภาพ

สารบัญรูปภาพและแผนภาพ (ต่อ)

บทที่ 1
บทนำ

งานวิจัยเรื่อง ข้อจำกัดของกระบวนการยุติธรรมเพื่อป้องกันและปราบปรามพิศวาส-อาชญากรรมและแนวทางสร้างความตระหนักรู้ให้กับประชาชนนี้ มุ่งศึกษาถึงอาชญากรรมไซเบอร์ ที่ต้องการมาตรการป้องกันและปราบปรามอาชญากรรมล่อลวงซึ่งทำลายความมั่นใจของผู้ใช้อินเตอร์ในการใช้บริการต่างๆ ในโลกออนไลน์จนกระทบกระเทือนต่อการใช้ชีวิตในแง่มุมต่างๆ บนพื้นที่ไซเบอร์ อย่างไว้วางใจต่อเทคโนโลยี โดยผู้วิจัยเลือกกรณีศึกษาพิศวาสอาชญากรรม (ROMANCE SCAM) ที่อาชญากรพัฒนากลยุทธ์ล่อลวงจากการแสวงหาเหยื่อผ่านการศึกษาข้อมูลส่วนบุคคลที่ผู้ใช้อินเตอร์เน็ตมักจะเปิดเผยในพื้นที่สาธารณะ หรือกึ่งสาธารณะ เป็นเหตุให้อาชญากรล่วงรู้ชีวิตส่วนตัวของเหยื่อและสามารถพลิกแพลงเป็นยุทธศาสตร์ยึดครองจิตใจเหยื่อจนอาจล่อลวงให้สูญเสียทรัพย์สินเงินทองหรือเนื้อตัวร่างกายได้ แม้จะอาศัยอยู่คนละประเทศก็ตาม

1.1 ที่มาและความสำคัญของปัญหา

การปฏิวัติคลื่นลูกที่สามเกิดขึ้นโดยอาศัยเทคโนโลยีสารสนเทศความเปลี่ยนแปลงโครงสร้างทางเศรษฐกิจ สังคม และวัฒนธรรมไปทั่วโลก โดยรัฐบาลต่างๆ ตระหนักถึงความพลิกพันที่เกิดขึ้นอย่างมหาศาลจึงพยายามแสวงหามาตรการต่างๆ เพื่อฉวยเอาเทคโนโลยีสารสนเทศมาขับเคลื่อนประเทศให้เจริญก้าวหน้า ในกรณีของรัฐบาลไทยซึ่งกำลังเผชิญปัญหาเศรษฐกิจที่ติดกับดักรายได้ปานกลาง (Middle-Income Trap) ก็ได้เสนอวาระพัฒนาชาติให้ขยับออกจากวิกฤตดังกล่าวด้วยการก้าวไปสู่ประเทศที่ใช้องค์ความรู้ (Knowledge) เป็นตัวขับเคลื่อนเศรษฐกิจและสังคม พัฒนาประชาชนและวิสาหกิจขนาดกลาง/ย่อม (SMEs) ให้สร้างสรรค์นวัตกรรมเพื่อขับเคลื่อนธุรกิจตั้งใหม่ (Startups) ภายใต้แบรนด์ไทยแลนด์ 4.0

จากนโยบายข้างต้นหน่วยงานภาครัฐมีแนวทางในการพัฒนาเทคโนโลยีเข้ามารองรับการบริหารทั้งด้านเศรษฐกิจ สังคม และการบริหารประเทศ เพื่อส่งเสริมกิจกรรมในยุคดิจิทัล แต่อย่างไรก็ตาม ยังมีเหตุการณ์สะเทือนอารมณ์ความรู้สึกของผู้ใช้อินเตอร์เน็ตอยู่เรื่อยมา โดยเฉพาะภัยคุกคามที่เกี่ยวพันกับกิจกรรมส่วนตัวของผู้ใช้อินเตอร์เน็ต คือ พิศวาสอาชญากรรมทางคอมพิวเตอร์ ซึ่งเป็นภัยทางเทคโนโลยีที่มีประชาชนผู้เปลี่ยวเหงาจำนวนมากมาย ถูกล่อลวงโดยนำเทคโนโลยีสารสนเทศมาเป็นช่องทางปฏิบัติการก่ออาชญากรรมอย่างแพร่หลาย ทั้งที่เป็นอาชญากรรมภายในประเทศ อาชญากรรมข้ามชาติ ในหลายกรณีมีลักษณะเป็นปฏิบัติการขององค์กรอาชญากรรมข้ามชาติด้วย

อาชญากรรมทางคอมพิวเตอร์เป็นภัยคุกคามทางเทคโนโลยีสารสนเทศที่สร้างความเสียหายทั้งต่อผู้ใช้งานส่วนบุคคลและเครือข่ายสังคมในวงกว้าง ซึ่งมีรูปแบบแตกต่างกันไป แต่มีผลกระทบร่วมกัน คือ สร้างความไม่ไว้วางใจต่อเทคโนโลยีให้กับผู้ใช้อินเตอร์เน็ตจนเกิดผลกระทบต่อผู้ประกอบการเว็บไซต์หาคู่ หรือเครือข่ายสังคมออนไลน์ที่ส่วนสำคัญในการขับเคลื่อนเศรษฐกิจดิจิทัล

ปัจจุบันเทคโนโลยีได้เข้ามามีบทบาทในชีวิตของประชาชนมากยิ่งขึ้น โดยเฉพาะเทคโนโลยีด้านการสื่อสารที่เข้ามามีอิทธิพลแทบจะทุกมิติของชีวิต ส่งผลให้พฤติกรรมด้านการปฏิสัมพันธ์ของประชาชนเปลี่ยนแปลงไปตามความก้าวหน้าของเทคโนโลยี มีประชาชนจำนวนมากที่ใช้เทคโนโลยีในการหา “คู่” หรือแม้แต่ “ความรัก” ก่อให้เกิดการกระทำความผิดที่เรียกว่า Romance Scam หรือ “การลวงรัก”

โดยทั่วไป Romance Scam หรือ “การลวงรัก” คือ การที่นักต้มตุ๋น (Scammer) ได้ใช้เทคนิคทางจิตวิทยาผ่านเครื่องมือทางเทคโนโลยีต่าง ๆ ในการหลอกลวงให้ เหยื่อ (Victim) หลงเชื่อ จนกระทั่งยินยอมให้สิ่งต่าง ๆ ที่นักต้มตุ๋นต้องการ[1] นั่นเอง ซึ่งวิธีการที่นักต้มตุ๋นมักใช้ในการหลอกลวง คือ การสร้างโปรไฟล์ปลอมๆ ขึ้นมาในโซเชียลมีเดียต่าง ๆ อาทิ Facebook หรือเว็บไซต์หาคู่ต่าง ๆ (Dating website/App) ซึ่งข้อมูลที่นำมาใช้ทำโปรไฟล์เหล่านี้ก็นำมาจากการขโมยข้อมูลเช่น ชื่อ ประวัติ และรูปภาพของคนอื่น แล้วเอามาดัดแปลงเป็นข้อมูลของตนเอง หรืออาจจะสร้างข้อมูลปลอมๆ ขึ้นมาเอง โดยเหยื่อที่นักต้มตุ๋นเหล่านี้มองหา มักจะเป็นมีคุณสมบัติหนึ่งที่สำคัญคือ ต้องเป็นคนขี้อ่อนไหว และขี้เหงา แบบต้องการใครสักคนมาอยู่เคียงข้าง[2]

ปัจจุบัน ประเทศไทยมีการก่ออาชญากรรมในลักษณะนี้มากขึ้น จากการสำรวจเบื้องต้นพบว่ามีผู้เสียหายจากการถูก Romance Scam เป็นจำนวนมาก โดย พ.ต.อ.ภาณุวัฒน์ ร่วมรักษ์ รองผู้บังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (TCSD) ได้เปิดเผยว่า ในปี 2558 ที่ผ่านมา เฉพาะคดีเกี่ยวกับ Romance Scam ถูกร้องเรียนเข้ามาถึง 80 คดี มูลค่าความเสียหาย 150 ล้านบาท ยังไม่นับคดีที่ถูกร้องเรียนไปยังสถานีตำรวจท้องที่และเหยื่อที่ไม่กล้าเข้าแจ้งความอีกเป็นจำนวนมาก[3] และ พ.ต.อ.ภาณุวัฒน์ ร่วมรักษ์ ยังเปิดเผยอีกว่า ผู้ที่ตกเป็นเหยื่อ ส่วนมากมักจะเป็นหญิงโสดอายุ 40-60 ปี การศึกษาดี หน้าที่การงานมั่นคง ที่สำคัญคือ “มีสตางค์” ที่น่าตกใจที่สุดคือ ที่ผ่านมาพบเหยื่อที่สูญเสียมากสุดอยู่ที่ 33 ล้านบาท โดยโดนหลอกโอนเงินไปให้คนรักออนไลน์ถึง 26 ครั้ง ภายในเวลา 2 ปี ทั้งที่ไม่เคยพบเจอหน้ากันเลยแม้แต่ครั้งเดียว บางคนถูกคนร้ายใช้จิตวิทยาหว่านล้อมจนหลงเชื่อโดนหลอกโอนเงินไปให้มากกว่า 83 ครั้ง รวมเป็นเงิน 13 ล้านบาท[4]

ซึ่งรูปแบบพฤติการณ์การหลอกลวงของกลุ่ม Romance Scam ที่ก่อเหตุและถูกจับกุมในประเทศไทยนั้น ผู้ต้องหาจะเป็นกลุ่มชาวแอฟริกันที่สร้างโปรไฟล์ในสื่อสังคมออนไลน์ต่างๆ โดยมักอ้างว่าตนเป็นชายหรือหญิงผิวขาว มีอาชีพเป็นทหาร สังกัดกองทัพสหรัฐ ซึ่งผู้เสียหายก็มีทั้งเพศหญิงและเพศชาย

ในปี 2559[5] ตำรวจท่องเที่ยวได้จับกุม 3 ผู้ต้องหา แก๊ง Romance Scam โดยผู้ต้องหาทั้งหมดเป็นคนผิวสี สัญชาติแอฟริกา, โมซัมบิก และ กานา ซึ่งการกระทำความผิดของผู้ต้องหากลุ่มนี้จะใช้

---

[1] วชิรวิทย์ คงคาลัย, (17 กรกฎาคม 2560). *Romance Scam: ไม่รักไม่ว่าอะไร แต่ใยต้องหลอกกันด้วย,* สืบค้นจาก https://www.the101.world/life/romance-scam/

[2] เรื่องเดียวกัน

[3] Rabbit finance Magazine, (ธันวาคม 2560). *“Romance Scam” หลอกรักออนไลน์ ภัยร้ายของสาวโสด!,* สืบค้นจาก https://finance.rabbit.co.th/blog/romance-scam-and-single-ladies

[4] เรื่องเดียวกัน

[5] Voice TV. (11 มิถุนายน 2559), *จับแก๊ง 'Romance scam' หลอกหญิงไทยโอนเงินซื้อของหมั้น,* สืบค้นจาก https://www.voicetv.co.th/read/376101

แอพพลิเคชั่น Facebook แชทกับหญิงไทย ด้วยการอ้างตนว่าเป็นฝรั่งผิวขาว จากนั้นก็จะหลอกให้โอนเงินเข้าบัญชีที่ได้จ้างให้คนไทยไปเปิดไว้ ส่วนบัตร ATM เก็บไว้ที่กลุ่มผู้ต้องหา โดยมักจะอ้างว่า ตนได้ซื้อของหมั้นมาให้ แต่ติดขั้นตอนที่กรมศุลกากร ทำให้ไม่สามารถเอาของหมั้นดังกล่าวของออกมาได้ ขอให้ผู้เสียหายโอนเงินเข้าบัญชีที่เตรียมไว้ ซึ่งเมื่อผู้เสียหายหลงเชื่อและโอนเงินเข้าบัญชีแล้ว กลุ่มผู้ต้องหาก็จะไปกดเงิน แล้วตัดการติดต่อไป จากการสอบสวนพบของกลางที่แสดงให้เห็นว่า ภายในระยะเวลา 3 เดือน มีเงินไหลเวียนในบัญชีดังกล่าวมากกว่าล้านบาท ทั้งๆ ที่ผู้ต้องหากลุ่มนี้ไม่มีงานทำเป็นหลักแหล่ง

และในปี 2560 ตำรวจ (ศูนย์หมายจับคนร้ายข้ามชาติ : สตม.) ได้จับผู้ต้องหาแก๊ง Romance Scam ชาวแอฟริกัน ที่มีความเชื่อมโยงกับขบวนการค้ายาเสพติดข้ามชาติ ด้วยการสวมรอยว่าเป็นทหารอเมริกา หลอก ผอ.และรอง ผอ.โรงเรียนชื่อดังแห่งหนึ่ง โดยอ้างว่าจะบริจาคทุนการศึกษาเด็ก มีผู้เสียหายตกเป็นเหยื่อกว่า 20 รายและเสียหายกว่าสิบล้านบาท[6]

ผู้เสียหายรายที่หนึ่งและที่สอง (ผอ.และรอง ผอ.) การหลอกลวง เริ่มจากผู้ต้องหาเข้ามาทักใน Facebook แล้วอ้างว่าเป็นทหารหญิงในกองทัพสหรัฐ ฝ่ายผู้เสียหายเห็นว่าเป็นโอกาสดีที่จะได้ฝึกภาษาและมีเพื่อนชาวต่างชาติจึงได้ติดต่อกันเรื่อยมา โดยไม่เคยพบตัวจริงหรือสนทนาทางโทรศัพท์ เมื่อติดต่อกันได้ระยะหนึ่ง ผู้ต้องหาอ้างว่าไปทำงานในพื้นที่สงครามในตะวันออกกลาง มีเงินที่ทางรัฐบาลสหรัฐฯ ส่งมาให้กองทัพในพื้นที่จำนวนหลายล้านดอลลาร์ และถูกฝ่ายตรงข้ามปล้นเงินไป แต่ต่อมากลุ่มทหารอเมริกันได้ยึดคืนมาได้ แต่ไม่ได้รายงานรัฐบาลและได้นำมาแบ่งกัน ผู้ต้องหาอ้างว่าตนได้รับส่วนแบ่งมาจำนวน 1 ล้านดอลลาร์ มีความประสงค์จะบริจาคเงินเพื่อเป็นทุนการศึกษาแก่เด็กไทย โดยจะส่งเงินใส่กระเป๋าผ่านบริษัทขนส่งข้ามประเทศ แล้วให้ผู้เสียหายรอรับ หลังจากนั้นได้มีคนไทยอ้างว่าเป็นเจ้าหน้าที่บริษัทขนส่ง แจ้งว่าเงินจำนวนดังกล่าวได้ส่งมาถึงแล้ว แต่ผู้รับปลายทางจะต้องชำระค่าธรรมเนียมจำนวนหนึ่ง ผู้เสียหายหลงเชื่อ จึงได้โอนเงินไปให้หลายครั้ง จนกระทั่งรู้ตัวว่าตกเป็นเหยื่อจึงได้ขอความช่วยเหลือมาที่ สตม.

ผู้เสียหายรายที่สาม เป็นหญิงไทย ได้ให้ข้อมูลว่า เมื่อเดือน มิ.ย.ที่ผ่านมา มีชายชาวอเมริกันหน้าตาดี ติดต่อตนมาทาง Facebook อ้างว่า เป็นนายทหารยศนายพล ปฏิบัติหน้าที่อยู่ในประเทศอัฟกานิสถาน ภรรยาเสียแล้ว อยากตั้งครอบครัวใหม่ในประเทศไทย พร้อมอ้างว่ามีเงินและของมีค่าที่ยึดได้จากสงครามมูลค่ากว่าห้าแสนดอลลาร์สหรัฐฯ จะส่งมาให้ผู้เสียหายเก็บรักษาไว้ เมื่อหมดภารกิจแล้วจะเดินทางมาแต่งงานกับผู้เสียหายที่ประเทศไทย และบอกว่าจะมีนักการทูตนำกระเป๋าใบนี้ไปส่งให้ ผู้เสียหายหลงเชื่อจึงรับดำเนินการ ต่อมามีคนไทยอ้างว่าเป็นเจ้าหน้าที่สถานทูต, เจ้าหน้าที่ศุลกากร และเจ้าหน้าที่บริษัทขนส่ง ติดต่อผู้เสียหายให้ชำระค่าธรรมเนียมต่างๆ ซึ่งผู้เสียหายได้หลงเชื่อและโอนเงินไปให้หลายครั้ง มูลค่าความเสียหายกว่าหนึ่งล้านบาท

ในปีพ.ศ. 2561 ตามรายงานข้อมูลการเข้าร้องทุกข์ของ ศูนย์บริการประชาชน กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ประจำสัปดาห์ (วันที่ 10-16 มี.ค. 2561) พบว่ามีผู้มาเข้าร้องทุกข์ทั้งหมด 66 ราย ในบริบทนี้เป็นคดีหลอกเกี่ยวกับความรัก (romance scam) 3 ราย แต่คดีดังกล่าวมีมูลค่าความเสียหายสูงที่สุดจากจำนวนคดีทั้งหมด คิดเป็น

[6] ไทยรัฐออนไลน์. (15 กรกฎาคม 2560), *จับแก๊งแอฟริกันแสบ! แชตเฟซบุ๊กสวมรอยทหารมะกัน ตุ๋นผอ. โรงเรียนดัง โอนเงิน*, สืบค้นจาก https://www.thairath.co.th/content/1005807

จำนวนเงิน 7,699,500 บาท[7] และล่าสุดสถิติข้อมูลเมื่อวันที่ 21 มิถุนายน พ.ศ. 2561 ถึง 31 พฤษภาคม พ.ศ. 2562 มีผู้เสียหายหลงเชื่อและโอนเงิน จำนวน 332 ราย รวมมูลค่าความเสียหายประมาณ 193,015,902.11 บาท[8]

อย่างไรก็ตามมาตรการทางกฎหมายและกระบวนการยุติธรรมที่เกี่ยวข้องก็ยังมีข้อจำกัดในการติดตามตัวผู้กระทำความผิดมาดำเนินคดีทางอาญาและชดเชยความเสียหายให้กับเหยื่อ ไม่ว่าจะเป็นความเสียหายทางทรัพย์สินที่ติดตามได้ยากเนื่องจากมักมีการยักย้ายถ่ายโอนไปยังผู้อื่นหรือนอกประเทศไทย ยิ่งถ้าเป็นเสียหายต่อชีวิตและทางเพศย่อมเป็นการยากที่ชดเชยให้กลับมาคืนสภาพเดิม นอกจากนี้ยังพบว่า ผู้ล่อลวงจำนวนมากปฏิบัติการจากต่างประเทศซึ่งเพิ่มความลำบากให้กับกระบวนการยุติธรรมทางอาญาที่ต้องผสานความร่วมมือไปยังประเทศเจ้าของเขตอำนาจให้ส่งผู้ร้ายข้ามแดนหรือยึดทรัพย์สินกลับมาชดเชยความเสียหายให้กับเหยื่อ การสร้างมาตรการป้องปรามโดยผู้ดูแลระบบและผู้บังคับใช้กฎหมาย และการสร้างความตระหนักรู้ให้กับประชาชนเพื่อให้รู้เท่าทันและไม่ตกเป็นเหยื่อจึงน่าจะเป็นผลดีกว่าการตามดำเนินคดีหลังเกิดความสูญเสียไปแล้ว

ดังนั้น เพื่อเป็นแนวทางในการป้องกันและปราบปรามพิศวาสอาชญากรรมทางคอมพิวเตอร์ซึ่งเป็นภัยคุกคามทางเทคโนโลยี งานวิจัยนี้จึงมุ่งทำการศึกษาวิจัยพิศวาสอาชญากรรมทางคอมพิวเตอร์ซึ่งทำลายความไว้วางใจในการใช้เทคโนโลยีในมิติต่างๆ เพื่อให้เกิดข้อเสนอแนะเชิงนโยบาย สร้างความตระหนักรู้ให้กับสังคม และสามารถนำไปใช้ให้เป็นมาตรการในการป้องกันปราบปรามพิศวาสอาชญากรรมทางคอมพิวเตอร์ ตลอดจนการพัฒนานโยบายของรัฐและเอกชนผู้ดูแลระบบให้เกิดประโยชน์ต่อการพัฒนาเศรษฐกิจดิจิทัลและคุ้มครองสิทธิประชาชนต่อไป

1.2 คำถามในการวิจัย

อาชญากรอาศัยช่องทางอินเตอร์เน็ตในการล่อลวงประชาชนให้หลงเชื่อในตัวตนอำพรางของตน จนก่อพิศวาสอาชญากรรมได้ด้วยรูปแบบและวิธีการใดบ้าง อาชญากรเรียนรู้เหยื่อได้อย่างไรและนำข้อมูลจากแหล่งไหนมาคิดค้นกลยุทธ์ในการล่อลวงให้เหยื่อหลงเชื่อจนตกบ่วงกล จนเหยื่อสูญเสียผลประโยชน์ทางเศรษฐกิจอย่างมหาศาลและถูกละเมิดสิทธิในชีวิตเนื้อตัวร่างกายอย่างร้ายแรง รัฐและผู้ดูแลระบบจะมีมาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมอย่างไรให้ผู้ใช้อินเตอร์เน็ตมีความไว้วางใจในการใช้ชีวิตบนโลกไซเบอร์ องค์ความรู้ใดบ้างที่ควรเผยแพร่ไปสู่ประชาชนเพื่อสร้างความตระหนักรู้เท่าทันพิศวาสอาชญากรรม

[7] รายงานประจำสัปดาห์ (วันที่ 10 มี.ค. 2561 – 16 มี.ค. 2561) ข้อมูลการเข้าร้องทุกข์ ณ ศูนย์บริการประชาชน กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)

[8] แนวหน้า, (31 พ.ค. 2562). *ปปง.เผยตั้งศปก.ปปง. 1ปี พบเหยื่อคดีโรแมนซ์สแกน 332 ราย เสียหาย 193 ล้าน*, สืบค้นจาก https://www.naewna.com/local/417058

1.3 สมมติฐานการวิจัย

การสื่อสารในยุคดิจิทัลเอื้อให้คนแปลกหน้าเข้าถึงข้อมูลส่วนบุคคลได้ง่ายด้วยข้อมูลที่ผู้ใช้แสดงออกในโลกไซเบอร์ ข้อมูลที่ผู้ใช้บันทึกเองนี้ได้เพิ่มความเสี่ยงให้อาชญากรนำมาเป็นฐานข้อมูลในการล่อลวงทางอินเตอร์เน็ต ซึ่งสร้างความเสียหายทั้งต่อตัวบุคคลและลดความเชื่อมั่นในหมู่ผู้ใช้อินเตอร์เน็ต มาตรการทางกฎหมายและกระบวนการยุติธรรมที่มีอยู่ไม่สามารถป้องปรามการจู่โจม หรือเยียวยาความเสียหายได้อย่างมีประสิทธิผลโดยเฉพาะอาชญากรรมข้ามชาติ ดังนั้น การสร้างมาตรการเตือนภัยล่วงหน้าและสร้างความตระหนักรู้อาจจะเป็นผลดีกว่าการเยียวยาเหยื่อและตามดำเนินคดีอาชญากรหลังเกิดความเสียหายแล้ว

1.4 วัตถุประสงค์

1) ศึกษาสภาพปัญหา รูปแบบ และวิธีการของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติ

2) พัฒนากฎหมายและมาตรการเฝ้าระวังและเตือนภัยล่วงหน้าเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม

3) สร้างแนวทางเพิ่มความตระหนักให้ประชาชนกลุ่มเสี่ยงตกเป็นเป้าหมายพิศวาสอาชญากรรมให้รู้เท่าทันพิศวาสอาชญากรรม

1.5 ขอบเขตของการวิจัย

งานวิจัยนี้มุ่งศึกษาพิศวาสอาชญากรรมและกระบวนการยุติธรรมที่เกี่ยวข้อง โดยมีขอบเขตการวิจัยครอบคลุมใน 3 ด้าน คือ

1) **ขอบเขตด้านเนื้อหา** เนื้อหาวิจัยจะครอบคลุมลักษณะของเหยื่อ วิธีการล่อลวงของอาชญากร และอุปสรรคในการป้องกันปราบปรามอาชญากรรมไซเบอร์ โดยไม่รวมคดีเกี่ยวกับการโอนเงิน เปิดบัญชีและการฟอกเงิน

2) **ขอบเขตด้านประชากร** ประชากรที่ศึกษานั้นเป็นผู้เกี่ยวข้องกับพิศวาสอาชญากรรม อาทิ เหยื่อ (victim) ผู้บังคับใช้กฎหมาย (law enforcement officer) ผู้ดูแลระบบ (system administrator) ซึ่งสัมผัสกับประสบการณ์ในสถานการณ์จริง แต่ไม่รวมเจ้าหน้าที่ปราบปรามการฟอกเงินและสถาบันการเงิน และมีการสัมภาษณ์นักวิชาการผู้เชี่ยวชาญด้านอาชญากรรมไซเบอร์เพื่อความสมบูรณ์ของงานวิจัย

3) **ขอบเขตด้านเวลา** จะสืบย้อนข้อมูลจากเอกสารและงานวรรณกรรมไปตั้งแต่ที่มีการใช้อินเตอร์เน็ตจนถึง เดือนสิงหาคม พ.ศ.2562 โดยมีระยะการสัมภาษณ์และเขียนงานวิจัยตั้งแต่ 1 กันยายน พ.ศ.2561 – 31 สิงหาคม พ.ศ.2562

1.6 นิยามศัพท์สำคัญในการศึกษา

พิศวาสอาชญากรรม (ROMANCE SCAM) คือ การใช้เทคนิคทางจิตวิทยาผ่านเครื่องมือทางเทคโนโลยีต่างๆ ในการหลอกลวงให้ เหยื่อ (Victim) หลงเชื่อ จนกระทั่งยินยอมให้สิ่งต่างๆ ที่นักต้มตุ๋นต้องการ ซึ่งวิธีการที่นักต้มตุ๋นมักใช้ในการหลอกลวง คือ การสร้างโปรไฟล์ปลอมๆ ขึ้นมาในโซเชียลมีเดียต่างๆ หรือเว็บไซต์หาคู่ต่างๆ (Dating website/App) เว็บบอร์ดในเว็บไซต์หาคู่ ซึ่งข้อมูลที่นำมาใช้ทำโปรไฟล์เหล่านี้ก็นำมาจากการขโมยข้อมูล เช่น ชื่อ ประวัติ และรูปภาพของคนอื่น แล้วเอามาดัดแปลงเป็นข้อมูลของตนเอง หรืออาจจะสร้างข้อมูลปลอมขึ้นมา โดยเหยื่อที่นักต้มตุ๋นเหล่านี้มองหามักจะเป็นมีคุณสมบัติหนึ่งที่สำคัญคือ ต้องเป็นคนอ่อนไหว และเหงาโดดเดี่ยว แสวงหาใครสักคนมาเคียงคู่ โดยอาชญากรจะทักทายในโซเชียลเน็ตเวิร์คแล้วสานต่อในช่องทางสื่อสารที่เป็นส่วนตัวมากขึ้น จนเหยื่อหลงเชื่อ และไว้ใจในความสัมพันธ์นั้น นักต้มตุ๋นจะเริ่มแสดงออกถึงความต้องการของตน เช่น มีการพูดคุยเรื่องเงินบ่อยขึ้น มีการสร้างสถานการณ์หลอกให้เหยื่อโอนเงิน หรือหลอกล่อให้เหยื่อยกสิ่งของมีค่าให้กับตน ซึ่งวิธีการของนักต้มตุ๋นมักจะมาพร้อมคำสัญญาต่างๆ เช่น สัญญามาจะมาแต่งงานด้วย สัญญาว่าจะมาสร้างครอบครัวด้วยกันกับเหยื่อ สัญญาว่าจะสร้างธุรกิจร่วมกัน เมื่อเหยื่อโอนเงินหรือยกทรัพย์สิน สิ่งของมีค่าให้นักต้มตุ๋นหมดแล้ว หรือกระทั่งเหยื่อเริ่มรู้สึกได้ว่าตน กำลังถูกหลอก นักต้มตุ๋นจะเปลี่ยนวิธีการ หรือปิดกั้นการคุยกับเหยื่อทันที จนสุดท้ายแล้วเหยื่อไม่สามารถติดต่อ หรือหาตัวนักต้มตุ๋นได้

Scammer คือ อาชญากร / นักต้มตุ๋น (Scammer) ที่ใช้เทคนิคทางจิตวิทยาผ่านเครื่องมือทางเทคโนโลยีต่าง ๆ ในการหลอกลวงให้ เหยื่อ (Victim) หลงเชื่อ เพื่อให้เหยื่อยินยอมให้สิ่งต่างๆ ที่ต้องการ

1.7 แผนดำเนินการศึกษา

แผนดำเนินการศึกษา ทีมวิจัยได้ดำเนินกิจกรรมโครงการ 3 ส่วน ได้แก่ **ส่วนแรก** การวิเคราะห์สาเหตุ รูปแบบและวิธีการล่อลวงของพิศวาสอาชญากรรม **ส่วนที่สอง** การพัฒนากฎหมายในการป้องกันและปราบปรามพิศวาสอาชญากรรม โดยการวิจัยเอกสาร ศึกษาเอกสารตำราต่างๆ หลักฐานชั้นต้นจากคำพิพากษา รวมถึงบทบัญญัติกฎหมายภายในและกฎหมายระหว่างประเทศที่เกี่ยวข้องกับกรณีพิศวาสอาชญากรรม เพื่อค้นหาสภาพปัญหา รูปแบบ และวิธีการของพิศวาสอาชญากรรม รวมถึงการลงพื้นที่สัมภาษณ์แหล่งข้อมูลผู้มีศักยภาพสูง (interviewing high potential sources) อาทิ เหยื่อ ผู้บังคับใช้กฎหมาย ผู้ดูแลระบบ (admin) และนักวิชาการ เพื่อรวบรวมข้อมูลรูปแบบวิธีการล่อลวงของพิศวาสอาชญากรรม และอุปสรรคในการบังคับใช้กฎหมายกับกรณีพิศวาสอาชญากรรม **ส่วนที่สาม** การวิเคราะห์เชื่อมโยงองค์ความรู้กับสภาพปัญหาพิศวาสอาชญากรรมและข้อจำกัดของกฎหมาย และการจัดเวทีสาธารณะในประเด็นพิศวาสอาชญากรรม ซึ่งมีรายละเอียดแผนการดำเนินกิจกรรมโครงการฯ ดังนี้

วัตถุประสงค์	กิจกรรม	ไตรมาส			
		1	2	3	4
1. เพื่อค้นหาสภาพปัญหา รูปแบบ และวิธีการของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติ	1.1 การหารือกรอบการศึกษา และการทบทวนวรรณกรรมเกี่ยวกับสาเหตุของพิศวาสอาชญากรรม	X			
	1.2 การทบทวนวรรณกรรมเอกสาร บริบท สถานการณ์เกี่ยวกับสาเหตุ รูปแบบของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติ	X	X		
	1.3 การสังเกตการณ์อย่างมีส่วนร่วมเพื่อศึกษารูปแบบวิธีการล่อลวงของอาชญากร และการสัมภาษณ์แหล่งข้อมูลผู้มีศักยภาพสูง (interviewing high potential sources) เช่น เหยื่อ ผู้บังคับใช้กฎหมาย, ผู้ดูแลระบบ (admin) เพื่อเก็บข้อมูลเกี่ยวกับสาเหตุ สถานการณ์ของปัญหาพิศวาสอาชญากรรม		X	X	
	1.4 การวิเคราะห์ข้อมูลที่ได้จากการทบทวนวรรณกรรมเกี่ยวกับสาเหตุของพิศวาสอาชญากรรม				X
2. เพื่อพัฒนากฎหมายและระบบระวังภัยในการป้องกันและปราบปรามพิศวาสอาชญากรรม รวมถึงการพัฒนาระบบให้สามารถนำมาใช้งานได้อย่างมีประสิทธิภาพต่อไป	2.1 การศึกษากฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามพิศวาสอาชญากรรม ทั้งที่เป็นกฎหมายระหว่างประเทศ และกฎหมายภายใน	X	X		
	2.2 การสัมภาษณ์แหล่ง ข้อมูลผู้มีศักยภาพสูง (interviewing high potential sources) เช่น ผู้บังคับใช้กฎหมาย, ผู้ดูแลระบบ (admin) ประเด็นเกี่ยวกับการบังคับใช้กฎหมายเกี่ยวกับพิศวาสอาชญากรรม และแนวทางการพัฒนาระบบเฝ้าระวังภัย เตือนภัยล่วงหน้า		X	X	
	2.3 การวิเคราะห์เปรียบเทียบกฎหมายและมาตรการระวังภัยที่เกี่ยวข้องกับการป้องกันและปราบปรามพิศวาสอาชญากรรม				X

วัตถุประสงค์	กิจกรรม	ไตรมาส			
		1	2	3	4
3. เพื่อสร้างความตระหนักรู้ให้ประชาชนรู้เท่าทันพิศวาส-อาชญากรรมและการเผยแพร่ข้อมูลให้กลุ่มเสี่ยงต่อการล่อลวง	3.1 การวิเคราะห์เชื่อมโยงองค์ความรู้กับสภาพปัญหาและข้อจำกัดของกฎหมาย เพื่อหาแนวทางสร้างการตระหนักรู้เกี่ยวกับพิศวาสอาชญากรรม แล้วเผยแพร่ข้อมูลให้กลุ่มสุ่มเสี่ยงต่อการล่อลวง รวมถึงผู้ดูแลระบบและผู้บังคับใช้กฎหมาย				X
	3.2 จัดทำคู่มือ 2 เล่ม และจัดเสวนาหัวข้อ “พิศวาสอาชญากรรม: แนวทางป้องกันและปราบปราม”				X

แผนดำเนินการศึกษา เพื่อให้บรรลุผลลัพธ์ของโครงการ โดยมีรายละเอียดการดำเนินกิจกรรมและผลลัพธ์ ดังนี้

วัตถุประสงค์	กิจกรรรม	ผลลัพธ์
1. เพื่อค้นหาสภาพปัญหารูปแบบ และวิธีการของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติ	1.1 การหารือกรอบการศึกษาและการทบทวนวรรณกรรมเกี่ยวกับสาเหตุของพิศวาสอาชญากรรม	กรอบแนวทางการศึกษาและการทบทวนสภาพปัญหารูปแบบ และวิธีการของพิศวาสอาชญากรรม รวมถึงกรอบระยะเวลาในการทำงาน
	1.2 การทบทวนวรรณกรรม เอกสาร บริบท สถานการณ์เกี่ยวกับสาเหตุ รูปแบบของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติ	สภาพปัญหา สถานการณ์ความรุนแรงของพิศวาสอาชญากรรม และสาเหตุของการก่อให้เกิดพิศวาสอาชญากรรม
	1.3 การสัมภาษณ์แหล่งข้อมูลผู้มีศักยภาพสูง (interviewing high potential sources) เพื่อเก็บข้อมูลเกี่ยวกับสาเหตุ สถานการณ์ของปัญหาพิศวาสอาชญากรรม	ข้อมูลจากการสัมภาษณ์แหล่งข้อมูลผู้มีศักยภาพสูง ในประเด็นสภาพปัญหารูปแบบและวิธีการก่อพิศวาส-อาชญากรรม

วัตถุประสงค์	กิจกรรรม	ผลลัพธ์
2. เพื่อพัฒนากฎหมายและระบบระวังภัยในการป้องกันและปราบปรามพิศวาสอาชญากรรม รวมถึงการพัฒนาระบบให้สามารถนำมาใช้งานได้อย่างมีประสิทธิภาพต่อไป	2.1 การศึกษากฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามพิศวาสอาชญากรรม ทั้งที่เป็นกฎหมายระหว่างประเทศ และกฎหมายภายใน	ข้อมูลบัญญัติและข้อจำกัดของกฎหมายในระดับพระราชบัญญัติ และกฎหมายระหว่างประเทศที่เกี่ยวข้องกับการป้องกันและปราบปรามพิศวาสอาชญากรรม
	2.2 การสัมภาษณ์แหล่ง ข้อมูลผู้มีศักยภาพสูง (interviewing high potential sources) ประเด็นเกี่ยวกับการบังคับใช้กฎหมายเกี่ยวกับพิศวาสอาชญากรรม และแนวทางการพัฒนาระบบเฝ้าระวังภัย	ข้อมูลจากการสัมภาษณ์แหล่งข้อมูลผู้มีศักยภาพสูง ในประเด็นการบังคับใช้กฎหมายและแนวทางการป้องปรามเกี่ยวกับพิศวาสอาชญากรรม
3. การสร้างความตระหนักรู้ให้ประชาชนรู้เท่าทันพิศวาส-อาชญากรรมและการเผยแพร่ข้อมูลให้กลุ่มเสี่ยงต่อการล่อลวง	3.1 การวิเคราะห์เชื่อมโยงองค์ความรู้กับสภาพปัญหาและข้อจำกัดของกฎหมาย เพื่อหาแนวทางป้องกันปราบปรามอาชญากรรมทางด้านการเผยแพร่ข้อมูลที่สุ่มเสี่ยงต่อการล่อลวงเพื่อก่อพิศวาส-อาชญากรรม 3.2 การจัดทำคู่มือสำหรับประชาชนที่เป็นกลุ่มเสี่ยง และคู่มือสำหรับผู้ดูแลระบบและผู้บังคับใช้กฎหมาย 3.3 การจัดเสวนาหัวข้อ “พิศวาสอาชญากรรม: แนวทางป้องกันและปราบปราม”	ข้อเสนอแนะปรับปรุงกฎหมายในการป้องกันและปราบปรามพิศวาสอาชญากรรม รวมถึงการพัฒนาระบบระวังภัยให้สามารถนำมาใช้งานได้อย่างมีประสิทธิภาพต่อไป คู่มือ 2 เล่มเพื่อเผยแพร่ให้กับกลุ่มเสี่ยงต่อการล่อลวงและกลุ่มผู้ดูแลระบบและบังคับใช้กฎหมายเพื่อป้องปรามพิศวาสอาชญากรรม การจัดงานเสวนาพิศวาสอาชญากรรม: แนวทางป้องกันและปราบปราม

1.8 ผลที่ได้รับเมื่อสิ้นสุดการวิจัย

ผลที่ได้รับจากการวิจัย มีดังต่อไปนี้

1.8.1 Output

1) องค์ความรู้เกี่ยวกับสภาพปัญหา รูปแบบ และวิธีการของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติ (เอกสารรายงานวิจัยฉบับสมบูรณ์)

2) ข้อเสนอแนะเชิงนโยบายในการป้องกันและปราบปรามพิศวาสอาชญากรรม รวมถึงการพัฒนาระบบระวังภัยให้สามารถนำมาใช้งานได้อย่างมีประสิทธิภาพต่อไป (เอกสารรายงานวิจัยฉบับสมบูรณ์)

3) องค์ความรู้เกี่ยวกับพิศวาสอาชญากรรมที่พร้อมเผยแพร่ให้แก่สุ่มเสี่ยงต่อการล่อลวง รวมถึงองค์ความรู้สำหรับผู้ดูแลระบบและผู้บังคับใช้กฎหมาย (คู่มือป้องกันพิศวาสอาชญากรรม ฉบับผู้ดูแลระบบและผู้บังคับใช้กฎหมาย / คู่มือป้องกันพิศวาสอาชญากรรม ฉบับประชาชน)

1.8.2 Outcome

องค์ความรู้เกี่ยวกับสาเหตุของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติ และการรักษาความปลอดภัยให้กับข้อมูลส่วนบุคคลและความลับในโลกไซเบอร์ รวมถึงองค์ความรู้สำหรับมาตรการเฝ้าระวังและเตือนภัยขององค์กรบังคับใช้กฎหมายและผู้ดูแลระบบ อีกทั้งข้อมูลสำหรับประชาชนที่เป็นกลุ่มเสี่ยงว่าอาจจะตกเป็นเหยื่อในการหลอกลวง เพื่อนำไปสู่ความรับรู้เข้าใจลักษณะของพิศวาสอาชญากรรม เกิดการปรับปรุงมาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมทั้งในภาครัฐและเอกชน และกลุ่มเสี่ยงตระหนักรู้ภัยคุกคามจากอาชญากรรมล่อลวง โดยองค์ความรู้ที่ได้จากงานวิจัยจะเผยแพร่อยู่ใน 3 รูปแบบ คือ

1) งานวิจัย

รายงานวิจัยฉบับสมบูรณ์ โดยมีเนื้อหาดังนี้

- สถานการณ์ปัจจุบันของพิศวาสอาชญากรรม (Romance Scam) ในโลกไซเบอร์กับผลกระทบที่เกิดกับสังคมไทย
- งานศึกษาที่เกี่ยวข้องกับปัญหาพิศวาสอาชญากรรม (Romance Scam) มาตรการแก้ไขที่ประสบความล้มเหลวและสำเร็จ และทางเลือกในการป้องกันปราบปรามพิศวาสอาชญากรรม
- การทบทวนบทบัญญัติทางกฎหมายและกระบวนการยุติธรรมที่เกี่ยวข้องกับพิศวาสอาชญากรรม (Romance Scam)
- กลยุทธ์เทคนิค วิธีการที่ scammer ในการก่อพิศวาสอาชญากรรม และหน้าฉาก-หลังฉากของวงการ romance scam
- ข้อเสนอแนะเชิงนโยบายในการป้องกันและปราบปรามพิศวาสอาชญากรรม

2) งานเสวนา

2.1) งานเสวนาวิชาการ “มหกรรมวิทยาการกฎหมายดิจิทัล Digital Grand Prix 2019” วันที่ 3 สิงหาคม 2562 เวลา 09.00 – 16.00 น. ณ ห้องประชุม 1 คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่ โดยในเวทีเสวนาได้นำเสนอร่างรายงานวิจัยฉบับสมบูรณ์โครงการวิจัยฯ และข้อเสนอแนะแนวทางการป้องกันและปราบปรามพิศวาสอาชญากรรม (Romance Scam)

2.2) เวทีเสวนา “พิศวาสอาชญากรรม: แนวทางป้องกันและปราบปราม” วันจันทร์ที่ 26 สิงหาคม 2562 เวลา 09.00 – 12.00 น. ณ โรงแรม Vic3 Bangkok นำเสนอร่างรายงานวิจัยฉบับสมบูรณ์โครงการวิจัย “ข้อจำกัดของกระบวนการยุติธรรมเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม (Romance Scam) และแนวทางสร้างความตระหนักรู้ให้กับประชาชน” และ แนะนำคู่มือ “การป้องกันและปราบปรามพิศวาสอาชญากรรม”

3) คู่มือ 2 เล่ม

3.1) คู่มือป้องกันพิศวาสอาชญากรรม ฉบับผู้ดูแลระบบและผู้บังคับใช้กฎหมาย

3.2) คู่มือป้องกันพิศวาสอาชญากรรม ฉบับประชาชน

1.8.3 Impact

1) เกิดการพัฒนามาตรการป้องกันและปราบปรามพิศวาสอาชญากรรม รวมถึงการพัฒนาระบบระวังความเสี่ยงและเตือนภัยล่วงหน้าให้สามารถนำมาใช้ป้องกันและค้นหาอาชญากรได้อย่างมีประสิทธิภาพต่อไป

2) ประชาชนเกิดความตระหนักรู้ถึงภัยของการเปิดเผยข้อมูลส่วนบุคคลให้คนแปลกหน้าเข้าถึง และรู้เท่าทันการล่อลวงของอาชญากรรมไซเบอร์

การเผยแพร่ความรู้กับพิศวาสอาชญากรรม และ แนวทางการป้องกันและปราบปรามพิศวาสอาชญากรรม (Romance Scam) ให้กับผู้บังคับใช้กฎหมาย ผู้ดูแลระบบและประชาชนทั่วไป โดยการส่งคู่มือคู่มือป้องกันพิศวาสอาชญากรรม ฉบับผู้ดูแลระบบและผู้บังคับใช้กฎหมาย / คู่มือป้องกันพิศวาสอาชญากรรม ฉบับประชาชน ให้กับหน่วยงาน/องค์กรต่าง ๆ ที่เกี่ยวข้อง และเผยแพร่ออนไลน์ในรูปแบบของ E-book ซึ่งมีหน่วยงาน/องค์กรที่จะจัดส่งคู่มือ ดังนี้

หน่วยงาน / องค์กรที่เกี่ยวข้อง

- ห้องสมุดในสถาบันศึกษา / มหาวิทยาลัย
- ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.)
- กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) (TCSD)
- กองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ
- กองบังคับการตำรวจท่องเที่ยว

เพจเตือนภัยพิศวาสอาชญากรรม

- เพจ ภัยผู้หญิง ในโลกออนไลน์
- เพจ Thai Anti Scam (สาวไทยรู้ทันกลลวง)

เพจ / เว็บไซต์สื่อกลางหาคู่

- Noonswoon
- Love4all
- Thaiflirting
- Koo25up
- Kooup
- Thaifriendly
- แม่สื่อแม่ชัก
- esync

1.9 กระบวนการผลักดันผลงานออกสู่การใช้ประโยชน์

1) การตีพิมพ์

การตีพิมพ์ในวารทางกฎหมายระดับ TCI 1 หรือ การนำเสนอบทความในเวทีประชุมระดับชาติ โดยนักวิจัยได้นำเสนอบทความในเวทีประชุมระดับชาติ ดังนี้

- การนำเสนอบทความ “รู้หน้าไม่รู้ใจเชื่อใครไม่ได้อีก: พิศวาสอาชญากรรม (Romance Scam) และความเสี่ยงในโลกไซเบอร์” โดย ผศ.ดร.ทศพล ทรรศนกุลพันธ์ ในการประชุมวิชาการทางมานุษยวิทยาครั้งที่ 13 “มนุษย์ในโลกดิจิทัล” เมื่อวันที่ 4 กรกฎาคม 2562 ณ ศูนย์มานุษยวิทยาสิรินธร (องค์การมหาชน)

- การนำเสนอบทความ “พิศวาสอาชญากรรม กับ กฎหมายไซเบอร์ใต้กรอบรัฐสมัยใหม่ (Romance Scam and Cyber Law in Modern State Realm)” ในการประชุม 10th National and International Conference on Humanities and Social Sciences, 28-29 October 2019 at Prince of Songkla University, Phuket Campus, Phuket, Thailand

2) การใช้ประโยชน์เชิงสาธารณะ โดยเผยแพร่ความรู้ สร้างการตระหนักรู้/การเรียนรู้ให้สังคม

การพัฒนาองค์ความรู้ในการรักษาความลับข้อมูลส่วนบุคคลแก่ประชาชนทั่วไป และการสร้างความสามารถในการระวังภัยให้กับผู้ใช้เว็บไซต์หาคู่และเครือข่ายสังคม ผ่านเวทีเสวนา และจัดทำคู่มือ 2 เล่ม (สำหรับประชาชนทั่วไป และสำหรับผู้ดูแลระบบและบังคับใช้กฎหมาย) โดยได้มีการเผยแพร่ผลวิจัยสู่สื่อสาธารณะ ดังต่อไปนี้

1. การให้สัมภาษณ์รายการเปิดบ้าน Thai PBS “รู้เท่าทันกลโกง Romance Scam แสร้งรักออนไลน์” ออกอากาศ เมื่อวันที่ 3 ส.ค. 2562 http://program.thaipbs.or.th/Openthaipbs/episodes/62309

2. ข่าว “นักวิจัยเผยปมหญิงโสดวัย 40 ต้องรู้ก่อนเป็นเหยื่อ พบรักออนไลน์” โดยผู้จัดการออนไลน์ เผยแพร่ เมื่อ 27 ส.ค. 2562 เวลา13:25 น. https://mgronline.com/

3. ข่าว “สาวโสด วัย 40- 60 การศึกษาดี – ฐานะมั่นคง แชมป์เหยื่อ Romance Scam” โดย PPTV Online เผยแพร่เมื่อ 28 ส.ค. 2562 เวลา 14:50 น. https://www.pptvhd36.com /news/

4. รายงานพิเศษ 'Romance Scam พิศวาสอาชญากรรม(ออนไลน์)' งานวิจัยชี้นักต้มตุ๋นมักสร้างบุคลิก 'คนดี 7 ลักษณะ' ให้เหยื่อเชื่อใจ โดยประชาไท เผยแพร่ 31 ส.ค. 2562 เวลา13:23 น. https://prachatai.com/journal/2019/08/84121

5. ข่าวประชาสัมพันธ์ สกสว. นักวิจัยเผยปม ‘พิศวาสอาชญากรรม’ หญิงโสด 40 อัพเหยื่อ “พบรักออนไลน์”เผยแพร่เมื่อ วันพฤหัสบดีที่ 29 สิงหาคม 2562 https://www.trf.or.th/ medicine -public-health-news/14033-romance-scam

6. การให้สัมภาษณ์แนวทางการป้องกันพิศวาสอาชญากรรม รายการข่าวภาคค่ำ Thai PBS ออกอากาศ เมื่อวันที่ 8 ส.ค.2562 https://www.facebook.com/tpbsnorth/videos/ 888570921524773/?t=166

7. ข่าว theisaander “ข่อยลักเจ่า : เริ่มจากรัก สุดท้ายได้เสีย... เงินทอง สาวอีสานระวังเด้อ” เผยแพร่เมื่อวันที่ 15 กันยายน 2562 https://www.theisaander.com/post/190915 romancescam?fbclid=IwAR1fVkNQwQLWk1-w2bJg2qeXAIO9n8PjDV0bA2wGYrMTaUbI7 lBIbwWUVOc

8. การเผยแพร่ข้อมูลการป้องกันพิศวาสอาชญากรรม โดย เพจ The Youngster เผยแพร่เมื่อวันที่ 27 กันยายน 2562 https://www.facebook.com/TheYoungsterTH/

9. การเผยแพร่ คู่มือป้องกันพิศวาสอาชญากรรม ฉบับผู้บังคับใช้กฎหมาย โดย ศูนย์ข้อมูลและข่าวสืบสวนเพื่อสิทธิพลเมือง Thai Civil Rights and Investigative Journalism (TCIJ) เผยแพร่เมื่อวันที่ 9 ตุลาคม 2562 https://www.tcijthai.com/news/2019/10/ebook/9472

10. การเผยแพร่ คู่มือป้องกันพิศวาสอาชญากรรม ฉบับประชาชน โดย ศูนย์ข้อมูลและข่าวสืบสวนเพื่อสิทธิพลเมือง Thai Civil Rights and Investigative Journalism (TCIJ) เผยแพร่เมื่อวันที่ 9 ตุลาคม 2562 https://www.tcijthai.com/news/2019/10/ebook/9470

11. การเผยแพร่บทความเรื่อง “การรวบรวมพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์” เขียนโดย สรชา สุเมธวานิชย์, ทศพล ทรรศนกุลพันธ์ ศูนย์ศึกษากฎหมายกับเทคโนโลยี เผยแพร่ทางเว็บประชาไท เมื่อวันที่ 3 ธันวาคม 2562 https://prachatai.com/journal/2019/ 12/85402

3) การใช้ประโยชน์เชิงนโยบาย และช่องทางการส่งข้อเสนอเชิงนโยบายสู่ผู้กำหนดนโยบาย

- พัฒนากระบวนการยุติธรรมที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ในลักษณะล่อลวงผ่านข้อเสนอแนะในงานวิจัยฉบับสมบูรณ์

- ได้มีการส่งผ่านแนวทางพัฒนาระบบระวังภัยและเตือนล่วงหน้าให้กับผู้ดูแลระบบเว็บไซต์หาคู่และเครือข่ายสังคม และสร้างระบบค้นหารูปแบบพฤติกรรมพิศวาสอาชญากรรมให้แก่เจ้าพนักงานที่ปราบปรามคดีเกี่ยวกับเทคโนโลยี และคดีเกี่ยวกับเด็กและสตรีในเวทีเผยแพร่งานวิจัยร่วมกับผู้มีส่วนได้เสียและใช้ประโยชน์

- ได้มีการพูดคุยแลกเปลี่ยนกับเจ้าพนักงานที่ปฏิบัติหน้าที่ป้องกันและปราบปรามพิศวาสอาชญากรรมโดยตรง และผู้ดูแลระบบของเว็บไซต์หาคู่และเครือข่ายสังคม การเผยแพร่คู่มือสู่สาธารณชนและสื่อมวลชน รวมถึงจัดเวทีเสวนาสาธารณะให้ผู้มีส่วนเกี่ยวข้องทั้งหลายเข้าร่วม

1.10 ปัญหาอุปสรรค

การขอพบและสัมภาษณ์ผู้ดูแลระบบ เพจและเว็บไซต์หาคู่ เนื่องจากทางผู้ดูแลระบบ เพจและเว็บไซต์หาคู่ให้เหตุผลทางเพจและเว็บไซต์มีกระบวนการป้องกันเกี่ยวกับพิศวาสอาชญากรรมแล้ว หรือบางระบบก็เพิกเฉยละเลยไม่ใส่ใจต่อการติดต่อประสานงานจากนักวิจัย จึงไม่ได้ให้ความร่วมมือการให้สัมภาษณ์กับทางนักวิจัย มีเพียงเพจภัยผู้หญิงในโลกออนไลน์ ที่ให้สัมภาษณ์/ข้อมูล ซึ่งทีมวิจัยได้ติดต่อเพจและเว็บไซต์หาคู่ เป็นจำนวน 10 เพจ/เว็บไซต์ ดังนี้

1) เพจ ภัยผู้หญิง ในโลกออนไลน์ (เป็นกลุ่มเดียวที่ให้ความร่วมมือในการวิจัยและเผยแพร่)
2) เพจ Thai Anti Scam (สาวไทยรู้ทันกลลวง)
3) Noonswoon
4) Love4all
5) Thaiflirting
6) Koo25up
7) Kooup
8) Thaifriendly
9) แม่สื่อแม่ชัก
10) esync

บทที่ 2

ทบทวนวรรณกรรม

บทนี้ประกอบไปด้วยการทบทวนวรรณกรรม 2 ส่วนหลัก คือ 1) การทบทวนวรรณกรรมที่เป็นงานวิชาการเกี่ยวกับการศึกษาวิจัยเรื่องพิศวาสอาชญากรรมทั้งทางตรงและทางอ้อมหรือเอกสารต่างๆ ที่รายงานสถานการณ์รูปแบบวิธีการก่ออาชญากรรมไปจนถึงข้อจำกัดในการดำเนินคดีกับอาชญากรและการเยียวยาเหยื่อผู้เสียหาย 2) การทบทวนวรรณกรรมเกี่ยวกับแนวคิดทฤษฎีที่สามารถนำมาปรับใช้เป็นกรอบแนวคิดเพื่อการวิเคราะห์ข้อมูลและสังเคราะห์ข้อเสนอแนะในการแก้ไขปัญหา โดยผลจากการทบทวนวรรณกรรมทำให้เห็นความก้าวหน้าและข้อจำกัดในการป้องกันและปราบปรามพิศวาสอาชญากรรมได้ ดังต่อไปนี้

2.1 การทบทวนวรรณกรรมที่เกี่ยวกับการศึกษาวิจัยเรื่องพิศวาสอาชญากรรม

งานวิจัยนี้ทำการศึกษากฎหมายที่ป้องกันและปราบปรามการล่อลวงผู้ใช้อินเตอร์เน็ตมิให้ตกเป็นเหยื่อของอาชญากรรม (Romance Scam) ซึ่งในส่วนนี้จะเป็นการศึกษา ทบทวนเอกสารที่มีความเกี่ยวข้องกับพฤติกรรมของการใช้อินเตอร์เน็ต การล่อลวงผ่านสื่อออนไลน์ รวมถึงบทบัญญัติกฎหมายที่มีความเกี่ยวข้องกับการกระทำความผิดดังกล่าวด้วย โดยมีการแบ่งเนื้อหาในการทบทวนออกเป็น 3 ส่วน ดังนี้ **ส่วนแรก** พฤติกรรมการใช้สื่อสังคมออนไลน์ ในส่วนนี้จะแสดงให้เห็นพฤติกรรมต่างๆ ที่เกิดขึ้นจากการใช้สื่อออนไลน์ เนื่องด้วยความเป็นอิสระทางพื้นที่ ความสะดวกและรวดเร็วต่อการใช้งานบนสื่อออนไลน์ รวมถึงการสร้างความสัมพันธ์กับบุคคลอื่นบนโลกออนไลน์ได้อย่างรวดเร็ว และความเป็นนิรนามของผู้ใช้สื่อออนไลน์ด้วย ซึ่งปัจจัยทั้งหลายนี้ถือเป็นพฤติกรรมที่มีความเสี่ยงต่อการถูกล่อลวงบนโลกอินเตอร์เน็ตได้ **ส่วนที่สอง** ศึกษารูปแบบและวิธีการล่อลวงบนสื่อออนไลน์ ในส่วนนี้จะขยับขอบเขตการศึกษาออกมาให้ใกล้เคียงกับพฤติกรรมการล่อลวงแบบพิศวาสอาชญากรรมมากที่สุด และจะทำการศึกษาทั้งงานวิจัยของไทยและต่างประเทศ เพื่อให้เข้าใจมากยิ่งขึ้นถึงพฤติกรรมการล่อลวงดังกล่าวกลายเป็นอาชญากรรมทางคอมพิวเตอร์ที่รุนแรงได้อย่างไร และ**ส่วนที่สาม** เป็นการศึกษาเกี่ยวกับบทบัญญัติทางกฎหมายที่เกี่ยวข้อง และกระบวนการบังคับใช้กฎหมาย ในส่วนนี้จะแสดงให้เห็นถึงข้อจำกัดที่เกิดขึ้นของกระบวนการยุติธรรม เพื่อนำไปสู่การตั้งคำถามการวิจัยและการวางสมมติฐานงานวิจัยต่อไปได้

<u>ส่วนที่หนึ่ง</u> พฤติกรรมการใช้สื่อสังคมออนไลน์และความเป็นอิสระทางสังคมออนไลน์

เมื่อยุคสมัยของโลกเปลี่ยนไป ส่งผลให้อินเตอร์เน็ตกลายเป็นปัจจัยสำคัญในการดำรงชีวิตสำหรับคนส่วนใหญ่ ไม่ว่าจะอยู่ในพื้นที่ใดส่วนมากผู้คนสามารถเข้าถึงอินเตอร์เน็ตได้ ทั้งเด็กที่สามารถเข้าถึงเกมส์ออนไลน์ได้อย่างง่ายดาย ผู้ใหญ่ที่ใช้โลกอินเตอร์เน็ตเป็นเครือข่ายหรือสังคมในการแลกเปลี่ยนข้อมูลข่าวสารกัน พูดคุยกับผู้คนในอีกซีกโลกหนึ่งได้ทุกเวลา การใช้อินเตอร์เน็ตในทุกวันกลายเป็นปัจจัยหนึ่งที่คนส่วนใหญ่ไม่คำนึงถึงความอันตรายที่แอบแฝงอยู่ในมุมเงียบ

เมื่อพฤติกรรมการใช้สื่อออนไลน์ส่งผลกระทบกับชีวิตประจำวันของผู้คนเป็นอย่างมากจึงมีผู้ศึกษาถึงแนวคิดทางอาชญากรรมคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ ซึ่งในความเข้าใจของคนทั่วไปแล้ว มีปัญหาความยุ่งยากและสับสนในการจำกัดความหมายอย่างมาก ในงานของ **สาวตรี สุขศรี** ในบทความวิชาการเรื่อง **อาชญากรรมคอมพิวเตอร์/ไซเบอร์กับทฤษฎีอาชญาวิทยา**[1] ได้อธิบายไว้ว่า อาชญากรรมคอมพิวเตอร์/ไซเบอร์ในขอบเขตของอาชญาวิทยา ในความเข้าใจโดยทั่วไปย่อมหมายถึงการศึกษาพฤติกรรมของอาชญากรหรือผู้กระทำความผิดเพื่อค้นหาว่าสาเหตุที่ทำให้บุคคลเหล่านี้ประกอบอาชญากรรมคอมพิวเตอร์/ไซเบอร์คืออะไร ซึ่งก็เป็นความยุ่งยากในการให้คำจำกัดความที่ชัดเจน ซึ่งการจำแนกประเภทของความผิดทางคอมพิวเตอร์มีหลายความคิดเห็น ฝ่ายหนึ่งให้ความเห็นว่า เป็นอาชญากรรมรูปแบบใหม่ ส่วนอีกฝ่ายบอกว่า เป็นการทำอาชญากรรมในรูปแบบเก่า เพียงแต่การกระทำนั้นไปเกิดอยู่บนพื้นที่ใหม่ ซึ่งก็ยังไม่ได้ข้อสรุปชัดว่า เหตุผลของฝ่ายใดที่ถูกต้อง ชัดเจนที่สุด แม้กระทั่งคำว่า อาชญากรรมไซเบอร์ ทางคณะมนตรียุโรปก็มิได้มีการบัญญัตินิยามของไว้อย่างชัดเจน คงจะมีความมุ่งหมายให้แต่ละประเทศที่ร่วมลงนามได้กำหนดคำนิยาม หรือขอบเขตในแบบฉบับที่สอดคล้องกับบริบททางสังคมของตนเอง โดยก็ยึดเอาอนุสัญญาดังกล่าวเป็นแนวทางหรือกรอบกว้างๆ เท่านั้น

ทั้งนี้ในมุมมองของนักกฎหมาย เพื่อใช้เป็นฐานในการทำความเข้าใจในบทความนี้ โดยจะให้คำอธิบายของ “อาชญากรรมทางคอมพิวเตอร์”ว่าการกระทำใดๆ ที่ฝ่าฝืนต่อบทบัญญัติแห่งกฎหมายโดยผู้กระทำอาศัยความรู้ด้านเทคโนโลยีคอมพิวเตอร์ในการกระทำผิด ไม่ว่าลักษณะของการกระทำนั้นจะเป็นการใช้คอมพิวเตอร์เป็นเครื่องมือ หรือมีระบบหรือข้อมูลคอมพิวเตอร์เป็นเป้าหมายซึ่งจำเป็นต้องอาศัยบุคลากรที่มีความรู้ความสามารถทางเทคโนโลยีคอมพิวเตอร์เข้ามาดำเนินการกับผู้กระทำความผิด ตั้งแต่กระบวนการสืบสวนสอบสวน การฟ้องร้อง ตลอดจนการพิจารณาคดี เพื่อลงโทษ[2]

การกระทำที่เป็นความผิดในอาชญากรรมทางคอมพิวเตอร์/ไซเบอร์ ก็มีแนวคิดทฤษฎีหลากหลายแนว ทั้งแนวคิดดั้งเดิมของ Robert K. Merton ผู้พัฒนา “ทฤษฎีความกดดัน” (Strain Theory) อธิบายว่า สาเหตุของการเกิดขึ้นของอาชญากรรมเกิดจากความขัดแย้งที่เกิดขึ้นระหว่างความคาดหวังของสังคมกับความสามารถในการบรรลุตามเป้าหมายตามที่สังคมคาดหวังไว้ ความสิ้นหวังที่เกิดจากการไม่สามารถบรรลุเป้าหมายที่สังคมคาดหวังได้นั้น จะทำให้เกิดพฤติกรรมเบี่ยงเบนจนนำไปสู่การประกอบอาชญากรรมในที่สุด และในทฤษฎีนี้ Merton บอกว่ามักจะเกิดกับ “คนชนชั้นล่างหรือคนชั้นต่ำ” เพราะเป็นผู้ที่ได้รับผลกระทบอย่างมากที่สุด โดยคนชนชั้นล่างจะมีนัยของการแสดงให้สังคมเห็นว่าเป็นผู้ถูกกระทำจากผู้มีอำนาจเหนือผู้ถูกกระทำ

ทฤษฎีความกดดัน ถูกนำไปทดสอบเพื่ออธิบายพฤติกรรมอันธพาล หรือ “การกลั่นแกล้งออนไลน์” (Cyberbullying) โดยการกระทำดังกล่าวมักจะเกิดขึ้นในกลุ่มเด็กและวัยรุ่นอีกด้วย โดยมีนัยของการแสดงให้สังคมเห็นถึงผู้มีอำนาจเหนือผู้ถูกกระทำ ซึ่งในโลกออฟไลน์การกระทำดังกล่าวผู้กระทำไม่สามารถกระทำได้ ไม่ว่าจะด้วยความคาดหวังจากทางครอบครัว หรือสังคมที่ผู้กระทำอยู่ด้วย ผู้กระทำจึงแสดงออกผ่านพื้นที่บนโลกออนไลน์ ซึ่งการแสดงออกดังกล่าวสามารถใช้อธิบายได้ทั้งพฤติกรรมอันธพาลแบบดั้งเดิม และพฤติกรรมอันธพาลที่เกิดขึ้นในโลกออนไลน์ แต่มีการตั้งข้อสังเกตว่า

---

[1] สาวตรี สุขศรี, (2560), อาชญากรรมคอมพิวเตอร์/ไซเบอร์กับทฤษฎีอาชญาวิทยา, *วารสารนิติศาสตร์,* ปีที 46 ฉบับที่ 2 (มิถุนายน 2560)

[2] เรื่องเดียวกัน. หน้า 420

การกระทำบนพื้นที่ออนไลน์นั้น ไม่แสดงถึงสภาพร่างกาย คือเหมือนกับว่าร่างกายไม่โดนทำร้าย แต่โดนสภาพจิตใจมากกว่า

และนักสังคมวิทยาและอาชญาวิทยาอีกคนหนึ่ง ที่อธิบายว่าการเกิดอาชญากรรมมีผลมาจากทางเศรษฐกิจ ชี้ให้เห็นว่าการเกิดอาชญากรรมไม่จำเป็นต้องเป็น “คนชั้นล่าง” เสมอไป เพราะคนชั้นกลางหรือคนชั้นสูงก็เป็นอาชญากรได้ โดยอธิบายผ่านทาง “ทฤษฎีคบค้าสมาคมที่แตกต่าง” (Different Association Theory) ของ Edwin H. Sutherland ซึ่งประเด็นสำคัญของทฤษฎีคบค้าสมาคมที่แตกต่างจากทฤษฎีความกดดันคือ ความเป็นอาชญากรสามารถเรียนรู้กันได้โดยการติดต่อสัมพันธ์กันอย่างใกล้ชิด โดยกระบวนการเรียนรู้สามารถเกิดได้หลากหลายรูปแบบไม่ว่าจะเป็นการอบรมสั่งสอน การเกิดแรงบันดาลใจรวมทั้งการเลียนแบบ เพียงแต่การถ่ายทอดจะเกิดขึ้นได้ก็ต่อเมื่อมีความใกล้ชิดและใช้ระยะเวลาที่เหมาะสม มิใช่เพียงชั่วคราวหรือพบปะกันอย่างฉาบฉวย

นอกจากแนวคิดดั้งเดิมอย่าง Merton และ Sutherland แล้ว ยังมีความพยายามในการนำเอาทฤษฎีต่างๆ มาใช้อธิบายสาเหตุการเกิดอาชญากรรมทางคอมพิวเตอร์/ไซเบอร์ ด้วย ไม่ว่าจะเป็นทฤษฎีของนักอาชญาวิทยาชาวอินเดีย K. Jaishankar ใน “ทฤษฎีการเปลี่ยนพื้นที่” (Space Transition Theory) โดยทฤษฎีนี้ขยายขอบเขตการศึกษาไปจนสามารถอธิบายถึง “อาชญาวิทยาไซเบอร์” (Cyber Criminology) ได้ และได้ให้คำนิยามคำดังกล่าวว่า “*การศึกษาสาเหตุของการก่ออาชญากรรมที่เกิดขึ้นในโลกไซเบอร์และผลกระทบในพื้นที่ทางกายภาพ*”[3] โดยการทฤษฎีของ Jaishankar อาศัยความรู้แบบสหวิทยาการ ไม่ว่าจะมีข้อมูลเชิงลึกจากทั้งทางสังคมและวิทยาศาสตร์คอมพิวเตอร์มาประกอบกัน พร้อมทั้งยังต้องทำความเข้าใจกับเทคโนโลยีคอมพิวเตอร์และธรรมชาติที่แตกต่างของพื้นที่ไซเบอร์ (Cyberspace) กับโลกทางกายภาพ หรือโลกออฟไลน์ (Physical space) ซึ่งเขาได้อธิบายทฤษฎีไว้ว่า “โดยธรรมชาติของมนุษย์นั้นพฤติกรรมของพวกเขามักเปลี่ยนแปลงไปเมื่อมีการเคลื่อนย้ายหรือเปลี่ยนแปลงพื้นที่ ซึ่งพฤติกรรมที่แสดงออกมามีได้ทั้งที่สอดคล้อง และไม่สอดคล้องกันในระหว่างสองพื้นที่” ซึ่งข้อสมมติฐานของการเกิดอาชญากรรมไซเบอร์ประกอบด้วย พฤติกรรมดังนี้[4]

1. คนทั่วไปมักชั่งน้ำหนักความเสี่ยงทั้งทางกฎหมายและทางสังคมระหว่างการกระทำความผิดของตนในพื้นที่ทางกายภาพกับพื้นที่ในโลกไซเบอร์ ซึ่งพวกเขาจะไม่ใส่ใจสิ่งนี้ในโลกไซเบอร์ เนื่องจากไม่มีคนคอยจับตาหรือตีตราพวกเขาอยู่ การกระทำความผิดจึงเกิดขึ้นได้ง่ายกว่าโดยไม่ต้องชั่งน้ำหนักผลเสียของอะไร

2. ความยืดหยุ่นจากการปิดบังตัวตนได้ และการขาดปัจจัยในการป้องปราม ทำให้โลกไซเบอร์เป็นพื้นที่ในการกระทำความผิด ด้วยสมาชิกในสังคมกายภาพส่วนใหญ่ต้องมีความซื่อสัตย์ หรือต้องทำสิ่งที่ถูกต้องต่อกัน ก็เพราะกลัวการถูกจับได้ เมื่อโลกไซเบอร์สร้างพื้นที่ที่ยากแก่การตรวจจับ จึงทำให้คนกล้าที่จะแสดงอารมณ์ความรู้สึกอันไม่พึงประสงค์ เช่น กล้าล่วงละเมิดบุคคลอื่น

3. พฤติกรรมที่เป็นอาชญากรรมในโลกไซเบอร์มีแนวโน้มที่จะถูกกระทำในโลกทางกายภาพ และเช่นเดียวกันพฤติกรรมอาชญากรรมในโลกทางกายภาพก็สามรถถูกนำไปกระทำในพื้นที่ในโลกไซเบอร์ เช่น ผู้ที่มีพฤติกรรมชอบล่วงละเมิดทางเพศเด็กและเยาวชนในโลกกายภาพ ก็มักเป็นผู้เผยแพร่สื่อลามกอนาจารเด็กในเครือข่ายอินเตอร์เน็ตด้วย

---

[3] เรื่องเดียวกัน. หน้า 422.

[4] เรื่องเดียวกัน. หน้า 429.

4. ธรรมชาติของโลกไซเบอร์ที่จะมีความไหลลื่น ไม่หยุดนิ่ง (Dynamic) ซึ่งอาจจะเป็นการเปิดช่องทางให้ผู้กระทำผิดหลบหนีได้ หมายความว่า มนุษย์ไม่ได้อาศัยหรือใช้ชีวิตอยู่บนโลกไซเบอร์ตลอดเวลา เหมือนกับโลกทางกายภาพ อินเตอร์เน็ตเป็นเพียงพื้นที่ที่ผู้คนสามารถแวะเข้ามาทำกิจกรรมและก็ออกไปได้ ซึ่งในโลกไซเบอร์ก็มีการเปลี่ยนอยู่ตลอดเวลา เนื้อหาหรือประเด็นที่ถูกโพสต์ลงสามารถถูกเผยแพร่ได้อย่างรวดเร็ว ซึ่งก็ส่งผลให้การสืบหาต้นตอของแหล่งข้อมูลทำได้ยากด้วยเช่นกัน

5. เกิดการสมาคมในโลกไซเบอร์ได้ง่าย จากการศึกษาพบว่า อินเตอร์เน็ตเป็นพื้นที่สื่อกลางที่มีประสิทธิภาพในการหาสมัครพรรคพวก และด้วยอัลกอลิทึ่ม (algorithm) ที่มักจะแสดงเนื้อหาที่ผู้ใช้งานสนใจ หรือเป็นไปในแนวทิศทางเดียวกันขึ้นมาให้ผู้ใช้งานอยู่ตลอดเวลา ทำให้การที่จะสร้างสมาคมหรือกลุ่มคนที่มีความสนใจที่เหมือนกันก็ย่อมที่จะทำได้ง่ายกว่า การสร้างกลุ่มในโลกกายภาพ

6. ผู้คนที่อยู่ในสังคมปิด (Close societies) มีแนวโน้มที่จะประกอบอาชญากรรมในโลกไซเบอร์ได้ง่ายกว่าผู้ที่อยู่ในสังคมเปิด (Open societies) อย่างเช่น กลุ่มคนที่อยู่ในสังคมปิดที่ต้องอาศัยความรุนแรง เมื่อต้องมีการเปลี่ยนแปลงบางสิ่งบางอย่าง ก็จะไม่มีเสรีภาพในแบบที่สังคมเปิดมี ซึ่งประชาชนกลุ่มสังคมเปิด สามารถมีการแสดงความคิดเห็นได้อย่างกว้างขวาง รวมถึงสามารถมีส่วนร่วมทางการเมืองได้ ก็จะมีแนวโน้มที่จะกระทำความผิดบนโลกออนไลน์น้อยกว่าคนที่อาศัยความรุนแรงและไม่สามารถแสดงออกได้ จึงไปปลดปล่อย ในพื้นที่ไซเบอร์แทน

7. ความขัดแย้งกันระหว่างมาตรฐานและคุณค่าของโลกกายภาพ กับโลกไซเบอร์ ทำให้นำไปสู่การเกิดอาชญากรรมไซเบอร์

จากแนวคิดในข้างต้นของ Jaishankar สามารถปรับใช้กับพฤติกรรมการใช้สื่อออนไลน์ได้อย่างมาก เพราะกลุ่มคนที่ใช้สื่อมีหลากหลายประเภทและหลายช่วงอายุ และสื่อออนไลน์ก็มีอยู่หลายประเภท ซึ่งก็รับรองในทุกๆ กลุ่มเป้าหมาย ทั้งสื่อสังคมออนไลน์ในแบบที่เสียเงินในการใช้งาน และแบบที่ผู้สร้างสื่อสังคมออนไลน์อนุญาตให้เข้าใช้งานได้โดยไม่เสียค่าใช้จ่ายใดๆ โดยผู้ใช้งานส่วนใหญ่พบว่าเป็นวัยรุ่นในช่วงอายุ 19-21 ปี โดยจากงานของ **นุชรีรัตย์ ขวัญคำ**[5] ศึกษางานวิจัยเรื่อง **รูปแบบการใช้สื่ออินเตอร์เน็ตของลุ่มวัยรุ่นในเขตกรุงเทพ** ได้อธิบายพฤติการณ์การใช้สื่อออนไลน์ของกลุ่มวัยรุ่นไว้ว่าจากการศึกษาลักษณะประชากรของกลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิงมากกว่าเพศชาย และมีอายุระหว่าง 19-21 ปี โดยลักษณะการใช้สื่ออินเตอร์เน็ตของกลุ่มวัยรุ่นนั้นจะมีการตอบสนองความต้องการของตนเองด้านการแสวงหาเพื่อนต่างเพศ ความต้องการเข้าสู่จินตนาการ ความต้องการที่จะประสบความสำเร็จ ความต้องการเป็นส่วนหนึ่งของสังคม รวมถึงความต้องการมีปฏิสัมพันธ์กับทุกคน โดยลักษณะการใช้สื่ออินเตอร์เน็ต พบว่า จะใช้สื่อออนไลน์ 1-7 ครั้งต่อสัปดาห์ ซึ่งผู้ใช้งานเห็นว่าอินเตอร์เน็ตเป็นสิ่งที่สะดวกสบาย สามารถยืดหยุ่นได้ในเรื่องเวลา และใช้งานได้ในทุกสถานที่ ซึ่งวิธีการใช้สื่อนั้นไม่ต้องระบุชื่อจริงของตนเอง ประกอบกับไม่ต้องเห็นหน้าซึ่งกันและกัน ทำให้รู้สึกดี มีสถานภาพเท่าเทียมกัน อีกทั้งยังสามารถปรับเปลี่ยนอัตลักษณ์ของตนเองได้ตลอดเวลา นอกจากนี้ ยังพบว่าความสามารถทางสื่ออินเตอร์เน็ตเป็นการโต้ตอบสื่อสารแบบสองทาง และเข้าถึงข้อมูลต่าง ๆ ได้ง่าย

[5] นุชรีรัตน์ ขวัญคำ, (2549), *รูปแบบการใช้สื่ออินเตอร์เน็ตของกลุ่มวัยรุ่นในเขตกรุงเทพมหานคร*, วิทยานิพนธ์นิเทศศาสตร์มหาบัณฑิต มหาวิทยาลัยธุรกิจบัณฑิตย์.

ซึ่งก็เป็นไปในทิศทางเดียวกับงานของ **พชรมน พิรินะสกุลยิ่ง**[6] เรื่อง **กระบวนการสร้างกลุ่มเพื่อนโดยการสนทนาแบบออนไลน์: ศึกษากรณีกลุ่มเพื่อนมิตรภาพ** พบว่า ปฏิสัมพันธ์แบบออนไลน์มีรูปแบบของพฤติกรรมที่เข้าถึงง่าย โดยเฉพาะความสัมพันธ์ในแบบของเพื่อน โดยปฏิสัมพันธ์แบบออนไลน์สามารถตอบสนองความผูกพันรักใคร่จากเพื่อนได้ดีกว่าแบบออฟไลน์ เพราะสื่อออนไลน์ทำให้พบกับเพื่อนต่างสถานที่ เพื่อนที่รู้จักกันมานานและไม่ได้เจอกัน รวมถึงเพื่อนจากประเทศหรือจากกลุ่มอื่นๆ ด้วย โดยกลุ่มเพื่อนออนไลน์สามารถทดแทนกลุ่มเพื่อนในสังคมสมัยใหม่ได้สำหรับบุคคลที่มีแนวคิดว่า การสนทนาแบบออนไลน์นั้นเป็นเครื่องมือที่จะช่วยในการสร้างมิตรภาพ โดยสามารถสนทนากับใครก็ได้โดยไม่มีข้อแม้ หรือเงื่อนไข แต่ในสังคมจริงไม่สามารถทำได้ เมื่อเริ่มรู้จักกันแล้วสนทนากันด้วยความเข้าใจ ก็จะมีการนัดพบ นัดเจอกันได้และตกลงที่จะเป็นเพื่อนที่ดีต่อกันต่อไป หรือเริ่มความสัมพันธ์หรือสถานะอื่นต่อไปได้

จากงานศึกษาของทั้ง**นุชรีรัตย์** และ **พชรมน**ยิ่งทำให้เห็นว่าอินเตอร์เน็ตกลายเป็นสิ่งที่เชื่อมความสัมพันธ์ต่างๆ ได้อย่างง่ายดาย และรวดเร็ว การพัฒนาไปของเทคโนโลยีต้องสอดคล้องกับการใช้ชีวิตของผู้คนส่วนใหญ่ นอกจากการสนทนากับกลุ่มเพื่อนของผู้ใช้งานแล้วนั้น ผู้ใช้งานอินเตอร์เน็ตสามารถพูดคุย สื่อสาร หรือแลกเปลี่ยนข้อมูลต่างๆ กับบุคคลอื่นที่ไม่รู้จักได้ด้วยเช่นกัน ในงานของ**ศุนิสา ทดลา**เรื่อง **รูปแบบพฤติกรรมการสื่อสารในห้องสนทนาบนเครือข่ายอินเตอร์เน็ต**[7] ได้อธิบายไว้ว่า รูปแบบพฤติกรรมการสื่อสารของผู้สนทนา ไม่ว่าจะเป็น www.pantip.com, www.hunsa.com และ www.sanook.com พบว่า ผู้สนทนามีอิสระเสรีในการแสดงออก ในการสื่อสารอย่างไร้ขอบเขต นอกจากนี้ผู้สนทนาจะใช้ข้อความในการติดต่อสื่อสารตลอดจนสัญลักษณ์ในการแสดงออกถึงอารมณ์และความรู้สึกในการสนทนา อีกทั้งผู้สนทนาจะคิดเพื่อสร้างคำและรูปแบบประโยคใหม่ๆขึ้นมา ซึ่งเป็นลักษณะเฉพาะของรูปแบบการสื่อสารผ่านตัวกลางด้วยคอมพิวเตอร์ เป็นปัจจัยที่มีอิทธิพลต่อการแสดงพฤติกรรมการสื่อสารของผู้สนทนา ประกอบด้วยลักษณะที่เป็นชุมชนจำลอง สภาวะไร้การขัดขวางและการควบคุม การไร้ขอบเขตในการสร้างความหมาย การไม่รู้จักผู้ที่สื่อสารด้วย การปลอมตัว การหลอกลวง ความเป็นตัวตนหลากหลาย การเปลี่ยนเพศ การสร้างจินตนาการ นอกจากนี้ยังมีปัจจัยทางด้านจิตวิทยาสังคม ได้แก่ แนวคิดเกี่ยวกับตนเอง รวมทั้งทัศนคติ ความเชื่อ ค่านิยม และความเห็นอีกส่วนหนึ่งด้วย

ด้วยความสัมพันธ์บนโลกออนไลน์ ที่สร้างโดยรู้จักกันผ่านเพียงรูปโปรไฟล์ และความคิดเห็นที่คล้ายกันบ้าง ทำให้เกิดความไว้ใจกับบุคคลที่เราไม่รู้จัก ในงานของ **ชไมพร คงเพชร**[8] เรื่อง **สื่อลวงออนไลน์: ปัจจัยที่มีความสัมพันธ์กับพฤติกรรมการหลอกลวงบนอินเตอร์เน็ต** เป็นการศึกษาปัจจัยที่มีความสัมพันธ์กับประสบการณ์ที่เคยถูกหลอกลวงผ่านสื่อออนไลน์ เนื่องจากเว็บบอร์ดเป็นสิ่งที่ทำให้ผู้ใช้งานอินเตอร์เน็ต สามารถส่งข้อมูลข่าวสาร แสดงความคิดเห็นของตนเองออกไปถึงผู้อื่นได้ ทำให้เกิดการรวมตัวกันขึ้นมาเสมือนหนึ่งเป็นชุมชนรูปแบบใหม่นี้ หรือชุมชนเสมือนจริง (Virtual

---

[6] พชรมน พิริยะสกุลยิ่ง, (2553), *กระบวนการสร้างกลุ่มเพื่อนโดยการสนทนาแบบออนไลน์: ศึกษากรณีกลุ่มเพื่อนมิตรภาพ,* วิทยานิพนธ์สังคมสิทยามหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย.

[7] ศุนิสา ทดลา, (2542), *รูปแบบพฤติกรรมการสื่อสารในห้องสนทนาบนเครือข่ายอินเตอร์เน็ต.* วิทยานิพนธ์นิเทศศาสตรมหาบัณฑิต. จุฬาลงกรณ์มหาวิทยาลัย.

[8] ชไมพร คงเพชร, (2548), *สื่อลวงออนไลน์: ปัจจัยที่มีความสัมพันธ์กับพฤติกรรมการหลอกลวงบนอินเตอร์เน็ต,* วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต, มหาวิทยาลัยเกษตรศาสตร์.

Communities) ซึ่งเป็นชุมชนที่ไม่มีขอบเขตทางภูมิศาสตร์เป็นตัวกำหนด แต่เกิดขึ้นจากการมีจิตสำนึกร่วม มีหลักการ และจุดมุ่งหมายเดียวกัน เป็นชุมชนที่มีโครงสร้างยืดหยุ่น ไม่มีความผูกพัน สมาชิกในชุมชนเกิดขึ้นโดยที่คนในชุมชนเอง ก็ไม่เคยเห็นหน้าค่าตากันมาก่อน ไม่รู้จักว่าใครมาจากที่ไหน มีพื้นฐานอย่างไร แต่เมื่อมีโอกาสเข้ามาแลกเปลี่ยนความคิดเห็น และเกิดการมีส่วนร่วม รวมถึงความรู้สึกร่วมในสิ่งเดียวกัน ก็จะเกิดการสานต่อความสัมพันธ์ไปเรื่อยๆ

ด้วยความสัมพันธ์ที่ไม่สามารถเห็นหน้าค่าตากันได้ รู้จักกันเพียงผิวเผิน หรือคาดเดาหน้าตาได้จากรูปประจำตัว แต่มีการร่วมแสดงความคิดเห็น ร่วมทำกิจกรรมต่างๆ ที่ชอบเหมือนๆกัน หรือมีความคิดเห็นไปในทิศทางเดียวกัน ก็จะเกิดความไว้เนื้อเชื่อใจกันและกัน ซึ่งจะนำไปสู่กระบวนการสานสัมพันธ์ต่อในโลกของความเป็นจริง โดยอาจจะเกิดการนัดพบ ซึ่งในจุดนี้เองเป็นสิ่งที่น่าเป็นห่วง เพราะบนพื้นฐานของความเชื่อใจกันของอีกฝ่าย ในขณะที่อีกฝ่ายอาจจะมีเจตนาที่ไม่ดีแอบแฝงอยู่ ซึ่งเมื่อนัดเจอกันก็มีโอกาสที่นำมาซึ่งผลร้ายที่ไม่คาดคิด ไม่ว่าจะเป็นการ หลอกลวงไปข่มขืน การหลอกยืมเงิน หรือถูกหลอกในรูปแบบอื่นๆ ก็สามารถเป็นไปได้

ซึ่งจากการศึกษาพบว่า เพศชายถูกหลอกลวงมากกว่าเพศหญิง เนื่องจาก การสนทนาผ่านอินเตอร์เน็ต คู่สนทนาไม่ต้องพบหน้ากัน ไม่มีความอาย ไม่ต้องมีความรู้สึกเกรงกลัวอีกฝ่าย ทำให้ผู้มีเจตนาไม่บริสุทธิ์สามารุจะแอบอ้างตัวอย่างไรก็ได้ หรือเป็นเพศใดก็ได้ ขอเพียงได้ใช้วาจาทำให้คู่สนทนาเกิดความรู้สึกไว้ใจ ก็เพียงพอแล้ว ในส่วนของอายุ พบว่า อายุตั้งแต่ 25 ปีขึ้นไปเคยถูกหลอกลวงมากที่สุด เพราะคู่สนทนามาสามารถแอบอ้างอายุของตนเองได้ เพราะวัตถุประสงค์ที่สำคัญคือ เพียงต้องการให้คู่สนทนาที่ตนต้องการจะหลอกนั้น มีความไว้เนื้อ เชื่อใจ เท่านั้น ส่วนเรื่องระดับการศึกษา พบว่ากลุ่มที่มีระดับการศึกษาสูงกว่าปริญญาตรี ถูกหลอกลวงมากกว่ากลุ่มที่มีระดับการศึกษาต่ำกว่าปริญญาตรี เพราะพื้นที่ของอินเตอร์เน็ต เป็นพื้นที่ที่เปิดกว้างสำหรับทุกคน ดังนั้นการสื่อสารถึงกันโดยไม่สามารถเห็นหน้า หรือน้ำเสียง ก็ถือเป็นช่องโหว่หนึ่งที่อันตราย และเหมาะแก่การจะล่อลวง หลอกหลวงเหยื่อได้ดีวิธีการหนึ่ง อีกทั้งยังรวมถึงการนำเสนอตัวตนว่ามีอาชีพมั่นคง เป็นแพทย์ ทหาร นักธุรกิจ ทำให้มองดูว่าเป็นที่น่าเชื่อถือได้อีกทางหนึ่งด้วย[9]

ดังนั้นงานของ ชไมพร จึงสรุปได้ว่า ปัจจัยที่มีผลต่อการถูกหลอกลวง คือ รายได้, พฤติกรรมระยะเวลาที่เริ่มใช้อินเตอร์เน็ต, พฤติกรรมของกิจกรรมที่นำไปใช้, ลักษณะการใช้เว็บไซต์ในการนำอินเตอร์เน็ตไปประกอบกิจกรรม ความรู้ ความเข้าใจ การใช้เว็บไซต์ ในการนำอินเตอร์เน็ตไปประกอบกิจกรรม ประสบการณ์ที่เคยใช้อินเตอร์เน็ต ด้านมูลเหตุจูงใจให้เลือกใช้อินเตอร์เน็ตในการติดต่อสื่อสาร และมูลเหตุจูงใจให้เลือกใช้อินเตอร์เน็ตเพื่อเสาะหาความรู้ ความบันเทิง ส่วนเพศ อายุ ระดับการศึกษา อาชีพ ความถี่ในการใช้อินเตอร์เน็ต ปัญหาที่เกิดจากการใช้อินเตอร์เน็ต และผลที่ได้รับจากการเลือกใช้อินเตอร์เน็ต ไม่มีผลต่อความสัมพันธ์กับประสบการณ์ที่เคยถูกหลอกลวง

อีกปัจจัยหนึ่งที่ส่งผลให้กลายเป็นพฤติกรรมที่ถูกล่อลวง คือ การเข้าถึงเนื้อหาเรื่องเพศและมีความเชื่อ หรือค่านิยมแบบผิดๆ และส่วนใหญ่มักจะถูกชักจูงโดยกลุ่มเพื่อนที่สนิทกัน งานของ **อุมาวัลย์ จันทะแก้ว**[10] ศึกษา **อิทธิพลของพฤติกรรมการเปิดรับเนื้อหาทางเพศผ่านสื่ออินเตอร์เน็ตที่**

[9] เรื่องเดียวกัน.

[10] อุมาวัลย์ จันทะแก้ว, (2547), *อิทธิพลของพฤติกรรมการเปิดรับเนื้อหาทางเพศผ่านสื่ออินเตอร์เน็ตที่ส่งผลต่อค่านิยมทางเพศของกลุ่มวัยรุ่นในเขตกรุงเทพมหานคร,* วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต, มหาวิทยาลัยศรีนครินทรวิโรฒ.

ส่งผลต่อค่านิยมทางเพศ ของกลุ่มวัยรุ่นในเขตกรุงเทพมหานคร พบว่า เนื้อหาของหน้าเว็บไซต์ในปัจจุบันมีความสะท้อนค่านิยมทางเพศ โดยเว็บไซต์ที่นิยม 3 อันดับแรก ได้แก่ www.sanook.com, www.kapook.com และ www.eotoday.com โดยทั้ง 3 เว็บไซต์จะวิเคราะห์เฉพาะห้องที่มีเนื้อหาทางเพศ ซึ่งพบว่าผู้คนมีพฤติกรรมเปิดรับเนื้อหาทางเพศผ่านสื่ออินเตอร์เน็ตมากขึ้น และเจตคติต่อพฤติกรรมการเปิดรับเนื้อหาทางเพศผ่านสื่ออินเตอร์เน็ตเป็นตัวแปรอิสระที่สำคัญร่วมกันทำนายพฤติกรรมทางเพศ และบุคคลที่เปิดรับเนื้อหาทางเพศมากที่สุดก็เป็นช่วงวัยรุ่น โดยเนื้อหาทางเพศที่เปิดรับ อาทิเช่น เรื่องราวเทคนิคบนเตียง การจีบกัน การใช้ชีวิตคู่ เนื้อหาเกี่ยวกับสุขภาพทางเพศ ซึ่งในแต่ละเว็บก็จะมีเนื้อหา และการแลกเปลี่ยนประเด็นต่างๆ เกิดขึ้น

ซึ่งสอดคล้องกับงานวิจัยของ **ฟ้าใส วิเศษกุล**[11] เรื่อง **การวิเคราะห์ค่านิยมและทัศนคติเกี่ยวกับเพศสภาพในสังคมไทยที่ปรากฏในสื่ออินเตอร์เน็ตเว็บบอร์ด** ได้อธิบายเพิ่มเติมว่า ในกระทู้เว็บบอร์ดของ www.pantip.com ในห้องเพศศึกษา พบว่ามีผู้เข้าใช้งานเป็นจำนวนมากและเนื้อหาภายในห้องนั้นก็เป็นเกี่ยวกับเรื่องเพศ เช่น ปัญหาสังคมเกี่ยวกับเพศ เนื้อหาเกี่ยวกับพฤติกรรมทางเพศ เรื่องเกี่ยวกับอวัยวะเพศชาย และพบว่ามีค่านิยมและทัศนะคติของการให้ความสำคัญกับขนาดของอวัยวะเพศชายด้วย และยังคงมีประเด็นอื่นๆ ด้วย เช่น การเลิกรา การหย่าร้าง การนอกใจ รวมถึงการให้คุณค่ากับความบริสุทธิ์ของเพศหญิง

ด้วยพฤติกรรมทางเพศที่มากขึ้นและสังคมออนไลน์ที่เป็นอิสระและเปิดกว้าง การปฏิสัมพันธ์ของผู้คนที่สามารถเข้าถึงกันอย่างง่าย และพฤติกรรมบางอย่างที่รู้เท่าไม่ถึงการณ์นำไปสู่การถูกล่อลวงทางอินเตอร์เน็ตได้ เช่น การเปิดเผยข้อมูลส่วนตัวให้บุคคลภายนอกรับรู้ การแสดงเจตนาหรือความสนใจของตนเองว่าต้องการ รวมถึงการแสดงฐานะทางสังคมของตนเองด้วย (Privacy and Personal Data) ในงานของ **พลัฏฐ์กร พวงทองทิพย์**[12] ได้อธิบายถึงพฤติกรรมและปัจจัยความเสี่ยงของการถูกล่อลวงทางอินเตอร์เน็ตในเรื่อง **ปัจจัยของความเสี่ยงจากการถูกล่อลวงทางอินเตอร์เน็ตของนักเรียนตอนต้น เขตบึงกุ่ม กรุงเทพมหานคร** พบว่า นักเรียนส่วนใหญ่ที่มีความเสี่ยงจากการถูกล่อลวงทางอินเตอร์เน็ต มีการสนทนาผ่านทางอินเตอร์เน็ต โดยจะมีปฏิสัมพันธ์ที่มีความสนิทสนมกันกับเพื่อนหรือบุคคลอื่น และมีการเปิดเผยข้อมูลส่วนตัวให้บุคคลภายนอกรับรู้ด้วย ความต้องการและความสนใจ ซึ่งสามารถทำให้ตกเป็นเหยื่อของผู้กระทำความผิดให้ถูกล่อลวงได้ง่าย อีกทั้งยังเป็นผู้ที่ใช้งานอินเตอร์เน็ตเป็นจำนวนมากต่อสัปดาห์ด้วย

ในงานของ **รองศาสตราจารย์ ดร. อุษา บิ้กกิ้นส์**[13] ก็มีผลการศึกษาไปในทิศทางเช่นเดียวกัน ในเรื่อง **ไซเบอร์เซ็กส์กับทัศนคติทางเพศของวัยรุ่น** จากการศึกษาพบว่า กลุ่มตัวอย่างเคยใช้อินเตอร์เน็ตเพื่อค้นหาเรื่องทางเพศผ่านช่องทาง google ค้นหาเนื้อหาทางเพศแบบภาพโป๊ มากที่สุด ส่วนการสื่อสารจะโต้ตอบกันผ่านทางช่องแชท (chat), เฟซบุ๊ค (facebook) และแคมฟร็อค (camfrog) โดยส่วนใหญ่กลุ่มตัวอย่างจะเปิดรับเนื้อหาทางเพศ เรื่องการพูดเกี่ยวกับเซ็กส์หรือกิจกรรมทางเพศ ใน

---

[11] ฟ้าใส วิเศษกุล, (2544), *การวิเคราะห์ค่านิยมและทัศนคติเกี่ยวกับเพศสภาพในสังคมไทย ที่ปรากฏในสื่ออินเทอร์เน็ตเว็บบอร์ด*, วิทยานิพนธ์นิเทศศาสตรมหาบัณฑิต, มหาวิทยาลัยธุรกิจบัณฑิตย์.

[12] พลัฏฐ์กร พวงทองทิพย์, (2554), *ปัจจัยของความเสี่ยงจากการถูกล่อลวงทางอินเตอร์เน็ตของนักเรียนตอนต้น เขตบึงกุ่ม กรุงเทพมหานคร,* วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต, มหาวิทยาลัยรามคำแหง.

[13] อุษา บิ้กกิ้นส์, (2559), ไซเบอร์เซ็กส์กับทัศนคติทางเพศของวัยรุ่น, *วารสารสุทธิปริทัศน์* ปีที่ 30 ฉบับพิเศษ: 104-114

ปริมาณที่ถี่มากที่สุด 1-2 วันต่อสัปดาห์ ใช้อินเตอร์เน็ตต่อวันในการค้นหาเรื่องทางเพศ น้อยกว่า 2 ชั่วโมง ซึ่งช่วงเวลาที่ใช้จะเป็นช่วงกลางดึกที่บ้านตนเอง หอพัก และโรงเรียน โดยการเปิดรับเรื่องทางเพศทำให้รู้เทคนิค รู้สึกผ่อนคลาย ทำให้ดูเป็นผู้ใหญ่ขึ้น รวมถึงความอยากรู้อยากเห็น ไม่ว่าจะเป็นรูปภาพโป๊ เปลือยกาย รวมถึงภาพของการมีเพศสัมพันธ์ด้วย ไม่เพียงการค้นหาเรื่องเพศผ่านทางเว็บไซต์เท่านั้น กลุ่มตัวอย่างบางคนยังมีประสบการณ์ในการเล่นเซ็กออนไลน์ตั้งแต่มัธยมต้น ทั้งเล่นในช่วงเวลาว่าง และเล่นเกือบทุกวัน โดยปัจจัยในการเข้าถึงก็มาจากเพื่อนในกลุ่มที่เคยทำ หรือดูจากโฆษณา คำเชิญชวนต่างๆ ที่ปรากฏอยู่บนเว็บไซต์ โดยเฉพาะช่องทางผ่านแคมฟร็อก และ เฟซบุ๊ค จากการเปิดรับเนื้อหาทางเพศที่กว้างมาก ไร้ขอบเขตผ่านสื่อออนไลน์ ทำให้เกิดค่านิยมหรือความเข้าใจแบบผิดๆ เช่น การไม่เคยมีแฟน หรือ ไม่เคยมีเพศสัมพันธ์กับแฟนเป็นเรื่องน่าอาย และไม่สามารถเข้ากับกลุ่มเพื่อนได้, การอยู่กินกันแบบไม่แต่งงานเป็นเรื่องธรรมดา หรือ การมีกิ๊กเป็นการพิสูจน์ความเป็นลูกผู้ชายอย่างหนึ่ง เป็นต้น จะเห็นว่าการเข้าถึงข้อมูลเกี่ยวกับเรื่องเพศบนสื่อออนไลน์ทำได้ง่าย และจะเข้าไปดูเมื่อไหร่ เวลาไหนก็ได้ ทำให้คนที่เข้าไปดูไม่สามารถเข้าใจเรื่องเพศได้อย่างถูกต้อง เพราะไม่มีผู้ปกครอง หรือ ผู้ให้คำแนะนำที่ถูกที่ควร และการเข้าถึงเว็บไซต์ก็ไม่มีมีมาตรการเรื่องของอายุจำกัดไว้ ทำให้การเข้าถึงเปิดกว้าง อิสระไร้การควบคุม อย่างเช่น โฆษณายาปลุกเซ็กส์ การใช้เครื่องกระตุ้นทางเพศ ก็สามารถพบเห็นได้ง่ายตามเว็บไซต์ต่างๆ บนสื่อออนไลน์ ส่วนการควบคุมพฤติกรรมที่เกิดขึ้นในบ้าน หรือ หอพัก ก็ไม่มีผู้ควบคุมดูแลอย่างเหมาะสม

นอกจากการเข้าถึงเว็บไซต์ หรือเนื้อหาที่ไม่เหมาะสมแล้ว พื้นที่ออนไลน์ยังมีประเด็นของการระบุตัวตน ความเป็นนิรนามบนโลกอินเตอร์เน็ตด้วย โดยความเป็นนิรนามหรือการไม่ระบุตัวตนก็มีทั้งข้อดี และข้อเสียแตกต่างกันไป อย่างเช่นการกระทำบางอย่างไม่สามารถกระทำได้บนโลกความจริง แต่สามารถกระทำได้อย่างง่ายดายบนโลกอินเตอร์เน็ต ในงานของ **สฤณี อาชวานันทกุล**[14] ได้อธิบายไว้อย่างชัดเจนถึงการไม่ถูกจำกัดสิทธิหรือการเอากฎเกณฑ์ ความเชื่อของผู้อื่นมาเกี่ยวข้องบนพื้นที่ออนไลน์ โดยงานศึกษาเรื่อง **กลไกกำกับดูแลอินเตอร์เน็ตและปัญหาในไทย: ค่านิยมสองขั้ว** พบว่าโลกออนไลน์มีความเป็นอิสระเสรีภาพมากกว่าโลกออฟไลน์ หากมองในแง่ของความเป็นนิรนามในโลกออนไลน์นั้น (หมายถึงการไม่เปิดเผยตัวตนที่แท้จริง) เราไม่จำเป็นต้องเปิดเผยตัวตนว่าอายุเท่าไหร่ เพศอะไร หน้าตาอย่างไร ทำงานอะไร อยู่ที่ไหน มีวุฒิการศึกษาสูงเพียงใด ซึ่งเป็นปัจจัยสำคัญที่ช่วยให้เรา “ละเลย” ค่านิยมเชิงลำดับขั้นในสังคมนอกจอได้ เช่น ความยำเกรงระหว่างเด็กกับผู้ใหญ่ มันจึงทำให้คนกล้าพูด กล้าแสดงออกมากกว่าในสังคมนอกจอ แต่ในขณะเดียวกันความเป็นนิรนามนั้นก็ทำให้เกิดปัญหาตามมาได้ อย่างเช่น กรณีการหลอกลวง การล่อลวงให้ไปพบเจอกัน เป็นต้น

งานของ **พิชญ์ พงษ์สวัสดิ์**[15] ในบทความเรื่อง **ประเทศไทย กับ เสรีภาพของอินเตอร์เน็ต 2559** พบว่า อินเตอร์เน็ตเข้ามามีส่วนสำคัญในวิถีชีวิตของเรามากขึ้น จากเดิมที่อาจจะรู้สึกว่าโลกออนไลน์เป็นเพียง “โลกใหม่” หรือ “โลกเสมือน” แต่ด้วยความที่โลกออนไลน์มีความเป็นอิสระเสรีภาพที่สูงมาก ทำให้เราสามารถทำอะไรก็ได้ อยากจะสมมุติตัวเองเป็นอะไรก็ได้ พอมาวันหนึ่งโลกออนไลน์กับโลกออฟไลน์มีการเชื่อมต่อกันอย่างสลับซับซ้อน จนทำให้ไม่แน่ใจว่า ส่วนไหนในโลกออนไลน์ที่เป็น

---

[14] สฤณี อาชวานันทกุล, (2558), *DIGITAL FUTURE กลไกกำกับดูแลอินเตอร์เน็ต และปัญหาในไทย: ค่านิยมในสังคมสองขั้ว*, กรุงเทพ: สำนักพิมพ์ open worlds, หน้า 118.

[15] พิชญ์ พงษ์สวัสดิ์, (2559), *ประเทศไทย กับ เสรีภาพของอินเตอร์เน็ต 2559*, สืบค้นจาก มติชนออนไลน์ : https://www.matichon.co.th/news/366683.

ความจริงบ้าง และส่วนไหนที่ไม่จริง รูปธรรมที่สำคัญที่ทำให้เห็นว่าโลกอินเตอร์เน็ตนั้นมีส่วนเชื่อมโยงหรือขยายจากโลกของความจริง เช่น การทำธุรกรรมในโลกออนไลน์ การลงทะเบียนโลกออนไลน์ด้วยชื่อจริง การถูกดำเนินคดีจากการแสดงความคิดเห็นในโลกออนไลน์

ซึ่งเมื่อมองจากมุมมองของพิชญ์ พงษ์สวัสดิ์ เห็นจะมีงานอีกชิ้นหนึ่ง ที่ได้อธิบายได้สอดรับกันว่า เราจะสามารถรู้ได้อย่างไรว่า ตัวตนที่อยู่ในโลกออนไลน์ จะเป็นตัวตนคนเดียวกันกับที่อยู่ในโลกออฟไลน์ สิ่งที่แสดงในโลกออนไลน์นั้น เป็นสิ่งที่คนในโลกออฟไลน์เป็นผู้กระทำจริงหรือไม่ ได้อธิบายไว้ในงานของ **โสรัจจ์ หงศ์ลดารมภ์**[16] ที่กล่าวไว้ใน **ตัวตนออนไลน์** ถึงเรื่องความเป็นตัวตนในโลกออนไลน์กับโลกออฟไลน์ว่าเราจะสามารถทราบได้อย่างไรว่าเป็นบุคคลคนเดียวกัน อย่างเช่น เครือข่ายสังคมที่มีผู้คนใช้งานมากที่สุด เช่น Facebook หรือ Twitter ที่เราจะต้องทำการสมัครสมาชิกหรือเข้าใช้งานใน user ของตัวเอง และผู้ใช้สามารถใส่ข้อมูลส่วนตัวที่เรียกว่า “โปรไฟล์” เพื่อแสดงให้บุคคลอื่น หรือเพื่อนเราทราบถึงการแสดงตัวตนของผู้ใช้งาน แต่ในขณะเดียวกันนั้นก็มีผู้ใช้งานบางกลุ่มที่ไม่อยากจะใช้ข้อมูลที่แท้จริงของตนเอง อาจจะใช้นามปากกา หรือ นามแฝง ตั้งรูปประจำตัวเป็นรูปที่ชอบ เช่นรูปสัตว์เลี้ยง ดอกไม้ วิวธรรมชาติ เป็นต้น ซึ่งก็ทำให้เกิดปัญหาขึ้นว่า ตัวตนในโลกออนไลน์นั้นเหมือนหรือต่างจากตัวตนปกติของเราอย่างไร การโพสต์เรื่องที่สนใจในปีที่แล้ว และปีนี้ก็ยังโพสต์ในแบบเดียวกันอีก ก็อาจจะพอเข้าใจได้ว่าเป็นบุคคลคนเดียวกันหรือไม่

เมื่อเป็นเช่นนี้ หนทางที่จะพิสูจน์ก็คงต้องเป็นการกลับไปอ้างอิงกับบุคคลในโลกออฟไลน์นั่นเอง หากบุคคลในโลกจริงหรือโลกออฟไลน์เป็นคนเดียวกัน เมื่อเวลาผ่านไปหนึ่งปี ตัวตนในโลกออนไลน์ของบุคคลนี้เมื่อปีที่แล้วกับปัจจุบันก็ควรเป็นบุคคลคนเดียวกันด้วย ซึ่งการแก้ปัญหาเช่นนี้เป็นการโยนภาระการพิสูจน์ไปให้แก่ตัวตนในโลกออฟไลน์ ซึ่งเราเองก็ไม่สามารถรู้ได้อย่างแท้จริงว่า บุคคลในโลกออฟไลน์จะเป็นคนเดียวกันกับบุคคลในโลกออนไลน์หรือไม่

และประเด็นสุดท้ายที่มีความสำคัญและน่าสนใจมากต่อพฤติกรรมที่มีความเสี่ยงต่อการถูกล่อลวงนั้น คือ ความรู้สึกเหงาและความไม่รู้สึกถึงการถูกเติมเต็มจากพื้นที่ออนไลน์ งานวิจัยจากต่างประเทศพบว่าพื้นที่ออนไลน์ แม้จะมีผู้คนที่เข้าใช้งานเป็นจำนวนมาก การพูดคุยสื่อสารทั้งกับคนรู้จักและคนที่ไม่รู้จัก ไม่ได้ช่วยให้ผู้ใช้งานอินเตอร์เน็ตที่รู้สึกว่าเหงา ถูกเติมเต็มหรือทำให้คลายแต่อย่างใด ซึ่งหลายคนอาจคิดว่าไม่จำเป็นจะต้องพูดคุยหรือให้ความสำคัญกับคนรอบข้างมากนัก เพราะเราเองก็มีเพื่อนในโลกออนไลน์อีกเป็นจำนวนมาก อย่างเช่น เฟสบุ๊ค หรือทวิสเตอร์ ที่มีการพูดคุย สื่อสารกับคนที่ไม่รู้จัก จนกลายเป็นเรื่องปกติไปแล้ว จากบทความของ **The Momentum**[17] เรื่อง **งานวิจัยชี้การเล่นโซเชียลมีเดียที่มากเกินไป อาจจะเป็นสาเหตุของความรู้สึกโดดเดี่ยว** มีการศึกษาถึง สาเหตุของความรู้สึกโดดเดี่ยว ซึ่งเมื่อสังออนไลน์กลายเป็นส่วนหนึ่งของคนในชีวิตประจำวัน จึงไม่แปลกใจที่ว่า การพูดคุย ติดต่อสื่อสาร รวมถึงการแสดงออกในเรื่องส่วนตัวต่างๆ ก็ถูกทำบนโซเชียลมีเดีย ซึ่งโซเชียลมีเดียกลายเป็นเหมือนโลกเสมือนจริงอีกใบหนึ่ง ที่มีผู้คนใช้ชีวิตกันอยู่ตลอดเวลา ไม่มีกลางวัน

---

[16] โสรัจจ์ หงศ์ลดารมภ์, (2555) ตัวตนออนไลน์, *มาราธอน ฉบับ "ออกตัว" : รวมบทความและบันทึกเสวนาว่าด้วยอินเทอร์เน็ต การเมือง และวัฒนธรรม*, นฤมล กล้าทุกวัน, บรรณาธิการ, หน้า 384.

[17] พชรพล เกตุจินากูล, (2560), *งานวิจัยชี้การเล่นโซเชียลมีเดียมากเกินไป อาจเป็นสาเหตุของความรู้สึกโดดเดี่ยว, (*20 พฤศจิกายน 2561), สืบค้นจาก The Momentum: https://themomentum.co/happy-self-help-use-social-media-more-cause-lonely/

หรือ กลางคืน ผู้คนจากซีกโลกหนึ่ง สามารถพูดคุย ติดต่อสื่อสารกับคนอีกซีกโลกหนึ่งได้ในเพียงเวลาไม่กี่วินาที ข้อมูลถูกส่งต่อกันแบบเรียลไทม์ ข้อกำจัดด้านมิติเวลาถูกก้าวข้ามไป เหมือนไม่เคยเกิดขึ้น

เมื่อเราหมกมุ่นอยู่กับความรู้สึกที่แสดงออกผ่านโลกออนไลน์มากเกินไป เราจะมีพฤติกรรมที่เป็นคนเก็บตัว ไม่สุงสิงกับโลกภายนอก ให้ความสำคัญกับสังคมออนไลน์ พฤตกรรมเหล่านี้อาจส่งผลทำให้เรากลายเป็นคนขี้เหงา หรืออาจถึงขึ้นเป็นโรคซึมเศร้าได้โดยไม่รู้ตัว ซึ่งก็มีงานวิจัยของ ดร. ไบรอัน เอ. พรีมัก ที่ศึกษาสังคมวัยรุ่นอเมริกา ที่ให้เหตุผลสนับสนุนว่า ถ้าใช้เวลากับโซเชียลเน็ตเวิร์กมากกว่า 2 ชั่วโมงต่อวัน มีโอกาสที่รู้สึกเหงามากกว่าปกติถึงสองเท่า ซึ่งจากผลสรุปพบว่า คนที่ติดการใช้งานโซเชียลมีเดียเกิน 58 ชั่วโมงต่อสัปดาห์ มีโอกาสที่จะเกิดความรู้สึกโดดเดี่ยวมากถึง 3 ครั้งต่อสัปดาห์ ถึงแม้ว่าการใช้สื่อสังคมออนไลน์จะมีส่วนช่วยให้ผู้ใช้งานตามเทรนด์ของโลกได้ทัน ไม่เป็นคนประเภทกลัวตกกระแส แต่การศึกษาครั้งนี้แสดงให้เห็นว่าอาการเสพติดโซเชียลมีเดีย สามารถทำให้คนหมกมุ่นกับความเหงาที่รุนแรงได้

ซึ่งก็สอดคล้องกับบทความของ **The Matter**[18] เรื่อง **โลกออนไลน์ ทำให้เราเหงามากขึ้น? วัยรุ่นอังกฤษ มีสัดส่วนความเหงาเยอะที่สุด ผลสำรวจชี้ อาจเกี่ยวกับจำนวนเพื่อนในเฟซบุ๊ค** พบว่า ผู้คนจำนวน 55,000 คน ซึ่งเป็นเด็กอายุ 16-24 ปี มีความรู้สึกเหงามากกว่ากลุ่มคนอายุอื่น โดยสองในห้าของผู้ที่อยู่ในกลุ่มนี้รายงานว่ารู้สึกเหงาหรือบ่อยครั้ง เมื่อเปรียบเทียบกับผู้ที่มีอายุ 65-74 ปี[19] ซึ่งจากการศึกษาทำให้เห็นว่า ยิ่งมีเพื่อนที่รู้จักแค่ในเฟซบุ๊คเยอะๆ อาจทำให้เรารู้สึกเหงามากยิ่งขึ้น บางคนมีเพื่อนในเฟซบุ๊คมากกว่า “เพื่อนในชีวิตจริง” ถึงหกเท่า[20] ซึ่งสิ่งที่น่าสนใจ คือ คนที่ให้คำตอบว่ารู้สึกเหงา หลายคนมีเพื่อนที่รู้จักกันผ่านเฟซบุ๊คโดยตรง (Online only Facebook friends) มากกว่าคนที่ตอบว่าไม่เหงา ซึ่งก็สอดคล้องกับงานวิจัยชิ้นก่อนๆ ที่มีข้อมูลชี้ไปในทางเดียวกันว่า การใช้ชีวิตในโลกออนไลน์ มันอาจทำให้รู้สึกโดดเดี่ยวและเหงาได้ยิ่งเราเห็นข้อเปรียบเทียบจากคนอื่น เช่น ไลฟ์สไตล์ที่เราชื่นชอบผ่านคนอื่นๆ เราก็นำพาตัวเองไปเปรียบเทียบโดยไม่รู้ตัว และสุดท้ายก็เลยรู้สึกเหงาขึ้นมา

จะเห็นว่าพฤติกรรมที่มีความเสี่ยงต่อการถูกล่อลวง เป็นประเด็นที่เกิดจากเรื่องเล็กๆ น้อยๆ ในชีวิตประจำวัน เพียงการเล่นอินเตอร์เน็ตแบบไม่จำกัดเวลา การพูดคุย หรือ เชื่อมความสัมพันธ์กับคนแปลกหน้าก็ถือเป็นความเสี่ยงต่อการถูกล่อลวงอย่างหนึ่ง และจากงานวิจัยข้างต้นก็ทำให้เห็นได้ชัดเจนยิ่งขึ้นว่าจากพฤติกรรมที่สนใจในเรื่องเพศ การมีความเชื่อ หรือ ค่านิยมแบบผิดๆ รวมถึงความรู้สึกเหงาเปล่าเปลี่ยวใจ ก็ส่งผลให้ตัวเองตกเป็นเหยื่อของอาชญากรบนโลกอินเตอร์เน็ตได้ ซึ่งจะนำไปสู่การศึกษางานวิจัยในส่วนที่สอง ซึ่งถือเป็นภัยร้ายแรงต่อโลกออนไลน์อย่างมาก เพราะการกระทำที่เกิดบนโลกออนไลน์ นำมาสู่ผลกระทบที่เลวร้ายที่สุดในโลกจริงของเหยื่อ

---

[18] The matter, (2561), *โลกออนไลน์ ทำให้เราเหงามากขึ้น? วัยรุ่นอังกฤษ มีสัดส่วนความเหงาเยอะที่สุด ผลสำรวจชี้ อาจเกี่ยวกับจำนวนเพื่อนในเฟซบุ๊ค.* (20 พฤศจิกายน 2561), สืบค้นจาก The Matter: https://thematter.co/brief/news-1538467201/61445

[19] Telegraph, (2561), *Loneliness is felt most intensely by young people, study finds (and turning to Facebook doesn't help)*, (3 กุมภาพันธ์ 2561), สืบค้นจาก https://www.telegraph.co.uk/news/2018/10/01/loneliness-felt-intensely-young-people-study-finds-turning-facebook/

[20] เรื่องเดียวกัน.

<u>ส่วนที่สอง</u> รูปแบบและวิธีการล่อลวงบนโลกไซเบอร์

จากส่วนแรกที่อธิบายถึงพฤติกรรมเสี่ยงต่อการถูกล่อลวงบนโลกออนไลน์ จะเห็นว่าพฤติกรรมที่ดูผิวเผินอาจจะไม่อันตราย กลายเป็นจุดอ่อนสำคัญให้อาชกรบนโลกออนไลน์นำมาล่อลวงเหยื่อได้สำเร็จ ซึ่งก็สอดคล้องกับเทคโนโลยีที่ถูกพัฒนาอย่างไม่หยุดยั้ง แอพพลิเคชั่นกลายเป็นช่องทางหนึ่งในการกระทำความผิด ในงานของ **Aziz Ansari** [21] เรื่อง **MODERN ROMANCE: ถอดรหัสรักออนไลน์ สุดท้ายความรักก็เป็นเรื่องของคนสองคน** เป็นงานวิจัยจากสหรัฐอเมริกา พบว่า การหาคู่ออนไลน์เริ่มต้นขึ้นในช่วงทศวรรษ 1960 พร้อมกับที่บริการหาคู่ผ่านคอมพิวเตอร์รุ่นแรกๆ ซึ่งบริการเหล่านี้อ้างว่าสามารถช่วยผู้ไร้โชคด้านความรักพบเนื้อคู่ด้วยวิธีการที่มีประสิทธิภาพและมีเหตุผล ซึ่งการหาคู่นี้จะให้ผู้เข้าร่วมตอบแบบสอบถามแล้วป้อนคำตอบต่างๆ เข้าไปในเครื่อง หลังจากนั้นก็จะมีการจัดแจง คัดแยกลูกค้าที่มีความเข้ากันออกมาตามอัลกอริทึมที่ตั้งต้นกำหนดไว้ และจึงส่งทั้งคู่ออกไปเดตกัน แต่ถึงอย่างไรนั้น บริการหาคู่ออนไลน์ดังกล่าวก็ไม่เป็นที่นิยมในขณะนั้น อาจจะเป็นเพราะเหตุผลในการจับคู่ดูง่ายเกินไป และระบบคอมพิวเตอร์ยังคงไม่เป็นที่นิยมในขณะนั้น ซึ่งก็มีการโต้แย้งว่าจะให้เครื่องคอมพิวเตอร์เครื่องหนึ่งมากำหนดชีวิตเราได้อย่างไร

กระทั่งในช่วงศตวรรษที่ 18 การประกาศหาคู่สมรสได้กลายเป็นส่วนหนึ่งของธุรกิจหนังสือพิมพ์ซึ่งมีความเจริญรุ่งเรือง และเฟื่องฟูมาก ทั้งในหนังสือพิมพ์รายวัน รายสัปดาห์ โดยเงื่อนไขในการลงหาคู่จะต้องเขียนข้อความสั้นๆประมาณ 50 คำ และเกริ่นนำด้วยข้อความที่มีความดึงดูด อย่างเช่น ชายขี้เหงา! หรือ สาวผมสีบลอนด์สตรอว์เบอร์รี่ เป็นต้น ทางหนังสือพิมพ์จะให้พื้นที่ลงฟรีประมาณ 4 บรรทัด แต่ถ้าหากคุณต้องการลงข้อความเพิ่มก็สามารถซื้อพื้นที่ได้ การหาคู่ผ่านทางพื้นที่ในหนังสือพิมพ์ดำเนินมาเรื่อย ๆ จนกระทั่งมีผู้นำเอาเทคโนโลยีเอามา คือ การหาคู่ผ่านวิดีโอ สิ่งที่พัฒนาขึ้นคือ ให้คนที่ต้องการหาคู่มาแนะนำตัวเองผ่านกล้องเพื่ออัดเป็นคลิปวิดีโอ ความยาวประมาณ 2-3 นาที แต่วิธีดังกล่าวก็ไม่เป็นที่นิยมกันมากนัก กลายเป็นคลิปที่คนเข้ามาดูเพื่อความสนุกเสียมากกว่า[22]

จนในช่วงปี 1995 ด้วยความที่เทคโนโลยีพัฒนามาอย่างต่อเนื่อง คอมพิวเตอร์สามารถเชื่อมต่อผู้ใช้อินเตอร์เน็ตได้อย่างกว้างขวางมากยิ่งขึ้น อินเตอร์เน็ตเริ่มเป็นที่นิยม การหาคู่ออนไลน์เริ่มได้รับความสนใจอีกครั้ง โดยเว็บไซต์ Macth.com พัฒนาบริการหาคู่รูปแบบใหม่ขึ้น แทนการจับคู่ลูกค้าด้วยอัลกอริทึม แต่จะให้ลูกค้าเป็นฝ่ายเลือกคู่เองแบบเรียลไทม์ แต่ก็ยังเกิดปัญหาว่าการบริการแบบดังกล่าวนี้จะสามารถช่วยอะไรได้จริงหรือไม่ จึงทำให้ทาง Match.com แก้ไข ปรับปรุงเว็บไซต์เรื่อยมา จนถึงช่วง ศตวรรษที่ 1990 อินเตอร์เน็ตเฟื่องฟูมากขึ้น ความสัมพันธ์ของคนกับคอมพิวเตอร์และวัฒนธรรมออนไลน์ได้เปลี่ยนแปลงพลิกผัน คนเริ่มคุ้นเคยกับการใช้งานคอมพิวเตอร์ขั้นพื้นฐานกันมากขึ้น เช่น การส่งอีเมล์ ห้องแชท โซเชียลมีเดีย เรื่องของการหาคู่ผ่านสื่อออนไลน์กลายเป็นเรื่องที่ยอมรับกันโดยสิ้นเชิง[23]

จนกระทั่งปัจจุบัน **ทินเดอร์ (Tinder)** แอพพลิเคชั่นหาคู่ออนไลน์บนมือถือ เป็นแอพฯที่ต่างจากการหาคู่แบบเดิมๆ ผู้ใช้สามารถเข้าใช้ทินเดอร์ได้โดยไม่เสียเวลามาก โดยสามารถเชื่อมต่อกับบัญชีเฟซบุ๊คได้อย่างง่ายดาย เมื่อเข้าใช้ทินเดอร์ จุดพิกัดจะปรากฏขึ้นและแสดงตำแหน่งที่ตั้งของคนอื่นๆที่

---

[21] Ansari, A., (2559), *ถอดรหัสลับออนไลน์ (Modern Romance),* แปลโดย สุนันทา วรรณสินธ์, กรุงเทพฯ: โอเพ่นเวิลด์ส (openworlds).

[22] เรื่องเดียวกัน.

[23] เรื่องเดียวกัน.

อยู่ในบริเวณใกล้เคียงด้วย และเริ่มแสดงรูปภาพของคู่ที่อาจเป็นไปได้ หรือสามารถแมท (Match) กับผู้ใช้งานได้อย่างไม่ขาดสาย หลังจากนั้นเราสามารถปัดขวา ถ้าหากสนใจคนคนนั้นและปัดซ้ายถ้าไม่สนใจ อีกทั้งยังสามารถเข้าไปสำรวจโปรไฟล์พื้นฐานของคนที่เราสนใจเพิ่มเติมได้ แต่คนส่วนใหญ่มักจะมองเพียงแค่รูปโปรไฟล์แล้วปัดซ้ายหรือขวาอย่างรวดเร็วเท่านั้น ถ้าเราและผู้ใช้อีกคนต่างสนใจกันและกัน (ซึ่งหมายความว่าทั้งสองคนปัดขวาเหมือนกัน) เมื่อเห็นหน้าของอีกฝ่าย แอพฯทินเดอร์จะแจ้งคุณว่าพบคู่แล้วและสามารถเริ่มส่งข้อความส่วนตัวหากันได้ ไม่ว่าจะนัดเดท หรือทำอะไรก็ตาม[24]

ทินเดอร์มีที่มาเช่นเดียวกับเฟซบุ๊ค คือถือกำเนิดขึ้นในมหาวิทยาลัย แต่ขณะที่เฟซบุ๊คเริ่มแพร่หลายในกลุ่มมหาวิทยาลัยไอวีลีก แต่ทินเดอร์มุ่งเป้าไปยังวิทยาลัยที่ขึ้นชื่อเรื่องปาร์ตี้อย่างมหาวิทยาลัยเซาเทิร์นแคลิฟอร์เนียหรือ USC และมหาวิทยาลัยแคลิฟอร์เนียในลอสแอนเจลิสหรือ UCLA โดยทินเดอร์ถูกคิดค้นขึ้นในปี 2011 จากนักศึกษาปริญญาตรีสองคนจากมหาวิทยาลัยเซาเทริน์แคลิฟอร์เนีย ผู้บุกเบิกสร้างประสบการณ์การหาคู่ออนไลน์ที่ไม่เหมือนการหาคู่ออนไลน์ ผู้คิดค้นต้องการให้เป็นเหมือนเกมที่ผู้ใช้งานสามารถเป็นผู้เล่นคนเดียวได้ มีความเสี่ยงน้อยและใช้งานง่าย

การใช้ทินเดอร์กลายเป็นสิ่งที่มีผู้วิพากษ์วิจารณ์อย่างมาก เพราะการใช้แอพฯส่วนใหญ่อาศัยความพึงพอใจในด้านรูปร่างหน้าตาเพียงอย่างเดียว จึงเป็นตัวแทนของความฉาบฉวยที่เพิ่มขึ้นในหมู่คนหาคู่ออนไลน์ อีกทั้งยังเป็นช่องโหว่สำคัญอย่างหนึ่งที่ทำให้ผู้ใช้งานหลายคนตกอยู่ในภาวะของการตกเป็นเหยื่อที่ถูกล่อลวง ไม่ว่าจะทั้งการถูกล่อลวงไปล่วงละเมิดทางเพศ หรือ ล่อลวงให้สูญเสียเงินจำนวนมาก แม้ว่าตัวแอพพลิเคชั่นเองจะไม่ได้มีเป้าหมาย หรือ วัตถุประสงค์ให้เกิดสิ่งชั่วร้ายต่างๆ แต่การกระทำที่เลวร้ายนั้น สามารถเกิดขึ้นได้จากการพบเจอ นัดเดตผ่านทางทินเดอร์ด้วย

การถูกล่อลวงโดยการหลอกให้รัก (Romance Scam) เป็นเรื่องละเอียดอ่อนและมีผลกระทบกับจิตใจของผู้ตกเป็นเหยื่ออย่างมาก เพราะเป็นการล่อลวงที่ใช้ความสัมพันธ์ไว้เนื้อเชื่อใจเข้ามาเกี่ยวข้องในงานของ **ปัทมาภรณ์ กฤษณายุทธ ศิริวัชรไพบูลย์**[25] เรื่อง **พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเตอร์เน็ต** ได้อธิบายถึงลักษณะพฤติกรรมการหลอกลวงของสแกมเมอร์ไว้อย่างชัดเจน โดยแบ่งประเภทของพฤติกรรมไว้เป็น 2 กลุ่ม คือ <u>กลุ่มแรก</u> การหลอกลวงทาง E-mail การส่งอีเมล์ให้แก่เหยื่อ โดยวิธีการนี้เป็นการส่ง E-mail ที่มีการติดต่อซื้อขาย การหลอกลวงเรื่องการจัดหางาน รวมถึงเป็นการหลอกลวงที่เป็นการปลอมอีเมล์ โดยส่วนมาก Scammer จะส่งอีเมล์ไปให้เหยื่อที่เป็นเป้าหมาย จะไม่มีการพบปะ หรือ นัดเจอกัน ซึ่งอีเมล์ที่ส่งจะเป็นเอกสารจากส่วนงานต่างๆ เช่น เอกสารสมัครงานปลอม เอกสารการโอนเงินปลอม หากเหยื่อไม่สังเกตอย่างรอบคอบก็จะถูกหลอกได้โดยง่าย เนื่องจากเอกสารดังกล่าวเป็นเพียงไฟล์รูปภาพ หรือไฟล์เอกสารอิเล็กทรอนิกส์เท่านั้น ต่อมาใน<u>กลุ่มที่สอง</u> เป็นการหลอกลวงทาง Social Media อย่างเช่น Facebook, Line, Instagram ซึ่งวิธีนี้เป็นวิธีที่ถูก Scammer ใช้มากที่สุด เนื่องจากว่า Social Media ดังกล่าวมีผู้คนเข้าใช้งานเป็นจำนวนมาก อีกทั้งพฤติกรรมของผู้ใช้งานยังถูกเปิดเผยถูกสาธารณะได้ง่าย จึงทำให้ Scammer สามารถเลือกเหยื่อ หรือเลือกเป้าหมายได้ไม่ยากนัก

[24] เรื่องเดียวกัน.

[25] ปัทมาภรณ์ กฤษณายุทธ ศิริวัชรไพบูลย์, (2554), *พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเตอร์เน็ต*, สืบค้นจาก : https://www.dsi.go.th/Files/20150123/F20150123160326-scammer-dsi-warning.pdf

วิธีการของกลุ่มแรก การหลอกลวงทาง E-mail มีหลายวิธีการ เช่น 1. การหลอกลวงว่าได้รับเงินจำนวนหนึ่ง โดยทาง Scammer จะส่ง E-mail มาให้เหยื่อ และสร้างสถานการณ์ว่าได้รับเงินจำนวนหนึ่ง แต่ติดปัญหาในเรื่องของค่าธรรมเนียมการนำเงินออก หรือการโอนเงินเข้าบัญชี โดย E-mail จะแนบเอกสารหลักฐานที่ได้รับเงิน พร้อมทั้งเอกสารให้ลงลายมือชื่อตอบกลับไป ซึ่งหากไม่ได้ตรวจสอบให้รอบคอบ และถี่ถ้วนก็จะไม่ทราบว่าเอกสารเหล่านั้นปลอมขึ้น 2. การหลอกลวงโดยการปลอมอีเมล์ (Fake-E-mail) ส่วนใหญ่จะเกิดในกรณีของการติดต่อซื้อขายสินค้าระหว่างประเทศ ระหว่างบุคคล 2 ฝ่าย ซึ่งในระหว่างการโต้ตอบทางอีเมล์ เหยื่อจะไม่ทราบว่ามีบุคคลอื่นเข้ามาแอบแฝงปลอมตัว และทำการโต้ตอบกับเหยื่อแทน เมื่อถึงขั้นตอนของการโอนเงิน จะมีการเปลี่ยนบัญชีเดิมที่เคยใช้มาแล้ว เป็นบัญชีใหม่โดยที่เหยื่อไม่ทันระวังตัว 3. การหลอกลวงเรื่องการจัดหางาน วิธีนี้จะเลือกเหยื่อที่ได้ลงทะเบียนไปทำงานต่างประเทศ ซึ่งเหยื่อได้กรอกรายละเอียดส่วนตัวไว้ ทีม Scammer จะทำตัวเป็นเจ้าหน้าที่ติดต่อชักชวนไปทำงานต่างประเทศ อ้างว่าได้รับข้อมูลจากกรมการจัดหางาน และจะสร้างสถานการณ์ว่าต้องทำเอกสารขอวีซ่า เหยื่อจะต้องโอนเงินมาเพื่อชำระค่ายื่นวีซ่า เมื่อเหยื่อโอนเงินแล้วก็จะส่งเอกสารการจ้างมาทาง E-mail ของเหยื่อ ต่อมา Scammer จะแจ้งเรื่องค่าเดินทาง ค่าตั๋วเครื่องบิน และให้เหยื่อโอนเงินเพื่อไปชำระค่าเดินทางต่างๆ และมีเอกสารยืนยัน ซึ่งกรณีกว่าเหยื่อจะรู้ตัวว่าโดยหลอกก็ไม่สามารถติดต่อหรือขอเงินคืนได้แล้ว[26]

จะเห็นว่าวิธีการของกลุ่มแรกนั้น เหยื่อแทบจะไม่มีทางรู้ได้เลยว่าตนเองกำลังถูกหลอก เนื่องจากเป็นเพียงการติดต่อกันผ่านทาง E-mail และทาง Scammer เองก็ส่งเอกสารที่ดูน่าเชื่อถือมาให้เหยื่ออยู่ตลอด ซึ่งการจะตรวจสอบว่าเอกสารดังกล่าวนั้นเป็นของจริงหรือของปลอมก็ต้องมีความละเอียด และช่างสังเกตเป็นอย่างดี อีกทั้งเนื่องจากเป็นเอกสารอิเล็กทรอนิกส์ จึงทำให้การตรวจเป็นไปได้ยาก ซึ่งเมื่อเทียบกลับวิธีการของกลุ่มที่สอง จะเป็นการสร้างความสนิทสนม ความคุ้นเคย และความไว้เนื้อเชื่อใจกัน เพราะเป็นการติดต่อสื่อสารกันผ่านทาง Social Media อย่างเช่น Facebook, Line, Instagram เป็นต้น

วิธีการในกลุ่มที่สอง จะมีการสร้างความรู้สึกรัก ความคุ้นเคยกับเหยื่อเข้าเกี่ยวข้อง ก่อนที่จะเริ่มกระทำการหลอกลวงเหยื่อ ในส่วนนี้ Scammer จะใช้วิธีการพูดคุยผ่านช่องทาง Social Media กับเหยื่อ โดยมีลักษณะของการพูดคำหวาน การจีบแบบชายหญิง จนเหยื่อหลงรักกับ Scammer เป็นการสร้างความคุ้นเคย ซึ่งบางกรณีเหยื่อเองเพิ่มจะรู้ตัวว่าถูกหลอกเมื่อคุยกันผ่านไปหลายเดือน บางกรณีมีระยะเวลาเป็นปี 1. หลอกลวงด้วยการขอแต่งงาน เมื่อ Scammer ทำความสนิทสนมคุ้นเคยกับเหยื่อแล้ว บางรายใช้เวลาเพียง 1-2 เดือน หลังจากนั้น Scammer ก็ออกปากว่าจะขอแต่งงาน และมีการส่งของมาให้เหยื่อ เช่น เงิน ทอง แหวนเพชร โทรศัพท์ เมื่อเหยื่อเชื่อและรอของส่งมา ทีมของ Scammer คนหนึ่งจะปลอมเป็นเจ้าหน้าที่ของศุลกากร แจ้งกับเหยื่อว่ามีพัสดุมาถึง แต่เมื่อตรวจสอบพบว่าข้างในในเงินสดอยู่ จึงต้องเสียค่าธรรมเนียม และหลอกให้เหยื่อโอนเงินเพื่อเป็นค่าธรรมเนียมและค่าภาษี 2. หลอกลวงด้วยการอาศัยความไว้เนื้อเชื่อใจและความสงสารของเหยื่อ กรณีนี้เมื่อ Scammer เชื่อว่าเหยื่อมีความรักใคร่ชอบพอกับตนแล้ว ก็จะสร้างเรื่องว่าต้องเดินทางไปต่างประเทศ เพื่อมารับเงินหรือทรัพย์สินที่บิดาของตน ได้สร้างเอาไว้ แต่เมื่อเดินทางมาถึงก็บอกกับเหยื่อว่าเงินสดที่ตนนำมาไม่เพียงพอที่จะดำเนินเรื่องที่จะรับเงินกับทรัพย์สินนั้น จึงขอให้เหยื่อโอนเงินมาให้ตนก่อน และเมื่อเสร็จธุระแล้วจะมาเจอเหยื่อ และจะนำเงินมาคืน 3. หลอกลวงด้วยการอ้างว่าเจ็บป่วย อาจจะเป็นการอ้างว่ามี

[26] เรื่องเดียวกัน.

บุตรสาว โดยขณะที่กำลังเดินทางไปหาเหยื่อ การเดินทางก็ต้องหยุดลงเนื่องจาก บุตรสาวของตนป่วย และเงินสดที่ตนเตรียมมามีไม่พอกับค่ารักษาพยาบาล ส่วนบัตรวีซ่าของตนก็มีปัญหาไม่สามารถใช้งานได้ จึงขอความช่วยเหลือจากเหยื่อให้โอนเงินมาช่วยตน และเมื่อบุตรสาวของตนออกจากโรงพยาบาลจะรีบเดินทางไปหาเหยื่อโดยทันที และ 4. หลอกลวงว่ามีธุรกิจส่วนตัว การสร้างโปรไฟล์ใน Facebook หรือ Social Media พวก Scammer จะสร้างบุคคลที่รูปร่างหน้าตาดี มีความมั่นคง ทำธุรกิจ ร่ำรวย หรือเป็นกลุ่มนายทหารยศสูง กรณีนี้ Scammer แนะนำตนเองว่าทำธุรกิจส่วนตัว ที่ประเทศหนึ่ง และต้องเดินทางไปเจรจาเรื่องธุรกิจ และหลังจากนั้นก็จะเดินทางมาหาเหยื่อที่ประเทศไทย ซึ่งกรณีนี้ก็จะสร้างสถานการณ์แบบเดิมในเรื่องการเจรจาธุรกิจมีปัญหาและขอความช่วยเหลือจากเหยื่อโดยการให้เหยื่อโอนเงินให้ตน[27]

ซึ่งพฤติกรรมของ Scammer มีความคล้ายคลึงกับบทความของ **The101.world** โดยบทความนี้จะเน้นในประเด็นการหลอกลวงที่ใช้ความรู้สึกของเหยื่อเข้ามาเกี่ยวข้องด้วย ในเรื่อง **Romance Scam: ไม่รักไม่ว่าอะไร แต่ใยต้องหลอกกันด้วย**[28] อธิบายไว้ว่า วิธีการของ Scammer มี 2 วิธีการด้วยกัน คือ 1. ขโมยข้อมูล ประวัติส่วนตัว หรือรูปภาพของคนอื่นมาดัดแปลงเป็นตัวเอง หรือ 2. อุปโลคข้อมูลส่วนตัวของตนเองขึ้นมา แล้วจะเลือกกลุ่มเป้าหมาย นั่นคือ การตีสนิทหรือการจีบ (Flirting) พอ Scammer สามารถจีบจนได้รับความไว้วางใจจากเหยื่อมากพอแล้ว พวกเขาก็จะเริ่มสร้างสัญญากับเหยื่อ (making a promise) โดยบอกว่าจะมาร่วมสร้างความสัมพันธ์ในระยะยาวและพวกเขาทั้งคู่จะย้ายมาอยู่ด้วยกัน เมื่อ Scammer ทำให้เหยื่อมั่นใจว่าพวกเขาจะได้อยู่ด้วยกันแน่ๆ Scammer ก็เริ่มหลอกเอาเงินหรือเอาสิ่งที่มีค่าจากเหยื่อมาทีละนิด เป็นต้นว่า อาจจะขอให้เหยื่อนั้นโอนเงินมาให้กับตนเพื่อที่ใช้เป็นค่าเดินทางไปหา หรือใช้เป็นการค่าช่วยเหลือในด้านอื่นๆ โดยการหลอกนั้นมีหลายประการ เช่น

การหลอกแล้ว Blackmail การที่ Scammer ไปตีสนิทโดยใช้ความรักเป็นตัวหว่านล้อม และหลอกเอาข้อมูลสำคัญของเหยื่อ เช่น ภาพโป๊เปลือยของเหยื่อ หรือข้อมูลทางธุรกิจบางประการ เป็นต้นว่า Scammer อาจจะหลอกให้เหยื่อมนั้น ‘ร่วมเพศ’ ผ่าน webcam โดยระหว่างที่เหยื่อกำลังมีความสุขกับการร่วมเพศออนไลน์ Scammer ก็จะแอบบันทึกภาพหรือวิดิโอของเหยื่อเอาไว้ จากนั้นก็ให้เวลาผ่านไปสักพัก Scammer ก็จะเอาภาพหรือวิดีโอเหล่านั้นมา blackmail เหยื่อ โดยบังคับขู่เข็ญให้เหยื่อต้องโอนเงินหรือสิ่งของมีค่าให้แก่ตน มิฉะนั้น จะมีการปล่อยภาพหรือวิดีโอเหล่านั้นเพื่อสร้างความเสียหายแก่ชื่อเสียงของเหยื่อ

การหลอกเพื่อฮุบมรดก ในกรณีนี้ Scammer จะเลือกเหยื่อที่ดูมีฐานะ เช่น อาจเป็นลูกหลานของเศรษฐีพันล้าน หรือเจ้าของกิจการ เพื่อที่จะได้หลอกล่อให้แต่งงานและจดทะเบียนสมรส จากนั้นก็จะได้มีความชอบธรรม (อย่างน้อยก็ครึ่งหนึ่ง) ต่อสมบัติของเหยื่อ จากนั้นพอเหยื่อเป็นอะไรไป Scammer ก็จะได้สมบัติไปครอง

การหลอกแบบ Pro-Daters โดยการหลอกลวงประเภทนี้จะมีความพิเศษหน่อยตรงที่จะมีการจัดการอย่างเป็นระบบอย่างมาก Scammer จะหลอกให้เหยื่อนั้นเดินทางข้ามประเทศมาที่ประเทศของ

---

[27] เรื่องเดียวกัน.

[28] The101.world, (2560), *Romance Scam: ไม่รักไม่ว่าอะไร แต่ใยต้องหลอกกันด้วย*. (25 มีนาคม 2561), สืบค้นจาก The101: https://www.the101.world/life/romance-scam/.

ตน และจะเริ่มการรีดไถเงินจากเหยื่อทีละเล็กละน้อยจนกว่าเหยื่อจะหมดตัว ในกรณีนี้ Scammer จะรวมกลุ่มกันทำงาน โดยให้คนในเครือข่ายของตนไปอยู่ตามเส้นทางต่างๆ ที่เหยื่อจะเข้ามาในประเทศและตามสถานที่เที่ยวต่างๆ ในประเทศ เป็นต้นว่า พวกเขาอาจจะหลอกให้เหยื่อจ่ายเงินข้ามประเทศให้คนกลางเพื่อดำเนินการจัดการค่าเดินทางให้ ซึ่งค่าเดินทางที่ว่านี้ก็จะแพงกว่าที่ควรจะเป็น จากนั้น เมื่อเหยื่อเข้ามาในประเทศแล้ว Scammer ก็จะพาไปตามสถานที่ท่องเที่ยวต่างๆ ซึ่งเป็นสถานที่ที่พวกเขา set เอาไว้แล้วสำหรับถลุงเงินเหยื่อ สุดท้ายเหยื่อจะไปตามที่ต่างๆ และโดนตุ๋นเงินไปเรื่อยๆ จนหมดตัว และเมื่อหมดตัวแล้ว Scammer ก็จะทิ้งเหยื่อไปดื้อๆ บางรายถึงขั้นกลายเป็น homeless ในประเทศนั้นไป

และสุดท้าย **แบบแอบอ้างว่าเป็นทหาร** Scammer จะแอบอ้างโดยการสร้าง profile ปลอมขึ้นมา โดยพวกเขาจะไปเอาข้อมูลและรูปภาพของทหารจากเว็บไซต์กองทัพ ซึ่งข้อมูลทหารที่ Scammer นำมาสร้าง profile ปลอมก็คือ ทหารของสหรัฐอเมริกา ส่วนหนึ่งเพราะคนส่วนมากมักคิดว่าทหารอเมริกันนั้นน่าสนใจ และมีความมั่นคง โดยเมื่อ Scammer ใช้ profile ดังกล่าวหลอกให้เหยื่อหลงเชื่อได้แล้ว พวกเขาก็จะเริ่มเรียกร้องให้เหยื่อโอนเงินมาให้ โดยมักอ้างว่า ตนเองนั้นมีลูกติด และลูกกำลังมีปัญหาอะไรบางอย่าง อยากให้ทางเหยื่อช่วยไปก่อน หรือ บอกว่าทางบ้านกำลังมีปัญหาเรื่องค่ารักษาพยาบาล เป็นต้น

จะเห็นว่าในงานของ **ปัทมาภรณ์** และ **The101.world** มีความคล้ายคลึงกันอย่างมาก ไม่ว่าจะเป็นวิธีการล่อลวงหรือพฤติกรรมที่ทาง Scammer ใช้หลอกลวงเหยื่อ ซึ่งจะเป็นการเน้นสร้างความไว้เนื้อเชื่อใจกันเป็นสำคัญ และการทำให้เหยื่อหลงรักตนเองอย่างรวดเร็ว เมื่อพิจารณาอย่างถี่ถ้วนแล้วสามารถเห็นได้ว่าการหลอกล่อเหยื่อ มีการสร้างรูปแบบของการหลอกล่อเอาไว้ อยู่ที่ว่าเหยื่อของ Scammer จะเหมาะสมกับวิธีการประเภทไหนบ้าง

เช่นเดียวกับเป็นงานวิจัยของต่างประเทศก็มีการศึกษาเกี่ยวกับการล่อลวงแบบ Romance Scam ไว้ในต่างประเทศมีการกระทำความผิดเช่นนี้มาตั้งแต่ปี 1970 โดยกลุ่มอาชญากรส่วนใหญ่เป็นคนไนจีเรีย หรือเป็นรู้จักกันในชื่อ “Nigerian Fraud 419 scam” ในอดีตวิธีการหลอกลวงนั้นจะใช้การส่งจดหมายและแฟกซ์ โดยมีเป้าหมายเป็นผู้ชายที่ซื้อนิตยสารผู้ใหญ่ และใช้ระยะเวลาในการสร้างความผูกพันกับเหยื่อในระยะเวลานานถึง 6-8 เดือน อาชญากรกลุ่มนี้มักแสร้งว่ามีเงินจำนวนมากแต่มีเหตุผลบางอย่างที่ไม่สามารถเอาเงินเหล่านั้นออกมากได้ เช่น ทรัพย์สินที่ไม่มีใครครอบครอง, ถูกโกง, ไร้ทายาท เป็นต้น อ้างว่าเหยื่อจะได้รับค่าตอบแทนอย่างสูงเพียงแค่ช่วยพวกเขาให้พ้นจากปัญหาต่างๆ จากเจ้าหน้าที่รัฐหรือคนในครอบครัว[29] ต่อมาการเข้าถึงอินเตอร์เน็ตอย่างแพร่หลายทำให้เกิดการหลั่งไหลของข้อมูลต่างๆ อย่างมากมายซึ่งเปิดโอกาสให้เกิดการฉ้อโกงง่ายยิ่งขึ้น เพราะอาชญากรสามารถใช้อินเตอร์เน็ตในการกำหนดเป้าหมายของเหยื่อได้ง่ายขึ้น[30] romance scam ถือเป็นการฉ้อโกงอย่างหนึ่งที่มีหลอกเหยื่อให้ตกหลุมรัก ด้วยการหว่านล้อมด้วยบทสนทนาความรักอันหอมหวานที่วาดฝันชีวิตคู่ที่สมบูรณ์ และให้ความหวังว่าความสัมพันธ์นี้จะมั่นคงและถาวร จากนั้นจะหลอกให้ส่งเงินไปยังอาชญากร (scammer) โดยใช้เว็บหาคู่ หรือเครือข่ายสังคมออนไลน์เป็นเครื่องมือ

[29] Whitty, M. T., (2015), Anatomy of the online dating romance scam. *Security Journal*, *28*(4), 443-455.

[30] Whitty, M. T.,(2015), Mass-marketing fraud: a growing concern. *IEEE Security & Privacy*, *13*(4), 84-87.

ในบทความงานวิจัยของ **Monica T. Whitty**[31] เรื่อง **Anatomy of the online dating romance scam** เป็นศึกษาจากการเก็บข้อมูล 3 ส่วน คือ การวิเคราะห์ posts จากกลุ่มสนับสนุนออนไลน์ การสัมภาษณ์เชิงลึกจากเหยื่อ และการสัมภาษณ์เจ้าหน้าที่ในองค์กรเพื่อป้องกันอาชญากรรมร้ายแรง (Serious Organised Crime Agency: SOCA) *การศึกษา 1:* เก็บ 200 โพสต์จากเว็บไซต์สาธารณะ แบ่งเป็น ผู้ชายและผู้หญิงที่สูญเงินจากการหลอกลวงอย่างละ 50 ราย และผู้ชายและผู้หญิงที่ไม่สูญเงินจากการหลอกลวงอย่างละ 50 ราย *การศึกษา 2:* สัมภาษณ์เชิงลึก ทั้งเพศชายและเพศหญิงที่อยู่ในประเทศอังกฤษ และอเมริกา จำนวน 20 ราย อายุระหว่าง 38-71 ปี โดยการสัมภาษณ์จะใช้ระยะเวลาประมาณ 3-5 ชั่วโมงต่อคน ส่วนการสัมภาษณ์ผู้ชำนาญการในการบังคับใช้กฎหมาย เป็นประเด็นเกี่ยวกับขั้นตอนการก่ออาชญากรรม ผลกระทบทางจิตใจของเหยื่อ และข้อเสนอเกี่ยวกับการป้องกันอาชญากรรมในอนาคต โดยจากการศึกษาทำให้เห็นลำดับการเกิดขึ้นของ Romance Scam เป็น 5 ขั้นตอนดังนี้

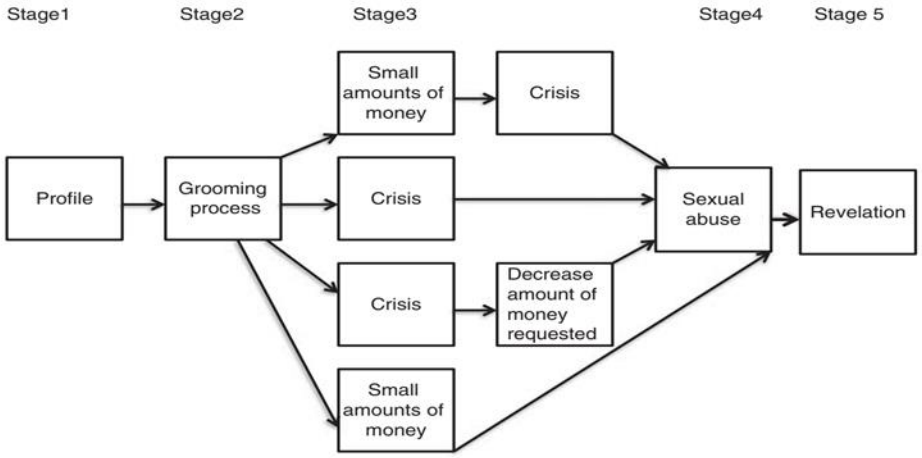


Figure 1: Romance scam trajectories.

ขั้นตอนที่หนึ่ง **โปรไฟล์ปลอม** เป็นขั้นตอนแรกของการหลอกลวงของ Scammer โดยการปลอมจะเป็นภายในโปรไฟล์ที่น่าดึงดูด บอกรายละเอียดส่วนตัว เช่น งานอดิเรก สิ่งที่สนใจ อาชีพ หน้าที่การงาน บางกรณีจะสร้างโปรไฟล์ว่าเป็นลูกครึ่งหรือมีเชื้อชาติเดียวกับเหยื่อ หรือมักโกหกว่าเป็นคนที่มีอำนาจ เช่น ทหาร เศรษฐี นักธุรกิจ หมอ เป็นต้น หากเป็นโปรไฟล์ผู้หญิงปลอม มักจะมีลักษณะคล้ายนางแบบและน่าหลงใหล โดยกลุ่มเป้าหมายจะเป็นชายอายุ 50 ปีขึ้นไป ส่วนโปรไฟล์ผู้ชายปลอมนั้น จะเป็นคนมีเสน่ห์ ลักษณะฐานะมั่นคง ร่ำรวย ซึ่งภาพทั้งหลายที่ใช้ในการสร้างโปรไฟล์ก็มาจากเครือข่ายสังคมออนไลน์ บางรายใช้รูปแต่งกายในเครื่องแบบทหาร ซึ่งเป้าหมายก็จะเป็นผู้หญิงวัยเกษียณ เป็นม่าย หย่าร้างแล้ว และกรณีของชายรักร่วมเพศปลอม จะต้องใช้ผู้ชายที่มีแรงดึงดูดสูงสำหรักลุ่มรักร่วมเพศโดยตรง หน้าตาดี บุคลิกดี คล้ายนายแบบ และอายุไม่มากนัก

ขั้นตอนที่สอง **Grooming** เป็นช่วงเวลาที่ Scammer ใช้สร้างความไว้ใจ และทำให้เหยื่อเชื่อว่าพวกเขามีเงินจริงๆ ซึ่งในขั้นตอนนี้จะมีความแตกต่างกันออกไปของลักษณะเหยื่อแต่ละราย บางรายทำให้เหยื่อรู้สึกว่าไม่เคยได้พบสิ่งนี้ เช่น ชอบอะไรเหมือนกัน คิดอะไรเหมือนกัน โดยมุ่งหมายให้เหยื่อตกหลุมรักตนอย่างรวดเร็วที่สุด บางกรณีใช้เวลาเพียง 1 อาทิตย์ บางกรณีใช้เวลา 1 เดือน หรือ 1 ปี

[31] Whitty, M. T., (2015), Anatomy of the online dating romance scam. *Security Journal*, *28*(4), 443-455.

แตกต่างกันไป โดยในขั้นตอนนี้ Scammer จะใช้เวลาเรียนรู้และทำความเข้าใจเหยื่อแต่ละคน และใช้วิธีที่ดึงดูดใจแต่ละคนแตกต่างกันไป ส่วนมากจะทำเป็นกิจวัตร เช่น ทุกๆ เช้า หรือเย็น เพื่อทำให้ความสัมพันธ์ดูน่าเชื่อถือ

เมื่อ Scammer แน่ใจว่าเหยื่อรู้สึกดีกับตนแล้ว จะสร้างเรื่องให้เหยื่อเชื่อว่า ตนต้องการที่จะมาหาเหยื่อ แต่ติดขัดด้วยเหตุผลบางอย่าง เช่น ต้องไปทำภารกิจทางทหาร หรือติดต่อธุรกิจ หรือยังหาตั๋วเครื่องบินไปหาเหยื่อยังไม่ได้ เป็นต้น และจะย้ำเสมอว่าอยากไปหาเหยื่อ รวมถึงคาดหวังที่จะสร้างความสัมพันธ์ที่ยืนยาว ซึ่งจะทำให้เหยื่อหลงเชื่อได้ง่ายและรวดเร็ว และท้ายที่สุดในขั้นตอนนี้ scammer จะร้องขอของขวัญบางอย่าง เช่น น้ำหอม โทรศัพท์มือถือ เพื่อเป็นการทดสอบศักยภาพทางการเงินของเหยื่อ เหยื่อคนหนึ่งเล่าว่า “ตนลังเลที่จะส่งของขวัญไปให้ และขณะเดียวกันนั้น scammer ส่งดอกกุหลาบสีแดงมาให้เธอ” เทคนิคดังกล่าวกระตุ้นให้เหยื่อทำตามคำขอของ scammer จากการศึกษาพบว่า เหยื่อทุกคนหลีกเลี่ยงการตกเป็นเหยื่อทางการเงิน

ขั้นตอนที่สาม **การทำให้เจ็บปวด (The Sting)** หลังจากที่ scammer พยายามล่อลวงให้เหยื่อโอนเงินให้ ถ้าพวกเขาทำพลาดในครั้งแรก พวกเขาจะล่อลวงเหยื่อต่อไป เพื่อรอโอกาสในการล่อลวงให้เหยื่อโอนเงิน ในขั้นตอนนี้ทำให้เหยื่อบางคนรู้ว่านี่คือการหลอกลวง และไม่ได้ส่งเงินให้ ซึ่ง scammer สร้างสถานการณ์ต่างๆ ดังนี้ 1. Small amounts to a crisis Scammer การเริ่มขอเงิน ไม่ว่าจะด้วยเทคนิค “the foot-in-door technique” หรือการสร้างสถานการณ์ขอความช่วยเหลือ (crisis) ถ้าสำเร็จ scammer ก็จะได้เงิน แต่ถ้าไม่สำเร็จ scammer ก็จะเงียบหายไป หรือไม่ก็หาวิธีเกลี่ยกล่อมด้วยวิธีอื่น และหลอกอีกครั้งหนึ่ง โดยที่ scammer จะขอให้เหยื่อส่งเงินจำนวนไม่มากนักให้ก่อนที่จะขอเงินในจำนวนมากๆ มักอ้างว่าต้องใช้เงินด่วน เช่น จ่ายค่ารักษาพยาบาล หรือมีเงินสดในกระเป๋าแต่ไม่ผ่านศุลกากร เป็นต้น ถ้าเหยื่อหลงเชื่อในครั้งแรก scammer ก็จะเริ่มขอเงินจำนวนมากขึ้นในครั้งต่อไป 2. The crisis สถานการณ์นี้เกิดขึ้นบ่อยที่สุด เป็นการขอเงินก้อนใหญ่ เนื่องจากได้พิจารณาแล้วว่าเหยื่อมีศักยภาพในการจ่ายเงินนั้น คือไม่มีการทดสอบศักยภาพทางการเงินของเหยื่อด้วยการขอเงินจำนวนน้อยๆ การอ้างว่า ทั้งคู่จะสร้างธุรกิจร่วมกัน หรือเกิดเหตุการณ์ไม่คาดคิด เช่น เกิดอุบัติเหตุ ลูกป่วยหนัก หรือธุรกิจต้องใช้เงินด่วน เป็นต้น 3. The crisis to a decrease in requested funds สถานการณ์นี้เกิดขึ้นบ้าง ในกรณีที่เหยื่อไม่ส่งเงินให้ scammer ตามที่ร้องขอ หรือ scammer ยอมลดจำนวนเงินที่ขอไปในครั้งก่อนหน้า เช่น scammer อ้างว่าต้องใช้เงินเพราะเกิดอุบัติเหตุฉุกเฉิน แต่เหยื่อให้ได้ในจำนวนที่น้อยกว่าที่ร้องขอ scammer ก็ยอมรับเงินจำนวนน้อยกว่านั้นด้วยการใช้เทคนิค “the door-in-the-face technique” เหยื่อคนหนึ่งเล่าว่า “เขาของเงิน 2,000 เหรียญ จากนั้นลดลงเหลือ 300 เหรียญ โดยอ้างงว่าเขาได้เงินมาบางส่วนแล้วและต้องการอีกแค่บางส่วนเท่านั้น” และ 4. Small amounts of money เหยื่อหลายคนไม่เจอสถานการณ์นี้ เพราะการหลอกลวงดังกล่าวต้องใช้เวลาล่อลวงเหยื่อเป็นเวลานาน 2-3 ปี scammer จะขอเงินที่ละน้อยๆ แต่บ่อยครั้ง เช่น ต้องเอาเงินค่าเครื่องบินที่จะเดินทางไปหาเหยื่อ ไปใช้จ่ายค่าเทอมก่อน หรือเอาไปใช้ในค่าใช้จ่ายจำเป็นอื่นๆ เป็นต้น ส่วนมากกรณีเหล่านี้จะเกิดขึ้นกับเหยื่อผู้ชาย

ขั้นตอนที่สี่ **Sexual abuse** บางกรณีที่ scammer ร้องขอให้เหยื่อแสดงกิจกรรมทางเพศหน้า webcam แต่ส่วนมากเหยื่อจะไม่รายงานเรื่องดังกล่าว เพราะถือเป็นเรื่องที่หน้าอับอาย สิ่งนี้เกิดขึ้นน้อยมาก และที่พบมักเป็นกรณีที่เหยื่อบอกว่าไม่มีเงิน เหยื่อจะถูกร้องขอให้ถอดเสื้อ หรือช่วยตัวเองผ่านเว็บแคม บางคนจะโดนขู่ว่าจะ blackmail

ขั้นตอนที่ห้า **Revelation** เหยื่อรู้ตัวว่าตนเองถูกหลอก แบ่งเป็น 2 กรณีคือ 1. เหยื่อที่ไม่สูญเงิน จะข้ามขั้นตอนที่ 3 และ 4 ไปอย่างรวดเร็วจนมาถึงขั้นตอนนี้ 2. เหยื่อที่สูญเงิน โดยเหยื่อบางคนจะพยายามหาหลักฐานมาสนับสนุนเมื่อพวกเขามีลางสังหรณ์ว่าถูกหลอก เช่น แจ้งสถานทูต ตำรวจ และบริษัท/เว็บหาคู่ ในบางกรณีเหยื่อบางคนได้รับแจ้งจากเจ้าหน้าที่ผู้เกี่ยวข้องว่าตนกำลังถูกหลอกลวง หรือมีเพื่อนแจ้งตำรวจว่าตนกำลังถูกหลอก ยิ่งไปกว่านั้นมีการซ้อนแผนของ scammer เมื่อทราบว่าเหยื่อรู้ตัวแล้วว่าถูกหลอก โดย scammer จะปลอมเป็นเจ้าหน้าที่ตำรวจของแอฟริกา ติดต่อเหยื่อว่า scammer ที่หลอกคุณถูกจับแล้ว และจะคืนเงินให้กับเหยื่อ แต่เหยื่อต้องจ่ายเงินค่าดำเนินการต่างๆ ในการรับเงินคืนดังกล่าว และทำให้เหยื่อยังคงอยู่ในวงจรของเหยื่อนั้นต่อไปซ้ำแล้วซ้ำเล่า

จะเห็นว่าการหลอกเหยื่อของต่างประเทศจะมีชั้นเชิงที่สูงกว่าประเทศไทยอยู่ในบางกรณี จากกรณีข้างต้นที่เหยื่อโดนหลอกซ้ำว่าได้จับตัว Scammer แล้ว โดยผู้หลอกเหยื่อก็เป็น Scammer ด้วยกันเอง ซึ่งก็เป็นส่วนหนึ่งที่ทำให้เหยื่อไม่หลุดพ้นออกจากวงจรของการหลอกลวงนี้ ถูกหลอกซ้ำไปซ้ำมาเรื่อยๆ จนบางรายถึงขั้นคิดฆ่าตัวตายเพื่อหนีปัญหาและความอับอายดังกล่าว

ในงานวิจัยที่ศึกษาถึงปัญหาที่น่าสนใจอย่างมากในงานของ **Tan Hooi Koon** และ **David Yoong**[32] เรื่อง **Preying on lonely hearts: A systematic deconstruction of an Internet romance scammer's online lover persona**เป็นการศึกษาว่าผู้เสียหายส่วนใหญ่ทำไมถึงถูกหลอกเรื่องภาษาได้ ทั้งที่ผู้เสียหายบางคนเป็นผู้ที่มีความรู้ความสามารถในด้านภาษาอังกฤษเป็นอย่างดี จากการศึกษาพบว่า Scammer ใช้วิธีการสร้างบทบาท บุคลิก ลักษณะของ "คนดี" เช่น การใช้คำพูดและสำนวนในแง่ดีที่จะสื่อนัยยะของการเป็นคนที่ซื่อสัตย์ จริงใจ และพึ่งพาได้ และอีกทางหนึ่งเพื่อพิสูจน์ความไว้วางใจและความซื่อสัตย์โดยการเต็มใจยอมรับข้อจำกัดและความผิดพลาดของเหยื่อ นอกจากนั้นยังมีการสร้างความน่าเชื่อถือด้วยการอ้างถึงตัวตนของสถาบันหรืออาชีพที่มีความมั่นคงและตรวจสอบได้ และสิ่งที่ดูน่าเชื่อถือที่ถูกใช้อ้างอยู่บ่อยครั้งคือ อ้างว่าตนเป็นคนเป็นมีชื่อเสียง หรืออ้างถึงความสำเร็จต่างๆ ในอดีตอันจะสามารถโน้มน้าวให้เชื่อถือความสำเร็จในอนาคตร่วมกัน จากนั้นจะพยายามสร้างความรู้สึกดีๆ และมีความเข้าอกเข้าใจเหยื่อในทุกๆ เรื่อง แสดงความห่วงใย การใส่ใจต่อผู้อื่น การให้ความสำคัญแก่ผู้อื่นก่อน ดังนั้นการเปิดเผยข้อมูลส่วนบุคคลจำนวนมากและบ่อยครั้งทั้งในแง่ของความคิดและความรู้สึก ทำให้เป็นเรื่องง่ายต่อการสร้างความสัมพันธ์ และการจัดการความสัมพันธ์ในโลกออนไลน์ สิ่งที่ทำให้ scammer บรรลุเป้าหมายของการหลอกลวงนั่นก็คือ ความน่าเชื่อถือ ดังนั้นพื้นฐานของความสำเร็จของ คือ ความเชื่อใจและข้อเท็จจริง scammer จะสร้างความเชื่อมั่นให้แก่เหยื่อในทุกๆ ด้าน ไม่ว่าจะเป็นการสร้างเว็บไซต์ที่เกี่ยวกับอาชีพของตน การแสดงภาพกิจวัตรประจำวัน รวมถึงการเต็มใจที่จะคุยกับเหยื่อทางโทรศัพท์เพื่อพิสูจน์ว่าพวกเขาเป็นคนจากสหราชอาณาจักรจริงๆ ด้วยสำเนียงการพูด เหยื่อคนหนึ่งอ้างว่าได้พูดคุยกับแม่ของชายที่เธอหลงรัก (scammer) เป็นเหตุผลที่ทำให้เธอเชื่อ และมั่นใจว่าคนที่เธอกำลังสานสัมพันธ์อยู่มีตัวตนจริงๆ ในส่วนของเรื่องไวยากรณ์นั้น แม้ว่าพวก scammer จะมีข้อบกพร่องเล็กน้อยในการเลือกใช้คำศัพท์ หรือเครื่องหมายวรรคตอน แต่ส่วนมากประโยคก็จะถูกต้อง และมีเนื้อหาสอดคล้องกัน ทั้งนี้อีกเหตุผลที่พอฟังขึ้นก็คือ คนส่วนใหญ่มักไม่ให้คามสำคัญกับความถูกต้อง ไวยากรณ์ หรือแบบฟอร์มของภาษาในการสนทนาอย่างไม่เป็นทางการนั่นเอง

[32] Tan, H. K., & David, Y., (2017). Preying on lonely hearts: A systematic deconstruction of an internet romance scammer's online lover persona. *Journal of Modern Languages*, *23*(1), 28-40.

ในประเด็นปัญหาเรื่อง Romance Scam เป็นประเด็นที่มีความละเอียดอ่อนและมีผลกระทบกับจิตใจของผู้ตกเป็นเหยื่อสูงมาก มันจึงกลายเป็นจุดอ่อนสำคัญที่ทำให้พวก Scammer ใช้ในการกระทำความผิดเรื่อยไป ซึ่งมีเหยื่อส่วนใหญ่จะรู้สึกเสียใจอย่างมากเมื่อทราบว่าตนถูกหลอก เพราะเหยื่อหลงรักพวก Scammer ไปแล้วจริงๆ ซึ่งการป้องกันการหลอกลวงนี้เป็นเรื่องที่จัดการได้ยากมาก ไม่ว่าจะโดยการจับหรือการติดตามดำเนินคดี เนื่องจากอาชญากรรมมักเป็นชาวต่างชาติที่อยู่คนละประเทศกับเหยื่อ นอกจากนั้นการติดตามก็เป็นเรื่องที่ยากและเวลานานพอสมควร จึงกลายเป็นปัญหาและอุปสรรคอย่างยิ่ง

แต่ถึงอย่างไรนั้นในต่างประเทศที่มีกฎหมายลงผู้กระทำความผิดแล้ว ยังมีวิธีการป้องกันและแนวทางแก้ไขอื่นๆ ด้วย ในงานของ **Andreas Zingerle** และ **Linda Kronman**[33] ในบทความเรื่อง **Humiliating Entertainment or Social Activism? Analyzing Scambaiting Strategies Against Online Advance Fee Fraud** ได้อธิบายถึงการเกิดชุมชนออนไลน์เพื่อโต้กลับกลุ่ม “419 scams” ซึ่งในบทความนี้จะกล่าวถึง 2 เว็บไซต์ที่เกี่ยวข้องคือ 419eater.com และ thescambaiter.com. และ Scambaiter จะเป็นคนที่ทำหน้าที่โต้กลับ Scammer ด้วยวิธีการดังกล่าวต่อไปนี้ **1. The scam alerters** เป็นการระบุและรายงานการหลอกลวงออนไลน์ เพื่อเพิ่มการตระหนักรู้โดยทั่วไปถึงการหลอกลวงทางอินเตอร์เน็ต พวกเขาจะเตือนทั้งแบบรายบุคคลและเป็นกลุ่มแก่ผู้ที่เสี่ยงต่อการหลอกลวงด้วยการให้ข้อมูลที่มีรายละเอียดและเชื่อถือได้ มีหลายเว็บไซต์และฟอรัม (forum) หลายแห่งที่คอยให้ข้อมูลผู้ที่จะตกเป็นเหยื่อ เช่น romancescam.com (เน้นเฉพาะเรื่องหลอกลวงรักออนไลน์) scamvictimsunited.com (ดูแลเหยื่อของการฉ้อโกง) scamwarners.com และ 419eater.com หลายๆ ฟอรัมทำหน้าที่เป็นแพลตฟอร์มในการตรวจและหารือเกี่ยวกับอีเมลไม่พึงประสงค์ต่างๆ ผลก็คือ ทำให้ผู้ที่อาจตกเป็นเหยื่อหลายคนได้รับแจ้งเตือนเกี่ยวกับการหลอกลวงรูปแบบใหม่ๆ และเตือนให้ระวังอีเมลที่ยื่นข้อเสนอที่ดีเกินกว่าจะเป็นจริงได้ และสำหรับผู้ที่เคยตกเป็นเหยื่อแพลตฟอร์มนี้จะให้ข้อมูลเกี่ยวกับคำถามที่พบบ่อยและคำแนะนำเพิ่มเติม **2. The Trophy Hunters** คือ กลุ่ม scambaiters ที่เป็นผู้ตอบกลับอีเมลหลอกลวงโดยทราบว่า scammer เป็นผู้เขียนอีเมลนั้น พวกเขาจะใช้กลลวงต่างๆ ตลบหลัง scammer ให้เหมือนว่าพวกเขาเป็นเหยื่อจริงๆ เพื่อล่อเอาข้อมูลต่างๆ จาก scammer ไม่ว่าจะเป็นรูปภาพ ข้อความการสนทนา เสียง หรือวิดีโอ เพื่อใช้เป็นหลักฐาน **3. The Website Reporters** บ่อยครั้งที่ scammer ปลอมเว็บไซต์ขึ้นมาเพื่อให้ดูเป็นมืออาชีพ และดูน่าเชื่อถือว่าเว็บไซต์ที่อ้างนั้นมีตัวตนจริง เช่น บริษัท เว็บขายของออนไลน์ ธนาคาร องค์กรการกุศล กลุ่มศาสนา หรือบริษัท IT เป็นต้น โดย scambaiter จะพิสูจน์เว็บไซต์เหล่านี้ด้วยการเชื่อมโยงรายการ DNS กับฐานข้อมูลผู้หลอกลวง จากนั้นจะทำการบันทึกกิจกรรมที่ผิดกฎหมายและรายงานการค้นพบดังกล่าวไปยังผู้ให้บริการ (hosting provider) เพื่อนำเว็บไซต์ดังกล่าวออกหรือแบนเว็บนั้นไป **4. The Bank Guards** คือ scambaiter บางคนมีความเชี่ยวชาญพิเศษที่ทำหน้าที่สังเกตและรายงานบัญชีธนาคารปลอม หรือบัญชีที่มีเงินเข้าออกมากอย่างผิดสังเกต พวกเขาเชื่อว่าพวก scammer ยอมเสียเงินอย่างถูกกฎหมายเพื่อจัดการกับบัญชีเหล่านี้ หรือบางครั้งหลอกให้เหยื่อเปิดบัญชีเพื่อรับเงินโอน พวกเขาจะเก็บข้อมูลและรายงานอาชญากรรมดังกล่าวต่อเจ้าหน้าที่ธนาคารให้ทำ

[33] Zingerle, A., & Kronman, L., (2013, October). Humiliating Entertainment or Social Activism? Analyzing Scambaiting Strategies Against Online Advance Fee Fraud. In *2013 International Conference on Cyberworlds* (pp. 352-355). IEEE.

การอายัดบัญชีและดำเนินการตามกฎหมาย **5. The Romance Scam Seekers** โดยปกติพวก scammer มักสร้างโปรไฟล์ปลอมเพื่อหาเหยื่อทั้งชาย และหญิงในเว็บหาคู่ ซึ่ง scambaiters จะเฝ้าระวังและสอดส่องในเว็บไซด์หาคู่ต่างๆ เพื่อเตือนผู้ที่อาจตกเป็นเหยื่อ หรือเหยื่อ ในบางครั้งจะแกล้งเป็นเหยื่อเพื่อให้ scammer ส่งข้อมูลต่างๆ มาให้ และเก็บรูปภาพและรวบรวมคำพูดหวานๆ ที่ scammer ใช้เป็นประจำ เพื่อจัดทำเอกสารชี้แจงแนวทางปฏิบัติของกลุ่ม scammer เพื่อโพสเตือนคนอื่นๆ เช่น scamdigger.com หรือทำเป็นหนังสือเล่มเล็กๆ ชื่อ 'Hello Sweaty' **6. The Safari Agents** คือ scambaiters กลุ่มที่พยายามจะล่อให้พวก scammer ออกมาจากถิ่นที่ทำงานของตนเอง โดยการแสร้งว่าตนเป็นเหยื่อและจะไปเที่ยวแถบใกล้ๆ กับไนจีเรีย และพักอยู่โรงแรมแถวนั้น จากนั้นจะหว่านล้อมให้ scammer ออกมาเจอที่โรงแรม ผ่านการใช้เว็บไซด์ safarihotelsgroup.com ในเว็บไซด์ซึ่งอ้างว่าเป็นตัวแทนธุรกิจขนาดเล็กที่ดำเนินกิจการแบบครอบครัว และมีเครือข่ายโรงแรมราคาประหยัดในแอฟริกาตะวันตก พวกเขาใช้เว็บโรงแรมเป็นเครื่องมือล่อเพื่อดักจับ scammer และทำให้เชื่อว่ามีเหยื่ออยู่ที่โรงแรมนั้นจริงๆ และวิธีการสุดท้าย **7. The Inbox Divers** จะเป็นกลุ่มวิศวกรสังคมที่สามารถเข้าถึงข้อมูลบัญชีอีเมลของเหล่า scammer และผู้อาจตกเป็นเหยื่อได้ไม่ว่าจะด้วยวิธีใดก็ตาม ทั้งนี้ทำหน้าที่เข้าไปเก็บข้อมูลการสนทนาต่างๆ และส่งข้อความเตือนผู้อาจตกเป็นเหยื่อ และเหยื่อว่า "คุณกำลังถูกหลอกจากบุคคลเหล่านี้"

วิธีการดังกล่าวข้างต้น ถือเป็นเครื่องมือส่วนหนึ่งที่ได้ช่วยเหลือ ป้องกันเหยื่อจากกลุ่ม Scammer ได้ และทำให้เหยื่อไม่ตกอยู่ในสภาวะของการถูกล่อลวง การสูญเสียเงิน รวมถึงเกิดความรู้สึกอับอายหลังจากที่รับรู้ว่าตนถูกหลอกด้วย จากบทหนึ่งในหนังสือของ **Markus Jakobsson**[34] ในเรื่อง **Understanding Social Engineering Based Scams** ที่มีการใช้เทคโนโลยีเพื่อช่วยในการตรวจจับ scammer บนโลกออนไลน์ และแจ้งเตือนผู้ที่อาจตกเป็นเหยื่อ โดยแสดงให้เห็นการใช้ประโยชน์จาก spam filter ในเว็บ Craigalist[35] เพื่อเป็นตัวช่วยในการสืบหาที่ตั้งของคนร้ายในทางคดีที่เกี่ยวกับ romance scam จากการทดลองในระยะเวลา 3 เดือน (เดือนเมษายน-กรกฎาคม 2015) พบว่า มี scammer เข้ามาติดกับดัก (spam) ที่ตั้งไว้ในเว็บไซด์ดังกล่าวจำนวน 314 ราย แต่มี scammer ที่ลงทะเบียน และส่งอีเมล์มายังผู้ทดลองเพียง 22 รายเท่านั้น โดย 60% มี IP address อยู่ที่แอฟริกา (ไนจีเรีย และแคเมอรูน) รองลงมาเป็นแคนนาดา นอกจากนั้นยังพบว่าอีเมล์ที่ตอบกลับมาจำนวน 50% เป็นระบบอัตโนมัติ (auto-response) ของ scammer สังเกตได้จาก e-mail address หรือ URL เหมือนกัน และมีความข้อความข้างในเหมือนกัน แสดงให้เห็นว่า scammer ใช้ระบบอัตโนมัติเพื่อเป็นกระบวนการเบื้องต้นในการหาเหยื่อรายใหม่ๆ อย่างไรก็ตามจากการศึกษานี้สังเกตเห็นว่า scammer ส่วนใหญ่จะไม่ลงทะเบียนในลิงก์หาคู่ หรือส่งอีเมล์ไปทั่วอย่างไม่มีเป้าหมาย เพราะถือว่าเป็นเรื่องเสี่ยงและอันตรายอย่างมากต่อการติดตามตัว ดังนั้น scammer เหล่านี้มักซุ่มดูเหยื่อและคัดเลือกเหยื่อเป็นอย่างดีก่อนการปฏิบัติการหลอกลวงรัก และสิ่งสร้างความลำบากสำหรับการติดตาม IP address คือการที่ scammer ใช้ VPN สิ่งนี้จะช่วยป้องกันในการตาม IP address ซึ่งถือเป็นกระบวนการที่ค่อนข้างยุ่งยากในการติดตามคนร้าย ประโยชน์ที่เห็นได้ชัดจากการใช้ระบบ spam filter ดังกล่าวคือ จะสามารถเตือนผู้ที่มีความเสี่ยงในการถูกหลอก เนื่องจากการทำงานของ spam filter ภายในเว็บไซด์ที่ถูกติดตั้งแล้ว ระบบจะเรียนรู้ template ของข้อความเชิง romance scam (เนื่องจาก

[34] Jakobsson, M. (Ed.), (2016). *Understanding social engineering based scams*. New York: Springer.

[35] Craigalist เป็นเครือข่ายชุมชนออนไลน์ที่ใช้ประกาศขายของ หาคู่ และหางาน

การศึกษาส่วนใหญ่พบว่า scammer มักใช้ template เดียวกัน เพียงแต่เปลี่ยนชื่อหรือสถานการณ์ที่สร้างขึ้นเล็กน้อย เพื่อประหยัดค่าจ้างในการตรวจสอบความถูกต้องของข้อความที่ส่งไป) จากนั้นเมื่อระบบตรวจพบว่ามีความข้อความที่เหมือนหรือคล้ายคลึงกัน ระบบจะทำเครื่องหมายและคำเตือนว่ามีความเสี่ยงในการถูกหลอกจากลิงก์ดังกล่าว

ในประเทศมาเลเซียมีความพยายามที่จะจัดการปัญหาและรับมือกับการเพิ่มขึ้นของการล่อลวงแบบ Romance Scam ด้วยการศึกษาข้อบกพร่องต่างๆ ที่กลายเป็นช่องโหว่ให้อาชญากรกลุ่มดังกล่าวเข้ามาหาผลประโยชน์ในประเทศ และนำผลการศึกษาที่ได้มาปรับเป็นข้อเสนอแนะเพื่อจัดการกับปัญหาดังกล่าวให้ตรงจุด ซึ่งได้กล่าวไว้ในบทความวิจัยของ **Ahmad Safwan Hamsi**[36] เรื่อง **Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors and Keys to the Problem** งานวิจัยชิ้นนี้แสดงให้เห็นช่องโหว่ของนโยบาย และการจัดการทั้งหมด 5 ประเด็น ที่เอื้อให้เกิดกลุ่ม scammer เข้ามาใช้พื้นที่ในประเทศมาเลเซีย เพื่อเป็นจุดพักพิงและรวมกลุ่มเพื่อก่ออาชญากรรมการหลอกลวงรักในโลกออนไลน์ รวมถึงได้ให้ข้อเสนอแนะในการจัดการกับปัญหา และรัฐบาลได้มีความพยายามในการจัดการกับปัญหาดังกล่าวไปแล้วบางส่วน **1.การใช้วีซ่านักเรียนผิดวัตถุประสงค์** ถือเป็นปัญหาหลัก เนื่องจากมาเลเซียมีนโยบายในการเป็นศูนย์กลางของการศึกษาโลก ซึ่งเป็นการเปิดรับผู้คนจากนานาประเทศด้วยการให้วีซ่านักเรียนเป็นจำนวนมาก และจากการสำรวจพบว่าคนไนจีเรียจำนวน 9,146 คนเข้าประเทศด้วยวีซ่านักเรียนจากจำนวนนักเรียนต่างประเทศทั้งหมด 123,000 คน ผู้วิจัยเสนอว่าสถานทูตควรร่วมมืออย่างใกล้ชิดกับตำรวจมาเลเซียและหน่วยงานตรวจคนเข้าเมืองเพื่อรายงานสถานะของนักเรียน และอัพเดทข้อมูลให้ทันสมัยอยู่เสมอ นอกจากนั้นเมื่อปี 2013 กระทรวงศึกษาธิการได้เข้ามามีส่วนร่วมในการจัดการเรื่องนี้โดยเริ่มมีการตรวจสอบและติดตามนักเรียน/นักศึกษาต่างประเทศให้เข้มงวดมากขึ้นกว่าเดิม[37] **2.ข้อบกพร่องของระบบธนาคาร** ระบบธนาคารที่ก้าวหน้าของมาเลเซียเป็นช่องโหว่ให้อาชญากรเปิดบัญชีและโอนเงินในต่างประเทศได้ง่ายขึ้น การเปิดบัญชีทำได้ง่ายๆ โดยการทำธุรกรรมออนไลน์ ซึ่งอาชญากรอาจขโมยข้อมูลส่วนบุคคลของเหยื่อเพื่อใช้การยืนยันตัวตน เช่น เลขบัตรประจำตัวประชาชน ที่อยู่ เบอร์โทรศัพท์ หรือข้อมูลทางการเงินอื่นๆ เป็นต้น มาเลเซียได้พยายามแก้ปัญหาด้วยการใช้เทคโนโลยีไบโอเมตริก (biometrics) เข้ามาช่วยแก้ปัญหาการยืนยันตัวตนของระบบธนาคาร สำนักข่าว The Associated Press รายงานว่ามีการพัฒนาใช้การตรวจจับเสียง (speaker recognition) ในธนาคารเพื่อตรวจจับอาชญากรและปกป้องผู้บริโภค ด้วยการใช้กรองเสียงระหว่างการพูดคุยโทรศัพท์กับธนาคาร ระบบจะทำการจับคู่กับเสียงของอาชญากรที่มีอยู่ในระบบ **3.การแก้ไขพระราชบัญญัติกฎหมายไซเบอร์ในปัจจุบัน** ต้องยอมรับก่อนว่าตำรวจมาเลเซียยังขาดแคลนทรัพยากรและผู้เชี่ยวชาญในการรับมือกับปัญหาดังกล่าว และยังปล่อยให้มีการฟ้องร้องคดีอาญาอยู่เป็นจำนวนมาก ดังนั้นรัฐบาลมาเลเซียจึงได้ดำเนินการก้าวไปอีกขั้นด้วยการเพิ่มเติมกฎหมายหลายฉบับเพื่อจัดการกับอาชญากรรมไซเบอร์ โดยกำหนดฐานความผิดเกี่ยวกับกระทำผิดโดยคอมพิวเตอร์

[36] Hamsi, A. S., Bahry, *Criminology* F. D. S., Tobi, S. N. M., & Masrom, M. (2015). Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors and Keys to the Problem. *Journal of Management Research*, *7*(2), 169.

[37] Reauters, (2014), *US American targeted as Malaysia becomes Internet scam haven*, สืบค้นจาก http://www.thestar.com.my/News/Nation/2014/07/09/Internet-scam-US-women-Nigerians-Malaysia.

เพิ่มเติม ผู้วิจัยเสนอเพิ่มเติมว่าควรมีการอัพเดทและแก้ไขกฎหมายไซเบอร์ในมาเลเซียอยู่เป็นประจำให้ทันต่อการพัฒนาของการเทคโนโลยีและการสื่อสารที่มีพัฒนาอย่างต่อเนื่อง **4.เว็บเดท/เว็บหาคู่เครือข่ายสังคมออนไลน์** scammer ส่วนใหญ่มักใช้ช่วงเวลาที่เหยื่ออ่อนแอและกำลังมองหารักแท้ในโลกออนไลน์ในการขโมยข้อมูลส่วนตัวหรือหลอกล่อเหยื่อ ดังนั้นสิ่งสำคัญที่สุดในการสร้างความสัมพันธ์บนเครือข่ายสังคมออนไลน์ คือการหลีกเลี่ยงการเปิดเผยความลับที่เป็นข้อมูลส่วนบุคคลทั้งหลายในช่วงระยะแรกที่สนทนากัน แต่ละคนควรป้องกันตนเองให้พ้นจากกลุ่มอาชญากรเหล่านี้ด้วยวิธีการดังนี้เช่น *ไม่ควรเปิดเผยข้อมูลทุกอย่างในโปรไฟล์* เพราะหลายคนมักจะเปิดเผยข้อมูลส่วนตัวหลายอย่างในเว็บไซต์เพื่อหวังว่าระบบจะจับคู่ที่เหมาะสมที่สุดมาให้ตน ไม่ว่าจะเป็นที่อยู่ ข้อมูลการงาน เบอร์โทรศัพท์ การศึกษา หรือข้อมูลภายในครอบครัว เป็นต้น ซึ่งสิ่งเหล่านี้ถือที่เป็นช่องโหวให้ scammer มาเข้าถึงตัวตนของผู้ใช้งานอย่างง่ายดาย *สอบถามบุคคลอื่นเกี่ยวกับเรื่องราวของเขา/เธอ* ทั้งนี้เพื่อตรวจสอบให้แน่ใจว่ามีบุคคลนี้อยู่ในโลกความเป็นจริง *ระวังการให้ความช่วยเหลือทางการเงินทุกชนิด* สำหรับผู้ที่รู้จักกันในโลกออนไลน์เพราะส่วนใหญ่มักจะเป็น scammer *สร้างรหัสผ่านให้รัดกุม* สำหรับเว็บหาคู่ไม่ควรเป็นรหัสผ่านที่เดาง่าย และมีคนรู้ *จำไว้เสมอว่าต้องแยกแยะระหว่างความรักและการเงินออกจากัน* และท้ายที่สุด *หากรู้ตัวหรือสงสัยว่ากำลังถูกหลอกให้รีบแจ้งความ/ร้องทุกข์โดยเร็วที่สุด* โดยแจ้งที่เจ้าหน้าที่ตำรวจในท้องที่ หรือศูนย์รับเรื่องอาชญากรรมอินเตอร์เน็ตในท้องที่ นอกจากนั้นในมาเลเซียมีหน่วยงานเฉพาะที่สืบสวนเกี่ยวกับเรื่องนี้คือ Bukit Aman Commercial Crime Investigations Department (CCID) **5.การควบคุมสถานการณ์ของรัฐบาล** ผู้วิจัยมองเห็นว่าบางครั้งเรื่องดังกล่าวรัฐบาลไม่สามารถเข้าไปจัดการและควบคุมได้ เนื่องจากการใช้งานอินเตอร์เน็ตเป็นเรื่องที่ควบคุมได้ยาก/และเกิดความรับผิดชอบของรัฐบาล ดังนั้นเขาจึงเสนอทางออกว่าควรให้มีการจำกัดการใช้งานบนโลกออนไลน์เช่นเดียวกับประเทศจีนเพื่อเป็นระบบคัดกรองและควบคุมปัญหาอาชญากรรมดังกล่าว

หลายประเด็นในการงานวิจัยของ Ahmad Safwan Hamsi ตรงกับสถานการณ์ที่เกิดขึ้นในประเทศไทย ไม่ว่าจะเป็นการให้วีซ่านักเรียน/นักศึกษา การขาดแคลนทรัพยากรและผู้เชี่ยวชาญในการรับมือกับปัญหา รวมถึงเรื่องการไม่ตระหนักถึงการเปิดเผยข้อมูลส่วนตัวบนโลกออนไลน์ ซึ่งข้อเสนอในงานวิจัยนี้จะเป็นประโยชน์ในการเสนอทางออกที่เหมาะสมให้แก่ประเทศไทยได้เช่นกัน

จากเพียงแค่ความเหงา หรือพฤติกรรมสุ่มเสี่ยงที่ทำเป็นประจำผ่านสังคมออนไลน์ ถูกทำให้กลายเป็นเป้าหมายหรือจุดอ่อนสำคัญให้กับ Scammer ที่จงใจเข้ามาหลอกล่อเหยื่อ โดยในงานวิจัยหลายชิ้นข้างต้นก็แสดงให้เห็นอย่างชัดเจนแล้วว่า การล่อลวงจะมีรูปแบบหรือพฤติกรรมอย่างไร ซึ่งทางประเทศอื่นๆ ก็ได้หาแนวทางป้องกันต่ออาชญากรรมทางคอมพิวเตอร์รูปแบบนี้แล้ว หากพิจารณาหน่วยงานของไทยก็มีเพียง กรมสอบสวนคดีพิเศษ (DSI) และ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ที่เป็นผู้ออกมาให้หารช่วยเหลือเหยื่อข้างต้น ซึ่งในส่วนต่อไปจะพูดถึงงานวิจัยที่เกี่ยวกับกฎหมาย กระบวนการและการดำเนินคดี รวมถึง ช่องว่างที่กฎหมายไทยที่ยังเป็นปัญหาในการช่วยเหลือเหยื่อที่ถูกล่อลวงด้วย

<u>ส่วนที่สาม</u> เป็นการศึกษาเกี่ยวกับบทบัญญัติทางกฎหมายที่เกี่ยวข้อง และกระบวนการบังคับใช้กฎหมาย

จากการศึกษางานที่เกี่ยวข้องกับการกระทำความผิดทางคอมพิวเตอร์หรืออาชญากรรมทางไซเบอร์พบว่ามีงานที่เกี่ยวข้องหลายชิ้น โดยแบ่งออกเป็นงานในประเทศและงานนอกประเทศ โดยงานในประเทศมีงานที่พูดถึงอาชญากรรมทางไซเบอร์ ดังต่อไปนี้

งานของ**ธนวัฒน์ สินเกษม**[38] เรื่อง **ปัญหาการนำเข้าข้อมูลคอมพิวเตอร์ปลอมหรือที่เป็นเท็จตามมาตรา 14(1) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550** ได้อธิบายว่าพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มิได้มีการบัญญัติถึงคำนิยามของ “ข้อมูลคอมพิวเตอร์ปลอม หรือข้อมูลคอมพิวเตอร์ อันเป็นเท็จไว้” ทำให้เกิดปัญหาในเรื่องการคุ้มครองผู้เสียหายจากการนำเข้าข้อมูลคอมพิวเตอร์ตามปัญหาที่เกิดขึ้นในเครือข่ายสังคมออนไลน์ ว่าจะถือเป็นการกระทำผิดตามมาตรา 14 หรือไม่ อีกทั้งยังส่งผลให้เกิดความไม่ชัดเจนในเรื่องการนำบทลงโทษในมาตรา 14 ไปบังคับใช้ ประกอบกับสภาพบังคับที่มีอยู่ไม่มีการแบ่งแยกตามระดับความร้ายแรงของฐานความผิดทั้งที่ฐานความผิดในมาตรา 14 มีลักษณะแตกต่างกัน ดังนั้น บทบัญญัติทางกฎหมายในมาตรา 14 นี้ จึงไม่มีความชัดเจน และครอบคลุมเพียงพอ

ซึ่งในงานวิจัยของทาง **ilaw หรือ สาวตรี สุขศรี เป็นหัวหน้าโครงการ** ก็เป็นอีกงานหนึ่งที่อธิบายถึงการบังคับใช้ พ.ร.บ. คอมพิวเตอร์ 2550 ในมาตรา 14 (1) ในงานวิจัยเรื่อง **ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น**[39] ไว้ว่า เป้าหมายของมาตรา 14 (1) ผู้บัญญัติกฎหมายต้องการใช้เพื่อเป็นการอุดช่องว่างของกฎหมายอาญา “ซึ่งตามกฎหมายในสมัยเดิมบัญญัติให้คำว่า “เอกสาร” หมายเฉพาะแต่ “กระดาษหรือวัตถุอื่นใดที่มีรูปร่างและจับต้องได้” เท่านั้น จึงทำให้ไม่สามารถตีความกฎหมายเหล่านั้นให้ครอบคลุมถึงการปลอมแปลงข้อมูลอิเล็กทรอนิกส์ได้ ซึ่งก่อให้เกิดช่องว่างของกฎหมาย ดังนั้น ความหายของมาตรา 14(1) จึงไม่ได้หมายถึงการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลที่มีเนื้อหา (ไม่ว่าจะเป็นความจริงหรือความเท็จก็ตาม) ที่อาจทำให้บุคคลอื่นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง อันเป็นองค์ประกอบความผิดในฐาน “หมิ่นประมาท” ตามประมวลกฎหมายอาญา แต่ความหมายแท้จริงคือ การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ไม่แท้จริง (ข้อมูลคอมพิวเตอร์ปลอม) ที่ถูกทำขึ้นโดยผู้ไม่มีอำนาจตามกฎหมายที่จะทำข้อมูลนั้นขึ้นมาได้ หรือมิเช่นนั้นก็คือการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่ง ข้อมูลคอมพิวเตอร์ที่แท้จริง แต่ต่อมาถูกผู้กระทำความผิดแก้ไข เปลี่ยนแปลง ทำให้ข้อมูลนั้นผิดความหมาย หรือเปลี่ยนแปลงไปจากเดิม อย่างเช่น กรณีการ Phishing เป็นต้น

---

[38] ธนวัฒน์ สินเกษม, (2558), *ปัญหาการนำเข้าข้อมูลคอมพิวเตอร์ปลอมหรือที่เป็นเท็จตามมาตรา 14(1) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธุรกิจบัณฑิตย์.

[39] สาวตรี สุขศรี, (2555), *อาชญากรรมคอมพิวเตอร์? : งานวิจัยหัวข้อ ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น,* กรุงเทพฯ: โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw) ในมูลนิธิเพื่อสังคม, หน้า 83.

ปัญหาของมาตรา 14 ที่ถือเป็นหัวใจสำคัญของ พ.ร.บ. คอมพิวเตอร์ 2550 ไม่ได้มีปัญหาเพียงอนุมาตรา 1 เท่านั้น เพราะในมาตรา 14 มีการกำหนดความผิดไว้หลายความผิด ทั้งความผิดเกี่ยวกับการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงแห่งราชอาณาจักร รวมถึงการนำเข้าข้อมูลอันลามก อนาจารด้วย ในงานของ ของ **สุวิชาภา อ่อนพึ่ง**[40] ได้อธิบายไว้อย่างชัดเจนในงานศึกษาเรื่อง **ปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษาความผิดเกี่ยวกับการเผยแพร่ข้อมูลกระทบต่อความมั่นคงแห่งราชอาณาจักร** ว่า ในส่วนของความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร ในพระราชบัญญัติคอมพิวเตอร์ฯ 2550 จะบัญญัติอยู่ในมาตรา 14 ที่กำหนดให้มีความผิดดังต่อไปนี้ คือ 1. ข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์เท็จ 2. ข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยบางประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน 3. ข้อมูลคอมพิวเตอร์อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา 4. ข้อมูลคอมพิวเตอร์ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

นอกจากนี้บทบัญญัติตามมาตรา 14 ยังมีปัญหาในการบังคับใช้อยู่มาก ซึ่งปัญหานั้นเกิดจากการบัญญัติถ้อยคำในกฎหมายบางประการที่ก่อให้เกิดความไม่ชัดเจนในการตีความ จึงทำให้การบังคับใช้ไม่ตรงตามเจตนารมณ์ที่แท้จริงของกฎหมาย และในการบังคับใช้กฎหมาย บุคคลที่บังคับใช้กฎหมายเอง ก็ยังไม่มีความเข้าใจที่แท้จริงเกี่ยวกับบทบัญญัติด้วย และความผิดในมาตรา 14 นี้ ยังสามารถเชื่อมโยงไปถึงผู้ให้บริการตามมาตรา 15[41] ได้ด้วย เพราะผู้ให้บริการจะต้องรับผิดเสมือนว่าตนเป็นผู้กระทำตามมาตรา 14 ซึ่งเมื่อพิจารณาถึงความหมายของ “ผู้ให้บริการอินเตอร์เน็ต” แล้วนั้น ไม่ว่าจะเป็นขอบเขตตาม พระราชบัญญัติคอมพิวเตอร์ฯ 2550 หรือ ประกาศของกระทรวงเทคโนโลยีสารสนเทศ ก็ยังมีการกำหนดประเภทและหน้าที่ของผู้ให้บริการที่ยังไม่ชัดเจนและไม่สอดคล้องกับความรับผิดด้วย ซึ่งก็ส่งผลกระทบต่อผู้ให้บริการในเรื่องของภาระหน้าที่ที่มากเกินไปอย่างแน่นอน

ในมาตรา 15 เป็นฐานความผิดของผู้ให้บริการ ซึ่งมีการอ้างอิงบทลงโทษกับมาตรา 14 และก็ยังพบว่ามีข้อบกพร่องในเนื้อหาของบทบัญญัติและความไม่เป็นธรรมกับผู้ให้บริการ ในการกำหนดประเภทหน้าที่ของผู้ให้บริการอินเตอร์เน็ต ไม่ว่าจะเป็นขอบเขตตามพระราชบัญญัติคอมพิวเตอร์ฯ 2550 หรือประกาศของกระทรวงเทคโนโลยีสารสนเทศ ก็ยังมีการกำหนดประเภทหน้าที่ ที่ยังไม่ชัดเจนและไม่สอดคล้องกับความรับผิดด้วย ซึ่งเกี่ยวกับประเด็นนี้งานของ **พิชัย โชติชัยพร**[42] ศึกษาเรื่อง **ปัญหาความรับผิดของผู้ให้บริการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550** อธิบายว่า พระราชบัญญัติคอมพิวเตอร์ฯ มีผลกระทบต่อผู้ให้บริการ ทั้งด้านภาระหน้าที่และความรับผิดชอบทางอาญาซึ่งไม่เป็นธรรมต่อผู้ให้บริการ เนื่องจากในมาตรา 15 มีถ้อยคำที่ไม่ชัดเจนซึ่งอาจจะนำไปสู่การตีความกฎหมายที่ไม่เป็นธรรมแก่ผู้ให้บริการ เพราะผู้ให้บริการ

---

[40] สุวิชาภา อ่อนพึ่ง, (2554), *ปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษาความผิดเกี่ยวกับการเผยแพร่ข้อมูลกระทบต่อความมั่นคงแห่งราชอาณาจักร,* วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย.

[41] มาตรา 15 ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

[42] พิชัย โชติชัยพร, (2555), *ปัญหาความรับผิดของผู้ให้บริการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550,* วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต มหาวิทยาลัยสุโขทัยธรรมาธิราช.

นั้นก็มีทั้งรายเล็ก เช่น คนทั่วไป ร้านอินเตอร์เน็ตขนาดเล็ก ไปจนถึงขนาดใหญ่ เช่น บริษัท 3BB, TRUE, AIS, TOT หรือ CAT อีกทั้งคำนิยามของ “ผู้ให้บริการอินเตอร์เน็ต” ที่กำหนดไว้ในพระราชบัญญัติ ยังมีความหมายกว้างเกินไป และไม่มีความสอดคล้องกัน ถือเป็นการโยนภาระหน้าให้กับผู้ให้บริการเพียงฝ่ายเดียว เมื่อเกิดการฟ้องร้องบังคับคดีขึ้น ผู้ให้บริการเองก็ต้องมีภาระหน้าที่พิสูจน์ ซึ่งถือเป็นภาระหน้าที่ที่มากเกินไป

ในขณะที่ **สุรางคนา ด่านพิทักษ์**[43] ก็เป็นอีกคนหนึ่งที่เห็นปัญหาของผู้ให้บริการในพระราชบัญญัติคอมพิวเตอร์ฯ 2550 โดยสุราคณา ได้กล่าวไว้ในงานวิจัยเรื่อง **ความรับผิดทางอาญาของผู้ให้บริการ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550** พบว่า พระราชบัญญัติคอมพิวเตอร์ฯ2550 นี้ มีสภาพปัญหาเกี่ยวกับการบังคับใช้กฎหมายกับความรับผิดทางอาญาของผู้ให้บริการ กล่าวคือ บทบัญญัติของกฎหมายมิได้บัญญัติไว้โดยชัดเจนและครอบคลุม โดยมองว่าหากจะกำหนดแต่เพียงเฉพาะให้ผู้ให้บริการมีส่วนร่วมในการป้องกันการกระทำความผิดแต่เพียงอย่างเดียว ผู้ให้บริการเองอาจจะไม่ถือประพฤติปฏิบัติตาม จึงพบปัญหาว่าในความรับผิดทางอาญาของผู้ให้บริการ กรณีที่การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้กระทำลงโดยนิติบุคคล โดยสภาพแล้วนิติบุคคลจะสามารถรับโทษได้แต่เพียงอัตราโทษปรับเท่านั้น เพราะอัตราโทษจำคุกที่เป็นการบังคับเอาจากเนื้อตัวร่างกายของบุคคล ไม่สามารถบังคับใช้ได้กับสถานะของนิติบุคคล ซึ่งการลงโทษแต่เพียงอัตราโทษปรับแก่สภาพการประกอบธุรกิจของนิติบุคคลแต่อย่างเดียว โดยไม่บังคับเอาแก่เนื้อตัวร่างกาย ถือเป็นอัตราโทษที่เบา เมื่อมาตรการทางกฎหมายที่มีอยู่นั้น ไม่สามารถนำมาบังคับใช้ได้โดยครอบคลุมอย่างเพียงพอในการที่จะป้องกันและปราบปรามการกระทำความผิดแก่ผู้ที่มีส่วนเกี่ยวข้องกับนิติบุคคลอย่างทั่วถึง เป็นเหตุทำให้ผู้กระทำความผิดไม่เกิดความเข็ดหลาบ ความหลาบจำ นำมาซึ่งการไม่เกรงกลัวต่อบทบัญญัติของกฎหมาย เกิดการกระทำความผิดซ้ำ ดังจะเห็นว่า แม้ในส่วนของความรับผิดตามพระราชบัญญัติก็ยังคงมีปัญหาในเรื่องของไม่ความชัดเจนและไม่ครอบคลุม

พ.ร.บ. คอมพิวเตอร์ 2550 นอกจากจะกำหนดบทบัญญัติทางกฎหมายไม่ครอบคลุม ชัดเจนแล้ว ยังส่งผลกระทบไปถึงการบังคับใช้ของกฎหมายด้วย ซึ่งไม่เพียงแค่มาตรา 14 ที่เป็นหัวใจสำคัญของพระราชบัญญัติเท่านั้น ยังกระทบไปถึงมาตราอื่นๆ อีกด้วย ประกอบกับพฤติกรรมและลักษณะของการใช้สื่อออนไลน์ของคนในสังคมด้วยทำให้เกิดปัญหาตามมาอีกมากมาย และเนื่องจากมาตราใน พ.ร.บ. คอมพิวเตอร์ 2550 ที่ยังไม่ครอบคลุมชัดเจน งานของ **ปัทมาภรณ์ กฤษณายุทธ ศิริวัชรไพบูลย์**[44] เรื่อง **กฎหมายที่เกี่ยวข้องกับ Scammer ชาวผิวสีที่อ้างตัวเป็นชาวต่างชาติผิวสี** ยังศึกษาถึงกฎหมายอื่นเพิ่มเติมด้วย โดยมีการได้ยกบทบัญญัติทางกฎหมายมาดังต่อไปนี้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, ประมวลกฎหมายอาญา, พระราชบัญญัติคนเข้าเมือง และพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ซึ่งกฎหมายดังกล่าวข้างต้นนั้น เป็นการเลือกแสดงถึงตัวบทบัญญัติที่มีความเกี่ยวข้องกับพฤติกรรมการกระทำ

---

[43] สุรางคณา ด่านพิทักษ์, (2553), *ความรับผิดทางอาญาของผู้ให้บริการ ตามพระราชบัญญัติว่าด้วยการกระทำความรับผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550,* วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต มหาวิทยาลัยรามคำแหง.

[44] ปัทมาภรณ์ กฤษณายุทธ ศิริวัชรไพบูลย์, (2554), *กฎหมายที่เกี่ยวข้องกับ Scammer ชาวผิวสีที่อ้างตัวเป็นชาวต่างชาติผิวสี*, สืบค้นจาก https://www.dsi.go.th/Files/20150605/F20150605144231-%E0%B8%9A%E0%B8%97%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%20%E0%B8%81%E0%B8%A1.scammer%20%E0%B8%9B%E0%B8%A3%E0%B8%B1%E0%B8%9A%E0%B8%9B%E0%B8%A3%E0%B8%B8%E0%B8%87.pdf

ความผิด อย่างเช่น การหลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือ การนำเข้าสู่ระบบคอมพิวเตอร์ที่เป็นข้อมูลปลอมหรือเท็จไม่ว่าทั้งหมดหรือบางส่วน

"ตัวอย่างเช่น การยกบทบัญญัติทางกฎหมายในประมวลกฎหมายอาญา มาตรา 1 (14) "บัตรอิเล็กทรอนิกส์" หมายความว่า (ก) เอกสารหรือวัตถุอื่นใดไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า (ข) ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ แต่มีวิธีการใช้ในทำนองเดียวกับ (ก) หรือ (ค) สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ

(15) "หนังสือเดินทาง" หมายความว่า เอกสารสำคัญประจำตัวไม่ว่าจะมีรูปลักษณะใดที่รัฐบาลไทย รัฐบาลต่างประเทศ หรือองค์การระหว่างประเทศออกให้แก่บุคคลใด เพื่อใช้แสดงตนในการเดินทางระหว่างประเทศ และให้หมายความรวมถึงเอกสารใช้แทนหนังสือเดินทางและแบบหนังสือเดินทางที่ยังไม่ได้กรอกข้อความเกี่ยวกับผู้ถือหนังสือเดินทางด้วย"

ซึ่งก็ทำให้เห็นว่าไม่เพียงแต่ พ.ร.บ. คอมพิวเตอร์ 2550 เท่านั้นที่บังคับใช้กับพื้นที่ออนไลน์ แต่ยังมีกฎหมายอาญาและพระราชบัญญัติที่เกี่ยวข้องในเรื่องอื่นๆ ที่สามารถบังคับใช้ได้ด้วย โดย **ปัทมาภรณ์** ยังอธิบายเพิ่มเติมไปถึงความแตกต่างระหว่างองค์กรอาชญากรรมและอาชญากรรมข้ามชาติ เพราะเนื่องจาก ความผิดที่เกิดขึ้นบนพื้นที่ไซเบอร์ (Cyberspace) สามารถกระทำการที่ใดก็ได้ทั้งในประเทศและต่างประเทศ แต่กระบวนการยุติธรรมและเขตอำนาจศาลยังมีขอบเขตในการบังคับใช้ด้านดินแดนของรัฐ

นอกจากงานที่ศึกษาเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ยังมีงานวิจัยที่ศึกษาถึง พระราชบัญญัติว่าด้วยการรักษาความมั่นคงไซเบอร์ พ.ศ. 2562 ซึ่งในงานวิจัยดังกล่าวเป็นการศึกษาถึงวัตถุประสงค์ และมุมมองของกฎหมายทั้งกฎหมายไทยและต่างประเทศ ในงานของ **ภูมินทร์ บุตรอินทร์**[45] ในเรื่อง **มาตรการที่เหมาะสมในการรักษาความมั่นคงปลอดภัยไซเบอร์: ศึกษา (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงไซเบอร์ พ.ศ. ...** โดยอธิบายเปรียบเทียบกฎหมายไว้ว่า เป็นการศึกษาถึงมุมมองของกฎหมายว่าด้วยความมั่นคงทางไซเบอร์ทั้งของประเทศไทยที่ยังเป็นร่างกฎหมาย และกฎหมายของต่างประเทศไม่ว่าจะเป็นประเทศจีน อเมริกา รวมถึงกฎหมายว่าด้วยความมั่นคงทางไซเบอร์ของสหภาพยุโรปด้วย ในปัจจุบันการนำระบบเทคโนโลยีสารสนเทศมาใช้กับการดำรงชีวิตประจำวัน ตลอดจนกลายมาเป็นการผลักดันไปสู่นโยบายภาครัฐ ซึ่ง

[45] ภูมินทร์ บุตรอินทร์ (2560), มาตรการที่เหมาะสมในการรักษาความมั่นคงปลอดภัยไซเบอร์: ศึกษา (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงไซเบอร์ พ.ศ. ..., *วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์,* ปีที่ 46 ฉบับที่ 2 (ธันวาคม 2560). อ้างใน วัชระ เนติวาณิชย์, *คู่มือกฎหมายการสื่อสารและเทคโนโลยีสารสนเทศ,* กำแพงเพชร: ห้างหุ้นส่วนจำกัดศรีสวัสดิ์การพิมพ์, หน้า 199.

การใช้เทคโนโลยีสารสนเทศอาจจะนำมาสู่การคุมคามทางไซเบอร์ก็ได้ โดยในงานศึกษาชิ้นนี้จำแนกภัยคุกคามไซเบอร์ออกเป็น 3 ประเภท ดังนั้น

1. อาชญากรรมทางไซเบอร์ (Cyber Crime) เป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือใช้คอมพิวเตอร์เป็นอุปกรณ์ในการกระทำความผิด เช่น การใช้คอมพิวเตอร์เพื่อเข้าถึงระบบคอมพิวเตอร์ของบุคคลอื่นโดยมิชอบ หรือการเข้าถึงคอมพิวเตอร์ของบุคคลอื่นเพื่อทำให้เกิดความเสียหาย แก้ไขเปลี่ยนแปลงข้อมูลผู้อื่นโดยไม่ชอบ นอกจากนี้ยังรวมถึงการกระทำใดๆ ต่อระบบคอมพิวเตอร์ไม่ว่าจะเป็นการกระทำทางกายภาพ หรือเทคโนโลยีอื่นอีกด้วย ซึ่งอาชญากรรมทางไซเบอร์ สามารถถูกดำเนินการโดยบุคคลกลุ่มที่ไม่ประสงค์ดี อาจจะมีมูลเหตุจูงใจทางด้านการเงิน ด้านการก่อกวน หรือด้านอุดมการณ์ทางการเมือง ซึ่งความเสียหายจะอยู่ในระดับปัจเจกบุคคลและยังมิได้เป็นการโจมตีระบบโครงข่าย

2. สงครามไซเบอร์ (Cyber Warfare) เป็นการดำเนินการใดๆ ที่มีลักษณะของการก่อวินาศกรรมหรือการโจรกรรม โดยมีวัตถุประสงค์เพื่อได้มาซึ่งข้อมูลอันเป็นความลับ หรือกระทำเพื่อการก่อกวน หรือกระทำเพื่อให้บรรลุเป้าหมาย ซึ่งการโจมตีในระดับนี้ มักจะเป็นภัยคุกคามชั้นสูง (An advanced persistent threat : APT)[46] หรือเป็นการโจมตีโครงข่ายซึ่งอาจจะเป็นการจารกรรมข้อมูล หรือการทำลายโครงข่ายก็ได้ โดยมีรูปแบบตั้งแต่เบาที่สุดไปจนถึงขั้นร้ายแรงที่สุด เช่น การโจมตีเว็บไซต์ การปิดกั้นเว็บไซต์ (Block website) การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลผิด (Fake News) การเจาะข้อมูลลับโดยแฮคเกอร์ (Hacker) การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน การโจมตีโครงสร้างพื้นฐานที่มีความสำคัญอย่างยิ่ง

3. การก่อการร้ายไซเบอร์ (Cyber Terrorism) เป็นการดำเนินการอันมีวัตถุประสงค์เพื่อก่อการร้าย โดยมีระบบดิจิทัลเป็นเป้าหมายในการโจมตี หรือการใช้ระบบดิจิทัลเป็นเครื่องมือในการกระทำความผิดเกี่ยวกับการก่อการร้าย การกระทำความผิดในข้อนี้จะส่งผลกระทบร้ายแรงต่อประชาชนเป็นวงกว้าง ไม่ได้จำกัดอยู่แค่เพียงบุคคลใด บุคคลหนึ่ง หรืออาจจะเป็นการก่อกวนระบบไฟฟ้าของประเทศนั้น การโจมตีระบบเครือข่ายของหน่วยงานรัฐที่สำคัญของประเทศหนึ่ง ซึ่งความเสียหายที่เกิดขึ้นนั้นไม่ได้กระเพียงหน่วยงานรัฐเท่านั้น ประชาชนในประเทศก็ยังได้รับผลกระทบไปด้วย

แต่คำนิยามทั้ง 3 คำดังกล่าวข้างต้นก็ยังไม่ใช้นิยามที่เป็นสากลและได้รับการยอมรับร่วมกันในระดับชาติ ซึ่งก็ยังมีความสับสนระหว่างการก่อการร้ายไซเบอร์กับสงครามไซเบอร์ เพราะองค์กระกอบของการกระทำความผิดและลักษณะของการกระทำมีความคล้ายคลึงกันในหลายประเด็น และยังมีข้อถกเถียงทางวิชาการในหลายๆ ด้าน

ในกฎหมายว่าด้วยการรักษาความมั่นคงทางไซเบอร์ในต่างประเทศ งานศึกษาชิ้นนี้ได้ศึกษากฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์แห่งสหภาพยุโรป (EU) กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ประเทศสาธารณรัฐประชาชนจีน และกฎหมายความมั่นคงปลอดภัยไซเบอร์ของประเทศ

[46] ภูมินทร์ บุตรอินทร์ (2560), มาตรการที่เหมาะสมในการรักษาความมั่นคงปลอดภัยไซเบอร์: ศึกษา (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงไซเบอร์ พ.ศ. ..., *วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์,* ปีที่ 46 ฉบับที่ 2 (ธันวาคม 2560). อ้างใน Margaret Rouse, (2018) *Advanced persistent threat (APT)*, สืบค้นจาก https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.

สหรัฐอเมริกา ซึ่งการคัดเลือกกลุ่มประเทศข้างต้นในการศึกษา เนื่องจากแต่ละแห่งมีพัฒนาการเรื่องความมั่นคงปลอดภัยไซเบอร์แล้ว

กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์แห่งสหภาพยุโรป (EU) มีวัตถุประสงค์เพื่อตอบสนองนโยบายของรัฐบาลในการสร้างความเชื่อมั่นสำหรับการสื่อสารบนเครือข่ายอินเตอร์เน็ตให้มีความปลอดภัยมากที่สุด โดยจะกำหนดมาตรฐานความปลอดภัยขั้นต่ำที่นำมาใช้กับระบบการติดต่อสื่อสารบนเครือข่ายอินเตอร์เน็ตและข้อมูลสารสนเทศทั้งหมดและมีการผลักดันนโยบาย การป้องกันภัยคุกคามทางไซเบอร์ผ่านยุทธศาสตร์ เช่น การสร้างความร่วมมือระหว่างประเทศสมาชิก การสร้างความพร้อมในการรับมือกับภัยคุกคามไซเบอร์สำหรับประเทศสมาชิก และการสร้างวัฒนธรรมในเชิงป้องกันและการใช้งานที่ปลอดภัยจากภัยคุมคามไซเบอร์[47] โดยมีหน่วยงานกลางที่ดำเนินการเชื่อมโยงและประสานการทำงานของประเทศสมาชิกของสหภาพยุโรปสำหรับการรับมือต่อภัยคุกคามไซเบอร์ที่เกิดขึ้นในสหภาพยุโรป เช่น หน่วยงานทางด้านความมั่นคงปลอดภัยทางโครงข่ายและสารสนเทศแห่งสหภาพยุโรป หน่วยงานตอบสนองเหตุการณ์ด้านความปลอดภัยคอมพิวเตอร์ เป็นต้น

กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของประเทศจีน มีการจำแนกมาตรการรักษาความมั่นคงไซเบอร์ได้เป็น 2 ส่วน กล่าวคือ 1. มาตรการที่ปรากฏในบทบัญญัติทั่วไปอันเป็นการกำหนดกฎเกณฑ์กว้างๆของการรักษาความมั่นคงไซเบอร์ โดยบังคับใช้กับผู้ประกอบการในหลายส่วน อาทิ ผู้ให้บริการโครงข่ายและผู้ใช้บริการ เป็นต้น ซึ่งมาตรการเหล่านี้จะปรากฏอยู่ในหมวด 2 ของกฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ 2. มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่มุ่งเน้นรักษาความมั่งคงปลอดภัยในโครงสร้างพื้นฐานด้านข้อมูลข่าวสารที่มีความสำคัญ (Critical infrastructure network operators) ซึ่งมาตรการนี้จะเน้นการคุ้มครองและปกป้องโครงสร้างพื้นฐานทางด้านสารสนเทศที่สำคัญของประเทศ และผู้ให้บริการโครงข่าย (Network operators)

กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของสหรัฐอเมริกา ในประเทศสหรัฐอเมริกาใช้ระบบการปกครองแบบสหพันธ์สาธารณรัฐ จึงมีกฎหมายทั้งในระดับมลรัฐและระดับสหพันธรัฐ โดยนำเสนอกฎหมายในระดับสหพันธรัฐอันเป็นกฎหมายที่มีผลผูกพันและครอบคลุมประเทศสหรัฐอเมริกาทั้งหมด ซึ่งกฎหมายหลักในเรื่องความมั่นคงปลอดภัยไซเบอร์คือ “รัฐบัญญัติว่าด้วยความมั่นคงปลอดภัยไซเบอร์ ค.ศ. 2015” (The Cybersecurity Act of 2015) ที่ออกมาบังคับใช้ในยุคสมัยของประธานาธิบดี บารัค โอบามา (Barack Obama) ซึ่งเป็นการตรากฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ฉบับล่าสุด และมีผลเป็นการเปลี่ยนแปลงวิธีการในวิธีการจัดการปัญหาความมั่นคงทางไซเบอร์ของประเทศอย่างมีนัยสำคัญ กล่าวคือ กฎหมายดังกล่าวมุ่งป้องกันโลกไซเบอร์ของประเทศให้มีความมั่นคงปลอดภัยด้วยความร่วมมือจากทุกภาคส่วนอย่างแท้จริง หรือกล่าวอีกนัยหนึ่งได้ว่าลำพังเพียงหน่วยงานของรัฐไม่เพียงพอที่สอดส่องดูแลโลกไซเบอร์ให้มีความปลอดภัยได้ จึงจำเป็นที่จะต้องมอบหมายหน้าที่บางประการให้กับภาคเอกชนในการทำหน้าที่สอดส่องดูแลการกระทำความผิดและการคุกคามบนโลกไซเบอร์ ดังนั้น กฎหมายฉบับนี้จึงเป็นผลผลิตจากการประนีประนอมหลายครั้งระหว่างหน่วยงานภาครัฐและหน่วยงานภาคเอกชน ที่อยู่ในขอบข่ายการบริหารความเสี่ยงในเรื่องความมั่นคงปลดภัยไซเบอร์

[47] European Commission, (2019), *The Directive on security of network and information systems (NIS Directive),* สืบค้นจาก https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

และยุทธวิธีในการสร้างความมั่นคงด้านไซเบอร์ตามที่ปรากฏในกฎหมายฉบับนี้ จึงมีผลในการเปลี่ยนแปลงวิถีการดำเนินธุรกิจในโลกไซเบอร์ของภาคเอกชนอย่างมีนัยสำคัญ

ส่วนในประเทศไทยมีกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ ซึ่งในขณะนี้ก็เป็นร่างกฎหมาย แต่มีหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย ประกอบด้วย 1.กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยมีอำนาจอำนาจหน้าที่เกี่ยวกับการวางแผน ส่งเสริม พัฒนา และดำเนินการเกี่ยวกับดิจิทัลเพื่อเศรษฐกิจและสังคม และกำกับดูแลกฎหมายด้านดิจิทัล 2. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) มีบทบาทในการประสานงานระหว่างหน่วยงานต่างประเทศที่เป็นสมาชิกขององค์กรเหล่านี้กับหน่วยงานในประเทศ ทั้งภาครัฐ เอกชน มหาวิทยาลัย ผู้ให้บริการอินเตอร์เน็ต เป็นต้น 3.ศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) มีหน้าที่ในการปฏิบัติการไซเบอร์ เพื่อเฝ้าระวัง แจ้งเตือน ป้องกันและแก้ไขปัญหาที่เกิดจากภัยคุกคามด้านไซเบอร์ และ 4. กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) มีอำนาจหน้าที่ในการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีอันเป็นอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อยป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวน ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญาและตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์[48]

จะเห็นว่ามีกฎหมายที่เกี่ยวข้องกับการกระทำทางเทคโนโลยีมากมาย แต่จากงานวิจัยและบทความข้างต้นเป็นส่วนของการศึกษากฎหมายที่เกี่ยวข้อง มีผู้ศึกษากฎหมายในเรื่องของการหลอกลวงหรือล่อลวง ในประเด็นที่ผู้ทำวิจัยได้ให้ความสนใจไว้เป็นอย่างมาก แต่ถึงอย่างไรนั้น กฎหมายที่มีการศึกษาไว้ดังกล่าวข้างต้น ก็ยังไม่เพียงพอต่อการศึกษา ผู้วิจัยจึงขยายขอบเขตการศึกษาออกไปโดยในส่วนต่อไปเป็นการศึกษางานวิจัยที่เกี่ยวกับพฤติกรรมของผู้ใช้งานสื่อออนไลน์ และรูปแบบวิธีการล่อลวงของอาชญากรในเครือข่ายสังคมออนไลน์ว่าเป็นอย่างไร เพื่อให้เห็นถึงสภาพปัญหาและสถานการณ์ที่เกิดขึ้นในปัจจุบันให้มากขึ้น อันจะเป็นประโยชน์ในการสร้างความตระหนักรู้และออกแบบระบบป้องกันและปราบปรามพิศวาสอาชญากรรมต่อไป

สำหรับงานในต่างประเทศ มีงานที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ ดังต่อไปนี้

Nir Kshetri[49] ผู้นำเสนอในงานเรื่อง “เศรษฐศาสตร์ง่ายๆของอาชญากรรมไซเบอร์และวงจรอุบาทว์” ว่าการร้องทุกข์ต่อความเสียหายที่เกิดจากอาชญากรรมนั้นอาจไม่เกิดขึ้นได้ง่ายเพราะมีต้นทุนทั้งต่อตัวเหยื่อเองที่ต้องอับอายขายหน้ามีภาพลักษณ์ไม่ดี นอกจากนี้ยังมีต้นทุนค่าเสียโอกาสความหน่วงเสียเวลาอีกมากมายหากต้องนำคดีเข้าสู่กระบวนการยุติธรรม รวมถึงความไม่คุ้มทุนของการบังคับใช้กฎหมายกับคดีที่ปัจจุบันรัฐยังไม่เห็นปริมาณหรือมูลค่าที่มากพอจะจัดสรรทรัพยากรมาแก้ไข

ข้อจำกัดในการนำคดีอาชญากรรมไซเบอร์เข้าสู่กระบวนการเยียวยาทางกฎหมายยังมีอีกมากมายดังที่ **EFG Ajayhi** [50] ได้จำแนกไว้ในงาน “ความท้าทายในการบังคับใช้กฎหมายและนโยบาย

---

[48] ภูมินทร์ บุตรอินทร์, (2560), หน้า 199.

[49] Kshetri, N., (2010), “Simple Economics of Cybercrime and the Vicious Circle”. *The Global Cybercrime Industry*, Berlin; Springer-Verlag.

[50] Ajayhi, E., (2015), “The Challenges to Enforcement of Cybercrimes Laws and Policy”. *International Journal of Information Security and Cybercrime*, 4(2), 33-48. สืบค้นจาก https://www.ijisc.com

เกี่ยวกับอาชญากรรมไซเบอร์" ว่ามีความเหนื่อยยากทั้งในมุมของเจ้าพนักงานที่ต้องแสวงหารวมรวมพยานที่อยู่ในรูปดิจิทัลที่ต้องใช้ผู้เชี่ยวชาญ และห้องตรวจพิสูจน์ที่ต้องได้รับการลงทุนหรือส่งไปตรวจในต่างประเทศ อีกทั้งยังตรวจพิสูจน์อัตลักษณ์ดิจิทัลของอาชญากรที่อำพรางตัวตนได้ยาก การขาดแคลนข้อกฎหมายและกระบวนการยุติธรรมที่เอื้อต่อการดำเนินคดีไซเบอร์ เหนือสิ่งอื่นใดคือข้อจำกัดด้านเขตอำนาจศาลเมื่ออาชญากรอยู่นอกดินแดนอันก่อให้เกิดต้นทุนและความยุ่งยากในการประสานความร่วมมือด้านกระบวนการยุติธรรม หรือการขอส่งผู้ร้ายข้ามแดน หรือยึดทรัพย์สินเพื่อเยียวยา

โดยปัญหาเรื่องเขตอำนาจศาลที่ขัดกันและไร้ซึ่งการประสานความร่วมมือระหว่างประเทศที่ดีพอนี้ได้ถูกขยายความโดย **Alexandra Perloff-Giles**[51] เน้นให้เห็นถึงลักษณะข้ามพรมแดนของอาชญากรรมไซเบอร์ที่เกิดขึ้นตลอดเวลาและไม่สอดคล้องกับลักษณะของกระบวนการยุติธรรมในรัฐสมัยใหม่ที่มีขอบเขตดินแดนของรัฐเป็นข้อจำกัด และเมื่อใช้เพียงกฎหมายหรือกระบวนการของรัฐใดรัฐหนึ่งย่อมไม่อาจดำเนินคดีกับอาชญากรและเยียวยาเหยื่อได้อย่างมีประสิทธิผล จนกว่ารัฐและประชาคมโลกจะมีฉันทามติหรือความร่วมมือในการริเริ่มข้อตกลงระหว่างประเทศที่ทำให้เกิดมาตรฐานในการกำหนดฐานความผิดร่วมกันและมีระบบประสานความร่วมมือระหว่างประเทศขึ้น

นอกจากนี้ยังมีงานของ **David M. Engel**[52] ใน **The pyramid of Tort Law** เป็นงานที่อธิบายถึง คดีละเมิดที่มีจำนวนเยอะมากที่ฐานของปีระมิด และน้อยลงเรื่อยๆ ในขั้นต่อไปเป็นลำดับจนถึงยอดปีระมิดอันเป็นการดำเนินคดีในชั้นศาลอุทธรณ์หรือเป็นคดีที่มีการพิพากษาจริงๆ ซึ่งขั้นตอนของการใช้กฎหมายเป็นเครื่องมือทั้ง 7 ขั้นตอนนี้เริ่มต้นด้วยการเกิดความเสียหาย (injuries) ขั้นที่สองเป็นการตระหนักได้ว่าความเสียหายนั้นเกิดขึ้นโดยการกระทำของผู้อื่น (perception of wrongdoing) ซึ่งคนส่วนใหญ่ติดอยู่ที่ขั้น 2 ของปีระมิด ด้วยเหตุผลที่ว่ากลัวความเสี่ยงและอำนาจของเจ้าหน้าที่ในระบบยุติธรรม เช่น กลัวตำรวจเข้าข้างอีกฝ่ายหนึ่งและกลัวว่าตนจะกลายเป็นฝ่ายที่ทำผิดกฎหมายเสียเอง บางคนมองว่ากฎหมายทำอะไรไม่ได้และหันเข้าทางคำสอนของพระพุทธเจ้าภาวนาให้กรรมตามสนอง ขั้นที่สามคือการเรียกร้อง (claims) และพบว่าการเรียกร้องค่าเสียหายส่วนใหญ่อาจยุติลงด้วยการยอมความกันนอกศาล ขั้นที่สี่เป็นการปรึกษาทนายความ (consulting an attorney) ขั้นที่ห้าเป็นการที่ทนายยื่นคำร้องฟ้องคดี (lawsuits) ขั้นที่หกเป็นการพิจารณาคดีในศาล (trials) และขั้นสุดท้ายคือการอุทธรณ์ศาลฎีกาซึ่งเป็นยอดสูงสุดทีมีจำนวนคดีขึ้นไปถึงน้อยที่สุด ภาพปีระมิดนี้สะท้อนให้เห็นสภาพปัญหาและข้อจำกัดของการใช้กฎหมายเป็นเครื่องมือในการแก้ข้อพิพาทของบุคคล ตามทฤษฎีจะเห็นได้ว่าคดีที่เกิดขึ้นไปถึงชั้นศาลมีจำนวนที่ต่างกันอย่างเห็นได้ชัด เนื่องจากคนส่วนใหญ่มักใช้การเจรจาต่อรองนอกกฎหมายเป็นการแก้ไขสิ่งที่เกิดขึ้น

หลายการศึกษาพบว่า คดีละเมิดที่ได้รับการพิจารณาคดีในชั้นศาลมีเพียง 10-15% เท่านั้น ส่วนที่เหลือคู่ความอาจตกลงยอมความ ถอนฟ้อง หรือทิ้งฟ้อง และอีกหลายงานวิจัยยังชี้ให้เห็นว่าโจทก์จะชนะคดี 50% ของคดีความทั้งหมด ดังนั้นจะเห็นได้ว่าถ้าหากเกิดคดีละเมิด 100 คดี คดีนั้นจะไปถึงศาลเพียง 10 – 15 คดีเท่านั้น ทั้งนี้อาจเกิดจากข้อจำกัดหลายประการ เช่น

---

[51] Perloff-Gile, A., (2017), *A"PROBLEM WITHOUT A PASSPORT": OVERCOMING JURISDICTIONAL CHALLENGES FOR TRANSNATIONAL CYBER AGGRESSIONS*. สืบค้นจาก https://law.yale.edu/system/files/area/center/global/document/perloff-giles_cyber_conflict_paper_-_final_draft.pdf

[52] Engel, D. M., (2557), "บทบาทของกฎหมายที่มีต่อชีวิตของสามัญชน," *นิติสังคมศาสตร์* ปีที่ 2 ฉบับ 1, หน้า 141- 163.

- *ขั้นตอนของระบบกฎหมายที่เป็นทางการ* สิ่งนี้หมายถึงการไม่รู้กฎหมาย การเข้าไม่ถึงกฎหมาย รวมถึงการไม่คุ้นเคยต่อระบบกฎหมายที่แยกออกชีวิตประจำวันของผู้คน ทำให้เกิดความไม่เชื่อมั่นและไม่ไว้วางใจระบบกฎหมาย
- *ต้นทุนของการดำเนินการ* ทั้งนี้หมายรวมถึงทั้งค่าใช้จ่ายและระยะเวลา การดำเนินการทางกฎหมายต้องอาศัยผู้เชี่ยวชาญในการดำเนินการ จึงต้องอาศัยทางเงินและระยะเวลาที่ยาวนาน บางครั้งผู้เสียหายอาจคำนวณแล้วว่าไม่คุมค่าต่อต้นทุนของการดำเนินการทางกฎหมาย หรือบางครั้งอาจได้รับการขอเจรจาประนีประนอมกันเสียก่อนที่จะถึงขั้นตอนของศาล
- *ความเป็นไปได้ในการชนะคดี* สิ่งนี้เป็นปัจจัยสำคัญในการตัดสินใจว่าจะต่อสู้ด้วยกระบวนการทางกฎหมายหรือไม่ ซึ่งผู้เสียหายต้องพิจารณาถึงความน่าเชื่อถือพยานหลักฐาน ความสามารถของทนายความ ความซับซ้อนของคดี และแนวโน้มการวินิจฉัยของศาล ซึ่งมีผลต่อการตัดสินใจให้ดำเนินคดีหรือให้ยุติการดำเนินคดี

นอกจากข้อจำกัดบางประการแล้วควรต้องมีการทำความเข้าใจตัวบทกฎหมายกับการบังคับใช้ในความเป็นจริง สิ่งนี้จะชี้ให้เห็นอุปสรรคหรือปัญหาที่เกิดขึ้นในขั้นตอนต่างๆ ของการบังคับใช้กฎหมายและผลต่อประสิทธิภาพของการบังคับใช้กฎหมาย ซึ่งหากอุปสรรคปัญหาเป็นผลมาจากระบบภายในระบบกฎหมายก็อาจต้องมีการปรับปรุงและแก้ไขให้ตรงจุด ไม่ว่าจะเป็นตัวบทกฎหมาย หรือกระบวนการดำเนินคดีก็ตาม แต่หากเป็นผลมาจากแง่มุมทางวัฒนธรรมก็อาจต้องยอมรับข้อจำกัดบางประการและพัฒนาเครื่องมือหรือนโยบายอื่นๆ มารองรับ

2.2 กรอบแนวคิดในการวิจัย (conceptual framework)

งานวิจัยเรื่องนี้จะใช้กรอบในการศึกษา 3 กรอบด้วยกัน คือ แนวคิดเกี่ยวกับความเป็นส่วนตัวและการข้อมูลส่วนบุคคลเพื่อแสดงให้เห็นจุดอ่อนความเปราะบางของผู้ที่สุ่มเสี่ยงจะตกเป็นเหยื่อเนื่องจากเปิดเผยข้อมูลส่วนบุคคลและเรื่องส่วนตัวของตนออกสู่สาธารณะ อันนำมาสู่การฉวยโอกาสของอาชญากรในการเรียนรู้เหยื่อเป้าหมายแล้วนำมาปรับเป็นกลยุทธ์ในการล่อลวงซึ่งจะใช้แนวคิดเกี่ยวกับการแสดงละครทางสังคมโดยสวมหน้ากากของผู้ล่อลวงให้ตรงกับความต้องการหรือจุดอ่อนของเหยื่อ โดยแนวคิดสุดท้ายจะนำมาวิเคราะห์มาตรการทางกฎหมายที่ใช้เยียวยาปัญหาการล่อลวงทางอินเตอร์เน็ตว่ามีความพร้อมในการป้องกันและปราบปรามพิศวาสอาชญากรรมแล้วหรือไม่ทำไมเหยื่อจึงไม่เลือกที่ใช้มาตรการทางกฎหมายโดยอาศัยแนวคิดปีระมิดแห่งการละเมิดมาช่วยวิเคราะห์

2.2.1 กรอบความคิดเกี่ยวกับการตกเป็นเหยื่อ

กรอบแนวคิดแรกที่จะนำมาใช้ คือ กรอบความคิดของบุคคลที่เสี่ยงจะตกเป็นเหยื่อ (Victimology) เนื่องจากได้เปิดเผยข้อมูลอ่อนไหวในพื้นที่สาธารณะ ทำให้อาชญากรรมสามารถรวบรวมข้อมูลของบุคคลเหล่านั้นเป็นข่าวกรองในการคิดค้นกลยุทธ์ในการล่อลวงเหยื่อได้ โดยผู้ใช้อินเตอร์เน็ตจำนวนมากมีกิจวัตรประจำวัน (Routine Activities Theory) ที่เปิดเผยวิถีชีวิตออนไลน์

ให้กับบุคคลภายนอกล่วงรู้ (Life Style Exposure Theory) แบบขาดความระมัดระวัง[53] โดยไม่มีกระบวนการรักษาความปลอดภัยดิจิทัล (Digital Guardian) ของตนเองที่เหมาะสม[54] รวมถึงไม่มีระบบเฝ้าระวังเตือนภัยให้กับผู้ใช้อินเตอร์เน็ตที่ดีพอเนื่องจากขาดผู้พิทักษ์ที่มีประสิทธิภาพ (Absence of a Capable Guardian) ทำให้ผู้ใช้อินเตอร์เน็ตที่เปิดเผยข้อมูลอ่อนไหวกลายเป็นเป้าหมายที่เหมาะสมต่อการล่อลวง (Suitable Target) [55]

มีงานศึกษาที่สะท้อนว่าข้อมูลส่วนบุคคลที่ผู้ใช้อินเตอร์เน็ตเปิดเผยแล้วจะสร้างความเสี่ยงให้ตนตกเป็นเหยื่อ และผู้ดูแลระบบ/ผู้บังคับใช้กฎหมาย ก็ควรเตือนประชาชนหรือผู้ใช้ระบบ ให้ระวังการเผยแพร่ข้อมูลเหล่านี้บนโลกไซเบอร์ ข้อมูลส่วนบุคคลอ่อนไหวประกอบไปด้วย 9 ลักษณะ ได้แก่[56]

1) การใช้ชื่อจริงชื่อเต็ม
2) สถานะความสัมพันธ์ทางครอบครัว การผูกพันทางจิตใจหรือสังคม
3) รสนิยมทางเพศ
4) เลขรหัสในโปรแกรมสนทนา (ID)
5) ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address)
6) ที่อยู่ออนไลน์ของบริการอื่นๆ ในเครือข่ายสังคมออนไลน์ หรือบล็อก
7) ความสนใจ โปรดปราน หรือกิจกรรมที่ชื่นชอบ
8) รูปภาพของตัวเอง (ทั้งที่ถ่ายตนคนเดียวหรือร่วมกับผู้อื่น)
9) วิดีโอของตัวเอง (ทั้งที่บันทึกตนคนเดียวหรือร่วมกับผู้อื่น)

ดังนั้น เพื่อเป็นการป้องกันการละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคล จึงต้องพัฒนาระบบเฝ้าระวังการคุกคามและสร้างมาตรการเตือนภัยล่วงหน้าเพื่อให้ข้อมูล โดยเฉพาะการใช้อินเตอร์เน็ตที่มีการใช้จูโจมล่อลวงได้ง่าย หรือระบุให้มีการมาตรการคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัวของผู้ใช้อินเตอร์เน็ต เช่น ข้อมูลส่วนบุคคลและความเป็นส่วนตัวในเว็บไซต์หาคู่ และเครือข่ายสังคมออนไลน์ ก็เป็นการลดโอกาสเกิดพิศวาสอาชญากรรมไปในตัว

ความเป็นส่วนตัว (Privacy) และข้อมูลส่วนบุคคล (Personal Data) ได้รับการคุ้มครองโดยกฎหมายสิทธิมนุษยชนที่รัฐไทยเป็นภาคีจึงมีผลผูกพันรัฐไทยให้มีพันธกรณีในการเคารพ ปกป้อง และ

---

[53] สาวตรี สุขศรี, (2560), “อาชญากรรมคอมพิวเตอร์/ไซเบอร์กับทฤษฎีอาชญาวิทยา.” *วารสารนิติศาสตร์*, ปีที 46 ฉบับที่ 2 (มิถุนายน 2560), หน้า 426.

[54] Marcum, C. D., (2011), “Adolescent Online Victimization and Constructs of Routine Activities Theory.” In K. Jaishankar (Eds). *Cyber Criminology Exploring Internet Crimes and Criminal Behavior*. Florida: CRC Press Taylor & Francis Group, P. 270.

[55] Cohen, L., Felson, M., (1979), “Social Change and Crime Rate Trends: A Routine Activity Approach.” *American Sociological Review*. Vol.44 No.4, pp. 588-608.

[56] Reyns, B. W., Henson, B., Fisher, B. S., (2013), “Applying Cyberlifestyle-routine activities theory to cyberstalking victimization.” In Thomas J. Holt (Eds), *Cybercrime and Criminological Theory Fundamental Reading on Hacking, Piracy, Theft and Harassment*. San Diego: Cognella Inc., pp. 105-119.

เติมเต็มให้กับบุคคลผู้เป็นเจ้าของสิทธิ รวมทั้งยังปรากฏอยู่ในรัฐธรรมนูญไทย พ.ศ. 2560 มาตรา 32 ดังนั้นผู้ควบคุมระบบหรือเจ้าของข้อมูลจำเป็นต้องมีมาตรการป้องกันความปลอดภัยของข้อมูลส่วนบุคคลหรือความเป็นส่วนตัว ครอบคลุมกิจกรรมดังต่อไปนี้[57]

1) การเข้าไปดูข้อความในเว็บไซต์ เครือข่ายสังคมออนไลน์ จดหมายอิเล็กทรอนิกส์และการบันทึกข้อมูลในเครื่อง คอมพิวเตอร์ รวมทั้งการบันทึก เก็บ แลกเปลี่ยนข้อมูลที่บุคคลเข้าไปใช้บริการเว็บไซต์และกลุ่มข่าวสาร โดยมิได้รับความยินยอม

2) การใช้เทคโนโลยีในการติดตามความเคลื่อนไหวหรือพฤติกรรมของบุคคล ซึ่งทำให้สูญเสียความเป็นส่วนตัว รวมถึงการสอดส่องโดยบุคคลต่อกิจกรรมส่วนตัวของเป้าหมายโดยไม่ได้รับอนุญาต

3) การใช้ข้อมูลของผู้ใช้จากแหล่งข้อมูลดิจิทัลต่างๆ เพื่อผลประโยชน์ที่มิชอบด้วยกฎหมาย

หากมีความเปราะบางรั่วไหลจะทำให้เกิดความเสี่ยงที่อาชญากรจะรวบรวมรสนิยม กิจกรรม หมายเลขโทรศัพท์ ที่อยู่อีเมล์ หมายเลขบัตรเครดิต และข้อมูลส่วนตัวอื่นๆ ของเหยื่อ เพื่อนำไปสร้างฐานข้อมูลประวัติกลุ่มเป้าหมายขึ้นมา แล้วนำไปใช้ประโยชน์อื่นที่ไม่ตรงกับวัตถุประสงค์ที่เจ้าของข้อมูลเผยแพร่หรือให้ความยินยอมไว้

2.2.2 กรอบความคิดเกี่ยวกับอาชญากรและกลยุทธ์ในก่ออาชญากรรม

กรอบแนวคิดที่สองซึ่งจะนำมาเป็นกรอบการวิจัยเพื่อเก็บข้อมูลกลยุทธ์ (Tactic) การล่อลวงทั้งหลายของอาชญากร (Criminal) ก็คือ ทฤษฎี “หน้ากาก” จากหนังสือของนักมานุษยวิทยาและสังคมวิทยาแนวกลยุทธ์ในชีวิตประจำวันชื่อดัง คือ “เบื้องหลังหน้ากาก”[58] ของ เจอรัลด์ ดี. แบรีแมน โดยให้แนวคิดว่าโลกคือละคร มนุษย์ทุกคนล้วนนำเสนอหน้ากากที่ต่างไปในสถานการณ์ที่เปลี่ยนไปเพื่อต่อสู้แข่งขันแย่งชิงให้ได้ประโยชน์สูงสุดกับตน เมื่อนำมาใช้ศึกษากรณีพิศวาสอาชญากรรมก็จะเห็นกลยุทธ์การอำพรางหรือดัดแปลงอัตลักษณ์บุคคลด้วยการแสดงผ่านช่องทางอินเตอร์เน็ตด้วยภาษาและสัญลักษณ์จำนวนมาก เพื่อสร้าง “ตัวตน” ใหม่ให้เกิดภาพลักษณ์และเรื่องราวต่างๆ ตรงกับความปรารถนาของเป้าหมายในการล่อลวง

โดยทฤษฎีในกลุ่มนี้มีรากฐานมาจากงานวิชาการของการศึกษาแบบเทียบกับละคร (Dramaturgical Approach) ของ Erving Goffman ได้อธิบายการควบคุมการสร้างภาพลักษณ์ของบุคคลในการเข้าสังคม โดยเทียบกับการแสดงละครเวที คือ หลังฉาก (back region) ใช้เพื่อเตรียมการแสดง หรือการสร้างภาพลักษณ์ เพื่อให้หน้าฉาก (front region) แสดงออกมาได้อย่างแนบเนียนและเป็นพอใจของผู้ชม โดยทุกการแสดงออกจะขึ้นอยู่กับปฏิกิริยาของผู้ชมจนไม่สามารถคาดเดาได้ว่าการกระทำจะเป็นแบบไหนที่ตายตัว

---

[57] UN Global Pulse. (1990). *PRIVACY AND DATA PROTECTION PRINCIPLES*. สืบค้นจาก https://www.unglobalpulse.org /privacy-and-data-protection.

[58] เจอรัลด์ ดี แบรีแมน, (2549), เบื้องหลังหน้ากาก, แปลโดย อู่ทอง ประศาสน์วินิจฉัย, กรุงเทพฯ: ศูนย์มานุษยวิทยาสิรินธร (องค์การมหาชน), หน้า 114-121.

ทฤษฎีการวิเคราะห์เชิงละคร (Dramaturgical Theory) ของ Erving Goffman เป็นการเทียบเคียงระหว่างเวทีกับปฏิสัมพันธ์ทางสังคม โดย Goffman เสนอว่า ในทุกๆ ปฏิสัมพันธ์ทางสังคม มนุษย์แต่ละคนกำลังแสดงอยู่บนเวที ที่หน้าเวทีมีผู้ชม (คนอื่นที่มนุษย์มีปฏิสัมพันธ์ด้วย) บนเวทีจะประกอบด้วย หน้าฉาก (front stage) คือการนำเสนอตัวตนของมนุษย์ตามที่อยากให้ผู้อื่นรับรู้ (presented self) เช่น การแต่งกาย ท่าทาง การพูด เป็นต้น และหลังฉาก (back stage) คือความรู้สึกนึกคิดที่ไม่ต้องการเปิดเผยหรือนำเสนอให้ผู้อื่นรับรู้ ที่เรียกว่า “ตัวตนที่ซ่อนเอาไว้” (hidden self) มนุษย์ต่างก็เล่นละครฉากแล้วฉากเล่าให้ผู้อื่นได้รับรู้ โดยนำมาศึกษาวิธีการที่อาชญากรทำการแสดงละคร[59] ซึ่งประกอบไปด้วย

1) การแสดงลักษณะตัวละคร (character) คือ การอุปโลกน์ตัวตนของอาชญากรที่มุ่งแสดงลักษณะของตนให้ปรากฏตามอุดมคติของเหยื่อกลุ่มเป้าหมาย

2) การเล่นบทบาท (role) คือ ศึกษาข้อมูลเหยื่อเพื่อคาดหมายความต้องการจากคู่ปฏิสัมพันธ์หรือสังคม อาชญากรจะเลือกบทบาทในแต่ละสถานการณ์เพื่อจัดระเบียบปฏิสัมพันธ์นั้น

3) การปรับเปลี่ยนตัวตน อันเป็นกระบวนการเคลื่อนไหวที่เปลี่ยนแปลงไปมาได้ ไม่มีลักษณะตายตัว ทั้งนี้เพื่อมุ่งให้เหยื่อเกิดความประทับใจ (impression) ด้วยการแสดงให้เหมาะสมกับบริบทของสถานการณ์ กลายเป็นตัวตนที่มีภาพลักษณ์ (self-image) น่าหลงใหล

Goffman จำแนกรูปแบบการแสดงออกไว้หลายประเภท[60]ซึ่งอาจนำมาประยุกต์ใช้กับการศึกษารูปแบบก่อพิศวาสอาชญากรรมดังต่อไปนี้

1) กิจวัตร (routine) การแสดงที่ทำอยู่เป็นประจำในการดำเนินชีวิตประจำวัน เช่น การแสดงเป็นคนรักที่เป็นห่วงเป็นใยสอบถามสารทุกข์สุกดิบสม่ำเสมอ

2) การแสดงแบบเกินจริง (dramatic realization) เป็นการแสดงเกินความจำเป็นเพื่อให้ผู้ชมตะหนักว่า *ประการแรก* นิยามสถานการณ์และภาพลักษณ์ของผู้แสดงนั้นยังดำรงอยู่ เช่น การใช้ถ้อยคำที่อ่อนหวานกว่าปกติเมื่อเป้าหมายเริ่มตีจาก เพื่อเป็นการเตือนว่าผู้แสดงยังมีสถานภาพเป็นคนรักที่ขาดเหยื่อไม่ได้ *ประการที่สอง* สิ่งที่ผู้แสดงทำอยู่นั้นเป็นเรื่องยากหรือเป็นการทุ่มเท เช่น การจดจำข้อมูลส่วนตัวที่เกี่ยวข้องกับชีวิตของเหยื่ออย่างตั้งใจเพื่อแสดงให้เห็นว่าเอาใจใส่รายละเอียดในชีวิตดุจคนสำคัญ

3) การแสดงตามแบบอุดมคติ (idealization) เป็นการแสดงตามอุดมคติของสังคมนั้นๆ (สังคมของเหยื่อ) Goffman กล่าวว่าการแสดงรูปแบบนี้เกิดขึ้นบ่อยที่สุดเมื่อต้องการเป็นที่ยอมรับของกลุ่ม เมื่อมีความต้องการจะเลื่อนชั้นทางสังคม หรือเมื่ออยากจะบอกว่าการกระทำเช่นนี้ฉันทำให้เธอคนเดียว การแสดงนี้ต้องมีการปิดบังการกระทำหรือความคิดความต้องการบางอย่างที่ขัดกับอุดมคติภาพลักษณ์นั้น และการแสดงนี้จำเป็นต้องอาศัยการแยกแยะผู้ชม (audience segregation) แต่ละกลุ่มออกจากกัน เช่น ไม่อยากให้มีการ

[59] สุภางค์ จันทวานิช, (2551), *การวิเคราะห์เชิงละคร* ทฤษฎีสังคมวิทยา, กรุงเทพฯ: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, หน้า 131-132.

[60] เจอรัลด์ ดี แบรีแมน, (2549), หน้า 114-121.

พบปะตัวตนที่แท้จริง หรือการพูดคุยสดแบบเห็นหน้าตาท่าทางหรือน้ำเสียงเพราะกลัวว่าจะจับได้ว่าไม่ใช่ฝรั่ง หรือคนที่ตัวเองได้อวดอ้างไว้ เป็นต้น

4) การปลอมตัว (misrepresentation) เป็นการนำเสนอภาพลักษณ์ที่ตัวเองไม่มีสิทธินำเสนอ เช่น อ้างว่าเป็นนักเรียนนอกทั้งๆ ที่ไม่เคยไปเรียนเมืองนอก หรือเป็นทหารอเมริกัน เป็นต้น

5) การทำให้ดูขลัง (mystification) เป็นการทำให้ผู้ชมรู้สึกว่าการแสดงของตนนั้นเป็นสิ่งที่คนอื่นไม่มีวันเข้าถึงได้ เช่น การอ้างว่าไม่อาจมาพบปะหรือพูดคุยได้เพราะมีธุรกิจหรือภารกิจสำคัญที่ไม่ว่างหรือต้องปิดลับ เมื่อเหยื่อไม่เชื่อก็จะตัดบทขู่ตัดความสัมพันธ์ด้วยท่าทีโกรธเกรี้ยว หาว่าเหยื่อนั้น “อยู่คนละชั้น” ไม่มีวันเข้าใจข้อจำกัดของนักธุรกิจสุดยุ่ง หรือทหารที่ต้องเก็บลับ

เมื่อปรับแนวคิดของ Goffman มาใช้กับงานวิจัยเรื่องพิศวาสอาชญากรรมก็สามารถนำมาออกแบบวิธีเก็บข้อมูลวิจัยได้ดังนี้

1) การสัมภาษณ์เชิงลึกกับเหยื่อ และอาชญากร scammer เราอาจเห็นได้ว่าอันไหนเป็นหน้าฉาก/หลังฉาก เพื่อให้ได้มากซึ่งข้อมูลที่เป็นจริงมากที่สุด

2) ใช้เพื่อวางกรอบจำแนกรูปแบบกลยุทธ์ที่อาชญากร scammer นำมาใช้กับเหยื่อว่ามีกี่ประเภท โดยอาจสะท้อนให้เห็นจากอดุมคติของหญิงไทยที่คาดหวังการมีคู่รักเป็นคนต่างชาติ โดยเฉพาะฝรั่ง

นอกจากนี้ความสัมพันธ์ระหว่างการเข้าใจกระบวนการสร้างภาพลักษณ์ก็สามารถนำมาพัฒนาทักษะการทำงานสนาม (การวิจัย/การพัฒนา) ได้โดยการปรับกระบวนทัศน์ของผู้ช่วยวิจัยในการเก็บข้อมูล[61] อาทิ

1) ภาพลักษณ์เป็นตัวกำหนดรูปแบบและระดับความสัมพันธ์ระหว่างเรากับประชากร เราอาจเปลี่ยนสถานภาพและบทบาทเราไม่ได้ แต่เราสามารถเปลี่ยนความคาดหวังและนิยามสถานภาพของเราได้จากการวางตัว
2) ภาพลักษณ์เป็นตัวกำหนดคุณภาพของงานข้อมูล ว่าเราจะได้ข้อมูลอะไร ลึกแค่ไหน ถูกต้องแค่ไหน ตรงกับความเป็นจริงเพียงใด
3) ความเข้าใจเรื่องนี้ ช่วยให้ไวในการสังเกตข้อมูลที่เขาต้องการปิดบัง และช่วยให้เข้าใจคำพูด ท่าที และปฏิกิริยา ของเขาได้ดีขึ้น

หลังจากได้ข้อมูลวิจัยแล้วใช้กรอบคิดของ Sinnicolas ที่พัฒนาการวิเคราะห์เชิงตัวละครของ Goffman เพื่อเป็นแนวทางในการศึกษาและทำความเข้าใจชุมชนเสมือนจริง (Virtual Society) เพื่อวิเคราะห์องค์ประกอบที่เอื้อให้เกิดการล่อลวงได้ทั้ง 4 ด้าน[62] คือ

1) การสร้างตัวตนออนไลน์ (online identity) ซึ่งเป็นตัวตนที่อาชญากรแสดงออกผ่านโลกเสมือนซึ่งอาจเป็นตัวตนที่แท้จริง ไม่แท้จริง หรือตัวตนที่เลือกแสดงออกก็ได้

[61] เจอรัลด์ ดี แบรีแมน, (2549), หน้า 142-143.

[62] นัฐวุฒิ สิงห์กุล, (2554), *แล้วเราจะศึกษามานุษยวิทยาในโลกไซเบอร์อย่างไร?*, สืบค้นจาก http://nattawutsingh.blogspot.com/2011/10/blog-post_2823.html

2) บริบททางสังคม (Social Context) ที่เอื้อให้เกิดพิศวาสอาชญากรรมแบบต่างๆ ขึ้นมาได้ เช่น สังคมที่หญิงต้องการมีคู่เป็นชาวต่างชาติ สังคมที่คนชอบสงสารและทำบุญทำทานให้คนตกยาก หรือสังคมที่หาโอกาสทางเศรษฐกิจยากจนตกเป็นเหยื่อการล่อลวงให้ลงทุนได้ง่าย

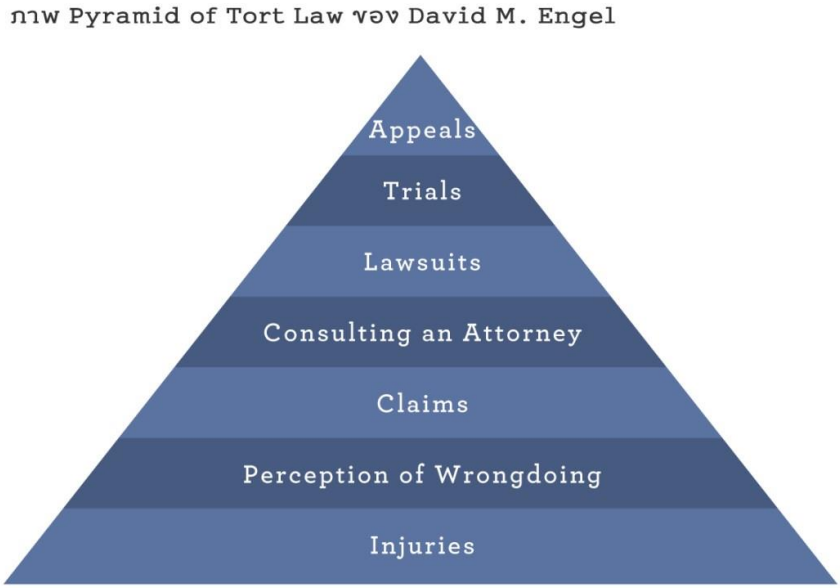
3) ปฏิสัมพันธ์ทางสังคม (Social Interaction) ที่ปรากฏผ่านพื้นที่อินเตอร์เน็ต โดยศึกษากลวีในการสร้างความประทับใจหลงใหลให้เกิดกับตัวเหยื่อ เช่น การเข้าอกเข้าใจ รู้ใจ จดจำรายละเอียดในชีวิตของเหยื่อได้ เสมือนเป็นคนพิเศษสุดในชีวิตของเหยื่อ

4) การติดต่อสื่อสาร (Communication) มองที่รูปแบบการสื่อสารผ่านช่องทางใด วิธีการสื่อสารในลักษณะไหนพัฒนาขึ้นมาจากการเก็บข้อมูลชุดใดของเป้าหมาย ภาษาที่ใช้ในการสื่อสารนั้นตรงกับอุดมคติของเหยื่อไหม และอื่นๆ

กรอบแนวคิดชุดที่สองนี้จะนำไปศึกษารูปแบบและวิธีการทั้งหลายที่อาชญากรใช้เป็นกลยุทธ์ในการล่อลวงเหยื่อให้หลงเชื่อเพื่อให้ได้มาซึ่งผลประโยชน์ โดยงานวิจัยจะใช้กรอบทฤษฎีในการอธิบายกลยุทธ์ทั้งหลายของอาชญากรในทุกขั้นตอน และสะท้อนให้เห็นการแสดงหน้าฉากของอาชญากรในแต่ละขั้นที่ปกปิดความจริงไว้หลังฉากด้วย

2.2.3 กรอบความคิดเกี่ยวกับกระบวนการยุติธรรมและการเยียวยาความเสียหาย

<u>กรอบแนวคิดที่สาม</u> คือ ทฤษฎีเกี่ยวกับการบังคับใช้กฎหมายกับอาชญากรรมไซเบอร์ทั้งที่เกิดภายในรัฐและอาชญากรรมข้ามชาติ โดยมีนักวิชาการทางกฎหมายได้พัฒนารูปแบบการวิเคราะห์ให้เห็นถึงอุปสรรคและต้นทุนในการใช้กระบวนการยุติธรรมของรัฐเพื่อป้องกันและปราบปรามอาชญากรรมไซเบอร์ โดยมีทฤษฎีที่สามารถนำมาปรับใช้เพื่อทำความเข้าใจเหยื่อผู้เสียหายว่าทำไมตัดสินใจไม่เข้าร้องทุกข์หรือยุติการดำเนินคดีไปเสียกลางคัน นั่นคือ ทฤษฎีปีระมิดของกฎหมายละเมิด (Pyramid of Tort Law) ของ Professor Dr. David M. Engel แห่ง University of Buffalo, USA.



ที่มา : https://www.the101.world/law-in-real-life/

ปีระมิดของกฎหมายละเมิด (The pyramid of Tort Law)[63] เป็นภาพที่อธิบายถึงคดีที่มีจำนวนเยอะมากที่ฐานของปีระมิด และน้อยลงเรื่อยๆ ในขึ้นต่อไปเป็นลำดับจนถึงยอดปีระมิดที่ไปถึงศาลอุทธรณ์หรือเป็นคดีที่มีการพิพากษาจริงๆ ขั้นตอนของการใช้กฎหมายเป็นเครื่องมือทั้ง 7 ขั้นตอนนี้ เริ่มต้นด้วยการเกิดความเสียหาย (injuries) ขั้นที่สองเป็นการตระหนักได้ว่าความเสียหายนั้นเกิดขึ้นโดยการกระทำของผู้อื่น(perception of wrongdoing) ซึ่งคนส่วนใหญ่ติดอยู่ที่ขั้น 2 ของปีระมิด ด้วยเหตุผลที่ว่ากลัวความเสี่ยงและอำนาจของเจ้าหน้าที่ในระบบยุติธรรม เช่น กลัวตำรวจเข้าข้างอีกฝ่ายหนึ่งและกลัวว่าตนจะกลายเป็นฝ่ายที่ทำผิดกฎหมายเสียเอง บางคนมองว่ากฎหมายทำอะไรไม่ได้และหันเข้าทางคำสอนของพระพุทธเจ้าภาวนาให้กรรมตามสนอง ขั้นที่สามคือการเรียกร้อง (claims) และพบว่าการเรียกร้องค่าเสียหายส่วนใหญ่อาจยุติลงด้วยการยอมความกันนอกศาล ขั้นที่สี่เป็นการปรึกษาทนายความ (consulting an attorney) ขั้นที่ห้าเป็นการที่ทนายยื่นคำร้องฟ้องคดี (lawsuits) ขั้นที่หกเป็นการพิจารณาคดีในศาล (trials) และขั้นสุดท้ายคือการอุทธรณ์ศาลฎีกาซึ่งเป็นยอดสูงสุดทีมีจำนวนคดีขึ้นไปถึงน้อยที่สุด ภาพปีระมิดนี้สะท้อนให้เห็นสภาพปัญหาและข้อจำกัดของการใช้กฎหมายเป็นเครื่องมือในการแก้ข้อพิพาทของบุคคล ตามทฤษฎีจะเห็นได้ว่าคดีที่เกิดขึ้นไปถึงชั้นศาลมีจำนวนที่ต่างกันอย่างเห็นได้ชัด เนื่องจากคนส่วนใหญ่มักใช้การเจรจาต่อรองนอกกฎหมายเป็นการแก้ไขสิ่งที่เกิดขึ้น

หากนำทฤษฎีนี้มาปรับใช้กับการละเมิดสิทธิด้ายพิศวาสอาชญากรรมก็จะช่วยสร้างกรอบในการวิเคราะห์ว่าเหตุใดการเยียวยาหลังเกิดเหตุล่อลวงไปแล้วจึงไม่เหมาะสมกับการป้องกันและปราบปรามอาชญากรรมชนิดนี้ โดยเมื่อเทียบกับคดีที่ง่ายกว่าอย่างการละเมิดสิทธิในชีวิตประจำวันที่เกิดในเขตอำนาจศาลเดียวกัน (ประเทศเดียวกัน) หลายการศึกษาพบว่า คดีละเมิดที่ได้รับการพิจารณาคดีในชั้นศาลมีเพียง 10-15% เท่านั้น ส่วนที่เหลือคู่ความอาจตกลงยอมความ ถอนฟ้อง หรือทิ้งฟ้อง และอีกหลายงานวิจัยยังชี้ให้เห็นว่าโจทก์จะชนะคดี 50% ของคดีความทั้งหมด ดังนั้นจะเห็นได้ว่าถ้าหากเกิดคดีละเมิด 100 คดี คดีนั้นจะไปถึงศาลเพียง 10 – 15 คดีเท่านั้น ทั้งนี้อาจเกิดจากข้อจำกัดหลายประการ เช่น

- *ขั้นตอนของระบบกฎหมายที่เป็นทางการ* สิ่งนี้หมายถึงการไม่รู้กฎหมาย การเข้าไม่ถึงกฎหมาย รวมถึงการไม่คุ้นเคยต่อระบบกฎหมายที่แยกออกชีวิตประจำวันของผู้คน ทำให้เกิดความไม่เชื่อมั่นและไม่ไว้วางใจระบบกฎหมาย
- *ต้นทุนของการดำเนินการ* ทั้งนี้หมายรวมถึงทั้งค่าใช้จ่ายและระยะเวลา การดำเนินการทางกฎหมายต้องอาศัยผู้เชี่ยวชาญในการดำเนินการ จึงต้องอาศัยทางเงินและระยะเวลาที่ยาวนาน บางครั้งผู้เสียหายอาจคำนวณแล้วว่าไม่คุมค่าต่อต้นทุนของการดำเนินการทางกฎหมาย หรือบางครั้งอาจได้รับการขอเจรจาประนีประนอมกันเสียก่อนที่จะถึงขั้นตอนของศาล
- *ความเป็นไปได้ในการชนะคดี* สิ่งนี้เป็นปัจจัยสำคัญในการตัดสินใจว่าจะต่อสู้ด้วยกระบวนการทางกฎหมายหรือไม่ ซึ่งผู้เสียหายต้องพิจารณาถึงความน่าเชื่อถือพยานหลักฐาน ความสามารถของทนายความ ความซับซ้อนของคดี และแนวโน้มการวินิจฉัยของศาล ซึ่งมีผลต่อการตัดสินใจให้ดำเนินคดีหรือให้ยุติการดำเนินคดี

[63] Engel, D. M., (2557), หน้า 141- 163

นอกจากข้อจำกัดบางประการแล้วควรต้องมีการทำความเข้าใจตัวบทกฎหมายกับการบังคับใช้ในความเป็นจริง สิ่งนี้จะชี้ให้เห็นอุปสรรคหรือปัญหาที่เกิดขึ้นในขั้นตอนต่างๆ ของการบังคับใช้กฎหมายและผลต่อประสิทธิภาพของการบังคับใช้กฎหมาย ซึ่งหากอุปสรรคปัญหาเป็นผลมาจากระบบภายในระบบกฎหมายก็อาจต้องมีการปรับปรุงและแก้ไขให้ตรงจุด ไม่ว่าจะเป็นตัวบทกฎหมาย หรือกระบวนการดำเนินคดีก็ตาม แต่หากเป็นผลมาจากแง่มุมทางวัฒนธรรมก็อาจต้องยอมรับข้อจำกัดบางประการและพัฒนาเครื่องมือหรือนโยบายอื่นๆ มารองรับ

ยิ่งไปกว่านั้นเมื่ออาศัยกรอบทฤษฎีของงานศึกษาด้านกฎหมายและกระบวนการยุติธรรมของนักวิชาการอีก 3 ท่านที่ศึกษาเรื่องพิศวาสอาชญากรรมโดยตรงก็จะยิ่งเห็นว่าทฤษฎีปีระมิดของกฎหมายละเมิดเหมาะเป็นอย่างยิ่งในการนำมาใช้อธิบายปรากฏการณ์ในกระบวนการป้องกันและปราบปรามพิศวาสอาชญากรรมโดยเฉพาะวิเคราะห์จากมุมของผู้เสียหายที่ต้องเผชิญกับกระบวนการยุติธรรมของรัฐสมัยใหม่ เช่น งานของ Nir Kshetri[64] เรื่อง “เศรษฐศาสตร์ง่ายๆของอาชญากรรมไซเบอร์และวงจรอุบาทว์” ที่เสนอว่าการร้องทุกข์ต่อความเสียหายที่เกิดจากอาชญากรรมนั้นมีต้นทุนทั้งต่อตัวเหยื่อเองที่ต้องอับอายขายหน้ามีภาพลักษณ์ไม่ดี ต้นทุนค่าเสียโอกาส เสียเวลาหากต้องนำคดีเข้าสู่กระบวนการยุติธรรม รัฐก็ยังมองว่าไม่คุ้มทุนต่อการบังคับใช้กฎหมายกับคดีที่รัฐยังไม่เห็นปริมาณหรือมูลค่าที่มากพอจะจัดสรรทรัพยากรมาแก้ไข เสริมด้วยงานด้านข้อจำกัดในการนำคดีอาชญากรรมไซเบอร์เข้าสู่กระบวนการทางกฎหมายยังมีอีกของ EFG Ajayhi [65] เรื่อง “ความท้าทายในการบังคับใช้กฎหมายและนโยบายเกี่ยวกับอาชญากรรมไซเบอร์” ว่าเจ้าพนักงานที่ต้องแสวงหารวมรวมพยานที่อยู่ในรูปดิจิทัลขาดความเชี่ยวชาญ และห้องตรวจพิสูจน์ที่ต้องได้รับการลงทุนหรือส่งไปตรวจในต่างประเทศทั้งอาชญากรยังอำพรางตัวตนตรวจสอบได้ยาก และขาดแคลนข้อกฎหมายและกระบวนการยุติธรรมที่เอื้อต่อการดำเนินคดีไซเบอร์ เหนือสิ่งอื่นใดคือข้อจำกัดด้านเขตอำนาจศาลเมื่ออาชญากรอยู่นอกดินแดน ซึ่งในประเด็นเขตอำนาจศาลนี้ Alexandra Perloff-Giles [66] ก็เน้นให้เห็นถึงลักษณะข้ามพรมแดนของอาชญากรรมไซเบอร์ที่เกิดขึ้นตลอดเวลาและไม่สอดคล้องกับลักษณะของกระบวนการยุติธรรมในรัฐสมัยใหม่ที่มีขอบเขตดินแดนของรัฐเป็นข้อจำกัด และเมื่อใช้เพียงกฎหมายหรือกระบวนการของรัฐใดรัฐหนึ่งย่อมไม่อาจดำเนินคดีกับอาชญากรและเยียวยาเหยื่อได้อย่างมีประสิทธิผล

กรอบแนวคิดทั้ง 3 ช่วยทำให้เห็นถึงสภาพปัญหาและแนวทางแก้ไขปัญหานี้ โดยในกรอบความคิดแรกจะแสดงให้เห็นถึงลักษณะของบุคคลที่เสี่ยงจะตกเป็นเหยื่ออันเนื่องมาจากการเปิดเผยข้อมูลส่วนบุคคลอ่อนไหวในพื้นที่สาธารณะโดยขาดความความระมัดระวังทั้งยังไม่มีระบบเฝ้าระวังเตือนภัยให้แก่ผู้ใช้อินเตอร์เน็ตอย่างมีประสิทธิภาพ ทำให้อาชญากรสามารถรวบรวมข้อมูลทั้งหลายเป็นข่าวกรองในการโจมตีเป้าหมายได้ง่ายขึ้น กรอบความคิดชุดที่สองแสดงให้เห็นถึงกลยุทธ์ของอาชญากรในการพลิกแพลงอัตลักษณ์ในโลกออนไลน์ให้ตรงตามความปรารถนาของเหยื่อเพื่อเพิ่มโอกาสในการล่อลวงเหยื่อได้ง่ายขึ้น ยิ่งไปกว่านั้นอาชญากรยังฉวยใช้การสื่อสารด้วยภาษาเขียนและรูปภาพผ่าน

---

[64] Kshetri, N., (2010), “Simple Economics of Cybercrime and the Vicious Circle.” *The Global Cybercrime Industry*, Berlin; Springer-Verlag.

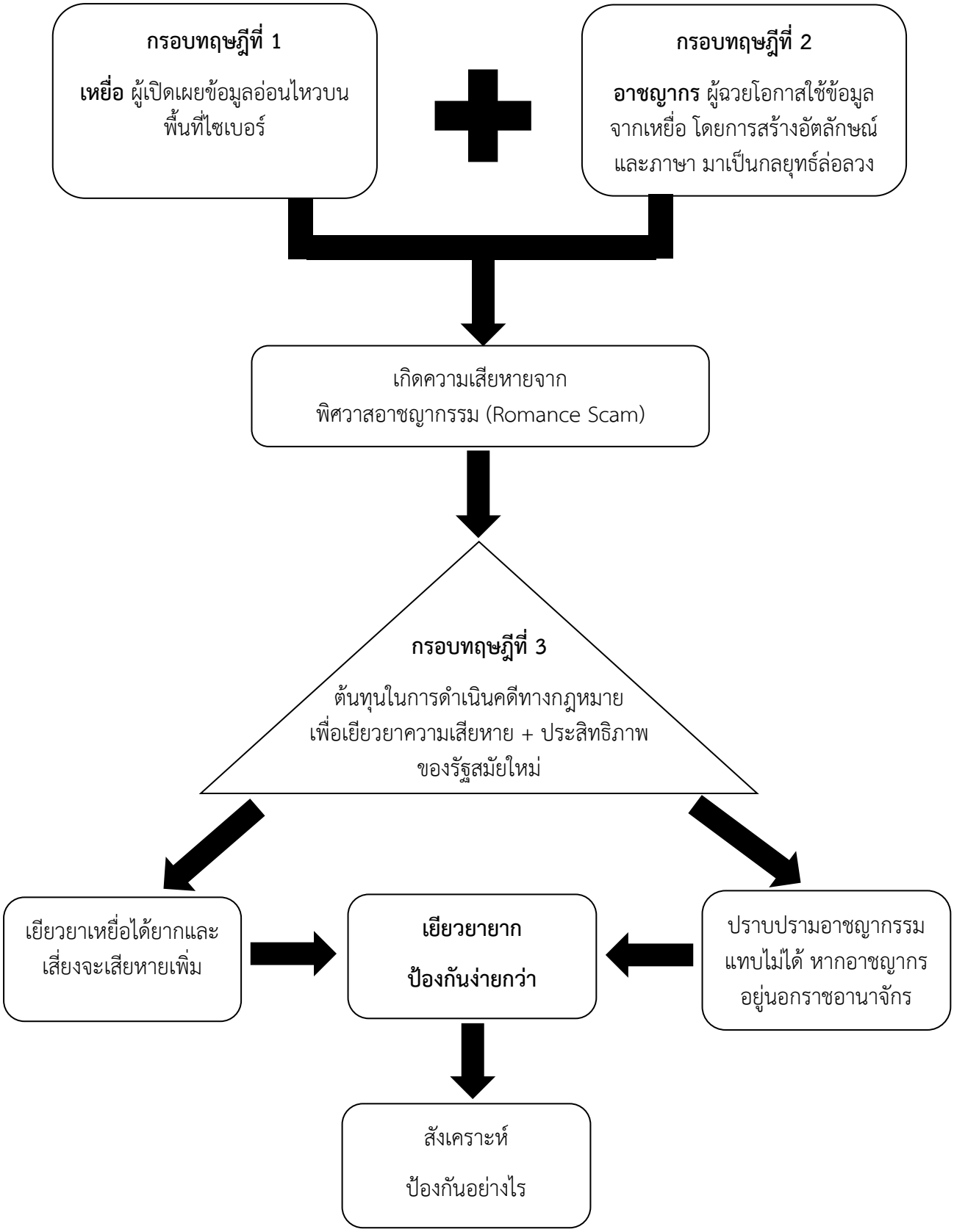
[65] Ajayhi, E., (2015), “The Challenges to Enforcement of Cybercrimes Laws and Policy.” *International Journal of Information Security and Cybercrime*, 4(2), 33-48, สืบค้นจาก https://www.ijisc.com

[66] Perloff-Giles, A., (2017), *A“PROBLEM WITHOUT A PASSPORT”: OVERCOMING JURISDICTIONAL CHALLENGES FOR TRANSNATIONAL CYBER AGGRESSIONS*, สืบค้นจาก https://law.yale.edu/system/files/area/center/global/document/perloff-giles_cyber_conflict_paper_-_final_draft.pdf

ข้อความในระบบอินเตอร์เน็ตซึ่งสามารถล่อลวงให้เหยื่อหลงรัก เห็นอกเห็นใจ ไปจนถึงการส่งมอบทรัพย์สินเงินทองให้แม้ไม่เคยพบปะตัวตนจริงๆ ในโลกกายภาพ และเมื่อเกิดความสูญเสียขึ้นแล้วกรอบความคิดชุดที่สามก็สะท้อนให้เห็นถึงต้นทุนในการฟ้องร้องดำเนินคดีทางกฎหมายต่ออาชญากรทั้งในมุมของตัวเหยื่อเองที่ต้องเผชิญกับความอับอายและกระบวนการยุติธรรมที่ไม่เอื้ออำนวยต่อการเยียวยาสิทธิ รวมถึงข้อจำกัดของกลไกบังคับใช้กฎหมายของรัฐสมัยใหม่ที่เป็นอุปสรรคสำคัญในการติดตามจับกุมอาชญากรที่อยู่นอกราชอาณาจักรมาดำเนินคดีและติดตามทวงคืนทรัพย์สิน จึงมีความจำเป็นต้องสร้างมาตรการป้องกันการเกิดเหตุอาชญากรรมเสียก่อน อันจำเป็นผลดีต่อประชาชนผู้ใช้อินเตอร์เน็ตมากกว่าการปราบปรามเยียวยาหลังอาชญากรรมเกิดขึ้นแล้ว

กรอบแนวคิดทั้งสามจะเป็นแนวทางในการวิจัยตลอดทั้งเรื่อง และนำมาสังเคราะห์มาตรการทางกฎหมายและชุดข้อมูลเสริมสร้างความตระหนักรู้พิศวาสอาชญากรรมเพื่อการป้องกันและระวังภัยให้แก่ผู้บังคับใช้กฎหมาย ผู้ควบคุมระบบ และประชาชนต่อไป

กรอบทฤษฎีในการวิจัย



บทที่ 3

ระเบียบวิธีวิจัย

งานวิจัยโครงการนี้มีระเบียบวิธีวิจัยเพื่อแสวงหาผล ดังต่อไปนี้

3.1. วิธีการศึกษา

งานวิจัยนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative) ที่มุ่งสะท้อนข้อเท็จจริงทางสังคมที่เกิดขึ้น (Social Facts) โดยมีระเบียบวิธีวิจัยที่ใช้แสวงหาคำตอบให้โจทย์วิจัยทั้ง 2 แบบ คือ

1) การวิจัยเอกสาร (Documentary Research) ศึกษาจากเอกสารชั้นต้นทั้งหลาย และเก็บหลักฐานบางส่วนจากกรณีศึกษาที่เป็นคดี การวิจัยเอกสารจะศึกษาเอกสาร หลักฐานชั้นต้นจากคำพิพากษา สำนวนคดีที่เข้าถึงได้ ซึ่งไม่รวมคดีเกี่ยวกับการโอนเงิน เปิดบัญชี และการฟอกเงิน
2) การวิจัยแบบตีความ (Interpretative Research) โดยศึกษาข้อมูลภาคสนาม (Field Study) ที่ได้มาด้วยวิธีการสัมภาษณ์เชิงลึก (In-Depth Interview) จากแหล่งข้อมูลผู้มีศักยภาพสูง (interviewing high potential sources) อาทิ เหยื่อ (victim) ผู้บังคับใช้กฎหมาย (law enforcement officer) ผู้ดูแลระบบ (system administrator) ซึ่งสัมผัสกับประสบการณ์ในสถานการณ์จริง เพื่อศึกษารูปแบบวิธีการล่อลวงของอาชญากรและอุปสรรคในการป้องกันปราบปรามอาชญากรรม แต่ไม่รวมเจ้าหน้าที่ปราบปรามการฟอกเงินและสถาบันการเงิน ทั้งยังสัมภาษณ์นักวิชาการผู้เชี่ยวชาญด้านอาชญากรรมไซเบอร์เพื่อความสมบูรณ์ในการวิเคราะห์ข้อมูลและการสังเคราะห์ข้อเสนอแนะในการวิจัย

3.2. ชุดคำถามสำหรับการสัมภาษณ์เชิงลึก

การสัมภาษณ์จะครอบคลุม 3 หัวข้อหลัก ได้แก่

1) สภาพปัญหา
2) รูปแบบ และวิธีการก่อพิศวาสอาชญากรรม
3) การบังคับใช้กฎหมาย และแนวทางการป้องปรามเกี่ยวกับพิศวาสอาชญากรรม

การสัมภาษณ์เชิงลึก (Depth interview) ในงานวิจัยนี้ จะสัมภาษณ์ผู้มีศักยภาพสูงทั้งหมด 20 คน ซึ่งแบ่งออกเป็น 4 กลุ่ม ได้แก่ 1)ผู้บังคับใช้กฎหมาย เช่น เจ้าหน้าที่ตำรวจ, เจ้าหน้าที่กรมสอบสวนคดีพิเศษ, อัยการ เป็นต้น 2) นักวิชาการ 3) เหยื่อ/ผู้เสียหาย และ 4) ผู้ดูแลระบบ (administrator) เช่น admin page, admin application หาคู่, admin สื่อออนไลน์ที่เกี่ยวข้อง เป็นต้น

1) กรอบคำถาม ผู้บังคับใช้กฎหมาย

1) สภาพปัญหา รูปแบบ และวิธีการก่อพิศวาสอาชญากรรม
2) กระบวนการพิจารณาคดีเกี่ยวกับกรณีพิศวาสอาชญากรรม ต้องมีพยานหลักฐานในระดับใดในการชั่งน้ำหนักพยานหลักฐาน และการพิจารณาคดี
3) การรับฟังพยานผู้เชี่ยวชาญมีผลต่อกระบวนการพิจารณาคดีหรือไม่ มากน้อยเพียงใด
4) การบังคับคดีเกี่ยวกับกรณีพิศวาสอาชญากรรมมีลักษณะเป็นอย่างไร
5) การบังคับใช้กฎหมาย / พ.ร.บ.คอมพิวเตอร์ กับกรณีพิศวาสอาชญากรรม มีข้อจำกัด/อุปสรรค และมีผลกระทบอย่างไร
6) กลุ่มคนที่ตกเป็นเหยื่อมีกี่กลุ่ม กลุ่มใดบ้าง
7) หน่วยงานที่ดูแลเรื่องดังกล่าวมีหน่วยงานใดบ้าง แต่ละหน่วยงานทำหน้าที่อะไร และประสานงานกันอย่างไร
8) ช่องทางการรับแจ้งความ/ข้อมูลเกี่ยวกับคดีดังกล่าวมีกี่ช่องทาง แต่ละช่องทางมีผลอย่างไร
9) สถิการรับแจ้งความเกี่ยวกับคดีดังกล่าว
10) ที่ผ่านมาสามารถใช้กฎหมายข้อใด เพื่อจัดการ/แก้ไขปัญหาดังกล่าว และกฎหมายนั้นๆ สามารถแก้ไขปัญหาได้จริงหรือไม่ อย่างไร
11) ประเทศไทยมีมาตรการจัดการกับปัญหาดังกล่าวอย่างไร
12) มีความเข้าใจเกี่ยวกับความเสียหาย และลักษณะของอาชญากรรมในหมู่ผู้บังคับกฎหมายเป็นการทั่วไปหรือไม่ หรือต้องอาศัยเจ้าพนักงานที่มีความเชี่ยวชาญชำนัญพิเศษ
13) ความยากลำบากในการรวบรวมพยานหลักฐานประกอบสำนวน
14) อุปสรรคในการเรียกตัวผู้ถูกกล่าวหา ขอหมายศาล เพื่อติดตามดำเนินคดีต้องผู้ต้องหา
15) การประสานความร่วมมือทางอาญาระหว่างประเทศในกรณีที่ผู้กระทำความผิดอยู่นอกเขตอำนาจศาลไทยเป็นอย่างไรบ้าง
16) มีความร่วมมือกับองค์การระหว่างประเทศในการติดตาม ดำเนินคดี ส่งผู้ร้ายข้ามแดน และความร่วมมือทางอาญาระหว่างประเทศกับรัฐอื่นในลักษณะใดบ้าง
17) ความพร้อมในเชิงทรัพยากรเพื่อสนับสนุนการปราบปรามพิศวาสอาชญากรรม
18) มีข้อเสนอในการปรับปรุงกระบวนวิธีการดำเนินคดีต่อพิศวาสอาชญากรรมเช่นไร
19) การปฏิรูปองค์กร หรือพัฒนาความร่วมมือเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรมระหว่างประเทศในลักษณะใดที่ท่านปรารถนา

2) กรอบคำถาม นักวิชาการ

1) เมื่อเทียบการล่อลวงในโลกจริงกับโลกไซเบอร์ ท่านคิดว่ามีความแตกต่างกันหรือไม่อย่างไร
2) ทำไมการป้องกันผู้ใช้อินเตอร์เน็ตจากการถูกล่อลวงด้วยความเสน่หาจึงทำได้ยาก
3) ท่านคิดว่าคนกลุ่มใดที่ตกเป็นเหยื่ออาชญากรรมได้เพราะอะไร
4) เมื่อดูสถิติเหยื่อและสถานะของผู้เสียหาย ท่านมีความประหลาดใจหรือไม่
5) อะไรเป็นเหตุผลที่ทำให้เหยื่อคนไทยถูกหลอกด้วยอาชญากรชาวต่างชาติได้
6) เหตุผลใดที่เป็นเงื่อนไขให้ผู้เสียหายไม่เข้าแจ้งความดำเนินคดี เรียกร้องชดเชยค่าเสียหาย
7) รัฐหรือผู้ประกอบการควรมีมาตรการป้องกันอย่างไร

8) มาตรการเชิงตักเตือนและระวังภัยมิให้มีพฤติกรรมเสี่ยงที่จะตกเป็นเหยื่อ เพียงพอไหมในปัจจุบัน
9) ควรปรับปรุงมาตรการเชิงเยียวยาหรือรับเรื่องราวร้องทุกข์ เอื้อให้ผู้เสียหายเข้าร้องทุกข์หรือไม่ อย่างไร
10) การดำเนินคดีกับอาชญากรจะมีอุปสรรคอย่างไรบ้าง
11) มาตรการคุ้มครองผู้เสียหาย และเยียวยา ควรมีหลักประกันเสริมพิเศษอย่างไร

3) กรอบคำถามสำหรับ เหยื่อ/ผู้เสียหาย

1) คุณเปิดเผยข้อมูลส่วนบุคคล เช่น ชื่อ อายุ ที่อยู่ อาชีพการงาน เบอร์โทรศัพท์ รูปภาพ lifestyle บนโลกออนไลน์มาก/น้อยแค่ไหน อย่างไร
2) คุณโสด สมรส หรือหย่าร้าง (มีบุตร?)
3) ทำไมถึงไว้ใจการหาคู่ออนไลน์ (ในกรณีที่เหยื่อใช้ web/app คู่)
4) โปรไฟล์ของ scammer มีลักษณะอย่างไร
5) ระยะเวลาในการพูดคุยติดต่อสื่อสาร/สร้างความสนิทสนม
6) ติดต่อสื่อสารกันด้วยวิธีใดบ้าง
7) เคยเห็นหน้าหรือมีการสื่อสารแบบถ่ายทอดสดกันหรือไม่
8) กลยุทธ์/รูปแบบ/ลักษณะที่ถูกหลอกเป็นอย่างไร
9) Scammer อ้างว่าเป็นคนประเทศอะไร อาชีพ แต่งงาน/ไม่ได้แต่งงาน ฐานะทางการเงิน
10) เสียทรัพย์สินให้แก่ scammer หรือไม่ อย่างไร
11) ท่านทราบหรือไม่ว่ามีหน่วยงานที่เกี่ยวข้องดูแลเรื่องดังกล่าวอยู่
12) ท่านได้ร้องเรียนกับทางผู้ดูแลระบบ app/เพจ หรือไม่
13) ท่านได้แจ้งความ ร้องทุกข์กับเจ้าหน้าที่ของรัฐบ้างหรือไม่ อย่างไร (เลือกร้องเรียน/แจ้งความที่หน่วยงานใด เพราะเหตุใด)
14) หากมีการร้องเรียน/แจ้งความแล้ว การดำเนินการเรื่องดังกล่าวมีขั้นตอน/ระยะเวลาอย่างไร มีความยากลำบาก/ยาวนานหรือไม่ อย่างไร และได้ผลจากการร้องเรียน/แจ้งความนั้นอย่างไร
15) ท่านได้รับการเยียวยาหรือไม่ ในลักษณะใดบ้าง เช่น ผู้ล่อลวงได้รับโทษทางอาญา ท่านได้รับค่าชดเชยในทางแพ่ง
16) ท่านรู้สึกว่าการเยียวยาที่เกิดขึ้นเพียงพอต่อความเสียหายที่ท่านได้รับหรือไม่
17) ท่านคิดว่าระบบที่ท่านใช้ติดต่อสื่อสารควรมีมาตรการในการป้องกันและเยียวยาปัญหาพิศวาสอาชญากรรมเช่นไร
18) หน่วยงานภาครัฐควรมีบทบาทอย่างไรในเฝ้าระวังภัย การรับเรื่องราวร้องทุกข์ และดำเนินการเพื่อเยียวยาความเสียหายให้กับประชาชน
19) ท่านต้องการให้ผู้ดูแลระบบและหน่วยงานรัฐสนับสนุนการป้องกันและปราบปรามพิศวาสอาชญากรรมระหว่างประเทศ
20) การเตือนภัย หรือมาตรการเฝ้าระวังล่วงหน้า ในลักษณะให้ข้อมูลความรู้เท่าทันในชีวิตดิจิทัลและกลยุทธ์ในการล่อลวงแบบต่างๆ จะช่วยลดโอกาสในการถูกล่อลวงหรือไม่

4) กรอบคำถามวิจัย ผู้ดูแลระบบ

1) มีการคัดกรองผู้เข้าใช้บริการอย่างไรบ้าง
2) ข้อมูลที่ระบบให้ผู้ใช้บริการกรอกมีอะไรบ้าง เพื่อยืนยันตัวตน
3) ระบบจัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการมีมาตรการป้องกันการรั่วไหลอย่างไร
4) มีระบบเฝ้าระวังและเตือนผู้ใช้มิให้เปิดเผยข้อมูลส่วนบุคคลอ่อนไหวในพื้นที่สาธารณะเช่นไร
5) มีกลไกตรวจตราและเตือนภัยคุกคามเกี่ยวกับ romance scam ด้วยหรือไม่หากไม่มีผู้ร้องเรียน
6) ปริมาณคนร้องเรียนเรื่องเกี่ยวกับ romance scam หรือเรื่องราวต่างๆ ที่เกี่ยวข้องบ้างหรือไม่ อย่างไร
7) ระบบมีมาตรการเพื่อเยียวยาปัญหาดังกล่าวหรือไม่ อย่างไร (หากมีผู้ดูแลระบบจัดการ/แก้ไขด้วยวิธีใด)
8) ผู้ดูแลระบบมีการประสานงานกับระบบอื่นๆ หรือองค์กรผู้เชี่ยวชาญหรือไม่ ในกิจกรรมใดบ้าง
9) ระบบมีความร่วมมือกับหน่วยงานบังคับใช้กฎหมายหรือไม่ อย่างไร
10) ระบบมีความร่วมมือระหว่างประเทศ หรือประสานงานกับองค์กรของรัฐบาลอื่นหรือไม่ ในลักษณะใด

3.3. จริยธรรมการวิจัยในคน

ทีมวิจัยได้ดำเนินการเสนอโครงการวิจัยเพื่อขอรับการพิจารณารับรองจริยธรรมการวิจัยในคน และได้รับการรับรองการพิจารณาจริยธรรมโครงการวิจัยในคน (Certificate of Approval) จากคณะกรรมการจริยธรรมการวิจัยในคน มหาวิทยาลัยเชียงใหม่ เมื่อวันที่ 29 มกราคม 2562 (ภาคผนวก ค)

บทที่ 4

ผลการศึกษาและการอภิปรายผลการศึกษา

บทนี้จะเป็นการรายงานผลการศึกษาที่ได้จากวิจัยด้วยระเบียบวิธีวิจัยตามที่ชี้แจงไว้ในบทที่ 3 โดยแบ่งเนื้อหาไว้เป็น 2 ส่วน คือ ส่วนที่ 1 ผลการศึกษา และ ส่วนที่ 2 การอภิปรายผลการศึกษา

ส่วนที่ 1 : ผลการศึกษา

ผลการศึกษาที่ได้จากการวิจัยสามารถตอบสนองต่อวัตถุประสงค์ทั้ง 3 ประการ อันได้แก่

1) ศึกษาสภาพปัญหา รูปแบบ และวิธีการของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติ

2) พัฒนากฎหมายและมาตรการเฝ้าระวังและเตือนภัยล่วงหน้าเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม

3) สร้างแนวทางเพิ่มความตระหนักให้ประชาชนกลุ่มเสี่ยงตกเป็นเป้าหมายพิศวาสอาชญากรรมให้รู้เท่าทันพิศวาสอาชญากรรม

โดยมีผลการศึกษาดังต่อไปนี้

4.1. สภาพปัญหา รูปแบบ และวิธีการของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติ

ในหัวข้อนี้จะแสดงให้เห็นผลของการศึกษาใน 2 ส่วนหลัก คือ

1) สถานการณ์ปัจจุบันและสภาพปัญหาพิศวาสอาชญากรรม

2) รูปแบบและวิธีการของพิศวาสอาชญากรรม

4.1.1 สถานการณ์ปัจจุบันและสภาพปัญหาพิศวาสอาชญากรรม

“ความรักในโลกออนไลน์ คุณคิดว่ามีจริง หรือแค่หลอกลวงกัน???”

หัวข้อสนทนาจากเว็บไซต์ Pantip.com[1]

ความรักเป็นสิ่งที่ใครหลายคนตามหา ไม่ว่าความรักแบบคนรัก หรือความรักแบบครอบครัวก็ตาม และเราอาจจะมีความรักในหลากหลายรูปแบบ จากหัวข้อสนทนาผ่านเว็บบอร์ดข้างต้นมีผู้ใช้งานเว็บบอร์ดจำนวนมากเข้ามาแสดงความคิดเห็นกันหลากหลาย ทั้งคำตอบที่พบรักแท้จากโลกออนไลน์

[1] Pantip.com, (2557), *ความรักในโลกออนไลน์ คุณคิดว่ามีจริง หรือ แค่หลอกลวง???,* (26 พฤศจิกายน 2561), สืบค้นจาก https://pantip.com/topic/31571701

และคำตอบที่บอกว่า มันเป็นเพียงเรื่องเพ้อฝัน หลอกลวง แต่ก่อนที่จะพูดถึงการตามหาความรักในโลกออนไลน์นั้น อยากจะพูดถึงโลกออนไลน์ หรือ สังคมออนไลน์ หรือ สื่อสังคมออนไลน์ ซึ่งไม่ว่าจะเป็นคำศัพท์คำใดก็อยากจะให้ทำความเข้าใจต่อคำศัพท์เหล่านี้เสียก่อน โดยคำศัพท์เหล่านี้ถูกเรียกและมีการใช้ เมื่อไม่นานหลังจากที่เทคโนโลยีสารสนเทศเข้ามาสู่โครงสร้างพื้นฐานในการใช้ชีวิตของทุกคนบนโลก เช่น การนำไปสู่การเปลี่ยนแปลงโครงสร้างทางเศรษฐกิจ สังคม และวัฒนธรรม เทคโนโลยีสารสนเทศถูกพัฒนาไปอย่างรวดเร็ว จนถึงขนาดที่ก้าวข้ามข้อจำกัดของเวลา และข้อจำกัดในเรื่องการสร้างความสัมพันธ์ของผู้คนในต่างสถานที่

ในสภาวะของสังคมขณะนี้ สมาร์ทโฟน (Smart Phone) ถือได้ว่ากลายเป็นอวัยวะที่ 33 ของร่างกาย สื่อสังคมออนไลน์เข้ามาเป็นส่วนหนึ่งของชีวิตประจำวัน ผู้คนจำนวนมากต่างให้ความสนใจและให้ความสำคัญต่อโลกออนไลน์เป็นอย่างมาก จากบทความของ David Ludden[2] พบว่า ผู้คนส่วนใหญ่หันเข้าสู่โลกออนไลน์มากกว่าแทนที่จะออกไปมีปฏิสัมพันธ์กับผู้อื่น และเลือกที่จะสื่อสารกันผ่านสื่อออนไลน์มากกว่า เพราะพวกเขาสามารถระบายหรือได้พูดคุยกับคนที่ไม่รู้จักตัวตนของพวกเขาเลย และนั่นทำให้พวกเขารู้สึกปลอดภัยกว่า สำนักงานสถิติแห่งชาติ ได้ระบุถึงผลการสำรวจประชากรอายุ 6 ปีขึ้นไปประมาณ 63.3 ล้านคนพบว่ามีผู้ใช้คอมพิวเตอร์ 17.9 ล้านคน (ร้อยละ 28.3) ผู้ใช้อินเตอร์เน็ต 36.0 ล้านคน (ร้อยละ 56.8) และผู้ใช้โทรศัพท์มือถือ 56.7 ล้านคน (ร้อยละ 89.6) เมื่อพิจารณาแนวโน้มการใช้อินเตอร์เน็ต ระหว่างปี 2557-2561 พบว่าผู้ใช้อินเตอร์เน็ตเพิ่มขึ้นจากร้อยละ 34.9 (จำนวน 21.8 ล้านคน) เป็นร้อยละ 56.8 (จำนวน 36.0 ล้านคน) สำหรับอุปกรณ์ในการเข้าถึงอินเตอร์เน็ตพบว่าผู้ใช้อินเตอร์เน็ตใช้โทรศัพท์มือถือแบบ Smart Phoneในการเข้าถึงอินเตอร์เน็ตค่อนข้างสูงคือ ร้อยละ 94.7 ใช้ PC ร้อยละ 38.8 ใช้ Notebook ร้อยละ 16.6 และ Tablet ร้อยละ 6.9[3] นอกจากนั้นยังมีรายงานจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้ระบุถึงผลสำรวจพฤติกรรมผู้ใช้งานอินเตอร์เน็ตประเทศไทยปี พ.ศ. 2561 พบว่าคนไทยใช้อินเตอร์เน็ตเฉลี่ยนานขึ้นเป็น 10 ชั่วโมง 5 นาทีต่อวัน เพิ่มขึ้นจากปีก่อน 3 ชั่วโมง 41 นาทีต่อวัน นอกจากนี้คนไทยยังนิยมใช้โซเชียลมีเดีย อาทิ Facebook, Instagram, Twitter และ Pantip สูงมากถึง 3 ชม. 30 นาทีต่อวัน ขณะที่การรับชมวีดีโอสตรีมมิ่ง เช่น YouTube หรือ Line TV มีชั่วโมงการใช้งานเฉลี่ยอยู่ที่ 2 ชม. 35 นาทีต่อวัน ส่วนการใช้แอปพลิเคชันเพื่อพูดคุย เช่น Messenger และ LINE เฉลี่ยอยู่ที่ 2 ชม. ต่อวัน การเล่นเกมออนไลน์อยู่ที่ 1 ชม. 51 นาทีต่อวัน และการอ่านบทความหรือหนังสือทางออนไลน์อยู่ที่ 1 ชม. 31 นาทีต่อวัน เมื่อดูการเปลี่ยนผ่านการใช้ชีวิตประจำวันไปสู่ชีวิตดิจิทัลจะเห็นได้ว่ามีผู้ใช้อินเตอร์เน็ตเพื่อการติดต่อสื่อสารผ่านทางออนไลน์มากกว่าแบบดั้งเดิมเป็นอันดับต้นๆ ของกิจกรรมออนไลน์หลายประเภท เช่น การส่งข้อความ ร้อยละ 94.5 การชำระค่าสินค้าและบริการ ร้อยละ 82.8 ใช้พูดคุย/อินเตอร์เน็ต ร้อยละ 68.4 ซื้อสินค้าและบริการ ร้อยละ 49.6 เป็นต้น[4] ด้วยจำนวนของผู้คนที่

---

[2] Ludden, D., (2018), *Does Using Social Media Make You Lonely?,* (26 พฤศจิกายน 2561), สืบค้นจาก Psychology Today: https://www.psychologytoday.com/intl/blog/talking-apes/201801/does-using-social-media-make-you-lonely

[3] สำนักงานสถิติแห่งชาติ, (2561), *การสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2561 (ไตรมาส 1),* กรุงเทพฯ: สำนักงานสถิติแห่งชาติ.

[4] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), (2561), *Thailand Internet User Profile 2018 ผลสำรวจพฤติกรรมการใช้อินเทอร์เน็ตของคนไทยประจำปี 2561,* กรุงเทพฯ: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน).

ให้ความสำคัญกับโลกออนไลน์ ปัจจุบันนี้ไม่เพียงเครือข่ายเน็ตเวิร์คเท่านั้น ที่พัฒนาต่อไปอย่างไม่สิ้นสุด แอปพลิเคชันต่างๆ ก็ถูกพัฒนาให้ทันยุค ทันสมัย ตอบสนองต่อความต้องการของผู้ใช้งานหลายล้านคนได้ อย่างเช่น เฟซบุ๊ค (Facebook) สื่อสังคมออนไลน์ที่มีผู้ใช้งานมากถึง 2,234 ล้านคน[5] ซึ่งก็ถูกพัฒนาขึ้นเพื่อสร้างเครือข่ายสังคมออนไลน์ ทำให้ผู้ใช้งานสามารถพบเจอผู้คนที่รู้จัก หรือ การสร้างกลุ่มของคนที่มีความคิด ความชอบที่เหมือนหรือคล้ายกัน ให้เข้ามาพบเจอกัน โดยจะเป็นการเน้นการสร้างชุมชน หรือ Community บนโลกออนไลน์ หรือแอปพลิเคชันอีกตัวหนึ่งที่ได้รับความนิยมไม่น้อยไปกว่ากัน อย่างทวิสเตอร์ (Twitter) เป็นแพลตฟอร์มในรูปแบบ Look at This คือ การที่ผู้ใช้งานเลือกที่จะเห็นว่าตนเองอยากเห็นอะไร สนใจเนื้อหา (Content) ในเรื่องใด ก็จะติดตามหรือเลือกที่จะเห็นเนื้อหาที่ตนสนใจ เพราะฉะนั้นเมื่อมีการแจ้งเตือนเนื้อหาที่ตนเองสนใจขึ้นมา เราก็สามารถเข้าไปดูเนื้อหาที่ตรงกับความสนใจของเราได้มากกว่า สังคมบนทวิสเตอร์จึงเป็นกลุ่มที่มีความสนใจและความคิดเห็นที่คล้ายๆกัน รวมอยู่ด้วยกัน[6]

ยิ่งไปกว่านั้น ยังมีการสร้างแอปพลิเคชันที่ตอบสนองต่อความต้องการของผู้ใช้งานที่ต้องการหาคู่ หาเพื่อนทานข้าว หรือหาเพื่อนเที่ยวด้วย อย่างเช่น Tinder และ YOUEX ก็ถูกสร้างและพัฒนาขึ้นเพื่อตอบสนองความต้องการของผู้ใช้งานกลุ่มหนึ่งที่รู้สึกเหงาและต้องการหาเพื่อน โดยทางแอปพลิเคชัน YOUEX[7] คือการบริการสำหรับคนเหงาและผู้ที่ต้องการหาเพื่อนทานข้าว ดูหนัง หรือ ช้อปปิ้ง ทางผู้พัฒนาแอพฯ ประกาศจุดยืนชัดเจนว่าไม่อนุญาตให้ผู้ใช้บริการและผู้รับจ้างงานแฝงไปด้วยการค้าประเวณี ซึ่งแอพฯดังกล่าวกลายเป็นกระแสเรียกเสียงฮือฮากันอย่างมาก แต่ถึงอย่างไร ความนิยมของผู้ใช้งานต่อแอปพลิเคชันดังกล่าวก็ยังไม่สูงเท่ากับแอปพลิเคชันที่ใช้ในการหาคู่ ไม่ว่าจะเป็น Tinder , OkCupid Japan , JapanCupid เป็นต้น โดย Tinder เป็นแอพฯที่จะทำการแมตช์คู่ให้กับผู้ใช้งาน ซึ่งผู้ใช้งานอาจจะต้องกรอกข้อมูลส่วนตัวบ้าง เพื่อที่จะให้ระบบหรืออัลกอริทึมสามารถจะจับคู่กับบุคคลอื่นๆ ได้ และยังสามารถให้ผู้ใช้งานสามารถเลือกคนที่ตนเองชอบหรือถูกใจได้ด้วยการปัดซ้าย หรือปัดขวา ตามที่ผู้ใช้งานต้องการ หลังจากนั้นเมื่อผู้ใช้งานจับคู่ได้กับผู้ใช้งานคนอื่นๆ ก็จะมีการสนทนา พูดคุยกับเกิดขึ้น เพื่อสานความสัมพันธ์กันต่อไป [8]

แต่ด้วยความที่เทคโนโลยีถูกพัฒนาออกมาเพื่อความสะดวก สบายของผู้ใช้งานได้เป็นอย่างดีนั้น ทำให้เราสื่อสารผ่านตัวอักษรกันมากขึ้น แต่กลับพบว่า การพบปะสังสรรค์กันน้อยลง เราให้ความสำคัญกับความสัมพันธ์ภายในโลกออนไลน์ เมื่อความรู้สึก หรือความต้องการที่ยึดติดและให้ความสำคัญกับโลกออนไลน์ที่มากขึ้นของคน ไม่เพียงความรักที่ต้องตามหากันในโลกออนไลน์ คนที่รู้สึก

---

[5] Arjin, (2561), *Facebook ไตรมาสล่าสุด รายได้โต 11% ผู้ใช้ในยุโรปลดลงเป็นครั้งแรก ราคาหุ้นร่วง 20%,* (28 พฤศจิกายน 2561), สืบค้นจาก Blogone: https://www.blognone.com/node/104131

[6] Ratirita, (2561), *ถอดรหัส! ทำไม Twitter ถึงโตอย่างรวดเร็วในประเทศไทย?*, (26 พฤศจิกายน 2561), สืบค้นจาก Brandinside: https://brandinside.asia/twitter-growth-in-thailand/

[7] ปณชัย อารีเพิ่มพร, (2561), YOUEX แอปฯ จ้างเพื่อนเที่ยว จ้างกินข้าวของประเทศไทย กับแนวโน้มกระแสนิยมธุรกิจจัดหาคู่ในปัจจุบัน, (20 พฤศจิกายน 2561), สืบค้นจาก The standard: https://thestandard.co/youexapp/

[8] Tinder, (ม.ป.ป.), *Tinder คืออะไร,* (28 พฤศจิกายน 2561), สืบค้นจาก Tinder: https://www.help.tinder.com/hc/th/articles/115004647686-Tinder-คืออะไร-

เหงา หรือคนที่เปล่าเปลี่ยวใจ ก็หันหน้าเข้าสู่โลกออนไลน์ผ่านแพลตฟอร์มต่างๆ ที่จะช่วยให้เราได้มีความสัมพันธ์กับคนใหม่ๆมากหน้าหลายตามากขึ้น[9]

ผู้คนส่วนใหญ่ใช้ชีวิตประจำวันไปกับโลกออนไลน์ กลายเป็นช่องโหว่ที่สำคัญอย่างมาก ที่จะทำให้ผู้ใช้งานตกเป็นเหยื่อ หรืออยู่ในอันตรายจากอาชญากรรมทางคอมพิวเตอร์ พฤติกรรมที่มักจะเห็นอยู่เป็นประจำกลายเป็นการสร้างความเสี่ยงต่อการถูกหลอกลวงโดยไม่รู้ตัว เพราะคนส่วนใหญ่มักจะโพสข้อความที่แสดงความรู้สึกต่าง ๆ ผ่านพื้นที่ออนไลน์ของตน รวมถึงรูปภาพการไปเที่ยว อาหารการกิน จนถึงไปชีวิตประจำวันในแต่ละวันของตน หรือการเปิดเผยข้อมูลส่วนตัวในพื้นที่ออนไลน์นั้น ซึ่งนั่นเป็นข้อมูลที่กลายเป็นสิ่งที่ย้อนกลับไปทำร้ายตัวเรา

ในโลกออนไลน์มีพฤติกรรมมากมายที่ถูกระบุไว้ว่าเป็นอาชญากรรมทางคอมพิวเตอร์ ไม่ว่าจะเป็นการดักจับข้อมูล การเข้าถึงข้อมูล หรือ ระบบคอมพิวเตอร์โดยมิชอบ และ Scammer ถือเป็นผู้ที่กระทำความผิดประเภทหนึ่งในอาชญากรรมทางคอมพิวเตอร์ โดยอาชญากรรมทางคอมพิวเตอร์เป็นภัยคุกคามทางเทคโนโลยีสารสนเทศที่สร้างความเสียหายทั้งต่อผู้ใช้งานส่วนบุคคลและเครือข่ายสังคมในวงกว้าง ซึ่งก็มีรูปแบบที่แตกต่างกันไป แต่มีผลกระทบร่วมกัน คือ สร้างความไม่ไว้วางใจต่อเทคโนโลยีให้กับผู้ใช้อินเตอร์เน็ตจนเกิดผลกระทบต่อผู้ประกอบการเว็บไซต์หาคู่ หรือเครือข่ายสังคมออนไลน์

โดยทั่วไปพิศวาสอาชญากรรม “Romance Scam” หรือ “การลวงรัก” คือ การที่นักต้มตุ๋น (Scammer) ได้ใช้เทคนิคทางจิตวิทยาผ่านเครื่องมือทางเทคโนโลยีต่าง ๆ ในการหลอกลวงให้เหยื่อ (Victim) หลงเชื่อจนกระทั่งยินยอมให้สิ่งต่างๆ ที่นักต้มตุ๋นต้องการ[10] ซึ่งวิธีการที่นักต้มตุ๋นมักใช้หลอกลวง คือ การสร้างโปรไฟล์ปลอมๆ ขึ้นมาในโซเชียล เช่น Facebook หรือเว็บไซต์หาคู่ต่างๆ (Dating Website/App) ซึ่งข้อมูลที่นำมาใช้ทำโปรไฟล์เหล่านี้ก็นำมาจากการขโมยข้อมูลเช่นกัน เช่น ชื่อ ประวัติ และรูปภาพของคนอื่น แล้วเอามาดัดแปลงเป็นข้อมูลของตนเอง หรืออีกวิธีหนึ่ง คือ จะสร้างข้อมูลปลอมๆ ขึ้นมาเองให้ดูสมจริงและน่าดึงดูดที่สุด โดยเหยื่อที่นักต้มตุ๋นเหล่านี้มองหา มักจะมีคุณสมบัติหนึ่งที่สำคัญคือ ต้องเป็นคนขี้เหงา และเป็นคนอ่อนไหว ต้องการใครสักคนมาอยู่เคียงข้าง[11]

ซึ่งก็สอดคล้องกับสังคมในปัจจุบัน ที่มักจะอยู่ในความรักแบบฉาบฉวย พูดคุยกับเพียงผิวเผิน รู้จักกันเพียงรูปโปรไฟล์ และข้อความแนะนำตัวเพียงสอง-สามประโยค และก็ตัดสินใจที่จะสานความสัมพันธ์ต่อในระยะเวลาที่รวดเร็ว[12] โดยนักต้มตุ๋นมักจะทำให้ตนเองดูน่าสนใจ ซึ่งจะทำให้สามารถสานความสัมพันธ์กับเหยื่อได้เร็วขึ้น เมื่อนักต้มตุ๋นเข้ามาเป็นเพื่อนในโซเชียลกับเหยื่อแล้วนั้น จะเข้ามาพูดคุยสร้างความสนิทสนมและอ้างว่าตนมีอาชีพการงานที่ดี เช่น วิศวกร นายทหารยศสูง เจ้าของบริษัท ซึ่งคำถามที่นักต้มตุ๋นมักจะถามเหยื่อก่อน คือ อายุเท่าไหร่ มีอาชีพอะไร และเหยื่อที่ตก

---

[9] พชรพล เกตุจินากูล, (2560), *งานวิจัยชี้การเล่นโซเชียลมีเดียมากเกินไป อาจเป็นสาเหตุของความรู้สึกโดเดี่ยว*, (24 พฤศจิกายน 2561), สืบค้นจาก Themomentum: https://themomentum.co/happy-self-help-use-social-media-more-cause-lonely/

[10] วชิรวิทย์ คงคาลัย, (2560), *“Romance Scam: ไม่รักไม่ว่าอะไร แต่ไยต้องหลอกกันด้วย”*, (25 พฤศจิกายน 2561), สืบค้นจาก The101.world: https://www.the101.world/romance-scam/

[11] เรื่องเดียวกัน

[12] ชลิตา สุนันทาภรณ์, (2560), *MODERN ROMANCE: ถอดรหัสรักออนไลน์ สุดท้ายความรักก็เป็นเรื่องของคนสองคน*, (20 พฤศจิกายน 2561), สืบค้นจาก Way magazine: https://waymagazine.org/modern-romance-waytoread/

เป็นเป้าหมาย คือ หญิงไทย วัยกลางคน มีอาชีพการงานที่ดี และส่วนใหญ่มีสถานะภาพโสด หย่าร้าง หรือสมรส (แล้วแต่กรณี) บวกกับค่านิยมของผู้หญิงไทยบางกลุ่มที่อยากมีสามีต่างชาติ จึงเป็นสิ่งที่ช่วยให้นักต้มตุ๋นหลอกลวงเหยื่อได้อย่างง่ายดาย[13]

โดยพฤติกรรมที่ใช้หลอกลวงทางอินเตอร์เน็ตมีหลากหลายรูปแบบ อย่างเช่น การหลอกเหยื่อว่าจะส่งของมาให้ โดยนักต้มตุ๋นจะใช้ความไว้เนื้อเชื่อใจของเหยื่อ จากการที่พูดคุยกันมาในระยะเวลาหนึ่ง และมั่นใจว่าเหยื่อให้ความไว้ใจ หรือให้ความสนิทสนมกับตนแล้ว โดยในกรณีนี้จะอ้างว่ามีความรู้สึกดีกับเหยื่อ และอยากมาสร้างครอบครัวอยู่ที่ประเทศไทย แต่ก่อนที่จะมา จะส่งของมาให้พร้อมเงินอีกจำนวนหนึ่ง ซึ่งอาจจะขอให้เหยื่อช่วยหาที่พักอาศัยให้ และหลังจากนั้นเมื่อเหยื่อตกลง ก็จะมีคนที่อ้างว่าเป็นเจ้าหน้าที่จากบริษัทขนส่ง แจ้งกับเหยื่อว่า พัสดุถูกส่งมาแล้ว แต่ต้องมีการชำระค่าธรรมเนียมก่อน และมีการหลอกให้เหยื่อโอนเงินให้หลายครั้ง ซึ่งกว่าเหยื่อจะรู้ว่าตัวเองโดนหลอกก็ใช้เวลานานพอสมควร และกลุ่มนักต้มตุ๋นเองก็สามารถหลบหนีไปได้ทัน[14]

หรือบางกรณี หลอกลวงเรื่องการจัดหางาน ซึ่งกรณีนี้นักต้มตุ๋นจะไปเอาข้อมูลของเหยื่อจากการที่เหยื่อไปลงชื่อสมัครงานไว้ในหลายๆ ที่ นักต้มตุ๋นจะเป็นคนทำหน้าที่ชักชวนเหยื่อไปทำงานที่ต่างประเทศ โดยอ้างว่าได้ข้อมูลการสมัครงานมาจากเว็บไซต์จัดหางาน โดยจะแจ้งรายละเอียดว่าต้องการคนไปทำงานที่ต่างประเทศ จำนวน 20 คน เมื่อเหยื่อสนใจที่จะไปทำงาน นักต้มตุ๋นจะให้เหยื่อไปติดต่อกับคนไทยอีกคนหนึ่ง ซึ่งก็เป็นหนึ่งในกลุ่มนักต้มตุ๋นเช่นกัน โดยจะให้ไปติดต่อในเรื่องเอกสารในการขอวีซ่า หลังจากนั้นก็ทำการเรียกเก็บเงินค่ายื่นขอวีซ่าคนละประมาณ 40,000 บาท โดยให้โอนผ่านบัญชีธนาคารหนึ่ง หลังจากนั้นก็จะเรียกเก็บค่าตั๋วเดินทาง ค่าเปิดบัญชีที่ต่างประเทศ ค่าดำเนินเรื่องให้ผ่าน ตม. เข้าประเทศ รวมถึงค่าธรรมเนียมอื่นๆ ด้วย[15]

การหลอกลวงแบบ Romance Scam เกิดขึ้นมาก่อนแล้วในต่างประเทศ จากรายงานของศูนย์ต่อต้านการฉ้อโกงประเทศแคนาดา (The Canadian Anti-Fraud Centre)[16] พบว่า การร้องเรียนเรื่อง romance scam เพิ่มขึ้นอย่างรวดเร็วตั้งแต่ปี 2008 โดยมีอัตราเพิ่มขึ้น 1,500% และมีค่าเสียหายเฉลี่ยคนละ 11,000 ดอลลาร์แคนาดา ในปี 2010 The International Mass Marketing Fraud Working Group[17] รายงานว่า romance scam กลายเป็นภัยคุกคามทั่วโลกซึ่งจากเดิมเป็นปัญหาแค่ในอเมริกาเหนือ จากรวบรวมสถิติของ The FBI's Internet Crime Complaint Center (IC3)[18] ในสหรัฐฯ ตั้งแต่ปี 2011-2014 พบว่า ผู้ที่ตกเป็นเหยื่อหลอกลวงรัก (romance scam) มีอายุเฉลี่ย 40-60 ปี มักเป็น

---

[13] ปัทมาภรณ์ กฤษณายุทธ ศิริวัชรไพบูลย์, *พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านอินเตอร์เน็ต,* (20 พฤศจิกายน 2561), สืบค้นจาก URL: https://www.dsi.go.th/Files/20150123/F20150123160326-scammer-dsi-warning.pdf

[14] เรื่องเดียวกัน.

[15] เรื่องเดียวกัน.

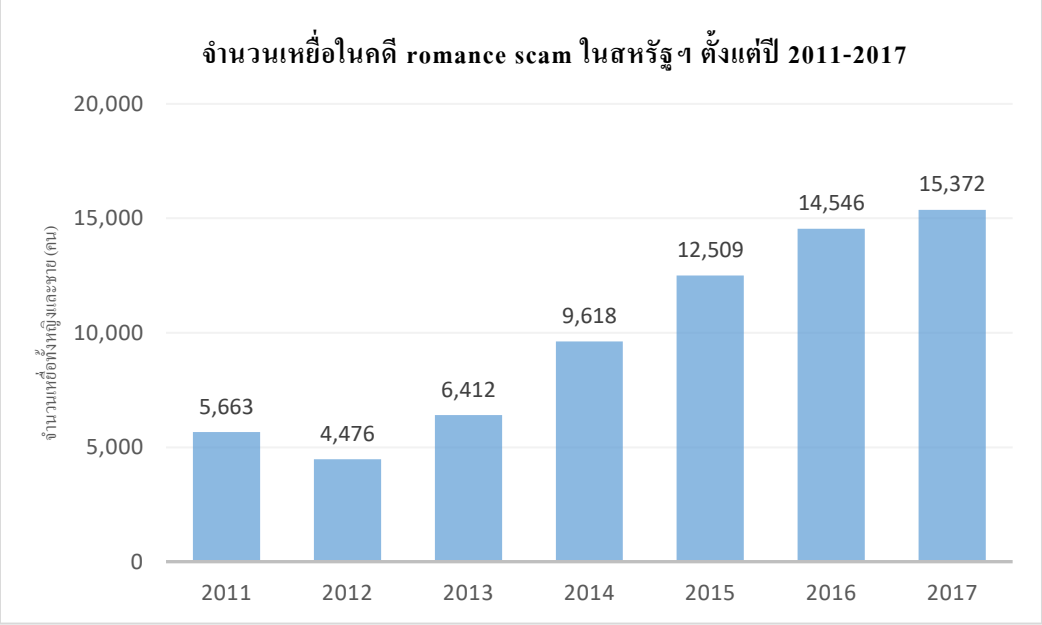
[16] La Rose, L., (2011, October 6), Online romance scam can hurt hearts and wallets. *The Canadian Press*. Retrieved 5 March 2013, สืบค้นจาก http://www.thestar.com/life/2011/10/06/online_romance_scams_can_hurt_hearts_and_wallets.html

[17] "Mass-Marketing Fraud: A Treat Assessment," Int'l Mass-Marketing Fraud Working Group, 2010; สืบค้นจาก www.ice.gov/doclib/cornerstone/pdf/immfa.pdf

[18] Internet Crime Complaint Center, (n.d), "Annual Reports 2011-2014 Internet Crime Report", สืบค้นจาก https://www.ic3.gov/default.aspx

คนที่หย่าร้าง ม่าย คนพิการ และบ่อยครั้งที่เป็นคนแก่ ซึ่งโดยส่วนใหญ่เป็นผู้หญิง นอกจากนั้นในปี 2012 คณะกรรมการการแข่งขันและผู้บริโภคของออสเตรเลีย (the Australian Competition and Consumer Commission (ACCC))[19] รายงานว่ามีผู้ที่ตกเป็นเหยื่อของ romance scam ทั้งสิ้น 2,110 คน และสูญเงินไปเกือบ 20.9 ล้านดอลลาร์ออสเตรเลีย และในปีเดียวกันมีรายงานของตำรวจมาเลเซีย (The Royal Malaysian Police (RMP)) ว่าได้รับการร้องเรียนจากเหยื่อสูงถึง 846 คนในเวลาเพียงหนึ่งปี และพบมูลค่าความเสียหายถึง 32.09 ล้านริงกิต เช่นเดียวกันกับ สหราชอาณาจักร พบว่าประมาณ 500,000 คนตกเป็นเหยื่อของ romance scam[20] และมีเพียง 10% เท่านั้นที่มีการแจ้งความ ส่วนหนึ่งเป็นเพราะอับอายและลำบากใจเมื่อทราบว่าตนเองตกเป็นเหยื่อของการหลอกลวงนี้ อีกทั้งยังขาดความรู้เกี่ยวกับขั้นตอน และสถานที่ของการแจ้งความเมื่อถูกหลอกลวง และเข้าใจว่าการแจ้งความไม่ได้เกิดประโยชน์อะไรเพราะไม่น่าจะดำเนินคดีกับอาชญากรได้

ข้อมูลสถิติ (รูปภาพที่1) แสดงให้เห็นว่า จำนวนเหยื่อที่คดี Romance Scam มีจำนวนสูงมากขึ้นเรื่อยๆ ในปี 2011 มีจำนวนมากถึง 5,663 คน แม้ว่าในปี 2012 มีจำนวนที่ลดลงมา แต่เพียง 1,187 ราย แต่เมื่อดูสถิติในปีถัดมาจำนวนตัวเลขของผู้ตกเป็นเหยื่อได้เพิ่มสูงขึ้นเรื่อยๆ และไม่มีท่าทีว่าจะลดต่ำลงมาแต่อย่างใด จนกระทั่งในปี 2017 พบว่าจำนวนเหยื่อสูงถึง 15,372 ราย ทั้งนี้ข้อมูลสถิติดังกล่าวก็ยังไม่รวมจำนวนของเหยื่อที่ไม่เข้ามาแจ้งความ ดำเนินคดีกับเจ้าหน้าที่ตำรวจด้วย ซึ่งก็สามารถคาดการณ์ได้ว่ายังมีอีกจำนวนมากอย่างแน่นอน



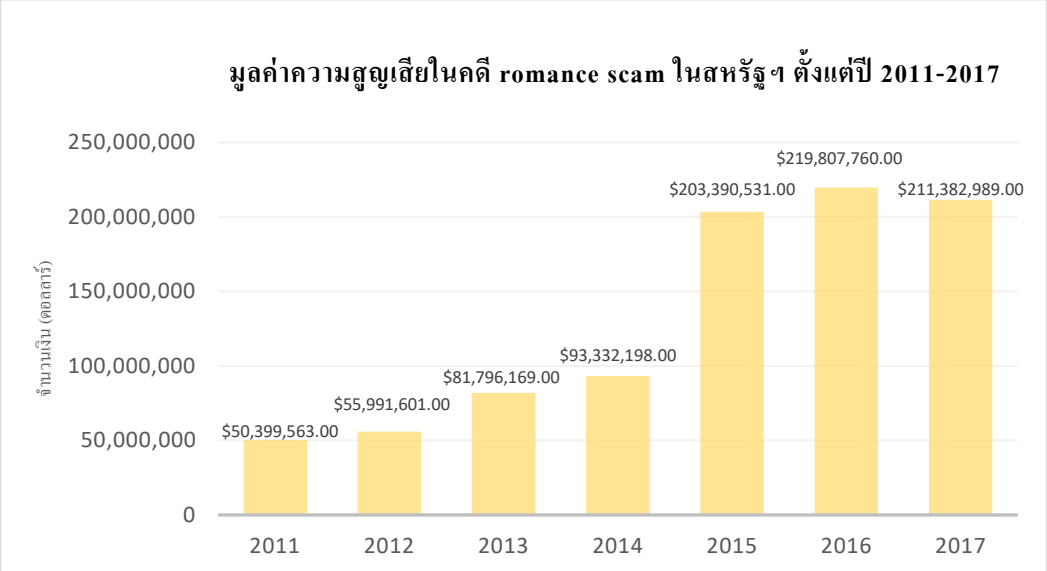
ภาพที่ 1 จำนวนเหยื่อในคดี Romance Scam ในสหรัฐฯ

ที่มา: Annual Reports : 2011-2017 Internet Crime Report form The FBI's Internet Crime Complaint Center (IC3).

[19] Australian Competition and Consumer Commission (ACCC), (2011), Dating and romance scams: Defining the harm. Australia: ACCC.

[20] Internet Crime Complaint Center, (2014), "2014 Internet Crime Report," Annual Reports, Internet Crime Complaint Center.

มูลค่าความเสียหายของคดี Romance Scam (ภาพที่ 2) แม้ในปี 2012 ที่จำนวนเหยื่อลดลงบ้างจากปี 2011 แต่เมื่อพิจารณามูลค่าความเสียหายแล้ว กลับไม่เป็นไปในทิศทางเดียวกันคือ มีมูลค่าความเสียหายที่เพิ่มขึ้นสูงกว่าปี 2011 อย่างมาก และความเสียหายได้พุ่งทะยานขึ้นสูงไปถึง 219,807,760 ล้านดอลลาร์สหรัฐ ในปี 2016 จึงเป็นการแสดงให้เห็นอย่างชัดเจนว่าคดีดังกล่าวมีความเป็นภัยอันตรายอย่างมากต่อผู้ใช้งานอินเตอร์เน็ตในปัจจุบัน



ภาพที่ 2 มูลค่าความเสียหายในคดี Romance Scam ในสหรัฐฯ

ที่มา: Annual Reports : 2011-2017 Internet Crime Report form The FBI's Internet Crime Complaint Center (IC3).

ส่วนในประเทศไทยนั้น ข้อมูลจาก พ.ต.อ. ภาณุวัฒน์ ร่วมรักษ์ รองผู้บังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (TCSD) ได้เปิดเผยว่าในปี 2558 ที่ผ่านมา เฉพาะคดีเกี่ยวกับ Romance Scam ถูกร้องเรียนเข้ามาถึง 80 คดี มูลค่าความเสียหายสูงถึง 150 ล้านบาท ยังไม่นับคดีที่ถูกร้องเรียนไปยังสถานีตำรวจท้องที่และเหยื่อที่ไม่กล้าเข้าแจ้งความอีกเป็นจำนวนมาก และทาง พ.ต.อ.ภานุวัฒน์ ร่วมรักษ์ ยังเปิดเผยอีกว่า ผู้ที่ตกเป็นเหยื่อส่วนมากมักจะเป็น หญิงไทยโสด อายุ 40-60 ปี การศึกษาดี หน้าที่การงานมั่นคง ที่สำคัญคือ "มีเงิน" ที่น่าตกใจที่สุดคือ ที่ผ่านมาพบเหยื่อที่สูญเสียมากสุดอยู่ที่ 33 ล้านบาท โดยโดนหลอกโอนเงินไปให้นักต้มตุ๋นถึง 26 ครั้ง ภายในเวลาสองปี ทั้งที่ไม่เคยพบเจอหน้ากันเลยแม้แต่ครั้งเดียว บางคนถูกนักต้มตุ๋นใช้จิตวิทยาหว่านล้อมตนหลงเชื่อ โดนหลอกให้โอนเงินไปมากกว่า 83 ครั้ง รวมเป็นเงิน 13 ล้านบาท[21]

[21] Rabbit finance Magazine, (2561), *Romance Scam หลอกรักออนไลน์ ภัยร้ายของสาวโสด!,* (25 พฤศจิกายน 2561), สืบค้นจาก Rabbit finance Magazine: https://finance.rabbit.co.th/blog/romance-scam-and-single-ladies.

ในปี 2559 ทางตำรวจท่องเที่ยว เข้าจับกุมนักต้มตุ๋ม ที่อ้างตนว่าเป็นฝรั่งผิวขาว โดยผู้ต้องหาทั้งหมดเป็นคนผิวสี สัญชาติแอฟริกา ไนจีเรีย, โมซัมบิก และ กานา ซึ่งการกระทำความผิดของผู้ต้องหากลุ่มนี้ คือ จะใช้แอปพลิเคชัน Facebook เข้าไปพูดคุยกับหญิงไทย จากนั้นจะหลอกให้โอนเงินเข้าบัญชีซึ่งไปจ้างคนไทยเปิดบัญชีไว้ แต่บัตรเอทีเอ็มอยู่ที่กลุ่มผู้ต้องหา โดยจะหลอกว่าได้ซื้อของหมั้นมาให้ แต่ติดขั้นตอนที่กรมศุลกากรให้โอนเงินมาที่บัญชีนี้ เมื่อโอนเงินแล้วเสร็จ กลุ่มผู้ต้องหาจะรีบกดเงินแล้วตัดขาดการติดต่อจากหญิงไทยไป โดยของกลางที่พบแสดงให้เห็นบัญชีไหลเวียนมากกว่าล้านบาทในระยะเวลาเพียงแค่ 3 เดือน ทั้ง ๆ ที่กลุ่มผู้ต้องหาไม่มีงานทำเป็นหลักแหล่งแต่อย่างใด[22]

ต่อมาในปี 2560 ตำรวจ (ศูนย์หมายจับคนร้ายข้ามชาติ: สำนักงานตำรวจตรวจคนเข้าเมือง - สตม.) ได้จับผู้ต้องหาชาวแอฟริกัน ที่มีความเชื่อมโยงกับขบวนการค้ายาเสพติดข้ามชาติ ด้วยการสวมรอยว่าเป็นทหารอเมริกัน หลอกผู้อำนวยการ และ รองผู้อำนวยการโรงเรียนชื่อดังแห่งหนึ่ง ซึ่งอ้างว่าจะบริจาคทุนการศึกษาเด็ก มีผู้เสียหายตกเป็นเหยื่อกว่า 20 ราย และเสียหายกว่าสิบล้านบาท[23] โดยผู้เสียหายรายที่หนึ่งและที่สอง (ผอ. และรอง ผอ.) ถูกหลอกลวงโดยเริ่มจากผู้ต้องหาเข้ามาทักใน Facebook แล้วอ้างว่าเป็นทหารหญิงในกองทัพสหรัฐ ฝ่ายผู้เสียหายเห็นว่าเป็นโอกาสดีที่จะได้ฝึกภาษาและมีเพื่อชาวจ่างชาติ จึงได้ติดต่อกันเรื่อยมา โดยไม่เคยพบตัวจริงหรือสนทนาทางโทรศัพท์ เมื่อติดต่อกันได้ระยะหนึ่ง ผู้ต้องหาอ้างว่าจะไปทำงานในพื้นที่สงครามในตะวันออกกลาง มีเงินที่ทางรัฐบาลสหรัฐฯ ส่งมาให้กองทัพในพื้นที่จำนวนหลายล้านดอลลาร์ และถูกฝ่ายตรงข้ามปล้นเงินไป แต่ต่อมากลุ่มทหารอเมริกันได้ยึดคืนมาได้ แต่ไม่ได้รายงานรัฐบาลและได้นำมาแบ่งกัน ผู้ต้องหาอ้างว่าตนได้รับส่วนแบ่งมาจำนวน 1 ล้านดอลลาร์ มีความประสงค์จะบริจาคเงินเพื่อเป็นทุนการศึกษาแก่เด็กไทย โดยจะส่งเงินใส่กระเป๋าผ่านบริษัทขนส่งข้ามประเทศ แล้วให้ผู้เสียหายรอรับ หลังจากนั้นนักต้มตุ๋นก็ดำเนินการตามแผนการของตน โดยได้ส่งคนไทยที่อ้างว่าเป็นเจ้าหน้าที่บริษัทขนส่ง แจ้งว่าเงินจำนวนดังกล่าวได้ส่งมาถึงแล้ว แต่ติดปัญหาที่ผู้รับปลายทางจะต้องชำระค่าธรรมเนียมจำนวนหนึ่งเสียก่อน ผู้เสียหายได้หลงเชื่อ จึงได้โอนเงินไปให้หลายครั้ง จนกระทั่งรู้ว่าตนถูกหลอกและตกเป็นเหยื่อ จึงได้ขอความช่วยเหลือมาที่ สตม. ทางด้านผู้เสียหายรายที่สาม เป็นหญิงไทย ได้ให้ข้อมูลว่า เมื่อเดือนมิถุนายน มีชายชาวอเมริกัน หน้าตาดี ติดต่อตนมาทาง Facebook อ้างว่าเป็นนายทหารยศนายพล ปฏิบัติหน้าที่อยู่ในประเทศอัฟกานิสถาน ภรรยาเสียแล้ว และตนอยากตั้งครอบครัวใหม่ที่ประเทศไทย พร้อมอ้างว่ามีเงินและของมีค่าที่ยึดได้จากสงครามมูลค่ากว่า 500,000 ดอลลาร์สหรัฐฯ จะส่งมาให้ผู้เสียหายเก็บรักษาไว้ เมื่อหมดภารกิจแล้วจะเดินทางมาแต่งงานกับผู้เสียหายที่ประเทศไทย และบอกว่าจะมีนักการทูตนำกระเป๋าใบนี้ไปส่งให้ ผู้เสียหายรายดังกล่าวนี้หลงเชื่อจึงรับดำเนินการ โดยต่อมามีคนไทยอ้างว่าเป็นเจ้าหน้าที่สถานทูต เจ้าหน้าที่ศุลกากร และเจ้าหน้าที่บริษัทขนส่ง ติดต่อมายังผู้เสียหายให้ชำระค่าธรรมเนียมต่างๆ ซึ่งผู้เสียหายได้หลงเชื่อและโอนเงินไปให้หลายครั้ง มูลค่าความเสียหายกว่าหนึ่งล้านบาท นอกจากนี้ยังพบว่านักต้มตุ๋นดังกล่าวมีความเชื่อมโยงกับขบวนการค้ายาเสพติดข้ามชาติ และยังมีหมายจับในคดีความผิดเกี่ยวกับยาเสพติดอีกด้วย

[22] Voicetv, (2559), *จับแก๊ง "Romance Scam" หลอกหญิงไทยโอนเงินซื้อของหมั้น.* (27 พฤศจิกายน 2561), สืบค้นจาก Voicetv: https://www.voicetv.co.th/read/376101

[23] ไทยรัฐออนไลน์, (2560), *จับแก๊งแอฟริกันแสบ! แชตเฟซบุ๊คสวมรอยทหารมะกัน ตุ๋น ผอ. โรงเรียนดังโอนเงิน.* (20 พฤศจิกายน 2561), สืบค้นจาก https://www.thairath.co.th/content/1005807

ในปี 2561 ทางสำนักงานตำรวจได้ทลายเครือข่าย Romance Scam มากถึง 8 เครือข่าย มีความเสียหายมากกว่า 5 ล้านบาท จากการสืบสวนติดตามกลุ่มคนร้ายทั้งชาวไทยและชาวต่างชาติ มีการรวบรวมข้อมูลของกลุ่มคนร้าย ที่ร่วมกันหลอกลวงประชาชน ด้วยวิธีการแสดงตนเป็นบุคคลอื่น เพื่อให้เหยื่อหลงเชื่อ จากนั้นจึงร่วมกันหลอกลวงให้ผู้เสียหายโอนเงินเข้าบัญชีธนาคารต่างๆ ในลักษณะที่กลุ่มคนร้ายมีการแบ่งหน้าที่กันทำอย่างชัดเจน เพื่อให้เกิดความสะดวกในการกระทำความผิด และเพื่อให้ยากต่อการสืบสวนติดตามของเจ้าหน้าที่ตำรวจ เช่น ทำหน้าที่เปิดบัญชีธนาคาร, จัดหาบัญชีธนาคาร, ถอนเงินจากบัญชี, โทรศัพท์ไปหลอกลวง, เป็นคนพูดคุยกับเหยื่อผ่านทางเฟซบุ๊ค เป็นต้น โดยเครือข่ายทั้ง 8 กลุ่มที่ถูกจับกุมนั้นมีการแบ่งหน้าที่กัน อย่างเช่น เป็นคนกดเงิน อ.ศรีราชา จ. ชลบุรี, คนกดเงิน อ.เกาะสมุย จ. สุราษฎร์ธานี, คนกดเงิน ย่านรามอินทรา, คนทำหน้าที่ส่งข้อมูลเหยื่อให้กับเครือข่ายต่อไป[24]

การเก็บข้อมูลกรณี Romance Scams จากเพจในเครือข่ายเฟซบุ๊คที่เตือนภัยและให้คำปรึกษาแห่งหนึ่ง พบว่า ตั้งแต่ปี 2560-2561 ยังพบว่า ความเสียหายที่เกิดขึ้นจากกรณี Romance scams มีมูลค่าสูงถึง 20,965,851 บาท ซึ่ง Scammer จะหลอกลวงให้ผู้เสียหายโอนเงินเข้าบัญชีของคนไทยที่เปิดบัญชีไว้ (ทั้งที่เป็นเครือข่าย Scammer และ ถูกจ้างให้เปิดบัญชี) โดยบัญชีที่ถูกนำมาใช้เพื่อให้ผู้เสียหายโอนเงินไป จะเป็นบัญชีที่ใช้ชื่อของผู้หญิง (เรียกว่า “นางบัญชี”) 63.55% บัญชีที่ใช้ชื่อของผู้ชาย (เรียกว่า “นายบัญชี”) 35.16% และบัญชีอื่น เช่น บัญชีบริษัท 1.29% ทั้งนี้ บัญชีธนาคารที่ถูกนำมาใช้มากที่สุด คือ ธนาคารไทยพาณิชย์ 36.45% รองลงมาเป็นธนาคารกรุงเทพ 23.32% ธนาคารกสิกรไทย 14.52% และธนาคารทหารไทย 13.23% ตามลำดับ[25]

ในปีพ.ศ. 2561 ตามรายงานข้อมูลการเข้าร้องทุกข์ของ ศูนย์บริการประชาชน กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ประจำสัปดาห์ (วันที่ 10-16 มี.ค. 2561) พบว่ามีผู้มาเข้าร้องทุกข์ทั้งหมด 66 ราย ในบริบทนี้เป็นคดีหลอกเกี่ยวกับความรัก (romance scam) 3 ราย แต่คดีดังกล่าวมีมูลค่าความเสียหายสูงที่สุดจากจำนวนคดีทั้งหมด คิดเป็นจำนวนเงิน 7,699,500 บาท[26] และล่าสุดสถิติข้อมูลเมื่อวันที่ 21 มิถุนายน พ.ศ. 2561 ถึง 31 พฤษภาคม พ.ศ. 2562 มีผู้เสียหายหลงเชื่อและโอนเงิน จำนวน 332 ราย รวมมูลค่าความเสียหายประมาณ 193,015,902.11 บาท[27]

จากข้อมูลที่รวบรวมมาจากเอกสารต่างๆ การสัมภาษณ์ และฐานข้อมูลทั้งหลาย ล้วนสะท้อนให้เห็นแนวโน้มของการเกิดคดีพิศวาสอาชญากรรมที่ยังไม่มีทีท่าว่าจะลดลง และยังปรากฏเหยื่อรายใหม่ที่มีลักษณะกระจายไปในประชากรหลากหลายกลุ่มเพศสภาวะ รวมถึงมีแตกต่างสถานะทาง

---

[24] กองบัญชาการตำรวจท่องเที่ยว, (2561), *ทลายเครือข่าย Romance Scam ผู้ต้องหา 17 ราย 8 เครือข่าย ผู้เสียหาย 48 ราย ความเสียหายมากกว่า 5,961,740 บาท,* (20 พฤศจิกายน 2561) สืบค้นจาก touristpolice: https://touristpolice.go.th/2018/09/15/romancescam/

[25] ผู้ดูแลเพจ. เพจภัยผู้หญิง ในโลกออนไลน์. (17 มกราคม 2562). สัมภาษณ์. และประมวลผลจากข้อมูลที่ทางผู้ดูแลเพจรวบรวมข้อมูลดิบไว้

[26] รายงานประจำสัปดาห์ (วันที่ 10 มี.ค. 2561 – 16 มี.ค. 2561) ข้อมูลการเข้าร้องทุกข์ ณ ศูนย์บริการประชาชน กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)

[27] แนวหน้า, (31 พ.ค. 2562), *ปปง.เผยตั้งศปก.ปปง.1ปี พบเหยื่อคดีโรแมนซ์สแกน 332 ราย เสียหาย 193 ล้าน,* สืบค้นจาก https://www.naewna.com/local/417058

เศรษฐกิจและสังคมมากขึ้น ย่อมเป็นปรากฏการณ์ที่สะท้อนว่ายังจำเป็นที่ต้องเข้าใจลักษณะพื้นฐานของพิศวาสอาชญากรรมว่าเหตุใดจึงมีศักยภาพในการหลอกลวงผู้คนได้อย่างกว้างขวางและมหาศาลถึงเพียงนี้ โดยหัวข้อถัดไปจะจำแนกให้เห็นกลวิธีทั้งหลายที่เหล่าอาชญากรใช้หลอกลวงเหยื่อ

4.1.2 รูปแบบและวิธีการของพิศวาสอาชญากรรม

"ศาสตร์และศิลป์ทำให้คนยอมทำตามความต้องการของเรา"

(Harl – People Hacking: The Psychology of Social Engineering, 2003)

ในหัวข้อนี้จะอธิบายกลยุทธ์ เทคนิค และวิธีการที่นักต้มตุ๋น (scammer) กระทำต่อเหยื่อตั้งแต่เริ่มกระบวนการ จนกระทั่งสิ้นสุดกระบวนการก่ออาชญากรรม เพื่อหลอกลวงให้เหยื่อโอนเงินหรือเสียทรัพย์ โดยไม่ได้คำนึงว่าที่มาของเงินจะมาจากเงินเก็บสะสม การแปลงทรัพย์สินที่มีอยู่ให้เป็นเงิน หรือการกู้ยืม ซึ่งถือว่าเป็นการก่ออาชญากรรมที่สร้างความเสียหายแก่เหยื่อ 2 ด้าน (double hit) ด้านแรกคือความเสียหายที่เป็นตัวเงิน/ทรัพย์สิน ด้านที่สองคือความเสียหายทางด้านจิตใจ โดยทั่วไปมีการตั้งข้อสังเกตว่าความเสียหายทางจิตใจที่เกิดจากการสูญเสียความสัมพันธ์เป็นเรื่องที่รุนแรงมากกว่า และยากที่จะเยียวยา คำอธิบายตามทฤษฎีทางจิตวิทยาจะช่วยให้เข้าใจในสิ่งเหยื่อแต่ละคนเผชิญอยู่ได้อย่างมีเหตุผลมากกว่าการตีตราว่าเหยื่อเป็น "คนโลภ" คนส่วนใหญ่เห็นว่าการที่จะตกเป็นเหยื่อได้นั้น คนๆนั้นต้องมี "ความโลภ" ด้วยความอยากได้ทรัพย์สินของผู้อื่นจึงเป็นสาเหตุให้คนๆนั้นสูญเงินไปมหาศาล แต่เหยื่อกรณี romance scam สามารถอธิบายได้ด้วยเหตุผลอื่นอีกที่มากกว่าการตีตรานั้น ซึ่งจะตอบคำถามได้ว่า ทำไมคนๆ หนึ่งจึงตกหลุมรัก และเชื่อใจคนที่อยู่โลกออนไลน์ได้? ทำไมจึงยอมโอนเงินให้? ทำไมจึงกลับไปเป็นเหยื่อซ้ำแล้วซ้ำเล่า? ซึ่งผู้เสียหายทั้งในต่างประเทศและในประเทศล้วนเผชิญกับกลยุทธ์การหลอกลวงที่ใกล้เคียงกัน[28]

ทฤษฎีทางจิตวิทยาแขนงหนึ่งซึ่งเป็นศาสตร์ของการรับรู้ข้อมูลของมนุษย์และการแสดงท่าทีต่อข้อมูลนั้นที่สามารถวิเคราะห์ด้วยสถิติและหาข้อสรุปด้วยวิธีทางวิทยาศาสตร์ได้ หรือที่เรียกว่า **วิศวกรรมสังคม (Social Engineering)** อันเกิดจากการนำเอาความรู้ทาง จิตวิทยา สังคมศาสตร์ รัฐศาสตร์ วิทยาศาสตร์คอมพิวเตอร์ และอีกหลายสิ่ง ซึ่งรวมไปถึงการศึกษา การออกแบบ การแก้ไข และการ วางแผนพฤติกรรมมนุษย์ มาประยุกต์เข้าด้วยกันเพื่อให้เป็นประโยชน์ทางจิตวิทยา ซึ่งในกรณีของ romance scam ทฤษฎีดังกล่าวจะถูกนำมาประยุกต์ใช้เป็นกลยุทธ์เทคนิคการหลอกลวงโดยใช้หลักการพื้นฐานทางจิตวิทยา ร่วมกับกลยุทธ์วิธีอื่นเพื่อให้เหยื่อเปิดเผยข้อมูลส่วนบุคคลต่างๆ รวมถึงการโน้มนำให้เหยื่อเป็นไปในแนวทางที่ scammer วางไว้ด้วยการปลอมตัวเป็นบุคคลอื่น และไม่มีวิธีการที่ตายตัว แต่จะมีรูปแบบร่วมกันอยู่[29] ขั้นตอนทางวิศวกรสังคมแบ่งออกได้หลายส่วนดังนี้

- การเก็บรวบรวมข้อมูล ในกรณีนี้จะเป็นการศึกษา ทำความเข้าใจ และเก็บรวบรวมข้อมูลของบุคคลที่มุ่งให้เป็นเหยื่อ โดยอาศัยข้อมูลต่างๆ ที่เหยื่อโพสต์ลงในเครือข่ายสังคม

[28] ผู้เสียหายไม่ประสงค์ออกนาม. ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม. (7 เมษายน 2562). สัมภาษณ์.

[29] ผู้ดูแลเพจ. เพจภัยผู้หญิง ในโลกออนไลน์. (17 มกราคม 2562). สัมภาษณ์.

ออนไลน์ ไม่ว่าจะเป็นสถานะข้อมูลส่วนบุคล สเตตัส รูปภาพ หรือการแชร์ข้อมูลต่างๆ เพื่อประเมิน และวิเคราะห์ก่อนการหลอกลวงในขั้นต่อไป

- การวิเคราะห์ข้อมูล การวิเคราะห์ข้อมูลอาจทำด้วยตนเอง หรือหากเป็นกลุ่มอาชญากรใหญ่อาจมีระบบคอมพิวเตอร์เพื่อช่วยในการรวบรวม และจำแนกข้อมูลของเหยื่อคนนั้น อันจะนำไปสู่การเลือกใช้สถานการณ์ที่สร้างเพื่อนำไปสู่การหลอกลวง
- การวางแผน เทคนิค หรือเรื่องราวต่างๆ ที่ scammer ได้กระทำลงไปนั้นล้วนแต่เกิดจากการวางแผนแล้วอย่างรอบคอบ เพื่อให้เหยื่อเชื่อใจและหลงคิดว่านั้นคือ “คนรัก” “คู่แท้” อย่างแท้จริงอันจะนำไปสู่การหลอกลวงด้วยวิธีการต่างๆ
- การดำเนินขั้นตอนตามที่วางแผนไว้ ในกรณีเป็นการโปรไฟล์ สร้างเรื่องราวต่างๆ นานาด้วยการสร้างความสัมพันธ์รักที่หอมหวานลึกซึ้ง เพื่อให้เหยื่อเชื่อใจและโอนเงินให้ท้ายที่สุด

ด้วยกลของการหลอกลวงที่ส่วนมากมักทำงานกันเป็นขบวนการนี้จะนำไปสู่ความสูญเสียทั้งทางการเงิน และทางจิตใจของเหยื่ออย่างแนบเนียน ซึ่งส่วนถัดไปจะแสดงให้เห็นกระบวนการโดยละเอียดที่ scammer จะกระทำต่อเหยื่อที่สามารถแบ่งออกเป็น 7 ขั้นตอน ดังนี้

1. การสร้างโปรไฟล์ปลอม

ถือเป็นขั้นตอนแรกของกระบวนการหลอกลวง โดย scammer จะเลือกขโมยรูปภาพบุคคลอื่นที่มีลักษณะบุคลิกภาพดี หน้าตาดี และดูภูมิฐานจากเว็บไซต์ เครือข่ายสังคมออนไลน์ต่างๆ เช่น Facebook, Instagram, twitter หรือเว็บเพจต่างๆ เพื่อสร้างโปรไฟล์ให้ตนเองดูน่าสนใจ และน่าดึงดูดต่อคู่สนทนา ซึ่ง scammer หนึ่งคนสามารถสร้างและบริหารโปรไฟล์ได้นับสิบตามแต่ความสามารถในการบริหารจัดการของตนเอง รูปแบบของโปรไฟล์ที่สามารถจัดเป็นกลุ่มได้อาจเพราะค่านิยมส่วนใหญ่ของการเลือกคู่ โดยผู้หญิงมักจะเลือกผู้ชายที่ให้ความมั่นคงในชีวิตแก่พวกเธอได้ ส่วนผู้ชายมักจะเลือกผู้หญิงที่รูปร่างหน้าตาเป็นหลัก “ไม่ว่าจะชนชาติใด ความต้องการเป็นเช่นนี้ทั้งนั้น” - กุลชุลี ทรัพย์สินอุดม (ผู้ก่อตั้งและผู้บริหารแบงคอก แมทชิ่ง บริษัทจัดหาคู่ในเมืองไทย)[30] จากการเก็บข้อมูลในประเทศไทยในปีพ.ศ. 2560-2561[31] พบว่าภาพถ่ายบนโปรไฟล์ที่ romance scammer เลือกใช้มากที่สุดคือฝรั่งผิวขาว 82.58% และส่วนใหญ่เป็นมักเป็นโปรไฟล์ผู้ชายปลอม มีจำนวนมากถึง 78.71% ผู้หญิง 18.06% และเพศทางเลือก 3.23% สามารถแบ่งออกได้ตามเพศดังนี้

1.1 *โปรไฟล์ผู้ชายปลอม*

1.1.1 ลักษณะภาพมักเป็นคนผิวขาวที่ดูมีเสน่ห์ อบอุ่น ภูมิฐาน มีฐานะ และมีท่าทางเป็นคนดี

1.1.2 อายุโดยเฉลี่ยประมาณ 40 – 50 ปี

[30] BBC News, (2018), *งานวิจัยไขความลับ เดทออนไลน์อย่างไรให้เจอรัก,* (30 พฤษภาคม 2562), สืบค้นจาก https://www.bbc.com/thai/international-45124922

[31] ข้อมูลกรณี Romance scams ตั้งแต่ปี 2560-2561 โดยการเก็บรวบรวมข้อมูลจากเพจภัยผู้หญิง ในโลกออนไลน์ พบว่า มีผู้เสียหายที่ให้ข้อมูลและขอความช่วยเหลือผ่านทางเพจ จำนวน 310 ราย

1.1.3 อ้างว่าเป็นทหาร วิศวกร นักธุรกิจ (โดยเฉพาะเกี่ยวกับน้ำมันปิโตรเลียม) แพทย์ หรือเจ้าหน้าที่รัฐ

1.1.4 อ้างว่าเป็นคนอเมริกัน อังกฤษ เยอรมัน หรือแคนาดา แต่ปัจจุบันเริ่มมีแนวโน้มว่าจะมีการอ้างว่าเป็นคนเอเชียเพิ่มมากขึ้นเช่น จีน ไต้หวัน สิงคโปร์ หรือแม้กระทั่งไทย นอกจากนั้นมีการอ้างว่าเป็นลูกครึ่ง เช่น อังกฤษ-ไทย จีน-สิงคโปร์ หรืออเมริกัน-ไทยเป็นต้น

1.1.5 ส่วนใหญ่จะอ้างว่า โสด หรือภรรยาเสียชีวิตแล้ว อยากมีชีวิตรักที่สมบูรณ์ ตามหารักแท้

ชื่อ Mark Harry อายุ 40 ปี ชาวอเมริกัน อาชีพวิศวกรการบินสายการบิน British และ Qatar Airways ภรรยาและลูกสาวเสียชีวิตแล้ว

ชื่อ Haley Vail Rogers มีหลายโปรไฟล์บางอันอ้างว่าเป็นคนแคนาดา บางอันเป็นอเมริกัน ทำงานเป็นทหารอยู่หลายแห่งเช่น ซีเรีย สิงคโปร์

ชื่อ Khaled Teriaki อายุ 41 ปี ทำงานเป็นนักกายภาพบำบัดที่เมืองคาบูล ประเทศอัฟกานิสถาน

ชื่อ Chan Wang เป็นคนจีนเรียนจบและทำงานอยู่ที่ประเทศอังกฤษมาหลายปีแล้ว

ชื่อ Peter Zeng ลูกครึ่งจีน-สิงคโปร์ ทำงานวิศวกรโรงงานกลั่นน้ำมันที่อเมริกา

ชื่อ Gabrial Ferdinand อายุ 41 ปี เป็นแพทย์อยู่ในกองทัพสหรัฐฯ สถานภาพหย่าร้าง

ภาพที่ 3 - 8 ตัวอย่างลักษณะภาพโปรไฟล์ผู้ชายปลอม

1.2 *โปรไฟล์ผู้หญิงปลอม* แบ่งออกเป็น 2 ลักษณะ

1.2.1 <u>มุ่งหวังเหยื่อเพศชาย</u>

1.2.1.1 ภาพโปรไฟล์มักมีลักษณะเป็นนางแบบหุ่นดี หน้าตาดี น่าหลงใหล

1.2.1.2 อายุเฉลี่ยไม่เกิน 35 ปี

1.2.1.3 อ้างว่าเป็นทหาร พยาบาล ครู พนักงาน หรือนักศึกษา ส่วนมากอาชีพที่ถูกอ้างถึงเป็นอาชีพที่มีรายได้น้อย เพื่อสร้างความน่าสงสาร และน่าเห็นใจ

1.2.1.4 ส่วนใหญ่มักอ้างว่าเป็นลูกครึ่ง มีเชื้อชาติเดียวกับเหยื่อ หรือฝรั่งผิวขาว เช่น อเมริกัน โรมาเนีย เป็นต้น

1.2.1.5 ส่วนมากมักอ้างว่าโสด หรือหย่าร้าง อยากมีคู่แท้ ที่เข้าใจและดูแลกันละกัน

อ้างว่าเป็นคนไทย อยู่ที่ประเทศอังกฤษ

ชื่อ Sophia Katherine เป็นคนอเมริกัน ทำงานในฐานกองกำลังรักษาสันติภาพแห่งสหประชาชาติในซีเรีย

ชื่อ Chen Jia อายุ 35 ปี เป็นคนจีน แต่เกิดที่ประเทศอังกฤษ เป็นนักธุรกิจต้องการมาลงทุนที่ประเทศไทย

ภาพที่ 9 - 11 ตัวอย่างลักษณะภาพโปรไฟล์ผู้หญิงปลอม ที่มุ่งหวังเหยื่อเพศชาย

1.2.2 <u>มุ่งหวังเหยื่อเพศหญิง</u>

1.2.2.1 ภาพโปรไฟล์มักมีลักษณะดูมีอายุ แต่งกายดี ดูมีฐานะ และน่าเชื่อถือ

1.2.2.2 อ้างว่าเป็นคนชาติเดียวกับเหยื่อ หรือมีเคยสามีเป็นต่างชาติและชาติเดียวกับเหยื่อ

1.2.2.3 ส่วนใหญ่มักอ้างว่าเป็นแม่หม้าย สามีเสียชีวิตพร้อมกับทิ้งมรดกไว้มหาศาล

ชื่อ Sasi Vimeks อยู่ที่เมืองฮานอยประเทศเวียดนาม สามีเป็นคนอังกฤษเพิ่งเสียชีวิตไป

ชื่อ Nafi Vimeks อยู่ที่เมืองฮานอยประเทศเวียดนาม สามีเป็นคนอังกฤษเพิ่งเสียชีวิตไป

ภาพที่ 12 - 13 ตัวอย่างลักษณะภาพโปรไฟล์ผู้หญิงปลอม ที่มุ่งหวังเหยื่อเพศหญิง

1.3 *โปรไฟล์เพศทางเลือก*

1.3.1 ภาพโปรไฟล์มักเป็นรูปผู้ชายที่มีลักษณะนายแบบ หุ่นดี แต่งกายดี ที่สามารถสร้างดึงดูดได้สูงสำหรับกลุ่มรักร่วมเพศ

1.3.2 มีลักษณะทางสังคมค่อนข้างหลากหลาย ทั้งอาชีพมั่นคง และไม่มั่นคง

1.3.3 อ้างว่าเป็นดีไซน์เนอ แพทย์ หรือนักธุรกิจ

ภาพที่ 14 - 15 ตัวอย่างลักษณะภาพโปรไฟล์ของเพศทางเลือก

อย่างไรก็ตาม แม้จะพบว่าการสร้างโปรไฟล์ปลอมส่วนใหญ่มักจะเป็นฝรั่งผิวขาว แต่ปัจจุบันพบว่า เริ่มมีการใช้โปรไฟล์ที่เป็นคนไทย หรือลูกครึ่งไทยเพิ่มมากขึ้น อีกทั้งยังใช้ภาษาไทยในการสนทนา แต่เป็นภาษาไทยที่ผ่านการแปลภาษาจาก google translator หรือบางครั้งอาจเป็นคนไทยเองที่เป็นผู้สนทนาแต่ใช้ภาพโปรไฟล์เป็นคนอื่น ดังนั้นการจะระวังภัยจาก scammer ไม่สามารถตัดสินจากภาพโปรไฟล์ฝรั่งผิวขาวเพียงอย่างเดียวอีกต่อไป ต้องตระหนักถึงโปรไฟล์ในรูปแบบอื่นๆ ด้วย

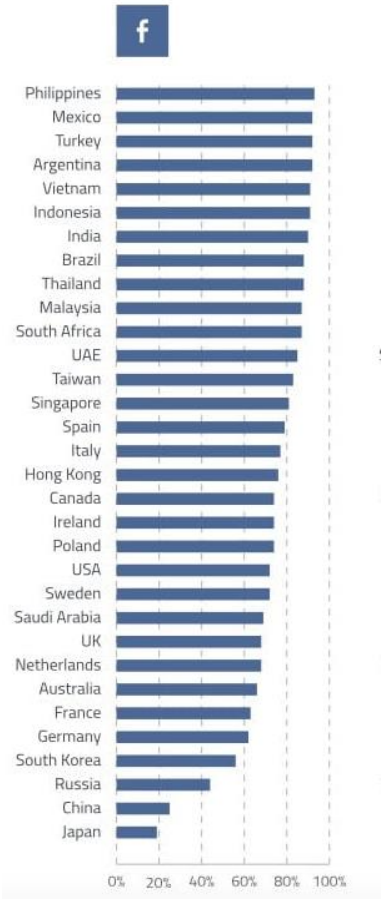
2. การเลือกแหล่งในการล่อเหยื่อ

หลังจากการสร้างโปรไฟล์แล้ว scammer จะเลือกพื้นที่ในการหลอกลวง ซึ่งในปัจจุบันพื้นที่เครือข่ายสังคมออนไลน์มีมากจนนับไม่ถ้วน และมีเพิ่มขึ้นทุกวันเพื่อตอบสนองความต้องการของผู้คนในโลกยุคปัจจุบัน ยิ่งจำนวนและพัฒนาการของเครือข่ายเหล่านี้มีมากขึ้นเท่าใด ยิ่งทำให้เหล่าอาชญากรมีช่องทางในการกระจายตัวมากขึ้นเท่านั้น จากสถิติในสหรัฐฯ เพียงประเทศเดียวมีเว็บไซต์ หาคู่มากถึง 2,500 เว็บไซต์ และมีเพิ่มขึ้นกว่า 1,000 เว็บไซต์ ในทุกๆ ปี และจากการประมาณการณ์เว็บไซต์ หาคู่ทั่วโลกอาจมีมากถึง 8,000 เว็บไซต์ [32] นอกจากนั้นเมื่อพิจารณาแนวโน้มการใช้อินเตอร์เน็ตของประเทศไทย ระหว่างปีพ.ศ. 2557-2561 พบว่าผู้ใช้อินเตอร์เน็ตเพิ่มขึ้นจาก 34.9% (จำนวน 21.8 ล้านคน) เป็น 56.8% (จำนวน 36.0 ล้านคน) [33] ดังนั้นการเลือกพื้นที่ของ scammer ย่อมแปรผันตรงกับการใช้บริการของผู้คนในปัจจุบัน อาชญากรจะโพสต์โปรไฟล์ปลอมทั้งหลายลงไปยังเว็บไซต์ หรือแอปพลิเคชันหาคู่ต่างๆ เช่น Skout, Tinder, Badoo, OkCupid, Twoo, Thai date VIP, Tagged และ Match.com เป็นต้น อีกทั้งยังมีการส่งข้อความสนทนาส่วนตัวไปยัง e-mail หรือเครือข่ายสังคมออนไลน์อื่นๆ เช่น Facebook และInstagram เป็นต้น จากการศึกษาในช่วง พ.ศ. 2560 -2561 พบว่าเหยื่อส่วนใหญ่ในประเทศไทยถูกหลอกลวงจากการถูกขอเป็นเพื่อน (friends requests) ในเว็บไซต์ Facebook มากถึง 94.19% รองลงมาคือ เว็บไซต์หาคู่ เช่น Tagged, ThaiFriendly, Thai date VIP 1.94% ซึ่งสอดคล้องกับรายงานสถิติของ GWI (Global Web Index) เมื่อต้นปี 2019 ว่าประเทศไทยติด 1 ใน 10 อันดับของประเทศที่มีผู้ใหญ่ Facebook มากที่สุดทั่วโลก ซึ่งมีผู้ใช้บริการมากกว่า 80% เมื่อเทียบกับจำนวนประชากร[34]

[32] Matthews, H., (2018), *27 Online Dating Statistics & What They Mean for the Future of Dating,* สืบค้นจาก https://www.datingnews.com/industry-trends/online-dating-statistics-what-they-mean-for-future/

[33] สำนักงานสถิติแห่งชาติ, (2561), *การสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2561 (ไตรมาส 1),* กรุงเทพฯ: สำนักงานสถิติแห่งชาติ.

[34] Chaffey, D., (2019), Global social media research summary 2019, from https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/



ภาพที่ 16 จำนวนร้อยละของผู้ใช้บริการ Facebook ในแต่ละประเทศ

กระบวนการล่อเหยื่อระหว่างเว็บไซต์ /แอปพลิเคชันหาคู่ กับเครือข่ายสังคมออนไลน์มีความแตกต่างกันเล็กน้อย สามารถอธิบายได้ดังนี้ *เว็บไซต์/แอปพลิเคชันหาคู่* ในขั้นตอนนี้ scammer ต้องสร้างโปรไฟล์ปลอมที่มีความหลากหลาย และตั้งเป้าหมายไว้แล้วว่าต้องการเหยื่อประเภทใดบ้าง เพื่อให้อัลกอริทึม (algorithm) จับคู่ (matching) เหยื่อได้อย่างเหมาะสม ซึ่งในขั้นตอนนี้ scammer บางกลุ่มจะเข้าไปเรียนรู้บุคคลแต่บุคคลในเว็บไซต์ หรือแอปพลิเคชันนั้นก่อน เพื่อศึกษาว่าควรสร้างของโปรไฟล์อย่างไรให้ตรงกับบุคคลที่มีแนวโน้มจะหลอกลวงได้ และมีฐานะทางการเงินมากพอ (ซึ่งจะอธิบายอย่างละเอียดในหัวข้อการเลือกเหยื่อ) *เครือข่ายสังคมออนไลน์* ในกรณีนี้ scammer ไม่จำเป็นต้องเรียนรู้เหยื่อก่อนการสร้างโปรไฟล์ เพียงแต่สร้างในโปรไฟล์ที่มีลักษณะเป็นสากลตามความต้องการหลักของมนุษย์ “ผู้หญิงมักจะเลือกผู้ชายที่ให้ความมั่นคงในชีวิตแก่พวกเธอได้ ส่วนผู้ชายมักจะเลือกผู้หญิงที่รูปร่างหน้าตาเป็นหลัก” จากนั้นจะสุ่มส่งคำขอเป็นเพื่อนให้แก่ผู้คนจำนวนมาก เพราะยิ่งส่งมาเท่าไรโอกาสในการมีผู้ติดต่อกลับก็มีมากเท่านั้น ดังนั้นพื้นที่เหล่านี้ไม่ว่าจะเป็น Facebook, Instagram, E-mail, kSkout, Tinder, Badoo, OkCupid, Twoo, Thai date VIP, Tagged, หรือ Match.com ถือว่าเป็นพื้นที่เสี่ยงต่อการเกิด romance scam ได้ทั้งสิ้น

3. การเลือกเหยื่อ และผู้ที่มีความเสี่ยงที่จะตกเป็นเหยื่อ

หลักการในการเลือกเหยื่อคือ การมองหาคน “ขี้เหงา” ต้องการหาเพื่อน/คู่ชีวิตในโลกออนไลน์ นั่นเป็นประการแรกที่อาชญากรจะเลือกสนใจ ต่อมาคือการประเมินความสามารถทางการเงินของบุคคลดังกล่าว ทั้งสองสิ่งสัมพันธ์กับที่ scammer เลือกพื้นที่ในการล่อเหยื่อ เนื่องจากผู้ที่ใช้บริการเว็บไซต์ หาคู่ ส่วนใหญ่เป็นคนเหงาที่หวังผลว่าตนจะพบรักแท้ในช่องทางดังกล่าว ตามผลจากการสำรวจของ Statista ฐานข้อมูลสถิติและบทวิเคราะห์สถิติของอุตสาหกรรมและประเทศทั่วโลกเปิดเผยว่า 84% ของผู้คนใช้เว็บไซต์ หาคู่เพื่อแสวงหาความสัมพันธ์ 43% เพื่อหาเพื่อน และ 24% เพื่อค้นหาคู่นอน[35] ซึ่งการที่จะประเมินบุคลิกลักษณะของผู้คนในโลกออนไลน์ย่อมต้องมาจากการศึกษาความเป็นตัวตนของคนคนนั้นผ่านข้อมูลที่อยู่ในพื้นที่ออนไลน์ กล่าวคือ scammer จะประเมินค่าเป้าหมายผ่านข้อมูลส่วนบุคคล (ชื่อ อายุ การทำงาน สถานะทางสังคม สถานะสมรส งานอดิเรก ความชื่นชอบส่วนตัว) การแสดงความคิดเห็น ภาพถ่าย สเตตัส หรือการแชร์ข้อมูลที่คนคนหนึ่งโพสต์ลงบนโลกออนไลน์ จากการศึกษาอนุมานได้ว่าผู้ที่มีความเสี่ยงที่จะตกเป็นเหยื่อมักจะมีลักษณะดังนี้

3.1 *เพศหญิง*

จากการศึกษาพบว่า ผู้หญิงเป็นเพศที่ตกเป็นเหยื่อของ romance scam มากที่สุด สถิติในประเทศไทยตั้งแต่ปี 2560-2561 พบว่า เพศหญิงตกเป็นเหยื่อมากถึง 85.61% เพศชาย 10.97% เพศอื่น 3.87% ซึ่งเป็นตัวเลขที่สอดคล้องกับอีกหลายประเทศในโลก ตัวอย่างเช่น สหราชอาณาจักรในปี 2017 มีเพศหญิงตกเป็นเหยื่อ 63% และเพศชาย 37%[36] ฮ่องกงในปี 2017 มีเพศหญิงตกเป็นเหยื่อ 93.62% และเพศชาย 6.38%[37] และประเทศออสเตรเลียในปี 2018 มีเพศหญิงตกเป็นเหยื่อ 79.5% เพศชาย 20.3% และเพศอื่น 0.3%[38]

3.2 *ส่วนมากมีอายุ 45 – 65 ปี ค่าเฉลี่ยอยู่ที่อายุ 50 ปี*

ผู้ถูกหลอกลวงส่วนมากมักเป็นวัยใกล้เกษียณอายุ หรือเกษียณอายุ เฉลี่ยอายุ 50 ปี มีทรัพย์สิน/เงินเก็บสะสมอยู่พอสมควร ทำให้กลุ่มอายุนี้จะมีโอกาสเสียทรัพย์มากกว่าวัยอื่นๆ อย่างไรก็ตามก็พบคนกลุ่มอายุที่น้อยกว่าตกเป็นเหยื่อด้วยเช่นกัน คืออายุตั้งแต่ 25 ปีขึ้นไป แต่จำนวนความเสียหายของทรัพย์สินไม่มากนัก ซึ่งค่าเฉลี่ยอายุเหล่านี้มีความสอดคล้องกันทั่วโลก ในอเมริกาพบว่าผู้สูญเสียทรัพย์มากที่สุดมีอายุ 40-69 ปี[39] เช่นเดียวกับออสเตรเลียมีอายุ 55–64 ปี[40] และประเทศ

---

[35] Matthews, H., (2018), *27 Online Dating Statistics & What They Mean for the Future of Dating,* from https://www.datingnews.com/industry-trends/online-dating-statistics-what-they-mean-for-future/

[36] Victims lost £41 million to romance fraud in 2017, from https://www.actionfraud.police.uk /news/victims -lost-41-million-to-romance-fraud-in-2017

[37] Snapshort of romance scam, from https://www.police.gov.hk/info/img/cpb/adcc/180517_en.pdf

[38] ACCC, (2018), *Scam statistics: dating & romance in 2018*, from https://www.scamwatch.gov.au /about-scamwatch/scam-statistics?scamid=13&date=2018

[39] Fletcher, E., (2019), *Romance scams rank number one on total reported losses*, from https://www.ftc.gov/news-events/blogs/data-spotlight/2019/02/romance-scams-rank-number-one-total-reported-lossesd

[40] ACCC, (2018), *Scam statistics: dating & romance in 2018*, from https://www.scamwatch.gov.au /about-scamwatch/scam-statistics?scamid=13&date=2018

อังกฤษมีอายุ 50 ปีขึ้นไป[41] อย่างไรก็ตามประเทศไทยมีความเปลี่ยนแปลงของกลุ่มเหยื่อไปตามบริบทของสังคมโดยจะเห็นได้ว่า ในยุคแรกๆ คือเมื่อ 10 ปีก่อน เหยื่อจะเป็นกลุ่มที่สามารถสื่อสารภาษาอังกฤษได้ มีหน้าที่การงานดี เช่น แพทย์ พยาบาล ข้าราชการชั้นสูงๆ ต่อมาเริ่มเป็นกลุ่มนักศึกษาโดยการเอาสิ่งของมาล่อว่าจะส่งของมาให้ แต่ในปัจจุบันเหยื่อจะเริ่มเป็นกลุ่มของแม่ค้าออนไลน์ และผู้สูงอายุ เพราะแม่ค้าออนไลน์จะรับแอดทุกคนเป็นปกติและมี โปรไฟล์เป็นสาธารณะง่ายต่อการเข้าถึง ส่วนผู้สูงอายุเป็นกลุ่มที่มีเงินเก็บสะสม และไม่ได้ติดตามข่าวสาร[42]

3.3 *หย่าร้าง/หม้าย*

สถานภาพทางครอบครัวเป็นอีกหนึ่งปัจจัยที่นำไปสู่การตกเป็นเหยื่อ เหยื่อจำนวนมากมักมีสถานะหม้าย หรือหย่าร้าง ด้วยความโดดเดี่ยวและความเหงาที่ต้องการชีวิตรักที่สมบูรณ์จึงนำไปสู่ความเสี่ยงของการตกเป็นเหยื่อ จากสถิติของประเทศอเมริกาพบว่าผู้เหยื่อเป็นแม่หม้าย หรือหย่าร้างเช่นกัน[43]

3.4 *ความเหงา และต้องการมีเพื่อนต่างชาติ*

ความเปลี่ยวเหงานอกโลกออนไลน์ที่ผลักดันให้คนส่วนใหญ่เลือกช่องทางในการแสวงว่าหาความรักทางโลกออนไลน์ ประกอบกับการเลือกคู่ และสนทนาผ่านโลกออนไลน์สามารถเข้าถึงได้ทุกที่ทุกเวลาตลอด 24 ชั่วโมง ไม่ว่าจะอยู่ที่บ้าน ที่ทำงาน หรือที่อื่นใดที่มีอินเตอร์เน็ตก็สามารถบรรเทาความเหงาได้ อีกทั้งภาวะนิรนามบนโลกอินเตอร์เน็ตทำให้มีพื้นที่ส่วนตัวในแสดงข้อความเชิงชู้สาว หรือความต้องการได้อย่างไม่เขินอายเมื่อเปรียบกับการพบเจอแบบต่อหน้า และการไม่มีใครให้คำปรึกษาอยู่ข้างกายในที่นี้อาจเป็น ญาติ พี่น้อง ลูก หลาน เป็นสิ่งที่ล่อแหลมต่อการเปิดเผยความรู้สึก และข้อมูลส่วนบุคคลทั้งหลายให้แก่คู่สนทนาในโลกออนไลน์ เพราะคนเหล่านั้นมักทำให้เหยื่อคิดว่า “พวกเขาเป็นที่ปรึกษาที่ดี เข้าใจคุณมากที่สุด และพร้อมที่จะเป็นผู้ให้การสนับสนุนทางความคิดอยู่เสมอ”

3.5 *การขาดความรู้เกี่ยวกับเทคโนโลยีดิจิทัล (digital literacy)*

การรู้เท่าทันเรื่องนี้เป็นสิ่งสำคัญในยุคที่ทุกอย่างในโลกล้วนสัมพันธ์กับดิจิทัล เหยื่อส่วนใหญ่มักมองข้ามความสำคัญของการนำข้อมูลส่วนบุคคล หรือวิถีชีวิต (lifestyle) เข้าสู่โลกดิจิทัล ไม่ว่าจะเป็นการแสดงข้อมูลชื่อ อายุ การทำงาน สถานะทางสังคม สถานะสมรส งานอดิเรก ความชื่นชอบส่วนตัว การแสดงความคิดเห็น ภาพถ่าย สเตตัส หรือการแชร์ข้อมูล สิ่งเหล่านั้นเสมือนเป็นเหรียญสองด้าน ด้านหนึ่งคุณอาจได้มีปฏิสัมพันธ์กับเพื่อนผ่านช่องทางดังกล่าว อีกด้านหนึ่งสิ่งนั้นอาจนำภัยมาถึงตัวได้เช่นกัน เพราะข้อมูลที่สื่อถือความเป็นตัวตนของแต่ละบุคคลยิ่งมีมากเท่าใด ยิ่งเกิดการเรียนรู้ของ scammer มากเท่านั้น สิ่งนำจะนำไปสู่การสร้างสถานการณ์ให้เข้าถึงตัวเหยื่อได้ง่ายกว่าผู้ที่รู้เท่าทัน อย่างไรก็ตามการให้ข้อมูลดังกล่าวเป็นเรื่องค่อนข้างลำบากหากบุคคลนั้นๆ ต้องการหาคู่ผ่านเว็บไซต์ /

---

[41] Eleanor Rose, Z., A Global Network of Scammers is Targeting Older People—Here’s How to Avoid Becoming a Victim, from vbv.scb.co.th/pam/pa.aspx

[42] ไทยรัฐออนไลน์, (2561), *แฉเหลี่ยม!! แก๊งแชตรักลวงโลก ภัยสาวไทยนิยมผัวฝรั่ง*, (18 มิถุนายน 2562), สืบค้นจาก https://www.thairath.co.th/news/society/1311031

[43] FBI, (2017), *Romance Scams: Online Imposters Break Hearts and Bank Accounts*, from https://www.fbi.gov /news/stories/romance-scams

แอปพลิเคชันหาคู่ เพราะบริการดังกล่าวบังคับกรอกข้อมูลส่วนตัวเพื่อให้อัลกอริทึมได้ทำงานจับคู่ให้เหมาะสมกับผู้ใช้บริการทั้งหลาย

3.6 *คนอ่อนไหวง่าย (sensitive)*

บุคคลที่มีอารมณ์อ่อนไหว หรือเรียกได้ว่า “ขี้สงสาร” คนเหล่านี้จะถูกชักจูงได้ง่ายจากนักหลอกลวงรัก เพราะเหตุผล/สถานการณ์ 108 ที่เหล่านักหลอกลวงรัก ได้รวมตัวกันปฏิบัติการหลอกลวงนั้นถูกวางแผนไว้หลายขั้นตอนให้มีความแนบเนียนมากที่สุด ซึ่งเหตุผล และสถานการณ์จะอธิบายในหัวข้อถัดไป ประกอบกับจากการศึกษาพบว่า มีผู้เสียหายอีกหลายคนที่ยอมโอนเงินให้เพราะความสงสาร และคิดว่าคู่สนทนากำลังเดือดร้อน ต้องการความช่วยเหลือ และตนเองพอจะช่วยเหลือได้จึงยอมช่วยเหลือ โดยเฉพาะเหตุการณ์ที่เกิดขึ้นในต่างประเทศก็พบว่ามีผู้เสียหายประเภทนี้อยู่เป็นจำนวนมาก

ลักษณะแต่ละข้อมีความสัมพันธ์กันที่นำไปสู่การตกเป็นเหยื่อของ romance scam เหยื่อบางคนอาจไม่ได้มีคุณสมบัติครบทุกข้อตามที่กล่าวมากข้างต้น หากแต่คุณเป็นผู้ที่ใช้บริการเครือข่ายออนไลน์ทั้งหลายที่มีความเหงา ขี้สงสาร และเปิดเผยข้อมูลส่วนบุคคลเป็นประจำ คุณย่อมมีความเสี่ยงในการตกเป็นเหยื่อของ romance scam ได้อย่างง่ายดาย ดั่งคำพูดของ scammer คนหนึ่งที่ว่า *หากคุณตอบกลับ มีโอกาสมากถึง 70% ที่คุณจะเสียเงิน”*[44]

4. การสร้างบทบาทเพื่อเข้าถึงเป้าหมาย

เมื่อ scammer ได้รับการตอบกลับหลังจากการหย่อนเบ็ดล่อลวงแล้วนั้น การทำให้เป้าหมายไว้ใจ และเชื่อใจเป็นสิ่งที่สำคัญที่สุดของขั้นตอนในการพูดคุยกับเป้าหมายเพื่อให้คนเหล่านั้นตกเป็นเหยื่อด้วยการสานสัมพันธ์เชิงชู้สาว เริ่มบทสนทนด้วยการทำความรู้จักเป้าหมายด้วยการส่งข้อความทักทายที่แสนหวานในครั้งแรกที่คุยกันนั้นมักขึ้นต้นด้วย *Hi dear, Hi honey* และปัจจุบันเริ่มเห็นการสนทนาด้วยภาษาไทย *สวัสดีที่รัก สวัสดีน้ำผึ้ง* เป็นการแปลภาษาด้วย google translation จากนั้นจะเริ่มถามข้อมูลส่วนบุคคลของเป้าหมายเช่น อายุ สถานะอาชีพ เชื้อชาติ เพื่อเป็นข้อมูลที่จะนำไปสร้างตัวตนของตนเองให้ตรงตามความต้องการของเป้าหมายให้มากที่สุดผ่านการแนะนำตัวเอง ตามโปรไฟล์ทั่วไปที่กล่าวไปแล้วในข้อหัวที่ 1 การสร้างโปรไฟล์ปลอม จากนั้นหากได้รับการตอบสนองที่ดีจากเป้าหมายก็จะเริ่มสานสัมพันธ์ต่อด้วยการเอาใจใส่ และส่งข้อความแสนหวานแก่เป้าหมายไปอย่างต่อเนื่อง เช่น การบอกฝันดีก่อนนอน การถามถึงความเป็นอยู่ประจำวัน พร่ำแต่บอกรัก สัญญารักว่าจะมั่นคงกับคุณคนเดียว วาดฝันแก่เป้าหมายว่าจะมาใช้ชีวิตบั้นปลายร่วมกัน หรือต้องการทำธุรกิจร่วมกันที่ประเทศไทย ทำให้เป้าหมายรู้สึกว่าคู่สนทนาเป็นคนดี เอาใจใส่ คอยเป็นห่วงเป็นใยอยู่เสมอ และมีลักษณะของ “คนดี” เช่น การใช้คำพูดและสำนวนในแง่ดีที่จะสื่อนัยยะของการเป็นคนที่ซื่อสัตย์ จริงใจ และพึ่งพาได้ เป็นต้น และอีกทางหนึ่งเพื่อพิสูจน์ความไว้วางใจและความซื่อสัตย์โดยการเต็มใจยอมรับข้อจำกัดและความผิดพลาดของเป้าหมาย การสานสัมพันธ์ด้วยวิธีการนี้ทำให้เป้าหมายหลายคนหลงเชื่อและฝันหวานว่าคนรักที่ดี และสมบูรณ์แบบ ที่แตกต่างกับชีวิตรักในโลกความเป็นจริงที่แสนจะน่าเบื่อ

[44] Dixon, R., (2005), *Nigerian Cyber Scammers*. Retrieved 5 April 2009, from http://www.latimes.com/technology/la-fgscammers20oct20,0,301315.story?page=1&coll=la-tot-promo

หน่าย และน่าผิดหวัง เพราะจากการเก็บข้อมูลพบว่า เหยื่อส่วนใหญ่เป็นผู้ที่ผิดหวังจากความรักในชีวิตจริงมาก่อน หรือคู่รักเสียชีวิตแล้ว

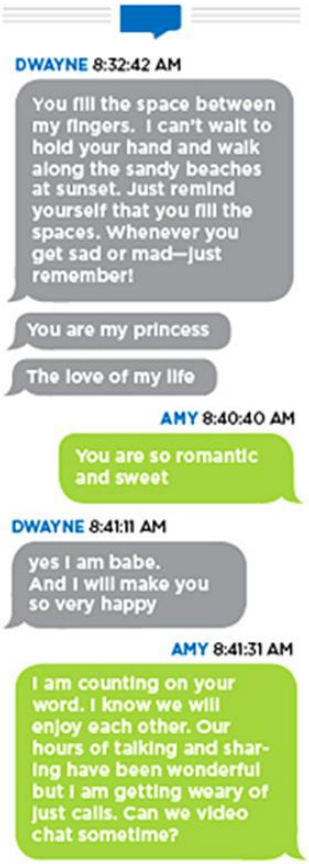
บางคนใช้เวลายาวนานถึง 2 ปีเพื่อสร้างความสัมพันธ์และความเชื่อมั่นนี้ แต่อย่างไรก็ตาม ส่วนมากscammer จะเร่งสร้างความสัมพันธ์รักชู้สาวนี้ให้ดำเนินไปให้เร็วที่สุดเพื่อที่จะได้นำสู่ขั้นตอนอื่นๆ อันนำมาซึ่งเงินโดยเร็วที่สุด ผู้เสียหายคนหนึ่งเล่าว่า *"เขาบอกรักฉันทุกวัน บอกฝันดีทุกคืน และแสดงความห่วงใยกับฉันในทุกๆ เรื่อง ฉันไม่เคยคิดว่าจะมีคนเอาใจใส่ชีวิตฉันมากขนาดนี้แม้ว่าจะไม่เคยพบกัน และสิ่งนี้เองที่ทำให้ฉันเคลิบเคลิ้มในทุกๆ เรื่อง"*[45] การสร้างความสัมพันธ์รักเป็นกระบวนการหนึ่งที่สำคัญในขบวนการทั้งหมด เพราะถ้าหากกระบวนการนี้ไม่สำเร็จการโอนเงินก็มักจะเป็นผล และแบบแผนประทุษกรรมเหล่านี้เกิดขึ้นเช่นเดียวกันในต่างประเทศ เรื่องราวของ Amy[46] ผู้หญิงอเมริกา อายุ 57 ปี เรียนจบวิทยาการคอมพิวเตอร์และจิตวิทยา และคิดว่าตนใช้งาน และกรอกข้อมูลส่วนบุคคลโนโลกเครือข่ายออนไลน์อย่างระมัดระวัง ได้พบผู้ชายคนหนึ่งใน Match.com เว็บไซต์ หาคู่ที่ใหญ่ที่สุดในอเมริกา ชื่อ "Duane" หรือ "Dwayne" อายุ 61 ผู้ที่ตรงสเปกตามที่เธอระบุไว้ในเว็บไซต์ ทุกประการ เรียกได้ว่าจับคู่กันได้ 100% เธอยังสงสัยว่าอัลกอริทึมเว็บหาคู่นี้ทำงานอย่างไร จึงสามารถหาคู่เดทให้เธอได้ตรงตามต้องการได้มากขนาดนี้ ข้อความแรกที่เธอได้รับจาก scammer พร้อมกับ Yahoo e-mail address ของเขา ซึ่งข้อความที่ทำให้เธอรีบตอบกลับโดยทันทีอย่างไม่คิดกังวลใดๆ มีเนื้อหาว่า .....

Hey you, เฮ้ เธอ

"How are you doing today? Thank you so much for the email and I am really sorry for the delay in reply, I don't come on here often, smiles ... I really like your profile and I like what I have gotten to know about you so far. I would love to get to know you as you sound like a very interesting person plus you are beautiful. Tell me more about you. In fact it would be my pleasure if you wrote me at my email as I hardly come on here often." วันนี้เป็นยังไงบ้างจ๊ะ ขอบคุณมากที่ตอบกลับอีเมล์มานะ ขอโทษด้วยนะที่ตอบกลับมาช้าไปหน่อย เราไม่ได้มีโอกาสเข้ามาดูข้อความในแชทได้บ่อยนะจ๊ะ แหะ แหะ... เราชอบตัวตนของคุณมากๆ เลยนะ แล้วก็ดีใจเป็นที่สุดที่ครั้งนึงได้รู้จักคนพิเศษอย่างคุณ ถ้ามีโอกาสเราก็อยากจะรู้จักเธอให้มากขึ้นอีกเพราะไม่บ่อยที่ได้เจอคนที่งดงามอย่างเธอ เล่าเรื่องเธอให้เราฟังเพิ่มขึ้นอีกได้ไหมจ๊ะ ถ้าไม่เป็นการรบกวนก็อยากได้อีเมล์จากเธออีกบ่อยๆ เลยนะเพราะเราแทบไม่ได้เข้ามาดูข้อความในแชทนี้เลยจ๊ะ

[45] ผู้ไม่ประสงค์ออกนาม, ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม, (30 เมษายน 2562). สัมภาษณ์.

[46] Shadel, D., and Dudley, D., AARP The Magazine, *"'Are You Real?' — Inside an Online Dating Scam"*, https://www.aarp.org/money/scams-fraud/info-2015/online-dating-scam.html



ภาพที่ 17 ตัวอย่างบทสนทนาระหว่าง Amy กับ Dwayne (scammer)

สิ่งสำคัญอีกประการหนึ่งในขั้นตอนนี้ คือการเรียนรู้โปรไฟล์ของเป้าหมาย ผ่านสิ่งที่พวกเธอ/พวกเขาโพสต์ลงไปในเครือข่ายสังคมออนไลน์ ไม่ว่าจะเป็นสถานการณ์ในชีวิตประจำวัน ภาพถ่าย และการโพสต์ข้อความ หรือการแชร์สิ่งที่ตนเองสนใจ สิ่งเหล่านี้ล้วนเป็นประโยชน์แก่กลุ่ม scammer ที่จะใช้เป็นเครื่องมือในการคาดเดาความต้องการ และความเป็นไปของเป้าหมาย ซึ่งเป็นจุดสำคัญที่ทำให้พวกเขาเข้าใจเหยื่อได้อย่างไม่ยุ่งยาก ผู้เสียหายคนหนึ่งเล่าว่า *“ภรรยาของเขาเสียชีวิตด้วยโรคมะเร็ง เหมือนกับที่สามีของฉันเสียชีวิตด้วยโรคมะเร็ง เหมือนกับเรามีอะไรหลายอย่างตรงกัน เข้าใจกันได้ง่ายในทุกๆ เรื่อง”* ข้อความเหล่านี้มีที่มาที่ไปอย่างชัดเจนจากโพสต์ข้อความอาลัยรักที่เหยื่อได้โพสต์ถึงสามีที่เสียชีวิตไปแล้วด้วยโรคมะเร็งบน Facebook ของเธอ ทำให้ scammer ใช้ประโยชน์จากจุดอ่อนทางอารมณ์ความรู้สึกนั้นมาสานสัมพันธ์รักของพวกเขาทั้งคู่

อีกทั้งมีการส่งภาพถ่ายกิจกรรมระหว่างวันให้เหมือนเป็นการสนทนากันแบบคู่รัก ที่เป็นการรายงานตัวว่ากำลังทำอะไรอยู่ ทำงานอยู่ที่ไหน กำลังจะไปที่ไหน ในอีกทางหนึ่งเป็นการทำให้เหยื่อเชื่อว่า คนคนนั้นมีตัวตนอยู่จริง เพราะสามารถมีภาพถ่ายมาแสดงได้อยู่เสมอ ส่วนภาพที่ได้นั้นเป็นไปได้อยู่ 2 ทางคือ การขโมยภาพถ่ายในเครือข่ายสังคมออนไลน์ และการตัดต่อภาพถ่าย นั่นหมายความได้ว่าหากผู้ใดที่โพสต์ภาพตนเองลงสื่อสังคมออนไลน์อยู่บ่อยครั้ง และเปิดให้เข้าชมภาพได้เป็นสาธารณะผู้นั้นอาจถูกขโมยภาพทั้งหลายไปใช้ในทางเสียหายได้

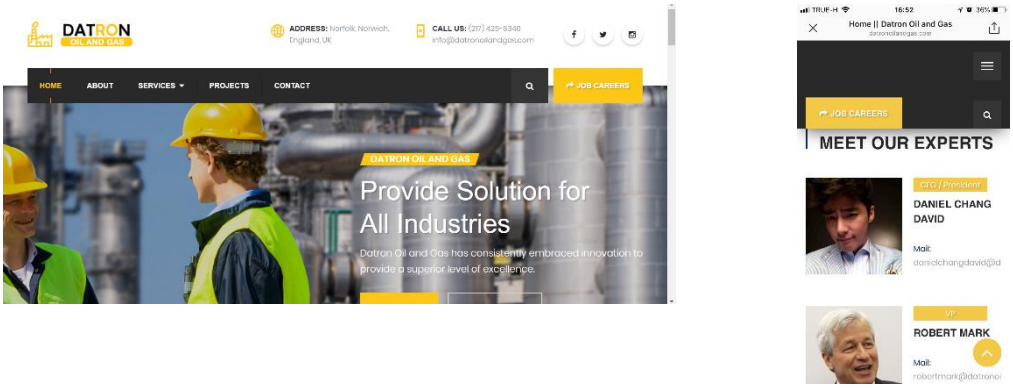
ภาพที่ 18 ตัวอย่างภาพที่ scammer ส่งให้แก่เป้าหมาย และบอกว่ากำลังออกกำลังกายที่ฟิตเนส

ภาพที่ 19 ตัวอย่างภาพที่ scammer ส่งให้แก่เป้าหมาย และบอกว่ากำลังทำงานอยู่

นอกจากนั้นยังมีการสร้างความน่าเชื่อถือด้วยการอ้างถึงตัวตนของสถาบันหรืออาชีพที่มีความมั่นคงและตรวจสอบได้ ซึ่งส่วนใหญ่มักใช้ภาพหนังสือเดินทางหรือบัตรเจ้าหน้าที่/พนักงานเพื่อยืนยันตัวตน เช่น ผู้ที่อ้างตนว่าเป็นทหาร จะส่งภาพหนังสือเดินทาง/บัตรประจำตัวที่มีภาพบุคคลแต่งเครื่องแบบทหาร หรือผู้ที่อ้างตนว่าเป็นวิศวกรในแหล่งขุดเจาะน้ำมัน มักจะส่งภาพถ่ายแท่นขุดเจาะน้ำมัน และภาพบุคคลสวมชุดวิศวกรสนาม และสิ่งที่ดูน่าเชื่อถือที่ถูกใช้อ้างอยู่บ่อยครั้งคือ อ้างว่าตนเป็นคนเป็นมีชื่อเสียงในโฆษณา และคนดูแลทรัพย์สินของการระดมทุนบางอย่าง อีกทั้งยังมักอ้างถึงความสำเร็จต่างๆ อันจะสามารถโน้มน้าวให้เป้าหมายเชื่อมั่นถึงความสำเร็จในอนาคตร่วมกัน

ภาพที่ 20 ตัวอย่างหนังสือเดินทาง (passport) และบัตรประจำตัวเจ้าหน้าที่ที่ scammer ดัดแปลงและใช้แอบอ้าง

ยิ่งไปกว่านั้นยังพบว่ามีการสร้างเว็บไซต์ ปลอมขึ้นมาเพื่อให้ตนเองอ้างอิงได้อย่างน่าเชื่อถือว่าทำงานในบริษัทนั้นจริงเมื่อนำชื่อบริษัทที่อ้างไว้ไปค้นหาใน google และทำให้เป้าหมายมั่นใจว่าสิ่งที่คู่สนทนาพูดมีเค้าว่าเป็นความจริง เหยื่อคนหนึ่งเล่าว่า[47] *“เริ่มพูดคุยกับ Daniel Chang David อายุ 38 ปี ครั้งแรกผ่าน Instagram จากนั้นเขาขอให้ย้ายมาพูดคุยที่แอปพลิเคชัน what’s app แทน เขาอ้างทำงานอยู่บริษัทเกี่ยวกับน้ำมันและก๊าซที่ประเทศอังกฤษ โดยมีพ่อเป็นเจ้าของบริษัท พร้อมกับส่งเว็บไซต์ ของบริษัทมาให้ดูและโปรโมทว่านี่คือบริษัทของเขาที่ต้องดูแลต่อเมื่อพ่อเสียชีวิต http://datronoilandgas.com ฉันก็เปิดดูและเห็นว่าบริษัทนั้นมีตัวตนอยู่จริงที่นิวยอร์ก พร้อมเห็นภาพว่าเขามีตำแหน่งเป็น CEO ในเว็บไซต์ นั้นจริง”*



ภาพที่ 21 ภาพจากเว็บไซต์ บริษัทที่ scammer สร้างขึ้นเพื่อแสดงความน่าเชื่อถือของอาชีพ

จากการศึกษาในกระบวนการของการทำให้เป้าหมายเชื่อใจ และไว้วางใจนั้น มี 6 บทบาทที่ scammer มักใช้เป็นเครื่องมือในการเข้าถึงเป้าหมาย และเมื่อกระบวนการนี้สำเร็จจะนำไปสู่การปฏิบัติการในขั้นต่อไป ดังนี้

1) การแสดงบทบาทของการเป็น “คนดีมีศีลธรรม” ด้วยการใช้ศาสนาเข้าถึงเป้าหมาย ซึ่งมีความเป็นไปได้ว่าโปรไฟล์ของเหยื่อในเว็บหาคู่อาจระบุสถานะทางศาสนา หรือระบุว่าเหยื่อกำลังหาคู่ที่เป็นผู้ศรัทธาในศาสนาเหมือนกัน ซึ่งผู้ที่ตกเป็นเหยื่อของอาชญากรมักเป็นผู้นับถือคริสต์ศาสนา โดยมักจะใช้คีย์เวิร์ดเกี่ยวกับศาสนาในการสนทนาให้มีความโดยนัย เช่น ‘pray’ (ภาวนา), ‘praying’ (อธิษฐาน), ‘thank God’ (ขอบคุณพระเจ้า), ‘grace’ (คุณธรรม) และ‘God fearing’ (กลัวบาป) เป็นต้น ตัวอย่างเช่น *“I pray about us yesterday, I think about us and it make me smile. (...) I am praying for you and your dad. and hope to meet you soon and share everything together. so that our joy shall be complete.”* (ฉันสวดภาวนาเกี่ยวกับเราเมื่อวานนี้ ฉันระลึกถึงเรื่องของเราแล้วมันก็ทำให้ฉันยิ้มได้ ฉันกำลังสวดภาวนาให้คุณและพ่อของคุณ และหวังว่าจะได้เจอคุณในเร็ววันเพื่อจะได้แบ่งหันทุกสิ่งทุกอย่างร่วมกัน สิ่งเหล่านี้จะนำมาซึ่งความอิ่มเอมใจอย่างบริบูรณ์) หรือ *“I have been looking for sincere and honest God fearing woman to spend the rest of my life together.”* (ฉันกำลังตามหาผู้หญิงที่จริงใจ ซื่อสัตย์ และเกรงกลัวต่อพระผู้เป็นเจ้า มาใช้ชีวิตร่วมกันตราบชั่วฟ้าดินสลาย) หรือ *“Honey, I believe in God and I believe you too”* (ที่รัก, ฉันเชื่อในพระเจ้าเหมือนกับที่ฉันเชื่อในคุณ) เป็นต้น คนส่วนใหญ่มองว่าคนที่เกี่ยวพันกับศาสนามักถูกมอง

[47] ผู้ไม่ประสงค์ออกนาม, ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม, (30 เมษายน 2562). สัมภาษณ์.

ว่าเป็นคนดีมีศีลธรรม ซื่อตรง น่านับถือ และประพฤติดี สิ่งนี้ช่วยลดความรู้สึกว่าเป็นคนแปลกหน้า เพราะปกติการคุยกับคนไม่รู้จักในโลกออนไลน์ต้องระมัดระวังและระแวงเป็นปกติ

2) การแสดงบทบาทของการเป็น “เนื้อคู่/คู่แท้ ไว้ใจได้” ด้วยการแสดงออกว่าเป็นคนใสซื่อ พยายามสร้างภาพว่าตนไม่ใช่คนที่ใช้บริการเว็บหาคู่นี้เป็นประจำ หรือเข้ามาใช้บริการเป็นครั้งแรก และแสดงให้เป้าหมายรู้สึกว่าการสุ่มจับคู่ครั้งนี้เป็นเรื่องของเนื้อคู่/คู่แท้ scammer มักอ้างว่าเพื่อนของเขาเป็นผู้แนะนำเว็บไซต์ นี้ให้ เพราะเพื่อนเขาเองได้พบเนื้อคู่จากเว็บไซต์ นี้ และเน้นถึงความไร้เดียงสาของตนเองที่เชื่อว่าเว็บดังกล่าวเป็นเว็บที่ไว้วางใจได้สำหรับผู้ที่กำลังต้องการสานสัมพันธ์กับใครสักคน โดยมีคีย์เวิร์ดที่ใช้บ่อยครั้งเช่น ‘honest’ (สุจริตใจ) ‘sincere’ (จริงใจ), ‘credible’ (น่าเชื่อถือ) และ ‘having faith’ (ไว้ใจได้) เป็นต้น ตัวอย่างเช่น *“I will always remain honest and sincere to you, and I wish to inform you that, I was married before with a daughter and I lost my wife, looking forward to hear from you again...it something credible to say that am well encourage in having faith and understanding with people around me. and I believe that you are such minded person too.”* (ผมจะซื่อสัตย์และจริงใจต่อคุณตลอดไป และขอเล่าเรื่องบางอย่างให้คุณรู้ว่า ผมเคยแต่งงานมาแล้วและมีลูกสาวหนึ่งคนแต่ภรรยาได้จากไปแล้ว ผมจึงอยากจะทราบจากคุณอีกครั้งว่าพอจะรับพ่อหม้ายเรือพ่วงอย่างผมได้ไหม การเล่าเรื่องจริงในชีวิตให้ทุกคนฟังอย่างจริงใจเป็นเครื่องยืนยันว่าคนที่ได้ฟังจะเข้าใจและศรัทธาในตัวผม ซึ่งผมก็เชื่อว่าคุณก็จะเข้าใจในความเป็นผมเช่นกันครับ)

3) การแสดงบทบาทของการเป็น “ผู้ที่มาจากครอบครัวที่ดี มีการศึกษาสูง และถูกเลี้ยงดูมาอย่างดี” มักแสดงออกว่า ตนเป็นผู้หาเลี้ยงครอบครัว และประสบความสำเร็จทางอาชีพทั้งกับหน่วยงานรัฐบาล/เอกชน โดยมักอ้างอาชีพที่มีชื่อเสียง น่านับถือ มีความมั่นคง และรายได้สูง เป็นต้น มักบอกเสมอว่าจะทำให้คู่ชีวิต (เหยื่อ) มีแต่ความสุขความสบาย ประโยคที่มักถูกนำมาใช้เช่น *“I am an arc tech, in engineering department. I work with both government and private company as a building engineer, both internationally and locally. am from Scotland, I like in dunblane city.”* (ฉันจบสถาปัตยกรรม จากมหาวิทยาลัยลอนดอน และสอนเกี่ยวกับเทคโนโลยีการออกแบบอยู่ที่คณะวิศวกรรม ฉันทำงานสองอย่างควบคู่กันไปทั้งสอนในมหาวิทยาลัย และเปิดบริษัทรับเหมาก่อสร้าง) หรือ *“I graduated from university of London, where I studied architectural.”* (ฉันเรียนจบสถาปัตยกรรมจากมหาวิทยาลัยลอนดอน) หรือมักอ้างว่า *“my position as engineer entitles me as, senior project surveyor monitoring in building department. am a good engineering, good in drawing both computer drawing and skillful drawing.”* (ผมเป็นวิศวกรที่ได้รับตำแหน่งช่างสำรวจอาวุโสประจำโครงการฝ่ายตรวจตราการก่อสร้าง ผมเป็นวิศวกรที่ดี เก่งฉกาจในการวาดเขียน ทั้งการวาดเขียนในคอมพิวเตอร์และทักษะในการวาดรูป) เป็นต้น

4) การแสดงบทบาทที่ทำให้เป้ารู้สึกว่า “เป็นคนสำคัญ” มักอ้างว่าต้องการเธอตลอดเวลา ขาดเธอไม่ได้ เธอเป็นเหมือนคู่ชีวิต ตัวอย่างเช่น *“I do think about you all the time, after reading your email again and again (...) you mean so much to me and my family too.”* (ฉันคิดถึงแต่เรื่องของคุณตลอดเวลา ฉันอ่าน e-mail ของคุณซ้ำไปซ้ำมาอย่างไม่เบื่อ....นั่นหมายความว่าคุณมีความหมายกับฉันเหลือเกินเสมือนเป็นส่วนหนึ่งครอบครัวของฉัน) หรือ “you are all I have been dreaming for and I cannot imagine more honor than living by your side modesty. I feel

moved by your deep faith and confidence." (คุณคือทุกสิ่งที่ผมเคยใฝ่ฝันและผมไม่อาจจินตนาการสิ่งใดได้มากกว่าการอยู่ร่วมกับคุณอย่างซื่อสัตย์และสุขสงบ ผมรู้สึกหวั่นไหวจากความศรัทธาและความเชื่อมั่นที่คุณมีให้ผมอย่างลึกซึ้ง) ผู้หญิงอังกฤษคนหนึ่งได้รับตุ๊กตาหมีพร้อมข้อความติดบนหน้าอกว่า 'I LOVE YOU' หลังจากที่คุยกันไม่ถึงสัปดาห์[48] ผู้หญิงอีกคนหนึ่งได้รับช่อดอกไม้ที่หน้าบ้านของเธอโดยหน้าการ์ดเขียนว่า 'My life will never be the same since I met you. Happy New Year. Love, Dwayne'[49] (ชีวิตของฉันจะไม่มีวันเหมือนเดิมอีกต่อไป สวัสดีปีใหม่ รักจาก ดเวนย์)

5) การแสดงบทบาทที่ทำให้เป้าหมายรู้สึกว่า "มีคุณค่า น่ายกย่อง น่าสรรเสริญ" โดยทำให้เป้าหมายรู้สึกว่าตนเป็นที่ต้องการ และเป็นพิเศษอยู่ตลอดเวลา ด้วยการใช้วลีที่เกินความจริง แสดงออกว่าคลั่งรักเหยื่อมาก ทั้งนี้ถือเป็นการทำให้เป้าหมายรู้สึกดีต่อตัวเอง และคู่สนทนา อันจะนำไปสู่การพัฒนาความสัมพันธ์ที่ใกล้ชิดได้รวดเร็วยิ่งขึ้น ตัวอย่างเช่น *"I found you to be a very responsible woman with a kind heart. I am so proud of you, and I feel moved by your deep faith and confidence."* (การที่ผมได้เจอคุณถือเป็นสิ่งที่วิเศษมาก เพราะคุณเป็นผู้หญิงที่มีความรับผิดชอบและมีจิตใจที่ดี ผมภูมิใจในตัวคุณเหลือเกิน และรู้สึกว่าคุณเป็นคนที่ไว้วางใจได้) หรือ *"I found you to be very interesting woman with a kind heart"* (ผมพบว่าคุณเป็นผู้หญิงที่น่าสนใจและจิตใจดีมาก) หรือ *"I must confess that i am so happy to hear from your previous message in AD, and it keeps putting smiles on my face."* (ผมต้องสารภาพเลยว่า ผมเป็นสุขอย่างยิ่งที่ได้รู้ข้อความจากคุณ และมันทำให้ผมมีรอยยิ้มบนใบหน้า) เป็นต้น

6) การแสดงบทบาทของการเป็น "คนที่รู้จักสำนึกบุญคุณ" ลักษณะประเภทนี้มักใช้เป็นข้ออ้างในการขอยืมเงิน และสัญญาว่าจะใช้คืนอย่างแน่นอน นอกจากการคืนเงินที่ยืมมาแล้วยังเตรียมของพิเศษบางอย่างสำหรับให้เหยื่อด้วย เช่น เราจะพบกันที่ประเทศของคุณ เป็นต้น ตัวอย่างเช่น *"I am very grateful for your help so far and I must pay you back even with interest. I shouldn't be that ungrateful not to surprise you with something you will marvel with as my beloved. I have something special for you as we finish with this and I coming to meet you over there in your country."* (ผมขอบคุณมากๆ สำหรับการช่วยเหลือครั้งนี้ และไม่ต้องห่วงเพราะผมจะจ่ายคืนคุณทั้งหมด คุณจะต้องประหลาดใจกับสิ่งที่ผมเตรียมไว้ให้คุณโดยเฉพาะ สุดที่รักของผม หลังจากเสร็จสิ้นภารกิจแล้ว ผมจะไปพบคุณที่ประเทศคุณทันที)

5. การสร้างสถานการณ์

เมื่อเป้าหมายเกิด "ตกหลุมรัก" รวมไปถึงการไว้วางใจ หรือเชื่อมั่นเรื่องราวต่างๆ ที่เหล่าอาชญากรประกอบสร้างขึ้นนั้นถือเป็นความสำเร็จอีกขั้นหนึ่ง ซึ่งจะนำไปสู่การสร้างสถานการณ์เรื่องราวต่างๆ เพื่อทำให้เป้าหมายตกเป็นเหยื่อของการโอนเงิน หรือจ่ายเงิน สถานการณ์ที่ scammer สร้างขึ้นมักทำให้เหยื่อรู้สึกสงสาร และต้องการให้ความช่วยเหลือ อาจด้วยเหตุผลจากการความสงสาร ประกอบ

[48] Whitty, M. T., (2015), Anatomy of the online dating romance scam. *Security Journal,* 28(4), 443-455.

[49] Shadel, D., and Dudley, D., AARP The Magazine, *"'Are You Real?' — Inside an Online Dating Scam",* https://www.aarp.org/money/scams-fraud/info-2015/online-dating-scam.html

กับความคาดหวังว่าการช่วยเหลือทางการเงินเป็นทางออกที่ทำให้ทั้งคู่ได้พบกันเร็วมากขึ้น รวมถึงความคาดหวังว่าทรัพย์สินเหล่านั้นจะตกเป็นของพวกเธอ/พวกเขาที่เป็นการพิสูจน์ว่าคู่สนทนาจะมาใช้ชีวิตร่วมกันที่ประเทศไทยอย่างแท้จริง จากการศึกษาพบว่า สถานการณ์ที่ถูกใช้อ้างอยู่บ่อยครั้งมีดังนี้

5.1 *มีปัญหาทางการเงินอย่างเร่งด่วน และต้องการขอความช่วยเหลือทางการเงิน* เช่น จ่ายค่ารักษาพยาบาลของตนเองหรือสมาชิกครอบครัว (พ่อ แม่ บุตร พี่น้อง) ค่าเล่าเรียน ธุรกิจถูกโกง ธุรกิจมีปัญหาต้องใช้เงินด่วน เกิดอุบัติเหตุ ลูกป่วยหนัก ขอเงินซื้อตั๋วเครื่องบิน/ทำวีซ่าเพื่อเดินทางมาพบเหยื่อ ค่าเช่าห้อง เป็นต้น และจะคืนเงินให้กับเหยื่อภายใน 2-3 วัน ข้อความจะเป็นรูปแบบคล้ายๆ กัน ดังนี้ *"I have little problem at the office now because I have got the cheque here in the office but I was told to go to the Bank to cash the cheque but here in the bank they say I have to open an account but the money that is why I call you……if you can help me with little money to complete everting and I promise you after I finish I have to return back the money to you"* (ตอนนี้ฉันมีปัญหานิดหน่อยที่สำนักงานเพราะฉันได้รับเช็คแต่ต้องไปขึ้นเงินที่ธนาคาร แต่ตอนนี้ธนาคารบอกกับฉันว่าต้องเปิดบัญชีเพื่อนำเงินเข้าอีก... ถ้าคุณสามารถช่วยฉันด้วยเงินจำนวนเล็กน้อยเพื่อให้ภารกิจลุล่วงไปได้ ฉันสัญญากับคุณว่าจะคืนเงินให้ทันที (ตอนนี้ฉันมีปัญหาทางธุรกิจนิดหน่อย) และพบตัวอย่างเรื่องราวที่เกิดขึ้นจริง ดังนี้

- ผู้หญิงไทย อายุ 33 ปี เข้าแจ้งความเพื่อให้เจ้าหน้าที่ตำรวจดำเนินคดีกับนายบรรพต เนียมกุล อายุ 40 ปี ด้วยข้อหาฉ้อโกง[50] เธอเล่าว่า *"ได้พบกับ scammer ผ่านทางแอพฯหาคู่ โดยชายใช้ชื่อ 'โชค' เป็นคนไม่มีครอบครัว เป็นเจ้าของธุรกิจรับเหมาแห่งหนึ่ง หลังจากนั้นก็มีการพูดคุยกันเรื่อยมารวมถึงมีการ Videocall กันแบบเห็นหน้าด้วย หลังจากสร้างความไว้ใจ สนิทสนมกันแล้ว เขาก็สร้างอุบายว่า....ลืมเอากระเป๋าเงินมาของยืมเงินประมาณ 1,000 บาทก่อน เพื่อจะเอาไว้ทานข้าว...หลังจากนั้นก็มีการอ้างเหตุการณ์ต่างๆ มาเรื่อยๆ เช่น ต้องเดินทางด่วน ต้องไปถ่ายรูปงาน ลืมเอากระเป๋าเงินมา ซึ่งในแต่ละครั้งก็โอนเงินไปให้มากน้อย ต่างกันไป จนวันหนึ่งได้อ้างว่าพ่อของเขาป่วย ต้องเข้าโรงพยาบาล มีเงินไม่พอที่ใช้จ่ายค่าโรงพยาบาล และตอนนี้ก็หมุนเงินไม่ทัน ตนก็ตกลงโอนเงินไปให้อีก 32,000 บาท เมื่อเหยื่อทวงถามก็บอกว่าจะคืนให้โดยเร็ว ละบอกว่ารักตนมาก จนกระทั่งเหยื่อเริ่มสงสัยเพราะเริ่มพูดแต่เรื่องเงินตลอด จึงได้นัดเจอกัน แต่นายโชคก็ไม่มา และไม่สามารถติดต่อเขาได้อีกเลย โดยเหยื่อเสียเงินไปทั้งหมด 650,000 บาท"*
- ผู้หญิงไทยอีกรายหนึ่งที่คุยกับวิศวกร ชาวอังกฤษ อ้างว่ามาติดต่อธุรกิจที่มาเลเซีย แต่พอมาถึงกลับพบว่าบัตรเครดิตใช้การไม่ได้จึงมาขอความช่วยเหลือ เขาบอกว่า *"Darling, I Need about 6'500 Malaysia money so that I can pay for my hotel because now I still don't have a better place to stay...the little money with me I can not take it because my credit card is not working here in .Malaysia that's why am. Worried"* (ที่รัก, ฉันต้องการเงินสัก 6,500

[50] คมชัดลึก, (2562), *แอปหาคู่ !! สาวถูกหลอกโอน 6 แสน*, (13 พฤษภาคม 2562), สืบค้นจาก http://www.komchadluek.net/news/crime/3 5 5 2 5 3 ?qt&fbclid=IwAR3 E4 EB8 7 6 yEhJhnh-oVYgIM_LU43GiVIdeywcCTbhhH_4X9 KRgqjr2yIWI

ริงกิต เพื่อจ่ายค่าโรงแรม เพราะตอนนี้ยังไม่มีที่ให้พักได้เลย เงินจำนวนเล็กน้อยนี้จะทำให้ฉันอยู่รอดได้ เพราะบัตรเครดิตของฉันใช้การที่มาเลเซียไม่ได้เลย ฉันเลยเป็นกังวลมาก) หลังจากการโอนค่าโรงแรมครั้งนั้น เขาเริ่มขอความช่วยเหลือทางธุรกิจที่เพิ่มขึ้น *"There said that i should paid 35,000,00 dollars for my tax rate before receiving my payment bet i have 30,000,00 dollars with me and mom have called her friend to help us to complete this money and her friend promise to send 3,000.00 dollars for us.....Can you been able to help me with the remaining 2,000.00 dollars to complete this money and pay for my tax.....Once i receive my payment here and join you over there i will be happy to pay you back Even if you can borrow for me once i recover my payment here and join you in Thailand i will pay you back and we can live a happy life together"* (มีการพูดกันว่าฉันต้องจ่ายเงินเป็นจำนวน 35,000 ดอลลาร์เป็นค่าภาษีสำหรับการรับการชำระเงินของฉันออกมา ฉันมีเงินอยู่แล้ว 30,000 ดอลลาร์ และแม่ขอฉันก็มีเงินอยู่แล้ว 3,000 ดอลลาร์เพื่อการนี้ ไม่ทราบคุณจะสามารถช่วยเหลือผมสัก 2,000 ดอลลาร์เพื่อเป็นค่าภาษีแล้วบรรลุภารกิจนี้ได้ไหมครับ เมื่อผมได้เงินของผมมาแล้วจะรีบไปหาคุณที่นู่นแล้วยินดีเป็นอย่างยิ่งที่จะคืนเงินให้กับคุณ หรือไม่ถ้าคุณสามารถหยิบยืมเงินมาให้ฉันได้ เมื่อฉันได้รับเงินของฉันจากที่นี่มาแล้วก็จะรีบไปหาคุณที่เมืองไทยเลย แล้วฉันจะคืนเงินให้แล้วเราก็จะได้ใช้ชีวิตร่วมกันอย่างมีความสุข)

- ผู้หญิงจากรัฐแท็กซัส สหรัฐอเมริกาอายุ 50 ปี เล่าว่า *"เธอตอบรับเพื่อนบน Facebook คนหนึ่งชื่อ Charlie เขาอ้างว่าทำงานในอุตสาหกรรมก่อสร้างที่ใกล้จะเสร็จแล้วในแคลิฟอร์เนีย เขาพูดถูกทุกอย่าง เขาเอาใจใส่เธอ และรู้ว่าอะไรจะทำฉันรู้สึกดีขึ้น เขาเป็นคนดีมากจริงๆ ฉันรู้สึกได้ถึงความดีงามเหล่านั้นจากเขา จากนั้นทั้งคู่ก็เปลี่ยนไปสนทนาทาง e-mail และเริ่มแลกรูปซึ่งกันและกัน ทั้งคู่ติดต่อกันอย่างสนิทสนมเป็นเวลาหลายเดือน จนกระทั่งเขาต้องการเงินบางส่วนที่จะทำให้งานเสร็จเร็วขึ้น ฉันสัญญาว่าจะคืนเงินภายใน 24 – 48 ชั่วโมง เธอคิดทบทวนอยู่นานมาก และส่งเงินให้เขาครั้งแรกเป็นจำนวน 30,000 ดอลลาร์สหรัฐ ด้วยระยะเวลาผ่านไป 2 ปีจนสุดท้ายการติดต่อระหว่างเธอกับเขาจบลงด้วยการสูญเสียเงิน 2 ล้านดอลลาร์สหรัฐ เธอตัดสินใจแจ้ง FBI แต่ไม่ได้บอกใครเกี่ยวกับความอึดอัดและเสียใจหลังจากที่ตกหลุมรักผู้ชายที่มาหลอกเธอ ผู้ชายที่เธอไม่เคยได้พบเจอ แต่เอาเงินทุกสตางค์ที่เธอมีไปจนหมดสิ้น"*[51]

[51] FBI, (2017), *Romance Scams: "Online Imposters Break Hearts and Bank Accounts"*, from https://www.fbi. gov/news/stories/romance-scams

- ผู้หญิงชาวนอร์เวย์ อายุ 29 ปี เป็นนักศึกษา ป. โทในประเทศอังกฤษ[52] เล่าว่า *“เธอถูกหลอกจาก Scammer ที่อ้างตัวว่าเป็นชายชาวอิสราเอล อายุ 28 ปี โดยทั้งคู่พบเจอกันผ่านแอปพลิเคชันหาคู่ Tinder ซึ่งทั้งสองได้พบเจอกัน และมีการไปเดทด้วยกันจริงๆ โดย Scammer หลอกว่าเขาเป็นนักธุรกิจ มีบริษัทขายเพชร ซึ่งได้สร้างความไว้ใจโดยการพาไปขึ้นเครื่องบิน Private Jet เพื่อไปดินเนอร์ในอีกประเทศหนึ่ง ซึ่งในระหว่างนั้นเหยื่อได้พบเจอกับเพื่อนของ Scammer และเขาก็ดูแลเธอเป็นอย่างดี หลังจากนั้นฝ่ายชายก็สร้างแผนการว่ามีปัญหาเรื่องธุรกิจ ติดขัด ต้องการเงินก่อน ซึ่ง Scammer ก็ขอใช้บัตรเครดิตของเหยื่อ เพื่อเอาไปแก้ปัญหาธุรกิจก่อน และยังให้เหยื่อขยายวงเงินเพื่อซื้อตั๋วเครื่องบิน ค่าโรงแรม ค่าอาหาร และจะบอกว่าคืนเงินให้อย่างเร็วที่สุด แต่ Scammer ก็อ้างกับเหยื่อว่ายืมเงินเพียงนิดเดียวเท่านั้น และจะรีบคืนเงินให้เร็วที่สุด ด้วยความไว้ใจและความร่ำรวยที่เขาทำให้เธอเห็น ทำให้เหยื่อหลงเชื่อว่าเขาจะคืนเงินให้อย่างแน่นอน หลังจากที่เหยื่อให้ยืมเงินและเขาบอกว่าอีก 1 สัปดาห์จะคืนเงินให้นั้น ก็ถูกผลัดเรื่อยมา จนกระทั่งวันหนึ่งที่เธอรู้ว่า เธอถูกหลอก ซึ่งรวมเป็นเงินทั้งหมดเกือบ 200,000 เหรียญ”*

[52] LAKE, Z., and EFFRON, L., (2019), *Woman says a man she met on Tinder swindled her out of $200K: 'He didn’t just dump you, he never existed'*, *ABCNews* (13 พฤษภาคม 2562), สืบค้นจาก https://abcnews.go.com/US/woman-man-met-tinder-swindled-200k-didnt-dump/story?id=62806053

ในกรณีนี้ scammer มักส่งภาพถ่ายเพื่อยืนยันแก่เหยื่อว่าสถานการณ์ที่เล่าไปนั้นเกิดจริง ไม่ว่าจะเป็นภาพตนเอง/สมาชิกครอบครัวป่วย ราคาตั๋วเครื่องบินที่มีชื่อของตน หรือหลักฐานเอกสารใบเสร็จชำระเงินต่างๆ เป็นต้น

London Heathrow Apt (LHR) Sun, 09 Apr, **10:25**	Kuala Lumpur International Apt (KUL) Mon, 10 Apr, **06:45**	MH3 Malaysia Airlines Berhad	Fare Family: MH Flex Non stop	
388				
Kuala Lumpur International Apt (KUL) Mon, 10 Apr, **09:05**	**Bangkok (BKK)** Mon, 10 Apr, **10:15**	MH784 Malaysia Airlines Berhad	Fare Family: MH Flex Non stop	
Boeing 737-800				
Bangkok (BKK) Sat, 29 Apr, **19:40**	Kuala Lumpur International Apt (KUL) Sat, 29 Apr, **22:50**	MH781 Malaysia Airlines Berhad	Fare Family: MH Smart Non stop	
Boeing 737-800				
Kuala Lumpur International Apt (KUL) Sun, 30 Apr, **09:50**	**London Heathrow Apt (LHR)** Sun, 30 Apr, **16:35**	MH4 Malaysia Airlines Berhad	Fare Family: MH Smart Non stop	
388				

FARE BREAKDOWN

Passenger Type	Fare per person	Surcharges per person	Taxes per person	Total Fare per person	No of passengers	Total Fare
Adult	665.00	298.00	134.97	1,097.97	x 1	GBP 1,097.97

Total Air Fare: GBP 1,097.97

Emirates

Important information

Your Booking Reference
2Z6UX9

* This is your E-Ticket Itinerary Receipt. You must bring it with you to the airport for check-in, and it is recommended you retain a copy for your records.
* Each passenger traveling needs a printed copy of this document for immigration, customs, airport security checks and duty free purchases.
* Please familiarise yourself with the Conditions of Carriage and other information contained in this document.

NOTE: This is ONE WAY E-Ticket Itinerary Receipt for a passenger.

Passenger Name	Gender	Frequent Flyer NO.	Ticket No.	Issued	Ticket Total*
Frank Philips/Mr	Male		092-3456090778	9th Sep.2016 at 11:13 am	£ 2,894.34
				"Ticket Total for all passengers"	£ 2,894.34

Your Itinerary

Date	Flight Number	Departure / Arrival	Terminal	Status	Aircraft Type	Flight Information
10TH SEP.2016	EK5110	LONDON HEATHROW(LHR) 01:30 PM	3	Business Class	AIRBUS A380-800	Est journey Time:6 hours 55 Minutes Distance:5504 Kilometers.
10TH SEP.2016		DUBAI (DXB) INT. AIRPORT 11:25 PM	3			
11TH SEP.2016	EK342	DUBAI (DXB) INT. AIRPORT 10:30 AM	3	Business Class	BOEING 777-300ER	Est journey Time: 7 hours 15 Minutes Distance:5560 Kilometers.
11TH SEP.2016		KUALA LUMPUR INT. AIRPORT 09:45 PM	M			

TOTAL TIME: 25 HOURS 15 MINUTES (1 stop)
Connection in Dubai: 11 hour 5 minutes

Your Receipt Details

Ticket Charges	Charges*	GST*	Total*
Fare	2100.00	0.00	2100.00
Fees/Taxes/Charges	500.00	0.00	500.00
Fuel Surcharges	200.00	0.00	200.00
Ticket values subtotal			2,800.00
Additional Charges			
Booking fee	94.34	0.00	94.34
Additional Charges subtotal			94.34
Ticket Total for all Passenger*	2,894.34		£ 2,894.34

* All amounts are displayed in U.S. dollar(USD)

Payment Details

Date	Payment	Reference Type	Amount*
9/9/2016	Visa	xxxx-xxxx-xxxx-7884	£ 2,894.34
		Total*	£ 2,894.34

This may appear as multiple transactions on your statement

Tax Information

GST does not apply to international travel. No tax invoice will be issued.

Issued by Emirates Airlines

ภาพที่ 22 ตัวอย่างภาพที่ scammer มักนำมายืนยันในสถานการณ์ขอความช่วยเหลือ เช่น ภาพการบาดเจ็บ ตั๋วเครื่องบิน เป็นต้น

5.2 *ชวนให้โอนเงินร่วมลงทุนสร้างธุรกิจ เพื่อเก็บเงินมาใช้ชีวิตร่วมกันในบั้นปลาย "หญิงสาววัยกลางคน ได้คุยกับ Scammer เป็นชาวอังกฤษผิวขาว คุยกับประมาณ 1 เดือน สร้างความคุ้นเคยและบอกว่าจะลงทุนทำธุรกิจด้วยกัน หลังจากนั้นก็เริ่มไถ่ถามขอยืมเงิน ครั้งแรกบอกว่าเป็นค่าเดินทางไปสร้างธุรกิจ 15,000 บาท ต่อมาอีก 2 วันก็ขอให้เหยื่อโอนเงินไปให้อีก 55,000 บาท เพราะครั้งแรกเป็นค่าเช่าไปก่อน แต่ครั้งนี้เป็นค่าดำเนินการธุรกิจจริงๆ แล้วก็จะเดินทางมาประเทศไทย หลังจากนั้นก็โอนไปเรื่อยๆ ทั้งหมด 18 ครั้ง จำนวนเงินทั้งหมด 1,200,000 บาท เหยื่อได้ไปหยิบยืมเงินจากคนอื่นมามากมาย ทั้งเพื่อน ญาติ พี่น้อง เหยื่อรู้ตัวจากเพื่อนที่ตนไปยืมเงิน โดยเพื่อนบอกว่าเคยเจอเพื่อนที่มายืมเงินด้วยเหตุการณ์แบบนี้ เหยื่อจะรู้ตัวได้ว่า ตอนนี้โดนหลอกแล้ว แต่ก็ได้สูญเงินไปกว่า 1 ล้านบาทแล้ว"*[53]

5.3 *ส่งทรัพย์สินมีค่าให้เหยื่อ* ได้รับมรดกจากพ่อแม่ หรือขอแต่งงาน และพร้อมที่จะย้ายมาอยู่ในประเทศของเหยื่อ หรือเป็นทหารที่ได้รับเงินจำนวนมากจากการยึดทรัพย์สินของศัตรู หรือเหตุผลอื่นใดเพื่อจะสื่อว่าต้องการส่งสิ่งของ หรือทรัพย์สินต่างๆ มาให้เหยื่อ แต่ติดปัญหาที่กรมศุลกากร สนามบิน หรือสถานีตำรวจ เหยื่อต้องโอนเงินค่าธรรมเนียมก่อนจึงจะได้รับทรัพย์สินเหล่านั้น scammer จะส่งภาพทรัพย์สิน ของมีค่าต่างๆ ให้แก่เหยื่อ เพื่อล่อตาล่อใจว่ามีสิ่งของดังกล่าวอยู่ในกล่องพัสดุนั้น ยิ่งเป็นแรงจูงใจให้เหยื่อยอมจ่ายค่าธรรมเนียมอื่นใดเพื่อให้ได้กล่องพัสดุนั้นมาตัวอย่างเช่น

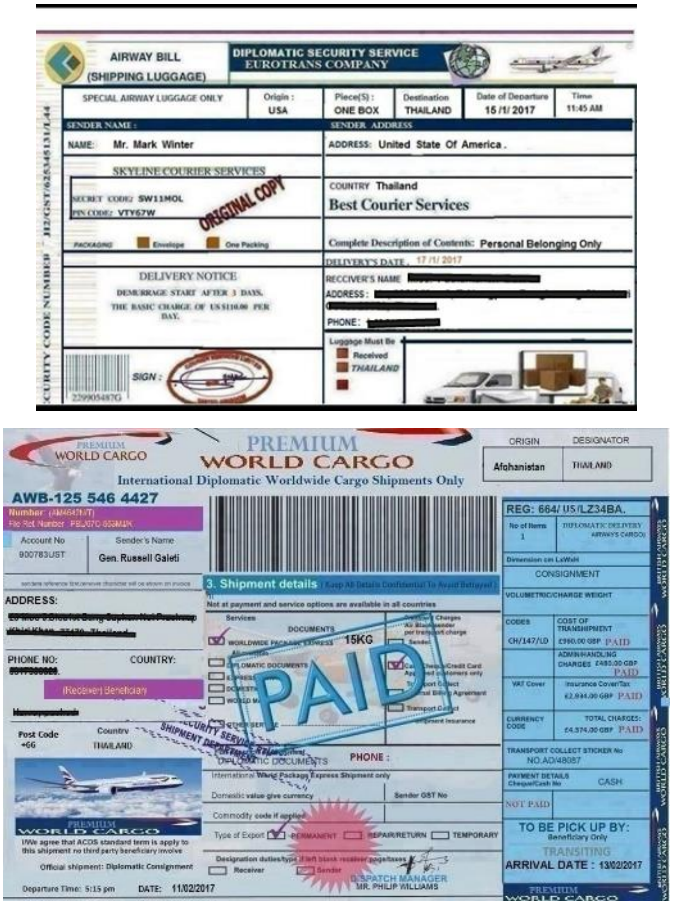
- คุณเกรท ผู้ก่อตั้งเพจ Thai anti Scam[54] เล่าว่า *"ถูกหลอกว่ามีเงินมรดก และจะต้องมาที่มาเลเซียเพื่อเอานำเงินออก และมรดกก็จ่ายเป็นเช็คอยู่ในบริษัทประกัน โดยจะเอาเงินนั้นมาเพื่อสร้างครอบครัวอยู่แล้วกัน ทั้งสองใช้เวลาพูดคุยกันประมาณ 1 เดือน เพื่อสร้างความผูกพัน ความไว้ใจ หลังจากนั้นก็เริ่มหลอกว่าเงินมรดกนั้น ต้องเสียภาษีก่อน โดย scammer บอกว่า ตอนนี้ขาดเงินอีก 400,000 กว่าบาท เพราะว่ายืมญาติ พี่น้อง ยืมเพื่อนมาแล้ว แต่มันยังไม่พอ ด้วยความที่เหยื่อเชื่อใจ และรู้สึกสงสารก็โอนเงินทั้งหมดไปให้ทาง เวสเทิร์น ยูเนี่ยน เป็นบัญชีของคนมาเลเซีย และบอกว่าเจ้าของบัญชีนั้นเป็นทนายที่อยู่ในประเทศมาเลเซีย เพิ่มน้ำหนักความน่าเชื่อถือให้เหยื่อ หลังจากนั้นก็ Scammer ก็ติดต่อกลับบอกว่าเอาเช็คมรดกออกมาแล้ว แต่มีค่าดำเนินการ ค่าเปิดบัญชีเพิ่มเข้ามา ประมาณ 44,000 บาท บอกเหยื่อให้ขายรถ ขายบ้าน มาช่วยเหลือตน แต่เหยื่อก็รู้จักแปลกใจหลังจากนั้นก็รู้ว่าตกเป็นเหยื่อ ซึ่ง Scammer ก็ได้ทำการบล็อกเหยื่อ และตัดการพูดคุยกันไปแล้ว"*

[53] PPTV, (2558), *แชทตุ๋นลวงโลก*, สืบค้นจาก https://www.pptvhd36.com/programs/%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A7%E0%B8%B2%E0%B9%84%E0%B8%A3%E0%B8%95%E0%B8%B5%E0%B9%89/%E0%B8%A5%E0%B9%88%E0%B8%B2/49470#part-3

[54] Thai Anti Scam (สาวไทยรู้ทันกลลวง), (2561), *ล่า (แชทตุ๋นลวงโลก) 41.3*, สืบค้นจาก https://www.facebook.com /sao.thai.rutan.kolluang/videos/1881064811975914/

- *“คู่สนทนาบอกว่าเป็นทหารอยู่ที่แคลิฟอร์เนีย อายุ 46 ปี โดยหลอกเหยื่อว่าจะส่งเงินสดมาทางเครื่องบินของ FedEx โดยอ้างว่าเงินไปติดอยู่ที่ศุลกากร จังหวัดภูเก็ต (จังหวัดที่เหยื่ออาศัยอยู่) และขอให้เหยื่อโอนเงินเพื่อจ่ายค่าภาษีในการนำกล่องพัสดุนั้นออกมา”*[55]
- *“ผมต้องบอกคุณทุกอย่างเกี่ยวกับผมเพราะคุณเป็นส่วนหนึ่งของอนาคตของฉันจากนั้นด้วยการไปถึงสิ่งที่ผมอยากจะบอกคุณที่จริงผมมีประมาณ $ 1.5 ล้านดอลลาร์ที่นี่ใน บริษัท รักษาความปลอดภัยให้เงินนี้เราทำให้มันจากจำนวนเงินที่ใหญ่ของเงินที่เรายึดมาจากห้องพักที่แข็งแกร่งของซัดดัมฮุสเซนในช่วงเวลาของการจับกุม ตอนนี้คุณมีความใกล้ชิดกับผมเป็นเพื่อนที่ดีที่สุดของฉันรักของฉันและภรรยาของฉันจะเป็นคนเดียวที่ฉันสามารถไว้วางใจและการแบ่งปันความลับนี้กับผมต้องการที่จะย้ายเงินนี้โดยบริการภูมิคุ้มกันจัดส่งทูตไปยังประเทศของคุณเพื่อให้ คุณสามารถบันทึกและเก็บเงินสำหรับการลงทุนของเราในอนาคตและการซื้อของบ้านจนกว่าฉันจะได้พบคุณมีในประเทศของคุณอีกครั้งภารกิจของฉันเสร็จเร็วๆ นี้”*
-

[55] Thai Anti Scam (สาวไทยรู้ทันกลลวง), (2561), สืบค้นจากhttps://www.facebook.com/sao.thai.rutan.kolluang/photos/pcb.2277156485700076/2277155959033462/?type=3&theater



ภาพที่ 23 ภาพหลักฐานที่เหยื่อได้รับจากคู่สนทนาชาวต่างชาติที่อ้างว่าส่งของมีค่ามาให้

ในกรณีนี้มักตามมาด้วยการติดต่อจากคนไทย ที่อ้างตนว่าเป็นเจ้าหน้าที่ศุลกากร เจ้าหน้าที่สนามบิน หรือเจ้าหน้าที่บริษัทส่งพัสดุ โดยการติดต่อกับเหยื่อในช่องทางนี้อาจเป็นทางโทรศัพท์ แชทข้อความทั้งทาง Line และ Messenger กลุ่มคนเหล่านี้มักบอกกับเหยื่อว่าพัสดุที่ส่งมามีค่ามากเกินไป ต้องเสียภาษีก่อนจะได้รับพัสดุ หรืออ้างว่าเจ้าหน้าที่ตรวจเจอทรัพย์สินมีค่าจำนวนมากจึงถูกกักไว้ตรวจสอบต้องจ่าค่าธรรมเนียมเพื่อเอาพัสดุออก หรืออ้างว่าพัสดุดังกล่าวไม่ได้ชำระค่าจัดส่งต้องชำระค่าจัดส่งก่อน ตัวอย่างของการกกล่าวอ้างเช่น

- บริษัท Air carrier delivery company โทรเข้ามาแล้วบอกว่า *“ทางบริษัทขอแจ้งว่ามีพัสดุมาจาก US ขอให้ชำระค่าส่งด่วนจำนวน 18,900 บาท เมื่อชำระแล้วของจะนำส่งภายใน 4 ชม. โดยส่งข้อความให้โอนเงินเข้าบัญชี ธนาคารกรุงเทพ เลขที่ XXX-X-XXX82-4 ชื่อ XXXXXXXXXX”* เมื่อเหยื่อถามกลับว่าทำไมต้องจ่ายเงิน ปลายสายตอบกลับมาว่า *“ค่าตอบแทนของตัวแทนที่เมืองไทยและข้างในมีของมูลค่า 2100,000 US”*
- มีเบอร์โทรแจ้งว่าให้จ่ายภาษีค่าพัสดุที่ได้ระวางและได้รับการประเมินจากศุลกากร อีกสองวันต่อมาได้รับ E-mail จากบริษัท HUBLINE DIPLOMATIC COURIER เพื่อให้จ่ายค่าภาษีและค่าธรรมเนียมทางบริษัทฯ จำนวนเงิน 36,355.00 บาท จะได้จัดส่งพัสดุในลำดับต่อไป โดยมีเลขบัญชีของ Account Name: XXXXXXXXXX Account

No : XXX-XXXX55-4 Bank Name : SCB THAI หลังจากโอนเงินก้อนแรกไปอีกสองวันได้รับ E-mail อีก 1 ฉบับจากบริษัทเดิมแจ้งเกี่ยวกับรายละเอียดการโอนเงินเพื่อประกันพัสดุ จำนวนเงิน 82,750.00 บาท ให้กับเจ้าของบัญชีอีกคนหนึ่ง ธนาคาร CIMB

5.4 *กำลังเดินทางมาหาเหยื่อ แต่เกิดปัญหาระหว่างการเดินทางทาง* เช่น กระเป๋าที่บรรจุเงิน/ทรัพย์สินมาจำนวนมากถูกยึด กระเป๋าเงินหาย ถูกกักตัวอยู่ที่สนามบิน บัตรเครดิตใช้การไม่ได้ เป็นต้น ต้องการขอความช่วยเหลือจากเหยื่อ และเป็นข้ออ้างของการหลีกเลี่ยงการมาพบกันในโลกความเป็นจริง เหตุผลนี้ยิ่งทำให้เหยื่อให้ความช่วยเหลืออย่างรวดเร็ว เพราะต้องการพบหน้าคู่สนทนาตามที่คาดหวังไว้ ตัวอย่างเช่น

- *"คู่สนทนากำลังจะเดินทางมาเพื่อสร้างครอบครัวกับเหยื่อ และถูกหลอกว่าเขามาถึงสนามบินภูเก็ตแล้ว แต่ถูกเจ้าหน้าที่ของสนามบินภูเก็ตกักตัวไว้ เพราะเขาเอาเงินสดและทรัพย์สินติดตัวมาด้วย และเจ้าหน้าที่บอกว่าเป็นเงินต่างประเทศที่นำเข้ามาไม่ถูกกฎหมาย ตีเป็นเงินไทยประมาณ 15 ล้านบาท ซึ่งจะต้องนำเงินมาเสียค่าปรับก่อนจึงจะปล่อยตัวเข้ามาได้ โดยเหยื่อก็หลงเชื่อและโอนเงินเข้าไปทั้งหมด 5 บัญชี โดยชื่อแต่ละอันก็ไม่ซ้ำกัน และหลายวันผ่านมาก็มีเจ้าหน้าที่โทรเข้ามาอีกว่า พบทองจำนวนหนึ่งและต้องเสียภาษีเพิ่ม ก็ให้โอนเงินเข้าไปอีก และด้วยความสงสาร Scammer ว่าตั้งใจมาหาตนแล้ว ก็ยอมโอนเงินไปให้อีก โดยครั้งสุดท้ายตนตัดสินใจเอาบ้านไปจำนองเพื่อเอาเงินมาจ่ายให้ จนสุดท้ายก็ติดต่อกับ Scammer ไม่ได้* และถูกหลอกให้โอนเงิน 800,000 บาท" [56]

ตัวอย่างจากเหยื่อในต่างประเทศที่สูญเงินนับ 100,000 ดอลลาร์ให้แก่ scammer - Georgina[57] เล่าว่า *"เธอเจอชายคนหนึ่งใน Facebook ชื่อ Jim เขาเป็นจ้าหน้าที่กองกำลังรักษาสันติภาพในอัฟกานิสถานที่ถูกส่งไปไนจีเรีย แต่ใกล้จะเกษียณแล้ว และสร้างอนาคตไว้ว่าจะออกมาใช้ชีวิตร่วมกัน Jim ตั้งใจจะเปิดร้านอัญมณีเพราะเขาชอบอัญมณี เราสนิทกันมากและคุยกันทาง e-mail ทุกวันเนื่องจาก Jim บอกว่ามันสะดวกกว่าการใช้เฟซบุ๊ก.....Jim บอกเธอว่ากำลังมาพบเธอ แต่บัตรเครดิตธนาคารของเขามีปัญหาใช้ในไนจีเรียไม่ได้ และไม่สามารถจ่ายภาษีส่งออกอัญมณีได้ Georgina จึงโอนเงินไปให้ 15,000 ดอลลาร์ เพราะหวังว่าเงินจำนวนนี้จะช่วยให้ทั้งคู่ได้ใช้ชีวิตร่วมกัน จากนั้น Jim บอกว่าได้หยุดพักระหว่างทางที่ประเทศมาเลเซีย เขาถูกยึดอัญมณีไว้และต้องจ่ายเงิน 20,000 ดอลลาร์ เพื่อนำมันออกมา ซึ่งตอนนั้นเธอก็ส่งให้กับเจ้าหน้าที่ของมาเลเซีย จากนั้นเจ้าหน้าที่แจ้งว่า Jim ติดคุกเพราะมีสิ่งของหนีภาษี Georgina ต้องติดต่อกับทนายของเขา และเป็นอีกครั้งที่เธอโอนเงิน*

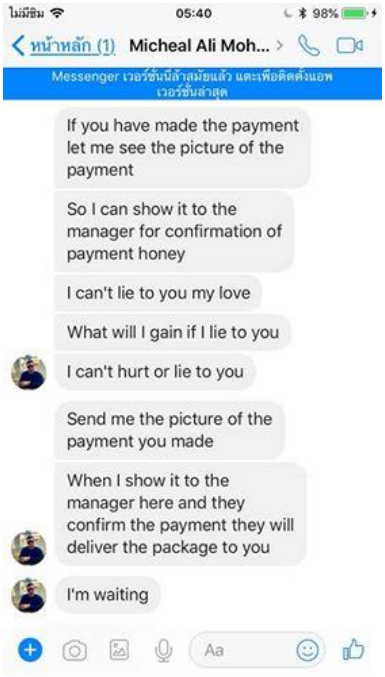
---

[56] บุญชู พวงมาลา, (2562), *หญิงวัย 60 ปีถูกชายต่างชาติอ้างเป็นทหารรักจริงหลอกโอนเงินสูญเงินเกือบล้านบาท, 77 ข่าวเด็ด*, (20 พฤษภาคม 2562), สืบค้นจาก https://www.77kaoded.com/content/483682?fbclid=IwAR3L8Gt7QEh-V5wQmXlQt0ADlG4kKutemSVY4gANVOzwEnvmdfYiHB7nsy0

[57] The ACCC and Scamwatch, *"Dating & romance scam: Georgina's Facebook fiancé leaves her flat broke"*, from https://www.scamwatch.gov.au/get-help/real-life-stories/dating-romance-scam-georginas-facebook-fianc%C3%A9-leaves-her-flat-broke

จำนวน 15,000 ดอลลาร์ ให้แก่ทนาย (เธอเชื่อแบบนั้น) เพื่อค่าธรรมเนียมศาล และทำใบรับรองการต่อต้านการก่อการร้ายและการฟอกเงิน”

อย่างไรก็ตามมีเหยื่อหลายคนที่ไม่ยอมโอนเงินให้แก่คู่สนทนา อาจด้วยเหตุผลที่ตระหนักได้แล้วว่าตนถูกหลอก หรือด้วยเหตุผลทางการเงิน scammer จะพยายามเกลี่ยกล่อมเหยื่อให้ถึงที่สุดด้วยการส่งข้อความแสนหวานมาอีกครั้ง หรือบางครั้งก็ขู่ว่าจะปิดการติดต่อกับเหยื่อหากไม่ยอมโอนเงิน ตัวอย่างเช่น



ภาพที่ 24 ตัวอย่างข้อความที่ scammer พยายามเกลี่ยกล่อมเหยื่อ

หากดูสถิติของสถานการณ์ที่ถูกอ้างในประเทศไทย มักเป็นการส่งทรัพย์สิน และของมีค่ามาทางบริษัทขนส่งให้ด้วยการอ้างเหตุผลต่างๆ นานา แต่สิ่งของเหล่านั้นไม่ผ่านการตรวจสอบ หรือติดอยู่ที่ศุลกากร/สนามบิน ต้องให้เหยื่อจ่ายค่าธรรมเนียมเพื่อนำพัสดุออกมาได้ครบถ้วน โดยจะมีผู้ที่เป็นตัวแทนติดต่อกับเหยื่อทั้งทางโทรศัพท์ Line หรือแชทข้อความ Messenger จะอ้างตนว่าเป็นเจ้าหน้าที่ศุลกากร เจ้าหน้าที่สนามบิน หรือเจ้าหน้าที่บริษัทส่งพัสดุ เป็นต้น ซึ่งผู้ที่ติดต่อกับเหยื่อในขั้นตอนนี้มักเป็นคนไทย จะทำการเจรจาด้วยการชักจูงและอ้างเหตุผลอีกมากมายเพื่อให้เหยื่อยอมโอนเงินให้กับบัญชีที่ถูกเปิดขึ้นในประเทศไทย

6. ช่องทางการโอนเงิน

ช่องทางการโอนเงินแบ่งได้ออกเป็น 3 ช่องทาง

6.1 โอนเงินไปยังบัญชีต่างประเทศ บัญชีปลายทางส่วนใหญ่มักจะเป็นประเทศมาเลเซีย หรือไนจีเรีย ด้วยการโอนเงินผ่านช่องทางสถาบันการเงิน Western Union ทั้งอาจเพราะการโอนเงินไปยังต่างประเทศด้วยช่องทางธนาคารมีขั้นตอนค่อนข้างยุ่งยาก เนื่องจากแต่ละธนาคารมีนโยบายอย่างชัดเจนในการป้องกันไม่ให้ธนาคารถูกใช้เป็นตัวกลางในการประกอบอาชญากรรมตามกฎหมายป้องกันและปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่ก่อการร้าย กรณีที่เหยื่อจะโอนเงินไปยังต่างประเทศโดยตรงมักเป็นเหตุการณ์ที่ scammer อ้างว่ามาติดต่อธุรกิจ หรือทำธุระต่างประเทศ และต้องการความช่วยเหลือทางการเงินจากเหยื่ออย่างด่วนที่สุด เพื่อให้หลุดพ้นจากเหตุฉุกเฉินที่กำลังเผชิญอยู่

6.2 โอนเงินไปยังบัญชีภายในประเทศ เป็นช่องทางหลักที่เหยื่อกว่า 90% ได้รับการร้องขอให้โอนเงินไปยังบัญชีของบุคคลอื่นที่ไม่ใช่คู่สนทนา และส่วนมากชื่อเจ้าของบัญชีมักเป็นชื่อของคนไทย แม้ว่าโปรไฟล์ที่ใช้หลอกเป็นคนละคนกัน แต่มักพบว่าจะอ้างแหล่งผู้รับเป็นชื่อซ้ำๆ กันอยู่มากพอสมควร อีกทั้งจากการเก็บข้อมูลพบว่าธนาคารที่ถูกร้องขอให้เหยื่อโอนเงินมากที่สุดคือ ธนาคารไทยพาณิชย์(SCB) รองลงมาคือ ธนาคารทหารไทย(TMB) ธนาคารกรุงเทพ(BBL) ธนาคารกสิกร(K Bank) ตามลำดับ อย่างไรก็ตามยังมีธนาคารอื่นที่พบได้คือ ธนาคารธนชาต ธนาคารซีไอเอ็มบี(CIMB) ธนาคารกรุงศรีอยุธยา เป็นต้น ผู้เสียหายผู้หญิงรายหนึ่งเล่าว่า *“คนรักของตนบอกว่าจะส่งของมาให้มูลค่าหลายล้านดอลลาร์ จากนั้นมีผู้หญิงโทรมาแจ้งว่าของติดอยู่ที่ศุลกากร ให้ตนโอนเงินเพื่อจะได้เอาของออกไปได้ ตนตกลงโอนเงินจำนวน 30,000 บาท โอนไปยังธนาคารไทยพาณิชย์ที่ชื่อบัญชีเป็นผู้หญิง หลังจากโอนเงิน 3-4 วัน คนรักคนนั้นก็ปิด Facebook ไปแล้ว”*[58]

6.3 นำเงินสดไปมอบด้วยตนเอง เหยื่อหลายคนคิดว่าการนำเงินไปให้คู่สนทนาด้วยตนเองนั้นถือเป็นโอกาสที่ดีที่จะได้พบกันในโลกความเป็นจริง เหยื่อคนหนึ่งเล่าผ่านเว็บไซต์ พันทิพย์ว่า *“เขาบอกนำเงินจำนวน 8,000,000 USD มาขอหมั้นด้วยเงินจำนวนนี้ก่อนและสิ้นปีจะมาแต่งงาน โดยจะให้นักการทูต 2 ท่านนำเงินเข้าประเทศไทยและให้เตรียมเงินไทย 200,000 สำหรับท่านทูตเป็นค่ายกกล่องเงินสด จากนั้นดิฉันเดินทางไปพารากอนซื้อผ้าพันคอ Hermes สำหรับ Clifford Rodney และซื้อของแบรนด์เนมอีก2 ชิ้นเพื่อเตรียมให้ท่านทูตเพื่อแสดงน้ำใจ มีผู้ชายโทรมาบอกว่าเป็นท่านทูตชื่อ Dr. George Anderson ได้เดินทางมาถึงสนามบินเรียบร้อยแล้วกำลังสำแดงของและจะให้ Dr. Johnson fedrick (ซึ่งเป็นทูตเช่นกัน) มารับเงินที่ CTW Starbucks ชั้น 3 เวลาประมาณ 11.00 น. ดิฉันไปตามนัดแต่งตัวภูมิฐานใส่สูทดูดีทำผมแต่งหน้า (พบท่านทูต UK นะต้องเป็นหน้า*

[58] ผู้ไม่ประสงค์ออกนาม, ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม, (7 เมษายน 2562). สัมภาษณ์.

เป็นตาให้หญิงไทยหน่อย) และได้มอบเงินครั้งแรก 200,000 บาทให้แต่โดยดีกับท่านทูตผิวดำชื่อ Dr.Johnson"[59]

เหยื่อหลายคนมักจะตระหนักได้ว่าตนเองถูกหลอกลวงก็ต่อเมื่อสูญเงินโอนเงิน/จ่ายเงินให้แก่ scammer ไปแล้วบางคนอาจตระหนักได้ในระยะเวลาอันสั้นโดยไม่เสียเงินมากเท่าใดนัก แต่บางคนสูญเงินไปนับแสนนับล้านจึงจะตระหนักได้ หรือบางคนให้เงินแก่ scammer จนสิ้นเนื้อประดาตัว และเริ่มหาเงินจากการกู้เงิน หรือยืมเงินคนรอบข้างเพื่อโอนไปยัง scammer เหยื่อส่วนมากที่กล้าไปแจ้งความเพื่อต้องการดำเนินคดีกับ scammer นั้นคือเหยื่อที่สูญเงินไปค่อนข้างมาก ทั้งนี้ยังมีเหยื่ออีกมากที่สูญเงินไปแต่ไม่กล้าไปแจ้งความเพราะความอับอายกับสถานการณ์ที่เกิดขึ้น ซึ่งสอดคล้องกับต่างประเทศตามรายงานของ The United States Attorney's Office Western District of Washington รายงานว่ามีเหยื่อพียง 15% ที่กล้าแจ้งความเพื่อดำเนินคดีตามกฎหมาย และเมืองที่พบผู้เสียหายเป็นอันดับต้นๆ คือ แคลิฟอร์เนีย เท็กซัส ฟอร์ลิด้า นิวยอร์ก และเพนซิวาเนีย[60] ซึ่งล้วนเป็นเมืองเศรษฐกิจสำคัญ

<u>กรณีพิเศษที่อาจพบได้เป็นการเฉพาะ</u>

มีบางกรณีที่ถือว่าเกิดขึ้นได้น้อยมาก แต่มิอาจละเลยได้คือการที่เหยื่อถูกกรรโชกทรัพย์ แบล็คเมล์ (Blackmail) เมื่อ scammer สานสัมพันธ์รักจนเหยื่ออยู่ในขั้นตกหลุมรัก และไว้วางใจคู่สนทนาแล้ว scammer มักชวนให้เหยื่อทำกิจกรรมรักออนไลน์ ไม่ว่าจะเป็นการส่งภาพโป๊เปลือย หรือร่วมเพศผ่านช่องทางการสื่อสารแบบเห็นหน้ากัน เช่น webcam, skype, video call เป็นต้น ซึ่งระหว่างที่เหยื่อกำลังทำกิจกรรมรักออนไลน์นั้น scammer จะบันทึกภาพเหล่านั้นไว้ และนำภาพเหล่านั้นกลับมา Blackmail เพื่อให้เหยื่อโอนเงิน แลกกับการไม่ปล่อยภาพกิจกรรมเหล่านั้นออกสู่โลกออนไลน์

อีกหนึ่งกรณีที่พบได้คือ การให้เหยื่อเดินทางไปต่างประเทศเพื่อพบกับ scammer แต่สุดท้ายเหยื่อก็ไม่ได้พบกับคู่สนทนาตามที่เหยื่อคาดหวังไว้ แต่เหยื่อจะพบกับคนอื่นๆ อีกมากมายที่เกี่ยวข้องกับคู่สนทนาของเหยื่อ และมีวัตถุประสงค์ที่จะหลอกเงินจากเหยื่อให้มากที่สุดในขณะที่เหยื่ออยู่ต่างประเทศนั้น ซึ่งเหตุการณ์ที่เกิดขึ้นจริงกับเหยื่อคนไทย คือ เหยื่อเป็นเจ้าของธุรกิจ อายุ 43 ปี หลังจากมีการพูดคุยติดต่อกับ Scammer เป็นระยะเวลา 5-6 เดือน ทาง Scammer บอกว่าจะมาหาตนที่ประเทศไทย แต่จะไปทำธุระที่ประเทศมาเลเซียก่อน จึงบอกให้ผู้เสียหายไปเจอกันที่มาเลเซีย เมื่อผู้เสียหายอยู่ที่มาเลเซีย Scammer โทรหาและบอกว่าตอนนี้ตนมีปัญหา คือ ไม่สามารถออกจากสนามบินได้ เพราะพกเงินสดมาเป็นจำนวนมาก ทางตรวจคนเข้าเมือง ไม่ให้ออกจากสนามบิน และต้องเสียภาษีก่อน จะให้ผู้เสียหายโอนเงินไปให้เพื่อตนจะออกจากสนามบินได้ แต่ในครั้งนี้ผู้เสียหายไม่ได้โอนเงินให้ เพราะอยู่ต่างประเทศ ต่อมาหลังจากที่ผู้เสียหายกลับมาประเทศไทย ทาง Scammer ได้ติดต่อมาว่า ตนออกจากสนามบินได้แล้ว เพราะญาติมาช่วยไว้ และตนกำลังเดินทางมาหาผู้เสียหายที่ประเทศไทย ให้มารอรับที่สนามบินสุวรรณภูมิด้วย ผู้เสียหายไปรอรับ Scammer และได้รับการติดต่อว่า ตม. ที่

---

[59] pantip.com, (ม.ป.ป), *เตือนภัยสาวไทย.....อยากมีแฟนชาวต่างชาติ แวะทางนี้หน่อยค่ะ!!!!*, สืบค้นจาก https://pantip.com/topic/ 34824282/page2

[60] Verafin, (2017), *Romance Fraud Scams: Five Key Indicators and Strategies for Uncovering Victims*, from https://verafin. com/2017/07/romance-fraud-scams/

สุวรรณภูมิไม่ให้ตนออกมา เพราะมีเงินสดมากเกินไป ในครั้งนี้ Scammer ให้โอนเงินจำนวน 1.5 แสนบาท หลังจากที่ผู้เสียหายโอนเงินให้ ก็ไม่สามารถติดต่อ Scammer ได้อีก[61]

ผลกระทบทางจิตใจที่ไม่สามารถประเมินค่าได้

เหยื่อส่วนใหญ่เสียใจมากเมื่อทราบว่าตนเองถูกหลอก มิใช่เพราะสูญเงิน แต่เพราะพวกเขารักอาชญากรอำพรางนั้นจริงๆ และผิดหวังกับความสัมพันธ์ดังกล่าวมากกว่าการสูญเงิน เนื่องจากพวกเข้าเชื่อจริงๆ ว่าการโอนเงินไปให้คู่แชทนั้นเป็นการแสดงความช่วยเหลือ และนำไปสู่การพัฒนาความสัมพันธ์ของพวกเขาทั้งคู่ เหยื่อหลายคนยอมรับว่าพวกเขาอายมาก ไม่กล้าเข้าแจ้งความ และเชื่อว่ากฎหมายไม่ได้ช่วยอะไร นอกจากนั้นบางคนยังตกเป็นเหยื่อของการมีส่วนร่วมในการฟอกเงินอีกด้วย บทความวิจัยของ Monica T. Whitty (2015) แสดงให้เห็นภาพรวมของปัญหาการฉ้อโกงรูปแบบหนึ่งที่เป็นการหาประโยชน์อย่างไม่ถูกต้องโดยการใช้เทคนิคทางสื่อสารมวลชน (เช่น อีเมล การแชทออนไลน์ หรือเว็บเครือข่ายสังคมออนไลน์) หรือที่เรียกว่า “Mass-Marketing Fraud” ซึ่งมีเป้าเหมายเป็นเหยื่อที่สามารถให้เงินแก่พวกอาชญากรได้ อันก่อให้เกิดผลกระทบทางจิตวิทยาต่อเหยื่อ[62] The Office of Fair Trading กล่าวว่า การหลอกลวงนี้ถือเป็นภัยเงียบ เพราะเหยื่อไม่สามารถมองเห็นว่านั่นคือผู้กระทำความผิด และจะรู้ตัวก็ต่อเมื่อการหลอกลวงนั้นสิ้นสุดไปแล้ว[63] ซึ่งก่อให้เกิดอันตรายทางจิตวิทยาไม่ว่าจะเป็น ความอับอาย ความละอาย ความอึดอัดลำบากใจ ความสะเทือนใจ ความหดหู่ ความโศกเศร้า ความรู้สึกอยากฆ่าตัวตาย ความวิตกกังวล และการสูญเสียความไว้วางใจ เป็นต้น ยิ่งไปกว่านั้นผู้ที่ตกเป็นเหยื่อมักถูกคนในสังคมมองว่าเป็นคนโง่และอ่อนต่อโลก และจากการสัมภาษณ์เหยื่อ romance scam ของ Markus Jakobsson (2016) พบว่า เหยื่อส่วนใหญ่มักถอนตัวออกกิจกรรมประจำโดยเฉพาะกิจกรรมที่เกี่ยวข้องกับอินเตอร์เน็ต เนื่องจากรู้สึกสูญเสียความไว้วางใจ และอับอายอย่างมากโดยที่ไม่ได้บอกให้ใครทราบเกี่ยวกับเรื่องที่เกิดขึ้น มันเป็นเรื่องอัปยศและยากที่จะเล่าเรื่องราวหรือประสบการณ์นั้นออกมา[64] อย่างไรก็ตามก็มีความพยายามในการให้ความสนับสนุนผู้ที่ตกเป็นเหยื่อผ่านทางเว็บไซด์ออนไลน์ เช่น www.romancescams.org และ www.scamsurvivors.com ถึงแม้ว่ายังไม่มีการศึกษาประสิทธิผลของการสนับสนุนนี้ในเชิงประจักษ์ก็ตาม

[61] ผู้ไม่ประสงค์ออกนาม, ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม, (7 เมษายน 2562). สัมภาษณ์.

[62] Whitty, M. T. (2015). Mass-marketing fraud: a growing concern. *IEEE Security & Privacy*, *13*(4), 84-87.

[63] “Helping People Affected by Scams: A Toolkit for Practitioners,” Office of Fair Trading, 2010.

[64] Yen, T. F., & Jakobsson, M. (2016). Case study: Romance scams. In Understanding Social Engineering Based Scams (pp. 103-113). Springer, New York, NY.

4.2. กฎหมายและมาตรการเฝ้าระวังและเตือนภัยล่วงหน้าเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม

ผลการศึกษาสะท้อนให้เห็นถึงอุปสรรคที่เกิดจากข้อจำกัดของกฎหมายและกลไกในการป้องกันและปราบปรามพิศวาสอาชญากรรม เพื่อนำไปสู่การพัฒนากฎหมายและมาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมให้ดียิ่งขึ้น จึงเกิดเป็นผลการศึกษา 2 หัวข้อ คือ

1) กฎหมายและมาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมในปัจจุบัน

2) แนวทางพัฒนากฎหมายและมาตรการเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม

4.2.1 กฎหมายและมาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมในปัจจุบัน

หากพิจารณาจากนิยามของ พิศวาสอาชญากรรม (Romance Scam) ซึ่งหมายถึง การที่นักต้มตุ๋น (Scammer) ได้ใช้เทคนิคทางจิตวิทยาผ่านเครื่องมือทางเทคโนโลยีต่างๆ ในการหลอกลวงให้ เหยื่อ (Victim) หลงเชื่อ จนกระทั่งยินยอมให้สิ่งต่างๆ ที่นักต้มตุ๋นต้องการ[65] โดยกลยุทธ์ที่นักต้มตุ๋นมักใช้ในการหลอกลวง คือ การสร้างโปรไฟล์ปลอมๆ ขึ้นมาในโซเชียลมีเดียต่างๆ อาทิ Facebook หรือเว็บไซต์หาคู่ต่างๆ (Dating website/App) โดยข้อมูลที่นำมาใช้ทำโปรไฟล์เหล่านี้ก็นำมาจากการขโมยข้อมูล เช่น ชื่อ ประวัติ และรูปภาพของคนอื่น แล้วเอามาดัดแปลงเป็นข้อมูลของตนเอง หรืออาจจะสร้างข้อมูลปลอมๆ ขึ้นมาเอง โดยเหยื่อที่นักต้มตุ๋นเหล่านี้มองหา มักจะเป็นมีคุณสมบัติหนึ่งที่สำคัญคือ ต้องเป็นคนขี้อ่อนไหว และขี้เหงา แบบต้องการใครสักคนมาอยู่เคียงข้าง[66]

กฎหมายที่เกี่ยวข้องกับความผิดฐานนี้มีหลายฉบับด้วยกัน ไม่ว่าจะเป็นประมวลกฎหมายอาญา ประมวลกฎหมายวิธีพิจารณาความอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560 หรือพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556 นอกจากนี้ ขั้นตอนหรือกระบวนการในการรวบรวมพยานหลักฐานของเจ้าพนักงานยังมีอุปสรรคต่าง ๆ มากมาย ประกอบกับลักษณะการกระทำความผิดที่ผู้ต้องหามักสร้างตัวตนและข้อมูลส่วนบุคคล เช่น Profile หรือ IP Address ปลอม มีรูปแบบการกระทำความผิดที่เป็นกระบวนการ และยังเป็นการกระทำความผิดที่เกี่ยวข้องกับเทคโนโลยี เมื่อนำมาพิจารณากับข้อจำกัดด้านทรัพยากร ไม่ว่าจะเป็นด้านงบประมาณ หรือเครื่องมือที่ใช้ตรวจสอบการกระทำความผิดที่ต้องมีความทันสมัยอยู่ตลอดเวลา เพื่อให้เท่าทันกับเทคโนโลยีที่เปลี่ยนไปอยู่ตลอดเวลาแล้ว ยังรวมถึงข้อจำกัดด้านจำนวนเจ้าหน้าที่ที่มีความรู้ความสามารถเฉพาะด้าน ทำให้การรวบรวมพยานหลักฐานเพื่อยืนยันตัวผู้กระทำความผิดเป็นไปได้ยาก

1) ข้อกฎหมายที่เกี่ยวข้อง

เนื่องด้วยคดีพิศวาสอาชญากรรม (Romance Scam) เป็นคดีที่มีรูปแบบการกระทำความผิดเป็นการเฉพาะตัว คือมีการใช้ “ความรัก” ในการหลอกลวงทรัพย์สินจากผู้เสียหาย ความผิดฐานแรกที่

---

[65] วชิรวิทย์ คงคาลัย, (2560), *“Romance Scam: ไม่รักไม่ว่าอะไร แต่ใยต้องหลอกกันด้วย”* (17 กรกฎาคม 2560), สืบค้นจาก https://www.the101.world/life/romance-scam/

[66] เรื่องเดียวกัน.

เกี่ยวข้องจึงเป็นความผิดฐานฉ้อโกง[67] และเนื่องจากเป็นการกระทำความผิดที่มีลักษณะร่วมมือกันอย่างเป็นกระบวนการ โดยที่ผู้กระทำความผิดมักเป็นคนต่างชาติที่ร่วมมือกับคนไทยในการกระทำความผิด โดยคนต่างชาติกลุ่มนี้จะเข้ามาในราชอาณาจักรในฐานะนักท่องเที่ยว และมีการเดินทางข้ามไปมาระหว่างประเทศไทยกับประเทศมาเลเซียซึ่งเป็นแหล่งที่มั่นสำคัญ[68] ความผิดที่เกี่ยวข้องประการต่อมาจึงเป็นความผิดตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ[69] และจะใช้วิธีการให้คนไทยผู้ร่วมขบวนการเป็นคนติดต่อกับผู้เสียหาย หรือเป็นเจ้าของบัญชีที่ใช้ในการกระทำความผิดในไทย[70] ดังนี้ ก็จะเป็นความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ไม่ว่าจะเป็นฐานมีหรือใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ[71] หรือฐานมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ[72] นอกจากนี้ยังรวมถึงความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในเรื่องการนำข้อมูลที่บิดเบือนหรือปลอมหรือเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ด้วย โดยประการที่น่าจะก่อให้เกิดความเสียหายแก่ประชาชน[73] และความผิดฐานนำเข้าสู่ระบบคอมพิวเตอร์ที่

---

[67] ประมวลกฎหมายอาญา มาตรา 341

มาตรา 341 ผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง และโดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สาม ทำ ถอน หรือทำลายเอกสารสิทธิ ผู้นั้นกระทำความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

[68] พนักงานอัยการ, (2562), อัยการจังหวัดประจำสำนักงานอัยการสูงสุด, (16 มกราคม 2562), สัมภาษณ์.

[69] พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556 มาตรา 3

“องค์กรอาชญากรรม” หมายความว่า คณะบุคคลตั้งแต่สามคนขึ้นไปที่รวมตัวกันช่วงระยะเวลาหนึ่งและร่วมกันกระทำการใด โดยมีวัตถุประสงค์เพื่อกระทำความผิดร้ายแรงและเพื่อได้มาซึ่งผลประโยชน์ทางการเงิน ทรัพย์สิน หรือผลประโยชน์ทางวัตถุอย่างอื่น ไม่ว่าโดยทางตรงหรือทางอ้อม

“องค์กรอาชญากรรมข้ามชาติ” หมายความว่า องค์กรอาชญากรรมที่มีการกระทำความผิดซึ่งมีลักษณะอย่างหนึ่งอย่างใด ดังต่อไปนี้

(1) ความผิดที่กระทำในเขตแดนของรัฐมากกว่าหนึ่งรัฐ

(2) ความผิดที่กระทำในรัฐใดรัฐหนึ่ง แต่การตระเตรียม การวางแผน การสั่งการ การสนับสนุน หรือการควบคุมการกระทำความผิดได้กระทำในอีกรัฐหนึ่ง

(3) ความผิดที่กระทำในรัฐหนึ่ง แต่เกี่ยวข้องกับองค์กรอาชญากรรมที่มีการกระทำความผิดมากกว่าหนึ่งรัฐ

(4) ความผิดที่กระทำในรัฐหนึ่ง แต่ผลของการกระทำที่สำคัญเกิดขึ้นในอีกรัฐหนึ่ง

[70] พนักงานสอบสวน, (2562), สถานีตำรวจแห่งหนึ่งในจังหวัดเชียงใหม่, (30 เมษายน 2562), สัมภาษณ์.

[71] ประมวลกฎหมายอาญา มาตรา 269/5

มาตรา 269/5 ผู้ใดใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

[72] ประมวลกฎหมายอาญา มาตรา 269/6

มาตรา 269/6 ผู้ใดมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/5 ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

[73] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14 (1)

มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น โดยเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง หรือได้รับความอับอายด้วย[74]

ความเป็นส่วนตัว (Privacy) และข้อมูลส่วนบุคคล (Personal Data) ได้รับการคุ้มครองโดยกฎหมายสิทธิมนุษยชนที่รัฐไทยเป็นภาคีจึงมีผลผูกพันรัฐไทยให้มีพันธกรณีในการเคารพ ปกป้อง และเติมเต็มให้กับบุคคลผู้เป็นเจ้าของสิทธิ รวมทั้งยังปรากฏอยู่ในรัฐธรรมนูญไทย พ.ศ. 2560 มาตรา 32 อย่างชัดเจน อย่างไรก็ดียังไม่มีกฎหมายเฉพาะในการให้นิยาม ขอบเขต ที่ชัดเจนเป็นการเฉพาะในการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการประกาศใช้ โดยมาตรา 6 ได้ให้นิยามคุ้มครอง “ข้อมูลส่วนบุคคล” หมายความถึง “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ” ดังนั้นจึงต้องอาศัยแนวทางของกฎหมายดังกล่าวมาใช้วิเคราะห์ ความเป็นส่วนตัว (Privacy) และข้อมูลส่วนบุคคล (Personal Data) ที่มักถูกกล่าวถึงแบบรวบยอดรวมกันว่า “ความเป็นส่วนตัวของข้อมูล” (Information Privacy) อันหมายถึง สิทธิที่จะอยู่ตามลำพังปราศจากการแทรกแซง และเป็นสิทธิที่เจ้าของจะสามารถควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น

2) ผู้เสียหาย

เมื่อการกระทำความผิดในคดี Romance Scam เป็นความผิดที่ใช้ความรักเป็นสาระสำคัญในการหลอกลวง จึงมีผู้เสียหายเป็นจำนวนมากที่ไม่เชื่อว่าตนนั้นกำลังถูกหลอก ส่งผลให้แม้ว่าจะมีคนตักเตือน แต่ผู้เสียหายส่วนมากก็เลือกที่จะไม่เชื่อและยังคงตกเป็นเหยื่อของผู้กระทำผิด[75] และเมื่อรู้ตัวว่าถูกหลอกแล้ว ผู้เสียหายส่วนมากก็จะไม่กล้าเข้าแจ้งความกับพนักงานตำรวจเนื่องจากความอับอาย[76]

ผู้เสียหายไม่ได้ไปแจ้งความเนื่องจากอับอายและขั้นตอนการดำเนินคดียุ่งยาก และถ้าไปแจ้งความจะต้องขาดงานไป รวบรวมพยานหลักฐาน ไปโรงพักบ่อยๆ ขาดงานบ่อย เลยตัดสินใจไม่ไปแจ้งความ แต่ได้ส่งข้อมูลการหลอกลวงทั้งหมดให้แอดมินเพจเพื่อให้เตือนภัย ป้องกันไม่ให้เกิดกรณีแบบนี้อีก แอดมินเพจ แนะนำทั้งหมดเกี่ยวกับการดำเนินคดี แต่ญาติกลัวอับอาย และความยุ่งยากไปโรงพักบ่อยๆ จึงตัดสินใจไม่ไปแจ้งความ[77]

---

(1) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอม ไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

[74] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 16

มาตรา 16 ผู้นำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

[75] พนักงานสอบสวน, (2562), สถานีตำรวจแห่งหนึ่งในจังหวัดเชียงใหม่, (30 เมษายน 2562), สัมภาษณ์.

[76] ผู้ดูแลเพจ, (2562), เพจภัยผู้หญิง ในโลกออนไลน์, (17 มกราคม 2562), สัมภาษณ์.

[77] ผู้เสียหายไม่ประสงค์ออกนาม คนที่ 2. ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม. (7 เมษายน 2562). สัมภาษณ์.

ผู้เสียหายได้เข้าร้องทุกข์แจ้งความดำเนินคดีต่อตำรวจมาแล้ว 2-3 ปี แต่พอรู้ว่าคนกระทำความผิดอยู่ต่างประเทศ จึงได้เข้าแจ้งความกับตำรวจท้องที่ และก็แจ้งปอท. แต่ก็ยังไม่มีความคืบหน้า ทางเจ้าหน้าที่ตำรวจติดตามคดีแต่ไม่มีความคืบหน้า จนคนรับทำคดีถูกย้ายไปหน่วยงานอื่นแล้ว[78]

การที่เหยื่อหรือผู้เสียหายไม่เข้าแจ้งความดำเนินคดี เรียกร้องชดเชยค่าเสียหาย หรือบางรายกว่าจะยอมมาดำเนินการแจ้งความก็ถูกหลอกจนเกือบจะหมดตัว แม้วันที่เหยื่อเข้ามาแจ้งความดำเนินคดีบางรายยังไม่เชื่อว่าตนเองจะถูกหลอก บางรายมีการนัดเจอตัวและจับเรียกค่าไถ่หรือถูกฆ่าปิดปากเสียด้วยซ้ำ เพราะด้วยกลุ่มที่ตกเป็นเหยื่อส่วนใหญ่ซึ่งเป็นกลุ่มวัยกลางคนที่เข้าใจว่าตนเองผ่านร้อนผ่านหนาวมามากมีประสบการณ์ในการใช้ชีวิตเป็นอย่างดี ตลอดจนการที่เหยื่อเป็นผู้มีการศึกษาดีย่อมเข้าใจว่าตนจะไม่ถูกหลอกจากเหล่าอาชญากรได้อย่างง่ายดาย แต่เหยื่อกลุ่มนี้ลืมไปว่าโลกในสังคมปัจจุบันมีการเปลี่ยนแปลงไปมาก เหยื่อเป็นกลุ่มคนที่ค่อนข้างมีฐานะและมีการศึกษาดีดังนั้นเหยื่อส่วนใหญ่จะอายและไม่กล้ามาแจ้งความ หรือบางรายไม่อยากเสียเวลาเนื่องจากการทำคดีประเภทนี้ค่อนข้างใช้เวลานาน[79]

ในบางกรณีผู้เสียหายเลือกไม่แจ้งความเพราะอับอาย และเป็นเรื่องที่อาจจะไม่มั่นใจในกระบวนการยุติธรรมหรือกระบวนการติดตามจับกุมผู้กระทำความผิดและสืบทรัพย์กลับคืนมาว่าจะตามได้หรือไม่ หรืออาจจะเป็นเพราะเวลาเกิดคดีเหล่านี้หากเป็นข่าวขึ้นมาในเครือข่ายสังคมออนไลน์ เกรงว่าจะนำไปสู่การเยาะเย้นถากถาง (Cyber Bully) ด้วย จึงไม่ต้องการที่จะเปิดเผยข้อเท็จจริง [80]

กอรปกับคนในสังคมไทยไม่ค่อยอยากจะไปยุ่งยากอะไรเกี่ยวกับกระบวนการทางกฎหมายหรือการขึ้นศาลหรือเจอตำรวจเพราะฉะนั้นถ้าสมมุติเขาไม่ได้เกิดความเสียหายมากนัก ก็คงไม่อยากจะดำเนินการก็อาจจะปล่อยไป เนื่องจากการเข้าสู่กระบวนการทางกฎหมายสร้างความยุ่งยากสำหรับเขา หากเป็นคนที่มีการศึกษามีหน้าตาในสังคมบางทีการเข้าไปแจ้งความแล้วบอกว่าตัวเองโดนหลอกมันทำให้เขาเสื่อมเสียชื่อเสียงเสื่อมเสียสถานะทางสังคมและอาจกระทบต่อหน้าที่การงานไปด้วย [81]

จากเงื่อนไขข้างต้นสะท้อนให้เห็นถึงความต้องการกระบวนการเยียวยาร้องทุกข์ที่มีลักษณะปกป้องเกียรติยศชื่อเสียงของเหยื่อ รวมไปถึงมีช่องทางร้องเรียนที่สามารถรักษาความเป็นส่วนตัวและรายงานความคืบหน้าของคดี ไปจนถึงมีประสิทธิผลในการบังคับใช้กฎหมายดำเนินคดีกับผู้กระทำความผิดและติดตามทวงทรัพย์สินกลับมาให้ผู้เสียหายได้

[78] ผู้เสียหายไม่ประสงค์ออกนาม คนที่ 3. ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม. (7 เมษายน 2562). สัมภาษณ์.

[79] นักวิชาการ. อาจารย์ประจำภาควิชาสังคมวิทยาและมานุษยวิทยา จุฬาลงกรณ์มหาวิทยาลัย. (14 กุมภาพันธ์ 2562). สัมภาษณ์.

[80] นักวิชาการ. อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. (17 มกราคม 2562). สัมภาษณ์.

[81] นักวิชาการ. อาจารย์ประจำ ภาควิชาสังคมและสุขภาพคณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล. (15 พฤษภาคม 2562). สัมภาษณ์.

3) กระบวนการยุติธรรม

ในคดีอาญาทั่วไป เมื่อมีความเสียหายเกิดขึ้นบุคคลซึ่งเป็นผู้เสียหายก็มีสิทธิในการแจ้งความร้องทุกข์[82] ต่อเจ้าหน้าที่ตำรวจ[83] หรืออาจยื่นฟ้องคดีต่อศาล[84] หรืออาจขอเข้าร่วมเป็นโจทก์กับพนักงานอัยการ[85] แต่ในคดี Romance Scam เมื่อมีความเสียหายเกิดขึ้น ขั้นตอนของการดำเนินคดีมักสะดุดและหยุดลงในชั้นของพนักงานสอบสวน เนื่องด้วยลักษณะการกระทำความผิดที่ไม่สามารถระบุได้อย่างแน่ชัดว่าเป็นกระทำผิดในขณะที่ผู้กระทำอยู่ในหรือนอกราชอาณาจักร อีกทั้งยังเป็นกรณีที่ผู้กระทำมักกระทำผิดด้วยการอำพรางตัวตนที่แท้จริงผ่านทาง Account หรือไอพี (IP Address) ปลอม ซึ่งทำให้ยากแก่การตรวจพิสูจน์และยืนยันตัวตนผู้กระทำความผิดด้วย

ในชั้นสอบสวน เมื่อผู้เสียหายได้เข้าแจ้งความร้องทุกข์ต่อพนักงานสอนสวนแล้ว ก็จะทำให้พนักงานสอบสวนมีอำนาจสอบสวนคดีอาญาทั้งปวง[86] และต้องเริ่มทำการสอบสวนโดยไม่ชักช้า[87] โดยต้องเป็นการรวบรวมพยานหลักฐานทุกชนิดเท่าที่จะกระทำได้ เพื่อทราบข้อเท็จจริงและพฤติการณ์ต่างๆ อันเกี่ยวกับความผิดที่ถูกกล่าวหา เพื่อจะรู้ตัวผู้กระทำผิดและพิสูจน์ให้เห็นความผิดหรือความบริสุทธิ์ของผู้ต้องหา[88] และเนื่องจากคดี Romance Scam เป็นคดีที่ผู้กระทำความผิดได้กระทำ

---

[82] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 1(7)

(7) “คำร้องทุกข์” หมายความถึง การที่ผู้เสียหายได้กล่าวหาต่อเจ้าหน้าที่ตามบทบัญญัติแห่งประมวลกฎหมายนี้ว่ามีผู้กระทำความผิดขึ้น จะรู้ตัวผู้กระทำความผิดหรือไม่ก็ตาม ซึ่งกระทำให้เกิดความเสียหายแก่ผู้เสียหาย และการกล่าวหาเช่นนั้นได้กล่าวโดยมีเจตนาจะให้ผู้กระทำความผิดได้รับโทษ

[83] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 123

มาตรา 123 ผู้เสียหายอาจต้องทุกข์ต่อพนักงานสอบสวนได้

คำร้องทุกข์นั้นต้องปรากฏชื่อและที่อยู่ของผู้ร้องทุกข์ ลักษณะแห่งความผิด พฤติการณ์ต่างๆ ที่ความผิดนั้นได้กระทำลง ความเสียหายที่ได้รับ และชื่อหรือรูปพรรณของผู้กระทำผิดเท่าที่จะบอกได้

คำร้องทุกข์นี้จะทำเป็นหนังสือหรือร้องด้วยปากก็ได้ ถ้าเป็นหนังสือต้องมีวันเดือนปีและลายมือชื่อของผู้ร้องทุกข์ ถ้าร้องด้วยปาก ให้พนักงานสอบสวนบันทึกไว้ ลงวันเดือนปีและลงลายมือชื่อผู้บันทุกกับผู้ร้องทุกข์ในบันทึกนั้น

[84] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 28

มาตรา 28 บุคคลเหล่านี้มีอำนาจฟ้องคดีอาญาต่อศาล

(1) พนักงานอัยการ

(2) ผู้เสียหาย

[85] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 30

มาตรา 30 คดีอาญาซึ่งพนักงานอัยการยื่นฟ้องต่อศาลแล้ว ผู้เสียหายจะยื่นคำร้องขอเข้าร่วมเป็นโจทก์ในระยะใดระหว่างพิจารณาก่อนศาลชั้นต้นพิพากษาคดีนั้นก็ได้

[86] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 120

มาตรา 120 ห้ามมิให้พนักงานอัยการยื่นฟ้องคดีใดต่อศาล โดยมิได้มีการสอบสวนในความผิดนั้นก่อน

[87] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 130

มาตรา 130 ให้เริ่มทำการสอบสวนรวบรวมหลักฐานทุกชนิด เท่าที่สามารถจะทำได้ เพื่อประสงค์จะทราบข้อเท็จจริงและพฤติการณ์ต่างๆ อันเกี่ยวกับความผิดที่ถูกกล่าวหา เพื่อจะรู้ตัวผู้กระทำผิดและพิสูจน์ให้เห็นความผิดหรือความบริสุทธิ์ของผู้ต้องหา

[88] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131

ความผิดทั้งในและนอกราชอาณาจักร และยังเป็นความผิดที่อาจไม่สามารถระบุถึงสถานที่ในการกระทำความผิดได้อย่างชัดเจน ดังนั้น จึงมีมักเกิดปัญหาขึ้นว่าพนักงานสอบสวนท้องที่ใดควรจะเป็นผู้มีอำนาจสอบสวน เพราะการสอบสวนโดยพนักงานสอบสวนที่ไม่มีอำนาจตามกฎหมายจะส่งผลให้การสอบสวนนั้นเป็นการสอบสวนที่ไม่ชอบด้วยกฎหมาย พนักงานอัยการไม่มีอำนาจฟ้อง[89] และศาลต้องยกฟ้องคดีนี้ในที่สุด[90]

กรณีความผิดเกิดขึ้นในราชอาณาจักร พนักงานสอบสวนสามารถดำเนินการสอบสวนและรวบรวมพยานหลักฐานต่าง ๆ สำหรับการกระทำความผิดที่เกิดขึ้นภายในเขตอำนาจของตนได้

กรณีที่ความผิดเกิดขึ้นในท้องที่เดียว และเป็นกรณีที่ความผิดเกิดขึ้นในจังหวัดอื่นนอกจากกรุงเทพมหานคร พนักงานสอบสวนที่มีอำนาจสอบสวนคือพนักงานสอบสวนในท้องที่ที่ความผิดอาญาได้เกิด หรืออ้าง หรือเชื่อว่าได้เกิดในเขตท้องที่ของตน หรือในท้องที่ที่ผู้ต้องหามีที่อยู่หรือถูกจับในท้องที่ของตน[91] แต่หากเป็นกรณีความผิดที่เกิดขึ้นในท้องที่เดียวและเป็นความผิดที่เกิดขึ้นในกรุงเทพมหานคร พนักงานสอบสวนที่มีอำนาจสอบสวนคือพนักงานสอบสวนในท้องที่ที่ความผิดได้เกิด หรืออ้าง หรือเชื่อว่าได้เกิด ภายในเขตอำนาจ หรือผู้ต้องหามีที่อยู่ หรือถูกจับภายในเขตอำนาจนั้น[92] ซึ่งโดยทั่วไปแล้วพนักงานสอบสวนที่เป็นผู้มีอำนาจสอบสวนจะเป็นพนักงานสอบสวนผู้รับผิดชอบในการรวบรวมสำนวนและทำความเห็นส่งให้พนักงานอัยการด้วย[93]

สำหรับความผิดในคดีพิศวาสอาชญากรรม Romance Scam มักเป็น**กรณีที่การเกิดขึ้นของความผิดเกี่ยวพันกับหลายท้องที่ หรือเป็นการไม่แน่ว่าการกระทำความผิดนั้นเกิดขึ้นในท้องที่ใดในระหว่างหลายท้องที่** เนื่องจากเป็นการกระทำความผิดที่เกิดขึ้นในอินเตอร์เน็ต พนักงานสอบสวนใน

มาตรา 131 ให้พนักงานสอบสวนรวบรวมพยานหลักฐานทุกชนิด เท่าที่สามารถจะทำได้ เพื่อประสงค์จะทราบข้อเท็จจริงและพฤติการณ์ต่างๆ อันเกี่ยวกับความผิดที่ถูกกล่าวหา เพื่อจะรู้ตัวผู้กระทำผิดและพิสูจน์ให้เห็นความผิดหรือความบริสุทธิ์ของผู้ต้องหา

[89] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 120

มาตรา 120 ห้ามมิให้พนักงานอัยการยื่นฟ้องคดีใดต่อศาล โดยมิได้มีการสอบสวนในความผิดนั้นก่อน

[90] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 161 วรรคหนึ่ง

มาตรา 161 ถ้าฟ้องไม่ถูกต้องตามกฎหมาย ให้ศาลสั่งโจทก์แก้ฟ้องให้ถูกต้องหรือยกฟ้องหรือไม่ประทับฟ้อง

[91] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 18 วรรคหนึ่ง

มาตรา 18 ในจังหวัดอื่นนอกจากจังหวัดพระนครและจังหวัดธนบุรี พนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ ปลัดอำเภอ และข้าราชการตำรวจซึ่งมียศตั้งแต่ชั้นนายร้อยตำรวจตรีหรือเทียบเท่านายร้อยตำรวจตรีขึ้นไป มีอำนาจสอบสวนความผิดอาญาซึ่งได้เกิด หรืออ้าง หรือเชื่อว่าได้เกิดภายในเขตอำนาจของตน หรือผู้ต้องหามีที่อยู่หรือถูกจับภายในเขตอำนาจของตนได้

[92] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 18 วรรคสอง

สำหรับในจังหวัดพระนครและจังหวัดธนบุรี ให้ข้าราชการตำรวจซึ่งมียศตั้งแต่ชั้นนายร้อยตำรวจตรีหรือเทียบเท่านายร้อยตำรวจตรีขึ้นไป มีอำนาจสอบสวนความผิดอาญาซึ่งได้เกิด หรืออ้าง หรือเชื่อว่าได้เกิดภายในเขตอำนาจของตน หรือผู้ต้องหามีที่อยู่หรือถูกจับภายในเขตอำนาจของตนได้

[93] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 18 วรรคสาม

ภายใต้บังคับแห่งบทบัญญัติในมาตรา 19 มาตรา 20 และมาตรา 21 ความผิดอาญาได้เกิดในเขตอำนาจพนักงานสอบสวนคนใด โดยปกติให้เป็นหน้าที่พนักงานสอบสวนผู้นั้นเป็นผู้รับผิดชอบในการสอบสวนความผิดนั้นๆ เพื่อดำเนินคดี เว้นแต่เมื่อมีเหตุจำเป็นหรือเพื่อความสะดวก จึงให้พนักงานสอบสวนแห่งท้องที่ที่ผู้ต้องหามีที่อยู่หรือถูกจับเป็นผู้รับผิดชอบในการดำเนินการสอบสวน

ท้องที่หนึ่งท้องที่ใดที่เกี่ยวข้องจึงเป็นพนักงานสอบสวนที่มีอำนาจสอบสวนในคดีนี้ และในกรณีที่ยังจับตัวผู้กระทำผิดไม่ได้ พนักงานสอบสวนในท้องที่ที่พบการกระทำความผิดก่อนหรือก็คือพนักงานสอบสวนในท้องที่ที่ผู้เสียหายเข้าร้องทุกข์ก่อน[94] จะเป็นพนักงานสอบสวนผู้รับผิดชอบ[95]

ส่วน**ความผิดที่มีโทษตามกฎหมายไทยได้กระทำลงไปนอกราชอาณาจักร**[96] อัยการสูงสุดหรือผู้รักษาการแทนจะเป็นพนักงานสอบสวนผู้รับผิดชอบ หรือจะมอบหมายหน้าที่นั้นให้กับพนักงานอัยการหรือพนักงานสอบสวนคนอื่นเป็นผู้รับผิดชอบทำการสอบสวนแทนก็ได้ และในกรณีจำเป็น ระหว่างที่รอคำสั่งจากอัยการสูงสุด พนักงานสอบสวนที่ผู้ต้องหาถูกจับในเขตอำนาจ หรือพนักงานสอบสวนซึ่งรัฐบาลประเทศอื่นหรือบุคคลที่ได้รับความเสียหายได้ร้องฟ้องให้ทำโทษผู้ต้องหานั้น พนักงานสอบสวนดังกล่าวมีอำนาจทำการสอบสวนไปพรางก่อนได้ อย่างไรก็ตาม ในกรณีที่ไม่แน่ว่าพนักงานสอบสวนคนใดในจังหวัดเดียวกันควรเป็นพนักงานสอบสวนผู้รับผิดชอบ ให้ผู้บังคับบัญชาของพนักงานสอบสวนนั้นเป็นผู้ชี้ขาด[97]

นอกจากนี้ การที่การกระทำความผิดในคดี Romance Scam มีลักษณะหรือรูปแบบของการกระทำความผิดที่เข้าข่ายเป็น<u>การกระทำความผิดขององค์กรอาชญากรรมข้ามชาติ</u>[98] ซึ่งผู้กระทำ

---

[94] คำพิพากษาฎีกาที่ 2880/2548, 1126/2544

[95] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 19

มาตรา 19 ในกรณีดังต่อไปนี้

(1) เป็นการไม่แน่ใจว่าการกระทำผิดอาญาได้กระทำในท้องที่ใดในระหว่างหลายท้องที่

(2) เมื่อความผิดส่วนหนึ่งกระทำในท้องที่หนึ่ง แต่อีกส่วนหนึ่งในอีกท้องที่หนึ่ง

(3) เมื่อความผิดนั้นเป็นความผิดต่อเนื่องและกระทำต่อเนื่องกันในท้องที่ต่างๆ เกินกว่าท้องที่หนึ่งขึ้นไป

(4) เมื่อเป็นความผิดซึ่งมีหลายกรรม กระทำลงในท้องที่ต่างๆ กัน

(5) เมื่อความผิดเกิดขึ้นขณะผู้ต้องหากำลังเดินทาง

(6) เมื่อความผิดเกิดขึ้นขณะผู้เสียหายกำลังเดินทาง

พนักงานสอบสวนในท้องที่หนึ่งท้องที่ใดที่เกี่ยวข้องมีอำนาจสอบสวนได้

ในกรณีข้างต้น พนักงานสอบสวนต่อไปนี้เป็นผู้รับผิดชอบในการสอบสวน

(ก) ถ้าจับผู้ต้องหาได้แล้ว คือ พนักงานสอบสวนซึ่งท้องที่ที่จับได้อยู่ในเขตอำนาจ

(ข) ถ้าจับผู้ต้องหายังไม่ได้ คือ พนักงานสอบสวนซึ่งท้องที่ที่พบการกระทำความผิดก่อนอยู่ในเขตอำนาจ

[96] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 20 วรรคหนึ่ง และวรรคห้า

มาตรา 20 ถ้าความผิดซึ่งมีโทษตามกฎหมายไทยได้กระทำลงนอกราชอาณาจักรไทย ให้อัยการสูงสุดหรือผู้รักษาการแทนเป็นพนักงานสอบสวนผู้รับผิดชอบหรือจะมอบหมายหน้าที่นั้นให้พนักงานอัยการหรือพนักงานสอบสวนคนใดเป็นผู้รับผิดชอบทำการสอบสวนแทนก็ได้

ในกรณีจำเป็น พนักงานสอบสวนต่อไปนี้มีอำนาจสอบสวนระหว่างรอคำสั่งจากอัยการสูงสุดหรือผู้รักษาการแทน

(1) พนักงานสอบสวนซึ่งผู้ต้องหาถูกจับในเขตอำนาจ

(2) พนักงานสอบสวนซึ่งรัฐบาลประเทศอื่นหรือบุคคลที่ได้รับความเสียหายได้ร้องฟ้องให้ทำโทษผู้ต้องหา

[97] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 21/1 วรรคหนึ่ง

มาตรา 21/1 สำหรับการสอบสวนซึ่งอยู่ในความรับผิดชอบของเจ้าพนักงานตำรวจ ในกรณีที่ไม่แน่ว่าพนักงานสอบสวนคนใดในจังหวัดเดียวกัน หรือในกองบัญชาการเดียวกันควรเป็นพนักงานสอบสวนผู้รับผิดชอบ ให้ผู้บัญชาการซึ่งเป็นผู้บังคับบัญชาของพนักงานสอบสวนนั้นเป็นผู้ชี้ขาด

[98] พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556 มาตรา 3

ความผิดและผู้ที่มีส่วนร่วมกระทำความผิดจะต้องรับโทษในราชอาณาจักรแม้ว่าจะได้กระทำความผิดเหล่านั้นนอกราชอาณาจักรก็ตาม ซึ่งพนักงานสอบสวนเป็นผู้มีหน้าที่ทำการสอบสวน เว้นแต่คณะกรรมการคดีพิเศษจะกำหนดให้คดีดังกล่าวต้องดำเนินการโดยกรมสอบสวนคดีพิเศษ[99] และเพื่อประโยชน์ในการประสานการทำงานให้อัยการสูงสุด ผู้บัญชาการตำรวจแห่งชาติ และหัวหน้าหน่วยงานของรัฐที่เกี่ยวข้องทำความตกลงกันเกี่ยวกับการปฏิบัติหน้าที่ระหว่างหน่วยงานของรัฐที่เกี่ยวข้องกับการกระทำความผิด[100]

4) ขั้นตอนในการสอบสวน

เมื่อผู้เสียหายได้เข้าแจ้งความแล้ว พนักงานสอบสวนก็จะต้องเริ่มทำการสอบสวนโดยไม่ชักช้า ซึ่งหนึ่งในขั้นตอนสำคัญที่จะทำให้ได้มาซึ่งตัวผู้กระทำความผิดคือ การรวบรวมพยานหลักฐานเพื่อเอาผิด และการจับกุมตัวผู้กระทำผิดมารับโทษนั่นเอง

การรวบรวมพยานหลักฐาน

ในคดีอาญา กฎหมายกำหนดให้โจทก์ต้องนำสืบพยานหลักฐานถึงขนาดที่ศาลเชื่อว่าจำเลยเป็นผู้กระทำผิดโดย “ปราศจากข้อสงสัย” หากโจทก์นำสืบไม่ได้ตามมาตรฐานที่กฎหมายกำหนด ศาลจะยกฟ้อง และพิพากษาว่าจำเลยไม่ได้กระทำความผิดตามที่โจทก์กล่าวหา[101] ดังนั้น การรวบรวมพยานหลักฐานของพนักงานสอบสวนจึงเป็นสิ่งสำคัญ เพราะพยานหลักฐานใดที่ได้มาโดยไม่ถูกต้องตามกระบวนการของกฎหมายย่อมไม่สามารถนำมาพิจารณาในชั้นศาลได้

“องค์กรอาชญากรรม” หมายความว่า คณะบุคคลตั้งแต่สามคนขึ้นไปที่รวมตัวกันช่วงระยะเวลาหนึ่งและร่วมกันกระทำการใด โดยมีวัตถุประสงค์เพื่อกระทำความผิดร้ายแรงและเพื่อได้มาซึ่งผลประโยชน์ทางการเงิน ทรัพย์สิน หรือผลประโยชน์ทางวัตถุอย่างอื่น ไม่ว่าโดยทางตรงหรือทางอ้อม

“องค์กรอาชญากรรมข้ามชาติ” หมายความว่า องค์กรอาชญากรรมที่มีการกระทำความผิดซึ่งมีลักษณะอย่างหนึ่งอย่างใด ดังต่อไปนี้

(1) ความผิดที่กระทำในเขตแดนของรัฐมากกว่าหนึ่งรัฐ

(2) ความผิดที่กระทำในรัฐใดรัฐหนึ่ง แต่การตระเตรียม การวางแผน การสั่งการ การสนับสนุน หรือการควบคุมการกระทำความผิดได้กระทำในอีกรัฐหนึ่ง

(3) ความผิดที่กระทำในรัฐหนึ่ง แต่เกี่ยวข้องกับองค์กรอาชญากรรมที่มีการกระทำความผิดมากกว่าหนึ่งรัฐ

(4) ความผิดที่กระทำในรัฐหนึ่ง แต่ผลของการกระทำที่สำคัญเกิดขึ้นในอีกรัฐหนึ่ง

[99] พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556 มาตรา 11

มาตรา 11 ในกรณีที่ความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ให้พนักงานสอบสวนทำการสอบสวนต่อไปได้ เว้นแต่คณะกรรมการคดีพิเศษได้มีมติให้คดีดังกล่าวต้องดำเนินการโดยกรมสอบสวนคดีพิเศษ ให้พนักงานสอบสวนส่งเรื่องให้กรมสอบสวนคดีพิเศษดำเนินการ

[100] พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556 มาตรา 12 วรรคหนึ่ง

มาตรา 12 เพื่อประโยชน์ในการประสานการปฏิบัติงานป้องกันและปราบปรามการกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ให้อัยการสูงสุด ผู้บัญชาการตำรวจแห่งชาติ และหัวหน้าหน่วยงานของรัฐที่เกี่ยวข้องตกลงกันเกี่ยวกับการปฏิบัติหน้าที่ในคดีระหว่างหน่วยงานของรัฐที่เกี่ยวข้อง

[101] อุดม รัฐอมฤต, (2558), *คำอธิบายกฎหมายลักษณะพยานหลักฐาน* (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม), กรุงเทพฯ : โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, หน้า 214.

สำหรับคดีที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ พยานหลักฐานที่ผู้เสียหายมีเมื่อนำคดีมาแจ้งความ สามารถแบ่งออกเป็น 3 รูปแบบ[102] คือ 1. คดีที่รู้ตัวผู้กระทำความผิดชัดเจน 2. คดีที่พอจะมีหลักฐานให้ตามสืบได้บ้างว่าผู้กระทำความผิดเป็นใคร 3. คดีที่ไม่รู้ตัวผู้กระทำความผิดเลย ผู้เสียหายทราบแต่เพียงว่าตนถูกหลอกลวง ซึ่งจำนวนและคุณภาพของพยานหลักฐานที่ผู้เสียหายมีนั้นจะส่งผลต่อการรวบรวมพยานหลักฐานของพนักงานสอบสวนด้วย

การสืบหาพยานหลักฐานอิเล็กทรอนิกส์

กระบวนการล่อลวงของ Romance Scam ถือเป็นอาชญากรรมทางคอมพิวเตอร์อย่างหนึ่ง ที่มีมูลค่าความเสียหายสูงอย่างมาก โดยผู้เสียหายมักจะถูกหลอกลวงผ่านทางแพลตฟอร์ม (platform) บนเครือข่ายอินเตอร์เน็ต เช่น Facebook, Tinder หรือ E-mail ซึ่งกระบวนการสืบหาผู้กระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์สามารถกระทำได้หลายวิธี ทั้งการสืบจาก IP Address หรือตรวจสอบจากข้อมูลจราจรทางคอมพิวเตอร์ (Traffics data) เพื่อให้ทราบว่าต้นทางที่ส่งมาจากสถานที่ใด รวมถึงกระบวนการที่มีความซับซ้อนอย่างเช่น กระบวนการสร้างค่า Hash ด้วย

เมื่อเกิดการกระทำความผิดขึ้นผู้เสียหายส่วนใหญ่มักจะนำหลักฐานที่เป็นเพียงรูปภาพที่เกิดจากการ Capture ผ่านหน้าจอคอมพิวเตอร์หรือโทรศัพท์ของตนเองมาเป็นหลักฐานในการแจ้งความดำเนินคดี[103] ซึ่งภาพเหล่านั้นเป็นสิ่งที่นำมาใช้ในการสืบหาผู้กระทำผิดได้ยาก หรือแทบจะระบุตัวผู้กระทำความผิดไม่ได้เลย จึงต้องมีการนำเอารายละเอียดที่เก็บอยู่ใน log file เพื่อจะนำเอาหมายเลขไอพี (IP Address) มาใช้ในการตรวจหาตัวผู้กระทำความผิด ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (แก้ไขเพิ่มเติม) 2560 นั้น ได้กำหนดขั้นตอนของการเก็บพยานหลักฐานดิจิตอลไว้ โดยกำหนดให้เฉพาะเจ้าหน้าที่ที่ได้รับแต่งตั้งขึ้นโดยอาศัยอำนาจตามพระราชบัญญัติฯ นี้เท่านั้นที่สามารถเรียกข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) จากผู้ให้บริการอินเตอร์เน็ตที่เกี่ยวข้องได้[104] โดยข้อมูลที่ได้จากผู้ให้บริการนั้นถือเป็นพยานหลักฐานทางดิจิทัล (Digital Evidence) ที่สำคัญอย่างหนึ่ง นอกจากนี้ พยานหลักฐานดังกล่าวจะต้องมีกระบวนการเก็บข้อมูลที่เรียกว่า Digital Forensics หรือ การพิสูจน์หลักฐานจากทางดิจิทัล[105] เพื่อป้องกันการปนเปื้อนของพยานหลักฐานด้วย ซึ่งการเก็บพยานหลักฐานดิจิทัลมีอยู่ 3 กระบวนการ ดังนี้

---

[102] พนักงานสอบสวน, (2562), สถานีตำรวจแห่งหนึ่งในจังหวัดเชียงใหม่, (30 เมษายน 2562), สัมภาษณ์.

[103] นักวิทยาศาสตร์ (สบ1), (2562), ศูนย์พิสูจน์หลักฐาน 5, (11 เมษายน 2562), สัมภาษณ์.

[104] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (แก้ไขเพิ่มเติม) 2560 ในมาตรา 18

มาตรา 18 ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่าการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอตามวรรคสองให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไป เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

[105] Digital Forensics หรือ การพิสูจน์หลักฐานจากทางดิจิทัล หมายถึง การเก็บรวบรวมและการจัดเตรียมข้อมูลที่เกี่ยวข้องจากคอมพิวเตอร์ เพื่อใช้ในการดำเนินคดีทางกฎหมาย ซึ่งกระบวนการนี้รวมถึงการกู้คืนไฟล์ หรือไฟล์ข้อมูลที่ต้องใช้วิธีการทางเทคนิคทางคอมพิวเตอร์ด้วย อ้างอิงจาก ETDA และ ThaiCERT, (2556), Digital Forensics, (20 มิถุนายน 2562), สืบค้นจาก https://www.thaicert.or.th/papers/general/2013/pa2013ge012.html

ก. การรวบรวมวัตถุพยานจากผู้เสียหาย

การรวบรวมวัตถุพยานอยู่ที่ต้นทาง คือ ผู้เสียหาย โดยผู้เสียหายจะเป็นคนรวบรวมวัตถุพยาน อย่างเช่น แชทที่มีการพูดคุยกัน รูปภาพที่ส่งมา account ปลอมที่ผู้เสียหายโดนหลอก ซึ่งไม่ว่าจะเป็นการรวบรวมเองของผู้เสียหายหรือจะเป็นการนำเครื่องคอมพิวเตอร์หรือเครื่องโทรศัพท์ดังกล่าวม าให้เจ้าหน้าที่เป็นคนรวบรวมตรวจสอบก็ได้[106] ในส่วนนี้จะเป็นการเริ่มต้นของกระบวนการหาตัวผู้กระทำความผิด กรณีที่ account ของผู้กระทำความผิดยังไม่ถูกปิดหรือถูกบล๊อคไป ก็ยังสามารถที่จะติดต่อพูดคุยกันต่อไปได้ แต่บางกรณีที่ผู้เสียหายไม่สามารถติดต่อกับผู้กระทำความผิดได้แล้วนั้น ก็จะเป็นการยากที่จะติดตามตัวผู้กระทำความผิด

ข. การรวบรวมพยานหลักฐานจากผู้ให้บริการอินเตอร์เน็ต

ในระหว่างการพูดคุยกันผ่านแพลตฟอร์ม อย่างเช่น Facebook เจ้าของแพลตฟอร์มหรือผู้ให้บริการอินเตอร์เน็ตต้องทำการเก็บ log file หรือข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) เอาไว้ตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (แก้ไขเพิ่มเติม) 2560 กำหนดไว้ คือ ให้ผู้ให้บริการอินเตอร์เน็ต (Internet Service Providers : ISP)[107] จะต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน[108] เพื่อให้เกิดความสะดวกรวดเร็วต่อการตรวจสอบของเจ้าหน้าที่หากมีการพบผู้กระทำผิดในภายหลัง โดยข้อมูลจราจรที่อาศัยอำนาจตามพระราชบัญญัติฉบับนี้สามารถใช้เป็นพยานหลักฐานในชั้นศาลได้[109] ซึ่งข้อมูลจราจรทางคอมพิวเตอร์ที่จะได้จากผู้ให้บริการอินเตอร์เน็ตนั้นจะแสดงรายละเอียดของไอพี (IP Address) ว่ามีไอพีใดบ้างที่ติดต่อสื่อสารกันอยู่ในขณะนั้น มีเวลาเริ่มต้นและสิ้นสุดอย่างไร หรือแสดงเบอร์โทรศัพท์ที่ใช้ในการติดต่อสื่อสาร เหล่านี้เป็นสิ่งที่เจ้าพนักงานหรือพนักงานสอบสวนสามารถแจ้งให้ผู้ให้บริการหมายเลขโทรศัพท์ดังกล่าวนั้นทำการ

---

[106] นักวิทยาศาสตร์ (สบ1), (2562), ศูนย์พิสูจน์หลักฐาน 5, (11 เมษายน 2562), สัมภาษณ์.

[107] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) 2560 มาตรา 3

มาตรา 3 ผู้ให้บริการ หมายความว่า

(1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเตอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

[108] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) 2560 มาตรา 26

มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มบริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร เมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรนี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

[109] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) 2560 มาตรา 25

มาตรา 25 ข้อมูล ข้อมูลคอมพิวเตอร์หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตราพระราชบัญญัตินี้หรือที่พนักงานสอบสวนได้ตามมาตรา 18 วรรคสอง ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำสั่งสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

ตรวจสอบให้ว่าเบอร์ดังกล่าวได้ลงทะเบียนไว้ในชื่อของใคร อาศัยอยู่ที่ไหน จนนำไปสู่การติดตามตัวผู้กระทำความผิดได้ แต่ในกรณีที่เป็นการพูดคุยผ่านแชทจะเป็นกรณีที่ไม่สามารถติดตามตัวได้ง่ายนัก เพราะสุดท้ายแล้วผู้เสียหายจะทราบเพียงว่าบุคคลที่เข้ามาคุยด้วยนั้นเป็น account ที่ถูกปลอมขึ้นมา ตัวจริงของบุคคลนั้นอาจจะไม่รู้จักหรือไม่เคยพูดคุยกับผู้เสียหายเลย ซึ่งกรณีดังกล่าวนี้หากทางผู้ให้บริการอินเตอร์เน็ตให้ความร่วมมือ เจ้าหน้าที่ก็จะสามารถตรวจสอบได้ถึงต้นตอหรือสามารถระบุได้ถึงที่อยู่ของผู้กระทำความผิดได้[110]

กระบวนการติดตามจากไอพี (IP Address) นี้เป็นสิ่งที่ต้องใช้เจ้าหน้าที่ที่มีความรู้ ความเชี่ยวชาญทางด้านคอมพิวเตอร์เป็นอย่างมาก และยังต้องเป็นเจ้าหน้าที่ที่ได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (แก้ไขเพิ่มเติม) พ.ศ. 2560 ด้วย[111] จึงจะมีอำนาจในการติดตามและรวบรวมพยานหลักฐาน เพราะกระบวนการเก็บรวบรวมและตรวจสอบหลักฐานทางดิจิทัลสามารถนำไปใช้เป็นพยานหลักฐานในชั้นศาลได้ การรวบรวมพยานหลักฐานจึงต้องมีการปฏิบัติตามขั้นตอน และต้องคุ้มครองพยานหลักฐานไว้อย่างดีที่สุด เพื่อป้องกันการปนเปื้อนของพยานหลักฐานนั้น

เมื่อได้ไอพี (IP Address) จากผู้ให้บริการอินเตอร์เน็ตหรือผู้ให้บริการที่เกี่ยวข้องแล้ว ขั้นตอนต่อไปที่เจ้าหน้าที่จะสามารถตรวจสอบได้ว่าใครเป็นเจ้าของไอพี (IP Address) หรือตำแหน่งที่ตั้งของผู้เป็นเจ้าของไอพีนั้น ซึ่งหมายเลขไอพี (IP Address) จะมีอยู่ 4 ชุด แต่ละชุดจะมีเครื่องหมายจุดขั้นระหว่างชุด (xxx.xxx.xxx.xxx) [112] ซึ่งไอพี (IP Address) ของเครื่องคอมพิวเตอร์แต่ละเครื่องจะมีค่าไม่ซ้ำกัน โดยสิ่งที่ตัวเลขทั้ง 4 ชุดนี้สามารถบ่งบอกได้ คือ เครื่องคอมพิวเตอร์นั้นอยู่ในเครือข่าย (network) ไหน เป็นเครื่องคอมพิวเตอร์เครื่องใดหรือของผู้ใดที่อยู่ในเครือข่าย (network) นั้น เพราะใน 1 เครือข่ายสามารถมีเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ร่วมกันได้หลายร้อยเครื่อง และหมายเลขไอพี (IP Address) นี้ยังทำให้ทราบได้ถึงตำแหน่งที่ตั้งของเครื่องคอมพิวเตอร์เครื่องนั้นด้วย ซึ่งเมื่อนำเอาหมายเลขดังกล่าวนั้นไปตรวจสอบ โดยอาจเป็นการตรวจสอบกับเว็บไซต์ที่ให้บริการในการตรวจสอบก็ได้ หรือใช้โปรแกรมสำหรับตรวจสอบ เป็นต้น และเมื่อใส่หมายเลขไอพี (IP Address) ลงไปในช่องที่ต้องการตรวจสอบแล้วจะปรากฏผลลัพธ์ออกมา เป็นชื่อของเครือข่ายหรือชื่อเจ้าของอินเตอร์เน็ตที่ใช้

---

[110] นักวิทยาศาสตร์ (สบ1), (2562), ศูนย์พิสูจน์หลักฐาน 5, (11 เมษายน 2562), สัมภาษณ์.

[111] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) 2560 มาตรา 28

มาตรา 28 การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

ผู้ที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ อาจได้รับค่าตอบแทนพิเศษตามที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

ในการกำหนดให้ได้รับค่าตอบแทนพิเศษต้องคำนึงภาระหน้าที่ ความรู้ความเชี่ยวชาญ ความขาดแคลนในการหาผู้มาปฏิบัติหน้าที่หรือมีการสูญเสียผู้ปฏิบัติงานออกจากระบบราชการเป็นจำนวนมากคุณภาพของงานและการดำรงตนอยู่ในความยุติธรรมโดยเปรียบเทียบค่าตอบแทนของผู้ปฏิบัติงานอื่นในกระบวนการยุติธรรม

[112] Mindphp, (4 ธันวาคม 2560), IP Address คืออะไร, (20 มิถุนายน 2562), สืบค้นจาก Mindphp: https://mindphp.com/%E0%B8%84%E0%B8%B9%E0%B9%88%E0%B8%A1%E0%B8%B7%E0%B8%AD/73-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3/2071-ip-address-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3.html

งานอยู่ รวมถึงชื่อประเทศ จังหวัด ชื่อเมือง ละติจูด ลองติจูด[113] เช่น OrgName : Yahoo.Inc , ISP : Advances Info Service Public Company Limited (AIS) , Country : Thailand และ City Name : Chiang Mai เป็นต้น

แต่ก็ยังมีกรณีที่ผู้กระทำความผิดใช้งาน VPN (Virtual Private Network) เพื่อปกปิดหมายเลขไอพี (IP Address) ไว้ หากเจอกรณีดังกล่าวนี้ก็จะก่อให้เกิดความยุ่งยากในการค้นหาตัวผู้กระทำความผิดเพิ่มมากขึ้น เพราะการใช้เครือข่ายอินเตอร์เน็ตผ่าน VPN นี้ จะทำให้ผู้ใช้บริการอินเตอร์เน็ตสามารถเชื่อมต่ออินเตอร์เน็ตกับเครือข่ายอินเตอร์เน็ตในประเทศใดก็ได้ เช่น ผู้กระทำความผิดอาศัยอยู่ที่ประเทศมาเลเซีย แต่ได้เชื่อมต่อบริการ VPN ให้เครือข่ายเน็ตเวิร์คของตนไปอยู่ที่ประเทศออสเตรเลีย ดังนั้นกระบวนการตรวจสอบจากไอพี (IP Address) ของผู้กระทำความผิดก็จะไม่แสดงว่าผู้กระทำความผิดอยู่ที่ประเทศมาเลเซีย แต่จะแสดงผลลัพธ์ว่าผู้กระทำความผิดอยู่ที่ประเทศออสเตรเลีย เป็นต้น หากเกิดกรณีดังกล่าวข้างต้นนี้ ก็จะทำให้ไม่สามารถตามตัวผู้กระทำความผิดได้เลย (ยกเว้นในประเทศที่มีการพัฒนาของเทคโนโลยีไปในขั้นสูงแล้วเท่านั้น)

ค. การรวบรวมพยานหลักฐานจากผู้กระทำความผิด

มักเป็นวัตถุพยานปลายทาง กล่าวคือ เป็นข้อมูลของผู้กระทำผิด ไม่ว่าจะเป็นโทรศัพท์มือถือ เครื่องคอมพิวเตอร์ รูปภาพ หรือไฟล์ข้อมูลอื่นๆ ที่ใช้ในการแอบอ้าง หรือปลอมผ่าน Account บนอินเตอร์เน็ต ซึ่งในขั้นตอนนี้ขึ้นอยู่กับว่าเจ้าหน้าที่จะสามารถจับกุมและยึดอุปกรณ์ในการกระทำความผิดได้หรือไม่[114] ด้วยเหตุที่ตัวผู้กระทำความผิดส่วนมากมักเป็นคนต่างชาติ และมีการเดินทางไปมาหลายพื้นที่ ไม่มีที่อยู่เป็นหลักเป็นแหล่ง หรือมีการหลอกลวงให้บุคคลอื่นเป็นผู้กระทำความผิดแทนตนเอง ทำให้การจับกุมตัวผู้กระทำผิดเป็นสิ่งที่ทำได้ยาก นอกเสียจากว่าบุคคลนั้นจะอยู่ในประเทศไทยในระยะเวลาหนึ่ง และเป็นผู้ที่ลงมือกระทำความผิดเอง โดยไม่ได้ใช้ให้บุคคลอื่นเป็นผู้กระทำแทน จึงจะมีโอกาสในการจับตัวได้ค่อนข้างสูง

ในกระบวนการนี้ เมื่อจับตัวผู้กระทำผิดพร้อมทั้งอุปกรณ์หรือเครื่องมือที่ใช้ในการกระทำความผิดได้แล้วนั้น เจ้าหน้าที่พิสูจน์หลักฐานจะต้องทำการตรวจสอบว่าเป็นผู้กระทำผิดที่จับตัวมานั้นเป็นผู้กระทำความผิดที่แท้จริงหรือไม่ ซึ่งในขั้นตอนนี้จะเป็นการตรวจสอบที่ต้องใช้เทคนิค และความรู้ความเชี่ยวชาญด้านคอมพิวเตอร์เป็นอย่างมาก กล่าวคือ กระบวนการตรวจสอบโดยการสร้างค่า Hash หรือการหาค่าตัวเลขเพื่อนำมายืนยันตัวผู้กระทำความผิด กระบวนการนี้จะต้องอาศัยรูปภาพ หรือไฟล์หลักฐานต่างๆ จากผู้เสียหาย ไม่ว่าจะเป็นข้อความต่างๆ ที่แชทคุยกัน ไฟล์รูปภาค หรือวีดีโอที่ได้ทำการพูดคุยกับผู้กระทำความผิดมาเปรียบเทียบ เพื่อยืนยันตัวผู้กระทำความผิดโดยปราศจากข้อสงสัย

กระบวนการสร้างค่า Hash ที่ใช้ในการตรวจพิสูจน์พยานหลักฐานดิจิทัลนี้ เป็นการคำนวณทางคณิตศาสตร์ที่ดำเนินการกับไฟล์ต่างๆ เช่น รูปภาพ เอกสาร หรือเนื้อหาในฮาร์ดไดรฟ์ โดยค่า Hash นี้เปรียบเสมือนลายพิมพ์นิ้วมือที่ผู้กระทำความผิดได้ทิ้งไว้ในประวัติการใช้เครื่องคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์นั้น โดยไฟล์หรือข้อมูลต่างๆ ที่เป็นหลักฐานดิจิทัลจะถูกระบุลักษณะเฉพาะตามที่ปรากฏอยู่ในเวลาที่ถูกสร้างค่า Hash ขึ้น ซึ่งค่า Hash นี้จะมีความคล้ายคลึงกับหมายเลขไอพี

[113] เว็บไซต์ที่ให้บริการในการตรวจสอบ IP Address : https://checkip.thaiware.com/

[114] นักวิทยาศาสตร์ (สบ1), (2562), ศูนย์พิสูจน์หลักฐาน 5, (11 เมษายน 2562), สัมภาษณ์.

(IP Address) ที่จะมีความเฉพาะเจาะจงและจะไม่มีความซ้ำซ้อนกันอย่างเด็ดขาด[115] การดำเนินการสร้างค่า Hash จะเป็นการนำเอกสารหรือไฟล์ที่ต้องการไปผ่านกระบวนวิธีการ Hash Function ซึ่งกระบวนการนี้จะไม่สนใจว่าไฟล์นามสกุลอะไร ชื่อไฟล์อะไร มีความยาวมากหรือน้อย ขนาดของไฟล์เท่าไหร่ โดยเครื่องมือที่นิยมใช้กันมากที่สุดในประเทศไทยคือ ค่า Hash จาก Message Digest 5 (MD5) และ Secure Hash Algorithm 1 (SHA1) เมื่อไฟล์ได้ผ่านกระบวนการ Hash Function เรียบร้อยแล้ว จะได้ผลลัพธ์เป็นค่า Hash Value ออกมา ซึ่งจะเป็นชุดข้อมูลตัวเลขที่มนุษย์ไม่สามารถทำความเข้าใจได้ โดยชุดข้อมูลดังกล่าวจะเป็นเครื่องมือชี้ชัดที่สำคัญของพยานหลักฐานดิจิทัลที่นำมาตรวจสอบ เพราะจะสามารถนำค่า Hash ที่ได้ไปเปรียบเทียบกับพยานหลักฐานที่ผู้กระทำความผิดมีหากชุดตัวเลขที่ได้จากผู้เสียหายและผู้กระทำความผิดตรงกัน หรือมีค่าที่แมตช์ (Match) กัน ก็จะสามารถอนุมานหรือยืนยันได้ว่าผู้กระทำความผิดนั้นเป็นผู้กระทำที่แท้จริง

ตัวอย่าง กรณีหลักฐานที่ผู้เสียหายเก็บรวบรวมมา เป็นรูปภาพที่ผู้กระทำความผิดส่งมา และผู้เสียหายได้ทำการเซฟ (save) รูปภาพดังกล่าวไว้ ทางเจ้าหน้าที่ก็จะทำการสร้างค่า Hash ผ่านกระบวนการที่เรียกว่า Hash Function จากรูปภาพที่ผู้เสียหายนำมา ซึ่งค่าที่ออกมาจะเป็นค่า Hash Value ที่จะนำมาใช้เปรียบเทียบกับหลักฐานที่ได้จากการจับกุมตัวผู้กระทำความผิดได้พร้อมทั้งเครื่องคอมพิวเตอร์ อุปกรณ์โทรศัพท์มือถือ หรืออุปกรณ์ต่างๆ ที่เกี่ยวข้อง และเมื่อพบว่ามีรูปภาพที่มีลักษณะเดียวกันกับไฟล์ที่ผู้เสียหายได้รับ เจ้าหน้าที่ก็จะนำรูปภาพดังกล่าวมาเข้าสู่กระบวนการ Hash อีกครั้งเพื่อให้ได้ค่า Hash Value ออกมา หลังจากนั้นหากปรากฏค่า Hash ที่ตรงกันก็สามารถยืนบันได้ว่าเป็นผู้กระทำความผิดจริง

แต่อย่างไรนั้นการสร้างค่า Hash ก็มีข้อจำกัดเช่นกัน กล่าวคือ เจ้าหน้าที่พิสูจน์หลักฐานจะต้องมีข้อมูลจากฝ่ายผู้กระทำความผิดมายืนยันด้วย เนื่องจาก หากมีเพียงแต่ค่า Hash ของฝ่ายผู้เสียหายเพียงฝ่ายเดียวจะไม่สามารถนำค่า Hash ที่สร้างขึ้นไปเปรียบเทียบได้ จึงทำให้เกิดการสร้างพยานหลักฐานเพียงฝ่ายเดียวและไม่สามารถนำไปสู่การจับตัวผู้กระทำความผิดได้ และในบางกรณีข้อมูลดิจิทัลมักจะถูกการบีบอัดไฟล์ เนื่องจากมีการส่งต่อข้อมูลผ่านแพลตฟอร์ม (platform) ต่างๆ ซึ่งทำให้ขนาดของไฟล์ถูกเปลี่ยนแปลงไปด้วย ทำให้ค่า Hash Value ที่ได้อาจจะมีความคลาดเคลื่อนหรือไม่ตรงกันทั้งหมด (ไม่สามารถได้ค่าที่ตรงกัน 100% ได้) ซึ่งกระบวนการดังกล่าวนี้ต้องอาศัยความรู้ความเชี่ยวชาญ และประสบการณ์จากเจ้าหน้าที่ในการพิสูจน์หลักฐานอย่างมาก

ความร่วมมือระหว่างประเทศ

การรวบรวมพยานหลักฐานในต่างประเทศ ประเด็นเรื่องหมายศาลพนักงานสอบสวนและอัยการต้องพิสูจน์ทราบตัวตนชัดเจนในขณะกระทำความผิดมันอาจจะอยู่ในเมืองไทยแล้วก็ไปมาระหว่างประเทศกระทำผิดหลายครั้งบางครั้งอยู่ต่างประเทศบางครั้งอยู่ในประเทศไทยก็ออกหมายจับได้ไม่ผิดตัวแน่เพราะฉะนั้นประเด็นเรื่องความร่วมมือระหว่างประเทศมันก็เป็นสิ่งที่ตามมา ประการต่อมาเรื่องของการทำ MLAT (Mutual Legal Assistance Treaty) ในการขอความร่วมมือเพื่อการขยายผลสืบสวนต่างประเทศอันนี้คือ กรณีที่ไอพีขึ้นต่างประเทศเราจะขอให้โครงข่ายสัญญาณโทรศัพท์ใน

[115] แลร์รี อี. แดเนียล, ลาร์ส อี แดนเนียล, สุนีย์ สกาวรัตน์ (ผู้แปล), (2559), *การตรวจพิสูจน์หลักฐานดิจิทัลสำหรับผู้ประกอบวิชาชีพกฎหมาย: เข้าใจพยานหลักฐานดิจิทัลจากขั้นตอนหมายถึงห้องพิจารณาคดี. บทที่ 26 ค่า Hash: มาตรฐานการพิสูจน์ยืนยัน,* กรุงเทพฯ: มูลนิธิเพื่ออินเตอร์เน็ตและวัฒนธรรมพลเมือง, หน้า 322.

ต่างประเทศนั้นทำการพิสูจน์ทราบว่า IP นี้ในวันเวลานั้นใครเป็นคนใช้ทำไปสองปียังไม่ได้กลับมาเลย เรื่องพยานหลักฐานเพราะฉะนั้นอะไรที่เกี่ยวข้องกับเรื่องนี้คาดหวังยากมาก[116]

ปัญหามหาศาลในชั้นสอบสวนที่ยังไม่ถึงศาล ก็คือ กระบวนการขอตาม พ.ร.บ. ความร่วมมือระหว่างประเทศทางอาญาฯ คือ พ.ร.บ. ให้อัยการสูงสุดเป็นผู้ประสานงานกลาง ในการขอความร่วมมือประสานงานไปต่างประเทศ ด้วยแบ่งประเทศทั่วโลกออกเป็น 2 กลุ่ม กลุ่มแรกเป็นกลุ่มที่มีสนธิสัญญาระหว่างกัน ที่จะช่วยเหลือกันทางอาญาตาม พรบ. นี้ เราก็จะเปิดที่สนธิสัญญาเลยว่าจะทำอย่างไร มีเงื่อนไขข้อยกเว้นอย่างไรบ้าง กลุ่มที่ 2 คือกลุ่มที่ไม่มีสนธิสัญญาอะไรกับเรา ใช้หลักทางการทูต ถ้าเราขอไปถ้าเขาช่วยเหลือเราก็จะบันทึกไว้ว่าถ้าเขาขอมาเราก็จะช่วยเหลือ แต่มีจำนวนมากที่เขาไม่ตอบไม่ยุ่งอะไรกับเรา เราก็ใช้หลักต่างตอบแทน[117]

เรื่องของค่าใช้จ่ายในการขอความร่วมมือระหว่างประเทศทางอาญา พนักงานสอบสวนจะต้องมานั่งสรุปข้อเท็จจริง แล้วบอกข้อกล่าวหาให้ชัดเจน ให้ฝ่ายที่รับคำร้องขอจะได้พิจารณาอย่างชัดเจนในการช่วยเหลือ แล้วพนักงานสอบสวนจะต้องมากำหนดประเด็นที่จะขอความช่วยเหลือ โดยให้ไปหาพยานหลักฐานอะไรสอบปากคำของใครถามประเด็นไหนให้รวบรวมอะไรบ้าง ต่อมาพนักงานสอบสวนจะต้องแปลภาษา ขอความร่วมมือจะต้องเป็นเรื่องทางธุรการ ถ้าส่งมายังอัยการสูงสุดจะต้องมีระดับเดียวกันของหน่วยงาน ดังนั้นจะต้องทำหนังสือผ่านผู้บังคับบัญชาเพื่อทำการขอให้อยู่ในระดับเดียวกัน โดยการส่งเรื่องไปยังอัยการสูงสุดเพื่อทำเรื่องระหว่างประเทศ กว่าจะออกจากประเทศไทยระยะเวลา 3 ถึง 6 เดือนเป็นอย่างน้อย แล้วถ้าเราต้องการ IP ADDRESS มาเพื่อที่จะมาเชื่อมกับในประเทศไทยก็ไม่ทันการณ์ และค่าใช้จ่ายก็มหาศาล[118]

จากสิ่งที่กล่าวมาข้างต้น เมื่อนำมาพิจารณากับกระบวนการพิจารณาคดีอาญาทั้งเรื่องหลักกฎหมายและการปฏิบัติงานของเจ้าหน้าที่ จะเห็นได้ว่าอุปสรรคในการรวบรวมพยานหลักฐานของพนักงานสอบสวน สามารถแบ่งออกเป็น 3 กรณี กล่าวคือ 1) อุปสรรคด้านเวลา 2) อุปสรรคด้านทรัพยากร ไม่ว่าจะเป็นด้านเครื่องมือ กำลังพล หรืองบประมาณ และ 3) อุปสรรคด้านการติดตามตัวผู้กระทำความผิด

<u>อุปสรรคด้านเวลา</u>

หากคดีที่รับแจ้งนั้นเป็นความผิดที่อยู่ในอำนาจสอบสวนหรือพนักงานสอบสวนผู้รับผิดชอบของหน่วยงานอื่น เช่น กรมสอบสวนคดีพิเศษ หรือสำนักงานอัยการสูงสุด พนักงานสอบสวนผู้รับแจ้งความร้องทุกข์นั้นจะต้องส่งสำนวนการสอบสวนไปให้หน่วยงานที่มีหน้าที่รับผิดชอบนั้น ซึ่งในคดี Romance Scam ถือเป็นคดีหนึ่งที่เข้าข่ายเป็นคดีที่อยู่ในอำนาจสอบสวนของกรมสอบสวนคดีพิเศษ เนื่องจากเป็นคดีความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์[119] ที่มีความซับซ้อนจำเป็นต้องใช้วิธีการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเป็นพิเศษ[120] ในกรณีดังกล่าวนี้

---

[116] อดีตรองอธิบดีกรมสอบสวนคดีพิเศษ กรมสอบสวนคดีพิเศษ. (13 มิถุนายน 2562). สัมภาษณ์.

[117] พนักงานอัยการ. อัยการจังหวัดประจำสำนักงานอัยการสูงสุด. (16 มกราคม 2562). สัมภาษณ์.

[118] พนักงานอัยการ. อัยการจังหวัดประจำสำนักงานอัยการสูงสุด. (16 มกราคม 2562). สัมภาษณ์.

[119] กฎกระทรวงว่าด้วยการกำหนดคดีพิเศษเพิ่มเติมตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ (ฉบับที่ 2) พ.ศ.2555 (6) คดีความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

[120] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 มาตรา 21 (1) (ก)-(ค)

พนักงานสอบสวนจะต้องรับคำร้องทุกข์นั้นและดำเนินการสอบสวน หรือดำเนินการอื่นตามหน้าที่ จนกว่าจะมีการส่งมอบสำนวนการสืบสวนสอบสวนให้กรมสอบสวนคดีพิเศษ โดยต้องส่งมอบภายใน 15 วัน นับตั้งแต่รับคำร้องทุกข์หรือคำกล่าวโทษ ซึ่งในระหว่างที่พนักงานสอบสวนยังไม่ได้ส่งสำนวนดังกล่าวให้กับกรมสอบสวนคดีพิเศษ พนักงานสอบสวนมีอำนาจในการควบคุม ขัง หรือปล่อยตัวชั่วคราว เก็บรักษาของกลาง และดำเนินการอย่างอื่นที่จำเป็น และหากมีการฝากขัง พนักงานสอบสวนต้องดำเนินการให้เสร็จก่อนครบกำหนดฝากขังไม่น้อยกว่า 3 วัน[121]

สำหรับคดีอาญาที่เป็นคดีความผิดต่อส่วนตัวและเป็นคดีความผิดเกี่ยวกับเทคโนโลยี[122] เมื่อผู้เสียหายมาแจ้งความกับพนักงานสอบสวน โดยทั่วไปแล้ว พนักงานสอบสวนจะตรวจสอบว่ามีการกระทำความผิดตามที่ผู้เสียหายแจ้งไว้หรือไม่ ตรวจสอบหาหมายเลขไอพี (IP Address) วัน เวลาในการกระทำความผิด โดยอาจสอบถามไปยังผู้ดูแลเว็บไซต์หรือผู้ให้บริการอินเตอร์เน็ต โดยอาศัยอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา หรือส่งไปยังพนักงานเจ้าหน้าที่ตามพระราชบัญญัติคอมพิวเตอร์ฯ ตรวจสอบให้ และหากพนักงานสอบสวนต้องการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ให้พนักงานสอบสวนประสานงานไปยังกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) หรือพนักงานเจ้าหน้าที่ตามพระราชบัญญัติคอมพิวเตอร์ฯ กระทรวงไอซีที ตรวจสอบข้อมูลเพื่อประโยชน์ในการแสวงหาพยานหลักฐานประกอบการกระทำความผิดต่อไป

ซึ่งระยะเวลาในการรวบรวมพยานหลักฐานเพื่อนำมาประกอบในสำนวนนั้น ในคดีอาญาทั่วไป พนักงานสอบสวนจะต้องทำการสอบสวนติดต่อกันมาแล้วไม่น้อยกว่า 3 เดือน นับตั้งแต่วันที่รับคำร้องทุกข์หรือกล่าวโทษ และเมื่อยังไม่ปรากฏว่าผู้ใดเป็นผู้กระทำความผิด พนักงานสอบสวนจะมีความเห็น “งดการสอบสวน” หรือ “เห็นควรให้งดการสอบสวน” แล้วเสนอสำนวนพร้อมความเห็นไปยังผู้บังคับบัญชาตามลำดับชั้นจนถึงผู้บังคับการหรือผู้บัญชาการสำหรับหน่วยงานที่มีอำนาจสอบสวนเพื่อพิจารณาและให้ความเห็นทางคดี[123] แล้วส่งสำนวนไปยังพนักงานอัยการ[124] ซึ่งอาจกล่าวได้ว่า อย่าง

มาตรา 21 คดีพิเศษที่จะต้องดำเนินการสืบสวนและสอบสวนตามพระราชบัญญัตินี้ ได้แก่ คดีความผิดทางอาญา ดังต่อไปนี้

(1) คดีความผิดทางอาญาตามกฎหมายที่กำหนดไว้ในบัญชีท้ายพระราชบัญญัตินี้ และที่กำหนดในกฎกระทรวงโดยการเสนอแนะของ กคพ. โดยคดีความผิดทางอาญาตามกฎหมายดังกล่าวจะต้องมีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้

(ก) คดีความผิดทางอายาที่มีความซับซ้อน จำเป็นต้องใช้วิธีการสืบสวนสอบสวนนและรวบรวมพยานหลักฐานเป็นพิเศษ

(ข) คดีความผิดทางอาญาที่มีหรืออาจมีผลกระทบอย่างรุนแรงต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน ความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศหรือระบบเศรษฐกิจหรือการคลังของประเทศ

(ค) คดีความผิดทางอาญาที่มีลักษณะเป็นการกระทำความผิดข้ามชาติที่สำคัญ หรือเป็นการกระทำขององค์กรอาชญากรรม

[121] กองบัญชาการตำรวจนครบาล, (2559), *คู่มือการปฏิบัติงานด้านการอำนวยความยุติธรรมในคดีอาญา เล่มที่ 1 (การทำสำนวนการสอบสวนของพนักงานสอบสวน) ของกองบัญชาการตำรวจนครบาล,* กรุงเทพฯ: กองบัญชาการตำรวจนครบาล, หน้า 14.

[122] เรื่องเดียวกัน, หน้า 22.

[123] เรื่องเดียวกัน, หน้า 43-44.

[124] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 140 (1)

น้อยภายในระยะเวลา 3 เดือน พนักงานสอบสวนจะต้องสามารถรวบรวมพยานหลักฐานในจำนวนที่เพียงพอต่อการสรุปข้อมูลได้ว่า คดีที่ผู้เสียหายนำมาแจ้งความร้องทุกข์นั้นเป็นอย่างไร มีแนวโน้มที่จะตามจับตัวผู้กระทำความผิดได้หรือไม่ เป็นต้น แต่ในคดี Romance Scam ซึ่งเป็นคดีที่ไม่มีประจักษ์พยานและผู้กระทำความผิดมักปลอมแปลงตัวตน ทำให้ยากต่อการแสวงหาพยานหลักฐาน ประกอบกับเป็นการกระทำความผิดเกี่ยวกับเทคโนโลยี ที่ยากต่อการระบุตำแหน่งและตัวตนของผู้กระทำความผิด อีกทั้งยังต้องมีการประสานงานกับเจ้าหน้าที่หลายฝ่าย แต่ระยะเวลาในการรวบรวมพยานหลักฐานเพื่อทำสำนวนคดีของพนักงานสอบสวนผู้รับผิดชอบนั้นกลับมีระยะเวลาเท่ากับการทำคดียาเสพติดเพียง 10 เม็ด[125]

<u>อุปสรรคด้านทรัพยากร (อุปกรณ์ กำลังพล งบประมาณ)</u>

คดี Romance Scam เป็นหนึ่งในคดีอาชญากรรมทางคอมพิวเตอร์ที่มีความซับซ้อน เนื่องจากผู้กระทำความผิดมักปลอมแปลงตัวตน ทำให้ยากต่อการระบุตำแหน่งที่อยู่และการยืนยันตัวตน อีกทั้งยังมักเป็นความผิดที่กระทำลงนอกราชอาณาจักรโดยผู้กระทำความผิดต่างชาติที่แฝงตัวเข้ามาในประเทศไทยในฐานะนักท่องเที่ยว เมื่อมีความเสียหายเกิดขึ้นก็ทำให้ยากแก่การตามตัวผู้กระทำความผิดมาลงโทษ ประกอบกับข้อจำกัดเรื่องทรัพยากร ไม่ว่าจะเป็นด้านอุปกรณ์ที่จำเป็นต้องมีอุปกรณ์ที่ทันสมัยอยู่ตลอดเวลา และต้องมีเจ้าหน้าที่ที่มีความรู้ความเชี่ยวชาญด้านคอมพิวเตอร์ในจำนวนที่เพียงพอต่อหน่วยงานในระดับภูมิภาค เพื่อรองรับกับการกระทำความผิดที่อาจเกิดขึ้น แต่ในปัจจุบันข้อจำกัดเหล่านี้เป็นสิ่งที่ถูกจำกัดด้วยงบประมาณ ทำให้ในขณะนี้ยังมีคดีอาชญากรรมทางคอมพิวเตอร์สจำนวนมาก โดยเฉพาะคดี Romance Scam ที่ไม่สามารถนำตัวผู้กระทำความผิดมาลงโทษ หรือชดใช้เยียวยาความเสียหายให้แก่ผู้เสียหายได้

<u>อุปสรรคด้านการติดตามตัวผู้กระทำความผิด</u>

เนื่องจากลักษณะความผิดของคดี Romance Scam มักเป็นกรณีที่ผู้เสียหายกับผู้กระทำความผิดได้มีการติดต่อสื่อสารกันผ่านทางโซเชียลมีเดียโดยที่ไม่เคยพบเห็นหน้าตาที่แท้จริงของกันและกันมาก่อน ซึ่งนอกจากผู้กระทำความผิดจะทำการปลอมแปลงตัวตนด้วยการนำรูปของบุคคลอื่นมาใช้ในการหลอกลวงแล้ว ผู้กระทำความผิดยังอาจใช้ช่องทางและความรู้ด้านเทคโนโลยีมาช่วยในการปลอมแปลงตัวตนให้ยากแก่การติดตามตัวได้มากยิ่งขึ้น เช่น การเล่นอินเตอร์เน็ตผ่านทาง VPN เพื่อบิดบังสถานที่กระทำความผิดที่แท้จริง เป็นต้น ซึ่งการกระทำความผิดที่เจ้าหน้าที่จะสามารถติดตามตัวผู้กระทำความผิดได้บ้างนั้น มักเป็นกรณีที่ผู้กระทำความผิดใช้ภรรยาหรือผู้หญิงชายไทยที่ตนคบหาด้วยมาเป็นผู้ช่วยในการกระทำความผิด เช่น ใช้ชื่อหญิงไทยเปิดบัญชีธนาคาร, หรือช่วยติดต่อประสานงาน

มาตรา 140 เมื่อพนักงานสอบสวนผู้รับผิดชอบในการสอบสวน เห็นว่าการสอบสวนเสร็จแล้ว ให้จัดการอย่างหนึ่งอย่างใด ดังต่อไปนี้

(1) ถ้าไม่ปรากฏว่าผู้ใดเป็นผู้กระทำความผิด และความผิดนั้นมีอัตราโทษจำคุกอย่างสูงไม่เกินสามปี ให้พนักงานสอบสวนงดการสอบสวน และบรรทุกเหตุที่งดนั้นไว้ แล้วให้ส่งบันทึกพร้อมกับสำนวนไปยังพนักงานอัยการ

ถ้าอัตราโทษอย่างสูงเกินกว่าสามปี ให้พนักงานสอบสวนส่งสำนวนไปยังพนักงานอัยการพร้อมทั้งความเห็นที่ควรให้งดการสอบสวน

ถ้าพนักงานอัยการสั่งให้งด หรือให้ทำการสอบสวนต่อไป ให้พนักงานสอบสวนปฏิบัติตามนั้น

[125] พนักงานสอบสวน, (2562), สถานีตำรวจแห่งหนึ่งในจังหวัดเชียงใหม่, (30 เมษายน 2562), สัมภาษณ์.

กับผู้เสียหาย เป็นต้น ดังนั้น เมื่อผู้เสียหายเข้าแจ้งความ สิ่งแรกที่เจ้าหน้าที่หรือพนักงานสอบสวนจะทำคือ การนำหมายเลขบัญชีธนาคารที่ผู้เสียหายได้โอนไปมาสืบหาเส้นทางการเงิน รวมถึงจับตัวเจ้าของบัญชีเพื่อสืบหาข้อมูลของผู้กระทำความผิดตัวจริง[126] แต่หญิงเหล่านี้ก็มักเป็นบุคคลที่ไม่รู้เรื่องการกระทำความผิดมากนัก เนื่องจากอาจเป็นบุคคลที่ถูกหลอกลวงจากผู้กระทำความผิดอีกทีหนึ่งเช่นกัน ทำให้โดยส่วนมากแล้วหญิงที่ถูกจับเหล่านี้จะให้การรับว่าเป็นเจ้าของบัญชีดังกล่าวจริง หรือเป็นคนติดต่อพูดคุยกับผู้เสียหายจริง แต่ไม่รู้และไม่มีส่วนเกี่ยวข้องกับการกระทำความผิดดังกล่าว ทำให้ในท้ายที่สุดแล้วเจ้าหน้าที่ก็ไม่ได้ข้อมูลหรือพยานหลักฐานจากบุคคลเหล่านี้มากนัก และเนื่องจากการที่ผู้เสียหายไม่เคยพบหรือเห็นหน้าผู้กระทำความผิดที่แท้จริงมาก่อน ทำให้ผู้เสียหายไม่สามารถบอกรูปพรรณสัณฐานของผู้กระทำความผิดเพื่อนำไปออกหมายจับได้ พนักงานสอบสวนจึงต้องแสดงให้ศาลเชื่อหรือเข้าใจได้ว่าคดี Romance Scam เป็นคดีที่มีลักษณะพิเศษที่ทำให้ไม่สามารถระบุถึงรูปพรรณสัณฐานของผู้กระทำความผิดได้[127] และแม้พนักงานสอบสวนจะสามารถขอให้ศาลออกหมายจับได้ก็ตาม แต่การตามจับตัวผู้กระทำความผิดก็ไม่ใช่เรื่องที่สามารถทำได้ง่ายนัก เนื่องจากผู้กระทำความผิดมักกระทำความผิดนอกราชอาณาจักร พนักงานสอบสวนจำเป็นต้องประสานงานไปที่หน่วยงานต่าง ๆ ตามขั้นตอนเพื่อนำไปสู่การขอส่งตัวผู้ร้ายข้ามแดน ซึ่งหากไม่ใช่ประเทศที่มีสนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างกัน ก็จะต้องประสานงานโดยผ่านวิธีการทางการทูต กระบวนการต่างๆ เหล่านี้จำเป็นต้องใช้ทั้งเงินและเวลา ทำให้การติดตามตัวผู้กระทำความผิดในคดี Romance Scam มักสะดุดหยุดลงที่การมีคำสั่ง “งดการสอบสวน” ของพนักงานสอบสวนเนื่องจากไม่สามารถรู้ตัวผู้กระทำความผิด[128] หรือหยุดลงที่ชั้นอัยการเนื่องจากการทำเรื่องขอส่งตัวผู้ร้ายข้ามแดนในคดี Romance Scam มักถูกมองว่าเป็นความผิดต่อส่วนตัวและไม่คุ้มทุน[129]

5) การจับกุม

ในการจะนำตัวผู้กระทำความผิดมาเพื่อให้การในฐานะผู้ต้องได้นั้น พนักงานสอบสวนจะต้องขอให้ศาลออกหมายจับ ซึ่งการจับ แบ่งออกเป็น 2 ประเภท คือ การจับแบบมีหมายจับ และการจับแบบไม่มีหมายจับ กล่าวคือ เมื่อพนักงานสอบสวนได้รวบรวมพยานหลักฐานคนสืบทราบได้ว่าผู้กระทำความผิดอยู่ที่ใด และจะต้องขอให้ศาลออกหมายจับเพื่อทำการจับกุมผู้กระทำผิดนั้น ซึ่งกล่าวได้ว่า ในการจับกุมจะต้องมีหมายจับเสมอ[130]

---

[126] เรื่องเดียวกัน

[127] เรื่องเดียวกัน

[128] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 140 (1)

มาตรา 140 เมื่อพนักงานสอบสวนผู้รับผิดชอบในการสอบสวน เห็นว่าการสอบสวนเสร็จสิ้นแล้ว ให้จัดการอย่างหนึ่งอย่างใด ดังต่อไปนี้

(1) ถ้าไม่ปรากฏว่าผู้ใดเป็นผู้กระทำความผิดและความผิดนั้นมีอัตราโทษจำคุกอย่างสูงไม่เกินสามปี ให้พนักงานสอบสวนงดการสอบสวน และบรรทุกเหตุที่งดนั้นไว้ แล้วให้ส่งบันทึกพร้อมกับสำนวนไปยังพนักงานอัยการ

ถ้าอัตราโทษอย่างสูงเกินกว่าสามปี ให้พนักงานสอบสวนส่งสำนวนไปยังพนักงานอัยการพร้อมทั้งความเห็นนที่ควรให้งดการสอบสวน

ถ้าพนักงานอัยการสั่งให้งด หรือให้ทำการสอบสวนต่อไป ให้พนักงานสอบสวนปฏิบัติตามนั้น

[129] ผู้พิพากษา, (2562), สำนักประธานศาลฎีกา, (16 มกราคม 2562), สัมภาษณ์.

[130] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 78 วรรคหนึ่ง

ในการขอออกหมายจับ พนักงานสอบสวนจะต้องแสดงพยานหลักฐานที่ทำให้ศาลเชื่อได้ว่ามีเหตุที่จะออกหมายจับนั้น แต่อย่างไรก็ตาม ด้วยลักษณะของการกระทำความผิดในคดี Romance Scam ที่ผู้กระทำความผิดมักไม่เปิดเผยโฉมหน้าหรือตัวตนที่แท้จริง ทำให้เป็นอุปสรรคในการขอออกหมายจับของเจ้าหน้าที่ เนื่องด้วยการที่จะขอออกหมายจับได้นั้น นอกจากจะต้องมีเหตุตามที่กฎหมายบัญญัติไว้แล้ว[131] ในกรณีที่ยังไม่รู้จักชื่อของผู้กระทำผิด เจ้าพนักงานต้องสามารถบอกได้ถึงรูปพรรณของผู้กระทำผิดให้ละเอียดเท่าที่จะทำได้ด้วย[132] ส่วนการจับโดยไม่มีหมายจับนั้นจะทำได้ต่อเมื่อเข้าข้อยกเว้นที่กฎหมายกำหนดไว้เท่านั้น[133] เช่น เป็นการกระทำความผิดที่เกิดขึ้นต่อหน้าพนักงานสอบสวน หรือ เมื่อพบบุคคลที่มีพฤติการณ์อันควรสงสัยว่าผู้นั้นน่าจะก่อเหตุร้ายให้เกิดภยันตรายแก่บุคคลหรือทรัพย์สินของผู้อื่น เป็นต้น อย่างไรก็ตามหากพนักงานสอบสวนกระทำการจับโดยไม่มีหมายจับและไม่ใช่กรณีที่เข้าข้อยกเว้นให้สามารถจับได้โดยไม่ต้องมีหมายจับ ย่อมส่งผลต่อความน่าเชื่อถือของพยานหลักฐาน กล่าวคือ พยานหลักฐานที่ได้มาจากการค้นอันสืบเนื่องมาจากการจับที่ไม่ชอบด้วยกฎหมายจะรับฟังไม่ได้[134] และการจับโดยไม่ชอบนั้นจะส่งผลให้การคุมขังที่ต่อเนื่องจากการจับนั้นไม่ชอบด้วยกฎหมายตามไปด้วย ผู้ถูกคุมขังมีสิทธิที่จะยื่นคำร้องขอให้ศาลปล่อยตัวได้[135]

มาตรา 78 พนักงานฝ่ายปกครองหรือตำรวจจะจับผู้ใดโดยไม่มีหมายจับหรือคำสั่งของศาลนั้นไม่ได้

[131] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 66 วรรคหนึ่ง

มาตรา 66 เหตุที่จะออกหมายจับได้มีดังต่อไปนี้

(1) เมื่อมีหลักฐานตามสมควรว่าบุคคลใดน่าจะได้กระทำความผิดอาญา ซึ่งมีอัตราโทษจำคุกอย่างสูงเกินสามปี หรือ

(2) เมื่อมีหลักฐานตามสมควรว่าบุคคลใดน่าจะได้กระทำความผิดอาญาและมีเหตุอันควรเชื่อว่าจะหลบหนีหรือจะไปยุ่งเหยิงกับพยานหลักฐาน หรือก่อเหตุอันตรายประการอื่น

[132] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 67

มาตรา 67 จะออกหมายจับบุคคลที่ยังไม่รู้จักชื่อก็ได้ แต่ต้องบอกรูปพรรณของผู้นั้นให้ละเอียดเท่าที่จะทำได้

[133] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 78

มาตรา 78 พนักงานฝ่ายปกครองหรือตำรวจจะจับผู้ใดโดยไม่มีหมายจับหรือคำสั่งของศาลนั้นไม่ได้ เว้นแต่

(1) เมื่อบุคคลนั้นได้กระทำความผิดซึ่งหน้า ดังได้บัญญัติไว้ในมาตรา 80

(2) เมื่อพบบุคคลโดยมีพฤติการณ์อันควรสงสัยว่าผู้นั้นน่าจะก่อเหตุร้ายให้เกิดภยันตรายแก่บุคคลหรือทรัพย์สินของผู้อื่น โดยมีเครื่องมือ อาวุธ หรือวัตถุอย่างอื่นอันสามารถอาจใช้ในการกระทำความผิด

(3) เมื่อมีเหตุที่จะออกหมายจับบุคคลนั้นตาม มาตรา 66 (2) แต่มีความจำเป็นเร่งด่วนที่ไม่อาจขอให้ศาลออกหมายจับบุคคลนั้นได้

(4) เป็นการจับผู้ต้องหาหรือจำเลยที่หนีหรือจะหลบหนีในระหว่างถูกปล่อยชั่วคราว ตามมาตรา 117

[134] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/1 วรรคหนึ่ง

มาตรา 226/1 ในกรณีที่ความปรากฏแก่ศาลว่าพยานหลักฐานใดเป็นพยานหลักฐานที่เกิดขึ้นโดยชอบแต่ได้มาเนื่องจากการกระทำโดยมิชอบ หรือเป็นพยานหลักฐานที่ได้มาโดยอาศัยข้อมูลที่เกิดขึ้นหรือได้มาโดยมิชอบ ห้ามมิให้ศาลรับฟังพยานหลักฐานนั้น เว้นแต่การรับฟังพยานหลักฐานนั้นจะเป็นประโยชน์ต่อการอำนวยความยุติธรรมมากกว่าผลเสียอันเกิดจากผลกระทบต่อมาตรฐานของระบบงานยุติธรรมทางอาญาหรือสิทธิเสรีภาพพื้นฐานของประชาชน

[135] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 90 วรรคหนึ่ง

มาตรา 90 เมื่อมีการอ้างว่าบุคคลใดต้องถูกคุมขังในคดีอาญาหรือในกรณีอื่นใดโดยมิชอบด้วยกฎหมาย บุคคลเหล่านี้มีสิทธิยื่นคำร้องต่อศาลท้องที่ที่มีอำนาจพิจารณาคดีอาญา ขอให้ปล่อย คือ

(1) ผู้ถูกคุมขังเอง

(2) พนักงานอัยการ

อุปสรรคจากประสิทธิภาพของกระบวนการยุติธรรม

จากสิ่งที่ได้กล่าวมาในข้างต้น จะเห็นได้ว่าพนักงานสอบสวนแทบจะไม่สามารถตามผู้กระทำความผิดที่แท้จริงมาลงโทษได้เลย แต่กลับสามารถตามจับได้เฉพาะผู้ร่วมกระทำความผิดที่ได้แต่งงานหรืออยู่กินฉันสามีภรรยากับผู้กระทำความผิดเท่านั้น ทำให้ในการสืบสวนสอบสวน พนักงานสอบสวนจึงทำได้เพียงการสืบทางเส้นทางการเงินของผู้ร่วมกระทำความผิดที่เป็นเจ้าของบัญชี และนำไปขยายผลเพื่อสืบหาตัวผู้กระทำความผิด แต่ก็มักทำได้ยาก เนื่องจากผู้กระทำความผิดมักอาศัยอยู่นอกราชอาณาจักร หรือไม่สามารถหาหลักฐานมายืนยันได้ว่าผู้กระทำความผิดที่แท้จริงคือใคร เนื่องจากการปลอมแปลงตัวตนและการข้อจำกัดด้านความรู้ความเชี่ยวชาญของเจ้าหน้าที่และข้อจำกัดด้านอุปกรณ์ นอกจากนี้อุปสรรคสำคัญอย่างหนึ่งในการดำเนินคดี Romance Scam คือ หากเจ้าพนักงานตำรวจตั้งฐานความผิดเป็นคดีฉ้อโกงย่อมส่งผลให้คดี Romance Scam เป็นความผิดที่ยอมความได้ ดังนั้น หากผู้เสียหายตัดสินใจถอนคำร้องทุกข์หรือยุติการดำเนินคดี เจ้าพนักงานตำรวจก็จะไม่สามารถดำเนินคดีนี้ต่อไปได้ ซึ่งสามารถแก้ไขได้ด้วยการดำเนินคดีนี้ต่อในฐานะที่ผู้กระทำความผิดเป็นองค์กรอาชญากรรมข้ามชาติ อันจะทำให้คดี Romance Scam กลายเป็นความผิดอาญาแผ่นดิน และเจ้าพนักงานตำรวจสามารถดำเนินคดีนี้ต่อไปได้แม้ว่าผู้เสียหายจะถอนคำร้องทุกข์หรือยุติการดำเนินคดีก็ตาม[136]

6) ชั้นกระบวนพิจารณาของศาล

นอกจากการสอบสวนเพื่อให้ได้มาซึ่งพยานหลักฐานในการยืนยันตัวผู้กระทำความผิดเป็นสิ่งที่ทำได้ยากแล้ว อีกหนึ่งอุปสรรคสำคัญในการนำตัวผู้กระทำความผิดมาลงโทษก็คือ หลักในการดำเนินคดีอาญา เนื่องจากในคดีอาญามีหลักการ “ต้องพิสูจน์จนสิ้นสงสัย” ทำให้เมื่อพนักงานสอบสวนไม่สามารถหาพยานหลักฐานมายืนยันจนศาล “สิ้นสงสัย” ว่าจำเลยเป็นผู้กระทำความผิดที่แท้จริงตามที่ถูกล่าวหาได้ เช่น ไม่สามารถยืนยันได้ว่าจำเลยเป็นบุคคลที่พูดคุยกับผู้เสียหาย แม้จะไม่ใช่เจ้าของเครื่องคอมพิวเตอร์หรือ account นั้นก็ตาม ทำให้ “เมื่อกรณียังเป็นที่สงสัย” ศาลก็ต้องปล่อยตัวจำเลยนั้นไป[137] และส่งผลให้มิอาจมีคำสั่งให้บังคับคดียึดทรัพย์ หรือให้ชดใช้สินไหมทดแทนในทางแพ่งได้

ความรับผิดตามกฎหมายแพ่ง ถ้าจะให้ผู้ให้บริการ (ISP) รับผิดชอบโดยใช้กฎหมายแพ่ง น่าจะเป็นเรื่องที่ได้ผลพอสมควรแล้วก็ยืดหยุ่น จะให้ศาลเข้าไปสร้างหลักกฎหมายในเชิงแพ่งให้ใครรับผิด ศาลค่อนข้างจะพอมีทางทำได้มากมาย แต่ถ้าเป็นทางอาญาคงไม่ได้เพราะศาลไม่มีหน้าที่ ถ้าไม่พิสูจน์ว่ามีความผิดศาลจะไม่ยุ่ง ถ้าไม่มีกฎหมายอาญาชัดเจนว่าผิดศาลก็จะไม่เข้าไปยุ่ง[138]

7) การบังคับคดี

ปกติหากศาลมีคำพิพากษาก็จบคดี แต่จะมีการเยียวยากันอย่างไรบ้างในการติดตามทรัพย์มาคืนผู้เสียหายยังเป็นที่สงสัย เนื่องจากถ้ากระทำความผิดศาลก็พิพากษาลงโทษทางอาญาอยู่แล้วหากติดตามจับกุมตัวได้ แต่ส่วนใหญ่ถ้าจะบังคับคดีผู้เสียหายได้รับการคืนเงินต้องสืบทรัพย์ให้เห็นว่ากระจาย

---

(3) พนักงานสอบสวน

(4) ผู้บัญชาการเรือนจำหรือพัศดี

(5) สามี ภริยา หรือญาติของผู้นั้น หรือบุคคลอื่นใดเพื่อประโยชน์ของผู้ถูกคุมขัง

[136] พนักงานสอบสวน, (2562), สถานีตำรวจแห่งหนึ่งในจังหวัดเชียงใหม่, (30 เมษายน 2562), สัมภาษณ์.

[137] ผู้พิพากษา, ผู้พิพากษาศาลชั้นต้นประจำสำนักประธานศาลฎีกา, (16 มกราคม 2562), สัมภาษณ์.

[138] ผู้พิพากษา. ผู้พิพากษาหัวหน้าศาลประจำสำนักประธานศาลฎีกา. (16 มกราคม 2562). สัมภาษณ์.

ไปเก็บอยู่อย่างไรบ้าง ซึ่งความยากก็จะอยู่ในส่วนการติดตามหา โดยคดีแพ่งโดยทั่วไปก็จะยากกับการติดตามทรัพย์สินของลูกหนี้อยู่แล้ว แต่ส่วนใหญ่ผู้กระทำผิดเป็นต่างชาติจึงยากขึ้นไปอีกว่าจะไปสืบทรัพย์อย่างไร หรือถ้าคนไทยเปิดบัญชีให้จะบังคับคดีได้ไหมก็ไม่แน่ใจเหมือนกันว่าพอตำรวจไปอายัดบัญชีแล้วจะดำเนินการอย่างไรต่อจะมีการดำเนินคดีอาญาฟอกเงินหรืออายัดบัญชีและทรัพย์สินไว้ด้วยหรือไม่ โดยบางครั้งสำนวนก็ฟ้องเจ้าของบัญชีมาด้วยว่าเป็นผู้สนับสนุน โดยพบว่ามีกรณีกรมสอบสวนคดีพิเศษ (DSI) ที่ฟ้องเจ้าของที่ช่วยเปิดบัญชี โดยอาจจะต้องอายัดบัญชีไว้ก่อนแล้วอาจจะได้เงินคืนในส่วนนั้น[139]

ขณะนี้ยังไม่มีมาตรการเยียวยาผู้ตกเป็นเหยื่ออย่างแท้จริงเนื่องจากเป็นคดีส่วนตัว ไม่ใช่คดีที่รัฐเป็นผู้เสียหาย ตามกฎหมายจึงยังไม่มีมาตรการของรัฐในการเยียวยาให้กับผู้ตกเป็นเหยื่อ ถ้าผู้ต้องหาไม่ยอมชดใช้ ผู้เสียหายต้องฟ้องเรียกร้องทางแพ่งเอง ผู้เสียหายต้องดิ้นรนด้วยตัวเอง ทำให้แม้มีการปรับปรุงมาตรการที่ช่วยเยียวยาหรือรับเรื่องร้องทุกข์ให้กับผู้เสียหายแล้วก็อาจจะไม่ทำให้ผู้ตกเป็นเหยื่อเข้ามาร้องทุกข์มากนัก[140] เพราะคิดว่าท้ายที่สุดจะไม่ได้ทรัพย์สินที่ถูกหลอกลวงไปกลับคืนมา

นอกจากนี้ยังมีประเด็นที่สำคัญยิ่งอีกประการ คือ **มาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมโดยอาศัยความร่วมมือระหว่างรัฐกับเอกชน** (Public and Private Partnership) ซึ่งกฎหมายได้เปิดโอกาสให้รัฐดำเนินการในลักษณะนี้ อย่างไรก็ดียังมีข้อจำกัดในการแก้ไขปัญหาด้วยแนวทางนี้เช่นกัน กล่าวคือ

การระบุว่าตัวผู้กระทำความผิดอยู่ไหนถ้าเราไม่ได้ข้อมูลเกี่ยวกับพวก log file คือการขอ log file มันก็ต้องไปที่พวก ISP (Internet Service Provider) ซึ่งกระบวนการเหล่านี้ค่อนข้างยุ่งยาก การขอความร่วมมือจากหน่วยงานเอกชน ถ้าว่าตามหลักกฎหมายก็สามารถที่จะปรับใช้ได้แต่ถ้าพูดตามหลักการในการทำธุรกิจ ISP คงไม่ชอบแน่ๆ ถ้าเราไปผลักภาระให้ ISP มากโดยใช้เรื่องของกฎหมายเข้ามากำกับ สิ่งที่เกิดขึ้นจะมีผลก็คือว่า ISP มีแนวโน้มที่เขาจะเอาอะไรที่เขาไม่แน่ใจลงตลอดซึ่งมันจะไปเชื่อมโยงในเรื่องของเสรีภาพในการแสดงออก freedom expression) [141] คือ เซ็นเซอร์พื้นที่ตัวเองไว้ก่อน

ปัจจุบันกฎหมายมีมาตรการเพียงพอแล้ว เพราะตัว พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เรื่องนี้ค่อนข้างเป็นเรื่องของการหากมองว่าเป็นคดีฉ้อโกง ก็เป็นความผิดอาญาต่อส่วนตัว สุดท้ายแล้วคนที่ตัดสินใจมันคือตัวของผู้เสียหายเอง หากรัฐออกกฎหมายในลักษณะกรอบการตัดสินใจมันล่วงละเมิดเสรีภาพมากเกินไป แต่ที่ทำได้เต็มที่ในแง่ของผู้ประกอบการเก็บ log file อะไรต่างๆ ที่จะย้อนรอยตามหาตัวอาชญากร เป็นแนวโน้มของต่างประเทศอยู่แล้วที่ผู้ประกอบการมีหน้าที่เก็บข้อมูลเหล่านี้เอาไว้ในระยะหนึ่ง หากดู พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตัวผู้ประกอบการอินเทอร์เน็ต ตัวโทรคมนาคมที่ต้องให้เก็บไว้ 90 วัน เพียงพอแล้ว อัยการบอกว่ากว่าจะ

[139] ผู้พิพากษา. ผู้พิพากษาศาลชั้นต้นประจำสำนักประธานศาลฎีกา. (16 มกราคม 2562). สัมภาษณ์.

[140] นักวิชาการ. อาจารย์ประจำภาควิชาสังคมวิทยาและมานุษยวิทยา จุฬาลงกรณ์มหาวิทยาลัย. (14 กุมภาพันธ์ 2562). สัมภาษณ์.

[141] นักวิชาการ. อาจารย์ประจำ ภาควิชาสังคมและสุขภาพคณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล. (15 พฤษภาคม 2562). สัมภาษณ์.

เชื่อมความสัมพันธ์กับผู้ประกอบการที่เซิร์ฟเวอร์อยู่ในต่างประเทศหรือผู้ประกอบการต่างประเทศ การขอข้อมูลไปแล้วกว่ารัฐบาลที่ต่างประเทศจะอนุมัติก็เกินกว่า 90 วันแล้ว เชื่อมข้อมูล 2 ชุดไม่ได้แล้ว อันนี้ก็ต้องเกี่ยวกับความร่วมมือระหว่างประเทศ ความร่วมมือทางอาญาระหว่างประเทศด้วย ตรงนี้แท้จริงแล้วกฎหมายภายในจะกำหนดอะไรไม่ได้มาก ไม่มีกรอบเวลาอยู่แล้ว[142]

แต่หากจะออกกฎหมายในลักษณะที่ควบคุมมากไปกว่านี้ มันเป็นการยาก เป็นการเพิ่มภาระและมีปัญหาเกี่ยวกับสิทธิและเสรีภาพแน่นอน ออกได้เต็มที่ในเรื่องของการรณรงค์ป้องกันเมื่อจับตัวอาชญากรได้แล้วน่าจะต้องนำเสนอข่าวสาร ว่ามีการจับได้จริง เพื่อสร้างความมั่นใจให้สำหรับผู้ที่ถูกหลอก ผู้ที่อาจกำลังจะถูกหลอก ว่ามีเหตุการณ์เช่นนี้ด้วย ปัญหาการแจ้งความน้อยเป็นปัญหาหนึ่ง แต่หากแจ้งความแล้วตำรวจจับได้ ไม่ค่อยมีการประชาสัมพันธ์ว่าสามารถปราบปรามได้จริง มีประสิทธิภาพในกระบวนการยุติธรรม คนจะมั่นใจในกระบวนการยุติธรรมมากขึ้น[143]

ถ้าเป็นหลอกผ่านโซเชียลมีเดีย ผู้ประกอบการส่วนใหญ่ไม่ได้อยู่ในประเทศไทย เขาจะอยู่ต่างประเทศอาจจะต้องมีการขอความร่วมมือในการที่จะสืบหาว่ามันมาจากที่ไหน ตำรวจในประเทศนั้นช่วยดูแลได้ระดับหนึ่ง แต่อาจจะไม่ถึงขนาดที่ว่าเหมือนกับผู้ประกอบการที่อยู่ในเมืองไทยที่เราสามารถไปใช้อำนาจ ไปตรวจเป็นค้นได้[144]

การใช้มาตรการเชิงตักเตือนและระวังภัยมิให้มีพฤติกรรมเสี่ยงที่จะตกเป็นเหยื่อ ปัจจุบันไม่เพียงพอ เพราะผู้ที่ตกเป็นเหยื่อส่วนใหญ่ไม่รู้ตัวหรือไม่คาดคิดว่าตนเองจะตกเป็นเหยื่อ ดังนั้น การตักเตือนให้คนในสังคมระวังตัวเพียงอย่างเดียวจึงไม่เพียงพอ เพราะการพยายามไม่ทำตนให้มีพฤติกรรมเสี่ยงในการตกเป็นเหยื่อเป็นไปได้ยากเนื่องจากปัจจุบันมีการเข้าใช้งานโลกไซเบอร์มากขึ้น ซึ่งเป็นโลกที่ให้พื้นที่ในการติดต่อสื่อสารระหว่างกันที่ง่าย ดังนั้น แม้จะมีความระมัดระวังตัวแล้วแต่อาชญากรผู้มีความเชี่ยวชาญมากย่อมหาวิธีการหลอกล่อเหยื่อจนกระทั่งสำเร็จได้[145]

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ มาตรา 14 (1) กับ เรื่องที่สร้างภาระให้กับผู้ประกอบการซึ่งเป็นตัวกลางตามมาตร 15 และ 19 ในการช่วยดูแลแพลตฟอร์มหรือพื้นที่อาจเป็นการเพิ่มภาระผู้ให้กับผู้ประกอบการมากเกินไป มาตรา 14 (1) ผิดเรื่องของการปลอมแปลงตัวบุคคลอยู่แล้ว Phishing และเรื่อง Identity Thief เป็นการปลอมเพื่อหลอกลวงด้วย ถ้าหากจับได้มีความผิดแน่นอน แต่ถ้าหากไปบอกว่าต่อไปนี้คือ หน้าที่ของผู้ให้บริการ มาตรา 15 หากบอกว่าจะกลายเป็นตัวการร่วม คิดว่ามีเป็นภาระมากเกินไป หากใช้หลักการแจ้งเตือนเพื่อให้นำข้อมูลออกจากระบบ (Notice and Take Down) ปัจจุบันมีตัวใหม่มาให้แล้วคือ กฎกระทรวงฉบับใหม่ ที่ออกมาในเรื่องของการแจ้งเตือน เข้าใจว่าไม่ได้ครอบคลุมในเรื่องของหมิ่นประมาทอย่างเดียว น่าจะครอบคลุมการกระทำความผิดตามมาตรา 14 ทั้งหมดอยู่แล้ว เพราะฉะนั้นอยู่ที่การบังคับใช้ คิดว่าพร้อมแล้ว แต่

[142] นักวิชาการ. อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. (17 มกราคม 2562). สัมภาษณ์.

[143] นักวิชาการ. อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. (17 มกราคม 2562). สัมภาษณ์.

[144] นักวิชาการ. อาจารย์ประจำ สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช. (11 มิถุนายน 2562). สัมภาษณ์.

[145] นักวิชาการ. อาจารย์ประจำภาควิชาสังคมวิทยาและมานุษยวิทยา จุฬาลงกรณ์มหาวิทยาลัย. (14 กุมภาพันธ์ 2562). สัมภาษณ์.

กฎหมายที่เขียนไว้ก็ยังไม่ดีมาก ปัญหาที่นำมาถกเถียงกันได้ แต่หากมองกันในเรื่องของหลักการที่ออกมา และบทบัญญัติปัจจุบันครอบคลุมอยู่แล้ว ก็ Notice ไปว่าน่าจะมีปัญหาเรื่องนี้ ณ ปัจจุบันนี้ใครจะ Notice ก็ได้ ผู้ใช้บริการอินเตอร์เน็ตก็ทำได้ แต่เรื่องที่เป็นความผิดในลักษณะแบบนี้เป็นการป้องปราม อาจจะเป็นการมุ่งเน้นไปที่เจ้าพนักงานที่เป็นคน Notice[146]

ยุคนี้เป็นยุคเศรษฐกิจดิจิทัล กฎหมายข้อมูลส่วนบุคคลก็ดี กฎหมายความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติคอมพิวเตอร์ก็ดีต้องสร้างปัจจัยแวดล้อมส่งเสริมให้คนเข้ามาใช้มีความเชื่อถือมั่นใจว่าเข้ามาแล้วปลอดภัย ไม่ใช่เข้ามาแล้วมันแรงไปกลัวว่าตลาดนี้คนจะมาเอาข้อมูลเราไปตลาดนี้ เราอาจจะติดคุกติดตะรางแต่ว่าตรงนี้เราไม่ได้ทำเลย อย่างผู้ประกอบการผู้ให้บริการเขาไม่ได้ทำความผิดอะไรเลย หากใช้มาตรา 15 ไปจำคุกในฐานะตัวการร่วมกระทำความผิดตามมาตรา 14 ย่อมไม่เป็นธรรมกับเขาเพราะว่าเขาไม่ได้ทำอะไรอันนั้นก็เป็นอันหนึ่งซึ่งอาจจะไม่ได้เหมาะสมเพราะว่าในต่างประเทศเองเขาก็ไม่ได้ให้ผู้ให้บริการมารับเป็นถังขยะ เขาเป็นแค่ทางส่งผ่าน ซึ่งเป็นการสร้างภาระทางกฎหมาย[147]

ประเด็นในเรื่องความสมดุลระหว่าง การรุกล้ำความเป็นส่วนตัว กับ มาตรการสอดส่องโดยรัฐหรือเจ้าของระบบ (surveillance) ว่าสอดส่องข้อมูลเพื่อป้องกันและปราบปรามอาชญากรรม ซึ่งก็อาจจะช่วยได้แต่ว่าถ้ามันมีเรื่องของปัญหาในการรุกล้ำความเป็นส่วนตัวแล้ว จะเป็นดาบสองคมทำให้คนที่ใช้อินเตอร์เน็ตที่เขาจะอยู่ในช่องทางการติดต่อแบบส่วนตัวอาจจะถูกจับตามอง อีกประเด็นหนึ่งก็คือ คนที่อยู่ในประเทศไทยเป็นเหยื่อมากกว่าที่จะเป็นผู้กระทำความผิดเพราะฉะนั้นการที่จะต้องให้ผู้ใช้อินเตอร์เน็ตในโลกไซเบอร์ ก็เท่ากับว่าให้เหยื่อเปิดเผยตัวเองมากไปจนกลายเป็นความเสี่ยง แล้วยังไม่สามารถบังคับให้คนที่เป็นอาชญากรแสดงตัวได้ ซึ่งมันก็จะเป็นมาตรการที่ไม่ได้ผลและแก้ปัญหาไม่ตรงจุด[148]

จากผลการศึกษาในหัวข้อนี้ทั้งหมดสะท้อนให้เห็นว่า มาตรการทางกฎหมายและกระบวนการยุติธรรมที่เกี่ยวข้องก็ยังมีข้อจำกัดในการติดตามตัวผู้กระทำความผิดมาดำเนินคดีทางอาญา และชดเชยความเสียหายให้กับเหยื่อ ไม่ว่าจะเป็นความเสียหายทางทรัพย์สินที่ติดตามได้ยากเนื่องจาก มีการยักย้ายถ่ายโอนไปยังผู้อื่นหรือบุคคลนอกประเทศ ยิ่งถ้าเป็นความเสียหายต่อชีวิตและทางเพศย่อมเป็นการยากที่จะชดเชยให้กลับคืนมาสภาพดังเดิม นอกจากนี้ยังพบว่านักต้มตุ๋นจำนวนมากปฏิบัติการจากต่างประเทศ ซึ่งเพิ่มความลำบากให้กับกระบวนการยุติธรรมทางอาญาที่ต้องผสานความร่วมมือไปยังประเทศเจ้าของเขตอำนาจให้ส่งผู้ร้ายข้ามแดน หรือยึดทรัพย์สินกลับมาชดเชยความเสียหายให้กับเหยื่อ การสร้างมาตรการป้องกัน ปราบปรามโดยผู้ดูแลระบบและผู้บังคับใช้กฎหมาย และการสร้างความตระหนักรู้ให้กับประชาชนเพื่อให้รู้เท่าทันและไม่ตกเป็นเหยื่อจึงน่าจะเป็นผลดีกว่าการตามดำเนินคดีหลังจากเกิดความสูญเสียไปแล้ว

---

[146] นักวิชาการ. อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. (17 มกราคม 2562). สัมภาษณ์.

[147] นักวิชาการ. อาจารย์ประจำ สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช. (11 มิถุนายน 2562). สัมภาษณ์.

[148] นักวิชาการ. อาจารย์ประจำ ภาควิชาสังคมและสุขภาพคณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล. (15 พฤษภาคม 2562). สัมภาษณ์.

ดังนั้น เพื่อเป็นแนวทางในการป้องกันและปราบปรามพิศวาสอาชญากรรมทางคอมพิวเตอร์ซึ่งเป็นภัยคุกคามทางเทคโนโลยี งานวิจัยชิ้นนี้จึงทำการศึกษาวิจัยพิศวาสอาชญากรรมทางคอมพิวเตอร์ซึ่งเป็นสิ่งที่ส่งผลกระทบร้ายแรงอย่างมากในการใช้งานบนเครือข่ายอินเตอร์เน็ต ไม่ว่าจะความไว้วางใจในการใช้เทคโนโลยี หรือ ความเป็นส่วนตัวของข้อมูลต่างๆ บนโลกออนไลน์ เพื่อให้เกิดข้อเสนอแนะเชิงนโยบาย สร้างความตระหนักรู้ให้กับสังคม และสามารถนำไปใช้ให้เป็นมาตรการในการป้องกันปราบปรามพิศวาสอาชญากรรมทางคอมพิวเตอร์ ตลอดจนการพัฒนานโยบายของรัฐและเอกชน ผู้ดูแลระบบให้เกิดประโยชน์ต่อการพัฒนาเศรษฐกิจดิจิทัล และคุ้มครองสิทธิประชาชนในหัวข้อถัดๆ ไป

4.2.2 แนวทางพัฒนากฎหมายและมาตรการเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม

ในหัวข้อนี้จะแสดงผลการวิจัยที่เป็นแนวทางในการป้องกันและปราบปรามพิศวาสอาชญากรรมโดยอาศัยการปรับใช้มาตรการที่รัฐไทยมีอยู่แล้ว การพัฒนามาตรการต่างๆ ให้รองรับปัญหาได้ดีมากยิ่งขึ้น การศึกษามาตรการเปรียบเทียบจากต่างประเทศ และการพัฒนาความร่วมมือระหว่างประเทศ

1) การปรับใช้กฎหมายและกลไกเดิมที่มีอยู่

พิศวาสอาชญากรรม (Romance Scam) ก่อให้เกิดความเสียหายขึ้นในประเทศไทยเป็นจำนวนมาก แต่กลับเป็นความผิดที่แทบจะไม่สามารถนำตัวผู้กระทำความผิดที่แท้จริงมารับโทษได้เลย เนื่องจาก Romance Scam เป็นความผิดที่ผู้กระทำใช้เทคโนโลยีในการอำพรางตัวตน ทำให้ยากต่อการสืบค้นจับกุม เพราะนอกจากจะมีอุปสรรคด้านอุปกรณ์หรือเทคโนโลยีที่จำเป็นจะต้องมีความทันสมัยเพื่อก้าวให้ทันต่อเทคโนโลยีที่มีความเปลี่ยนแปลงอยู่ตลอดเวลาแล้ว ยังมีอุปสรรคในด้านความรู้ความเข้าใจของเจ้าหน้าที่ผู้มีส่วนเกี่ยวข้องต่อรูปแบบการกระทำความผิดของ Romance Scam อันมีลักษณะเฉพาะด้วย

แต่อย่างไรก็ตาม นอกจากความผิดฐานฉ้อโกง และความผิดตามพระราชบัญญัติคอมพิวเตอร์แล้ว Romance Scam ยังเป็นความผิดที่เกี่ยวโยงกับความผิดหลายฐานในกฎหมายหลายฉบับด้วยกัน ไม่ว่าจะเป็นความผิดตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542[149] พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 และพระราชบัญญัติคนเข้าเมือง พ.ศ. 2522 อีกด้วย กฎหมายเหล่านี้ได้กำหนดหลักเกณฑ์การได้มาซึ่งพยานหลักฐานไว้แตกต่างจากประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งจะส่งผลต่อการรับฟัง

[149] พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542 ลักษณะความผิดในคดี Romance Scam ถือเป็นหนึ่งในความผิดมูลฐานของพระราชบัญญัตินี้ กล่าวคือ เป็นความผิดเกี่ยวกับทรัพย์ตามประมวลกฎหมายอาญาอันมีลักษณะเป็นปกติธุระ ตามมาตรา 3 (18) คือ

(18) ความผิดเกี่ยวกับการลักทรัพย์ กรรโชก รีดเอาทรัพย์ ชิงทรัพย์ ปล้นทรัพย์ ฉ้อโกง หรือยักยอก ตามประมวลกฎหมายอาญา อันมีลักษณะเป็นปกติธุระ

พยานหลักฐานของศาลที่มิจำเป็นต้องปฏิบัติตามเงื่อนไขที่ระบุไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา แต่สามารถรับฟังพยานหลักฐานภายใต้เงื่อนไขและหลักเกณฑ์ของกฎหมายต่างๆ เหล่านี้แทนได้

สำหรับการทำงานของเจ้าหน้าที่นั้น กฎหมายต่างๆ เหล่านี้ได้กำหนดให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัติมีอำนาจในการสืบสวนสอบสวนได้เช่นเดียวกับพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา[150] แต่กลับมีอำนาจกระทำการมากกว่าพนักงานสอบสวนหรือเจ้าพนักงานตามประมวลกฎหมายวิธีพิจารณาความอาญา กล่าวคือ

พนักงานเจ้าหน้าที่ตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 นั้น นอกจากจะมีอำนาจหน้าที่ในการสืบสวนสอบสวนได้เหมือนดังเช่นพนักงานสอบสวนแล้ว ในกรณีมีเหตุอันควรเชื่อได้ว่าหากเนิ่นช้ากว่าจะรอหมายค้นมาได้ ทรัพย์สินหรือพยานหลักฐานนั้นอาจถูกยักย้าย ซุกซ่อน ทำลาย หรือทำให้เปลี่ยนสภาพไปจากเดิมได้ พนักงานเจ้าหน้าที่มีอำนาจเข้าไปในเคหสถาน สถานที่ หรือยานพาหนะใดๆ ที่มีเหตุอันควรสงสัยว่าจะมีการซุกซ่อนทรัพย์สินที่เกี่ยวกับการกระทำความผิด หรือพยานหลักฐานที่เกี่ยวกับการกระทำความผิดฐานฟอกเงินได้โดยไม่ต้องมีหมายค้น[151] ด้วย นอกจากนี้ พนักงานเจ้าหน้าที่ตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงินฯ นี้ยังมีอำนาจในการเข้าถึงบัญชีของลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ที่ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน[152] และยังมีอำนาจในการจัดทำเอกสารหลักฐานหรืออำพรางตนเพื่อประโยชน์ในการตรวจสอบและรวบรวม

---

[150] พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542 มาตรา 12 และ พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556 มาตรา 14

พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542 มาตรา 12

มาตรา 12 ในการปฏิบัติการตามพระราชบัญญัตินี้ ให้กรรมการ อนุกรรมการ กรรมการธุรกรรม เลขาธิการ รองเลขาธิการ และพนักงานเจ้าหน้าที่ เป็นเจ้าพนักงานตามประมวลกฎหมายอาญา

พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556 มาตรา 3

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งอัยการสูงสุด หรือผู้บัญชาการตำรวจแห่งชาติ แต่งตั้งให้ช่วยเหลือพนักงานสอบสวนในการสืบสวนสอบสวนและป้องกันปราบปรามการกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติตามพระราชบัญญัตินี้

[151] พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 38 (3)

(3) เข้าไปในเคหสถาน สถานที่ หรือยานพาหนะใดๆ ที่มีเหตุอันควรสงสัยว่ามีการซุกซ่อนหรือเก็บรักษาทรัพย์สินที่เกี่ยวกับการกระทำความผิด หรือพยานหลักฐานที่เกี่ยวกับการกระทำความผิดฐานฟอกเงิน เพื่อตรวจค้นหรือเพื่อประโยชน์ในการติดตาม ตรวจสอบ หรือยึด หรืออายัดทรัพย์สิน หรือพยานหลักฐาน เมื่อมีเหตุอันควรเชื่อได้ว่าหากเนิ่นช้ากว่าจะเอาหมายค้นมาได้ ทรัพย์สินหรือพยานหลักฐานดังกล่าวนั้นจะถูกยักย้าย ซุกซ่อน ทำลาย หรือทำให้เปลี่ยนสภาพไปจากเดิม

[152] พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 46 วรรคหนึ่ง

มาตรา 46 ในกรณีที่มีพยานหลักฐานตามสมควรว่าบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน พนักงานเจ้าหน้าที่ซึ่งเลขาธิการมอบหมายเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่อศาลแพ่ง เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าถึงบัญชี ข้อมูลทางการสื่อสาร หรือข้อมูลคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลดังกล่าวนั้นก็ได้

พยานหลักฐานเพื่อดำเนินการกับทรัพย์สินที่เกี่ยวกับการกระทำความผิด หรือดำเนินคดีฐานฟอกเงินด้วย[153]

ส่วนอำนาจที่นอกเหนือไปจากพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญานั้น พนักงานเจ้าหน้าที่ผู้ได้รับมอบหมาย ตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มีอำนาจในการยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุมัติให้กระทำการใดๆ ให้ได้มาซึ่งเอกสารหรือข้อมูลข่าวสารซึ่งส่งทางคอมพิวเตอร์ เครื่องมือ อุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีใดที่ถูกใช้หรืออาจถูกใช้เพื่อให้ได้รับประโยชน์จากการกระทำความผิดได้[154] รวมถึงมีอำนาจในการจัดทำเอกสารหรือหลักฐานใดขึ้นหรือปฏิบัติการอำพรางใดเพื่อประโยชน์ในการสืบสวนสอบสวน ซึ่งการกระทำเหล่านี้ถือว่าเป็นการกระทำโดยชอบด้วยกฎหมาย[155] ทั้งยังมีอำนาจในการใช้เครื่องมือสื่อสารโทรคมนาคม เครื่องมืออิเล็กทรอนิกส์ หรือด้วยวิธีการใด ในการสะกดรอยผู้ต้องสงสัยว่ากระทำหรือจะกระทำความผิด เพื่อสืบสวน จับกุม แสวงหา และรวบรวมพยานหลักฐานได้[156]

---

[153] พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 46/1

มาตรา 46/1 ในการปฏิบัติการตามอำนาจหน้าที่ หากพนักงานเจ้าหน้าที่มีความจำเป็นต้องจัดทำเอกสารหลักฐานหรือการอำพรางตนเพื่อประโยชน์ในการตรวจสอบและรวบรวมพยานหลักฐานเพื่อดำเนินการกับทรัพย์สินที่เกี่ยวกับการกระทำความผิด การดำเนินคดีฐานฟอกเงิน หรือการดำเนินคดีเกี่ยวกับการสนับสนุนทางการเงินแก่การก่อการร้ายตามกฎหมายว่าด้วยการป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้าย ให้เลขาธิการมีอำนาจสั่งเป็นหนังสือให้พนักงานเจ้าหน้าที่ดำเนินการดังกล่าวได้ตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการกำหนด

[154] พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 17 วรรคหนึ่ง

มาตรา 17 ในกรณีที่มีเหตุอันควรเชื่อว่าเอกสารหรือข้อมูลข่าวสารซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีใด ถูกใช้หรืออาจถูกใช้เพื่อให้ได้รับประโยชน์จากการกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พนักงานสอบสวนซึ่งได้รับอนุมัติจากอัยการสูงสุด ผู้บัญชาการตำรวจแห่งชาติ หรือผู้ซึ่งได้รับมอบหมาย แล้วแต่กรณี อาจยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้ได้มาซึ่งเอกสารหรือข้อมูลข่าวสารดังกล่าวก็ได้

[155] พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 19 วรรคหนึ่งและวรรคสาม

มาตรา 19 ในกรณีจำเป็นและเพื่อประโยชน์ในการสืบสวนสอบสวนเกี่ยวกับความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ให้อัยการสูงสุด ผู้บัญชาการตำรวจแห่งชาติ หรือผู้ซึ่งได้รับมอบหมาย แล้วแต่กรณี มอบหมายให้บุคคลใดจัดทำเอกสารหรือหลักฐานใดขึ้นหรือปฏิบัติการอำพรางเพื่อประโยชน์ในการสืบสวนสอบสวน ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่อัยการสูงสุดกำหนดในข้อบังคับ

การจัดทำเอกสารหรือหลักฐานใด หรือการปฏิบัติการอำพรางตามวรรคหนึ่งให้ถือว่าเป็นการกระทำโดยชอบด้วยกฎหมาย

[156] พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 21

มาตรา 21 พนักงานสอบสวนหรือพนักงานเจ้าหน้าที่อาจใช้เครื่องมือสื่อสารโทรคมนาคม เครื่องมืออิเล็กทรอนิกส์ หรือด้วยวิธีการใด เฉพาะในการสะกดรอยผู้ต้องสงสัยว่ากระทำความผิดหรือจะกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ เพื่อสืบสวน จับกุม แสวงหาและรวบรวมพยานหลักฐาน ทั้งนี้ ตามข้อบังคับที่อัยการสูงสุดกำหนด

จากหลักกฎหมายที่ได้กล่าวมาข้างต้น จะเห็นได้ว่าพนักงานเจ้าหน้าที่สามารถนำหลักกฎหมายเหล่านี้มาใช้เพื่อนำตัวผู้กระทำความผิดมาลงโทษได้ และเนื่องจากผู้กระทำความผิดส่วนมากในคดี Romance Scam มักเป็นชาวต่างชาติที่มีทั้งกระทำความผิดในขณะที่อยู่นอกราชอาณาจักร หรือแบบที่เดินทางเข้ามาอาศัยอยู่ในราชอาณาจักรเป็นการชั่วคราวเพื่อกระทำความผิดโดยมีคนไทยเป็นผู้ร่วมกระทำความผิด ในกรณีดังกล่าวนี้พนักงานเจ้าหน้าที่สามารถนำพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 พระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 และพระราชบัญญัติคนเข้าเมือง พ.ศ. 2522 มาใช้บังคับได้

สำหรับผู้กระทำความผิดชาวต่างชาติที่จะเข้ามาอาศัยอยู่ในราชอาณาจักรนั้น พนักงานเจ้าหน้าที่มีอำนาจตรวจบุคคลที่เดินทางเข้ามาในหรือออกไปนอกราชอาณาจักร[157] โดยมีอำนาจสั่งห้ามมิให้คนต่างด้าวที่มีพฤติการณ์เป็นที่น่าเชื่อว่าเป็นบุคคลที่เป็นภัยต่อสังคม หรือจะก่อเหตุร้ายให้เกิดอันตรายต่อความสงบสุขหรือความปลอดภัยของประชาชน หรือเข้ามาเพื่อประกอบกิจการอื่นที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนเข้ามาในราชอาณาจักรได้[158] และเนื่องจากผู้กระทำความผิดในคดี Romance Scam มักขอเข้ามาในราชอาณาจักรเพื่อการท่องเที่ยว[159] ทำให้ยากต่อการคัดกรองของเจ้าหน้าที่ แต่หากคนต่างด้าวเหล่านั้นมีพฤติการณ์ที่สมควรเพิกถอนการอนุญาตให้อยู่ในราชอาณาจักร พนักงานเจ้าหน้าที่โดยคณะกรรมการพิจารณาคนเข้าเมืองหรืออธิบดีกรมตำรวจมีอำนาจเพิกถอนการอนุญาตให้อยู่ในราชอาณาจักรของคนต่างด้าวเหล่านั้นได้[160]

---

[157] พระราชบัญญัติคนเข้าเมือง พ.ศ. 2522 มาตรา 18

มาตรา 18 พนักงานเจ้าหน้าที่มีอำนาจตรวจบุคคลซึ่งเดินทางเข้ามาหรือออกไปนอกราชอาณาจักร

เพื่อการนี้ บุคคลซึ่งเดินทางเข้ามาหรือออกไปนอกราชอาณาจักรต้องผ่านกมาตรวจอนุญาตของพนักงานเจ้าหน้าที่ของด่านตรวจคนเข้าเมืองประจำเส้นทางนั้น และถ้าผู้นั้นเป็นคนต่างด้าวต้องยื่นรายการตามแบบที่กำหนดในกฎกระทรวงด้วย

[158] พระราชบัญญัติคนเข้าเมือง พ.ศ. 2522 มาตรา 12 (7) (8)

มาตรา 12 ห้ามมิให้คนต่างด้าวซึ่งมีลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้ เข้ามาในราชอาณาจักร

(7) มีพฤติการณ์เป็นที่น่าเชื่อว่าเป็นบุคคลที่เป็นภัยต่อสังคม หรือจะก่อเหตุร้ายให้เกิดอันตรายต่อความสงบสุขหรือความปลอดภัยของประชาชน หรือความมั่นคงแห่งราชอาณาจักร หรือบุคคลซึ่งเจ้าหน้าที่รัฐบาลต่างประเทศได้ออกหมายจับ

(8) มีพฤติการณ์เป็นที่น่าเชื่อว่าเข้ามาเพื่อการค้าประเวณี การค้าหญิงหรือเด็ก การค้ายาเสพติดให้โทษ การลักลอบหนีศุลกากร หรือเพื่อประกอบกิจการอื่นที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

[159] พระราชบัญญัติคนเข้าเมือง พ.ศ. 2522 มาตรา 34 (3)

มาตรา 34 คนต่างด้าวซึ่งจะเข้ามาในราชอาณาจักรเป็นการชั่วคราวได้ จะต้องเข้ามาเพื่อการดังต่อไปนี้

(3) การท่องเที่ยว

[160] พระราชบัญญัติคนเข้าเมือง พ.ศ. 2522 มาตรา 36 วรรคหนึ่ง

มาตรา 36 คนต่างด้าวซึ่งได้รับอนุญาตให้อยู่ในราชอาณาจักรเป็นการชั่วคราว หากมีพฤติการณ์ที่สมควรเพิกถอนการอนุญาตให้อยู่ในราชอาณาจักร ให้อธิบดีหรือคณะกรรมการมีอำนาจเพิกถอนการอนุญาตที่ได้อนุญาตไว้นั้นได้ ไม่ว่าอธิบดีหรือผู้ซึ่งอธิบดีมอบหมายเป็นผู้อนุญาต

ส่วนผู้กระทำความผิดที่อยู่นอกราชอาณาจักร ก็สามารถนำพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 พระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 มาบังคับใช้ได้ โดยหากผู้กระทำความผิดไม่ได้อาศัยอยู่ในประเทศที่ไทยมีสนธิสัญญาว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา หรือไม่ได้อาศัยอยู่ในประเทศที่ไทยมีสนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างกัน ก็สามารถขอความร่วมมือจากประเทศที่ผู้กระทำความผิดอาศัยอยู่ได้โดยอาศัยวิธีการทางการทูตได้[161]

จะเห็นได้ว่าความผิดในคดี Romance Scam เป็นการกระทำที่ถือเป็นความผิดตามกฎหมายหลายฉบับด้วยกัน ทำให้พนักงานเจ้าหน้าที่ที่เกี่ยวข้องทั้งหมดมีอำนาจทำการสืบสวนสอบสวนคดีนี้ได้ ดังเช่นพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา และในขณะเดียวกันพนักงานสอบสวนก็สามารถนำหลักเกณฑ์และวิธีการสืบสวนสอบสวนซึ่งก็คือการค้นหาพยานหลักฐานในกฎหมายหลากหลายฉบับที่เกี่ยวข้องเหล่านี้มาใช้แทนประมวลกฎหมายวิธีพิจารณาความอาญา รวมถึงขอความร่วมมือกับต่างประเทศได้โดยอาศัยช่องทางทางการทูตหรือสนธิสัญญา ซึ่งจะช่วยลดข้อจำกัดในเรื่องการรับฟังพยานหลักฐานของศาลไปได้ อันจะนำมาซึ่งการนำตัวผู้กระทำความผิดมารับโทษได้ในที่สุด

2) การพัฒนากฎหมายและมาตรการเพื่อป้องกันและปราบปรามให้ดียิ่งขึ้น

ในรัฐเสรีนิยมประชาธิปไตยไม่สนับสนุนการที่รัฐจะเข้าไปควบคุมพฤติกรรมของคน หรือการเข้าไปสอดส่องมากเกินไปเพราะเสี่ยงต่อการละเมิดสิทธิมนุษยชนขั้นพื้นฐานและทำลายบรรยากาศทางเศรษฐกิจ ดังนั้น มาตรการที่พึงประสงค์ ก็คือ การสร้างภูมิคุ้มกันในเชิงการรณรงค์ การประชาสัมพันธ์ การสร้างความเชื่อมั่นในกระบวนการยุติธรรม ให้ประชาชนรู้ มีช่องทางเพิ่มมากขึ้นในการแจ้งข่าวสาร การร้องทุกข์ หรือการเตรียมบุคลากรให้พร้อม บุคลากรอาจจะต้องมีทั้งหญิงและชายมีความหลากหลายมากยิ่งขึ้น เพราะบางครั้งเรื่องพวกนี้เป็นความผิดเกี่ยวกับเพศด้วย มันเกี่ยวพันกับทางเพศ การที่ผู้เสียหายจะกล้าเข้ามาแจ้งความร้องทุกข์ก็ไม่ต่างกับคดีข่มขืนคดีอนาจาร ถ้าหากเป็นคนที่ไม่มีความ

---

[161] พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 มาตรา 9 (1) และ พระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 มาตรา 8 วรรคสอง

พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 มาตรา 9 (1)

มาตรา 9 การให้ความช่วยเหลือแก่ต่างประเทศต้องอยู่ในหลักเกณฑ์ ดังต่อไปนี้

(1) ประเทศไทยอาจให้ความช่วยเหลือแก่ประเทศผู้ร้องขอได้ แม้ว่าจะไม่มีสนธิสัญญาว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญาระหว่างกัน แต่ประเทศผู้ร้องขอต้องแสดงว่าจะให้ความช่วยเหลือในทำนองเดียวกันเมื่อประเทศไทยร้องขอ

พระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 มาตรา 8 วรรคหนึ่งและวรรคสอง

มาตรา 8 การส่งผู้ร้ายข้ามแดนให้เริ่มต้นด้วยการมีคำร้องขอให้ส่งผู้ร้ายข้ามแดนจากประเทศผู้ร้องขอ

คำร้องขอให้ส่งผู้ร้ายข้ามแดนของประเทศผู้ร้องขอที่มีสนธิสัญญาส่งผู้ร้ายข้ามแดนกับประเทศไทย ให้จัดส่งไปยังผู้ประสานงานกลาง ในกรณีที่ประเทศผู้ร้องขอมิได้มีสนธิสัญญาส่งผู้ร้ายข้ามแดนกับประเทศไทย ให้จัดส่งคำร้องขอดังกล่าวโดยผ่านวิธีการทางการทูต

เชื่อมั่นว่าจะเป็นการเปลือยเปล่าชีวิตเขาอีกครั้งหนึ่งหรือไม่ เขาจะสับสนไม่กล้ามาแจ้งความ จึงต้องอาศัยการรณรงค์ประชาสัมพันธ์[162]

การออกแบบวิธีการร้องทุกข์และดำเนินคดีที่ไม่ต้องเปิดเผยตัวตนหรือเป็นช่องทางร้องเรียนประสานงานออนไลน์เพื่อที่จะลดความอับอายเพราะผู้เสียหายไม่อยากจะเปิดเผยตัวตน และกล้าเล่าเรื่องราวความรู้สึกของเขาออกมา ก็จะเพิ่มความเป็นไปได้ในการแก้ปัญหา[163]

การพัฒนากระบวนการที่สามารถช่วยเหลือเยียวยาเหยื่อในความเสียหายทางแพ่งและการติดตามทรัพย์สินกลับคืนมาชดใช้สินไหมทดแทน หากมีมาตรการที่ช่วยเยียวยาหรือรับเรื่องร้องทุกข์ให้กับผู้เสียหายแล้วก็อาจจะทำให้ผู้ตกเป็นเหยื่อเข้ามาร้องทุกข์มากขึ้น[164]

การสร้างบุคลากรเพิ่ม มิใช่เพียงสร้างศูนย์ประสานงานแต่บุคลากรไม่เพียงพอ การสร้างบุคลากรที่เข้าใจอาชญากรรมเกี่ยวกับคอมพิวเตอร์ในภาพรวมทั้งหมด อาจจะต้องมีศูนย์อย่างน้อยที่สุดจังหวัดหรือภาคละ 1 ศูนย์ เริ่มต้นเอาจะมีภาคละ 1 ศูนย์ คือ ให้ความรู้บุคลากรในกระบวนการยุติธรรมและสร้างบุคลากรใหม่ด้วย คิดว่าวิธีการแบบนี้เหมาะสมในแง่ที่เอาคนที่มีความรู้ความเชี่ยวชาญด้านนั้น ๆ มาเป็นเจ้าหน้าที่ ไม่ได้เอาเพียงเจ้าหน้าที่ไปอบรม เทียบกับต่างประเทศผู้ที่ทำเรื่องดังกล่าวต้องเป็นผู้เชี่ยวชาญมาก่อนแล้วค่อยมาอบรมการเป็นเจ้าพนักงาน[165]

การฝึกอบรมเจ้าพนักงานหรือการสร้างช่องทางรับเรื่องราวร้องทุกข์ในอุดมคติจะต้องเอาตัวประชาชนเป็นตัวตั้ง คือ ผู้เสียหายสะดวกที่ไหนเขาควรจะไปได้โดยไม่ลำบากยากเข็ญ เช่น เขาอยู่ต่างจังหวัดตำบลหรืออำเภอไกลๆ โรงพักซึ่งมีอยู่ทั่วประเทศต้องสามารถที่จะรับแจ้งความเป็นการเบื้องต้นได้ ถ้าจะเป็นการดีพนักงานสอบสวนเราเรียกว่าเขาเข้าใจใน 3-D หนึ่ง Digital Context คือ บริบททางเทคโนโลยี สอง คือ Digital Fact รู้ข้อเท็จจริงทางเทคโนโลยี เมื่อพิจารณาร่วมกับบริบททางเทคโนโลยีก็จะวินิจฉัยได้ว่าขณะที่มือถือปิดเครื่องเฉย ๆ มันเป็นดิจิตอลไหมมันเป็นคอมพิวเตอร์หรือเปล่า ซึ่งมันไม่เป็นเพราะมันไม่อยู่ในภาวะที่สามารถประมวลผลได้ สาม Digital Way คือ วิถีทางทางดิจิตอล เช่น การทำลายลบเปลี่ยนแปลงแก้ไขมันจะต้องเป็นวิถีทางพรางดิจิตอลมันต้องอยู่ในไซเบอร์กฎหมายคุ้มครองในโลกไซเบอร์ พอนอกโลกไซเบอร์เป็นกฎหมายปกติก็เป็นกฎหมายอาญาเป็นสาระบัญญัติทางอาญาทั่วไปทางกายภาพทั่วไป[166]

เมื่อต้องทำสำนวนหรือขึ้นเป็นพยานในศาลก็ต้องเข้าใจเรื่องเหตุอันควรเชื่อคำพยาน ซึ่งต้องประกอบไปทุกอย่างไม่ว่าจะเป็นตัวผู้เบิกความ หนึ่ง มีอำนาจหน้าที่หรือไม่ สอง คุณมีประสบการณ์ความรู้ความเชี่ยวชาญตรงนี้อย่างไร ใช้เครื่องมืออะไรในการตรวจ เครื่องมือมีใบอนุญาต (License) ไหม ถูกลิขสิทธิ์ไหมเครื่องมือฮาร์ด / ซอฟต์แวร์ได้รับมาตรฐานไหมคุณใช้ยี่ห้ออะไร บางคนก็ถามอย่าง

---

[162] นักวิชาการ. อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. (17 มกราคม 2562). สัมภาษณ์.

[163] นักวิชาการ. อาจารย์ประจำ สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช. (11 มิถุนายน 2562). สัมภาษณ์.

[164] นักวิชาการ. อาจารย์ประจำภาควิชาสังคมวิทยาและมานุษยวิทยา จุฬาลงกรณ์มหาวิทยาลัย. (14 กุมภาพันธ์ 2562). สัมภาษณ์.

[165] นักวิชาการ. อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. (17 มกราคม 2562). สัมภาษณ์.

[166] ตำรวจท่องเที่ยว. ผู้บังคับการตำรวจท่องเที่ยว กองบังคับการตำรวจท่องเที่ยว 2. (12 มิถุนายน 2562). สัมภาษณ์.

นี้มันถูกปนเปื้อนอะไรหรือเปล่า ฉะนั้นเมื่อทางทนายถามก็ต้องพยายามตอบให้รักษารูปคดีได้ ปกติแล้วการสอบสวนก็จะมีหลัก “ใช่ เชื่อ ชอบ” นั่นคือ[167]

ใช่ ก็คือ ตรงประเด็นตรงเป้าเพื่อพิสูจน์พยานหลักฐานทั้งหมดมีความสอดคล้องต้องการอย่างไร

เชื่อ กระบวนการสืบสวนสอบสวนน่าเชื่อถือหรือเปล่ากระบวนการ (process) ถูกกฎหมายไหมหรือกระบวนการในห้อง lab มันมีการปนเปื้อนไหนมีโอกาสที่จะข้อมูลดิจิทัลจะหายไปได้ไหม ข้อมูลดิจิทัลชุดนี้จะถูกเปลี่ยนแปลงหรือถูกทำลายได้ไหม

ชอบ ก็คือ ชอบด้วยกฎหมายหรือไม่ ฉะนั้นถ้าทนายเก่งก็พยามที่จะมาถามค้านในเรื่องของกระบวนการทั้งหมดว่าอาจจะไม่น่าเชื่อถือ ซึ่งเจ้าพนักงานก็ต้องดำเนินการทุกขั้นตอนให้เป็นไปตามกรอบกฎหมายเพื่อป้องกันมิให้สูญเสียความน่าเชื่อถือ

การทำงานเชิงรุกในหน่วยงานรัฐโดยเฉพาะหน่วยงานที่บังคับใช้กฎหมาย คือ ตำรวจน่าจะมีการเผยแพร่ข้อมูลในการดำเนินการว่าสมมุติเราตกเป็นเหยื่อหรือมีข้อสงสัยว่าเราจะตกเป็นเหยื่อเราจะดำเนินการยังไงได้บ้างในการที่จะดำเนินการในการร้องทุกข์แล้ว อีกอย่างหนึ่งก็คือมันเป็นปัญหาที่มันคาบเกี่ยวกันกรณีอื่นด้วยคนส่วนใหญ่คิดว่า ถ้ามันเกิดขึ้นบนอินเตอร์เน็ตก็จะไป ปอท. แต่กรณีนี้มันใช้เรื่องของฉ้อโกงธรรมดาก็ได้ ถ้าสมมุติมันเป็นฉ้อโกงธรรมดา ปอท. ก็อาจจะมองว่ามันเป็นเรื่องของกฎหมายอาญาธรรมดาซึ่งดำเนินการได้โดยหน่วยงานใดก็ดี จึงต้องมีการเผยแพร่ชุดความรู้ที่ชัดเจนว่าตกลงถ้ามีลักษณะนี้มันจะเข้ากฎหมายเรื่องนี้หน่วยงานใดบ้างที่สามารถที่จะดำเนินการได้อาจจะไม่จำเป็นต้องมาปอท.แค่แจ้งความตามปกติทั่วไป[168]

มาตรการที่หน่วยงานรัฐพึงทำ คือ สร้างมาตรฐานว่าเว็บไหนที่มีมาตรฐานความปลอดภัยเพื่อสร้างความมั่นใจให้ประชาชนเข้าใช้ระบบหรือแอปพลิเคชันเหล่านั้น แต่อย่างน้อยมันต้องมีการมีมาตรฐานกับเว็บไซต์ มาตรการในการป้องกันว่าอันตรายที่มันจะมีให้มันน้อยที่สุด มาตรการในการสร้างความตระหนักรู้ ให้คุณเข้าใจหรือว่าการใช้สื่อออนไลน์มันไม่ได้ปลอดภัยอย่างที่คิดไว้ มีความสะดวกแต่มันมีภัยซ่อนอยู่เพราะฉะนั้นการใช้ทุกอย่างต้องใช้อย่างมีสติแล้วก็มีความตระหนักรู้ถึงโทษและก็คุณของสิ่งที่เราใช้อยู่ เพราะฉะนั้นมาตรการหลังๆ มันเป็นปลายทางแม้กระทั่งกฎหมายเองก็เป็นปลายทาง[169]

[167] ตำรวจท่องเที่ยว. ผู้บังคับการตำรวจท่องเที่ยว กองบังคับการตำรวจท่องเที่ยว 2. (12 มิถุนายน 2562). สัมภาษณ์.

[168] นักวิชาการ. อาจารย์ประจำ ภาควิชาสังคมและสุขภาพคณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล. (15 พฤษภาคม 2562). สัมภาษณ์.

[169] นักวิชาการ. อาจารย์ประจำ สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช. (11 มิถุนายน 2562). สัมภาษณ์.

มาตรการป้องกันไม่ให้เกิดอาชญากรรมซ้ำอีก คือ การให้ความรู้เผยแพร่ความรู้ความเข้าใจเกี่ยวกับกรณีพิศวาสอาชญากรรม เพื่อรู้เท่าทันสถานการณ์ มีการโฆษณาบ่อยๆ เตือนภัยเรื่องการล่อลวงรูปแบบต่างๆ [170] ควรมีการแจ้งเตือนจากหน่วยงานรัฐ หรือทำละครออกมาเป็นข้อคิดให้ประชาชน และการให้กำลังใจเหยื่อเพื่อดำเนินคดีไม่ถอดใจหรือใช้ชีวิตต่อไปได้ไม่สิ้นหวัง[171]

3) มาตรการป้องกันและแนวทางการแก้ไขโดยศึกษาเปรียบเทียบจากต่างประเทศ

การป้องกันการหลอกลวงนี้เป็นเรื่องที่จัดการยากมาก ไม่ว่าจะโดยการจับหรือการดำเนินคดี เนื่องจากอาชญากรมักเป็นชาวต่างชาติที่อยู่คนละประเทศกับเหยื่อ นอกจากนั้นการติดตามก็เป็นเรื่องที่ยากและใช้เวลานานพอสมควร ดังนั้นควรมีการกระตุ้นให้ผู้ใช้งานบนเครือข่ายออนไลน์รายงานเมื่อทราบว่าโปรไฟล์นั้นเป็นโปรไฟล์ปลอมเพื่อลดจำนวนโปรไฟล์ของอาชญากรในเว็บไซต์นั้น ส่วนด้านการบังคับใช้กฎหมายก็พยายามที่จะกำหนดให้มีการเปลี่ยนแปลงวิธีการโอนเงินให้รัดกุมมากยิ่งขึ้นผ่านบริษัทต่างๆ เช่น Western Union และ MoneyGram เป็นต้น[172] ซึ่งทำให้ติดตามและจับกุมง่ายยิ่งขึ้น แต่อย่างไรก็ตามยังพบว่าอาชญากรมีทักษะสูงในการหาช่องโหว่ทางกฎหมายเพื่อทำหลอกลวงดังกล่าว เช่น จูงใจให้เหยื่อโอนเงินให้เหยื่ออีกคนหนึ่ง เพื่อให้ทำเหยื่ออีกคนนั้นตกอยู่กระบวนการฉ้อโกงหรือการฟอกเงินนี้ด้วย นอกจากนั้นควรต้องให้ผู้ดูแลระบบสร้างการรักษาความปลอดภัยในระบบและการเตือนผู้ใช้งานในเว็บไซต์ว่าเสี่ยงต่อการถูกหลอกแล้วหรือไม่

การดำเนินงานของตำรวจนครบาลอังกฤษ ในปี 2012-2013 พบว่า ผู้กระทำผิดในอังกฤษถูกนำตัวเข้าพิจารณาคดี และสารภาพผิดกับการสมรู้ร่วมคิดในการกระทำความผิดโดยการบิดเบือนความจริง พบผู้เสียหาย 62 ราย จากอเมริกา, แคนนาดา, และเกาะในประเทศตรินิแดดและโตเบโก (ผู้หญิง 18 ราย ในนั้นจำนวนนั้นยินดีที่จะช่วยตำรวจในการฟ้องร้องคดีอาญา) มีความพยายามในการจัดการป้องกันปัญหาดังกล่าวโดยการจัดอบรมหลักสูตร “London City Police National Fraud Course”[173] เป็นหลักสูตรเข้มข้น 3 สัปดาห์ ด้วยการฝึกตำรวจ 30-50 คน ให้จัดการกับการหลอกลวง ในปี 2012-2013 แบ่งการฝึกออกเป็น 2 ช่วงคือ การอบรม และการให้คำแนะนำเกี่ยววิธีการที่ดีกว่าที่ตำรวจต้องใช้จัดการกับผู้ที่ตกเป็นเหยื่อของ romance scams เช่น การพิจารณาถึงผลกระทบที่จะตามมา, ผลกระทบทางจิตใจ และการกลับไปเป็นเหยื่อซ้ำแล้วซ้ำเล่า Monica T. Whitty ได้แนะนำทางที่ดีที่สุดของการสืบสวนสอบสวนเหยื่อ และการให้การสนับสนุนอย่างต่อเนื่องสำหรับการดำเนินคดีอาญาระหว่างประเทศ เหยื่อมักให้การปฏิเสธในขั้นต้น และต้องการกำลังใจที่จะยอมรับว่าความสัมพันธ์ของพวกเขาเป็นเรื่องที่หลอกลวง นอกจากนั้นยังเหยื่อต้องการการสนับสนุนจากครอบครัวแต่พวกเขาไม่เคย

---

[170] ผู้เสียหายไม่ประสงค์ออกนาม คนที่ 1. ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม. (7 เมษายน 2562). สัมภาษณ์.

[171] ผู้เสียหายไม่ประสงค์ออกนาม คนที่ 5. ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม. (7 เมษายน 2562). สัมภาษณ์.

[172] Whitty, M. T., (2015). Mass-marketing fraud: a growing concern. *IEEE Security & Privacy*, *13*(4), 84-87.

[173] Research Excellence Framework 2014. (2014) “Confronting online dating scams: working with police and the industry.” 36 Communication Cultural and Media Studies. University of Leicester.

ได้รับเลย Monica T. Whitty ร่วมกับ SOCA ส่งจดหมายถึงเหยื่อ 50 ราย ในละเวกนั้นเพื่อหวังว่าจะขัดขวางไม่ให้พวกเหยื่อโอนเงินให้กับ scammer และออกทีวี และวิทยุเพื่อเตือนให้คนตระหนักถึงภัยดังกล่าว อีกทั้งมีหน่วยงานที่จัดการเรื่องดังกล่าวดังนี้ [174]

- Ghana prosecution by the Serious Organised Crime Agency (2011-ongoing) – ร่วมมือกันเพื่อเตรียมความพร้อมของเหยื่อพิศวาสอาชญากรรมเมื่อต้องขึ้นศาลในประเทศกานา และเตรียมหลักฐานงานวิจัยต่างๆ เพื่อต่อสู้กับข้อโต้แย้งของอาชญากรที่ว่า “เหยื่อมีความบกพร่องทางจิต” ไม่ใช่การกระทำความตามผิดกฎหมายของเหล่าอาชญากร
- Establishment of the Economic Crime Unit (for new National Crime Agency) (2012) - ตั้งขึ้นเมื่อปี ค.ศ. 2012 ตามคำแนะนำของนักวิชาการในมหาวิทยาลัยสหราชอาณาจักร เพื่อให้ผู้บังคับใช้กฎหมายเข้าใจถึงความสูญเสียของผู้ที่ตกเป็นเหยื่อนำไปสู่การชดใช้ความเสียหายอย่างแท้จริง
- International Mass Marketing Fraud Working Group (2011-ongoing) - เป็นการรวมกลุ่มของตัวแทนหน่วยงานบังคับใช้กฎหมายทั่วโลก เพื่อแลกเปลี่ยนข้อมูลและกลยุทธ์ในการป้องกันเรื่องดังกล่าว เช่น Serious Organised Crime Agency, FBI, Federal Trade Authority, Secret Service, the Royal Canadian Mounted Police, Netherlands Police, the Queensland Police, Ghanaian police and Nigerian Police เป็นต้น

4) การพัฒนาความร่วมมือระหว่างประเทศ

การพัฒนาความร่วมมือระหว่างประเทศในเชิงปราบปราม ถือว่ารัฐต่างๆ รวมทั้งประเทศไทยมีข้อด้อยจุดนี้ เนื่องจากว่าอาชญากรรมทางคอมพิวเตอร์มีลักษณะข้ามพรมแดน ข้อมูลต้องเร็ว แล้วความสัมพันธ์ระหว่างประเทศ เรื่องข้อมูล เรื่องการประสานงานของไทยยังเชื่องช้าอยู่ ตัวอย่างการขอข้อมูลผ่านความร่วมมือระหว่างประเทศทางอาญา (Mutual Legal Assistance Treaty - MLAT) นั้น ขอไปเป็นปีแล้วข้อมูลที่จะนำมาเป็นพยานหลักฐานได้ก็อาจจะหายไปแล้ว อันนี้ก็จะเป็นข้อด้อยของไทยอยู่ด้วย และถ้าหากเคยได้พยานหลักฐานมาในเชิงสืบสวนนั้น อาจจะเป็นความสัมพันธ์ส่วนบุคคล (connection) ที่ให้มา ซึ่งไม่มีความชัดเจนในเรื่องของกฎหมายรับรองจุดแม้จะมีเพื่อความรวดเร็ว หากมี connection ติดต่อจากผู้ให้บริการและหน่วยงานบังคับใช้กฎหมายในต่างประเทศหรือระหว่างประเทศได้เลยก็จะรวดเร็วแก้ปัญหาได้ ยิ่งถ้าเกิดมีการรับรองสถานะของพยานหลักฐานที่ได้มาด้วยช่องทางนี้ชัดเจนเข้าสำนวนได้จะยิ่งดี[175]

การเสริมศักยภาพในระดับประเทศเพื่อรองรับภัยคุกคามข้ามชาติ ต้องเป็นหน่วยงานที่เกี่ยวข้องกับกระบวนการยุติธรรมทั้งหมด มานั่งพูดคุยกัน เพราะเป็นคดีนอกราชอาณาจักร และเป็นเรื่องระหว่างประเทศ บุคคลากรที่เกี่ยวข้องในกระบวนการยุติธรรมและกระบวนการระหว่างประเทศ กระทรวงการต่างประเทศ ตำรวจเองมีหลายหน่วยที่จะต้องเข้ามา ตม. (สำนักงานตรวจคนเข้าเมือง)

[174] Research Excellence Framework 2014. (2014) “Confronting online dating scams: working with police and the industry.” 36 Communication Cultural and Media Studies. University of Leicester.

[175] เจ้าหน้าที่คดีพิเศษ, กองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ, (18 มกราคม 2562), สัมภาษณ์.

เวลาเข้ามาจะดูอย่างไรว่าใช่พวกนี้หรือไม่ หรือใช้ พาสปอร์ต (หนังสือเดินทาง) ปลอมตั้งแต่เข้าประเทศ ต้องติดตามเป็นบุคคลไป เป็นรายชื่อเฝ้าระวัง (Watch List) ตำรวจสากลต้องประสาน ปอท. ต้องดำเนินคดีหรือจับมาให้ได้ หรือถ้าไม่ได้ก็ต้องขอความร่วมมือ ให้เกิดสัมฤทธิ์ผลที่แท้จริง[176]

มาตรการทั้งหลายที่แสดงให้เห็นข้างต้นสะท้อนให้เห็นถึงเส้นทางที่ยาวไกลของการเดินสู่เป้าหมายการคุ้มครองสิทธิให้กับกลุ่มเสี่ยง และยังต้องเผชิญกับความท้าทายจากภัยที่มีลักษณะข้ามพรมแดนแต่รัฐทั้งหลายยังมีข้อจำกัดเรื่องเขตอำนาจศาล ความสลับซับซ้อนของกระบวนการยุติธรรม และประสิทธิภาพของการปฏิบัติหน้าที่ของเจ้าพนักงาน ดังนั้น แนวทางในการสร้างความเข้มแข็งให้กับกลุ่มเสี่ยงที่อาจตกเป็นเหยื่อจึงมีความสำคัญยิ่ง อันจะมีการแจกแจงในหัวข้อถัดไป

4.3 แนวทางเพิ่มความตระหนักให้ประชาชนกลุ่มเสี่ยงตกเป็นเป้าหมายพิศวาสอาชญากรรมให้รู้เท่าทันพิศวาสอาชญากรรม

จากผลการศึกษาในหัวข้อก่อนหน้านี้แสดงให้เห็นถึงความจำเป็นในการสร้างความตระหนักถึงภัยคุกคามไซเบอร์ในรูปแบบของพิศวาสอาชญากรรมแก่แก่ผู้บังคับใช้กฎหมาย ผู้ดูแลระบบ และประชาชนโดยเฉพาะกลุ่มเสี่ยงที่มีความรู้ความเข้าใจต่อเทคโนโลยีและการรับรู้ข้อมูลข่าวสาร โดยการรู้เท่าทันกลยุทธ์ของอาชญากรจัดเป็นประเด็นที่สำคัญเนื่องจากอาชญากรรมประเภทนี้มาในรูปแบบการล่อลวงโดยอำพรางและสร้างความผูกพันทางจิตใจโดยอาศัยการสื่อสารผ่านอินเตอร์เน็ต การแสดงให้เห็นถึงกลยุทธ์ที่อาชญากรแสดงออกมาหน้าฉากให้เหยื่อเห็นกับความจริงหลังฉากที่อาชญากรหลบซ่อนจะเป็นการล้างภาพลวงตาและสร้างความเข้มแข็งให้กับกลุ่มเสี่ยงที่จะตกเป็นเหยื่อ และในหลายกรณีอาชญากรได้อาศัยข้อมูลส่วนบุคคลที่เหยื่อเปิดเผยเองมาพลิกแพลงเป็นกลยุทธ์หลอกลวงให้ตรงใจเหยื่อมากขึ้น

4.3.1 กลุ่มเป้าหมาย

โดยกลุ่มเสี่ยงที่จะตกเป็นเป้าหมายและต้องเตือนภัยให้เฝ้าระวัง ก็คือ กลุ่มคนที่เข้าไปแสวงหาความรักความสัมพันธ์ในอินเตอร์เน็ตโดยมีการเปิดเผยข้อมูลส่วนตัวในพื้นที่สาธารณะ ซึ่งถือเป็นลักษณะการขาดความระมัดระวังตัว จำเป็นต้องมีการให้ข้อมูลเพื่อรู้เท่าทันกลวิธีของอาชญากรที่จะเข้ามาล่อลวงในลักษณะพิศวาสอาชญากรรมและความเสี่ยงรูปแบบต่างๆ ที่เกิดในโลกไซเบอร์ (Digital Literacy on Cyber Threats)

กลุ่มถัดมาที่ต้องรับรู้ข้อมูล ก็คือ เจ้าพนักงานของรัฐที่ทำหน้าที่บังคับใช้กฎหมายเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม อันประกอบไปด้วย เจ้าหน้าที่ตำรวจ เจ้าพนักงานคดีพิเศษ รวมไปถึงพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ ซึ่งมีอำนาจหน้าที่ได้การติดตามดำเนินคดีต่ออาชญากร และทำหน้าที่แจ้งเตือนผู้ดูแลระบบในกรณีมีพฤติกรรมที่เข้าข่ายการกระทำความผิดทางอาญาฐานหลอกลวง

[176] โฆษก บก.ปอท., กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.), (4 เมษายน 2562), สัมภาษณ์.

กลุ่มสุดท้ายที่มีความสำคัญมาก คือ ผู้ดูแลระบบคอมพิวเตอร์ ซึ่งมีความสามารถในการรวบรวมพยานหลักฐานในกรณีเกิดการกระทำความผิดตามนัยของกฎหมาย เนื่องจากมีหน้าที่ในการจัดเก็บข้อมูลไว้เพื่อใช้ในการดำเนินคดี 90 วันย้อนหลัง นอกจากนี้ยังเป็นผู้ดูแลระบบที่ควบคุมเนื้อหาและการจราจรอินเตอร์เน็ตสามารถนำข้อมูลอันเป็นเท็จ ปลอม บิดเบือน ออกจากระบบได้ อันเป็นแนวทางในการยุติการหลอกลวงทางอินเตอร์เน็ต

4.3.2 การเปิดเผย “หน้าฉาก” และ “หลังฉาก” ของอาชญากร

ข้อมูลที่จำเป็นต้องให้แก่กลุ่มเป้าหมายรู้เท่าทันและระวังภัยไปจนถึงการเตือนกลุ่มเสี่ยงให้ระมัดระวังหากพบเหตุการณ์สุ่มเสี่ยง ก็คือ “หน้าฉากคนดี” ที่ใช้อำพราง “หลังฉากอาชญากร”เพื่อก่ออาชญากรรมในลักษณะหลอกลวงทั้ง 5 ขั้นตอน

รูปภาพที่ล่อตาล่อใจ ถ้อยคำที่แสนหวาน คำสัญญาว่าจะรักมั่น อนาคตที่วาดฝันไว้ร่วมกัน กริยาท่าทางที่ตรึงใจอย่างที่ไม่เคยพบมาก่อนในโลกความเป็นจริง สิ่งเหล่านี้แสดงออกมาอย่างท่วมท้นในการสนทนาระหว่างผู้เสียหายกับนักต้มตุ๋น หน้าฉากที่แสนหวานเป็นดั่งฝันของหลายคนที่ต้องการหาใครสักคนในเครือข่ายสังคมออนไลน์มาเป็นคู่ชีวิต อันเป็น *หน้าฉาก* ที่ปิดบังตัวตน *หลังฉาก* ในทุกขั้นตอน ดังจะฉีกหน้ากากให้เห็นดังต่อไปนี้

1) ภาพถ่ายบนโปรไฟล์

หน้าฉาก ภาพโปรไฟล์ที่น่าดึงดูดใจไม่ว่าจะเป็นภาพของผู้หญิงหรือผู้ชาย อาจเป็นภาพเดี่ยว ภาพครอบครัว ภาพถ่ายคู่กับสัตว์ หรือภาพการทำกิจกรรมงานอดิเรกต่างๆ เป็นสิ่งแรกที่เชื้อเชิญให้ผู้ที่หาคู่ออนไลน์ส่วนใหญ่ให้ความสนใจ จากการเก็บรวบรวมข้อมูลทั้งการสัมภาษณ์ผู้เสียหายและข่าวในประเทศไทยพบว่าส่วนใหญ่ scammer อ้างว่าเป็นคนอเมริกัน หรือคนอังกฤษ ทั้งนี้เพราะผู้เสียหายส่วนใหญ่เป็นเพศหญิง อาจอธิบายได้จากค่านิยม “สามีฝรั่ง” ของไทย ทำให้แนวโน้มผู้เสียหายที่เป็นผู้หญิงถูกลอกโดยโปรไฟล์ “ฝรั่งผิวขาว หน้าตาดี ดูภูมิฐาน” ค่านิยมดังกล่าวเกิดขึ้นตั้งแต่ก่อนความรุ่งเรืองของเทคโนโลยีการสื่อสารบนโลกอินเตอร์เน็ตที่เชื่อว่า การมีสามีฝรั่งเป็นการยกระดับชีวิตให้ดีขึ้นทั้งทางเศรษฐกิจและสังคม[177] [178] [179] ประกอบกับสถิติของการใช้ภาพโปรไฟล์รูปแบบดังกล่าวในต่างประเทศเป็นไปในทิศทางเดียวกันว่า scammer จะแอบอ้างว่าเป็นคนอเมริกันมากถึง 63% รองลงมาคือ คนอังกฤษจำนวน 11% คนเยอรมนี 3% และคนแคนนาดาจำนวน 2%[180] อย่างไรก็ตามแม้จะพบผู้เสียหายที่เป็นเพศชายอยู่บ้างแต่กลับพบว่าชาติพันธ์มิใช่ประเด็นสำคัญ เห็นได้จากสถิติการแอบอ้างว่าเป็นคนประเทศใดนั้นไม่สามารถจับกลุ่มก้อนได้ชัดเจน อาจมีทั้งคนอเมริกัน ลูกครึ่งไทยไต้หวัน ลูกครึ่งไทยฟิลิปปินส์ เป็นต้น เพราะโปรไฟล์ที่ดึงดูดความสนใจผู้เสียหายชายมักจะเป็น “หญิง

---

[177] ปราโมทย์ ประสาทกุล, (2552), เขยฝรั่งในแดนอีสาน, *ประชากรและการพัฒนา สถาบันวิจัยประชากรและสังคม มหาวิทยาลัยมหิดล*, 29(3), 4-5.

[178] วันดี สันติวุฒิเมธี, (2560), *มองทะลุม่านมายาคติ “หญิงไทยกับสามีฝรั่ง” : เมื่อสิ่งที่เห็น อาจไม่ใช่สิ่งที่เป็น*, (4 เมษายน 2562), สืบค้นจาก https://www.the101.world/the-myth-of-thai-wife-and-her-foreign-husband/

[179] พิทักษ์ พงศ์กางการ, (2560), การแต่งงานข้ามวัฒนธรรมของผู้หญิงในชนบทอีสาน: กรณีศึกษาจังหวัดชัยภูมิ, *วารสารวิชาการ มหาวิทยาลัยกรุงเทพธนบุรี*, 6(2), 70-79.

[180] Edwards, M., Suarez-Tangil, G., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2018). The Geography of Online Dating Fraud. IEEE S&P 2018.

สาว รูปร่างหน้าตาดี มีเสน่ห์” และมักอ้างตัวว่าเป็นลูกครึ่ง ซึ่งผลที่ได้นี้สอดคล้องกับการศึกษาในต่างประเทศของ Monica T. Whitty[181] ที่พบว่า scammer จะเลือกภาพโปรไฟล์ผู้หญิงในลักษณะคล้ายนางแบบและน่าหลงใหล ดังนั้นสามารถอนุมานได้ว่า การเลือกใช้ภาพโปรไฟล์ในรูปแบบต่าง ๆ มีลักษณะร่วมกันทั่วทั้งโลก หลายการศึกษาให้เหตุผู้หญิงมักมองหาผู้ชายรวยมีสถานะทางสังคมสูง ส่วนผู้ชายมักมองหาผู้หญิงสวยมีเสน่ห์ [182] [183] [184] ดังนั้นโปรไฟล์ผู้หญิงปลอมส่วนใหญ่มักใช้การดึงดูดทางกายภาพ ที่มีลักษณะเป็นผู้หญิงที่ต้องการการอุปการะเลี้ยงดู ส่วนโปรไฟล์ผู้ชายปลอมมักจะเป็นคนรวย การศึกษาสูง มีหน้าที่การงานดี เป็นต้น

หลังฉาก การสร้างโปรไฟล์ปลอมอย่างละเอียดรอบคอบ โดยเริ่มตั้งแต่การขโมยรูปภาพใครสักคนหนึ่งที่มีลักษณะน่าดึงดูดใจจากเว็บไซต์ เครือข่ายสังคมออนไลน์ต่างๆ อันเป็นพื้นที่สาธารณะที่ใครต่อใครสามารถเข้าไปค้นหาและนำภาพถ่ายเหล่านั้นออกมาได้ ไม่ว่าจะเป็น Facebook, Instagram หรือเว็บเพจต่างๆ และเรียบเรียงคำโปรยเกี่ยวกับงานอดิเรก และสิ่งอื่นๆ ให้ดูน่าในสนใจในเชิงชู้สาว เป็นเพียงฉากหน้าของการหลอกลวงรัก ในประเทศไทยเองมีกรณีที่ผู้เสียหายเข้าแจ้งความกับผู้กำกับการกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีว่า ตนถูกนำข้อมูลส่วนตัวประกาศลงเว็บไซต์หาคู่ Thaiflirting.com โดยพบว่ามีการนำรูปภาพจาก Facebook ส่วนตัวของตนไปใช้เป็นภาพโปรไฟล์ และใช้ชื่อเป็นภาษาอังกฤษว่า “Pangtoleamak1” โดยบรรยายโปรไฟล์ว่า “แป้งนะคะ อายุ 27 ปี อาศัยอยู่ประเทศไทย นนทบุรี ปากเกร็ด สนใจผู้ชายอายุ 40-60 ปี ฉันชอบแต่งตัวเซ็กซี่ หวังว่าคงจะชอบนะคะ”[185]

ภาพที่ 25 ภาพโปรไฟล์ที่ถูกนำไปแอบอ้างในเว็บไซต์ Thaiflirting.com

[181] Whitty, M. T., (2015), Anatomy of the online dating romance scam. *Security Journal*, 28(4), 443-455.

[182] Buss, D. M. and Barnes, M., (1986), Preferences in human mate selection. *Journal of Personality and Social Psychology,* 50 (3): 559 – 570.

[183] Ellis, B. and Symons, D., (1990), Sex differences in sexual fantasy: An evolutionary psychological approach. *Journal of Sex Research*, 27 (4): 527 – 555.

[184] Townsend, J., (1993), Sexuality and partner selection: Sex differences among college students. *Ethology and Sociobiology*, 14 (5): 305 – 330.

[185] INNNews, (2018), *เตือนภัย!สาวถูกฉกข้อมูลลงประกาศเว็บไซต์หาคู่*, (20 พฤษภาคม 2562), สืบค้นจาก https://www.innnews.co.th/crime/news_211157/

ซึ่งเบื้องหลังความสวยงามเหล่านั้นเป็นกลุ่มอาชญากร โดยคนส่วนใหญ่มักจะคิดว่าผู้ล่อลวงมาจากประเทศไนจีเรียแต่หลายการศึกษาพบว่ายังมีกลุ่มอาชญากรอีกหลายประเทศที่ก่ออาชญากรรมนี้ ได้แก่ กานา มาเลเซีย รัสเซีย สหราชอาณาจักร และบางประเทศในทวีปยุโรป งานวิจัยของ Matthew Edwards และคณะ[186] ที่วิเคราะห์ IP address ที่แท้จริงของกลุ่ม scammer พบว่ามากกว่า 30% มาจากประเทศไนจีเรีย ซึ่งมองโดยรวมแล้วเกือบ 50% มาจากทางตะวันตกของแอฟริกา ตามมาด้วยประเทศมาเลเซีย และแอฟริกาใต้ สหราชอาณาจักร ตามภาพที่ 12

	Nation	Count	Proportion
1	Nigeria	488	0.302
2	Ghana	216	0.134
3	Malaysia	178	0.110
4	South Africa	140	0.087
5	United Kingdom	86	0.053
6	United States	57	0.035
7	Turkey	50	0.031
8	India	47	0.029
9	Togo	41	0.025
10	Senegal	40	0.025
11	Philippines	29	0.018
12	Ukraine	28	0.017
13	Russia	24	0.015
14	Ivory Coast	23	0.014
15	Kenya	22	0.014

ภาพที่ 26 จำนวนประเทศที่สามารถระบุตำแหน่งได้จากการวิเคราะห์ IP address ของอาชญากร

จากเก็บข้อมูลสัมภาษณ์ผู้บังคับใช้กฎหมายในประเทศไทยนั้น พบว่า ผู้เสียหายมักถูกหลอกโดยอาชญากรกลุ่มไนจีเรีย และกลุ่มมาเลเซีย ซึ่งมีเพียงบางส่วนเท่านั้นที่ทราบตัวผู้กระทำผิดนั้น เนื่องจากผู้เสียหายได้โอนเงินให้กับผู้รับจ้างเปิดบัญชีบังหน้าในประเทศไทยจึงมีการสืบสวนสอบสวนจนทราบถึงตัวผู้กระทำความผิด หรือบางครั้งเป็นคนไทยเองที่ก่ออาชญากรรมเช่นนี้ แต่ส่วนมากไม่สามารถสืบหาจนทราบตัวผู้กระทำความผิดได้เพราะฐานการกระทำความผิดอยู่ต่างประเทศ และติดปัญหาเรื่องการขอ IP address ระหว่างประเทศเพื่อยืนยันถิ่นที่อยู่ที่แท้จริงของโปรไฟล์ปลอมเหล่านั้น

2) การแนะนำตัวเอง อาชีพการงาน และสถานะทางสังคม

หน้าฉาก การมีอาชีพการงานที่มั่นคง และฐานะทางการเงินที่ดีย่อมเป็นที่ยอมรับของคนส่วนใหญ่ในสังคม ดังนั้นนอกจากภาพโปรไฟล์ที่ชวนหลงใหลแล้ว การนำเสนอภาพลักษณ์ที่ดีของเหล่า scammer ย่อมเป็นสิ่งที่ต้องกระทำเช่นกัน จากการศึกษาพบว่า อาชีพที่ถูกอ้างมากเป็นอันดับต้นๆ ในประเทศไทยคือ ทหารทั้งชายและหญิง และวิศวกร/นักธุรกิจเกี่ยวกับน้ำมันปิโตรเลียม[187] ตัวอย่างจากข่าวภายในประเทศ เช่น

[186] Edwards, M., Suarez-Tangil, G., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M., (2018), The Geography of Online Dating Fraud. IEEE S&P 2018.

[187] จากการสัมภาษณ์ผู้เสียหาย และ ข่าวภายในประเทศ

“หญิงชาวไทย อายุ 60 ปี ถูก scammer อ้างว่าเป็นทหารของสหรัฐอเมริกา อายุ 58 ปี โดยทั้งสองรู้จักกันผ่านแอปพลิเคชัน Hangouts ซึ่งครั้งแรกฝ่ายชายแอดเพื่อนมาทาง Facebook และได้พูดคุยกัน และต่อมาก็ขอเปลี่ยนเป็น Hangouts โดยให้เหตุผลว่าแอพฯนั้นมีความปลอดภัยมากกว่า”[188]

“เขาเป็นคนอังกฤษ อายุ 40 กว่าๆ มาทำธุรกิจน้ำมันที่มาเลเซีย มีลูกแต่ภรรยาเสียชีวิตแล้ว เข้ามาหลอกชวนให้ลงทุนธุรกิจน้ำมัน และพูดเชิงชู้สาว คุยกันได้ไม่นานเขาก็อ้างว่าเช่าบ้านอยู่ เดือดร้อนไม่มีค่าเช่าบ้าน เลยจะขอยืมเงินหลายหมื่นบาท แต่ครั้งแรกยังไม่ได้โอนเงินให้ ครั้งต่อมายืมเงิน 10,000 บาท ตนจึงยอมโอนเงินให้ และมีอีกหลายครั้ง...” – จากการสัมภาษณ์ผู้เสียหาย

ทั้งนี้ไม่เพียงแต่ในประเทศไทยเท่านั้นที่ scammer สวมบทบาทเป็นทหาร และวิศวกร ในต่างประเทศก็พบการอ้างอาชีพเหล่านี้เป็นอันดับต้นๆ เช่นกัน นอกจากนั้นยังมีอาชีพอื่นๆ เช่น แพทย์ นักธุรกิจ เจ้าหน้าที่บังคับใช้กฎหมาย เป็นต้น[189] *“I am an arc tech, in engineering department. I work with both government and private company as a building engineer, both internationally and locally. am from Scotland, I like in dunblane city.”* (ฉันเป็นอาจารย์ในคณะคณะวิศวกรรมศาสตร์ ฉันทำงานให้ทั้งภาครัฐและเอกชนในฐานะวิศวกรก่อสร้าง จากเมือง Dunblane ของสก็อตแลนด์) - ตัวอย่างการแนะนำตัวที่ผู้เสียหายคนหนึ่งได้รับ ด้วยลักษณะของอาชีพที่ดูมั่นคง น่าเชื่อถือ และมีรายได้สูงทำให้หลายคนมองว่า ไม่ใช่เรื่องแปลกที่คนเหล่านั้นจะมีฐานะทางการเงินที่ดี และมีทรัพย์สินมากมายตามที่อวดอ้าง อีกทั้งยังเชื่อว่า ตนจะไม่ถูกหลอกแน่นอน

[188] บุญชู พวงมาลา, (2562), หญิงวัย 60 ปีถูกชายต่างชาติอ้างเป็นทหารรักจริงหลอกโอนเงินสูญเงินเกือบล้านบาท, *77ข่าวเด็ด*, (20 พฤษภาคม 2562), สืบค้นจาก https://www.77kaoded.com/content/483682?fbclid=IwAR3L8Gt7QEh-V5wQmXlQt0ADlG4kKutemSVY4gANVOzwEnvmdfYiHB7nsy0

[189] Whitty, M. T., (2015), Anatomy of the online dating romance scam. *Security Journal*, 28(4), 443-455.

Nation (SOURCE IP)	N	Age		Gender		Occupation			Ethnicity			Marital Status		
		$\bar{x}$	z	$\bar{x}$	z	x	$\bar{x}$	z	x	$\bar{x}$	z	x	$\bar{x}$	
Nigeria	488	42.61	0.95	**0.73**	**4.13**	military	0.19	1.54	white	0.60	-1.38	single	0.47	-1.
Ghana	216	40.01	-2.81	**0.46**	**-5.34**	military	0.22	2.07	white	0.68	1.65	**single**	**0.63**	**3.**
Malaysia	178	**46.53**	**5.33**	**0.79**	**4.29**	**engineer**	**0.30**	**5.71**	white	0.60	-0.86	single	0.46	-1.
South Africa	140	**48.61**	**6.95**	**0.81**	**4.35**	engineer	0.22	2.15	**white**	**0.77**	**3.57**	**widow**	**0.57**	**7.**
UK	86	**46.15**	**3.38**	**0.93**	**5.64**	**military**	**0.33**	**4.09**	white	0.66	0.71	**divorce**	**0.33**	**5.**
USA	57	**47.33**	**3.56**	0.84	3.21	**engineer**	**0.34**	**3.71**	white	0.61	-0.20	widow	0.30	0.
Turkey	50	46.08	2.53	0.72	1.21	military	0.26	1.82	**white**	**0.86**	**3.48**	**widow**	**0.58**	**4.**
India	47	42.62	0.30	**1.00**	**5.17**	**business**	**0.32**	**8.14**	white	0.62	-0.14	single	0.53	0.
Togo	41	**39.44**	**-1.56**	**0.20**	**-5.89**	**military**	**0.37**	**3.52**	white	0.39	-3.20	single	0.68	2.
Senegal	40	**33.98**	**-4.67**	**0.10**	**-7.07**	**student**	**0.57**	**11.23**	**black**	**0.38**	**7.75**	**single**	**0.88**	**4.**
Philippines	29	**27.66**	**-7.07**	**0.03**	**-6.75**	**sales**	**0.50**	**14.85**	**mixed**	**0.48**	**7.81**	**single**	**0.97**	**5.**
Ukraine	28	**29.15**	**-6.11**	**0.07**	**-6.23**	**academic**	**0.22**	**9.82**	**white**	**1.00**	**4.24**	**single**	**0.89**	**4.**
Russia	24	**29.25**	**-5.72**	**0.08**	**-5.65**	**accounts**	**0.43**	**23.18**	**white**	**0.96**	**3.51**	single	0.79	2.
Ivory Coast	23	36.52	-2.44	**0.30**	**-3.32**	**student**	**0.30**	**3.86**	**black**	**0.48**	**8.02**	single	0.65	1.
Kenya	22	35.73	-2.72	0.45	-1.79	**self**	**0.32**	**3.28**	white	0.55	-0.82	single	0.64	1.
Italy	19	39.37	-1.09	0.89	2.33	**realty**	**0.63**	**23.74**	white	0.89	2.55	**single**	**0.89**	**3.**
SOURCE	*1666*	*42.13*	-	*0.64*	-	*military*	*0.17*	-	*white*	*0.63*	-	*single*	*0.50*	

ภาพที่ 27 แสดงถึงรายละเอียดที่ scammer มักใช้แนะนำตัวกับเหยื่อด้วยการวิเคราะห์จากโปรไฟล์จำนวน 1,666 โปรไฟล์ ด้วย Z-test ที่มีค่าความเชื่อมั่นที่ 0.05[190]

จากภาพที่ 27 แสดงให้เห็นว่าค่าเฉลี่ยของอายุที่ scammer มักบอกกับเหยื่อคือประมาณ 42 ปี ส่วนใหญ่มีอาชีพทหาร ผิวขาว และโสด ซึ่งสอดคล้องกับโปรไฟล์ส่วนใหญ่ที่ผู้เสียหายในไทยถูกหลอก และสอดคล้องกับข้อมูลที่ว่า scammer ที่มาหลอกคนในประเทศไทยส่วนใหญ่เป็นกลุ่มไนจีเรีย และมาเลเซีย ซึ่งจากภาพจะเห็นว่า scammer กลุ่มไนจีเรียมักอ้างว่าเป็นทหาร ผิวขาว และกลุ่มมาเลเซียมักอ้างว่าเป็นวิศวกร ผิวขาว ดังนั้นจึงการหลอกลวงรักที่เกิดในประเทศไทยจึงมีโปรไฟล์ที่ไม่ต่างไปจากกันมากนัก

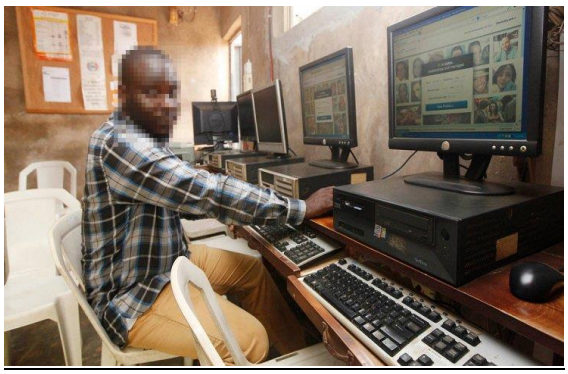
หลังฉาก ภาพที่คุณเห็นอาจไม่ใช่สิ่งที่เป็น ฉากหลังของเหล่านักต้มตุ๋นที่ทำงานกันอย่างแข็งขันจนสามารถกล่าวได้ว่า การหลอกลวงรักเป็นอาชีพหนึ่งในไนจีเรียที่ทำเงินได้อย่างมหาศาล[191] ผู้ที่จะเข้าสู่วงการนี้ต้องมีทักษะพื้นฐานทั่วไปคือ ทักษะทางคอมพิวเตอร์และการติดต่อสื่อสารบนโลกออนไลน์ นักหลอกลวงรักไม่จำเป็นต้องมีความสามารถในการ hack ข้อมูล ต้องการเพียงแค่ความสามารถในการสร้างโปรไฟล์ปลอมบนเว็บไซต์ หาคู่ และทักษะทางสังคมที่ใช้ในการคุยกับเหยื่อให้ราบรื่นเพื่อสร้างความมั่นใจ และความเชื่อใจให้แก่เหยื่อ นักต้มตุ๋นหลายคนทำงานในร้านอินเตอร์เน็ตเวลา 22.30 – 07.00 น. และถ้าเป็นกลุ่มใหญ่จะมีที่ทำงานเป็นองค์กรของตนเอง โดยจะแบ่งหน้าที่กันหลายกลุ่ม เช่น บางกลุ่มทำหน้าที่ส่งข้อความหลอกลวงไปทาง e-mail ประมาณ 500 ฉบับต่อวัน ส่วนกลุ่มอื่นทำหน้าที่สร้างโปรไฟล์ปลอม โดยใช้ภาพจากเว็บไซต์ โมเดลลิ่ง และบางกลุ่มทำหน้าที่สร้างข้อความโรแมนติกต่างๆ ไว้ใช้สำหรับการหลอกลวง หนึ่งในสมาชิกเครือข่ายไนจีเรียกล่าวว่า *“หากคุณตอบกลับ มีโอกาสมากถึง 70% ที่คุณจะเสียเงิน”*[192] อาชญากรกลุ่มนี้มีรายได้จากการฉ้อโกงด้วยความรักมากถึง 45 ล้าน

[190] Edwards, M., Suarez-Tangil, G., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M., (2018), The Geography of Online Dating Fraud. IEEE S&P 2018.

[191] Rege, A, (2009), What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. *International Journal of Cyber Criminology*, 3(2).

[192] Dixon, R., (2005), Nigerian Cyber Scammers. Retrieved April 5, 2009, from http://www.latimes.com/technology/la-fgscammers20oct20,0,301315.story?page=1&coll=la-tot-promo

ดอลลาร์ต่อปี[193] Patrick Giblin ถูกกล่าวหาในปี 2005 ว่าฉ้อโกงผู้หญิงเกือบ 130 คน เว็บไซต์หาคู่ เช่น Quest Personals, Lavalife, Intimate Connections, และ Private Lines เป็นต้น ได้เงินไปจำนวนทั้งสิ้น 320,241 ดอลลาร์สหรัฐ Giblin อ้างว่าตนเป็นเจ้าหน้าที่บังคับใช้กฎหมาย อีกทั้งพ่อและพี่ชายทำงานในกระทรวงยุติธรรมทางอาญา หลังจากการเริ่มต้นพูดคุยกับเหยื่อทางโทรศัพท์ลายๆ วันหรือหลายสัปดาห์ โดยให้คำสัญญาว่าสร้างความสัมพันธ์ที่มั่นคงและดึงเหยื่อออกจากความเหงาที่มีอยู่ จากนั้นจะเริ่มขอเงินเหยื่อด้วยเหตุผลที่ต่างกันออกไปโดยให้เหยื่อโอนเงินผ่าน Western Union[194]



ภาพที่ 28 ฉากหลังของเหล่าทหารและนักวิศวกร ผิวขาวที่หลายคนตกหลุมรัก

Eintan เคยเป็นหนึ่งในสมาชิกนักต้มตุ๋นกลุ่มที่เรียกว่า **Yahoo boys** เขาออกจากวงการ romance scam ตั้งแต่ปี 2008 และเล่าว่า เขาอาศัยอยู่ในหมู่บ้านเล็กๆ นอกเมือง Lagos ของไนจีเรีย และกำลังตั้งใจจะไปหางานทำในโรงไฟฟ้าของประเทศที่เศรษฐกิจกำลังเติบโตและมีประชากรมากที่สุดในแอฟริกา แต่เขาได้พบกับ “the game” ที่เป็นระบบเศรษฐกิจใต้ดิน (shadow economy) ของไนจีเรีย หรือที่ถูกเรียกว่า “419 scams” Eintan ทำอาชีพต้มตุ๋นตั้งแต่ปี 2004 ตอนนั้นอายุ 18 ปี ใช้เวลาประมาณ 4 ปี ได้เงินมากกว่า 800,000 ดอลลาร์สหรัฐ จากเหยื่อทั้งหญิงและชายจำนวน 20 คน *“เมื่อคุณออกจากเกมส์นี้ (the game) คุณจะถูกมองว่าเป็นคนทรยศทันที และคุณคือศัตรูของคนที่ยังทำงานอยู่ในนั้น”* เขาเรียนรู้เทคนิคและวิธีการหลอกลวงต่างๆ จากรุ่นพี่ และเขาเองก็ถ่ายทอดทักษะและเทคนิคต่างๆ สู่รุ่นน้องที่เข้ามาทีหลัง[195]

[193] DeBrosse, J., (2008), ID theft victim becomes pawn in dating scam. Retrieved April 4, 2009 from http://www.daytondailynews.com/n/content/oh/story/news/local/2008/04/06/ddn040608scammers.html

[194] USDOJ (United States Department of Justice), (2005), United States of America v. Patrick M. Giblin. Retrieved April 4, 2009, from http://www.usdoj.gov/usao/nj/press/files/pdffiles/SuperIndict.pdf

[195] Shadel, D. and Dudley, D., AARP The Magazine, “'Are You Real?' — Inside an Online Dating Scam”, from https://www.aarp.org/money/scams-fraud/info-2015/online-dating-scam.html

ในงานศึกษาของ Aunshul Rege[196] พบว่า ในองค์กร romance scam อาชญากรหลายคนมักทำงานร่วมกันเพื่อสร้างองค์กรให้มั่งคั่ง และส่วนใหญ่จะแบ่งปันข้อมูล เทคนิควิธีที่ดีสุดของการหลอกลวงให้แก่กันและกัน องค์กรอาชญากรรมนี้แบ่งได้เป็น 3 กลุ่ม คือ ทำงานคนเดียว กลุ่มเล็ก (กลุ่มที่ทำงานคนเดียว และกลุ่มเล็กมักจะเป็นคนที่มีทักษะหลายด้าน ไม่ว่าจะเป็นการพิมพ์ภาษาอังกฤษ และการแฮค) และเครือข่ายใหญ่ กลุ่มที่ทำงานเป็นเครือข่ายจะไม่เคร่งครัดเรื่องคุณสมบัติสมาชิกกลุ่ม เช่นกลุ่มไนจีเรีย (Nigerian network) และ Lazarev group องค์กรเหล่านี้จะจ้างคนที่ต้องการเป็นสมาชิก โดยไม่คำนึงถึงจำนวนของสมาชิก และมีเป้าหมายเพียงอย่างเดียวคือ scammer ทุกคนต้องทำเงินได้ นอกจากนั้น scammer ไม่จำเป็นต้องแสดงทรัพย์สินใดๆ ต่อองค์กร ทำให้ scammer ส่วนใหญ่ออกจากวงการไปเมื่อได้บรรลุเป้าหมายทางการเงินแล้ว ส่วนสำคัญของเครือข่ายอาชญากรรมมีดังนี้ ***organizer*** ทำหน้าที่กำหนดขอบเขตของกิจกรรม ***extender*** มีหน้าที่ขยายเครือข่าย เป็นผู้รับสมาชิกใหม่ๆ และทำความร่วมมือกับกลุ่มธุรกิจผิดกฎหมาย รัฐบาล และหน่วยงานยุติธรรม ***executor*** เป็นผู้บริหารที่คอยทำหน้าที่รับผิดชอบงานหลายอย่างให้เป็นไปตามเป้าหมายที่วางไว้ หน้าที่นี้ต้องมีความสามารถหลายด้าน เช่น สื่อสารภาษาต่างประเทศได้ เขียน e-mail ได้ คุยโทรศัพท์กับเหยื่อได้ เป็นต้น ***enforce*** เป็นผู้ปกป้องเครือข่ายอาชญากรรม และใช้เครื่องมือที่จำเป็นเพื่อทำให้มั่นใจว่าเหยื่อจะยอมทำตาม เมื่อเหยื่อไม่เต็มใจที่จะส่งเงินมาให้ บ่อยครั้งที่ scammer จะใช้ประโยคเหล่านี้กับเหยื่อ *“you don’t have any feelings for me”* หรือ *“I thought we had a real relationship here”* หรือ *“you’re heartless”* เพื่อล่อให้เหยื่อกลับมาในวังวงของการหลอกลวงอีกครั้ง และในบางครั้งที่ scammer ใช้เว็บแคม (webcam) เพื่อติดต่อสื่อสารกับเหยื่อ พวกเขาจะบันทึกวิดีโอเหล่านั้นไว้เพื่อในข่มขู่เหยื่อให้ส่งเงินไม่เช่นนั้นจะนำภาพและวิดีโอทั้งหลายเผยแพร่ลงเว็บโป๊ อีกตำแหน่งหนึ่งคือ ***money mover*** เป็นผู้ที่รับเงินจากเหยื่อ และส่งเงินกลับไปยังองค์กรอาชญากรรมของตน ซึ่งส่วนมากส่งเงินผ่าน Western Union และสุดท้ายคือ ***crossovers*** ทำหน้าที่เชื่อมโยงเครือข่ายทั้งหมด คนเหล่านี้จะเป็นสมาชิกของหน่วยงานรัฐที่ถูกกฎหมาย หน่วยงานทางการเงิน หรือภาคธุรกิจถูกกฎหมาย เป็นผู้ที่จัดทำเอกสารต่างๆ ให้มีความน่าเชื่อถือโดยเป็นเอกสารที่มีหัวราชการ มีแสตมป์ หรือตราประทับราชการ เพื่อทำให้เหยื่อมั่นใจว่าสิ่งที่ scammer แอบอ้างนั้นเป็นความจริง สิ่งเหล่านี้ถือเป็นภาพกว้างๆ ที่ทำให้มองเห็นเบื้องหลังการทำงานของพวกเหล่านักหลอกลวงรัก

3) การสร้างความเชื่อมั่น และความไว้เนื้อเชื่อใจ

หน้าฉาก ข้อความแสนหวานชวนฝันของเหล่านักหลอกลวงที่ส่งให้แก่เหยื่อในทุกๆ วัน ความเอาใจใส่อย่างสม่ำเสมอ “Good night” ในทุกคืน “Good morning” ทุกยามเช้า คำเรียกที่อ่อนโยน “Sweetheart, honey, my love, baby” สิ่งเหล่านี้ล้วนชวนฝันสำหรับผู้ที่กำลังเหงา และมองหาคนรักดีๆ ในอุดมคติบนโลกออนไลน์ ข้อความที่ผู้เสียหายได้รับมักเป็นข้อความเชิงชู้สาวที่พร่ำแต่บอกรักและสัญญารักว่าจะมั่นคงกับคุณคนเดียว หลายครั้งที่สร้างฝันว่าจะมาใช้ชีวิตบั้นปลายร่วมกัน หรือต้องการทำธุรกิจร่วมกันที่ประเทศไทย ประกอบผู้เสียหายส่วนใหญ่เป็นผู้ที่ผิดหวังจากความรักในชีวิตจริงมาก่อน หรือคู่รักเสียชีวิตแล้ว นั่นจึงเป็นปัจจัยที่ทำให้ถ้อยคำเหล่านี้มีคุณค่ามากสำหรับพวกเขา

[196] Rege, A., (2009), What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. *International Journal of Cyber Criminology*, *3*(2).

การสร้างความสัมพันธ์ดังกล่าวจะมีระยะเวลามากน้อยต่างกันไปตั้งแต่ 10 วัน บางคนใช้เวลา 3 สัปดาห์ และบางคนใช้เวลานานถึง 8 เดือนจึงจะสำเร็จ ผู้เสียหายต่างกล่าวเป็นเสียงเดียวกันว่า คนๆ นั้นที่อยู่ในโลกออนไลน์แสดงความรักต่อพวกเขาอย่างที่ไม่เคยได้รับมาก่อน และดูจะเข้าใจพวกเขาไปหมดเสียทุกเรื่อง ความสัมพันธ์นี้มันดูลึกซึ้งและรวดเร็วมาก การสร้างความสัมพันธ์รักเป็นเพียงฉากหนึ่งในขบวนการทั้งหมด และแบบแผนประทุษกรรมเหล่านี้เกิดขึ้นเช่นเดียวกันในต่างประเทศ

> *"He sent me a love poem every morning and we were on chat (IM) for hours every night and he called in the morning to say good morning and every night to tell me he loved me and would never let me go."* (เขาส่งกลอนรักหาฉันทุกเช้า และเราแชทคุยกันทุกคืน และโทรหาฉันทุกเช้าเพื่อทักทายในตอนเช้า และบอกรักก่อนนอน) เรื่องเล่าจากผู้เสียหายคนหนึ่งในต่างประเทศ[197]

> *"I do think about you all the time, after reading your email again and again (...) you mean so much to me and my family too."*[198] (ฉันคิดถึงแต่เรื่องของคุณตลอดเวลา ฉันอ่าน e-mail ของคุณซ้ำไปซ้ำมาอย่างไม่เบื่อ....นั่นหมายความว่าคุณมีความหมายกับฉันเหลือเกินเสมือนเป็นส่วนหนึ่งครอบครัวของฉัน)

นอกจากความสัมพันธ์ที่ดูหวานซึ้งแล้ว สิ่งที่ทำให้เหยื่อเชื่อมั่น และวางใจในตัวของคู่สนทนาว่าคนนั้นจะไม่หลอกลวงคือ การที่คู่สนทนาได้ส่งภาพถ่ายหลักฐานต่างๆ เพื่อยืนยันในสิ่งที่พวกเขากำลังเล่าอยู่ เช่น ส่งภาพกิจกรรมระหว่างวัน หลักฐานทางอาชีพ หรือสิ่งที่สามารถบงชี้ได้ว่าพวกเขามีทรัพย์สินสมฐานะที่ได้อ้างไว้ ดังภาพที่ 29-32

[197] Whitty, M. T., (2015), Anatomy of the online dating romance scam. Security Journal, 28(4), 443-455.

[198] Tan, H. K., & David, Y., (2017), Preying on lonely hearts: A systematic deconstruction of an Internet romance scammer's online lover persona. Journal of Modern Languages, 23(1), 28-40.

ภาพที่ 29 คู่สนทนาส่งให้เหยื่อที่เป็นคนไทย เพื่อยันตัวตนว่าเธอเป็นทหารสหรัฐ

ภาพที่ 30 คู่สนทนาส่งเหยื่อ ขณะที่กำลังบอกเหยื่อว่าวันนี้มาออกกำลังกายที่ฟิตเนส

ภาพที่ 31 คู่สนทนาส่งให้เหยื่อ เพื่อยันตัวตนว่าเขาเป็นวิศวกรปิโตรเลียม

ภาพที่ 32 แสดงถึงฐานะทางการเงินที่ดี

ภาพถ่ายต่างๆ ประกอบบทสนทนาที่ถูกสร้างขึ้นอย่างรอบคอบทำให้หลายคนเชื่อสิ่งที่ตนเองรับรู้นั้นเป็นความจริง ซึ่งหากผู้ที่ไม่ได้มีความรู้ความเชี่ยวชาญก็ไม่อาจสามารถทราบได้ว่าภาพนั้นถูกตัดต่อ หรือภาพเหล่านั้นเป็นสามารถหาได้ทั่วไปบนโลกอินเตอร์เน็ต ผู้เสียหายบางคนได้รับสิ่งของจาก scammer เช่น ตุ๊กตา ดอกไม้ ส่งมายังหน้าบ้านของเหยื่อ ผู้หญิงอีกคนหนึ่งได้รับช่อดอกไม้ที่หน้าบ้านของเธอโดยหน้าการ์ดเขียนว่า ‘My life will never be the same since I met you. Happy New Year. Love, Dwayne’ บางครั้งอาจมีการแลกเบอร์โทรศัพท์ หรือติดต่อสื่อสารกันด้วยวิธีอื่นที่นอกเหนือจากการส่งข้อความ ยิ่งทำให้เหยื่อเชื่อว่าคนคู่สนทนาเหล่านั้นมีตัวตนอยู่จริง

> “เขาโทรมาจากมาเลเซีย และเริ่มคุยกันทุกวันทั้งตอนเช้าและก่อนนอน....*น้ำเสียงของเขาช่างสะกดใจฉันเหลือเกิน*....Amy กล่าว ทั้งคู่เริ่มพูดถึงความสัมพันธ์ในอนาคตที่วาดฝันไว้ร่วมกัน”- หญิงอเมริกาอายุ 57 ปี[199]

ไม่ว่าจะเป็นคนชาติไหนๆ ก็สามารถตกหลุมรักจากความรักที่หอมหวานนี้ได้อย่างมิอาจหาเหตุผลใดใดมาบรรยายได้

หลังฉาก การวางแผนและการทำงานอย่างมีขั้นตอนของกลุ่มอาชญากรเหล่านี้ทำให้สร้างหน้าฉากได้อย่างแนบเนียน ด้วยการส่งความเป็นกิจวัตร การรอคอย และการสร้างความไว้วางใจเป็นหน้าที่หลักของเหล่า scammer เป็นที่ทราบกันดีในบรรดานักต้มตุ๋นว่า พวกเขาต้องมีความอดทนในการหลอกล่อเหยื่อ โดยจะต้องแบ่งเวลา และยอมสละเวลาไม่ว่าจะต้องใช้เวลานานเพียงใด จะต้องหว่านคำ

[199] Shadel, D. and Dudley, D., AARP The Magazine, “'Are You Real?' — Inside an Online Dating Scam”, from https://www.aarp.org/money/scams-fraud/info-2015/online-dating-scam.html

หวานมากแค่ไหนเพื่อทำให้เหยื่อไว้วางใจ และเชื่อว่ามีทรัพย์สินอยู่จริง บางครั้งต้องใช้เวลา 6-8 เดือน เพื่อทำให้ขั้นตอนนี้สำเร็จ scammer มักสร้างความสัมพันธ์แบบซาบซึ้ง (hyperpersonal relationships) ที่ทำให้เหยื่อรู้สึกว่าไม่เคยได้พบสิ่งนี้โลกความเป็นจริง เช่น ชอบอะไรเหมือนกัน คิดอะไรเหมือนกัน ทั้งนี้เพราะเป็นการสื่อสารกันแบบออนไลน์ที่ scammer สามารถสร้างภาพลวงตาเพื่อให้เหยื่อตกหลุมรักได้อย่างเต็มที่ไม่เหมือนการสื่อสารกันต่อหน้าในโลกความเป็นจริง โดยทั่วไปจะใช้เวลาคุยกันอย่างน้อยๆ 1 อาทิตย์ และส่วนมากจะทำเป็นกิจวัตร เช่น ทุกๆ เช้า/เย็น เพื่อทำให้ความสัมพันธ์ดูน่าเชื่อถือ และทำให้รู้สึกว่าไม่อยากให้ความสัมพันธ์นี้หายไปไหน และสิ่งสำคัญเหล่า scammer ทำคือการเรียนรู้โปรไฟล์ของเหยื่อจากสิ่งที่เหยื่อโพสต์ลงไปในเครือข่ายสังคมออนไลน์ เหยื่อหลายคนมักสงสัยว่าทำไมคู่สนทนารู้ใจหมดทุกเรื่อง ทั้งนี้เพราะเรื่องราวต่างๆ ไม่ว่าจะเป็นภาพถ่ายและการโพสต์ข้อความ หรือการแชร์สิ่งที่ตนเองสนใจ สิ่งเหล่านี้ล้วนเป็นประโยชน์แก่กลุ่ม scammer ที่จะใช้เป็นเครื่องมือในการคาดเดาความต้องการ และความเป็นไปของเหยื่อ ซึ่งเป็นจุดสำคัญที่ทำให้พวกเขาเข้าใจเหยื่อได้อย่างไม่ยุ่งยาก ผู้เสียหายหนึ่งเล่าว่า *"ภรรยาของเขาเสียชีวิตด้วยโรคมะเร็ง เหมือนกับที่สามีของฉันเสียชีวิตด้วยโรคมะเร็ง เหมือนกับเรามีอะไรหลายอย่างตรงกัน เข้าใจกันได้ง่ายในทุกๆ เรื่อง"* ทั้งนี้ เนื่องจากข้อความอาลัยรักที่เธอได้โพสต์ถึงสามีที่เสียชีวิตไปแล้วด้วยโรคมะเร็งบน Facebook ของเธอ ทำให้ scammer ได้ใช้เป็นประโยชน์จากจุดอ่อนทางอารมณ์ความรู้สึกนั้นมาสานสัมพันธ์รักของพวกเขาทั้งคู่ ทั้งนี้ การทำงานเป็นกลุ่มของนักหลอกลวงรักที่มีการแบ่งปันข้อมูลให้เพื่อนร่วมงาน และมีการสอนเทคนิคการพูดคุยให้ผู้ที่เข้ามาทำงานใหม่เหมือนที่อดีต scammer เล่าว่า "เขาเรียนรู้เทคนิคและวิธีการหลอกลวงต่างๆ จากรุ่นพี่ และเขาเองก็ถ่ายทอดทักษะ และเทคนิคต่างๆ สู่รุ่นน้องที่เข้ามาทีหลัง"[200]

คำบอกเล่าของ scammer ประกอบกับตัวอย่างบทสนทนาที่ผู้วิจัยได้เก็บรวบรวมการจากการสัมภาษณ์แอดมินเพจภัยผู้หญิงออนไลน์[201] มีความสอดคล้องกันกับการศึกษาของประเทศอังกฤษที่พบว่า ข้อความที่ scammer ส่งมีการใช้ซ้ำ (copy/paste) หรือปรับข้อความเพียงเล็กน้อยในการนำเสนอตัวตนของแต่ละโปรไฟล์ ทีมวิจัยสามารถตรวจสอบได้ว่า มีข้อความเช่นเดียวกันอยู่ในโปรไฟล์ต่างกัน ซึ่งการทำความเข้าใจแหล่งที่มาของข้อความที่เหมือนกันจะช่วยในการระบุถึงกลุ่มอาชญากรได้จากข้อสันนิษฐานที่ว่า กลุ่มอาชญากรเดียวกันจะแบ่งปันข้อความซึ่งกันและกัน ซึ่งเป็นเรื่องปกติของวงการ scammer ผลการศึกษาคือ จากการจับคู่ข้อความที่เหมือนกันมากกว่า 10 คำขึ้นไป จำนวน 899 โปรไฟล์ที่ไม่ซ้ำกัน พบว่ามี 241 โปรไฟล์ (11%) ที่มีการใช้คำซ้ำกันและสืบถึงที่มาของต้นทางได้อย่างชัดเจน[202] สิ่งสำคัญของการสานสัมพันธ์มิใช่เพียงเพื่อแสดงความรัก แต่เพื่อแสดงฐานะทางการเงินให้เหยื่อเชื่อว่า คู่สนทนาที่เหยื่อตกหลุมรักนั้นมีทรัพย์สินมากมาย ไม่ใช่นักต้มตุ๋นที่จะมาหาผลประโยชน์จากเหยื่อ และอีกนัยหนึ่งเป็นการล่อใจเหยื่อเช่นกัน ซึ่งพื้นฐานเหล่านี้ไม่ว่าจะเป็นการเลือกใช้โปรไฟล์และการแอบอ้างตัวต่างๆ รวมถึงการสร้างความเชื่อมั่นให้เหยื่อไว้วางใจ และจงรักภักดีต่อ scammer โดยทำให้เหยื่อคิดว่า 'ความฝันของฉันคือความฝันของคุณ เป้าหมายของฉันคือเป้าหมายของคุณ

[200] เรื่องเดียวกัน

[201] ผู้ดูแลเพจ, เพจภัยผู้หญิง ในโลกออนไลน์, (17 มกราคม 2562), สัมภาษณ์.

[202] Edwards, M., Suarez-Tangil, G., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M., (2018), The Geography of Online Dating Fraud. IEEE S&P 2018.

ผลประโยชน์ทางการเงินของฉันคือผลประโยชน์ทางการเงินของคุณ' สิ่งเหล่านี้เป็นสิ่งสำคัญเพราะจะไม่สามารถขอเงินจากเหยื่อได้สำเร็จหากไม่ปฏิบัติขั้นตอนเบื้องต้นอย่างรอบคอบ

4) การสร้างสถานการณ์ต่างๆ เพื่อหลอกเอาทรัพย์สิน

หน้าฉาก จากความสัมพันธ์ที่หอมหวานเริ่มเข้าสู่ช่วงทดสอบความรัก 108 เรื่องราวและเหตุผลที่เหยื่อได้รับจากคู่สนทนนาเพื่อขอให้เหยื่อโอนเงินให้ เหยื่อหลายคนมักคิดว่าเงินจะเป็นตัวช่วยแก้ปัญหาของคู่สนทนาเพื่อให้ทั้งคู่ได้พบกันเร็วขึ้น และบางคนคิดว่าการได้รับทรัพย์สินจากคู่สนทนาเป็นเครื่องพิสูจน์ว่าคู่สนทนาจะมาใช้ชีวิตร่วมกันที่ประเทศของตน จากการศึกษาพบว่าสถานการณ์ที่ถูกใช้อยู่บ่อยครั้งมีดังนี้

- มีปัญหาทางการเงินอย่างเร่งด่วน และต้องการขอความช่วยเหลือทางการเงิน เช่น จ่ายค่ารักษาพยาบาลของตนเองหรือสมาชิกครอบครัว (พ่อ แม่ บุตร พี่น้อง) ค่าเล่าเรียน ธุรกิจถูกโกง ธุรกิจมีปัญหาต้องใช้เงินด่วน เกิดอุบัติเหตุ ลูกป่วยหนัก ขอเงินซื้อตั๋วเครื่องบิน/ทำวีซ่าเพื่อเดินทางมาพบเหยื่อ ค่าเช่าห้อง เป็นต้น และจะคืนเงินให้กับเหยื่อภายใน 2-3 วัน
- ชวนให้โอนเงินร่วมลงทุนสร้างธุรกิจ เพื่อเก็บเงินมาใช้ชีวิตร่วมกันในบั้นปลาย ตามเรื่องราวที่เกิดขึ้นจริงดังนี้
- ได้รับมรดกจากพ่อแม่ และพร้อมที่จะย้ายมาอยู่ในประเทศของเหยื่อ หรือเป็นทหารที่ได้รับเงินจำนวนมากจากการยึดทรัพย์สินของศัตรู จึงต้องการส่งสิ่งของ หรือทรัพย์สินต่างๆ มาให้เหยื่อ แต่ติดปัญหาที่กรมศุลกากร สนามบิน หรือสถานีตำรวจ เหยื่อต้องโอนเงินค่าธรรมเนียมก่อนจึงจะได้รับทรัพย์สินเหล่านั้น
- กำลังเดินทางมาหาเหยื่อ แต่เกิดปัญหาระหว่างการเดินทางทาง เช่น กระเป๋าที่บรรจุเงิน/ทรัพย์สินมาจำนวนมากถูกยึด กระเป๋าเงินหาย ถูกกักตัวอยู่ที่สนามบิน บัตรเครดิตใช้การไม่ได้ เป็นต้น
- ขอแต่งงาน โดยจะส่งเงินจำนวนหลายล้านดอลลาร์เป็นของหมั้น หรือให้นำเงินนั้นซื้อที่ สร้างบ้านก่อนที่จะเดินทางมาแต่งงานจริงในประเทศของเหยื่อ จากนั้นจะมีคนโทรมาหาเหยื่อ (อ้างว่าเป็นเจ้าหน้าที่ศุลกากร/นักการทูต หรือเจ้าหน้าที่ของรัฐที่เกี่ยวข้อง) โดยจะร้องขอให้เหยื่อจ่ายค่าธรรมเนียมในการรับเงินนั้น

ในบางกรณี เหยื่อตระหนักได้ว่าตนถูกหลอก แต่ยังคงหวนกลับไปเป็นเหยื่ออีกครั้งด้วยคารมที่แสนหวาน และเหตุผลอีกมากมายที่ที่จูงใจให้เหยื่อขาดการตระหนักนั้นไป เมื่อเหยื่อถามถึงความเป็นจริงว่าคู่สนทนาเป็น scammer หรือไม่ หรือเริ่มมีบทสนทนาในทิศทางที่ตั้งคำถามว่าคู่สนทนามาเพื่อหลอกลวงเหยื่อหรือไม่ พวกเหยื่อจะได้รับข้อความตอบกลับที่เป็นแพทเทินคล้ายๆ กันว่า "คุณรู้ดีว่าฉันเป็นยังไง" ตัวอย่างที่เหยื่อตั้งคำถามกับคู่สนทนาว่า *"How do I know you're not a Nigerian scammer?"* (ฉันจะมั่นใจได้ยังไงว่าคุณไม่ใช่นักต้มตุ๋นชาวไนจีเนีย?) scammer หัวเราะและตอบ

กลับมาว่า *"Oh, Amy. You know me better than that."* (โอ้, เอมมี่ คุณรู้จักฉันดีกว่านั้น)[203] หรือได้รับข้อความเชิงชู้สาวที่แสดงความรักมากล้นเกินพรรณนาด้วยวิธีการต่างๆ เช่น การส่งเพลง *"Baby I Know, I really want to meet you too. But you have to accept me first before we plan how to me. I will not visit someone that is not my love, someone I'm not dating. But if we are in love I will plan my trip to visit you in Thailand.....I love this song, it's for you.... พร้อมส่งเพลงเกี่ยวกับความรักมาให้"*[204]

หลังฉาก เครือข่าย romance scam เป็นหนึ่งในกลุ่มเครือข่ายหลอกลวงอื่นๆ บางคนเป็นสมาชิกของกลุ่มหลอกลวงอื่นด้วย พวกเขาแบ่งปันข้อมูลต่างๆ ซึ่งกันและกัน แบ่งปันอินเตอร์เน็ต และฝึกฝนนักต้มตุ๋นหน้าใหม่อยู่อย่างต่อเนื่องบางคนอายุเพียงแค่ 6 ขวบเท่านั้น ดังนั้นแรงจูงใจใน 'การทำยอด' หรือ'การปั่นยอด' ของ เหล่า scammer ในองค์กรอาชญากรรมนี้คือ การได้รับของสวัสดิการต่างๆ ในการทำงาน และการเลื่อนขั้น ดังนั้นยิ่งได้รับเงินจากเหยื่อมากเท่าใด ยิ่งส่งผลให้สวัสดิการที่ดีมีมากขึ้นเท่านั้น เป้าหมายโดยทั่วไปของ scammer คือต้องได้รับเงินโอนจากเหยื่ออย่างน้อย 2-3 ครั้งต่อสัปดาห์ และแต่ละเดือนต้องได้เงิน 1,000 ดอลลาร์ และหากผู้ใดทำเงินได้มากกว่าเดือนละ 30,000 ดอลลาร์ จะได้รับของสวัสดิการเช่น เสื้อผ้าใหม่ ห้องพักในโรงแรม และดื่มไวน์สุดหรูใน "VVIP" คลับ[205,206] scammer รายหนึ่งชื่อ Banjo กล่าวว่า มีช่วงที่รายได้ดีๆ ก็สามารถทำเงินได้ถึง 60,000 ดอลลาร์ต่อเดือน[207] การสร้างสถานการณ์ฉุกเฉิน หรือเรื่องราวต่างๆ ที่จะนำไปสู่การร้องขอให้เหยื่อโอนเงินนั้นไม่มีรูปแบบเฉพาะตายตัว ทั้งนี้สืบเนื่องจากความแตกต่างหลากหลายทั้งเพศ อายุ สถานะทางสังคมของคู่สนทนาตามบริบทของแต่ละสังคม ซึ่ง scammer จะเรียนรู้ลักษณะของเหยื่อทั้งจากข้อมูลส่วนบุคคลของเหยื่อที่โพสต์ลงบนเครือข่ายสังคมออนไลน์ และการสนทนา สิ่งเหล่านี้จะถูกนำไปใช้เป็นส่วนหนึ่งในการเลือกสถานการณ์ที่ใช้หลอกลวง ซึ่งหากวิเคราะห์จากบทสนทนา หรือสถานการณ์ต่างๆ ที่เกิดขึ้นนั้นจะเห็นว่าสิ่งเหล่านั้นล้วนเป็นการเป็นประยุกต์ใช้เทคนิคทางจิตวิทยาเพื่อโน้มน้าวใจให้เหยื่อปฏิบัติตามคำร้องขอของตนไม่ว่าทางตรงหรือทางอ้อม ที่เห็นได้อย่างชัดเจนมี 2 เทคนิค คือ

Foot in the door technique (FITD) "เท้าค่อยย่างเข้าประตู" เป็นการโน้มน้าวด้วยการร้องขอทีละเล็กละน้อยและเพิ่มจำนวนขึ้นเรื่อยๆ โดยคำร้องขอในตอนแรกจะฟังมีเหตุผลมากจนมิอาจปฏิเสธได้จากนั้นคำร้องขอที่มากขึ้นจะตามมาเรื่อยๆ มีการศึกษาพบว่า "การยอมศิโรราบในเรื่อง

---

[203] Shadel, D. and Dudley, D., AARP The Magazine, "'Are You Real?' — Inside an Online Dating Scam", from https://www.aarp.org/money/scams-fraud/info-2015/online-dating-scam.html

[204] ตัวอย่างบทสนทนาจากการสัมภาษณ์ผู้เสียหาย เมื่อวันที่ 30 เมษายน พ.ศ.2562

[205] Brulliard, K., (2009), Worldwide Slump Makes Nigeria's Online Scammers Work That Much Harder, from http://www.washingtonpost.com/wp-dyn/content/article/2009/08/06/AR2009080603764_pf.html

[206] Rege, A., (2009), What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud, *International Journal of Cyber Criminology*, 3(2).

[207] Brulliard, K., (2009), Worldwide Slump Makes Nigeria's Online Scammers Work That Much Harder, from http://www.washingtonpost.com/wp-dyn/content/article/2009/08/06/AR2009080603764_pf.html

สำคัญมักเกิดขึ้นเมื่อบุคคลได้ยอมรับ/ยินยอมในเรื่องเล็กๆ ก่อนแล้วในตอนแรก”[208] ตัวอย่างเช่น ครั้งแรก scammer จะขอให้เหยื่อโอนเงินจำนวนไม่มากนักโดยมักอ้างว่าต้องใช้เงินด่วน ขอยืมเงินบางส่วน เช่น จ่ายค่ารักษาพยาบาล หรือมีเงินสดในกระเป๋าแต่ไม่ผ่านศุลกากร เป็นต้น ซึ่งถ้าเหยื่อหลงเชื่อในครั้งแรก scammer ก็จะเริ่มขอเงินจำนวนมากขึ้นในครั้งต่อไปด้วยการสร้างสถานการณ์อื่นๆ เช่น เกิดอุบัติเหตุ ลูกไม่สบายต้องเข้าโรงพยาบาลด่วน ธุรกิจมีปัญหาถูกโกง เป็นต้น หรือตามเหตุการณ์จริงของผู้หญิงไทย อายุ 33 ปี ตามที่กล่าวไปแล้วข้างต้น เหตุผลทางจิตวิทยาที่ทำให้การโน้มน้าวด้วยเทคนิคดังกล่าวประสบความสำเร็จนั้นอาจเป็นเพราะ ประเด็นเกี่ยวกับการรับรู้ตัวเองของคนเราที่มองเห็นว่าตนเป็นผู้ให้ความช่วยเหลือผู้อื่นเมื่อถูกขอร้อง ต่อมาเมื่อถูกขอร้องในเรื่องที่ใหญ่จึงตกลงเพื่อที่จะรักษาความต่อเนื่องของทัศนคติและพฤติกรรมที่เป็นไปในขั้นต้น

เทคนิคต่อมาตรงข้ามกับเทคนิคแรกโดยสิ้นเชิงคือ **Door in the face technique (DITF) “ประตูใส่หน้า”** เป็นการโน้มน้าวใจด้วยการร้องขอครั้งแรกเป็นเรื่องใหญ่มากหรือปริมาณมากโดยมั่นใจว่าจะถูกปฏิเสธ จากนั้นจะเริ่มลดปริมาณการร้องขอลงมาเรื่อยๆ จนถึงข้อเสนอที่ต้องการ ตัวอย่างเช่น scammer คนหนึ่งขอให้เหยื่อโอนเงิน 2,000 ดอลลาร์ เมื่อเหยื่อปฏิเสธว่าไม่มีเงินมากขนาดนั้น เขาก็ลดจำนวนเหลือ 300 ดอลลาร์ โดยอ้างเหตุผลว่าได้เงินมาบางส่วนแล้วและต้องการอีกแค่บางส่วนเท่านั้น ดังเหตุการณ์เกิดขึ้นจริงกับหญิงไทยคนหนึ่ง *“เธอถูก scammer ขอยืมเงินหลายหมื่นบาทเพื่อนำจ่ายค่าเช่าบ้าน แต่เหยื่อไม่ยอมโอนให้ scammer จึงลดจำนวนลงเหลือ 10,000 บาท ซึ่งเป็นจำนวนที่เหยื่อโอนให้ จากนั้นก็มีเหตุผลต่างๆ นานา มาขอให้เหยื่อโอนเงินจนสูญเงินทั้งหมดเกือบหนึ่งล้านบาท”*[209] เหตุผลที่ทำให้การโน้มน้าวนี้เป็นผลสำเร็จอาจเพราะเหตุผลทางจิตวิทยาที่เหยื่อต้องตอบเสนอในเชิงบวกต่อคู่สนทนา เพื่อให้คงความสัมพันธ์ที่ดีต่อกันและกันหากยังต้องการสานสัมพันธ์กับคนนี้ต่อไป และหากจะอธิบายถึงพฤติกรรมของอาชญากร ในสมมุติฐานที่ว่า หากผู้ก่ออาชญากรรมมีเหตุผลที่จะอธิบายการกระทำของตนเองได้ จนไม่รู้สึกว่าตนกำลังกระทำความผิด หรือคิดว่าตนมิใช่คนชั่วร้าย หรือใช้เป็นข้ออ้างในการฝ่าฝืนละเมิดกฎหมายได้ **“ทฤษฎีการแก้ตัว” (Neutralization Theory)** ถือเป็นทฤษฎีที่ช่วยอธิบายพฤติกรรมดังกล่าวได้ ทฤษฎีดังกล่าวเป็นการแก้ตัวสำหรับผู้กระทำผิดกฎหมาย เพื่อให้ตนมีความรู้สึกว่าไม่ได้กระทำผิดกฎหมาย มิได้เป็นคนชั่วร้าย หรือทำให้รู้สึกว่าการฝ่าฝืนกฎหมายเป็นสิ่งที่ยอมรับได้แม้ว่าสิ่งนั้นจะไม่ถูกต้อง ซึ่งเทคนิคการแก้ตัวที่ถูกใช้องค์กรอาชญากรรมนี้ มี 3 ประการ ได้แก่ *1. การปฏิเสธผู้เสียหาย (The Denial of Victim)* หมายถึง การมองว่าผู้เสียหายควรได้รับผลจากการกระทำของตน สามารถอธิบายได้ว่า การที่เหยื่อเสียเงินหรือทรัพย์สินไปเป็นการรับผลจากการกระทำของเหยื่อเอง เพราะเหยื่อโลภ และต้องการมีส่วนร่วมกับทรัพย์สินเหล่านั้นเอง ไม่ใช่ความผิดของ scammer เองทั้งหมด *2. การปฏิเสธความเสียหาย (The Denial of Injury)* หมายถึง การปฏิเสธความเสียหายโดยอ้างว่า ไม่ได้หลอกลวง ไม่มีผู้ใดได้รับบาดเจ็บ หรือเกิดอันตรายใดๆ แต่ทรัพย์สินที่ scammer ได้มานั้นเกิดจากความใคร่ ความเสน่ห์หาทั้งสิ้น และ *3. การอ้างถึงความซื่อสัตย์ความจงรักภักดีต่อกลุ่ม (The Appeal to Higher Loyalties)* หมายถึง คำอ้างของผู้กระทำความผิดที่ว่าการกระทำสิ่งเหล่านี้จำเป็นที่ต้องปฏิบัติตามบรรทัดฐานของกลุ่มองค์กรที่พวกเขาเป็นส่วนหนึ่ง เพราะพวกเขาให้คำยึดถือและซื่อสัตย์ จงรักภักดีต่อกลุ่มองค์กรเหล่านั้นมากการกว่าปฏิบัติตาม

---

[208] Pascual, A., & Gue'guen, N., (2005), Foot-in-the-door and door-in-the-face : A comparative meta-analytic study, *Psychological Reports,* 96, 122-128

[209] ผู้ไม่ประสงค์ออกนาม, ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม, (7 เมษายน 2562). สัมภาษณ์.

กฎหมายและบรรทัดฐานทางสังคม ซึ่งโดยปกติแล้วเทคนิคนี้มักถูกปลูกฝังในวัฒนธรรมองค์กรอาชญากรรมทุกประเภทอย่างแน่นแฟ้น จึงทำให้การแบ่งปันข้อมูล การทำเงิน และทักษะการสอนจากรุ่นสู่รุ่นอย่างที่เหล่านักหลอกลวงรักทำนั้นเป็นสิ่งที่ขับเคลื่อนองค์กรนี้ได้อย่างไม่มีวันจบสิ้น ซึ่งจากการศึกษาของ Hamlin[210] พบว่า เทคนิคการแก้ตัวนี้อาจช่วยให้อาชญากรมีความรู้สึกผิดน้อยลงจากการกระทำผิด และทำให้อาชญากรคิดว่าตนยังเป็นคนที่มีคุณค่า ดังจะเห็นได้ว่าขโมยมักไม่คิดว่าตนเป็นขโมย พวกเขายังใช้ชีวิตไปตามระเบียบของสังคม เช่น ทำงาน เรียนหนังสือ และคบหาสมาคมกับเพื่อนเป็นต้น

5) การส่งเงินเพื่อแสดงความรัก

หน้าฉาก เงินที่เหยื่อมอบให้คนรักเพื่อหวังว่าเป็นการช่วยเหลือ ช่วยพัฒนาความสัมพันธ์ รวมถึงช่วยให้ตนและคู่รักได้พบเจอกันเร็วขึ้น สถานการณ์ที่จะเกิดขึ้นกับเหยื่อแต่ละรายนั้นจะแตกต่างกันออกไปตามเรื่องราวที่ถูกสร้างมาตั้งแต่ต้น ซึ่งในประเทศไทยพบ 3 วิธีการมอบเงิน ดังนี้ *1. วิธีการโอนเงินผ่านธนาคารไปต่างประเทศโดยตรง* ในรายละเอียดของวิธีการนี้พบได้หลายกรณี เช่น คู่สนทนาอ้างว่าให้ผู้เสียหายโอนเงินผ่านบัญชีอื่นซึ่งเป็นเพื่อนของพวกเขาด้วยเหตุผลต่างๆ หรือผู้เสียหายอาจได้รับโทรศัพท์จากเจ้าหน้าที่ศุลกากร ตำรวจ พยาบาล หรือเจ้าหน้าที่อื่นๆ ที่เกี่ยวข้องให้โอนเงินไปต่างประเทศโดยตรงและให้เหตุผลว่าต่างๆ นานา ของการใช้เงิน ไม่ว่าจะเป็นการชำระค่าธรรมเนียมการนำสินค้าออก ค่าธรรมเนียมการประกันตัวเนื่องจากทรัพย์สินที่นำมาด้วยมีราคาสูง/วีซ่าหมดอายุ หรือเกิดอุบัติเหตุกะทันหันต้องใช้เงินค่ารักษาพยาบาล เป็นต้น ซึ่งในกรณีนี้ส่วนมากมักพบโอนผ่านช่องทางของสถาบันการเงิน Western Union ไปยังประเทศปลายทางที่ส่วนมากจะเป็นไนจีเรีย และมาเลเซีย อาจเป็นเพราะการโอนเงินผ่านช่องทางธนาคารมีวิธีขั้นตอนที่ค่อนข้างยุ่งยาก ทั้งนี้เพราะแต่ละธนาคารมีนโยบายอย่างชัดเจนในการป้องการการป้องกันไม่ให้ธนาคารถูกใช้เป็นตัวกลางในการประกอบอาชญากรรมตามกฎหมายป้องกันและปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่ก่อการร้าย *2. การโอนเงินผ่านบัญชีที่เปิดขึ้นในประเทศไทย* ในกรณีนี้มีรายละเอียดและเหตุผลคล้ายกับข้อแรก แต่ต่างกันที่บัญชีผู้รับเงินปลายทางอยู่ในประเทศไทย ซึ่งหลายครั้งที่ชื่อเจ้าของบัญชีเป็นชื่อคนไทย ผู้เสียหายคนหนึ่งเล่าว่า *"เธอโอนเงินครั้งแรก ให้กับชื่อบัญชีคนต่างชาติ แต่เปิดบัญชีในไทย โอนไปทั้งหมด 13 ครั้ง ครั้งแรก 15,000 บาท และครั้งต่อมาจำนวนหลายหมื่นโดยชื่อบัญชีนั้นเป็นของคนต่างชาติ 2 บัญชี และคนไทย 2 บัญชีชื่อ วรดี และรังสิมา (เป็นการโอนครั้งสุดท้ายจำนวนเงินประมาณ 300,000 บาท) รวมทั้งหมดเกือบล้านบาท ในระยะเวลาประมาณ 1 เดือน"*[211] *3. การนำเงินสดไปมอบด้วยตัวเอง* ในกรณีนี้เหยื่อหลายคนหวังว่าการเดินทางนำเงินสดไปให้ด้วยตัวเองจะเป็นโอกาสที่ดีในการพบกันในโลกความเป็นจริง แต่กลับถูกปฏิเสธการพบกันด้วยเหตุผลต่างๆ นานา เช่น ติดธุระ/ติดอยู่ที่สนามบินเพราะพกเงินสดมาจำนวนมากไม่สามารถมาพบได้จึงส่งคนมารับเงินแทน (คนรับเงินมีหลายบทบาท เช่น เจ้าหน้าที่ทูต เพื่อน เป็นต้น) เหยื่อคนหนึ่งเล่าผ่านเว็บไซต์ พันทิพย์ว่า *"เขาบอกนำเงินจำนวน 8,000,000 USD มาขอหมั้นด้วยเงินจำนวนนี้ก่อนและสิ้นปีจะมาแต่งงาน โดยจะให้นักการทูต 2 ท่านนำเงินเข้าประเทศไทยและให้เตรียมเงินไทย 200,000 สำหรับท่านทูตเป็นค่ายกกล่องเงินสด จากนั้นดิฉันเดินทางไปพารากอนซื้อผ้าพันคอ Hermes สำหรับ Clifford Rodney และซื้อของแบรนด์เนมอีก2 ชิ้นเพื่อเตรียมให้ท่านทูตเพื่อแสดงน้ำใจ มีผู้ชายโทรมาบอกว่าเป็นท่านทูตชื่อ*

[210] Conklin, J. E., (1995), *Criminology,* (5th ed.). Massachusetts: Allyn and Bacon.

[211] ผู้ไม่ประสงค์ออกนาม, ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม, (7 เมษายน 2562). สัมภาษณ์.

Dr. George Anderson ได้เดินทางมาถึงสนามบินเรียบร้อยแล้วกำลังสำแดงของและจะให้ Dr. Johnson fedrick (ซึ่งเป็นทูตเช่นกัน) มารับเงินที่ CTW Starbucks ชั้น 3 เวลาประมาณ 11.00 น. ดิฉันไปตามนัดแต่งตัวภูมิฐานใส่สูทดูดีทำผมแต่งหน้า (พบท่านทูต UK นะต้องเป็นหน้าเป็นตาให้หญิงไทยหน่อย) และได้มอบเงินครั้งแรก 200,000 บาทให้แต่โดยดีกับท่านทูตนิโกรธผิวดำชื่อ Dr.Johnson"[212] วิธีการเหล่านี้เป็นแบบแผนเดียวกันทั่วโลกมิใช่เพียงประเทศไทย ซึ่งผู้เสียหายมักมาแจ้งความเมื่อตนได้มอบเงินให้แก่บุคคลที่อ้างตนว่าเป็นผู้รับเงินเพื่อจะนำเงินไปให้คู่รักของตนไปแล้ว และไม่ได้รับเงินคืนตามสัญญา หรือไม่ได้รับสิ่งของหรือทรัพย์สินที่คู่รักของตนอ้างว่าจะส่งมาให้

หลังฉาก นอกจากสถานการณ์ที่คู่สนทนาเล่า และการส่งหลักฐานภาพถ่ายต่างๆ เพื่อขอให้เหยื่อโอนเงินแล้ว การใช้ตัวละครอื่นเข้ามาเพื่อทำให้แผนการแนบเนียนขึ้นก็เป็นวิธีการเสริมอีกรูปแบบหนึ่ง การวางโครงสร้างตัวละครต่างๆ ให้แสดงบทบาทสมมุติเป็นการร่วมมือกันขององค์กรนักหลอกลวงรัก ที่กล่าวไปแล้วข้างตนว่าแต่ละคนในองค์กรจะมีหน้าที่ต่างกันออกไปนั้น การอ้างตนว่าเป็นเพื่อน เจ้าหน้าที่รัฐ นักการทูต หรือบุคคลอื่นๆ เพื่อเป็นฐานการรับโอนเงิน เป็นละครฉากหนึ่งของขั้นตอนการหลอกลวงรัก บุคคลดังกล่าวอาจเป็นคนไทย หรือคนต่างชาติก็ได้ไม่มีรูปแบบตายตัวที่ต้องมีความสามารถในพูดคุยการต่อรองให้เหยื่อเชื่อว่าสถานการณ์ที่เกิดขึ้นนั้นมีความเป็นไปได้จริง นอกจาการโทรศัพท์ที่อ้างว่าเจ้าหน้าที่ศุลกากร หรือเจ้าหน้าที่สถานทูตที่พบได้บ่อยครั้งแล้ว ในบางครั้งมีคนแต่งชุดทหารอเมริกันมาหาถึงบ้านและอ้างตัวว่าเป็นหัวหน้าของคนที่เราคุยด้วย จากนั้นขอตรวจสอบบัตรประชาชนเพื่อยืนยันว่าเรามีตัวตนจริงไหม ซึ่งทำให้เหยื่อเชื่อว่าคู่สนทนานั้นมีตัวตนอยู่จริงๆ จากนั้นก็จะเริ่มแสดงตัวเป็นผู้รับเงินแทนคู่สนทนา ในกรณีของประเทศไทยจะสามารถสืบรู้ตัวละครเหล่านี้ได้จากการแจ้งความของผู้เสียหายแก่เจ้าหน้าที่ตำรวจ ไม่ว่าจะเป็น DIS ปอท. กองปราบปรามฯ หรือตำรวจท้องที่ จากนั้นเจ้าหน้าที่ฯ จะสืบสวนสอบสวนจากชื่อเจ้าของบัญชีที่รับการโอนเงินของเหยื่อ ซึ่งผู้ที่ได้รับเงินมีได้หลายกรณี เช่น การสมรู้ร่วมคิดกับกระบวนหลอกลวง การถูกหลอกให้เปิดบัญชีหรือการถูกขโมยข้อมูลบัญชีเพื่อใช้เป็นแหล่งรับเงิน เป็นต้น ดังเช่นตัวอย่างการจับกุม น.ส.กาญจนา มะเดื่อชุมพร อายุ 44 ปีชาวโคราช ที่ร่วมขบวนการกับชายผิวดำชาวไนจีเรีย ชื่อนายอเล็กซ์ อโคนโน โดยนายอเล็กซ์อ้างตัวชื่อ เจฟ ฮาเก้น ใช้เฟซบุ๊คติดต่อผู้หญิง คนหนึ่งที่ จ.พิษณุโลก หลอกว่าจะส่งของขวัญมาให้ทางพัสดุ น.ส.กาญจนาก็จะรับหน้าที่ต่อด้วยการโทร.ไปลวงว่าต้องชำระค่าพัสดุซึ่งภายในมีเงินอยู่ 500,000 ดอลลาร์สหรัฐ ผู้หญิงคนนี้หลงเชื่อจึงยอมโอนเงินไปให้ 2 ครั้งรวมเป็นเงิน 584,755 บาท จากนั้นนายเจฟ ฮาเก้น ก็หายไปเลย ผู้ต้องหาสารภาพว่าร่วมกับสาวไทยอีกหลายคนโทร.หลอกเหยื่อ และเปิดบัญชีรอรับเงิน สาเหตุที่ทำก็เพราะรู้จักกันทางเฟซบุ๊คเหมือนกัน จนมีความสัมพันธ์ลึกซึ้งก็ช่วยแก๊งนี้ทำมาแล้ว 4 เดือนได้เงินไปกว่า 1 ล้านบาท[213]

ข้อมูลเหล่านี้เหมาะแก่การใช้เป็นฐานข้อมูลในการตรวจสอบกิจกรรมการสื่อสารที่เกิดขึ้นในโลกไซเบอร์เพื่อใช้เปรียบเทียบในการพิสูจน์ความจริง หรือใช้เป็นเครื่องมือคัดกรองบุคคลที่อาจใช้พื้นที่ไซเบอร์เป็นช่องทางในการก่ออาชญากรรม หากประชาชนทั่วไปพบสถานการณ์ข้างต้นอาจแจ้งให้เจ้า

---

[212] pantip.com, (ม.ป.ป), *เตือนภัยสาวไทย.....อยากมีแฟนชาวต่างชาติ แวะทางนี้หน่อยค่ะ!!!!*, สืบค้นจาก https://pantip.com/topic/ 34824282/page2

[213] ปัญญา อินทร และอุดม อนุชา แก้วคำมา, (2557), สาวเปิดเฟซบุ๊กเตือนภัย แฉชาวต่างชาติสุดแสบ ต้มตุ๋นสาวไทยแต่งงาน, *ข่าวสด, (6 มิถุนายน 2562), สืบค้นจาก https://www.khaosod.co.th/view_newsonline.php ?newsid=TVRRe E5ETXp PREF4Tnc9PQ==*

พนักงานที่เกี่ยวข้องหรือผู้ดูแลระบบรับรู้ แล้วผู้บังคับใช้กฎหมายและผู้ควบคุมระบบอาจใช้อำนาจตามกฎหมายในการติดตามจับกุมผู้กระทำความผิด หรือนำข้อมูลเท็จ ปลอม บิดเบือน ออกจากระบบได้อย่างทันท่วงที

4.3.3 ข้อมูลส่วนบุคคลที่ไม่ควรเผยสู่พื้นที่ไซเบอร์สาธารณะ

นอกจากอาชญากรจะถ่ายทอดกลยุทธ์ในการอำพรางตนและล่อลวงเหยื่อผ่านการถ่ายทอดความรู้ผ่านองค์กรอาชญากรรมแล้ว อาชญากรบางส่วนยังฉวยใช้ข้อมูลส่วนบุคคลที่กลุ่มเสี่ยงเป้าหมายเผยแพร่ในอินเตอร์เน็ตเองอันนำมาซึ่งความเสี่ยง เนื่องจากได้กลายเป็นข้อมูลในการพัฒนากลยุทธ์ล่อลวงให้เหมาะกับเหยื่อรายเป้าหมาย โดยข้อมูลส่วนบุคคล 9 ประการที่ผู้ใช้อินเตอร์เน็ตไม่ควรเปิดเผยบนโลกไซเบอร์ อันจะนำมาซึ่งความเสี่ยงในการตกเป็นเป้าหมาย (เหยื่อ) ของเหล่านักหลอกลวงรัก (Romance Scam) ได้แก่

1. การใช้ชื่อเต็ม
2. สถานะความสัมพันธ์
3. รสนิยมทางเพศ
4. ID ในโปรแกรมสนทนา
5. ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address)
6. ที่อยู่ออนไลน์ของบริการอื่นๆ ในเครือข่ายสังคมออนไลน์ หรือบล๊อค
7. สิ่งที่สนใจ หรือกิจกรรมที่ชื่นชอบ
8. รูปภาพของตัวเอง
9. วิดีโอของตัวเอง

ผลการศึกษาทั้งหมดปรากฏตามวัตถุประสงค์ทั้งสามประการของการวิจัยที่ได้ทั้งจากการทบทวนเอกสารที่เกี่ยวข้อง การสัมภาษณ์ อันประกอบกันเข้าเป็นผลวิจัย แต่ยังต้องได้รับการอภิปรายผลการศึกษาต่อไปในส่วนที่ 2

ส่วนที่ 2 : การอภิปรายผลการศึกษา

จากผลการศึกษาที่ได้นำเสนอไปแล้วในหัวข้อก่อนหน้านี้ มีประเด็นที่ต้องทำการอภิปรายผลการศึกษาวิจัยในแต่ละประเด็น ดังต่อไปนี้

1) เมื่อเห็นผลการศึกษาสภาพปัญหา รูปแบบ และวิธีการของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติแล้ว เกิดข้อสังเกตดังต่อไปนี้

จากข้อมูลสถานการณ์ปัจจุบันของพิศวาสอาชญากรรมยิ่งทำให้เห็นว่าในปัจจุบันประเทศไทยมีผู้เสียหายจากการก่ออาชญากรรมในลักษณะนี้มากขึ้น แต่การนำตัวผู้กระทำความผิดมารับโทษกลับเป็นไปได้อย่างยากลำบาก และประสบความสำเร็จน้อยเมื่อเทียบกับความจำนวนผู้เสียหายและความเสียหายที่เกิดขึ้น

สาเหตุสำคัญที่ประสิทธิผลของการป้องกันและปราบปรามการก่ออาชญากรรมที่เกี่ยวกับคอมพิวเตอร์ ก็ด้วยเหตุที่อาชญากรอาศัยเทคนิควิธีพื้นฐานในการอำพรางตัวตนด้วยเทคโนโลยีคอมพิวเตอร์และแสดงตัวในโลกเสมือน อีกทั้งยังซ่อนตัวจริงด้วยระบบการไม่เปิดเผยตัวตนของโซเชียลเน็ตเวิร์คและอินเตอร์เน็ตใต้เกราะกำบังป้องกันการสืบย้อนหาตัวผู้กระทำความผิดที่แท้จริง หากขาดความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายกับเจ้าของแพลตฟอร์มผู้ควบคุมระบบก็เป็นการยากที่จะระบุเจาะจงตัวผู้กระทำความผิดจากผู้ใช้งานระบบนับล้านคน

จากการศึกษาพบว่า แม้คดีพิศวาสอาชญากรรมที่เกิดขึ้นในเขตอำนาจศาลเดียวกัน (คดีในประเทศ) ก็ยังมีจำนวนคดีน้อยมากที่คดีจะผ่านจากชั้นตำรวจ อัยการขึ้นไปสู่ศาล ถ้าหากคิดเป็นเปอร์เซ็นต์จะเห็นว่าไม่ถึง 10% เท่านั้นที่ไปคดีเหล่านี้จะไปถึงอัยการ และมีเพียง 2% เท่านั้นที่จะรอดไปถึงศาล ส่วนคดีนอกราชอาณาจักรแม้มีการแจ้งความแต่ก็เป็นไปได้ยากที่จะติดตามตัวผู้กระทำความผิดที่อยู่นอกประเทศมาดำเนินคดี ซึ่งเปอร์เซ็นต์เหล่านี้ยังไม่นับรวมกลุ่มผู้เสียหายที่ไม่กล้าแจ้งความเพื่อดำเนินคดี[214] และถ้าหากนับรวมแล้วอาจพบตัวเลขที่น่าประหลาดใจยิ่งกว่านี้ได้อีก ทั้งนี้อาจเป็นเพราะข้อจำกัดทางทั้งทางกระบวนการยุติธรรม เช่น ข้อจำกัดของเจ้าหน้าที่ในการเก็บรวบรวมหลักฐาน รวมทั้งความรู้ในวิธีการและขั้นตอนในหารสืบหาพยานหลักฐาน การเลือกใช้กฎหมายในการดำเนินคดี ระยะเวลาในการดำเนินคดี เป็นต้น อีกทั้งยังข้อมีจำกัดทางวัฒนธรรมของสังคมไทยเมื่อนำมาปรับใช้กับคดีพิศวาสอาชญากรรมที่สังคมมักตีตราบาปให้กับผู้เสียหายกลุ่มนี้ เช่น เมื่อผู้เสียหายตัดสินใจไปแจ้งความก็มักถูกเจ้าหน้าที่ตำรวจตอบกลับว่า *“ก็คุณเป็นคนโอนเงินให้เขาเอง” “ทำไมคุณเชื่อคนง่าย?”* รวมถึงความไม่รู้กฎหมายและความรู้สึกของการเข้าไม่ถึงกระบวนการยุติธรรมของผู้เสียหายเอง[215]

หากเป็นคดีที่มีลักษณะข้ามพรมแดนมีผู้เกี่ยวข้องมากกว่าหนึ่งรัฐยิ่งสร้างอุปสรรคในการดำเนินคดีด้วยข้อจำกัดของรัฐสมัยใหม่ที่มีขอบเขตอำนาจศาลเป็นเขตแดนที่ทำให้การจับกุมผู้กระทำความผิดและเยียวยาความเสียหายแก่ผู้เสียหายเป็นเรื่องยากยิ่ง

เมื่อวิเคราะห์ตามทฤษฎีปิระมิดของการละเมิดทำให้ผู้วิจัยเข้าใจถึงสถานการณ์ปัญหาที่เกิดขึ้นสะท้อนให้เห็นทางออกของปัญหาที่รอบด้านมากกว่าการมุ่งเป้าไปยังการแก้ไขตัวบทกฎหมายที่มีอยู่เดิมแล้ว ทั้งนี้การเลือกใช้ทางออกด้วยวิธีการป้องปรามอาจเป็นทางออกที่มีประสิทธิภาพที่ดีกว่าการปราบปราม หรืออาจเสนอการเลือกใช้กฎหมายมาตราอื่นในการดำเนินคดีที่จะสามารถเยียวยาและนำมาซึ่งความยุติธรรมให้แก่ผู้เสียหายมากกว่าที่ผ่านมา และสร้างการรับรู้ให้แก่ประชาชนระวังภัยจากใช้ความรักเป็นเครื่องมือในการหลอกลวง ทั้งในเชิงรูปแบบกลยุทธ์ป้องกันภัยล่วงหน้า และการรับมือเยียวยาสถานการณ์ที่เกิดขึ้นแล้ว เป็นต้น

2) โอกาสที่จะพัฒนากฎหมายและมาตรการเฝ้าระวังและเตือนภัยล่วงหน้าเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรมมีอยู่ เพียงแต่ต้องระลึกถึงเงื่อนไข ดังนี้

หากจะนำพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ มาตรา 14 (1) มาใช้กับการดึงผู้ควบคุมระบบมาร่วมมาตรการเฝ้าระวังและเตือนภัย ก็อาจเป็นเรื่องที่สร้างภาระให้กับ

---

[214] เจ้าหน้าที่ตำรวจ, โฆษกกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, (4 เมษายน 2562), สัมภาษณ์.

[215] ผู้ไม่ประสงค์ออกนาม, ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม, (7 เมษายน 2562). สัมภาษณ์.

ผู้ประกอบการซึ่งเป็นตัวกลางตามมาตรา 15 และ 19 ในการช่วยดูแล platform หรือพื้นที่มากเกินไป มาตรา 14 (1) กำหนดความรับผิดเรื่องของการปลอมแปลงตัวบุคคลอยู่แล้ว โดยให้หมายรวมทั้ง Scamming Phishing และ Identity Thief ซึ่งเป็นเรื่องของการปลอมเพื่อหลอกลวงด้วย ถ้าหากจับผู้กระทำได้ก็มีความผิดแน่นอน แต่ถ้าหากไปบอกว่าต่อไปนี้คือ เป็นหน้าที่ของผู้ให้บริการในการป้องกันและปราบปรามพิศวาสอาชญากรรม หาไม่จะมีความผิดตามมาตรา 15 ในฐานะ “ตัวการร่วม” กระทำความผิด ถือว่าเป็นภาระและสร้างต้นทุนในการประกอบธุรกิจของผู้ให้บริการมากเกินไป หากใช้หลักการแจ้งเตือนเพื่อให้นำข้อมูลออกจากระบบ (Notice and Take Down) ตามมาตรา 19 ให้เป็นหน้าที่ของผู้ควบคุมระบบในการลบเนื้อหาหลอกลวงหรือบัญชีผู้ใช้ที่สุ่มเสี่ยงว่าจะเป็นอาชญากร ก็ย่อมเป็นภาระที่มากเกินกว่าผู้ให้บริการขนาดกลางหรือขนาดย่อมจะบริหารจัดการได้เพราะมีทุนประกอบการน้อย โดยปัจจุบันมีกฎหมายลูกฉบับใหม่มาให้แล้วคือ กฎกระทรวงฉบับใหม่ ที่ออกมาในเรื่องของการแจ้งเตือน โดยครอบคลุมการกระทำความผิดตามมาตรา 14 ทั้งหมดอยู่แล้ว เพราะฉะนั้นอยู่ที่การบังคับใช้หน่วยงานรัฐที่เกี่ยวข้อง โดยบทบัญญัติปัจจุบันครอบคลุมให้เจ้าพนักงานแจ้งเจ้าของระบบให้นำข้อมูลสุ่มเสี่ยงออกจากระบบตามมาตรา 19 อยู่แล้ว ซึ่งเป็นการให้อำนาจแก่หน่วยงานบังคับใช้กฎหมายทำการแจ้งเตือน (Notice) โดยชอบด้วยกฎหมาย รวมถึงผู้ใช้บริการอินเตอร์เน็ตก็อาจแจ้งได้เช่นกันหากพบข้อมูลที่เป็นความผิด แต่เรื่องที่เป็นความผิดในลักษณะแบบนี้เป็นการป้องปรามอาจจะเป็นการมุ่งเน้นไปที่เจ้าพนักงานของรัฐที่เป็นคนแจ้งเตือน หาไม่แล้วจะนำไปสู่การใช้มาตรการนี้ในการเซ็นเซอร์ข้อมูลอื่นๆ ในอินเตอร์เน็ตอันขัดต่อเจตนารมณ์ที่แท้จริงของกฎหมายในการป้องกันและปราบปรามอาชญากรรมหลอกลวง

อุปสรรคในการดำเนินคดีที่สำคัญเป็นอันดับแรกๆ คือ การติดตามตัวผู้ต้องหามารับโทษนั่นเอง เนื่องจากโดยพื้นฐานแล้ว Romance Scam จะเป็นกรณีที่ผู้ต้องหาจะกระทำความผิดอยู่นอกราชอาณาจักรซึ่งทำให้ยากต่อการติดตามตัว หรือแม้ว่าผู้ต้องหาจะอาศัยอยู่ในราชอาณาจักร เจ้าหน้าที่ก็ยังต้องประสบกับปัญหาอีกหลายประการในการที่จะนำตัวผู้กระทำความผิดมาลงโทษ อุปสรรคส่วนหนึ่งมาจากการที่ผู้คนในปัจจุบันได้แบ่งปันเรื่องราวกิจกรรมต่างๆ ในชีวิตประจำวันของตนเองลงไปในสื่อสังคมออนไลน์ ไม่ว่าจะเป็นความคิดเห็น ภาพถ่ายส่วนตัว หรือแม้กระทั่งตำแหน่งที่ตนอยู่ ยิ่งไปกว่านั้นการที่ผู้ใช้บริการสามารถเข้าไปลงทะเบียนเข้าใช้งานสื่อสังคมออนไลน์ต่างๆ ได้โดยไม่จำเป็นต้องยืนยันตัวตน กล่าวคือ ผู้ใช้บริการสามารถลงทะเบียนเข้าใช้งานได้โดยไม่จำเป็นต้องระบุข้อมูลส่วนบุคคลที่เป็นความจริง และผู้ให้บริการสื่อสังคมออนไลน์เหล่านี้ก็ไม่ได้มีมาตรการในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของผู้ใช้บริการที่ดีพอ ดังนั้น นอกจากที่เหล่าอาชญากรจะสามารถเข้าไปลงทะเบียนเข้าใช้งานในสื่อสังคมออนไลน์เหล่านี้ได้โดยไม่จำเป็นต้องลงทะเบียนเข้าใช้งาน หรือลงทะเบียนเข้าใช้งานโดยใช้ข้อมูลเท็จได้แล้วนั้น เหล่าอาชญากรยังสามารถหาประโยชน์จากสื่อสังคมออนไลน์เหล่านี้ได้ด้วยการเข้าไปขโมยข้อมูลส่วนบุคคลต่างๆ ของผู้ใช้บริการ เช่น รูปภาพ รูปแบบการใช้ชีวิต หรือข้อมูลส่วนบุคคลอื่นๆ เพื่อนำมาใช้ในการหลอกลวงเหยื่อคนอื่นๆ อีกด้วย และในทางกลับกันการที่เหล่าผู้ใช้บริการมักจะโพสรูปภาพหรือข้อมูลต่างๆ ของตนเองลงไปในสื่อสังคมออนไลน์ทำให้กลุ่มอาชญากรสามารถใช้ข้อมูลเหล่านี้มาเลือกเหยื่อที่เหมาะสมกับรูปแบบการหลอกลวงของตนได้เช่นกัน

ขั้นตอนและความซับซ้อนของระบบราชการในการขอความร่วมมือไปยังหน่วยงานอื่นๆ ที่เกี่ยวข้อง ไม่ว่าจะเป็นหน่วยงานภายในประเทศ หรือหน่วยงานนอกประเทศในเรื่องของการขอส่งตัว

ผู้ร้ายข้ามแดน ระบบราชการที่ซับซ้อนและมีหลายขั้นตอนไม่สอดคล้องกับรูปแบบการสืบสวนเพื่อตามจับตัวคนร้ายที่ต้องอาศัยความชำนาญและความรวดเร็ว การดำเนินคดีที่ประสบความสำเร็จน้อยมาก แทบไม่ถึง 1% คนที่เข้ามาเกี่ยวข้องในภาพรวมของอาชญากรรม คนที่เข้ามาเกี่ยวกับกระบวนการนี้จะมีจำนวนมากแต่มักเป็นคนที่พิมพ์ข้อความหลอกลวงซึ่งส่วนใหญ่อยู่นอกราชอาณาจักร กลุ่มที่ไปคอยหาคนเปิดบัญชี กลุ่มเจ้าของบัญชีที่ถูกหลอกบ้างหรือที่รู้เห็นเป็นใจบ้าง[216] เช่นเดียวกับการประสานขอความร่วมมือจากผู้ให้บริการแอปพลิเคชันออนไลน์ที่ยากลำบากเนื่องจากไร้ระเบียบพิธีการที่ได้มาตรฐานร่วมกันระดับสากล และยิ่งไปกว่านั้นยังมีอุปสรรคด้านภาษาที่ถือเป็นปราการด่านสำคัญที่ก่อให้เกิดอุปสรรคในการทำงานของเจ้าหน้าที่อีกด้วย

การสร้างความร่วมมือระหว่างประเทศเป็นสิ่งจำเป็น ปัญหาอาชญากรรมไซเบอร์ต้องเป็นปัญหาความร่วมมือระหว่างประเทศ เนื่องจากไม่มีประเทศใดประเทศหนึ่งที่จะแก้ปัญหานี้ได้เพียงลำพัง แต่ปัญหาสำคัญก็คือว่ามีประชาชนในประเทศด้อยเทคโนโลยีจำนวนมากตกเป็นเหยื่อ ประเทศที่มีความก้าวหน้าทางเทคโนโลยีและพลเมืองรู้เท่าทันสื่อและภัยดิจิทัลอาจจะไม่ได้เดือดร้อน เพราะฉะนั้นสนธิสัญญา หรืออนุสัญญาที่จะแก้ไขปัญหาอาชญากรรมประเภทนี้ก็อาจจะมีความอยากทำแค่ฝ่ายเดียว คู่ภาคีอีกฝ่ายหนึ่งอาจจะไม่ยินดีที่จำเข้าร่วมทำให้การประสานงานไม่ประสบผลสำเร็จ โดยเฉพาะการแสวงหาความร่วมมือระหว่างประเทศจากรัฐที่เป็นพื้นที่พำนักของกลุ่มอาชญากรหรือรัฐที่อาชญากรโยกย้ายสินทรัพย์ไปหลบซ่อน ก็อาจต้องพบความยุ่งยากมากยิ่งขึ้น

3) หากจะสร้างแนวทางเพิ่มความตระหนักให้ประชาชนกลุ่มเสี่ยงตกเป็นเป้าหมายพิศวาสอาชญากรรมให้รู้เท่าทันพิศวาสอาชญากรรม ต้องคำนึงถึงประเด็นเหล่านี้

กลุ่มประชากรที่จำเป็นต้องเตือนให้เฝ้าระวังภัยเพราะเสี่ยงจะตกเป็นเป้าหมาย ก็คือ กลุ่มคนที่เข้าไปแสวงหาความรักความสัมพันธ์ในอินเตอร์เน็ตโดยมีการเปิดเผยข้อมูลส่วนตัวในพื้นที่สาธารณะ ซึ่งถือเป็นลักษณะการขาดความระมัดระวังตัว จำเป็นต้องมีการให้ข้อมูลเพื่อรู้เท่าทันกลวิธีของอาชญากรที่จะเข้ามาล่อลวงในลักษณะพิศวาสอาชญากรรมและความเสี่ยงรูปแบบต่างๆ ที่เกิดในโลกไซเบอร์ โดยต้องให้ข้อมูลเหล่านี้แก่ผู้บังคับใช้กำหมายเพื่อนำไปเป็นแนวทางในการดำเนินคดีและทำสำนวนฟ้องร้อง รวมถึงการให้ข้อมูลแก่ผู้ดูแลระบบคอมพิวเตอร์เพื่อทำการเฝ้าระวังและเตือนภัยให้แก่ผู้ใช้บริการหรือติดตามนำข้อมูลหลอกลวงเหล่านี้ออกจากระบบ

แนวทางในการป้องกันและปราบปรามพิศวาสอาชญากรรมทางคอมพิวเตอร์ซึ่งเป็นภัยคุกคามทางเทคโนโลยี ที่เกิดจากบทเรียนของพิศวาสอาชญากรรมทางคอมพิวเตอร์ซึ่งทำลายความไว้วางใจของประชาชนในการใช้เทคโนโลยีในมิติต่างๆ ต้องการข้อเสนอแนะเชิงนโยบายในลักษณะการสร้างความตระหนักรู้ให้กับสังคมดิจิทัล และสามารถนำไปใช้ให้เป็นมาตรการในการป้องกันปราบปรามพิศวาสอาชญากรรมทางคอมพิวเตอร์ด้วยตนเอง ตลอดจนการพัฒนานโยบายแลกเปลี่ยนกระจายข้อมูลเชิงเฝ้าระวังภัยของภาครัฐ และมาตรการเตือนภัยล่วงหน้าโดยเอกชนผู้ดูแลระบบ อันจะฟื้นฟูความไว้วางใจของประชาชนให้ใช้อินเตอร์เน็ตได้อย่างมั่นใจอันเป็นประโยชน์ต่อการพัฒนาเศรษฐกิจดิจิทัลควบคู่ไปกับการคุ้มครองสิทธิประชาชน โดยข้อมูลที่ควรเผยแพร่ให้ประชาชนตระหนักรู้ มีดังต่อไปนี้

<u>ข้อมูลส่วนบุคคลที่เผยแพร่ในอินเตอร์เน็ตอันนำมาซึ่งความเสี่ยง</u>

[216] พนักงานอัยการ. อัยการจังหวัดประจำสำนักงานอัยการสูงสุด. (16 มกราคม 2562). สัมภาษณ์.

ข้อมูลส่วนบุคคลที่ผู้ใช้อินเตอร์เน็ตไม่ควรเปิดเผยบนโลกไซเบอร์ อันจะนำมาซึ่งความเสี่ยงในการตกเป็นเป้าหมาย (เหยื่อ) ของเหล่านักหลอกลวงรัก (Romance Scam) ได้แก่ ชื่อเต็ม สถานะความสัมพันธ์ รสนิยมทางเพศ ID ที่อยู่จดหมายอิเล็กทรอนิกส์และในเครือข่ายสังคมออนไลน์ หรือบล็อก สิ่งที่สนใจหรือกิจกรรมที่ชื่นชอบ รูปภาพและวิดีโอของตัวเอง

<u>กลยุทธ์การล่อลวงที่ทำให้เหยื่อเสียทรัพย์</u>

ลักษณะการล่อลวงของนักหลอกลวงรัก (Romance Scammer) อาศัยหลักการพื้นฐานทางจิตวิทยาร่วมกับการเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูล การวางแผน และการดำเนินขั้นตอนตามที่วางแผนไว้ หรือเรียกรวมๆ ว่า “วิศวกรรมสังคม” (Social Engineering) โดยกระบวนการล่อลวงนี้สามารถแบ่งได้เป็นขั้นตอนหลัก 6 ขั้นตอน ดังนี้

1. การปลอมโปรไฟล์
2. เลือกช่องทางในการล่อเป้าหมาย
3. เลือกเป้าหมาย (เหยื่อ)
4. สร้างบทบาทเพื่อเข้าถึงเป้าหมาย
5. การสร้างสถานการณ์
6. บรรลุภารกิจทางการเงิน

<u>ขั้นตอนการร้องทุกข์ที่ในคดีพิศวาสอาชญากรรม (Romance Scam)</u>

1. ให้ผู้เสียหาย เตรียมเอกสารส่วนตัว และ สำเนาบัตรประจำตัวประชาชน

2. กรณีที่เสียหายต่อชื่อเสียง ให้เตรียมหลักฐาน ที่พบว่ามีการกระทำความผิด เช่น ปริ้นท์เอกสารหน้าจอ หน้าเว็บไซต์ หน้าโปรแกรมไลน์ โปรแกรมเฟซบุ๊ค หรือหน้าเพจที่พบการกระทำความผิด

3. กรณีที่เสียหายต่อทรัพย์ ให้เตรียมหลักฐานที่พบการกระทำความผิด การหลอกลวง เช่น หลักฐานการโอนเงิน โดยปริ้นท์เอกสารออกมาจากระบบคอมพิวเตอร์ให้เรียบร้อย

4. ให้ไปแจ้งความ ณ สถานีตำรวจท้องที่เกิดเหตุ สถานีตำรวจนครบาล หรือสถานีตำรวจภูธร ตามภูมิลำเนาตน หรือร้องทุกข์ที่กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) หรือศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.)

ผลการศึกษาและการอภิปรายผลการศึกษาทั้งหมดที่ได้จะนำไปสู่การสรุปผลการศึกษาและสร้างข้อเสนอแนะในการป้องกันและปราบปรามพิศวาสอาชญากรรม รวมไปถึงแนวทางสร้างความตระหนักรู้ให้กับประชาชนที่เสี่ยงจะตกเป็นเหยื่อต่ออาชญากรรมในบทถัดไป

บทที่ 5

บทสรุปและข้อเสนอแนะ

ผลการศึกษาที่ได้จากการวิจัยสามารถตอบสนองต่อวัตถุประสงค์ทั้ง 3 ประการ อันได้แก่

1. ศึกษาสภาพปัญหา รูปแบบ และวิธีการของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติ

2. พัฒนากฎหมายและมาตรการเฝ้าระวังและเตือนภัยล่วงหน้าเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม

3. สร้างแนวทางเพิ่มความตระหนักให้ประชาชนกลุ่มเสี่ยงตกเป็นเป้าหมายพิศวาสอาชญากรรมให้รู้เท่าทันพิศวาสอาชญากรรม

โดยมีผลการศึกษา ดังต่อไปนี้

5.1 สภาพปัญหา รูปแบบ และวิธีการของพิศวาสอาชญากรรมทั้งที่เป็นการล่อลวงภายในประเทศและการล่อลวงข้ามชาติ

ในหัวข้อนี้จะแสดงให้เห็นผลของการศึกษาใน 2 ส่วนหลัก คือ

1) สถานการณ์ปัจจุบันและสภาพปัญหาพิศวาสอาชญากรรม

2) รูปแบบและวิธีการของพิศวาสอาชญากรรม

5.1.1 สถานการณ์ปัจจุบันและสภาพปัญหาพิศวาสอาชญากรรม

พิศวาสอาชญากรรม “Romance Scam” คือ การที่นักต้มตุ๋น (Scammer) ได้ใช้เทคนิคทางจิตวิทยาผ่านเครื่องมือทางเทคโนโลยีต่าง ๆ ในการหลอกลวงให้เหยื่อ (Victim) หลงเชื่อจนกระทั่งยินยอมให้ทรัพย์สินที่นักต้มตุ๋นต้องการ ซึ่งวิธีการที่นักต้มตุ๋นมักใช้หลอกลวง คือ การสร้างโปรไฟล์ปลอมๆ ขึ้นมาในโซเชียลมีเดีย หรือเว็บไซต์หาคู่ โดยข้อมูลที่นำมาใช้ทำโปรไฟล์ปลอมก็นำมาจากการขโมยข้อมูลผู้อื่นเช่นกัน เช่น ชื่อ ประวัติ และรูปภาพ แล้วเอามาดัดแปลงเป็นข้อมูลของตนเอง หรืออีกวิธีหนึ่ง คือ จะสร้างข้อมูลเท็จขึ้นมาเองให้ดูสมจริงและน่าดึงดูดที่สุด โดยเหยื่อที่นักต้มตุ๋นเหล่านี้มองหาคนขี้เหงาและเป็นคนอ่อนไหวต้องการใครสักคนมาอยู่เคียงข้างเป็นเหยื่อ

ประเทศไทยมีผู้เสียหายจากพิศวาสอาชญากรรมมากขึ้น และไม่มีแนวโน้มจะลดลง ในปี 2558 มีผู้ร้องเรียนเข้ามาถึง 80 คดี มูลค่าความเสียหาย 150 ล้านบาท และล่าสุดสถิติข้อมูลเมื่อวันที่ 21 มิถุนายน พ.ศ. 2561 ถึง 31 พฤษภาคม พ.ศ. 2562 มีผู้เสียหายหลงเชื่อและโอนเงิน จำนวน 332 ราย รวมมูลค่าความเสียหายประมาณ 193,015,902.11 บาท ยังไม่นับคดีที่ถูกร้องเรียนไปยังสถานีตำรวจท้องที่และเหยื่อที่ไม่กล้าเข้าแจ้งความอีกเป็นจำนวนมาก และผู้ที่ตกเป็นเหยื่อส่วนมากจะเป็นหญิงโสด

อายุ 40-60 ปี การศึกษาดี หน้าที่การงานมั่นคง ที่สำคัญคือ “มีทรัพย์สิน” และมีเพียงไม่ถึง 10% เท่านั้นที่มีการแจ้งความ เหตุผลหนึ่งเพราะอับอายและลำบากใจเมื่อทราบว่าตนเองตกเป็นเหยื่อของการหลอกลวงนี้ อีกทั้งยังขาดความรู้เกี่ยวกับขั้นตอน และสถานที่ของการแจ้งความเมื่อถูกหล อกลวง และเข้าใจว่าการแจ้งความไม่ได้เกิดประโยชน์อะไรเพราะไม่น่าจะดำเนินคดีกับอาชญากรได้

อาชญากรรมชนิดนี้ไม่มีแนวโน้มที่จะลดลงเมื่อเทียบกับอาชญากรรมที่ใกล้เคียงกันอย่างคอล เซ็นเตอร์ที่ลดจำนวนลงอย่างมากหลังหน่วยงานรัฐที่ถูกอ้างชื่อได้ออกประกาศแจ้งเตือน เนื่อง จาก พิศวาสอาชญากรรมใช้วิธีการตีสนิทและทำให้ผูกพันเป็นรายบุคคลแตกต่างเรื่องราวกันไป โดยมิได้อ้างอิงกับสถาบันหรือองค์กรที่หน่วยงานจริงจะสามารถออกมาแจ้งเตือนให้ข้อมูลทำลายความน่าเชื่อถือได้ จึงมีความจำเป็นต้องเปิดเผยความจริง “หลังฉาก” เพื่อฉีกหน้ากากที่อาชญา กรสร้าง “หน้าฉาก” เพื่อหลอกให้เหยื่อตกลงปลงใจ

อีกสาเหตุที่อาชญากรรมประเภทนี้เกิดขึ้นแพร่หลายในยุคดิจิทัล ก็เพราะ ผู้คนจำนวนมากหันเข้าสู่โลกออนไลน์แทนที่จะออกไปมีปฏิสัมพันธ์กับผู้อื่น และเลือกที่จะสื่อสารเรื่องส่วนตัวกันผ่านสื่อออนไลน์มากกว่า เพราะพวกเขาสามารถระบายหรือได้พูดคุยกับคนที่ไม่รู้จักตัวตนของพวกเขาโดยอาจไม่ต้องเปิดเผยตัวตนที่แท้จริงอันทำให้พวกเขารู้สึกสบายใจกว่า เว็บไซต์และแอพพลิเคชั่นกระตุ้นให้ผู้ใช้สร้างเครือข่ายสังคมออนไลน์เพื่อพบเจอผู้คนที่อาจไม่รู้จัก แต่มีความคิด ความชอบที่เหมือนหรือคล้ายกัน ให้เข้ามาพบเจอกัน โดยเฉพาะเครือข่ายที่เป็นการสร้างชุมชนบนโลกออนไลน์ในลักษณะการใส่ข้อมูลส่วนตัวให้คนอื่นมาสนใจแบบมองมาที่ฉัน (Look at Me) อันเป็นการสร้างความเสี่ยงให้กับผู้ใช้มากขึ้น เนื่องจากผู้ใช้ได้เผยข้อมูลอ่อนไหวของตนให้คนแปลกหน้าซึ่งอาจจะเป็นอาชญากรที่มองหาเหยื่อ

5.1.2 รูปแบบและวิธีการของพิศวาสอาชญากรรม

กลยุทธ์ที่ใช้หลอกลวงทางอินเตอร์เน็ตมีหลากหลายรูปแบบ อย่างเช่น การหลอกเหยื่อว่าจะส่งของมาให้ โดยนักต้มตุ๋นจะใช้ความไว้เนื้อเชื่อใจของเหยื่อ จากการที่พูดคุยกันมาในระยะเวลาหนึ่ง และมั่นใจว่าเหยื่อให้ความไว้ใจ หรือให้ความสนิทสนมกับตนแล้ว พฤติกรรมการหลอกลวงของสแกมเมอร์มีพัฒนาการตามรูปแบบวิธีการสื่อสาร เมื่อถึงยุคเทคโนโลยีสารสนเทศ 3.0 จะเป็นการหลอกลวงทาง Social Media อย่างเช่น Facebook, Instagram เครือข่ายเหล่านี้เป็นช่องทางที่ถูกอาชญากรใช้มากที่สุด เนื่องจากมีผู้คนเข้าใช้งานเป็นจำนวนมาก อีกทั้งพฤติกรรมของผู้ใช้งานยังถูกเปิดเผยถูกสาธารณะได้ง่าย จึงทำให้อาชญากรสามารถเลือกเหยื่อเป้าหมายได้ไม่ยากนัก

หลักการพื้นฐานทางจิตวิทยาร่วมกับการเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูล การวางแผนและการดำเนินขั้นตอนตามที่วางแผนไว้ หรือเรียกรวมๆ ว่า “วิศวกรรมสังคม” (Social Engineering) โดยกระบวนการล่อลวงนี้สามารถแบ่งได้เป็นขั้นตอนหลัก 6 ขั้นตอน ดังนี้

1) การปลอมโปรไฟล์

สร้างโปรไฟล์ทั้งเพศชาย เพศหญิง และเพศทางเลือกด้วยการขโมยรูปภาพบุคคลอื่นที่มีลักษณะบุคลิกภาพดี หน้าตาดี และดูภูมิฐานจากเว็บไซด์เครือข่ายสังคมออนไลน์ต่างๆ เช่น Facebook, Instagram, twitter หรือเว็บเพจต่างๆ ส่วนใหญ่มักอ้างตัวเป็น “ฝรั่งผิวขาว” ที่เป็นเพศชายมากกว่า

เพศหญิง ลักษณะร่วมของคนเหล่านี้มักอ้างว่าโสด หรือหย่าร้าง/หม้าย ต้องการตามหารักแท้และชีวิตรักที่สมบูรณ์ หากปลอมเป็นหญิงก็จะเป็นนางแบบหุ่นดี หน้าตาดี น่าหลงใหล อายุไม่เกิน 35 ปี มีอาชีพทหาร พยาบาล ครู หรืออาชีพที่มีรายได้น้อยเพื่อสร้างความสงสารและน่าเห็นใจ แต่ถ้าเป็นเพศทางเลือกก็จะภาพมักเป็นนายแบบ/นางแบบหุ่นดี แต่งกายดี เจาะกลุ่มรักร่วมเพศ มีอาชีพที่ค่อนข้างมั่นคง

2) เลือกช่องทางในการล่อเป้าหมาย

พื้นที่ในการก่อเหตุที่พบมากที่สุด คือ Facebook รองลงมาคือ Instagram และเว็บไซต์/แอพพลิเคชั่นหาคู่ เช่น Skout, Tinder, Badoo, OkCupid, Twoo, Thai date VIP, Tagged และ Match.com เป็นต้น

3) เลือกเป้าหมาย (เหยื่อ)

หลักการของการเหยื่อคือ การมองหา “คนขี้เหงา” ที่ต้องการหาเพื่อน / คู่ชีวิตในโลกออนไลน์ ต่อมาคือการประเมินศักยภาพทางการเงิน โดยสิ่งเหล่านี้จะถูกประเมินผ่านข้อมูลส่วนบุคคลที่แสดงในเครือข่ายสังคมออนไลน์ เช่น ชื่อ อายุ อาชีพ สถานะทางการเงิน สภาพคู่ครอง และวิถีการดำเนินชีวิต เป็นต้น รวมถึงการแชร์เรื่องราว/รูปภาพ หรือการแสดงความคิดเห็นบนโลกออนไลน์ด้วย ผู้ที่ขาดความรู้ในการอยู่รอดในโลกดิจิทัล เพราะนำข้อมูลส่วนบุคคล หรือวิถีชีวิต (lifestyle) เข้าสู่พื้นที่สาธารณะ อย่างไรก็ตามเพียงแค่การเปิดเผยข้อมูลส่วนบุคคลเป็นประจำ ประกอบกับเป็นคนขี้เหงา / ขี้สงสาร และหลงเชื่อที่จะตอบกลับข้อความจากแชทคนแปลกหน้า ถือว่ามีความเสี่ยงในการตกเป็นเป้าหมาย (เหยื่อ) ของนักหลอกลวงรัก (romance scam) ได้ถึง 70%

4) สร้างบทบาทเพื่อเข้าถึงเป้าหมาย

สร้างความน่าเชื่อถือทางอาชีพ ด้วยวิธีการส่งภาพหนังสือเดินทาง หรือบัตรเจ้าหน้าที่/พนักงาน ที่ผ่านการปลอมแปลงแล้วด้วยการตัดต่อภาพถ่าย และข้อมูลส่วนบุคคล ที่พบมากสุดคือ การแต่งกายด้วยเครื่องแบบทหาร วิศวกรสนาม ภาพถ่ายแท่นขุดเจาะน้ำมันกลางทะเล เว็บไซด์บริษัท/สถานที่ทำงานให้เป้าหมาย เพื่อให้ตรวจสอบได้ว่าตนได้ทำงานอยู่ที่แห่งนั้นจริง ด้วยการสร้างเว็บไซด์ปลอมขึ้นมา

ลักษณะร่วมของการแสดงบทบาทของนักหลอกลวงรักคือการสานสัมพันธ์เชิงชู้สาวจนกลายเป็น “คนรักในอุดมคติ” ด้วยการแสดงออกด้วยวิธีต่างๆ อาทิ การส่งข้อความทักทายและใช้คำพูดที่แสนหวาน ทำให้เป้าหมายรู้สึกว่า “เป็นคนสำคัญ” แสดงความเอาใจใส่ แสดงตัวว่ามีลักษณะของ “คนดี” เช่น การใช้คำพูดและสำนวนในแง่ดีที่จะสื่อนัยยะของการเป็นคนที่ซื่อสัตย์ จริงใจ และพึ่งพาได้ รวมถึงยอมรับข้อเสียและจุดบกพร่องของเป้าหมาย (เหยื่อ) ได้ทุกอย่าง มีการสานสัมพันธ์อย่างรวบรัดและรวดเร็วตั้งแต่ 2-3 วัน หรือไม่ก็เป็นการอดทนยอมใช้เวลาเพื่อสานสัมพันธ์ไปเรื่อยๆ จนกว่าเป้าหมาย (เหยื่อ) จะตกหลุมพราง บางครั้งยาวนานถึง 2 ปี โดยมีการส่งภาพถ่ายกิจกรรมระหว่างวันวิถีชีวิต ให้เหมือนเป็นการสนทนาแบบคู่รัก และแสดงให้เห็นว่ามีตัวตนอยู่จริง

5) การสร้างสถานการณ์

สถานการณ์ที่สร้างความสงสาร ความเห็นใจ และความหวังว่าจะได้พบกันจะถูกสร้างขึ้นเพื่อร้องขอเงินจากเป้าหมาย (เหยื่อ) อันนำไปสู่การสูญเสียทรัพย์สิน ตั้งแต่มีปัญหาทางการเงินเร่งด่วนจากสถานการณ์ฉุกเฉิน ชักชวนให้ร่วมลงทุนสร้างธุรกิจเพื่อใช้ชีวิตบั้นปลายร่วมกัน ส่งสิ่งของ/ทรัพย์สินมาให้แต่ติดปัญหาที่กรมศุลกากร สนามบิน หรือสถานีตำรวจ ต้องจ่ายเงินค่าธรรมเนียมเพื่อรับสิ่งของ/ทรัพย์สินเหล่านั้น การขอแต่งงาน และส่งทรัพย์สินของหมั้นมาให้ยังประเทศไทย แต่ถูกยึดทรัพย์สินต้องจ่ายค่าธรรมเนียมก่อนอาจมีทีมงานแสดงตัวว่าเป็นเจ้าหน้าที่ของรัฐโทรศัพท์มาแจ้งค่าธรรมเนียมและเกิดปัญหาฉุกเฉินระหว่างการเดินทางมาพบกันและต้องการใช้เงินด่วน

เทคนิคการร้องขอเงินหรือผลประโยชน์ มี 2 เทคนิคหลัก คือ 1. Foot in the door technique (FITD) ตัวอย่างเช่น ครั้งแรกนักหลอกลวงรักจะขอให้เป้าหมาย (เหยื่อ) โอนเงินจำนวนไม่มากนักโดยมักอ้างว่าต้องใช้เงินด่วน ขอยืมเงินบางส่วน ซึ่งถ้าเหยื่อหลงเชื่อในครั้งแรก นักหลอกลวงรักก็จะเริ่มขอเงินจำนวนมากขึ้นในครั้งต่อไปด้วยการอ้างสถานการณ์อื่นๆ 2. Door in the face technique (DITF) ตัวอย่างเช่น นักหลอกลวงรักขอให้เหยื่อโอนเงินจำนวนมาก เมื่อเหยื่อปฏิเสธว่าไม่มีเงินมากขนาดนั้น เขาก็ลดจำนวนเงินลง โดยอ้างเหตุผลว่าได้เงินมาบางส่วนแล้วและต้องการอีกแค่บางส่วนเท่านั้น ซึ่งถ้าเหยื่อยอมโอนเงินในครั้งแรกก็จะมีการขอครั้งต่อไปเรื่อยๆ หรือบางครั้งนักหลอกลวงรักก็จะหายตัวไปทันที

6) บรรลุภารกิจทางการเงิน

นักหลอกลวงรักจะร้องขอให้มีการโอนเงินจาก 3 ช่องทางหลักดังนี้ 1. โอนเงินไปบัญชีธนาคารภายในประเทศไทย เป็นช่องทางที่จะถูกร้องขอบ่อยที่สุดถึง 90% และส่วนมากชื่อเจ้าของบัญชีเป็นชื่อคนไทย ซึ่งการโอนเงินนี้มักเกิดจากกรณีที่ผู้ร่วมขบวนการอ้างตัวว่าเป็นเจ้าหน้าที่ศุลกากร/เจ้าหน้าที่สนามบิน/เจ้าหน้าที่ส่งพัสดุ/เจ้าหน้าที่ของรัฐอื่นๆ โทรศัพท์แจ้งเป้าหมาย (เหยื่อ) ว่า “มีผู้ส่งพัสดุมูลค่ามหาศาลมาให้ ต้องจ่ายค่าธรรมเนียมเพื่อรับพัสดุดังกล่าว” และอีกกรณีที่พบได้คือนักหลอกลวงอ้างว่าเป็นบัญชีของเพื่อน หรือคนกลางที่สามารถส่งเงินต่อไปยังต่างประเทศได้อย่างรวดเร็ว 2. โอนเงินไปต่างประเทศ ส่วนใหญ่ประเทศปลายทางคือ ไนจีเรีย และมาเลเซีย ผ่านธนาคาร หรือสถาบันทางการเงินระหว่างประเทศโดยมักเป็นกรณีที่อ้างว่าเกิดเหตุฉุกเฉินระหว่างการติดต่อธุรกิจ หรือทำธุรกิจต่างประเทศ 3. มอบเงินด้วยตนเอง ด้วยเหตุผลว่าจะได้พบตัวจริงของคู่สนทนาจากออนไลน์ แต่เมื่อถึงเวลานัดหมายกันมักได้รับการปฏิเสธโดยอ้างเหตุผลว่าโดนกักตัวในสนามบินเพราะพกทรัพย์สินและเงินสดมาเป็นจำนวนมาก จึงให้ตัวแทน (แสดงเป็นเพื่อน นักการทูต เจ้าหน้าที่ศุลกากร) ถือทรัพย์สิน/เงินสดมาให้แทน และต้องมีการจ่ายเงินเพื่อแลกกับสิ่งของเหล่านั้น

เหยื่อหลายรายโดนหลอกซ้ำว่าได้จับตัวอาชญากรคนรักถูกจับแล้วแล้ว โดยผู้หลอกเหยื่อคนใหม่จะแสร้งว่าเป็นผู้มาช่วยเหลือให้อาชญากรหลุดพ้นคดี แต่จริงๆ แล้วก็เป็นอาชญากรด้วยกันเอง ทำให้เหยื่อยังติดกับวงจรของการหลอกลวงนี้ถูกหลอกซ้ำไปซ้ำมาเรื่อยๆ

5.2. กฎหมายและมาตรการเฝ้าระวังและเตือนภัยล่วงหน้าเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม

ผลการศึกษาสะท้อนให้เห็นถึงอุปสรรคที่เกิดจากข้อจำกัดของกฎหมายและกลไกในการป้องกันและปราบปรามพิศวาสอาชญากรรม เพื่อนำไปสู่การพัฒนากฎหมายและมาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมให้ดียิ่งขึ้น จึงเกิดเป็นผลการศึกษา 2 หัวข้อ คือ

1) กฎหมายและมาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมในปัจจุบัน

2) แนวทางพัฒนากฎหมายและมาตรการเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม

5.2.1 กฎหมายและมาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมในปัจจุบัน

พิศวาสอาชญากรรมเป็นความผิดที่ใช้ความรักเป็นสาระสำคัญในการหลอกลวง โดยอาศัยหลักการพื้นฐานทางจิตวิทยาร่วมกับการเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูล การวางแผน และการดำเนินขั้นตอนตามที่วางแผนไว้ เป็นการกระทำความผิดที่มีการกระทำผิดเป็นขบวนการ โดยลักษณะของการกระทำผิดเหล่านี้อาจเข้าข่ายความผิดตามกฎหมายได้หลายฐานอยู่แล้ว ไม่ว่าจะเป็นความผิดตามประมวลกฎหมายอาญา ความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ โดยในแต่ละประเด็นมีข้อสังเกตดังต่อไปนี้

1) ข้อกฎหมายที่เกี่ยวข้อง

คดีพิศวาสอาชญากรรมเป็นทั้งคดีที่มีรูปแบบการกระทำความผิดเป็นการเฉพาะตัว คือ มีการใช้ “ความรัก” ในการหลอกลวงทรัพย์สินจากผู้เสียหาย ความผิดฐานแรกที่เกี่ยวข้องจึงเป็นความผิดฐานฉ้อโกง ทั้งยังเป็นความผิดต่อแผ่นดินฐานฉ้อโกงประชาชนเมื่อมีการกระทำผิดอย่างเป็นระบบต่อสาธารณชน ทั้งนี้มีการกระทำความผิดในลักษณะร่วมมือกันอย่างเป็นกระบวนการ โดยที่ผู้กระทำความผิดมักเป็นคนต่างชาติที่ร่วมมือกับคนไทยในการกระทำความผิด โดยคนต่างชาติกลุ่มนี้จะเข้ามาในราชอาณาจักร ความผิดที่เกี่ยวข้องประการต่อมาจึงเป็นความผิดตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ และจะใช้วิธีการให้คนไทยผู้ร่วมขบวนการเป็นคนติดต่อกับผู้เสียหาย หรือเป็นเจ้าของบัญชีที่ใช้ในการกระทำความผิดในไทย ดังนี้ก็จะเป็นความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ไม่ว่าจะเป็นฐานมีหรือใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบหรือฐานมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ นอกจากนี้ยังรวมถึงความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในเรื่องการนำข้อมูลที่บิดเบือนหรือปลอมหรือเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ด้วย โดยประการที่น่าจะก่อให้เกิดความเสียหายแก่ประชาชน และความผิดฐานนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น โดยเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง หรือได้รับความอับอายด้วย

2) ผู้เสียหาย

ผู้เสียหายในสังคมไทยไม่ค่อยอยากจะไปยุ่งยากอะไรเกี่ยวกับกระบวนการทางกฎหมายหรือการขึ้นศาลหรือเจอตำรวจซึ่งสร้างยุ่งยากและมีต้นทุนด้านเวลาแก่เหยื่อ ทั้งยังไม่มีความแน่ใจว่าคดีมีความคืบหน้าหรือในท้ายที่สุดจะได้ทรัพย์สินที่เสียไปกลับคืนมาหรือไม่ หากเป็นคนที่มีการศึกษามีหน้าตาในสังคมการเข้าไปแจ้งความแล้วบอกว่าตัวเองโดนหลอกมันทำให้เขาเสื่อมเสียชื่อเสียงเสื่อมเสียสถานะทางสังคมและอาจกระทบต่อหน้าที่การงานไปด้วย จากเงื่อนไขข้างต้นสะท้อนให้เห็นถึงความต้องการกระบวนการเยียวยาร้องทุกข์ที่มีลักษณะปกป้องเกียรติยศชื่อเสียงของเหยื่อ รวมไปถึงมีช่องทางร้องเรียนที่สามารถรักษาความเป็นส่วนตัวและรายงานความคืบหน้าของคดี ไปจนถึงมีประสิทธิผลในการบังคับใช้กฎหมายดำเนินคดีกับผู้กระทำความผิดและติดตามทวงทรัพย์สินกลับมาให้ผู้เสียหายได้

3) กระบวนการยุติธรรม

เมื่อบุคคลซึ่งเป็นผู้เสียหายก็มีสิทธิในการแจ้งความร้องทุกข์ต่อเจ้าหน้าที่ตำรวจ หรืออาจยื่นฟ้องคดีต่อศาล หรืออาจขอเข้าร่วมเป็นโจทก์กับพนักงานอัยการ แต่ในคดีพิศวาสอาชญากรรมขั้นตอนของการดำเนินคดีมักสะดุดและหยุดลงในชั้นของพนักงานสอบสวน เนื่องด้วยลักษณะการกระทำความผิดที่ไม่สามารถระบุได้อย่างแน่ชัดว่าเป็นกระทำผิดในขณะที่ผู้กระทำอยู่ในหรือนอกราชอาณาจักร อีกทั้งยังเป็นกรณีที่ผู้กระทำมักกระทำผิดด้วยการอำพรางตัวตนที่แท้จริงผ่านทางบัญชีปลอม Account หรือไอพี (IP Address) ต่างประเทศ ซึ่งทำให้ยากแก่การตรวจพิสูจน์และยืนยันตัวตนผู้กระทำความผิด

เมื่อผู้กระทำความผิดได้กระทำความผิดทั้งในและนอกราชอาณาจักร และยังเป็นความผิดที่อาจไม่สามารถระบุถึงสถานที่ในการกระทำความผิดได้อย่างชัดเจน ดังนั้น จึงมีมักเกิดปัญหาขึ้นว่าพนักงานสอบสวนท้องที่ใดควรจะเป็นผู้มีอำนาจสอบสวน เพราะการสอบสวนโดยพนักงานสอบสวนที่ไม่มีอำนาจตามกฎหมายจะส่งผลให้การสอบสวนนั้นเป็นการสอบสวนที่ไม่ชอบด้วยกฎหมาย พนักงานอัยการไม่มีอำนาจฟ้อง และศาลต้องยกฟ้องคดีนี้ในที่สุด

4) ขั้นตอนในการสอบสวน

พนักงานสอบสวนเมื่อเริ่มทำการสอบสวนเพื่อให้ได้มาซึ่งตัวผู้กระทำความผิด โดยการรวบรวมพยานหลักฐานเพื่อเอาผิด และการจับกุมตัวผู้กระทำผิดมารับโทษ เมื่อนำมาพิจารณากับกระบวนการพิจารณาคดีอาญาทั้งเรื่องหลักกฎหมายและการปฏิบัติงานของเจ้าหน้าที่ จะเห็นได้ว่าอุปสรรคในการรวบรวมพยานหลักฐานของพนักงานสอบสวน สามารถแบ่งออกเป็น 3 กรณี กล่าวคือ 1) อุปสรรคด้านเวลา 2) อุปสรรคด้านทรัพยากร ไม่ว่าจะเป็นด้านเครื่องมือ กำลังพล หรืองบประมาณ และ 3) อุปสรรคด้านการติดตามตัวผู้กระทำความผิด

นอกจากนี้อุปสรรคสำคัญอย่างหนึ่งในการดำเนินคดี Romance Scam คือ หากเจ้าพนักงานตำรวจตั้งฐานความผิดเป็นคดีฉ้อโกงย่อมส่งผลให้คดี Romance Scam เป็นความผิดที่ยอมความได้ ดังนั้น หากผู้เสียหายตัดสินใจถอนคำร้องทุกข์หรือยุติการดำเนินคดี เจ้าพนักงานตำรวจก็จะไม่สามารถดำเนินคดีนี้ต่อไปได้ ซึ่งสามารถแก้ไขได้ด้วยการดำเนินคดีนี้ต่อในฐานะที่ผู้กระทำความผิดเป็นองค์กรอาชญากรรมข้ามชาติ อันจะทำให้คดี Romance Scam กลายเป็นความผิดอาญาแผ่นดิน และเจ้าพนักงานตำรวจสามารถดำเนินคดีนี้ต่อไปได้แม้ว่าผู้เสียหายจะถอนคำร้องทุกข์หรือยุติการดำเนินคดีก็ตาม

การขอความร่วมมือเพื่อการขยายผลสืบสวนต่างประเทศ (MLAT - Mutual Legal Assistance Treaty) กับรัฐบาลต่างชาติเพื่อขอให้ผู้ดูแลระบบในต่างประเทศช่วยเหลือ กรณีที่มีการกระทำผิดในต่างประเทศเราจะขอให้โครงข่ายสัญญาณโทรศัพท์ในต่างประเทศนั้นทำการพิสูจน์ทราบว่า IP นี้ในวันเวลานั้นใครเป็นคนใช้ ซึ่งขอความร่วมมือไปสองปียังไม่ได้กลับมาเลยเรื่องพยานหลักฐาน เพราะฉะนั้นอะไรที่เกี่ยวข้องกับเรื่องนี้คาดหวังยากมาก

5) การจับกุม

พนักงานสอบสวนแทบจะไม่สามารถตามผู้กระทำความผิดที่แท้จริงมาลงโทษได้เลย แต่กลับสามารถตามจับได้เฉพาะผู้ร่วมกระทำความผิดที่ได้แต่งงานหรืออยู่กินฉันสามีภรรยากับผู้กระทำความผิดเท่านั้น ทำให้ในการสืบสวนสอบสวน พนักงานสอบสวนจึงทำได้เพียงการสืบทางเส้นทางการเงินของผู้ร่วมกระทำความผิดที่เป็นเจ้าของบัญชี และนำไปขยายผลเพื่อสืบหาตัวผู้กระทำความผิด แต่ก็มักทำได้ยาก เนื่องจากผู้กระทำความผิดมักอาศัยอยู่นอกราชอาณาจักร หรือไม่สามารถหาหลักฐานมายืนยันได้ว่าผู้กระทำความผิดที่แท้จริงคือใคร เนื่องจากการปลอมแปลงตัวตนและการข้อจำกัดด้านความรู้ความเชี่ยวชาญของเจ้าหน้าที่ ข้อจำกัดด้านอุปกรณ์ และทรัพยากรทั้งหลายรวมถึงเวลา

6) ชั้นกระบวนพิจารณาของศาล

เนื่องจากในคดีอาญามีหลักการ “ต้องพิสูจน์จนสิ้นสงสัย” ทำให้เมื่อพนักงานสอบสวนไม่สามารถหาพยานหลักฐานมายืนยันจนศาล “สิ้นสงสัย” ว่าจำเลยเป็นผู้กระทำความผิดที่แท้จริงตามที่ถูกล่าวหาได้ ไม่สามารถยืนยันได้ว่าจำเลยเป็นบุคคลที่พูดคุยกับผู้เสียหาย ทำให้ “เมื่อกรณียังเป็นที่สงสัย” ศาลก็ต้องปล่อยตัวจำเลยนั้นไป และส่งผลให้มิอาจมีคำสั่งให้บังคับคดียึดทรัพย์ หรือให้ชดใช้สินไหมทดแทนในทางแพ่งได้

7) การบังคับคดี

การบังคับคดีให้ผู้เสียหายได้รับการคืนเงินต้องสืบทรัพย์ให้เห็นว่ากระจายไปอยู่ที่ใดบ้าง ซึ่งการติดตามหาจะทำได้ยาก ยิ่งส่วนใหญ่ผู้กระทำผิดเป็นต่างชาติจึงยากขึ้นไปอีกว่าจะไปสืบทรัพย์อย่างไร หรือถ้าคนไทยเปิดบัญชีให้จะบังคับคดีได้ไหมก็ไม่แน่ใจเหมือนกันว่าพอตำรวจไปอายัดบัญชีแล้วจะดำเนินการอย่างไรต่อจะมีการดำเนินคดีอาญาฟอกเงินหรืออายัดบัญชีและทรัพย์สินไว้ด้วย หาไม่แล้วทรัพย์สินก็จะถูกยักย้ายถ่ายโอนจนยากจะติดตามกลับมาชดใช้ให้ผู้เสียหาย

8) มาตรการป้องกันและปราบปรามพิศวาสอาชญากรรมโดยอาศัยความร่วมมือระหว่างรัฐกับเอกชน

กฎหมายได้เปิดโอกาสให้รัฐดำเนินการ แต่ยังมีข้อจำกัดในการแก้ไขปัญหา เพราะกฎหมายข้อมูลส่วนบุคคลก็ดี กฎหมายความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติคอมพิวเตอร์ก็ดีต้องสร้างปัจจัยแวดล้อมส่งเสริมให้คนเข้ามาใช้มีความเชื่อถือมั่นใจว่าเข้ามาแล้วปลอดภัย หากสร้างมาตรการให้ผู้ประกอบการผู้ให้บริการต้องโทษทางกฎหมายจากการไม่ให้ความร่วมมือในการสอดส่องและนำข้อมูลปลอมเท็จบิดเบือนออกจากระบบทั้งที่ไม่ได้ทำความผิดอะไรเอง หรือใช้มาตรา 15 ไปจำคุกในฐานะตัวการร่วมกระทำความผิดตามมาตรา 14 หรือมาตรา 19 ไปบีบให้ต้องคอยสอดส่องข้อมูลในระบบและลบทิ้งตลอดเวลา ย่อมไม่เป็นธรรมเพราะว่าในต่างประเทศเองเขาก็ไม่ได้ให้ผู้ให้บริการมารับ ซึ่งจะกระทบต่อการส่งเสริมเศรษฐกิจดิจิทัลเพราะเป็นการสร้างต้นทุนมหาศาลให้ผู้ประกอบการ

5.2.2 แนวทางพัฒนากฎหมายและมาตรการเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม

ผลการวิจัยที่เป็นแนวทางในการป้องกันและปราบปรามพิศวาสอาชญากรรมมี 2 แนว คือ การพัฒนามาตรการภายในประเทศให้รองรับปัญหาได้ดีมากยิ่งขึ้น และการพัฒนาความร่วมมือระหว่างประเทศ

1) การพัฒนามาตรการภายในประเทศ

การพัฒนามาตรการที่พึงประสงค์ได้แก่

- การสร้างภูมิคุ้มกันในเชิงการรณรงค์ การประชาสัมพันธ์ การสร้างความเชื่อมั่นในกระบวนการยุติธรรม ให้ประชาชนรู้ มีช่องทางเพิ่มมากขึ้นในการแจ้งข่าวสารการร้องทุกข์ หรือการเตรียมบุคลากรให้พร้อม
- บุคลากรอาจจะต้องมีทั้งหญิงและชายมีความหลากหลายมากยิ่งขึ้น เพราะบางครั้งเรื่องพวกนี้เป็นความผิดเกี่ยวกับเพศด้วย มันเกี่ยวพันกับทางเพศ การที่ผู้เสียหายจะกล้าเข้ามาแจ้งความร้องทุกข์
- การออกแบบวิธีการร้องทุกข์และดำเนินคดีที่ไม่ต้องเปิดเผยตัวตนหรือเป็นช่องทางร้องเรียนประสานงานออนไลน์
- การพัฒนากระบวนการที่สามารถช่วยเหลือเยียวยาเหยื่อในความเสียหายทางแพ่งและการติดตามทรัพย์สินกลับคืนมาชดใช้สินไหมทดแทน
- การสร้างบุคลากรเพิ่ม มิใช่เพียงสร้างศูนย์ประสานงานแต่บุคลากรไม่เพียงพอ การสร้างบุคลากรที่เข้าใจอาชญากรรมเกี่ยวกับคอมพิวเตอร์ในภาพรวมทั้งหมด สั่งสมความรู้บุคลากรในกระบวนการยุติธรรมและสร้างบุคลากรใหม่ด้วย เข้าใจใน 3-D หนึ่ง Digital Context คือบริบททางเทคโนโลยี สอง คือ Digital Fact รู้ข้อเท็จจริงทางเทคโนโลยี สาม Digital Way คือ วิถีทางทางดิจิตอล
- การทำงานเชิงรุกในหน่วยงานรัฐโดยเฉพาะหน่วยงานที่บังคับใช้กฎหมาย มีการเผยแพร่ข้อมูลในการดำเนินการว่าถ้าตกเป็นเหยื่อหรือมีข้อสงสัยว่าเราจะตกเป็นเหยื่อเราจะดำเนินการยังไงได้บ้าง และมีการรายงานความคืบหน้าว่ารัฐมีการดำเนินการหลังการร้องทุกข์ไปถึงขั้นใดแล้ว
- สร้างมาตรฐานว่าเว็บไหนที่มีมาตรฐานความปลอดภัยเพื่อสร้างความมั่นใจให้ประชาชนเข้าใช้ระบบหรือแอพลิเคชันเหล่านั้น
- มาตรการป้องกันไม่ให้เกิดอาชญากรรมซ้ำอีก คือ การให้ความรู้เผยแพร่ความรู้ความเข้าใจเกี่ยวกับอาชญากรรมไซเบอร์ เตือนภัยเรื่องการล่อลวงรูปแบบต่างๆ หรือทำละครออกมาเป็นข้อคิดให้ประชาชน และการให้กำลังใจเหยื่อเพื่อดำเนินคดีไม่ถอดใจหรือใช้ชีวิตต่อไปได้ไม่สิ้นหวัง

2) การพัฒนาความร่วมมือระหว่างประเทศ

การพัฒนาความร่วมมือระหว่างประเทศ มีศูนย์ประสานงานข้อมูลและความสัมพันธ์ระหว่างประเทศ เรื่องผ่านความร่วมมือระหว่างประเทศทางอาญา (Mutual Legal Assistance Treaty - MLAT) หาเคยได้พยานหลักฐานมาในเชิงสืบสวนนั้น อาจจะเป็นความสัมพันธ์ส่วนบุคคล (connection) ที่ให้มา หากมี connection ติดต่อจากผู้ให้บริการและหน่วยงานบังคับใช้กฎหมายในต่างประเทศหรือระหว่างประเทศได้เลยก็จะรวดเร็วแก้ปัญหาได้ ยิ่งถ้าเกิดมีการรับรองสถานะของพยานหลักฐานที่ได้มาด้วยช่องทางนี้ชัดเจนเข้าสำนวนได้

การเสริมศักยภาพในระดับประเทศเพื่อรองรับภัยคุกคามข้ามชาติแบบบูรณาการกระบวนการยุติธรรมทั้งหมด สามารถเฝ้าระวังติดตามเป็นบุคคลต้องสงสัยสร้างเป็นรายชื่อเฝ้าระวัง (Watch List) ต้องประสาน ตำรวจสากล เพื่อดำเนินคดีหรือจับมาให้ได้ หรือถ้าไม่ได้ก็ต้องขอความร่วมมือให้เกิดสัมฤทธิ์ผลที่แท้จริง

มาตรการทั้งหลายยังต้องเผชิญกับความท้าทายจากภัยที่มีลักษณะข้ามพรมแดนแต่รัฐทั้งหลายยังมีข้อจำกัดเรื่องเขตอำนาจศาล ความสลับซับซ้อนของกระบวนการยุติธรรม และประสิทธิภาพของการปฏิบัติหน้าที่ของเจ้าพนักงาน ดังนั้นแนวทางในการสร้างความเข้มแข็งให้กับผู้บังคับใช้กฎหมาย ผู้ดูแลระบบ และกลุ่มเสี่ยงที่อาจตกเป็นเหยื่อจึงมีความสำคัญ ดังจะกล่าวถึงต่อไปนี้

5.3. แนวทางเพิ่มความตระหนักให้ประชาชนกลุ่มเสี่ยงตกเป็นเป้าหมายพิศวาสอาชญากรรมให้รู้เท่าทันพิศวาสอาชญากรรม

การสร้างความตระหนักถึงภัยคุกคามไซเบอร์ในรูปแบบของพิศวาสอาชญากรรมแก่ผู้บังคับใช้กฎหมาย ผู้ดูแลระบบ และประชาชนโดยเฉพาะกลุ่มเสี่ยงที่มีความรู้ความเข้าใจต่อเทคโนโลยีและการรับรู้ข้อมูลข่าวสาร โดยการรู้เท่าทันกลยุทธ์ของอาชญากรจัดเป็นประเด็นที่สำคัญเนื่องจากอาชญากรรมประเภทนี้มาในรูปแบบการล่อลวงโดยอำพรางและสร้างความผูกพันทางจิตใจโดยอาศัยการสื่อสารผ่านอินเตอร์เน็ต การแสดงให้เห็นถึงกลยุทธ์ที่อาชญากรแสดงออกมาหน้าฉากให้เหยื่อเห็นกับความจริงหลังฉากที่อาชญากรหลบซ่อน จะเป็นการล้างภาพลวงตาและสร้างความเข้มแข็งให้กับกลุ่มเสี่ยงที่จะตกเป็นเหยื่อ

5.3.1 กลุ่มเป้าหมาย

กลุ่มเสี่ยงที่จะตกเป็นเป้าหมายและต้องเตือนภัยให้เฝ้าระวัง ก็คือ กลุ่มคนที่เข้าไปแสวงหาความรักความสัมพันธ์ในอินเตอร์เน็ตโดยมีการเปิดเผยข้อมูลส่วนตัวในพื้นที่สาธารณะ

เจ้าพนักงานของรัฐที่ทำหน้าที่บังคับใช้กฎหมายเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม อันประกอบไปด้วย เจ้าหน้าที่ตำรวจ เจ้าพนักงานคดีพิเศษ รวมไปถึงพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ

ผู้ดูแลระบบคอมพิวเตอร์ ซึ่งมีความสามารถในการรวบรวมพยานหลักฐานในกรณีเกิดการกระทำความผิดตามนัยของกฎหมาย

5.3.2 กลยุทธ์ในการสร้างหน้าฉากคนดีเพื่อหลอกลวงอำพรางหลังฉากอาชญากร

การสร้างความตระหนักรู้ผ่านการเผยแพร่งานวิจัยและเปิดเผยตัวตนที่แท้จริงของอาชญากรในแต่ละขั้นตอนเพื่อให้เห็นความจริงหลังฉากของอาชญากรย่อมทำให้ประชาชนสามารถเข้าใจถึงลักษณะของพิศวาสอาชญากรรมและรู้เท่าทันอาชญากรที่มาล่อลวงได้ดียิ่งขึ้น โดยข้อมูลที่จำเป็นที่สุดคือ ตัวตนหน้าฉาก-หลังฉาก ของอาชญากร ดังนี้

	หน้าฉาก	หลังฉาก
1. ภาพถ่ายบนโปรไฟล์	**โปรไฟล์ผู้ชาย** - ลักษณะภาพมักเป็นคนผิวขาวที่ดูมีเสน่ห์ อบอุ่น ภูมิฐาน มีฐานะ และมีท่าทางเป็นคนดี - อายุประมาณ 40 – 50 ปี - เป็นคนอเมริกัน อังกฤษ เยอรมัน หรือแคนาดา จีน สิงคโปร์ หรือเป็นลูกครึ่งไทยกับชาติอื่น	กลุ่ม ‘นักต้มตุ๋น’ อาชญากรจากหลายประเทศ เช่น ไนจีเรีย กานา มาเลเซีย รัสเซีย สหราชอาณาจักร ตุรกี เป็นต้น เริ่มจากการขโมยภาพถ่ายบุคคลที่มีลักษณะตรงตามที่บรรยายใน*หน้าฉาก*จากเว็บไซต์เครือข่ายสังคมออนไลน์ต่างๆ เรียบเรียงคำโปรยแนะนำตนเองให้ดูน่าสนใจ ด้วยการคัดลอกข้อความมาเป็นทอดทอดจากอินเตอร์เน็ต และกลุ่มอาชญากรเดียวกัน
	โปรไฟล์ผู้หญิง <u>*เป้าหมาย – ผู้ชาย*</u> - ภาพมีลักษณะเป็นนางแบบหุ่นดี หน้าตาดี น่าหลงใหล - อายุไม่เกิน 35 ปี - เป็นคนอเมริกัน โรมาเนีย หรือลูกครึ่งไทยกับชาติอื่น <u>*เป้าหมาย – ผู้หญิง*</u> - ภาพถ่ายดูมีอายุ แต่งกายดี ดูมีฐานะและน่าเชื่อถือ เป็นคนไทย เวียดนาม	
	โปรไฟล์เพศทางเลือก - มีลักษณะคล้ายนายแบบหุ่นดี แต่งกายดี	

	หน้าฉาก	หลังฉาก
2.การแนะนำตัวเองอาชีพการงานและสถานะทางสังคม	**โปรไฟล์ผู้ชาย** - มีอาชีพทหาร วิศวกร นักธุรกิจ (โดยเฉพาะเกี่ยวกับน้ำมัน ปิโตรเลียม) แพทย์ หรือเจ้าหน้าที่รัฐ - สถานภาพโสด หรือภรรยาเสียชีวิตแล้ว - อยากมีชีวิตรักที่สมบูรณ์ ตามหารักแท้ **โปรไฟล์ผู้หญิง** <u>*เป้าหมาย – ผู้ชาย*</u> - มีอาชีพทหาร พยาบาล ครู พนักงาน - สถานภาพโสด หรือ หย่าร้าง - อยากมีคู่แท้ ที่เข้าใจและดูแลกันละกัน <u>*เป้าหมาย – ผู้หญิง*</u> - สถานภาพแม่หม้าย ที่เคยมีสามีเป็นคนไทย หรือฝรั่งที่ทิ้งมรดกไว้มหาศาล **โปรไฟล์เพศทางเลือก** - มีอาชีพดีไซน์เนอร์ แพทย์ นักธุรกิจ	นักตุ้มตุ๋น ‘หลอกลวงรัก’ เป็นอาชีพหนึ่งในไนจีเรียที่ทำเงินได้อย่างมหาศาล ซึ่งผู้ที่จะเป็นนักต้มตุ๋นต้องมีทักษะดังนี้ - ทักษะทางคอมพิวเตอร์ และการติดต่อสื่อสารบนโลกออนไลน์ - สามารถสร้างโปรไฟล์ปลอมได้ - ทักษะทางสังคมที่ใช้พูดคุยกับเหยื่อให้ราบรื่น องค์กรอาชญากรรมดังกล่าวแบ่งได้เป็น 3 กลุ่ม ดังนี้ 1. ทำงานคนเดียว (พบค่อนข้างน้อย) 2. ทำเป็นกลุ่มเล็ก 3. ทำเป็นเครือข่ายใหญ่ (แบ่งหน้าที่การทำงานอย่างชัดเจน สามารถเลื่อนขั้นไปตำแหน่งอื่นๆ ได้ มีการแข่งขันเพื่อให้ได้รับสวัสดิการที่ดีในใช้ชีวิต)
3. การสร้างความเชื่อมั่น และความไว้เนื้อเชื่อใจ	ความเอาใจอย่างสม่ำเสมอของคู่สนทนาที่สร้างความผูกพันฉันชู้สาวอย่างรวดเร็ว บางคนใช้เวลาเพียง 2 สัปดาห์ บางคนนานหลายเดือน หรือยาวนานเป็นปี ดังเช่น - ข้อความแสนหวานที่ถูกส่งมาอย่างสม่ำเสมอ เช่น sweetheart, honey, my love, good night เป็นต้น - ความเอาใจใส่ ความเป็นห่วงเป็นใยทุกสถานการณ์ - แสดงตัวว่าเป็น “คนดี”	การกระทำในขั้นนี้มีการแบบแผนมาแล้วระดับหนึ่ง เนื่องจากหน้าที่หลักของนักต้มตุ๋น คือ การส่งความให้เป็นกิจวัตร การรอคอย และการสร้างความไว้วางใจ การสร้างความสัมพันธ์แบบซาบซึ้ง ถูกนำมาใช้ในขั้นตอนนี้เพื่อให้เป้าหมาย (เหยื่อ) เชื่อว่าคู่สนทนาเป็นคนดี ไว้วางใจได้ และมีทรัพย์สิน จริง ซึ่งจะนำไปสู่การชักจูง และโน้มน้าวใจได้ง่ายยิ่งขึ้น

	หน้าฉาก	หลังฉาก
	- คำกล่าวอ้างว่าอยากมีรักมั่นคง ร่วมกันสร้างฝัน และใช้บั้นปลายชีวิตร่วมกัน - บางครั้งมีการส่งรูปภาพกิจวัตรในแต่ละวัน มักเป็นกิจกรรมที่มีลักษณะของ 'กิจกรรมคนรวย' เช่น ขับรถหรู ใช้สิ่งของแบรนด์เนม เข้าฟิสเนต - บางครั้งมีการส่งสิ่งของให้ เช่น ตุ๊กตา ดอกไม้ พร้อมกับการ์ดข้อความหวานซึ้งที่พร่ำบอกรัก - บางครั้งมีการพูดคุยทางโทรศัพท์	ทั้งนี้ปฏิบัติการในขั้นนี้มักเกิดจากการเรียนรู้จากโปรไฟล์ และสิ่งต่างๆ ที่เป้าหมาย (เหยื่อ) ได้แชร์และโพสต์ลงไปในเครือข่ายสังคมออนไลน์ สิ่งเหล่านั้นจะเป็นประโยชน์อย่างยิ่งสำหรับนักต้มตุ๋นที่จะใช้ในการพิชิตใจเป้าหมาย (เหยื่อ) กลวิธี และเทคนิคต่างๆ ที่เหล่านักต้มตุ๋นใช้แล้วได้ผลลัพธ์ดีจะถูกถ่ายทอดและสอนให้แก่รุ่นสู่รุ่นไปเรื่อยๆ
4. การสร้างสถานการณ์ต่างๆ เพื่อหลอกเอาทรัพย์สิน	จากความสัมพันธ์ที่หอมหวานขยับเข้าสู่ 'การพิสูจน์รักแท้' ด้วยการร้องขอให้โอนเงิน หรือจ่ายเงิน เรื่องราวสถานการณ์ที่คู่สนทนาได้พร่ำบอกเพื่อใช้เป็นเหตุผลในการขอทรัพย์สินถูกใช้บ่อยครั้ง ดังนี้ - มีปัญหาทางการเงินเร่งด่วน เช่น ค่ารักษาพยาบาล ค่าเล่าเรียน ธุรกิจถูกโกง/มีปัญหา เกิดอุบัติเหตุ ซื้อตั๋วเครื่องบิน/ทำวีซ่าเพื่อเดินทางมาพบกัน ค่าเช่าห้องพัก เป็นต้น - ชักชวนให้ร่วมลงทุนสร้างธุรกิจ - ส่งสิ่งของ/ทรัพย์สินมาให้ แต่ติดปัญหาที่กรมศุลกากร สนามบิน หรือสถานีตำรวจ ต้องจ่ายเงินค่าธรรมเนียมเพื่อรับสิ่งของ/ทรัพย์สินเหล่านั้น - ขอแต่งงาน และส่งทรัพย์สินของหมั้นมาให้ยังประเทศไทย แต่ถูกยึดทรัพย์สินต้องจ่ายค่าธรรมเนียมก่อน (แสดงตัวว่าเป็นเจ้าหน้าที่ของรัฐโทรศัพท์มาแจ้งค่าธรรมเนียมต่างๆ) - เกิดปัญหาฉุกเฉินระหว่างการเดินทางมาพบกันและต้องการใช้เงินด่วน เช่น	ในวงการอาชญากรรมนี้ 'การทำยอด' หรือ 'การปั่นยอด' เป็นแรงจูงใจสำคัญของนักต้มตุ๋น เพื่อให้ได้รับสวัสดิการที่ดี (ได้เสื้อผ้าใหม่ ห้องพักในโรงแรม และดื่มไวน์สุดหรูใน "VVIP" คลับ) และเลื่อนตำแหน่งงาน ดังนั้นหากได้รับเงินโอนจากเหยื่อมากเท่าใดยิ่งเป็นสิ่งที่ดีมากเท่านั้น เช่น เป้าหมายทั่วไปต้องเงินอย่างน้อย 2-3 ครั้งต่อสัปดาห์ หรือแต่ละเดือนต้องได้เงิน 1,000 ดอลลาร์ เทคนิคที่ถูกนำไปใช่ใน 'การพิสูจน์รักแท้' มี 2 เทคนิค คือ 1. Foot in the door technique (FITD) เป็นการร้องขอเงินจำนวนน้อยๆ ได้ถ้ารับเงินครั้งแรกแล้ว จะเพิ่มจำนวนเงินขึ้นเรื่อยๆ ด้วยข้ออ้างต่างๆ 2. Door in the face technique (DITF) เป็นการร้องขอเงินจำนวนมากแบบสุดโต่งในครั้งแรก เมื่อเหยื่อปฏิเสธว่าไม่มีเงินจำนวนนั้น จึงค่อยๆ จำนวนลง

	หน้าฉาก	หลังฉาก
	ทรัพย์สินจำนวนมากที่นำมาถูกยึด กระเป๋าเงินหาย ถูกกักตัวที่สถานบิน บัตรเครดิตใช้งานไม่ได้ เป็นต้น สถานการณ์ต่างๆ เหล่านี้มักมาพร้อมกับภาพถ่ายที่ว่าเกิดเหตุการณ์นั้นขึ้นจริง รวมทั้งภาพถ่ายทรัพย์สินต่างๆ เพื่อแสดงว่าคนนั้นมีทรัพย์สินที่กล่าวอ้างอยู่จริง	ตามความเป็นไปได้ของเหยื่อแต่ละคน
5.บรรลุภารกิจทางการเงิน	การร้องขอเงินนั้นเป็นไปได้ 3 วิธีการ ดังนี้ 1. การโอนเงินไปต่างประเทศ ส่วนใหญ่ประเทศปลายทางคือ ไนจีเรีย และมาเลเซีย 2. การโอนเงินไปบัญชีธนาคารภายในประเทศไทย ซึ่งหลายครั้งเจ้าของบัญชีเป็นชื่อคนไทย 3. การมอบเงินด้วยตนเอง ด้วยเหตุผลว่าจะได้พบตัวจริงของคู่สนทนาจากออนไลน์ แต่เมื่อถึงเวลานัดหมายกันมักได้รับการปฏิเสธโดยอ้างเหตุผลว่าโดนกักตัวในสนามบินเพราะพกทรัพย์สินและเงินสดมาเป็นจำนวนมาก จึงให้ตัวแทน (เพื่อน นักการทูต เจ้าหน้าที่ศุลกากร) ถือทรัพย์สิน/เงินสดมาให้แทน และต้องมีการจ่ายเงินเพื่อแลกกับสิ่งของเหล่านั้น	เบื้องหลังกระบวนการ รับเงินนั้นเป็นไปได้ 2 แนวทางหลัก 1. นักต้มตุ๋น ทำงานคนเดียว มักจะให้โอนไปยังต่างประเทศด้วย การส่งภาพถ่ายเป็นหลักฐานของการมีตัวตน มีทรัพย์สินต่างๆ อาจใช้การปลอมแปลงเอกสารใบเสร็จต่างๆ ด้วย 2. นักต้มตุ๋นที่เป็นองค์กร/เครือข่าย มักใช้วิธีการแสดงบทบาทสมมุติหลายบทบาท จากเหล่านักต้มตุ๋นในองค์กร เช่น การอ้างตนว่าเป็นเพื่อน เจ้าหน้าที่รัฐ นักการทูต หรือบุคคลอื่นๆ โดยคนนั้นอาจเป็นชาวต่างชาติ หรือคนไทยก็ได้ไม่มีแบบแผนที่ชัดเจน คนเหล่านั้นมีหน้าที่รับเงินที่ถูกโอนมา หรือบางครั้งต้องเป็นผู้เจราจาต่อรองเพื่อให้เป้าหมาย (เหยื่อ) เชื่อว่าสถานการณ์ที่นักต้มตุ๋นคนหลักได้สร้างไว้เป็นเรื่องจริง ซึ่งที่พบได้บ่อยครั้งคือการอ้างว่าเป็นเจ้าหน้าที่ศุลกากร แจ้งว่าพัสดุที่ส่งมาเป็นมีมูลค่ามหาศาลต้องจ่ายค่าธรรมเนียมเพื่อรับพัสดุนั้น

	หน้าฉาก	หลังฉาก
		การเปิดบัญชีในประเทศไทยเป็นไปได้ 3 กรณีหลัก คือ 1.ถูกขโมยข้อมูลใช้เปิดบัญชี 2.ถูกหลอกให้เปิดบัญชี 3.สมรู้ร่วมคิดกับเครือข่ายอาชญากร

5.3.3 แนวทางการป้องกันตนเองของประชาชน

ประชาชนพึงระวังรักษาข้อมูลส่วนบุคคลอ่อนไหวที่ผู้ใช้อินเตอร์เน็ตไว้ไม่เปิดเผยสู่พื้นที่สาธารณะโดยเฉพาะบนโลกไซเบอร์ อันจะนำมาซึ่งความเสี่ยงในการตกเป็นเป้าหมายของเหล่าอาชญากร ได้แก่ ชื่อเต็ม สถานะความสัมพันธ์ รสนิยมทางเพศ ID ที่อยู่จดหมายอิเล็กทรอนิกส์และในเครือข่ายสังคมออนไลน์ หรือบล็อก สิ่งที่สนใจหรือกิจกรรมที่ชื่นชอบ รูปภาพและวิดีโอของตัวเอง หากจะเปิดเผยต้องจำกัดวงในการเข้าถึงเพียงคนที่รู้จักและไว้ใจได้ในชีวิตจริงเท่านั้น

5.3.4 แนวทางเฝ้าระวังและเตือนภัยโดยผู้ดูแลระบบและผู้บังคับใช้กฎหมาย

แนวทางในการป้องกันพิศวาสอาชญากรรมทางคอมพิวเตอร์ซึ่งเป็นภัยคุกคามทางเทคโนโลยีอันเหมาะแก่การเป็นมาตรการเตือนภัยล่วงหน้าโดยเอกชนผู้ดูแลระบบและหน่วยงานบังคับใช้กฎหมายภาครัฐเพื่อพิทักษ์สิทธิประชาชน โดยข้อมูลที่ควรเผยแพร่ หรือเฝ้าระวังเตือนภัยให้ประชาชนตระหนักรู้มีดังต่อไปนี้

<u>การแจ้งเตือนเมื่อประชาชนเผยข้อมูลส่วนบุคคลอ่อนไหวในอินเตอร์เน็ตอันนำมาซึ่งความเสี่ยง</u> อันได้แก่ ชื่อเต็ม สถานะความสัมพันธ์ รสนิยมทางเพศ ID ที่อยู่จดหมายอิเล็กทรอนิกส์และในเครือข่ายสังคมออนไลน์ หรือบล็อก สิ่งที่สนใจหรือกิจกรรมที่ชื่นชอบ รูปภาพและวิดีโอของตัวเอง โดยปราศจากการบริหารความเป็นส่วนตัวมิให้รั่วไหลสู่คนแปลกหน้า

<u>การเตือนประชาชนให้รู้เท่าทันกลยุทธ์การล่อลวงที่ทำให้เหยื่อเสียทรัพย์</u> กลยุทธ์ที่อาชญากรใช้การเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูล การวางแผน และการดำเนินขั้นตอนตามที่วางแผนไว้ หรือเรียกรวมๆ ว่า “วิศวกรรมสังคม” (Social Engineering) โดยกระบวนการล่อลวงนี้สามารถแบ่งได้เป็นขั้นตอนหลัก 5 ขั้นตอน ได้แก่ 1.การอำพรางปลอมโปรไฟล์ 2.การเลือกช่องทางในการล่อเป้าหมาย 3.วิธีการเลือกเหยื่อเป้าหมาย 4.การสร้างบทบาทเพื่อเข้าถึงเป้าหมาย 4.การสร้างสถานการณ์วิกฤติฉุกเฉิน 5.การทำให้เสียทรัพย์สินเงินทอง

5.4 ปัญหาและข้อจำกัดของการศึกษา

ความร่วมมือของผู้ควบคุมระบบ (Administrator) ที่เป็นผู้ดูแลแอพพลิเคชันและเว็บไซต์จับคู่ทั้งหลายมักไม่ให้ความสนใจในพัฒนาองค์ความรู้ด้านมาตรการป้องกันและปราบปรามพิศวาสอาชญากรรม การติดต่อไปขอสัมภาษณ์หรือเชิญมาร่วมงานประชุมเผยแพร่ผลการวิจัยกลับไม่มีการตอบรับ มีเพียงภาคประชาชนที่ทำงานด้านการระวังภัยที่สนใจแลกเปลี่ยนข้อมูล จึงเห็นได้ชัดว่าอุปสรรคหลักของป้องกันและสร้างความตระหนักรู้ให้กับประชาชนที่อยู่ในความเสี่ยง ก็คือ การขาดเครือข่ายแลกเปลี่ยนความรู้และระวังภัยให้กับประชาชนในหมู่ผู้ให้บริการแอพพลิเคชันและเว็บไซต์จับคู่ทั้งหลาย ทั้งยังขาดการประสานงานระหว่างผู้ให้บริการออนไลน์กับผู้บังคับใช้กฎหมาย โดยมีการอ้างว่าระบบของตนมีความปลอดภัยดีอยู่แล้วหรือผู้ให้บริการบางส่วนก็อยู่นอกราชอาณาจักรยากจะประสานงานในการสัมภาษณ์หรือแลกเปลี่ยนความรู้

ยิ่งไปกว่านั้นงานศึกษาวิจัยอื่นในไทยและต่างประเทศเกี่ยวกับอาชญากรรมไซเบอร์อื่นๆ อันท้าทายต่อการบังคับใช้กฎหมายของรัฐสมัยใหม่ยังมีอยู่ไม่มาก และปัญหาอาชญากรรมไซเบอร์มีความเปลี่ยนแปลงตามความพัฒนาการของเทคโนโลยีที่รวดเร็วมากจึงต้องมีการศึกษาวิจัยอย่างต่อเนื่อง

5.5 ข้อเสนอแนะจากการศึกษา

หลังจากได้ศึกษาวิจัยไปจนครบถ้วนแล้วเกิดข้อเสนอแนะในการพัฒนากฎหมายและมาตรการเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรมในโลกไซเบอร์ รวมถึงแนวทางการสร้างความตระหนักรู้ให้กับประชาชนกลุ่มเสี่ยงดังนี้

5.5.1 ข้อเสนอแนะเชิงนโยบาย

แม้มาตรการทางกฎหมายและกระบวนการยุติธรรมที่เกี่ยวข้องยังมีข้อจำกัดในการติดตามตัวผู้กระทำความผิดมาดำเนินคดีทางอาญาและชดเชยความเสียหายให้กับเหยื่อ ไม่ว่าจะเป็นความเสียหายทางทรัพย์สินที่ติดตามได้ยากเนื่องจากมักมีการยักย้ายถ่ายโอนไปยังผู้อื่นหรือนอกประเทศไทย ยิ่งถ้าเป็นเสียหายต่อชีวิตและทางเพศย่อมเป็นการยากที่ชดเชยให้กลับมาคืนสภาพเดิม ทั้งยังพบว่าผู้ล่อลวงจำนวนมากปฏิบัติการจากต่างประเทศซึ่งเพิ่มความลำบากให้กับกระบวนการยุติธรรมทางอาญาที่ต้องผสานความร่วมมือไปยังประเทศเจ้าของเขตอำนาจให้ส่งผู้ร้ายข้ามแดนหรือยึดทรัพย์สินกลับมาชดเชยความเสียหายให้กับเหยื่อ การสร้างมาตรการป้องปรามโดยผู้ดูแลระบบและผู้บังคับใช้กฎหมาย และการสร้างความตระหนักรู้ให้กับประชาชนเพื่อให้รู้เท่าทันและไม่ตกเป็นเหยื่อจึงน่าจะเป็นผลดีกว่าการตามดำเนินคดีหลังเกิดความสูญเสียไปแล้ว

แนวทางในการป้องกันและปราบปรามพิศวาสอาชญากรรมทางคอมพิวเตอร์ซึ่งเป็นภัยคุกคามทางเทคโนโลยี ที่เกิดจากบทเรียนของพิศวาสอาชญากรรมทางคอมพิวเตอร์ซึ่งทำลายความไว้วางใจของประชาชนในการใช้เทคโนโลยีในมิติต่างๆ ต้องการข้อเสนอแนะเชิงนโยบายในลักษณะการสร้างความตระหนักรู้ให้กับสังคมดิจิทัล และสามารถนำไปใช้ให้เป็นมาตรการในการป้องกันปราบปรามพิศวาสอาชญากรรมทางคอมพิวเตอร์ด้วยตนเอง ตลอดจนการพัฒนานโยบายแลกเปลี่ยนกระจายข้อมูลเชิงเฝ้าระวังภัยของภาครัฐ และมาตรการเตือนภัยล่วงหน้าโดยเอกชนผู้ดูแลระบบ อันจะฟื้นฟูความไว้วางใจ

ของประชาชนให้ใช้อินเตอร์เน็ตได้อย่างมั่นใจอันเป็นประโยชนต่อการพัฒนาเศรษฐกิจดิจิทัลควบคู่ไปกับการคุ้มครองสิทธิประชาชนต่อไป

5.5.2 ข้อเสนอแนะเชิงปฏิบัติการ

ข้อเสนอแนะเชิงปฏิบัติการประกอบไปด้วย 2 ส่วน คือ ขั้นตอนการร้องทุกข์ของผู้เสียหาย และแนวทางการดำเนินคดีของเจ้าพนักงานบังคับใช้กฎหมาย อันได้แก่

1) ขั้นตอนการการแจ้งความที่เกี่ยวกับคดีพิศวาสอาชญากรรมทางคอมพิวเตอร์

1. ให้ผู้เสียหาย เตรียมเอกสารส่วนตัว และ สำเนาบัตรประจำตัวประชาชน

2. กรณีที่เสียหายต่อชื่อเสียง ให้เตรียมหลักฐาน ที่พบว่ามีการกระทำความผิด เช่น ปริ้นท์เอกสารหน้าจอ หน้าเว็บไซต์ หน้าโปรแกรมไลน์ โปรแกรมเฟซบุ๊ค หรือหน้าเพจที่พบการกระทำความผิด

3. กรณีที่เสียหายต่อทรัพย์ ให้เตรียมหลักฐานที่พบการกระทำความผิด การหลอกลวง เช่น หลักฐานการโอนเงิน โดยปริ้นท์เอกสารออกมาจากระบบคอมพิวเตอร์ให้เรียบร้อย

4. ให้ไปแจ้งความ ณ สถานีตำรวจท้องที่เกิดเหตุ สถานีตำรวจนครบาล หรือสถานีตำรวจภูธร หรือร้องทุกข์ที่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) หรือศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.)

2) แนวทางการดำเนินคดีพิศวาสอาชญากรรม

การล่อลวงให้ผู้เสียหายสูญเสียทรัพย์สินเงินทองมิใช่ “การให้โดยเสน่หา” แต่เป็นความผิดทางอาญา ในคดีพิศวาสอาชญากรรมหลายกรณียังเป็นการกระทำที่เข้าข่ายองค์กรอาชญากรรมข้ามชาติอีกด้วย เนื่องจากเป็นการกระทำที่มีลักษณะของการกระทำผิดแบบข้ามพรมแดน กล่าวคือ เป็นการกระทำความผิดที่ได้กระทำลงมากกว่าในหนึ่งประเทศหรือมีส่วนหนึ่งส่วนใดของการกระทำผิดหรือผลกระทบเกี่ยวข้องตั้งแต่ 2 ประเทศขึ้นไป ซึ่งเป็นการกระทำที่สามารถส่งตัวผู้กระทำผิดที่อยู่นอกราชอาณาจักรกลับมารับโทษในราชอาณาจักรได้

ฐานความผิดที่แตกต่างกันเหล่านี้ส่งผลกับรูปแบบการดำเนินคดี โดยความผิดฐานฉ้อโกงเพียงฐานเดียวเท่านั้นที่เป็นความผิดต่อส่วนตัวหรือเป็นความผิดที่ยอมความได้ ดังนั้น ความผิดฐานนี้จึงจำเป็นต้องมีผู้เสียหาย และผู้เสียหายจะต้องมีการแจ้งความร้องทุกข์ต่อเจ้าพนักงานตำรวจด้วย เจ้าพนักงานตำรวจจึงจะมีอำนาจทำการสืบสวนคดีนั้นต่อไปได้ และหากต่อมาผู้เสียหายตัดสินใจถอนแจ้งความอำนาจในการสืบสวนสอบสวนคดีดังกล่าวก็จะสิ้นสุดลงเช่นกัน ส่วนความผิดฐานอื่นๆ เช่น ความผิดตามเกี่ยวกับการล่อลวง การใช้ภาพโปรไฟล์หรือข้อมูลปลอม อันเป็นความผิดตามพระราชบัญญัติคอมพิวเตอร์ฯ นั้นเป็นความผิดอาญาแผ่นดินผู้เสียหายไม่สามารถยอมความได้ ทำให้เจ้าพนักงานมีอำนาจในการสืบสวนสอบสวนคดีนี้ต่อไปได้โดยไม่จำเป็นต้องมีผู้เสียหาย โดยเฉพาะอย่างยิ่งหากเป็นกรณีองค์กรอาชญากรรมข้ามชาติเจ้าพนักงานยังสามารถนำตัวผู้กระทำผิดที่อยู่นอกราชอาณาจักรมารับโทษในราชอาณาจักรได้อีกด้วย

นอกจากความผิดฐานฉ้อโกง และความผิดตามพระราชบัญญัติคอมพิวเตอร์แล้ว พิศวาสอาชญากรรมยังเป็นความผิดที่เกี่ยวโยงกับความผิดหลายฐานในกฎหมายหลายฉบับด้วยกัน ไม่ว่าจะเป็นความผิดตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 และพระราชบัญญัติคนเข้าเมือง พ.ศ. 2522 อีกด้วย กฎหมายเหล่านี้ได้กำหนดหลักเกณฑ์การได้มาซึ่งพยานหลักฐานไว้แตกต่างจากประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งจะส่งผลต่อการรับฟังพยานหลักฐานของศาลที่มิจำเป็นต้องปฏิบัติตามเงื่อนไขที่ระบุไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา แต่สามารถรับฟังพยานหลักฐานภายใต้เงื่อนไขและหลักเกณฑ์ของกฎหมายต่างๆ เหล่านี้แทนได้ กล่าวคือ

พนักงานเจ้าหน้าที่ตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 นั้น ในกรณีมีเหตุอันควรเชื่อได้ว่าหากเนิ่นช้ากว่าจะรอหมายค้นมาได้ ทรัพย์สินหรือพยานหลักฐานนั้นอาจถูกยักย้าย ซุกซ่อน ทำลาย หรือทำให้เปลี่ยนสภาพไปจากเดิมได้ พนักงานเจ้าหน้าที่มีอำนาจเข้าไปในเคหสถาน สถานที่ หรือยานพาหนะใดๆ ที่มีเหตุอันควรสงสัยว่าจะมีการซุกซ่อนทรัพย์สินที่เกี่ยวกับการกระทำความผิด หรือพยานหลักฐานที่เกี่ยวกับการกระทำความผิดฐานฟอกเงินได้โดยไม่ต้องมีหมายค้น ทั้งมีอำนาจในการเข้าถึงบัญชีของลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ที่ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน และยังมีอำนาจในการจัดทำเอกสารหลักฐานหรืออำพรางตนเพื่อประโยชน์ในการตรวจสอบและรวบรวมพยานหลักฐานเพื่อดำเนินการกับทรัพย์สินที่เกี่ยวกับการกระทำความผิด หรือดำเนินคดีฐานฟอกเงินด้วย

พนักงานเจ้าหน้าที่ผู้ได้รับมอบหมายตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มีอำนาจในการยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุมัติให้กระทำการใดๆ ให้ได้มาซึ่งเอกสารหรือข้อมูลข่าวสารซึ่งส่งทางคอมพิวเตอร์ เครื่องมือ อุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีใดที่ถูกใช้หรืออาจถูกใช้เพื่อให้ได้รับประโยชน์จากการกระทำความผิดได้ รวมถึงมีอำนาจในการจัดทำเอกสารหรือหลักฐานใดขึ้น หรือปฏิบัติการอำพรางใดเพื่อประโยชน์ในการสืบสวนสอบสวน ซึ่งการกระทำเหล่านี้ถือว่าเป็นการกระทำโดยชอบด้วยกฎหมาย ทั้งยังมีอำนาจในการใช้เครื่องมือสื่อสารโทรคมนาคม เครื่องมืออิเล็กทรอนิกส์ หรือด้วยวิธีการใด ในการสะกดรอยผู้ต้องสงสัยว่ากระทำหรือจะกระทำความผิด เพื่อสืบสวน จับกุม แสวงหา และรวบรวมพยานหลักฐานได้

กรณีอาชญากรเป็นชาวต่างชาติที่พนักงานเจ้าหน้าที่สามารถนำพระราชบัญญัติคนเข้าเมือง พ.ศ. 2522 มาใช้บังคับได้ สำหรับผู้กระทำความผิดชาวต่างชาติที่จะเข้ามาอาศัยอยู่ในราชอาณาจักรนั้น พนักงานเจ้าหน้าที่มีอำนาจตรวจบุคคลที่เดินทางเข้ามาในหรือออกไปนอกราชอาณาจักร โดยมีอำนาจสั่งห้ามมิให้คนต่างด้าวที่มีพฤติการณ์เป็นที่น่าเชื่อว่าเป็นบุคคลที่เป็นภัยต่อสังคม หรือจะก่อเหตุร้ายให้เกิดอันตรายต่อความสงบสุขหรือความปลอดภัยของประชาชน หรือเข้ามาเพื่อประกอบกิจการอื่นที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนเข้ามาในราชอาณาจักรได้ หากอาชญากรเข้ามาในราชอาณาจักรเพื่อการท่องเที่ยว ทำให้ยากต่อการคัดกรองของเจ้าหน้าที่ แต่หากคนต่างด้าวเหล่านั้นมีพฤติการณ์ที่สมควรเพิกถอนการอนุญาตให้อยู่ในราชอาณาจักร พนักงานเจ้าหน้าที่โดยคณะกรรมการพิจารณาคนเข้าเมืองหรืออธิบดีกรมตำรวจมีอำนาจเพิกถอนการอนุญาตให้อยู่ในราชอาณาจักรของคนต่างด้าวเหล่านั้นได้

ส่วนผู้กระทำความผิดที่อยู่นอกราชอาณาจักรก็สามารถนำพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 พระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 มาบังคับใช้ได้ โดยหากผู้กระทำความผิดไม่ได้อาศัยอยู่ในประเทศที่ไทยมีสนธิสัญญาว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา หรือไม่ได้อาศัยอยู่ในประเทศที่ไทยมีสนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างกัน ก็สามารถขอความร่วมมือจากประเทศที่ผู้กระทำความผิดอาศัยอยู่ได้โดยอาศัยวิธีการทางการทูตได้

พนักงานสอบสวนสามารถนำหลักเกณฑ์และวิธีการสืบสวนสอบสวนซึ่งก็คือการค้นหาพยานหลักฐานในกฎหมายหลากหลายฉบับที่เกี่ยวข้องเหล่านี้มาใช้แทนประมวลกฎหมายวิธีพิจารณาความอาญา รวมถึงขอความร่วมมือกับต่างประเทศได้โดยอาศัยช่องทางทางการทูตหรือสนธิสัญญา ซึ่งจะช่วยลดข้อจำกัดในเรื่องการรับฟังพยานหลักฐานของศาลไปได้ อันจะนำมาซึ่งการนำตัวผู้กระทำความผิดมารับโทษและตรวจสอบยึดทรัพย์สินได้ในที่สุด

5.5.3 ข้อเสนอแนะในการศึกษาวิจัยเพิ่มเติม

ความรู้ที่ควรจะศึกษาเพิ่มเติมเพื่อทำให้เกิดมาตรการในการป้องกันและปราบปรามอาชญากรรมไซเบอร์อย่างครบถ้วน ตั้งแต่การสร้างความเข้มแข็งให้กับประชาชนผู้เสี่ยงว่าจะตกเป็นเหยื่อ การสร้างมาตรการเฝ้าระวังเตือนภัยของผู้ควบคุมระบบ การติดตามดำเนินคดีและบังคับใช้กฎหมาย

ประเด็นที่จำเป็นต้องศึกษาวิจัยต่อไปได้

1) ความเข้าใจพื้นฐานเกี่ยวกับการความเสี่ยงในโลกดิจิทัล
2) ลักษณะของอาชญากรรมที่เกิดขึ้นในโลกดิจิทัล
3) พฤติกรรมใดบ้างที่กลุ่มเสี่ยงทำแล้วมักตกเป็นเหยื่อของอาชญากรรม
4) กลยุทธ์ที่อาชญากรใช้ในการล่อลวงแบบ Phishing ในรูปแบบต่างๆ
5) กลยุทธ์ที่อาชญากรใช้ในการล่อลวงแบบ Scamming ในรูปแบบต่างๆ
6) กลยุทธ์ที่อาชญากรใช้ในการล่อลวงแบบ หลอกให้ซื้อของถูกหรือลงทุน แล้วโอนเงินล่วงหน้า
7) กลยุทธ์ที่อาชญากรใช้ในการล่อลวงแบบ ชักชวนให้เข้าทำธุรกิจหรือบริการผิดกฎหมาย
8) กลยุทธ์ที่อาชญากรใช้ในการล่อลวงแบบ ข่มขู่ให้หวาดกลัวโดยปลอมเป็นเจ้าหน้าที่รัฐ
9) กลยุทธ์ที่อาชญากรใช้ในการล่อลวงแบบ Pharming ยึดเพจ เว็บไซต์ที่ดูแล
10) กลยุทธ์ที่อาชญากรใช้ในการล่อลวงไปค้ามนุษย์ ด้วยการข่มขู่ กรรโชก แบล็คเมล์
11) การสำรวจจุดอ่อนของตนในการใช้ชีวิตเชื่อมโยงกับเทคโนโลยีดิจิทัล

12) การรักษาความปลอดภัยในดำรงตนในสังคมดิจิทัล

13) การรักษาความมั่นคงของระบบสื่อสารของที่พักอาศัย สถานที่ทำงาน และองค์กรสาธารณะ

14) การแลกเปลี่ยนข้อมูลเพื่อเตือนภัยและสร้างเครือข่ายเฝ้าระวังภัยสาธารณะ

15) การเยียวยาความเสียหายที่เกิดจากอาชญากรรมล่อลวงในยุคดิจิทัล

บรรณานุกรม

ภาษาไทย

กองบัญชาการตำรวจท่องเที่ยว. (2561). *ทลายเครือข่าย Romance Scam ผู้ต้องกา 17 ราย 8 เครือข่าย ผู้เสียหาย 48 ราย ความเสียหายมากกว่า 5.961.740 บาท.* (20 พฤศจิกายน 2561) สืบค้นจาก touristpolice: https://touristpolice.go.th/2018/09/15/romancescam/

กองบัญชาการตำรวจนครบาล. (2559). *คู่มือการปฏิบัติงานด้านการอำนวยความยุติธรรมในคดีอาญา เล่มที่ 1 (การทำสำนวนการสอบสวนของพนักงานสอบสวน) ของกองบัญชาการตำรวจนครบาล.* กรุงเทพฯ: กองบัญชาการตำรวจนครบาล. หน้า 14.

คมชัดลึก. (2562). *แอปหาคู่ !! สาวถูกหลอกโอน 6 แสน*. (13 พฤษภาคม 2562). สืบค้นจาก http://www.komchadluek.net/news/crime/355253?qt&fbclid=IwAR3E4EB876yEhJhnh-oVYgIM_LU43GiVIdeywcCTbhhH_4X9 KRgqjr2yIWI

เจอรัลด์ ดี แบรีแมน. (2549). เบื้องหลังหน้ากาก. แปลโดย อู่ทอง ประศาสน์วินิจฉัย. กรุงเทพฯ: ศูนย์มานุษยวิทยาสิรินธร (องค์การมหาชน).

ชไมพร คงเพชร. (2548). *สื่อลวงออนไลน์: ปัจจัยที่มีความสัมพันธ์กับพฤติกรรมการหลอกลวงบนอินเตอร์เน็ต.* วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต. มหาวิทยาลัยเกษตรศาสตร์.

ชลิตา สุนันทาภรณ์. (2560). *MODERN ROMANCE: ถอดรหัสรักออนไลน์ สุดท้ายความรักก็เป็นเรื่องของคนสองคน*. (20 พฤศจิกายน 2561). สืบค้นจาก Way magazine: https://waymagazine.org/modern-romance-waytoread/

ชิตพล กาญจนกิจ. (2559). ความท้าทายของรัฐอาเซียนในการต่อต้านอาชญากรรมข้ามชาติ. *วารสารสังคมศาสตร์ คณะนิติศาสตร์ จุฬาฯ*. ปีที่ 46 (ฉบับที่ 1). 54.

ไทยรัฐออนไลน์. (15 กรกฎาคม 2560). จับแก๊งแอฟริกันแสบ! แชตเฟซบุ๊กสวมรอยทหารมะกัน ตุ๋นผอ.โรงเรียนดังโอนเงิน. [ข่าวออนไลน์]. สืบค้นจาก https://www.thairath.co.th/content/1005807

ไทยรัฐออนไลน์. (2561). แฉเหลี่ยม!! แก๊งแชตรักลวงโลก ภัยสาวไทยนิยมผัวฝรั่ง. (18 มิถุนายน 2562). สืบค้นจาก https://www.thairath.co.th/news/society/1311031

ธนวัฒน์ สินเกษม. (2558). *ปัญหาการนำเข้าข้อมูลคอมพิวเตอร์ปลอมหรือที่เป็นเท็จตามมาตรา 14(1) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธุรกิจบัณฑิตย์.

นัฐวุฒิ สิงห์กุล. (2554). *แล้วเราจะศึกษามานุษยวิทยาในโลกไซเบอร์อย่างไร?*. สืบค้นจาก http://nattawutsingh. blogspot.com/2011/10/blog-post_2823.html

นุชรีรัตน์ ขวัญคำ. (2549). *รูปแบบการใช้สื่ออินเตอร์เน็ตของกลุ่มวัยรุ่นในเขตกรุงเทพมหานคร*. วิทยานิพนธ์นิเทศศาสตร์มหาบัณฑิต. มหาวิทยาลัยธุรกิจบัณฑิตย์.

แนวหน้า. (31 พ.ค. 2562). *ปปง.เผยตั้งศปก.ปปง.1ปี พบเหยื่อคดีโรแมนซ์สแกน 332 ราย เสียหาย 193 ล้าน.* สืบค้นจาก https://www.naewna.com/local/417058

บุญชู พวงมาลา. (2562). *หญิงวัย 60 ปีถูกชายต่างชาติอ้างเป็นทหารรักจริงหลอกโอนเงินสูญเงินเกือบล้านบาท. 77ข่าวเด็ด*. (20 พฤษภาคม 2562). สืบค้นจาก https://www.77kaoded.com/content/483682?fbclid=IwAR3L8Gt7QEh-V5wQmXIQt0ADlG4kKutemSVY4gANVOzwEnvmdfYiHB7nsy0

ปณชัย อารีเพิ่มพร. (2561). YOUEX แอปฯ จ้างเพื่อนเที่ยว จ้างกินข้าวของประเทศไทย กับแนวโน้มกระแสนิยมธุรกิจจัดหาคู่ในปัจจุบัน. (20 พฤศจิกายน 2561). สืบค้นจาก The standard: https://thestandard.co/youexapp/

ปราโมทย์ ประสาทกุล. (2552). เขยฝรั่งในแดนอีสาน. *ประชากรและการพัฒนา สถาบันวิจัยประชากรและสังคม มหาวิทยาลัยมหิดล*. 29(3). 4-5.

ปัญญา อินทร และอุดม อนุชา แก้วคำมา. (2557). สาวเปิดเฟซบุ๊กเตือนภัย แฉชาวต่างชาติสุดแสบ ต้มตุ๋นสาวไทยแต่งงาน. *ข่าวสด. (6 มิถุนายน 2562). สืบค้นจาก https://www.khaosod .co.th/view_newsonline.php ?newsid=TVRRe E5ETXp PREF4Tnc9PQ==*

ปัทมาภรณ์ กฤษณายุทธ ศิริวัชรไพบูลย์. (2554). *กฎหมายที่เกี่ยวข้องกับ Scammer ชาวผิวสีที่อ้างตัวเป็นชาวต่างชาติผิวสี*. สืบค้นจาก https://www.dsi.go.th/Files/20150605/F20150605144231-%E0%B8%9A%E0%B8%97%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%20%E0%B8%81%E0%B8%A1.scammer%20%E0%B8%9B%E0%B8%A3%E0%B8%B1%E0%B8%9A%E0%B8%9B%E0%B8%A3%E0%B8%B8%E0%B8%87.pdf

ปัทมาภรณ์ กฤษณายุทธ ศิริวัชรไพบูลย์. (2554). *พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเตอร์เน็ต*. สืบค้นจาก : https://www.dsi.go.th/Files/20150123/F20150123160326-scammer-dsi-warning.pdf

พชรพล เกตุจินากูล. (2560). *งานวิจัยชี้การเล่นโซเชียลมีเดียมากเกินไป อาจเป็นสาเหตุของความรู้สึกโดดเดี่ยว. (*20 พฤศจิกายน 2561). สืบค้นจาก The Momentum: https://themomentum.co/happy-self-help-use-social-media-more-cause-lonely/

พชรมน พิริยะสกุลยิ่ง. (2553). *กระบวนการสร้างกลุ่มเพื่อนโดยการสนทนาแบบออนไลน์: ศึกษากรณีกลุ่มเพื่อนมิตรภาพ.* วิทยานิพนธ์สังคมสิทยามหาบัณฑิต. จุฬาลงกรณ์มหาวิทยาลัย.

พลัฏฐ์กร พวงทองทิพย์. (2554). *ปัจจัยของความเสี่ยงจากการถูกล่อลวงทางอินเตอร์เน็ตของนักเรียนตอนต้น เขตบึงกุ่ม กรุงเทพมหานคร.* วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต. มหาวิทยาลัยรามคำแหง.

พิชญ์ พงษ์สวัสดิ์. (2559). *ประเทศไทย กับ เสรีภาพของอินเตอร์เน็ต 2559*. สืบค้นจาก มติชนออนไลน์ : https://www.matichon.co.th/news/366683.

พิชัย โชติชัยพร. (2555). *ปัญหาความรับผิดของผู้ให้บริการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550.* วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต มหาวิทยาลัยสุโขทัยธรรมมาธิราช.

พิทักษ์ พงศ์กางการ. (2560). การแต่งงานข้ามวัฒนธรรมของผู้หญิงในชนบทอีสาน: กรณีศึกษาจังหวัดชัยภูมิ. *วารสารวิชาการ มหาวิทยาลัยกรุงเทพธนบุรี*. 6(2). 70-79.

ฟ้าใส วิเศษกุล. (2544). *การวิเคราะห์ค่านิยมและทัศนคติเกี่ยวกับเพศสภาพในสังคมไทย ที่ปรากฏในสื่ออินเทอร์เน็ตเว็บบอร์ด*. วิทยานิพนธ์นิเทศศาสตรมหาบัณฑิต. มหาวิทยาลัยธุรกิจบัณฑิตย์.

ภูมินทร์ บุตรอินทร์ (2560). มาตรการที่เหมาะสมในการรักษาความมั่นคงปลอดภัยไซเบอร์: ศึกษา (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงไซเบอร์ พ.ศ. .... *วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.* ปีที่ 46 ฉบับที่ 2 (ธันวาคม 2560). อ้างใน วัชระ เนติวาณิชย์. *คู่มือกฎหมายการสื่อสารและเทคโนโลยีสารสนเทศ.* กำแพงเพชร: ห้างหุ้นส่วนจำกัดศรีสวัสดิ์การพิมพ์. หน้า 199.

รายงานประจำสัปดาห์ (วันที่ 10 มี.ค. 2561 – 16 มี.ค. 2561) ข้อมูลการเข้าร้องทุกข์ ณ ศูนย์บริการประชาชน กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)

แลร์รี อี. แดเนียล. ลาร์ส อี แดนเนียล. สุนีย์ สกาวรัตน์ (ผู้แปล). (2559). *การตรวจพิสูจน์หลักฐานดิจิทัลสำหรับผู้ประกอบวิชาชีพกฎหมาย: เข้าใจพยานหลักฐานดิจิทัลจากขั้นตอนหมายถึงห้องพิจารณาคดี. บทที่ 26 ค่า Hash: มาตรฐานการพิสูจน์ยืนยัน.* กรุงเทพฯ: มูลนิธิเพื่ออินเตอร์เน็ตและวัฒนธรรมพลเมือง.

วชิรวิทย์ คงคาลัย. (17 กรกฎาคม 2560). *Romance Scam: ไม่รักไม่ว่าอะไร แต่ใยต้องหลอกกันด้วย.* [เว็บบล็อก]. สืบค้นจาก https://www.the101.world/life/romance-scam/

วันดี สันติวุฒิเมธี. (2560). *มองทะลุม่านมายาคติ “หญิงไทยกับสามีฝรั่ง” : เมื่อสิ่งที่เห็น อาจไม่ใช่สิ่งที่เป็น.* (4 เมษายน 2562). สืบค้นจาก https://www.the101.world/the-myth-of-thai-wife-and-her-foreign-husband/

ศุนิสา ทดลา. (2542). *รูปแบบพฤติกรรมการสื่อสารในห้องสนทนาบนเครือข่ายอินเตอร์เน็ต.* วิทยานิพนธ์นิเทศ ศาสตรมหาบัณฑิต. จุฬาลงกรณ์มหาวิทยาลัย.

สฤณี อาชวานันทกุล. (2558). *DIGITAL FUTURE กลไกกำกับดูแลอินเตอร์เน็ต และปัญหาในไทย: ค่านิยมในสังคมสองขั้ว*. กรุงเทพ: สำนักพิมพ์ open worlds. หน้า 118.

สาวตรี สุขศรี. (2555). *อาชญากรรมคอมพิวเตอร์? : งานวิจัยหัวข้อ ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น.* กรุงเทพฯ: โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLaw) ในมูลนิธิเพื่อสังคม. หน้า 83.

สาวตรี สุขศรี. (2560). “อาชญากรรมคอมพิวเตอร์/ไซเบอร์กับทฤษฎีอาชญาวิทยา.” *วารสารนิติศาสตร์*. ปีที 46 ฉบับที่ 2 (มิถุนายน 2560). หน้า 415-432.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2561). *Thailand Internet User Profile 2018 ผลสำรวจพฤติกรรมการใช้อินเทอร์เน็ตของคนไทยประจำปี 2561*. กรุงเทพฯ: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน).

สำนักงานสถิติแห่งชาติ. (2561). *การสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2561 (ไตรมาส 1).* กรุงเทพฯ: สำนักงานสถิติแห่งชาติ.

สุภางค์ จันทวานิช. (2551). *การวิเคราะห์เชิงละคร* ทฤษฎีสังคมวิทยา. กรุงเทพฯ: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย. หน้า 131-132.

สุวิชาภา อ่อนพึ่ง. (2554). *ปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษาความผิดเกี่ยวกับการเผยแพร่ข้อมูลกระทบต่อความมั่นคงแห่งราชอาณาจักร.* วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย.

โสรัจจ์ หงศ์ลดารมภ์. (2555) ตัวตนออนไลน์. *มาราธอน ฉบับ "ออกตัว" : รวมบทความและบันทึกเสวนาว่าด้วยอินเทอร์เน็ต การเมือง และวัฒนธรรม*. นฤมล กล้าทุกวัน. บรรณาธิการ.

อุดม รัฐอมฤต. (2558). *คำอธิบายกฎหมายลักษณะพยานหลักฐาน* (พิมพ์ครั้งที่ 6 แก้ไขเพิ่มเติม). กรุงเทพฯ : โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. หน้า 214.

อุมาวัลย์ จันทะแก้ว. (2547). *อิทธิพลของพฤติกรรมการเปิดรับเนื้อหาทางเพศผ่านสื่ออินเตอร์เน็ตที่ส่งผลต่อค่านิยมทางเพศของกลุ่มวัยรุ่นในเขตกรุงเทพมหานคร*. วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต. มหาวิทยาลัยศรีนครินทรวิโรฒ.

อุษา บิ้กกิ้นส์. (2559). ไซเบอร์เซ็กส์กับทัศนคติทางเพศของวัยรุ่น. *วารสารสุทธิปริทัศน์* ปีที่ 30 ฉบับพิเศษ: 104-114

Ansari. A. (2559). *ถอดรหัสลับออนไลน์ (Modern Romance).* แปลโดย สุนันทา วรรณสินธ์. กรุงเทพฯ: โอเพ่นเวิลด์ส (openworlds).

Arjin. (2561). *Facebook ไตรมาสล่าสุด รายได้โต 11% ผู้ใช้ในยุโรปลดลงเป็นครั้งแรก ราคาหุ้นร่วง 20%.* (28 พฤศจิกายน 2561). สืบค้นจาก Blogone: https://www.blognone.com/node/104131

BBC News. (2018). *งานวิจัยไขความลับ เดทออนไลน์อย่างไรให้เจอรัก.* (30 พฤษภาคม 2562). สืบค้นจาก https://www.bbc.com/thai/international-45124922

Engel. D. M. (2557). “บทบาทของกฎหมายที่มีต่อชีวิตของสามัญชน.” *นิติสังคมศาสตร์* ปีที่ 2 ฉบับ 1. หน้า 141- 163.

INNNews. (2018). *เตือนภัย!สาวถูกฉกข้อมูลลงประกาศเว็บไซต์หาคู่*. (20 พฤษภาคม 2562). สืบค้นจาก https://www.innnews.co.th/crime/news_211157/

Mindphp. (4 ธันวาคม2560). IP Address คืออะไร. (20 มิถุนายน 2562). สืบค้นจาก Mindphp: https://mindphp.com/%E0%B8%84%E0%B8%B9%E0%B9%88%E0%B8%A1%E0%B8%B7%E0%B8%AD/73-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0% B8%A3/2071-ip-address-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8% B0%E0%B9%84%E0%B8 %A3.html

Pantip.com. (2557). *ความรักในโลกออนไลน์ คุณคิดว่ามีจริง หรือ แค่หลอกลวง???.* (26 พฤศจิกายน 2561). สืบค้นจาก https://pantip.com/topic/31571701

pantip.com. (ม.ป.ป). *เตือนภัยสาวไทย.....อยากมีแฟนชาวต่างชาติ แวะทางนี้หน่อยค่ะ!!!!*. สืบค้นจาก https://pantip.com/topic/ 34824282/page2

Perloff-Gile. A. (2017). *A"PROBLEM WITHOUT A PASSPORT": OVERCOMING JURISDICTIONAL CHALLENGES FOR TRANSNATIONAL CYBER AGGRESSIONS*. สืบค้นจาก https://law.yale.edu/ system/files/area/center/global/document/perloff-giles_cyber_conflict_paper_-_final_draft.pdf

PPTV. (2558). *แชทตุ๋นลวงโลก*. สืบค้นจาก https://www.pptvhd36.com/programs/%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A7%E0%B8%B2%E0%B9%84%E0%B8%A3%E0%B8%95%E0%B8%B5%E0%B9%89/%E0%B8%A5%E0%B9%88%E0%B8%B2/49470#part-3

Rabbit finance Magazine. (2561). *Romance Scam หลอกรักออนไลน์ ภัยร้ายของสาวโสด!.* (25 พฤศจิกายน 2561). สืบค้นจาก Rabbit finance Magazine: https://finance .rabbit.co.th /blog/romance-scam-and-single-ladies.

Ratirita. (2561). *ถอดรหัส! ทำไม Twitter ถึงโตอย่างรวดเร็วในประเทศไทย?*. (26 พฤศจิกายน 2561). สืบค้นจาก Brandinside: https://brandinside.asia/twitter-growth-in-thailand/

Thai Anti Scam (สาวไทยรู้ทันกลลวง). (2561). *ล่า (แชทตุ๋นลวงโลก) 41.3*. สืบค้นจาก https://www.facebook.com /sao.thai.rutan.kolluang/videos/1881064811975914/

Thai Anti Scam (สาวไทยรู้ทันกลลวง). (2561). สืบค้นจากhttps://www.facebook.com/sao.thai.rutan.kolluang/photos/pcb.2277156485700076/2277155959033462/?type=3&theater

The matter. (2561). *โลกออนไลน์ ทำให้เราเหงามากขึ้น? วัยรุ่นอังกฤษ มีสัดส่วนความเหงาเยอะที่สุด ผลสำรวจชี้ อาจเกี่ยวกับจำนวนเพื่อนในเฟสบุ๊ค.* (20 พฤศจิกายน 2561). สืบค้นจาก The Matter: https://thematter.co /brief/news-1538467201/61445

The101.world. (2560). *Romance Scam: ไม่รักไม่ว่าอะไร แต่ใยต้องหลอกกันด้วย*. (25 มีนาคม 2561). สืบค้นจาก The101: https://www.the101.world/life/romance-scam/.

Tinder. (ม.ป.ป.). *Tinder คืออะไร.* (28 พฤศจิกายน 2561). สืบค้นจาก Tinder: https://www.help.tinder.com/hc/th/articles/115004647686-Tinder-คืออะไร-

Voice TV. (11 มิถุนายน 2559). *จับแก๊ง 'Romance scam' หลอกหญิงไทยโอนเงินซื้อของหมั้น.* สืบค้นจาก https://www.voicetv.co.th/read/376101

ภาษาอังกฤษ

ACCC. (2018). *Scam statistics: dating & romance in 2018*. from https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=13& date=2018

Ajayhi. E.. (2015). “The Challenges to Enforcement of Cybercrimes Laws and Policy”. *International Journal of Information Security and Cybercrime*. 4(2). 33-48. from https://www.ijisc.com

Australian Competition and Consumer Commission (ACCC). (2011). Dating and romance scams: Defining the harm. Australia: ACCC.

Brulliard. K.. (2009). Worldwide Slump Makes Nigeria's Online Scammers Work That Much Harder. from http://www.washingtonpost.com/wp-dyn/content/article /2009/08/06/AR2009080603764_ pf.html

Buss. D. M. and Barnes. M.. (1986). Preferences in human mate selection. *Journal of Personality and Social Psychology.* 50 (3): 559 – 570.

Chaffey. D.. (2019). Global social media research summary 2019. from https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

Cohen. L., Felson. M.. (1979). “Social Change and Crime Rate Trends: A Routine Activity Approach.” *American Sociological Review*. Vol.44 No.4. pp. 588-608.

Conklin. J. E.. (1995). *Criminology.* (5th ed.). Massachusetts: Allyn and Bacon.

DeBrosse. J.. (2008). ID theft victim becomes pawn in dating scam. Retrieved April 4. 2009 from http://www.daytondailynews.com/n/content/oh/story/news/ local/2008/04 /06/ddn040608scammers.html

Dixon. R. (2005). *Nigerian Cyber Scammers*. Retrieved 5 April 2009. from http://www.latimes.com/technology/la-fgscammers20oct20.0.301315.story?page=1&coll=la-tot-promo

Edwards. M., Suarez-Tangil. G., Peersman. C., Stringhini. G.. Rashid. A.. & Whitty. M.. (2018). The Geography of Online Dating Fraud. IEEE S&P 2018.

Eleanor Rose. Z.. A Global Network of Scammers is Targeting Older People—Here’s How to Avoid Becoming a Victim. from vbv.scb.co.th/pam/pa.aspx

Ellis. B. and Symons. D.. (1990). Sex differences in sexual fantasy: An evolutionary psychological approach. *Journal of Sex Research*. 27 (4): 527 – 555.

ETDA and ThaiCERT. (2556). Digital Forensics. (20 July 2562). from https://www. thaicert.or.th/papers/general/2013 /pa2013ge012.html

European Commission. (2019). *The Directive on security of network and information systems (NIS Directive).* From https://ec.europa.eu/digital-single-market/en /network-and-information-security-nis-directive.

FBI. (2017). *Romance Scams: "Online Imposters Break Hearts and Bank Accounts"*. from https://www.fbi. gov/news/stories/romance-scams

Fletcher. E.. (2019). *Romance scams rank number one on total reported losses*. from https://www.ftc.gov/news-events/blogs/data-spotlight/2019/02/romance-scams-rank-number-one-total-reported-lossesd

Hamsi, A. S., Bahry. Criminology F. D. S., Tobi, S. N. M.. & Masrom, M. (2015). Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors and Keys to the Problem. *Journal of Management Research*. 7(2), 169.

Helping People Affected by Scams: A Toolkit for Practitioners. (2010). Office of Fair Trading.

Internet Crime Complaint Center. (n.d). "Annual Reports 2011-2014 Internet Crime Report". From https://www.ic3.gov/default.aspx

Jakobsson. M. (Ed.). (2016). *Understanding social engineering based scams*. New York: Springer.

Kshetri. N.. (2010). "Simple Economics of Cybercrime and the Vicious Circle". *The Global Cybercrime Industry*. Berlin; Springer-Verlag.

La Rose. L.. (2011. October 6). Online romance scam can hurt hearts and wallets. *The Canadian Press*. Retrieved 5 March 2013. From http://www.thestar.com/life/ 2011/10/06/online_ romance_scams_can_hurt_hearts_and_wallets.html

LAKE. Z. and EFFRON. L.. (2019). *Woman says a man she met on Tinder swindled her out of $200K: 'He didn't just dump you. he never existed'*. *ABCNews* (13 พฤษภาคม 2562). form https://abcnews.go.com/US/woman-man-met-tinder-swindled-200k-didnt-dump/story?id= 62806053

Ludden. D.. (2018). *Does Using Social Media Make You Lonely?.* from Psychology Today: https://www.psychologytoday.com/intl/blog/ talking-apes/201801/does-using-social-media-make-you-lonely

Marcum. C. D.. (2011). “Adolescent Online Victimization and Constructs of Routine Activities Theory.” In K. Jaishankar (Eds). *Cyber Criminology Exploring Internet Crimes and Criminal Behavior*. Florida: CRC Press Taylor & Francis Group.

Mass-Marketing Fraud Working Group. (2010). *“Mass-Marketing Fraud: A Treat Assessment.”;* From www.ice.gov/doclib/cornerstone/pdf/immfa.pdf

Matthews. H.. (2018). *27 Online Dating Statistics & What They Mean for the Future of Dating.* From https://www.datingnews.com/industry-trends/online-dating-statistics-what-they-mean-for-future/

Pascual. A.. & Gue'guen. N.. (2005). Foot-in-the-door and door-in-the-face : A comparative meta-analytic study. *Psychological Reports.* 96. 122-128

Reauters. (2014). *US American targeted as Malaysia becomes Internet scam haven*. From http://www.thestar.com.my/News/Nation/2014/07/09/Internet-scam-US-women-Nigerians-Malaysia.

Rege. A. (2009). What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. *International Journal of Cyber Criminology*. 3(2).

Research Excellence Framework 2014. (2014) “Confronting online dating scams: working with police and the industry.” 36 Communication Cultural and Media Studies. University of Leicester.

Reyns. B. W., Henson. B., Fisher. B. S.. (2013). “Applying Cyberlifestyle-routine activities theory to cyberstalking victimization.” In Thomas J. Holt (Eds). *Cybercrime and Criminological Theory Fundamental Reading on Hacking. Piracy. Theft and Harassment*. San Diego: Cognella Inc.. pp. 105-119.

Shadel D. and Dudley. D.. AARP The Magazine. *“'Are You Real?' — Inside an Online Dating Scam”.* https://www.aarp.org/money/scams-fraud/info-2015/online-dating-scam.html

Snapshort of romance scam. from https://www.police.gov.hk/info/img/cpb/adcc /180 517_en.pdf

Tan. H. K.. & David. Y.. (2017). Preying on lonely hearts: A systematic deconstruction of an Internet romance scammer’s online lover persona. Journal of Modern Languages. 23(1). 28-40.

Telegraph. (2561). *Loneliness is felt most intensely by young people. study finds (and turning to Facebook doesn't help).* (3 February 2561). From https://www.telegraph.co.uk/news /2018/10/01/loneliness-felt-intensely-young-people-study-finds-turning-facebook/

The ACCC and Scamwatch. *"Dating & romance scam: Georgina's Facebook fiancé leaves her flat broke"*. From https://www.scamwatch.gov.au/get-help/real-life-stories/dating-romance-scam-georginas-facebook-fianc%C3%A9-leaves-her-flat-broke

Townsend. J.. (1993). Sexuality and partner selection: Sex differences among college students. *Ethology and Sociobiology*. 14 (5): 305 – 330.

UN Global Pulse. (1990). *PRIVACY AND DATA PROTECTION PRINCIPLES*. Form https://www.unglobalpulse.org /privacy-and-data-protection.

USDOJ (United States Department of Justice). (2005). United States of America v. Patrick M. Giblin. Retrieved April 4. 2009. from http://www.usdoj.gov/usao/nj/ press/files/pdffiles/SuperIndict.pdf

Verafin. (2017). *Romance Fraud Scams: Five Key Indicators and Strategies for Uncovering Victims*. from https://verafin. com/2017/07/romance-fraud-scams/

Victims lost £41 million to romance fraud in 2017. from https://www.actionfraud. police.uk/news/victims -lost-41-million-to-romance-fraud-in-2017

Whitty. M. T.. (2015). Anatomy of the online dating romance scam. *Security Journal*. *28*(4). 443-455.

Whitty. M. T.. (2015). Mass-marketing fraud: a growing concern. *IEEE Security & Privacy*. *13*(4). 84-87.

Yen, T. F., & Jakobsson, M.. (2016). Case study: Romance scams. In Understanding Social Engineering Based Scams (pp. 103-113). Springer. New York.

Zingerle, A., & Kronman, L.. (2013, October). *Humiliating Entertainment or Social Activism? Analyzing Scambaiting Strategies Against Online Advance Fee Fraud*. In 2013 International Conference on Cyberworlds (pp. 352-355). IEEE.

การสัมภาษณ์

เจ้าหน้าที่คดีพิเศษ. (2562). กองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ. (18 มกราคม 2562). สัมภาษณ์.

เจ้าหน้าที่ตำรวจ. (2562). โฆษกกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี. (4 เมษายน 2562). สัมภาษณ์.

เจ้าหน้าที่ตำรวจ. (2562). ผู้กำกับสอบสวน กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี. (18 มกราคม 2562). สัมภาษณ์.

นักวิชาการ. (2562). อาจารย์ประจำ ภาควิชาสังคมและสุขภาพ คณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล. (15 พฤษภาคม 2562). สัมภาษณ์.

นักวิชาการ. (2562). อาจารย์ประจำ สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช. (11 มิถุนายน 2562). สัมภาษณ์.

นักวิชาการ. (2562). อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. (17 มกราคม 2562). สัมภาษณ์.

นักวิชาการ. (2562). อาจารย์ประจำภาควิชาสังคมวิทยาและมานุษยวิทยา จุฬาลงกรณ์มหาวิทยาลัย. (14 กุมภาพันธ์ 2562). สัมภาษณ์.

นักวิทยาศาสตร์ (สบ1). (2562). ศูนย์พิสูจน์หลักฐาน 5. (11 เมษายน 2562). สัมภาษณ์.

ผู้ดูแลเพจ. (2562). เพจภัยผู้หญิง ในโลกออนไลน์. (17 มกราคม 2562). สัมภาษณ์.

ผู้พิพากษา. (2562). ผู้พิพากษาศาลจังหวัดเชียงใหม่. (7 เมษายน 2562). สัมภาษณ์.

ผู้พิพากษา. (2562). ผู้พิพากษาศาลชั้นต้นประจำสำนักประธานศาลฎีกา. (16 มกราคม 2562). สัมภาษณ์.

ผู้พิพากษา. (2562). ผู้พิพากษาหัวหน้าศาลประจำสำนักประธานศาลฎีกา. (16 มกราคม 2562). สัมภาษณ์.

ผู้ไม่ประสงค์ออกนาม. (2562). ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม. (30 เมษายน 2562). สัมภาษณ์.

ผู้ไม่ประสงค์ออกนาม. (2562). ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม. (7 เมษายน 2562). สัมภาษณ์.

พนักงานสอบสวน. (2562). สถานีตำรวจแห่งหนึ่งในจังหวัดเชียงใหม่. (30 เมษายน 2562). สัมภาษณ์.

พนักงานอัยการ. (2562). อัยการจังหวัดประจำสำนักงานอัยการสูงสุด. (16 มกราคม 2562). สัมภาษณ์.

อดีตรองอธิบดีกรมสอบสวนคดีพิเศษ. (2562). กรมสอบสวนคดีพิเศษ. (13 มิถุนายน 2562). สัมภาษณ์.

กฎหมายที่เกี่ยวข้อง

1. ประมวลกฎหมายอาญา
2. ประมวลกฎหมายวิธีพิจารณาความอาญา
3. พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547
4. พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556
5. พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542
6. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560