


รายงานวิจัยฉบับสมบูรณ์

เสียงของผู้เสียหายจากอาชญากรรมออนไลน์สู่ข้อเสนอแนะในการรับมือและสร้างการรู้เท่าทัน

FROM CYBER CRIME SUFFERERS' VOICE TO RECOMMENDATIONS

โดย

ผู้ช่วยศาสตราจารย์ ดร.เจษฎา ศาลาทอง

อาจารย์วิษชญะ ศิลาน้อย

จันทร์สินี แก่นแก้ว

เสาวภาคย์ รัตนพงศ์

กันยายน 2567

รายงานนี้เป็นส่วนหนึ่งของ โครงการศึกษาสถานการณ์ภัยคุกคามทางออนไลน์

ดำเนินการโดย คณะเศรษฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ภายใต้การสนับสนุนของ สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ (สสส.)

บทสรุปผู้บริหาร

ปัญหาอาชญากรรมออนไลน์ในประเทศไทยมีแนวโน้มสูงขึ้นอย่างต่อเนื่อง โดยเฉพาะในช่วงปี 2565-2567 ที่จำนวนคดีและมูลค่าความเสียหายเพิ่มขึ้นอย่างมีนัยสำคัญ ความรุนแรงและการเติบโตอย่างรวดเร็วของการหลอกลวงออนไลน์ไม่เพียงจะสร้างความเสียหายและบอบช้ำในระดับบุคคล แต่ยังสร้างความสูญเสียอย่างมากต่อประเทศทั้งในเชิงเศรษฐกิจและสังคม งานวิจัยนี้จึงมุ่งเน้นศึกษาและทำความเข้าใจประสบการณ์ของผู้เสียหายจากอาชญากรรมออนไลน์ เพื่อนำไปสู่ข้อเสนอแนะเชิงนโยบายที่เป็นรูปธรรมในการสร้างการรู้เท่าทันการหลอกลวงออนไลน์และแนวทางในการรับมือกับภัยคุกคามทางออนไลน์ที่กำลังทวีความรุนแรงมากขึ้นในสังคมไทย

งานวิจัยชิ้นนี้ได้ทำการสัมภาษณ์เชิงลึกกลุ่มผู้เสียหายจากอาชญากรรมออนไลน์ ทั้ง 4 ประเภท ได้แก่ การหลอกขายสินค้าออนไลน์ การหลอกให้ลงทุน แก๊งคอลเซ็นเตอร์ และการหลอกให้รัก จำนวน 16 คน รวมถึงผู้เชี่ยวชาญจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง จำนวน 14 คน ได้แก่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) กรมสอบสวนคดีพิเศษ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) สมาคมธนาคารไทย สื่อมวลชน ศูนย์ชัวร์ก่อนแชร์ รายการสถานีประชาชน Thai PBS ผู้เชี่ยวชาญด้านจิตวิทยา และผู้เชี่ยวชาญด้านอาชญาวิทยา เพื่อนำข้อมูลที่ได้มาวิเคราะห์และสังเคราะห์

ผลการศึกษาพบว่า ปัจจัยสำคัญที่ทำให้ประชาชนตกเป็นผู้เสียหายของอาชญากรรมออนไลน์ มาจาก 2 ปัจจัยหลัก ได้แก่ 1) การตระหนักรู้ แต่ไม่ฉุกคิด (awareness) แม้ว่าในปัจจุบันประชาชนจะมีการรับรู้ข่าวสารของภัยออนไลน์มากขึ้น แต่ก็ยังไม่สามารถสร้างภูมิคุ้มกันได้ เนื่องจากรูปแบบการหลอกลวงมีการปรับเปลี่ยนอยู่ตลอดเวลา รวมถึงมิจฉาชีพมีการใช้เทคนิคทางจิตวิทยาเล่นกับความรู้สึกของผู้เสียหาย ได้แก่ ความโลภ ความกลัว ความเหงา ทำให้ยากต่อการตรวจสอบ 2) การป้องกันยังไม่เพียงพอ ประชาชนมีระดับการรักษาความปลอดภัยทางไซเบอร์ต่ำ (Poor cyber hygiene) ทำให้มิจฉาชีพใช้ช่องว่างมาโจมตีได้ง่ายและหลากหลายรูปแบบมากขึ้น

ในด้านผลกระทบอาชญากรรมออนไลน์ต่อผู้เสียหาย นอกจากความเสียหายด้านการเงินแล้ว ปัญหาอาชญากรรมออนไลน์ยังส่งผลกระทบต่อสภาพจิตใจของผู้เสียหาย เช่น ความเครียดและความวิตกกังวล และผู้เสียหายยังต้องเผชิญกับการถูกสังคมตีตราและซ้ำเติม ทำให้ผู้เสียหายไม่กล้าออกมาแจ้งความและเปิดเผยเรื่องของตนเอง

นอกจากนี้ งานวิจัยยังพบว่า ปัญหาสำคัญที่ทำให้การรับมือกับอาชญากรรมออนไลน์เป็นไปอย่างยากลำบาก คือ บทบาทและมาตรการของภาครัฐและหน่วยงานที่เกี่ยวข้องที่ยังไม่ครอบคลุมต่อการแก้ไขปัญหา ทั้ง การดำเนินงานล่าช้า ขาดความเป็นเอกภาพและการบูรณาการที่เหมาะสม ทำให้ไม่สามารถแลกเปลี่ยนความร่วมมือระหว่างกันได้ ส่งผลให้การช่วยเหลือผู้เสียหายเป็นไปได้ยากและไม่ทันท่วงที ทำให้ประชาชนขาดความเชื่อมั่นต่อระบบภาครัฐ

จากปัญหาและข้อจำกัดต่าง ๆ ที่เกิดขึ้น คณะผู้วิจัยได้นำเสนอข้อเสนอแนะเชิงนโยบายต่อหน่วยงานที่เกี่ยวข้อง เพื่อใช้เป็นแนวทางในการปรับปรุงและพัฒนากระบวนการทำงานให้มีประสิทธิภาพมากยิ่งขึ้น เพื่อที่จะสามารถจัดการกับภัยคุกคามทางออนไลน์ที่ทวีความรุนแรงมากขึ้นในปัจจุบันและอนาคตได้อย่างทันท่วงที

ข้อเสนอแนะเชิงนโยบายที่สำคัญ ได้แก่

- การสร้างความตระหนักรู้และให้ความรู้แก่ประชาชนเกี่ยวกับภัยออนไลน์อย่างต่อเนื่อง โดยใช้ช่องทางการสื่อสารที่หลากหลายและเข้าถึงง่าย รวมถึงจัดทำหลักสูตรการฝึกอบรมให้ความรู้แก่ประชาชนในลักษณะเชิงรุก
- พัฒนาแอปพลิเคชันในลักษณะสำหรับการเตือนภัย อาจนำมาประยุกต์และพัฒนาเป็นแอปพลิเคชันเตือนภัยที่รวบรวมข้อมูลสำคัญเกี่ยวกับอาชญากรรมออนไลน์และช่องทางการร้องเรียน ซึ่งประชาชนสามารถใช้งานได้อย่างครบวงจร (one-stop service)
- การพัฒนากฎหมายและกฎระเบียบที่เกี่ยวข้องกับอาชญากรรมออนไลน์ ให้มีความทันสมัยและครอบคลุมภัยคุกคามรูปแบบใหม่ ๆ
- การเสริมสร้างความเข้มแข็งให้กับหน่วยงานที่รับผิดชอบในการป้องกันและปราบปรามอาชญากรรมออนไลน์ ทั้งในด้านบุคลากร งบประมาณ และเทคโนโลยี
- ผสานความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาสังคม ในการแก้ไขปัญหาอาชญากรรมออนไลน์
- การจัดให้มีระบบการช่วยเหลือและเยียวยาผู้เสียหายจากอาชญากรรมออนไลน์ ทั้งทางด้านกฎหมาย การเงิน และจิตใจ

โดยสรุปแล้ว รายงานวิจัยนี้ได้สะท้อนให้เห็นถึงความรุนแรงและซับซ้อนของปัญหาอาชญากรรมออนไลน์ในประเทศไทย ตลอดจนผลกระทบที่ร้ายแรงต่อผู้เสียหายทั้งทางด้านการเงินและจิตใจ ข้อเสนอแนะเชิงนโยบายที่นำเสนอในงานวิจัยนี้ หวังเป็นอย่างยิ่งว่าจะเป็นประโยชน์ต่อการกำหนดนโยบายและมาตรการในการ

ป้องกันและปราบปรามอาชญากรรมออนไลน์ของประเทศไทยให้มีประสิทธิภาพมากยิ่งขึ้น เพื่อคุ้มครองประชาชนจากภัยคุกคามทางออนไลน์และสร้างสังคมดิจิทัลที่ปลอดภัย

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อถอดบทเรียนจากผู้เสียหายจากอาชญากรรมออนไลน์และผู้เชี่ยวชาญ เพื่อนำไปสู่ข้อเสนอแนะในการรับมือและสร้างการรู้เท่าทันภัยคุกคามทางออนไลน์ โดยมุ่งเน้นศึกษาอาชญากรรมออนไลน์ 4 ประเภท ได้แก่ การหลอกขายสินค้าออนไลน์ การหลอกให้ลงทุน แก๊งคอลเซ็นเตอร์ และพิศวาสอาชญากรรม (Romance Scam) โดยงานวิจัยนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative research) เก็บรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึก (In-depth interview) และการสัมภาษณ์แบบกลุ่ม (Focus group) จาก 2 กลุ่ม ได้แก่ กลุ่มผู้เสียหายจากอาชญากรรมทางออนไลน์ 4 ประเภท จำนวน 16 คน และกลุ่มผู้เชี่ยวชาญจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง จำนวน 14 คน

ผลการศึกษาพบว่า ปัจจัยสำคัญที่ทำให้ประชาชนตกเป็นผู้เสียหายของอาชญากรรมออนไลน์ มาจาก 2 ปัจจัยหลัก ได้แก่ 1) การตระหนักรู้ แต่ไม่ฉุกคิด (awareness) แม้ว่าในปัจจุบันประชาชนจะมีการรับรู้ข่าวสารของภัยออนไลน์มากขึ้น แต่ก็ยังไม่สามารถสร้างภูมิคุ้มกันได้ เนื่องจากรูปแบบการหลอกลวงมีการปรับเปลี่ยนอยู่ตลอดเวลา รวมถึงมิจฉาชีพมีการใช้เทคนิคทางจิตวิทยาเล่นกับความรู้สึกของผู้เสียหาย ได้แก่ ความโลภ ความกลัว ความเหงา ทำให้ยากต่อการตรวจสอบ 2) การป้องกันยังไม่เพียงพอ ประชาชนมีระดับการรักษาความปลอดภัยทางไซเบอร์ต่ำ (Poor cyber hygiene) ทำให้มิจฉาชีพใช้ช่องว่างมาโจมตีได้ง่ายและหลากหลายรูปแบบมากขึ้น

ความท้าทายในการรับมือกับปัญหาภัยคุกคามออนไลน์ พบว่า มาตรการในการรับมือและการช่วยเหลือของภาครัฐและหน่วยงานที่เกี่ยวข้องยังไม่เพียงพอ ขาดการบูรณาการที่เป็นรูปธรรม ส่งผลให้การช่วยเหลือผู้เสียหายเป็นไปได้ยากและไม่ทันท่วงที ทำให้ประชาชนขาดความเชื่อมั่นต่อระบบภาครัฐ และผู้เสียหายยังถูกตีตราจากสังคม

จากปัญหาและความท้าทายในการรับมือกับภัยออนไลน์ที่เกิดขึ้น คณะผู้วิจัยมีข้อเสนอแนะต่อการช่วยเหลือผู้เสียหายและการสร้างการรู้เท่าทัน 3 ระยะ ได้แก่ 1) การเตรียมพร้อม คือ การสร้างความตระหนักรู้และฉุกคิดให้กับประชาชนกลุ่มต่าง ๆ เกี่ยวกับภัยไซเบอร์ 2) การรับมือเมื่อถูกโจมตีจากภัยไซเบอร์ หน่วยงานต่าง ๆ ต้องมีความเชี่ยวชาญ มีเอกภาพและเข้าถึงได้ง่าย ไม่ซับซ้อนและรวดเร็ว และ 3) การฟื้นตัว ควรมีหน่วยงานที่ให้ความช่วยเหลือผู้เสียหายทั้งในด้านกฎหมาย การเงินและสุขภาพจิต และข้อเสนอแนะเชิงนโยบายต่อหน่วยงานที่เกี่ยวข้อง เพื่อนำไปสู่การแก้ปัญหาอย่างเป็นรูปธรรมและยั่งยืน ได้แก่ การผลักดันให้อาชญากรรมออนไลน์เป็นวาระแห่งชาติหรือวาระเร่งด่วน โดยให้อำนาจแก่ผู้ปฏิบัติงานตามกฎหมายอย่างจริงจัง จัดสรรจำนวนบุคลากรที่เพียงพอและมีทักษะสอดคล้องกับภาระงาน บูรณาการความร่วมมือกับ

หน่วยงานที่เกี่ยวข้อง จัดตั้งให้มีศูนย์กลางในการให้ข้อมูลที่ถูกต้อง ครบถ้วน เหมาะสม มีแอปพลิเคชันเตือนภัยและประชาสัมพันธ์ข้อมูล จัดทำหลักสูตรฝึกอบรมและให้ความรู้แก่ประชาชนในลักษณะเชิงรุก รณรงค์และส่งเสริมการป้องกันตนเองจากอาชญากรรมออนไลน์ให้ประชาชนทุกกลุ่ม

คำสำคัญ : อาชญากรรมออนไลน์, ภัยไซเบอร์, การหลอกลวงออนไลน์, การรู้เท่าทันสื่อ

สารบัญ

บทที่ 1
ความสำคัญ ที่มาของปัญหาที่ทำวิจัย และระเบียบวิธีวิจัย

ปัญหาอาชญากรรมออนไลน์ถือเป็นปัญหาใหญ่ในระดับสากลที่ทุกประเทศกำลังประสบ และก่อให้เกิดความเสียหายมากขึ้นในวงกว้าง ในประเทศไทยจากข้อมูลของสำนักงานตำรวจแห่งชาติพบว่า ปัจจุบัน คดีอาชญากรรมทางเทคโนโลยี มีแนวโน้มสูงขึ้น โดยตั้งแต่วันที่ 1 มีนาคม 2565 – 10 กุมภาพันธ์ 2567 ตำรวจได้รับการแจ้งความเกี่ยวกับการหลอกลวงออนไลน์แล้วกว่า 463,712 คดี มีมูลค่าความเสียหาย รวมแล้วกว่า 5.9 หมื่นล้านบาท (ประชาชาติธุรกิจ, 2567)

สำหรับกลโกงออนไลน์ที่มิจฉาชีพนิยมใช้มีทั้งหมด 18 รูปแบบ ได้แก่ หลอกขายสินค้าออนไลน์ หลอกให้ทำงานเสริมออนไลน์ เงินกู้ออนไลน์ คอลเซ็นเตอร์ หลอกลวงให้ลงทุนในรูปแบบต่าง ๆ หลอกให้รักแล้วลงทุน หลอกให้รักแล้วโอนเงิน ปลอมหรือแฮ็กบัญชี Line/Facebook แล้วมาหลอกยืมเงิน แชร์ลูกโซ่ การพนันออนไลน์ หลอกให้โหลดโปรแกรมควบคุมคอมพิวเตอร์ทางไกล เพื่อขโมยข้อมูลหรือถอนเงินจากบัญชี เหยื่อ ส่ง QR code หลอกให้โอนเงิน ฉ้อโกงรูปแบบอื่น ๆ โฆษณาเชิญชวนไปทำงานต่างประเทศ หลอกลวงให้ถ่ายภาพโป๊เปลือย เพื่อข่มขู่เรียกเงิน ยินยอมให้ผู้อื่นใช้บัญชีธนาคาร (บัญชีม้า) ข่าวปลอม และการเรียกค่าไถ่ทางคอมพิวเตอร์ (สำนักงานข้าราชการตำรวจ, ม.ป.ป.)

ทั้งนี้ การหลอกขายสินค้าเป็นภัยออนไลน์ที่มีการหลอกลวงมากที่สุด ขณะที่ การหลอกให้ลงทุนได้ก่อให้เกิดเสียหายมากที่สุด โดยคิดเป็นมูลค่ากว่า 2 หมื่นล้านบาท

สถิติของการหลอกลวงออนไลน์สูงสุด 15 อันดับ ได้แก่

1. หลอกลวงซื้อขายสินค้าหรือบริการไม่เป็นขบวนการ 181,565 เรื่อง คิดเป็น 41.94% ความเสียหาย 2,605,660,173 บาท
2. หลอกให้โอนเงินเพื่อทำงาน 55,624 เรื่อง คิดเป็น 12.85% ความเสียหาย 6,996,292,003 บาท
3. หลอกให้กู้เงิน 47,422 เรื่อง คิดเป็น 10.95% ความเสียหาย 2,156,248,393 บาท
4. หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ 36,318 เรื่อง คิดเป็น 8.39% ความเสียหาย 20,001,574,842 บาท
5. ข่มขู่ทางโทรศัพท์ (call center) 29,741 เรื่อง คิดเป็น 6.87% ความเสียหาย 7,546,200,539 บาท
6. หลอกเป็นบุคคลอื่นเพื่อยืมเงิน 17,248 เรื่อง คิดเป็น 3.98% ความเสียหาย 514,577,052 บาท
7. หลอกให้ติดตั้งโปรแกรมควบคุมระบบ 13,796 เรื่อง คิดเป็น 3.19% ความเสียหาย 1,931,459,338 บาท

8. หลอกให้โอนเงินเพื่อรับรางวัล 13,392 เรื่อง คิดเป็น 3.09% ความเสียหาย 1,125,954,045 บาท
9. หลอกลวงซื้อขายสินค้าหรือบริการเป็นขบวนการ 8,549 เรื่อง คิดเป็น 1.97% ความเสียหาย 69,985,581 บาท
10. กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ 4,130 เรื่อง คิดเป็น 0.95% ความเสียหาย 979,326,633 บาท
11. หลอกให้รักแล้วโอนเงิน (romance scam) 3,376 เรื่อง คิดเป็น 0.78% ความเสียหาย 1,173,620,700 บาท
12. หลอกให้ลงทุนตาม พระราชกำหนดกู้ยืมเงิน 3,218 เรื่อง คิดเป็น 0.74% ความเสียหาย 666,982,688 บาท
13. หลอกเกี่ยวกับสินทรัพย์ดิจิทัล 2,631 เรื่อง คิดเป็น 0.61% ความเสียหาย 3,159,574,945 บาท
14. เข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่น (ransomware) 150 เรื่อง คิดเป็น 0.03% ความเสียหาย 84,977,100 บาท
15. คดีออนไลน์อื่น ๆ รวมกัน 10,819 เรื่อง คิดเป็น 2.50% คิดเป็น 10,126,193,807 บาท (ประชาชาติธุรกิจ, 2567)

จากรายงานผลการปฏิบัติงานและสถิติการดำเนินคดีทางอาชญากรรมออนไลน์ในปี 2565 ซึ่งนำเสนอต่อที่ประชุมคณะกรรมการป้องกันปราบปรามและแก้ไขปัญหาอาชญากรรมทางออนไลน์ ที่จัดตั้งขึ้นเพื่อแก้ปัญหาอาชญากรรมออนไลน์อย่างบูรณา โดยประกอบไปด้วย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ กองบัญชาการตำรวจสืบสวนสอบสวนทางอาชญากรรมทางเทคโนโลยี (บช.สอท.) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กรมสอบสวนคดีพิเศษ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ธนาคารแห่งประเทศไทย สมาคมธนาคารไทย และกองบังคับการปราบปรามการค้ามนุษย์ นั้น พบว่า ในปีดังกล่าวได้จัดการกลุ่มอาชญากรรมออนไลน์ ดังต่อไปนี้

1. ดำเนินคดีแก๊ง call center ในต่างประเทศ 8 ครั้ง จับกุมผู้ต้องหา 166 คน
2. ปิดกั้นการโทรหลอกลวง/ข้อความ SMS จำนวน 118,530 หมายเลข
3. การอายัดบัญชีม้าจำนวน 58,463 บัญชี และปิดกลุ่มโซเชียลมีเดียซื้อขายบัญชีม้า จำนวน 8 กลุ่ม
4. การดำเนินคดีหลอกลวงลงทุน - ระดมทุน ออนไลน์และหลอกลวงทางการเงิน จำนวน 657 คดี จับกุมผู้ต้องหาจำนวน 673 ราย

5. การปราบพนันออนไลน์ โดยดำเนินคดี 318 คดี มีผู้ต้องหาจำนวน 461 ราย และปิดกั้นเว็บพนันจำนวน 1,830 เว็บ
6. การดำเนินคดีหลอกลวงซื้อขายสินค้าบริการออนไลน์ จำนวน 263 คดี และจับกุมผู้ต้องหาจำนวน 270 ราย (โพสต์ทูเดย์, 2566)

ขณะที่ ผู้สูงอายุมักตกเป็นเหยื่อของมิจฉาชีพได้ง่าย โดยเฉพาะเพศชายที่มีแนวโน้มถูกมิจฉาชีพหลอกมากกว่าเพศหญิง คนที่เพิ่งเริ่มเข้าสู่วัยเกษียณ (55-64 ปี) มีแนวโน้มเป็นเหยื่อมิจฉาชีพมากกว่าคนสูงอายุมาก ๆ ทั้งนี้คนที่ถูกมิจฉาชีพหลอก ส่วนใหญ่เป็นคนที่มีความรู้และรู้จักการใช้เทคโนโลยี (มนุษย์ต่างวัย, ม.ป.ป.) โดยช่องทางที่มิจฉาชีพในการหลอกลวงเหยื่อสูงอายุมากที่สุดคือ Facebook มากถึง 44% รองมาคือ Line คิดเป็น 31.25% และ Instagram คิดเป็น 5.25% (เดอะ แอคทีฟ นิวส์, 2566)

ด้วยความรุนแรงและการเติบโตอย่างรวดเร็วของการหลอกลวงออนไลน์ที่ไม่เป็นเพียงจะสร้างความเสียหายและบอบช้ำในระดับบุคคล แต่ยังสร้างความสูญเสียอย่างมากต่อประเทศทั้งในเชิงเศรษฐกิจและสังคม การถอดบทเรียนจากผู้ตกเป็นเหยื่อของการถูกหลอกลวงออนไลน์และผู้เชี่ยวชาญเพื่อนำไปสู่ข้อเสนอแนะต่อการรับมือของหน่วยงานที่มีส่วนเกี่ยวข้องในการรับมือและช่วยเหลือผู้ตกเป็นเหยื่อ รวมถึงการสร้างการรู้เท่าทันการหลอกลวงออนไลน์จึงมีความสำคัญอย่างยิ่ง

วัตถุประสงค์

ถอดบทเรียนจากผู้เสียหายจากอาชญากรรมออนไลน์และผู้เชี่ยวชาญเพื่อนำไปสู่

1. ข้อเสนอแนะต่อการรับมือของหน่วยงานที่มีส่วนเกี่ยวข้องในการรับมือและช่วยเหลือผู้เสียหาย
2. ข้อเสนอแนะต่อการสร้างการรู้เท่าทันการหลอกลวงออนไลน์

ขอบเขตการศึกษา

อาชญากรรมออนไลน์ที่งานวิจัยชิ้นนี้ศึกษาประกอบไปด้วย

1. การหลอกขายสินค้า
2. การหลอกให้ลงทุน
3. แก๊ง call center
4. พิศวาสอาชญากรรม (romance scam) หรือ การหลอกลวงรัก

ระเบียบวิธีวิจัย

งานวิจัยนี้เป็นการวิจัยเชิงคุณภาพประกอบไปด้วย 2 ส่วน

ส่วนที่ 1 เป็นการรวบรวมข้อมูลทุติยภูมิ (secondary data) โดยการวิจัยเอกสาร (documentary research) โดยรวบรวมและวิเคราะห์ข้อมูลจากเอกสารทางวิชาการ บทความ เอกสารราชการ วารสาร ตำรา สิ่งพิมพ์ รวมทั้งจากเว็บไซต์ และสื่อออนไลน์ที่เกี่ยวข้อง รวมถึงกรณีศึกษาในต่างประเทศ

ส่วนที่ 2 เป็นการเก็บข้อมูลปฐมภูมิ (primary data) จากการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้าง (semi-structured in-depth interview) ซึ่งจะทำให้การสัมภาษณ์มีเป้าหมายที่ชัดเจนแต่ก็ยังเปิดโอกาสให้ผู้วิจัยสามารถประเด็นใหม่ ๆ ที่อาจจะพบเจอระหว่างการสัมภาษณ์ได้ด้วย (Jamshed, 2014) และการสัมภาษณ์แบบกลุ่ม (focus group interview) โดยเลือกกลุ่มตัวอย่างแบบเจาะจง (purposive sampling) จะมีแหล่งข้อมูล จำนวน 30 คน ซึ่งจะมาจาก 2 กลุ่ม คือ ผู้เสียหายจากอาชญากรรมออนไลน์ จำนวน 16 คน โดยใช้วิธีการสัมภาษณ์เชิงลึก (in-depth interview) และการสัมภาษณ์แบบกลุ่ม (focus group interview) และกลุ่มของผู้เชี่ยวชาญจากหน่วยงานและองค์กรที่ จำนวน 14 คน ได้แก่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช) บช.สอท. กรมสอบสวนคดีพิเศษ กสทช. สมาคมธนาคารไทย สื่อมวลชน - ศูนย์ชัวร์ก่อนแชร์และรายการสถานีประชาชน Thai PBS ผู้เชี่ยวชาญด้านจิตวิทยา ผู้เชี่ยวชาญด้านอาชญาวิทยาโดยการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้าง ทั้งนี้ การสัมภาษณ์บุคคลทั้งหมดจะไม่เปิดเผยชื่อส่วนบุคคลแต่อย่างใด

กระบวนการวิจัยและขั้นตอนการดำเนินงาน

ระยะเวลาดำเนินการทั้งหมด 15 เดือน

- เดือนที่ 1-5 การรวบรวมและวิเคราะห์ข้อมูลเอกสาร ทั้งเอกสารทางวิชาการ บทความ เอกสารราชการ วารสาร ตำรา สิ่งพิมพ์ รวมทั้งจากเว็บไซต์และสื่อออนไลน์ที่เกี่ยวข้อง รวมถึงกรณีศึกษาในต่างประเทศ
- เดือนที่ 6-7 ขอพิจารณาจริยธรรมวิจัยในคน
- เดือนที่ 8-9 การเก็บข้อมูลโดยการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้าง (semi-structured in-depth interview) และการสัมภาษณ์แบบกลุ่ม (focus group interview) โดยเลือกกลุ่มตัวอย่างแบบเจาะจง (purposive sampling) จำนวน 30 คน ซึ่งจะมาจากกลุ่มเป้าหมาย 2 กลุ่ม ดังต่อไปนี้
    1. ผู้เสียหายจากอาชญากรรมออนไลน์ จำนวน 16 คน
    2. ผู้เชี่ยวชาญจากหน่วยงานหรือองค์กรที่เกี่ยวข้อง จำนวน 14 คน

ได้แก่ สกมช บช.สอท. กรมสอบสวนคดีพิเศษ กสทช. สมาคมธนาคารไทย สื่อมวลชน - ศูนย์ชัวร์ก่อนแชร์และรายการสถานีประชาชน Thai PBS ผู้เชี่ยวชาญด้านจิตวิทยา ผู้เชี่ยวชาญด้านอาชญาวิทยา

- เดือนที่ 10 วิเคราะห์ข้อมูลเบื้องต้น จัดทำรายงานความก้าวหน้าและนำเสนอเพื่อให้ผู้ทรงคุณวุฒิพิจารณา
- เดือนที่ 11 เก็บข้อมูลเพิ่มเติม จัดทำร่างรายงานวิจัยฉบับสมบูรณ์ และนำเสนอเพื่อให้ผู้ทรงคุณวุฒิพิจารณา
- เดือนที่ 12- 15 แก้ไขรายงานตามคำแนะนำของผู้ทรงคุณวุฒิ และจัดส่งรายงานวิจัยฉบับสมบูรณ์

เกณฑ์การคัดเลือกกลุ่มตัวอย่างในการเก็บข้อมูล

ในการวิจัยครั้งนี้จะเลือกกลุ่มตัวอย่างแบบเจาะจง (purposive sampling) โดยมีแหล่งข้อมูล จาก 2 กลุ่ม คือ ผู้เสียหายจากอาชญากรรมออนไลน์ จำนวน 16 คน โดยใช้วิธีการสัมภาษณ์แบบกลุ่ม (focus group interview) และกลุ่มผู้เชี่ยวชาญจากหน่วยงานที่เกี่ยวข้อง จำนวน 14 คน ใช้วิธีการสัมภาษณ์เชิงลึก (in-depth interview) ทั้งนี้ การสัมภาษณ์ทั้งสองกลุ่มจะไม่มีการเปิดเผยชื่อส่วนบุคคลแต่อย่างใด

กลุ่มผู้เสียหาย

ผู้วิจัยจะเลือกกลุ่มตัวอย่างแบบเจาะจง โดยจะต้องเป็นผู้เสียหายที่ได้รับความสูญเสียจากการถูกหลอกลวงทางออนไลน์ 4 ประเภท ได้แก่ การหลอกขายสินค้า การหลอกให้ลงทุน แก๊งคอลเซ็นเตอร์และการหลอกลวงให้รัก โดยเป็นตัวแทนจากทุกประเภท รวมทั้งสิ้น 16 คน

กลุ่มผู้เชี่ยวชาญจากหน่วยงานที่เกี่ยวข้อง

ผู้วิจัยจะเลือกกลุ่มตัวอย่างแบบเจาะจง โดยจะต้องเป็นตัวแทนจากหน่วยงานที่มีหน้าที่ในการกำกับดูแลและรับผิดชอบโดยตรง รวมถึงมีความรู้ ความเชี่ยวชาญในการรับมือกับปัญหาการหลอกลวงทางออนไลน์ รวมทั้งสิ้น 14 คน ได้แก่

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	2 คน
เจ้าหน้าที่ตำรวจทั่วไป	2 คน
เจ้าหน้าที่ตำรวจไซเบอร์	2 คน
ธนาคารเอกชน	1 คน
สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ	2 คน

ตัวแทนของสื่อและภาคประชาสังคม	2 คน
ผู้เชี่ยวชาญด้านจิตวิทยา	2 คน
ผู้เชี่ยวชาญอาชญาวิทยา	1 คน

รายละเอียดเกี่ยวกับวิธีการติดต่อและวิธีการเข้าถึง

ผู้มีส่วนร่วมในการวิจัย

ผู้วิจัยและผู้ช่วยวิจัยจะติดต่อและเข้าถึง ผู้มีส่วนร่วมในการวิจัย ตามรายละเอียดดังต่อไปนี้

1. กลุ่มผู้เสียหาย ติดต่อจากผู้เสียหายที่ติดต่อเข้ามาขอความช่วยเหลือผ่านทางศูนย์ชัวร์ก่อนแชร์ สำนักข่าวไทย หรือ ที่ปรากฏในสื่ออื่น ๆ รวมถึง การสุ่มตัวอย่างแบบอ้างอิงด้วยบุคคลและผู้เชี่ยวชาญ (snowball sampling)
2. กลุ่มผู้เชี่ยวชาญติดต่อผ่านต้นสังกัดโดยตรงหรือการสุ่มตัวอย่างแบบอ้างอิงด้วยบุคคลและผู้เชี่ยวชาญ (snowball sampling)

วิธีการพิทักษ์สิทธิ ป้องกันความเสี่ยง และรักษาความลับของกลุ่มตัวอย่าง/ผู้มีส่วนร่วมในการวิจัย

ข้อมูลที่ได้จากการสัมภาษณ์ ผู้วิจัยจะขออนุญาตบันทึกเสียงและถอดเทปบันทึกเสียง และจะดำเนินการทำลายข้อมูลตลอดจนข้อมูลอื่น ๆ ทั้งหมดที่เกี่ยวข้องกับผู้มีส่วนร่วมในการวิจัยภายหลังเสร็จสิ้นการวิจัย โดยการลบไฟล์ข้อมูลเสียงและไฟล์ข้อมูลอื่น ๆ ที่เกี่ยวข้องกับผู้มีส่วนร่วมในการวิจัยภายใน 1 สัปดาห์หลังส่งงานวิจัยฉบับสมบูรณ์

ในระหว่างการสัมภาษณ์ ในบางคำถามจะเกี่ยวข้องกับเหตุการณ์ที่ผู้มีส่วนร่วมในการวิจัยประสบและผลกระทบเกี่ยวกับตัวท่านที่เกิดขึ้น ซึ่งทำให้อาจรู้สึกอึดอัด หรืออาจรู้สึกไม่สบายใจอยู่บ้างกับบางคำถาม ผู้มีส่วนร่วมในการวิจัยมีสิทธิ์ที่จะไม่ตอบคำถามเหล่านั้นได้ รวมถึงมีสิทธิถอนตัวออกจากโครงการนี้เมื่อใดก็ได้ โดยไม่ต้องแจ้งให้ทราบล่วงหน้า และการไม่เข้าร่วมวิจัยหรือถอนตัวออกจากโครงการวิจัยนี้ จะไม่มีผลกระทบต่อผู้มีส่วนร่วมในการวิจัยแต่อย่างใด

ข้อมูลส่วนตัวของผู้มีส่วนร่วมในการวิจัยจะถูกเก็บรักษาไว้ ไม่เปิดเผยต่อสาธารณะเป็นรายบุคคล แต่จะรายงานผลการวิจัยเป็นภาพรวม ผู้ที่มีสิทธิ์เข้าถึงข้อมูลของท่านจะมีเฉพาะผู้ที่เกี่ยวข้องกับการวิจัยนี้ และคณะกรรมการจริยธรรมการวิจัยในคนเท่านั้น

บทที่ 2
การทบทวนวรรณกรรม

2.1 นิยามและประเภทของอาชญากรรมออนไลน์

2.1.1 การหลอกขายสินค้า

นิติธร แก้วโต (2563) กล่าวว่า การหลอกขายสินค้าเป็นพฤติการณ์ที่ผู้ขายมีเจตนาหลอกลวงผู้ซื้อ แบ่งเป็น 2 ลักษณะ คือ

1) การลวงขาย คือ กรณีที่ผู้ซื้อและผู้ขายตกลงซื้อขายสินค้ากัน และผู้ซื้อ “ได้รับสินค้า” แล้วแต่สินค้านั้นผู้ขายได้หลอกลวงด้วยการแสดงข้อความอันเท็จเกี่ยวกับ แหล่งกำเนิด สภาพ คุณภาพ หรือปริมาณแห่งสินค้า เช่น ผู้ขายอ้างว่า แหล่งกำเนิดของสินค้าอยู่ที่ประเทศอังกฤษ แต่สินค้าจริงผลิตที่ประเทศจีน สภาพหรือคุณภาพไม่เป็นไปตามที่ผู้ขายโฆษณาอวดอ้าง หรือปริมาณสินค้าไม่ครบตามจำนวนที่ผู้ขายโฆษณา เป็นต้น การลวงขาย เป็นความผิด ตามประมวลกฎหมายอาญา มาตรา 271 ผู้ใดขายของโดยหลอกลวงด้วยประการใด ๆ ให้ผู้ซื้อหลงเชื่อในแหล่งกำเนิด สภาพ คุณภาพ หรือปริมาณแห่งของนั้นอันเป็นเท็จถ้าการกระทำนั้นไม่เป็นความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ รวมทั้งพระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ.2522

มาตรา 22 ระบุว่า การโฆษณาจะต้องไม่ใช้ข้อความที่เป็นการไม่เป็นธรรมต่อผู้บริโภคหรือใช้ข้อความที่อาจก่อให้เกิดผลเสียต่อสังคมเป็นส่วนรวม ทั้งนี้ไม่ว่าข้อความดังกล่าวนั้นจะเป็นข้อความที่เกี่ยวกับแหล่งกำเนิด สภาพ คุณภาพ หรือลักษณะของสินค้าหรือบริการ ตลอดจนการส่งมอบ การจัดหา หรือการใช้สินค้าหรือบริการ

ข้อความดังต่อไปนี้ถือว่าเป็นข้อความที่เป็นการไม่เป็นธรรมต่อผู้บริโภค หรือเป็นข้อความที่อาจก่อให้เกิดผลเสียต่อสังคมเป็นส่วนรวม

(1) ข้อความที่เป็นเท็จหรือเกินความจริง

(2) ข้อความที่จะก่อให้เกิดความเข้าใจผิดในสาระสำคัญเกี่ยวกับสินค้าหรือบริการ ไม่ว่าจะกระทำโดยใช้หรืออ้างอิงรายงานทางวิชาการ สถิติ หรือสิ่งใดสิ่งหนึ่งอันไม่เป็นความจริงหรือเกินความจริงหรือไม่ก็ตาม

2) การฉ้อโกง คือ กรณีที่ผู้ซื้อ “ไม่ได้รับสินค้า” จากผู้ขายโดยผู้ขายไม่มีเจตนาจะขายสินค้าให้แก่ผู้ซื้อจริง ๆ หรือผู้ขายไม่มีสินค้าอยู่จริง การเสนอขายสินค้าเป็นเพียงขั้นตอนการหลอกลวงผู้ซื้อ เพื่อเอาเงินจากผู้ซื้อ หรือไม่มีสินค้าอยู่จริง แต่เอาภาพสินค้าของคนอื่นมาหลอกขาย โดยมีเจตนาหลอกลวง เพื่อเอาเงินจากผู้ซื้อ

มาตั้งแต่ต้น การฉ้อโกงเป็นความผิด ตามประมวลกฎหมายอาญา มาตรา 341 ระบุว่า ผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง และโดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สาม ทำ ถอน หรือทำลายเอกสารสิทธิ ผู้นั้นกระทำความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ทั้งนี้ ผู้กระทำความผิดจะต้องรับโทษหนักขึ้น หากเป็นการฉ้อโกงประชาชน ตามประมวลกฎหมายอาญา มาตรา 343 มีโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ นอกจากนี้ การฉ้อโกงหรือการฉ้อโกงประชาชน ยังเป็นการนำเข้าข้อมูลอันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ มาตรา 14 (1) มีโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท อีกส่วนหนึ่ง

2.1.2 การหลอกให้ลงทุน

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ม.ป.ป.) กล่าวว่า วิธีหนึ่งที่มิจฉาชีพใช้ในการหลอกลวงคือหลอกลงทุน เช่น แชร์ลูกโซ่ ชักชวนร่วมหุ้น เทรดหุ้นและ**FOREX** ที่เข้าข่ายแชร์ลูกโซ่ การทำกล่องสุ่ม ฯลฯ เนื่องจากการลงทุนเป็นเรื่องที่ทุกคนให้ความสนใจ เพราะมีโอกาสสร้างผลตอบแทนสูง สามารถสร้างอิสรภาพทางการเงินได้ การชักจูงด้วยผลตอบแทนที่ล่อตาล่อใจจึงทำให้คนตกหลุมพรางนั้นได้ง่าย โดยมีการชักชวน 5 รูปแบบที่กลโกงส่วนใหญ่มักใช้หลอกลวงหรือจูงใจ ได้แก่

1. ให้ผลตอบแทนสูงในเวลาอันสั้น ชวนเชื่อว่าจะได้ผลตอบแทนหรือกำไรจากการลงทุนจำนวนมากอย่างรวดเร็วและง่ายดาย และใช้ เทคนิค กระตุ้นด้วยรูปถ่ายคู่กับเงินก้อนโต หรือรถหรู สร้างความหวังว่าทุกคนเป็นเจ้าของได้ สะกิดต่อมความโลภ

2. การันตีผลตอบแทน บอกว่าจะได้ผลตอบแทนสูงเท่านั้นเท่านี้เป็นตัวเลขแน่นอน เช่น 10% - 15% ต่อสัปดาห์ หรือ 40% ต่อเดือน

3. เร่งรัดให้ตัดสินใจ โดยมักจะเสนอสิทธิพิเศษเฉพาะในช่วงเวลานั้น เช่น วันนี้วันเดียวเท่านั้น, เหลือเวลาแค่ 5 นาที หรือเหลือที่ไม่มากแล้ว เพื่อลดโอกาสในการไตร่ตรองของเรา

4. อ้างว่าใคร ๆ ก็ลงทุน ถ้าไม่รีบอาจพลาดตกขบวน หรืออ้างบุคคลที่มีชื่อเสียง เพื่อเพิ่มความน่าเชื่อถือในการลงทุน ถ้าไม่เข้าร่วมจะตกขบวนความร่ำรวย

5. ธุรกิจจับต้องไม่ได้ บอกว่าทำธุรกิจแต่ไม่เห็นสินค้า หรือชักชวนลงทุนในแพลตฟอร์มต่างประเทศที่ไม่ได้รับอนุญาต อ้างธุรกิจว่าได้รับการรับรอง แต่ไม่สามารถตรวจสอบธุรกิจได้

แชร์ลูกโซ่ เป็นกลโกงที่หลอกให้ประชาชนลงทุนหรือซื้อสินค้า โดยอ้างว่าจะได้รับกำไรจำนวนมากในเวลาอันรวดเร็ว มักจะจ่ายเงินให้จริงในระยะแรกเพื่อให้หลงเชื่อ ทั้งที่จริงแล้วไม่ได้ประกอบธุรกิจอะไรเลย

เพียงแค่นำเงินของผู้ที่ลงทุนทีหลังมาจ่ายให้กับผู้ที่ลงทุนก่อนเท่านั้น เมื่อถึงจุดที่ไม่สามารถหาสมาชิกใหม่ได้เพิ่มจนไม่สามารถจ่ายเงินได้ หรือได้เงินจำนวนมากเพียงพอแล้ว ก็จะหลบหนีไปสร้างความเสียหายให้แก่ประชาชนเป็นจำนวนมาก โดยแชร์ลูกโซ่ มักแอบอ้างสินค้าหรือบริการต่าง ๆ รวมทั้ง หุ้น คริปโต หรือสินทรัพย์ดิจิทัล ด้วย หากถูกชักชวนลงทุนต้องระมัดระวังให้มาก และควรลงทุนกับผู้ประกอบธุรกิจที่ได้รับอนุญาตเท่านั้น ลักษณะของการหลอกลวงที่อาจเข้าข่ายเป็นกลโกงแชร์ลูกโซ่ คือ

1. เน้นสร้างเครือข่ายมากกว่าขายของ

2. ให้ชักชวนคนร่วมจำนวนมาก

3. ได้โบนัสเพิ่ม ถ้าชวนคนมาเป็นสมาชิก เช่น ปกติได้ 10% ต่อสัปดาห์ ถ้าชวนคนได้เพิ่มจะได้อีก 5% ต่อสัปดาห์ เป็นต้น

2.1.3 แก๊งคอลเซ็นเตอร์

อาริยา สุขโต (2565) กล่าวว่า ภัยการหลอกลวงทางโทรศัพท์ มิจฉาชีพคอลเซ็นเตอร์ หรือแก๊งคอลเซ็นเตอร์ (Call center) เป็นอาชญากรรมทางเศรษฐกิจระหว่างประเทศรูปแบบหนึ่งในยุคดิจิทัล ซึ่งนอกจากจะก่อให้เกิดความเสียหายทางเศรษฐกิจต่อผู้ถูกหลอกลวง จำนวนมากแล้ว ยังก่อให้เกิดความเสียหายต่อเศรษฐกิจในภาพรวมระดับประเทศอีกด้วย ภัยคอลเซ็นเตอร์ถือได้ว่าเป็นอาชญากรรมทางเศรษฐกิจข้ามชาติที่เป็นภัยร้ายแรงและเฝ้าระวังในช่วงปีที่ผ่านมา โดยเฉพาะอย่างยิ่งในยุคปัจจุบันซึ่งเป็นยุคข้อมูลข่าวสารที่การติดต่อในรูปแบบดิจิทัลมีบทบาทมากขึ้นเรื่อย ๆ ตามรายงานจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศเปิดเผยว่า ประเทศไทยพบการใช้โทรศัพท์เพื่อหลอกลวงมากกว่า 6.4 ล้านครั้ง โดยเพิ่มขึ้นกว่าร้อยละ 270 จากปี 2563 และในไทยพบการส่งข้อความขนาดสั้นหรือเอสเอ็มเอส (SMS) หลอกลวงเพิ่มขึ้นถึงร้อยละ 57 และในปี 2564 ที่ผ่านมา มีผู้เสียหายเข้าแจ้งความกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) กว่า 1,600 คน มูลค่าความเสียหายสูงกว่า 1,000 ล้านบาท นับแต่เดือนมกราคมถึง 15 กุมภาพันธ์ 2565 เข้าแจ้งความแล้ว 129 คดี สถิติทางคดีดังกล่าวแสดงให้เห็นถึงแก๊งคอลเซ็นเตอร์ยังคงระบาดอย่างต่อเนื่อง สำหรับมูลเหตุจูงใจการกระทำผิด คือ รายได้ที่ได้รับจากการก่อเหตุมีมูลค่าเป็นจำนวนมหาศาล ในขณะที่บทลงโทษตามกฎหมายไม่มีความรุนแรง

แก๊งคอลเซ็นเตอร์เป็นกลุ่มมิจฉาชีพที่มีรูปแบบการทำงานเป็นขบวนการ มีการแบ่งหน้าที่ชัดเจน โดยการใช้ช่องทางความตื่นกลัว ความโลภ และการสร้างความสัมพันธ์อันดีกับผู้เสียหาย เกิดขึ้นครั้งแรกในไต้หวัน โดยในครั้งแรกนั้นไม่ได้ใช้คำว่าคอลเซ็นเตอร์ แต่ใช้คำว่า เอทีเอ็มเกม (ATM game) เนื่องจากเป็นการสร้างกล

โกงโดยการแอบอ้างแสดงตนเป็นผู้อื่น เพื่อหลอกลวงให้ผู้เสียหายหลงเชื่อทางโทรศัพท์แล้วให้ไปที่ตู้เอทีเอ็ม และให้ทำการโอนเงินแก่คนร้าย โดยมีรูปแบบที่ใช้ในการหลอกลวงผู้เสียหาย ใน 2 ลักษณะ คือ การหลอกลวงด้วยความโลภ เช่น การหลอกลวงผู้เสียหายว่าได้รับคืนภาษี ได้รับเงินจากการถูกรางวัล หรือได้รับเช็คคืนภาษี โดยอ้างว่าต้องจ่ายค่าบริการเบื้องต้นเพื่อเป็นค่าบริการและค่าธรรมเนียมต่าง ๆ เมื่อผู้เสียหายหลงเชื่อเพราะความโลภอยากได้เงินหรือทรัพย์สิน ก็จะโอนเงินเข้าบัญชีธนาคารของคนร้ายที่ได้เตรียมเปิดรองรับไว้ อีกรูปแบบ คือ การหลอกลวงด้วยความกลัว โดยหลอกลวงผู้เสียหายว่าเป็นหนี้ค่าโทรศัพท์ หนี้บัตรธนาคาร มีบัญชีธนาคารพัวพันกับยาเสพติด บัญชีธนาคารจะต้องถูกอายัดและถูกตรวจสอบโดยสำนักงานป้องกันและปราบปรามการฟอกเงิน เมื่อผู้เสียหายหลงเชื่อจะทำธุรกรรมทางการเงินตามที่กลุ่มคนร้ายแจ้ง ซึ่งในปัจจุบันส่วนใหญ่ลักษณะการหลอกลวงจะใช้วิธีทำให้ผู้เสียหายเกิดความกลัว

2.1.4 พิศวาสอาชญากรรม (romance scam) หรือ การหลอกลวงรัก

ทศพล ทรรศนกุลพันธ์ (2562) อธิบายว่า พิศวาสอาชญากรรม Romance scam” หมายถึงกระบวนการที่นักต้มตุ๋น (scammer) ใช้เทคนิคทางจิตวิทยาผ่านเครื่องมือทางเทคโนโลยีต่าง ๆ ในการหลอกลวงให้ผู้เสียหาย (Victim) หลงเชื่อจนกระทั่งยินยอมให้ทรัพย์สินที่นักต้มตุ๋นต้องการ พฤติกรรมการหลอกลวงของสแกมเมอร์มีพัฒนาการตามรูปแบบวิธีการสื่อสาร ปัจจุบันมักพบการหลอกลวงทางโซเชียลมีเดีย (Social media) เช่น เฟซบุ๊ก (Facebook), อินสตาแกรม (Instagram) ซึ่งเป็นช่องทางที่ถูกอาชญากรใช้มากที่สุด เนื่องจากมีผู้คนเข้าใช้งานเป็นจำนวนมาก อีกทั้งพฤติกรรมของผู้ใช้งานยังถูกเปิดเผยสู่สาธารณะได้ง่าย จึงทำให้อาชญากรสามารถเลือกเป้าหมายได้ไม่ยากนัก เช่น การสร้างโปรไฟล์ปลอม ขึ้นมาในโซเชียลมีเดียหรือเว็บไซต์หาคู่ โดยขโมยข้อมูลส่วนตัวของผู้อื่น แล้วนำมาดัดแปลงเป็นข้อมูลของตนเอง หรือสร้างข้อมูลเท็จขึ้นมาเองให้ดูสมจริงและน่าดึงดูดที่สุด โดยนักต้มตุ๋นมักจะมองหาเป้าหมายที่มีลักษณะขี้เหงาและอ่อนไหว ต้องการใครสักคนมาอยู่เคียงข้าง

2.2 กลยุทธ์การหลอกลวง

มีการใช้หลักการพื้นฐานทางจิตวิทยาร่วมกับการเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูล การวางแผนและการดำเนินขั้นตอนตามที่วางแผนไว้ เรียกว่า “วิศวกรรมสังคม” (Social engineering) โดยกระบวนการล่อลวงนี้สามารถแบ่งได้เป็นขั้นตอนหลัก 6 ขั้นตอน (ทศพล ทรรศนกุลพันธ์, 2562) ดังนี้

2.2.1 การปลอมโปรไฟล์

มีการสร้างโปรไฟล์ทั้งเพศชาย เพศหญิง และเพศทางเลือกด้วยการขโมยรูปภาพบุคคลอื่นที่มีลักษณะบุคลิกภาพดี หน้าตาดี และดูภูมิฐานจากโซเชียลมีเดียหรือเว็บเพจต่าง ๆ ส่วนใหญ่มักอ้างตัวเป็น “ฝรั่งผิวขาว” ที่

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

2.2.2 เลือกช่องทางในการหลอกล่อ

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

2.2.3 เลือกเป้าหมาย

หลักการเลือกเป้าหมาย คือ มองหา “คนขี้เหงา” ที่ต้องการหาเพื่อน/คู่ชีวิตในโลกออนไลน์ ต่อมาคือการประเมินศักยภาพทางการเงิน โดยสิ่งเหล่านี้จะถูกประเมินผ่านข้อมูลส่วนบุคคลที่แสดงในโซเชียลมีเดีย เช่น ชื่อ อายุ อาชีพ สถานะทางการเงิน สภาพคู่ครอง และวิถีการดำเนินชีวิต เป็นต้น รวมถึงการแชร์เรื่องราว/รูปภาพหรือการแสดงความคิดเห็นบนโลกออนไลน์ด้วย ดังนั้น ผู้ที่เผยแพร่ข้อมูลส่วนบุคคล หรือวิถีชีวิต (lifestyle) ในพื้นที่สาธารณะเป็นประจำ และหลงเชื่อที่จะตอบกลับข้อความจากคนแปลกหน้า ถือว่ามีความเสี่ยงในการตกเป็นเป้าหมายของนักหลอกลวงรัก (Romance scam) ได้ถึงร้อยละ 70

2.2.4 สร้างบทบาทเพื่อเข้าถึงเป้าหมาย

นักหลอกลวงรักจะสร้างความน่าเชื่อถือทางอาชีพด้วยวิธีการส่งภาพหนังสือเดินทาง หรือบัตรเจ้าหน้าที่/พนักงานที่ผ่านการตัดต่อภาพถ่ายและข้อมูลส่วนบุคคล ที่พบมากสุดคือ การแต่งกายด้วยเครื่องแบบทหาร วิศวกรสนาม ภาพถ่ายแท่นขุดเจาะน้ำมันกลางทะเล เว็บไซต์บริษัท/สถานที่ทำงาน ซึ่งล้วนแต่ถูกปลอมแปลงแล้วทั้งสิ้น เพื่อให้เป้าหมายตรวจสอบได้ว่าตนได้ทำงานอยู่ที่แห่งนั้นจริง

ลักษณะร่วมของการแสดงบทบาทของนักหลอกลวงรักคือการสานสัมพันธ์เชิงชู้สาวจนกลายเป็น “คนรักในอุดมคติ” เช่น การส่งข้อความทักทายและใช้คำพูดที่แสนหวาน ทำให้เป้าหมายรู้สึกว่าเป็นคนสำคัญ แสดงความเอาใจใส่ แสดงตัวว่ามีลักษณะของ “คนดี” เช่น การใช้คำพูดและสำนวนในแง่ดีที่จะสื่อนัยยะของการเป็นคนที่ซื่อสัตย์ จริงใจ และพึ่งพาได้ รวมถึงยอมรับข้อเสียและจุดบกพร่องของเป้าหมายได้ทุกอย่าง มีการสานสัมพันธ์อย่างรวบรัดและรวดเร็วตั้งแต่ 2-3 วัน หรือไม่ก็เป็นการอดทนยอมใช้เวลาเพื่อสานสัมพันธ์ไปเรื่อย ๆ จนกว่าเป้าหมายจะตกหลุมพราง บางครั้งยาวนานถึง 2 ปี โดยมีการส่งภาพถ่ายกิจกรรมระหว่างวัน วิถีชีวิต ให้เหมือนเป็นการสนทนาแบบคู่รัก และแสดงให้เห็นว่ามีตัวตนอยู่จริง

2.2.5 การสร้างสถานการณ์

เมื่อเป้าหมายให้ความสนิทสนมและไว้ใจแล้ว นักหลอกลวงรักจะสร้างสถานการณ์เรียกร้องความสงสาร ความเห็นใจ และความหวังว่าจะได้พบกัน เพื่อร้องขอเงินจากเป้าหมาย เริ่มตั้งแต่มีปัญหาทางการเงินเร่งด่วนจากสถานการณ์ฉุกเฉิน ชักชวนให้ร่วมลงทุนสร้างธุรกิจเพื่อใช้ชีวิตบั้นปลายร่วมกัน ส่งสิ่งของ/ทรัพย์สินมาให้แต่ติดปัญหาที่กรมศุลกากร สนามบิน หรือสถานีตำรวจ ต้องจ่ายเงินค่าธรรมเนียมเพื่อรับสิ่งของ/ทรัพย์สินเหล่านั้น การขอแต่งงาน และส่งทรัพย์สินของหมั้นมาให้ยังประเทศไทย แต่ถูกยึดทรัพย์สินต้องจ่ายค่าธรรมเนียมก่อนอาจมีทีมงานแสดงตัวว่าเป็นเจ้าหน้าที่ของรัฐโทรศัพท์มาแจ้งค่าธรรมเนียม และเกิดปัญหาฉุกเฉินระหว่างการเดินทางมาพบกันและต้องการใช้เงินด่วน

เทคนิคการร้องขอเงินหรือผลประโยชน์ มี 2 เทคนิคหลัก คือ 1. Foot in the door technique (FITD) เช่น ครั้งแรกนักหลอกลวงรักจะขอให้เป้าหมายโอนเงินจำนวนไม่มากนัก โดยอ้างว่าต้องใช้เงินด่วน ขอยืมเงินบางส่วน ซึ่งถ้าผู้เสียหายหลงเชื่อก็จะเริ่มขอเงินจำนวนมากขึ้นในครั้งต่อไปด้วยการอ้างสถานการณ์อื่น ๆ 2. Door in the face technique (DITF) เช่น นักหลอกลวงรักขอให้ผู้เสียหายโอนเงินจำนวนมาก เมื่อผู้เสียหายปฏิเสธว่าไม่มีเงินมากขนาดนั้น เขาก็ลดจำนวนเงินลง โดยอ้างเหตุผลว่าได้เงินมาบางส่วนแล้วและต้องการอีกแค่บางส่วนเท่านั้น ซึ่งถ้าผู้เสียหายยอมโอนเงินในครั้งแรกก็จะมีการขอครั้งต่อไปเรื่อย ๆ หรือบางครั้งก็หายตัวไปทันที

2.2.6 บรรลุภารกิจทางการเงิน

นักหลอกลวงรักจะร้องขอให้มีการโอนเงินจาก 3 ช่องทางหลัก ได้แก่

1) โอนเงินไปบัญชีธนาคารภายในประเทศไทย เป็นช่องทางที่จะถูกร้องขอบ่อยที่สุดถึงร้อยละ 90 ส่วนมากชื่อเจ้าของบัญชีเป็นชื่อคนไทย ซึ่งการโอนเงินนี้มักเกิดจากกรณีที่ผู้ร่วมขบวนการอ้างตัวว่าเป็นเจ้าหน้าที่ศุลกากร/เจ้าหน้าที่สนามบิน/เจ้าหน้าที่ส่งพัสดุ/เจ้าหน้าที่ของรัฐอื่น ๆ โทรศัพท์แจ้งเป้าหมายว่า “มีผู้ส่งพัสดุมูลค่ามหาศาลมาให้ ต้องจ่ายค่าธรรมเนียมเพื่อรับพัสดุดังกล่าว” และอีกกรณีที่พบได้คืออ้างว่าเป็นบัญชีของเพื่อนหรือคนกลางที่สามารถส่งเงินต่อไปยังต่างประเทศได้อย่างรวดเร็ว

2) โอนเงินไปต่างประเทศผ่านธนาคารหรือสถาบันทางการเงินระหว่างประเทศ ส่วนใหญ่ประเทศปลายทางคือ ไนจีเรียและมาเลเซีย โดยมักอ้างว่าเกิดเหตุฉุกเฉินระหว่างการติดต่อธุรกิจ หรือทำธุรกิจต่างประเทศ

3) มอบเงินด้วยตนเอง ด้วยเหตุผลว่าจะได้พบตัวจริงของคู่สนทนาจากออนไลน์ แต่เมื่อถึงเวลานัดหมายมักได้รับการปฏิเสธด้วยเหตุผลว่าโดนกักตัวในสนามบินเพราะพกทรัพย์สินและเงินสดมาเป็นจำนวนมาก จึงให้ตัวแทน (อ้างว่าเป็นเพื่อน นักการทูต เจ้าหน้าที่ศุลกากร) ถือทรัพย์สิน/เงินสดมาให้แทน และต้องจ่ายเงินเพื่อแลก

กับสิ่งของเหล่านั้น ผู้เสียหายหลายรายโดนหลอกซ้ำว่านักหลอกลวงรักถูกจับกุมในฐานะอาชญากร โดยมิจฉาชีพคนใหม่จะแสร้งว่าเป็นผู้มาช่วยเหลือให้อาชญากรหลุดพ้นคดี แต่จริง ๆ แล้วก็เป็นอาชญากรด้วยกันเอง ทำให้ผู้เสียหายติดกับดักวงจรของการหลอกลวงนี้ซ้ำไปซ้ำมาเรื่อย ๆ

2.3 แนวคิดเกี่ยวกับอาชญากรรม/ทฤษฎีอาชญาวิทยา

2.3.1 ความหมาย

สาวตรี สุขศรี (2560) อาชญากรรมไซเบอร์ หรืออาชญากรรมคอมพิวเตอร์ (computer crime) หมายถึง การกระทำใด ๆ ที่ฝ่าฝืนต่อบทบัญญัติแห่งกฎหมาย โดยผู้กระทำอาศัยความรู้ด้านเทคโนโลยีคอมพิวเตอร์ในการกระทำผิด ไม่ว่าลักษณะของการกระทำนั้นจะเป็นการใช้คอมพิวเตอร์เป็นเครื่องมือ หรือมีระบบหรือข้อมูลคอมพิวเตอร์เป็นเป้าหมาย ซึ่งจำเป็นต้องอาศัยบุคลากรที่มีความรู้ความสามารถทางเทคโนโลยีคอมพิวเตอร์เข้ามาดำเนินการกับผู้กระทำความผิด ตั้งแต่กระบวนการสืบสวนสอบสวน การฟ้องร้อง ตลอดจนการพิจารณาคดีเพื่อลงโทษ

2.3.2 สาเหตุการเกิดอาชญากรรม

Robert K. Merton (1938, อ้างถึงใน สาวตรี สุขศรี, 2560) นักสังคมวิทยาและอาชญาวิทยาชาวอเมริกัน ผู้พัฒนาทฤษฎีความกดดันทางสังคม (Strain theory) กล่าวว่า สาเหตุการเกิดอาชญากรรมจากปรากฏการณ์ความขัดแย้งที่เกิดขึ้นระหว่างความคาดหวังของสังคมกับความสามารถหรือโอกาสในการบรรลุสิ่งที่สังคมคาดหวัง หากบุคคลเกิดความผิดหวังหรือสิ้นหวัง เพราะไม่สามารถบรรลุสิ่งที่สังคมคาดหวัง หรือดำเนินการต่าง ๆ ตามค่านิยมของสังคมแล้ว จะเกิดพฤติกรรมเบี่ยงเบนจนนำไปสู่การประกอบอาชญากรรมในที่สุด ทฤษฎีนี้เรียกอีกชื่อหนึ่งว่า ทฤษฎีโอกาสถูกปิดกั้น (Blocked opportunity theory) ที่มองว่าโครงสร้างทางสังคมเป็นแรงกดดันให้บุคคลไม่สามารถประสบความสำเร็จตามแบบแผนของสังคมได้ไม่ว่าด้วยเหตุผลใด โดยเฉพาะการถูกเอารัดเอาเปรียบทางชนชั้น หรือถูกลิดรอนสิทธิต่าง ๆ จากระบบเศรษฐกิจ ทำให้อาชญากรมักเป็นคนชนชั้นล่าง (the lower class) ซึ่งถูกปิดกั้นโอกาสหรือถูกโครงสร้างทางสังคมเอาเปรียบ ส่วนพวกชนชั้นกลางและชนชั้นสูง (the middle and upper class) ไม่ค่อยกระทำความผิด เพราะมักจะไม่ประสบกับสภาวะดังกล่าว

2.3.3 แนวคิดเกี่ยวกับเหยื่ออาชญากรรม

ในช่วงต้นทศวรรษที่ 70 นักอาชญาวิทยาให้ความสนใจศึกษาพฤติกรรมของผู้เสียหายที่มีความเกี่ยวข้องกับสาเหตุการเกิดอาชญากรรม เรียกว่า “เหยื่อวิทยา (Victimology)” โดย Cohen และ Felson (1979, อ้างถึงใน

สาวตรี สุขศรี, 2560) ได้พัฒนาทฤษฎีกิจวัตรประจำวัน (Routine activities theory) ที่มีแนวคิดว่า การที่คนเรามีกิจวัตรประจำวัน หรือมีกิจกรรมที่กระทำบ่อยครั้งเป็นประจำสม่ำเสมอ จะเป็นการเปิดช่องให้อาชญากรที่คอยสังเกตอยู่สามารถวางแผนกระทำความผิดต่อบุคคลนั้นได้ สมมติฐานสำคัญคือ อาชญากรรมเกิดขึ้นได้เมื่อมีองค์ประกอบครบ 3 ประการ ได้แก่

1) บุคคลที่มีแนวโน้มหรือแรงจูงใจที่จะกระทำความผิด (Likely and motivated offenders)

2) เหยื่อหรือเป้าหมายที่เหมาะสม (Suitable target) อาจจำแนกได้ 3 ประเภท คือ คน สิ่งของ และสถานที่ โดยสิ่งใดที่เคยตกเป็นเหยื่อแล้ว สามารถตกเป็นเหยื่อซ้ำได้อีก

3) การขาดผู้พิทักษ์ที่มีประสิทธิภาพ หรือการไร้ความสามารถที่จะปกป้องตนเอง (Absence of a capable guardian) อาชญากรรมคอมพิวเตอร์ส่วนใหญ่มักเกิดขึ้นจากองค์ประกอบข้อนี้ เนื่องจากผู้ใช้งานคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อระบบอินเทอร์เน็ต โดยไม่มีมาตรการรักษาความปลอดภัยที่มีประสิทธิภาพและทันสมัย รวมทั้งคนที่มีวิถีชีวิตออนไลน์ (Online lifestyle) แบบขาดความระมัดระวัง เช่น การเปิดเผยภาพส่วนตัวหรือข้อมูลส่วนบุคคลให้แก่คนที่รู้จักกันในโลกออนไลน์ผ่านโปรแกรมสนทนา หรือการโพสต์สิ่งเหล่านั้นลงในโซเชียลมีเดีย ล้วนแต่สร้างแรงจูงใจในการกระทำผิดให้กับอาชญากรได้

งานศึกษาของ Reyns, Henson และ Fisher (2013, อ้างถึงใน สาวตรี สุขศรี, 2560) อธิบายว่า ผู้ใช้อินเทอร์เน็ตที่มีแนวโน้มจะกลายเป็นเป้าหมายของเหล่าอาชญากรมักจะขึ้นอยู่กับข้อมูลที่นำมาเปิดเผย ซึ่งโดยหลักจะประกอบด้วย 9 ประเภท ได้แก่ 1) การใช้ชื่อเต็ม (full name) 2) สถานะความสัมพันธ์ (relationship status) 3) รสนิยมทางเพศ (sexual orientation) 4) ID ในโปรแกรมสนทนา (Instant Messenger ID) 5) ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) 6) ที่อยู่ออนไลน์ของบริการอื่น ๆ ในโซเชียลเน็ตเวิร์กหรือบล็อก (addresses for other social network/blog sites) 7) สิ่งที่สนใจหรือกิจกรรมที่ชื่นชอบ (interests and/or activities) 8) รูปภาพตนเอง (photo of themselves) 9) วิดีโอตนเอง (video of themselves)

2.4 แนวคิดเกี่ยวกับอาชญากรรมไซเบอร์

นักอาชญาวิทยาในยุคหลังได้นำทฤษฎีความกดดันทางสังคม (Strain theory) ของ Robert K. Merton มาใช้ในการศึกษาอาชญากรรมคอมพิวเตอร์ เช่น “Internal hacker” คือ นักเจาะระบบคอมพิวเตอร์ที่เป็นคนในมักจะเป็น/เคยเป็นลูกจ้างหรือพนักงานขององค์กรที่ตกเป็นผู้เสียหาย เนื่องจากความกดดันที่ได้รับในขณะทำงานอยู่ภายในองค์กร ทั้งการกลั่นแกล้งจากเพื่อนร่วมงาน การถูกกดขี่หรือไม่ได้รับความเป็นธรรมจากนายจ้าง จนนำไปสู่พฤติกรรมการเจาะระบบคอมพิวเตอร์เพื่อโจมตี ทำลาย หรือขโมยข้อมูล อีกกรณีหนึ่งคือการกลั่นแกล้งออนไลน์ (Cyberbullying) ที่มักพบในกลุ่มเด็กและวัยรุ่น ซึ่งการล้อเลียน ด่าว่า หรือกลั่นแกล้งผู้อื่นด้วยวิธีการใด ๆ มีนัยของการแสดงให้สังคมเห็นว่า “ผู้กระทำมีอำนาจเหนือผู้ถูกกระทำ” ซึ่งวัยรุ่นที่มักมีความ

โกรธหรืออารมณ์ขุ่นมัวเมื่อต้องตกอยู่ภายใต้ความกดดันบางอย่าง อาจเกิดจากการที่ไม่สามารถบรรลุสิ่งที่สังคมหรือพ่อแม่ผู้ปกครองคาดหวังได้ จึงมักหาทางแสดงอำนาจเหนือผู้อื่น โดยเฉพาะคนที่อ่อนแอกว่า เพื่อลบล้างหรือเยียวยาความรู้สึกแย่ ๆ ของตนเอง (สาวตรี สุขศรี, 2560)

ขณะที่ K. Jaishankar (2008, อ้างถึงใน สาวตรี สุขศรี, 2560) นักอาชญาวิทยาชาวอินเดีย ได้เสนอทฤษฎีการเปลี่ยนพื้นที่ (Space transition theory) มีแนวคิดว่า โดยธรรมชาติของมนุษย์นั้นมักจะเปลี่ยนแปลงพฤติกรรมเมื่อมีการเคลื่อนย้ายหรือเปลี่ยนพื้นที่ ซึ่งพฤติกรรมที่แสดงออกมามีทั้งสอดคล้องและไม่สอดคล้องกันในระหว่าง 2 พื้นที่ สมมติฐานของการเกิดอาชญากรรมไซเบอร์ประกอบด้วยพฤติกรรมดังนี้

1) คนทั่วไปมักประเมินความเสี่ยงทางกฎหมายและทางสังคมของการกระทำความผิดในพื้นที่ทางกายภาพกับพื้นที่ในโลกไซเบอร์ ซึ่งโลกไซเบอร์ไม่มีคนคอยจับตาพวกเขา การกระทำความผิดจึงเกิดขึ้นง่ายกว่า

2) ความยืดหยุ่นจากการปิดบังตัวตนได้และการขาดปัจจัยในการป้องปราม เมื่อโลกไซเบอร์สร้างพื้นที่ที่ยากแก่การตรวจจับ จึงทำให้คนกล้าที่จะแสดงความรู้สึกอันไม่พึงประสงค์ เช่น กล้าล่วงละเมิดบุคคลอื่น

3) อาชญากรรมในโลกไซเบอร์มีแนวโน้มที่จะถูกกระทำในโลกทางกายภาพ ขณะเดียวกันอาชญากรรมในโลกทางกายภาพก็สามารถกระทำในโลกไซเบอร์ เช่น ผู้ที่มีพฤติกรรมชอบล่วงละเมิดทางเพศเด็กและเยาวชนในโลกกายภาพ ก็มักเป็นผู้เผยแพร่สื่อลามกอนาจารเด็กในเครือข่ายอินเทอร์เน็ตด้วย

4) โลกไซเบอร์มีลักษณะไหลลื่น ไม่หยุดนิ่ง (Dynamic) ซึ่งอาจจะเป็นการเปิดช่องทางให้ผู้กระทำผิดหลบหนีได้ เนื่องจากมนุษย์ไม่ได้ใช้ชีวิตอยู่บนโลกไซเบอร์ตลอดเวลา แต่เป็นเพียงพื้นที่ที่ผู้คนสามารถแวะเข้ามาทำกิจกรรมและออกไปได้ เนื้อหาที่ถูกโพสต์สามารถเผยแพร่ได้อย่างรวดเร็ว ส่งผลให้การสืบหาต้นตอของแหล่งข้อมูลทำได้ยากด้วยเช่นกัน

5) เกิดการรวมกลุ่มในโลกไซเบอร์ได้ง่าย เนื่องจากอินเทอร์เน็ตเป็นพื้นที่สื่อกลางที่มีประสิทธิภาพในการหาพรรคพวก อีกทั้งอัลกอริทึม (Algorithm) มักจะแสดงเนื้อหาที่ผู้ใช้งานสนใจขึ้นมาตลอดเวลา ทำให้การที่จะสร้างสมาคมหรือกลุ่มคนที่มีความสนใจเหมือนกันก็ย่อมทำได้ง่ายกว่าการสร้างกลุ่มในโลกกายภาพ

6) ผู้คนที่อยู่ในสังคมปิด (Close societies) มีแนวโน้มที่จะประกอบอาชญากรรมในโลกไซเบอร์ได้ง่ายกว่าผู้ที่อยู่ในสังคมเปิด (Open societies) เช่น กลุ่มคนที่อยู่ในสังคมปิดจะไม่มีเสรีภาพเหมือนเช่นสังคมเปิด ประชาชนกลุ่มสังคมเปิดสามารถแสดงความคิดเห็นได้อย่างกว้างขวางและมีส่วนร่วมทางการเมืองได้ รวมทั้งมีแนวโน้มที่จะกระทำความผิดบนโลกออนไลน์น้อยกว่าคนที่ไม่สามารถแสดงออกได้ จึงไปปลดปล่อย ในพื้นที่ไซเบอร์แทน

7) ความขัดแย้งกันระหว่างมาตรฐานและคุณค่าของโลกกายภาพกับโลกไซเบอร์ นำไปสู่การเกิดอาชญากรรมไซเบอร์

2.5 สถานการณ์การหลอกลวงในไทยและต่างประเทศ

2.5.1 สถานการณ์การหลอกลวงทางออนไลน์ในประเทศไทย

จากรายงานประจำปี 2566 ของแอปพลิเคชัน Whoscall พบว่า คนไทยเสี่ยงโดนหลอกจากสายโทรศัพท์เข้าและข้อความ รวม 79 ล้านครั้ง เพิ่มขึ้นร้อยละ 18 จากยอดรวม 66.7 ล้านครั้ง ในปี 2565 โดยเป็นจำนวนสายโทรเข้า 20.8 ล้านครั้ง เพิ่มขึ้น ร้อยละ 22 จาก 17 ล้านครั้ง ในปี 2565 และข้อความหลอกลวงเพิ่มขึ้น ร้อยละ 17 สูงถึง 58.3 ล้านข้อความ จาก 49.7 ล้านข้อความ ในปี 2565

โดยเฉลี่ยคนไทย 1 คน ต้องรับ SMS ที่น่าสงสัย 20.3 ข้อความ ซึ่งมากที่สุดในเอเชีย โดยอันดับ 2 คือ ฟิลิปปินส์ จำนวน 19.3 ข้อความ และฮ่องกง จำนวน 16.2 ข้อความ โดยส่วนใหญ่เป็นเรื่องพนันออนไลน์และหลอกปล่อยเงินกู้ คีย์เวิร์ดสำคัญ อาทิ ยูสใหม่ แจกฟรี ฟรี 500 ฝากครั้งแรกรับ และสร้างการหลอกลวงใหม่ ๆ โดยแอบอ้างบริษัทขนส่ง และหน่วยงานรัฐ อาทิ พัสดุของท่านเสียหาย เคลมค่าเสียหาย จดตัวเลขมิเตอร์ผิดประกันมิเตอร์ (ชัวร์ก่อนแชร์, 2567)

ด้านมูลนิธิอาเซียน (2567) ได้เผยแพร่รายงานการประชุมในหัวข้อ ‘One Divide or Many Divides? Underprivileged ASEAN Communities’ Meaningful Digital Literacy and Response to Disinformation’ พบว่า รูปแบบข้อมูลหลอกลวงที่พบได้ในกลุ่มผู้ด้อยโอกาสในประเทศไทย ได้แก่ ประเด็นเรื่องสุขภาพ การหลอกลวงทางการเงิน สำหรับผู้สูงอายุ พบในประเด็นข้อมูลบิดเบือนเกี่ยวกับสุขภาพ การถูกหลอกจากการซื้อสินค้าทางออนไลน์ การหลอกลวงทางการเงิน และการขโมยข้อมูลส่วนบุคคล ส่วนกลุ่มเด็กและเยาวชน พบเกี่ยวกับการหลอกลวงทางการเงิน ได้แก่ รางวัลเงินดิจิทัล สินเชื่อ การกู้เงินนอกระบบ การลงทุน ข้อมูลสุขภาพที่ทำให้เข้าใจผิด เช่น ข้อเสนอการตรวจสุขภาพฟรี และการประกาศบริการภาครัฐที่เป็นเท็จ ซึ่งมักพบผ่าน SMS และสื่อสังคมออนไลน์

นอกจากนั้นในรายงานยังได้ศึกษาเกี่ยวกับการคุ้มครองความเป็นส่วนตัว โดยศึกษาใน 3 ปัจจัย พบว่า ปัจจัยด้านอายุ กลุ่มวัยรุ่นในประเทศไทยมีความสามารถและมีความตระหนักถึงการป้องกันความเป็นส่วนตัวถึงร้อยละ 80 แต่มีผู้สูงอายุเพียง ร้อยละ 7.5 เท่านั้นมีความตระหนักถึงความสำคัญ ปัจจัยด้านเพศ พบว่า กลุ่ม non-binary หรือกลุ่มที่ไม่ต้องระบุเพศ มีความตระหนักในระดับสูง ร้อยละ 100 ในการปกป้องความเป็นส่วนตัว ตามด้วยเพศชาย ร้อยละ 71.4 และเพศหญิง ร้อยละ 41.5 ปัจจัยด้านสุดท้าย คือ ภูมิหลังทางการศึกษา โดยผู้ที่สำเร็จการศึกษาจากโรงเรียนมัธยมศึกษาตอนต้นมีความตระหนักรู้ในการคุ้มครองความเป็นส่วนตัวในระดับที่สูงที่สุด ร้อยละ 71.6 ระดับชั้นมัธยมศึกษาตอนปลายมีความตระหนักรู้ในการคุ้มครองความเป็นส่วนตัว ร้อยละ 10.5 และคนที่จบการศึกษาระดับหาวิทยาลัย มีความตระหนักรู้ในการคุ้มครองความเป็นส่วนตัว ร้อยละ 16.7 แสดงให้เห็นว่าการมีการศึกษาระดับสูงไม่ได้รับประกันว่าบุคคลนั้นจะมีความตระหนักในการป้องกันความเป็นส่วนตัวในโลกออนไลน์

สอดคล้องกับดัชนีชี้วัด สุขภาวะดิจิทัล Thailand Cyber Wellness Index (TCWI) (2566) ที่จัดทำโดย บริษัท AIS ร่วมกับ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี และนักวิชาการทั้งด้านเทคโนโลยี ด้านสุขภาพ ด้านสื่อสารมวลชน ด้านการศึกษา และด้านการวัดประเมินผล ที่ได้ศึกษาพฤติกรรมการใช้งานดิจิทัลของคนไทย 7 ด้าน ได้แก่ ทักษะการใช้ดิจิทัล (Digital use) ทักษะการรู้เท่าทันดิจิทัล (Digital literacy) ทักษะด้านการสื่อสารและการทำงานร่วมกันบนดิจิทัล (Digital communication and collaboration) ทักษะด้านสิทธิทางดิจิทัล (Digital rights) ทักษะด้านความมั่นคงความปลอดภัยทางไซเบอร์ (Cyber security and safety) ทักษะด้านการกลั่นแกล้งทางไซเบอร์ (Cyberbullying) และ ทักษะด้านความสัมพันธ์ทางดิจิทัล (Digital relationship) พบว่า ภาพรวมของคนไทยมีสุขภาวะทางดิจิทัล อยู่ในระดับพื้นฐาน แต่ในขณะเดียวกันก็ยังมีถึงร้อยละ 44.04 ที่ยังอยู่ในระดับต้องพัฒนา แสดงให้เห็นว่าประเทศไทยจำเป็นต้องสร้างความรู้ความเข้าใจในการใช้ดิจิทัลให้กับประชาชนเพิ่มขึ้น

2.5.2 กรณีศึกษาปัญหาอาชญากรรมออนไลน์และการรับมือในต่างประเทศ

1) ระดับโลก

ความก้าวหน้าทางด้านเทคโนโลยีที่เป็นไปอย่างรวดเร็วในอีกทางหนึ่งก็เป็นปัจจัยสำคัญที่ทำให้ปัญหาอาชญากรรมออนไลน์มีเพิ่มมากขึ้นและกลายมาเป็นภัยคุกคามข้ามพรมแดน ที่มีความซับซ้อนและหลากหลายรูปแบบ ซึ่งจำเป็นอย่างยิ่งที่ต้องอาศัยความร่วมมือระหว่างรัฐและหน่วยงานที่เกี่ยวข้องจากภาคส่วนต่าง ๆ ในการช่วยกันหยุดยั้งปัญหาที่เกิดขึ้น

จากรายงานขององค์การตำรวจอาชญากรรมระหว่างประเทศ (International Criminal Police Organization: Interpol) หรือที่เรียกกันสั้น ๆ ว่า ตำรวจสากล (2022) พบว่า อาชญากรรมออนไลน์เป็น 1 ใน 5 อาชญากรรมที่เกิดขึ้นมากสุดในโลกโดยการโจมตีด้วยมัลแวร์เรียกค่าไถ่ (ransomware) การใช้อีเมลหรือเว็บไซต์ปลอมหรือที่เรียกว่าฟิชชิง (phishing) มิจฉาชีพออนไลน์ (online scams) และการเจาะระบบคอมพิวเตอร์ (computer intrusions) ถือเป็นภัยคุกคามในระดับที่รุนแรงหรือรุนแรงมากสุดในโลก ทั้งนี้ ความรุนแรงของอาชญากรรมออนไลน์ทั่วโลกมีแนวโน้มจะเพิ่มขึ้นและสร้างความเสียหายอย่างมหาศาล โดยคาดการณ์ว่าอาจสูงถึง 10.5 ล้านล้านเหรียญสหรัฐ ภายในปี 2568 (Xinhua, 2022)

เพื่อเร่งแก้ปัญหาที่เกิดขึ้น ตำรวจสากลได้ร่วมมือกับหน่วยงานต่าง ๆ ทั่วโลก ในการป้องกันการโจมตีทางไซเบอร์ รวมถึงการสร้างความตระหนักรู้ในภาคประชาชนเกี่ยวกับอาชญากรรมออนไลน์ผ่านทางสื่อช่องทางต่าง ๆ รวมถึงการสร้างแฮชแท็กต่าง ๆ เช่น #YouMayBeNext, #JustOneClick, #OnlineCrimeIsRealCrime หรือ #BECareful เพื่อรณรงค์ให้ประชาชนมีความระมัดระวังการจากถูกโจมตีทางออนไลน์ เป็นต้น

นอกจากนี้ ยังมีหน่วยงานอิสระและภาคประชาชนที่มีการผนึกกำลังกันเพื่อร่วมต้านภัยไซเบอร์ มีการสร้างเว็บไซต์เพื่อรับเรื่องร้องเรียนเกี่ยวกับปัญหาดังกล่าว ให้ความรู้ความเข้าใจเพื่อสร้างความตื่นตัวในเรื่องภัยออนไลน์ ให้กับประชาชน รวมถึงการคอยให้คำปรึกษากับประชาชนที่รับความเสียหายจากภัยดังกล่าว เว็บไซต์ที่คอยให้ความช่วยเหลือในเรื่องนี้ เช่น econsumer.gov หรือ globalantiscam เป็นต้น

2) ระดับภูมิภาค

การประชุมผู้นำอาเซียนในเดือนพฤษภาคม 2566 ณ ประเทศอินโดนีเซีย มีการประกาศความร่วมมือในการต่อสู้กับอาชญากรรมออนไลน์ที่กำลังแพร่ระบาดและสร้างความเสียหายให้กับภูมิภาค โดยผู้นำประเทศอาเซียน 10 ประเทศ ได้แสดงความกังวลเกี่ยวกับกลุ่มมิจฉาชีพที่มีการใช้โซเชียลมีเดียหรือช่องทางออนไลน์ต่าง ๆ ในการโจมตีและสร้างความเสียหายให้กับประชาชน ไม่เพียงเท่านั้น อาชญากรรมออนไลน์ที่เกิดขึ้นยังเชื่อมโยงกับปัญหาการค้ามนุษย์ในภูมิภาค เมื่อมีการหลอกหลวงคนเพื่อทำงานไปต่างประเทศ แต่สุดท้ายกลับถูกหลอกให้ทำงานให้แก๊งคอลเซ็นเตอร์ หรือหลอกหลวงคนอื่นแทน ในเวทีประชุมดังกล่าวได้มีการเห็นพ้องที่จะร่วมกันกำหนดมาตรการคุมเข้มทางพรมแดน การบังคับใช้ข้อกฎหมายรวมถึงการให้ความรู้แต่สาธารณชนในการต่อสู้กับอาชญากรรมออนไลน์ (Edna Tarigan, 2023)

จากรายงานของเว็บไซต์ (โนว์สแกม, 2566) พบว่า ในปี 2565 1 ใน 4 ของผู้บริโภคในเอเชียแปซิฟิก จะตกเป็นผู้เสียหายทางการหลอกลวงทางอินเทอร์เน็ต ขณะที่ ในทุก ๆ ปี มีคนกว่าหนึ่งพันคน หลงเชื่อ ‘ประกาศหางานปลอม’ โดยจะสูญเสียเงิน ถูกขโมยข้อมูลส่วนตัว รวมถึงไปพัวพันกับขบวนการค้ามนุษย์ นอกจากนี้ ยังมีงานวิจัยที่จัดทำขึ้นในภูมิภาคเอเชียตะวันออกเฉียงใต้ พบว่า 45% ของผู้ตอบแบบสอบถาม 1,618 คน ตกเป็นผู้เสียหายของมิจฉาชีพหลอกให้รักออนไลน์ ไม่เพียงเท่านั้น มีการตรวจจับการขโมยอัตลักษณ์กว่า 11 ล้านครั้ง อีกด้วย

ในรายงาน ยังพบว่า ประชาชนในประเทศอาเซียนยังได้รับความเสียหายจากมิจฉาชีพออนไลน์ในรูปแบบที่แตกต่างกัน โดยมูลค่าความเสียหายที่เกิดขึ้นมีมูลค่าที่สูงไม่ยิ่งหย่อนไปกว่ากัน ยกตัวอย่างเช่น ชาวมาเลเซียได้รับความเสียหายจากอาชญากรรมไซเบอร์สูงถึง 2.23 พันล้านริงกิต สืบเนื่องมาตั้งแต่ปี 2560 หรือ มีการบันทึกคดีหลอกลวงทางอินเตอร์เน็ตในประเทศฟิลิปปินส์ในช่วงเดือนมีนาคมถึงกันยายนปี 2563 มากถึง 869 คดี จากผู้เสียหายที่เป็นทั้งบุคคลธรรมดาและองค์กร เพิ่มขึ้น 37% เมื่อเทียบกับช่วงเวลาเดียวกันของปีก่อน โดยคดีที่เกิดขึ้นส่วนใหญ่ก่อให้เกิดความเสียหายโดยเฉลี่ยสูงถึง 100,000 เหรียญสหรัฐต่อธุรกิจ ซึ่ง 31% ของคดีหลอกลวงออนไลน์มีมูลค่าความเสียหายอยู่ระหว่าง 50,000-100,000 เหรียญสหรัฐ ขณะเดียวกัน ในปี 2564 เวียดนามมีสัดส่วนหลอกลวงทางอินเทอร์เน็ตสูงถึงมาก โดยคิดเป็น 0.89 คดีต่อ 1,000 คน โดยมีบันทึกรวมไว้ถึง 87,000 คดี โดยสร้างความเสียหายเฉลี่ย 4,200 เหรียญสหรัฐ เป็นต้น (โนว์สแกม, 2566)

ปัจจัยสำคัญที่ทำให้ปัญหาอาชญากรรมออนไลน์ทวีความรุนแรงและสร้างความเสียหายเพิ่มมากขึ้น คือจุดอ่อนเรื่องกฎหมาย เปิดโอกาสให้กลุ่มมิจฉาชีพเหล่านี้ทำงานได้ง่ายขึ้น โดยกลุ่มมิจฉาชีพจะมีการเคลื่อนไหวจากแหล่งหนึ่งไปยังจุดหนึ่งที่ที่มีการบังคับทางกฎหมายหรือการตรวจจับที่หละหลวม หรือในพื้นที่ที่มีความขัดแย้ง เช่น เมียนมา ที่มีการสู้รบระหว่างรัฐบาลทหารเมียนมากับกลุ่มผู้ต่อต้านรัฐบาลหรือชนกลุ่มน้อย เป็นต้น

Jeremy Douglas ผู้แทน U.N. Office on Drugs and Crime (Vitjitra Duangdee, 2022) เตือนว่า กลุ่มมิจฉาชีพออนไลน์เหล่านี้จะย้ายฐานการปฏิบัติการไปยังพื้นที่ในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่มีการบังคับกฎหมายที่ไม่เข้มงวด เว้นแต่รัฐบาลในกลุ่มประเทศอาเซียนจะร่วมมือกันในการจัดการกลุ่มมิจฉาชีพเหล่านี้ การรับมือกับปัญหานี้จำเป็นต้องมียุทธศาสตร์และเป็นความร่วมมือระหว่างภูมิภาค เนื่องจากวันนี้กลุ่มมิจฉาชีพอาจจะปฏิบัติการในกัมพูชา และเมื่อถูกรัฐบาลควบคุมอย่างเข้มงวด วันถัดมาก็อาจจะย้ายฐานไปยังเมียนมา สปป. ลาว หรือ ฟิลิปปินส์ เป็นต้น

จากรายงานของ VOA พบว่า เครือข่ายมิจฉาชีพได้สร้างโจมตีประชาชนในภูมิภาคและสร้างความเสียหายเป็นมูลค่าหลายล้านเหรียญสหรัฐ ด้วยการสร้างโปรไฟล์ปลอม การหลอกให้รัก หลอกให้ลงทุน โดยอ้างว่าจะสร้างผลตอบแทนสูง หรือปลอมเป็นเจ้าหน้าตำรวจเพื่อเรียกเก็บผลตอบแทน เป็นต้น โดยจีน ไต้หวัน เวียดนาม ไทย สหรัฐอเมริกา และออสเตรเลีย คือประเทศเป้าหมายของกลุ่มมิจฉาชีพเหล่านี้ (Vitjitra Duangdee, 2022)

2.5.3 ระดับประเทศ

1) สิงคโปร์

จากการรายงานของกองกำลังตำรวจของสิงคโปร์ (Singapore Police Force: SPF) พบว่าในปี 2565 มูลค่าความเสียหายในอาชญากรรมออนไลน์ในประเทศสูงถึง 660.7 ล้านเหรียญสิงคโปร์ ซึ่งเพิ่มขึ้นกว่า 4.5% จากปีก่อนหน้าที่อยู่ที่ 632 ล้านเหรียญสิงคโปร์ โดยผู้เสียหายส่วนใหญ่อยู่ในช่วงอายุ 20-39 ปี และโดนหลอกให้ทำงานมากที่สุด ทั้งนี้ คดีหลอกลวงและอาชญากรรมไซเบอร์เพิ่มขึ้นถึง 33,669 คดีในปี 2565 สูงกว่าปีก่อนหน้านี้ที่อยู่ที่ 26,886 คดี โดยการหลอกลวงคิดเป็น 94.2% ของคดีทั้งหมด ซึ่งคดีการหลอกลวงที่เจอมากสุด 5 อันดับคือ ฟิชชิง หลอกให้ทำงาน หลอกขายของออนไลน์ หลอกให้ลงทุนและโทรมาหลอกว่าเป็นเพื่อน (Davina Tham, 2023)

2) ญี่ปุ่น

ในปี 2565 คดีอาชญากรรมไซเบอร์ในญี่ปุ่นเพิ่มสูงขึ้นไปอยู่ที่ 12,369 คดี โดยส่วนใหญ่เป็นการโจมตีด้วยมัลแวร์เรียกค่าไถ่ ซึ่งส่วนใหญ่มันจะพบในบริษัทขนาดกลางและเล็ก มากกว่าที่จะเป็นบริษัทใหญ่

ทั้งนี้ ใน 12, 369 คดี เป็นคดีเกี่ยวกับการหลอกลวงถึง 3,304 คดี ขณะที่ 1,560 คดีเป็นเกี่ยวข้องกับการละเมิดกฎหมายโสเภณีเด็กและสื่อลามก และอีก 522 คดีเป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และเพื่อแก้ปัญหาที่เกิดขึ้น ได้มีการจัดหน่วยงานที่ทำหน้าที่ในเรื่องการสืบสวนและดำเนินคดีเฉพาะขึ้นในสำนักงานตำรวจแห่งชาติของญี่ปุ่น (Kyodo News, 2023)

2.6 แนวคิดเกี่ยวกับผู้เสียหายและการรู้เท่าทัน

2.6.1 แนวคิดเกี่ยวกับ Victim blaming

Victim blaming คือ การกล่าวโทษเหยื่ออาชญากรรม โดยที่เห็นได้ชัดเจนที่สุด คือกรณีของการถูกล่วงละเมิดทางเพศ ที่คนในสังคมรอบตัวผู้เสียหาย หรือในสื่อสังคมออนไลน์ มักตั้งคำถามไปในทางกล่าวโทษผู้เสียหาย แทนที่จะโทษผู้กระทำผิด เช่น ยั่วเขาหรือไม่ แต่งตัวไม่มิดชิดหรือไม่ เป็นต้น (นิตยสารปลูก, 2564) ยิ่งในโลกยุคดิจิทัล ที่คนเราสามารถแสดงความคิดเห็นได้อย่างเสรีผ่านสังคมออนไลน์ ความคิดเห็นลักษณะกล่าวโทษเหยื่อพบได้เป็นจำนวนมาก ซึ่งในทางกลับกัน หากมีโอกาสเผชิญหน้ากับเหยื่อตรง ๆ มีคนจำนวนมากที่ไม่กล้าเผชิญเช่นนั้น การมีสังคมออนไลน์จึงทำให้เราเห็นพฤติกรรม Victim blaming เด่นชัดขึ้นกว่าเดิม รวมถึง Victim blaming ยังสามารถนิยามไปถึงการกล่าวโทษเหยื่ออาชญากรรมทางการเงิน ซึ่งปัจจุบันถือว่าเป็นปัญหาใหญ่ที่สังคมกำลังถูกกระทำจากกลุ่มคนที่กระทำผิด และตามข่าวสังคมสื่อมวลชน จะพบว่ามีเหยื่อเกิดขึ้นจากการกระทำแบบนี้เป็นจำนวนมาก (สุภาวดี ไชยชะลอ, 2565)

นีล คริสตี นักอาชญาวิทยาชาวนอร์เวย์ ให้ความหมาย ‘เหยื่อในอุดมคติ’ (Ideal victim) ว่าเป็นบุคคลที่มีลักษณะทางบุคคลอ่อนแอ ไม่สามารถช่วยเหลือตัวเองได้ เช่น กลุ่มเปราะบาง มีอาชีพเป็นที่น่ายอมรับเคารพนับถือ หรือไม่อยู่ในที่ที่มีความเสี่ยงต่าง อธิบายเพิ่มเติมได้ว่า ไม่ใช่เพื่อระบุว่าคนกลุ่มนี้จะมีโอกาสเป็นเหยื่อมากกว่าคนกลุ่มอื่น ๆ แต่เพื่อทำความเข้าใจปฏิกิริยาสังคมต่อเหยื่อที่ถูกกระทำว่า เมื่อใดก็ตามที่เหยื่อมีลักษณะตรงกับเหยื่อในอุดมคติ สังคมมักไม่สงสัย ไม่ตั้งคำถาม แต่กลับรู้สึกว่าเป็นเรื่องที่ ‘หลีกเลี่ยงไม่ได้’ หรือเป็น ‘โชคร้าย’ ของเหยื่อ (สุภาวดี ไชยชะลอ, 2565) เพราะฉะนั้นการถูกหลวงลวงในรูปแบบต่าง ๆ โดยเฉพาะการหลอกลวงทำธุรกรรมทางการเงิน นำมาซึ่งความเสียหายทางทรัพย์สิน เหยื่อมักจะถูกหลอกลวงได้ง่าย และมักเป็นกลุ่มเหยื่อที่ได้กล่าวไปข้างต้น ทำให้การกล่าวโทษเหยื่อพบได้มาก โดยเฉพาะคนใกล้ตัวเหยื่อ ยกตัวอย่างประโยค เช่น หน้าที่การงานก็สูง ไม่น่าให้เขาหลอก, ไม่แปลกใจบ้างหรือ โอนเงินให้คนแปลกหน้าจำนวนมาก หรือ ทำไมไม่คิดให้ดี ๆ ก่อน เป็นต้น

2.6.2 Cyber hygiene

Cyber hygiene คือ แนวทางปฏิบัติเพื่อรักษาความปลอดภัยทางไซเบอร์เบื้องต้น หรือ สุขภาวะทางไซเบอร์/ดิจิทัล ซึ่งคำว่า Cyber hygiene ถูกพูดถึงแล้วหลายปีโดยเฉพาะอย่างยิ่งในแวดวงของคนในสายอาชีพไอที (Information technology) หลังจากที่เทคโนโลยีสารสนเทศ กลายมาเป็นเครื่องมือสำคัญต่อการขับเคลื่อนธุรกิจและองค์กรให้มีความก้าวหน้ารวดเร็ว รวมถึงการเปลี่ยนองค์กรต่างเข้าสู่สังคมดิจิทัล (Digital transformation) โดยอาจใช้คำว่า Digital hygiene ได้เช่นเดียวกัน มีความหมายเดียวกันนั่นเอง

การเปลี่ยนผ่านสู่สังคมดิจิทัล ธุรกิจและบริษัทมักพบเจอกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber threats) ที่มากขึ้น การรักษาความปลอดภัยจึงมีบทบาทสำคัญเป็นอย่างมาก และ Cyber hygiene ก็เป็นแนวทางที่สามารถจัดการกับความเสี่ยงที่อาจเกิดขึ้นเมื่อต้องใช้งานดิจิทัลต่าง ๆ

ประโยชน์ของ Cyber hygiene

การนำ Cyber hygiene มาปรับใช้สำหรับผู้ใช้งานทั่วไป สามารถช่วยลดความเสี่ยงจากภัยคุกคามต่าง ๆ เช่น

1) ทำให้บัญชีสื่อสังคมออนไลน์ และ บัญชีธนาคารปลอดภัยจากผู้ไม่หวังดี
2) ป้องกันการสูญเสียทรัพย์สิน
3) ทำให้ข้อมูลส่วนตัว เช่น รูปภาพ และ วิดิโอ ปลอดภัย
4) ป้องกันการเข้าถึงจากองค์กรธุรกิจที่ไม่พึงประสงค์
5) ป้องกันไม่ให้ผู้ไม่หวังดี เข้าถึงอุปกรณ์ส่วนตัวได้

แนวทางการปฏิบัติในการสร้าง Cyber hygiene สำหรับคนทั่วไป

1) การสร้างรหัสผ่านและการอัปเดตรหัสผ่าน - รหัสผ่านเป็นสิ่งสำคัญอันดับต้น ๆ สำหรับผู้ใช้งานอินเทอร์เน็ต เพราะเป็นเหมือนกำแพงด่านสุดท้ายระหว่าง โจร กับ ตัวเรา ดังนั้นการจัดการเกี่ยวกับรหัสผ่าน ถือเป็นทักษะขั้นพื้นฐานในการดูแลสุขภาวะทางไซเบอร์ ซึ่งมีแนวทางเบื้องต้น เช่น

- ตั้งรหัสผ่านให้ยากต่อการเดา เช่น ตั้งรหัสให้ประกอบด้วยตัวอักษรตัวใหญ่ ตัวเลข หรือเครื่องหมาย ควรคำนึงว่ารหัสผ่านที่ดี ต้องมีแค่คุณที่จำได้
- ไม่ตั้งรหัสที่สั้นเกินไป งานวิจัยพบว่า โปรแกรมคาดเดารหัสผ่านจะเริ่มเดาไม่ถูก เมื่อรหัสผ่านมีความยาว 12 ตัวอักษรขึ้นไป
- ไม่ควรใช้ข้อมูลส่วนตัว นำมาตั้งเป็นรหัสผ่าน เช่น ชื่อ นามสกุล ที่อยู่ วันเกิด เพราะข้อมูลเหล่านี้เป็นข้อมูลที่คาดได้ง่าย

- ไม่ควรใช้รหัสผ่านเดียวสำหรับหลายบัญชี ในกรณีที่ข้อมูลรหัสผ่านรั่วไหล นั่นอาจทำให้ทุกบัญชีใช้งานของเรา ก็จะถูกเข้าถึงไปพร้อม ๆ กัน

2) เปิดการใช้งาน การยืนยันตัวตนหลายขั้นตอน (Two-factor authentication (2FA) หรือ multi-factor authentication (MFA))

ในทุกการเข้าบัญชีนั้น ถึงแม้ว่าเราจะมีรหัสผ่านที่เดายากแค่ไหน แต่ก็อาจมีโอกาสที่จะถูกแฮกได้ ดังนั้นจึงต้องเปิดการยืนยันตัวตนของเราให้มากกว่าแค่การมีรหัสผ่าน ซึ่งจะทำให้บุคคลอื่นเข้าถึงบัญชีเรายากมากขึ้น โดยลักษณะการยืนยันตัวตนนี้ในชีวิตประจำวัน มีการใช้งานกันอยู่แล้ว เช่น One time password หรือ OTP เป็นต้น ซึ่งแม้ว่า OTP จะเป็นวิธีที่ปลอดภัยในระดับหนึ่งแล้ว แต่ก็ยังมีความเสี่ยง เพราะแฮกเกอร์ก็อาจจะเข้าถึง OTP ในอีเมล หรือ ข้อความโทรศัพท์ ของเราได้ ซึ่งในปัจจุบัน มีการใช้แอปพลิเคชัน ที่ช่วยสร้างรหัสผ่านแบบเฉพาะเวลา เพื่อยืนยันตัวตนผู้ใช้งาน

ตัวอย่างแอปพลิเคชันที่ให้บริการด้านการยืนยันตัวตนหลายขั้นตอน เช่น Google Authenticator, Authy และ Microsoft Authenticator เป็นต้น

3) ใช้งาน Anti-virus

สำหรับผู้ใช้งานคอมพิวเตอร์ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ถือเป็นเรื่องสำคัญ เพราะเป็นเหมือนการป้องกันด่านแรกของการถูกแฮกนั่นเอง โดยเมื่อมีโปรแกรมแล้ว ก็ควรตรวจสอบ สแกนเครื่องอย่างสม่ำเสมอ

4) สำรองข้อมูลอยู่เสมอ

การสำรองข้อมูลสามารถป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อถูกแฮก เพราะเป้าหมายของผู้ร้าย ส่วนหนึ่งคือการตัดการเข้าถึงข้อมูลสำคัญของเรา ดังนั้น ข้อมูลที่สำคัญมาก ๆ ควรสำรองไว้หลายแห่ง (ที่ปลอดภัย) เป็นต้น สำหรับระบบเครื่องแบบ MacOS ระบบสำรองข้อมูลคือ Time Machine และสำหรับ Window คือ File History การสำรองข้อมูลในปัจจุบันเปลี่ยนจากการสำรองในรูปแบบ offline อย่าง flash drive หรือ hard disk มาเป็นแบบ Cloud ซึ่งสะดวกและมีราคาที่ถูกลง และมีการการันตีจากผู้ให้บริการว่าปลอดภัย

5) อัปเดตระบบปฏิบัติการของอุปกรณ์อยู่เสมอ – นักพัฒนาระบบจะเพิ่มเติมการรักษาความปลอดภัยของระบบอยู่เสมอ ดังนั้น การอัปเดตเวอร์ชันล่าสุด ทำให้มีการป้องกันที่ทันสมัยนั่นเอง การปล่อยให้เครื่องคอมพิวเตอร์ของเรามีระบบการทำงานที่เก่า อาจมีความเสี่ยงที่จะรับมือกับการคุกคามที่ถูกสร้างขึ้นมาใหม่อยู่เรื่อย ๆ เป็นต้น

6) ลบข้อมูลส่วนตัวออกจากสื่อสังคมออนไลน์ - รายละเอียดเรื่องส่วนตัว เช่น วันเกิด ชื่อคน

ในครอบครัว เบอร์โทรศัพท์ และสถานที่เกิด หากมิจฉาชีพนำมาปะติดปะต่อรวมกัน นั่นอาจทำให้มีความเสี่ยงต่อการถูกติดตาม แบล็กเมล์ได้ ดังนั้นควรตั้งค่าความเป็นส่วนตัวและประเมินความเสี่ยงเสมอก่อนลงข้อมูลเหล่านั้น โดยเฉพาะอย่างยิ่ง บัตรประจำตัวประชาชน “ห้ามโพสต์ลงสื่อสังคม” เด็ดขาด

7) ลบข้อมูลให้หมดก่อนขาย หรือ ทิ้งอุปกรณ์ - เป็นเรื่องที่ใกล้ตัวมาก ๆ เพราะอุปกรณ์ทั้งหลายต่างมีอายุการใช้งานที่จำกัด และการซื้อขายก็เป็นเรื่องปกติที่มักทำกัน ดังนั้น ก่อนทิ้ง หรือ ส่งต่ออุปกรณ์ ควรทำให้แน่ใจว่า ข้อมูลของเราจะไม่ติดไปด้วย และไปอยู่ในมือคนอื่น ซึ่งมีความเสี่ยงอย่างมากต่อความปลอดภัย อาจเห็นได้จากกรณีศึกษาในอดีตหลายกรณี เช่น วิดีโอส่วนตัวหลุด จดเลขบัตรเครดิตไว้ในเครื่อง เป็นต้น

ความเสียหายที่อาจเกิดขึ้นจากการมี Cyber hygiene ต่ำ

1) ถูกนำไปใช้ในทางผิดกฎหมาย เช่น เลขบัตรประชาชน ถูกใช้ในการเปิดบัญชีปลอม หรือ “บัญชีม้า”

2) โดนโจรกรรมทางการเงิน เช่น ใช้บัตรเครดิตซื้อสินค้า หรือ โอนเงินออกจากบัญชี

3) ข้อมูลถูกนำไปทำการตลาด เช่น ทำให้ถูกรบกวนด้วยการโฆษณาขายสินค้าต่าง ๆ ทั้งรูปแบบโทรศัพท์และอีเมล์

4) ถูกปลอมแปลงตัวตน คือ ถูกนำไปใช้เพื่อปลอมเป็นเรา และทำการผิดกฎหมาย ส่งผลให้ตัวเรากลายเป็นผู้กระทำ

ทักษะ Cyber hygiene ยังสอดคล้องกับแนวทาง มาตรฐานสากล DQ (digital intelligence) ของ สภาเศรษฐกิจโลก (World Economic Forum : WEF) กล่าวคือ กลุ่มความสามารถทางสังคม อารมณ์ และการรับรู้ ที่จะทำให้คน ๆ หนึ่งสามารถเผชิญกับความท้าทายของชีวิตดิจิทัล และสามารถปรับตัวให้เข้ากับชีวิตดิจิทัลได้ ความฉลาดทางดิจิทัลครอบคลุมทั้งความรู้ ทักษะ ทัศนคติและค่านิยม ที่จำเป็นต่อการใช้ชีวิตในฐานะสมาชิกของโลกออนไลน์ กล่าวอีกนัยหนึ่งคือ ทักษะการใช้สื่อ และการเข้าสังคมในโลกออนไลน์ ซึ่งมีความมุ่งมั่นให้เด็ก ๆ ทุกประเทศได้รับการศึกษาด้านทักษะพลเมืองดิจิทัลที่มีคุณภาพและใช้ชีวิต บนโลกออนไลน์อย่างปลอดภัยด้วยความก้าวหน้าของเทคโนโลยีสมัยใหม่ แบ่งออกเป็น 8 ด้าน ดังนี้

1. การสร้างและรักษาอัตลักษณ์ในโลกดิจิทัล (Digital identity)
2. การใช้เครื่องมือและสื่อดิจิทัล (Digital use)
3. การอยู่ในโลกดิจิทัลอย่างปลอดภัย (Digital safety)
4. ความมั่นคงปลอดภัยในโลกดิจิทัล (Digital security)
5. ความฉลาดทางอารมณ์ในโลกดิจิทัล (Digital emotional intelligence)

6. การสื่อสารดิจิทัล (Digital communication)

7. การรู้เท่าทันสื่อดิจิทัล (Digital literacy)

8. การบริหารจัดการลิขสิทธิ์ (Digital rights)

2.6.3 การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital empathy)

Digital empathy หรือ ‘การเอาใจเขามาใส่ใจเราทางดิจิทัล’ มีความสำคัญอย่างมากในการอยู่ร่วมกันของคนในสังคมดิจิทัล สรานนท์ อินทนนท์ (2563) มองว่าการที่เราจะเป็นพลเมืองดิจิทัลได้นั้น นอกจากจะต้องมีการเรียนรู้เรื่องมารยาททางอินเทอร์เน็ต (Digital etiquette) แล้ว ทักษะการเอาใจเขามาใส่ใจเราทางดิจิทัลมีความจำเป็นอย่างมาก เนื่องจะช่วยให้เราสามารถใช้เทคโนโลยีได้อย่างมีจริยธรรม รู้จักการสื่อสารและมีปฏิสัมพันธ์กับผู้ใช้งานอื่นด้วยมารยาทอันดี รู้จักเอาใจเขามาใส่ใจเรา โดยเข้าอกเข้าใจ เห็นใจผู้ที่มีความแตกต่าง ไม่เพิกเฉยเมื่อเห็นผู้อื่นได้รับการปฏิบัติที่ไม่ถูกต้องในสังคม และมีส่วนร่วมในการสร้างสรรค์สังคมให้ดีขึ้น

หากพิจารณาจากคำว่า ‘การเอาใจเขามาใส่ใจเราทางดิจิทัล’ จะเห็นได้มา คำเหล่านี้มีพื้นฐานมาจากคำว่าการเอาใจเขามาใส่ใจเรา (Empathy) ซึ่งหมายถึง ศักยภาพของมนุษย์ในการที่จะแบ่งปันและเข้าอกเข้าใจความคิดและความรู้สึกของคนอื่น (Decety and Yoder, 2016) ด้าน Yonty Friesem (2016) มองว่าการเอาใจเขามาใส่ใจเราทางดิจิทัล คือ การขยายความของการเอาใจเขามาใส่ใจเราแบบดั้งเดิมมาไว้ในสังคมโลกดิจิทัล ซึ่งในอยู่ร่วมกันในสังคมดิจิทัลได้อย่างสงบสุขนั้นก็ทุกคนจำเป็นต้องมีทักษะในการเอาใจเขามาใส่ใจเราไม่แตกต่างไปการอยู่ร่วมกันในโลกชีวิตจริง เช่นเดียวกับที่ วรัชญ์ ครุจิต (2564, อ้างถึงในกองทุนพัฒนาสื่อปลอดภัยและสร้างสรรค์, 2564) กล่าวว่า การสื่อสารผ่านสื่อออนไลน์ทุกคนมีโอกาสกระทำความรุนแรงได้หมด เพราะความรู้สึกชั่ววูบ พิมพ์แล้วกดส่งเลย ถึงลบก็มีคนเห็น เป็นการพิมพ์ตามความรู้สึกโดยไม่ผ่านกระบวนการยับยั้งชั่งใจเพราะอยู่หน้าจอไม่เห็นหน้าตรง ๆ เลยมีความกล้าจะแสดงออกตามที่รู้สึก ซึ่งทางแก้เพื่อไม่ให้มีใครต้องเจ็บปวดจากสิ่งดังกล่าว คือต้องมีความเห็นอกเห็นใจในการสื่อสาร ต้องรู้เท่าทัน เริ่มจากมีสติ รู้ทันอารมณ์ตัวเอง ต้องยับยั้งชั่งใจก่อนจะพิมพ์ข้อความอะไรส่งไป

แม้โลกดิจิทัลจะทำให้คนเราสามารถใกล้ชิดกันมากขึ้น ทว่า ความเห็นอกเห็นใจที่มีให้กันในโลกออนไลน์กลับมีน้อยลง ผศ.ดร.ชนัญสรา อรนพ ณ อยุธยา (2564, อ้างถึงในกองทุนพัฒนาสื่อปลอดภัยและสร้างสรรค์, 2564) มองว่า สาเหตุมาจาก 1) สภาวะนิรนาม (anonymity) ที่เราทุกคนไม่เปิดเผยตัวตนในโลกออนไลน์ ทำให้มีอิสระในการแสดงตัวตนที่ไม่ใช่ตัวเรา 2) ข้อจำกัดเรื่องอวัจนภาษา ในโลกออนไลน์เราสื่อสารกันเป็นตัวอักษรเป็นหลัก ไม่สามารถรับส่งอวัจนภาษาได้ ทำให้ไม่เห็นสีหน้า แววตาหรือท่าทางและน้ำเสียงของคู่สนทนา ทำให้ยากต่อการคาดเดาความรู้สึกของกันและกัน ซึ่งเป็นสาเหตุที่ทำให้มีความเข้าใจผิดและทะเลาะกันได้ง่ายกว่าในโลกชีวิตจริง 3) ห้องแห่งเสียงสะท้อน (echo chamber) คือปรากฏการณ์การสื่อสารที่

ระบบอัลกอริทึมช่วยกรองและแสดงผลข้อมูลที่ตรงกับความสนใจของผู้ใช้งาน ซึ่งทำให้ผู้ใช้ตกอยู่ในฟองสบู่ของข้อมูล (filter bubble) ที่จำกัดโอกาสถึงข้อมูลอื่น ๆ ส่งผลกระทบในแง่การขาดความหลากหลายทางความคิดพร้อม ๆ กับการสร้างความสุดโต่งและไม่อดทนต่อความเห็นต่างในสังคม (Cappucoff Hopper, 2566)

อย่างไรก็ดี ทักษะการเห็นอกเห็นใจทางดิจิทัลนั้นสามารถสร้างได้ โดยการเคารพความเห็นที่แตกต่าง ไม่เอาอารมณ์เป็นที่ตั้งและใช้ภาษาที่สุภาพ ไม่ขู่คุกคามผู้อื่น ไม่เข้าถึงข้อมูลส่วนตัวของบุคคลอื่นโดยไม่จำเป็น ไม่กลั่นแกล้งกันในโลกออนไลน์ (cyberbullying) รวมถึง ไม่สร้างหรือส่งต่อข้อมูลที่เป็นเท็จ และควรมีการตรวจสอบข้อมูลที่รับมาก่อนทุกครั้ง เป็นต้น

เมื่อการพัฒนาด้านเทคโนโลยียังคงเป็นไปอย่างต่อเนื่อง การเอาใจเขามาใส่ใจเราทางดิจิทัลย่อมกลายมาเป็นสิ่งที่สำคัญที่ทุกฝ่ายจะต้องหันมาให้ความสนใจและร่วมกันสร้างความเห็นอกเห็นใจกันให้มีความมากขึ้น เพื่อส่งเสริมสังคมออนไลน์ที่สร้างสรรค์และสันติสุขให้เกิดขึ้น

2.6.4 วิศวกรรมสังคม (social engineering)

วิศวกรรมสังคม (social engineering) คือ การโจมตีรูปแบบหนึ่งทางออนไลน์ ซึ่งมีการใช้ความรู้ทางจิตวิทยาในการสร้างสถานการณ์ต่าง ๆ ประกอบกับการใช้ศาสตร์และศิลป์ทางคอมพิวเตอร์เพื่อเข้าถึงระบบของอีกฝ่าย (Harl, 1997) โดยอาศัยช่องโหว่จากพฤติกรรมของผู้ใช้งาน

อาจมีการปลอมตัวเป็นบุคคลอื่น ปลอมแปลงข้อมูล การติดสินบน การข่มขู่ การสร้างสถานการณ์ (SANS Institute, n.d.) เพื่อหลอกล่อให้ผู้ถูกโจมตีหลงเชื่อในข้อมูลนั้น และยอมเปิดเผยข้อมูลที่เป็นความลับ เช่น พาสเวิร์ด (Hansson, 2006) รวมถึงข้อมูลส่วนบุคคลต่าง ๆ ในเว็บไซต์ปลอมหรือดาวน์โหลดข้อมูลซึ่งมีมัลแวร์รวมถึงไวรัสต่าง ๆ สู่ระบบของผู้ถูกโจมตี (Krombholz et al., 2015) เพื่อที่แฮกเกอร์จะทำการโจมตีระบบ และทำให้เกิดความเสียหายต่อผู้ใช้งานได้

การโจมตีทางวิศวกรรมทำได้ทั้งแบบออฟไลน์ (physical) และออนไลน์ (online) โดยในอดีตผู้โจมตีมักจะเข้าหาเหยื่อในลักษณะออฟไลน์ เช่น การโทรศัพท์ไปหลอกถามข้อมูล ทั้งการอ้างตัวว่ามาจากธนาคารหรือบริษัทผู้ให้บริการทางอินเทอร์เน็ต เพื่อหลอกถามข้อมูลส่วนตัว (โทรคมนาคมแห่งชาติ, 2020) รวมถึง การค้นหาขยะขององค์กรเพื่อหาข้อมูลสำคัญ แต่ในปัจจุบันเมื่ออินเทอร์เน็ตเข้ามามีบทบาทมากขึ้น การโจมตีทางวิศวกรรมสังคมมักจะอยู่ในรูปแบบออนไลน์ (Granger, 2001) โดยลักษณะที่พบบ่อยที่สุด คือ ฟิชชิง (Abraham and Chengalur, 2010; Hatfield, 2018)

นอกจากนั้นยังมี ช่องทางออนไลน์อื่น ๆ ที่ผู้โจมตีแบบวิศวกรรมสังคมเลือกใช้ Abraham and Chengalur (2010) ประกอบไปด้วย

1) อีเมล์ (e-mail) เป็นช่องทางที่พบได้บ่อยที่สุดในการโจมตีด้วยวิธีการวิศวกรรมสังคม ในรูปแบบของฟิชชิง มักจะแนบมาพร้อมกับลิงก์ปลอมที่มีเนื้อหาเชิญชวนให้เหยื่อกดลิงก์เข้าไป และต้องกรอกข้อมูลส่วนบุคคลก่อน ถึงจะเปิดดูข้อมูลส่วนอื่น ๆ ได้ นอกจากนั้นแฮกเกอร์ยังมีการใช้เทคนิคปลอมแปลงเป็นบุคคลสำคัญของบริษัทต่าง ๆ เพื่อสร้างความน่าเชื่อถือ สร้างสถานการณ์เพื่อความสมจริง รวมถึงสร้างสถานการณ์ให้มีความเร่งด่วน เช่น ใกล้จะหมดเวลาแล้ว ให้เหยื่อควรรีบตัดสินใจก่อนโปรโมชันจะหมดลง

2) สื่อสังคมออนไลน์ (social networks) ผู้โจมตีมักสร้างตัวตนปลอมเพื่อให้เหยื่อหลงเชื่อ และหลอกเอาข้อมูลจากเหยื่อ รวมถึงมีการแฮกบัญชีสื่อสังคมออนไลน์ของบุคคลใกล้ชิดกับเหยื่อ และติดต่อเหยื่อผ่านโปรแกรมแชท (instant messaging) เพื่อขอยืมเงิน หรือเสนอผลตอบแทน โปรโมชันเพื่อสร้างแรงจูงใจ

3) เว็บไซต์ (websites) เป็นอีกหนึ่งช่องทางที่พบได้บ่อย สามารถดัดแปลงไปใช้ ประกอบกับวิธีอื่น ๆ เช่น อีเมลฟิชชิง โดยแฮกเกอร์จะหลอกเหยื่อให้เข้าเว็บไซต์ปลอมที่มีการซ่อนหรืออำพราง URL หรือโดเมนให้เหมือน URL ของจริง หากผู้ใช้งานไม่ตรวจสอบ URL หรือ โดเมนอย่างละเอียด และเข้าไปกรอกข้อมูลส่วนตัว เช่น เลขที่บัตรประชาชน ชื่อ-นามสกุล เบอร์โทรศัพท์ ซึ่งข้อมูลเหล่านี้เป็นข้อมูลส่วนบุคคลที่มีความสำคัญสำหรับการยืนยันตัวตนเพื่อทำธุรกรรมต่าง ๆ ทั้งของทางภาครัฐ ธนาคาร หรือบริษัททางการเงินด้านอื่น ๆ เมื่อแฮกเกอร์ได้ข้อมูลเหยื่อไปแล้ว ก็สามารถสวมรอยเป็นเหยื่อเพื่อนำข้อมูลไปใช้ในทางมิชอบ ทำให้เกิดความเสียหายได้

โทรคมนาคมแห่งชาติ (2020) ได้สรุปแนวทางการป้องกันตนเองจากวิศวกรรมสังคม ดังนี้

1) คิดวิเคราะห์สถานการณ์ก่อนหลงเชื่อ หากได้รับอีเมล์จากธนาคารหรือหน่วยงานต่าง ๆ ควรตรวจสอบว่าเป็นหน่วยงานจริงหรือไม่ โดยใช้ข้อมูลจากหลายส่วนประกอบการพิจารณา เช่น เช็กในเว็บไซต์ธนาคารเกี่ยวกับ นโยบายการขอข้อมูลส่วนบุคคลผ่านทางอีเมล์ หรือ ข้อมูลการโอนเงินจากแอปพลิเคชันธนาคารก่อนทุกครั้งว่า ได้โอนเงินหรือมีเงินเข้าบัญชีจริงหรือไม่

2) ไม่กรอกรหัสผ่านในเว็บไซต์ที่ไม่น่าเชื่อถือ หากได้รับอีเมลที่ไม่มั่นใจว่ามาจากหน่วยงานจริงหรือไม่ รวมถึงลิงก์แปลกที่ให้กรอก username หรือ password ผู้ใช้งานต้องตรวจสอบก่อนทุกครั้ง โดยเฉพาะเกี่ยวกับบัญชีธนาคาร เนื่องจากธนาคารไม่มีนโยบายสอบถามข้อมูลส่วนบุคคลกับผู้ใช้งาน

3) หลีกเลี่ยงการกดลิงก์ที่ไม่แน่ใจ หรือ ลิงก์ ที่แนบมากับอีเมล์ที่ไม่รู้จัก หากเป็นคนที่รู้จักส่งมา ก็ต้องมีการตรวจสอบเพื่อยืนยันตัวตนก่อนทุกครั้ง และผู้ใช้งานต้องพิจารณาไว้เสมอว่า แฮกเกอร์สามารถปลอมแปลงเป็นใครก็ได้ในโลกออนไลน์

2.6.5 ชีพเฟค (Cheapfake)

Samsung SDS (2022) กล่าวว่า ชีฟเฟค หรือ แชลโลว์เฟค (shallowfake)” คือ การหลอกลวงหรือบิดเบือนข้อมูลด้วยวิธีการแบบง่าย ไม่ซับซ้อน อาจมีการใช้เทคโนโลยีเข้ามาช่วย แต่ไม่จำเป็นต้องอาศัยชุดความรู้ชั้นสูง แตกต่างจาก deepfake ที่ผู้ใช้งานจำเป็นต้องมีองค์ความรู้เรื่อง AI และ machine learning วิธีการหลอกลวงแบบชีพเฟค พบได้ทั้งการแต่งภาพด้วยโปรแกรมโฟโตชอป ตัดต่อคลิปวิดีโอด้วยการเร่งหรือลดความเร็ว รวมถึงนำภาพเหตุการณ์ที่เคยเกิดขึ้นมาแล้ว มาบรรยายในบริบทอื่น (re – contextualizing) ซึ่งไม่ตรงกับเหตุการณ์จริง ทำให้เกิดความเข้าใจผิด

ด้านของสำนักข่าวออนไลน์ Slate (2019) ได้เตือนประชาชนว่าถึงแม้ ดีพเฟค (deepfake) จะเป็นเทคโนโลยีที่มีความน่ากังวล แต่ความเสียหายจากการหลอกลวงทางออนไลน์หลายครั้งเกิดจากเทคนิคจากการหลอกลวงแบบชีพเฟค ในบริบทของสังคมไทย โคแฟก (2567) ได้รายงานว่า พบว่ามีมิจฉาชีพใช้เทคนิคดังกล่าวในการหลอกลวงผู้เสียหาย ในลักษณะของการนำภาพของบุคคลอื่นมาโพสต์เพื่อขอรับเงินบริจาค รวมถึงใช้ข่าวเก่า และเปลี่ยนชื่อและบัญชีผู้รับเงินบริจาค รวมถึงมีการเปิดเพจเฟซบุ๊กจำหน่ายป้ายทะเบียนรถยนต์ปลอมและป้ายแสดงการเสียภาษีประจำปี ซึ่งตัดต่อโดยใช้โปรแกรมโฟโตชอป ดังนั้นจะเห็นได้ว่า แม้เทคโนโลยีสมัยใหม่อาจทำให้การหลอลวงทางออนไลน์เป็นไปได้อย่างแนบเนียนและจับผิดได้ยากมากขึ้น แต่ในขณะเดียวกันการหลอกลวงโดยใช้เทคนิค ชีพเฟค ที่สามารถทำได้ง่าย ก็ยังสามารถหลอกและทำให้ผู้เสียหายตกหลุมพรางได้เช่นเดียวกัน

2.7 กฎหมายและหน่วยงานที่เกี่ยวข้อง

ศูนย์วิจัยเพื่อการพัฒนาสังคมและธุรกิจ จำกัด (2565) ได้ศึกษาเกี่ยวกับคนไทยกับการถูกหลอกลวงผ่านอินเทอร์เน็ต พบว่าประเทศไทยมีกฎหมายและฐานความผิดที่เกี่ยวข้องกับการหลอกลวงผ่านระบบอินเทอร์เน็ต ดังนี้

2.7.1 ความผิดฐานฉ้อโกง ตามประมวลกฎหมายอาญา

มาตรา 341 ผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้ แจ้ง และโดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สาม ทำ ถอน หรือทำลายเอกสารสิทธิ ผู้นั้นกระทำความผิดฐานฉ้อโกง มีโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ

มาตรา 343 ถ้าการกระทำความผิด ตามมาตรา 341 ได้กระทำด้วยการแสดงข้อความอันเป็นเท็จต่อประชาชน หรือ ด้วยการปกปิดความจริงซึ่งควรบอกให้แจ้งแก่ประชาชน มีโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่

เกิน 100,000 บาท หรือทั้งจำทั้งปรับ หากแสดงตัวเป็นคนอื่น แอบอ้างคนอื่น หรือเป็นการหลอกลวงเด็ก หรือคนที่มีความอ่อนแอทางจิตใจผู้กระทำต้องระวาง โทษจำคุกตั้งแต่ 6 เดือนถึง 7 ปี และปรับตั้งแต่ 10,000 ถึง 140,000 บาท

มาตรา 342 ถ้าในการกระทำความผิดฐานฉ้อโกง ผู้กระทำ

(1) แสดงตนเป็นคนอื่น หรือ

(2) อาศัยความเบาปัญญาของผู้ถูกหลอกลวงซึ่งเป็นเด็ก หรืออาศัยความอ่อนแอแห่งจิตของผู้ถูกหลอกลวง ผู้กระทำต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

2.7.2 การลวงขาย ตามประมวลกฎหมายอาญา

มาตรา 271 ผู้ใดขายของโดยหลอกลวงด้วยประการใด ๆ ให้ผู้ซื้อหลงเชื่อในแหล่งกำเนิด สภาพ คุณภาพ หรือ ปริมาณแห่งของนั้นอันเป็นเท็จ ถ้าการกระทำนั้นไม่เป็นความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกิน หกหมื่นบาท หรือทั้งจำทั้งปรับ

ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ตามประมวลกฎหมายอาญา

มาตรา 269/5 ผู้ใดใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือ ประชาชน ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

มาตรา 269/6 ผู้ใดมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/5 ในประการที่ น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือทั้ง จำทั้งปรับ

มาตรา 269/7 ถ้าการกระทำดังกล่าวในหมวดนี้ เป็นการกระทำเกี่ยวกับบัตรอิเล็กทรอนิกส์ที่ผู้ออกได้ออกให้แก่ผู้ มีสิทธิใช้ เพื่อใช้ประโยชน์ในการชำระค่าสินค้า ค่าบริการหรือหนี้อื่นแทนการชำระด้วยเงินสด หรือใช้เบิกถอนเงินสด ผู้กระทำต้องระวางโทษหนักกว่าที่บัญญัติไว้ในมาตรานั้น ๆ กึ่งหนึ่ง

2.7.3 ความผิดตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่า ทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การ กระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

มาตรา 16 ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลง ด้วยวิธีการทางอิเล็กทรอนิกส์หรือ วิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษ จำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

2.7.4 ความผิดตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ

มาตรา 5 ผู้ใดกระทำการอย่างหนึ่งอย่างใดดังต่อไปนี้

(1) เป็นสมาชิกหรือเป็นเครือข่ายดำเนินงานขององค์กรอาชญากรรมข้ามชาติ

(2) สมคบกันตั้งแต่สองคนขึ้นไปเพื่อกระทำความผิดร้ายแรงอันเกี่ยวข้องกับองค์กรอาชญากรรมข้ามชาติ

(3) มีส่วนร่วมกระทำการใด ๆ ไม่ว่าโดยทางตรงหรือทางอ้อมในกิจกรรมหรือการดำเนินการขององค์กรอาชญากรรมข้ามชาติ โดยรู้ถึงวัตถุประสงค์และการดำเนินกิจกรรมหรือโดยรู้ถึงเจตนาที่จะกระทำความผิดร้ายแรงของ องค์กรอาชญากรรมข้ามชาติดังกล่าว

(4) จัดการ สั่งการ ช่วยเหลือ ยุยง อำนวยความสะดวก หรือให้คำปรึกษาในการกระทำความผิดร้ายแรงของ องค์กรอาชญากรรมข้ามชาติ โดยรู้ถึงวัตถุประสงค์และการดำเนินกิจกรรม หรือโดยรู้ถึงเจตนาที่จะกระทำความผิดร้ายแรง ขององค์กรอาชญากรรมข้ามชาติดังกล่าว ผู้นั้นกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ

มาตรา 6 ผู้ใดกระทำความผิดตามมาตรา 5 นอกราชอาณาจักร ผู้นั้นจะต้องรับโทษในราชอาณาจักรตามที่ กำหนดไว้ในพระราชบัญญัตินี้

มาตรา 25 ผู้ใดกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ต้องระวางโทษจำคุกตั้งแต่ส 4 ปีถึง 15 ปี หรือปรับตั้งแต่ 80,000 บาทถึง 300,000 บาท หรือทั้งจำทั้งปรับ

*ความผิดร้ายแรง หมายความว่า ความผิดอาญาที่กฎหมายกำหนดโทษจำคุกขั้นสูงตั้งแต่ 4 ปีขึ้นไปหรือโทษสถานที่หนักกว่านั้น

2.7.5 พระราชกำหนดอาชญากรรมไซเบอร์ 2566

เมื่อวันที่ 16 มีนาคม 2566 ราชกิจจานุเบกษา เผยแพร่พระราชกำหนด มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มีผลบังคับใช้ตั้งแต่วันที่ 17 มีนาคม 2566 ทั้งหมด 14 มาตรา โดยมีสาระสำคัญ ได้แก่

-ผู้เสียหายสามารถโทรแจ้งให้ธนาคารระงับบัญชีต้องสงสัยได้ทันที และยับยั้งการโอนเงินทุกธนาคารที่รับโอนเงินต่อ ประชาชนแจ้งความที่สถานีตำรวจใดก็ได้ ทั่วประเทศหรือออนไลน์

-ธนาคารระงับบัญชีต้องสงสัยได้ชั่วคราว ไม่ต้องรอเกิดเหตุ

-ธนาคาร ผู้ให้บริการทางโทรศัพท์ อินเทอร์เน็ตแลกเปลี่ยนข้อมูลธุรกรรมต้องสงสัยได้รวดเร็ว

-ผู้เปิดบัญชีม้า ซิมม้า มีโทษจำคุก 3 ปี หรือ ปรับไม่เกิน 300,000 บาท

-ผู้เป็นธุระจัดหา หรือ โฆษณาบัญชีม้า ซิมม้า มีโทษจำคุก 2-5 ปี หรือปรับ 200,000-500,000 บาท

-เกิดระบบแลกเปลี่ยนข้อมูลและใช้เทคโนโลยี AI ตรวจสอบและระบุธุรกรรมต้องสงสัย เพื่อป้องกันตัดวงจรอาชญากรรมก่อนเกิดเหตุ

2.7.6 การดำเนินการและหน่วยงานให้ความช่วยเหลือเมื่อถูกหลอกหลวง

1) แจ้งความออนไลน์

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสำนักงานตำรวจแห่งชาติ (สตช.) รวมถึงหน่วยงาน ที่เกี่ยวข้อง ได้เปิดศูนย์รับแจ้งความออนไลน์อาชญากรรมทางเทคโนโลยี ผ่านเว็บไซต์ **www. thaipoliceonline.co.th** หรือเบอร์สายด่วน **1441** เพื่อเพิ่มความสะดวกให้แก่ผู้เสียหาย ไม่ต้องเดินทางไปแจ้งความยังโรงพัก นอกจากนี้ยังได้มีการทำบันทึกข้อตกลงความร่วมมือ **(Memorandum of Understanding: MOU)** ระหว่างสตช. กับสมาคมสถาบันการเงินของรัฐ สมาคมธนาคารไทย และธนาคารสมาชิก **21** ธนาคาร เพื่อร่วมมือในการแก้ปัญหาอาชญากรรมทางเทคโนโลยีให้มีประสิทธิภาพมากขึ้น

ปัจจุบันการแจ้งความออนไลน์ยังทำได้เฉพาะคดีอาชญากรรมทางเทคโนโลยี ได้แก่ การหลอกลวงออนไลน์ทางด้านการเงินจำหน่ายสิ่งของผิดกฎหมาย หลอกลวงจำหน่ายสินค้าออนไลน์ การเผยแพร่ข่าวปลอม และความผิดตามพระราชบัญญัติคอมพิวเตอร์ การล่วงละเมิดทางเพศต่อเด็กหรือสตรีทางอินเทอร์เน็ต และการค้ามนุษย์ การพนันออนไลน์ อาชญากรรมข้ามชาติ นอกเหนือจากหมวดหมู่นี้ ยังคงต้องเดินทางไปแจ้งความที่โรงพักในท้องที่ที่เกิดเหตุ

ผู้เสียหายสามารถเตรียมเอกสารหลักฐาน เช่น ภาพเฟซบุ๊ก แชทไลน์หรือช่องทางการติดต่ออื่น ๆ หมายเลขบัญชีธนาคาร เบอร์โทรศัพท์ ที่มีเพื่อเป็นประโยชน์ต่อการสืบสวนได้ ซึ่งหากคนร้ายทำความผิดหลายท้องที่ ทางเจ้าหน้าที่ตำรวจก็สามารถเชื่อมโยงข้อมูลและคดี เพื่อนำไปขอศาลออกหมายจับ รวมถึงติดต่อไปยังธนาคารเพื่อระงับการทำธุรกรรมทางการเงินได้พร้อมกัน (ชัวร์ก่อนแชร์, 2566)

2) แผนกคดีซื้อขายออนไลน์ในศาลแพ่ง

ศาลยุติธรรมจึงได้ดำเนินการจัดตั้งแผนกคดีซื้อขาย ออนไลน์ในศาลแพ่ง เผยแพร่ในราชกิจจานุเบกษา มีผลบังคับใช้เมื่อวันที่ 20 ธันวาคม 2564 และเปิดแผนก ไปเมื่อวันที่ 27 มกราคม 2565 เพื่อเป็นช่องทางให้ผู้บริโภคเข้าถึงบริการของศาลได้สะดวกมากขึ้น โดยใช้กระบวนการศาลอิเล็กทรอนิกส์เต็มรูปแบบ ทุกขั้นตอนผ่านระบบอิเล็กทรอนิกส์ (e-filing) ได้ตลอด 24 ชั่วโมง และสามารถติดตามความ คืบหน้าได้ใน 12 ชั่วโมงนับแต่ยื่นเรื่อง ไม่กำจัดชนิดสินค้าและวงเงินความเสียหาย รวมถึงไม่เสียค่าใช้จ่ายและค่าธรรมเนียมศาล ไม่จำเป็นต้องมีทนายความ หากหลักฐานไม่ครบถ้วนจะมีเจ้าพนักงานคดีติดต่อกลับไปหาผู้เสียหาย

3) ช่องทางการร้องเรียนของผู้บริโภค

- สำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.) มีหน้าที่ในการรับเรื่องร้องทุกข์และช่วยเหลือผู้บริโภคที่ไม่ได้รับความเป็นธรรมจากการซื้อสินค้าและบริการ รวมถึงมีหน้าที่ติดตาม สอดส่องผู้ประกอบธุรกิจ มีสายงานที่รับผิดชอบโดยตรง ได้แก่ กองคุ้มครองผู้บริโภคด้านโฆษณา กองคุ้มครองผู้บริโภคด้านฉลาก กองคุ้มครองผู้บริโภคด้านสัญญา และ สำนักงานกฎหมายและคดี ติดต่อขอคำปรึกษาทางสายด่วน สคบ.**1166** หรือร้องทุกข์ผ่าน **http://complaint.ocpb.go.th**
- สำนักงานคณะกรรมการอาหารและยา (อย.) กระทรวงสาธารณสุข มีหน้าที่ในการคุ้มครองสุขภาพและความปลอดภัยของประชาชนจากการบริโภคผลิตภัณฑ์สุขภาพ ทั้งด้านการผลิต จำหน่าย และโฆษณาสินค้า ประเภทยา อาหาร เครื่องสำอาง วัตถุอันตราย เครื่องมือทางการแพทย์ รวมถึงมีภารกิจในการเผยแพร่ความรู้ ความเข้าใจที่ถูกต้องเกี่ยวกับการเลือกบริโภคผลิตภัณฑ์สุขภาพอย่างเหมาะสม ปลอดภัย ได้มาตรฐานและปกป้องสิทธิ์ของตนเอง
  - ร้องเรียนได้ที่สายด่วน อย. **1556** หรือ โทรศัพท์ **0 2590 1556**
  - อีเมล **1556@fda.moph.go.th**
  - แอปพลิเคชัน **Oryor Smart Application** เมนูร้องเรียน
  - ร้องเรียนด้วยตนเอง กรณีมีตัวอย่างผลิตภัณฑ์มามอบให้
- สภาองค์กรของผู้บริโภค เกิดจากการรวมตัวขององค์กรผู้บริโภค มีสถานะองค์กรเป็นนิติบุคคล เป็นตัวแทนผู้บริโภคที่มีความเป็นอิสระ และมีวัตถุประสงค์เพื่อคุ้มครองผู้บริโภคในทุกด้าน ทั้งการ

ถูกหลอกจากการซื้อของออนไลน์ กรณีไม่ได้รับความเป็นธรรมจากการซื้อของออนไลน์อื่น ๆ รวมถึงกู้เงินออนไลน์จากแอปพลิเคชันหลอกลวง

- แจ้งเรื่องผ่านทางเว็บไซต์

  https://crm.tcc.or.th/?entryPoint=Portal&action=warning

- แจ้งเรื่องผ่านโทรศัพท์ **0-2239-1839**

- แจ้งเรื่องผ่านอีเมล **contact@tcc.or.th**

4) ศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์1212

ศูนย์กลางการรับเรื่องร้องเรียนให้แก่ผู้บริโภคหรือผู้ประกอบการทั้งภาครัฐและเอกชน โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Development Agency: ETDA) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ครอบคลุม 4 กลุ่มหลัก ได้แก่ การกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ รวมถึงการกระทำความผิดทางเทคโนโลยีสารสนเทศ การซื้อขายทางออนไลน์และภัยคุกคามทางไซเบอร์

- ติดต่อ 1212OCC ได้ทางหมายเลขโทรศัพท์ 1212 หรือโทรสาร 02- 127-5789
- อีเมล์ 1212@mdes.go.th
- เว็บไซต์ www.1212OCC.com

- แอปพลิเคชัน 1212 OCC

5) หน่วยงานดูแลด้านภัยการเงิน

- **ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย (ศคง.)**

ศูนย์กลางในการดำเนินงานด้านการคุ้มครองผู้ใช้บริการทางการเงินอย่างเป็นระบบ โดยธนาคารแห่งประเทศไทย มีวัตถุประสงค์เพื่อคุ้มครองสิทธิและส่งเสริมการให้ความรู้ทางการเงินแก่ผู้ใช้บริการทางการเงินดูแลความเสี่ยงและความเสียหายที่อาจจะเกิดขึ้นจากการใช้บริการ รวมทั้งรู้เท่าทันการหลอกลวงทางการเงินจากกลุ่มมิจฉาชีพเพื่อไม่ตกเป็นผู้เสียหายภัยทางการเงินในรูปแบบต่าง ๆ ศคง. มีบทบาทหน้าที่ 3 ประการ ได้แก่ ให้คำปรึกษาและรับเรื่องร้องเรียนเกี่ยวกับบริการทางการเงิน ส่งเสริมความรู้เกี่ยวกับบริการทางการเงินให้แก่ประชาชนและส่งเสริมบทบาทหน้าที่ของ ธปท. ในการกำกับดูแลให้สถาบันการเงินให้บริการแก่ลูกค้าอย่างเป็นธรรม โดยการส่งผ่านข้อมูล ข้อร้องเรียน ข้อเสนอแนะไปยังหน่วยงานที่เกี่ยวข้องเพื่อตรวจสอบและดำเนินการอย่างถูกต้อง ประชาชนสามารถโทรแจ้งเหตุภัยการเงินได้ที่ 1213 แฟกซ์ 0-2283-6151 และอีเมล์ facc@bot.or.th

สายด่วนธนาคารต่าง ๆ

กระทรวงการคลัง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ธนาคารแห่งประเทศไทย (ธปท.) และหน่วยงานที่เกี่ยวข้อง ได้ทำงานร่วมกับสมาคมธนาคารไทยและธนาคารของรัฐอย่างใกล้ชิด เพื่อป้องกันปัญหาและบรรเทาความเสียหายที่จะเกิดแก่ประชาชน โดยธนาคารพาณิชย์และธนาคารเฉพาะกิจ ได้เปิดศูนย์รับแจ้งเหตุภัยทางการเงินจากมิจฉาชีพของธนาคาร เพื่อเป็นช่องทางให้ประชาชนที่ได้รับผลกระทบ โทรแจ้งเหตุได้ตลอด 24 ชั่วโมง เพื่อสกัดกั้นความเสียหายให้เร็วที่สุด

ธนาคารกสิกรไทย 0-2888-8888 กด 001

ธนาคารกรุงไทย 0-2111-1111 กด 108

ธนาคารกรุงศรีอยุธยา 1572 กด 5

ธนาคารกรุงเทพ 1333 หรือ 0-2645-5555 กด *3

ธนาคารไทยพาณิชย์ 0-2777-7575

ธนาคารทหารไทยธนชาต 1428 กด 03

ธนาคารออมสิน 1115 กด 6

ธนาคารซีไอเอ็มบีไทย 0-2626-7777 กด 00

ธนาคารยูโอบี 0-2344-9555

ธนาคารแลนด์ แอนด์ เฮ้าส์ 0-2359-0000 กด 8

ธนาคารอาคารสงเคราะห์ 0-2645-9000 กด 33

ธนาคารไทยเครดิต เพื่อรายย่อย 0-2697-5454

นอกจากนี้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ธนาคารแห่งประเทศไทย (ธปท.) สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) และสมาคมธนาคารไทย อยู่ระหว่างการพัฒนาระบบกลางที่เรียกว่า ศูนย์ตรวจเช็กธุรกรรมที่มีความเสี่ยงทุจริต (central fraud registry) เพื่อเป็นกลไกด้านข้อมูลที่จะช่วยในการยับยั้งความเสียหายที่อาจเกิดกับประชาชนเจ้าของบัญชีที่ตกเป็นเป้าหมายของมิจฉาชีพ

- **ส่วนป้องปรามการเงินนอกระบบ**

กรณีโดนหลอกลวงแบบแชร์ลูกโซ่ ร่วมลงทุนออนไลน์แล้วเกิดความเสียหาย นอกจากแจ้งตำรวจยัง สามารถส่งเรื่องร้องเรียนมาที่ส่วนป้องปรามการเงินนอกระบบ สำนักนโยบายพัฒนาระบบการเงินภาค ประชาชน สำนักงานเศรษฐกิจการคลัง ซึ่งจะประสานหน่วยงานที่เกี่ยวข้องดำเนินการตามกฎหมาย โดยสามารถติดต่อสอบถามที่ เบอร์ 0 2169 7128 ถึง 36 ต่อ 153 - 160 หรือศูนย์รับแจ้งการเงินนอกระบบ โทร. 1359 หรือ e-mail 1359@mof.go.th

- **กรมสอบสวนคดีพิเศษ (Department of Special Investigation: DSI)**

ขอบเขตหน้าที่ดูแลคดีความทางอาญาที่มีความซับซ้อน จำเป็นต้องใช้วิธีการสืบสวนสอบสวนและรวบรวม พยานหลักฐานเป็นพิเศษ หรือ มีผลกระทบอย่างรุนแรงต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน หรือ เป็นการกระทำความผิดข้ามชาติที่สำคัญ หรือการกระทำขององค์กรอาชญากรรม โทร 0-2831-9888 หรือ 1202

- **สำนักงานป้องกันและปราบปรามการฟอกเงิน**

คดีความผิดมูลฐานฟอกเงิน เช่น ความผิดเกี่ยวกับการฉ้อโกงประชาชน ตามกฎหมายอาญา ร้องเรียนได้ทางเบอร์โทรศัพท์ 02-219-3600 หรือ 1710

- **สำนักรับเรื่องร้องเรียนและคุ้มครองผู้บริโภคในกิจการโทรคมนาคม**

สังกัดกสทช. ดำเนินการที่เกี่ยวข้องกับการคุ้มครองผู้บริโภคในกิจการโทรคมนาคม กรณีได้รับ SMS ข้อความ หรือโทรศัพท์จากมิจฉาชีพ แจ้งได้หลายช่องทาง

- เบอร์สายด่วน 1200
- แอปพลิเคชัน Mobile NBTC 1200
- ร้องเรียนผ่านอีเมล 1200@nbtc.go.th
- ร้องเรียนผ่านเว็บไซต์ http://tcp.nbtc.go.th
- เดินทางมาร้องเรียนด้วยตนเองหรือร้องเรียนผ่านจดหมายที่สำนักรับเรื่องร้องเรียนและคุ้มครองผู้บริโภคในกิจการโทรคมนาคม สำนักงาน กสทช. เลขที่ 404 อาคารพหลโยธินเซ็นเตอร์

บทที่ 3
ผลจากการศึกษาจากผู้เสียหาย

การศึกษาในครั้งนี้ได้มีการสัมภาษณ์เชิงลึก (in-depth interview) และสัมภาษณ์แบบกลุ่ม (focus group interview) ผู้เสียหายจากอาชญากรรมออนไลน์ทั้ง 4 ประเภท ได้แก่ การหลอกขายสินค้า การหลอกให้ลงทุน แก๊ง call center และการหลอกให้รัก จำนวน 16 คน ซึ่งเป็นกลุ่มวัยทำงานและมีความคุ้นชินกับเทคโนโลยีเป็นอย่างดี โดยมีข้อค้นพบตามประเด็นดังต่อไปนี้

3.1 ปัจจัยในการถูกหลอกลวง

3.1.1 ตระหนักรู้ แต่ไม่ฉุกคิด (awareness)

อาชญากรรมออนไลน์ที่เกิดขึ้นในปัจจุบันไม่ใช่เรื่องใหม่ ทว่า ด้วยความรุนแรงและความเสียหายที่เกิดขึ้นมีมูลค่ามหาศาลกระทบต่อประชาชนจำนวนมาก จึงทำให้สังคมได้เริ่มหันมาตระหนักรู้และตื่นตัวในการป้องกันภัยดังกล่าวเพิ่มมากขึ้น ผู้เสียหาย ง (การสื่อสารส่วนบุคคล, 30 มีนาคม 2567) ซึ่งถูกโจมตีจากมิจฉาชีพที่แฝงมาในรูปแบบของการหลอกให้รักในช่วงก่อนการแพร่ระบาดของโควิด 19 เล่าว่า ไม่เคยรู้จักเรื่องการหลอกให้รัก (scammer) มาก่อน เป็นเรื่องที่ใหม่ มารู้จักก็หลังจากที่เกิดขึ้นกับตัวเองแล้ว โดยในช่วงนั้น ในไทยยังไม่มีข้อมูลมากนัก ทำให้ต้องไปค้นจากอินเทอร์เน็ต และเจอบทความของต่างประเทศที่มีการพูดถึงเรื่องนี้

ปัจจุบัน ประชาชนสามารถรับรู้ข้อมูลข่าวสารเกี่ยวกับภัยไซเบอร์ผ่านทางสื่อหลัก ไม่ว่าจะเป็นโทรทัศน์และวิทยุ สื่อออนไลน์ต่าง ๆ เช่น Facebook, YouTube หรือ TikTok หรือการลงพื้นที่เพื่อให้ความรู้ของหน่วยงานต่าง ๆ ทว่า มิจฉาชีพเองก็มีการปรับเปลี่ยนรูปแบบการโจมตีให้สอดคล้องกับสถานการณ์ในขณะนั้น มีการใช้กลยุทธที่หลากหลาย โดยเฉพาะการโจมตีแบบวิศวกรรมสังคม (Social engineering) ที่ใช้หลักจิตวิทยาดึงเอาจุดอ่อนของมนุษย์มาโจมตี ไม่ว่าจะเป็นการสร้างข้อจำกัด เช่น เวลาหรือการขู่คุกคาม มากดดัน รวมถึงการโน้มน้าวให้คนหลงเชื่อด้วยการสร้างเว็บไซต์ปลอมมาหลอกลวงหรือบิดเบือนข้อมูลเพียงนิดหน่อยด้วยวิธีการง่าย ๆ (Cheapfake) ก็อาจจะทำให้ประชาชนที่แม้จะมีการรับรู้ในเรื่องภัยออนไลน์มาก่อน ก็อาจจะต้องตกเป็นผู้เสียหายจากการโจมตีจากกลุ่มมิจฉาชีพออนไลน์ได้

“เหมือนเราอยู่ในที่สว่างแต่เขาอยู่ในที่มืด เขาจะโจมตีเมื่อไหร่ไม่สามารถคาดการณ์ได้ ต่อให้เรียนรู้จากประสบการณ์คนอื่นแต่มันละแบบ” ผู้เสียหาย ก (การสื่อสารส่วนบุคคล, 27 มกราคม 2567)

“ตระหนักรู้ แต่ป้องกันไม่ได้ เพราะรูปแบบเปลี่ยนไปเรื่อย ๆ กว่าจะรู้ต้องมีผู้เสียหายก่อนค่อยไปถึงคนอื่น” ผู้เสียหาย ค (การสื่อสารส่วนบุคคล, 28 มกราคม 2567)

“ที่หลงเชื่อเพราะมีการปลอมตัวอย่างแนบเนียนว่าเป็นเจ้าหน้าที่ของกรมที่ดิน ด้วยการสร้างบรรยากาศ สร้างความน่าเชื่อถือจากการให้ข้อมูลส่วนตัว ข้อมูลที่ดิน ซึ่งเป็นข้อมูลระดับลึก พร้อมกับอ้างชื่อเจ้าหน้าที่ที่ดินคนนึง เราก็ตรวจสอบแบบผ่านๆ และเจอว่ามีเจ้าหน้าที่คนนี้จริง” ผู้เสียหาย จ (การสื่อสารส่วนบุคคล, 11 กุมภาพันธ์ 2567)

“ข้อมูลมีเยอะ จากข่าวที่ออกมาในแต่ละวัน และก็รู้ว่ารูปแบบการหลอกลวงก็มีหลากหลาย เพียงแต่ในช่วงขณะนั้นลืมนึกถึง ลืมตรวจเช็คว่าเป็นญาติ หรือพิจารณาได้ว่าเป็นการหลอกลวง” ผู้เสียหาย ช (การสื่อสารส่วนบุคคล, 11 กุมภาพันธ์ 2567)

“จริง ๆ ตอนนั้นคิดว่าตัวเองเป็นรอบคอบระดับหนึ่งจะไม่โดนหลอก แต่ว่าตอนนั้นด้วยความที่งานยุ่งด้วย อะไรดลใจก็ไม่รู้ถึงเชื่อหมดเลย ยิ่งแบบว่าใส่ชุดตำรวจดูน่าเชื่อถือ แล้วเขาก็ส่งรูปมาเป็นแบบตัดต่อสมุดบัญชีเป็นชื่อเรา แต่ตอนนั้นไม่ได้ดูดี ๆ ถ้าสังเกตดี ๆ จะเห็นว่าชื่อมันเป็นรอยนิดหนึ่ง ไม่ได้ซูมเข้า แต่มองไกล ๆ เห็นว่าเป็นชื่อเรานี้ก็เลยเชื่อหมดเลย” ผู้เสียหาย ต (การสื่อสารส่วนบุคคล, 11 มีนาคม 2567)

3.1.2 การป้องกันยังไม่เพียงพอ (Poor cyber hygiene)

ข้อมูลข่าวสารเกี่ยวกับการป้องกันจากภัยไซเบอร์ช่วยให้ประชาชนมีความตระหนักรู้ในการป้องกันได้ในระดับหนึ่งเท่านั้น เช่น ผู้เสียหาย ข (การสื่อสารส่วนบุคคล, 28 มกราคม 2567) ยอมรับว่า ไม่ได้มีการป้องกันมากนัก เนื่องจากเชื่อว่าถ้ายังไม่ได้กดเข้าไปในเข้าถึงลิงก์ที่มิจฉาชีพส่งมาให้ ก็จะไม่มีอะไรเกิดขึ้น และคิดว่าตัวเองใช้ชีวิตปลอดภัย เช่นเดียวกับ ผู้เสียหาย ด (การสื่อสารส่วนบุคคล, 11 กุมภาพันธ์ 2567) ที่ให้คะแนนระดับการป้องกันตัวเองจากแค่ 2 จาก 10 เท่านั้น และจากที่ติดตามข่าวว่ามีการโทรมาหลอก ก็เลยทำให้ไม่ค่อยรับสายเท่านั้น

การที่ประชาชนมีระดับรักษาความปลอดภัยทางไซเบอร์เบื้องต้นที่จำเป็น (Cyber hygiene) ต่ำย่อมเปิดช่องให้เหล่ามิจฉาชีพออนไลน์สามารถโจมตีได้ง่ายยิ่งขึ้น เช่น การตั้งระบบพาสเวิร์ดของแอปพลิเคชันต่าง ๆ เหมือนกัน หรือการเปิดเผยข้อมูลส่วนตัวให้กับคนแปลกหน้าได้ทราบ เป็นต้น จากการสัมภาษณ์ผู้เสียหายส่วนใหญ่ พบว่า ความตื่นตัวในการป้องกันต่าง ๆ จะมีเพิ่มขึ้นอย่างมาก หลังจากที่ตัวเองกลายเป็นผู้เสียหายแล้ว หรือมีคนรอบข้างถูกโจมตีทางไซเบอร์

“Mindset เรื่องการจัดการบัญชีเปลี่ยนไป เปลี่ยนพฤติกรรมการฝากเงินใหม่ หากมีเงินเข้าหลักแสนก็จะนำไปซื้อกองทุน หรือฝากกับบัญชีที่สามารถถอนเงินได้ยาก มีการจัดการเรื่อง password ใหม่ และก็

เปลี่ยนมือถือไปใช้ iPhone เพราะอัตราการเกิดเหตุน้อยกว่า Android” ผู้เสียหาย จ (การสื่อสารส่วนบุคคล, 11 กุมภาพันธ์ 2567)

“ระวังตัวเองมากขึ้น เวลามีข้อความหรือให้กดลิงก์ ก็ไม่เคยกด กลัวแล้ว ไม่กล้าแล้วกับการหารายได้ที่ไม่มีที่มาที่ไป ซื้อของออนไลน์ก็ไม่กล้า เพราะกลัว หรือ มีงานทำอยู่บ้านง่ายๆ เช่น gift shop แพ็กยางใส่ถุง confirm order ของ Flash อันนี้เราก็รู้แล้ว เราก็ไม่ทำ ไม่กล้าแล้ว” ผู้เสียหาย ถ (การสื่อสารส่วนบุคคล, 24 กุมภาพันธ์ 2567)

“ถ้าไม่โดนกับตัวก็ไม่ระวังขนาดนี้ เหมือนประมาณว่าถ้าเราไม่โดนกับตัวเราก็จะเสพข่าวแค่ว่ามันก็ไม่คงไม่ถึงวันของเรา คงไม่มีทางโดน เหมือนเราก็จะละเลยพอเราโดนเองกับตัวเราจะรอบคอบขึ้นมาก ๆ ” ผู้เสียหาย ท (การสื่อสารส่วนบุคคล, 27 กุมภาพันธ์ 2567)

นอกจากนี้ แม้รู้ว่ามีความเสี่ยงในการที่จะถูกโจมตีจากมิจฉาชีพ แต่ด้วยความจำเป็นต่าง ๆ ในด้านการใช้งาน ความสะดวกสบาย หรือเหตุผลด้านการเงิน ทำให้เป็นการยากที่หลายคนจะเลิกใช้ช่องทางออนไลน์ที่เคยถูกโจมตีทางไซเบอร์ อย่างไรก็ดี ก็มีการเพิ่มความระมัดระวังมากยิ่งขึ้น เช่น ผู้เสียหาย ก (การสื่อสารส่วนบุคคล, 27 มกราคม 2567) เล่าว่า ช่วงแรกหลังจากที่ถูกหลอกขายของออนไลน์ จะหันมาซื้อผ่านแฟลตฟอร์มทางการมากขึ้น แต่สุดท้ายก็หันกลับมาซื้อแบบเดิม เนื่องจากราคาถูกกว่า เกิดการเปลี่ยนแปลงแค่ระยะชั่วคราว เช่นเดียวกับผู้เสียหาย ฆ (การสื่อสารส่วนบุคคล, 5 กุมภาพันธ์ 2567) ที่ยังคงเล่นแอปพลิเคชันหาคู่อยู่แต่มีความระมัดระวังและตรวจสอบมากยิ่งขึ้น เป็นต้น

3.2 ปัญหาและความท้าทาย

3.2.1 มาตรการรับมือและช่วยเหลือของภาครัฐและหน่วยงานที่เกี่ยวข้องยังไม่เพียงพอ

แม้ปัจจุบันภาครัฐและหน่วยงานที่เกี่ยวข้องจะมีการประชาสัมพันธ์เกี่ยวกับช่องทางการให้ความช่วยเหลือเมื่อถูกโจมตีจากมิจฉาชีพออนไลน์ ทว่า ระดับการรับรู้และความเข้าใจของประชาชนในขั้นตอนการดำเนินการยังคงอยู่ในระดับต่ำ จากการสัมภาษณ์ผู้เสียหายส่วนใหญ่พบว่ายังมีความสับสน ไม่ว่าจะเป็นขั้นตอนการดำเนินการที่มีความยุ่งยาก ซับซ้อน เจ้าหน้าที่ที่รับเรื่องไม่มีความเป็นเอกภาพและให้ข้อมูลไม่ชัดเจน ทำให้รู้สึกยุ่งยากในการดำเนินการและมองว่าการเข้าถึงหน่วยงานเหล่านี้ทำได้ยาก

นอกจากนี้ การติดตามความคืบหน้ากับหน่วยงานที่เกี่ยวข้องก็ทำได้ยาก ไม่มีข้อมูล ทำให้ผู้เสียหายต้องเป็นฝ่ายรอคอยการติดต่อจากภาครัฐและหน่วยงานที่เกี่ยวข้องเพียงทางเดียว

“ฟ้องออนไลน์เคยกรอกแล้วหยุมหยิมมาก ทำให้คนที่เหนื่อยใจอยู่แล้ว พอเจอแบบนี้เลยทำให้เหนื่อยใจไม่อยากทำต่อ คิดว่าระบบการรับคำร้องหรือการเข้าถึงตำรวจไม่เอื้อต่อผู้เสียหายและใช้เวลานาน” ผู้เสียหาย ก (การสื่อสารส่วนบุคคล, 27 มกราคม 2567)

“สิ่งที่รับรู้จากการเกิดเรื่องแล้ว ไม่ใช่กระบวนที่รู้ว่ามีอะไรบ้าง ก่อนเกิดเรื่องพอรู้คร่าวๆ แต่ไม่รู้รายละเอียด แต่เกิดเรื่องค่อยรู้ว่าต้องทำอะไรบ้าง” ผู้เสียหาย ค (การสื่อสารส่วนบุคคล, 28 มกราคม 2567)

“ในการดำเนินการมีความล่าช้า และไม่รู้ว่าจุดจบของคดีความคือตอนไหน เพราะไม่มีการแจ้งเตือนผู้เสียหายกลับมา มันควรมีการอัปเดตข้อมูลการดำเนินคดีให้ผู้เสียหายทราบหลังจากแจ้งความเรียบร้อยไปแล้ว” ผู้เสียหาย ช (การสื่อสารส่วนบุคคล, 11 กุมภาพันธ์ 2567)

“ทั้งธนาคาร ตำรวจด้วย ตำรวจเองจนถึงตอนนี้ผ่านไปหนึ่งปีแล้วไม่ได้มีอะไรคืบหน้าเลย อย่างน้อยตามได้ หรือไม่ได้ควรจะบอก” ผู้เสียหาย ต (การสื่อสารส่วนบุคคล, 11 มีนาคม 2567)

“หน่วยงานภาครัฐก็ไม่รู้ว่าจะช่วยได้จริงหรือไม่ ไม่รู้ว่าโดนหลอกแล้วต้องโทรไปเบอร์ไหน” ผู้เสียหาย ธ (การสื่อสารส่วนบุคคล, 24 กุมภาพันธ์ 2567

อาชญากรรมออนไลน์มีความเกี่ยวข้องอย่างมากกับเทคโนโลยีต่าง ๆ ดังนั้น เจ้าหน้าที่หรือหน่วยงานที่ให้ความช่วยเหลือจำเป็นอย่างยิ่งที่ต้องมีความรู้หรือความเชี่ยวชาญในเรื่องเทคโนโลยี เพื่อให้สามารถสื่อสารและเข้าใจกับสิ่งที่เกิดขึ้นเมื่อผู้เสียหายเข้าไปขอรับความช่วยเหลือ นอกจากนี้ กฎหมายหรือข้อบังคับในเรื่องอาชญากรรมออนไลน์ที่มีปัจจุบันยังคงตามหลังความก้าวหน้าของกลุ่มมิจฉาชีพที่อาศัยช่องโหว่ทางกฎหมายในการทำร้ายประชาชน เช่น การหลอกให้ลงทุน ซึ่งมีมูลค่าความเสียหายสูง เป็นต้น

“มิจฉาชีพมีเยอะและการหลอกลวงก็มีหลากหลายรูปแบบ มีการใช้เทคโนโลยี อย่าง AI เลียนเสียงมาใช้หลอกลวง แต่ความเร็วและการจัดการไม่เพียงพอ ต่อให้มีการโปรโมท แต่มิจฉาชีพก็อาศัยช่องว่างต่าง ๆ และก็มีการปรับรูปแบบใหม่ให้การหลอกลวงเพิ่มขึ้น เทคโนโลยีภาครัฐยังสู้มิจฉาชีพไม่ได้ รัฐต้องหาคนเก่งที่ทำโปรแกรมหรืออะไรสักอย่างมาป้องกันมิจฉาชีพเพื่อให้คนใช้ให้มีความปลอดภัยมากขึ้น” ผู้เสียหาย ค (การสื่อสารส่วนบุคคล, 28 มกราคม 2567)

“ตำรวจเหมือนไม่ค่อยมีความรู้ความเข้าใจเกี่ยวกับเทคโนโลยี หรือสื่อออนไลน์ เพราะเราต้องไปนั่งอธิบายถึงแพลตฟอร์มออนไลน์ให้เขาฟัง” ผู้เสียหาย ฉ (การสื่อสารส่วนบุคคล, 11 กุมภาพันธ์ 2567)

3.2.2 ไม่มีความเชื่อมั่นต่อระบบของรัฐและหน่วยงานที่เกี่ยวข้อง

ภาพลักษณ์ด้านลบของภาครัฐ โดยเฉพาะในเรื่องทุจริตคอร์รัปชัน ความไม่ต่อเนื่องของการทำงาน การเลือกปฏิบัติ และความไม่เป็นเอกภาพของหน่วยงานที่เกี่ยวข้อง ทำให้เกิดความไม่ไว้วางใจ (trust) ในกลุ่มประชาชน เมื่อได้รับความเสียหายจากอาชญากรรมออนไลน์ ก็ทำให้ไม่อยากขอรับความช่วยเหลือ เพราะ

คิดว่า ‘เสียเวลาโดยสูญเปล่า’ ทำให้ผู้เสียหายหลายคนยอมแพ้ที่จะเข้าสู่กระบวนการดำเนินการทางกฎหมาย และเลือกที่จะยอมรับและจัดการความสูญเสียด้วยตัวเอง ซึ่งไม่เพียงจะเป็นการเอื้อประโยชน์กับเหล่ามิจฉาชีพแล้ว ยังเป็นการปิดโอกาสให้กับภาครัฐและหน่วยงานที่เกี่ยวข้องในการที่จะรับทราบข้อมูลที่เป็นประโยชน์ต่อการดำเนินการกับกลุ่มเครือข่ายมิจฉาชีพ อีกด้วย

“พอรัฐมีการโกงกันเยอะ เมืองไทยมีการโกงเยอะตั้งแต่โกงเข้ามาทำงาน เพราะฉะนั้นเราจะหวังให้คนเหล่านี้จะเป็นคนทำคดีได้อย่างไรและอีกภาคหนึ่งของคนทำงานให้รัฐเก่งๆ แต่ก็อาจจะเป็นมิจฉาชีพเองก็ได้” ผู้เสียหาย ค (การสื่อสารส่วนบุคคล, 28 มกราคม 2567)

“คิดว่าประชาชนต้องดูแลตัวเอง อาชญากรรมไปไกล ขณะที่หน่วยงานรัฐยังทำงานแบบวัวหายล้อมคอก ไม่ทันมิจฉาชีพ รัฐทำเพื่อเป็นหน้าเป็นตา ไม่ได้ทำเพื่อแก้ปัญหาให้ประชาชน ไม่มีการแก้ปัญหาที่เป็นรูปธรรม ถ้าเป็นผู้มีชื่อเสียงในสังคมอาจจะได้รับการแก้ไข” ผู้เสียหาย ฆ (การสื่อสารส่วนบุคคล, 5 กุมภาพันธ์ 2567)

“การรั่วไหลของข้อมูล เกิดขึ้นได้อย่างไร มีการวิเคราะห์ว่า อาจมีคนในหน่วยงานราชการเอาข้อมูลไปขายใน dark web หรือเปล่า” ผู้เสียหาย จ (การสื่อสารส่วนบุคคล, 11 กุมภาพันธ์ 2567)

“ไม่แจ้งความเลย เพราะรู้ยังไงก็ไม่ได้คืน พอเกิดเรื่องก็เลยเข้าไปดู ควรทำอะไรยังไงแล้วไปดู คนที่โดนแจ้งความไปก็ไม่เกิดอะไรขึ้น ทำอะไรไม่ได้ ไม่มีอะไรเกิดขึ้นเลย ได้แค่ทำใจ กลัวไม่อยากให้ตัวเองไปมีประวัติในการจดบันทึก ไม่อยากให้ชื่อเราไปยุ่งอะไรกับเรื่องแบบนี้ด้วย” ผู้เสียหาย ท (การสื่อสารส่วนบุคคล, 27 กุมภาพันธ์ 2567)

3.2.3 ความเอาใจเขามาใส่ใจเรา (Empathy) ในสังคมมีน้อย ผู้เสียหายถูกตีตราจากสังคม

ภาพมายาคติที่สร้างขึ้นในสังคมที่ว่า “เพราะโง่ เพราะโลภ เพราะหลง” ถึงต้องตกเป็นเหยื่อ เป็นการตอกย้ำความเจ็บปวดให้กับผู้เสียหายเพิ่มมากยิ่งขึ้น (Victim blaming) และเพราะไม่อยากถูกตราหน้าว่า “เพราะโง่ เพราะโลภ เพราะหลง” เลยทำให้ผู้เสียหายหลายคนเลือกที่จะไม่เล่าให้ใครฟัง และไม่ดำเนินการทางกฎหมายกับมิจฉาชีพ เพื่อหลีกเลี่ยงการตอกย้ำบาดแผลที่ถูกโจมตีจากมิจฉาชีพออนไลน์

ทั้งนี้ จากการศึกษาพบว่า “ทุกคน”สามารถที่จะตกเป็นเหยื่อการโจมตีจากมิจฉาชีพออนไลน์ได้เสมอ ไม่เกี่ยวกับเพศ วัย การศึกษา หน้าที่การงาน ฐานะทางสังคม หรือแม้แต่คนที่ตระหนักรู้ในเรื่องภัยไซเบอร์เป็นอย่างดีก็ตาม ดังนั้น การที่สังคมมองภาพผู้เสียหายว่าโง่ โลภ หลง และไม่ระวัง ถือเป็นการซ้ำเติมผู้เสียหาย ผู้ซึ่งควรที่จะได้รับความช่วยเหลือหรือเห็นใจจากสังคมมากกว่า โดยเฉพาะอย่างยิ่งโลกออนไลน์ที่ทุกคนสามารถแสดงความคิดเห็นได้อย่างเสรี เนื่องจากไม่ได้มีการเปิดเผยตัวอย่างชัดเจน การกล่าวโจมตีผู้เสียหายก็

ยิ่งทำได้ง่ายและมีมากขึ้น ความเห็นอกให้ใจในสังคม โดยเฉพาะในสังคมออนไลน์ (Social empathy) ต่อผู้เสียหายมีน้อยลง ซึ่งจะเป็นการบีบให้ผู้เสียหายรู้สึกโดดเดี่ยวและฟื้นฟูกลับมาสู่การดำรงชีวิตปกติได้ยากยิ่งขึ้น

“80% สื่อให้ภาพผู้เสียหายว่า โง่เอง ไม่ระวัง โทษผู้เสียหาย และไม่ได้ดูน่าสงสาร มี 20% ที่ดูน่าสงสาร” และ “การสอบสวนของตำรวจ ควรมีความเชี่ยวชาญด้านการสอบสวน การถามคำถามกับผู้เสียหายที่ดูมีความเห็นอกเห็นใจมากกว่าเป็นการ Blame ผู้เสียหาย และสื่อเองก็ต้องปรับตัว เพราะสื่อเป็นตัวการในการผลิตซ้ำภาพของผู้เสียหาย” ผู้เสียหาย ฉ (การสื่อสารส่วนบุคคล, 11 กุมภาพันธ์ 2567)

“บอกที่บ้านไม่ได้ ปรึกษาใครไม่ได้ โตขนาดนี้ ทำไมยังทำให้ถูกหลอก มันคือความไม่รู้ มันเอาความไม่รู้ ความสนใจมาเป็นช่องทางในการหลอกลวง เหมือนเราสนใจหางาน เราอาจจะไปพูดกับคนนั้นคนนี้แล้วมันก็เด้งขึ้นมา” ผู้เสียหาย ถ (การสื่อสารส่วนบุคคล, 24 กุมภาพันธ์ 2567)

“ไม่เล่าให้คนอื่นฟัง เพราะอายและกลัวโดนด่าว่าโง่” ผู้เสียหาย ธ (การสื่อสารส่วนบุคคล, 24 กุมภาพันธ์ 2567)

3.2.4 ไม่มีมาตรการหรือหน่วยงานช่วยในการเยียวยาผู้เสียหาย ผู้เสียหายต้องจัดการตัวเอง

การให้ความช่วยเหลือผู้เสียหายเพื่อให้สามารถกลับมาใช้ชีวิตปกติได้เป็นอีกหนึ่งประเด็นที่ภาครัฐและหน่วยงานที่เกี่ยวข้องจำเป็นต้องให้ความสำคัญ ที่ผ่านมาผู้เสียหายจำนวนมากต้องพึ่งพาตัวเองเพื่อให้ก้าวผ่านจากความสูญเสียที่เกิดขึ้น ทั้งนี้ อาชญากรรมออนไลน์ไม่ได้เพียงแค่สร้างความเสียหายทางด้านมูลค่าทรัพย์สิน หากแต่ยังรวมถึงสภาพจิตใจ ที่จำเป็นต้องได้รับการเยียวยา หลังจากที่ถูกโจมตีจากภัยไซเบอร์ ผู้เสียหายจำนวนมากต้องเผชิญกับปัญหาด้านการเงิน ไม่ว่าจะเป็นเสียทรัพย์สินของตัวเอง แต่อาจรวมถึงหนี้สินใหม่ที่ต้องแบกรับ ซึ่งเป็นผลพวงมาจากธุรกรรมที่เกิดขึ้นที่เกี่ยวข้องกับภัยโซเบอร์โดยที่ไม่ได้ตั้งใจ เมื่อไม่มีหน่วยงานที่จะช่วยแก้ไขหรือให้คำปรึกษาในเรื่องการเงินหรือด้านกฎหมายที่ชัดเจน ผู้เสียหายที่ไม่สามารถจัดการกับปัญหาดังกล่าวที่เกิดขึ้น จำนวนไม่น้อยที่ตัดสินใจปลิดชีพตัวเองเพื่อจบปัญหา ซึ่งเหตุการณ์เหล่านี้มีให้เห็นเพิ่มขึ้นในสังคม

นอกจากนี้ การฟื้นฟูสุขภาพจิตใจของผู้เสียหายก็ถือเป็นเรื่องสำคัญ เพราะผู้เสียหายหลายคนไม่สามารถที่จะเล่าให้ครอบครัวหรือคนใกล้ชิดของตัวเองฟังได้ การกล่าวโทษตัวเองซ้ำ ๆ และจมอยู่กับความทุกข์ที่เกิดจากการถูกทำร้ายจากอาชญากรรมออนไลน์ ทำให้การฟื้นฟูเพื่อกลับมาใช้ชีวิตอย่างปกติทำได้ยากยิ่งขึ้น

“หลายๆหน่วยงานที่เกี่ยวข้องยังไม่มีมาตรการชัดเจนที่ช่วยเยียวยาผู้เสียหาย ทั้งธนาคาร ตำรวจ สคบ. (สมาคมคุ้มครองผู้บริโภค)” ผู้เสียหาย ช (การสื่อสารส่วนบุคคล, 11 กุมภาพันธ์ 2567)

“อยากให้มีนักจิตวิทยาเข้ามาช่วยในการพูดคุยแลกเปลี่ยน / การพูดคุยระหว่างผู้เสียหายด้วยกัน” ผู้เสียหาย ซ (การสื่อสารส่วนบุคคล, 11 กุมภาพันธ์ 2567)

3.3 การสร้างการรู้เท่าทัน

3.3.1 ติดตามข่าวสารเพื่อให้รู้เท่าทันมิจฉาชีพ

จากการศึกษาพบว่า ประชาชนมีการรับรู้ข่าวสารในเรื่องอาชญากรรมออนไลน์ช่องทางที่แตกต่างกันตามการดำรงชีวิตและความสนใจของแต่ละคน เช่น บางคนรับรู้ผ่านสื่อหลัก เช่น โทรทัศน์หรือวิทยุ ขณะที่บางกลุ่มจะเป็นการรับข่าวสารผ่านสื่อออนไลน์และโซเชียลมีเดีย หรือบางกลุ่มก็มีการรับรู้น้อยมากแม้ว่าจะมีการใช้สื่อออนไลน์และโซเชียลมีเดียอย่างเป็นประจำ เนื่องจากระบบอัลกอริทึม (algorithm) เลือกนำเสนอข้อมูลที่ผู้ใช้สนใจเป็นหลัก ซึ่งข้อมูลนั้นอาจจะไม่เกี่ยวข้องกับเรื่องภัยไซเบอร์ ทำให้คนกลุ่มดังกล่าวไม่สามารถเข้าถึงข้อมูลเกี่ยวกับอาชญากรรมออนไลน์ต่าง ๆ ได้

“Facebook ไม่มีฟังก์ชันช่วยบล็อก ก็หลอกได้เรื่อย ๆ ถ้าจะให้อัลกอริทึมเลือกข้อมูลให้ แต่ก็ต้องมีวิธีที่ช่วยสแกนด้วย ไม่งั้นเพจปลอมพวกนี้จะเพียบ จะต้องช่วยกัน รัฐอาจจะไม่มีหน่วยงานที่ดูแลเรื่องนี้ก็ต้องไปต้อนให้พวกบริษัทโซเชียลที่มีสาขาในไทยช่วยนิดหนึ่ง และโปรโมทมากกว่านี้ สสส. (สำนักงานกองทุนสนับสนุนการเสริมสร้างสุขภาพ) ทำโฆษณาให้ความรู้ประชาชน คนไทยเป็นคนซื่อ ไม่น่าจะโดนหลอก แต่ก็โดน” ผู้เสียหาย ง (การสื่อสารส่วนบุคคล, 30 มีนาคม 2567)

“เป็นบางคนที่มีความตระหนักรู้ ถ้าแบบว่าผู้สูงอายุ กับคนที่ไม่ได้รับรู้ข่าวสารมีจำนวนมากอยู่เหมือนกัน ผู้สูงอายุ คนที่ไม่มีประสบการณ์โดนแบบเดียวกัน คิดว่าอาจจะมีโอกาส” ผู้เสียหาย ต (การสื่อสารส่วนบุคคล, 11 มีนาคม 2567)

“บางคนไม่ค่อยได้ติดตามข่าวออนไลน์มาก อาจจะต้องมีช่องทางการประชาสัมพันธ์ที่เข้าถึงตัวโดยตรง อย่างเช่นกับคนที่อยู่กับบ้าน ทำป้ายประชาสัมพันธ์ที่มันหลากหลายรูปแบบ ที่มากกว่าสื่อ เพราะบางคนไม่ได้ดูสื่อตลอด” ผู้เสียหาย ถ (การสื่อสารส่วนบุคคล, 24 กุมภาพันธ์ 2567

“คนที่เขาไม่ได้เข้าถึงสื่อ คนที่เขาไม่ได้ใช้โซเชียลมีเดีย ไม่มีอินเทอร์เน็ต ไม่มีสื่ออะไรที่จะแนะนำเตือนภัยอะไรเขาได้ ต่อให้เขาเตือนภัยบางคน ต่อให้คนที่เข้าถึงอย่างเรายังโดนเลย แล้วคนที่เขาไม่ได้อยู่ในโลกออนไลน์ ไม่ได้มีสื่อโทรทัศน์ หรือว่าอะไรเข้าถึงเขาก็คงช้ากว่าเราอยู่แล้ว มองว่ามันยังไม่โอเค ยังน้อยมากๆ” ผู้เสียหาย ท (การสื่อสารส่วนบุคคล, 27 กุมภาพันธ์ 2567)

3.3.2 ฉุกคิดและคิดเสมอว่ามีโอกาสถูกโจมตีได้ตลอดเวลา แม้จะเคยถูกโจมตีมาแล้ว

การสร้างความตระหนักในปัญหาภัยไซเบอร์ นอกจากจะมุ่งเน้นให้ความรู้แก่ประชาชนแล้ว สิ่งสำคัญที่เป็นด่านกันภัยสำหรับประชาชนก่อนที่จะหลงกลเหล่ามิจฉาชีพออนไลน์ คือ การฉุกคิด ไม่ชะล่าใจ แม้จะมีการป้องกันที่ดีแล้ว หรือเคยถูกโจมตีมาแล้ว เพราะจากทฤษฎีเกี่ยวกับเหยื่ออาชญากรรม พบว่าคนที่เคยเป็นเหยื่อแล้ว อาจจะตกเป็นผู้เสียหายซ้ำได้

วิธีการที่เห็นผลช่วยให้ประชาชนหยุดคิดได้บ้างก่อนที่จะหลงกลเหล่ามิจฉาชีพออนไลน์ เช่น การที่แอปพลิเคชันธนาคารมีการเตือนอีกรอบการก่อนทำธุรกรรม หรือมีการติดประชาชาสัมพันธ์เตือนเกี่ยวกับภัยไซเบอร์และเบอร์ติดต่อเพื่อขอความช่วยเหลือในที่สาธารณะที่สามารถพบเห็นได้ง่าย เป็นต้น

“อะไรที่มาเป็นแบบ too good to be true ต้องตั้งคำถามไว้ก่อน” ผู้เสียหาย ง (การสื่อสารส่วนบุคคล, 30 มีนาคม 2567)

“เรื่องของการลงทุน หรือการซื้อของ ถ้ามันได้เงินมาไว ก็ให้คิดไว้ว่าไม่มีหรอก น่าจะโดนหลอก” ผู้เสียหาย ถ (การสื่อสารส่วนบุคคล, 24 กุมพาพันธ์ 2567)

3.3.3 แบ่งปันประสบการณ์การที่เกิดขึ้นให้กับคนรอบข้าง เพื่อสร้างการตระหนักรู้และป้องกัน

การแบ่งปันเรื่องราวให้คนรอบข้างหรือสังคมได้รับรู้ ก็เป็นอีกหนึ่งช่องทางที่ช่วยช่วยสร้างการตระหนักรู้ให้กับสังคม และขณะเดียวกันก็ถือเป็นการช่วยเยียวยาจิตใจผู้ที่ได้รับความเสียหาย ซึ่งได้ระบายและบอกเล่าเรื่องราวต่าง ๆ ที่เกิดขึ้นออกมา เช่น ผู้เสียหาย ช (การสื่อสารส่วนบุคคล, 11 กุมภาพันธ์ 2567) ที่เล่าเรื่องภัยออนไลน์ที่เกิดขึ้นกับตนเองให้กับเพื่อนและคนรอบตัวฟัง เนื่องจากไม่อยากให้คนอื่นต้องถูกกระทำแบบตัวเอง เช่นเดียวกับผู้เสียหาย ซ (การสื่อสารส่วนบุคคล, 11 กุมภาพันธ์ 2567) ที่แบ่งปันประสบการณ์ที่เกิดขึ้นให้กับกลุ่มออนไลน์เพื่อเตือนภัยให้สมาชิกในกลุ่มระวังตัว

“รู้ตัวตอนใช้ Twitter บอกว่าตัวเองกำลังเจอเหตุการณ์แบบนี้ และก็มีหนึ่งในผู้เสียหายเข้ามาแสดงตนและบอกว่าโดนเพื่อนออนไลน์คนนี้หลอกเหมือนกัน และได้ตรวจสอบข้อมูลจากผู้ใช้ Twitter ท่านอื่นที่ได้โพสต์ข้อมูลไว้ และพบว่ามี 1 บัญชี (ชื่อบัญชีรับเงิน) ที่ตรงกับชื่อบัญชีที่ได้โอนเงินไป จึงได้ส่งข้อความหาผู้ใช้ Twitter ที่ได้โพสต์ข้อมูล และพบว่ามีผู้เสียหายกว่า 20 ราย” ผู้เสียหาย ฉ (การสื่อสารส่วนบุคคล, 11 กุมภาพันธ์ 2567)

บทที่ 4
ผลการศึกษาจากหน่วยงานที่เกี่ยวข้อง

การศึกษาในครั้งนี้ได้ทำการสัมภาษณ์เชิงลึก (In-depth interview) บุคลากรจากหน่วยงานที่เกี่ยวข้อง จำนวน 14 คน ที่มีความเชี่ยวชาญและมีบทบาทหน้าที่ที่เกี่ยวข้องกับการทำงานด้านภัยออนไลน์ในมิติต่าง ๆ ทั้งจากภาครัฐ เอกชน และ สื่อ โดยมีข้อค้นพบตามประเด็นดังต่อไปนี้

4.1 ปัจจัยที่นำไปสู่การถูกหลอกลวง

ผู้ให้ข้อมูลส่วนใหญ่มองว่า ปัญหาภัยออนไลน์ที่เกิดขึ้นสืบเนื่องมาจากปัญหาหลักๆ ได้แก่

4.1.1 ขาดข้อมูล (Digital divide/ Digital literacy/ Digital hygiene)

การถูกหลอกลวงเป็นผลมาจากประชาชนไม่ได้รับข่าวสารหรือไม่ติดตามข่าวสารเกี่ยวกับภัยออนไลน์ทางช่องทางต่าง ๆ เพราะพฤติกรรมการเสพข่าวของประชาชนแต่ละคนมีความแตกต่างกัน ทำให้ขาดข้อมูลและความตระหนักรู้ต่อภัยออนไลน์

“บางคนไม่ตามข่าว คนเรามีเป้าหมายไม่เหมือนกัน เสพข่าวไม่เหมือนกัน ยิ่งต่างจังหวัดจะมีคนซื่อ ทำตามโดยง่าย โดนหลอกให้กดก็กดตามเขาไป หรือกรณีที่ไม่ค่อยมีคนโทรหาหรือส่งข้อความมา แล้วดีใจจนโดนหลอก ซึ่งเป็นความชะล่าใจของตัวเราเอง” (ผู้เชี่ยวชาญด้านจิตวิทยา สัมภาษณ์ 5 กุมภาพันธ์ 2567)

“สาเหตุหนึ่งที่ทำให้ผู้เสียหายหลงเชื่อ เนื่องจากบางคนไม่ได้รับข่าวสารและสกู๊ปข่าวต่าง ๆ เกี่ยวกับภัยออนไลน์ ซึ่งสื่อของเราเป็นสื่อกลางเพื่อสร้างการรับรู้ให้ประชาชน ต้องคิดว่าจะทำอย่างไรดีให้เราได้เป็นสื่อกลางทุกพื้นที่ และทุกครอบครัว” (นักสื่อมวลชน สัมภาษณ์ 15 กุมภาพันธ์ 2567)

4.1.2 โซเชียลมีเดีย / แพลตฟอร์ม / เทคโนโลยี

ปัจจัยสำคัญประการหนึ่งที่ทำให้มีผู้ถูกหลอกลวงก็คือ การพัฒนาทางเทคโนโลยี การใช้สื่อสังคมออนไลน์หรือโซเชียลมีเดียในแพลตฟอร์มต่าง ๆ มาเป็นเครื่องมือในการหลอกลวง เนื่องจากเป็นแหล่งรวบรวมข้อมูลขนาดใหญ่ (Big data) มีระบบอัลกอริทึม (Algorithm) ที่คัดสรรสิ่งที่ผู้บริโภคให้ความสนใจ โดยพิจารณาจากตัวแปรต่าง ๆ เช่น การเลือกรับสาร การรับชมโฆษณา ฯลฯ ทำให้เกิดการใช้โซเชียลมีเดียหลายแพลตฟอร์มร่วมกันในการหลอกลวง เช่น เฟซบุ๊กทำให้ผู้บริโภคเห็นและเข้าไปดูข้อมูล เมื่อผู้บริโภคหลงเชื่อก็จะโน้มน้าวให้เพิ่มเพื่อนในไลน์ จากนั้นใช้ไลน์ในการส่งข้อมูล เพราะเป็นแอปพลิเคชันที่ใช้งานง่าย ได้รับความนิยมจากประชาชนไทย มีรูปแบบการสื่อสารที่น่าเชื่อถือ เช่น ไลน์กลุ่ม, โอเพนแชท (OpenChat) ฯลฯ ซึ่งการ

ตรวจสอบก็เป็นไปได้ยาก นอกจากนี้ ยังมีการใช้โทรศัพท์ในการหลอกลวงผู้บริโภคด้วย โดยปัจจุบันมีการสร้างเบอร์ปลอม ส่งข้อความ (SMS) ปลอม ซึ่งทำให้หน่วยงานที่เกี่ยวข้องไม่สามารถบล็อกเบอร์ได้อย่างถูกจุด สอดคล้องกับรายงานขององค์การตำรวจอาชญากรรมระหว่างประเทศ (International Criminal Police Organization: Interpol) หรือที่เรียกกันสั้น ๆ ว่า ตำรวจสากล (2022) พบว่า อาชญากรรมออนไลน์เป็น 1 ใน 5 อาชญากรรมที่เกิดขึ้นมากสุดในโลก การใช้อีเมลหรือเว็บไซต์ปลอมหรือที่เรียกว่าฟิชชิง (Phishing) มิจฉาชีพออนไลน์ (Online scam) และการเจาะระบบคอมพิวเตอร์ (computer intrusions) ถือเป็นภัยคุกคามในระดับที่รุนแรงหรือรุนแรงมากสุดในโลก

“จุดเริ่มต้นของการหลอกลวงมาจากการโฆษณาบนโซเชียลมีเดีย สิ่งที่เหยื่อจะเห็นคือโฆษณาผ่านลิงก์ในแอปพลิเคชัน 100%เมื่อเราอยากดูหรือมีความชอบในเรื่องตรงนี้มันก็จะเยอะขึ้น พอขึ้นมารวมกับคอนเทนต์ที่เราเสพอยู่ทุกวัน เรามองเห็นเป็นอันดับต้นๆ เดี๋ยวมันก็มาอีก จนกระทั่งเรารู้สึกว่ามันตรงใจ แล้วก็เข้าไปสนใจ เริ่มติดต่อถูกกลไกการหลอกลวง” (เจ้าหน้าที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) สัมภาษณ์ 21 กุมภาพันธ์ 2567)

“มิจฉาชีพเข้ามาทั้งในออนไลน์และออฟไลน์โดยใช้เทคโนโลยี โลกออนไลน์มีข้อมูลมาก มีระบบอัลกอริทึมทำให้คนเราเจอแต่สิ่งที่เราสนใจ เช่น เซียนพระเข้าเน็ตไปก็จะเจอแต่เซียนพระ” (ผู้เชี่ยวชาญด้านจิตวิทยา สัมภาษณ์ 5 กุมภาพันธ์ 2567)

4.1.3 กลยุทธ์ของมิจฉาชีพ

มิจฉาชีพมีการปรับเปลี่ยนกลยุทธ์ให้สอดคล้องกับกลุ่มเป้าหมายมากขึ้น สร้างความน่าเชื่อถือของข้อมูล โดยใช้ฐานข้อมูลที่ไหลรั่วออกมาจากหน่วยงานสำคัญต่าง ๆ และใช้ข้อมูลใกล้ชิดกับตัวประชาชน เช่น ข้อมูลส่วนตัว ประวัติการทำธุรกรรม การเกษียณ ฯลฯ การดำรงชีพในชีวิตประจำวัน สอดคล้องกับ การพัฒนาทฤษฎีกิจวัตรประจำวัน (Routine activities theory) ของ Cohen และ Felson ที่มีแนวคิดว่า การที่คนเรามีกิจวัตรประจำวัน หรือมีกิจกรรมที่กระทำบ่อยครั้งเป็นประจำสม่ำเสมอ จะเป็นการเปิดช่องให้อาชญากรที่คอยสังเกตอยู่สามารถวางแผนกระทำความผิดต่อบุคคลนั้นได้ หรือการใช้เทคนิควิศวกรรมสังคม (social engineering) อันเป็นศิลปะในการหลอกลวงที่ใช้หลักการทางจิตวิทยาให้เหยื่อเปิดเผยข้อมูล ทำให้สามารถเจาะกลุ่มเป้าหมายได้อย่างแม่นยำยิ่งขึ้น ซึ่งจะพบว่าผู้ถูกหลอกลวงไม่ใช่เพียงคนมีการศึกษาน้อยเท่านั้น แต่ยังรวมไปถึงกลุ่มที่มีการศึกษา และกลุ่มมิจฉาชีพด้วยกันเอง โดยมูลค่าความเสียหายเพิ่มขึ้นเรื่อย ๆ เพราะเหยื่อเป็นกลุ่มที่มีฐานะการเงินดี แต่ละรายมักจะถูกหลอกลวงเป็นจำนวนเงินหลักแสนหรือหลักล้าน เนื่องจากเหยื่อถูกหลอกล่อด้วยหลักจิตวิทยาให้เกิดการหลงเชื่อ

“สถิติเรื่องแจ้งความนี้ลดลง แต่ความเสียหายที่เกิดขึ้นมีมูลค่าเพิ่มขึ้น โดยความหมายก็คือ โจรเจาะกลุ่มเป้าหมายได้แม่นยำขึ้น เช่น พรุ่งนี้เราเกษียณ เขาโทรหาเราแล้วบอกว่าติดต่อมามอบเงินบำเหน็จบำนาญ คนเกษียณก็เชื่อ เพราะข้อมูลมีความใกล้ชิดกับตัวเขามาก จนทำให้เกิดความน่าเชื่อมากขึ้น ถามว่าเพราะอะไร เพราะข้อมูลมีความน่าเชื่อมาก จนทำให้คนหลงเชื่อได้ง่ายขึ้น” (เจ้าหน้าที่สำนักงานคณะกรรมการกิจการกระจายเสียงและกิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) สัมภาษณ์19 กุมภาพันธ์ 2567)

4.1.4 พฤติกรรรมศาสตร์/จิตวิทยา

ปัจจัยส่วนบุคคลที่ทำให้ประชาชนถูกหลอกลวง คือ การขาดความรู้ ขาดความตระหนัก ขาดการควบคุมตนเอง ซึ่งปัจจัยเหล่านี้ไม่สามารถทำงานได้อย่างเต็มที่ แต่หากมีตัวกระตุ้นก็สามารถส่งผลกระทบอย่างรุนแรงได้ อาจกล่าวได้ว่า ในภาพรวมนั้นไม่ได้มีเพียงสาเหตุใดสาเหตุหนึ่งที่ทำให้คนเกิดพฤติกรรมจนนำไปสู่การถูกหลอกลวง เนื่องจากแต่ละคนมีบริบทแวดล้อมแตกต่างกัน เช่น สถานที่พำนักอาศัย ช่วงเวลาที่ถูกหลอกลวง ปัจจัยทางจิตใจ ฯลฯ เมื่อประกอบกับลักษณะนิสัยโดยพื้นฐานของคนไทยที่มีความไว้ใจหรือเชื่อใจคนง่าย รวมทั้งชอบซื้อสินค้าราคาถูกกว่าตลาด ชอบเสี่ยงโชค ชอบปฏิสัมพันธ์กับเพื่อนใหม่ จึงเป็นองค์ประกอบที่เอื้อให้มิจฉาชีพทำงานง่ายขึ้น เช่น ทำสลิปเงินปลอม เพราะแม่ค้ามักจะชะล่าใจ ไม่ดูสลิปการโอนเงิน, มิจฉาชีพทำทีช่วยเหลือผู้สูงอายุในการกดเงินสดผ่านตู้เอทีเอ็ม การหลอกให้รัก (Romance scam) ฯลฯ อย่างไรก็ตาม หากเหยื่อมีสภาพแวดล้อมใกล้ตัว เช่น ครอบครัว เพื่อน ชุมชน สื่อ ฯลฯ ที่ให้ความช่วยเหลือกัน ก็จะสามารถช่วยสร้างพฤติกรรมป้องกันให้เกิดขึ้นได้ ซึ่งสอดคล้องกับแนวคิดวิศวกรรมสังคม (Social engineering) ว่าด้วยเรื่องการโจมตีรูปแบบหนึ่งทางออนไลน์ ซึ่งมีการใช้ความรู้ทางจิตวิทยาในการสร้างสถานการณ์ต่าง ๆ ประกอบกับการใช้ศาสตร์และศิลป์ทางคอมพิวเตอร์เพื่อเข้าถึงระบบของอีกฝ่าย โดยอาศัยช่องโหว่จากพฤติกรรมของผู้ใช้งาน (Harl, 1997)

“หากมองลึกลงไปในระดับบุคคล ระดับของสาเหตุที่ส่งผลต่อการเกิดพฤติกรรม หรือการตกเป็นเหยื่อไม่เท่ากัน เพราะแต่ละคนมีบริบท ช่วงเวลา สถานที่ที่ต่างกัน ดังนั้น หากมองในภาพรวมหรือค่าเฉลี่ยของคนส่วนใหญ่ จะวิเคราะห์ว่าสาเหตุที่ทำให้คนถูกหลอกลวง คือ คนขาดความรู้ ขาดความตระหนัก ขาดการควบคุมตน สิ่งเหล่านี้เป็นปัจจัยส่วนบุคคล เราจะมองว่าปัจจัยส่วนบุคคลทำงานได้ไม่เต็มที่หรอก แต่หากอยู่ในครอบครัว สังคม สื่อ เพื่อนช่วยเพื่อน มันก็จะเป็นตัวช่วยให้เกิดพฤติกรรมป้องกัน ดังนั้น ตัวแปรสภาพแวดล้อมจึงสำคัญ” (เจ้าหน้าที่สถาบันวิจัยพฤติกรรมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ สัมภาษณ์ 20 กุมภาพันธ์ 2567)

“คนรู้เยอะ แต่คนไม่รู้เยอะกว่า บางทีรู้นะว่ามี Call center แต่จิตวิทยาที่เขาใช้มันดีมาก ๆ ที่ทำให้เชื่อและโดนหลอก และข้อมูลก็สำคัญกับประชาชน เราทำไปเยอะมาก แต่ก็มีคนที่ยังถูกหลอก แสดงว่าเรา

ประชาสัมพันธ์ยังไม่ตรง หรือมันไม่โดนจริง ๆ เพราะคนที่โดนคือคนที่รู้ และเป็นคนมีเงิน” (เจ้าหน้าที่สำนักงานกสทช. สัมภาษณ์ 19 กุมภาพันธ์ 2567)

4.2 ความท้าทายในการรับมือ

ผู้ให้ข้อมูลส่วนใหญ่มองว่า ความท้าทายของปัญหาในการรับมือ ได้แก่

4.2.1 การทำงานยังไม่ครอบคลุมปัญหา

การทำงานยังขาดความครบถ้วน ขาดการทำความเข้าใจปัญหาโดยแท้จริงว่ามีองค์ประกอบอะไรบ้าง เช่น เฟซบุ๊กเป็นส่วนหนึ่งของวงจรการหลอกให้ลงทุน และแอปพลิเคชันดูดเงิน ในฐานะเครื่องมือหลอกลวงประชาชน แต่มีวิธีการใช้คนละแบบในแต่ละกรณี จึงต้องแยกแยะประเภทของวิธีดำเนินการ

“เราต้องแยกองค์ประกอบ อย่างเช่น เฟซบุ๊ก ก็เป็นส่วนหนึ่งใน Cycle ของการหลอกบางส่วน เช่น หลอกให้ลงทุน ซึ่งมันอาจจะมีความแตกต่างกันพอสมควรกับแอปพลิเคชันดูดเงิน ศูนย์ AOC ก็ไม่ได้รองรับได้ทั้งหมด หรือไม่ได้มีการแยะประเภทของสิ่งเหล่านี้ไว้ การดำเนินการก็ต่างกัน อย่างเช่น เราไม่มีส่วนที่จะบอกให้ปิดเฟซบุ๊กทันที สกมช เห็นก็เลยเข้าไปช่วย ดังนั้นเรายังไม่ครบ” (เจ้าหน้าที่สำนักงานสกมช. สัมภาษณ์21 กุมภาพันธ์ 2567)

“การประกอบกิจการของผู้ที่ได้รับอนุญาตในหลายๆ ประเภทยังมีช่องว่างที่ทำให้เกิดการใช้ประโยชน์ของแก๊งคอลเซ็นเตอร์ หรือว่ากลุ่มที่ก่ออาชญากรรม เช่น การให้บริการโทรศัพท์มือถือ มีการตั้งสถานีฐานโทรศัพท์เคลื่อนที่ ถ้าตั้งในแนวชายแดนแล้วหันทิศทางของเสาออกไป จะทำให้เกิดการใช้ประโยชน์จากกลุ่มพวกนี้... ถ้าการกำกับการประกอบกิจการมีความเข้มแข็ง การที่ผู้ให้บริการหรือผู้ได้รับใบอนุญาตจากเราจะนำไปให้มิจฉาชีพใช้ประโยชน์ก็มีโอกาสน้อย” (เจ้าหน้าที่สำนักงานกสทช. สัมภาษณ์ 19 กุมภาพันธ์ 2567)

4.2.2 จรรยาบรรณในการช่วยเหลือประชาชน

ในการทำงานของภาคส่วนที่เกี่ยวข้องเกิดปัญหาด้านจริยธรรมและจรรยาบรรณในการปฏิบัติงาน เช่น ตำรวจสื่อสารกับประชาชนที่ไปขอความช่วยเหลืออย่างไม่เหมาะสม มีการตวาด หรือติดต่อยาก หรือความล่าช้าในการติดตามคดี สื่อมวลชนอาจนำเสนอข้อมูลผู้เสียหายมากเกินไป ซึ่งโดยหลักแล้วต้องป้องกันอันตรายให้แก่ผู้เสียหาย โดยปกปิดข้อมูลส่วนบุคคล รวมทั้งห้ามซ้ำเติมผู้เสียหาย แต่ต้องให้กำลังใจ

“ต้องเซฟผู้เสียหาย เพราะอาจจะเป็นอันตรายต่อแหล่งข่าว ทั้งชื่อ เสื้อผ้า หน้าผม ใช้นามสมมติแทน บางเคสครอบครัวยังไม่รู้ต้องปกปิด นักข่าวจะสัมผัสได้ว่าผู้เสียหายรู้สึกอย่างไร เขาดาวน์ เขาอยากฆ่าตัวตาย... ไม่ใช่ทุกสื่อที่สามารถรับเรื่องร้องเรียนได้ เพราะเขาอาจจะไม่ได้สัมผัสผู้เสียหายโดยตรง รับข่าวมาอีกทีเพื่ออ่านเอามัน หรือความนิยม” (นักสื่อสารมวลชน สัมภาษณ์ 15 กุมภาพันธ์ 2567)

4.1.5 ปัญหาด้านการทำงานของภาครัฐ

จากการเก็บข้อมูลพบว่า การทำงานของภาครัฐต้องเผชิญกับปัญหาหลากหลายประการ ได้แก่

4.1.5.1 ขาดมาตรการเชิงรุก

หน่วยงานภาครัฐต่าง ๆ ทำหน้าที่ในส่วนของการรับมือและการป้องกัน แต่ยังขาดการทำงานหรือมาตรการเชิงรุกกับประชาชน จึงทำได้เพียงตั้งรับเป็นหลัก แม้ว่าจะมีการออกกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 เป็นต้น แต่ก็ยังไม่สามารถสร้างความเกรงกลัวให้แก่อาชญากรได้ เนื่องจากกฎหมายยังขาดบทลงโทษที่จริงจัง อีกทั้งภัยไซเบอร์มีความแตกต่างจากภัยประเภทอื่น ๆ ในประเด็น “ไม่รู้ตัวผู้กระทำ” และหน่วยงาน “ช้ากว่าอาชญากร” เพราะอาชญากรมีการอัปเดตข้อมูลและวิธีการใหม่ๆ อย่างต่อเนื่อง ขณะที่ประชาชนในปัจจุบันมีองค์ความรู้มากขึ้นกว่าเมื่อ 5-6 ปีที่ผ่านมา แต่ก็ยังไม่ทันกับรูปแบบอาชญากรรมที่เข้ามาประชิดตัวได้เร็วขึ้น ประชาชนและเจ้าหน้าที่จึงต้องมีการเรียนรู้ไปพร้อมกัน เพื่อนำมาช่วยปรับวิธีการรับมือ สอดคล้องกับแนวคิดของ Jeremy Douglas ผู้แทน U.N. Office on Drugs and Crime (Vitjitra Duangdee, 2022) เตือนว่า กลุ่มมิจฉาชีพออนไลน์เหล่านี้จะย้ายฐานการปฏิบัติการไปยังพื้นที่ในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่มีการบังคับกฎหมายที่ไม่เข้มงวด เว้นแต่รัฐบาลในกลุ่มประเทศอาเซียนจะร่วมมือกันในการจัดการกลุ่มมิจฉาชีพเหล่านี้

“หากกฎหมายมีความรุนแรงสามารถทำให้คนกลัว ก็จะหยุดการกระทำ แต่อาชญากรสามารถชั่งน้ำหนักได้ เพราะโทษไม่รุนแรง เมื่อเทียบกับมูลค่าที่อาชญากรสามารถทำได้ และก็ไม่สามารถรู้ตัวผู้กระทำได้ จึงเสี่ยงที่จะทำ มันจึงเป็นความท้าทาย ดังนั้น ต่อให้มีการอัปเดตฐานข้อมูลเรื่องรูปแบบอาชญากรรมออนไลน์มากแค่ไหน อาชญากรก็ยังนำหน้าเสมอ” (ผู้เชี่ยวชาญด้านอาชญาวิทยา สัมภาษณ์ 14 กุมภาพันธ์ 2567)

4.1.5.2 การทำงานแบบแยกส่วน (Silo)

หน่วยงานภาครัฐมีลักษณะการทำงานแบบต่างฝ่ายต่างทำ แต่ละคนจะรู้เฉพาะงานในส่วนของตนเอง แต่ไม่รู้ภาพรวมหรืองานของคนอื่น ๆ เนื่องมาจากขาดการสื่อสารที่ชัดเจน ทำให้ไม่สามารถแลกเปลี่ยนความร่วมมือระหว่างกันได้ ซึ่งเป็นข้อจำกัดในการช่วยเหลือผู้เสียหาย แม้ว่าจะมีองค์ความรู้ครบถ้วนและหน่วยงานที่เกี่ยวข้องจำนวนมาก แต่ขาดการบูรณาการที่มีประสิทธิภาพ ทำให้ประชาชนสับสนว่าเมื่อเกิดเหตุการณ์ขึ้นแล้วควรติดต่อที่หน่วยงานใด ขาดจุดบริการแบบครบวงจร (One stop service) กระบวนการและขั้นตอนของหน่วยงานยังไม่สามารถช่วยในการยับยั้งการเกิดเหตุหลอกลวงได้ นอกจากนี้ก็ยังมีปัญหาในด้าน

การแบ่งปันข้อมูลระหว่างหน่วยงานที่เกี่ยวข้อง ซึ่งอาชญากรก็อาศัยช่องว่าง (Gap) เหล่านี้ในการก่อเหตุ สอดคล้องกับแนวทางการเยียวยาผู้เสียหายของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และ สำนักงานตำรวจแห่งชาติ (สตช.) รวมถึงหน่วยงาน ที่เกี่ยวข้อง ได้เปิดศูนย์รับแจ้งความออนไลน์อาชญากรรมทางเทคโนโลยี ผ่านเว็บไซต์ www. thaipoliceonline.co.th แต่ปัจจุบันการแจ้งความออนไลน์ยังทำได้เฉพาะคดีอาชญากรรมทางเทคโนโลยี นอกเหนือจากหมวดหมู่นี้ ยังคงต้องเดินทางไปแจ้งความที่โรงพักในท้องที่ที่เกิดเหตุ

“หน่วยงานมีเยอะ แต่ไม่สามารถรวมหน่วยงานได้ เนื่องจากเป็นภารกิจที่ไม่ได้ร่วมกันตั้งแต่ต้น ภาคีมีอยู่มากมาย แต่มีแค่ชื่อ จะทำอย่างไรให้คนเหล่านี้เข้ามาทำงานร่วมกัน ในขณะเดียวกันถ้าบังคับให้มาทำงานเฉพาะด้านนี้ไม่ได้ ก็ต้องจัดตั้งขึ้นมาใหม่และทุกคนมี mission เดียวกัน value เดียวกันก็น่าจะเป็นหน่วยงานที่ดี” (เจ้าหน้าที่สถาบันวิจัยพฤติกรรมศาสตร์ฯ สัมภาษณ์ 20 กุมภาพันธ์ 2567)

“พ.ร.ก. เขียนไว้อยู่แล้วว่าค่ายมือถือแลกเปลี่ยนข้อมูลกัน ระงับยับยั้ง มีหน้าที่ในการป้องกัน และธนาคารก็ทำแบบเดียวกัน แต่ปัญหาที่เกิดขึ้นคือค่ายมือถือก็ไม่คุยกันเอง ธนาคารก็ไม่คุยกันเอง เพราะลึกๆ แล้วเขาก็หวงข้อมูลระหว่างกัน ไม่อยากแชร์ข้อมูลลูกค้าให้อีกฝ่ายหนึ่งรับรู้” (เจ้าหน้าที่ตำรวจ กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ (บช.สอท.) สัมภาษณ์ 19 กุมภาพันธ์ 2567)

“การทำงานของหน่วยงานหลักอาจยังไม่เพียงพอที่จะช่วยประชาชนรับมือ ความเป็นหน่วยงานมีเพียงพอต่อการมอนิเตอร์ แต่สิ่งสำคัญคือจะทำอย่างไรให้ประชาชนเข้าถึง หรือมีเครื่องมือติดตัวช่วยเหลือประชาชนได้... ในส่วนของบ้านเรา องค์ความรู้มีพร้อม แต่ขาดเรื่องบูรณาการ ต่างคนต่างทำ จึงทำให้ประชาชนสับสนว่า เมื่อเกิดเหตุการณ์ขึ้นแล้ว ควรไปแจ้งที่หน่วยงานใด” (ผู้เชี่ยวชาญด้านอาชญาวิทยา สัมภาษณ์14 กุมภาพันธ์ 2567)

“กว่าเราจะคุยกัน ออกกฎหมาย มันใช้เวลานาน พอออกกฎหมายมาแล้วก็ยังมีปัญหาการบังคับใช้ที่ยังมาตีความตามกฎหมายว่าตกลงทำได้ไหม อำนาจตามกฎหมายมันทำได้แค่ไหน อย่างไร ผิด PDPA ไหม คุณมีหน้าที่ในการระงับยับยั้งแลกเปลี่ยน คุณระงับเองก็ได้ ทำได้หมดทุกอย่าง แต่ก็ยังบอกว่าไม่สบายใจอยากจะให้ตำรวจหรือเจ้าหน้าที่เป็นคนสั่งแล้วก็ทำ” (เจ้าหน้าที่ตำรวจบช.สอท. สัมภาษณ์, 19 กุมภาพันธ์ 2567)

“ทุกภาคส่วนทั้งรัฐเอกชน ต้องมามีส่วนร่วม คนที่ถูกหลอกผู้เสียหาย ตอนนี้ไต่ระดับเล็กลงไปเรื่อย ๆ เพราะมีมือถือ โซเชียล เด็กผู้สูงอายุ จะถูกมิจฉาชีพหลอกได้ ตอนนี้ไม่ได้ระบุว่าอายุน้อยมาก จะกระจายอยู่ที่โซเชียลได้มากที่สุด การศึกษา อายุ เพศ ไม่เกี่ยว” (เจ้าหน้าที่ตำรวจทั่วไป สัมภาษณ์ 13 กุมภาพันธ์ 2567)

4.1.5.3 ปัญหาทรัพยากรบุคคล (Human resource) หรือกำลังคน (Manpower)

แม้ว่ากฎหมายได้ให้อำนาจและวิธีการกับตำรวจอย่างเต็มที่แล้ว โดยกฎหมายไม่ได้บอกว่าให้ใช้พนักงานสอบสวน แต่ใช้คำว่า “พนักงานผู้มีอำนาจดำเนินคดีอาญา” ซึ่งทางตำรวจก็มองว่าอาจให้เจ้าหน้าที่อื่น ๆ เช่น นักสืบของตำรวจ สามารถปฏิบัติหน้าที่ตรงนี้ได้ แต่หน่วยงานที่เกี่ยวข้อง เช่น ธนาคาร ผู้ให้บริการสัญญาณมือถือ ต่างก็ต่อต้าน เนื่องจากทุกคนรู้สึกปลอดภัยกับการใช้วิธีแบบเดิมที่ใช้อำนาจพนักงานสอบสวน อย่างไรก็ตาม ภาระจะตกอยู่ที่พนักงานสอบสวน ซึ่งมีจำนวนไม่เพียงพอ ทั้งยังมีภาระงานจำนวนมาก และภัยไซเบอร์ก็ยากต่อการจับกุมอาชญากรซึ่งส่วนใหญ่อยู่นอกประเทศ อีกประเด็นคือการสื่อสารให้ประชาชนรับรู้ช่องทางในการร้องเรียนภัยไซเบอร์ยังไม่ประสบผลสำเร็จ ทำให้ประชาชนมุ่งตรงมาที่ตำรวจเพียงอย่างเดียว แม้ว่าจะมีช่องทางอื่น ๆ อีกก็ตาม

“ปัญหาคือพอเคสเข้ามาที่ตำรวจ เวลาตำรวจไปขอข้อมูล มันไม่ได้เร็ว มันใช้เวลา และคดีก็ถาโถมมาเรื่อย ๆ คดีเร่งด่วนก็เข้ามา มีเวลาโฟกัสในการทำคดีออนไลน์จริง ๆ น้อยมาก... พนักงานสอบสวนทั้งของไซเบอร์และทั่วไปที่เป็นหัวใจในการรับสำนวนมันมีจำนวนไม่เยอะ ดังนั้น พนักงานสอบสวนจึงเป็นจุดวิกฤตของตำรวจไซเบอร์ แล้วบัญชีม้าและการอายัดเงินต้องใช้พนักงานสอบสวน ทุกอย่างจะถาโถมคนที่เป็นพนักงานสอบสวน คนที่เราบอกว่ามีน้อยมากที่สุด แต่เราต้องไปให้เขาทำหมดเลย มันก็ยิ่งหนัก” (เจ้าหน้าที่ตำรวจบช.สอท. สัมภาษณ์19 กุมภาพันธ์ 2567)

“คนไม่รู้ว่าจะต้องไปหาหน่วยงานไหน ภาระจึงไปตกที่ตำรวจ เรื่องร้องเรียนในกิจการโทรคมนาคมน้อยลง เพราะคนไม่รู้ ขี้เกียจคุยกับเอไอ มันต้องวิเคราะห์ว่าทำไมการร้องเรียนถึงลดลง หรือคนไม่รู้เบอร์ 1200 เพราะฉะนั้นการกด 191 มันง่ายกว่า” (เจ้าหน้าที่สถาบันวิจัยพฤติกรรมศาสตร์ฯ สัมภาษณ์ 20 กุมภาพันธ์ 2567)

“เจ้าหน้าที่ตำรวจสอบสวน 1 คน ต่อหนึ่งสำนวน และ 1 คนแจ้ง ถ้าเคสออนไลน์ เจ้าหน้าที่ไม่เพียงพอ ทำงานภายใต้กรอบในมนุษย์ที่จะทำได้ ประสิทธิภาพประสิทธิผลอาจจะไม่ได้เพียงพอ ลำบากใจว่าจะเลือกเคสไหนสำคัญที่สุด มันยากในการเลือกช่วยเหลือ เพราะทุกคนก็อยากได้ความคืบหน้า” (เจ้าหน้าที่ตำรวจทั่วไป สัมภาษณ์13 กุมภาพันธ์ 2567)

4.1.5.4 ความเชี่ยวชาญ

หน่วยงานแต่ละฝ่ายต่างก็มีความเชี่ยวชาญ แต่กลับไม่สามารถทำหน้าที่ได้อย่างเต็มความสามารถ ในแง่หนึ่งคือทุกฝ่ายต้องเรียนรู้เรื่องภัยออนไลน์ไปพร้อมกับประชาชน เพราะทุกคนยังเดิน

ตามหลังมิจฉาชีพ คือเจอปัญหาก่อนแล้วค่อยหาทางแก้ไข ดังนั้น ความเชี่ยวชาญต่าง ๆ ควรมีการบูรณาการมากขึ้น จากการเก็บข้อมูลจะพบว่าแต่ละหน่วยงานทำหน้าที่ดังนี้

1) **สกมช.** เป็นส่วนหนึ่งในคณะทำงานของศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (Anti Online Scam Operation Center : AOC) โดยมีภารกิจหลักดูแลในส่วนของการหลอกลวงที่มาจากแพลตฟอร์มโซเชียลมีเดีย คือ มอนิเตอร์เพจต่าง ๆ ที่มีการหลอกลวง และสนับสนุนการระงับ การปิดกั้น หรือเผยแพร่ ในลักษณะของการตัดวงจร หรือยุติการทำงานของสิ่งนั้น

2) **สำนักกำกับดูแลกิจการโทรคมนาคม** ดูแลด้านตรวจการประกอบกิจการโทรคมนาคม ตรวจสอบว่าการประกอบกิจการเหล่านั้นได้ดำเนินการอย่างครบถ้วนถูกต้องตามกฎหมาย ซึ่งก็มองเห็นว่าการประกอบกิจการของผู้ที่ได้รับใบอนุญาตหลายประเภทยังมีช่องว่างที่ทำให้เกิดการใช้ประโยชน์ของแก๊งคอลเซ็นเตอร์หรือกลุ่มอาชญากร

3) **สถาบันวิจัยพฤติกรรมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ** มีเป้าหมายยกระดับกำลังคนด้านการวิจัยพฤติกรรมศาสตร์และจิตวิทยาเพื่อแก้ปัญหาทางสังคม เช่น การหลอกลวงออนไลน์ โดยเข้าไปมีส่วนร่วมทั้งการทำวิจัย ฝึกอบรม วิเคราะห์สถานการณ์ มีระบบให้คำปรึกษาทั้งออนไลน์และออฟไลน์ เพื่อช่วยเยียวยาผู้เสียหาย

4) **ตำรวจไซเบอร์** มีภารกิจในเรื่อง 1) การเงิน เป็นปัญหาหลักที่ประชาชนโดนโกง ซึ่งต้องประสานงานกับ ธนาคารแห่งประเทศไทย สมาคมธนาคาร สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) 2) การติดต่อสื่อสาร ก็คือค่ายโทรศัพท์มือถือ โดยอำนาจในการระงับเงิน คือ ประชาชน หรือธนาคาร หรือเจ้าหน้าที่ สามารถเป็นผู้แจ้งได้ทั้งหมด

5) **ดีเอสไอ** ดูแลคดีความผิดทางอาญา เช่น คดีที่มีความซับซ้อน มีผลกระทบอย่างรุนแรงต่อความมั่นคงของประเทศ มีลักษณะเป็นการกระทำความผิดข้ามชาติ มีผู้ทรงอิทธิพลเป็นตัวการ คดีฉ้อโกงประชาชน ความผิดเกี่ยวกับคอมพิวเตอร์ ฯลฯ โดยมีการแจ้งเตือนภัยแก่ประชาชน ได้แก่ ลงพื้นที่ให้ความรู้ จัดทำสื่อสารสนเทศเพื่อให้ข้อมูล

6) **มหาวิทยาลัยเกษตรศาสตร์** จัดให้มีคอร์สเรียนฟรีด้านประเด็นสำคัญทางสังคม เน้นให้ประชาชนสามารถเข้ามาเรียนรู้และนำไปใช้ในชีวิตประจำวันได้ เช่น จิตวิทยาการใช้ชีวิต การดูแลสุขภาพจิต อาชญากรรมไซเบอร์ ศาสตร์ด้านนักอาชญาวิทยา เพื่อให้สามารถวิเคราะห์รูปแบบของอาชญากรรม นำไปสู่การมองหาแนวทางการป้องกันหรือการรับมือ

7) **สื่อมวลชน** ทำหน้าที่ 1) สะท้อนปัญหา สร้างความตระหนักรู้ว่ามีพิษภัยยังไง 2) นำเสนอทางแก้ หาทางออก ประสานความช่วยเหลือ เป็นตัวกลางในการประชาสัมพันธ์ระหว่างหน่วยงานกับประชาชนในการเตือนภัย

4.1.5.5 ระบบนิเวศ (คอขวด) ของการแก้ปัญหา (Ecosystem)

การทำงานของหน่วยงานภาครัฐมีข้อจำกัดมาก เช่น ปัญหาด้านข้อกฎหมาย กฎระเบียบ ทำให้มีขั้นตอนซับซ้อน ใช้เวลามาก จึงจัดการปัญหาได้อย่างล่าช้า ยกตัวอย่างการออกกฎหมายฉบับหนึ่งใช้เวลา 8 เดือน มีขั้นตอนการพิจารณาและประกาศใช้ค่อนข้างนาน ทำให้อาชญากรไหวตัวทันและปรับเปลี่ยนกลยุทธ์รูปแบบของการหลอกลวงพัฒนาไปเรื่อย ๆ ในขณะที่ภาครัฐปรับตัวไม่ทันต่อสถานการณ์

นอกจากนี้ ยังมีกรณีของหน่วยงานที่ไม่ได้มีความมั่นคงมากพอในเชิงปฏิบัติ จนทำให้เกิดปัญหาในการปฏิบัติงาน เช่น ขาดการประสานและสื่อสารที่ดี ขาดบุคลากรมืออาชีพ ต้องจ้างหน่วยงานภายนอก (Outsource) มาช่วยเหลือ เป็นต้น รวมทั้งการขาดความต่อเนื่องในการทำงาน เนื่องจากมีการปรับเปลี่ยนตำแหน่งและโยกย้ายบุคลากร เช่น เจ้าหน้าที่ที่ดูแลงานเรื่องนี้อาจย้ายไปทำงานที่ส่วนอื่น ทำให้ต้องหาเจ้าหน้าที่คนใหม่มาแทน ซึ่งต้องใช้เวลาในการส่งมอบงานและเรียนรู้งาน ทำให้งานไม่ไหลลื่น

“งานมันไม่ได้ช่วยต่อกันโดยตรง มันเลยอาจไม่ได้เป็นองค์รวมเวลาสั่งการ ตรงนี้นายทำ ตรงนี้เราทำ แม้ว่าเรื่องแจ้งความจะลดลง แต่มูลค่าความเดือดร้อนเสียหายยังสูงอยู่... วิธีกำหนดมาตรการต่าง ๆ เป็นจุดอ่อนของหน่วยงานรัฐในการจะพลิกแพลงสถานการณ์ให้ทันรูปแบบที่เขาเปลี่ยน กฎหมายฉบับหนึ่งเราใช้เวลาออกแปดเดือน โจรก็เปลี่ยนพรุ่งนี้เลย แปดเดือนที่ทำมาแทบจะล้มเหลวไปเลย หน่วยงานรัฐมีข้อกำกัดในส่วนนี้เยอะ ทำให้เราปรับตัวไม่ทันกับสถานการณ์ ไม่เพียงพอแต่ต้องทำต่อไป” (เจ้าหน้าที่สำนักงานกสทช. สัมภาษณ์ 19 กุมภาพันธ์ 2567)

“กฎหมายไม่ได้บอกให้ทำศูนย์ Anti Online Scam Operation Center (AOC) โครงสร้างของศูนย์มีความรับผิดชอบจริง แต่ความแข็งแรงในเชิงปฏิบัติยังไม่ดีพอ เพราะว่าไม่ได้เกิดตามกฎหมาย แต่เกิดจากกระทรวง DE (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม: Ministry of Digital Economy and Society) เป็นเจ้าภาพให้... มันต้องให้ศูนย์มีอำนาจหน้าที่ตามกฎหมายได้ เหมือนบางประเทศเขาจัดตั้งโดยอาศัยกฎหมาย พอตั้งเป็นศูนย์ก็สามารถของบง่าย กระบวนการจัดการก็ง่าย ข้อสำคัญคือจะมีอำนาจหน้าที่ผลักดันหน่วยงานอื่นได้” (เจ้าหน้าที่สำนักงานสกมช. สัมภาษณ์ 21 กุมภาพันธ์ 2567)

4.3 การสร้างการรู้เท่าทัน

4.3.1 ความรู้เท่าทันสื่อ

สิ่งที่ควรส่งเสริมให้เกิดขึ้นคือ ประชาชนต้องมีความตระหนักรู้และรู้เท่าทัน ตั้งข้อสงสัยให้มากขึ้น ไม่ทำพฤติกรรมสุ่มเสี่ยง เช่น หลงเชื่อคนในโลกออนไลน์ การคลิกลิงก์ การแอดไลน์ที่ไม่รู้จัก การเปิดบัญชีให้คนอื่นใช้ เป็นต้น และหากกลายเป็นผู้เสียหายแล้วต้องตั้งสติและไปยังหน่วยงานที่เกี่ยวข้อง ทั้งนี้ การสร้างความตระหนักรู้อาจไม่ได้ทำเพียงผิวเผิน แต่ควรมีการจัดหลักสูตรฝึกอบรม หรือบรรจุอยู่ในหลักสูตรพื้นฐานตั้งแต่เด็ก ๆ เช่น ฝึกอบรมการสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Education, Training and Awareness - ETA) นอกจากนี้ยังอาจใช้สื่อบุคคลเข้ามาช่วย เนื่องจากข้อได้เปรียบด้านความใกล้ชิดประชาชน เช่น ผู้ใหญ่บ้านประกาศเสียงตามสายเพื่อแจ้งเตือนภัย เป็นต้น สอดคล้องกับแนวคิด “เหยื่อวิทยา (Victimology)” ของ Cohen และ Felson ว่าด้วยเรื่องการขาดผู้พิทักษ์ที่มีประสิทธิภาพ หรือการไร้ความสามารถที่จะปกป้องตนเอง (absence of a capable guardian)

“เรื่องของการสร้างความตระหนักรู้ สิ่งที่แตกต่างก็คือมันเป็นองค์ความรู้ แต่ที่จริงในองค์ความรู้นี้ต้องมีการฝึกฝน เพราะแค่ได้รู้ ได้อ่าน ก็ยังไม่เข้าใจ การฝึกต้องมีคอร์สหรืออยู่ในหลักสูตรบางอย่าง สิ่งต่าง ๆ ต้องถูกบรรจุอยู่ในหลักสูตรพื้นฐาน ระดับประถมศึกษาก็ดี เหมือนในอเมริกาที่เด็กเล็กสามารถช่วยเหลือเด็กจมน้ำได้ เขาสามารถตีความบางอย่างได้ตั้งแต่เด็ก เพราะว่ามันอยู่ในชีวิตเขา” (เจ้าหน้าที่สำนักงานสกมช. สัมภาษณ์21 กุมภาพันธ์ 2567)

“การรู้เท่าทันกลโกงของมิจฉาชีพออนไลน์ เทคโนโลยีและสื่อ การตรวจสอบ เฝ้าระวังตนเองเพื่อไม่ให้ตนเองตกเป็นผู้เสียหาย ใช้วิธีการป้องกันมากกว่าการไปแก้ปัญหา... อาจารย์จะหยิบยกข้อความสำคัญ โฆษณา ประชาสัมพันธ์ วิดิโอเตือนภัย ชวนให้ผู้เข้าร่วมได้ดูและร่วมกันวิเคราะห์ เพื่อร่วมกันหาสาเหตุของปัญหาว่าคืออะไร สาเหตุที่แท้จริงคืออะไร แล้วจะป้องกันอย่างไร และถ้าหากเป็นตัวเองจะทำอย่างไร” (เจ้าหน้าที่สถาบันวิจัยพฤติกรรมศาสตร์ฯ สัมภาษณ์ 20 กุมภาพันธ์ 2567)

“ตั้งข้อสงสัยให้มากขึ้น เราเตือนทุกวันๆ ทำอย่างไรให้คนไทยไม่ถูกหลอก...คนที่โดนต้องทำใจ ตั้งสติ ต้องยกเคสตัวอย่างให้มีพลังขึ้น ต้องสู้คดีให้ถึงที่สุด ต้องใช้เวลา ตำรวจไซเบอร์มีช่องทางให้ผู้เสียหายมาลงทะเบียนไว้ก่อนว่าคุณเคยโดนโอนเงินให้บัญชีม้านี้ไหม หรือโดนหลอกในแพลตฟอร์มนี้ไหม” (นักสื่อสารมวลชน สัมภาษณ์ 15 กุมภาพันธ์ 2567)

4.3.2 ความรู้พื้นฐานด้านเทคโนโลยี

เนื่องจากภัยไซเบอร์เกิดขึ้นด้วยการพัฒนาทางเทคโนโลยี ดังนั้น ประชาชนควรมีความรู้เท่าทันเทคโนโลยี เรียนรู้และเข้าใจหลักพื้นฐานของการใช้เทคโนโลยี ทั้งอินเทอร์เน็ตและโทรศัพท์มือถือ เช่น การตั้งรหัส (Password) ให้มีความซับซ้อนและมีหลักการ หลีกเลี่ยงการคลิกลิงก์หรือเข้าเว็บไซต์ที่มีความสุ่มเสี่ยง ไม่น่าเชื่อถือ ใช้การยืนยันตัวตนแบบ 2 ขั้นตอน (Two-factor authentication) เปิดใช้ล็อคดาวน์โหมดป้องกันแอปพลิเคชันดูดเงิน เป็นต้น รวมทั้งการกระจายความเสี่ยงของตนเอง ไม่ฝากเงินในธนาคารเพียงแห่งเดียว หรือการเรียนรู้เทคนิคตรวจสอบมิจฉาชีพ เช่น การตรวจสอบว่าคนที่โทรมาเป็นเจ้าหน้าที่จริงหรือไม่ ให้ตัดสายแล้วลองโทรกลับ ถ้าไม่มีใครรับสายหรือสายไม่ว่างคือมิจฉาชีพ เพราะใช้ซิมบล็อกแล้วรีโหมดมาจากประเทศเพื่อนบ้านสามารถปลอมเบอร์ได้ แต่ไม่สามารถรับสายได้

นอกจากนี้ หน่วยงานที่เกี่ยวข้องยังมีความพยายามในการออกมาตรการช่วยเหลือประชาชน เช่น วัคซีนไซเบอร์ให้ประชาชนทดสอบตนเอง ผ่านทาง thaipoliceonline.go.th, มหาวิทยาลัยเกษตรศาสตร์มีการจัดคอร์สสอนประชาชนในหัวข้อที่เกี่ยวข้อง เช่น จิตวิทยาการใช้ชีวิต การดูแลสุขภาพจิตอาชญากรรมไซเบอร์ ศาสตร์ด้านนักอาชญาวิทยา ฯลฯ เพราะการหลอกลวงเป็นการเล่นกับจิตใจ อาชญากรต้องรู้ว่าเหยื่อที่เหมาะสมต้องอยู่ในสภาวะแบบใด และจะเล่นกับความกลัว ความโลภ สร้างเรื่องราวเพื่อเข้าสู่กระบวนการของอาชญากร ซึ่งพวกเขามีองค์ความรู้ระดับหนึ่ง มีการอบรมและมีลักษณะเหมือนบริษัทหรือองค์กรที่มีการรวมตัวกันของคนพนักงาน และมีกระบวนการ ดังนั้น ประชาชนต้องเรียนรู้ที่จะรับมือและป้องกันตนเองด้วย โดยใช้ทักษะ Cyber hygiene ที่มีสอดคล้องกับแนวทาง มาตรฐานสากล DQ (digital intelligence) ของ สภาเศรษฐกิจโลก (World Economic Forum : WEF) กล่าวคือ กลุ่มความสามารถทางสังคม อารมณ์ และการรับรู้ ที่จะทำให้คน ๆ หนึ่ง สามารถเผชิญกับความท้าทายของชีวิตดิจิทัล และสามารถปรับตัวให้เข้ากับชีวิตดิจิทัลได้ ความฉลาดทางดิจิทัลครอบคลุมทั้งความรู้ ทักษะ ทัศนคติและค่านิยม ที่จำเป็นต่อการใช้ชีวิตในฐานะสมาชิกของโลกออนไลน์ กล่าวอีกนัยหนึ่งคือ ทักษะการใช้สื่อ และการเข้าสังคมในโลกออนไลน์ ซึ่งมีความมุ่งมั่นให้เด็ก ๆ ทุกประเทศได้รับการศึกษาด้านทักษะพลเมืองดิจิทัลที่มีคุณภาพและใช้ชีวิต บนโลกออนไลน์อย่างปลอดภัยด้วยความก้าวหน้าของเทคโนโลยีสมัยใหม่

“ชุดความรู้ง่ายๆ แบบนี้ แต่ประชาชนไม่มีความรู้ สิ่งที่เราพยายามบอกให้ค่ายมือถือและธนาคารส่งข้อความให้กับผู้เสียหายแบบนี้ เขามองว่าประชาชนควรจะรู้อยู่แล้ว แต่ทำงานมาจนกระทั่งได้ข้อสรุปแล้วว่าประชาชนโดนหลอกแบบนี้ทุกวัน ทำไมคุณถึงไม่เตือน อันนี้มันก็วนไปวนมา เรายังไม่ได้เริ่มนับหนึ่ง คุยกับคนที่เกี่ยวข้องก็โดนปฏิเสธหมด อะไรที่ต้องจ่ายก็ไม่มีใครอยากทำ เพราะฉะนั้นการแก้ปัญหาตรงนี้จะต้องมีผู้ที่มีอำนาจและต้องมีงบประมาณในการขับเคลื่อน ผู้มีอำนาจต้องมารับฟังจากผู้ที่มีปัญหาอย่างแท้จริง

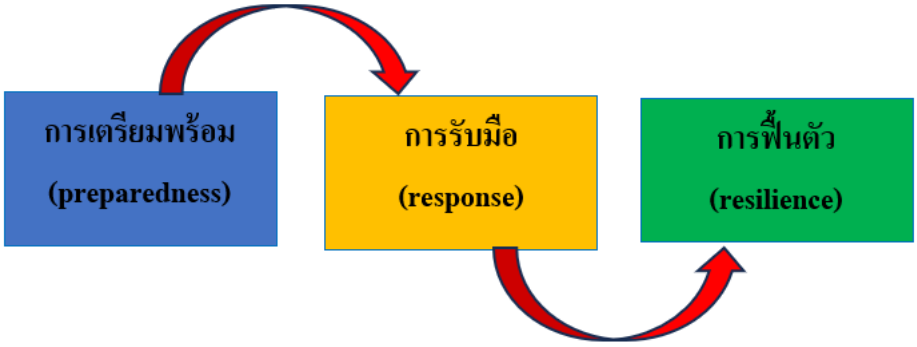
มันถึงจะเริ่มนับหนึ่ง ถ้าผู้มีอำนาจของประเทศยังไม่ได้เริ่มเข้าใจปัญหาตรงนี้ สั่งอย่างเดียวมันก็ไม่จบ” (เจ้าหน้าที่สำนักงานสกมช. สัมภาษณ์21 กุมภาพันธ์ 2567)

บทที่ 5
ข้อเสนอแนะ

จากผลการศึกษาทั้งจากหน่วยงานที่เกี่ยวข้องและผู้เสียหาย คณะวิจัยมีข้อเสนอแนะใน 2 ส่วน ส่วนแรกคือข้อเสนอแนะต่อการช่วยเหลือผู้เสียหายและการสร้างการรู้เท่าทัน ส่วนที่สอง ข้อเสนอแนะเชิงนโยบายต่อหน่วยงานที่เกี่ยวข้อง

5.1 ข้อเสนอแนะต่อการช่วยเหลือผู้เสียหายและการสร้างการรู้เท่าทัน

การช่วยเหลือผู้เสียหายและการสร้างการรู้เท่าทัน สามารถทำได้ใน 3 ระยะ ดังต่อไปนี้



5.1.1 การเตรียมพร้อม (Preparedness)

การเตรียมความพร้อมให้กับประชาชนถือเป็นขั้นตอนที่สำคัญสุดในการป้องกันภัยไซเบอร์ เพราะเปรียบเสมือนกับ ‘ต้นน้ำ’ ที่หากจำนวนผู้เสียหายมีปริมาณมาก ย่อมส่งผลกระทบไปส่วนต่าง ๆ ที่เกี่ยวข้อง ทำให้ประสิทธิภาพในการจัดการกับกลุ่มมิจฉาชีพไม่สามารถทำได้เต็มที่อย่างที่ควรจะเป็น

ทั้งนี้ ไม่เพียงแค่ข้อมูลข่าวสารในเรื่องภัยไซเบอร์เท่านั้น ประชาชนจำเป็นต้องมีความรู้เพื่อจัดการในกรณีที่ตกเป็นผู้เสียหาย เพื่อลดความตื่นตระหนกและสามารถเข้าถึงหน่วยงานที่เกี่ยวข้องกับภัยไซเบอร์ได้อย่างถูกต้อง

1) สร้างความตระหนักรู้และฉุกคิดให้กับประชาชนกลุ่มต่าง ๆ เกี่ยวกับภัยไซเบอร์

แม้ว่าในปัจจุบัน ประชาชนจะมีการรับรู้ในเรื่องภัยไซเบอร์เพิ่มขึ้น เมื่อเปรียบเทียบกับช่วงก่อนการแพร่ระบาดของโควิด-19 อานิสงส์จากการประชาสัมพันธ์และให้ความรู้กับประชาชนของหน่วยงานต่าง ๆ ที่

เกี่ยวข้อง ทว่า ก็ยังมีอีกหลายกลุ่ม เช่น กลุ่มที่เป็นเด็กเยาวชน ผู้สูงอายุ หรือแม้แต่วัยทำงาน ที่ปัจจุบันหลายคนหันมารับรู้ข่าวสารจากทางออนไลน์เป็นหลัก ซึ่งระบบอัลกอริทึม (Algorithm) มันจะเลือกนำเสนอข้อมูลที่ผู้ใช้สนใจเท่านั้น ทำให้ไม่มีความรู้ในเรื่องภัยไซเบอร์ที่เพียงพอ

นอกจากการสร้างความตระหนักรู้ในเรื่องภัยไซเบอร์ที่เกิดขึ้นกับประชาชนแล้ว การสร้างความ ‘ฉุกคิด’ ก็เป็นอีกขั้นตอนที่สำคัญที่ช่วยกันไม่ให้หลงกลกลุ่มมิจฉาชีพ จากการสัมภาษณ์ผู้เสียหายพบว่า ส่วนใหญ่มีการรับรู้เรื่องภัยไซเบอร์เป็นอย่างดี แต่เมื่อถูกจู่โจมโดยกลุ่มมิจฉาชีพแม้จะพยายามระมัดระวังและตรวจเช็คอย่างดีทว่า แต่ละคนก็จะมีจุด ๆ หนึ่งทำให้เผลอหลงกลไปกับกลุ่มมิจฉาชีพ และนำไปสู่การโจมตีได้ ดังนั้น การทำให้ประชาชน ‘ฉุกคิด’ ก่อนที่จะหลงกลเหล่ามิจฉาชีพ ก็จะเป็นปราการป้องกันสำคัญที่หลายฝ่ายและรวมถึงประชาชนจะต้องร่วมกันสร้าง เช่น ในแอปพลิเคชันธนาคารที่มีการย้ำให้ประชาชนมีความระวังก่อนการโอนเงินทุกครั้ง ก็ถือเป็นการช่วยให้ประชาชนได้ฉุดคิดก่อนที่จะหลงกลโอนเงินไป เป็นต้น

2) ให้ความรู้และความชัดเจนกับประชาชนเกี่ยวกับแนวทางในการดำเนินการเมื่อถูกโจมตี

การสร้างการตระหนักรู้ให้กับประชาชนในเรื่องภัยไซเบอร์ ไม่ควรมองเพียงแค่การให้ความรู้เรื่องรูปแบบของภัยไซเบอร์เพียงอย่างเดียว แต่ประชาชนจำเป็นต้องมีความรู้และข้อมูลที่เพียงพอเพื่อสามารถจัดการได้ถูกต้องเมื่อต้องตกเป็นผู้เสียหาย เนื่องจากเมื่อถูกโจมตี ประชาชนเสียขวัญไปกับเรื่องที่เกิดขึ้นแล้ว ความไม่รู้ว่าจะต้องจัดการอย่างไรต่อไปก็ย่อมส่งให้สภาพจิตใจของผู้เสียหายย่ำแย่ลงไปอีก นอกจากนี้ ยังทำให้เกิดความล่าช้าในการจัดการกับกลุ่มมิจฉาชีพหรือนำไปสู่ความถอดใจในการที่จะดำเนินการกับมิจฉาชีพเนื่องจากจับต้นชนปลายไม่ถูกว่าต้องทำอย่างไร

หน่วยงานที่เกี่ยวข้องจำเป็นต้องมีการประชาสัมพันธ์ช่องทางในการดำเนินการเมื่อถูกโจมตีด้วยภัยไซเบอร์ เบอร์โทรศัพท์เข้าถึงแต่ละหน่วยงานที่เกี่ยวข้อง และขั้นตอนในการดำเนินงานว่าจะต้องดำเนินการอย่างไร เพื่อให้ประชาชนสามารถรับรู้และเข้าใจเพิ่มขึ้น นอกจากนี้ เจ้าหน้าที่รัฐหรือหน่วยงานที่เกี่ยวข้องเองจำเป็นต้องให้ข้อมูลที่มีมาตรการในการดำเนินงานที่เป็น ‘เอกภาพ’ ไปในทิศทางเดียวกัน เพื่อหลีกเลี่ยงการสร้างความสับสนให้กับประชาชนที่เข้าไปรับความช่วยเหลือ อีกด้วย

3) บทบาทของสื่อในการส่งเสริมการรู้เท่าทันภัยไซเบอร์

สื่อถือเป็นกระบอกเสียงสำคัญที่จะช่วยให้เสริมสร้างความตระหนักรู้ให้กับประชาชน การนำเสนอข่าวของสื่อจำเป็นต้องมีเป้าหมายในการสร้างการตระหนักรู้และรู้เท่าทันภัยไซเบอร์ให้กับประชาชน **และเป็นตัวกลาง**ในการสร้างความเข้าใจระหว่างประชาชนและหน่วยงานที่เกี่ยวข้องเพื่อร่วมมือกันต่อสู้กับภัยไซเบอร์ ไม่ใช่การนำเสนอข่าวเพียงเพื่อเรียกความสนใจหรือสร้างความตื่นตระหนกเท่านั้น

5.1.2 การรับมือเมื่อถูกโจมตีจากภัยไซเบอร์ (Response)

- **รวดเร็ว ชัดเจน เป็นเอกภาพ และติดตามได้ของรัฐและหน่วยงานที่เกี่ยวข้อง**

เมื่อถูกโจมตีจากมิจฉาชีพ ประชาชนอยากเห็นการดำเนินงานของภาครัฐและหน่วยงานที่เกี่ยวข้องเป็นไป อย่างรวดเร็ว ชัดเจน มีเอกภาพและสามารถเข้าถึงได้ง่าย ขั้นตอนไม่ยุ่งยากและไม่ซับซ้อนในการดำเนินงานเป็นสิ่งสำคัญที่จะช่วยบรรเทาความทุกข์ใจของผู้เสียหาย รวมถึงสนับสนุนให้ผู้เสียหายออกมาแจ้งความดำเนินคดีกับกลุ่มมิจฉาชีพเพิ่มขึ้น นอกจากนี้ การจัดทำระบบติดตามความก้าวหน้าในการดำเนินงานคดีที่เกิดขึ้น ก็จะช่วยคลายความวิตกกังวลให้กับประชาชนที่ไปแจ้งความได้ และเป็นการสร้างความเชื่อมั่นให้กับประชาชนว่าภาครัฐและหน่วยงานที่เกี่ยวข้องไม่ได้นิ่งเฉยแต่อย่างใด

- **มีความเชี่ยวชาญและความเห็นอกเห็นใจ ไม่โทษเหยื่อและตอกย้ำบาดแผลของผู้เสียหาย**

การจัดการกับภัยไซเบอร์ โดยเฉพาะที่เกี่ยวข้องกับการหลอกลวงออนไลน์หรือการหลอกลงทุนคริปโทเคอร์เรนซีต่าง ๆ ที่เกี่ยวกับข้องเทคโนโลยีต่าง ๆ ถือเป็นเรื่องเฉพาะด้าน ซึ่งผู้ที่มีส่วนเกี่ยวข้องในการจัดการต้องมีความรู้ความเชี่ยวชาญเฉพาะเพื่อสามารถให้ความช่วยเหลือผู้เสียหายได้อย่างเข้าใจและมีประสิทธิภาพ นอกจากนี้ การดำเนินการของภาครัฐและหน่วยงานที่เกี่ยวข้องต้องทำด้วยความเห็นอกเห็นใจ ไม่ตอกย้ำและเปิดบาดแผลที่เกิดขึ้นของผู้เสียหาย และไม่โทษว่าเป็นเพราะ “ความโง่ รัก โลภ และหลง” ถึงทำให้หลงกลเหล่ามิจฉาชีพ ไม่เช่นนั้นแล้ว ก็จะยิ่งทำให้ผู้เสียหายไม่อยากที่จะหันไปพึ่งพาภาครัฐและหน่วยงานที่เกี่ยวข้อง กลายเป็นการเอื้อประโยชน์ให้กับเหล่ามิจฉาชีพในการทำร้ายประชาชนเพิ่มมากขึ้น

- **สื่อต้องไม่ผลิตมายาคติในการโทษผู้เสียหาย ทำให้ไม่กล้าที่จะดำเนินคดีกับมิจฉาชีพ**

นอกจากการนำเสนอเรื่องราวเพื่อแบ่งปันข้อมูลและป้องกันภัยไซเบอร์ที่เกิดขึ้น สื่อสามารถช่วยสร้างทัศนคติในการ ‘เห็นอกเห็นใจ’ ของสังคมที่มีต่อผู้เสียหายได้ ต้องไม่เน้นย้ำหรือผลิตภาพมายาคติซ้ำที่ว่าคนที่ตกเป็นผู้เสียหายคือคนที่มีความ “รัก โลภ กลัว หลง” ไม่โทษผู้เสียหาย ในทางกลับกัน ควรเชิญชวนให้ผู้เสียหายกล้าที่จะออกมาแจ้งความดำเนินคดีกับเหล่ามิจฉาชีพ สร้างความเชื่อมั่นให้กับประชาชนว่าภาครัฐและหน่วยงานที่เกี่ยวข้องมีความจริงใจและพร้อมที่จะเป็นที่พึ่งให้กับประชาชนเพราะยิ่งมีผู้เสียหายออกมาเปิดเผยตัวและแจ้งความมากเท่าไหร่ ย่อมช่วยให้ภาครัฐและหน่วยงานที่เกี่ยวข้องมีข้อมูลในการจัดการกับเหล่ามิจฉาชีพได้มากยิ่งขึ้น สื่อต้องทำหน้าที่ในการเชื่อมประชาชนกับภาครัฐและหน่วยงานที่เกี่ยวข้องให้เป็นทีมเดียวกันเพื่อสู้กับเหล่ามิจฉาชีพ

5.1.3 การฟื้นตัว (Resilience)

- **มีหน่วยงานที่ให้ความช่วยเหลือผู้เสียหายทั้งในด้านกฎหมาย การเงินและสุขภาพจิต**

การฟื้นฟูผู้เสียหายจากภัยไซเบอร์เป็นสิ่งที่สำคัญไม่น้อยไปกว่าการเตรียมความพร้อมและการรับมือเมื่อเกิดความเสียหายขึ้น ผู้เสียหายจำนวนมากต้องการผู้ที่มีความเชี่ยวชาญทั้งในด้านกฎหมาย การเงินและสุขภาพจิตที่สามารถเข้าถึงได้ เพื่อขอคำแนะนำในการฟื้นฟูกลับมาใช้ชีวิตอย่างปกติได้อีกครั้ง การที่มีผู้ที่สามารถให้คำแนะนำดังกล่าวได้ จะช่วยทำให้ผู้เสียหายมีความรู้สึกว่าไม่ได้อยู่อย่างโดดเดี่ยว

- **จัดตั้งกลุ่มเครือข่ายผู้เสียหายเพื่อช่วยในการเยียวยาจิตใจ**

ผู้เสียหายจำนวนมากไม่กล้าที่จะพูดคุยเรื่องที่เกิดขึ้นกับครอบครัวหรือคนใกล้ตัว และบางครั้งก็กลัวว่าการเล่าให้คนอื่นฟัง อาจจะถูกมองไม่ดี เลยจำเป็นต้องเก็บปัญหาไว้กับตัวเองเพียงลำพัง การจัดตั้งกลุ่มเครือข่ายผู้เสียหายเป็นหนึ่งช่องทางที่เปิดพื้นที่ให้ผู้เสียหายสามารถพูดคุย แลกเปลี่ยนความคิดเห็นหรือปรึกษาแนวทางในการจัดการกับเรื่องที่เกิดขึ้น กับคนที่มีประสบการณ์แบบเดียวกันและมีความเห็นอกเห็นใจ รวมถึงเข้าใจกันเป็นอย่างดี ช่วยให้ผู้เสียหายรู้สึกว่าสิ่งที่เกิดขึ้นไม่ใช่แค่ตัวเองที่ประสบ แต่ทุกคนก็สามารถตกเป็นผู้เสียหายจากภัยไซเบอร์ได้ สิ่งเหล่านี้จะช่วยในการเสริมสร้างพลังใจให้ผู้เสียหายในก้าวผ่านเหตุการณ์ความสูญเสียที่เกิดขึ้นและกลับมาใช้ชีวิตปกติได้

- **สื่อต้องส่งเสริมการเรียนรู้และถอดบทเรียนที่เกิดขึ้นเพื่อป้องกันในอนาคต**

สื่อต้องสร้างการตระหนักรู้ในสังคมในเรื่องภัยไซเบอร์ ไม่เพียงแค่นำเสนอข่าวเพียงอย่างเดียว ทว่าต้องร่วมสร้างบรรยากาศการตื่นตัวของสังคมในการที่จะร่วมกันเรียนรู้และถอดบทเรียนจากเหตุการณ์ที่นำเสนอเพื่อช่วยให้ประชาชนมีความรู้ ระมัดระวังและป้องกันภัยไซเบอร์ในอนาคต เพราะแม้จะเคยโดนโจมตีจากภัยไซเบอร์แล้ว แต่ถ้าหากไม่ระวังก็อาจจะตกเป็นเป้าโจมตีได้อีกครั้งในอนาคต ดังนั้น การส่งเสริมให้ประชาชนมีความตระหนักรู้และฉุกคิดตลอดเวลาย่อมเป็นการป้องกันภัยไซเบอร์ที่ดี ในขณะเดียวกัน สื่อจะต้องช่วยนำเสนอข้อมูลและแนวทางสำหรับผู้เสียหายในการรับความช่วยเหลือเพื่อเยียวยาความเสียหายที่เกิดขึ้น สร้างบรรยากาศสังคมที่ไม่ผลักให้ผู้เสียหายต้องรู้สึกว่าอยู่คนเดียวในสังคม

5.2 ข้อเสนอแนะเชิงนโยบายต่อหน่วยงานที่เกี่ยวข้อง

การสื่อสาร

1) ควรสื่อสารให้ประชาชนตระหนักถึงภัยอาชญากรรมออนไลน์อย่างรอบด้าน เช่น รูปแบบการหลอกลวง การรับมือและป้องกัน การแก้ไขปัญหากรณีที่ได้รับความเสียหาย เป็นต้น โดยไม่ได้มุ่งเน้นแค่กลุ่มเป้าหมายกลุ่มใดกลุ่มหนึ่ง แต่ควรกระจายความรู้ไปให้ครอบคลุม เพราะประชาชนทุกคนมีโอกาสถูกหลอกลวงได้

2) การสื่อสารประเด็นอาชญากรรมออนไลน์ควรแยกแยะลักษณะเฉพาะของอาชญากรรมและรูปแบบให้ชัดเจน เช่น แอปพลิเคชันดูดเงิน มักจะใช้ชื่อหน่วยงานราชการ เช่น การไฟฟ้า ขณะที่คอลเซ็นเตอร์มักจะใช้วิธีโทรศัพท์พูดคุยกับเหยื่อเพื่อสร้างความน่าเชื่อถือก่อน

3) ควรเปิดโอกาสให้ผู้ที่มีชื่อเสียงหรือมีอิทธิพลต่อผู้รับสาร (influencer) รวมทั้งสื่อบุคคลที่มีความใกล้ชิดกับประชาชน เช่น อาสาสมัครชุมชน คณะกรรมการหมู่บ้าน เป็นต้น มีส่วนร่วมในการสื่อสารประเด็นด้านภัยไซเบอร์แก่ประชาชน ด้วยรูปแบบและวิธีการสื่อสารที่เข้าใจง่าย สร้างการจดจำ

4) มุ่งสื่อสารประเด็นอาชญากรรมออนไลน์ผ่านทางสื่อสารมวลชน เช่น สื่อโทรทัศน์ สื่อวิทยุ เป็นต้น เนื่องจากเป็นช่องทางที่มีความน่าเชื่อถือ และสามารถเข้าถึงประชาชนจำนวนมากได้ในเวลาอันรวดเร็ว สามารถเตือนภัยได้อย่างทันต่อสถานการณ์

5) การสื่อสารของหน่วยงานภาครัฐควรมีหน่วยงานที่ทำหน้าที่เป็นศูนย์กลาง (center) ด้านข้อมูล ซึ่งต้องผ่านกระบวนการตรวจสอบข้อมูลให้มีความถูกต้อง ครบถ้วน เหมาะสม สร้างความเข้าใจได้ดี ไม่สร้างความแตกตื่นในหมู่ประชาชน แล้วจึงส่งต่อไปยังหน่วยงานอื่น ๆ เพื่อเผยแพร่ต่อไป หรืออาจทำงานประสานข้อมูลระหว่างกัน เนื่องจากการที่แต่ละหน่วยงานต่างก็สื่อสารข้อมูลของตนเองอาจเกิดปัญหาการสื่อสารที่คลาดเคลื่อนหรือสร้างความสับสนให้แก่ประชาชนได้

6) การสื่อสารทุกประเด็น นักสื่อสารต้องแบ่งของกลุ่มเป้าหมายหลักที่ต้องการจะสื่อสารไปถึงกลุ่มเป้าหมายให้ชัดเจน เพราะแต่ละกลุ่มมีปัจจัยต่าง ๆ และลักษณะการโดนหลอกที่แตกต่างกัน ดังนั้นวิธีการสื่อสารก็จะมีความแตกต่างเช่นต่างกัน เช่น ที่ศาลออสเตรเลียมีการหลอกลวงผู้บริโภคให้หลงเชื่อว่าบริษัทบางบริษัทดูแลอนุรักษ์สิ่งแวดล้อม ลดการปล่อยก๊าซเรือนกระจก แต่ความจริงแล้ว มีความเกี่ยวข้องกับอุตสาหกรรมที่ใช้เชื้อเพลิงฟอสซิล ธุรกิจบ่อนการพนัน และธุรกิจเครื่องดื่มแอลกอฮอล์ ทำให้นักลงทุนเข้าใจผิด ซึ่งนักสื่อสารไปยังนักลงทุนต้องใช้วิธีที่เหมาะสมกับการอธิบายและการเตือน เป็นต้น

5.2.2 ข้อเสนอต่อหน่วยงานที่เกี่ยวข้อง

1) ควรพัฒนาแอปพลิเคชันเตือนภัยและประชาสัมพันธ์ให้ประชาชนรู้จักอย่างแพร่หลาย เช่น การจัดทำแอปพลิเคชันลักษณะคล้าย “เป๋าตัง” ที่ประชาชนรู้จักกันทั่วไป ซึ่งภายในแอปพลิเคชันจะมีหัวข้อที่ครบถ้วน ใช้งานง่าย อาจนำมาประยุกต์และพัฒนาเป็นแอปพลิเคชันเตือนภัยที่รวบรวมข้อมูลสำคัญเกี่ยวกับอาชญากรรมออนไลน์และช่องทางการร้องเรียน ซึ่งประชาชนสามารถใช้งานได้อย่างครบวงจร (one-stop service) หรือส่งเสริมให้แอปพลิเคชันของหน่วยงานต่าง ๆ เพิ่มหัวข้อหรือประเด็นด้านการเตือนภัยอาชญากรรมออนไลน์

2) ควรจัดหลักสูตรฝึกอบรมหรือให้ความรู้แก่ประชาชนในลักษณะเชิงรุก เช่น ลงพื้นที่ตามโรงเรียน มหาวิทยาลัย ชุมชน เป็นต้น รวมทั้งการผลิตสื่อสำหรับเตือนภัยที่เหมาะสมกับกลุ่มเป้าหมายในแต่ละกลุ่มและแต่ละพื้นที่ เช่น สื่อสังคมออนไลน์ โปสเตอร์ การประชาสัมพันธ์เสียงตามสาย เป็นต้น

3) รณรงค์ให้ภาครัฐและภาคเอกชนเพิ่มมาตรการส่งเสริมการป้องกันตนเองจากอาชญากรรมออนไลน์ให้แก่เจ้าหน้าที่และพนักงานในสังกัด เช่น การเปลี่ยนรหัสผ่านอีเมล์ทุกสามเดือน การจัดอบรมให้ความรู้และสร้างความรู้เท่าทันอาชญากรรมออนไลน์ให้แก่บุคลากรทุกปี เป็นต้น

4) การผลักดันให้อาชญากรรมออนไลน์เป็นวาระแห่งชาติหรือวาระเร่งด่วน โดยให้อำนาจแก่ผู้ปฏิบัติงานตามกฎหมายอย่างจริงจัง จัดสรรจำนวนบุคลากรที่เพียงพอและมีทักษะสอดคล้องกับภาระงาน เนื่องจากในปัจจุบันศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (Anti Online Scam Operation Center : AOC) ยังมีลักษณะเป็นศูนย์เฉพาะกิจที่ขาดความแข็งแรงในเชิงปฏิบัติ

5) หน่วยงานภาครัฐควรบูรณาการความร่วมมือในการทำงานอย่างจริงจัง มีการวางโครงสร้างในการทำงานอย่างชัดเจน และบุคลากรต้องมีความรู้ความสามารถสอดคล้องกับงานที่ทำ มีการพัฒนาทักษะบุคลากรให้ทันต่อกลยุทธ์ของมิจฉาชีพที่ปรับเปลี่ยนอยู่ตลอดเวลา อาจเชิญหน่วยงานภายนอกหรือภาคเอกชนที่มีความเกี่ยวข้องเข้ามาร่วมด้วย เช่น หน่วยงานด้านสุขภาพจิต ฝึกฝนบุคลากรให้มีความรอบรู้ด้านการใช้จิตวิทยาในการสื่อสารกับผู้เสียหาย ธนาคารแห่งประเทศไทย อาจมีส่วนร่วมในการแก้ไขปัญหาบัญชีม้า โดยออกมาตรการกำกับดูแลและปิดช่องโหว่ของธนาคารต่าง ๆ ผู้ให้บริการสัญญาณมือถือในไทย ส่งข้อความสั้น (SMS) เตือนภัยประชาชน หรือสกัดกั้นลิงก์น่าสงสัยที่ส่งมาพร้อมข้อความสั้น (SMS) เป็นต้น

6) ควรจัดทำคำแนะนำในลักษณะชุดคำแนะนำและสรุปของการหลอกหลวงต่าง ๆ เพื่อจะได้ใช้สำหรับประชาชนทุกคน เหมือนยาชุดที่จะช่วยป้องกันและรักษาการหลอกหลวงที่มีทุกรูปแบบ ก่อนเกิดเหตุการณ์ที่เป็นภัยต่อตัวเอง

7) ภาครัฐต้องจัดหาเบอร์โทรที่ติดต่อในเรื่องการหลอกลวงเป็นเบอร์กลางเบอร์เดียว ในลักษณะ COFACT ที่ทำให้ทุกคนกลายเป็นคนตรวจสอบข่าว หรือ Fact Checker และสร้างพื้นที่ในการแสวงหา

ข้อเท็จจริงร่วมกันให้เกิดขึ้นในประเทศไทย โดยภาครัฐจะต้องเป็นผู้ช่วยตรวจสอบ ก่อนที่ทุกเหตุการณ์หลอกลวงจะเกิดขึ้นกับประชาชนของตน หรือมีอาสาสมัครมาช่วยคัดกรอง ก่อนจะนำข่าวลวงไปสู่สังคม

8) ภาครัฐมีทรัพยากรจำกัด ควรจัดลำดับความสำคัญของเรื่องการหลอกลวง อาจจะต้องเริ่มเน้นจากการหลอกลวงที่ถูกพบมากที่สุดในประเทศไทย และความเสียหายที่เกิดขึ้นมากที่สุด เพื่อที่จะรณรงค์โดยใช้สติให้สามารถขับเคลื่อนให้เกิดขึ้นในสังคมได้อย่างเป็นรูปธรรมที่สุด และหลังจากนั้นจึงค่อยกระจายหลากหลายเรื่องให้ครอบคลุม และสามารถสร้างภูมิคุ้มกันได้ทุกคนในสังคม

9) ควรใช้กรอบการทำงานทางอิเล็กทรอนิกส์มาเป็นหลักในการพัฒนา (ETA framework) โดยออกแบบเป็น 2 ส่วน ได้แก่ 1) ส่วนของภาครัฐ เช่น การออกแบบบทเรียนเกี่ยวกับอาชญากรรมออนไลน์ให้แก่เยาวชน โดยมีการทดสอบ การประเมิน และมีระดับความเข้มข้นของเนื้อหาปรับเปลี่ยนไปตามช่วงวัยและสถานการณ์ปัจจุบัน 2) ส่วนของภาคเอกชน เช่น แพลตฟอร์มโซเชียลมีเดียต่าง ๆ ควรมีมาตรการป้องกันและจำกัดพฤติกรรมต้องสงสัยที่มีแนวโน้มจะเป็นอาชญากรรมออนไลน์

10) กระบวนการทำงานเกี่ยวกับอาชญากรรมออนไลน์ควรยึดแนวคิดแบบเฉพาะตัว (Tailor-made) เพราะแต่ละกรณีมีความแตกต่างกัน แต่ละกลุ่มเป้าหมายก็มีความแตกต่างกัน อาจต้องพิจารณาปัจจัยแวดล้อมอย่างครบถ้วนจึงจะสามารถหาแนวทางที่เหมาะสมกับแต่ละปัญหาได้ อีกทั้งควรผลักดันให้เกิดความร่วมมือระหว่างภาครัฐกับภาคเอกชน จึงจะเกิดประสิทธิภาพในการดำเนินงาน

11) หน่วยงานภาครัฐควรเพิ่มมาตรการความปลอดภัยในการปฏิบัติงาน เช่น การเก็บรักษาข้อมูลของประชาชนอย่างรอบคอบ การป้องกันข้อมูลราชการรั่วไหล พัฒนาเว็บไซต์ที่มีระบบรักษาความปลอดภัยอย่างมีประสิทธิภาพ เป็นต้น

12) การสร้างการรู้เท่ากันสื่อ แทนที่ทุกภาคส่วนและองค์กรจะไปสอนและอธิบายหลักการ หรือเกิดปัญหาค่อยไปหาหน่วยงานอื่น ๆ แต่ควรให้มีการเข้าถึงของข้อมูลทั้งหมดในด้านนี้ ทั้งการเรียนรู้ วิธีป้องกัน หน่วยงานที่จะช่วยหลังจากเกิดเหตุการณ์ขึ้น และวิธีการในการเยียวยาจิตใจให้หายจากเหตุการณ์ที่เกิดขึ้น สิ่งเหล่านี้ควรจะทำให้เกิดขึ้นในแต่ละตัวบุคคล เพื่อที่จะได้ไม่เกิดความร้ายแรงของเหตุการณ์ในระดับสูงมาก และลดการปะทะของความรุนแรง หากต้องมีการเกิดขึ้นในช่วงเริ่มต้น

รายการอ้างอิง

ภาษาไทย

กรมประชาสัมพันธ์. (2566, 29 มีนาคม). *ประชาชนแจ้งความออนไลน์ลดลงเฉลี่ยสัปดาห์ละ 700 ราย จับมือสื่อมวลชนเผยแพร่กลโกงให้ประชาชนรู้เท่าทัน*. https://thainews.prd.go.th/th/news/details/ ท TCATG230329144959892

กองทุนพัฒนาสื่อปลอดภัยและสร้างสรรค์. (2564). Digital Empathy: เพราะโลกนี้ไม่ได้มีแค่ (พวก) เรา. *จดหมายข่าวคณะอนุกรรมการเกี่ยวกับการเฝ้าระวังสื่อที่ไม่ปลอดภัยและไม่สร้างสรรค์,* 2(7), 1-20.

โคแฟก. (2567, 23 มีนาคม). '*AI-DEEPFAKE'เทคโนโลยีซับซ้อนปลอมเนียนน่ากังวล แต่อย่าประมาท 'CHEAPFAKE' ทริกง่ายๆ ก็หลงเชื่อกันได้*. https://blog.cofact.org/specialreport31-67/

ชัวร์ก่อนแชร์. (2566, 4 มีนาคม). *เปิดขั้นตอน "แจ้งความออนไลน์" แจ้งง่ายได้ทุกที่ แค่มีอินเทอร์เน็ต*. https://tna.mcot.net/latest-news-1127215

ชัวร์ก่อนแชร์. (2566, 31 มีนาคม). *Whoscall เผยคนไทยเบอร์โทรรั่ว 13 ล้านเบอร์ เป็นอันดับ 4 รองจากมาเลเซีย ไต้หวัน ญี่ปุ่น*.https://tna.mcot.net/sureandshare-1145872

ชัวร์ก่อนแชร์. (2567, 28 มีนาคม). *SMS ยังเสี่ยง! เผยมิจฯ ยังกระหน่ำส่งข้อความ SMS หลอกลวงหลายรูปแบบ พนัน-ปล่อยกู้-แอบอ้าง*. https://tna.mcot.net/sureandshare-1342212

ฐานเศรษฐกิจ. (2566, 11 กุมภาพันธ์*). ผวา คนไทยเป็นเหยื่อภัยไซเบอร์ ถูกตุ๋นออนไลน์เสียหายวันละ 100 ล้าน*. https://www.thansettakij.com/news/555872

เดอะ แอคทีฟ นิวส์. (2566, 10 เมษายน). *วิจัยเผย ผู้สูงวัย* 44% *ถูกหลอกบนเฟซบุ๊ก เตือนอย่างหลงเชื่อโฆษณาออนไลน์*. https://theactive.net/news/marginalpeople-20220410-2/

ตำรวจสอบสวนกลาง. (2566, 21 มีนาคม). *สถิติแจ้งความอาชญากรรมทางออนไลน์*. https://web.facebook.com/photo.php?fbid=230761169457428&set=a.1272789698056 49 &type=3

ทศพล ทรรศนกุลพันธ์. (2562). *ข้อจำกัดของกระบวนการยุติธรรมเพื่อป้องกันและปราบปราม พิศวาสอาชญากรรม (Romance Scam) และแนวทางสร้างความตระหนักรู้ ให้กับประชาชน*. สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.).

นิตรสารปลูก. (2564). *Victim Blaming เตือนให้อยู่ในกรอบ หรือลดทอนความเป็นมนุษย์*. https://www.trueplookpanya.com/plookfriends

นิติธร แก้วโต. (2563, 7 กรกฎาคม). *ลวงขาย กับ ฉ้อโกง แตกต่างกันอย่างไร*. https://www.thairath.co.th/news/society/1883501

โนว์สแกม. (2566). *ความเสียหายที่เกิดจากการหลอกหลวงทางอินเตอร์เน็ต (Online Scams)*. https://www.unodc.org/roseap/uploads/documents/KnowScam/images/B1_04_Damage-of-online-scamsin-the-region-01.png

แนวหน้า. (2565, 14 ธันวาคม). *เปิด 10 อันดับภัยออนไลน์ รอรับเลยส่งเตือน 18 รูปแบบกลโกงถึงบ้าน*. https://www.naewna.com/local/698041

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน). (2020, 13 เมษายน). *Social Engineering การหลอกหลวงที่แฝงภัยจากแฮกเกอร์*. https://www.cyfence.com/article/what-is-social-engineering/

บริษัท เอไอเอส จำกัด (มหาชน). (2566, 16 มิถุนายน). *Thailand Cyber Wellness Index (TCWI) by AIS ดัชนีชี้วัดสุขภาวะดิจิทัลของคนไทย*. https://sustainability.ais.co.th/th/sustainability-projects/thailands-cyber-wellness-index

ประชาชาติธุรกิจ. (2567, 3 มีนาคม). *เปิดสถิติแจ้งความออนไลน์ คนไทยสูญเงินรวมกว่า 5.9 หมื่นล้านบาท*. https://www.prachachat.net/ict/news-1514260

โพสต์ทูเดย์. (2566, 11 มกราคม). *ปิดบัญชีม้ากว่า 5.8 หมื่นบัญชี*. https://www.posttoday.com/business/689458

ศูนย์วิจัยเพื่อการพัฒนาสังคมและธุรกิจ จำกัด. 2565. *คนไทยกับการถูกหลอกลวงผ่านอินเทอร์เน็ต/เทคโนโลยีสมัยใหม่*.

สรานนท์ อินทนนท์. (2563). *ทักษะการเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)*. มูลนิธิส่งเสริมสื่อเด็กและเยาวชน.

สาวตรี สุขศรี. (2560). อาชญากรรมคอมพิวเตอร์/ไซเบอร์กับทฤษฎีอาชญาวิทยา. *วารสารนิติศาสตร์*, 46:2. น.415-432.

สุภาวดี ไชยชะลอ (2565,พฤษภาคม). *Victim Blaming : หรือพฤติกรรม 'โทษเหยื่อ' ทำไปเพื่อปลอบใจตัวเอง?*. https://plus.thairath.co.th/topic/everydaylife/101454

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (ม.ป.ป.). *เจอแบบนี้ต้องระวัง "แชร์ลูกโซ่"* https://www.sec.or.th/TH/Pages/SCAMCENTER-01-03.aspx

สำนักงานคณะกรรมการข้าราชการตำรวจ. (ม.ป.ป.). *18 ข้อ กลโกงมิจฉาชีพ*. http://opc.police.go.th/OPC_Police/18-frauds-online/

อาริยา สุขโต. (2565, กรกฎาคม). *ภัยอาชญากรรมแก๊งคอลเซ็นเตอร์*. https://library.parliament.go.th/th/radioscript/rr2565-jul7

ภาษาอังกฤษ

Aasen Foundation. (2024, 25 March). *One Divide or Many Divides? Underprivileged ASEAN Communities' Meaningful Digital Literacy and Response to Disinformation. https://www.aseanfoundation.org/one_divide_or_many_divides_underprivileged_asean_communities_meaningful_digital_literacy_and_response_to_disinformation*

Abraham, S. & Chengalur, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32, 183-196.

Cain, A.A., Edwards, M.E. and Still, J.D. (2018) 'An exploratory study of cyber hygiene behaviors and knowledge', *Journal of Information Security and Applications*, 42, pp. 36–45. doi:10.1016/j.jisa.2018.08.002.

Decety, J., & Yoder, K. J. (2016). Empathy and motivation for justice: Cognitive empathy and concern, but not emotional empathy, predict sensitivity to injustice for others. *Social neuroscience*, *11*(1), 1-14.

DQ institute. (n.d.). *What the DQ Framework?.* https://www.dqinstitute.org/global-standards/

Duangdee, Vijitra. (2022, 29 September). *Nation Must Work Together to Fight Online Fraud, UN Official Says.* https://www.voanews.com/a/nations-must-work-together-to-fight-online-fraud-un-official-says/6768260.html

Friesem, Yonty. Empathy for the digital age: Using video production to enhance social, emotional, and cognitive skills. In *Emotions, technology, and behaviors* (pp. 21-45). Academic Press.

Granger, S. (2001, 18 December). *Social engineering fundamentals, Part I: hacker tactics.* https://s3.amazonaws.com/academia.edu.documents/3172114/04SocialEngineeringWebQuest.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1533316766&Signature=JnMxTdW3AeTxETmBpx7kIvrM4h o%3D&response-content-disposition=inline%3B%20filename%3D04Social_Engineering_Web_Quest.pdf.

Hansson, S. O. (2006). A note on social engineering and the public perception of technology. *Technology in Society, 28*, 389-392.

Harl. (1997, 7 March). *People Hacking: The Psychology of Social Engineering*. http://www.textfiles.com/russian/cyberlib.narod.ru/lib/cin/se10.html.

Interpol. (2022). 2022 Interpol Global Crime Trend summary report. October. INTERPOL General Secretariat: France.

J.R. Tietsort (2023, 7 September*). What is Cyber Hygiene? top 10 ways to stay safe online*https://www.aura.com/learn/cyber-hygiene

Jamshed, Shazia (2014) 'Qualitative research method-interviewing and observation,' *Journal of basic and clinical pharmacy*, 5(4), 87–88, at: https://doi.org/10.4103/0976-0105.141942

Krombholz, K., Hobel, H., Huber, M. & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113-122

Kyodo news. (2023, 16 March). *Cybercrime in Japan hits record high in 2022, ransomware cases surge. ABS-CBN News*. https://news.abs- cbn.com/overseas/03/16/23/cybercrime-in-japan-hits-record-high

Livesey, B. (n.d.). *Cyber hygiene 101: Endpoint, Tanium*. https://www.tanium.com/blog/cyber-hygiene-101/

SamSung SDS. (2022, 23 May). *What Are Cheapfakes (Shallowfakes)?*. https://www.samsungsds.com/en/insights/what-are-cheapfakes.html

SANS Institute. (n.d.). *Glossary of Security Terms*. https://www.sans.org/security-resources/glossary-of-terms.

Slate. (2019, 12 June). *Beware the Cheapfakes.* https://slate.com/technology/2019/06/drunk-pelosi-deepfakes-cheapfakes-artificial-intelligence-disinformation.html

Tarigan, Edna. (2023, 10 May). *ASEAN leaders to agree to cooperate in fighting cyber scams.* https://apnews.com/article/asean-myanmar-humantrafficking- 6d8d9b1c32cf4ed82edec79523db30e3

Tham, Davina. (2023, 8 February). *S$661 million lost to scams in 2022, with young adults most likely to fall victim: SPF.* https://www.channelnewsasia.com/singapore/police-scam- cybercrime-statistics-young-adults-2022- 3262141

Xinhua. (2022, 18 October). *Global cost of cybercrime may reach $10.5 trillion by 2025: Interpol official. In Global Times*. https://www.globaltimes.cn/page/202210/1277410.shtml

ภาคผนวก

รายชื่อผู้เชี่ยวชาญที่ให้สัมภาษณ์

เจ้าหน้าที่ตำรวจกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ (บช.สอท.). (2567, 19 กุมภาพันธ์) *เจ้าหน้าที่รัฐที่เกี่ยวข้องกับการปราบปรามอาชญากรรมออนไลน์*. สัมภาษณ์.

เจ้าหน้าที่ตำรวจทั่วไป. (2567, 13 กุมภาพันธ์) *เจ้าหน้าที่รัฐที่เกี่ยวข้องกับการปราบปรามอาชญากรรมออนไลน์*. สัมภาษณ์.

เจ้าหน้าที่สถาบันวิจัยพฤติกรรมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ. (2567, 20 กุมภาพันธ์) เจ้าหน้าที่รัฐที่เกี่ยวข้องกับอาชญกรรมออนไลน์. สัมภาษณ์.

เจ้าหน้าที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช). (2567, 21 กุมภาพันธ์) *เจ้าหน้าที่รัฐที่เกี่ยวข้องการกับการรักษาความมั่นคงปลอดภัยจากอาชญากรรมออนไลน์*. สัมภาษณ์

เจ้าหน้าที่สำนักงาน คณะกรรมการกิจการกระจายเสียงและกิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.). (2567, 19 กุมภาพันธ์ 2567) *เจ้าหน้าที่รัฐที่เกี่ยวข้องกับการป้องกันอาชญากรรมออนไลน์*. สัมภาษณ์.

นักสื่อสารมวลชน. (2567, 15 กุมภาพันธ์) *นักสื่อสารมวลชนที่เกี่ยวข้องกับอาชญากรรมออนไลน์*. สัมภาษณ์

ผู้เชี่ยวชาญด้านจิตวิทยา. (2567, 5 กุมภาพันธ์). เจ้าหน้าที่รัฐที่ให้คำปรึกษาเกี่ยวกับผู้เสียหายจากอาชญากรรมออนไลน์. สัมภาษณ์.

ผู้เชี่ยวชาญด้านอาชญาวิทยา. (2567, 14 กุมภาพันธ์). เจ้าหน้าที่รัฐที่เกี่ยวข้องกับอาชญากรรมออนไลน์. สัมภาษณ์.

เครื่องมือวิจัย

แนวทางการสัมภาษณ์แบบกลุ่ม (focus group interview)

1. ก่อนเกิดเหตุ ท่านมีการรับรู้ข่าวสารเกี่ยวกับอาชญากรรมออนไลน์มากน้อยเพียงใด จากแหล่งใด สื่อ หน่วยงานรัฐ คนรู้จักเป็นผู้เสียหาย หรืออื่น ๆ

2. ท่านคิดว่าสังคมไทยมีความตระหนักรู้เรื่องดังกล่าวมากพอที่จะเป็นภูมิคุ้มกันตนเองได้หรือไม่

3. ท่านมีการป้องกันตัวเองจากอาชญากรรมออนไลน์มากน้อยเพียงใด

4. หลังจากเกิดเหตุ การรับรู้ข่าวสารที่เคยได้ยินมาเกี่ยวกับอาชญากรรมออนไลน์ ท่านคิดว่ามีประโยชน์ในการรับมือต่อท่านอย่างไร

5. ท่านโดนกลโกงออนไลน์ในรูปแบบใด มิจฉาชีพสามารถเข้าถึงท่านได้อย่างไร

6. อะไรที่ทำให้ท่านรู้ตัวว่ากำลังตกเป็นผู้เสียหายจากอาชญากรรมออนไลน์ ความสูญเสียที่เกิดขึ้นมีอะไรบ้าง

7.ท่านตกเป็นผู้เสียหายมากกว่า1ครั้งหรือไม่ (หมายถึงคนละกรณีกับครั้งแรก) หากเคย อธิบายถึงประสบการณ์ในครั้งถัดมา

8. หากท่านสามารถแบ่งปันประสบการณ์กับผู้ที่อยู่ในสถานการณ์เดียวกัน หรือ ยังไม่ถูกหลอกลวงท่านอยากแบ่งปันประสบการณ์ใด

9. ท่านเล่าเหตุการณ์ที่เกิดขึ้นให้ครอบครัวหรือคนใกล้ชิดฟังหรือไม่ เพราะเหตุใด

10. ผลกระทบและความเปลี่ยนแปลงต่อการดำรงชีวิตที่เกิดขึ้นหลังจากที่เกิดเหตุคืออะไรบ้าง

11. ท่านยังต้องการความช่วยเหลือในการก้าวผ่านเรื่องที่เกิดขึ้นเพื่อใช้กลับไปชีวิตตามปกติหรือไม่ ในด้านใดบ้าง

12. หลังจากที่รู้ตัวว่าเป็นผู้เสียหายจากอาชญากรรมออนไลน์ ท่านจัดการอย่างไร หน่วยงานใดที่ท่านคิดถึงเป็นหน่วยงานแรก และท่านประสบปัญหาอะไรบ้างในการจัดการเรื่องดังกล่าว

13. ท่านคิดว่าหน่วยงานทั้งภาครัฐและเอกชนที่เกี่ยวข้องกับเรื่องนี้ ได้ทำหน้าหรือมีมาตรการในรับมือและเอื้อต่อผู้เสียหายมากน้อยเพียงใด อย่างไร

14. ท่านคิดว่าการป้องกันหรือการดำเนินการของภาครัฐในการป้องกันอาชญากรรมออนไลน์เพียงพอหรือไม่ ระบุเหตุผล

แนวคำถามสัมภาษณ์เชิงลึกสำหรับตัวแทนหน่วยงานที่เกี่ยวข้อง (คำถามร่วม)

1. ท่านคิดว่าหน่วยงานของท่านมีส่วนเกี่ยวข้องกับการแก้ปัญหาการหลอกลวงออนไลน์อย่างไรบ้าง โปรดระบุแนวนโยบาย บทบาท และมาตรการที่เกี่ยวข้อง

2. บทบาทของหน่วยงานท่านในการดำเนินมาตรการป้องกันและให้ความรู้ต่อประชาชน ในประเด็นเรื่องการหลอกลวงออนไลน์มีอะไรบ้าง (หากยังไม่ดำเนินการ คิดว่าถ้ามี ควรจะมีในรูปแบบใด)

3. ท่านคิดว่า ปัญหาเรื่องการหลอกลวงออนไลน์ควรมีหน่วยงานอื่นใด (ทั้งรัฐและเอกชน) เข้ามามีส่วนร่วมอีกบ้าง

4. หน่วยงานของท่านมีการประสานความร่วมมือกับหน่วยงานอื่น ๆ หรือไม่ และอย่างไร

5. หน่วยงานใด ควรเป็นเจ้าภาพในการแก้ไขปัญหา หรือ ควรมีหน่วยงานกลางขึ้นมาใหม่

6. เมื่อได้รับการร้องเรียนความเสียหาย หน่วยงานของท่านมีวิธีการ ขั้นตอนในการดำเนินการอย่างไร ตั้งแต่ การประสานงาน ไปจนถึงการช่วยเหลือผู้เสียหาย (ช่องทาง, เบอร์โทร)

7. ในการดำเนินการมีข้อกำจัด หรือปัญหา อย่างไรบ้าง

8.มาตรการใดที่หน่วยงานของท่านดำเนินการแล้ว และรู้สึกว่าเกิดประโยชน์ต่อการแก้ไขปัญหาการหลอกลวงออนไลน์

9. ท่านคิดว่า มาตรการที่ออกกมาทั้งหมดในปัจจุบันนั้นเพียงพอหรือไม่ อะไรคือปัญหาและความท้าทาย อะไรที่ยังขาดหายไปหรือควรปรับปรุง

10. คิดว่าในอนาคต หน่วยงานของท่านควรมีรูปแบบ, แผนในการรับมือปัญหาการหลอกลวงนี้อย่างไรบ้าง

11. ท่านคิดว่า ประชาชนควรมีชุดความรู้ในด้านใดบ้างที่จะช่วยป้องกันความเสียหายจากการหลอกลวงออนไลน์

12. ข้อเสนอแนะในการสร้างภูมิคุ้มกัน หรือ การรู้เท่าทัน

แนวคำถามสัมภาษณ์เฉพาะหน่วยงาน/องค์กร

1. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มีแผนงานหรือนโยบายในการรับมือในระดับชาติอย่างไร และจะบูรณาการใครเข้ามาบ้าง

2. เจ้าหน้าที่ตำรวจทั่วไป

2.1 บทบาทของตำรวจในการดำเนินการต่อเรื่องดังกล่าวเป็นอย่างไรบ้าง หน่วยงานตำรวจใดที่เป็นหลักในเรื่องนี้

2.2 คดีส่วนใหญ่ที่ได้รับแจ้ง คืออะไร

2.3 นับตั้งแต่มีตำรวจไซเบอร์ มีประชาชนเข้ามาแจ้งความที่สน. มากน้อยเพียงใด

2.4 มีการบูรณาการการดำเนินงานร่วมกับตำรวจไซเบอร์มากน้อยเพียงใด โดยเฉพาะอย่างยิ่งประชาชนมีการแจ้งความทั้งกับตำรวจที่สถานีตำรวจและตำรวจไซเบอร์ จะมีการแนะนำประชาชน หรือมีการประสานงานกับตำรวจไซเบอร์ เพื่อลดความซับซ้อนและความสับสนให้กับประชาชนอย่างไร

2.5 เมื่อได้รับแจ้งเหตุ เปอร์เซ็นที่ผู้เสียหายจะได้รับทรัพย์สินคืนหรือสามารถดำเนินการจับกุมผู้กระทำความผิดมาลงโทษมีมากเพียงใด และใช้ระยะเวลานานมากแค่ไหน

2.6 ทำอย่างไรที่ตำรวจจะมีมาตรการป้องกันที่เท่าทันกลุ่มโจรไซเบอร์ที่มีการพัฒนามาตรการต่าง ๆ และะอัปเดทความก้าวหน้าด้านเทคโนโลยีในการทำลายผู้เสียหายตลอดเวลา

2.7 การดำเนินการในเรื่องมิจฉาชีพออนไลน์กับการค้ามนุษย์มีความเกี่ยวโยงกันมากน้อยเพียงใด

2.8 มีการประสานงานกับหน่วยงานอื่น ๆ หรือประเทศเพื่อนบ้านมากน้อยเพียงใด

3. เจ้าหน้าที่ตำรวจไซเบอร์

3.1 บทบาทของตำรวจไซเบอร์ในการดำเนินการต่อเรื่องดังกล่าวเป็นอย่างไรบ้าง หน่วยงานตำรวจใดที่เป็นหลักในการจัดการมิจฉาชีพออนไลน์

3.2 คดีส่วนใหญ่ที่ได้รับแจ้ง คืออะไร

3.3 นับตั้งแต่มีตำรวจไซเบอร์ ยังมีประชาชนที่สับสนในการทำงานของตำรวจปกติและตำรวจไซเบอร์ โดยเข้ามาแจ้งความที่สถานีตำรวจมากน้อยเพียงใด

3.4 มีบูรณาการการดำเนินงานร่วมกับตำรวจอื่น ๆ มากน้อยเพียงใด โดยเฉพาะอย่างยิ่งมีประชาชนมีการแจ้งความทั้งกับตำรวจที่สถานีตำรวจและตำรวจไซเบอร์ จะมีการแนะนำประชาชน หรือมีการประสานงานกับตำรวจไซเบอร์ เพื่อลดความซับซ้อนและความสับสนให้กับประชาชนอย่างไร

3.5 เมื่อได้รับแจ้งเหตุ เปอร์เซ็นที่ผู้เสียหายจะได้รับทรัพย์สินคืนหรือสามารถดำเนินการจับกุมผู้กระทำความผิดมาลงโทษมีมากเพียงใด และใช้ระยะเวลานานมากแค่ไหน

3.6 ทำอย่างไรก็ตำรวจจะมีมาตรการป้องกันที่ทันแต่กลุ่มโจรไซเบอร์ที่มีการพัฒนามาตรการต่าง ๆ และอัพเดทความก้าวหน้าด้านเทคโนโลยีในการทำลายผู้เสียหายตลอดเวลา

3.7 การดำเนินการในเรื่องมิจฉาชีพออนไลน์กับการค้ามนุษย์มีความเกี่ยวโยงกันมากน้อยเพียงใด

3.8 มีการประสานงานกับหน่วยงานอื่น ๆ หรือประเทศเพื่อนบ้านมากน้อยเพียงใด

4. ธนาคารแห่งประเทศไทย

4.1 บทบาทของหน่วยงานต่อการให้ความรู้และป้องกันอย่างไร

4.2 มีการประสานและบูรณาการทำงานร่วมกับธนาคารต่าง ๆ อย่างไร

4.3 กฎหมาย ข้อบังคับ และกลไกทางการเงินและนาคารที่มีอยู่มีประสิทธิภาพเพียงพอสำหรับการรับมือหรือไม่

5. ธนาคารเอกชน

5.1 บทบาทของธนาคารในการให้ดำเนินมาตรการป้องกันและให้ความรู้ต่อประชาชนมีอย่างไรบ้าง–เช่น ป้องกันการเปิดบัญชีม้า หรือการระงับเมื่อเกิดความเสียหาย

5.2 ธนาคารได้รับการร้องเรียนจากลูกค้าที่เป็นผู้เสียหายมากน้อยเพียงใด

5.3 เมื่อมีความเสียหายเกิดขึ้น ธนาคารมีการดำเนินการอย่างไรทั้งในฐานะที่เป็นธนาคารที่เป็นบัญชีของผู้เสียหาย และธนาคารที่โดนแจ้งว่าเป็นธนาคารของบัญชีมิจฉาชีพอย่างไร

5.4 ข้อจำกัดของธนาคารในการดำเนินมาตรการป้องกันในเรื่องดังกล่าวคืออะไร

5.5 ปัจจุบัน การเข้าถึงสายด่วนของธนาคารเพื่อแจ้งอายัดหรือระงับธุรกิจสามารถทำอย่างไรได้บ้าง

6. สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ

6.1 กสทช มีการหารือกับหน่วยงานที่เกี่ยวข้อง หรือบริษัทโทรคมนาคม หรือ platform เพื่อร่วมกันแก้ปัญหาดังกล่าวมากน้อยเพียงใด

6.2 กฎหมาย ข้อบังคับ และกลไกที่มีอยู่มีประสิทธิภาพเพียงพอสำหรับการรับมือหรือไม่

7. ตัวแทนของสื่อและภาคประชาสังคม

7.1 บทบาทของหน่วยงานท่านต่อการช่วยเหลือ/ประชาสัมพันธ์ และสร้างความรู้เท่าทัน ในเรื่องดังกล่าวเป็นอย่างไร

7.2 ปัจจุบันประชาชนได้รับความตระหนักรู้/รู้เท่าทันจากสื่อและภาคประชาสังคมมากน้อยเพียงใด

7.3. มีผู้เสียหายได้เข้ามารอรับความช่วยเหลือมากน้อยเพียงใดและส่วนใหญ่จะเป็นผู้เสียหายในด้านใด และทางหน่วยงานมีการดำเนินการช่วยเหลืออย่างไรบ้าง

7.4 อะไรที่คิดว่าทำให้ประชาชนเลือกที่จะติดต่อขอความช่วยเหลือกับหน่วยงานท่าน

7.5 การติดต่อขอความช่วยเหลือผ่านทางหน่วยงาน มีข้อดี/ข้อเสียอย่างไรเมื่อเปรียบเทียบกับการที่ผู้เสียหายดำเนินการเอง

8. ผู้เชี่ยวชาญด้านจิตวิทยา

8.1 อะไรที่เป็นสาเหตุให้คนตกเป็นผู้เสียหาย แม้ว่าจะมีการประชาสัมพันธ์หรือมีการรับรู้เรื่องดังกล่าวก็ตาม

8.2 ในช่วง1-2 ปีที่ผ่านมา มีประชาชนมาปรึกษาในเรื่องดังกล่าวมากน้อยเพียงใด

8.3 ปัจจุบัน มีช่องทางในการติดต่อขอคำปรึกษาที่ช่วยให้ประชาชนสามารถเข้าถึงมากน้อยเพียงใด

8.4 มองว่ามาตรการในการเยียวยาจิตใจผู้เสียหายมีความจำเป็นมากเพียงใด และปัจจุบันหน่วยงานที่เกี่ยวข้อให้ได้ความสำคัญมากน้องเพียงใด