รายงานฉบับสมบูรณ์
โครงการวิจัยความรับผิดชอบของสถาบันการเงินต่อภัยออนไลน์ผ่านระบบ mobile banking

นำเสนอ

สภาองค์กรของผู้บริโภค

(Thailand Consumers Council)

จัดทำโดย

บริษัท ป่าสาละ จำกัด

17 มีนาคม 2568

สารบัญ

สารบัญรูปภาพ

สารบัญตาราง

บทสรุปผู้บริหาร

ปัจจุบันผู้บริโภคสามารถเข้าถึงและใช้บริการการทำธุรกรรมทางการเงินผ่านระบบเทคโนโลยีสารสนเทศ ไม่ว่าจะเป็นทางอินเทอร์เน็ต หรือแอปพลิเคชันบนมือถือของธนาคารต่าง ๆ เพื่อทำธุรกรรมที่หลากหลาย อย่างไรก็ตาม ที่ผ่านมาพบว่าการฉ้อโกงทางระบบดิจิทัล ทั้งจากภัยคุกคามทางไซเบอร์ รวมถึงปัญหาบัญชีม้า กลายเป็นประเด็นเร่งด่วนที่สร้างความเสียหายมากขึ้นอย่างต่อเนื่อง ด้วยเหตุนี้ การเรียกร้องความรับผิดชอบที่ชัดเจนจากธนาคารจึงถือเป็นเรื่องสำคัญ และหากธนาคารบกพร่องในมิติใดมิติหนึ่งของการรักษาความมั่นคงปลอดภัยไซเบอร์ หน่วยงานกำกับดูแลก็ควรกำหนดให้มีมาตรการเยียวยาผู้บริโภคอย่างเป็นธรรมและทันท่วงที รวมถึงมีการกำหนดบทลงโทษต่อธนาคารอย่างเหมาะสม

งานวิจัยนี้มีวัตถุประสงค์เพื่อจัดทำข้อเสนอแนะเชิงนโยบายต่อหน่วยงานกำกับดูแลว่าด้วยการยกระดับมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการยกระดับความรับผิดชอบของธนาคาร ต่อกรณีปัญหาทางเทคนิค การฉ้อโกง และการเปิดและใช้บัญชีม้า ที่เกิดกับบริการธนาคารบนมือถือ ผ่านกระบวนการสำรวจข้อมูลเกี่ยวกับกรณีปัญหาทางเทคนิค เหตุการณ์ผิดปกติ การฉ้อโกงของมิจฉาชีพและการเปิดและใช้บัญชีม้า มาตรการแจ้งเตือนและเยียวยาของธนาคารไทย 11 แห่ง ซึ่งเป็นธนาคารที่แนวร่วมการเงินที่เป็นธรรมประเทศไทย (Fair Finance Thailand) ประเมินนโยบายการเปิดเผยข้อมูลตามเกณฑ์ Fair Finance Guide International อย่างต่อเนื่อง การสำรวจนโยบายการกำกับดูแลและแนวปฏิบัติของหน่วยงานที่เกี่ยวข้อง ทั้งในไทยและต่างประเทศ เกี่ยวกับมาตรการรักษาความปลอดภัยทางไซเบอร์ การจัดการบัญชีม้า และแนวทางการชดเชยเยียวยาผู้เสียหาย รวมถึงการสัมภาษณ์เชิงลึกผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง

จากการทบทวนวรรณกรรมและการสัมภาษณ์เชิงลึก พบว่า มิจฉาชีพมีการปรับตัวและพัฒนารูปแบบภัยคุกคามทางไซเบอร์ ซึ่งไม่เพียงแต่การใช้เทคโนโลยีในการโจมตีระบบความปลอดภัยของธนาคารเท่านั้น หากยังรวมถึงการหลอกลวงผู้ใช้ปลายทาง โดยเฉพาะการใช้เทคนิค social engineering หรือการที่มิจฉาชีพใช้จิตวิทยาเพื่อชักจูงให้เหยื่อเปิดเผยข้อมูลสำคัญเอง (authorize) แทนการเจาะระบบของธนาคารโดยตรง ภัยคุกคามทางไซเบอร์เหล่านี้จะมี *“บัญชีม้า”* ทำหน้าที่เป็นตัวกลางในการรับโอนเงินที่ได้จากการหลอกลวง และกระจายเงินไปยังบัญชีปลายทางเพื่อปกปิดตัวตน ทั้งนี้ การใช้บัญชีม้าทำให้การติดตามธุรกรรมผิดกฎหมายทำได้ยาก เนื่องจากมีการพัฒนาเทคนิคการใช้บัญชีม้าที่ซับซ้อนมากขึ้น ไม่เพียงแต่เป็นบัญชีที่บุคคลถูกจ้างให้เปิด แต่ยังรวมถึงการใช้ *“ซิมม้า”* การใช้เอกสารปลอมเพื่อเปลี่ยนเจ้าของบัญชี และการสร้างเครือข่ายบัญชีม้าหลายชั้นเพื่อกระจายเส้นทางการเงินให้ตรวจสอบได้ยากขึ้น

ทั้งนี้ จากการทบทวนแนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินในต่างประเทศ พบว่า หลายประเทศให้ความสำคัญกับการที่สถาบันการเงินต้องมีนโยบายด้านความปลอดภัยไซเบอร์ที่ชัดเจน มีการประเมินความเสี่ยงด้านไซเบอร์ที่อาจเกิดขึ้น มีกระบวนการควบคุมภายในและ

การตรวจสอบ รวมถึงการบูรณาการความเสี่ยงด้านไซเบอร์เข้าไปเป็นส่วนหนึ่งของความเสี่ยงองค์กร มีแผนจัดการความเสี่ยง/การตอบสนองต่อภัยคุกคามทางไซเบอร์ที่ชัดเจน มีการทบทวนและวิเคราะห์บทเรียนจากเหตุการณ์ที่เกิดขึ้น เพื่อนำไปปรับปรุงแผนการตอบสนองเพิ่มเติม มีการพัฒนาระบบติดตาม/เฝ้าระวัง การทดสอบเจาะระบบ/กู้คืนระบบ เป็นต้น

แนวปฏิบัติดังกล่าวสอดคล้องกับแนวปฏิบัติของธนาคารแห่งประเทศไทย (ธปท.) ซึ่งกำหนดให้สถาบันการเงินมีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ครอบคลุมการตรวจสอบและเฝ้าระวังการโจมตีทางไซเบอร์จากช่องโหว่ของระบบ มีการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับมาตรฐานสากล

ขณะที่การจัดการปัญหาบัญชีม้าในต่างประเทศ ในภาพรวมพบว่ามีหน่วยงานที่เกี่ยวข้องหลายหน่วยงานทำงานประสานกัน บางประเทศมีการจัดตั้งคณะทำงานระหว่างหน่วยงานเพื่อทำหน้าที่ในการจัดการปัญหาบัญชีม้าโดยเฉพาะ รวมถึงมีการจัดทำกลไกรับเรื่องร้องเรียนและจัดการปัญหาบัญชีม้าด้วย

สำหรับประเทศไทย พบว่ามีแนวปฏิบัติในการจัดการปัญหาบัญชีม้าที่คล้ายคลึงกับแนวปฏิบัติของหลายประเทศ อาทิ พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี กำหนดบทบาทหน้าที่ให้สถาบันการเงิน ธนาคารแห่งประเทศไทย สำนักงานตำรวจแห่งชาติ สำนักงานป้องกันและปราบปรามการฟอกเงิน กรมสอบสวนคดีพิเศษ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และผู้ให้บริการโทรคมนาคม ร่วมกันแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี ซึ่งรวมถึงบัญชีม้าด้วย นอกจากนี้ ยังมีการจัดตั้งศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (Anti Online Scam Operation Center : AOC) เพื่อเป็นศูนย์กลางในการรับเรื่องและจัดการบัญชีม้าที่บูรณาการความร่วมมือกับทุกภาคส่วน และการพัฒนาระบบ Central Fraud Registry (CFR) เพื่อใช้ในการแลกเปลี่ยนข้อมูลบัญชีต้องสงสัยระหว่างสถาบันการเงิน

สำหรับแนวทางการชดเชยเยียวยาผู้เสียหายจากภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินนั้น พบว่ามีบางประเทศ อาทิ สิงคโปร์ สหรัฐอเมริกา และแคนาดา ที่กำหนดให้สถาบันการเงินมีมาตรการชดเชยเยียวยา กรณีที่เกิดภัยคุกคามทางไซเบอร์ โดยผู้บริโภคไม่จำเป็นต้องรับผิดชอบความเสียหายที่เกิดขึ้น หากการถูกละเมิดหรือฉ้อโกงทางออนไลน์ไม่ได้เป็นผลมาจากความประมาทของผู้บริโภคเอง

สำหรับประเทศอื่น ๆ ส่วนใหญ่ยังอยู่ในขั้นตอนการพัฒนานโยบายหรือมาตรการที่กำหนดความรับผิดชอบที่ชัดเจนในกรณีที่เกิดภัยคุกคามทางไซเบอร์ขึ้น แนวทางการชดเชยเยียวยาผู้เสียหายจากภัยคุกคามทางไซเบอร์ของประเทศกลุ่มนี้มักจะเป็นรูปแบบการฟ้องร้อง พิสูจน์ความผิด เพื่อพิจารณาค่าเสียหายในลำดับถัดไป โดยอาจมีหน่วยงานที่ให้การสนับสนุนในการให้คำแนะนำและดำเนินการฟ้องร้อง เช่น ประเทศออสเตรเลีย นอกจากนี้ยังมีกระบวนการชดเชยเยียวยาอีกทางเลือกหนึ่งในรูปแบบการเรียกร้องค่าสินไหมจากบริษัทประกันภัย เช่น ประเทศฝรั่งเศส ที่มีการออกกฎหมายรองรับในส่วนประกันภัยไซเบอร์โดยตรง เป็นต้น

สำหรับประเทศไทย อาจจัดอยู่ในกลุ่มประเทศที่ยังไม่มีมาตรการชดเชยเยียวยาจากสถาบันทางการเงินอย่างเป็นรูปธรรมเช่นกัน ทั้งนี้ แม้ว่าที่ผ่านมา ธปท. ได้จัดทำแนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน ซึ่งกำหนดชัดเจนว่ากรณีเหตุการณ์ทุจริตที่มีผู้เสียหายจากการทำธุรกรรมการชำระเงิน โดยไม่ได้เกิดจากความผิดของผู้เสียหาย ผู้ให้บริการต้องเยียวยาความเสียหายอย่างครบถ้วน อย่างไรก็ตาม ในทางปฏิบัติ ผู้บริโภคในประเทศไทยอาจไม่ได้รับการเยียวยาความเสียหายอย่างครบถ้วนตามข้อกำหนด แต่จำเป็นต้องมีการพิจารณาเป็นรายกรณี โดยอัตราการชดเชยเยียวยาขึ้นอยู่กับคำพิพากษาของศาล

คณะวิจัยสกัดข้อสังเกตและข้อค้นพบที่สำคัญจากการทบทวนวรรณกรรมและการสัมภาษณ์ และจัดทำเป็นข้อเสนอแนะเชิงนโยบาย เพื่อให้การกำกับดูแลและคุ้มครองผู้บริโภคจากภัยคุกคามทางไซเบอร์และมิจฉาชีพออนไลน์ มีประสิทธิภาพมากขึ้น ดังนี้

1) การยกระดับความเข้มงวดในการตรวจสอบข้อมูลและยืนยันตัวตนในการเปิดบัญชีและการทำธุรกรรมทางการเงินต่าง ๆ

ที่ผ่านมาแม้ว่า ธปท. ให้ความสำคัญกับการกำกับดูแลให้สถาบันการเงินดำเนินการตามแนวปฏิบัติความปลอดภัยด้านเทคโนโลยีสารสนเทศและบัญชีม้าอยู่แล้ว อย่างไรก็ตาม คณะวิจัยมีข้อเสนอว่า ธปท. ควรพิจารณาและศึกษาความเป็นไปได้ในการทบทวนและปรับปรุงแนวปฏิบัติของสถาบันการเงินให้มีความเข้มงวดมากขึ้นในการตรวจสอบข้อมูลและยืนยันตัวตนในการเปิดบัญชี และการทำธุรกรรมทางการเงินต่าง ๆ เพื่อให้สามารถเฝ้าระวังและตรวจสอบพฤติกรรมผิดปกติในระบบได้ก่อนที่จะเกิดเหตุการณ์ขึ้น เช่น

- การตรวจสอบพฤติกรรมก่อนอนุมัติการเปิดบัญชี เช่น การวิเคราะห์ข้อมูลพฤติกรรมทางการเงินของบุคคลที่มาขอเปิดบัญชี หากมีแนวโน้มเป็นบัญชีม้า หรือมีความเสี่ยงสูง ควรมีการตรวจสอบเชิงลึกเพิ่มเติม (enhanced due diligence)
- การจำกัดจำนวนบัญชีที่บุคคลใดบุคคลหนึ่งสามารถเปิดได้ เพื่อป้องกันไม่ให้มิจฉาชีพใช้ตัวตนเดียวเปิดหลายบัญชี แล้วนำไปใช้ในกิจกรรมผิดกฎหมาย ทั้งนี้ หากตรวจพบ “เปิดบัญชีหลายสิบบัญชี” ในชื่อเดียว อาจเข้าข่ายบัญชีม้า ควรแจ้งเตือน/ตรวจสอบเป็นพิเศษ
- การกำหนดให้ลูกค้าใช้วิธียืนยันตัวตนหลายวิธีร่วมกัน เช่น การใช้รหัสผ่านร่วมกับรหัส OTP เมื่อทำธุรกรรมสำคัญ หรือเกี่ยวข้องกับบัญชีต้องสงสัย เช่น การโอนเงิน หรือการเพิ่มบัญชีผู้รับโอน
- การกำหนดให้สถาบันการเงินพัฒนาและใช้เทคโนโลยี AI และ machine learning ที่สามารถวิเคราะห์พฤติกรรมของบัญชีธนาคารและธุรกรรมที่ผิดปกติ โดยระบบสามารถแจ้งเตือนและระงับธุรกรรมชั่วคราวหากพบพฤติกรรมผิดปกติ

- การกำหนดให้สถาบันการเงินพัฒนาระบบแจ้งเตือนอัตโนมัติเมื่อมีการทำธุรกรรมที่มีความเสี่ยงสูง และอนุญาตให้ผู้ใช้สามารถระงับการทำธุรกรรมได้เองในช่วงระยะเวลาหนึ่ง โดยเฉพาะธุรกรรมที่มีมูลค่าสูง หรือมีรูปแบบแตกต่างจากธุรกรรมปกติ

ทั้งนี้ การศึกษาความเป็นไปได้ในการทบทวนและปรับปรุงแนวปฏิบัติดังกล่าว ควรเปิดให้มีการรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องและครอบคลุมทุกกลุ่ม เพื่อให้มีข้อมูลที่ครบถ้วน เพียงพอ และสามารถรักษาสมดุลระหว่างการยกระดับมาตรการความปลอดภัยกับความสะดวกของประชาชนได้ นอกจากนี้ ธปท. ควรพิจารณาทบทวนประสิทธิผลของมาตรการที่ผ่านมาของ ธปท. อย่างน้อยปีละ 1 ครั้ง เนื่องจากมิจฉาชีพเปลี่ยนแปลงเทคนิคการหลอกลวงอยู่เสมอมาตรการที่เคยได้ผลในอดีตอาจไม่จำเป็น หรือได้ประโยชน์ไม่คุ้มค่ากับต้นทุนหรือความเสี่ยงอีกต่อไป ตัวอย่างเช่น มาตรการสแกนใบหน้าทุกครั้งที่โอนเงินขั้นต่ำ 50,000 บาท สร้างภาระให้กับผู้ใช้บริการ เพิ่มความเสี่ยงที่ข้อมูลชีวมิติ (biometric) อาจรั่วไหลจากสถาบันการเงิน ในขณะเดียวกันก็ไม่สามารถแก้ปัญหาการหลอกลวงของมิจฉาชีพปัจจุบันที่ใช้วิธีล่อหลอกให้ผู้ใช้บริการทำธุรกรรมด้วยตัวเอง มิได้สวมรอยเป็นผู้ใช้แต่อย่างใด

2) การบูรณาการความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้อง

การจัดการกับปัญหาภัยคุกคามทางไซเบอร์และบัญชีม้าเป็นปัญหาสำคัญที่ต้องได้รับความร่วมมือจากทุกภาคส่วนที่เกี่ยวข้อง ที่ผ่านมาหลายหน่วยงานมีความพยายามจะบูรณาการความร่วมมือในการจัดการปัญหา เช่น การจัดตั้งศูนย์ AOC หรือความร่วมมือของธนาคารในการดำเนินงานร่วมกันผ่านกลไกของ TB-CERT เป็นต้น อย่างไรก็ตาม ความร่วมมือดังกล่าวยังไม่สามารถจัดการปัญหาภัยคุกคามทางไซเบอร์ได้อย่างเด็ดขาด และยังไม่รวดเร็วพอที่จะรับมือรับมือกับมิจฉาชีพที่ปรับตัวได้ตลอดเวลา

คณะวิจัยมีข้อเสนอว่า หน่วยงานที่เกี่ยวข้องควรมีการดำเนินการเชิงรุกในการผลักดันความร่วมมือระหว่างกัน เพื่อให้การจัดการปัญหาดังกล่าวมีประสิทธิภาพมากยิ่งขึ้น ดังนี้

- **การสร้างระบบแบ่งปันข้อมูลบัญชีม้าแบบเรียลไทม์** ซึ่งจะทำให้เข้าถึงข้อมูลธุรกรรมต้องสงสัยได้เร็วขึ้น และยกระดับการป้องกันและติดตามเส้นทางการเงินของบัญชีม้าได้อย่างมีประสิทธิภาพมากขึ้น
- **การจัดตั้งคณะทำงานร่วมเพื่อศึกษาความเป็นไปได้ในการปรับปรุงกฎหมายเพื่อทลายข้อจำกัดของสถาบันการเงินในการจัดการบัญชีม้า** อาทิ การเพิ่มอำนาจของธนาคารในการอายัดบัญชีได้โดยไม่ต้องรอคำสั่งจากตำรวจ หรือสามารถขยายระยะเวลาการระงับบัญชีต้องสงสัยได้ (ปัจจุบันระยะเวลาการระงับบัญชีอยู่ที่ 72 ชั่วโมง) หากมีหลักฐานเพียงพอว่าบัญชีดังกล่าวอยู่ในฐานข้อมูลบัญชีม้าหรือมีพฤติกรรมผิดปกติ และการปรับปรุงแนวปฏิบัติในกระบวนการดำเนินคดี โดยกำหนดให้หน่วยงานภาครัฐและธนาคารต้องให้ความช่วยเหลือทางกฎหมายแก่ผู้เสียหาย โดยไม่ต้องรอให้ผู้เสียหายดำเนินการด้วยตนเอง

- **การจัดตั้งคณะทำงานร่วมเพื่อจัดทำแผนและดำเนินการสื่อสาร ประชาสัมพันธ์ และสร้างความตระหนักรู้ให้กับประชาชน** เกี่ยวกับภัยคุกคามทางไซเบอร์ การรับมือกลลวงของมิจฉาชีพ โทษจากการมีส่วนร่วมในการเปิดบัญชีม้า รวมถึงการประชาสัมพันธ์ศูนย์ AOC ให้เป็นที่รู้จักในฐานะศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ที่สามารถดำเนินการได้แบบเบ็ดเสร็จ โดยดำเนินการเชิงรุกในลักษณะแผนการสื่อสารประชาสัมพันธ์ที่เป็นวาระแห่งชาติ มีช่องทางการสื่อสารที่หลากหลาย เข้าถึงประชาชนทุกกลุ่ม โดยเฉพาะกลุ่มเปราะบาง

3) การกำหนดความรับผิดชอบของสถาบันการเงินในกระบวนการเยียวยาผู้เสียหายให้ชัดเจนมากขึ้น

ปัจจุบันผู้บริโภคที่เป็นผู้เสียหายจากภัยคุกคามทางไซเบอร์และสูญเสียเงินฝากในธนาคารต้องดำเนินการฟ้องร้องธนาคารพาณิชย์ด้วยตนเอง และสุดท้ายอาจได้รับการชดเชยเยียวยาความเสียหายเพียงบางส่วน (พิจารณาเป็นรายคดี ขึ้นอยู่กับคำพิพากษาของศาล) นอกจากนี้ แม้ว่ากระบวนการยุติธรรมจะสิ้นสุดแล้ว แต่ผู้เสียหายอาจไม่ได้รับเงินคืน เนื่องจากมิจฉาชีพได้โอนเงินออกจากบัญชีไปยังบัญชีม้าอื่น ๆ เรียบร้อยแล้ว หรือแม้ว่าจะสามารถติดตามเงินคืนจากมิจฉาชีพได้ แต่กระบวนการยึดทรัพย์เพื่อเฉลี่ยคืนให้กับผู้เสียหายอาจต้องใช้ระยะเวลามากกว่า 1 ปี อีกทั้งยังไม่มีแนวปฏิบัติที่ชัดเจนในกระบวนการพิจารณาลักษณะการเยียวยาหรือการเฉลี่ยทรัพย์ให้แก่ผู้เสียหายแต่ละราย ทั้งนี้ ผู้เสียหายอาจได้รับเงินคืนน้อยกว่ามูลค่าที่เสียหาย เนื่องจากต้องเฉลี่ยเงินคืนให้แก่ผู้เสียหายรายอื่น ๆ ด้วย

เพื่อปรับปรุงกระบวนการเยียวยาให้มีความชัดเจนและรวดเร็วมากขึ้น คณะวิจัยมีข้อเสนอให้ ธปท. พิจารณาจัดทำหลักเกณฑ์ แนวปฏิบัติ และความรับผิดชอบของสถาบันการเงินในการเยียวยาผู้เสียหายที่มีความชัดเจนมากยิ่งขึ้น โดยอย่างน้อยควรพิจารณาประเด็นดังต่อไปนี้

- การจัดทำหลักเกณฑ์ในการชดเชยเยียวยาผู้เสียหายที่มีความชัดเจนมากขึ้น โดยเฉพาะในกรณีที่ผู้เสียหายถูกมิจฉาชีพหลอกลวงให้ทำธุรกรรมเอง (authorized fraud)
- การกำหนดมาตรฐานการชดเชยเยียวยาที่เป็นธรรม โดยผู้เสียหายควรได้รับการชดเชยเยียวยาภายในระยะที่เหมาะสม หลังจากที่สามารถพิสูจน์ได้ว่าถูกมิจฉาชีพหลอกลวง และสถาบันการเงินควรต้องชดเชยเยียวยา หรือ “คืนเงินโดยอัตโนมัติ” โดยไม่ต้องให้ผู้เสียหายดำเนินการทางกฎหมายเอง หากสามารถพิสูจน์ได้ว่าความเสียหายดังกล่าวเกิดจากความบกพร่องของธนาคาร เช่น ไม่ได้แจ้งเตือนธุรกรรมที่มีความเสี่ยง

4) การเพิ่มความเข้มงวดในการลงทะเบียนซิมโทรศัพท์

ซิมม้าเป็นช่องโหว่สำคัญที่มิจฉาชีพใช้ในการเข้าถึงระบบธนาคาร เนื่องจากเป็นขั้นตอนสุดท้ายของการยืนยันตัวตนของผู้ใช้บริการ ดังนั้น กสทช. ในฐานะหน่วยงานกำกับดูแลผู้ให้บริการโทรคมนาคม

ควรพิจารณาและศึกษาความเป็นไปได้ในการทบทวนและปรับปรุงแนวปฏิบัติของผู้ให้บริการโทรคมนาคมให้มีความเข้มงวดมากขึ้นในการตรวจสอบข้อมูลและยืนยันตัวตนในการเปิดซิม เช่น

- ผู้ให้บริการโทรคมนาคมต้องตรวจสอบตัวตนเข้มงวด เมื่อลูกค้าขอออกซิมใหม่/ย้ายซิม
- ผู้ให้บริการโทรคมนาคมต้องติดตั้งระบบ AI-based Filtering เพื่อตรวจสอบและบล็อก SMS ที่มีลิงก์ฟิชชิงหรือข้อความน่าสงสัย ก่อนถึงลูกค้า

นอกจากนี้ ควรกำหนดให้มีการยืนยันตัวตนผู้ใช้งานซิมเป็นระยะ เช่น เจ้าของซิมต้องกดยืนยันความเป็นเจ้าของซิมภายในระยะเวลาที่กำหนด รวมทั้งควรจัดทำหลักเกณฑ์ในการตรวจสอบและสุ่มตรวจหมายเลขโทรศัพท์ที่มีพฤติกรรมผิดปกติ เช่น หมายเลขที่ใช้ทำธุรกรรมที่มีความเสี่ยงสูง และกำหนดให้ผู้ให้บริการโทรคมนาคมรายงานผลการตรวจสอบเป็นประจำ รวมถึงเผยแพร่ผลการตรวจสอบต่อสาธารณะ

5) การกำกับดูแลและยกระดับการป้องกันการใช้แพลตฟอร์มออนไลน์ในการหลอกลวง

มิจฉาชีพจำนวนมากใช้แพลตฟอร์มออนไลน์ในการหลอกลวงเหยื่อ ไม่ว่าจะเป็นการลงทุนปลอม การหลอกขายของออนไลน์ หรือการปลอมตัวเป็นหน่วยงานราชการ ดังนั้น หน่วยงานที่เกี่ยวข้องควรกำหนดมาตรการเพื่อยกระดับการป้องกันการใช้แพลตฟอร์มออนไลน์ในการหลอกลวง เช่น

- การกำหนดแนวปฏิบัติให้ผู้ให้บริการแพลตฟอร์มออนไลน์ต้องมีมาตรการตรวจสอบตัวตนผู้ใช้งาน เช่น การยืนยันตัวตนของผู้ขายที่เข้มงวดขึ้น เพื่อลดการใช้บัญชีปลอมในการขายของหลอกลวง และหากมีการโอนเงินภายในแพลตฟอร์ม ควรบันทึกข้อมูลบัญชีธนาคารที่ชัดเจน และไม่เปิดช่องให้ใช้เกิดบัญชีร้านค้าแบบไม่มีการยืนยันตัวตน
- การกำหนดแนวปฏิบัติให้ผู้ให้บริการแพลตฟอร์มออนไลน์มีระบบรายงานร้านค้าที่มีความเสี่ยงฉ้อโกง เช่น การกำหนดให้มี ปุ่มรายงาน (Report) สำหรับผู้บริโภคใช้ร้องเรียนร้านค้าต้องสงสัย การตั้งทีมตรวจสอบเร่งด่วน หากพบหลักฐานฉ้อโกง จะต้องแบน/ระงับร้านหรือบัญชี หรืออายัดเงินค้างในระบบทันที
- การจัดทำ “บัญชีขาว” (White List) สำหรับบัญชีที่สามารถทำธุรกรรมทางการเงินได้ และเปิดให้ธนาคารสามารถตรวจสอบความน่าเชื่อถือของบัญชีปลายทางก่อนอนุมัติการโอนเงินได้

บทที่ 1 ที่มาและความสำคัญ

1.1 ความสำคัญและที่มา

ปัจจุบัน ผู้บริโภคสามารถเข้าถึงและใช้บริการการทำธุรกรรมทางการเงินผ่านระบบเทคโนโลยีสารสนเทศ ไม่ว่าจะเป็นทางอินเทอร์เน็ต หรือแอปพลิเคชันบนมือถือของธนาคารต่าง ๆ เพื่อทำธุรกรรมที่หลากหลาย เช่น การโอนเงิน การจ่ายชำระค่าสินค้าและบริการ การจ่ายชำระค่าสาธารณูปโภค การจ่ายชำระบัตรเครดิต และรวมถึงการลงทุนต่าง ๆ ในตลาดเงินและตลาดทุน ผู้บริโภคสามารถทำธุรกรรมทางการเงินได้อย่างสะดวก รวดเร็ว ไม่จำกัดเวลาและสถานที่ ปัจจุบันประเทศไทยกลายเป็นหนึ่งในประเทศที่คนใช้บริการทางการเงินดิจิทัลสูงสุด รายงาน Digital 2021 ระบุว่าคนไทยใช้แอปพลิเคชันธนาคารบนมือถือ (mobile banking) มากเป็นอันดับต้น ๆ ของโลก และเป็นหนึ่งในห้าอันดับแรกสำหรับธุรกรรม e-commerce การชำระเงินผ่านมือ และการใช้ QR โค้ด (Leesa-Nguansuk, 2021) ขณะที่ธนาคารแห่งประเทศไทยรายงานว่า ในปี 2565 มีปริมาณการโอนเงินผ่านแอปพลิเคชันธนาคารบนมือถือ 22.8 พันล้านรายการ คิดเป็นมูลค่ากว่า 66,231 พันล้านบาท เพิ่มขึ้นร้อยละ 17.91 จากปีก่อนหน้า (Bank of Thailand, 2024)

นอกจากนี้ การฉ้อโกงทางระบบดิจิทัลได้กลายเป็นประเด็นเร่งด่วนที่สร้างความเสียหายมากขึ้นอย่างต่อเนื่อง สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (สศช.) พบว่า รูปแบบการหลอกลวงที่แพร่หลายในประเทศไทยคือการแอบอ้างข้อมูล ซึ่งมักก่อให้เกิดความเสียหายสูง กรณีที่พบบ่อยคือการโทรศัพท์ ส่ง SMS หรืออีเมลปลอมแปลงเป็นองค์กรที่น่าเชื่อถือเพื่อหลอกให้ผู้ใช้ทำธุรกรรมหรือป้อนข้อมูลส่วนตัวสำคัญ เช่น รหัสผ่านและหมายเลขบัตรเครดิต โดย สศช. ระบุว่าในปี 2564 คนไทยได้รับสายหลอกลวงจากแก๊งค้าโทรศัพท์ (รูปแบบหนึ่งของการแอบอ้างข้อมูล) มากกว่า 6.4 ล้านสาย จากรายงานการฟ้องร้องและการร้องเรียน พบว่ามีผู้เสียหายจากแก๊งค้าโทรศัพท์มากกว่า 1,600 รายด้วยมูลค่าความเสียหายรวมกว่า 1 พันล้านบาท คนไทยได้รับสายหลอกลวงและ SMS หลอกลวงเพิ่มขึ้น 270 เปอร์เซ็นต์และ 57 เปอร์เซ็นต์ตามลำดับในช่วงหลายปีที่ผ่านมา

ด้วยเหตุนี้ การเรียกร้องความรับผิดชอบที่ชัดเจนจากสถาบันการเงิน อาทิ การกำหนดมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (cybersecurity)[1] ระดับสูง จึงถือเป็นเรื่องสำคัญ หากธนาคารไม่มีระบบการรักษาความมั่นคงปลอดภัยของระบบที่ดีเพียงพอก็เป็นความเสี่ยงที่ผู้บริโภคและธนาคารจะได้รับความเสียหายทางการเงินเป็นอย่างมาก ความมั่นคงปลอดภัยไซเบอร์จึงเป็นเรื่องสำคัญที่ผู้ใช้บริการและสถาบันการเงินควรให้ความสนใจ ซึ่งวัตถุประสงค์หลักของความมั่นคงปลอดภัยไซเบอร์ครอบคลุมตั้งแต่ การรักษาความลับของ

[1] ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking คือ การปกป้องข้อมูลทางการเงินและธุรกรรมบนแอปธนาคารมือถือหรืออุปกรณ์แท็บเล็ตจากภัยคุกคามไซเบอร์ เช่น การฟิชชิง มัลแวร์ การโจมตีเครือข่าย และการเข้าถึงโดยไม่ได้รับอนุญาต โดยใช้มาตรการต่าง ๆ เช่น การเข้ารหัสข้อมูล การยืนยันตัวตนสองขั้นตอน การอัปเดตแอปและระบบปฏิบัติการ การใช้ซอฟต์แวร์ป้องกันไวรัส การตรวจสอบสิทธิ์แอป และการให้ความรู้แก่ผู้ใช้งาน รวมถึงมาตรการที่เกี่ยวข้องกับการวินิจฉัยและการเยียวยาผู้ได้รับความเสียหายจากมิจฉาชีพ

ระบบและข้อมูล (confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) (ITU, 2020)

เมื่อสถาบันการเงินบกพร่องในมิติใดมิติหนึ่งของการรักษาความมั่นคงปลอดภัยไซเบอร์ หน่วยงานกำกับดูแลก็ควรกำหนดให้มีมาตรการเยียวยา (remedy) ผู้บริโภคอย่างเป็นธรรมและทันท่วงที รวมถึงมีการกำหนดบทลงโทษ (penalty) ต่อธนาคารอย่างเหมาะสม เพื่อเพิ่มแรงจูงใจในการลงทุนเพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันการฉ้อโกงและปัญหาทางเทคนิคที่เกิดกับระบบ mobile banking

1.2 วัตถุประสงค์โครงการ

1) รวบรวมและนำเสนอสถิติต่อสาธารณะอย่างเป็นระบบ เกี่ยวกับกรณีปัญหาทางเทคนิค เหตุการณ์ผิดปกติ รวมถึงการฉ้อโกงของมิจฉาชีพและการเปิดและใช้บัญชีม้า รวมถึงมาตรการแจ้งเตือนและเยียวยา สำหรับบริการธนาคารบนมือถือ (mobile banking) ของธนาคารพาณิชย์ชั้นนำ 11 แห่ง
2) นำเสนอข้อเสนอแนะเชิงนโยบายต่อหน่วยงานกำกับดูแล ว่าด้วยการยกระดับมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ (cybersecurity) และมาตรการยกระดับความรับผิดชอบของธนาคาร (accountability) ต่อกรณีปัญหาทางเทคนิค การฉ้อโกง และการเปิดและใช้บัญชีม้า ที่เกิดกับบริการธนาคารบนมือถือ

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1) ประชาชนหรือผู้สนใจสามารถเข้าถึงข้อมูลสถิติกรณีปัญหาทางเทคนิค เหตุการณ์ผิดปกติและการฉ้อโกงของมิจฉาชีพได้
2) ธนาคารไทยมีตัวอย่างแนวปฏิบัติที่ดีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการป้องกันการฉ้อโกง รวมถึงมาตรการเยียวยาที่เหมาะสม เพื่อลดความเสียหายจากเหตุการณ์ผิดปกติและการฉ้อโกงของมิจฉาชีพ อันจะนำไปสู่การพัฒนาระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของธนาคารได้ต่อไป
3) หน่วยงานกำกับดูแลมีแนวทางในการยกระดับมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรการยกระดับความรับผิดชอบของธนาคาร (accountability) ต่อกรณีปัญหาทางเทคนิค การฉ้อโกง และการเปิดและใช้บัญชีม้าที่เกิดกับบริการธนาคารบนมือถือ ซึ่งจะเป็นประโยชน์ต่อประชาชนและผู้ใช้บริการทางการเงิน

1.4 ระเบียบวิธีวิจัย

คณะวิจัยใช้ระเบียบวิธีวิจัยหลัก ๆ ดังนี้

- การทบทวนวรรณกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และการฉ้อโกงของมิจฉาชีพของภาคธนาคารในประเทศไทย โดยมีเนื้อหาอย่างน้อยประกอบด้วย

- สำรวจข้อมูลปัญหาหรือเหตุการณ์ผิดปกติ รวมถึงการฉ้อโกงของมิจฉาชีพ และการเปิดและใช้บัญชีม้า สำหรับบริการธนาคารบนมือถือ (mobile banking) ในช่วงเวลา 15 เดือน ระหว่างวันที่ 1 มกราคม 2566 – 31 มีนาคม 2567
- สำรวจข้อมูลนโยบายความยั่งยืนประจำปีที่เกี่ยวข้อง ของธนาคารไทย 11 แห่ง ที่แนวร่วมการเงินที่ธรรมประเทศไทย (Fair Finance Thailand) ได้แก่ ธนาคารกรุงเทพ ธนาคารกรุงไทย ธนาคารไทยพาณิชย์ ธนาคารกสิกรไทย ธนาคารทหารไทยธนชาต ธนาคารกรุงศรีอยุธยา ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ธนาคารเกียรตินาคินภัทร ธนาคารออมสิน ธนาคารทิสโก้ ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย
- สำรวจแนวทางการแก้ปัญหา การแจ้งเตือน และการเยียวยาของธนาคารพาณิชย์ในกรณีที่เกิดปัญหาหรือเหตุการณ์ผิดปกติ รวมถึงการฉ้อโกงของมิจฉาชีพ รวมถึงนโยบายการกำกับดูแลของหน่วยงานที่เกี่ยวข้อง เช่น ธนาคารแห่งประเทศไทย และสำนักงานตำรวจแห่งชาติ เป็นต้น
- สำรวจมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรการความรับผิดชอบของธนาคารต่อกรณีที่เกิดปัญหาทางเทคนิค หรือการฉ้อโกงผ่าน mobile banking ในประเทศสหรัฐอเมริกา สิงคโปร์ อินโดนีเซีย ฟิลิปปินส์ และบราซิล

- สัมภาษณ์ตัวแทนธนาคารพาณิชย์ ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ และหน่วยงานกำกับดูแลที่เกี่ยวข้อง (รวม 30 ราย)
  - จัดทำคำถามสัมภาษณ์เชิงลึกสำหรับผู้มีส่วนได้ส่วนเสียแต่ละกลุ่ม
  - สัมภาษณ์เชิงลึกตัวแทนธนาคารพาณิชย์ ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ หน่วยงานกำกับดูแลที่เกี่ยวข้อง และตัวแทน
- นำผลจากการทบทวนวรรณกรรมและการสัมภาษณ์เชิงลึกมาจัดทำรายงานฉบับสมบูรณ์

1.5 แผนการดำเนินงาน

ระยะเวลาดำเนินงาน 225 วัน โดยมีแผนการดำเนินงาน ดังนี้

กิจกรรม	ส.ค. 67				ก.ย.67				ต.ค.67				พ.ย.67				ธ.ค.67				ม.ค.68				ก.พ.68				มี.ค.68	
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2
จัดทำเค้าโครงการศึกษาวิจัยและแผนการดำเนินงาน																														
เก็บรวบรวมและสังเคราะห์ข้อมูลปัญหาหรือเหตุการณ์ผิดปกติ รวมถึงการฉ้อโกงของมิจฉาชีพ การเปิดและใช้บัญชีม้า รวมถึงนโยบายของธนาคารพาณิชย์ 11 แห่ง ในช่วงวันที่ 1 มกราคม 2566 – 31 มีนาคม 2567																														
สำรวจมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรการความรับผิดชอบของธนาคาร ต่อกรณีที่เกิดปัญหาทางเทคนิค หรือการฉ้อโกงผ่าน mobile banking ในประเทศ สหรัฐอเมริกา สิงคโปร์ อินโดนีเซีย ฟิลิปปินส์ และบราซิล																														
จัดทำคำถามสัมภาษณ์สำหรับ ผู้แทนธนาคาร - ผู้เชี่ยวชาญ - หน่วยงานกำกับดูแล - ตัวแทนผู้บริโภค																														
นัดหมายสัมภาษณ์เชิงลึก ธนาคาร ตัวแทนผู้บริโภค นักวิชาการ และหน่วยงานกำกับดูแล																														
สัมภาษณ์เชิงลึก ธนาคาร ตัวแทนผู้บริโภค นักวิชาการ และหน่วยงานกำกับดูแล																														
จัดทำผลการสัมภาษณ์เชิงลึก																														
จัดทำข้อเสนอแนะเชิงนโยบาย																														
ปรับปรุงแก้ไขร่างรายงานฉบับสมบูรณ์																														
ผลผลิต																														
งวดที่ 1 เค้าโครงการศึกษาวิจัยและแผนการดำเนินงาน																														
งวดที่ 2 รายงานความก้าวหน้า: การทบทวนวรรณกรรมเกี่ยวกับการสำรวจข้อมูลปัญหาจากอาชญากรรมทางเทคโนโลยี และการเปิดและใช้บัญชีม้าในไทย รวมถึงมาตรการรักษาความปลอดภัยไซเบอร์ของไทยและต่างประเทศอย่างน้อย 5 ประเทศ																														
งวดที่ 3 ร่างรายงานฉบับสมบูรณ์: ผลการสัมภาษณ์เชิงลึกและข้อเสนอแนะเชิงมาตรการเพื่อคุ้มครองผู้บริโภค																														
งวดที่ 4 จัดทำรายงานวิจัยฉบับสมบูรณ์																														

บทที่ 2 การทบทวนวรรณกรรมที่เกี่ยวข้อง

ในบทนี้ คณะวิจัยทบทวนวรรณกรรมในประเด็นภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงิน โดยครอบคลุมสภาพปัจจุบันของปัญหาภัยคุกคามทางไซเบอร์ในประเทศไทย รูปแบบภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงิน ปัญหาบัญชีม้าที่เชื่อมโยงกับภัยคุกคามทางไซเบอร์ บทบาทหน้าที่ของหน่วยงานในประเทศที่เกี่ยวข้อง ตลอดจนแนวปฏิบัติในการป้องกันภัยคุกคามทางไซเบอร์และการจัดการบัญชีม้าในต่างประเทศ โดยมีรายละเอียด ดังนี้

2.1 ภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงิน

2.1.1 นิยามและรูปแบบของภัยทางการเงินออนไลน์

ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking หรือภัยทางการเงินออนไลน์ (Online Financial Fraud) มีการให้ความหมายโดยรวม หมายถึง การกระทำที่มุ่งหวังผลประโยชน์ทางการเงินโดยมิชอบผ่านช่องทางออนไลน์ เช่น การหลอกลวงให้โอนเงิน การขโมยข้อมูลส่วนบุคคล หรือการเข้าถึงบัญชีการเงินโดยไม่ได้รับอนุญาต ซึ่งในแต่ละบริบท/ประเทศ อาจมีการให้คำนิยามหรือรูปแบบที่แตกต่างกันออกไป โดยสามารถสรุปนิยามจากการอ้างอิงบทกฎหมายของแต่ละประเทศ ดังนี้

ไทย ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking ในกฎหมายไทยครอบคลุมการกระทำที่ใช้คอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ในการหลอกลวง ยักยอก หรือเข้าถึงข้อมูลทางการเงินของผู้อื่นโดยมิชอบ จนทำให้เกิดความเสียหายทางทรัพย์สินแก่บุคคลทั่วไปหรือสาธารณะ ซึ่งกฎหมายที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (แก้ไขเพิ่มเติม พ.ศ. 2560) มาตรา 14 (1) ที่กำหนดโทษกรณีบันทึกข้อมูลอันเป็นเท็จหรือฉ้อฉลเข้าสู่ระบบคอมพิวเตอร์โดยทุจริต รวมถึงมาตรา 14 (4) ที่ครอบคลุมถึงการกระทำใด ๆ ที่ก่อให้เกิดความเสียหายต่อประชาชน ซึ่งมักรวมถึงการหลอกลวงทางการเงินออนไลน์ การเจาะระบบเพื่อนำข้อมูลทางการเงินไปใช้โดยมิชอบ หรือการสร้างเว็บไซต์ปลอมเพื่อรับข้อมูลบัตรเครดิตเป็นต้น (Society, Ministry of Digital Economy and, 2017)

นอกจากนี้ พรก. มาตรการป้องกันอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ระบุว่านิยามความผิดเกี่ยวกับภัยออนไลน์ว่าเป็นความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือการกระทำความผิดฐานฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ

สหรัฐอเมริกา ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking ถูกกำหนดภายใต้กฎหมายของรัฐและรัฐบาลกลาง เช่น กฎหมาย 18 U.S.C. 1343 ที่ครอบคลุมการฉ้อโกงทางไซเบอร์ทั่วไป ซึ่งอาจมีโทษจำคุกสูงสุดถึง 30 ปี และปรับสูงสุดถึง 1 ล้านดอลลาร์สหรัฐ ขึ้นอยู่กับความร้ายแรงของอาชญากรรม โดยในสหรัฐฯ การกระทำที่เข้าข่ายเป็น “ภัยทางการเงินออนไลน์” มักถูกตีความว่าเป็น

การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบหรือหลอกลวงผ่านเครือข่ายอิเล็กทรอนิกส์ อันก่อให้เกิดความเสียหายทางการเงิน ซึ่งกฎหมายหลักที่เกี่ยวข้องคือ Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 ที่กำหนดโทษสำหรับผู้ที่เข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือกระทำการเกินกว่าที่ได้รับอนุญาตเพื่อจุดประสงค์ในการฉ้อโกง การลักลอบข้อมูล หรือการก่อให้เกิดความเสียหายต่อทรัพย์สินและข้อมูล อีกทั้ง Wire Fraud (18 U.S.C. § 1343) ยังเกี่ยวข้องโดยตรงกับการหลอกลวงผ่านช่องทางสื่อสารอิเล็กทรอนิกส์ ซึ่งรวมถึงการโกงออนไลน์เกี่ยวกับธุรกรรมทางการเงิน (United States Code., 2012)

สหราชอาณาจักร ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking หมายถึงการใช้เทคโนโลยีดิจิทัลเพื่อหลอกลวงหรือขโมยข้อมูลส่วนบุคคลหรือข้อมูลทางการเงิน ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรม เช่น การขโมยข้อมูลประจำตัว การหลอกลวงทางอีเมล และการหลอกลวงผ่านเว็บไซต์ปลอม โดยในสหราชอาณาจักร “ภัยทางการเงินออนไลน์” โดยทั่วไปจะเกี่ยวข้องกับการหลอกลวงผ่านระบบคอมพิวเตอร์หรือเครือข่ายอินเทอร์เน็ต ทำให้เหยื่อสูญเสียเงินหรือทรัพย์สิน โดยกฎหมายสำคัญคือ Fraud Act 2006 ซึ่งกำหนดนิยามของการทุจริต (fraud) ผ่านการแสดงข้อความอันเป็นเท็จ หรือการละเว้นข้อมูลที่จำเป็น (มาตรา 2) เพื่อให้ได้มาซึ่งประโยชน์ทางการเงิน นอกจากนี้ Computer Misuse Act 1990 กำหนดบทลงโทษแก่การเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือเพื่อประโยชน์ทางการเงินอย่างมิชอบ รวมถึงการสร้างหรือเผยแพร่ข้อมูลที่ใช้ในการเจาะระบบ (Legislation.gov.uk., 2006)

ออสเตรเลีย ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking หมายถึงการใช้เทคโนโลยีดิจิทัลเพื่อหลอกลวงหรือขโมยข้อมูลส่วนบุคคลหรือข้อมูลทางการเงิน การฉ้อโกงประเภทนี้มีหลายรูปแบบ เช่น การขโมยข้อมูลประจำตัว การหลอกลวงทางอีเมล และการหลอกลวงผ่านเว็บไซต์ปลอม โดยในออสเตรเลีย ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking มักถูกจัดอยู่ในกลุ่มการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือการฉ้อโกงทางไซเบอร์ ซึ่งอาศัยเทคโนโลยีในการหลอกลวงหรือเจาะระบบเพื่อแสวงหาผลประโยชน์ทางการเงิน กฎหมายหลักที่เกี่ยวข้องคือ Criminal Code Act 1995 (Cth) โดยเฉพาะใน Division 477 และ 478 ซึ่งกล่าวถึงการเข้าถึง แก้ไข หรือก่อให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต เพื่อจุดประสงค์ในการฉ้อโกงหรือก่ออาชญากรรมทางทรัพย์สิน นอกจากนี้ ยังกำหนดโทษผู้ที่กระทำการหลอกลวงผ่านเครือข่ายอิเล็กทรอนิกส์เพื่อนำข้อมูลทางการเงิน หรือเงินทุนจากผู้อื่นโดยมิชอบ (Federal Register of Legislation., 1995)

สิงคโปร์ ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking หมายถึงการใช้เทคโนโลยีดิจิทัลเพื่อหลอกลวงหรือขโมยข้อมูลส่วนบุคคลหรือข้อมูลทางการเงิน การฉ้อโกงประเภทนี้มีหลายรูปแบบ เช่น การขโมยข้อมูลประจำตัว การหลอกลวงทางอีเมล และการหลอกลวงผ่านเว็บไซต์ปลอม โดยในสิงคโปร์ การกระทำที่เข้าข่ายภัยทางการเงินออนไลน์ ได้แก่ การใช้งานหรือเข้าถึงระบบคอมพิวเตอร์โดยมิชอบเพื่อผลประโยชน์ทางการเงิน การหลอกลวงออนไลน์ หรือการเผยแพร่ข้อมูลเท็จเพื่อขโมยข้อมูลบัตรเครดิตหรือข้อมูลทางการเงิน กฎหมายสำคัญคือ Computer Misuse Act 1993

(เดิมชื่อ Computer Misuse and Cybersecurity Act) โดยเฉพาะมาตรา 3 ที่บัญญัติถึงการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต รวมถึงการกระทำใด ๆ เพื่อให้ได้มาซึ่งข้อมูลหรือเงินโดยมิชอบ โดยผู้ฝ่าฝืนอาจได้รับโทษปรับหรือจำคุก ทั้งนี้ยังกำหนดโทษกรณีเผยแพร่โปรแกรมที่มุ่งโจมตีความปลอดภัยทางไซเบอร์ (Attorney-General's Chambers., 2020)

<u>อินเดีย</u> ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking หมายถึงการกระทำใด ๆ ที่ใช้ระบบคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ในการหลอกลวง ขโมย หรือเปลี่ยนแปลงข้อมูลทางการเงินของบุคคลหรือองค์กรโดยมิชอบ ก่อให้เกิดความเสียหายต่อทรัพย์สินหรือข้อมูลที่มีมูลค่า ซึ่งกฎหมายที่เกี่ยวข้องคือ The Information Technology Act, 2000 (แก้ไขเพิ่มเติม) โดยมาตรา 66C กล่าวถึงการขโมยอัตลักษณ์ (identity theft) เช่น การนำข้อมูลส่วนบุคคลหรือข้อมูลทางการเงินไปใช้โดยไม่ได้รับอนุญาต ส่วนมาตรา 66D ว่าด้วยการโกงโดยใช้ทรัพยากรทางคอมพิวเตอร์ (cheating by personation) ซึ่งครอบคลุมการหลอกลวงและฉ้อโกงทางออนไลน์ รวมถึงการฉ้อฉลเกี่ยวกับบัญชีหรือข้อมูลทางการเงิน (Government of India., 2000)

<u>ฟิลิปปินส์</u> ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking ครอบคลุมการกระทำที่มีเป้าหมายทำให้เกิดความเสียหายแก่บุคคลหรือองค์กรในด้านการเงิน ผ่านวิธีการเจาะระบบคอมพิวเตอร์ การปลอมแปลงข้อมูล หรือการหลอกลวงทางไซเบอร์ กฎหมายที่เกี่ยวข้องหลัก ๆ คือ Republic Act No. 10175: Cybercrime Prevention Act of 2012 โดยเฉพาะในมาตรา 4 (Section 4) ที่ระบุถึง "Computer-related Offenses" เช่น การฉ้อโกง (fraud) การปลอมแปลง (forgery) และการโจรกรรมข้อมูล (identity theft) เพื่อผลประโยชน์ทางการเงิน การกระทำดังกล่าวอาจถูกลงโทษทางอาญาหากพบว่าก่อให้เกิดความเสียหายต่อทรัพย์สินหรือข้อมูลอิเล็กทรอนิกส์โดยมิชอบ (Republic of the Philippines., 2012)

อาจกล่าวโดยสรุปได้ว่า ทุกประเทศมีจุดร่วมที่นิยามความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking ว่าเป็นการกระทำที่มีเจตนาหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลสำคัญหรือทรัพย์สิน เช่น รหัสผ่าน ข้อมูลบัตรเครดิต หรือเงินสด ทั้งนี้การกระทำดังกล่าวมักใช้เทคโนโลยีดิจิทัลหรือแพลตฟอร์มออนไลน์เป็นเครื่องมือ เช่น สหรัฐฯ เน้นการขโมยข้อมูลส่วนบุคคลผ่านการหลอกลวง (identity theft) ขณะที่สหราชอาณาจักร เน้นการหลอกลวงผ่านธุรกรรมทางการเงิน (payment fraud) รวมถึงการมุ่งเน้นการใช้เทคโนโลยีเป็นเครื่องมือ เป็นต้น

นอกจากนี้ ยังรวมถึงการนิยามที่เกี่ยวข้องกับการใช้เทคโนโลยี เช่น การโจมตีด้วยมัลแวร์ การหลอกลวงผ่านฟิชชิง หรือการใช้วิธีการอื่นผ่านช่องทางออนไลน์ เช่น อีเมล โซเชียลมีเดีย หรือเว็บไซต์ปลอม ที่ส่งผลกระทบต่อบุคคลและองค์กร โดยทุกนิยามต่างยอมรับว่าผลกระทบไม่ได้จำกัดเฉพาะบุคคล แต่ยังส่งผลต่อองค์กรทางการเงิน เช่น ธนาคาร และธุรกิจที่เกี่ยวข้อง เนื่องจากมีการจารกรรมข้อมูลบัญชีและทำให้ระบบทางการเงินเสียหาย โดยนิยามในแต่ละประเทศสะท้อนถึงความซับซ้อนของเทคโนโลยีที่ใช้และลักษณะพฤติกรรมมิจฉาชีพในบริบทที่แตกต่างกัน การกำหนดนิยามในประเทศพัฒนาแล้วมักครอบคลุม

ถึงการใช้เทคโนโลยีขั้นสูงและการปกป้องข้อมูลส่วนบุคคล ในขณะที่นิยามในประเทศกำลังพัฒนามุ่งเน้นการจัดการกับภัยที่เกิดขึ้นจากพฤติกรรมการใช้งานทั่วไป เช่น การหลอกลวงผ่านบัญชีม้าและโซเชียลมีเดีย โดยทุกประเทศต่างมีเป้าหมายเดียวกันคือการป้องกันและลดความเสี่ยงที่เกิดจากภัยทางการเงินออนไลน์อย่างมีประสิทธิภาพ ซึ่งหากพิจารณาถึงจุดร่วมที่สะท้อนถึงบริบทเฉพาะของแต่ละประเทศทั้ง ในแง่ความเหมือน เช่น ภัยนี้มักถูกนิยามให้เกี่ยวข้องกับความเสียหายทางการเงิน การใช้เทคโนโลยีเป็นเครื่องมือ เช่น ฟิชชิง (Phishing) มัลแวร์ (Malware) และการเข้าถึงข้อมูลส่วนบุคคล เช่น รหัสผ่านหรือข้อมูลธนาคาร และในด้านความแตกต่างในประเทศพัฒนาแล้ว เช่น สหรัฐอเมริกาและสหราชอาณาจักร นิยามภัยนี้โดยมีรายละเอียดเชิงลึกในกฎหมายเฉพาะ เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคลและไซเบอร์ ในขณะที่ประเทศกำลังพัฒนา เช่น อินเดียและฟิลิปปินส์ อาจนิยามในลักษณะที่ครอบคลุมทั่วไปมากกว่า ในประเทศที่มีการใช้เทคโนโลยีขั้นสูง เช่น ญี่ปุ่นและเกาหลีใต้ มีการนำปัญญาประดิษฐ์ (AI) มาใช้ในหลายภาคส่วน (Kawase, 2024) รวมถึงการทหารและบริการสาธารณะ (Lee, 2024) อย่างไรก็ตาม ไม่พบข้อมูลที่ระบุถึงการใช้ AI โดยมิจฉาชีพในประเทศเหล่านี้โดยเฉพาะ ในขณะเดียวกัน ประเทศที่มีโครงสร้างเทคโนโลยีพื้นฐานน้อยกว่า เช่น อินโดนีเซีย พบว่ามีการใช้ AI ในการสร้างข่าวปลอมเพื่อก่อกวนการเลือกตั้ง และมีการล่อลวงผ่านโซเชียลมีเดีย ทั้งนี้ นิยามของภัยทางการเงินออนไลน์นั้นมีเป้าหมายร่วมกันในการป้องกันความเสียหาย แต่ลักษณะเฉพาะทางกฎหมายและเศรษฐกิจในแต่ละประเทศส่งผลต่อวิธีการนิยามและมาตรการป้องกันที่แตกต่างกันอย่างชัดเจน

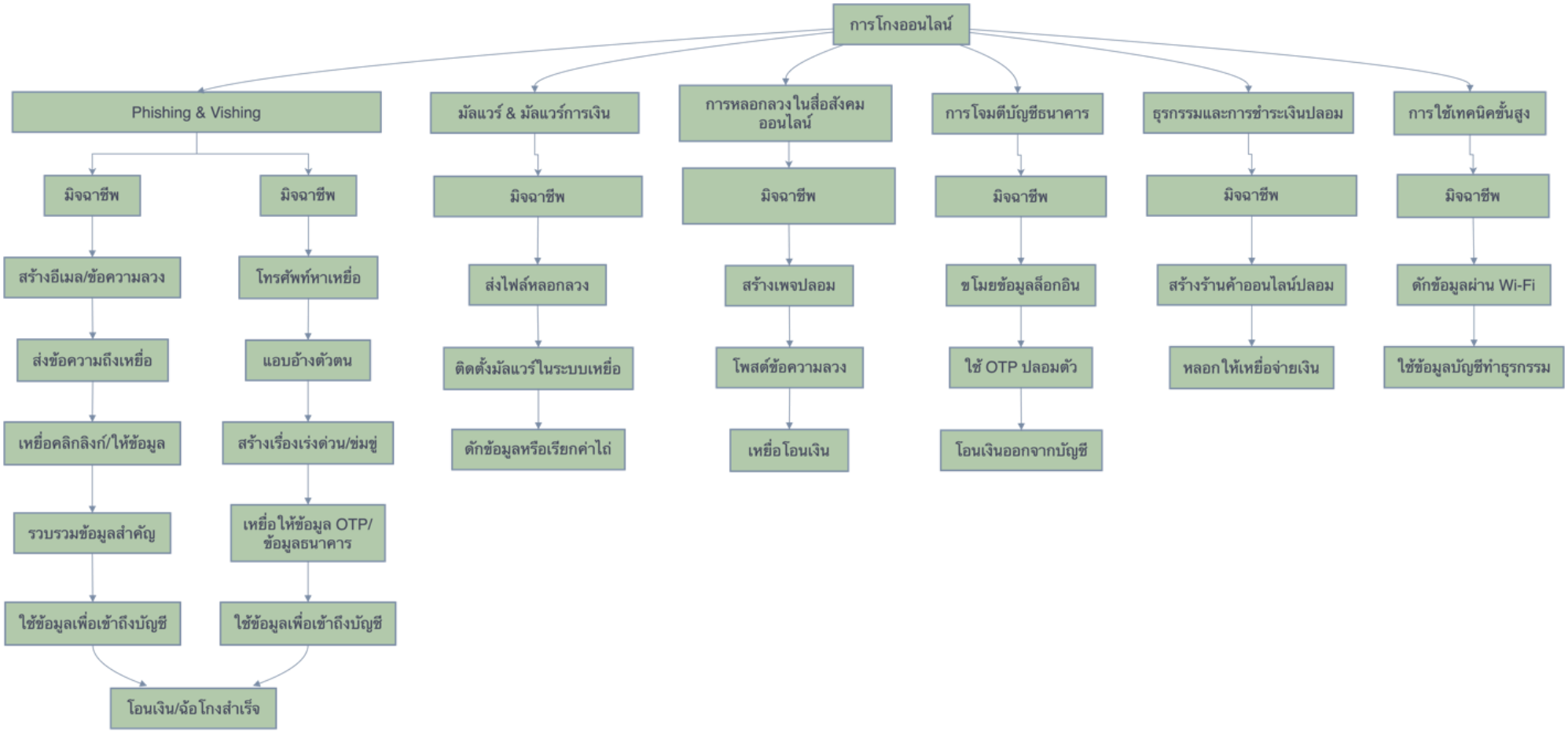
สำหรับรูปแบบภัยทางการเงินออนไลน์ อาจแบ่งออกเป็นหมวดหมู่ที่เชื่อมโยงถึงวิธีการและเป้าหมายที่เกี่ยวข้องได้ 6 หมวดหมู่หลัก ดังนี้

1) **การหลอกลวงทางอิเล็กทรอนิกส์และโทรศัพท์** (Phishing & Vishing) คือ การสร้างอีเมลหรือข้อความลวงเพื่อหลอกให้เหยื่อคลิกลิงก์หรือกรอกข้อมูลสำคัญ เช่น รหัสผ่านหรือข้อมูลบัญชีธนาคาร (Microsoft, 2024) (NT cyfence, 2019) ขณะที่ วิชชิง คือ การโทรศัพท์หาเหยื่อโดยอ้างตัวตนปลอม หรือแก๊งคอลเซ็นเตอร์ เช่น ปลอมเป็นเจ้าหน้าที่ธนาคาร และใช้คำพูดเพื่อข่มขู่หรือสร้างสถานการณ์เร่งด่วนเพื่อหลอกให้เหยื่อให้ข้อมูล OTP หรือข้อมูลทางการเงิน (iT24Hrs, 2567)
2) **มัลแวร์** (Mulware) คือ การส่งไฟล์หลอกลวงที่มีมัลแวร์ฝังไว้ เมื่อเหยื่อเปิดไฟล์ มิจฉาชีพสามารถติดตั้งมัลแวร์ในระบบคอมพิวเตอร์ของเหยื่อได้ และทำให้เกิดข้อมูลสำคัญถูกดักจับ หรือระบบถูกล็อกและเรียกค่าไถ่ (ransomware) (Microsoft, 2024)
3) **การหลอกลวงในสื่อสังคมออนไลน์** (Social Media Fraud) คือ การสร้างเพจปลอมหรือโพสต์ข้อความลวงในสื่อสังคมออนไลน์ เช่น facebook หรือ instagram และหลอกให้เหยื่อโอนเงินโดยมิจฉาชีพอาจแสดงสินค้า/บริการปลอม หรือสร้างเรื่องราวเพื่อดึงดูดความสนใจ (Phansuathong, 2023)

4) **การโจมตีบัญชีธนาคาร** (Bank Account Hacking) คือการใช้ข้อมูลล็อกอินที่ได้จากการแอบอ้างหรือดักข้อมูล เพื่อล็อกอินบัญชีเหยื่อ และอาจมีวิธีการเพิ่มเติม โดยใช้ OTP ปลอมเพื่อยืนยันตัวตนและโอนเงินออกจากบัญชี (NT cyfence, 2019)
5) **ธุรกรรมและการชำระเงินปลอม** (Fraudulent Payments) คือ การสร้างร้านค้าออนไลน์ปลอม หรือหลอกให้เหยื่อจ่ายเงินโดยไม่มีสินค้าหรือบริการจริง วิธีนี้นิยมใช้ในตลาดออนไลน์หรือโซเชียลมีเดีย (NT cyfence, 2019)
6) **การใช้เทคนิคขั้นสูง** (Advanced Persistent Threats) เช่น การดักจับข้อมูลผ่าน Wi-Fi สาธารณะ โดยนำข้อมูลที่ได้ทำธุรกรรมหรือแอบอ้างตัวตนของเหยื่อในระบบต่าง ๆ (Anti-Fake News Center Thailand , 2022)

ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking ข้างต้นทั้งหมดนี้ จะมี *“บัญชีม้า”* (money mule accounts) ทำหน้าที่เป็นตัวกลางในการรับโอนเงินที่ได้จากการหลอกลวง และกระจายเงินไปยังบัญชีปลายทางเพื่อปกปิดตัวตน การใช้บัญชีม้าทำให้การติดตามธุรกรรมผิดกฎหมายทำได้ยาก เนื่องจากเงินมักถูกโอนผ่านหลายบัญชีและมีปลายทางอยู่ในต่างประเทศ แนวทางแก้ไขปัญหาบัญชีม้าที่พบในปัจจุบัน อาทิ การตรวจสอบและปิดบัญชีที่เกี่ยวข้อง การพัฒนาระบบตรวจจับธุรกรรมผิดปกติ และสร้างความตระหนักให้ประชาชนเกี่ยวกับการเปิดบัญชีม้า ซึ่งเป็นการช่วยลดเครือข่ายการโกงและเพิ่มโอกาสในการติดตามผู้กระทำผิด

แผนภาพที่ 1 ประเภทและรูปแบบของภัยทางการเงินออนไลน์



ที่มา: จากการรวบรวมของคณะวิจัย

2.1.2 ข้อมูลสถิติภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์สามารถเกิดขึ้นได้หลากหลายรูปแบบ โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ[2] (Thailand Computer Emergency Response Team: ThaiCERT) รายงานสถิติรูปแบบของการโจมตีทางไซเบอร์สูงสุด 10 อันดับ (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ , ม.ป.ป.) ดังตารางที่ 1

ตารางที่ 1 สถิติภัยคุกคามทางไซเบอร์ ตุลาคม พ.ศ. 2564 - ธันวาคม พ.ศ. 2566

หน่วย: จำนวนครั้ง

รูปแบบภัยคุกคาม	นิยาม	2564	2565	2566	รวม
Hacked Website (Gambling)	เว็บไซต์ที่ถูกแฮ็กและเปลี่ยนแปลงเนื้อหาให้เชื่อมโยงหรือโฆษณาเกี่ยวกับการพนันออนไลน์โดยไม่ได้รับอนุญาต	0	257	515	772
Hacked Website (Defacement)	เว็บไซต์ที่ถูกแฮ็กและเปลี่ยนแปลงหน้าเว็บไซต์ไปยังเว็บไซต์ของมิจฉาชีพ	8	287	336	631
Fake Website	การสร้างเว็บไซต์ปลอมที่เลียนแบบเว็บไซต์ทางการขององค์กรต่าง ๆ เพื่อโจรกรรมข้อมูลของผู้ที่หลงเชื่อเข้าไปใช้งาน	1	45	301	347
Vulnerability	การโจมตีระบบผ่านจุดอ่อนที่มีระบบการรักษาความปลอดภัยที่ไม่เข้มงวด (SkySoft, 2022)	19	75	228	322
Finance scam (เป้าหมายหลักของงานวิจัยนี้)	**การหลอกหลวงทางการเงินผ่านระบบอินเทอร์เน็ต** (ETDA, 2561)	0	0	112	112
Data Breach	การเจาะระบบและขโมยข้อมูล ทั้งข้อมูลส่วนบุคคลและข้อมูลในระดับองค์กร เพื่อนำข้อมูลไปขาย หรือขโมยความลับทางการค้า	11	44	47	102
Data leak	การรั่วไหลของข้อมูลสำคัญไปยังองค์กรหรือบุคคลภายนอก โดยมีสาเหตุหลายประการ เช่น ความผิดพลาดของบุคลากร ความอ่อนแอของซอฟต์แวร์ และการมีระบบรักษาความปลอดภัยของข้อมูลที่ไม่เข้มงวด (proofpoint, n.d.)	0	0	100	100
Hacked Website (Phishing)	การโจมตีโดยที่มิจฉาชีพจะปลอมตัวเป็นองค์กรที่น่าเชื่อถือ จากนั้นจะหลอกล่อเหยื่อผ่านการส่งลิงก์ที่เป็นอันตรายผ่านอีเมลหรือข้อความ เพื่อโจมตีระบบของผู้ใช้งาน (imperva, n.d.)	5	44	38	87

[2] ThaiCERT หน่วยงานภายใต้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ถูกจัดตั้งขึ้นโดยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อวัตถุประสงค์เฝ้าระวังความเสี่ยง ติดตาม วิเคราะห์ และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์

รูปแบบภัยคุกคาม	นิยาม	2564	2565	2566	รวม
Ransomware	การเข้ารหัสหรือจำกัดการเข้าถึงไฟล์บนคอมพิวเตอร์ จากนั้นมิจฉาชีพดำเนินการส่งข้อความหาเหยื่อ เพื่อเรียกค่าไถ่ เช่น ไฟล์ของคุณถูกเข้ารหัส ถ้าอยากได้ไฟล์คืนต้องโอนเงินมาให้เรา (Trend Micro, n.d.)	4	24	27	55
DDos	การโจมตีระบบเครือข่ายคอมพิวเตอร์ ผ่านการส่งข้อมูลจำนวนมหาศาลเข้าโจมตี จนส่งผลให้ไม่สามารถใช้บริการหรือใช้งานได้	0	4	33	37

หมายเหตุ: ThaiCERT เปิดเผยข้อมูลสถิติภัยคุกคามทางไซเบอร์ตั้งแต่ เดือนตุลาคม พ.ศ. 2564 จนถึงเดือนธันวาคม พ.ศ. 2566

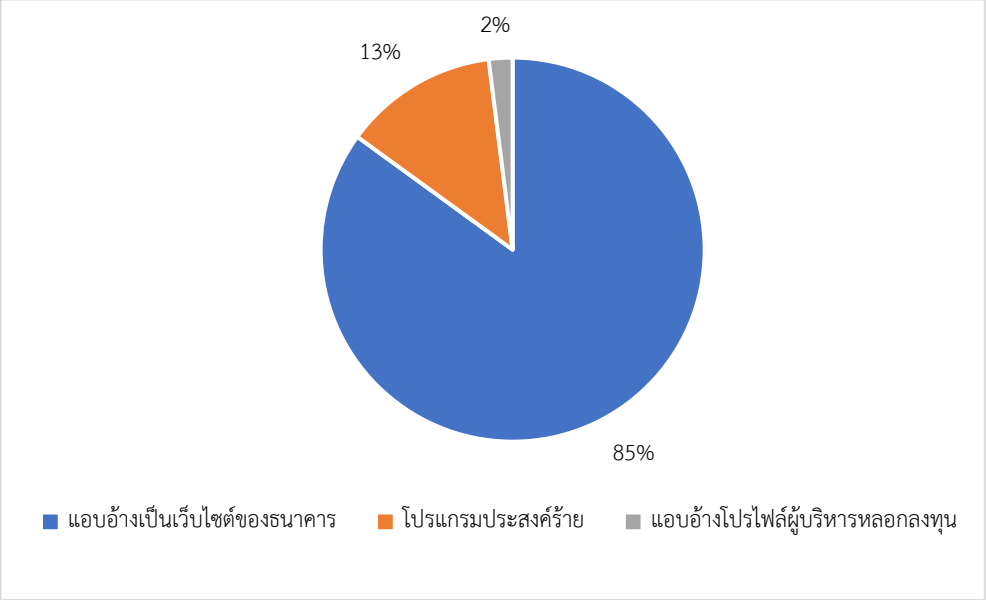
จากตารางที่ 1 จะเห็นได้ว่าภัยคุกคามทางไซเบอร์เกือบทุกรูปแบบมีแนวโน้มเพิ่มขึ้นตลอดช่วง 3 ปีที่ผ่านมา ซึ่งรวมถึงภัยทางการเงินออนไลน์ โดยเฉพาะอย่างยิ่งการหลอกลวงทางการเงินผ่านระบบอินเทอร์เน็ต (finance scam) ซึ่งแม้จะมีการเก็บข้อมูลการหลอกลวงรูปแบบนี้เป็นปีแรก แต่สถิติการเกิดเหตุการณ์กลับขึ้นมาอยู่ในอันดับที่ 5 ของภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในประเทศไทย

และเมื่อพิจารณาเฉพาะรูปแบบภัยทางการเงินออนไลน์ ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (Thailand Banking Sector Computer Emergency Response Team: TB-CERT) รายงานว่า ในปี พ.ศ. 2566 TB-CERT ได้รับแจ้งเหตุการณ์หลอกลวงทางไซเบอร์ 3 รูปแบบหลัก ได้แก่

1) การแอบอ้างเป็นเว็บไซต์ของธนาคาร: มิจฉาชีพดำเนินการปลอมแปลงและแอบอ้างเป็นเว็บไซต์ของธนาคารและดำเนินการปล่อยกู้สินเชื่อ โดยลักษณะของการดำเนินการมิจฉาชีพสร้างเว็บไซต์และใช้ตราสัญลักษณ์จริงของธนาคาร จากนั้นดำเนินการขอข้อมูลส่วนตัวของเหยื่อ เช่น เลขบัตรประจำตัวประชาชน และเบอร์โทรศัพท์ เป็นต้น
2) การใช้โปรแกรมประสงค์ร้าย: มิจฉาชีพดำเนินการปลอมแปลงแอปพลิเคชันของธนาคารเพื่อหลอกให้เหยื่อหลงเชื่อและติดตั้งแอปพลิเคชันดังกล่าว จากนั้นมิจฉาชีพจะดำเนินการดักจับอุปกรณ์ โดยเฉพาะการดักจับ PIN สำหรับการเข้าใช้งาน mobile banking เพื่อดูดเงินออกจากบัญชีของเหยื่อจากการควบคุมระยะไกล
3) การแอบอ้างโปรไฟล์ของผู้บริหาร: มิจฉาชีพดำเนินการสร้างเพจ และแอบอ้างใช้โปรไฟล์ของผู้บริหารธนาคาร เพื่อสร้างความน่าเชื่อในการลงทุนให้แก่ผู้หลงเชื่อ โดยลักษณะของการประชาสัมพันธ์มักเป็นไปในแนวทางการชักชวนมาร่วมลงทุนที่ได้รับผลตอบแทนดี

ทั้งนี้ จากสถิติพบว่า รูปแบบการหลอกลวงโดยการแอบอ้างเป็นเว็บไซต์ของธนาคารมีจำนวนมากที่สุด คิดเป็นร้อยละ 85 รองลงมาคือการใช้โปรแกรมประสงค์ร้าย คิดเป็นร้อยละ 13 และการแอบอ้างโปรไฟล์ผู้บริหาร คิดเป็นร้อยละ 2 (ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร, 2566) ดังแสดงในแผนภาพที่ 2

แผนภาพที่ 2 รูปแบบการหลอกลวงทางไซเบอร์ภาคการธนาคารประจำปี พ.ศ. 2566



ที่มา: รายงานประจำปี TB-CERT พ.ศ. 2566

แม้ว่าภัยโจมตีทางไซเบอร์ในรูปแบบการใช้โปรแกรมประสงค์ร้ายมีสัดส่วนของเหตุการณ์การโจมตีอยู่ในอันดับที่ 2 อย่างไรก็ตาม ความเสียหายที่เกิดขึ้นต่อประชาชนผู้ถูกหลอกลวง จากกรณีการโจมตีทางไซเบอร์ผ่านการหลอกให้ติดตั้งแอปพลิเคชันเพื่อขโมยเงินหรือที่เรียกว่าแอปดูดเงิน (mobile banking trojan) คิดเป็นมูลค่ากว่า 2.6 พันล้านบาท (สถิติระหว่างวันที่ 1 มีนาคม 2565 ถึงวันที่ 31 พฤษภาคม 2567) (MRG ONLINE, 2567) ซึ่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้จัดภัยคุกคามดังกล่าวเป็นภัยทางไซเบอร์ระดับร้ายแรง (ไทยโพสต์, 2567)

- *ข้อมูลสถิติระบบเทคโนโลยีสารสนเทศขัดข้องที่กระทบต่อการให้บริการสำคัญของธนาคารพาณิชย์*

ธนาคารแห่งประเทศไทย (ธปท.) กำหนดให้ธนาคารพาณิชย์ที่ดำเนินการให้บริการทางการเงินแก่ลูกค้ารายย่อยผ่านช่องทาง mobile banking ต้องรายงานข้อมูลสถิติระบบเทคโนโลยีสารสนเทศขัดข้องจากการให้บริการทางการเงินผ่านช่องทางดังกล่าว (รายละเอียดของข้อกำหนดคณะวิจัยกล่าวถึงในส่วนที่ 2.3.1)[3]

[3] ธปท. กำหนดให้สถาบันการเงินที่มีการให้บริการทางการเงินผ่าน mobile banking application ต้องกำกับดูแลให้ระบบปฏิบัติงานหยุดชะงักไม่เกิน 8 ชั่วโมง ในรอบ 1 ปีปฏิทิน (ธปท., 2566)

ทั้งนี้ จากข้อมูลพบว่า ในระยะเวลา 15 เดือน (ไตรมาส 1 พ.ศ. 2566 – ไตรมาส 1 พ.ศ. 2567) ธนาคารพาณิชย์ที่มีสถิติจำนวนเหตุการณ์ระบบ Mobile banking ขัดข้องมากที่สุด 3 อันดับ ได้แก่ ธนาคารไทยพาณิชย์ (6 ครั้ง) ธนาคารกรุงเทพ (5 ครั้ง) และธนาคารทหารไทยธนชาต (5 ครั้ง) (ธปท., ม.ป.ป.) โดยมีรายละเอียดดังแสดงในตารางที่ 2

ตารางที่ 2 สถิติระบบ Mobile banking ธนาคารพาณิชย์ขัดข้อง
(ไตรมาส 1 พ.ศ. 2566 – ไตรมาส พ.ศ. 2567)

หน่วย: จำนวนครั้ง/ระยะเวลาการเกิดเหตุการณ์

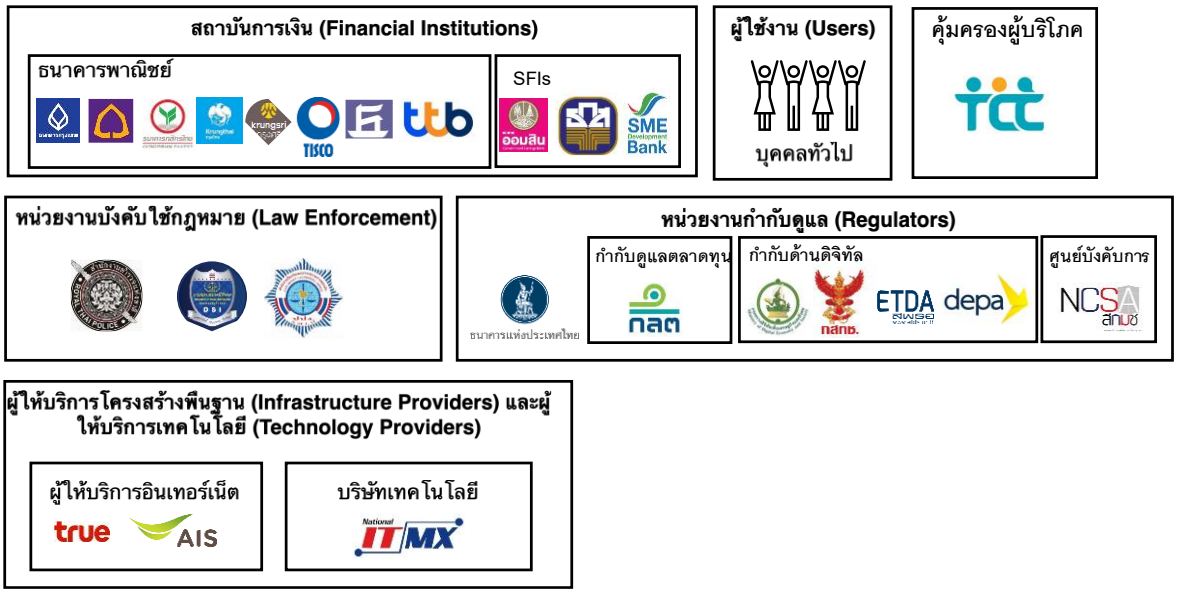
ธนาคาร	พ.ศ. 2566				พ.ศ. 2567	รวม (จำนวนครั้ง)
	ไตรมาส 1	ไตรมาส 2	ไตรมาส 3	ไตรมาส 4	ไตรมาส 1	
ธ.กรุงเทพ	1 ครั้ง/<1ชม.	2 ครั้ง/5 ชม.	1 ครั้ง/<1 ชม.		1 ครั้ง/<1 ชม.	5
ธ.กรุงไทย	1 ครั้ง/2 ชม.	1 ครั้ง/1 ชม.				2
ธ.กรุงศรีอยุธยา		1 ครั้ง/2 ชม.				1
ธ.กสิกรไทย		1 ครั้ง/2 ชม.				1
ธ.เกียรตินาคินภัทร						0
ธ.ทหารไทยธนชาต		1 ครั้ง/<1 ชม.	1 ครั้ง/2 ชม.	1 ครั้ง/1 ชม.	2 ครั้ง/2 ชม.	5
ธ.ทิสโก้						0
ธ.ไทยพาณิชย์	2 ครั้ง/1 ชม.		2 ครั้ง/1 ชม.	2 ครั้ง/2 ชม.		6

ที่มา: รายงานข้อมูลสถิติระบบเทคโนโลยีสารสนเทศขัดข้องที่กระทบต่อการให้บริการสำคัญของธนาคารพาณิชย์ ธปท.

2.2 หน่วยงาน/องค์กรที่เกี่ยวข้องกับการป้องกันภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงิน

การสร้างความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking มีโครงสร้างที่ซับซ้อน และมีผู้เล่นหลากหลายกลุ่มที่มีบทบาทเฉพาะ ซึ่งล้วนมีความสัมพันธ์ที่เชื่อมโยงกันทั้งในแง่ของการทำงาน การกำกับดูแล และการสร้างมาตรการเพื่อจัดการกับภัยคุกคามที่เกี่ยวข้องกับ ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking โดยสามารถแยกองค์ประกอบของระบบนิเวศได้ ดังนี้

แผนภาพที่ 3 ระบบนิเวศของผู้เล่นและบทบาทที่เกี่ยวข้องในกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking



ที่มา: จากการรวบรวมของคณะวิจัย

1) สถาบันการเงิน (Financial Institutions) ประกอบด้วยธนาคารพาณิชย์ และสถาบันการเงินเฉพาะกิจ (Specialized Financial Institutions : SFIs) มีบทบาทเกี่ยวข้องโดยตรงกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบ mobile banking เนื่องจากเป็นผู้ให้บริการทางการเงินและการทำธุรกรรมต่าง ๆ บนช่องทางออนไลน์ และเป็นช่องทางที่มิจฉาชีพพยายามเข้าถึงข้อมูลสำคัญหรือเพื่อเปิดบัญชีม้า สถาบันการเงินจึงต้องมีแนวทางการดำเนินงานที่คำนึงถึงความปลอดภัยของข้อมูล การบริหารจัดการความเสี่ยงทางการเงินและภัยคุกคามที่อาจเกิดขึ้น ตลอดจนมีส่วนสำคัญในจัดการการฟอกเงินและมิจฉาชีพทางการเงิน

2) หน่วยงานกำกับดูแล มีบทบาทในการจัดทำนโยบาย หรือแนวปฏิบัติที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ รวมถึงการกำกับดูแลให้หน่วยงานที่เกี่ยวข้องดำเนินการตามนโยบาย หรือแนวปฏิบัติที่ได้จัดทำขึ้น โดยมีเป้าหมายร่วมกัน คือ การสร้างความปลอดภัย ความน่าเชื่อถือ และความโปร่งใสในระบบ Mobile Banking และธุรกรรมดิจิทัล การกำกับดูแลและสร้างมาตรการเพื่อป้องกันการฉ้อโกง รวมถึงสนับสนุนการปฏิบัติงานของผู้เล่นรายอื่นในระบบนิเวศ ทั้งนี้ หน่วยงานกำกับดูแลในขอบเขตงานวิจัยนี้ ประกอบด้วย

- ธนาคารแห่งประเทศไทย (ธปท.)
- สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)
- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศส.)
- คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.)
- สำนักงานส่งเสริมเศรษฐกิจดิจิทัล (สศด. หรือ depa)

- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ. หรือ ETDA)
- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และศูนย์รักษาความมั่นคงปลอดภัยไซเบอร์

3) หน่วยงานบังคับใช้กฎหมาย มีบทบาทในการดำเนินคดีกับผู้กระทำผิดที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์ เช่น การใช้บัญชีม้า การฟอกเงิน และการโจมตีทางไซเบอร์ โดยหน้าที่หลักของหน่วยงานกลุ่มนี้ คือ การสืบสวนและดำเนินการทางกฎหมาย เช่น การตรวจสอบ/สืบสวนเหตุการณ์ที่เกิดขึ้น การดำเนินการทางกฎหมายต่อผู้กระทำผิด การป้องกันภัยคุกคามทางไซเบอร์ หรือใช้เครื่องมือดิจิทัล เช่น การติดตาม IP Address และการวิเคราะห์ข้อมูลทางไซเบอร์ รวมถึงกระบวนการคืนเงินหรือทรัพย์สินให้กับผู้ที่ได้รับผลกระทบ และส่งเสริมความรู้ให้ประชาชนเพื่อป้องกันตนเองจากภัยออนไลน์ หน่วยงานบังคับใช้กฎหมายในขอบเขตงานวิจัยนี้ ประกอบด้วย

- สำนักงานตำรวจแห่งชาติ (สตช.)
- กรมสอบสวนคดีพิเศษ (Department of Special Investigation : DSI)
- สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.)

4) ผู้ให้บริการโครงสร้างพื้นฐาน (Infrastructure Providers) และผู้ให้บริการเทคโนโลยี (Technology Providers) ประกอบด้วยผู้ให้บริการอินเทอร์เน็ตและผู้ให้บริการคลาวด์ทำหน้าที่สนับสนุนการเชื่อมต่อและจัดเก็บข้อมูลที่ใช้ในระบบการเงินดิจิทัล ซึ่งเป็นรากฐานสำคัญที่ทำให้ระบบ Mobile Banking และธุรกรรมออนไลน์สามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมถึงบริษัทเทคโนโลยีและบริษัทที่พัฒนาโซลูชันด้านความปลอดภัยมีบทบาทในการพัฒนาระบบและเครื่องมือสำหรับการตรวจจับและป้องกันการโกง เช่น การใช้ AI และ Machine Learning เพื่อระบุพฤติกรรมที่น่าสงสัยในธุรกรรมออนไลน์

5) ผู้ใช้งาน (Users) คือ บุคคลทั่วไปและองค์กรธุรกิจที่ใช้บริการทางการเงินดิจิทัล ผู้ใช้งานเป็นกลุ่มที่มีความเสี่ยงต่อการตกเป็นเหยื่อของการโกงออนไลน์ผ่านช่องทางต่าง ๆ นอกจากนี้ มีองค์กรหรือหน่วยงานคุ้มครองผู้บริโภค ซึ่งทำหน้าที่ในการให้คำแนะนำ ให้ความรู้ การรับข้อร้องเรียน และการช่วยเหลือทางกฎหมาย เพื่อป้องกันไม่ให้ผู้บริโภคตกเป็นเหยื่อของมิจฉาชีพ

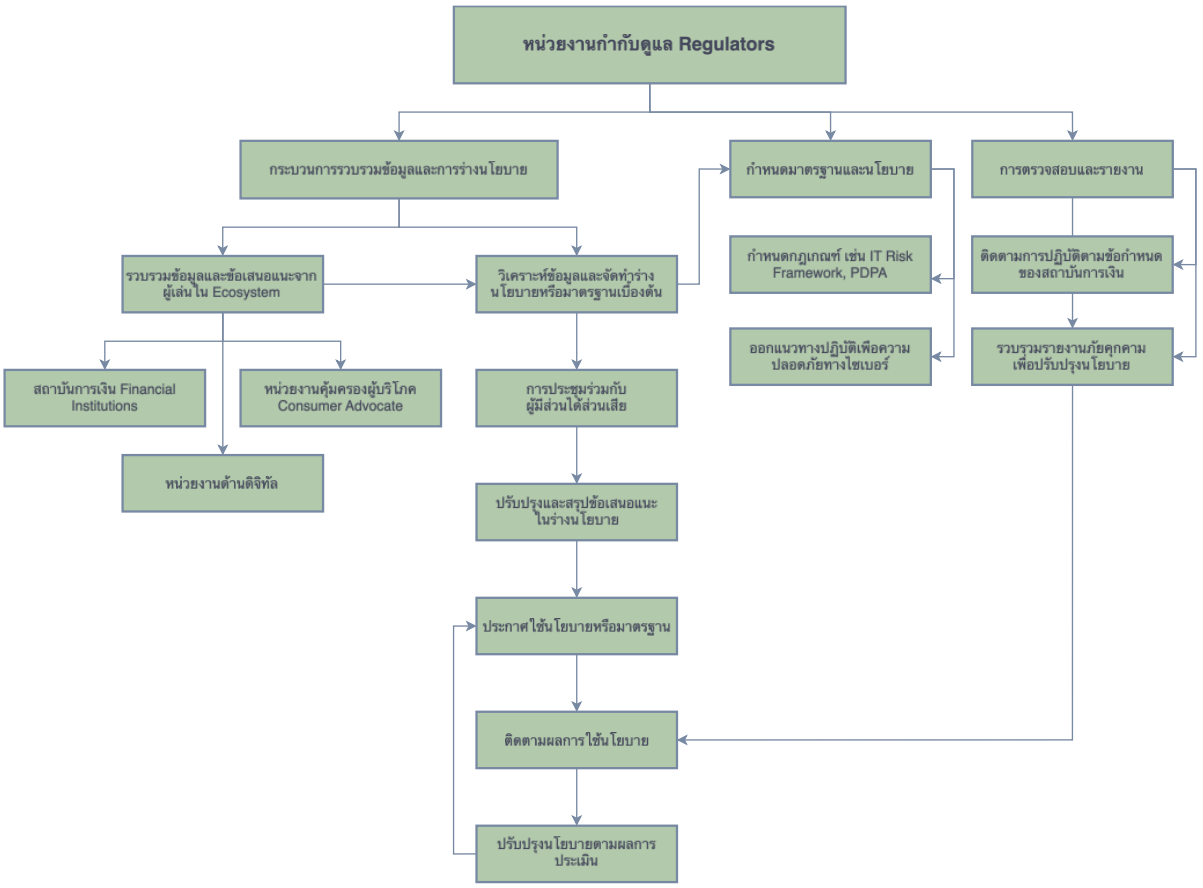
คณะวิจัยได้สรุปบทบาทการทำงานของหน่วยงานหรือองค์กรต่าง ๆ ข้างต้น เพื่อให้เห็นรูปแบบความเชื่อมโยงของการดำเนินการป้องกันภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินทั้งหมด โดยมีรายละเอียด ดังนี้

- *การกำหนดนโยบายและมาตรฐาน*

การกำหนดนโยบายและมาตรฐานเป็นกระบวนการสำคัญที่หน่วยงานกำกับดูแล เช่น ธนาคารแห่งประเทศไทย หรือหน่วยงานที่เกี่ยวข้อง ทำงานร่วมกับสถาบันการเงิน หน่วยงานคุ้มครองผู้บริโภค และผู้เล่นในระบบนิเวศอื่น ๆ เพื่อสร้างแนวปฏิบัติและกฎเกณฑ์ที่ครอบคลุม เช่น IT Risk Framework และ PDPA กระบวนการนี้ครอบคลุมตั้งแต่การรวบรวมข้อมูล วิเคราะห์ความเสี่ยง การประชุมร่วมกับผู้มีส่วนได้ส่วนเสีย

ไปจนถึงการประกาศใช้และติดตามผลนโยบาย ทั้งนี้เพื่อให้มั่นใจว่าสามารถตอบสนองต่อปัญหาความปลอดภัยทางไซเบอร์และลดความเสี่ยงในระบบการเงินได้อย่างมีประสิทธิภาพ

แผนภาพที่ 4 รูปแบบกระบวนการกำหนดนโยบายและมาตรฐาน

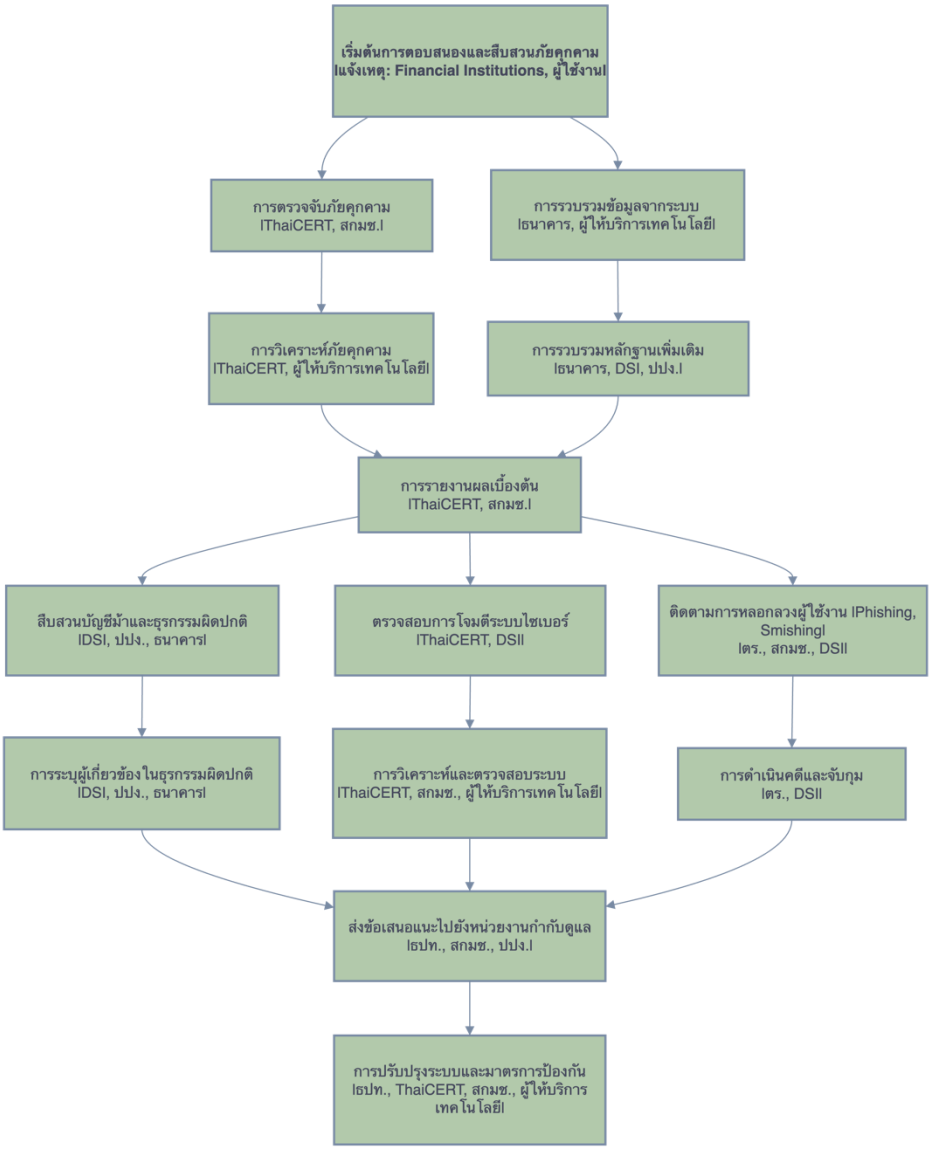


ที่มา: จากการรวบรวมของคณะวิจัย

- *การตอบสนองและสืบสวนภัยคุกคาม*

การตอบสนองและสืบสวนภัยคุกคามเป็นกระบวนการที่ครอบคลุมการตรวจสอบภัยไซเบอร์ การจัดการเหตุการณ์ฉุกเฉิน และการดำเนินการทางกฎหมายเพื่อป้องกันและลดความเสียหาย กระบวนการนี้เกี่ยวข้องกับความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมาย สถาบันการเงิน และหน่วยงานด้านความปลอดภัยทางไซเบอร์ เช่น การสืบสวนบัญชีม้า การตรวจจับการโจมตี และการจับกุมผู้กระทำผิด ความสัมพันธ์เชิงกระบวนการนี้ช่วยสร้างกลไกตอบสนองต่อภัยคุกคามที่รวดเร็วและมีประสิทธิภาพ

แผนภาพที่ 5 รูปแบบกระบวนการการตอบสนองและสืบสวนภัยคุกคาม

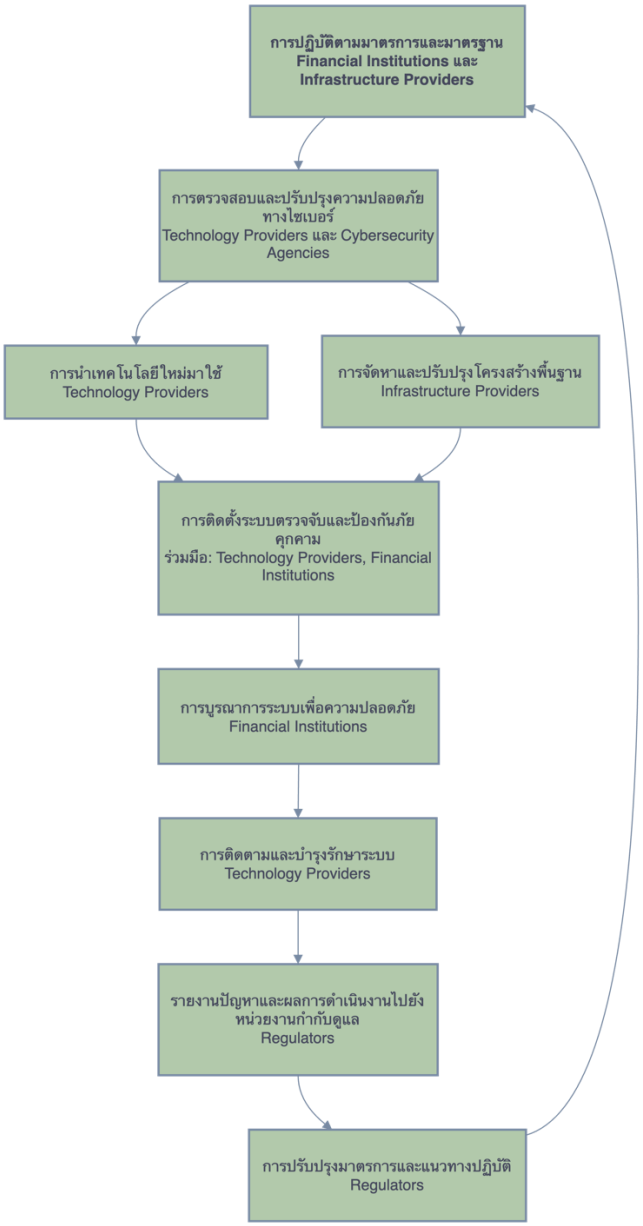


ที่มา: จากจากการรวบรวมของคณะวิจัย

- *การพัฒนาระบบและการปฏิบัติตามมาตรการและมาตรฐาน*

การพัฒนาระบบและโครงสร้างพื้นฐานเกี่ยวข้องกับผู้ให้บริการโครงสร้างพื้นฐานและเทคโนโลยีที่ทำงานร่วมกับสถาบันการเงินเพื่อสร้างระบบที่ปลอดภัยและตอบสนองต่อความต้องการของตลาด เช่น การจัดหาโครงสร้างพื้นฐานด้านอินเทอร์เน็ต การสนับสนุนเทคโนโลยีตรวจจับภัยคุกคาม และการพัฒนาระบบป้องกันข้อมูล การทำงานในส่วนนี้ช่วยให้ระบบการเงินดิจิทัลสามารถดำเนินงานได้อย่างปลอดภัยและมั่นคง ทั้งยังรองรับการเปลี่ยนแปลงด้านเทคโนโลยีและมาตรฐานสากล

แผนภาพที่ 6 รูปแบบกระบวนการพัฒนาระบบและโครงสร้างพื้นฐานด้านความปลอดภัยทางไซเบอร์



ที่มา: จากการรวบรวมของคณะวิจัย

- *การสร้างความตระหนักรู้และการคุ้มครองผู้บริโภค*

การสร้างความตระหนักรู้และการคุ้มครองผู้บริโภคเป็นส่วนสำคัญที่ช่วยเสริมสร้างความมั่นใจให้แก่ผู้ใช้งานระบบการเงินดิจิทัล โดยหน่วยงานคุ้มครองผู้บริโภคและผู้เล่นในระบบนิเวศ เช่น ธนาคารและผู้ให้บริการเทคโนโลยี ทำงานร่วมกันเพื่อให้ความรู้เกี่ยวกับภัยไซเบอร์ เช่น การป้องกันการหลอกลวงออนไลน์ รวมถึงการสร้างมาตรการที่ชัดเจนสำหรับการรับเรื่องร้องเรียนและการเยียวยาความเสียหาย กระบวนการนี้ช่วยลดความเสี่ยงและเพิ่มความปลอดภัยให้แก่ผู้ใช้งานในระบบการเงิน อาทิ

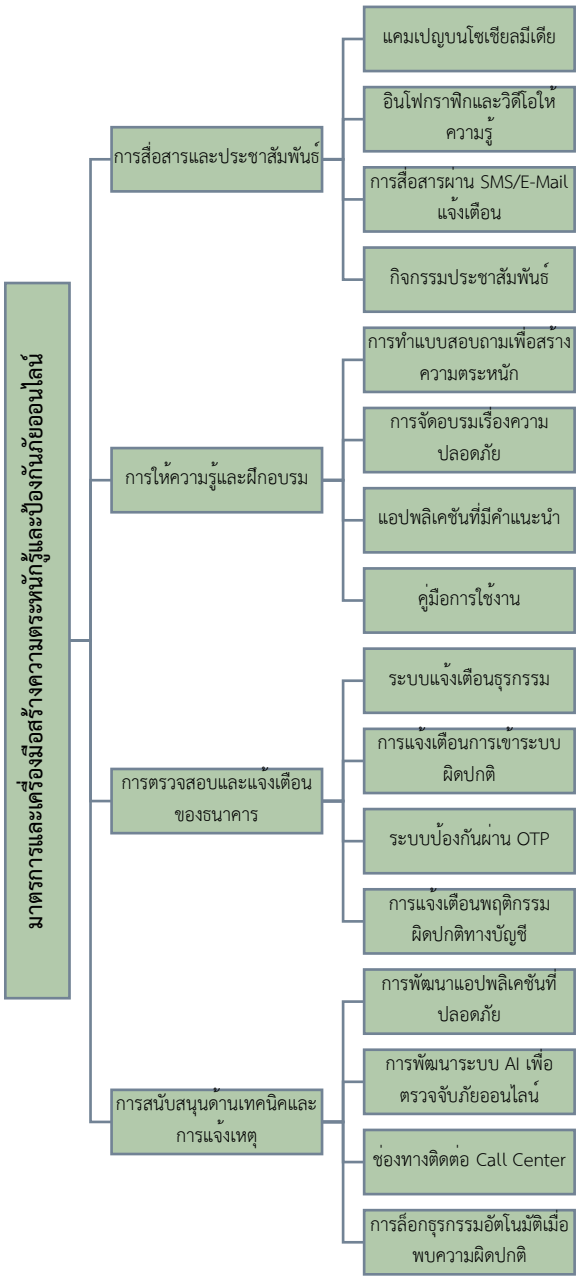
(1) การสื่อสารและประชาสัมพันธ์ ที่มุ่งเน้นการเผยแพร่ข้อมูลและสร้างความตระหนักรู้ผ่านช่องทางที่ผู้บริโภคเข้าถึงได้ง่าย เช่น การจัดแคมเปญผ่านสื่อสังคมออนไลน์ การผลิตอินโฟกราฟิกและวิดีโอให้ความรู้ รวมถึงการส่งข้อความแจ้งเตือนผ่าน SMS หรือ E-Mail เพื่อเน้นย้ำถึงความสำคัญของความปลอดภัยในการทำธุรกรรม นอกจากนี้ยังมีการจัดกิจกรรมประชาสัมพันธ์ เช่น งานสัมมนา เพื่อสร้างความเข้าใจที่ลึกซึ้งยิ่งขึ้นแก่ผู้บริโภคในวงกว้าง

(2) การให้ความรู้และฝึกอบรม ซึ่งเน้นการเสริมสร้างความรู้และพฤติกรรมที่เหมาะสมในการใช้งานเทคโนโลยีดิจิทัล โดยใช้เครื่องมือหลากหลาย เช่น การทำแบบสอบถามเพื่อประเมินและสร้างความตระหนักรู้ของผู้ใช้งานก่อนการเริ่มใช้บริการ เช่น E-Banking หรือแอปพลิเคชันการเงิน การอบรมเชิงปฏิบัติการเกี่ยวกับความปลอดภัยไซเบอร์ และการพัฒนาแอปพลิเคชันหรือคู่มือที่มีคำแนะนำเกี่ยวกับการป้องกันภัยออนไลน์ในตัว นอกจากนี้ยังมีการจัดทำคู่มือใช้งานที่เน้นการเตือนภัยเพื่อป้องกันการถูกหลอกลวงในระบบดิจิทัล

(3) การตรวจสอบและแจ้งเตือน ซึ่งเสริมสร้างระบบป้องกันภัยในเชิงรุก ด้วยการพัฒนาระบบแจ้งเตือนธุรกรรม การแจ้งเตือนการเข้าระบบผิดปกติ และการส่ง OTP (One-Time Password) ให้แก่ผู้ใช้เพื่อยืนยันธุรกรรม นอกจากนี้ยังมีระบบแจ้งเตือนพฤติกรรมผิดปกติในบัญชี เช่น การพยายามเข้าสู่ระบบจากอุปกรณ์หรือสถานที่ที่ไม่ได้รับอนุญาต ซึ่งมาตรการนี้ช่วยให้ผู้บริโภครับทราบและตอบสนองต่อภัยไซเบอร์ได้อย่างทันท่วงที

(4) การสนับสนุนด้านเทคนิค ซึ่งเน้นการพัฒนาเทคโนโลยีและการให้บริการเพื่อลดความเสี่ยงภัยคุกคามทางไซเบอร์ เช่น การออกแบบแอปพลิเคชันธนาคารที่มีระบบรักษาความปลอดภัยสูง การใช้ระบบ AI เพื่อตรวจจับและวิเคราะห์พฤติกรรมที่ผิดปกติ นอกจากนี้ยังมีช่องทางสนับสนุนลูกค้า เช่น Call Center ที่พร้อมให้บริการตลอด 24 ชั่วโมง และระบบล็อกธุรกรรมอัตโนมัติเมื่อพบพฤติกรรมที่น่าสงสัย

แผนภาพที่ 7 รูปแบบกระบวนการสร้างความตระหนักรู้และการคุ้มครองผู้บริโภค



ที่มา: จากการรวบรวมของคณะวิจัย

คณะวิจัยจะใช้รูปแบบความเชื่อมโยงของการดำเนินการป้องกันภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินข้างต้นเป็นกรอบในการจัดทำแบบสัมภาษณ์เชิงลึกเพื่อจัดเก็บข้อมูลจากผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง

2.3 แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) สำหรับสถาบันการเงิน

คณะวิจัยสำรวจแนวปฏิบัติ กฎระเบียบ และนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สถาบันการเงินต้องปฏิบัติตาม โดยมีรายละเอียด ดังนี้

2.3.1 แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของธนาคารแห่งประเทศไทย

ธนาคารแห่งประเทศไทย (ธปท.) มีหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน ซึ่งให้ความสำคัญกับการรักษาความลับของข้อมูล (confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability) ซึ่งต้องสอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยี โดยได้ออกหลักเกณฑ์เกี่ยวกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) สำหรับสถาบันการเงิน โดยอาศัยอำนาจตามพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ใน มาตรา 41 มาตรา 47 และมาตรา 71 ซึ่งให้อำนาจ ธปท. ในการกำกับดูแลและกำหนดแนวปฏิบัติด้านความมั่นคงปลอดภัยทางเทคโนโลยี และได้ออกหลักเกณฑ์เกี่ยวกับ การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) สำหรับสถาบันการเงินเฉพาะกิจ โดยอาศัยอำนาจตาม มาตรา 120/1 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 และที่แก้ไขเพิ่มเติม

สำหรับหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินแบ่งได้เป็น 6 ด้าน (ธปท., 2566) ดังนี้

1) ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance)

สถาบันการเงินต้องมีโครงสร้างในระดับคณะกรรมการและผู้บริหารระดับสูงในการจัดทำนโยบายและกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้เป็นไปตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง รวมทั้งต้องมีหน่วยงานในระดับปฏิบัติการที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และสื่อสารให้ความรู้แก่บุคลากรทั้งองค์กร

2) การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security management)

สถาบันการเงินต้องให้ความสำคัญกับการบริหารจัดการ ดูแลระบบเทคโนโลยีสารสนเทศให้มีความปลอดภัย มีระบบรักษาความลับของข้อมูลที่ถูกต้องและน่าเชื่อถือ มีความพร้อมใช้งาน ซึ่งสถาบันการเงินต้องดำเนินการครอบคลุมประเด็นต่าง ๆ อาทิ

- มีระบบรักษาความลับของข้อมูลที่ครอบคลุมระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องและสอดคล้องกับมาตรฐานที่น่าเชื่อและเป็นที่ยอมรับในระดับสากล ทั้งในการจัดชั้นความลับของข้อมูล (information classification) การเก็บรักษาและทำลายข้อมูล การเข้ารหัสข้อมูล (cryptography) มีการกำหนดบัญชีผู้ใช้งานที่มีสิทธิสูง (privileged user) ในการเข้าถึงข้อมูล

สำคัญของสถาบันการเงินหรือข้อมูลของลูกค้า ตลอดจนกำหนดให้มีการยืนยันตัวตนโดยใช้หลายปัจจัย (multi-factor authentication)[4] ในการเข้าถึงข้อมูลดังกล่าว

- มีการบริหารขีดความสามารถของระบบเทคโนโลยีสารสนเทศให้สามารถรองรับปริมาณธุรกรรมผ่านช่องทางดิจิทัลที่อาจเพิ่มขึ้นอย่างรวดเร็ว
- มีการรักษาความมั่นคงปลอดภัยของระบบแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint) เพื่อป้องกันการโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ หรือภัยจากโปรแกรมไม่ประสงค์ดี (malware) รวมถึงต้องมีระบบรักษาความมั่นคงปลอดภัยกรณีเกิดเหตุการณ์ไม่คาดคิด เช่น ภัยธรรมชาติ เพื่อให้สามารถให้บริการได้อย่างต่อเนื่อง
- มีกระบวนการหรืออุปกรณ์ที่สามารถติดตามดูแลระบบ และตรวจจับเหตุการณ์ความผิดปกติและภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที
- มีการประเมินช่องโหว่ในระบบงานที่มีความเสี่ยง และระบบงานสำคัญอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
- มีการทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญที่มีความเป็นอิสระ และต้องครอบคลุมระบบงานและระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (Internet facing) อย่างน้อยปีละ 1 ครั้ง
- มีการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT disaster recovery plan : IT DRP) ซึ่งต้องมีการทบทวนและทดสอบการปฏิบัติตามแผนดังกล่าวอย่างน้อยปีละ 1 ครั้ง
- กรณีเกิดเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์ ต้องมีการบันทึก วิเคราะห์ และรายงานต่อคณะกรรมการ และผู้บริหารระดับสูง รวมทั้งต้องจัดให้มีการป้องกันไม่ให้เกิดเหตุการณ์ซ้ำอีกในอนาคต
- จัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบย้อนกลับได้อย่างครบถ้วน รวมถึงสถาบันการเงินต้องดำเนินการบำรุงรักษาและบริหารทรัพย์สินด้านเทคโนโลยีสารสนเทศให้สามารถใช้งานได้อย่างเหมาะสมและเท่ากันกับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีการเปลี่ยนแปลงตลอดเวลา
- มีการจัดทำหลักเกณฑ์ในการจัดหาระบบเทคโนโลยีสารสนเทศ/บุคคลภายนอกที่ให้บริการด้านเทคโนโลยีสารสนเทศ[5] (IT Outsourcing) ที่สอดคล้องกับมาตรฐานสากล คำนึงถึงความมั่นคงปลอดภัย ทั้งนี้ กรณีที่สถาบันการเงินที่ใช้บริการด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก

---

[4] การยืนยันตัวตนโดยใช้หลายปัจจัย คือ *"กระบวนการเข้าสู่ระบบบัญชีแบบหลายขั้นตอนที่กำหนดให้ผู้ใช้ป้อนข้อมูลเพิ่มเติมนอกเหนือจากรหัสผ่าน ยกตัวอย่าง ระบบอาจขอให้ผู้ใช้ป้อนรหัสที่ส่งไปยังอีเมล ตอบคำถามลับ หรือสแกนลายนิ้วมือร่วมกับการป้อนรหัสผ่าน รูปแบบที่สองของการยืนยันตัวตนอาจช่วยป้องกันการเข้าถึงบัญชีโดยไม่ได้รับอนุญาตได้ในกรณีที่รหัสผ่านของระบบหลุดรอดออกไป"* (AWS, n.d.)

[5] บุคคลภายนอก หมายถึง *"บุคคลหรือนิติบุคคลภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของสถาบันการเงินหรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของสถาบันการเงินหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยสถาบันการเงินได้"* (ธปท., 2562)

หรือมีการเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอกให้สามารถเข้าถึงข้อมูลสำคัญได้ สถาบันการเงินต้องมีการกำกับดูแลความเสี่ยง กระบวนการบริหารความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยทางไซเบอร์ด้วย

3) การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)

สถาบันการเงินต้องจัดทำนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และจัดให้มีโครงสร้าง/หน่วยงานที่รับผิดชอบ และสายการรายงานที่ชัดเจน รวมถึงจัดทำกรอบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ครอบคลุมตั้งแต่กระบวนการประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามและทบทวนความเสี่ยง และการรายงานความเสี่ยง

นอกจากนี้ ธปท. ได้จัดทำกรอบการประเมินความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Assessment Framework : CRAF) ที่สอดคล้องกับมาตรฐานสากล เช่น National Institute of Standards and Technology (NIST) และแนวทางกำกับดูแลในต่างประเทศ อย่างประเทศสหรัฐอเมริกา (FFIEC) สิงคโปร์ (MAS) และฮ่องกง (HKMA) (ธปท., 2564) เพื่อให้สถาบันการเงินใช้เป็นแนวทางอ้างอิงในการประเมินความเสี่ยงตั้งต้นด้านไซเบอร์ (cyber inherent risk assessment) และใช้เป็นแนวทางบริหารจัดการความเสี่ยงด้านไซเบอร์ที่สอดคล้องกับระดับความเสี่ยงตั้งต้นของตนเองได้

กรอบการประเมินความเสี่ยง CRAF มีสาระสำคัญ คือ สถาบันการเงินต้องระบุและประเมินความเสี่ยงพื้นฐานทางเทคโนโลยีสารสนเทศจำนวน 5 ด้าน ได้แก่ เทคโนโลยีและการเชื่อมต่อ ช่องทางการให้บริการ ลักษณะผลิตภัณฑ์และการให้บริการ ลักษณะเฉพาะขององค์กร และประวัติการถูกคุกคามทางไซเบอร์

เมื่อประเมินและจัดระดับความเสี่ยงตามเกณฑ์ที่ ธปท. ได้กำหนดไว้แล้ว สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดทำแนวทางบริหารความเสี่ยงที่สอดคล้องกับระดับความเสี่ยงตั้งต้นของตนเอง โดยความเข้มงวดของการบริหารความเสี่ยงขึ้นอยู่กับระดับความเสี่ยงของสถาบันการเงิน เช่น ในมิติของการกำหนดบทบาทหน้าที่ของคณะกรรมการสถาบันการเงินและผู้บริหารระดับสูงในสถาบันการเงินมีความเสี่ยงตั้งต้นด้านไซเบอร์ต่ำ ธปท. กำหนดให้มีคณะกรรมการสถาบันการเงินที่รับหน้าที่กำกับดูแล และติดตามให้มีการรักษาความมั่นคงปลอดภัยไซเบอร์ กำหนดกลยุทธ์ นโยบาย และแผนด้านเทคโนโลยีสารสนเทศให้ครอบคลุมเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการกำหนดแผนการประเมินและตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยคณะกรรมการสถาบันการเงินอย่างน้อย 1 ท่าน ต้องมีความรู้และประสบการณ์ในการกำกับดูแลด้านเทคโนโลยีสารสนเทศ ซึ่งแตกต่างจากสถาบันการเงินที่มีความเสี่ยงต้นด้านไซเบอร์สูง ซึ่ง ธปท. กำหนดให้มีคณะกรรมการหรือผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของสถาบันการเงิน (Chief Information Security Officer : CISO) อย่างเฉพาะเจาะจง เป็นต้น

4) การปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance)

สถาบันการเงินต้องจัดทำกรอบการกำกับการปฏิบัติตามกฎเกณฑ์ที่สอดคล้องตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง ต้องจัดให้มีหน่วยงานที่รับผิดชอบ สายการรายงาน รวมถึงจัดให้มีกระบวนการระบุและประเมินความเสี่ยง กำหนดแผนการบริหารความเสี่ยง มีการติดตามและรายงานผลการสอบทานที่เกี่ยวข้องกับการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เช่น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายว่าด้วยคุ้มครองข้อมูลส่วนบุคคล เป็นต้น

5) การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

สถาบันการเงินต้องจัดทำแผนการตรวจสอบด้านเทคโนโลยีสารสนเทศ ที่ครอบคลุมถึงการใช้บริการและการเชื่อมต่อจากบุคคลภายนอก และจัดให้มีหน่วยงานที่รับผิดชอบการตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีความเป็นอิสระ และมั่นใจได้ว่าผู้รับผิดชอบงานด้านการตรวจสอบเทคโนโลยีสารสนเทศมีความรู้ ประสบการณ์ และความเชี่ยวชาญ ที่เพียงพอ

6) การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management)

สถาบันการเงินต้องศึกษาความจำเป็นและประโยชน์ที่คาดว่าจะได้รับจากการนำระบบเทคโนโลยีสารสนเทศมาใช้ ต้องพิจารณาความเสี่ยงที่อาจส่งผลกระทบต่อระบบและฝ่ายงานที่เกี่ยวข้อง รวมถึงกำหนดกรอบการบริหารจัดการโครงการที่ครอบคลุมตั้งแต่การเริ่มโครงการ การดำเนินการและการควบคุมโครงการ การปิดและการสอบทานโครงการ ตลอดจนมีการกำหนดโครงสร้างการกำกับดูแลโครงการ (project governance) ที่ชัดเจน

นอกจากการกำหนดหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินทั้ง 6 ด้านที่กล่าวไปข้างต้น ธปท. ยังได้กำหนดแนวนโยบายในการรักษาความมั่นคงปลอดภัยของการใช้บริการทางการเงินบนอุปกรณ์เคลื่อนที่ และกำหนดแนวทางในการเปิดเผยข้อมูลของสถาบันการเงินที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

- *การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่*

ธปท. กำหนดแนวนโยบายการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) เพื่อป้องกันภัยคุกคามทางไซเบอร์ (cyber threat) ที่อาจเกิดขึ้นกับให้บริการทางการเงินแก่ลูกค้ารายย่อย (ธปท., 2562) โดยแนวนโยบายดังกล่าวประกอบไปด้วยมาตรการ 2 ระดับ ได้แก่

มาตรการขั้นต่ำที่จำเป็นต้องดำเนินการเพื่อความรัดกุมด้านความมั่นคงปลอดภัยในการให้บริการ คือ มาตรการป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อผู้ใช้บริการทางการเงินในวงกว้าง ซึ่งครอบคลุมทั้งระบบการให้บริการทางการเงินของสถาบันการเงินบนอุปกรณ์เคลื่อนที่ เช่น การไม่อนุญาตให้อุปกรณ์เคลื่อนที่ที่ใช้ระบบล้าสมัย (obsolete Operating System : OS) มีช่องโหว่ร้ายแรงที่ประกาศจากหน่วยงานด้านความมั่นคงปลอดภัยที่เป็นสากล และกระทบการใช้งานของผู้ใช้บริการในวงกว้างเข้าใช้งานแอปพลิเคชัน และการตรวจสอบและรับมือแอปพลิเคชันปลอมบนแพลตฟอร์มอิเล็กทรอนิกส์ที่เป็นที่ยอมรับและน่าเชื่อถือ (official e-Marketplace) เช่น Google Play Store, App Store เพื่อช่วยลดความเสี่ยงที่เกิดขึ้นต่อลูกค้า จากการติดตั้งแอปพลิเคชันปลอม เป็นต้น ตลอดจนมาตรการด้านการดูแลลูกค้าให้ปลอดภัยจากการใช้บริการทางการเงินผ่านอุปกรณ์เคลื่อนที่ เช่น การเสริมสร้างความรู้ ความเข้าใจเชิงรุกที่เกี่ยวข้องกับเทคโนโลยีทางการเงิน ภัยคุกคามทางไซเบอร์ และการกำกับดูแลพนักงานในการให้บริการแก่ลูกค้าตามแนวปฏิบัติด้านการให้บริการทางการเงินบนอุปกรณ์เคลื่อนที่ที่สถาบันการเงินได้จัดทำไว้

มาตรการเพิ่มเติมที่อาจพิจารณาดำเนินการเพื่อให้เกิดความรัดกุมปลอดภัยยิ่งขึ้น คือ มาตรการที่ผู้ให้บริการพิจารณาดำเนินการเพิ่มเติม เพื่อเพิ่มการรักษาความมั่นคงปลอดภัยการให้บริการผ่านแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ที่รัดกุมมากยิ่งขึ้น เช่น การตรวจสอบการเปลี่ยนแปลงแก้ไขแอปพลิเคชัน เมื่อผู้ใช้บริการเข้าใช้งานในทันที (Anti-Tampering) เพื่อป้องกันไม่ให้ข้อมูลผู้ใช้บริการรั่วไหลหรือเกิดความเสียหายจากแอปพลิเคชันที่มีการแก้ไขโดยฝัง malicious code ไว้ และการป้องกันภัยคุกคามในระดับแอปพลิเคชัน (application layer) เช่น การเข้ารหัสข้อมูลสำคัญระหว่างรับ/ส่ง การป้องกัน DDoS Attack เพื่อป้องกันการรั่วไหลของข้อมูลและป้องกันการถูกโจมตีจนไม่สามารถให้บริการได้ เป็นต้น

นอกจากนี้ เมื่อวันที่ 7 กุมภาพันธ์ 2568 ธปท. ได้ออกประกาศธนาคารแห่งประเทศไทย ที่ 4/2568 เรื่องการรักษาความมั่นคงปลอดของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่สำหรับสถาบันการเงิน เพื่อยกระดับมาตรการในการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินของสถาบันการเงินผ่านระบบ mobile banking ให้เท่าทันความเสี่ยงจากภัยคุกคามทางไซเบอร์มากยิ่งขึ้น ซึ่งประกอบไปด้วยมาตรการ 2 ส่วน ได้แก่ (ธปท., 2567)

การป้องกันการสวมรอยทำธุรกรรมแทนผู้ใช้บริการ ธปท. กำหนดให้สถาบันการงดเว้นการแนบลิงก์ผ่านข้อความ (SMS) และช่องทางอีเมล กำหนดให้สถาบันการเงินมีกระบวนการติดตามและรับมือกับการปลอมแปลงและแอบอ้างเป็นผู้ให้บริการทางการเงินของมิจฉาชีพ ตลอดจนการกำหนดให้สถาบันการเงินต้องจัดให้มีการยืนยันตัวตนในการทำธุรกรรมทางการเงิน โดยใช้เทคโนโลยีการเปรียบเทียบใบหน้า (face recognition) ร่วมกับการตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection) เพื่อป้องกันการสวมรอยของมิจฉาชีพ เป็นต้น

การรักษาความมั่นคงปลอดภัยของแอปพลิเคชัน mobile banking ธปท. กำหนดการรักษาความมั่นคงปลอดภัยของ mobile banking ภายใต้กรอบ 3 ประการ ได้แก่ (1) การรักษาความมั่นคงปลอดภัยของข้อมูล เช่น การมีกระบวนการจัดเก็บข้อมูลที่ปลอดภัย และต้องมีการเข้ารหัสไฟล์ข้อมูล (file encryption)

หรือการปิดบังการแสดงหน้าจอเมื่อมีการย่อหน้าแอปพลิเคชัน เป็นต้น (2) การรักษาความมั่นคงปลอดภัยของแอปพลิเคชัน เช่น การไม่อนุญาตให้บริการแอปพลิเคชันที่มีช่องโหว่ที่อาจก่อให้เกิดความเสี่ยงจากการสวมรอยทำธุรกรรมแทน เป็นต้น และ (3) การรักษาความมั่นคงปลอดภัยของอุปกรณ์ เช่น การระงับการใช้งาน mobile banking หากอุปกรณ์เคลื่อนที่ของผู้ใช้บริการมีระบบปฏิบัติการที่ล้าสมัย (obsolete Operating System : OS) เป็นต้น

- *การเปิดเผยข้อมูลของสถาบันการเงินที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์*

ธปท. กำหนดให้ธนาคารพาณิชย์ต้องรายงานชุดข้อมูล (Data Set) เพื่อให้ ธปท. สามารถกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ ทั้งนี้ ความถี่ในการรายงานชุดข้อมูลที่เกี่ยวข้องจะแตกต่างกันไป ดังรายละเอียดในตารางที่ 3

ตารางที่ 3 ชุดข้อมูลด้านเทคโนโลยีสารสนเทศที่ธนาคารพาณิชย์ต้องรายงานต่อ ธปท.

ชุดข้อมูล	ความถี่
ข้อมูลการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Audit)	รายไตรมาส
ข้อมูลความสามารถของระบบเทคโนโลยีสารสนเทศ (IT Capacity)	รายเดือน
ข้อมูลศูนย์คอมพิวเตอร์หลักและสำรอง (IT DC-DR)	ราย 6 เดือน
ข้อมูลโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT Infrastructure)	รายเดือน
ข้อมูลโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ (IT Project)	รายปี/รายไตรมาส
ข้อมูลบุคลากรด้านเทคโนโลยีสารสนเทศ (IT Staff)	รายไตรมาส
ข้อมูลภาพรวมระบบเทคโนโลยีสารสนเทศ (IT System Profile)	ราย 6 เดือน
ข้อมูลการนำเทคโนโลยีมาใช้ (Technology Implementation)	รายไตรมาส
ข้อมูลการใช้บริการ การเชื่อมต่อระบบหรือการเข้าถึงข้อมูลจากบุคคลภายนอก (Third Party)	รายไตรมาส

นอกจากนี้ ธปท. กำหนดให้ธนาคารพาณิชย์ที่มีการให้บริการทางการเงินแก่ลูกค้ารายย่อยผ่านช่องทาง Mobile Banking, Internet Banking, ATM/CDM และสาขา ต้องรายงานข้อมูลกรณีระบบเทคโนโลยีในการให้บริการทางการเงินเหล่านี้ขัดข้อง เพื่อให้ประชาชนผู้บริโภคสามารถใช้ข้อมูลดังกล่าวประกอบการตัดสินใจในการใช้บริการทางการเงินของธนาคารพาณิชย์แต่ละแห่ง ทั้งนี้ ธปท. ได้กำหนดหลักเกณฑ์การเปิดเผยข้อมูลสถิติและการรายงานปัญหาหรือเหตุการณ์ขัดข้อง ดังนี้

- หากช่องทาง Mobile Banking, Internet Banking, ATM/CDM และสาขาของธนาคารพาณิชย์เกิดปัญหาระบบเทคโนโลยีสารสนเทศขัดข้อง และส่งผลให้ไม่สามารถให้บริการแก่ลูกค้ารายย่อยได้

ทั้งหมดหรือบางส่วน ธนาคารพาณิชย์ต้องนับเหตุการณ์ที่เกิดขึ้นในแต่ละช่องทางเป็น 1 เหตุการณ์ และใช้ระยะเวลาการเกิดเหตุการณ์เป็นหน่วยชั่วโมง

- การคำนวณผลกระทบจากการเกิดปัญหาเทคโนโลยีสารสนเทศขัดข้อง ธนาคารพาณิชย์เริ่มคำนวณหลังจากเกิดเหตุการณ์ไปแล้ว 15 นาที เพื่อให้ธนาคารพาณิชย์มีระยะเวลาในการวิเคราะห์ว่าปัญหาดังกล่าวเกิดขึ้นภายใต้ระบบของธนาคารพาณิชย์หรือไม่
- ธปท. กำหนดหลักเกณฑ์สำหรับปัญหาหรือเหตุการณ์ขัดข้องที่ธนาคารพาณิชย์ต้องดำเนินการเปิดเผยข้อมูล ดังนี้
    - สำหรับบริการทางการเงินผ่านช่องทาง Mobile Banking และ Internet Banking ธนาคารพาณิชย์ต้องเปิดเผยข้อมูลหากเหตุการณ์ขัดข้องก่อให้เกิดผลกระทบ ดังนี้ (1) มีธุรกรรมทางการเงินที่ดำเนินการไม่สำเร็จมากกว่าร้อยละ 10 ของธุรกรรมที่มีการดำเนินการทั้งหมด (2) จำนวนผู้ใช้บริการได้รับผลกระทบมากกว่าร้อยละ 10 ของจำนวนผู้ใช้บริการจริง (Active User) หรือมีจำนวนผู้ใช้บริการที่ได้รับผลกระทบมากกว่า 10,000 ราย
    - สำหรับบริการทางการเงินผ่านช่องทางตู้ ATM/CDM และสาขา ธนาคารพาณิชย์ต้องเปิดเผยข้อมูลหากเหตุการณ์ขัดข้องส่งผลให้จำนวนตู้ ATM/CDM หรือจำนวนสาขาไม่สามารถให้บริการทางการเงินได้มากกว่าร้อยละ 10 ในช่วงระยะเวลาการเกิดเหตุการณ์ขัดข้อง
- ธปท. กำหนดรูปแบบการเปิดเผยสถิติ และการรายงานข้อมูลให้แก่ธนาคารพาณิชย์ โดยธนาคารพาณิชย์ต้องเปิดเผยข้อมูลบนเว็บไซต์ของธนาคารเป็นรายไตรมาส ภายใน 30 วัน นับถัดจากวันสิ้นไตรมาส

สำหรับการแจ้งข้อมูลปัญหาหรือเหตุการณ์ขัดข้องของระบบเทคโนโลยีสารสนเทศแก่ลูกค้ารายย่อย ธปท. กำหนดให้ (1) ธนาคารพาณิชย์ต้องดำเนินแจ้งข้อมูลอย่างชัดเจนถึงปัญหาและเหตุการณ์ขัดข้อง การดำเนินการแก้ไข และทางเลือกในการใช้บริการช่องทางอื่น (2) ธนาคารพาณิชย์ต้องกำหนดระยะเวลาในการแจ้งข้อมูลระยะเวลาการแก้ไข หรือแจ้งความคืบหน้าของสถานการณ์แก้ไขปัญหาให้เป็นปัจจุบัน หากปัญหาหรือเหตุการณ์ขัดข้องไม่สามารถแก้ไขได้โดยเร็ว และ (3) ธนาคารพาณิชย์ต้องสื่อสารถึงปัญหาหรือเหตุการณ์ขัดข้องให้ลูกค้าทราบโดยเร็ว ผ่านช่องทางการรับข้อมูลที่ประชาชนนิยมใช้ เช่น social media เป็นต้น (ธปท., 2562)

2.3.2 แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (พ.ร.บ. ไซเบอร์) มีวัตถุประสงค์เพื่อเฝ้าระวัง ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจจะกระทบความมั่นคงของรัฐ โดยหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(รวมถึงภาคธนาคาร) คือ หน่วยงานหลักที่ต้องดำเนินมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ตาม พ.ร.บ. ดังกล่าว (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, ม.ป.ป.)

พ.ร.บ. ไซเบอร์ กำหนดให้มีการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ทำหน้าที่ในการเสนอแนะนโยบาย แผนปฏิบัติการ ประสานงาน และสนับสนุนหน่วยงานต่าง ๆ ในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ รวมถึงการเฝ้าระวัง วิเคราะห์ แจ้งเตือนภัย และเสริมสร้างความรู้ความเข้าใจด้านไซเบอร์ พร้อมทั้งร่วมมือกับหน่วยงานในและต่างประเทศ และจัดตั้งศูนย์ประสานงานในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, ม.ป.ป.) ดังนั้น สกมช. จึงจัดทำ “แนวทางการปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” (ปรับปรุงล่าสุด 4 สิงหาคม พ.ศ. 2566) ซึ่งครอบคลุมการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ , ม.ป.ป.) ดังรายละเอียดต่อไปนี้

- *แนวปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment)*

สถาบันการเงินต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับหลักการสากล เช่น NIST Special Publication 800-300 Rev.1, Guide for Conducting Risk Assessments, ISO/IEC 27001, COBIT, CIS CSC, ISA/IEC 62443 เป็นต้น ทั้งนี้ ในกระบวนการประเมินความเสี่ยงสถาบันการเงินควรใช้ผู้ตรวจประเมินความเสี่ยงที่มีความเชี่ยวชาญเกี่ยวกับการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และผ่านการอบรมหัวข้อประเมินความเสี่ยง หัวข้อการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือหัวข้อผู้นำการประยุกต์ใช้หลักการตาม ISO/IEC 27001 เป็นต้น โดยเมื่อสถาบันการเงินดำเนินการประเมินความเสี่ยงเรียบร้อยแล้วจะต้องส่งรายงานประเมินความเสี่ยงให้ สกมช. ทราบต่อไป

- *แนวปฏิบัติในการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Auditing)*

สถาบันการเงินต้องดำเนินการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับหลักการสากล เช่น NIST Special Publication 800-53A Rev.5 Assessing Security and Privacy Controls in Information System and Organizations, ISO 19011, ISO/IEC 27000 series เป็นต้น ทั้งนี้สถาบันการเงินต้องดำเนินการตรวจสอบอย่างน้อยปีละ 1 ครั้ง โดยมีขอบเขตการตรวจสอบครอบคลุมกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA) และบริการที่สำคัญของสถาบันการเงิน (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข, ม.ป.ป.) นอกจากนี้สถาบันการควรใช้ผู้ตรวจสอบที่มีความเชี่ยวชาญเกี่ยวกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

และผ่านการอบรมหัวข้อการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ หรือหัวข้อผู้นำการตรวจสอบตาม ISO/IEC 27001 เป็นต้น โดยเมื่อสถาบันการเงินดำเนินการประเมินความเสี่ยงเรียบร้อยแล้วจะต้องส่งรายงานประเมินความเสี่ยงให้ สกมช. ทราบต่อไป

นอกจากนี้ พ.ร.บ. ไซเบอร์ กำหนดให้มีการจัดตั้ง “ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT)” ขึ้นเป็นหน่วยงานในสังกัด สกมช. ทำหน้าที่ติดตามและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ตลอดจนวิเคราะห์และประมวลผลข้อมูล และแจ้งเตือนเหตุการณ์ที่เกี่ยวข้องกับการคุกคามทางไซเบอร์ (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ, ม.ป.ป.)

2.3.3 แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) มีบทบาทหน้าที่ในการส่งเสริมและพัฒนา รวมถึงการกำกับดูแลตลาดทุน ซึ่งสถาบันการเงินเป็นหนึ่งในองค์กรที่มีบริการทางการเงินที่เกี่ยวข้องกับตลาดทุน เช่น การเป็นที่ปรึกษาการลงทุน การค้าหลักทรัพย์อันเป็นตราสารหนี้ หรือการเป็นนายหน้าซื้อขายหลักทรัพย์ที่เป็นหน่วยลงทุน เป็นต้น ดังนั้น เพื่อให้การให้บริการเงินผ่านระบบเทคโนโลยีสารสนเทศในตลาดทุนมีความมั่นคงปลอดภัย ก.ล.ต. จึงออกประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ เรื่อง “ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจที่เกี่ยวข้องกับตลาดทุน” โดยอาศัยอำนาจตาม พระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535 ซึ่งเป็นกฎหมายหลักที่กำหนดอำนาจหน้าที่ของ ก.ล.ต. ในการกำกับดูแลและควบคุมกิจการที่เกี่ยวข้องกับตลาดทุนในประเทศไทย (พระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์, 2535)

สถาบันการเงินต้องดำเนินการด้านเทคโนโลยีสารสนเทศทั้งหมด 3 ด้าน ได้แก่ การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security) และการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit) (สำนักงานคณะกรรมการ ก.ล.ต., 2565) ดังรายละเอียดต่อไปนี้

- *การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)*

สถาบันการเงินต้องกำหนดบทบาทหน้าที่และความรับผิดชอบของคณะกรรมการด้านเทคโนโลยีสารสนเทศที่ครอบคลุมตั้งแต่การกำหนดกรอบการกำกับดูแลด้านเทคโนโลยีสารสนเทศ การจัดสรรทรัพยากร (ครอบคลุมถึงทรัพยากรบุคคล) การกำหนดนโยบายที่เกี่ยวข้อง การกำหนดขั้นตอนการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัย การสร้างความตระหนักรู้ด้านความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้เกิดขึ้น

ตลอดทั้งองค์กร ตลอดจนการติดตาม ตรวจสอบ และรายงานผลการปฏิบัติงานด้าน เทคโนโลยีสารสนเทศ ทั้งนี้สถาบันการเงินการเงินต้องกำหนดให้โครงสร้างการกำกับดูแลมีความเป็นอิสระ และมีความสอดคล้องกับหลักแบ่งแยกหน้าที่ 3 ระดับ (three Lines of Defense)[6] นอกจากนี้ สถาบันการเงินต้องจัดให้มีนโยบายบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) ซึ่งมีสาระสำคัญครอบคลุมบทบาทหน้าที่ของผู้ที่รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และครอบคลุมกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (สำนักงานคณะกรรมการ ก.ล.ต., 2567)

- *การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security)*

สถาบันการเงินต้องจัดให้มีนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ที่ครอบคลุมโครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารจัดการบุคลากร และบุคคลภายนอก การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ การรักษาความมั่นคงปลอดภัยของข้อมูล การควบคุมการเข้าถึงข้อมูลและระบบ การควบคุมการเข้ารหัส การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ การจัดหา พัฒนาและบำรุงรักษาระบบ การบริหารจัดการเหตุการณ์ผิดปกติด้าน เทคโนโลยีสารสนเทศ และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยสถาบันการเงินต้องดำเนินการทบทวนนโยบายข้างต้นอย่างน้อยปีละ 1 ครั้ง เพื่อให้นโยบายมีความคลุมต่อภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น (สำนักงานคณะกรรมการ ก.ล.ต., 2567)

- *การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)*

สถาบันการเงินต้องดำเนินตรวจสอบด้านเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น โดยในกระบวนการตรวจสอบสถาบันการเงินต้องจัดให้มีผู้ตรวจสอบมีความเป็นอิสระจากฝ่ายปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และผ่านการรับรองมาตรฐาน เช่น Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) หรือ ISO/IEC 27001 Lead Auditor โดยแผนของการตรวจสอบด้านเทคโนโลยีสารสนเทศ สถาบันการเงินจะต้องดำเนินการทบทวนปีละ 1 ครั้ง ทั้งนี้หลังจากสถาบันการเงินดำเนินการตรวจสอบเสร็จสิ้นแล้ว สถาบันการเงินต้องจัดทำแผนการแก้ไข

[6] มาตรการตรวจสอบการใช้ดุลพินิจ (three Lines of Defense) คือ *"หลักการควบคุมดูแลแบบเป็นลำดับขั้นให้เป็นไปตามกฎระเบียบขั้นตอนปฏิบัติงาน โดยประกอบไปด้วยหน่วยงานที่เป็น 1st Line , 2nd Line และ 3rd Line ซึ่งกระบวนการในแต่ละระดับ (Line) จะก่อให้เกิดกระบวนการกำกับดูแลที่ดี ทำให้ธนาคารบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพ ไม่มีความเสี่ยง อีกทั้งยังเป็นการเตรียมความพร้อม เพื่อรองรับรูปแบบการทำธุรกิจที่เปลี่ยนแปลงไปอย่างรวดเร็ว"* โดยแต่ละระดับมีหน้าที่ ดังนี้ 1st Line มีหน้าที่ในการปฏิบัติงาน 2nd Line มีหน้าที่บริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง และ 3rd Line มีหน้าที่ในการตรวจสอบ (สำนักงานคณะกรรมการ ก.ล.ต., 2567)

ข้อบกพร่องด้านเทคโนโลยีสารสนเทศที่พบจากการตรวจสอบ และรายงานผลแก่สำนักงาน ก.ล.ต. ภายใน 3 เดือนหลังสิ้นปีปฏิทิน (สำนักงานคณะกรรมการ ก.ล.ต., 2567)

นอกจากนี้ สถาบันการเงินต้องดำเนินการประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศตามแบบ Risk Level Assessment (RLA) และรายงานผลการประเมินความเสี่ยงต่อ ก.ล.ต. ภายในไตรมาสที่ 4 ของทุกปี (สำนักงานคณะกรรมการ ก.ล.ต., ม.ป.ป.)

2.3.4 แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) มีบทบาทในการกำหนดมาตรการหรือกลไกการกำกับดูแลระบบการทำธุรกรรมผ่านอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือและมั่นคงปลอดภัยต่อผู้ใช้บริการ อาศัยอำนาจตาม พ.ร.บ. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562 (มาตรา 5) ดังนั้น สพธอ. จึงได้มีการผลักดัน พ.ร.ฎ. การประกอบธุรกิจบริการแพลตฟอร์มดิจิทัลที่ต้องแจ้งให้ทราบ พ.ศ. 2565 หรือที่เรียกว่า กฎหมาย DPS (Digital Platform Services) โดยสาระสำคัญของกฎหมายดังกล่าวกำหนดให้ผู้ให้บริการหรือผู้ประกอบการแพลตฟอร์มดิจิทัล (รวมถึงสถาบันการเงินที่มีการให้บริการทางการเงินผ่านแพลตฟอร์มดิจิทัล) ต้องดำเนินการจดแจ้งข้อมูลกับ สพธอ. โดยข้อมูลที่ใช้ในการจดแจ้ง เช่น ชื่อบริษัท ลักษณะของการให้บริการบนแพลตฟอร์มดิจิทัล และจำนวนผู้ใช้บริการ เป็นต้น นอกจากนี้แพลตฟอร์มที่ดำเนินการลงทะเบียนกับ สพธอ. ต้องดำเนินการให้มีการพิสูจน์และยืนยันตัวตนทางดิจิทัลในขั้นตอนลงทะเบียนของผู้ใช้บริการ เพื่อให้เกิดความมั่นคงปลอดภัยและสร้างความน่าเชื่อถือให้กับผู้บริโภคในการเข้าใช้บริการแพลตฟอร์ม ทั้งนี้กฎหมาย DPS มีผลบังคับใช้เมื่อวันที่ 21 สิงหาคม พ.ศ. 2566 (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ , 2566)

2.3.5 แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานส่งเสริมเศรษฐกิจดิจิทัล

สำนักงานส่งเสริมเศรษฐกิจดิจิทัล (สศด.) มีบทบาทในการส่งเสริมเศรษฐกิจดิจิทัลของประเทศไทย เพื่อยกระดับความขีดความสามารถของภาคธุรกิจผ่านเทคโนโลยี โดยหนึ่งในผู้เล่นหลักที่มีส่วนเกี่ยวข้องกับสถาบันการเงินอย่างผู้ประกอบการในอุตสาหกรรมดิจิทัล (digital provider) ต้องดำเนินการขึ้นทะเบียนผู้ประกอบการ อันเป็นไปตามประกาศสำนักงานส่งเสริมเศรษฐกิจดิจิทัล เรื่อง หลักเกณฑ์ในการขึ้นทะเบียนผู้ประกอบการในอุตสาหกรรมดิจิทัล เพื่อสนับสนุนการประยุกต์ใช้เทคโนโลยีดิจิทัลในภาคธุรกิจอุตสาหกรรม ประจำปี พ.ศ. 2567 อาศัยอำนาจตามความในมาตรา 51 แห่งพระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560 โดยผู้ประกอบการต้องได้รับการรับรองมาตรฐานกระบวนการผลิตหรือพัฒนาซอฟต์แวร์ อุปกรณ์ ฮาร์ดแวร์อัจฉริยะ และบริการดิจิทัล เช่น ISO/IEC 29110, Capability Maturity Model

Integration (CMMI) หรือมาตรฐานอื่น ๆ ตามที่สำนักงานกำหนด จึงจะผ่านคุณสมบัติของผู้ประกอบการที่มีสิทธิขอขึ้นทะเบียนผู้ประกอบการในอุตสาหกรรมดิจิทัล (สำนักงานส่งเสริมเศรษฐกิจดิจิทัล, 2566)

2.3.6 สรุปแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของธนาคารไทย

จากการทบทวนแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สถาบันการเงินต้องปฏิบัติตาม พบว่า หน่วยงานกำกับดูแลและหน่วยงานที่เกี่ยวข้องอื่น ๆ จัดทำแนวปฏิบัติที่ครอบคลุมตั้งแต่การกำหนดโครงสร้างการกำกับดูแลของสถาบันการเงินให้คณะกรรมการ ผู้บริหารระดับสูง และเจ้าหน้าที่ในระดับปฏิบัติการมีหน้าที่กำกับและดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศสอดคล้องกับหลักแบ่งแยกหน้าที่ 3 ระดับ (three Lines of Defense) รวมถึงการกำหนดให้สถาบันการเงินต้องดำเนินการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ครอบคลุมการตรวจสอบและเฝ้าระวังการโจมตีทางไซเบอร์จากช่องโหว่ของระบบเทคโนโลยีสารสนเทศ เช่น การบริหารจัดการช่องโหว่ (vulnerability management) หรือการทดสอบเจาะระบบ (penetration test) เป็นต้น ทั้งในส่วนของระบบเทคโนโลยีของสถาบันการเงินเองและระบบเทคโนโลยีของบุคคลภายนอก ตลอดจนการกำหนดให้สถาบันการเงินต้องจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และกระบวนการจัดการของสถาบันการเงินกรณีการเกิดเหตุการณ์โจมตีทางไซเบอร์

นอกจากนี้ หน่วยงานกำกับดูแลกำหนดให้สถาบันการเงินต้องดำเนินการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีกรอบการประเมินความเสี่ยงสอดคล้องกับมาตรฐานสากล เช่น National Institute of Standards and Technology (NIST) ISO/IEC 27001 และแนวทางกำกับดูแลในต่างประเทศ ได้แก่ ประเทศสหรัฐอเมริกา (FFIEC) สิงคโปร์ (MAS) และฮ่องกง (HKMA) เป็นต้น รวมถึงการกำหนดให้สถาบันการเงินดำเนินการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit) โดยใช้ผู้ตรวจสอบที่มีความเป็นอิสระและมีความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้นำตรวจสอบตาม ISO/IEC 27001

ในส่วนของการปกป้องและคุ้มครองผู้ใช้บริการทางการเงินรายย่อยให้ได้รับความปลอดภัยจากภัยคุกคามทางไซเบอร์ ธปท. กำหนดนโยบายที่เกี่ยวข้องกับใช้บริการทางการเงินผ่านอุปกรณ์เคลื่อนที่เพื่อป้องกันภัยคุกคามทางไซเบอร์ผ่านการทำธุรกรรมทางการเงินของลูกค้ารายย่อย ทั้งในมิติของการดำเนินมาตรการที่ควบคุมความปลอดภัยของระบบการให้บริการทางการเงิน ตลอดจนการเสริมสร้างความรู้ความเข้าใจแก่ลูกค้ารายย่อยให้รู้เท่าทันภัยทางการเงินออนไลน์ รวมถึงการกำหนดให้ธนาคารพาณิชย์ที่มีการให้บริการทางการเงินแก่ลูกค้ารายย่อยผ่านช่องทาง Mobile Banking Internet Banking ATM/CDM และสาขา ต้องดำเนินการรายงานข้อมูลระบบเทคโนโลยีในการให้บริการทางการเงินขัดข้องในช่องทางดังกล่าวเพื่อให้ประชาชนผู้บริโภคสามารถใช้ข้อมูลดังกล่าวประกอบการตัดสินใจในการใช้บริการทางการเงินของธนาคารพาณิชย์แต่ละแห่ง

นอกจากนี้ สพธอ. กำหนดให้สถาบันการเงินที่มีการให้บริการทางการเงินผ่านแพลตฟอร์มดิจิทัลต้องดำเนินการจดแจ้งข้อมูลกับ สพธอ. โดยอาศัยอำนาจตามพระราชกฤษฎีกาการประกอบธุรกิจบริการแพลตฟอร์มดิจิทัลที่ต้องแจ้งให้ทราบ พ.ศ. 2565 เพื่อให้เกิดความมั่นคงปลอดภัยและสร้างความน่าเชื่อถือให้กับผู้บริโภคในการเข้าใช้บริการแพลตฟอร์มภายใต้กฎหมาย DPS รวมถึงการจัดตั้ง ThaiCERT (หน่วยงาน

ภายใต้ สกมช.) ขึ้นมาเป็นหน่วยงานกลางในการประสานงานและเฝ้าระวังความเสี่ยงในการคุกคามทางไซเบอร์ อย่างไรก็ตาม คณะวิจัยไม่พบแนวปฏิบัติที่เกี่ยวข้องกับการเยียวยาผู้ที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

2.4 ปัญหาบัญชีม้าและการฉ้อโกงของมิจฉาชีพในภาคธนาคาร

ดังที่กล่าวในหัวข้อ 2.1.1 ว่ารูปแบบภัยทางการเงินออนไลน์ทั้งหมด จะมี *"บัญชีม้า"* ทำหน้าที่เป็นตัวกลางในการรับโอนเงินที่ได้จากการหลอกลวง และกระจายเงินไปยังบัญชีปลายทางเพื่อปกปิดตัวตน ทั้งนี้ บัญชีม้าเป็นปัญหาสำคัญที่ส่งผลกระทบต่อเศรษฐกิจและสังคม โดยเฉพาะในด้านอาชญากรรมทางการเงิน เช่น การฟอกเงินและการฉ้อโกง ซึ่งมักมีการใช้บัญชีม้าเพื่อปกปิดเส้นทางการเงินที่ผิดกฎหมาย ดังนั้น การจัดการปัญหาบัญชีม้าจึงมีความสำคัญอย่างมากในการลดภัยคุกคามทางไซเบอร์ โดยปัจจุบันรัฐบาลไทยออก พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ซึ่งกำหนดบทบาทหน้าที่ให้หน่วยงานอย่าง สถาบันการเงิน ธนาคารแห่งประเทศไทย สำนักงานตำรวจแห่งชาติ สำนักงานป้องกันและปราบปรามการฟอกเงิน กรมสอบสวนคดีพิเศษ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และผู้ให้บริการโทรคมนาคม ในการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี ซึ่งรวมถึงบัญชีม้าร่วมกัน

2.4.1 นิยามและประเภทของบัญชีม้า

ธนาคารแห่งประเทศไทยกำหนดนิยามบัญชีม้า หมายถึง บัญชีเงินฝากธนาคารหรือกระเป๋าเงินอิเล็กทรอนิกส์ (e-wallet) ของบุคคลอื่น ที่นำมาใช้เป็นช่องทางการทำธุรกรรมทางการเงิน เช่น การถ่ายโอนเงิน การรับเงินการโอนเงิน ซึ่งเงินที่ได้มาจากการกระทำผิด เพื่อป้องกันไม่ให้มีพยานหลักฐานเชื่อมโยงมาถึงตัวผู้กระทำผิดได้ (ธปท., 2565) โดยบัญชีม้าสามารถแบ่งได้เป็น 3 ประเภทได้แก่

1. บัญชีม้าแบบขายขาด เป็นบัญชีที่เหยื่อหรือผู้รับจ้างดำเนินการเปิดบัญชีธนาคาร เพื่อขายขาดให้กลุ่มมิจฉาชีพนำไปก่ออาชญากรรม ปัจจุบันมีราคาซื้อ-ขายตั้งแต่ 1,500 บาทขึ้นไป โดยผู้ที่รับซื้อบัญชีลักษณะนี้มักจะเป็นแก๊งคอลเซ็นเตอร์ (Call center) หรือเป็นการซื้อบัญชีม้าเพื่อใช้งานส่วนตัว ไม่ได้ใช้สำหรับก่ออาชญากรรม (มติชนออนไลน์, 2567)
2. บัญชีม้าแบบเช่ารายเดือน หรือบัญชีม้าเลี้ยง เป็นบัญชีที่มิจฉาชีพจะให้เหยื่อหรือผู้รับจ้างดำเนินการเปิดบัญชีธนาคาร พร้อมจ่ายเงินค่าดูแลบัญชีเป็นรายเดือน ปัจจุบันมีราคาซื้อ-ขายตั้งแต่ 30,000 บาท และค่าดูแลบัญชีเดือนละ 5,000-10,000 บาท โดยผู้ที่รับซื้อบัญชีลักษณะนี้มักจะเป็นกลุ่มคนในวงการพนันออนไลน์ (มติชนออนไลน์, 2567)
3. บัญชีม้าแบบนิติบุคคล ซึ่งราคาสูงถึง 150,000 บาท (ประชาชาติธุรกิจ, 2567)

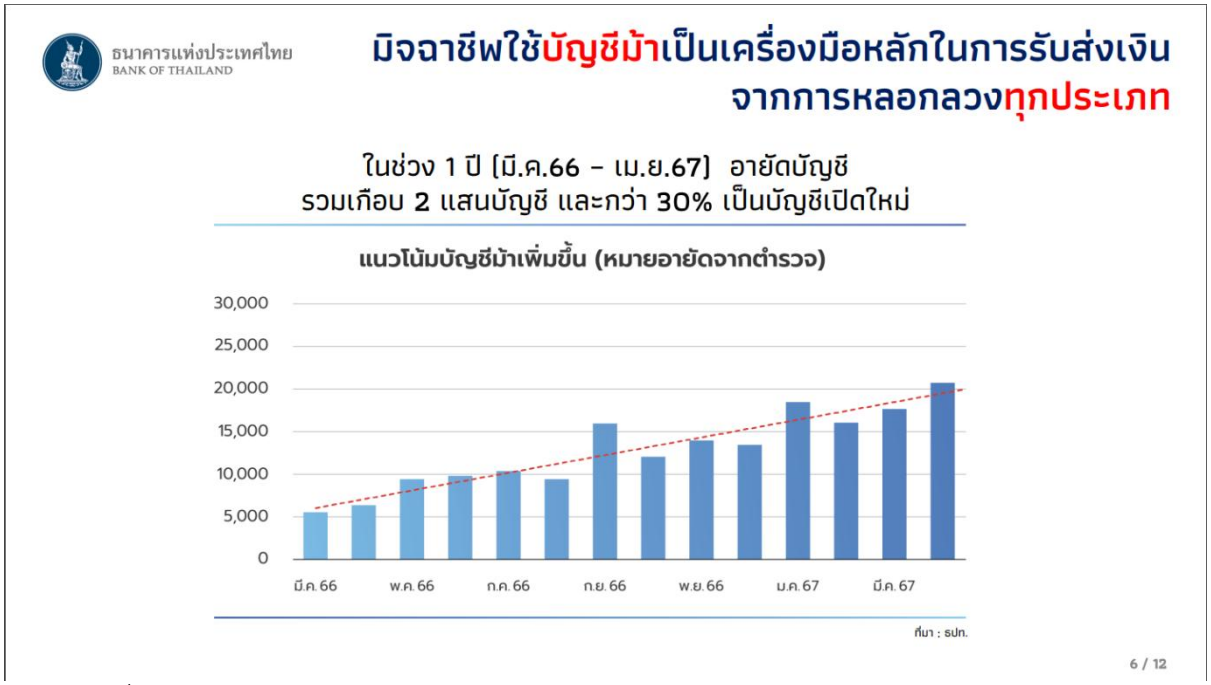
บัญชีม้าถูกนำไปใช้อย่างแพร่หลายมากขึ้นในการกระทำความผิดที่เกี่ยวกับการหลอกลวงฉ้อโกงในหลายรูปแบบ เช่น การหลอกให้ทำงานเสริมผ่านทางออนไลน์ การข่มขู่ให้เกิดความหวาดกลัว

การหลอกให้ลงทุน ไปจนถึงการพนันออนไลน์ (สตช., 2565) ซึ่งกลุ่มผู้ก่อเหตุมักจะมีบัญชีม้าในการทำธุรกรรมหลายบัญชี เพื่อโอนเงินส่งต่อกันเป็นทอด ๆ เช่น เมื่อเหยื่อโอนเงินเข้าสู่บัญชีม้าที่ 1 ผู้ก่อเหตุจะโอนเงินออกไปยังบัญชีที่ 2 จากนั้นทำธุรกรรมในลักษณะนี้ต่อกันไปอีกหลายบัญชีภายในเวลาไม่กี่นาทีก่อนจะถอนเงินของเหยื่อออกจากบัญชีธนาคาร

โดยขั้นตอนการหลอกลวงของกลุ่มมิจฉาชีพเริ่มต้นด้วยการประกาศตามหาบัญชีธนาคารที่สามารถเปิดผ่านออนไลน์หรือผ่านการลงพื้นที่ในชุมชน ต่อมา ผู้เปิดบัญชีม้าจะนำข้อมูลไปเปิดบัญชีธนาคาร บัตร ATM และเบอร์โทรศัพท์มือถือ สำหรับใช้เปิดบัญชีธนาคารออนไลน์ (e-banking) จากนั้น เจ้าของบัญชีม้าจะขายขาดข้อมูลต่าง ๆ ไม่ว่าจะเป็นสมุดบัญชีธนาคาร บัตร ATM ข้อมูลส่วนบุคคล รูปหลังบัตรประชาชน ซิมการ์ด ให้กับกลุ่มผู้ก่อเหตุ ในกรณีของบัญชีม้าเลี้ยง เจ้าของบัญชีจะมีหน้าที่ในการโอนเงินตามคำสั่งของผู้ก่อเหตุ หรือหากเกิดปัญหาในการทำธุรกรรมทางการเงินหรือเกิดคดีความ เจ้าของบัญชีจะต้องเป็นผู้แสดงตัวตนที่ธนาคาร (ธปท., 2565)

จากสถิติการรับแจ้งความออนไลน์ คดีอาชญากรรมทางเทคโนโลยี ตั้งแต่วันที่ 1 มีนาคม 2565 ถึง 30 มิถุนายน 2567 พบว่ามีการแจ้งความผ่านระบบแจ้งความออนไลน์ทั้งหมด 575,507 เรื่อง มูลค่าความเสียหายรวมกว่า 65,715 ล้านบาท (สตช., 2567) และในช่วงตั้งแต่เดือนมีนาคม 2566 ถึงเดือนเมษายน 2567 ตำรวจออกคำสั่งอายัดบัญชีธนาคารรวมเกือบ 200,000 บัญชี ในจำนวนนี้ราวร้อยละ 30 เป็นบัญชีธนาคารที่เปิดใหม่ ทั้งนี้ บัญชีม้ามีจำนวนเพิ่มขึ้นอย่างมาก โดยในเดือนมีนาคม 2566 มีบัญชีม้าประมาณ 6,000 บัญชี และเพิ่มขึ้นเป็น 20,000 บัญชี ในเดือนเมษายน 2567 หรือเพิ่มขึ้นเกือบ 4 เท่าภายในช่วงเวลา 1 ปี (ธปท., 2567)

แผนภาพที่ 8 แนวโน้มปัญหาบัญชีม้าในช่วง มีนาคม 2566-เมษายน 2567



ที่มา: ธนาคารแห่งประเทศไทย

นอกจากนี้ แม้ว่าจะมีการกำหนดโทษของการเปิดบัญชีม้าตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 มาตรา 9 ซึ่งระบุโทษของบัญชีม้าและซิมม้า คือ ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ รวมถึงอาจถูกดำเนินคดีในฐานะตัวการร่วมหรือผู้สนับสนุนในการทำความผิด (พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566, 2566) แต่ก็ยังไม่สามารถลดจำนวนบัญชีม้า การพัฒนาแนวทางป้องกันที่เข้มงวดจากการร่วมมือกันของภาคส่วนต่าง ๆ จึงมีความสำคัญเป็นอย่างมากในการจัดการปัญหาบัญชีม้า

2.5 แนวปฏิบัติในการจัดการปัญหาบัญชีม้า

คณะวิจัยใช้กรอบความสัมพันธ์ในการดำเนินงานของหน่วยงาน/องค์กรที่เกี่ยวข้องในการจัดการปัญหาบัญชีม้า ดังที่นำเสนอในหัวข้อ 2.2 ซึ่งประกอบด้วย

1) สถาบันการเงิน (Financial Institutions) มีบทบาทในการยกระดับมาตรการป้องกันบัญชีม้า เช่น จำกัดการใช้งาน mobile banking ให้ใช้ได้เพียง 1 อุปกรณ์ต่อบัญชี ยืนยันตัวตนลูกค้าด้วยเทคโนโลยี biometrics แจ้งเตือนก่อนทำธุรกรรม และพัฒนาระบบตรวจจับบัญชีหรือธุรกรรมต้องสงสัย พร้อมรายงานต่อหน่วยงานกำกับดูแลที่เกี่ยวข้อง

2) หน่วยงานกำกับดูแล มีบทบาทในการจัดทำนโยบายและกำกับดูแลให้บริษัทจดทะเบียนที่เกี่ยวข้องในการแก้ไขปัญหาบัญชีม้า ปฏิบัติตามกฎหมายและข้อบังคับของหน่วยงานนั้นๆ ซึ่งประกอบด้วย ธนาคารแห่งประเทศไทย และคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.)

3) หน่วยงานบังคับใช้กฎหมาย มีบทบาทในการดำเนินคดีกับผู้กระทำผิดที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์ และระงับบัญชีม้าในการสนับสนุนอาชญากรรมตามขอบเขตที่กฎหมายกำหนด ประกอบด้วย สำนักงานตำรวจแห่งชาติ (สตช.) กรมสอบสวนคดีพิเศษ (Department of Special Investigation : DSI) และสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.)

4) หน่วยงานคุ้มครองผู้บริโภค มีหน้าที่รับเรื่องร้องเรียนและช่วยเหลือผู้บริโภคที่ได้รับผลกระทบ รวมถึงเสนอมาตรการและกฎหมายที่เกี่ยวข้องกับการแก้ปัญหาบัญชีม้า

ทั้งนี้ คณะวิจัยได้สรุปบทบาท หน้าที่ ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง ตลอดจนกฎหมายและแนวปฏิบัติที่แต่ละหน่วยงานต้องดำเนินการพอสังเขป เพื่อให้เห็นภาพความเชื่อมโยงของการป้องกันปัญหาบัญชีม้าที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ในภาคการเงิน โดยมีรายละเอียด ดังนี้

2.5.1 แนวปฏิบัติในการจัดการปัญหาบัญชีม้าของธนาคารแห่งประเทศไทย

ธปท. กำหนดมาตรฐานขั้นต่ำของสถาบันการเงิน เพื่อยกระดับการดูแลและจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน ตลอดจนลดผลกระทบจากความเสี่ยงและความเสียหายที่อาจเกิดขึ้นต่อผู้ใช้บริการและผู้ให้บริการทางการเงิน โดยมีสาระสำคัญ ดังนี้

<u>ด้านธรรมาภิบาล</u> ผู้ให้บริการทางการเงินต้องมีนโยบายในการบริการจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน การประเมิน วัดผล และติดตามประสิทธิภาพและประสิทธิผลของการจัดการภัยทุจริต มีโครงสร้างคณะกรรมการและผู้บริหารระดับสูงในการกำกับดูแล และบริหารจัดการภัยทุจริตที่เกิดขึ้นและบรรเทาผลกระทบที่อาจเกิดขึ้นต่อผู้เสียหาย นอกจากนี้ ผู้ให้บริการทางการเงินควรสร้างความตระหนักรู้เรื่องภัยทุจริตจากการทำธุรกรรมให้ทราบทั้งองค์กร ทั้งในมิติของการบริหารความเสี่ยง และความเข้าใจเกี่ยวกับภัยรูปแบบใหม่ ๆ ที่อาจเกิดขึ้น

<u>ด้านบริหารจัดการภัยทุจริต</u> ธปท. กำหนดกรอบดำเนินการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน โดยมีสาระสำคัญ ดังนี้ (ธปท., 2566)

- *การเพิ่มมาตรการป้องกันผ่านการปิดช่องว่างที่มิจฉาชีพอาจฉวยโอกาสหลอกลวงประชาชน*

เพื่อป้องกันไม่ให้มิจฉาชีพเข้าถึงประชาชนได้ง่ายขึ้น ธปท. กำหนดให้สถาบันการเงินงดการส่งลิงก์ทุกประเภทผ่าน SMS หรืออีเมล และหลีกเลี่ยงการส่งลิงก์ขอข้อมูลสำคัญ เช่น ชื่อผู้ใช้ รหัสผ่าน หรือเลขบัตรประชาชนผ่านช่องทางโซเชียลมีเดีย การจำกัดจำนวนบัญชีผู้ใช้ mobile banking ให้ใช้ได้เพียง 1 อุปกรณ์ต่อบัญชีเท่านั้น และต้องแจ้งเตือนลูกค้าทุกครั้งก่อนการทำธุรกรรม พร้อมทั้งพัฒนาระบบความปลอดภัยของ mobile banking ให้ทันสมัยอยู่เสมอ เพื่อตอบรับกับภัยการเงินรูปแบบใหม่

นอกจากนี้ สถาบันการเงินต้องยกระดับการยืนยันตัวตนอย่างเข้มงวด ด้วยการใช้เทคโนโลยีเปรียบเทียบอัตลักษณ์ทางกายภาพ (biometrics) เช่น การสแกนใบหน้า ในกรณีที่ลูกค้าขอเปิดบัญชีผ่านแอปพลิเคชันธนาคาร และกำหนดเพดานการทำธุรกรรมผ่าน mobile banking ที่เหมาะสมกับระดับความเสี่ยงของกลุ่มลูกค้าแต่ละประเภท โดยลูกค้าสามารถขอปรับวงเงินตามความจำเป็นได้ แต่จะต้องผ่านการยืนยันตัวตนอย่างเคร่งครัด

- *การเพิ่มมาตรการตรวจจับและติดตามบัญชี หรือธุรกรรมต้องสงสัย*

เพื่อลดการใช้บัญชีม้า และสามารถจำกัดความเสียหายจากธุรกรรมต้องสงสัยได้เร็วขึ้น ธปท. กำหนดเงื่อนไขสำหรับการตรวจจับและติดตามธุรกรรมที่เข้าข่ายผิดปกติหรือมีการกระทำที่อาจเกี่ยวข้องกับการทุจริต เพื่อให้สถาบันการเงินรายงานข้อมูลเหล่านี้ต่อสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ได้อย่างรวดเร็ว นอกจากนี้ ธปท. ยังระบุให้สถาบันการเงินต้องพัฒนาเกณฑ์การคัดกรองบัญชีม้า โดยพิจารณาจากพฤติกรรมการโอน มูลค่าธุรกรรม และรูปแบบการทำธุรกรรมที่ผิดปกติ เพื่อให้สามารถติดตามและจัดการบัญชีต้องสงสัยได้อย่างครอบคลุม และให้ระงับบัญชีม้าความเสี่ยงสูงได้ทันที ส่วนบัญชีที่อยู่ในระดับความเสี่ยงต่ำกว่า อาจให้เจ้าของบัญชียืนยันตัวตนใหม่เพื่อป้องกันการใช้บัญชีโดยมิจฉาชีพ

ธนาคารต้องเพิ่มความเข้มงวดในการจัดการธุรกรรมต้องสงสัย โดยขยายขอบเขตการระงับการโอนเงินจากบัญชีที่มีความเสี่ยงสูง และปฏิเสธการเปิดบัญชีใหม่ในกรณีที่เข้าข่ายต้องสงสัย แม้จะยังไม่มีการแจ้งความเสียหายอย่างเป็นทางการก็ตาม และควรมีมาตรการในการระงับเงินที่กำลังจะถูกโอนเข้าสู่บัญชีม้าหรือบัญชีต้องสงสัย พร้อมแจ้งเตือนผู้โอนเงินทันทีหากปลายทางเป็นบัญชีที่มีความเสี่ยง เพื่อป้องกันความเสียหายล่วงหน้า และช่วยลดขั้นตอนการดำเนินคดีหรือการเรียกเงินคืนในภายหลัง

- *การเพิ่มมาตรการเยียวยาผู้ที่ได้รับผลกระทบจากภัยทุจริต*

เพื่อจัดการปัญหาให้ผู้เสียหายได้อย่างรวดเร็ว ธปท. กำหนดให้สถาบันการเงินต้องจัดให้มีช่องทางติดต่อเร่งด่วน (hotline) ซึ่งแยกออกจากช่องทางให้บริการปกติ และให้บริการตลอด 24 ชั่วโมง เพื่อให้ผู้ใช้บริการสามารถแจ้งเหตุทุจริตหรือความเสียหายได้ทันที และหากพบว่าความเสียหายเกิดจากข้อบกพร่องของสถาบันการเงินเอง สถาบันการเงินจะต้องเยียวยาความเสียหายอย่างเป็นธรรมและเหมาะสมแก่ผู้ที่ได้รับความเสียหายภายใน 5 วัน

นอกจากนี้ ธปท. ดำเนินการยกระดับมาตรการการกวาดล้างบัญชีม้า ผ่านการใช้ข้อข้อมูลจาก 3 แหล่ง ได้แก่ สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ระบบข้อมูล Central Fraud Registry (CFR) และข้อมูลบัญชีที่ธนาคารตรวจสอบว่ามีพฤติกรรมต้องสงสัย เช่น บัญชีที่โอนเงินเข้า-ออกมูลค่าน้อยในเวลาสั้น ๆ หลายครั้งก่อนมีเงินโอนเข้า-ออกมูลค่าสูง เพื่อจัดระดับความเสี่ยงในการดำเนินการกับบัญชีเหล่านั้น ซึ่งทุกธนาคารจะมีมาตรฐานเดียวกัน เช่น การระงับการใช้บัญชีผ่านช่องทางอิเล็กทรอนิกส์ทันที พิสูจน์ข้อเท็จจริงเพิ่มเติมตามระดับความเสี่ยง ซึ่งจะทำให้การกวาดล้างบัญชีม้าทำได้ครอบคลุมและรวดเร็วขึ้น (ธปท., 2567)

2.5.2 แนวปฏิบัติในการจัดการปัญหาบัญชีม้าของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) มีบทบาทในการตรวจสอบเบอร์โทรศัพท์ที่ผูกเข้ากับระบบ mobile banking โดยชื่อผู้ใช้ mobile banking ดังกล่าวจะต้องตรงกับชื่อเจ้าของหมายเลขโทรศัพท์ เพื่อเป็นการยืนยันว่าเป็นเจ้าของบัญชีตัวจริง

ทั้งนี้ สำนักงาน กสทช. ได้ตรวจสอบเบอร์โทรศัพท์ที่ผูกกับระบบ mobile banking จำนวนราว 106 ล้านเลขหมาย และพบว่ามีจำนวนราว 30 ล้านเลขหมายที่มีชื่อไม่ตรงกับชื่อเจ้าของบัญชี ซึ่งบัญชีดังกล่าวจะถูกส่งต่อให้ ธปท. และ ปปง. ในการตรวจสอบต่อไป นอกจากนี้ กสทช. ยังมีหน้าที่ในการระงับเบอร์โทรศัพท์มือถือที่ไม่มีการลงทะเบียน หรือลงทะเบียนด้วยข้อมูลที่ไม่ถูกต้อง รวมไปถึงเบอร์โทรศัพท์ที่คาดว่าอาจจะใช้ในการเปิดบัญชีม้าด้วย (กสทช., 2567)

อย่างไรก็ตาม มิจฉาชีพมีการปรับตัวต่อมาตรการดังกล่าวอย่างรวดเร็วโดยการซื้อทั้งบัญชีม้าและซิมม้าจากผู้ใช้ เพื่อให้ชื่อขอบัญชีและหมายเลขเบอร์โทรตรงกัน นอกจากนี้ยังมีคความกังวลต่อมาตรการดังกล่าวว่าจะส่งผลกระทบต่อผู้บริโภคในการต้องเสียเวลาไปยืนยันตัวตนเพิ่มเติมอีกด้วย (The MATTER, 2024)

2.5.3 แนวปฏิบัติในการจัดการปัญหาบัญชีม้าของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (สศด.)

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมมีบทบาทสำคัญในการจัดการปัญหาบัญชีม้าโดยเน้นการสร้างระบบตรวจสอบและป้องกันอาชญากรรมทางการเงินผ่านเทคโนโลยีดิจิทัล หนึ่งในมาตรการหลักคือการพัฒนาฐานข้อมูลร่วมระหว่างหน่วยงานที่เกี่ยวข้อง เช่น สำนักงาน กสทช. และธนาคารแห่งประเทศไทย เพื่อเชื่อมโยงข้อมูลหมายเลขโทรศัพท์และบัญชีธนาคารที่ต้องสงสัยว่ามีการใช้งานในทางที่ผิด กระทรวงยังมีบทบาทในการส่งเสริมการพัฒนาระบบการยืนยันตัวตนดิจิทัล (Digital ID) ที่ช่วยเพิ่มความปลอดภัยและลดความเสี่ยงในการเปิดบัญชีธนาคารปลอม

นอกจากนี้ กระทรวงดิจิทัลฯ ยังมุ่งเน้นการให้ความรู้และสร้างความตระหนักแก่ประชาชนเกี่ยวกับความเสี่ยงของบัญชีม้าและอาชญากรรมทางการเงิน โดยใช้สื่อดิจิทัลและแพลตฟอร์มออนไลน์ในการเผยแพร่ข้อมูล ทั้งยังร่วมมือกับหน่วยงานด้านกฎหมายเพื่อปรับปรุงกฎระเบียบและมาตรการบังคับใช้กฎหมายในการจัดการบัญชีม้าอย่างเข้มงวด

2.5.4 แนวปฏิบัติในการจัดการปัญหาบัญชีม้าของสำนักงานตำรวจแห่งชาติ

สำนักงานตำรวจแห่งชาติ (สตช.) มีบทบาทสำคัญในการปราบปรามปัญหาบัญชีม้า โดย สตช. เป็นผู้รับแจ้งความทั้งกรณีที่ถูกนำชื่อไปใช้เป็นบัญชีม้าและกรณีถูกโกงออนไลน์ และเป็นหน่วยงานที่ดำเนินการสืบสวนและจับกุมผู้กระทำความผิดที่เกี่ยวข้องกับการใช้บัญชีม้าเพื่อกิจกรรมที่ผิดกฎหมาย เช่น การฉ้อโกงออนไลน์ นอกจากนี้ ยังร่วมมือกับหน่วยงานต่าง ๆ เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สถาบันการเงิน และสำนักงานป้องกันและปราบปรามการฟอกเงิน เพื่อแลกเปลี่ยนข้อมูลและประสานงานในการระงับบัญชีม้าและตัดเส้นทางการเงินของมิจฉาชีพ

นอกจากนี้ สำนักงานตำรวจแห่งชาติยังมีการดำเนินการเชิงรุกในการจัดตั้งศูนย์รับแจ้งความออนไลน์[7] เพื่ออำนวยความสะดวกให้ประชาชนสามารถรายงานเหตุการณ์ที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีได้อย่างรวดเร็วและมีประสิทธิภาพ และจัดตั้งเว็บไซต์ “ฉลาดโอน[8]” และ “เช็กก่อน[9]” เพื่อให้ประชาชนตรวจสอบและแจ้งเบาะแสบัญชีต้องสงสัยอีกด้วย

[7] ศูนย์รับแจ้งความออนไลน์สามารถเข้าถึงได้ที่: https://thaipoliceonline.com/

[8] เว็บไซต์ฉลาดโอนสามารถเข้าถึงได้ที่: https://www.chaladohn.com/

[9] เว็บไซต์เช็กก่อนสามารถเข้าถึงได้ที่: https://www.checkgon.com/

2.5.5 แนวปฏิบัติในการจัดการปัญหาบัญชีม้าของสำนักงานป้องกันและปราบปรามการฟอกเงิน

สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) มีบทบาทสำคัญในการจัดการปัญหาบัญชีม้า โดยดำเนินการตรวจสอบและระงับบัญชีที่เกี่ยวข้องกับกิจกรรมผิดกฎหมาย เช่น การฟอกเงินและการฉ้อโกงออนไลน์ รวมถึงกระบวนการโอนเงินคืนผู้เสียหาย (ปปง., n.d.) โดยปปง. จะทำงานร่วมกับสถาบันการเงินอย่างใกล้ชิดทั้งในการตรวจจับและระงับบัญชีม้าอย่างทันท่วงที โดยบัญชีที่ถูกระงับจะสามารถทำธุรกรรมได้ที่สาขาธนาคารเท่านั้นและสามารถยื่นเอกสารรายการเดินบัญชีย้อนหลังเพื่อยืนยันว่าไม่มีส่วนเกี่ยวข้องกับการกระทำผิดต่อสำนักงานตำรวจแห่งชาติ เพื่อหยุดการระงับบัญชีดังกล่าวได้ (ปปง., 2566)

โดยก่อนเดือนเมษายนปี พ.ศ. 2567 ที่ผ่านมา ปปง. ระงับบัญชีม้าแล้วจำนวนกว่า 7 แสนบัญชี และกำหนดมาตรการและเงื่อนไขการเปิดบัญชีใหม่โดยเพิ่มกระบวนการพิสูจน์ทราบข้อเท็จจริง Customer Due Diligence หรือ CDD ในกลุ่มที่มีความเสี่ยงสูงเพิ่มขึ้น (ปปง., 2567)

ปปง. มีบทบาทสำคัญในการรวบรวมรายชื่อผู้กระทำความผิด และจัดทำฐานข้อมูลรายชื่อ ‘บุคคลที่มีรายชื่อเสี่ยงสูงต่อการฟอกเงิน การสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ ขยายอาวุธที่มีอานุภาพทำลายล้างสูงในกรณีบุคคลผู้ที่เกี่ยวข้องกับการกระทำความผิดมูลฐานหรือเป็นเจ้าของ บัญชีเงินฝากธนาคารที่ถูกใช้ในการกระทำความผิดมูลฐาน รหัส HR-03’ เพื่อให้สถาบันทางการเงิน ใช้ตรวจสอบข้อมูลของลูกค้า และป้องกันบัญชีม้าต่อไป

ฐานข้อมูลดังกล่าวแบ่งกลุ่มรายชื่อเป็น 2 ประเภท ประเภทแรก เป็นรายชื่อเจ้าของบัญชีที่ถูกดำเนินคดีตามกฎหมายอาญาแล้ว (HR-03-1) และประเภทที่ 2 เป็นรายชื่อเจ้าของบัญชีเงินที่ถูกใช้ในการกระทำความผิด แต่ยังไม่มีการดำเนินคดีตามกฎหมายอาญา (HR-03-2)

สถาบันการเงินจะจำกัดช่องทางการทำธุรกรรมออนไลน์ของบัญชีตามฐานข้อมูลรายชื่อทั้ง 2 ประเภทข้างต้น กล่าวคือ เจ้าของบัญชีหรือลูกค้าที่มีรายชื่อปรากฏในฐานข้อมูลดังกล่าว จะสามารถทำธุรกรรมได้ที่สาขาธนาคารเท่านั้น ทั้งนี้ เจ้าของบัญชีสามารถยื่นรายการเดินบัญชีธนาคารย้อนหลัง 6 เดือน ให้กองบัญชาการตำรวจสืบสวนอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ เพื่อตรวจสอบข้อมูล หากตรวจสอบพบว่ามีข้อมูลและหลักฐานที่สามารถชี้แจงได้ว่าเจ้าของบัญชีไม่มีส่วนเกี่ยวข้องกับการกระทำผิด สำนักงานตำรวจแห่งชาติจะแจ้งกลับไปยังสถาบันการเงิน เพื่อเปิดให้สามารถทำธุรกรรมออนไลน์ได้ (ปปง., 2566)

โดย ปปง. มีหน้าที่ดำเนินการคืนเงินให้ผู้เสียหาย โดยผู้เสียหายจะต้องเขียนคำร้องตาม แบบคำขอรับทรัพยสินที่ถูกยึดและ/หรืออายัดคืน (แบบ ปปง.บส. 04) จากนั้น สำนักงาน ปปง. จะโอนเงินเข้าบัญชีธนาคารของผู้เสียหาย (ปปง., n.d.)

นอกจากนี้ ปปง. เป็นหนึ่งในหน่วยงานที่เสนอร่างกฎหมายแก้ไขเพิ่มเติมพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 กำหนดให้สถาบันการเงินมีหน้าที่อายัดบัญชีที่ตรวจพบว่ารับโอนเงินที่เกี่ยวกับการกระทำความผิดหรือเป็นบัญชีม้า และกำหนดความผิดอาญาฐานรับจ้างเปิดบัญชีม้า (MGR Online, 2567)

2.6 แพลตฟอร์มที่เกี่ยวข้องกับการจัดการปัญหาบัญชีม้า

แม้ว่าแต่ละองค์กรจะมีบทบาทหน้าที่อย่างชัดเจนในการแก้ไขปัญหาบัญชีม้า แต่การทำงานแยกส่วนกันอาจทำให้เกิดความล่าช้าและไม่สามารถแก้ปัญหาได้อย่างทันท่วงที ดังนั้น ภายใต้พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีจึงกำหนดให้มีการตั้งแพลตฟอร์มในการทำงานร่วมกันทั้งในการร้องเรียนและการแบ่งปันข้อมูล ดังนี้

2.6.1 ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์

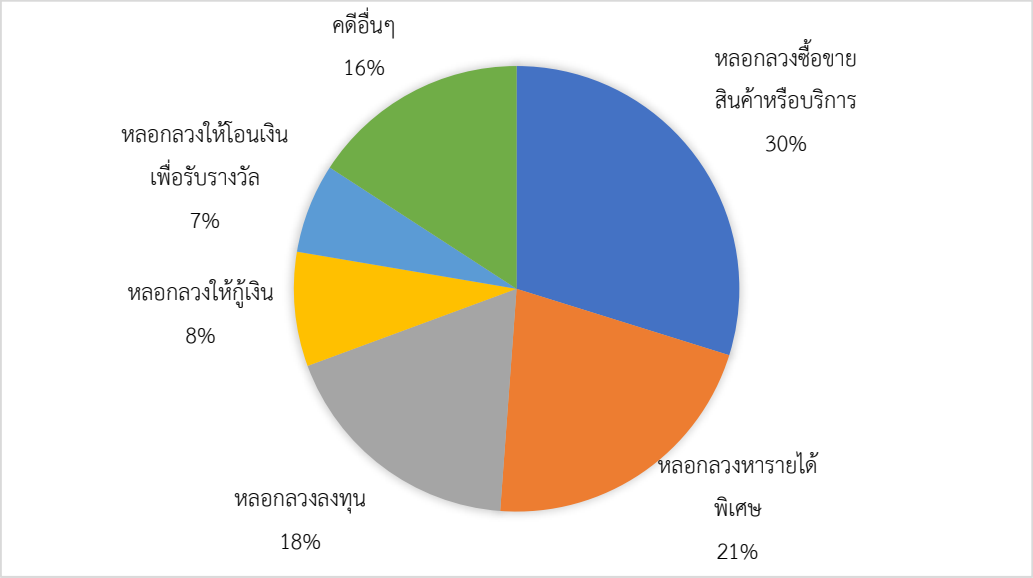
ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (Anti Online Scam Operation Center ; AOC) ถือเป็นเจ้าภาพในการเชื่อมโยงข้อมูล เช่น ข้อมูลบัญชีม้า ซิมม้า ข้อมูล URL/Line ของเว็บพนัน หรือข้อมูลอื่น ๆ ตามที่ศูนย์ AOC ร้องขอ และมีการพัฒนาระบบให้มีความมั่นคงปลอดภัยจาก กสทช., ธปท., สมาคมธนาคารไทย, กลต., ปปง., DSI และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ในรูปแบบ One stop service เพื่อรับมือปัญหาอาชญากรรมออนไลน์ (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2566)

เป้าหมายของศูนย์ AOC ได้แก่ ระงับหรืออายัดบัญชีของคนร้ายให้ผู้เสียหาย ติดตามสถานะและแก้ไขปัญหาให้ผู้เสียหาย เร่งการคืนเงินให้ผู้เสียหาย รวมไปถึงการใช้เทคโนโลยีดิจิทัลช่วยงานบูรณาการข้อมูลและร่วมทำงานทันทีทุกหน่วยงานเกี่ยวข้อง เมื่อได้รับแจ้งจากผู้เสียหาย

ภายในศูนย์ AOC มีการจัดตั้งสำนักงานดูแลและวางแผนการสื่อสารในเชิงรุก (war room) เพื่อแก้ปัญหาหลอกลวงออนไลน์แบบเชิงรุก โดยสามารถอายัดบัญชีการเงินได้ ใน 1 ชั่วโมง นับจากเวลาที่รับแจ้งเรื่องจากผู้เสียหาย ด้วยการใช้เทคโนโลยี Intelligent Assistant (IA) และ Intelligence based platform เพื่อประมวลผลข้อมูลขนาดใหญ่ (Big Data) วิเคราะห์ข้อมูลทางการเงิน ข้อมูลการใช้โทรศัพท์ ข้อมูลธุรกรรมต้องสงสัย (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2566)

โดยผลการดำเนินงานของ ศูนย์ AOC 1441 ตั้งแต่วันที่ 1 พฤศจิกายน 2566 ถึงวันที่ 31 มีนาคม 2567 พบว่าภายในระยะเวลา 6 เดือน ศูนย์ AOC มีสายโทรเข้า 1441 จำนวน 504,917 สาย ระงับบัญชีธนาคาร จำนวน 96,397 บัญชี โดยแบ่งตามประเภทคดีสูงสุด 5 ประเภท ได้แก่ หลอกลวงซื้อขายสินค้าหรือบริการ 28,742 บัญชี คิดเป็นร้อยละ 29.81 หลอกลวงหารายได้พิเศษ 20,589 บัญชี คิดเป็นร้อยละ 21.36 หลอกลวงลงทุน 17,543 บัญชี คิดเป็นร้อยละ 18.20 หลอกลวงให้กู้เงิน 7,995 บัญชี คิดเป็นร้อยละ 8.29 และหลอกลวงให้โอนเงินเพื่อรับรางวัล 6,262 บัญชี คิดเป็นร้อยละ 6.50 และคดีอื่นๆ 15,266 บัญชี คิดเป็นร้อยละ 15.84 (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2567)

แผนภาพที่ 9 จำนวนบัญชีที่ศูนย์ AOC ดำเนินการระงับบัญชี ตั้งแต่วันที่ 1 พฤศจิกายน 2566 ถึง วันที่ 31 มีนาคม 2567



ที่มา : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

2.6.2 ระบบแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

ระบบ Central Fraud Registry (CFR) พัฒนาโดย บริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ จำกัด (NITMX) เป็นระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าที่เกี่ยวข้องในระหว่างสถาบันการเงิน (สมาคมธนาคารไทย, 2023) โดยหน่วยงานที่เกี่ยวข้อง เช่น สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) สำนักงานตำรวจแห่งชาติ (สตช.) และสถาบันทางการเงินจะร่วมกันนำรายชื่อของผู้กระทำความผิดเข้าระบบ CFR เพื่อใช้ในการสืบสวนสอบสวนและอายัดบัญชีของผู้ต้องสงสัย มาใช้ข้ามธนาคาร เพื่อดำเนินการกับบัญชีต้องสงสัยได้ครอบคลุมและรวดเร็วขึ้น นอกจากนี้ CFR ยังเป็นฐานข้อมูลที่สำคัญที่ช่วยให้ธนาคารสมาชิกสามารถประเมินและบริหารความเสี่ยงจากฐานข้อมูลที่ใหญ่ขึ้นได้

ดังนั้น ผู้ที่มีรายชื่อในระบบ CFR จะถูกดำเนินการอย่างเข้มงวด เช่น พิจารณาระงับการใช้งานบัญชีในรายชื่อนั้นทั้งหมดทันที โดยธนาคารพาณิชย์ทุกแห่งได้เริ่มแลกเปลี่ยนข้อมูลข้ามธนาคารผ่านระบบ CFR ตั้งแต่วันที่ 1 สิงหาคม 2567 (ธปท., 2567)

2.7 แนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินในต่างประเทศ

คณะวิจัยสำรวจแนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินในต่างประเทศ จำนวน 5 ประเทศ ได้แก่ สหรัฐอเมริกา สิงคโปร์ อินโดนีเซีย ฟิลิปปินส์ และบราซิล โดยสองประเทศแรกจัดอยู่ในกลุ่มประเทศที่มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ดี (best practice) และสามประเทศหลังจัดอยู่ในกลุ่มประเทศที่มีบริบท และเศรษฐกิจใกล้เคียงกับประเทศไทย

ทั้งนี้ ในปี 2567 สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union) ได้จัดอันดับดัชนีความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index) จากการประเมินทั้งหมด 194 ประเทศ (International Telecommunication Union, 2024) พบว่า สหรัฐอเมริกา สิงคโปร์ อินโดนีเซีย และบราซิล มีคะแนนอยู่ในกลุ่มประเทศที่ควรยกเป็นต้นแบบด้านความปลอดภัยไซเบอร์ หรือเทียร์ 1 และฟิลิปปินส์มีคะแนนอยู่ในกลุ่มประเทศที่มีความก้าวหน้าด้านความมั่นคงปลอดภัยไซเบอร์ หรือเทียร์ 2 โดยมีรายละเอียดดังแสดงในตารางที่ 4

ตารางที่ 4 อันดับดัชนีความมั่นคงปลอดภัยไซเบอร์

ประเทศ	คะแนน (เต็ม 100)	กลุ่มประเทศ
สหรัฐอเมริกา	99.86	ประเทศที่ควรยกเป็นต้นแบบด้านความปลอดภัยไซเบอร์
สิงคโปร์	99.86	
อินโดนีเซีย	98.82	
บราซิล	96.38	
ไทย	*99.22*	
ฟิลิปปินส์	93.49	ประเทศที่มีความก้าวหน้าด้านความมั่นคงปลอดภัยไซเบอร์

ที่มา : สหภาพโทรคมนาคมระหว่างประเทศ

คณะวิจัยได้สรุปแนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินของทั้ง 5 ประเทศ โดยมีรายละเอียด ดังนี้

2.7.1 แนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินในสหรัฐอเมริกา

ในสหรัฐอเมริกา สภาการตรวจสอบสถาบันการเงินแห่งรัฐบาลสหรัฐอเมริกา (The Federal Financial Institutions Examination Council : FFIEC) ซึ่งเป็นองค์กรที่มีบทบาทในการกำหนดหลักการมาตรฐาน และการรายงานข้อมูลที่เป็นรูปแบบเดียวกันสำหรับการกำกับดูแลสถาบันการเงินในสหรัฐอเมริกา ได้จัดทำคู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Examination Handbook) สำหรับสถาบันการเงิน เพื่อเป็นแนวทางในการระบุ ประเมิน และบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Gatekeeper, n.d.) โดยมีการจัดทำแนวทางสำหรับผู้ตรวจสอบและสถาบันการเงินที่ครอบคลุมในประเด็นต่าง ๆ อาทิ

- การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการควบคุมภายใน เพื่อให้สามารถบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ และสามารถผนวกการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นส่วนหนึ่งของการบริหารความเสี่ยงของสถาบันการเงิน
- การพัฒนาและบำรุงรักษาระบบ เพื่อไม่ให้เกิดช่องว่างด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

- การจัดทำแผนจัดการความต่อเนื่องทางธุรกิจที่คำนึงถึงความปลอดภัยด้านเทคโนโลยีสารสนเทศ การคุ้มครองผู้บริโภค และสอดคล้องกับกฎระเบียบที่เกี่ยวข้อง
- แนวทางป้องกันความปลอดภัยของข้อมูล ทั้งในกระบวนการสร้าง การรวบรวม การจัดเก็บ การใช้งาน การส่งผ่าน และการกำจัดข้อมูลที่ละเอียดอ่อน ซึ่งให้ความสำคัญกับการรักษาความลับของข้อมูล (confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และความพร้อมใช้งาน (availability)
- แนวทางตรวจสอบด้านการออกแบบระบบและโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ รวมถึงแนวทางการตรวจสอบและจัดการความเสี่ยงระบบการชำระเงินรายย่อย (retail payment systems) และระบบการชำระเงินมูลค่าสูง (wholesale payment systems) เช่น ระบบการชำระเงินระหว่างธนาคาร เป็นต้น
- แนวทางในการกำกับและตรวจสอบผู้ให้บริการด้านเทคโนโลยีสารสนเทศภายนอก (outsourcing technology services) และผู้ให้บริการเทคโนโลยี (supervision of technology service providers) ในกรณีที่สถาบันการเงินต้องใช้บริการเหล่านี้

ทั้งนี้ FFIEC ให้ความสำคัญกับการยกระดับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง โดยในปี พ.ศ. 2557 FFIEC ได้จัดทำ Cybersecurity Assessment Tool (CAT) เป็นเครื่องมือสำหรับสถาบันการเงินในการประเมินและเตรียมความพร้อมรับมือความเสี่ยงด้านเทคโนโลยีสารสนเทศ และปัจจุบัน FFIEC ได้ประกาศยกเลิกการใช้เครื่องมือ CAT ภายในวันที่ 31 สิงหาคม พ.ศ. 2568 โดยจะปรับเปลี่ยนไปใช้แนวทางในการประเมินความเสี่ยงใหม่ คือ Cybersecurity Performance Goals ซึ่งถูกพัฒนาโดย Cybersecurity and Infrastructure Security Agency (CISA) โดยแนวทางในการประเมินความเสี่ยงใหม่นี้สามารถใช้ในการบริหาร และลดความเสี่ยงทางจากการโจมตีไซเบอร์ได้กับองค์กรทุกขนาดและทุกอุตสาหกรรม (FFIEC, n.d.)

สำหรับมาตรการในการตอบสนองต่อเหตุการณ์การโจมตีทางไซเบอร์ FFIEC กำหนดขั้นตอนในการดำเนินการเมื่อเกิดเหตุการณ์ (FFIEC, n.d.) ดังนี้

(1) ประเมินลักษณะและขอบเขตของเหตุการณ์ และระบุว่ามีระบบข้อมูลและประเภทของข้อมูลใดบ้างที่ถูกเข้าถึงหรือถูกนำไปใช้ในทางที่ไม่ถูกต้อง

(2) แจ้งให้หน่วยงานกำกับดูแลหลักของสถาบันการเงินทราบอย่างรวดเร็ว เมื่อเกิดเหตุการณ์ที่เกี่ยวข้องกับการเข้าถึงหรือการใช้ข้อมูลลูกค้าที่ละเอียดอ่อนโดยไม่ได้รับอนุญาต หรือเกิดเหตุการณ์ใด ๆ ที่อาจส่งผลกระทบต่อสถาบันการเงินอย่างมีนัยสำคัญ

(3) ปฏิบัติตามข้อบังคับและแนวทางการรายงานเหตุการณ์ความผิดปกติ และตรวจสอบให้แน่ใจว่าได้แจ้งเจ้าหน้าที่หรือหน่วยงานกำกับดูแลได้อย่างทันท่วงที

(4) ดำเนินการขั้นตอนที่เหมาะสมเพื่อลดและควบคุมเหตุการณ์เพื่อป้องกันการเข้าถึงหรือการใช้ข้อมูลโดยไม่ได้รับอนุญาตในอนาคต

(5) แจ้งลูกค้าโดยเร็วที่สุดเมื่อมีการตรวจสอบแล้วว่ามีการนำข้อมูลลูกค้าที่ละเอียดอ่อนไปใช้ในทางที่ไม่ถูกต้องหรือมีความเป็นไปได้ในทางที่เหมาะสม

ในระดับมลรัฐ คณะวิจัยศึกษามาตรการควบคุมความปลอดภัยทางไซเบอร์ในภาคการเงินการธนาคารของมหานครนิวยอร์ก ซึ่งเป็นเมืองศูนย์กลางการเงินโลกอันดับที่ 1 ตามการจัดอันดับของดัชนีเมืองศูนย์กลางการเงินโลก (The Global Financial Centres Index : GFCI) ประจำปี พ.ศ. 2566 (THE STANDARD, 2023)

ทั้งนี้ ในมหานครนิวยอร์ก กรมบริการทางการเงินแห่งรัฐนิวยอร์ก (The Department of Financial Services : DFS) เป็นหน่วยงานกำกับดูแลสถาบันการเงินหรือผู้ให้บริการทางการเงินอื่น ๆ เช่น สหกรณ์เครดิต บริษัทประกันภัย หรือบริษัทการลงทุน เป็นต้น ซึ่งสถาบันการเงินหรือผู้ให้บริการทางการเงินเหล่านี้ต้องดำเนินการมาตรการความปลอดภัยทางไซเบอร์ตาม NYCRR Part 500 (DFS, n.d.) ซึ่งเป็นข้อบังคับด้านความปลอดภัยทางไซเบอร์ ที่มุ่งเน้นการทำความเข้าใจความเสี่ยงที่เฉพาะเจาะจงในแต่ละองค์กร การสร้างโปรแกรมที่มีความปลอดภัยทางไซเบอร์เพื่อป้องกันความเสี่ยงจากการถูกโจมตี และการสร้างความโปร่งใสและความรับผิดชอบขององค์กรในการดำเนินงานที่คำนึงถึงความปลอดภัยทางไซเบอร์

NYCRR Part 500 ถูกประกาศใช้ครั้งแรกเมื่อเดือนมีนาคม พ.ศ. 2560 เพื่อป้องกันการโจมตีทางไซเบอร์และการเข้าถึงข้อมูลอย่างไม่ถูกต้องในภาคบริการทางการเงินของรัฐนิวยอร์ก ต่อมาในเดือนพฤศจิกายน พ.ศ. 2566 ได้มีการปรับปรุงกฎระเบียบเพิ่มเติม โดยให้ความสำคัญกับโปรแกรมการรักษาความปลอดภัยทางไซเบอร์ การกำกับดูแล และแนวทางการรายงานของหน่วยงานที่เกี่ยวข้อง และเริ่มมีผลบังคับใช้ตั้งแต่วันที่ 29 เมษายน พ.ศ. 2567

ทั้งนี้ สาระสำคัญของข้อบังคับดังกล่าว (Secureframe, 2024) คือ องค์กรต้องมีนโยบายความปลอดภัยทางไซเบอร์ ซึ่งต้องครอบคลุมทั้งนโยบายความปลอดภัยของข้อมูล นโยบายจัดการความเสี่ยง นโยบายความปลอดภัยจากผู้ให้บริการภายนอก แผนการตอบสนองต่อเหตุการณ์โจมตีทางไซเบอร์และแผนความต่อเนื่องทางธุรกิจหากเกิดเหตุดังกล่าว

นอกจากนี้ องค์กรต้องมีหน่วยงานกำกับดูแลหรือผู้รับผิดชอบด้านความปลอดภัยทางไซเบอร์ ซึ่งต้องมีความเชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ที่เพียงพอ ทำหน้าที่ในการพัฒนาและควบคุมดูแลโปรแกรมความปลอดภัยทางไซเบอร์ รวบรวมและทบทวนรายงานการจัดการเกี่ยวกับความปลอดภัยทางไซเบอร์ ตรวจสอบและอนุมัตินโยบายความปลอดภัยทางไซเบอร์ของหน่วยงานที่เกี่ยวข้อง และจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินการด้านความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ

องค์กรต้องมีมาตรการรักษาความปลอดภัยทางไซเบอร์ที่เข้มงวด เช่น มาตรการการตรวจสอบสิทธิการเข้าถึงข้อมูล มาตรการการเข้ารหัสข้อมูล มาตรการความปลอดภัยของระบบและเครือข่าย เป็นต้น รวมถึงการฝึกอบรมให้บุคลากรในองค์กรตระหนักถึงความปลอดภัยทางไซเบอร์

องค์กรต้องมีการประเมินความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นอย่างสม่ำเสมอ ต้องจัดให้มีโปรแกรมรักษาความปลอดภัยทางไซเบอร์ เพื่อป้องกันการรั่วไหลของข้อมูล สามารถป้องกัน ตอบสนองและกู้คืนข้อมูลจากเหตุการณ์โจมตีทางไซเบอร์ได้ ทั้งนี้ องค์กรต้องทดสอบการเจาะระบบเป็นประจำทุกปี และประเมินช่องโหว่ทุก ๆ สองปี เพื่อทดสอบประสิทธิภาพของโปรแกรมด้านความปลอดภัยทางไซเบอร์ และต้องจัดให้มีระบบบันทึกเหตุการณ์ความผิดปกติทางไซเบอร์ และต้องเก็บบันทึกนี้ไว้เป็นระยะเวลาขั้นต่ำ 5 ปี รวมทั้งต้องแจ้งให้ NYDFS ทราบถึงเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ทั้งขององค์กรเองและเหตุการณ์ที่เกิดขึ้นกับผู้ให้บริการภายนอก ภายใน 72 ชั่วโมงหลังจากระบุเหตุการณ์ดังกล่าวได้

2.7.2 แนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินในสิงคโปร์

ธนาคารกลางสิงคโปร์ (Monetary Authority of Singapore : MAS) จัดทำแนวทางการบริหารความเสี่ยงด้านเทคโนโลยี (Technology Risk Management : TRM) ในปี 2564 เพื่อยกระดับความสามารถของสถาบันการเงินในการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบหลังเกิดเหตุภัยคุกคามทางไซเบอร์ ซึ่งสถาบันการเงินต้องดำเนินการครอบคลุมทั้งมาตรการป้องกันและมาตรการจัดการปัญหาเมื่อเกิดเหตุ (Monetary Authority of Singapore, 2021) ดังนี้

ในการป้องกันภัยคุกคามทางไซเบอร์ สถาบันการเงินต้องติดตามข่าวสารหรือข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ให้เป็นปัจจุบันอยู่เสมอ เพื่อนำข้อมูลมาใช้ประเมินความเสี่ยง ร่วมกับการตรวจสอบและเฝ้าระวังเหตุการณ์ทางไซเบอร์ที่อาจเกิดขึ้น ต้องมีการวิเคราะห์พฤติกรรมของผู้ใช้ เพื่อตรวจจับและวิเคราะห์เหตุการณ์ไซเบอร์แบบเป็นปัจจุบัน (real time) รวมทั้งควรจัดตั้งศูนย์ปฏิบัติการด้านความปลอดภัย (Security Operations Centre : SOC) เพื่อทำหน้าที่ติดตามและจัดการปัญหาด้านความปลอดภัยไซเบอร์ในองค์กร

สถาบันการเงินต้องประเมินความเปราะบางของระบบ (vulnerability assessment) และทดสอบเจาะระบบ (penetration testing) สำหรับบริการทางการเงินออนไลน์ในสภาพแวดล้อมการใช้งานจริงอย่างน้อยปีละ 1 ครั้ง เพื่อให้ได้การประเมินความเข้มแข็งของมาตรการรักษาความปลอดภัยอย่างถูกต้อง

นอกจากนี้ เพื่อให้สถาบันการเงินจัดการแก้ไขปัญหาเมื่อเกิดเหตุได้อย่างมีประสิทธิภาพ สถาบันการเงินต้องมีแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ที่สามารถตรวจพบและตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็ว โดยแผนดังกล่าวต้องระบุวิธีการสื่อสาร การประสานงาน การตอบสนองต่อภัยคุกคามทางไซเบอร์ แผนการกู้คืนระบบ (disaster recovery plan) ที่สามารถกู้คืนระบบให้สามารถกลับมาใช้งานได้ตามปกติในระยะเวลาที่เหมาะสม ทั้งนี้ สถาบันการเงินควรมีการทบทวนแผนการตอบสนองดังกล่าวอย่างน้อยปีละ 1 ครั้ง โดยนำข้อมูลจากเหตุการณ์ที่เคยเกิดขึ้นและบทเรียนที่ได้รับมาใช้ในการทบทวนและปรับปรุงแผนดังกล่าวด้วย

อย่างไรก็ตาม นอกจากธนาคารกลางสิงคโปร์ยังมีหน่วยงานภาครัฐที่สนับสนุนและดูแลเรื่องภัยคุกคามไซเบอร์ ได้แก่ หน่วยงานความมั่นคงปลอดภัยทางไซเบอร์แห่งสิงคโปร์ (Cyber Security Agency of Singapore : CSA) และ กองกำลังตำรวจสิงคโปร์ (Singapore Police Force : SPF) ซึ่งเป็นหน่วยงานที่มีการดำเนินงานร่วมกับองค์กรระดับนานาชาติ เช่น INTERPOL และหน่วยงานในภูมิภาค ASEAN เพื่อปรับปรุงการรับมือกับภัยไซเบอร์ รวมถึงการเผยแพร่ข้อมูลและคำแนะนำผ่าน Singapore Computer Emergency Response Team (SingCERT) (Chambers and Partners, 2024)

2.7.3 แนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินในอินโดนีเซีย

อินโดนีเซียเป็นประเทศที่มีประชากรใช้อินเทอร์เน็ตจำนวนมาก และมีการเติบโตทางเศรษฐกิจดิจิทัลอย่างรวดเร็ว ส่งผลให้รัฐบาลอินโดนีเซียให้ความสำคัญกับการพัฒนามาตรการความปลอดภัยทางไซเบอร์อย่างจริงจัง แต่ยังพบความท้าทายในการบริหารจัดการด้านความมั่นคงไซเบอร์ (องค์การรักษาความปลอดภัยฝ่ายพลเรือน สำนักข่าวกรองแห่งชาติ, 2024)

สำนักงานความมั่นคงปลอดภัยทางไซเบอร์และการเข้ารหัสแห่งชาติ (Badan Siber dan Sandi Negara : BSSN) ซึ่งเป็นหน่วยงานป้องกันความปลอดภัยทางไซเบอร์ของอินโดนีเซียรายงานว่า ในปี 2566 มีการโจมตีทางไซเบอร์เกิดขึ้นมากกว่า 361 ล้านครั้ง ซึ่งภาคการเงินเป็นเป้าหมายที่ถูกโจมตีมากที่สุด (Asia Pacific Solidarity Network, 2023)

BSSN เป็นหน่วยงานหลักในการจัดทำและขับเคลื่อนยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ พ.ศ. 2563-2567 (National Cyber Security Strategy 2020-2024) ซึ่งมีเป้าหมายในการยกระดับความสามารถในการป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามทางไซเบอร์ การสร้างระบบนิเวศด้านความปลอดภัยทางไซเบอร์ที่แข็งแกร่ง การส่งเสริมการพัฒนาอุตสาหกรรมความปลอดภัยทางไซเบอร์ภายในประเทศ และการสร้างความร่วมมือระหว่างประเทศด้านความมั่นคงปลอดภัยทางไซเบอร์ (Putra & Herdiyanti, 2021)

ในภาคการเงิน หน่วยงานกำกับดูแลด้านการเงินของอินโดนีเซีย (Indonesian Financial Services Authority : OJK) มีการจัดทำแนวทางการรักษาความปลอดภัยทางไซเบอร์ในภาคการเงิน (Cybersecurity Guidelines for Financial Sector Technology Innovation : FSTI) ซึ่งมุ่งเน้นการสร้างกรอบการดำเนินงานด้านไซเบอร์ที่มั่นคงและปลอดภัยในภาคการเงิน เพื่อปกป้อง รักษาข้อมูล และสร้างเสถียรภาพให้การทำธุรกรรมออนไลน์ (OJK, 2024)

FSTI กำหนดมาตรการจัดการความเสี่ยงครอบคลุมตั้งแต่กระบวนการประเมินความเสี่ยงด้านไซเบอร์ ซึ่งสถาบันการเงินต้องดำเนินการเป็นรายไตรมาส หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในโครงสร้างระบบ มีการประเมินช่องโหว่ (vulnerability assessment) การทดสอบเจาะระบบ (penetration test) มีมาตรการลดความเสี่ยง เช่น การติดตั้งไฟร์วอลล์ (firewall) การเข้ารหัสข้อมูล (encryption) และการควบคุมการเข้าถึง (access control) ต้องมีมาตรการจัดการความเสี่ยง (risk treatment) ที่เหมาะสม

กับระดับความเสี่ยง และมีการติดตามประสิทธิผลของมาตรการรักษาความปลอดภัยอย่างต่อเนื่องและสม่ำเสมอ รวมถึงการอบรมและให้ความรู้เกี่ยวกับการป้องกันภัยทางไซเบอร์ให้กับพนักงานอย่างต่อเนื่อง

นอกจากนี้ สถาบันการเงินต้องมีหน่วยงานตอบสนองต่อเหตุการณ์ (incident response team) และจัดทำแผนการดำเนินการที่ชัดเจน เพื่อให้สามารถตรวจจับและจัดการเหตุการณ์ได้ทันทีเพื่อลดความเสียหายและความสูญเสีย ต้องมีแผนจำกัดความเสียหาย (containment) การกำจัดมัลแวร์ (eradication) และการกู้คืนระบบ (recovery) ให้กลับมาใช้งานได้อย่างปลอดภัย รวมถึงควรมีการทบทวนและวิเคราะห์บทเรียนจากเหตุการณ์ที่เกิดขึ้น เพื่อนำไปปรับปรุงแผนการตอบสนองเพิ่มเติม พร้อมทั้งแบ่งปันข้อมูลเชิงลึกกับหน่วยงานที่เกี่ยวข้องเพื่อป้องกันเหตุการณ์ปัญหาในอนาคต

อย่างไรก็ตาม แนวทางการรักษาความปลอดภัยทางไซเบอร์ในภาคการเงินของอินโดนีเซียยังไม่มีการกำหนดกรอบเวลาที่ชัดเจนสำหรับการแก้ไขเหตุการณ์

2.7.4 แนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินในฟิลิปปินส์

รัฐบาลฟิลิปปินส์จัดทำแผนความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (National Cybersecurity Plan : NCSP) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นอย่างต่อเนื่อง (OpenGov Asia, 2017) รวมถึงการเสริมสร้างความแข็งแกร่งของระบบป้องกันทางไซเบอร์ของประเทศ (Philippine government, 2024)

แผน NCSP มุ่งเน้นการปกป้องโครงสร้างพื้นฐานที่สำคัญของประเทศ โดยเฉพาะอย่างยิ่งในภาคส่วนที่มีความสำคัญ เช่น การโทรคมนาคม พลังงาน การธนาคาร และการบริการของรัฐบาล (Digital Watch newsletters, 2024) (Magno et al., 2021) อีกทั้งเน้นย้ำถึงความสำคัญของการสร้างความร่วมมือระหว่างภาครัฐและภาคเอกชน ซึ่งถือเป็นกุญแจสำคัญในการบรรลุเป้าหมายด้านความมั่นคงปลอดภัยทางไซเบอร์ด้วย

แผน NCSP ประกอบด้วยการพัฒนาและปรับปรุงกรอบกฎหมายและนโยบายที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ การเสริมสร้างขีดความสามารถของบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ และการส่งเสริมการวิจัยและพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยทางไซเบอร์ (OpenGov Asia, 2017)

รวมถึงให้ความสำคัญกับการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ในหมู่ประชาชนทั่วไป และการส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ในองค์กรทั้งภาครัฐและเอกชน (OpenGov Asia, 2017)

สำหรับแนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ในภาคการเงิน ธนาคารกลางฟิลิปปินส์ (Bangko Sentral ng Pilipinas : BSP) จัดทำแนวทางการบริหารความเสี่ยงด้านเทคโนโลยี (Information Technology Risk Management : ITRM) ในปี 2561 เพื่อกำกับดูแลสถาบันการเงินครอบคลุมทั้งมาตรการป้องกันและมาตรการจัดการปัญหาเมื่อเกิดเหตุ (Bangko Sentral ng Pilipinas, 2018) ดังนี้

มาตรการป้องกันภัยไซเบอร์ที่กำหนดโดยธนาคารกลางฟิลิปปินส์ มุ่งเน้นที่การลดความเสี่ยงและเสริมสร้างความปลอดภัยทางไซเบอร์ในสถาบันการเงินที่อยู่ภายใต้การกำกับดูแล โดย BSP ได้กำหนดให้

สถาบันการเงินมีการจัดตั้งกรอบการบริหารความเสี่ยงด้านเทคโนโลยีที่ครอบคลุม (IT Risk Management Framework) ซึ่งประกอบไปด้วยการบริหารจัดการข้อมูล การกำหนดมาตรฐานและขั้นตอนการดำเนินงานด้านความปลอดภัย การตรวจสอบความปลอดภัยอย่างสม่ำเสมอ และการเสริมสร้างความตระหนักรู้ในองค์กร นอกจากนี้ BSP ยังได้กำหนดให้มีการบริหารจัดการบุคลากรด้าน IT อย่างเหมาะสม เช่น การฝึกอบรมเพื่อเพิ่มพูนทักษะและความรู้ รวมถึงการบริหารจัดการระบบที่สำคัญให้สอดคล้องกับความซับซ้อนของระบบไอทีของแต่ละสถาบันการเงิน

นอกจากนี้ BSP กำหนดสถาบันการเงินเสริมสร้างความพร้อมและความสามารถในการรับมือเมื่อเกิดเหตุการณ์ภัยไซเบอร์ โดยกำหนดให้สถาบันการเงินมีแผนรับมือเหตุการณ์ฉุกเฉินด้านไซเบอร์ (Incident Response Plan) ซึ่งครอบคลุมการแจ้งเตือน การตอบสนอง การวิเคราะห์เหตุการณ์ และการฟื้นฟูระบบที่เสียหาย โดย BSP ให้ความสำคัญกับการตรวจสอบและการวิเคราะห์เหตุการณ์อย่างต่อเนื่อง เพื่อระบุจุดอ่อนและแนวทางแก้ไขปัญหาในอนาคต อีกทั้ง BSP ยังเน้นการสื่อสารและการรายงานเหตุการณ์ต่อหน่วยงานกำกับดูแลในเวลาที่กำหนด เพื่อช่วยลดผลกระทบที่อาจจะเกิดต่อผู้บริโภคอีกด้วย

2.7.5 แนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินในบราซิล

ธนาคารกลางบราซิล (Banco Central do Brasil : BCB) จัดทำมติ Resolution BCB 85/2021 ซึ่งเป็นมาตรการความปลอดภัยทางไซเบอร์ในภาคการเงินที่มีความเข้มงวดทั้งในด้านการป้องกันและการจัดการเมื่อเกิดเหตุ รวมถึงการป้องกันปัญหาบัญชีม้า (Money Mule) (Banco Central Do Brazil, 2021)

สาระสำคัญของ Resolution BCB 85/2021 คือ การกำหนดให้สถาบันการเงินมีนโยบายความปลอดภัยทางไซเบอร์ที่เหมาะสมกับขนาดของสถาบันการเงิน ความเสี่ยงด้านไซเบอร์ที่อาจเกิดขึ้นและความซับซ้อนของผลิตภัณฑ์และบริการที่นำเสนอ สถาบันการเงินต้องมีการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต มีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ การจัดทำแผนการตอบสนองต่อเหตุการณ์ และการจัดการความปลอดภัยของข้อมูลภายนอก เช่น การใช้ระบบคลาวด์และการประมวลผลข้อมูลจากภายนอก นอกจากนี้ สถาบันการเงินยังต้องสร้างวัฒนธรรมความปลอดภัยไซเบอร์ในองค์กร โดยจัดให้มีการฝึกอบรมและประเมินผลการทำงานของพนักงานเป็นระยะ เพื่อให้พนักงานมีความรู้และความสามารถในการป้องกันและจัดการกับภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง

2.7.6 สรุปแนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินในต่างประเทศ

จากการทบทวนแนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินข้างต้น พบว่า การจัดทำนโยบายหรือมาตรการป้องกันความปลอดภัยทางไซเบอร์ในแต่ละประเทศ อาจมีรูปแบบแตกต่างกัน เช่น การจัดทำแผนยุทธศาสตร์ของประเทศ การจัดทำกฎหมายหรือมาตรการของหน่วยงานภาครัฐหรือธนาคารกลางในประเทศนั้น ๆ หรืออาจมีหน่วยงานที่เกี่ยวข้องหลายหน่วยงาน

อย่างไรก็ตาม สาระสำคัญของแนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินของทุกประเทศให้ความสำคัญกับการที่สถาบันการเงินต้องมีนโยบายด้านความปลอดภัยไซเบอร์ที่ชัดเจน มีการประเมินความเสี่ยงด้านไซเบอร์ที่อาจเกิดขึ้น มีกระบวนการควบคุมภายในและการตรวจสอบ รวมถึงการบูรณาการความเสี่ยงด้านไซเบอร์เข้าไปเป็นส่วนหนึ่งของความเสี่ยงองค์กร มีแผนจัดการความเสี่ยง/การตอบสนองต่อภัยคุกคามทางไซเบอร์ที่ชัดเจน มีการทบทวนและวิเคราะห์บทเรียนจากเหตุการณ์ที่เกิดขึ้นเพื่อนำไปปรับปรุงแผนการตอบสนองเพิ่มเติม มีการพัฒนาระบบติดตาม/เฝ้าระวัง การทดสอบเจาะระบบ/กู้คืนระบบ

นอกจากนี้ หลายประเทศระบุชัดเจนว่าสถาบันการเงินต้องกำหนดให้มีหน่วยงานรับผิดชอบในการตอบสนองต่อภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมถึงการอบรมให้ความรู้แก่พนักงานของสถาบันการเงิน รวมถึงสร้างความตระหนักให้กับประชาชนถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นด้วย

2.8 แนวปฏิบัติในการจัดการปัญหาบัญชีม้าในต่างประเทศ

2.8.1 แนวปฏิบัติในการจัดการปัญหาบัญชีม้าในสหรัฐอเมริกา

สหรัฐอเมริกามีโครงการ “Money Mule Initiative”[10] เป็นโครงการความร่วมมือหลายหน่วยงานเพื่อหยุดยั้งขบวนการและกิจกรรมการหลอกลวงทางการเงิน ผ่านการดำเนินคดีและยื่นฟ้องแพ่ง หรือการสร้างความตระหนักรู้ให้แก่ประชาชนเพื่อไม่ให้หลงกลมิจฉาชีพ เช่น หน่วยงานตำรวจไปรษณีย์จัดทำใบปลิวเกี่ยวกับบัญชีม้า เพื่อนำไปติดตามสำนักงานไปรษณีย์ทั่วประเทศ การออกประกาศสร้างความตระหนักรู้เรื่อง Money mule ของศูนย์รับเรื่องร้องเรียนอาชญากรรมทางอินเทอร์เน็ตของ FBI (IC3) หรือสำนักงานผู้ตรวจการแผ่นดิน กรมแรงงาน มอบข้อมูลข่าวสารเกี่ยวกับบัญชีม้า ให้แก่หน่วยงานแรงงานของรัฐ เป็นต้น (U.S. Department of Justice, 2021)

สำหรับกรณีถูกมิจฉาหลอกลวงเงิน สมาคมธนาคารอเมริกัน (American Bankers Association) สรุปขั้นตอนการดำเนินการไว้ 3 ขั้นตอน ได้แก่ (1) ผู้เสียหายต้องหยุดติดต่อกับมิจฉาชีพ และหยุดการส่งผ่านใด ๆ ให้แก่กลุ่มมิจฉาชีพ (2) แจ้งให้ธนาคารทราบถึงเหตุการณ์ที่เกิดขึ้น และ (3) แจ้งเรื่องไปที่ The Federal Trade Commission (American Bankers Association , 2020) ได้ที่เว็บไซต์ https://reportfraud.ftc.gov เพื่อให้ผู้เสียหายขอเข้ารับความช่วยเหลือ และทราบถึงการดำเนินการสอบสวนทางกฎหมายที่จะเกิดขึ้นต่อไป (FEDERAL TRADE COMMISSION, n.d.)

[10] Money Mule Initiative เป็นโครงการภายใต้ความร่วมมือระหว่างกระทรวงยุติธรรม (The Department of Justice) สำนักงานสอบสวนกลาง (Federal Bureau of Investigation: FBI) ตำรวจไปรษณีย์ (Postal Inspection Service) และหน่วยงานบังคับใช้กฎหมายของรัฐบาลสหรัฐอเมริกา อีก 5 แห่ง ได้แก่ สำนักงานผู้ตรวจการกระทรวงแรงงาน (Department of Labor Office of Inspector General) กองปฏิบัติการระหว่างประเทศ หน่วยสืบสวนเพื่อความมั่นคงแห่งมาตุภูมิ (U.S. Immigration and Customs Enforcement’s Homeland Security Investigations), สำนักงานผู้ตรวจการสำนักงานบริหารธุรกิจขนาดย่อม (Small Business Administration Office of Inspector General) กรมกิจการลับของสหรัฐอเมริกา (U.S. Secret Service) และผู้ตรวจการกระทรวงการคลังสหรัฐสำหรับการบริหารจัดการภาษี (U.S. Treasury Inspector General for Tax Administration)

2.8.2 แนวปฏิบัติในการจัดการปัญหาบัญชีม้าในสิงคโปร์

ปัญหาบัญชีม้าในประเทศสิงคโปร์ได้รับความสนใจอย่างมาก เนื่องจากมีการใช้บัญชีเหล่านี้ในกิจกรรมอาชญากรรมข้ามชาติสูงมาก โดยเฉพาะการหลอกลวงทางออนไลน์และการฉ้อโกงผ่านแพลตฟอร์มดิจิทัล ทั้งนี้ ในช่วงปี 2563-2565 มีการสืบสวนคดีบัญชีม้ากว่า 19,000 คดี ที่ผ่านมากฎหมายของสิงคโปร์กำหนดให้ต้องพิสูจน์ได้ว่าผู้ถือบัญชีมีส่วนรู้เห็นในกิจกรรมผิดกฎหมายที่เกิดขึ้น จึงจะสามารถดำเนินคดีต่อไปได้ จึงทำให้มีเพียงไม่กี่คดีที่สามารถดำเนินคดีต่อได้ (comply advantage, 2023)

ดังนั้น รัฐบาลสิงคโปร์จึงได้ปรับปรุงกฎหมายให้มีความเข้มงวดมากขึ้น โดยกำหนดให้สามารถดำเนินคดีกับผู้ที่มีส่วนเกี่ยวข้องกับบัญชีม้า แม้ว่าผู้ถือบัญชีอาจไม่มีเจตนาชัดเจนในการมีส่วนร่วมในอาชญากรรม เช่น การแนะนำข้อหาความผิดในการฟอกเงินแบบไม่ระมัดระวัง (Rash Money Laundering) ซึ่งครอบคลุมถึงกรณีที่ผู้ถือบัญชียังคงดำเนินการโอนเงินแม้จะมีข้อสงสัยเกี่ยวกับที่มาของเงินก็ตาม

นอกจากนี้ รัฐบาลสิงคโปร์ยังได้ร่วมมือกับหน่วยงานต่าง ๆ เช่น ศูนย์ต่อต้านการฉ้อโกง (Anti-Scam Centre) เพื่ออายัดบัญชีธนาคารที่เกี่ยวข้องกับการฉ้อโกง โดยเน้นการใช้เทคโนโลยีและข้อมูลเชิงลึกเพื่อตรวจจับพฤติกรรมที่น่าสงสัย รวมถึงการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับความเสี่ยงของการเปิดเผยข้อมูลส่วนบุคคล เช่น รหัสผ่าน Singpass หรือข้อมูลบัญชีธนาคาร ซึ่งเป็นกลยุทธ์สำคัญที่ทำให้บัญชีม้าลดลง

สำหรับการกำหนดโทษของการเป็นบัญชีม้าในสิงคโปร์ มีตั้งแต่โทษปรับและจำคุก ดังนี้

- การฟอกเงินแบบเร่งด่วน (Rash Money Laundering) มีโทษปรับสูงสุด 250,000 ดอลลาร์สิงคโปร์ หรือจำคุกไม่เกิน 5 ปี หรือทั้งจำและปรับ
- การฟอกเงินโดยประมาท (Negligent Money Laundering) มีโทษปรับสูงสุด 150,000 ดอลลาร์สิงคโปร์ หรือจำคุกไม่เกิน 3 ปี หรือทั้งจำและปรับ
- การช่วยเหลือผู้อื่นในการรักษาประโยชน์จากการกระทำผิด (Assisting Another to Retain Benefits from Criminal Conduct) มีโทษปรับสูงสุด 50,000 ดอลลาร์สิงคโปร์ หรือจำคุกไม่เกิน 3 ปี หรือทั้งจำและปรับ

ทั้งนี้ สิงคโปร์ได้พัฒนาระบบการร้องเรียนและติดตามปัญหาผ่านหลายช่องทาง อาทิ

- ศูนย์ต่อต้านการฉ้อโกง (Anti-Scam Centre)[11]: ร่วมมือกับสถาบันการเงินเพื่ออายัดบัญชีที่น่าสงสัยและรวบรวมข้อมูลจากพฤติกรรมของบัญชีม้า
- แอปพลิเคชัน ScamShield[12]: ช่วยบล็อกหมายเลขโทรศัพท์ที่น่าสงสัย และกรองข้อความ SMS ที่อาจเป็นการฉ้อโกง นอกจากนี้ ยังสามารถรายงานหมายเลขโทรศัพท์หรือข้อความที่น่าสงสัยได้ทันทีผ่านแอปพลิเคชัน

[11] ศูนย์ต่อต้านการฉ้อโกงของประเทศสิงคโปร์สามารถเข้าถึงได้ที่: https://www.police.gov.sg/media-room/news/20240109_anti_scam_centre_and_four_partnering_banks_utilize_technology

[12] แอปพลิเคชัน ScamShield ของประเทศสิงคโปร์สามารถเข้าถึงได้ที่: https://www.scamshield.gov.sg/

2.8.3 แนวปฏิบัติในการจัดการปัญหาบัญชีม้าในอินโดนีเซีย

แนวทางการรักษาความปลอดภัยทางไซเบอร์ในภาคการเงินของอินโดนีเซีย กำหนดให้สถาบันการเงินต้องใช้มาตรการรักษาความปลอดภัยที่ครอบคลุมเพื่อต่อต้านการฉ้อโกง รวมถึงปัญหาบัญชีม้า มาตรการดังกล่าวรวมถึงการเข้ารหัสข้อมูลสำคัญ การยืนยันตัวตนหลายปัจจัย และการควบคุมการเข้าถึงที่เข้มงวด ซึ่งเป็นสิ่งสำคัญในการแก้ไขปัญหาบัญชีม้า (OJK, 2024)

นอกจากนี้ รายงานจาก The Asian Banker ระบุว่าสถาบันการเงินอินโดนีเซียควรลงทุนในแพลตฟอร์มการจัดการการฉ้อโกงแบบครบวงจร ซึ่งจะช่วยในการตรวจจับ ป้องกัน และบรรเทาการฉ้อโกงผ่านเทคโนโลยีการตรวจสอบและการปฏิบัติตามข้อกำหนดอย่างมีประสิทธิภาพ รวมถึงการตรวจสอบธุรกรรมแบบเรียลไทม์และการยืนยันตัวตนที่เข้มงวดเพื่อแก้ไขปัญหาบัญชีม้า (GBG and The Asian Banker, 2020)

2.8.4 แนวปฏิบัติในการจัดการปัญหาบัญชีม้าในฟิลิปปินส์

ปัญหาบัญชีม้าในฟิลิปปินส์มีแนวโน้มเพิ่มขึ้นอย่างมีนัยสำคัญในช่วงไม่กี่ปีที่ผ่านมา โดยเฉพาะอย่างยิ่งในช่วงการระบาดของโควิด-19 ที่มีการทำธุรกรรมออนไลน์เพิ่มขึ้น (Bangko Sentral ng Pilipinas, 2023) ตามรายงานของสำนักงานป้องกันและปราบปรามการฟอกเงินของฟิลิปปินส์ (Anti-Money Laundering Council, 2023) พบว่า จำนวนผู้เสียหายจากการใช้บัญชีม้าในฟิลิปปินส์เพิ่มขึ้นร้อยละ 30 ในปี 2565

เมื่อเทียบกับปีก่อนหน้า คิดเป็นมูลค่าความเสียหายที่เกิดจากการใช้บัญชีม้าสูงถึง 3.5 พันล้านเปโซฟิลิปปินส์ (ประมาณ 2.1 พันล้านบาท) และกว่าร้อยละ 60 ของผู้ตกเป็นเหยื่อเป็นผู้สูงอายุและผู้ที่มีความรู้ทางการเงินจำกัด

การแก้ไขปัญหาบัญชีม้าในฟิลิปปินส์เกี่ยวข้องกับหน่วยงานหลายภาคส่วน โดยมีการประสานงานและร่วมมือกันดังนี้

- ธนาคารกลางฟิลิปปินส์ (BSP) เป็นหน่วยงานหลักในการกำกับดูแลสถาบันการเงินและออกนโยบายเพื่อป้องกันการฟอกเงินและการทุจริตทางการเงิน
- สำนักงานตำรวจแห่งชาติฟิลิปปินส์ (PNP) รับผิดชอบในการสืบสวนและจับกุมผู้กระทำความผิด
- สำนักงานสอบสวนแห่งชาติ (NBI) ให้ความช่วยเหลือในการสืบสวนคดีที่ซับซ้อนและมีมูลค่าความเสียหายสูง
- หน่วยงานข่าวกรองทางการเงิน (AMLC) ทำหน้าที่ตรวจสอบธุรกรรมที่น่าสงสัยและประสานงานกับหน่วยงานบังคับใช้กฎหมาย
- กระทรวงยุติธรรม (DOJ) ให้คำปรึกษาทางกฎหมายและดำเนินคดีกับผู้กระทำความผิด

นอกจากนี้ หน่วยงานเหล่านี้ได้ร่วมกันจัดตั้ง "คณะทำงานร่วมต่อต้านอาชญากรรมทางการเงิน" (Joint Financial Crime Task Force) เพื่อแบ่งปันข้อมูล ประสานงาน และวางแผนยุทธศาสตร์ร่วมกันในการต่อสู้กับปัญหาบัญชีม้าและอาชญากรรมทางการเงินอื่น ๆ ด้วย

สำหรับกลไกรับเรื่องร้องเรียนและดำเนินคดีเกี่ยวกับบัญชีม้าในฟิลิปปินส์ มีแนวปฏิบัติ ดังนี้

สถาบันการเงิน

- จัดตั้งศูนย์รับเรื่องร้องเรียน 24 ชั่วโมงสำหรับลูกค้าที่สงสัยว่าตกเป็นเหยื่อของบัญชีม้า
- ใช้ระบบตรวจจับธุรกรรมที่น่าสงสัยแบบเรียลไทม์ (Real-time Transaction Monitoring System)
- ระงับบัญชีที่ต้องสงสัยทันทีเพื่อป้องกันการโอนเงินต่อ
- รายงานธุรกรรมที่น่าสงสัยไปยัง AMLC ภายใน 24 ชั่วโมง
- ให้ความร่วมมือกับหน่วยงานบังคับใช้กฎหมายในการสืบสวนและรวบรวมหลักฐาน

สำนักงานตำรวจแห่งชาติ

- จัดตั้งหน่วยเฉพาะกิจด้านอาชญากรรมไซเบอร์ (Cybercrime Task Force) เพื่อรับมือกับคดีบัญชีม้าและอาชญากรรมทางการเงินออนไลน์
- เปิดช่องทางรับแจ้งเหตุออนไลน์และสายด่วนสำหรับประชาชนที่ตกเป็นเหยื่อ
- ประสานงานกับธนาคารและ AMLC เพื่อติดตามเส้นทางการเงินและระบุตัวผู้กระทำความผิด
- ใช้เทคโนโลยีสืบสวนดิจิทัลในการรวบรวมและวิเคราะห์หลักฐาน
- ดำเนินการจับกุมและส่งฟ้องผู้ต้องสงสัยร่วมกับ DOJ

นอกจากนี้ ทั้งสถาบันการเงินและสำนักงานตำรวจแห่งชาติยังร่วมมือกันในการให้ความรู้และสร้างความตระหนักแก่สาธารณชนเกี่ยวกับภัยของบัญชีม้าและวิธีการป้องกันตนเอง ผ่านการรณรงค์ประชาสัมพันธ์และโครงการฝึกอบรมต่าง ๆ (Anti-Cybercrime Group, 2023)

2.8.5 แนวปฏิบัติในการจัดการปัญหาบัญชีม้าในบราซิล

ปัญหาบัญชีม้าในบราซิลมีการจัดการอย่างเข้มงวด โดยหน่วยงานหลักที่รับผิดชอบคือ Financial Intelligence Unit (FIU) ซึ่งทำหน้าที่ในการตรวจสอบและวิเคราะห์ธุรกรรมที่น่าสงสัยเพื่อป้องกันการฟอกเงินและการฉ้อโกงทางการเงิน รวมถึงทำงานร่วมกับธนาคารกลางบราซิล (BCB) ซึ่งมีบทบาทสำคัญในการกำกับดูแลสถาบันการเงินให้ปฏิบัติตามกฎหมายไซเบอร์และการฟอกเงินตาม Resolution BCB 85/2021

ผู้ที่เกี่ยวข้องกับการฟอกเงินผ่านบัญชีม้าอาจเผชิญโทษปรับและจำคุกตามกฎหมายหมายเลข 9,613/1998 (Law No. 9,613/1998) ว่าด้วยการฟอกเงิน โดยผู้กระทำผิดอาจถูกจำคุกเป็นเวลา 3-10 ปี และปรับสูงถึงหลายล้านเรียลบราซิล ขึ้นอยู่กับความรุนแรงของการกระทำผิด นอกจากนี้ ผู้ที่กระทำผิดอาจถูกยึดทรัพย์สินที่ได้มาจากการกระทำผิด โดยไม่จำเป็นต้องรอการตัดสินจากศาลในบางกรณี (FATF, 2023)

หน่วยงานรับผิดชอบในการจัดการปัญหาบัญชีม้าในบราซิล ได้แก่

- ธนาคารกลางบราซิล (BCB) มีหน้าที่กำกับดูแลและรับผิดชอบในการบังคับใช้กฎหมายที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์และการป้องกันการฟอกเงิน โดยสถาบันการเงินต้องรายงานเหตุการณ์ไซเบอร์ที่น่าสงสัยต่อธนาคารกลางบราซิล
- Financial Intelligence Unit (FIU) ทำหน้าที่ตรวจสอบธุรกรรมที่น่าสงสัยที่เกี่ยวข้องกับบัญชีม้าและแบ่งปันข้อมูลกับหน่วยงานต่างประเทศเพื่อจัดการปัญหาฟอกเงินข้ามพรมแดน

ทั้งนี้ ประชาชนสามารถรายงานปัญหาการฟอกเงินหรือบัญชีม้าผ่านหน่วยงานบังคับใช้กฎหมายท้องถิ่น หรือผ่านแพลตฟอร์มออนไลน์ของ FIU และ BCB เพื่อให้หน่วยงานเหล่านี้สามารถตรวจสอบและดำเนินการตามกฎหมายได้

2.8.6 สรุปแนวปฏิบัติในการจัดการปัญหาบัญชีม้าในต่างประเทศ

จากการทบทวนแนวปฏิบัติในการจัดการปัญหาบัญชีม้าในต่างประเทศ ในภาพรวมพบว่า มีหน่วยงานที่เกี่ยวข้องหลายหน่วยงานทำงานประสานกัน ตั้งแต่ธนาคารกลาง ซึ่งทำหน้าที่กำกับดูแลสถาบันการเงิน หน่วยงานบังคับใช้กฎหมาย เพื่อติดตามและดำเนินคดีกับผู้กระทำความผิด บางประเทศมีการ จัดตั้งคณะทำงานระหว่างหน่วยงานเพื่อทำหน้าที่ในการจัดการปัญหาบัญชีม้าโดยเฉพาะ รวมถึงมีการจัดทำกลไกรับเรื่องร้องเรียนและจัดการปัญหาบัญชีม้า

ตารางที่ 5 เปรียบเทียบแนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินและการจัดการปัญหาบัญชีม้าในต่างประเทศ

ประเด็น	สหรัฐอเมริกา	สิงคโปร์	อินโดนีเซีย	ฟิลิปปินส์	บราซิล
มาตรการป้องกันที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ของสถาบันการเงิน	- สถาบันการเงินต้องระบุ ประเมิน และบริหารความเสี่ยงด้านการจัดการความปลอดภัยของข้อมูล การใช้บริการเทคโนโลยีสารสนเทศจากบุคคลภายนอก และการออกแบบเทคโนโลยีบริการทางการเงินด้วยกรอบการประเมินความเสี่ยง Cybersecurity Performance Goals โดย Cybersecurity and Infrastructure Security Agency (CISA) ให้ครอบคลุมองค์กรทุกขนาด	- สถาบันการเงินต้องติดตามข่าวสารและข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ให้เป็นปัจจุบันอยู่เสมอ รวมถึงต้องมีการวิเคราะห์พฤติกรรมของผู้ใช้เพื่อตรวจจับและวิเคราะห์เหตุการณ์ไซเบอร์แบบเป็นปัจจุบัน (real time) - สถาบันการเงินควรควรจัดตั้งศูนย์ปฏิบัติการด้านความปลอดภัย (Security Operations Centre - SOC) เพื่อทำหน้าที่ติดตามและจัดการปัญหาด้านความปลอดภัยไซเบอร์ในองค์กร	- สถาบันการเงินต้องประเมินความเสี่ยงด้านไซเบอร์ทุกไตรมาส และจัดการความเสี่ยงให้เหมาะสมกับผลการประเมินความเสี่ยง โดยต้องมีการติดตามประสิทธิผลของมาตรการรักษาความปลอดภัยอย่างเหมาะสม - สถาบันการเงินต้องมีทีมตอบสนองต่อเหตุการณ์และแผนการดำเนินการที่ชัดเจนเพื่อการตรวจจับและจัดการเหตุการณ์ได้ทันทีเพื่อลดความเสียหายและความสูญเสีย - สถาบันการเงินต้องมีแผนการจำกัดความเสียหาย (Containment) การกำจัดมัลแวร์ (Eradication) และการกู้คืนระบบ (Recovery) ให้กลับมาใช้งานได้อย่างปลอดภัย	- ผู้ควบคุมข้อมูลมีหน้าที่และความรับผิดชอบการรักษาความปลอดภัยของข้อมูล การแจ้งเตือนกรณีเกิดการรั่วไหลของข้อมูล และการจัดทำมาตรการรักษาความปลอดภัยที่เหมาะสม - จำเป็นต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) เพื่อกำกับดูแลการปฏิบัติตามกฎหมาย - สร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ในหมู่ประชาชนทั่วไป และการส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ในองค์กรทั้งภาครัฐและเอกชน	- สถาบันการเงินต้องมีนโยบายความปลอดภัยทางไซเบอร์ที่ชัดเจนเพื่อรักษาความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล

ประเด็น	สหรัฐอเมริกา	สิงคโปร์	อินโดนีเซีย	ฟิลิปปินส์	บราซิล
มาตรการการจัดการปัญหาที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ของสถาบันการเงิน	- สถาบันการเงินต้องประเมินลักษณะของข้อมูลที่ถูกโจมตี ขอบเขตความเสียหาย และแจ้งให้หน่วยงานกำกับดูแลทราบ รวมถึงแจ้งให้ลูกค้าทราบถึงผลกระทบต่อลูกค้าอย่างทันท่วงที - สถาบันการเงินต้องดำเนินงานการตามแนวทางการรายงานเหตุการณ์ความผิดปกติ และถอดบทเรียนเพื่อนำมาปรับปรุงมาตรการการรักษาความปลอดภัยทางไซเบอร์	- สถาบันการเงินต้องมีแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ ที่ระบุวิธีการสื่อสาร การตอบสนองต่อภัยคุกคาม และแผนกู้คืนระบบที่สามารถกู้คืนระบบกลับมาในระยะเวลาที่เหมาะสม โดยแผนดังกล่าวควรมีการทบทวนอย่างน้อยปีละ 1 ครั้ง	- สถาบันการเงินต้องกำหนดให้มีการเข้ารหัสข้อมูลสำคัญ การยืนยันตัวตนหลายปัจจัย และการควบคุมการเข้าถึงที่เข้มงวด	- จัดตั้งศูนย์ประสานงานป้องกันอาชญากรรมทางไซเบอร์แห่งชาติ (NCPC) เพื่อดำเนินการประสานงานและสืบสวนคดีอาชญากรรมทางไซเบอร์ รวมถึงการจัดตั้งศาลอาชญากรรมทางไซเบอร์เฉพาะทางเพื่อพิจารณาคดีที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์	- สถาบันการเงินต้องจัดทำแผนการตอบสนองต่อเหตุการณ์ และการจัดการความปลอดภัยของข้อมูลภายนอกเช่น การใช้ระบบคลาวด์และการประมวลผลข้อมูลจากภายนอก
มาตรการเยียวยาเมื่อเกิดเหตุที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ของสถาบันการเงิน	- ไม่พบข้อมูล	- สถาบันการเงินต้องมีขั้นตอนการแก้ไขปัญหาที่ครอบคลุม และมีการติดตามปัญหาที่เกิดขึ้นจากการประเมินความปลอดภัยไซเบอร์อย่างต่อเนื่อง เพื่อให้มั่นใจว่าปัญหาถูกแก้ไขอย่างรวดเร็วและมีประสิทธิภาพ	- ไม่พบข้อมูล	- ไม่พบข้อมูล	- ไม่พบข้อมูล
มาตรการการจัดการปัญหาบัญชีม้าและปัญหามิจฉาชีพ	- จัดตั้งโครงการ “Money Mule Initiative” เพื่อหยุดยั้ง	- รัฐบาลสิงคโปร์มีการปรับปรุงกฎหมายให้สามารถดำเนินคดี	- สถาบันการเงินต้องมีมาตรการการเข้ารหัสข้อมูลสำคัญ การ	- มีการจัดตั้ง "คณะทำงานร่วมต่อต้านอาชญากรรมทาง	- Financial Intelligence Unit (FIU) ทำหน้าที่ในการ

ประเด็น	สหรัฐอเมริกา	สิงคโปร์	อินโดนีเซีย	ฟิลิปปินส์	บราซิล
	ขบวนการและกิจกรรมการหลอกลวงทางการเงิน ผ่านการดำเนินคดีและยื่นฟ้องแพ่ง หรือการสร้างความตระหนักรู้ให้แก่ประชาชนเพื่อไม่ให้หลงกลมิจฉาชีพ - จัดตั้งศูนย์รับเรื่องร้องเรียนให้ผู้เสียหายกรณีที่ถูกหลอกให้เป็นตัวกลางในส่งผ่านเงิน เพื่อให้ผู้เสียหายขอเข้ารับความช่วยเหลือ และทราบถึงการดำเนินการสอบสวนทางกฎหมายที่จะเกิดขึ้นต่อไป	กับผู้ที่มีส่วนเกี่ยวข้องกับบัญชีม้า แม้ว่าผู้ถือบัญชีอาจไม่มีเจตนาชัดเจนในการมีส่วนร่วมในอาชญากรรม รวมถึงปรับบทลงโทษให้มีความรุนแรงยิ่งขึ้น - ศูนย์ต่อต้านการฉ้อโกง (Anti-Scam Centre) เพื่ออายัดบัญชีธนาคารที่เกี่ยวข้องกับการฉ้อโกง โดยเน้นการใช้เทคโนโลยีและข้อมูลเชิงลึกเพื่อตรวจจับพฤติกรรมที่น่าสงสัย - จัดทำแอปพลิเคชัน ScamShield ซึ่งช่วยบล็อกหมายเลขโทรศัพท์ที่น่าสงสัย และกรอง SMS ที่อาจเป็นการฉ้อโกง นอกจากนี้ ยังสามารถรายงานหมายเลขโทรศัพท์หรือข้อความที่น่าสงสัยได้ทันทีผ่านแอปพลิเคชัน	ยืนยันตัวตนหลายปัจจัย และการควบคุมการเข้าถึงที่เข้มงวด ซึ่งเป็นสิ่งสำคัญในการแก้ไขปัญหาบัญชีม้า	การเงิน" เพื่อแบ่งปันข้อมูลประสานงาน และวางแผนยุทธศาสตร์ร่วมกันในการจัดการกับปัญหาบัญชีม้าและอาชญากรรมทางการเงินอื่น ๆ - มีการจัดตั้งศูนย์รับเรื่องร้องเรียน 24 ชั่วโมงสำหรับลูกค้าที่สงสัยว่าตกเป็นเหยื่อของบัญชีม้า - ใช้ระบบตรวจจับธุรกรรมที่น่าสงสัยแบบเรียลไทม์ - ระงับบัญชีที่ต้องสงสัยทันทีเพื่อป้องกันการโอนเงินต่อ - ธนาคารและตำรวจยังร่วมมือกันในการให้ความรู้และสร้างความตระหนักแก่สาธารณชนเกี่ยวกับภัยของบัญชีม้าและวิธีการป้องกันตนเอง	ตรวจสอบและวิเคราะห์ธุรกรรมที่น่าสงสัยเพื่อป้องกันการฟอกเงินและการฉ้อโกงทางการเงิน - กำหนดโทษที่เกี่ยวข้องกับบัญชีม้ามีโทษจำคุก 3-10 ปี และปรับสูงถึงล้านเรียลบราซิล และสามารถถูกยึดทรัพย์ได้โดยไม่ต้องรอการตัดสินจากศาลในบางกรณี - ประชาชนสามารถรายงานปัญหาการฟอกเงินหรือบัญชีม้าผ่านหน่วยงานบังคับใช้กฎหมายท้องถิ่น หรือผ่านแพลตฟอร์มออนไลน์ได้

ที่มา : จากการรวบรวมของคณะวิจัย

2.9 มาตรการชดเชยเยียวยาผู้เสียหายจากภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงิน

คณะวิจัยสำรวจและรวบรวมข้อมูลแนวทางการชดเชยเยียวยาผู้เสียหายจากภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินในต่างประเทศ โดยมีรายละเอียดดังนี้

2.9.1 กลุ่มประเทศที่มีมาตรการชดเชยเยียวยาจากสถาบันทางการเงิน กรณีที่เกิดภัยคุกคามทางไซเบอร์

สำหรับประเทศที่มีมาตรการชดเชยเยียวยาจากสถาบันการเงินหรือหน่วยงานที่เกี่ยวข้อง เมื่อเกิดภัยคุกคามทางไซเบอร์ขึ้น คณะวิจัยได้สำรวจและรวบรวมข้อมูลจากประเทศที่มีแนวทางการปฏิบัติที่ดีเพื่อนำมาเป็นกรณีศึกษา ได้แก่ ประเทศสิงคโปร์ ประเทศสหรัฐอเมริกา และประเทศแคนาดา โดยมีรายละเอียดหน่วยงานที่รับผิดชอบ และการกระบวนการดำเนินงานของแต่ละประเทศ ดังต่อไปนี้

- *สิงคโปร์*

สิงคโปร์เป็นประเทศที่มีการระบุความรับผิดชอบของหน่วยงานในการชดเชยเยียวยาผู้เสียหายจากภัยคุกคามทางไซเบอร์อย่างชัดเจน โดยสิงคโปร์ได้จัดทำ Phishing Loss Management Framework (PLMF) หรือ Shared Responsibility Framework (SRF) เป็นกรอบการทำงานที่กำหนดหน้าที่และความรับผิดชอบร่วมกันระหว่างสถาบันการเงิน บริษัทโทรคมนาคม และผู้บริโภคขึ้น เพื่อรับมือกับปัญหาการหลอกลวงทางออนไลน์ โดยเฉพาะอย่างยิ่งการหลอกลวงผ่านการฟิชชิง (Phishing) ได้แก่ การสร้างหน้าเว็บหรือการส่งข้อความปลอมเพื่อลวงเอาข้อมูลสำคัญของผู้ใช้งาน

กรอบการทำงาน Shared Responsibility Framework (SRF) ได้กำหนดให้ธนาคารและผู้ให้บริการโทรคมนาคมต้องเป็นผู้รับผิดชอบความเสียหายหลักในกรณีที่มีการละเลยหน้าที่ในการป้องกันภัยคุกคามทางไซเบอร์ (Monetary Authority of Singapore, 2023) เช่น การไม่ตรวจจับพฤติกรรมฟิชชิงหรือปล่อยให้ลิงก์อันตรายผ่านไปถึงผู้ใช้งาน ในขณะเดียวกัน ผู้บริโภคจะมีหน้าที่รายงานความผิดปกติภายใน 3 วันเพื่อขอรับการชดเชยความเสียหายจากธนาคารและผู้ให้บริการโทรคมนาคมได้ภายใต้กรอบดังกล่าว โดยกระบวนการหลักในการพิจารณาค่าชดเชยเยียวยาตามกรอบการทำงาน ประกอบไปด้วย การรับเรื่องร้องเรียน การตรวจสอบข้อเท็จจริง การประเมินความรับผิดชอบ และการยื่นร้องเรียนเพิ่มเติม กรณีที่มีการพิจารณาการชดเชยเยียวยาจากธนาคารและผู้ให้บริการโทรคมนาคมตามกรอบแล้ว แต่ผู้บริโภคไม่เห็นด้วยกับผลการพิจารณาเยียวยา จะสามารถยื่นคำร้องต่อ Financial Industry Disputes Resolution Centre (FIDReC) ซึ่งเป็นองค์กรที่ให้บริการไกล่เกลี่ยข้อพิพาทที่เกี่ยวข้องกับการเงินโดยไม่มีค่าใช้จ่าย และยังช่วยอำนวยความสะดวกในการเรียกร้องค่าชดเชยหรือแก้ไขปัญหาที่ไม่ได้รับการแก้ไขโดยธนาคารหรือผู้ให้บริการทางการเงินได้ในลำดับถัดไป (Monetary Authority of Singapore, 2024)

สำหรับกรอบการทำงาน Shared Responsibility Framework (SRF) ในประเทศสิงคโปร์ มีกำหนดประกาศใช้งานในวันที่ 16 ธันวาคม พ.ศ. 2567 มีรายละเอียดดังนี้ (The Straitstimes, 2024)

1) หน้าที่และแนวทางการดำเนินงานสำหรับสถาบันการเงิน

- การกำหนดเว้นระยะการทำธุรกรรมจำนวน 12 ชั่วโมง เมื่อมีเหตุการณ์ที่ส่งผลต่อระบบความปลอดภัย เช่น การตั้งค่าบัญชีบนโทรศัพท์เครื่องใหม่ รวมไปถึงการผูกบัญชี e-wallet ต่างๆ บนโทรศัพท์เครื่องใหม่ โดยในระยะเวลานี้จะไม่สามารถทำธุรกรรมใดๆ ที่มีความเสี่ยงสูงได้
- แจ้งเตือนลูกค้าทันทีเมื่อพบกิจกรรมผิดปกติ ภายในระยะเวลา 12 ชั่วโมงเพื่อให้ลูกค้าสามารถดำเนินการแก้ไขและป้องกันในลำดับถัดไป
- สถาบันการเงินต้องแจ้งเตือนลูกค้า เมื่อมีการทำธุรกรรม เช่น การโอนเงินออกจากบัญชีผ่านการแจ้งเตือนแบบเป็นปัจจุบัน เพื่อให้ลูกค้าสามารถรายงานการหลอกลวงที่อาจเกิดขึ้นได้ทันที
- ผู้ใช้ควรมีสิทธิ์เข้าถึงช่องทางฉุกเฉิน หรือช่องทางการรายงานและอายัดบัญชีของตน เพื่อป้องกันการทำธุรกรรมที่ไม่ได้รับอนุญาตเพิ่มเติมกรณีที่เกิดการหลอกลวงขึ้น
- สถาบันการเงินจะต้องพัฒนาระบบเฝ้าระวังการฉ้อโกงแบบเป็นปัจจุบัน ตามกรอบการทำงาน Shared Responsibility Framework (SRF) โดยจะต้องสามารถตรวจจับได้เมื่อมีเงินถูกโอนจากบัญชี และบล็อกธุรกรรมที่น่าสงสัยจนกว่าจะได้รับการยืนยันจากลูกค้า หรือระงับการทำธุรกรรมเป็นเวลาอย่างน้อย 24 ชั่วโมง ซึ่งหากสถาบันการเงินไม่ปฏิบัติตามจะต้องรับผิดชอบในการเยียวยาให้กับเหยื่อเต็มจำนวน

2) แนวทางการดำเนินงานสำหรับผู้ให้บริการโทรคมนาคม

- ปิดกั้นข้อความและการโทรที่น่าสงสัย โดยลูกค้าควรได้รับข้อความที่แสดงชื่อผู้ส่ง เฉพาะในกรณีที่ข้อความมาจากผู้ส่งที่ลงทะเบียนกับทะเบียนผู้ส่ง SMS และควรมีการระบุข้อความแจ้งเตือนลูกค้าไว้ให้ชัดเจน หากมีข้อความถูกส่งมาจากผู้ใช้ที่ยังไม่ได้ลงทะเบียน
- ผู้ให้บริการโทรคมนาคมต้องปิดกั้นข้อความจากผู้ที่ไม่ได้รับอนุญาตทั้งหมด เพื่อป้องกันไม่ให้ลูกค้ารับข้อความจากช่องทางภายนอก รวมถึงเครือข่ายที่ไม่รู้จัก
- ผู้ให้บริการโทรคมนาคมจะต้องพัฒนาระบบการกรองข้อความ SMS ทั้งหมดที่ส่งผ่านเครือข่ายของตน เพื่อคัดแยกข้อความที่มี URL ที่ตรงกับฐานข้อมูลซึ่งเป็นอันตราย

นอกจากนี้ สิงคโปร์ยังมีกฎหมายที่เกี่ยวข้อง ได้แก่ Personal Data Protection Act (PDPA) หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ ซึ่งกำหนดบทลงโทษต่อองค์กรที่ละเมิดมาตรการป้องกันข้อมูล เช่น การปรับเงินสูงสุดคิดเป็นร้อยละ 10 ของรายได้ประจำปีในประเทศสำหรับองค์กร

ขนาดใหญ่ หรือหนึ่งล้านดอลลาร์สิงคโปร์สำหรับองค์กรขนาดเล็ก ซึ่งช่วยส่งเสริมการคุ้มครองข้อมูลของผู้บริโภค

- *สหรัฐอเมริกา*

สหรัฐอเมริกาใช้นโยบาย Zero Liability Policy ซึ่งพัฒนาโดยเครือข่ายบัตรเครดิตบนพื้นฐานของกฎหมายคุ้มครองผู้บริโภคเกี่ยวกับธุรกรรมอิเล็กทรอนิกส์ หรือ Electronic Fund Transfer Act (EFTA) (FRB, n.d.) โดย Zero Liability Policy เป็นนโยบายคุ้มครองผู้บริโภคในกรณีที่ตกเป็นเหยื่อการฉ้อโกง การทำธุรกรรมที่ไม่ได้รับอนุญาต หรือการถูกละเมิดข้อมูลจากบัญชีธนาคาร บัตรเครดิตและบัตรเดบิต ที่ออกโดยธนาคารหรือสถาบันการเงิน เช่น Visa Mastercard และ American Express ทั้งในรูปแบบออนไลน์และออฟไลน์ โดยผู้บริโภคจะไม่ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น ยกเว้นกรณีที่เกิดการปล่อยปละละเลยหรือผิดพลาดโดยเจตนาซึ่งจะทำให้ผู้บริโภคไม่ได้รับความคุ้มครอง เช่น การเปิดเผยรหัส PIN หรือการรายงานล่าช้าเกินระยะเวลาที่กำหนด นอกจากนี้จะมีผลคุ้มครองเฉพาะกรณีที่ธุรกรรมเกิดขึ้นโดยบุคคลที่สามที่ไม่ได้รับอนุญาตเท่านั้น (FDIC, 2018)

สำหรับขั้นตอนการดำเนินงานตามนโยบาย Zero Liability Policy เมื่อผู้บริโภคเผชิญกับการทำธุรกรรมที่ไม่ได้รับอนุญาต ขั้นตอนแรกจะต้องรายงานปัญหาไปยังสถาบันการเงินทันทีผ่านทางช่องทางโทรศัพท์หรืออีเมล (หรือช่องทางอื่นๆ ตามที่สถาบันการเงินกำหนดไว้) จากนั้นสถาบันการเงินจะทำการตรวจสอบและแก้ไขปัญหา รวมทั้งพิจารณาชดเชยเยียวยาค่าเสียหายต่อไป ซึ่งจะมีระยะเวลาในการดำเนินการโดยทั่วไป 5 วันทำการเพื่อคืนเงินให้กับผู้เสียหาย (Visa, 2024) นอกจากนี้ผู้บริโภคยังสามารถร้องเรียนความเสียหายและยื่นคำร้องขอเงินชดเชยผ่านทางช่องทางของหน่วยงานรัฐ เช่น Federal Trade Commission (FTC) (FTC, n.d.) หรือ Consumer Financial Protection Bureau (CFPB) (CFPB, n.d.) ในกรณีที่บริษัทหรือสถาบันการเงินที่เกี่ยวข้องไม่ดำเนินการแก้ไขปัญหาหรือชดเชยเยียวยาอย่างเหมาะสม ซึ่งประเทศสหรัฐอเมริกานั้นนับเป็นประเทศที่มีข้อกฎหมายและขั้นตอนในการดำเนินการการฟ้องร้องที่ชัดเจนในกรณีที่สถาบันการเงินไม่ปฏิบัติตาม (U.S. Bank, 2024)

- *แคนาดา*

ประเทศแคนาดามีการใช้นโยบายที่มีลักษณะใกล้เคียงกับในประเทศสหรัฐอเมริกา ได้แก่ นโยบาย Zero Liability Policy ซึ่งพัฒนาโดยสถาบันการเงินและเครือข่ายบัตรเครดิตภายใต้กฎหมายที่รองรับ ได้แก่ Cost of Borrowing Regulations ภายใต้ Bank Act ระบุให้จำกัดความรับผิดของผู้บริโภคในกรณีการใช้บัตรโดยไม่ได้รับอนุญาตไว้ที่ 50 ดอลลาร์ (CPA Canada, 2019) โดย Zero Liability Policy เป็นนโยบายคุ้มครองผู้บริโภคที่ประสบปัญหาการฉ้อโกงหรือการใช้บัตรโดย

ไม่ได้รับอนุญาต โดยผู้บริโภคจะไม่ต้องรับผิดชอบความเสียหายที่เกิดจากธุรกรรมดังกล่าว และธนาคารหรือสถาบันการเงินที่ออกบัตรจะเป็นผู้รับผิดชอบค่าเสียหายแทนผู้บริโภค (Mastercard Canada, 2024) ทั้งนี้มีเงื่อนไขคือ ผู้บริโภคจะต้องไม่เป็นฝ่ายแสดงความประมาท เช่น การเปิดเผยรหัส PIN หรือไม่ดูแลรักษาบัตรของตนเอง และจะต้องรายงานปัญหาไปยังสถาบันการเงินทันทีที่ทราบ

ผู้บริโภคที่ตกเป็นเหยื่อการฉ้อโกงสามารถเรียกร้องค่าเสียหายได้โดยการยื่นเรื่องร้องเรียนต่อธนาคารหรือสถาบันการเงินโดยตรง เพื่อตรวจสอบและแก้ไขปัญหา รวมทั้งพิจารณาชดเชยเยียวยาค่าเสียหายต่อไป หรือหากมีการติดต่อแล้วปัญหาไม่ได้รับการแก้ไข หรือไม่เห็นด้วยกับผลการพิจารณาชดเชยเยียวยา สามารถติดต่อ Financial Consumer Agency of Canada (FCAC) ซึ่งเป็นหน่วยงานที่เกี่ยวข้องกับการเยียวยาผู้บริโภคที่ได้รับผลกระทบจากการถูกโกงทางการเงินหรือภัยคุกคามทางไซเบอร์ ให้การปกป้องสิทธิและผลประโยชน์ของผู้บริโภคในภาคการเงิน ในการรับคำปรึกษาเกี่ยวกับกระบวนการร้องเรียนเพิ่มเติม รวมถึงการยื่นเรื่องต่อหน่วยงานอิสระที่ดูแลข้อพิพาท เช่น Ombudsman for Banking Services and Investments (OBSI) (Government of Canada, 2024)

จากแนวทางการดำเนินงานสำหรับประเทศที่มีมาตรการชดเชยเยียวยาผู้เสียหายจากภัยคุกคามทางไซเบอร์อย่างชัดเจนดังที่กล่าวมาข้างต้น ได้แก่ ประเทศสิงคโปร์ ประเทศสหรัฐอเมริกา และประเทศแคนาดา พบว่าทั้งสามประเทศมีแนวคิดในการกำหนดมาตรการที่คล้ายคลึงกัน กล่าวคือกำหนดว่าผู้บริโภคไม่จำเป็นต้องรับผิดชอบความเสียหายที่เกิดขึ้น หากการถูกละเมิดหรือฉ้อโกงทางออนไลน์ไม่ได้เป็นผลมาจากความประมาทของผู้บริโภคเอง โดยผู้ที่ต้องรับผิดชอบความเสียหายแทนผู้บริโภค ได้แก่ สถาบันการเงินสำหรับทั้ง 3 ประเทศ และมีการเพิ่มเติมขอบเขตความรับผิดชอบไปถึงผู้ให้บริการโทรคมนาคมในกรณีของประเทศสิงคโปร์

2.9.2 กลุ่มประเทศที่ต้องมีการดำเนินการฟ้องร้อง พิสูจน์ความผิด หรือดำเนินการเรียกร้องค่าสินไหมจากบริษัทประกันภัย

สำหรับกลุ่มประเทศถัดไป ได้แก่ กลุ่มประเทศที่ปัจจุบันยังอยู่ในขั้นตอนการพัฒนานโยบายหรือมาตรการที่กำหนดความรับผิดชอบที่ชัดเจนในกรณีที่เกิดภัยคุกคามทางไซเบอร์ขึ้น ดังนั้นผู้เสียหายจากภัยคุกคามทางไซเบอร์ในปัจจุบันจึงจำเป็นต้องดำเนินการฟ้องร้อง พิสูจน์ความผิด หรือเรียกร้องค่าสินไหมจากบริษัทประกันภัยเพื่อรับค่าชดเชยเยียวยาจากคู่กรณีและหน่วยงานที่เกี่ยวข้องในลำดับถัดไป ยกตัวอย่างเช่นประเทศดังต่อไปนี้

- *ประเทศออสเตรเลีย*

ในประเทศออสเตรเลียมีการจัดตั้งกรอบการป้องกันและการชดเชยที่เกี่ยวข้องกับการถูกโกงทางไซเบอร์ เพื่อช่วยเหลือผู้บริโภคที่ได้รับผลกระทบจากการถูกฉ้อโกง ภายใต้ชื่อบริการ Scamwatch ซึ่งดำเนินการโดยหน่วยงาน Australian Competition and Consumer Commission (ACCC) ของรัฐบาลออสเตรเลีย เสนอช่องทางให้ผู้บริโภคเข้าไปรายงานการฉ้อโกงและรับคำแนะนำในการป้องกันการถูกโกงทางไซเบอร์ บริการดังกล่าวจะช่วยให้ผู้บริโภคที่ตกเป็นเหยื่อของการฉ้อโกงสามารถติดต่อหน่วยงานที่เกี่ยวข้อง เช่น ธนาคารหรือหน่วยงานคุ้มครองผู้บริโภค เพื่อรับการพิจารณาค่าเสียหายหรือการชดเชยเยียวยาได้สะดวกยิ่งขึ้น รวมทั้งดำเนินการแก้ไขปัญหาต่อไป (ACCC, n.d.)

หากผู้บริโภคไม่พึงพอใจกับความช่วยเหลือหรือการเยียวยาจากธนาคารหรือสถาบันการเงินที่เกี่ยวข้อง สามารถดำเนินการร้องเรียนและขอรับค่าชดเชยได้จาก Australian Financial Complaints Authority (AFCA) ซึ่งเป็นหน่วยงานที่ให้บริการช่วยเหลือและระงับข้อพิพาททางการเงินระหว่างผู้บริโภคและองค์กรด้านการเงิน เช่น ธนาคาร บริษัทประกันภัย รวมไปถึงการให้คำแนะนำและคำปรึกษาเกี่ยวกับสิทธิและวิธีการดำเนินการต่างๆ ในกรณีที่ AFCA ออกคำตัดสิน (Determination) คำตัดสินนั้นจะมีผลผูกพันและสถาบันการเงินต้องปฏิบัติตามคำตัดสิน หากสถาบันการเงินไม่ปฏิบัติตาม AFCA จะรายงานการไม่ปฏิบัติตามนี้ไปยัง Australian Securities and Investments Commission (ASIC) ซึ่งเป็นหน่วยงานที่ดูแลการปฏิบัติตามกฎหมายทางการเงินในประเทศออสเตรเลีย ทั้งนี้หากผู้บริโภคไม่เห็นด้วยกับคำตัดสินของ AFCA สามารถดำเนินการเรื่องนี้ผ่านกระบวนการทางกฎหมายได้ โดยจะต้องนำคดีขึ้นสู่ศาล (AFCA, 2018)

นอกจากนี้ รัฐบาลออสเตรเลียได้ออกกฎหมาย Scam Code กรณีที่พบการฉ้อโกง กำหนดให้สถาบันการเงินและบริษัทที่เกี่ยวข้องต้องดำเนินการแก้ไขปัญหาหรือจัดตั้งกระบวนการตรวจสอบการฉ้อโกงทันที รวมถึงการให้ข้อมูลและคำแนะนำแก่ผู้บริโภคในการระวังภัยคุกคามทางไซเบอร์ โดยสถาบันการเงินและผู้ให้บริการทางการเงินต้องรับผิดชอบในการดำเนินการเยียวยาผู้บริโภค โดยการคืนเงินหรือจัดหาวิธีการป้องกันการฉ้อโกงที่มีประสิทธิภาพต่อไป (Comply Advantage, 2024)

- *กลุ่มประเทศสหภาพยุโรป*

กลุ่มประเทศสหภาพยุโรปมีกฎหมาย General Data Protection Regulation (GDPR) หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประชากรในสหภาพยุโรป ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 25 พฤษภาคม 2018 โดยมีเป้าหมายเพื่อคุ้มครองสิทธิในข้อมูลส่วนบุคคล และกำหนดแนวทางที่องค์กรต่างๆ ต้องปฏิบัติเพื่อประมวลผลข้อมูลส่วนบุคคลอย่างปลอดภัยและโปร่งใส (GDPR, n.d.) ซึ่งมีขอบเขตรวมไปถึงกรณีที่เกิดการรั่วไหลของข้อมูล (Data Breach) ไม่ว่าจะเป็นการถูกเข้าถึงข้อมูล

โดยไม่ได้รับอนุญาตจากการถูกแฮ็ก หรือการรั่วไหลของข้อมูลส่วนบุคคลจากวิธีการอื่น ๆ (DataBleach, n.d.) โดย GDPR จะให้สิทธิ์แก่เจ้าของข้อมูลในการเรียกร้องค่าชดเชยจากองค์กรที่ละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล ครอบคลุมทั้งความเสียหายที่เป็นรูปธรรม (Material Damage) เช่น การสูญเสียเงิน และความเสียหายที่ไม่เป็นรูปธรรม (Non-Material Damage) เช่น ความทุกข์ใจ สนับสนุนให้ผู้ได้รับผลกระทบสามารถดำเนินการทางกฎหมายเพื่อเรียกร้องค่าชดเชย หากองค์กรที่ละเมิดไม่ยินยอมชดเชย ทั้งนี้ผู้บริโภคจะต้องดำเนินการฟ้องร้องเพื่อพิจารณาค่าเสียหายหรือการชดเชยเยียวยาในลำดับถัดไป

- *ประเทศฝรั่งเศส*

ประเทศฝรั่งเศสมีการประกาศใช้กฎหมาย LOPMI (Loi d'Orientation et de Programmation du Ministère de l'Intérieur) ในวันที่ 24 มกราคม 2566 กฎหมายการป้องกันและการตอบสนองต่อภัยคุกคามทางไซเบอร์ฉบับนี้กำหนดว่า บุคคลธรรมดาหรือองค์กรที่ได้รับความเสียหายหรือสูญเสียจากการโจมตีทางไซเบอร์ที่เกี่ยวข้องกับการประกอบอาชีพ ต้องแจ้งความภายใน 72 ชั่วโมงหลังจากทราบเหตุ เพื่อให้มีสิทธิ์ได้รับการชดเชยจากบริษัทประกัน มาตรการนี้มีเป้าหมายเพื่อให้หน่วยงานที่เกี่ยวข้องสามารถเข้าถึงข้อมูลในการติดตามและดำเนินคดีกับผู้กระทำผิดได้อย่างรวดเร็ว อย่างไรก็ตามในกรณีที่การโจมตีเกิดขึ้นในบริบทส่วนตัว บุคคลไม่จำเป็นต้องยื่นคำร้องเพื่อรับความคุ้มครองจากประกัน หากการคุ้มครองนั้นถูกระบุไว้ในสัญญาประกันภัย (Entreprendre Service Public, 2023) การประกาศใช้กฎหมายดังกล่าวแสดงให้เห็นว่าประเทศฝรั่งเศสมีกระบวนการชดเชยเยียวยาผู้เสียหายที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ ในรูปแบบการเรียกร้องค่าสินไหมจากบริษัทประกันภัย

- *ประเทศไนจีเรีย*

กฎหมาย Nigerian Consumer Protection Council Act ให้การคุ้มครองผู้บริโภคในบริการต่างๆ เช่น การทำธุรกรรมทางอิเล็กทรอนิกส์ โดยหน่วยงาน Consumer Protection Council (CPC) มีอำนาจบังคับให้ผู้ให้บริการชดเชยความเสียหายแก่ผู้บริโภค ยกตัวอย่างเช่นในกรณีที่มีการทำธุรกรรมโดยไม่ได้รับอนุญาตจากบัญชีลูกค้าธนาคาร เนื่องจากความบกพร่องในระบบความปลอดภัย อย่างไรก็ตาม การบังคับใช้กฎหมายนี้ยังไม่มีสามารถสร้างผลลัพธ์อย่างมีนัยสำคัญ เนื่องจาก CPC ขาดทรัพยากรบุคคลและเทคโนโลยีที่จำเป็นในการจัดการปัญหาที่เกี่ยวกับการธนาคารและการชำระเงินอิเล็กทรอนิกส์ (Orji, 2019)

- *ประเทศอินโดนีเซีย*

ในประเทศอินโดนีเซีย การเยียวยาผู้บริโภคจากภัยคุกคามทางไซเบอร์ในภาคการเงินยังคงอยู่ในขั้นตอนการพัฒนา ซึ่งจำเป็นต้องอาศัยการร่วมมือจากหลายภาคส่วน เช่น สถาบันทางการเงินและหน่วยงานรัฐบาลที่เกี่ยวข้อง โดยหน่วยงานที่เกี่ยวข้องกับการป้องกันภัยคุกคามทางไซเบอร์ในประเทศอินโดนีเซีย ได้แก่ Financial Services Authority (OJK) ได้มีการออกมาตรการและกฎระเบียบเพื่อการรับมือกับภัยคุกคามทางไซเบอร์ และขอความร่วมมือสถาบันการเงินต่างๆ ให้มีการประเมินความเสี่ยง และจัดทำมาตรการจัดการเหตุการณ์ที่รัดกุมมากยิ่งขึ้น (Teja, 2023) อย่างไรก็ตาม การชดเชยเยียวยาผู้บริโภคจากภัยคุกคามทางไซเบอร์ในอินโดนีเซียยังไม่มีการกำหนดขอบเขตชัดเจนเทียบเท่ากับประเทศที่มีนโยบายชดเชยให้แก่ผู้บริโภคโดยตรง โดยแนวทางการจัดการทางด้านภัยคุกคามทางไซเบอร์ส่วนใหญ่จะเกี่ยวข้องกับการให้คำแนะนำ การเสริมสร้างความร่วมมือและจัดการฝึกอบรมเพื่อสร้างภูมิคุ้มกันให้กับประชาชน (Sury, 2021)

- *ประเทศฟิลิปปินส์*

ในฟิลิปปินส์ การเยียวยาผู้บริโภคจากภัยคุกคามทางไซเบอร์ในภาคการเงินมีการจัดการผ่านหน่วยงานต่าง ๆ เช่น ธนาคารกลางของฟิลิปปินส์ (BSP) มีหน้าที่ส่งเสริมให้ธนาคารและสถาบันการเงินมีมาตรการควบคุมความเสี่ยงทางไซเบอร์ โดยมุ่งสร้างความมั่นใจและความปลอดภัยให้กับผู้บริโภคในระบบการเงิน ให้การคุ้มครองผู้บริโภคจากการโกงออนไลน์ เช่น การฟิชชิงและการโจรกรรมข้อมูลผ่านบัญชีธนาคารหรือกระเป๋าเงินอิเล็กทรอนิกส์ (e-wallets) (FSF, 2021) นอกจากนี้ ยังมีกฎหมายที่ระบุบทลงโทษสำหรับการกระทำที่เกี่ยวข้องกับการโจรกรรมทางไซเบอร์ ซึ่งรวมถึงการเปิดบัญชีธนาคารหรือกระเป๋าเงินอิเล็กทรอนิกส์โดยใช้ชื่อปลอมและการใช้บัญชีเหล่านี้ในการโอนเงินที่ได้มาอย่างผิดกฎหมาย อย่างไรก็ตาม การชดเชยหรือการเยียวยาผู้บริโภคที่ตกเป็นเหยื่อจากภัยคุกคามทางไซเบอร์ทางภาคการเงินในประเทศฟิลิปปินส์ยังไม่ปรากฏแนวทางที่ชัดเจน (Filane, 2022)

- *ประเทศบราซิล*

สำหรับประเทศบราซิล ธนาคารกลางของบราซิล (Banco Central do Brasil) ได้ออกระเบียบ 4,658/2018 ซึ่งกำหนดให้สถาบันการเงินต้องจัดทำแผนการตอบสนองต่อเหตุการณ์และรักษาความปลอดภัยของข้อมูล โดยมุ่งเน้นการสร้างระบบป้องกันที่มีประสิทธิภาพและการปฏิบัติตามมาตรการที่เป็นไปตามกฎหมายที่เกี่ยวข้อง (Banco Central do Brasil, 2018) ซึ่งแม้รัฐบาลจะมีการริเริ่มและออกกฎหมายเกี่ยวกับไซเบอร์ แต่กลยุทธ์ที่มีอยู่ยังไม่เพียงพอ ขาดการประสานงานระหว่างหน่วยงานและการลงทุนในเทคโนโลยีที่ทันสมัย ทำให้บราซิลยังคงเสี่ยงต่อการโจมตีทางไซเบอร์ (Stronell, 2020)

อย่างไรก็ตาม การเยียวยาผู้บริโภคในภาคการเงินจากภัยคุกคามทางไซเบอร์ยังไม่มีมาตรการชดเชยที่กำหนดไว้อย่างชัดเจน โดยสถาบันการเงินมักมีนโยบายในการปกป้องและช่วยเหลือลูกค้าที่ได้รับผลกระทบจากการโจมตีทางไซเบอร์ ซึ่งอาจรวมถึงการคืนเงินหรือชดเชยความเสียหาย ทั้งนี้ขึ้นอยู่กับกรณีและนโยบายของแต่ละสถาบัน ยกตัวอย่างเช่น PagBrazil หรือบริษัทที่ให้บริการระบบชำระเงินในบราซิล โดยเฉพาะธุรกิจอีคอมเมิร์ซที่ต้องการรับชำระเงินในสกุลเงินท้องถิ่น มีการพัฒนาระบบยื่นคำร้องขอเงินคืน (Chargeback) ซึ่งเป็นระบบที่ผู้บริโภคสามารถขอเงินคืนในกรณีที่เกิดธุรกรรมจากการฉ้อโกงหรือจากปัญหาอื่นๆ โดยยื่นเรื่องไปยังธนาคารผู้ออกบัตรให้ยกเลิกการชำระเงิน และดำเนินการหักเงินจากบัญชีปลายทางก่อนจะคืนเงินไปยังบัญชีต้นทาง (PagBrazil, 2024)

จากการสืบค้นรวบรวมข้อมูลในกลุ่มประเทศที่ยังไม่มีมาตรการชดเชยเยียวยาจากสถาบันทางการเงินอย่างชัดเจน พบว่าแนวทางการชดเชยเยียวยาผู้เสียหายจากภัยคุกคามทางไซเบอร์มักจะเป็นรูปแบบการฟ้องร้อง พิสูจน์ความผิด เพื่อพิจารณาค่าเสียหายในลำดับถัดไป โดยอาจมีหน่วยงานที่ให้การสนับสนุนในการให้คำแนะนำและดำเนินการฟ้องร้อง เช่น ประเทศออสเตรเลีย นอกจากนี้ยังมีกระบวนการชดเชยเยียวยาอีกทางเลือกหนึ่งในรูปแบบการเรียกร้องค่าสินไหมจากบริษัทประกันภัย เช่น ประเทศฝรั่งเศส ที่มีการออกกฎหมายรองรับในส่วนประกันภัยไซเบอร์โดยตรง

สำหรับประเทศไทย อาจจัดอยู่ในกลุ่มประเทศที่ยังไม่มีมาตรการชดเชยเยียวยาจากสถาบันทางการเงินอย่างเป็นรูปธรรมเช่นกัน เนื่องจากโดยทั่วไปเมื่อเกิดภัยคุกคามทางไซเบอร์ขึ้น ความเสียหายมักจะตกอยู่ที่ผู้บริโภคเพียงฝ่ายเดียวโดยไม่ได้รับการเยียวยาใด ๆ ถึงแม้ว่าความเสียหายอาจมีส่วนเกิดจากความผิดพลาดของผู้ให้บริการ อย่างไรก็ตาม ผู้บริโภคในประเทศไทยที่ได้รับความเสียหายจากภัยคุกคามทางไซเบอร์และสูญเสียเงินฝากในธนาคาร อาจทำการฟ้องร้องธนาคารพาณิชย์เพื่อให้รับผิดตามประมวลกฎหมายแพ่งและพาณิชย์ ว่าด้วยการฝากทรัพย์มาตรา 657 ดังเช่นกรณีศึกษาจากคำพิพากษาศาลฎีกา ที่ 6233/2564 ผู้เสียหายได้ทำการฟ้องร้องธนาคารพาณิชย์ให้ชำระค่าเสียหาย เนื่องจากถูกหลอกให้กดลิงก์ ทำให้คนร้ายสามารถเข้าควบคุมข้อมูลในมือถือ และทำการโอนเงินออกไปยังบัญชีเงินฝากของผู้อื่น (ฐานเศรษฐกิจ, 2566) คดีความนี้ศาลได้มีคำพิพากษาให้ธนาคารรับผิดกึ่งหนึ่ง โดยให้เหตุผลว่าธนาคารขาดความระมัดระวังในการเก็บรักษาทรัพย์สิน แต่ผู้บริโภคเองก็มีส่วนทำให้เกิดความเสียหาย (เส้งสุย และ ทิพย์มณี, 2566)

ทั้งนี้ ตามแนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงินของธนาคารแห่งประเทศไทย ระบุถึงเรื่องการบริหารจัดการภัยทุจริตจากการทำธุรกรรมการชำระเงิน โดยมีการกำหนดชัดเจนว่ากรณีเหตุการณ์ทุจริตที่มีผู้ถือบัตรได้รับความเสียหายที่เกี่ยวข้องกับการทำธุรกรรมชำระเงินผ่านบัตร และมีเหตุอันเชื่อได้ว่าไม่ได้เกิดจากความผิดของผู้ถือบัตรหรือผู้ถือบัตรไม่มีส่วนเกี่ยวข้อง ผู้ให้บริการต้องเยียวยาความเสียหายให้กับผู้ถือบัตรอย่างครบถ้วน (ธปท., 2566) จะเห็นได้ว่าในทางปฏิบัติ ผู้บริโภคในประเทศไทย

อาจไม่ได้รับการเยียวยาความเสียหายอย่างครบถ้วนตามข้อกำหนด แต่จำเป็นต้องมีการพิจารณาเป็นรายกรณี โดยอัตราการชดเชยเยียวยาขึ้นอยู่กับคำพิพากษาของศาล

2.10 ความคืบหน้าของนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ และมาตรการการชดเชยเยียวยาผู้เสียหายจากภัยคุกคามทางไซเบอร์ในประเทศไทย (ณ วันที่ 3 มีนาคม 2568)

ในการประชุมคณะรัฐมนตรี เมื่อวันที่ 28 มกราคม พ.ศ. 2568 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ระบุว่า *"พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ในปัจจุบันยังไม่เพียงพอต่อรูปแบบอาชญากรรมทางเทคโนโลยีที่ได้มีการพัฒนาขึ้นของกลุ่มมิจฉาชีพ โดยจากสถิติปีที่ผ่านมา ตั้งแต่เดือนตุลาคม พ.ศ. 2566 จนถึงเดือนพฤศจิกายน พ.ศ. 2567 พบคดีฉ้อโกงออนไลน์กว่า 402,542 คดี คิดเป็นมูลค่าความเสียหาย 42,662 ล้านบาท ซึ่งส่งผลเสียหายต่อประชาชน เศรษฐกิจและสังคมเป็นวงกว้าง ดังนั้น เพื่อรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ และความมั่นคงทางเศรษฐกิจให้ทันต่อสถานการณ์ จึงจำเป็นต้องตราเป็นพระราชกำหนดขึ้น ตามมาตรา 172 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย ซึ่งคณะรัฐมนตรีได้มีมติอนุมัติหลักการร่างพระราชกำหนดดังกล่าว โดยจะเป็นการแก้ไขเพิ่มเติมพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566"* (รัฐบาลไทย, 2568) มีรายละเอียดดังแสดงในตารางที่ 6

ตารางที่ 6 การเปรียบเทียบพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 กับร่างแก้ไขเพิ่มเติม พ.ศ. 2568

ประเด็น	พระราชกำหนด พ.ศ. 2566	ร่างแก้ไขเพิ่มเติม พ.ศ. 2568
การระงับใช้หมายเลขโทรศัพท์ต้องสงสัย	มาตราที่ 5 ระบุให้สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ หรือสำนักงานป้องกันและปราบปรามการฟอกเงิน มีอำนาจสั่งให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคม หรือผู้ให้บริการอื่นที่เกี่ยวข้อง เปิดเผยข้อมูลที่จำเป็นเพื่อสนับสนุนกระบวนการสืบสวนเมื่อได้รับคำสั่ง แต่ไม่มีบทบัญญัติในการระงับใช้หมายเลขโทรศัพท์ต้องสงสัย	เพิ่มอำนาจให้กับสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) และผู้ให้บริการโทรศัพท์มือถือ มีอำนาจสั่งระงับการให้บริการหมายเลขโทรศัพท์มือถือชั่วคราว หากพบเหตุอันควรสงสัยว่าหมายเลขดังกล่าวเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี เช่น การฉ้อโกงออนไลน์ หรือแก๊งคอลเซ็นเตอร์ (มาตรการระงับ "ซิมม้า" เพื่อป้องกันการนำไปใช้ในกิจกรรมผิดกฎหมาย)
การควบคุมการซื้อขายสินทรัพย์ดิจิทัลผ่านแพลตฟอร์มที่มีความเสี่ยง เพื่อป้องกันการ	ไม่มีบทบัญญัติในการควบคุมการซื้อขายสินทรัพย์ดิจิทัลผ่านแพลตฟอร์มที่มีความเสี่ยง	ห้ามการซื้อขายสินทรัพย์ดิจิทัลผ่านแพลตฟอร์ม Peer-to-Peer Lending (P2P) โดยห้ามให้บริการหรือแสดงว่าพร้อมจะให้บริการซื้อขายแลกเปลี่ยนสินทรัพย์

ประเด็น	พระราชกำหนด พ.ศ. 2566	ร่างแก้ไขเพิ่มเติม พ.ศ. 2568
ใช้สินทรัพย์ดิจิทัลเป็นเครื่องมือในการฟอกเงิน		ดิจิทัลประเภทคริปโทเคอร์เรนซี โทเคนดิจิทัล เพื่อการใช้ประโยชน์ที่มิได้มีวัตถุประสงค์หลักเพื่อการอุปโภคบริโภค (การซื้อสินทรัพย์ดิจิทัลอย่างผิดกฎหมาย) นอกจากนี้ ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องปฏิเสธการเปิดบัญชี หรือระงับธุรกรรมของลูกค้าที่มีประวัติหรือใช้กระเป๋าเงินดิจิทัลที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี
เร่งรัดกระบวนการคืนเงินให้แก่ผู้เสียหาย	ไม่มีบทบัญญัติในกระบวนการคืนเงินให้แก่ผู้เสียหาย	กำหนดให้คณะกรรมการธุรกรรมตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน มีอำนาจในการพิจารณาคืนเงินให้แก่ผู้เสียหาย โดยไม่ต้องรอคำสั่งศาลถึงที่สุด เพื่อให้กระบวนการเยียวยาเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ ลดภาระและความเดือดร้อนของประชาชนที่ได้รับผลกระทบจากอาชญากรรมไซเบอร์
เพิ่มบทลงโทษทางกฎหมายและขอบเขตความรับผิดชอบต่อความเสียหายสำหรับอาชญากรรมทางเทคโนโลยี	ไม่มีบทกำหนดโทษสำหรับผู้ให้บริการซื้อขายหรือแลกเปลี่ยนสินทรัพย์ดิจิทัล	ผู้ให้บริการซื้อขายหรือแลกเปลี่ยนสินทรัพย์ดิจิทัลที่มีส่วนเกี่ยวข้องกับการฟอกเงินจากอาชญากรรมไซเบอร์ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ
	ไม่มีบทกำหนดโทษสำหรับผู้กระทำผิดเกี่ยวกับการพนันออนไลน์	ผู้กระทำผิดเกี่ยวกับการพนันออนไลน์ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ
	มาตราที่ 12 ระบุว่าผู้ที่ได้รับหรือครอบครองข้อมูลส่วนบุคคล ไม่สามารถเปิดเผยแก่บุคคลที่ไม่มีหน้าที่เกี่ยวข้อง แต่ไม่มีบทกำหนดโทษสำหรับผู้ซื้อขายข้อมูลส่วนบุคคล	ผู้ซื้อขายข้อมูลส่วนบุคคล ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินห้าล้านบาท หรือทั้งจำทั้งปรับ
	ไม่มีบทบัญญัติในการร่วมรับผิดชอบต่อความเสียหายที่เกิดขึ้น	สถาบันการเงิน ผู้ให้บริการโทรคมนาคม ผู้ให้บริการแพลตฟอร์มออนไลน์ รวมถึงสื่อสังคมออนไลน์ ต้องร่วมรับผิดชอบต่อความเสียหายที่เกิดขึ้นกับผู้เสียหาย หากพบว่าไม่ได้

ประเด็น	พระราชกำหนด พ.ศ. 2566	ร่างแก้ไขเพิ่มเติม พ.ศ. 2568
		ดำเนินมาตรการที่เหมาะสมในการป้องกันอาชญากรรมทางเทคโนโลยี

ที่มา : พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และสรุปข่าวการประชุม ครม. 28 มกราคม 2568 (รัฐบาลไทย, 2568)

นอกจากนี้ เมื่อวันที่ 30 มกราคม 2568 ธนาคารแห่งประเทศไทย (ธปท.) ได้มีประกาศยกระดับมาตรการเชิงป้องกัน ด้วยการเพิ่มความเข้มงวดและขยายขอบเขตการตรวจสอบบัญชีต้องสงสัย เพื่อเสริมสร้างศักยภาพให้ธนาคารสามารถดำเนินการเชิงรุกในการป้องกันความเสี่ยง และรับมือกับภัยทุจริตทางการเงินได้อย่างมีประสิทธิภาพมากยิ่งขึ้น พร้อมทั้งผลักดันแนวทางการร่วมรับผิดชอบระหว่างธนาคารพาณิชย์และผู้ให้บริการทางการเงิน เพื่อเพิ่มความคุ้มครองให้แก่ประชาชนจากมิจฉาชีพทางไซเบอร์ (ธนาคารแห่งประเทศไทย, 2568) โดยมีรายละเอียดดังต่อไปนี้

1. เพิ่มประสิทธิภาพในการกวาดล้างบัญชีม้า

ธปท. กำหนดให้ธนาคารมีการพัฒนาเกณฑ์การคัดกรองบัญชีม้าอย่างต่อเนื่อง และเพิ่มความเข้มงวดและแม่นยำมากขึ้น โดยพิจารณาจาก พฤติกรรมการโอน มูลค่าธุรกรรม และรูปแบบการทำธุรกรรมที่ผิดปกติ เพื่อให้สามารถติดตามและจัดการบัญชีต้องสงสัยได้อย่างครอบคลุม ทั้งนี้ ปัจจุบันธนาคารต่างๆ มีฐานข้อมูลที่ดีขึ้น ทำให้สามารถตรวจจับบัญชีม้าได้อย่างมีประสิทธิภาพมากขึ้น เช่น การพิจารณาจากพฤติกรรมการโอนเงินออกไปในรูปแบบเงินดิจิทัล ซึ่งเป็นหนึ่งในแนวโน้มของมิจฉาชีพในปัจจุบัน โดยธนาคารแห่งประเทศไทยได้มีการกำหนดระดับความเสี่ยงของบัญชีม้าแบ่งเป็นสีต่างๆ ตามลักษณะและสถานะของบัญชี ดังนี้

- ม้าดำ: บัญชีที่ได้รับแจ้งจากฐานข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.)
- ม้าเทา: เป็นกรณีที่มีผู้เสียหายเกิดขึ้นแล้ว
  - ม้าเทาเข้ม กรณีที่ผู้เสียหายแจ้งความแล้ว
  - ม้าเทาอ่อน กรณีที่ผู้เสียหายยังไม่แจ้งความ
- ม้าน้ำตาล: บัญชีที่ยังไม่มีผู้เสียหายเกิดขึ้น แต่มีพฤติกรรมต้องสงสัย
  - ม้าน้ำตาลเข้ม กรณีที่ธนาคารมีข้อมูลมากพอในการแจ้งตำรวจ
  - ม้าน้ำตาลอ่อน กรณีที่ธนาคารกำหนดให้เป็นบัญชีต้องสงสัย

เมื่อพบว่าบัญชีใดเข้าข่ายบัญชีม้าที่มีความเสี่ยงสูง ธนาคารจะดำเนินการระงับบัญชีในทันที ส่วนบัญชีที่อยู่ในระดับความเสี่ยงต่ำกว่า อาจให้เจ้าของบัญชียืนยันตัวตนใหม่เพื่อป้องกันการใช้บัญชีโดยมิจฉาชีพ

ในอดีตบัญชีม้าน้ำตาลยังไม่มีระบบหรือกลไกที่ชัดเจนในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เนื่องจากยังไม่มีความเสียหายหรือเกิดเป็นคดีความขึ้น แต่ในปัจจุบันธนาคารมีรูปแบบพฤติกรรมที่สามารถระบุบัญชีม้าได้มากขึ้น และสามารถแจ้งไปยังหน่วยงานบังคับใช้กฎหมายได้ในทันทีที่ตรวจพบ

2. เพิ่มความเข้มข้นในการควบคุมบัญชีม้าระดับบุคคล

ธนาคารต้องขยายขอบเขตการระงับการโอนเงินออกจากบัญชีต้องสงสัยและปฏิเสธการเปิดบัญชีใหม่ให้ครอบคลุมถึงบัญชีที่มีความเสี่ยงสูงแม้ยังไม่มีรายงานความเสียหาย นอกจากนี้จะต้องมีการกันเงินที่กำลังโอนเข้าสู่บัญชีม้าหรือบัญชีต้องสงสัย พร้อมทั้งกำหนดให้ธนาคารมีการแจ้งเตือนผู้โอนเงินหากปลายทางเป็นบัญชีต้องสงสัย ป้องกันความเสียหายที่อาจเกิดขึ้นตั้งแต่ต้น และช่วยลดภาระในการดำเนินการทางกฎหมายเพื่อเรียกร้องเงินคืน

3. ขยายความร่วมมือระหว่างธนาคารให้ครอบคลุมมากขึ้น

ธนาคารจะต้องแลกเปลี่ยนข้อมูลบุคคลที่มีพฤติกรรมต้องสงสัยระหว่างกัน แม้จะยังไม่ได้รับแจ้งจากผู้เสียหาย จากเดิมที่มีการแลกเปลี่ยนเฉพาะรายชื่อในฐานข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) และรายชื่อที่ถูกแจ้งความหรือมีส่วนเกี่ยวข้องในการทุจริต เพื่อให้สามารถป้องกันภัยได้อย่างครอบคลุมรวดเร็ว และเป็นมาตรฐานเดียวกัน

4. การรับผิดชอบในหน้าที่ของตนเองตามขอบเขตมาตรฐานที่ผู้กำกับดูแลกำหนดไว้ (Shared responsibility)

ธนาคารแห่งประเทศไทย ได้ให้ความคิดเห็นว่าการแก้ไขปัญหาภัยทุจริตทางการเงินอย่างยั่งยืนนั้นจำเป็นต้องอาศัยความร่วมมือจากทุกฝ่าย ไม่ว่าจะเป็นภาคธนาคาร ผู้ให้บริการโทรคมนาคม หน่วยงานที่เกี่ยวข้อง รวมถึงประชาชน ในการรับผิดชอบหน้าที่ของตนตามขอบเขตที่ผู้กำกับดูแลกำหนด โดยหากฝ่ายใดฝ่ายหนึ่งละเลยในหน้าที่ของตน ควรเป็นฝ่ายชดเชยความเสียหายที่เกิดขึ้น

2.11 นโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของธนาคารในประเทศไทย

คณะวิจัยสำรวจนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของธนาคารไทยที่มีการเปิดเผยต่อสาธารณะ ประกอบด้วยธนาคารพาณิชย์ 8 แห่ง ได้แก่ ธนาคารกรุงเทพ ธนาคารกรุงไทย ธนาคารกรุงศรีอยุธยา ธนาคารกสิกรไทย ธนาคารไทยพาณิชย์ ธนาคารทหารไทยธนชาต ธนาคารเกียรตินาคินภัทร ธนาคารทิสโก้ และสถาบันการเงินเฉพาะกิจของรัฐ 3 แห่ง ได้แก่ ธนาคารออมสิน ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย

ธนาคารทุกแห่งเปิดเผยนโยบายด้านความปลอดภัยไซเบอร์ในรายงานประจำปี รายงานความยั่งยืนหรือเว็บไซต์ของธนาคาร โดยในภาพรวมพบว่าเนื้อหานโยบายที่เปิดเผยสอดคล้องกับแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของธนาคารแห่งประเทศไทย (นำเสนอในหัวข้อ 2.3.1) สามารถสรุปรายละเอียดในภาพรวมได้ ดังนี้

ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

ธนาคารกำหนดโครงสร้างความรับผิดชอบในการกำกับดูแลความปลอดภัยทางไซเบอร์ให้เป็นไปตามนโยบายที่กำหนด โดยกำหนดให้คณะกรรมการธนาคารมีหน้าที่ติดตามการบริหารจัดการความมั่นคงปลอดภัยด้านไซเบอร์ มีคณะทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งมีบทบาทหน้าที่ครอบคลุม อาทิ การติดตามความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ การพัฒนานโยบาย มาตรฐาน และการปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การประเมินความมั่นคงปลอดภัยทางไซเบอร์ การบริหารจัดการช่องโหว่และภัยคุกคาม การตรวจสอบเหตุการณ์ผิดปกติทางไซเบอร์ และการเสริมสร้างวัฒนธรรมความเสี่ยงทางไซเบอร์ในองค์กร เป็นต้น

ธนาคารจัดทำนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ที่สอดคล้องกับมาตรฐานสากล รวมถึงมีการจัดทำคู่มือหรือแนวทางรักษาความปลอดภัยทางไซเบอร์สำหรับพนักงานในการปฏิบัติงานให้สอดคล้องกับนโยบายของธนาคาร

ธนาคารทุกแห่งให้ความสำคัญกับนโยบายคุ้มครองข้อมูลส่วนบุคคลและมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ธนาคารหลายแห่ง อาทิ ธนาคารกรุงเทพ ธนาคารไทยพาณิชย์ มีการกำหนดผู้รับผิดชอบหรือหน่วยงานคุ้มครองข้อมูลส่วนบุคคล รับผิดชอบในการดูแลงานด้านการคุ้มครองข้อมูลส่วนบุคคล รวมถึงบริหารความเสี่ยงด้านข้อมูลส่วนบุคคลให้สอดคล้องกับการบริหารความเสี่ยงขององค์กรด้วย

การบริหารความเสี่ยงและการตรวจสอบด้านเทคโนโลยีสารสนเทศ

ธนาคารหลายแห่งบูรณาการประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงระดับองค์กร อาทิ ธนาคารทหารไทยธนชาตกำหนดให้คณะกรรมการความเสี่ยงองค์กร (Enterprise Risk Management Committee) มีหน้าที่ติดตามความเสี่ยงด้านเทคโนโลยีสารสนเทศ ธนาคารกรุงเทพ ระบุให้ “ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใหม่” เป็นประเด็นความเสี่ยงระดับองค์กรที่ธนาคารต้องเผชิญในระยะ 3-5 ปีข้างหน้า และจำเป็นต้องติดตามวิเคราะห์สถานการณ์และเตรียมพร้อมรับมือ ธนาคารเกียรตินาคินภัทร กำหนดให้ความเสี่ยงจากภัยคุกคามทางไซเบอร์ เป็นปัจจัยความเสี่ยงที่อาจเกิดขึ้นกับธนาคารในอนาคต โดยธนาคารจะประเมินและติดตามความเสี่ยง พร้อมทั้งรายงานแก่คณะกรรมการกำกับความเสี่ยง และคณะกรรมการธนาคารเป็นรายไตรมาส เป็นต้น

ธนาคารกำหนดให้มีการตรวจสอบกระบวนการจัดการด้านความปลอดภัยของเทคโนโลยีสารสนเทศ เช่น ธนาคารกรุงเทพ กำหนดให้มีการตรวจสอบกระบวนการจัดการด้านความปลอดภัยของเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยหน่วยงานรับรองอิสระภายนอก ธนาคารเกียรตินาคินภัทร ระบุว่าธนาคารมีการเฝ้าระวัง และตรวจสอบประสิทธิภาพความพร้อมของระบบเทคโนโลยีสารสนเทศเป็นประจำอย่างสม่ำเสมอ เป็นต้น

การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ธนาคารทุกแห่งให้ความสำคัญกับการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังเห็นได้จากการดำเนินงานที่สอดคล้องกับมาตรฐานสากล อาทิ มาตรฐาน NIST มาตรฐาน ISO/IEC 27001 : 2013 สำหรับระบบการโอนเงินทางอิเล็กทรอนิกส์ระหว่างสถาบันการเงิน (BAHTNET) และระบบการหักบัญชีเช็กด้วยภาพและการจัดเก็บภาพเช็ก (ICAS) เป็นต้น

ธนาคารกำหนดระเบียบที่เข้มงวดสำหรับการเข้าถึงข้อมูลที่คำนึงถึงความมั่นคงปลอดภัยทางไซเบอร์ อาทิ การกำหนดชั้นความลับและสิทธิ์การเข้าถึงข้อมูล การเข้ารหัสข้อมูล การติดตั้งระบบความปลอดภัยให้กับอุปกรณ์ฮาร์ดแวร์ของธนาคาร การตรวจจับมัลแวร์อย่างสม่ำเสมอ การตรวจสอบข้อมูลรั่วไหลจากแหล่งต่าง ๆ และนำข้อมูลมาวิเคราะห์เพื่อหาแนวทางป้องกัน เป็นต้น

ในด้านการติดตามเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ ธนาคารหลายแห่งนำเทคโนโลยีมาช่วยในการตรวจจับและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ อาทิ ธนาคารกสิกรไทย และธนาคารไทยพาณิชย์ ระบุว่าใช้เทคโนโลยี AI และ Machine Learning ในการตรวจจับภัยคุกคาม เป็นต้น

นอกจากนี้ ธนาคารหลายแห่งกำหนดให้มีหน่วยงานในการเฝ้าระวังและตรวจจับสถานการณ์หรือเหตุผิดปกติที่อาจสร้างความเสียหายต่อข้อมูลและระบบสารสนเทศของธนาคาร ตลอด 24 ชั่วโมง อาทิ ธนาคารกรุงไทย จัดตั้งศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ (Hybrid CSOC) และเฝ้าระวังตลอด 24 ชั่วโมง หรือธนาคารกรุงเทพ กำหนดให้มีหน่วยงานติดตามเหตุการณ์หรือภัยคุกคามทางไซเบอร์ โดยแบ่งเป็น 3 ระดับ คือ หน่วยงานเฝ้าระวัง (Tier 1) มีหน้าที่ติดตามเหตุการณ์ทางไซเบอร์ตลอด 24 ชั่วโมง โดยหากพบเหตุผิดปกติ จะต้องทำบันทึกเหตุการณ์และแจ้งให้ผู้ดูแลระบบหรือผู้รับผิดชอบอุปกรณ์ด้านความปลอดภัยที่เกี่ยวข้อง (Tier 2) เพื่อวิเคราะห์และตรวจสอบเหตุผิดปกติเชิงลึก และหากเหตุดังกล่าวมีความซับซ้อนมากก็จะมีหน่วยงานด้านความปลอดภัย (Tier 3) ช่วยตรวจสอบเหตุผิดปกติดังกล่าว รวมถึงวิเคราะห์สาเหตุและหาแนวทางจัดการร่วมกับผู้เกี่ยวข้องต่อไป

ธนาคารหลายแห่งเปิดเผยแนวปฏิบัติในการจัดการเหตุฉุกเฉิน และกำหนดให้มีการทดสอบและซ้อมแผนรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ 1 ครั้ง รวมถึงเข้าร่วมซ้อมแผนรับมือภัยคุกคามทางไซเบอร์กับธนาคารอื่นที่อยู่ภายใต้ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) ด้วย

ธนาคารมีการสื่อสาร อบรม สร้างความตระหนักให้พนักงานเท่าทันภัยคุกคามทางไซเบอร์ อาทิ การจัดทำหลักสูตรอบรมหรือเผยแพร่ความรู้ผ่านช่องทางของธนาคาร การสร้างสถานการณ์จำลองโดยส่ง Phishing email ให้ผู้บริหาร และพนักงาน เพื่อทดสอบการตอบสนองของผู้ได้รับอีเมล เป็นต้น

การรับเรื่องร้องเรียนจากลูกค้า และมาตรการชดเชยเยียวยา กรณีภัยคุกคามทางไซเบอร์หรือการละเมิดข้อมูลส่วนบุคคล

ธนาคารทุกแห่งเปิดเผยช่องทางการรับเรื่องร้องเรียนจากลูกค้า อย่างไรก็ตาม มีธนาคารเพียงบางแห่งที่ระบุช่องทางรับเรื่องร้องเรียนกรณีได้รับผลกระทบจากการโจมตีทางไซเบอร์ หรือเกิดเหตุละเมิดข้อมูลส่วนบุคคล รวมถึงเปิดเผยแนวทางในการดำเนินการเมื่อได้รับข้อร้องเรียนดังกล่าว อาทิ ธนาคารกรุงเทพ เปิดเผยขั้นตอนการดำเนินการเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล และระบุให้ลูกค้าสามารถแจ้งเรื่องร้องเรียนกรณีการละเมิดข้อมูลส่วนบุคคลผ่านช่องทางร้องเรียนของธนาคาร หรือผ่านหน่วยงานคุ้มครองข้อมูลส่วนบุคคล ธนาคารเกียรตินาคินภัทร กำหนดให้มีช่องทางการรับเรื่องร้องเรียนด้านความปลอดภัยของข้อมูลผ่านหน่วยงาน KKP Contact Center เป็นต้น

สำหรับมาตรการชดเชยเยียวยานั้น คณะวิจัยไม่พบข้อมูลที่ชัดเจนเกี่ยวกับมาตรการชดเชยเยียวยาในกรณีภัยคุกคามทางไซเบอร์หรือการละเมิดข้อมูลส่วนบุคคล ทั้งนี้ แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงินของธนาคารแห่งประเทศไทย ระบุว่ากรณีเหตุการณ์ทุจริตที่มีผู้เสียหายจากการทำธุรกรรมการชำระเงิน โดยไม่ได้เกิดจากความผิดของผู้เสียหาย ผู้ให้บริการต้องเยียวยาความเสียหายอย่างครบถ้วน (ดังที่ได้นำเสนอในหัวข้อ 2.9.2) หรือกล่าวอีกนัยหนึ่ง การชดเชยเยียวยาผู้เสียหายจะเป็นการพิจารณาเป็นรายกรณี โดยอัตราการชดเชยเยียวยาขึ้นอยู่กับคำพิพากษาของศาล

บทที่ 3 สรุปผลการสัมภาษณ์เชิงลึก

คณะวิจัยได้สัมภาษณ์เชิงลึกผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ระหว่างวันที่ 2 ธันวาคม พ.ศ. 2567 จนถึงวันที่ 14 กุมภาพันธ์ พ.ศ. 2568 ใน 8 กลุ่มเป้าหมายและหน่วยงานของผู้มีส่วนได้ส่วนเสีย รวมจำนวนผู้ให้สัมภาษณ์ทั้งสิ้น 47 คน จาก 32 หน่วยงานและผู้มีส่วนได้ส่วนเสีย

ตารางที่ 7 สรุปจำนวนผู้ให้สัมภาษณ์ตามประเภทของกลุ่มเป้าหมายและหน่วยงาน

ประเภทหน่วยงาน	จำนวนผู้ให้สัมภาษณ์ (คน)	จำนวนหน่วยงาน
หน่วยงานกำกับดูแลธนาคาร	1	1
ธนาคาร	12	5
หน่วยงานด้านความมั่นคงไซเบอร์และการให้บริการดิจิทัล	8	4
หน่วยงานบังคับใช้กฎหมาย	2	2
หน่วยงานกำกับดูแลด้านโทรคมนาคม	4	1
องค์กรภาคประชาสังคมในต่างประเทศ	4	3
หน่วยงานคุ้มครองผู้บริโภค	2	2
ผู้บริโภค		
ทนาย	4	4
ผู้เชี่ยวชาญ	2	2
ผู้เสียหาย	8	8
รวม	**47**	**32**

โดยคณะวิจัยได้สรุปผลการสัมภาษณ์ และข้อค้นพบที่น่าสนใจ จำแนกเป็นรายกลุ่มและรายประเด็นดังนี้

3.1 ภาพรวมของภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงิน

ภัยคุกคามทางไซเบอร์เป็นอุปสรรคสำคัญต่อความมั่นคงทางการเงิน โดยเฉพาะอย่างยิ่งในยุคที่บริการ mobile banking เป็นช่องทางหลักของธุรกรรมทางการเงิน ที่ทำให้ปัจจุบันรูปแบบการโจมตีของมิจฉาชีพมุ่งเน้นการหลอกลวงผู้ใช้ปลายทาง โดยเฉพาะการใช้เทคนิค social engineering หรือการที่มิจฉาชีพใช้จิตวิทยาเพื่อชักจูงให้เหยื่อเปิดเผยข้อมูลสำคัญเอง (Authorize) แทนการเจาะระบบของธนาคารโดยตรง เพื่อลดความเสี่ยงในการถูกตรวจจับ

ทั้งนี้ ผู้ให้สัมภาษณ์ทุกกลุ่มเห็นตรงกันว่าการเพิ่มขึ้นของการหลอกลวงทางไซเบอร์ การใช้บัญชีม้าและการใช้ซิมม้าเป็นเครื่องมือหนึ่งในการก่ออาชญากรรมทางการเงิน และส่งผลให้ทุกฝ่ายที่เกี่ยวข้องต้อง

ดำเนินมาตรการต่าง ๆ ที่เข้มงวดขึ้น อย่างไรก็ตาม เนื่องจากการจัดการภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับภาคการเงินมีหน่วยงานที่เกี่ยวข้องจำนวนมาก และมีบทบาทหน้าที่แตกต่างกัน เช่น หน่วยงานกำกับดูแลด้านโทรคมนาคมให้ความสำคัญกับการควบคุมการใช้โทรศัพท์ แพลตฟอร์มดิจิทัล และซิมม้า หน่วยงานกำกับดูแลทางการเงินมุ่งเน้นไปที่การควบคุมบัญชีม้าและตรวจสอบธุรกรรมที่ผิดปกติ หน่วยงานบังคับใช้กฎหมายเผชิญกับความท้าทายในการติดตามและดำเนินคดีกับมิจฉาชีพ เป็นต้น ดังนั้น การจัดการภัยคุกคามดังกล่าวจึงจำเป็นต้องมีการบูรณาการความร่วมมือระหว่างหน่วยงานให้มีแนวทางที่เป็นรูปธรรมมากขึ้น

3.1.1 ลักษณะของภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงิน

จากการสัมภาษณ์ผู้มีส่วนได้ส่วนเสียในภาพรวม พบว่าภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อระบบธนาคารและผู้ใช้บริการมีหลายรูปแบบ ได้แก่

- การโจมตีแบบฟิชชิง (phishing attacks) กล่าวคือ มิจฉาชีพใช้เว็บไซต์หรือข้อความปลอมแปลงเพื่อขโมยข้อมูลผู้ใช้ กลโกงฟิชชิงพัฒนาขึ้นให้สามารถเลียนแบบเว็บไซต์ธนาคารได้อย่างแนบเนียนมากขึ้น ทำให้ผู้ใช้หลายรายตกเป็นเหยื่อโดยไม่รู้ตัว นอกจากนี้ ยังพบว่าการโจมตีฟิชชิงในปัจจุบันมีการใช้ข้อมูลส่วนบุคคลที่ถูกขโมยมาจากแหล่งอื่นเพื่อเพิ่มความน่าเชื่อถือของข้อความหลอกลวง
- ภัยจากการหลอกการลงทุน มีลักษณะสำคัญที่คล้ายคลึงกันในหลายกรณี โดยมิจฉาชีพมักสร้างแพลตฟอร์มการลงทุนปลอมและโฆษณาผ่านช่องทางออนไลน์ เพื่อดึงดูดให้ประชาชนลงทุนในระบบที่ไม่มีอยู่จริง ผู้ให้สัมภาษณ์จากหลายหน่วยงานระบุว่ากลโกงการลงทุนปลอมมีการพัฒนาให้ซับซ้อนขึ้น โดยมิจฉาชีพมักใช้การแอบอ้างเป็นหน่วยงานภาครัฐหรือองค์กรทางการเงิน เพื่อทำให้เหยื่อหลงเชื่อ
- มัลแวร์และแอปพลิเคชันปลอม (malware & fake applications) โดยมีการแพร่กระจายมัลแวร์ผ่านแอปพลิเคชันปลอมที่หลอกให้ผู้ใช้ติดตั้ง มัลแวร์เหล่านี้สามารถเข้าถึงข้อมูลสำคัญ เช่น รหัสผ่าน รายละเอียดบัญชีธนาคาร และสามารถสอดแนมพฤติกรรมการใช้โทรศัพท์มือถือของเหยื่อเพื่อหาช่องโหว่ในการโจมตี
- การโจมตีระบบธนาคารด้วยปริมาณคำขอจำนวนมากเพื่อให้บริการล่มชั่วคราว ส่งผลให้ผู้ใช้บริการไม่สามารถเข้าถึง mobile banking ได้ในช่วงเวลาสำคัญ การโจมตีประเภทนี้มักถูกใช้เพื่อเบี่ยงเบนความสนใจของทีมรักษาความปลอดภัยไซเบอร์ ในขณะที่มิจฉาชีพดำเนินการโจมตีข้อมูลทางการเงินแบบอื่น ๆ ควบคู่ไปด้วย
- การใช้ social engineering หรือเทคนิคทางจิตวิทยาที่มิจฉาชีพใช้เพื่อโน้มน้าวให้เหยื่อดำเนินการตามที่ต้องการ เช่น ให้โอนเงินหรือเปิดเผยข้อมูลส่วนตัว ในบางกรณีมีการใช้ Deepfake หรือ AI-generated voice เพื่อเพิ่มความสมจริงในการหลอกลวงผ่านการโทรศัพท์หรือวิดีโอคอล

- การเจาะระบบและขโมยข้อมูล มีการใช้เทคนิคการเจาะระบบเพื่อขโมยฐานข้อมูลลูกค้าของธนาคาร ซึ่งข้อมูลที่ถูกขโมยสามารถนำไปขายในตลาดมืด หรือนำไปใช้เป็นเครื่องมือสำหรับการหลอกลวงในรูปแบบอื่น ๆ
- การโจมตีผ่าน IoT และอุปกรณ์เชื่อมต่ออินเทอร์เน็ต มิจฉาชีพเริ่มใช้ประโยชน์จากความไม่ปลอดภัยของอุปกรณ์ IoT เช่น กล้องวงจรปิดหรือสมาร์ทโฮม เพื่อเข้าถึงเครือข่ายธนาคารและขโมยข้อมูลสำคัญ

3.1.2 การใช้บัญชีม้าในกระบวนการฉ้อโกง

บัญชีม้าเป็นเครื่องมือสำคัญที่ถูกใช้ในการฟอกเงินและทำธุรกรรมผิดกฎหมาย ซึ่งพบว่ามีการพัฒนาเทคนิคการใช้บัญชีม้าที่ซับซ้อนมากขึ้น ไม่เพียงแต่เป็นบัญชีที่บุคคลถูกจ้างให้เปิด แต่ยังรวมถึงการใช้เอกสารปลอมเพื่อเปลี่ยนเจ้าของบัญชี และการสร้างเครือข่ายบัญชีม้าหลายชั้นเพื่อกระจายเส้นทางการเงินให้ตรวจสอบได้ยากขึ้น บัญชีม้าจึงมีบทบาทสำคัญในการฟอกเงินและอำนวยความสะดวกให้มิจฉาชีพ โดยมีการแบ่งประเภทของบัญชีต้องสงสัยออกเป็น 3 กลุ่ม คือ

1) บัญชีม้าดำ เป็นบัญชีที่ได้รับการยืนยันว่าเกี่ยวข้องกับการฉ้อโกงและอยู่ในรายการเฝ้าระวัง

2) บัญชีม้าเทา บัญชีที่มีธุรกรรมผิดปกติแต่ยังไม่มีหลักฐานเพียงพอในการบ่งชี้ว่าเป็นบัญชีอาชญากรรม

3) บัญชีม้าน้ำตาล บัญชีที่มีพฤติกรรมเสี่ยงแต่ยังไม่ถูกนำเข้าระบบแจ้งเตือน

ผู้ให้สัมภาษณ์ในกลุ่มหน่วยงานกำกับดูแลธนาคารและกลุ่มธนาคารมีมุมมองร่วมกันว่า การใช้บัญชีม้าเป็นภัยที่สำคัญต่อระบบการเงิน จำเป็นต้องมีมาตรการเฝ้าระวังที่เข้มงวด และควรบูรณาการการทำงานร่วมกันระหว่างหน่วยงานเพิ่มขึ้น เพื่อป้องกันการใช้บัญชีม้าในกระบวนการฉ้อโกง รวมทั้งมีข้อเสนอให้พัฒนาและใช้เทคโนโลยีในการตรวจจับบัญชีต้องสงสัย เช่น การใช้ AI และการแลกเปลี่ยนข้อมูลผ่านระบบกลาง

โดยผู้ให้สัมภาษณ์ในกลุ่มธนาคารให้ความสำคัญกับการจัดทำมาตรการความปลอดภัยภายในองค์กร เช่น การตรวจสอบพฤติกรรมการทำธุรกรรมแบบเรียลไทม์และการใช้ Central Fraud Registry เพื่อระบุบัญชีต้องสงสัย ผู้ให้สัมภาษณ์ในกลุ่มหน่วยงานคุ้มครองผู้บริโภคให้ความสำคัญกับการให้ลูกค้าสามารถเข้าถึงข้อมูลเกี่ยวกับบัญชีที่มีความเสี่ยงก่อนทำธุรกรรม และผู้ให้สัมภาษณ์ในกลุ่มหน่วยงานกำกับดูแลและ หน่วยงานด้านนโยบาย ให้ความสำคัญกับการเพิ่มบทลงโทษให้รุนแรงขึ้น เพื่อป้องกันไม่ให้ประชาชนถูกชักจูงให้เปิดบัญชีม้า อย่างไรก็ตาม ผู้ให้สัมภาษณ์บางส่วนเห็นว่าการบังคับใช้กฎหมายที่รุนแรงอาจทำให้ผู้ที่ตกเป็นเหยื่อโดยไม่รู้ตัวได้รับผลกระทบที่ไม่เป็นธรรม

3.1.3 การใช้ซิมม้าในกระบวนการฉ้อโกง

ซิมม้าเป็นปัจจัยที่ช่วยให้มิจฉาชีพสามารถกระทำผิดโดยไม่สามารถตรวจสอบตัวตนที่แท้จริงได้ โดยมีการลงทะเบียนซิมโดยใช้ข้อมูลปลอม เอกสารปลอม หรือบางกรณีผู้เปิดซิมอาจเป็นบุคคลที่ไม่รู้ตัวว่า

ข้อมูลของตนถูกนำไปใช้ รวมถึงมีการซื้อขายซิมม้ากันในตลาดมืด มิจฉาชีพอาจใช้ซิมม้าในการปลอมเป็นเจ้าหน้าที่รัฐเพื่อลวงให้เหยื่อโอนเงิน หรือการใช้ซิมม้าในการรับรหัส OTP สำหรับเข้าถึงบัญชีธนาคารของเหยื่อโดยไม่ได้รับอนุญาต หรือใช้ในการหลอกลวงผ่านโทรศัพท์ เป็นต้น

โดยผู้ให้สัมภาษณ์ส่วนใหญ่เห็นตรงกันว่าการตรวจสอบซิมม้ายังต้องเผชิญความท้าทาย เนื่องจากมิจฉาชีพมักปรับตัวและหาช่องทางใหม่ ๆ ในการหลบเลี่ยงข้อกำหนดทางกฎหมาย ผู้ให้สัมภาษณ์บางส่วนเห็นว่าควรมีการเพิ่มความเข้มงวดในการลงทะเบียนซิม ซึ่งที่ผ่านมาสำนักงาน กสทช. ได้มีมาตรการเพิ่มความเข้มงวดในการลงทะเบียนซิม เช่น การใช้ระบบ e-KYC (Electronic Know Your Customer) และการจำกัดจำนวนซิมที่บุคคลหนึ่งสามารถลงทะเบียนได้ ควบคู่กับการบังคับใช้กฎหมายที่ของหน่วยงานบังคับใช้กฎหมายให้เข้มงวดมากขึ้น เพื่อป้องกันการแพร่กระจายของซิมม้าในตลาดมืด

อย่างไรก็ตาม ผู้ให้สัมภาษณ์ที่อยู่ในภาคธนาคารพาณิชย์และภาคเอกชนเห็นว่า การบังคับใช้มาตรการที่เข้มงวดเกินไปอาจกระทบต่อความสะดวกของผู้ใช้งานทั่วไป หรือผู้ใช้งานที่ต้องมีซิมหลายเบอร์เพื่อวัตถุประสงค์ทางธุรกิจ

ทั้งนี้ ผู้ให้สัมภาษณ์ในกลุ่มหน่วยงานคุ้มครองผู้บริโภคเห็นว่าควรมีระบบแจ้งเตือนหมายเลขโทรศัพท์ต้องสงสัยก่อนรับสายหรือทำธุรกรรมแบบเรียลไทม์ รวมถึงระดับความเสี่ยงของลิงก์ที่ได้รับผ่าน SMS และควรเพิ่มการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับอันตรายของซิมม้า เพื่อลดการใช้ซิมม้าในการกระทำความผิดทางการเงิน

3.2 ผู้มีส่วนได้ส่วนเสียในกลุ่มธนาคาร

3.2.1 ข้อจำกัดและความท้าทายในการจัดการปัญหาภัยคุกคามทางไซเบอร์

ผู้ให้สัมภาษณ์เห็นว่ามิจฉาชีพปรับเปลี่ยนกลยุทธ์และพัฒนาเทคนิคการโจมตีอยู่ตลอดเวลา ทำให้รูปแบบภัยคุกคามทางไซเบอร์มีการเปลี่ยนแปลงอย่างรวดเร็วและซับซ้อนมากขึ้น การป้องกันระบบเทคโนโลยีสารสนเทศของธนาคารให้ปลอดภัยจึงเป็นความท้าทายอย่างยิ่ง

เพื่อลดช่องโหว่และเพิ่มขีดความสามารถในการรับมือกับภัยคุกคาม ธนาคารต่าง ๆ จึงมีการดำเนินงานร่วมกันผ่านกลไกของศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (Thailand Banking Sector Computer Emergency Response Team : TB-CERT) ซึ่งเป็นหน่วยงานกลางที่ช่วยให้ธนาคารสามารถแลกเปลี่ยนองค์ความรู้ เทคโนโลยี และข้อมูลเกี่ยวกับรูปแบบภัยคุกคามทางไซเบอร์ล่าสุด เพื่อเสริมสร้างมาตรการป้องกันและเพิ่มความพร้อมในการรับมือกับภัยไซเบอร์ที่อาจเกิดขึ้น

อย่างไรก็ตาม ธนาคารยังเผชิญอุปสรรคสำคัญในการป้องกันธุรกรรมที่มีความเสี่ยง โดยเฉพาะภัยคุกคามประเภทที่ผู้ใช้งานเป็นผู้ดำเนินการเอง (Authorize Fraud) ซึ่งมิใช่การโจมตีระบบของธนาคาร แต่มิจฉาชีพมุ่งเป้าหลอกลวงเจ้าของบัญชีให้ดำเนินการโอนเงินด้วยตนเอง ทำให้ธนาคารไม่สามารถตรวจจับความผิดปกติของธุรกรรมได้ เนื่องจากกรณีนี้มักมีลักษณะเหมือนการโอนเงินโดยทั่วไป นอกจากนี้

ผู้ให้สัมภาษณ์เห็นว่ามิจฉาชีพยังไม่มีความเกรงกลัวต่อกฎหมาย ส่งผลให้การเพิ่มมาตรการควบคุมหรือบทลงโทษ อาจไม่ได้ช่วยแก้ไขปัญหาปัญคุกคามทางไซเบอร์ได้

ทั้งนี้ แม้ว่าในภาคธนาคารจะมีการสร้างความร่วมมือกันผ่านกลไก TB-CERT แต่ผู้ให้สัมภาษณ์เห็นว่าการจัดการปัญหาภัยคุกคามทางไซเบอร์ในภาพรวม ยังขาดความร่วมมือที่เป็นระบบจากหน่วยงานที่มีส่วนเกี่ยวข้อง ส่งผลให้มิจฉาชีพสามารถใช้ช่องโหว่ในระบบเพื่อก่ออาชญากรรมได้อย่างต่อเนื่อง อาทิ

- ผู้ให้บริการแพลตฟอร์มดิจิทัลยังไม่มีมาตรการที่เข้มงวดในการตรวจสอบบัญชีปลอม (Fake Account) ทำให้มิจฉาชีพสามารถใช้บัญชีเหล่านี้เพื่อหลอกลวงประชาชนได้อย่างง่ายดาย
- ผู้ให้บริการโทรคมนาคมและ สำนักงาน กสทช. ยังไม่มีมาตรการเด็ดขาดในการบล็อก SMS ปลอม และสาย Call Center ของมิจฉาชีพ ส่งผลให้ประชาชนยังคงได้รับข้อความและสายโทรศัพท์หลอกลวงอยู่เป็นประจำ
- สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ยังไม่ได้กำหนดมาตรการควบคุมที่เข้มงวดในการป้องกันการใช้สินทรัพย์ดิจิทัล มิจฉาชีพสามารถโอนเงินออกนอกประเทศผ่านสินทรัพย์ดิจิทัลได้ง่าย ส่งผลให้การติดตามเส้นทางการเงินเป็นไปอย่างยากลำบาก
- เมื่อเกิดเหตุขึ้นกระบวนการดำเนินคดีของตำรวจยังล่าช้า เนื่องจากประชาชนยังมีความเข้าใจที่จำกัดเกี่ยวกับบทบาทและหน้าที่ของศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (Anti Online Scam Center : AOC) ดังนั้น เมื่อประชาชนตกเป็นเหยื่อของมิจฉาชีพ ประชาชนมักจะแจ้งความที่สถานีตำรวจหรือแจ้งมายังธนาคาร แทนที่จะติดต่อไปยังศูนย์ AOC โดยตรง ส่งผลให้กระบวนการส่งเรื่องไปยังตำรวจไซเบอร์เกิดความล่าช้า
- จำนวนบุคลากรของศูนย์ AOC มีไม่เพียงพอต่อการให้ความช่วยเหลือในคดีหลอกลวงทางการเงินที่เพิ่มขึ้นอย่างต่อเนื่อง นอกจากนี้ ศูนย์ AOC ยังขาดกระบวนการรายงานความคืบหน้าในการสืบสวนและสอบสวนให้ประชาชนรับทราบ ส่งผลต่อความเชื่อมั่นของประชาชนที่ลดลง

ผู้ให้สัมภาษณ์เห็นว่า ความรู้ ความเข้าใจในประเด็นการป้องกันภัยคุกคามทางไซเบอร์เป็นหนึ่งในข้อจำกัดสำคัญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยจากการสัมภาษณ์พบว่า ธนาคารมีการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้แก่เจ้าหน้าที่ของธนาคาร แต่ยังขาดกระบวนการวัดและติดตามผลความเข้าใจในประเด็นดังกล่าว

ขณะที่ในด้านการสร้างความตระหนักรู้ให้กับประชาชน ผู้ให้สัมภาษณ์เห็นว่า ผู้ใช้บริการทางการเงินคือ ช่องว่างสำคัญที่เปิดโอกาสให้มิจฉาชีพสามารถก่ออาชญากรรมทางการเงินหรือขโมยข้อมูลส่วนตัวได้ วิธีการที่มิจฉาชีพใช้มักอาศัยจิตวิทยาในการล่อลวงเหยื่อ เพื่อให้หลงเชื่อและดำเนินธุรกรรมโดยไม่รู้ตัว เช่น ประชาชนกลุ่มเปราะบาง โดยเฉพาะในกลุ่มผู้สูงอายุหรือเกษตรกร ซึ่งยังมีข้อจำกัดในการพิจารณาว่าข้อมูลที่ตนเองได้รับผ่านช่องทางออนไลน์นั้นเป็นข้อมูลจริงหรือเป็นการหลอกลวงจากมิจฉาชีพ รวมถึงกรณีที่มิจฉาชีพปลอมแปลงเป็นเจ้าหน้าที่หน่วยงานภาครัฐ การข่มขู่ (เช่น การอ้างว่ามีคดีความ) หรือการใช้รูปโปรไฟล์ของบุคคลที่มีหน้าตาดี (romance scam) เพื่อหลอกผ่านแอปพลิเคชันไลน์ เป็นต้น

นอกจากนี้ ประชาชนกลุ่มเปราะบาง โดยเฉพาะกลุ่มเกษตรกรยังมีระดับความสนใจต่อมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับต่ำ เห็นได้จากระดับความสนใจต่อการทำแบบสอบถามการตระหนักรู้ต่อภัยทุจริตผ่านระบบ mobile banking ที่กลุ่มเกษตรกรมักจะไม่สนใจในการทำแบบประเมินดังกล่าว

3.2.2 ข้อจำกัดและความท้าทายในการจัดการปัญหาบัญชีม้า

ผู้ให้สัมภาษณ์ให้ข้อมูลว่า การจำกัดปริมาณการเปิดบัญชีต่อคน เป็นหนึ่งในแนวทางการจัดการปัญหาบัญชีม้า อย่างไรก็ตาม ธนาคารไม่สามารถจำกัดจำนวนบัญชีที่ลูกค้าสามารถเปิดได้ เนื่องจากส่งผลกระทบต่อรายได้ของธนาคาร นอกจากนี้ ธนาคารต้องเผชิญความท้าทายในตรวจสอบพฤติกรรมของบัญชีที่มีความผิดปกติ เนื่องจากมิจฉาชีพมีการปรับเปลี่ยนรูปแบบของบัญชีม้าที่ทำให้ตรวจสอบได้ยากขึ้น เช่น การเปิดบัญชีทิ้งไว้เป็นระยะเวลานาน และฝากเงินขั้นต่ำไว้เพื่อหลีกเลี่ยงการจ่ายค่ารักษาบัญชี ส่งผลให้บัญชีมีลักษณะคล้ายคลึงกับบัญชีปกติของประชาชนทั่วไป และรอดจากการตรวจจับของธนาคาร หรือการเปิดบัญชีที่สาขาและช่องทางดิจิทัล จากนั้นจึงขายต่อให้มิจฉาชีพอีกทอดหนึ่ง ส่งผลให้ธนาคารไม่สามารถตรวจจับบัญชีม้าได้ตั้งแต่กระบวนการเปิดบัญชี เป็นต้น ที่ผ่านมาธนาคารมีการแลกเปลี่ยนข้อมูลบัญชีต้องสงสัยระหว่างกันเพื่อช่วยในการติดตามและตรวจสอบบัญชีต้องสงสัยได้เร็วขึ้น

นอกจากนี้ การพัฒนาและปรับปรุงระบบตรวจจับบัญชีม้าเป็นกระบวนการภายในของธนาคารที่ต้องใช้ระยะเวลาดำเนินการ ไม่สามารถดำเนินการได้ทันที และบางธนาคารมีงบประมาณจำกัดสำหรับการพัฒนาระบบดังกล่าว ซึ่งเป็นอุปสรรคที่ทำให้ธนาคารอาจไม่สามารถรับมือมิจฉาชีพได้อย่างทันท่วงที

ผู้ให้สัมภาษณ์ให้ข้อมูลว่า ข้อจำกัดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act : PDPA) ทำให้ยังไม่สามารถแลกเปลี่ยนข้อมูลผู้ต้องสงสัยระหว่างหน่วยงานภาครัฐและธนาคารได้แบบเรียลไทม์ ธนาคารจึงไม่สามารถระงับหรืออายัดบัญชีต้องสงสัยได้ (บัญชีที่ต้องสงสัยว่าจะเป็นบัญชีม้า แต่ยังไม่ได้รับการแจ้งความ)

ความล่าช้าในกระบวนการอายัดบัญชีม้าเป็นอีกหนึ่งสาเหตุที่ทำให้การระงับเส้นทางทางการเงินของมิจฉาชีพไม่สามารถดำเนินการได้อย่างทันท่วงที เนื่องด้วยธนาคารไม่มีอำนาจหน้าที่ในการอายัดบัญชีโดยตรง แต่ต้องอาศัยอำนาจของตำรวจ หรือสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ในการระงับบัญชี โดยกระบวนการแจ้งความจนถึงกระบวนการอายัดบัญชียังมีความล่าช้า และไม่ทันต่อการส่งผ่านเงินของมิจฉาชีพ โดยเฉพาะกรณีที่เงินถูกโอนไปยังต่างประเทศ

ผู้ให้สัมภาษณ์เห็นว่ามาตรการในการคืนสถานะบัญชีม้ายังมีช่องโหว่ในกระบวนการยกเลิกสถานะบัญชีม้า ซึ่งนำไปสู่ปรากฏการณ์ "บัญชีม้าหมุนเวียน" หรือ "ม้าที่ไม่ตาย" โดยเมื่อบุคคลใดถูกระบุว่าเป็น “บัญชีม้าเทา” และต้องการปลดล็อกบัญชี สามารถดำเนินการทางกฎหมายได้โดยเข้าสู่กระบวนการไกล่เกลี่ยหรือใช้วิธีการให้ผู้เสียหายยินยอมถอนแจ้งความ และเมื่อการไกล่เกลี่ยสำเร็จ สถานะของบัญชีจะถูกปลดจาก

ม้าเทากลายเป็น "ม้าขาว" กล่าวคือ บุคคลนั้นสามารถกลับมาใช้บัญชีธนาคารได้ตามปกติ (สามารถกลับไปเปิดบัญชีใหม่ได้)

นอกจากนี้ ผู้ให้สัมภาษณ์เห็นว่าบทลงโทษของผู้ที่รับเปิดบัญชีม้ายังไม่เข้มงวดมากพอ ดังเห็นได้จากผู้ที่ถูกดำเนินคดีจากการเปิดบัญชีม้ายังมีสัดส่วนที่น้อย ขณะที่บทลงโทษยังไม่รุนแรงพอจนทำให้ประชาชนไม่กล้ารับจ้างเปิดบัญชีม้า

3.2.3 ข้อจำกัดและความท้าทายในการเยียวยาปัญหาภัยคุกคามทางไซเบอร์และบัญชีม้า

ผู้ให้สัมภาษณ์ระบุว่า ธนาคารยังมีความท้าทายในการกำหนดมาตรฐานและหลักเกณฑ์กลางที่ชัดเจนสำหรับการเยียวยาผู้เสียหาย โดยปัจจุบันเมื่อลูกค้าของธนาคารได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ การเยียวยาผู้เสียหายจะพิจารณาเป็นรายกรณี เช่น กรณีที่ความเสียหายเกิดจากความผิดพลาดของระบบธนาคาร ลูกค้ามักจะได้รับเงินคืนเต็มจำนวน แต่หากกรณีที่ความเสียหายเกิดจากความประมาทของลูกค้าเอง เช่น ลูกค้าเป็นผู้เปิดเผยข้อมูลส่วนตัวให้มิจฉาชีพ ธนาคารจะไม่สามารถคืนเงินให้ลูกค้าได้เต็มจำนวน เป็นต้น

3.2.4 ข้อเสนอแนะของผู้มีส่วนได้ส่วนเสียในกลุ่มธนาคาร

ผู้ให้สัมภาษณ์ในกลุ่มธนาคารเห็นว่า ภาคธนาคารควรดำเนินมาตรการรักษาความปลอดภัยแบบครบวงจร ตั้งแต่การตรวจสอบข้อมูลลูกค้า การแจ้งเตือนธุรกรรมที่มีความเสี่ยง ไปจนถึงการใช้ข้อมูลจากผู้ให้บริการโทรคมนาคมเพื่อตรวจจับพฤติกรรมที่ผิดปกติของบัญชีต้องสงสัย นอกจากนี้ ควรพัฒนาระบบแจ้งเตือนลูกค้าแบบเชิงรุกผ่านแอปพลิเคชันของธนาคาร และกำหนดให้มีแบบสอบถามประเมินความเข้าใจเกี่ยวกับการทำธุรกรรมออนไลน์ทุก ๆ 6 เดือน

ขณะเดียวกัน การยกระดับมาตรการการป้องกันภัยคุกคามทางไซเบอร์และบัญชีม้าจำเป็นต้องอาศัยความร่วมมือและการบูรณาการข้อมูลและมาตรการจากหลายภาคส่วน สามารถสรุปประเด็นได้ ดังนี้

หน่วยงานกำกับดูแลควรยกระดับมาตรการป้องกันภัยคุกคามทางไซเบอร์ เช่น กสทช. ควรออกกฎระเบียบให้ผู้ให้บริการโทรคมนาคมสามารถบล็อกหมายเลขโทรศัพท์และ IP Address จากต่างประเทศที่เกี่ยวข้องกับธุรกรรมต้องสงสัย และ ธปท. ควรส่งเสริมมาตรฐานการยืนยันตัวตนของ mobile banking และ e-Wallets ให้มีความเข้มงวดขึ้น รวมถึงนำข้อมูลข่าวกรองด้านไซเบอร์มาวิเคราะห์รูปแบบการโจมตีทางออนไลน์เพื่อปรับปรุงมาตรการให้มีประสิทธิภาพมากขึ้น เป็นต้น

ผู้ให้บริการโทรคมนาคมควรมีบทบาทในการบล็อกหมายเลขโทรศัพท์และเครือข่ายที่เกี่ยวข้องกับธุรกรรมต้องสงสัย และสนับสนุนธนาคารและภาครัฐในการตรวจสอบพฤติกรรมการใช้หมายเลขโทรศัพท์และ IP Address ที่ผิดปกติ นอกจากนี้ ควรมีมาตรการป้องกัน Fake SMS โดยใช้แนวทางบล็อกลิงก์ที่ไม่ได้รับการรับรองภายใน 4 ชั่วโมง เช่นเดียวกับประเทศไต้หวัน ซึ่งเป็นมาตรการที่ได้รับการพิสูจน์แล้วว่าสามารถลดความเสียหายจากการฉ้อโกงได้อย่างมีประสิทธิภาพ

ผู้ให้สัมภาษณ์เห็นว่าควรปรับปรุงกระบวนการรับแจ้งความของผู้เสียหายให้รวดเร็วขึ้น โดยเฉพาะการพัฒนาศูนย์ AOC ให้สามารถทำงานได้แบบเบ็ดเสร็จ (one-stop service) เพื่อให้การรับแจ้งเหตุและประสานงานกับหน่วยงานที่เกี่ยวข้องเป็นไปอย่างรวดเร็ว นอกจากนี้ ควรพัฒนากลไกในการติดตามเส้นทางการเงินของบัญชีม้า และเพิ่มความร่วมมือกับหน่วยงานระหว่างประเทศเพื่อสกัดกั้นเครือข่ายฟอกเงินที่ใช้บัญชีม้าเป็นเครื่องมือ

นอกจากนี้ ควรมีการกำหนดหลักเกณฑ์ในการเยียวยายาผู้เสียหายที่เป็นมาตรฐานเดียวกัน รวมทั้งควรเพิ่มบทลงโทษสำหรับผู้ที่มีส่วนเกี่ยวข้องกับการกระทำผิด โดยเฉพาะอย่างยิ่งในกลุ่มผู้ที่เปิดบัญชีม้าหรือเป็นผู้จัดหาข้อมูลส่วนบุคคลเพื่อใช้ในการเปิดบัญชี โดยผู้ให้สัมภาษณ์ให้ข้อมูลว่า ผู้กระทำการดังกล่าวได้รับค่าตอบแทนเฉลี่ย 25,000 บาท ดังนั้น ควรมีบทลงโทษที่รุนแรงพอที่จะทำให้ผู้กระทำผิดไม่กล้าหรือไม่สามารถกระทำซ้ำได้ รวมถึงสนับสนุนให้ผู้ที่เคยเปิดบัญชีม้านำบัญชีของตนมาปิดด้วยความสมัครใจ

ทั้งนี้ ในกลุ่มของผู้ที่มีความเสี่ยงจะรับจ้างเปิดบัญชีม้าซ้ำ ผู้ให้สัมภาษณ์เห็นว่าควรใช้แนวคิดที่เรียกว่า "การทำให้ม้าตาย" คือ การทำให้บุคคลหรือบัญชีที่เคยถูกระบุว่าเป็นบัญชีม้าและถูกอายัดแล้ว มีเงื่อนไขที่เข้มงวดมากขึ้นในทำธุรกรรมทางการเงินต่าง ๆ เช่น บุคคลที่เคยถูกระบุว่าเป็นบัญชีม้าจำเป็นต้องทำธุรกรรมทางการเงินผ่านสาขาของธนาคารเท่านั้น ไม่สามารถเข้าถึงสิทธิ์การใช้ mobile banking หรือ internet banking ในช่วง 2-3 ปีแรกหลังจากถูกยกเลิกการอายัดบัญชี เป็นต้น

นอกจากนี้ การบังคับใช้กฎหมายควรมีการขยายผลติดตามถึงบุคคลที่อยู่เบื้องหลังบัญชีม้า ไม่ใช่เพียงแค่ผู้ที่ถือบัญชีเท่านั้น แต่ควรเพิ่มบทลงโทษแก่ผู้ที่ให้บริการบัญชีม้า เช่น ตัวกลางที่ทำหน้าที่จัดหาบัญชีให้ขบวนการฉ้อโกง เป็นต้น รวมถึงการมีมาตรการลงโทษที่เข้มงวดต่อทั้งบัญชีม้าและขบวนการที่เกี่ยวข้อง ครอบคลุมถึงองค์กรหรือบุคคลที่มีส่วนทำให้ข้อมูลส่วนบุคคลรั่วไหล เพราะช่องโหว่ของข้อมูลเหล่านี้ถือเป็นปัจจัยสำคัญที่เอื้อให้เกิดบัญชีม้าและอาชญากรรมทางการเงินในระบบเศรษฐกิจดิจิทัล

ผู้ให้สัมภาษณ์เห็นว่า นอกจากบทบาทหน้าที่ที่แต่ละหน่วยงานต้องรับผิดชอบแล้ว ทุกภาคส่วนต้องร่วมกันสร้างความตระหนักรู้ให้กับประชาชนเรื่องภัยคุกคามทางไซเบอร์และบัญชีม้าควบคู่กันไปด้วย โดยควรมีการเผยแพร่ข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์และผลกระทบที่เกิดขึ้นจากการมีส่วนร่วมในการเปิดบัญชีม้า การให้ความรู้แก่ประชาชนเกี่ยวกับวิธีการหลอกลวงของมิจฉาชีพ โดยควรมีการเพิ่มช่องทางการสื่อสารเผยแพร่ผ่านสื่อที่หลากหลายมากขึ้น และควรมีการเผยแพร่ข้อมูลในช่วงเวลาที่มีผู้ชมโทรทัศน์มากที่สุด (prime time) เช่น ระหว่างละครหรือข่าวภาคค่ำ เป็นต้น เพื่อให้ครอบคลุมกลุ่มเป้าหมายมากขึ้น

นอกจากนี้ ภาครัฐและหน่วยงานที่เกี่ยวข้องจำเป็นต้องสร้างความเข้าใจที่ถูกต้องให้แก่ประชาชนเกี่ยวกับช่องทางการติดต่อที่สามารถเชื่อถือได้ เพื่อป้องกันการถูกมิจฉาชีพปลอมแปลงเป็นหน่วยงานของรัฐในการหลอกลวงประชาชน

3.3 ผู้มีส่วนได้ส่วนเสียในกลุ่มหน่วยงานกำกับดูแลด้านนโยบายความมั่นคงไซเบอร์และการให้บริการดิจิทัล

3.3.1 ข้อจำกัดและความท้าทายในการจัดการปัญหาภัยคุกคามทางไซเบอร์

ผู้ให้สัมภาษณ์เห็นว่า ภัยคุกคามทางไซเบอร์มีการปรับเปลี่ยนเทคนิคการโจมตีอย่างต่อเนื่อง จากการใช้ “แอปดูดเงิน” ไปเป็นการส่งลิงก์หรือ QR code เพื่อหลอกให้เหยื่อโอนเงินเอง หรือการใช้เทคโนโลยีปัญญาประดิษฐ์ และเทคโนโลยีปลอมแปลงภาพหรือเสียง (Deepfake) เพื่อเลียนแบบเสียงและภาพเจ้าของบัญชี ทำให้การตรวจจับเป็นไปได้ยากขึ้น

นอกจากนี้ มิจฉาชีพปรับรูปแบบการโจมตี โดยหลีกเลี่ยงการโจมตีโดยตรงต่อระบบธนาคาร ซึ่งมีระบบความปลอดภัยทางไซเบอร์ที่เข้มงวด ไปเป็นการหลอกลวงให้ผู้ใช้เปิดเผยข้อมูลสำคัญหรือทำธุรกรรมด้วยตัวเอง โดยใช้วิธีการโจมตีแบบฟิชชิง และการหลอกลวงเชิงจิตวิทยา หรือการเจาะช่องโหว่ที่อุปกรณ์ของผู้ใช้งาน เช่น การควบคุมเครื่องเหยื่อผ่านมัลแวร์ ส่งผลให้ธุรกรรมถูกทำผ่านอุปกรณ์ของเหยื่อเอง เป็นต้น ส่งผลให้การตรวจจับธุรกรรมที่ผิดปกติทำได้ยาก

ผู้ให้สัมภาษณ์เห็นว่ากฎหมายและมาตรฐานความปลอดภัยไซเบอร์ที่มีอยู่ในปัจจุบันยังไม่ครอบคลุมทุกมิติ และจำเป็นต้องปรับปรุงแก้ไขเพิ่มเติมเพื่อให้ทันต่อสถานการณ์ เช่น การให้อำนาจหน่วยงานกำกับดูแลด้านดิจิทัลและความมั่นคงไซเบอร์ สามารถกำหนดมาตรฐานหรือออกคำสั่งบังคับใช้กับสถาบันการเงินได้โดยตรง ซึ่งในทางปฏิบัติอาจต้องรอขั้นตอนทางกฎหมายหรือการปรับปรุงระเบียบที่ใช้เวลานาน

นอกจากนี้ การจัดการภัยไซเบอร์มีความซับซ้อน และต้องอาศัยความร่วมมือจากหลายหน่วยงาน ทำให้มีข้อจำกัดด้านความรวดเร็วของกระบวนการดำเนินงาน รวมถึงกรณีที่การกระทำความผิดมีต้นทางอยู่ในต่างประเทศ ซึ่งเป็นอุปสรรคสำคัญอย่างยิ่งต่อการบังคับใช้กฎหมายข้ามพรมแดน

ผู้ให้สัมภาษณ์เห็นว่า การเพิ่มมาตรการรักษาความปลอดภัย เช่น การหน่วงเวลาการทำธุรกรรม หรือการยืนยันตัวตนหลายชั้น แม้ว่าจะสามารถเพิ่มความปลอดภัยและป้องกันมิจฉาชีพได้มากขึ้น แต่ก็ส่งผลกระทบต่อความสะดวกของประชาชนในการทำธุรกรรมเช่นกัน ซึ่งเป็นความท้าทายของหน่วยงานที่เกี่ยวข้องที่จะต้องพิจารณาให้เกิดความสมดุลเช่นกัน

3.3.2 ข้อจำกัดและความท้าทายในการจัดการบัญชีม้า

นอกจากการปรับตัวของมิจฉาชีพที่ทำให้การเปิดบัญชีม้ามีความซับซ้อนมากยิ่งขึ้น ดังที่ได้กล่าวข้างต้นแล้ว ผู้ให้สัมภาษณ์เห็นว่า ธนาคารยังไม่สามารถระงับบัญชีที่ต้องสงสัยว่าเป็นบัญชีม้าได้ทันที เนื่องจากต้องมีการตรวจสอบให้มั่นใจได้ว่าบัญชีดังกล่าวเป็นบัญชีม้าจริงหรือไม่ ประกอบกับธนาคารไม่มีอำนาจในการระงับบัญชีได้ด้วยตัวเอง จำเป็นต้องรอคำสั่งจากหน่วยงานที่เกี่ยวข้อง ทำให้การระงับบัญชีใช้ระยะเวลานาน และเปิดช่องให้มิจฉาชีพย้ายเงินหนีไปได้

ผู้ให้สัมภาษณ์เห็นว่า การปราบปรามบัญชีม้าควรดำเนินการควบคู่ไปกับการเพิ่มโทษทางกฎหมาย และการเผยแพร่ความรู้ให้ประชาชนรับรู้ถึงโทษของการขายบัญชีหรือให้บุคคลอื่นยืมใช้บัญชีของตน

เมื่อบทลงโทษรุนแรงเพียงพอ และประชาชนตระหนักถึงความเสี่ยง กรณีที่มีผู้ยินยอมขายบัญชีหรือให้ยืมบัญชีก็จะลดลง อีกทั้งราคาบัญชีม้าก็อาจสูงจนไม่คุ้มความเสี่ยงทางกฎหมาย

3.3.3 ข้อจำกัดและความท้าทายในการเยียวยาปัญหาภัยคุกคามทางไซเบอร์และบัญชีม้า

แม้ผู้ใช้บริการบางรายจะได้รับการชดเชยจากธนาคารเมื่อเกิดเหตุการณ์แอปดูดเงินหรือการถูกหลอกโอนเงิน แต่โดยทั่วไปแล้ว ยังไม่มีมาตรฐานกลางที่กำหนดให้ธนาคารต้องรับผิดชอบความเสียหายทั้งหมด การชดเชยส่วนใหญ่จึงเป็นผลจากการเจรจาระหว่างธนาคารกับผู้เสียหายเป็นกรณี ๆ ไป ทำให้เกิดความเหลื่อมล้ำในการคุ้มครองผู้บริโภค

3.3.4 ข้อเสนอแนะของผู้มีส่วนได้ส่วนเสียในกลุ่มหน่วยงานกำกับดูแลด้านนโยบายความมั่นคงไซเบอร์และการให้บริการดิจิทัล

ผู้ให้สัมภาษณ์เห็นว่าควรเพิ่มความเข้มงวดในการยืนยันตัวตนสำหรับการเปิดบัญชีธนาคารและการลงทะเบียนซิมโทรศัพท์มือถือ ผ่านกระบวนการ e-KYC (Electronic Know Your Customer) ที่เชื่อมโยงกับฐานข้อมูลประชาชนและระบบตรวจจับเอกสารปลอม การใช้เทคโนโลยี AI ตรวจจับพฤติกรรมที่ผิดปกติ การใช้ระบบยืนยันตัวตนหลายขั้นตอน การยืนยันตัวตนด้วยข้อมูลชีวมิติ การจำกัดจำนวนบัญชี/ซิมที่สามารถเปิดได้ในชื่อเดียวกัน เพื่อยกระดับความปลอดภัยให้มากขึ้น

นอกจากนี้ ควรมีการพัฒนาระบบแจ้งเตือนและวิเคราะห์ภัยคุกคามทางไซเบอร์แบบเรียลไทม์ การจัดทำรายชื่อผู้ให้บริการหรือแพลตฟอร์มที่มีมาตรฐานความปลอดภัยสูง (white list) ตลอดจนมีการฝึกซ้อมรับมือการถูกโจมตีทางไซเบอร์ (cyber drill) ร่วมกันอย่างสม่ำเสมอ ทั้งหน่วยงานภาครัฐ ธนาคารและภาคเอกชนที่เกี่ยวข้อง เพื่อเตรียมความพร้อมและประสานงานกันได้อย่างมีประสิทธิภาพในสถานการณ์จริง

ผู้ให้สัมภาษณ์เห็นว่าการให้ความรู้เรื่องภัยคุกคามทางไซเบอร์และบัญชีม้าเป็นสิ่งสำคัญอย่างยิ่ง โดยหน่วยงานที่เกี่ยวข้องควรมีการสื่อสาร หรือจัดกิจกรรมที่เข้าถึงประชาชนในวงกว้าง โดยเฉพาะกลุ่มเปราะบาง เช่น ผู้สูงอายุที่มีเงินเก็บมาก นักเรียน นักศึกษา และกลุ่มที่ขาดโอกาสเข้าถึงข้อมูล โดยอาจใช้สื่อท้องถิ่น ภาษาถิ่น หรือผ่านผู้นำชุมชนเพื่อให้เข้าถึงง่ายและมีประสิทธิภาพมากขึ้น

นอกจากนี้ ควรเพิ่มบทลงโทษสำหรับบัญชีม้าและซิมม้าที่เข้มงวดขึ้น ทั้งกับผู้ที่จงใจเปิดบัญชีหรือซิมเพื่อหลอกลวง และผู้ที่ปล่อยให้บัญชีหรือซิมของตนถูกนำไปใช้โดยประมาทหรือรู้เห็นเป็นใจ

ผู้ให้สัมภาษณ์เห็นว่า ควรกำหนดกรอบความรับผิดชอบของธนาคารให้ชัดเจนในกรณีความเสียหายทางการเงินที่เกิดจากภัยไซเบอร์หรือการหลอกลวง เช่น กรณีใดธนาคารต้องร่วมรับผิดชอบต่อความสูญเสียของลูกค้า และกรณีใดที่ลูกค้าต้องเป็นผู้รับผิดแต่เพียงผู้เดียว เป็นต้น นอกจากนี้ ควรเพิ่มอำนาจให้ธนาคารสามารถระงับบัญชีที่ต้องสงสัยได้ทันที ก่อนจะเกิดการโอนเงินต่อไปยังบัญชีปลายทาง

ในบางกรณี ธนาคารหรือผู้ให้บริการอาจพิจารณาใช้ “มาตรการหน่วงเวลา” ในการโอนเงินจำนวนมากหรือธุรกรรมที่มีความเสี่ยงสูง เพื่อเปิดโอกาสให้ระบบสามารถตรวจสอบความถูกต้องได้อย่างรัดกุมยิ่งขึ้น

ผู้ให้สัมภาษณ์เสนอว่าอาจพิจารณาจัดตั้งกองทุนเยียวยาหรือสนับสนุนการทำประกันภัยไซเบอร์เพื่อลดภาระของผู้เสียหาย

3.4 ผู้มีส่วนได้ส่วนเสียในกลุ่มหน่วยงานบังคับใช้กฎหมาย

3.4.1 ข้อจำกัดและความท้าทายในการจัดการปัญหาภัยคุกคามทางไซเบอร์

ผู้ให้สัมภาษณ์เห็นว่าปัจจุบันมิจฉาชีพมีการปรับตัวอย่างรวดเร็ว และมีรูปแบบการหลอกลวงที่หลากหลาย เช่น การหลอกลวงทางอีเมลหรือ SMS การฟิชชิง การใช้เทคโนโลยีเพื่อการหลอกลวง เช่น การใช้ AI Deepfake หรือการสร้างคลิปภาพและเสียงปลอม ซึ่งทำให้ประชาชนหลงเชื่อได้ง่ายขึ้น การโจมตีโดยแอปดูดเงิน ซึ่งมิจฉาชีพอาจมีการเขียนโปรแกรมให้สามารถโอนเงินออกไปได้อย่างรวดเร็ว โดยธนาคารกำลังเร่งอุดช่องโหว่เพื่อป้องกันปัญหาดังกล่าว นอกจากนี้ในปัจจุบันกลุ่มมิจฉาชีพยังมีการปรับรูปแบบการใช้งานเครือข่ายไปใช้ระบบอินเทอร์เน็ตผ่านทางดาวเทียม Starlink ซึ่งทำให้การติดตามย้อนกลับเป็นไปได้ยากขึ้น รวมไปถึงการลักลอบใช้สัญญาณในเขตชายแดนประเทศเพื่อนบ้าน ทำให้เจ้าหน้าที่จากไทยไม่สามารถเข้าจับกุมหรือดำเนินคดีได้ เนื่องจากกระบวนการดังกล่าวจำเป็นต้องได้รับความร่วมมือจากหน่วยงานในประเทศเพื่อนบ้าน และต้องใช้ระยะเวลาดำเนินการ

ผู้ให้สัมภาษณ์เห็นว่ารัฐบาลให้ความใส่ใจปัญหาภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการทางการเงินและดำเนินการได้ดีพอสมควร อย่างไรก็ตาม ยังมีข้อจำกัดทางกฎหมายในการเปิดเผยข้อมูลข้ามหน่วยงานระหว่างสถาบันทางการเงิน ผู้ให้บริการโทรคมนาคม และผู้ให้บริการแพลตฟอร์ม กับหน่วยงานสืบสวน ทำให้ขั้นตอนตั้งแต่การตรวจจับมิจฉาชีพไปจนถึงการดำเนินการจับกุมต่อไปไม่รวดเร็วเพียงพอที่จะสามารถติดตามทรัพย์คืนให้กับผู้เสียหาย เนื่องจากยังมีขั้นตอนในกระบวนการยุติธรรม เช่น การเรียกสอบปากคำ การขอข้อมูลจากธนาคารและผู้ให้บริการโทรคมนาคม หรือการฟ้องร้อง อีกทั้งจำนวนเจ้าหน้าที่ที่รับผิดชอบคดีภัยคุกคามทางไซเบอร์ในปัจจุบันมีน้อยเกินไปเมื่อเทียบกับจำนวนคดีที่เกิดขึ้น ทำให้มีข้อจำกัดในการดำเนินคดี โดยเฉพาะการสืบสวนไปยังต้นตอของมิจฉาชีพ ซึ่งจำเป็นต้องมีการทุ่มเททรัพยากรบุคคลและระยะเวลามาก

อย่างไรก็ตาม ผู้ให้สัมภาษณ์เห็นว่าประชาชนโดยทั่วไปมีความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ค่อนข้างดี แต่ปัญหามักจะเกิดจากการที่มิจฉาชีพมีการพัฒนารูปแบบใหม่อยู่เสมอ อีกทั้งคนบางกลุ่มยังถูกหลอกลวงให้เกิดความโลภและความกลัว ทำให้ความสามารถในการวิเคราะห์ลดลงและตกเป็นเหยื่อของ

มิจฉาชีพในที่สุด ดังนั้นจึงจำเป็นต้องสร้างความตระหนักรู้ให้ประชาชนเท่าทันต่อภัยคุกคามทางไซเบอร์ทุกรูปแบบ

3.4.2 ข้อจำกัดและความท้าทายในการจัดการปัญหาบัญชีม้า

การทำธุรกรรมออนไลน์ในปัจจุบันมีความสะดวกสบายมากขึ้น ทำให้โอกาสเกิดอาชญากรรมทางเทคโนโลยีเพิ่มสูงขึ้นด้วยเช่นกัน ตัวอย่างเช่น การสแกนจ่ายเงินหรือการโอนเงินผ่านแอปพลิเคชันต่าง ๆ ในปัจจุบันที่มีความสะดวกรวดเร็ว ทำให้เมื่อผู้บริโภคถูกมิจฉาชีพหลอกลวงให้โอนเงิน ยอดเงินดังกล่าวก็จะถูกโอนต่อไปยังบัญชีม้าอื่น ๆ ได้อย่างรวดเร็ว ซึ่งสุดท้ายแล้วมิจฉาชีพมักจะโอนเงินออกไปในรูปแบบคริปโตเคอร์เรนซี ทำให้ตรวจสอบและติดตามเงินคืนได้ยาก เนื่องจากการเปิดบัญชีคริปโตเคอร์เรนซีในปัจจุบันยังคงมีช่องโหว่ซึ่งมิจฉาชีพสามารถใช้เบอร์โทรศัพท์ปลอมในการยืนยันตัวตนได้ ผู้ให้สัมภาษณ์บางส่วนเห็นว่าควรมีมาตรการหน่วงเงินที่จะช่วยชะลอระยะเวลาในการโอนเงินไปยังมิจฉาชีพ โดยมาตรการดังกล่าวจะมีประสิทธิภาพมากยิ่งขึ้นหากในช่วงเวลาที่ถูกหน่วงเงิน มีการประชาสัมพันธ์เพิ่มความตระหนักรู้ควบคู่ไปด้วย

นอกจากนี้การอำนวยความสะดวกของธนาคารในการเปิดบัญชีออนไลน์ในปัจจุบัน ทำให้เกิดช่องว่างสำหรับมิจฉาชีพในการสร้างบัญชีม้าได้ง่ายยิ่งขึ้น โดยผู้ให้สัมภาษณ์ได้ให้ข้อมูลเกี่ยวกับระบบการเปิดบัญชีในช่วงระยะเวลาที่ผ่านมาว่ากรณีที่มีผู้ที่ขายบัญชีม้าให้มิจฉาชีพโดยสมัครใจ อาจทำให้เกิดบัญชีม้าเพิ่มเข้ามาในระบบมากกว่า 20 บัญชีต่อผู้ขายบัญชีม้าหนึ่งคน อีกทั้งกลุ่มมิจฉาชีพยังมีการพัฒนารูปแบบการเปิดบัญชีม้าอย่างต่อเนื่อง เช่น การจดทะเบียนบริษัทเพื่อสร้างความน่าเชื่อถือ ซึ่งหน่วยงานที่เกี่ยวข้องยังไม่สามารถยับยั้งปัญหาดังกล่าวได้ และประชาชนที่ไม่รู้เท่าทันอาจตกเป็นเหยื่อได้ สะท้อนให้เห็นถึงความจำเป็นในการพัฒนากลไกป้องกันและมาตรการรักษาความปลอดภัยทางการเงินให้มีประสิทธิภาพมากยิ่งขึ้น

ทั้งนี้ แม้ว่าหน่วยงานภาครัฐมีความพยายามยกระดับมาตรการระงับบัญชีม้าให้รวดเร็วมากขึ้น แต่ก็ยังไม่เพียงพอที่จะสามารถระงับการโอนเงินออกจากบัญชีได้อย่างทันท่วงที โดยผู้ให้สัมภาษณ์เห็นว่าแม้ปัจจุบันจะมีการระงับบัญชีม้าได้เป็นจำนวนมาก แต่ยังคงมีเหยื่อที่ได้รับความเสียหายจากการหลอกลวงมากกว่า 1,000 ครั้งต่อวัน สะท้อนให้เห็นว่ายังคงมีบัญชีม้าหลงเหลืออยู่ในระบบอีกจำนวนมาก ดังนั้นควรมุ่งเน้นการระงับบัญชีม้าที่สามารถตรวจจับเจ้าของบัญชีได้แล้ว รวมถึงระงับบัญชีอื่น ๆ ของเจ้าของบัญชีม้าดังกล่าวด้วย เนื่องจากเจ้าของบัญชีม้ามักมีบัญชีม้ามากกว่าหนึ่งบัญชี

3.4.3 ข้อจำกัดและความท้าทายในการเยียวยาปัญหาภัยคุกคามทางไซเบอร์และบัญชีม้า

ผู้ให้สัมภาษณ์ให้ความคิดเห็นเกี่ยวกับการชดเชยเยียวยาผู้เสียหายว่าควรมีการกำหนดแนวทางและอัตราส่วนความรับผิดชอบของแต่ละหน่วยงานให้ชัดเจน ซึ่งระบบที่มีอยู่ในปัจจุบันทำให้ผู้เสียหายมีโอกาสได้รับการเยียวยาได้ยาก หรือมีความล่าช้า เนื่องจากการบูรณาการร่วมกันระหว่างหน่วยงานยังติดปัญหาบางประการ เช่น การที่หน่วยงานบังคับใช้กฎหมายไม่สามารถเข้าถึงข้อมูลจากสถาบันการเงิน เนื่องมาจากการบังคับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล นอกจากนี้กระบวนการยุติธรรมยังจำเป็นต้องมีการดำเนินการ

หลายขั้นตอน เช่น การเรียกสอบปากคำ การฟ้องร้อง การขอข้อมูลจากธนาคารและผู้ให้บริการโทรคมนาคม เป็นต้น ทำให้ต้องใช้ระยะเวลาดำเนินการที่ค่อนข้างนาน และไม่สามารถจัดการกับมิจฉาชีพได้อย่างทันท่วงที

ในช่วงเวลาที่ผ่านมา พบว่าผู้เสียหายอาจไม่ได้รับเงินคืนแม้กระบวนการยุติธรรมจะสิ้นสุดแล้ว เนื่องจากมิจฉาชีพได้โอนเงินออกจากบัญชีไปยังบัญชีม้าอื่น ๆ และโอนเงินออกไปในรูปแบบคริปโตเคอร์เรนซี เรียบร้อยแล้ว หรือแม้ว่าจะสามารถติดตามยึดทรัพย์คืนจากมิจฉาชีพได้ กระบวนการเฉลี่ยทรัพย์คืนให้กับผู้เสียหายอาจต้องใช้ระยะเวลามากกว่าหนึ่งปี อีกทั้งผู้เสียหายอาจได้รับเงินคืนน้อยกว่ามูลค่าที่เสียหาย เนื่องจากต้องเฉลี่ยทรัพย์คืนให้ผู้เสียหายรายอื่น ๆ ด้วย

3.4.4 ข้อเสนอแนะของผู้มีส่วนได้ส่วนเสียในกลุ่มหน่วยงานบังคับใช้กฎหมาย

ผู้ให้สัมภาษณ์เห็นว่าควรมีการเพิ่มความร่วมมือกับหน่วยงานในต่างประเทศ โดยเฉพาะประเทศเพื่อนบ้าน เพื่อจัดการกับภัยคุกคามทางไซเบอร์ ซึ่งเมื่อเกิดการกระทำผิดขึ้นมักจะมีอุปสรรคในการเข้าจับกุม เนื่องจากไม่อยู่ในเขตพื้นที่ประเทศไทย นอกจากนี้ ควรมีการบูรณาการระหว่างหน่วยงานมากขึ้น โดยควรกำหนดแนวปฏิบัติและบทบาทหน้าที่ของแต่ละหน่วยงานให้ชัดเจน รวมถึงกำหนดความรับผิดชอบต่อความเสียหาย กรณีมีข้อเท็จจริงที่พิสูจน์ได้ว่าหน่วยงานดังกล่าวปฏิบัติหน้าที่ไม่รัดกุมเพียงพอจนเกิดความเสียหาย

นอกจากนี้ ควรมีการดูแลปรับปรุงข้อกฎหมายต่าง ๆ ที่เกี่ยวข้องกับแต่ละหน่วยงานในประเด็นภัยคุกคามทางไซเบอร์ให้ทันสมัยและสอดคล้องกับสถานการณ์อยู่เสมอ เพื่อปิดช่องโหว่ทางกฎหมายที่อาจทำให้การบูรณาการระหว่างหน่วยงานไม่มีประสิทธิภาพเท่าที่ควร โดยเฉพาะการบูรณาการด้านข้อมูลข้ามหน่วยงาน

ในส่วนการพัฒนาทางด้านเทคโนโลยี ควรมุ่งเน้นการพัฒนาระบบ Central Fraud Registry (CFR) หรือระบบแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมที่ต้องสงสัยระหว่างสถาบันการเงิน ที่สามารถใช้เทคโนโลยีในการตรวจจับและวิเคราะห์พฤติกรรมบัญชีต้องสงสัย และระงับบัญชีต้องสงสัยได้แบบอัตโนมัติทันท่วงที

นอกจากนี้ ในการอำนวยความสะดวกแก่ประชาชน ควรเพิ่มเติมช่องทางการรายงานบัญชีม้าผ่านทางแอปพลิเคชันของธนาคารเพื่อเพิ่มความรวดเร็วในการระงับบัญชี และควรเร่งจัดทำรายชื่อบัญชีที่ปลอดภัยและบัญชีต้องสงสัยให้ประชาชนสามารถเข้าถึงได้ โดยให้มีกระบวนการตรวจสอบและแสดงหลักฐานยืนยันตัวตนที่รัดกุม ควรมีระบบการแจ้งเตือนประชาชนถึงความเสี่ยงที่จะถูกฉ้อโกง ในกรณีที่มีความประสงค์จะโอนเงินไปยังบัญชีม้า รวมไปถึงระบบการตรวจสอบบัญชีของตนเอง เพื่อให้ประชาชนสามารถตรวจสอบได้ว่าชื่อของตนได้ถูกนำไปใช้เปิดบัญชีม้าหรือไม่

อย่างไรก็ตาม ผู้ให้สัมภาษณ์ยังให้ความคิดเห็นว่าอีกสิ่งที่ควรให้ความสำคัญ ได้แก่ การเพิ่มการประชาสัมพันธ์เกี่ยวกับภัยคุกคามทางไซเบอร์แก่ประชาชน ควบคู่ไปกับมาตรการอื่น ๆ เช่น หากมีมาตรการหน่วงเงิน ควรมีการประชาสัมพันธ์เพิ่มความตระหนักรู้ควบคู่ไปด้วย จะทำให้การป้องกันความเสี่ยง

จากการถูกฉ้อโกงมีประสิทธิภาพมากยิ่งขึ้น นอกจากนี้ควรอาศัยความร่วมมือจากภาคเอกชนให้มีส่วนช่วยในการเสริมสร้างความตระหนักรู้แก่ประชาชนผ่านช่องทางการโฆษณาที่มีอยู่

3.5 ผู้มีส่วนได้ส่วนเสียในกลุ่มหน่วยงานกำกับดูแลภาคโทรคมนาคม

3.5.1 ข้อจำกัดและความท้าทายในการจัดการปัญหาภัยคุกคามทางไซเบอร์

ผู้ให้สัมภาษณ์ไม่มีบทบาทหน้าที่ที่เกี่ยวข้องกับการจัดการปัญหาภัยคุกคามทางไซเบอร์โดยตรง

3.5.2 ข้อจำกัดและความท้าทายในการจัดการบัญชีม้า

ผู้ให้สัมภาษณ์ให้ข้อมูลว่า ปัญหาซิมม้าที่พบส่วนใหญ่จะเป็นการลงทะเบียนโดยใช้ข้อมูลชาวต่างชาติจากประเทศเพื่อนบ้าน ซึ่งลงทะเบียนซิมด้วยบัตรประจำตัวคนซึ่งไม่มีสัญชาติไทย (บัตรสีชมพู) ซึ่งอยู่ในขอบเขตความรับผิดชอบของกรมการปกครอง ทำให้ขั้นตอนในการตรวจสอบเอกสารมีความซับซ้อนและใช้เวลานานกว่ากรณีที่มิจฉาชีพเป็นคนไทย อย่างไรก็ตาม ปัจจุบันหน่วยงานที่เกี่ยวข้องอยู่ระหว่างเตรียมความพร้อมเพื่อพัฒนาระบบเชื่อมโยงข้อมูลเหล่านี้ นอกจากนี้ ผู้ให้สัมภาษณ์ให้ข้อมูลว่า กสทช. อยู่ระหว่างเตรียมพัฒนาระบบสำหรับแลกเปลี่ยนและวิเคราะห์ข้อมูลในการเชื่อมโยงเพื่อสกัดซิมม้า มีลักษณะใกล้เคียงกับระบบ Central Fraud Registry (CFR) ซึ่งจะช่วยลดการเข้าถึงข้อมูลโดยตรง ทำให้ลดความเสี่ยงในการละเมิดความเป็นส่วนตัวของผู้ใช้บริการ เพิ่มประสิทธิภาพในการตรวจจับและวิเคราะห์ข้อมูลเกี่ยวกับซิมที่มีพฤติกรรมเสี่ยง หน่วยงานต่าง ๆ สามารถนำข้อมูลมาแลกเปลี่ยนและประมวลผลร่วมกันได้ และคาดว่าจะทำให้การสืบสวนและดำเนินคดีรวดเร็วขึ้น

ผู้ให้สัมภาษณ์ระบุถึงช่องว่างกรณีที่มิจฉาชีพใช้สัญญาณในบริเวณเขตชายแดนที่มาจากเสาสัญญาณของประเทศไทยในการกระทำความผิด การที่เจ้าหน้าที่ไทยจะเข้าดำเนินการในพื้นที่ดังกล่าวต้องอาศัยความร่วมมือจากหลายหน่วยงาน รวมถึงหน่วยงานด้านความมั่นคงของประเทศเพื่อนบ้าน ส่งผลให้การดำเนินการตรวจสอบและจับกุมใช้ระยะเวลานาน ผู้ให้สัมภาษณ์ให้ข้อมูลว่า ปัจจุบัน กสทช. อยู่ระหว่างการจำกัดพื้นที่สัญญาณให้อยู่ภายในเขตประเทศไทยเท่านั้น

นอกจากนี้ ผู้ให้สัมภาษณ์เห็นว่าการปิดกั้นหรือสกัดกั้นช่องทางการสื่อสาร ต้องคำนึงถึงสิทธิความเป็นส่วนตัวของประชาชนด้วย ในปัจจุบันยังไม่มีข้อกฎหมายที่ชัดเจนว่าหน่วยงานภาครัฐหรือผู้ให้บริการโทรคมนาคมสามารถเข้าถึงข้อมูลการติดต่อของผู้ใช้งานได้มากน้อยเพียงใด แม้ว่าการตรวจสอบข้อมูลดังกล่าวอาจช่วยลดภัยคุกคามทางไซเบอร์ได้ก็ตาม

3.5.3 ข้อจำกัดและความท้าทายในการเยียวยาปัญหาภัยคุกคามทางไซเบอร์และบัญชีม้า

ผู้ให้สัมภาษณ์เห็นว่ามาตรการเยียวยาหรือการติดตามเงินคืนให้กับผู้เสียหายมีความท้าทายในกระบวนการพิจารณาลักษณะการเยียวยาหรือการเฉลี่ยทรัพย์ให้ผู้เสียหายแต่ละราย ซึ่งปัจจุบันยังไม่มีแนวปฏิบัติที่ชัดเจน

3.5.4 ข้อเสนอแนะของผู้มีส่วนได้ส่วนเสียในกลุ่มหน่วยงานกำกับดูแลภาคโทรคมนาคม

ผู้ให้สัมภาษณ์เห็นว่าควรมีการปรับปรุงกฎหมายให้ครอบคลุมการตรวจสอบการลงทะเบียนซิมโดยใช้ข้อมูลชีวมิติ เช่น ลายนิ้วมือหรือการจดจำใบหน้า เพื่อป้องกันการลงทะเบียนซิมโดยใช้ข้อมูลปลอม หรือข้อมูลของบุคคลอื่น

สำหรับปัญหาจากเงื่อนไขความเป็นส่วนตัวของผู้ใช้งาน ดังที่ระบุในปัญหาหรือช่องว่างของนโยบาย/มาตรการที่มีอยู่ในปัจจุบัน ผู้ให้สัมภาษณ์เห็นว่าไม่ควรแทรกแซงช่องทางการติดต่อสื่อสารของประชาชน โดยอาจต้องมีการออกกฎหมายรองรับในการกลั่นกรองเนื้อหาต่าง ๆ ก่อนเป็นลำดับแรก หรืออาจหาข้อสรุปที่ชัดเจนร่วมกับหน่วยงานอื่น ๆ ว่าสามารถเข้าถึงข้อมูลอย่างถูกต้องตามกฎหมายได้ถึงระดับใด

ผู้ให้สัมภาษณ์เห็นว่าหน่วยงานภาครัฐควรมุ่งเน้นการสร้างความตระหนักรู้ของประชาชนเชิงรุก ซึ่งเป็นแนวทางการป้องกันมิจฉาชีพที่ยั่งยืนกว่าการจำกัดหรือปิดกั้นช่องการสื่อสารของมิจฉาชีพ เนื่องจากมิจฉาชีพสามารถพัฒนารูปแบบในการกระทำความผิดได้ตลอดเวลา

3.6 ผู้มีส่วนได้ส่วนเสียในกลุ่มองค์กรภาคประชาสังคมในต่างประเทศ

คณะวิจัยได้สัมภาษณ์ผู้แทนภาคประชาสังคมจากเครือข่ายแนวร่วมการเงินนานาชาติ (Fair Finance International) จาก 3 ประเทศที่มีลักษณะปัญหาด้านความมั่นคงปลอดภัยไซเบอร์และบัญชีม้าใกล้เคียงกับไทย ได้แก่ อินโดนีเซีย ฟิลิปปินส์ และบราซิล โดยสรุปข้อจำกัด ความท้าทาย และข้อเสนอแนะได้ดังนี้

3.6.1 ข้อจำกัดและความท้าทายในการจัดการปัญหาภัยคุกคามทางไซเบอร์

ผู้ให้สัมภาษณ์ทุกรายเห็นตรงกันว่าภัยคุกคามไซเบอร์เป็นความเสี่ยงสำคัญที่กำลังเผชิญอยู่ โดยมีจุดร่วมของปัญหาใกล้เคียงกัน เช่น การถูกขโมยข้อมูลส่วนบุคคล การหลอกลวงว่าเป็นเจ้าหน้าที่รัฐ และการใช้แอปปลอมในการเข้าถึงโทรศัพท์ของเหยื่อ กรณีที่น่าสนใจและส่งผลต่อความเชื่อมั่นของผู้บริโภคอย่างมากคือกรณีที่ธนาคาร BDO ในประเทศฟิลิปปินส์เคยประสบปัญหาการถูกโจมตีทางไซเบอร์ ส่งผลให้มีบัญชีผู้ใช้มากกว่า 700 บัญชีถูกลักลอบถอนเงินโดยไม่ได้รับอนุญาต โดยคาดว่ามูลค่าความเสียหายที่เกิดขึ้นจากเหตุการณ์ดังกล่าวสูงถึงกว่า 50 ล้านเปโซ อย่างไรก็ตาม ในกรณีนี้ ธนาคาร BDO ได้แสดงความรับผิดชอบต่อเหตุการณ์ที่เกิดขึ้นโดยดำเนินการชดเชยความเสียหายให้แก่ผู้ได้รับผลกระทบทั้งหมดเต็มจำนวน อย่างไรก็ตาม ไม่มีรายงานแน่ชัดว่าธนาคารดังกล่าวถูกสั่งปรับหรือลงโทษจากเหตุการณ์ดังกล่าวหรือไม่

ผู้ให้สัมภาษณ์ให้ข้อมูลว่ามีเพียงธนาคารกลางฟิลิปปินส์ที่ระบุว่าความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นความเสี่ยงสำคัญ โดยเฉพาะกับธนาคารดิจิทัล (digital bank) อย่างไรก็ตาม ธนาคารฟิลิปปินส์มักปรับปรุงระบบการป้องกันภัยไซเบอร์หลังเกิดเหตุเท่านั้น เนื่องจากขาดแรงจูงใจในการพัฒนาและการพัฒนาระบบมีค่าใช้จ่ายสูง ซึ่งไม่คุ้มค่าแก่ธนาคารขนาดเล็กในการลงทุน นอกจากนี้ ธนาคารกลางฟิลิปปินส์ได้กำหนดให้ธนาคารต้องเปิดเผยข้อมูลการละเมิดความปลอดภัยทางไซเบอร์ในรายงานประจำปีของ

ธนาคาร และหากไม่เปิดเผยอาจถูกลงโทษ ซึ่งเป็นมาตรการที่อาจช่วยสร้างแรงจูงใจให้ธนาคารปรับปรุงระบบรักษาความปลอดภัยทางไซเบอร์ให้ดีขึ้นอย่างต่อเนื่อง

3.6.2 ข้อจำกัดและความท้าทายในการจัดการบัญชีม้า

จากการสัมภาษณ์ตัวแทนภาคประชาสังคมจากทั้ง 3 ประเทศพบว่าปัญหาการจัดการบัญชีม้าในแต่ละประเทศมีบริบทที่ค่อนข้างแตกต่างกันดังนี้ :

- **ในประเทศฟิลิปปินส์** ปัญหาบัญชีม้าเกิดจากการถูกขโมยข้อมูลส่วนบุคคลไปเปิดบัญชี เนื่องจากยังไม่มีกระบวนการตรวจสอบที่เข้มงวดมากพอ โดยบัญชีม้าส่วนใหญ่ถูกใช้ในการฟอกเงินมากกว่าการหลอกลวงประชาชน การมีระบบสแกนใบหน้าหรือลายนิ้วมือน่าจะช่วยให้ปัญหาดังกล่าวดีขึ้น
- **ในประเทศอินโดนีเซีย** กระบวนการเปิดบัญชีของธนาคารในอินโดนีเซียต้องใช้บัตรประชาชนและเอกสารยืนยันการทำงาน โดยเอกสารเหล่านี้ต้องเปิดกับธนาคารในเขตที่ตรงกับข้อมูลในเอกสารเท่านั้น เว้นแต่มีเหตุผลรับรองจากที่ทำงานในการเปิดบัญชีนอกเขตที่อยู่อาศัยของตน ผู้ให้สัมภาษณ์จึงคาดว่าบัญชีม้าเกิดจากการขายบัญชีโดยสมัครใจให้มิจฉาชีพมากกว่า
- **ในประเทศบราซิล** ธนาคารกลางบราซิลกำลังพัฒนากลไกการเชื่อมโยงรูปแบบการใช้งานบัญชีเพื่อระบุพฤติกรรมเข้าข่ายบัญชีม้า รวมถึงการพัฒนาเทคโนโลยีและกฎหมาย แต่ความท้าทายสำคัญในการปรับปรุงกฎหมายประชาชนมักไม่ทราบว่าตนถูกหลอก ดังนั้นการแก้กฎหมายและปรับปรุงกฎหมายให้มีโทษสูงขึ้นอาจเป็นการซ้ำเติมเหยื่อที่ถูกหลอกจากบัญชีม้า จึงควรเน้นไปที่การส่งเสริมให้หน่วยงานกำกับดูแลและสถาบันการเงินพัฒนากลไกการป้องกันและตรวจจับให้ดียิ่งขึ้น

3.6.3 ข้อจำกัดและความท้าทายในการเยียวยาปัญหาภัยคุกคามทางไซเบอร์และบัญชีม้า

ผู้ให้สัมภาษณ์จากทั้งสามประเทศมีความเห็นสอดคล้องกันว่า หนึ่งในอุปสรรคสำคัญในการเยียวยาปัญหาภัยคุกคามทางไซเบอร์และบัญชีม้าคือ ทัศนคติของธนาคารที่มองว่าความเสียหายที่เกิดขึ้นเป็นความรับผิดชอบของผู้บริโภคเอง ด้วยเหตุนี้ เมื่อเกิดเหตุการณ์ฉ้อโกงทางออนไลน์ ผู้บริโภคจำเป็นต้องดำเนินการเรียกร้องค่าเสียหายผ่านกระบวนการยุติธรรม ซึ่งการพิจารณาคดีมักยึดหลักว่าธนาคารจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นก็ต่อเมื่อมีหลักฐานบ่งชี้ว่า ธนาคารไม่มีมาตรการรักษาความปลอดภัยที่เพียงพอ หรือไม่มีการแจ้งข้อมูลเกี่ยวกับความเสี่ยงและแนวทางป้องกันให้แก่ผู้ใช้บริการ อย่างไรก็ตาม หนึ่งในผู้ให้สัมภาษณ์ให้ความเห็นว่าการดำเนินการทางกฎหมายมีค่าใช้จ่ายสูง ส่งผลให้กระบวนการดังกล่าวไม่สามารถเป็นแนวทางเยียวยาที่มีประสิทธิภาพสำหรับผู้เสียหายทั้งหมด โดยเฉพาะอย่างยิ่งในกรณีที่มูลค่าความเสียหายไม่สูงมาก ทำให้การจ้างทนายความอาจไม่คุ้มค่ากับค่าเสียหายที่คาดว่าจะได้รับคืน

นอกจากนี้ เหยื่อของการฉ้อโกงทางการเงินยังประสบปัญหาในการเรียกคืนเงิน เนื่องจากระบบของธนาคารไม่ได้ดำเนินการอายัดบัญชีต้องสงสัยในทันที อีกทั้งยังขาดระบบอัตโนมัติในการตรวจจับและระงับบัญชีของมิจฉาชีพ ส่งผลให้มิจฉาชีพสามารถโยกย้ายเงินออกจากบัญชีม้าได้อย่างรวดเร็ว ในขณะเดียวกัน

การระงับบัญชีต้องสงสัยจำเป็นต้องใช้ความรอบคอบ เนื่องจากอาจก่อให้เกิดผลกระทบต่อบัญชีของลูกค้าปกติที่ไม่มีส่วนเกี่ยวข้องกับการกระทำความผิด

ผู้ให้สัมภาษณ์จากอินโดนีเซียยังระบุว่าหนึ่งในความท้าทายที่สำคัญในการเข้าถึงกระบวนการเยียวยา คือ ระบบการแจ้งความยังไม่มีประสิทธิภาพเพียงพอ โดยมีรายงานว่าบางกรณีเจ้าหน้าที่ตำรวจเรียกรับสินบนเพื่อดำเนินคดี ทำให้ผู้เสียหาย โดยเฉพาะผู้ที่ได้รับความเสียหายในจำนวนเล็กน้อย ไม่สามารถเข้าถึงความยุติธรรมได้อย่างแท้จริง ปัจจัยดังกล่าวส่งผลให้มาตรการเยียวยาผู้เสียหายจากภัยคุกคามทางไซเบอร์และบัญชีม้ายังไม่สามารถดำเนินการได้อย่างมีประสิทธิภาพและทั่วถึง

3.6.4 ข้อเสนอแนะของผู้มีส่วนได้ส่วนเสียในกลุ่มองค์กรภาคประชาสังคมในต่างประเทศ

ผู้ให้สัมภาษณ์จากบราซิลและฟิลิปปินส์มีความเห็นว่าธนาคารควรยกระดับมาตรการรักษาความปลอดภัยทางไซเบอร์ให้ครอบคลุมทั้งระบบป้องกันภัยไซเบอร์โดยรวมและแนวทางป้องกันบัญชีม้า โดยหน่วยงานกำกับดูแลควรมีบทบาทสำคัญในการสร้างแรงจูงใจให้ธนาคารพาณิชย์พัฒนาระบบความปลอดภัยทางไซเบอร์ให้ทันสมัยและสอดคล้องกับภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว พร้อมทั้งกำหนดมาตรการทางกฎหมายหรือข้อบังคับที่ชัดเจน หากพบว่าธนาคารละเลยการพัฒนาแนวทางป้องกันและปล่อยให้เกิดความเสี่ยงต่อผู้บริโภค

ผู้ให้สัมภาษณ์บางรายเสนอให้ธนาคารเก็บข้อมูลเพิ่มเติม เช่น ข้อมูลฐานรายได้ของลูกค้าและตำแหน่งที่ตั้งของแต่ละธุรกรรม เพื่อใช้ประกอบการวิเคราะห์พฤติกรรมที่อาจเข้าข่ายบัญชีม้า การมีข้อมูลเชิงลึกที่มากขึ้นจะช่วยให้ระบบตรวจจับบัญชีม้ามีความแม่นยำยิ่งขึ้น และสามารถอายัดบัญชีต้องสงสัยได้อย่างทันท่วงที นอกจากนี้ ควรพัฒนาแพลตฟอร์มที่เปิดให้ประชาชนสามารถแจ้งข้อมูลบัญชีม้าต้องสงสัยเข้าสู่ระบบได้ เพื่อเป็นแหล่งข้อมูลเพิ่มเติมสำหรับการตรวจสอบและป้องกันการฉ้อโกง

นอกจากนี้ ผู้ให้สัมภาษณ์ทุกรายเห็นตรงกันว่ามาตรการหน่วงเงินอาจช่วยลดความเสียหายจากการถูกหลอกลวงทางการเงินได้ อย่างไรก็ตาม มาตรการดังกล่าวอาจส่งผลกระทบต่อระบบเศรษฐกิจโดยเฉพาะธุรกิจขนาดเล็กที่ต้องการรับเงินจากผู้ซื้อในทันทีเพื่อรักษาสภาพคล่องทางการเงิน ดังนั้น หน่วยงานกำกับดูแลควรพิจารณาหาจุดดุลยภาพของมาตรการนี้ โดยอาจใช้กลไกที่สามารถจำแนกประเภทของธุรกรรมและนำมาตรการเงินไปใช้กับธุรกรรมที่มีความเสี่ยงสูงโดยเฉพาะ แทนที่จะใช้กับธุรกรรมทั้งหมดเพื่อให้สามารถลดความเสี่ยงจากการฉ้อโกงโดยไม่กระทบต่อระบบเศรษฐกิจโดย

3.7 ผู้มีส่วนได้ส่วนเสียในกลุ่มหน่วยงานคุ้มครองผู้บริโภค

3.7.1 ข้อจำกัดและความท้าทายในการจัดการปัญหาภัยคุกคามทางไซเบอร์และบัญชีม้า

ผู้ให้สัมภาษณ์เห็นว่ามิจฉาชีพพัฒนาเทคนิคการหลอกลวงอย่างต่อเนื่อง โดยเฉพาะการใช้ Social Engineering เช่น การปลอมเป็นเจ้าหน้าที่รัฐ หรือจากธนาคาร โดยมิจฉาชีพโทรแจ้งเหยื่อว่ามีปัญหาทางกฎหมาย หรือบัญชีมีธุรกรรมผิดปกติ เพื่อให้เหยื่อทำธุรกรรมโดยสมัครใจ ผู้ให้สัมภาษณ์ยกตัวอย่างกรณี

ที่ผู้บริโภครายหนึ่งได้รับ SMS ปลอมจากธนาคาร ซึ่งแจ้งว่ามีการล็อกบัญชีและต้องกดลิงก์เพื่อปลดล็อก ทำให้มิจฉาชีพสามารถเข้าถึงข้อมูลบัญชีได้ นอกจากนี้ มิจฉาชีพยังใช้แพลตฟอร์มออนไลน์ เช่น Facebook Marketplace เป็นช่องทางในการหลอกลวงเหยื่อ ผู้ให้สัมภาษณ์ยกตัวอย่างกรณีที่เหยื่อถูกหลอกให้โอนเงินเพื่อซื้อสินค้าแต่ไม่ได้รับของ อีกทั้งเมื่อเหยื่อแจ้งเรื่องไปยังผู้ให้บริการแพลตฟอร์ม ก็มักไม่ได้รับการตอบสนอง เมื่อแจ้งเรื่องไปยังแพลตฟอร์มมักไม่ได้รับการตอบสนอง

ผู้ให้สัมภาษณ์เห็นว่า กระบวนการแจ้งเหตุยังมีความซับซ้อนและล่าช้า ผู้เสียหายต้องเผชิญกับการส่งต่อระหว่างหน่วยงาน เช่น ตำรวจและธนาคาร โดยไม่มีระบบกลางในการรับเรื่อง ทำให้ต้องเดินเรื่องหลายรอบและใช้เวลานานกว่าจะดำเนินการอายัดบัญชีได้ นอกจากนี้ บัญชีม้ามีเครือข่ายที่ซับซ้อน ทำให้การติดตามเส้นทางการเงินเป็นไปได้ยาก และการบังคับใช้กฎหมายในปัจจุบันยังมีข้อจำกัด เช่น ไม่สามารถอายัดบัญชีได้ทันทีหากไม่มีหลักฐานที่ชัดเจนจากตำรวจ เป็นต้น

ผู้ให้สัมภาษณ์เห็นว่า ประเด็นการเยียวยาผู้เสียหายยังเป็นประเด็นสำคัญ ซึ่งธนาคารมักปฏิเสธความรับผิดชอบ โดยอ้างว่าเป็นธุรกรรมที่ลูกค้าดำเนินการเอง เป็นการให้ข้อมูลโดยสมัครใจ ทำให้ผู้เสียหายได้รับเงินคืนเพียงบางส่วนหรือไม่ได้เลย ทั้งนี้ ผู้ให้สัมภาษณ์สะท้อนว่าระบบป้องกันผู้บริโภคที่มีอยู่ยังไม่เพียงพอ และยังไม่สามารถป้องกันการหลอกลวงของมิจฉาชีพได้ ผู้ให้สัมภาษณ์เห็นว่าจำเป็นต้องมีการทบทวนมาตรการป้องกัน อาทิ การหน่วงเงินธุรกรรมต้องสงสัย การแลกเปลี่ยนข้อมูลบัญชีม้าแบบเรียลไทม์ระหว่างธนาคารและหน่วยงานที่เกี่ยวข้อง เป็นต้น ซึ่งหากสามารถปรับปรุงหรือบังคับใช้มาตรการเหล่านี้ได้ ก็จะช่วยจะช่วยลดโอกาสที่มิจฉาชีพจะถอนเงินออกจากระบบได้อย่างรวดเร็ว

3.7.2 ข้อเสนอแนะของผู้มีส่วนได้ส่วนเสียในกลุ่มหน่วยงานคุ้มครองผู้บริโภค

ผู้ให้สัมภาษณ์ในกลุ่มนี้เน้นย้ำว่า การป้องกันผู้บริโภคจากการหลอกลวงของมิจฉาชีพที่มีประสิทธิภาพทุกภาคส่วน ได้แก่ ธนาคาร หน่วยงานรัฐ และประชาชน ต้องมีการดำเนินงานร่วมกันอย่างจริงจัง และมีข้อเสนอแนะ ดังนี้

- บังคับใช้มาตรการหน่วงเงินธุรกรรมต้องสงสัย โดยเฉพาะธุรกรรมที่มีมูลค่าสูง หรือธุรกรรมที่เงินถูกโอนไปยังบัญชีต้องสงสัย รวมทั้งต้องเปิดช่องทางให้ผู้เสียหายสามารถขอระงับการโอนเงินได้ทันทีเมื่อรู้ตัวว่าถูกมิจฉาชีพหลอก ทั้งนี้ ผู้ให้สัมภาษณ์ยกตัวอย่างกรณีที่ผู้บริโภคโอนเงินไปยังบัญชีปลอม แต่เมื่อรู้ตัวแล้วกลับต้องรอแจ้งความภายใน 2 ชั่วโมง ซึ่งหากมีมาตรการหน่วงเงินก็อาจจะช่วยป้องกันความเสียหายได้
- พัฒนาและจัดทำฐานข้อมูลบัญชีม้าที่สามารถแลกเปลี่ยนข้อมูลแบบเรียลไทม์ ระหว่างธนาคาร หน่วยงานรัฐ และองค์กรผู้บริโภค เพื่อให้สามารถตรวจสอบก่อนทำธุรกรรมได้ เช่น หากมีการโอนเงินไปยังบัญชีต้องสงสัยที่อยู่ในฐานข้อมูล ระบบจะต้องเตือนผู้ใช้ก่อนโอนเงินได้ เป็นต้น
- ควรปรับปรุงกฎหมายที่เพิ่มความรับผิดชอบของธนาคาร ผู้ให้บริการโทรคมนาคม หรือแพลตฟอร์มออนไลน์ ที่ปล่อยให้เกิดการหลอกลวงซ้ำ ๆ โดยไม่ดำเนินมาตรการป้องกัน เช่น หาก

ธนาคารมีการปล่อยให้บัญชีหรือธุรกรรมรูปแบบที่ต้องสงสัยทำธุรกรรมต่อไปโดยไม่ตรวจสอบ ควรมีบทลงโทษ หรือในกรณีที่ระบบมีช่องโหว่ หรือผู้บริโภคไม่ได้มีเจตนาให้ข้อมูลโดยสมัครใจ เช่น กรณีที่มิจฉาชีพใช้แอปปลอมดักจับข้อมูลการเข้าสู่ระบบธนาคาร ธนาคารต้องมีส่วนร่วมในการรับผิดชอบความเสียหายที่เกิดขึ้นด้วย เป็นต้น

- เพิ่มมาตรการป้องกัน โดยให้ธนาคารเพิ่มขั้นตอนการยืนยันตัวตนที่เข้มงวดขึ้น เช่น ต้องใช้การสแกนใบหน้าในการทำธุรกรรมที่มีมูลค่าสูง แทนการใช้ OTP เพียงอย่างเดียว
- ควรปรับปรุงกฎหมายเกี่ยวกับบัญชีม้าให้มีความเข้มงวดมากขึ้น เช่น ให้ธนาคารสามารถระงับบัญชีที่มีพฤติกรรมผิดปกติได้โดยไม่ต้องรอคำสั่งศาล เป็นต้น
- กำกับดูแลแพลตฟอร์มออนไลน์ให้มีมาตรการคัดกรองบัญชีและร้านค้าต้องสงสัย เช่น Facebook Marketplace ควรมีระบบยืนยันตัวตนของผู้ขาย และตรวจสอบบัญชีที่ถูกรายงานบ่อยครั้ง
- พัฒนาช่องทางแจ้งเหตุให้มีประสิทธิภาพและเข้าถึงง่ายจากเดิมที่มีอยู่ หรือเพิ่มการพัฒนาแอปพลิเคชันที่สามารถแจ้งเหตุและติดตามความคืบหน้าได้แบบเรียลไทม์ รวมถึงศูนย์ต้องมีอำนาจในการสั่งการหรือขอความร่วมมือกับหน่วยงานที่เกี่ยวข้องทุกภาคส่วน
- ให้ความรู้แก่ประชาชนเกี่ยวกับภัยไซเบอร์ โดยเฉพาะกลุ่มเปราะบาง เช่น ผู้สูงอายุ และผู้ที่ไม่มีความเชี่ยวชาญด้านเทคโนโลยี ผ่านสื่อสารสาธารณะ เช่น คลิปวิดีโอที่อธิบายรูปแบบการโกงที่พบได้บ่อย โดยอาจทำผ่านภาคธนาคาร หรือบริษัทโทรคมนาคม
- หน่วยงานกำกับดูแลภาคโทรคมนาคมได้มีการกำหนดหลักเกณฑ์การบังคับทางปกครองในกิจการโทรคมนาคมเอาไว้แล้ว โดยมีอัตราค่าปรับทางปกครองต้องไม่ต่ำกว่าสองหมื่นบาทต่อวัน และมีกรอบอัตราสูงสุดคำนวณตามระดับความรุนแรงของการฝ่าฝืนหรือไม่ปฏิบัติตาม (ราชกิจจานุเบกษา, 2566) แต่ในปัจจุบันยังคงพบการส่งข้อความ SMS หลอกลวงประชาชนได้โดยทั่วไป ดังนั้น หน่วยงานกำกับดูแลภาคโทรคมนาคมควรเพิ่มความเข้มงวดในการกำกับดูแล รวมถึงการลงโทษปรับทางปกครองต่อผู้ให้บริการโทรคมนาคม กรณีที่ละเลยหรือไม่สามารถปิดกั้นข้อความ SMS จากมิจฉาชีพที่หลอกลวงประชาชนได้

3.8 ผู้มีส่วนได้ส่วนเสียในกลุ่มทนายและผู้เชี่ยวชาญ

3.8.1 ข้อจำกัดและความท้าทายของปัญหาในคดีฉ้อโกงออนไลน์และบัญชีม้า

ผู้ให้สัมภาษณ์ในกลุ่มนี้เห็นว่า การฉ้อโกงออนไลน์ไม่ได้เป็นเพียงปัญหาทางเทคโนโลยีหรือระบบการเงินเท่านั้น แต่ยังเป็นข้อท้าทายเชิงกฎหมายและกระบวนการยุติธรรมที่ส่งผลกระทบโดยตรงต่อผู้เสียหาย โดยเฉพาะรูปแบบการหลอกลวงที่มีความซับซ้อนและพัฒนาอย่างต่อเนื่อง ทำให้ระบบกฎหมายซึ่งมีความล้าหลัง และขาดมาตรการบังคับใช้ที่มีประสิทธิภาพ ไม่สามารถจัดการปัญหาดังกล่าวได้

ผู้ให้สัมภาษณ์เห็นว่า แม้ว่าธนาคารและหน่วยงานกำกับดูแลจะเพิ่มมาตรการด้านความปลอดภัยมากขึ้น แต่กระบวนการช่วยเหลือผู้เสียหายยังคงล่าช้า และเต็มไปด้วยอุปสรรคทางกฎหมาย เช่น

- กฎหมายคุ้มครองข้อมูลส่วนบุคคล (หรือ PDPA) ทำให้การเข้าถึงข้อมูลบัญชีม้าหรือธุรกรรมที่เกี่ยวข้องทำได้ยาก เนื่องจากธนาคารไม่เปิดเผยข้อมูลให้ทนายหรือผู้เสียหายโดยตรง
- ระบบอายัดบัญชีของธนาคาร ต้องได้รับเอกสารแจ้งความอย่างเป็นทางการก่อนจึงจะสามารถดำเนินการได้ ทำให้ไม่สามารถสกัดกั้นมิจฉาชีพได้อย่างทันท่วงที
- ผู้ให้สัมภาษณ์ที่เป็นทนาย ให้ข้อมูลว่าที่ผ่านมาคดีที่ผู้เสียหายฟ้องร้องธนาคารเพื่อเรียกร้องการชดเชยเยียวยากรณีมิจฉาชีพออนไลน์ ผู้เสียหายต้องรับภาระในการพิสูจน์ข้อเท็จจริงด้วยตัวเอง ขณะที่ธนาคารซึ่งเป็นคู่กรณีนั้น เป็นฝ่ายที่มีข้อมูลที่เกี่ยวข้องครบถ้วนมากกว่าผู้เสียหาย และธนาคารอาจปฏิเสธการเปิดเผยข้อมูลดังกล่าว ส่งผลให้การรวบรวมข้อมูลเพื่อนำมาใช้ประกอบการดำเนินคดีในฝั่งผู้เสียหายต้องเผชิญความยากลำบากและใช้ระยะเวลานาน
- การตัดสินคดีไม่มีมาตรฐานที่ชัดเจน และขาดความคงเส้นคงวา เช่น บางคดีศาลพิจารณาให้ธนาคารร่วมรับผิดชอบ แต่บางคดีศาลกลับพิจารณาว่าเป็นความผิดที่ผู้เสียหายไม่ระมัดระวังตัวเอง เป็นต้น

ผู้ให้สัมภาษณ์ที่เป็นทนายหลายท่านสะท้อนว่า หากไม่มีการแก้ไขปัญหาเชิงโครงสร้างและปรับปรุงกฎหมายให้ทันสมัยขึ้น ผู้เสียหายจำนวนมากจะยังคงติดอยู่ในวังวนของการเรียกร้องสิทธิ์ที่ไม่ได้รับความเป็นธรรม

ผู้ให้สัมภาษณ์รายหนึ่งสะท้อนปัญหาของกลุ่มเปราะบาง ได้แก่ คนไร้บ้าน ซึ่งถูกบังคับหรือถูกหลอกให้เปิดบัญชีม้า โดยมิจฉาชีพใช้วิธีข่มขู่ให้เปิดบัญชี หรือหลอกคนกลุ่มนี้ว่าการเปิดบัญชีจะทำให้ได้รับสิทธิสวัสดิการจากภาครัฐ เป็นต้น หลังจากนั้นมิจฉาชีพจะพาคนกลุ่มนี้ไปเปิดบัญชีที่ธนาคาร โดยมีการซักซ้อมกระบวนการเปิดบัญชีหรือเตรียมคำตอบต่าง ๆ และเมื่อเปิดบัญชีเรียบร้อยแล้ว ก็จะยึดสมุดบัญชีไปทันที

เมื่อมีการดำเนินคดี และจับกุมคนไร้บ้านซึ่งเป็นเจ้าของบัญชีม้า ส่งผลกระทบซ้ำเติมคนกลุ่มนี้ เช่น ถูกฟ้องร้อง ต้องจ่ายค่าปรับ และที่สำคัญที่สุด คือ ไม่สามารถเปิดบัญชีใหม่ได้ ทำให้ไม่สามารถเข้าถึงสิทธิสวัสดิการจากภาครัฐ ไม่สามารถรับเงินค่าจ้างจากการทำงานเพื่อเข้าบัญชีโดยตรงได้ (จำเป็นต้องรับเงินสดและมีความเสี่ยงที่จะถูกขโมยเงิน) หรือที่รุนแรงที่สุดคือไม่สามารถกลับคืนสู่สังคมการทำงานได้ อีกทั้งคนกลุ่มนี้ไม่กล้าแจ้งความ เนื่องจากมิจฉาชีพมักเป็นผู้มีอิทธิพลในพื้นที่ ซึ่งทำให้เกิดความกังวลเรื่องความปลอดภัย

นอกจากนี้ กลุ่มเยาวชนและผู้สูงอายุก็ตกเป็นเหยื่อของมิจฉาชีพที่ถูกหลอกให้เปิดบัญชีม้าเช่นกัน โดยเฉพาะเยาวชนที่ถูกชักชวนผ่านงานออนไลน์หรือเว็บพนัน ส่งผลให้บัญชีถูกอายัดและไม่สามารถรับทุนการศึกษาได้

ผู้ให้สัมภาษณ์เห็นว่า การจับกุมและดำเนินคดีกับกลุ่มเปราะบางเหล่านี้ สะท้อนถึงความไม่เป็นธรรมในการจัดการกับปัญหาบัญชีม้า เนื่องจากไม่สามารถจับกุมมิจฉาชีพหรือผู้กระทำความผิดที่แท้จริงได้

3.8.2 ข้อเสนอแนะของผู้มีส่วนได้ส่วนเสียในกลุ่มทนายและผู้เชี่ยวชาญ

ปัญหาการฉ้อโกงออนไลน์ไม่เพียงแต่สะท้อนถึงความอ่อนแอของระบบธนาคารและความก้าวหน้าของมิจฉาชีพเท่านั้น แต่ยังเผยให้เห็นถึงช่องโหว่ทางกฎหมายและความล่าช้าในกระบวนการยุติธรรม ทั้งนี้ ผู้ให้สัมภาษณ์ที่เป็นทนายหลายท่านเห็นพ้องกันว่าการป้องกันและแก้ไขปัญหานี้ไม่สามารถพึ่งพามาตรการเชิงเทคนิคเพียงอย่างเดียว แต่ต้องมีการปรับปรุงกฎหมายที่ชัดเจนและบังคับใช้ได้จริง ผู้ให้สัมภาษณ์เห็นว่า แม้จะมีมาตรการด้านการเงินและเทคโนโลยีที่พัฒนาไปมาก แต่หากระบบกฎหมายยังคงล้าหลัง ไม่สามารถดำเนินคดีได้อย่างรวดเร็วและมีประสิทธิภาพ โอกาสที่ผู้เสียหายจะได้รับความเป็นธรรมก็จะยิ่งน้อยลง

ผู้ให้สัมภาษณ์มีข้อเสนอแนะในการจัดการปัญหาในคดีฉ้อโกงออนไลน์และบัญชีม้า ดังนี้

1) การปรับปรุงกฎหมายและกระบวนการที่เกี่ยวข้อง

- ควรปรับปรุงให้ระเบียบของ ธปท. มีสภาพบังคับเป็นกฎหมายที่สามารถใช้เป็นหลักฐานในชั้นศาลได้
- ควรขอความร่วมมือจากศาลให้พิจารณาคดีฉ้อโกงออนไลน์เป็นประเภทคดีผู้บริโภค ทั้งนี้ แม้ว่ากฎหมายได้มีการออกแบบขั้นตอนการพิจารณาคดีผู้บริโภคไว้แล้ว กล่าวคือ เมื่อประชาชนมีคู่กรณีเป็นธนาคาร ไม่ว่าจะเป็นฝ่ายที่ฟ้องร้องหรือถูกฟ้องร้อง ธนาคารจะต้องเป็นฝ่ายพิสูจน์ข้อมูลการเงินในบัญชี อย่างไรก็ตาม ในทางปฏิบัติ พบว่า ศาลมักจะพิจารณาคดีฉ้อโกงออนไลน์โดยใช้หลักการพิจารณาคดีทั่วไป (ไม่ได้นำหลักการพิจารณาคดีประเภทคดีผู้บริโภคมาใช้) ซึ่งผู้อ้างเหตุจะต้องเป็นผู้พิสูจน์ความบริสุทธิ์ ทำให้ผู้บริโภคที่ต้องการอ้างเหตุว่าไม่ได้เป็นผู้ใช้จ่ายยอดเงินที่โดนมิจฉาชีพหลอก ต้องเป็นผู้พิสูจน์ความบริสุทธิ์และดำเนินการหาหลักฐานมาต่อสู้คดีด้วยตนเอง อีกทั้งธนาคารยังสามารถปฏิเสธการให้ข้อมูลได้ ยิ่งส่งผลให้การหาหลักฐานมาต่อสู้คดีเป็นไปได้ยากขึ้น
- ควรปรับปรุงกระบวนการอายัดบัญชีม้าให้รวดเร็วขึ้น โดยให้ธนาคารสามารถอายัดบัญชีต้องสงสัยได้ทันทีหากมีหลักฐานเพียงพอ โดยไม่ต้องรอคำสั่งจากตำรวจ
- ควรออกกฎหมายให้แพลตฟอร์มออนไลน์ต้องรับผิดชอบต่อการโฆษณาหลอกลวง เช่น หากพบว่า Facebook หรือ Line มีการเผยแพร่โฆษณาหลอกลวงซ้ำ ๆ ต้องมีบทลงโทษที่ชัดเจน

2) การปรับปรุงด้านข้อมูลและการรายงาน

- ควรพัฒนาศูนย์กลางข้อมูลบัญชีม้าที่สามารถแลกเปลี่ยนข้อมูลได้แบบเรียลไทม์ ระหว่างธนาคาร หน่วยงานกำกับดูแล และตำรวจไซเบอร์ เพื่อให้สามารถติดตามเงินได้เร็วขึ้น
- ควรมีกลไกในการรวบรวมรายชื่อของผู้ที่ถูกหลอกให้เปิดบัญชีม้า โดยเฉพาะกลุ่มเปราะบาง และส่งข้อมูลให้ ธปท. เพื่อตรวจสอบ อันจะเป็นช่องทางที่ช่วยพิสูจน์ความบริสุทธิ์ของผู้ที่ถูกหลอกเหล่านี้ได้

3) การพัฒนาระบบป้องกันภัยไซเบอร์

- ธนาคารควรมีระบบวิเคราะห์พฤติกรรมการใช้จ่ายของลูกค้า และพัฒนาเทคโนโลยีในการป้องกัน อาทิ การใช้ AI ในการตรวจจับธุรกรรมผิดปกติ ที่สามารถแจ้งเตือนและหน่วงเวลาการโอนเงินได้
- ธนาคารควรเพิ่มระบบตรวจสอบหลายชั้น (Multi-Factor Authentication) โดยเฉพาะในธุรกรรมที่มีมูลค่าสูง หรือเป็นธุรกรรมที่ดำเนินการจากอุปกรณ์ที่ไม่เคยใช้งานมาก่อน

3.9 ผู้มีส่วนได้ส่วนเสียในกลุ่มผู้เสียหาย

3.9.1 รูปแบบของภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับผู้เสียหาย

จากการสัมภาษณ์ผู้เสียหาย พบว่า มิจฉาชีพมักหลอกให้ผู้เสียหายเปิดเผยข้อมูลสำคัญและการยืนยันตัวตน เพื่อเข้าถึงแอปพลิเคชันธนาคารของผู้เสียหาย ตัวอย่างเช่น มิจฉาชีพปลอมเป็นเจ้าหน้าที่รัฐ หรือหน่วยงานที่ผู้เสียหายเกี่ยวข้อง หรือแอบอ้างเป็นเจ้าหน้าที่หน่วยงานภาครัฐหรือองค์กรที่มีอำนาจเกี่ยวข้องกับเงินเดือน บำนาญ หรือสวัสดิการ หรือปลอมเป็นเจ้าหน้าที่ขนส่ง เป็นต้น มิจฉาชีพจะหลอกให้ผู้เสียหายเชื่อว่าจำเป็นต้องอัปเดตข้อมูลหรือยืนยันตัวตน หรือชักชวนให้ติดตั้งแอปพลิเคชันปลอม หรือส่งลิงก์เพื่อให้ผู้เสียหายกรอกข้อมูลสำคัญ เช่น รหัสผ่าน เลขบัญชี ข้อมูลบัตรเครดิต รหัสยืนยันตัวตน (OTP) หรือการสแกนหน้า ทำให้มิจฉาชีพสามารถเข้าถึงแอปพลิเคชันธนาคารหรือบัญชีของผู้เสียหายได้ สามารถควบคุมโทรศัพท์หรือบัญชีธนาคารเพื่อเปลี่ยนแปลงรหัสผ่านได้ โดยมีกรณีตัวอย่างที่มิจฉาชีพใช้ในการหลอกลวงผู้เสียหาย อาทิ

- การฟิชชิงผ่าน SMS และลิงก์ปลอม โดยมิจฉาชีพส่งข้อความ SMS หรืออีเมลแอบอ้างเป็นองค์กรที่น่าเชื่อถือ เช่น ธนาคาร บริษัทขนส่ง หรือผู้ให้บริการโทรคมนาคม เพื่อหลอกให้ผู้เสียหายกดลิงก์และใส่ข้อมูลส่วนตัว เช่น เลขบัตรประชาชน รหัส OTP หรือรหัสผ่าน ตัวอย่างเช่น ผู้เสียหายได้รับ SMS ปลอมแจ้งว่าไม่สามารถจัดส่งพัสดุได้ เมื่อกดลิงก์ซึ่งนำไปสู่การสแกนใบหน้า มิจฉาชีพใช้ข้อมูลดังกล่าวรีเซตรหัสผ่านแอปพลิเคชันธนาคารและถอนเงินออกจากบัญชีทันที หรือกรณีผู้เสียหายถูกหลอกผ่าน SMS ปลอมจากผู้ให้บริการโทรคมนาคมว่าแต้มใกล้หมดอายุ ให้กดลิงก์เพื่อแลกของรางวัล เมื่อกรอก OTP หลายครั้ง พบว่าเงินถูกตัดออกจากบัตรเครดิตโดยไม่รู้ตัว เป็นต้น
- การหลอกให้ติดตั้งแอปพลิเคชันปลอม โดยมิจฉาชีพหลอกให้ผู้เสียหายติดตั้งแอปพลิเคชันปลอมที่มีมัลแวร์ฝังอยู่ ซึ่งสามารถขโมยข้อมูลสำคัญหรือควบคุมโทรศัพท์ของผู้เสียหายได้ ตัวอย่างเช่น มิจฉาชีพแอบอ้างว่าเป็นเจ้าหน้าที่กรมบัญชีกลาง แจ้งให้ผู้เสียหายไปปรับปรุงข้อมูลบัญชีบำนาญที่สำนักงาน เมื่อผู้เสียหายแจ้งว่าไม่สะดวกเดินทางไป มิจฉาชีพจึงให้ติดตั้งแอปพลิเคชันปลอมผ่านลิงก์ที่ส่งให้ โดยเมื่อเหยื่อเปิดแอปพลิเคชันทำให้โทรศัพท์ถูกควบคุมและถูกถอนเงินในบัญชีออกไปกว่า 1 ล้านบาท
- การหลอกลวงผ่านบริการออนไลน์ที่ใช้ประจำ โดยมิจฉาชีพใช้ความคุ้นเคยของผู้เสียหายในการใช้บริการออนไลน์ เช่น Netflix Lazada หรือ LINE เพื่อหลอกให้กรอกข้อมูล ตัวอย่างเช่น ผู้เสียหายได้รับอีเมลปลอมจาก Netflix แจ้งว่าการชำระค่าบริการไม่สำเร็จ (ซึ่งตรงกับช่วงที่ผู้เสียหาย

เปลี่ยนบัตรเครดิตพอดี) ทำให้ผู้เสียหายเชื่อ และกรอกข้อมูลและ OTP ทำให้ถูกตัดเงินจากบัตรเครดิตรวมกว่า 6,000 ดอลลาร์สหรัฐ

- การหลอกลองให้โอนเงินปลอม โดยมิจฉาชีพหลอกให้ผู้เสียหายโอนเงินไปยังบัญชีม้าโดยอ้างว่าเกี่ยวข้องกับธุรกรรมที่จำเป็น เช่น ค่าขนส่ง หรือค่าธรรมเนียมปลอม ตัวอย่างเช่น กรณีผู้เสียหายได้รับ SMS จากมิจฉาชีพแจ้งว่า "พัสดุมีปัญหา" ซึ่งตรงกับสถานะจริงในแอปสั่งซื้อของ ทำให้ผู้เสียหายหลงเชื่อและโอนเงินเข้าบัญชีปลอม

จากการสัมภาษณ์ พบว่า ผู้เสียหายหลายรายถูกหลอกให้ทำธุรกรรมโดยสมัครใจ โดยมิจฉาชีพใช้วิธี Social Engineering หรือการสนทนาโดยใช้จิตวิทยาและมีการพูดคุยหรือแชทกันหลายครั้ง เพื่อโน้มน้าวทางจิตวิทยาให้ผู้เสียหายโอนเงินเอง เช่น การข่มขู่ว่าเหยื่อมีคดีความ หรือแอบอ้างเป็นเจ้าหน้าที่ธนาคาร เช่นเหตุการณ์ที่ถูกมิจฉาชีพหลอกให้ใช้แต้มของผู้ให้บริการโทรคมนาคมแลกซื้อสินค้า และหลอกว่าให้จ่ายเงินจำนวนเล็กน้อย เช่น 10 บาท เพื่อใช้สิทธิ์แลกของรางวัล เมื่อทำรายการสำเร็จกลับพบว่ามีการยอดใช้บัตรเครดิตจากการปลอมและมีการใช้จ่ายยอดจากบัตรเครดิตที่ไม่ได้ทำเกิดขึ้นเพิ่มเติมบางกรณี ซึ่งแท้จริงแล้วเป็นการดักรับข้อมูลบัตรเครดิต/OTP เพื่อนำไปตัดวงเงิน เป็นต้น

คณะวิจัยมีข้อสังเกตว่า ผู้ให้สัมภาษณ์บางส่วนไม่สามารถให้ข้อมูลที่ครบถ้วนสมบูรณ์ได้ ตัวอย่างเช่น ปัญหามิจฉาชีพออนไลน์เกิดขึ้นเมื่อนานมากแล้ว ทำให้ผู้ให้สัมภาษณ์ไม่สามารถจดจำรายละเอียดที่เกิดขึ้นได้ทั้งหมด หรือไม่สามารถให้ข้อมูลได้อย่างชัดเจน หรือผู้ให้สัมภาษณ์บางส่วนกังวลว่าการเปิดเผยข้อมูลทั้งหมดอาจส่งผลกระทบต่อกระบวนการพิจารณาคดี นอกจากนี้ แม้ว่าจะมีการประสานนัดหมายผู้มีส่วนได้ส่วนเสียกลุ่มนี้ล่วงหน้าแล้ว แต่เมื่อคณะวิจัยติดต่อขอสัมภาษณ์ พบว่า ผู้มีส่วนได้ส่วนเสียบางส่วนปฏิเสธการให้สัมภาษณ์ เนื่องจากเกิดความไม่มั่นใจ และเกรงว่าจะเป็นการติดต่อจากมิจฉาชีพ ซึ่งคณะวิจัยเห็นว่าเป็นข้อจำกัดในการจัดเก็บข้อมูลในครั้งนี้

อย่างไรก็ตาม แม้ว่าข้อมูลที่ได้อาจจะไม่ครบถ้วนสมบูรณ์ แต่คณะวิจัยเห็นว่าข้อมูลที่ได้จากผู้มีส่วนได้ส่วนเสียกลุ่มนี้สะท้อนให้เห็นผลกระทบที่เกิดขึ้นจากปัญหามิจฉาชีพออนไลน์ได้ในระดับหนึ่ง และคณะวิจัยจะใช้ข้อมูลที่ได้จากการสัมภาษณ์ผู้มีส่วนได้ส่วนเสียกลุ่มอื่นประกอบการวิเคราะห์ด้วย

3.9.2 ความเสียหายที่เกิดขึ้น

จากการสัมภาษณ์ พบว่า ผู้เสียหายที่ตกเป็นเหยื่อของมิจฉาชีพออนไลน์ ไม่เพียงสูญเสียทรัพย์สินจำนวนมากเท่านั้น แต่ยังได้รับผลกระทบทางจิตใจและต้องเผชิญกับกระบวนการขอคืนเงินที่ซับซ้อนและใช้เวลานาน

ผู้เสียหายให้ข้อมูลว่ากระบวนการแจ้งความซับซ้อน บางรายต้องแจ้งเรื่องผ่านหลายหน่วยงานและไม่ได้รับความช่วยเหลือที่รวดเร็วเพียงพอ นอกจากนี้ เมื่อผู้เสียหายสามารถเดินเรื่องเข้าสู่กระบวนการตรวจสอบข้อมูลแล้ว พบว่า กระบวนการตรวจสอบใช้ระยะเวลายาวนาน โดยธนาคารใช้เวลาตรวจสอบหลาย

สัปดาห์จนถึงหลายเดือน หรือถูกเลื่อนตรวจสอบจาก 90 วันเป็น 120 วัน สุดท้ายธนาคารเรียกเก็บเงินทั้งหมด อีกทั้งผู้เสียหายกลับถูกเรียกเก็บเงิน ทำให้ต้องจ่ายดอกเบี้ยที่เป็นหนี้ก้อนใหญ่ในบัตรเครดิต

ผู้เสียหายส่วนใหญ่ถูกปฏิเสธการเยียวยาหรือรับผิดชอบ โดยธนาคารหลายแห่งมองว่าลูกค้าเป็นผู้ยืนยันการทำธุรกรรมด้วยตัวเอง เช่น การใส่รหัส OTP หรือสแกนใบหน้า ซึ่งระบบของธนาคารถือว่าเป็นการ ยินยอมให้มีการทำธุรกรรมดังกล่าว ทำให้ผู้เสียหายต้องดำเนินการฟ้องร้องทางแพ่ง หรือผู้เสียหายบางรายต้องจ่ายหนี้ที่เกิดจากธุรกรรมผ่านบัตรเครดิตที่ถูกหลอกด้วยเงินเก็บส่วนตัว

ผู้เสียหายหลายรายให้สัมภาษณ์ว่าการถูกมิจฉาชีพหลอกลวงยังผลกระทบทางจิตใจ หลายคนเกิดความเครียด ซึมเศร้า และขาดความมั่นใจในการทำธุรกรรมออนไลน์

3.9.3 ข้อเสนอแนะของผู้มีส่วนได้ส่วนเสียในกลุ่มผู้เสียหาย

ผู้เสียหายมีข้อเสนอแนะ ดังนี้

1) ธนาคารควรมีการพัฒนาระบบตรวจสอบอัจฉริยะที่สามารถระบุธุรกรรมที่มีความเสี่ยงสูง เช่น การโอนเงินมูลค่าสูงผิดวิสัย หรือการใช้บัตรเครดิตในต่างประเทศโดยไม่เคยปรากฏมาก่อน เป็นต้น เพื่อให้สามารถตรวจจับธุรกรรมที่ผิดปกติอย่างทันท่วงที และเมื่อพบธุรกรรมที่เข้าข่ายผิดปกติ ควรดำเนินการระงับธุรกรรมชั่วคราวหรือชะลอการทำธุรกรรม พร้อมทั้งโทรศัพท์สอบถามยืนยันกับผู้เป็นเจ้าของบัญชี ก่อนจะดำเนินการให้แล้วเสร็จ
2) การปรับปรุงกระบวนการยืนยันตัวตน (KYC) ให้มีความปลอดภัยสูงขึ้น ควรกำหนดมาตรการยืนยันตัวตนหลายชั้น เช่น กรณีการถูกหลอกว่ามาจากบริษัทขนส่ง และมิจฉาชีพโน้มน้าวเหยื่อให้ยืนยันตัวตนเพื่อตรวจสอบสถานะการจัดส่งพัสดุโดยการสแกนใบหน้าอย่างเดียว อันเป็นช่องทางให้มิจฉาชีพสามารถรีเซตรหัสผ่านของการใช้แอปธนาคารได้ ถือกลายเป็นช่องโหว่สำคัญให้เหยื่อสูญเสียทรัพย์สินมูลค่ามหาศาล และต้องเข้าสู่กระบวนการฟ้องร้องยืดเยื้อในภายหลัง
3) ธนาคารและผู้ให้บริการต่าง ๆ ต้องสร้างความตระหนักแก่ประชาชนถึงวิธีป้องกันการตกเป็นเหยื่อ เช่น ไม่กดลิงก์ไม่ทราบที่มา และไม่ส่งข้อมูลบัตรเครดิตหรือรหัสยืนยันผ่านช่องทางที่ไม่ปลอดภัย
4) มาตรการหน่วงเงินหรือชะลอการตัดเงิน ควรกำหนดระยะเวลาหน่วงเงินสำหรับธุรกรรมที่มีมูลค่าสูงหรือมีลักษณะผิดปกติ เพื่อเปิดโอกาสให้เจ้าของบัญชีสามารถอายัดหรือยกเลิกธุรกรรมได้หากพบความผิดปกติ และระบบธนาคารอาจพิจารณากำหนดให้ธุรกรรมมูลค่าสูงมากต้องผ่านการอนุมัติหรือยืนยันขั้นสุดท้ายจากเจ้าของบัญชีในรูปแบบอื่นเพิ่มเติม (เช่น การโทรศัพท์ยืนยันโดยตรงกับเจ้าของบัญชี)
5) ธนาคารหรือสถาบันการเงินควรมีช่องทางสื่อสารเชิงรุกกับผู้เสียหาย เช่น การแจ้งเตือนสถานะการดำเนินการหรือการตรวจสอบข้อร้องเรียนเป็นระยะ เพื่อสร้างความเชื่อมั่นแก่ลูกค้า (ผู้เสียหายบางรายให้ข้อมูลว่าไม่ได้รับข้อมูลความคืบหน้าจากธนาคารอย่างเพียงพอ ทำให้เกิดความล่าช้าและขาดความชัดเจนในกระบวนการแก้ไขปัญหา)

6) การประสานงานระหว่างธนาคารและหน่วยงานบังคับใช้กฎหมาย ควรจัดตั้งกลไกหรือแพลตฟอร์มกลางในการแลกเปลี่ยนข้อมูลคดีอาชญากรรมทางไซเบอร์ เพื่อให้ตำรวจ ธนาคาร และศูนย์ AOC สามารถติดตามกรณีต่าง ๆ ได้อย่างเป็นระบบ รวมถึงแนะนำให้มีการกำหนดขั้นตอนปฏิบัติที่ชัดเจนระหว่างตำรวจและธนาคาร เมื่อลูกค้าแจ้งความว่าถูกหลอกโอนเงินหรือถูกดูดเงินไป ควรมีระบบการแลกเปลี่ยนข้อมูลเพื่อระงับหรืออายัดบัญชีปลายทางได้อย่างรวดเร็ว
7) การบูรณาการความร่วมมือระหว่างภาครัฐ ธนาคาร และผู้ให้บริการโทรคมนาคม ซึ่งภาครัฐและหน่วยงานที่เกี่ยวข้องควรออกกฎระเบียบหรือแนวปฏิบัติร่วมกันในการตรวจสอบหมายเลขโทรศัพท์หรือข้อความ SMS ที่สงสัยว่าเป็นการหลอกลวง รวมถึงการเฝ้าระวังบัญชีม้า ซึ่งเป็นบัญชีที่มิจฉาชีพใช้รับโอนเงิน และสร้างความร่วมมือเชิงบูรณาการจะช่วยให้สามารถระงับหรือสกัดกั้นเส้นทางการเงินของมิจฉาชีพได้อย่างมีประสิทธิภาพและทันการณ์

บทที่ 4 ข้อเสนอแนะเชิงนโยบาย

คณะวิจัยสกัดข้อสังเกตและข้อค้นพบที่สำคัญจากการทบทวนวรรณกรรมและการสัมภาษณ์ เรียบเรียงเป็นประเด็นสำคัญได้ 4 ประเด็น ดังนี้

1. *หน่วยงานกำกับดูแลเผชิญความท้าทายในการรักษาสมดุลระหว่างการยกระดับมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ กับความสะดวกของประชาชนในการใช้บริการ*

หน่วยงานกำกับดูแลต้องเผชิญความท้าทายมากยิ่งขึ้นในการพิจารณาปรับปรุงกฎระเบียบ แนวปฏิบัติ เพื่อเพิ่มมาตรการรักษาความปลอดภัยและป้องกันมิจฉาชีพได้มากขึ้น เช่น การหน่วงเวลาการทำธุรกรรม การยืนยันตัวตนหลายชั้น เป็นต้น อย่างไรก็ตาม มาตรการดังกล่าวก็ส่งผลกระทบต่อความสะดวกของประชาชนเช่นกัน ดังนั้น หน่วยงานกำกับดูแลจำเป็นต้องมีการติดตามสถานการณ์อย่างใกล้ชิด รวมทั้งทบทวนแนวปฏิบัติหรือมาตรการที่สามารถตอบสนองและรับมือกับปัญหาดังกล่าวอย่างสม่ำเสมอ

2. *การบูรณาการความร่วมมือในการจัดการปัญหาภัยคุกคามทางไซเบอร์และบัญชีม้ายังเผชิญความท้าทาย*

การจัดการกับปัญหาภัยคุกคามทางไซเบอร์และบัญชีม้าเป็นปัญหาสำคัญที่ต้องได้รับความร่วมมือจากทุกภาคส่วนที่เกี่ยวข้อง ที่ผ่านมาหลายหน่วยงานมีความพยายามจะบูรณาการความร่วมมือในการจัดการปัญหา เช่น การจัดตั้งศูนย์ AOC หรือความร่วมมือของธนาคารในการดำเนินงานร่วมกันผ่านกลไกของ TB-CERT เป็นต้น อย่างไรก็ตาม ความร่วมมือดังกล่าวยังไม่สามารถจัดการปัญหาภัยคุกคามทางไซเบอร์ได้อย่างเด็ดขาด และยังไม่รวดเร็วพอที่จะรับมือรับมือกับมิจฉาชีพที่ปรับตัวได้ตลอดเวลา ดังนั้น การเพิ่มความเข้มข้นในการทำงานร่วมกันระหว่างหน่วยงานจึงเป็นปัจจัยสำคัญที่จะทำให้การจัดการปัญหาดังกล่าวมีประสิทธิภาพมากยิ่งขึ้น อาทิ การกำหนดบทบาท หน้าที่ ความรับผิดชอบของแต่ละหน่วยงานให้มีความชัดเจน เป็นรูปธรรมมากขึ้น การปรับปรุงกฎระเบียบที่เกี่ยวข้องให้สามารถตอบสนองการจัดการปัญหาได้อย่างรวดเร็วมากขึ้น รวมถึงการพัฒนาศูนย์ AOC ให้สามารถทำงานได้แบบเบ็ดเสร็จ

3. *กระบวนการเยียวยายังล่าช้าและขาดความชัดเจน*

ปัจจุบันผู้บริโภคที่เป็นผู้เสียหายจากภัยคุกคามทางไซเบอร์และสูญเสียเงินฝากในธนาคารต้องดำเนินการฟ้องร้องธนาคารพาณิชย์ด้วยตนเอง และสุดท้ายอาจได้รับการชดเชยเยียวยาความเสียหายเพียงบางส่วน (พิจารณาเป็นรายคดี ขึ้นอยู่กับคำพิพากษาของศาล) นอกจากนี้ แม้ว่ากระบวนการยุติธรรมจะสิ้นสุดแล้ว แต่ผู้เสียหายอาจไม่ได้รับเงินคืน เนื่องจากมิจฉาชีพได้โอนเงินออกจากบัญชีไปยังบัญชีม้าอื่น ๆ เรียบร้อยแล้ว หรือแม้ว่าจะสามารถติดตามเงินคืนจากมิจฉาชีพได้ แต่กระบวนการยึดทรัพย์เพื่อเฉลี่ยคืนให้กับผู้เสียหายอาจต้องใช้ระยะเวลามากกว่า 1 ปี อีกทั้งยังไม่มีแนวปฏิบัติที่ชัดเจนในกระบวนการพิจารณาลักษณะ

การเยียวยาหรือการเฉลี่ยทรัพย์ให้แก่ผู้เสียหายแต่ละราย ทั้งนี้ ผู้เสียหายอาจได้รับเงินคืนน้อยกว่ามูลค่าที่เสียหาย เนื่องจากต้องเฉลี่ยเงินคืนให้แก่ผู้เสียหายรายอื่น ๆ ด้วย

4. <u>การสร้างความตระหนักรู้ให้กับประชาชนเป็นกลไกสำคัญที่จำเป็นต้องดำเนินการเร่งด่วน</u>

ปัจจุบันรูปแบบการโจมตีของมิจฉาชีพมุ่งเน้นการหลอกลวงผู้ใช้ปลายทาง โดยเฉพาะการใช้เทคนิค social engineering ซึ่งมิจฉาชีพใช้จิตวิทยาเพื่อชักจูงให้เหยื่อเปิดเผยข้อมูลสำคัญเอง แทนการเจาะระบบของธนาคารโดยตรง เพื่อลดความเสี่ยงในการถูกตรวจจับ ดังนั้น การปรับปรุงการสื่อสาร ประชาสัมพันธ์ สร้างความตระหนักรู้ให้กับประชาชน เกี่ยวกับภัยคุกคามทางไซเบอร์และการรับมือกลลวงของมิจฉาชีพ รวมถึงโทษจากการมีส่วนร่วมในการเปิดบัญชีม้า จึงเป็นกลไกที่จำเป็นต้องดำเนินการเร่งด่วน และควรปรับปรุงให้เป็นการสื่อสารเชิงรุกที่สามารถเข้าถึงประชาชนทุกกลุ่ม

จากประเด็นสำคัญข้างต้น คณะวิจัยนำมาวิเคราะห์เพิ่มเติมและสังเคราะห์เป็นข้อเสนอแนะเชิงนโยบาย 7 ประการ โดยมีรายละเอียดดังนี้

4.1 ข้อเสนอแนะสำหรับธนาคารแห่งประเทศไทย ในฐานะหน่วยงานกำกับดูแลสถาบันการเงิน

ที่ผ่านมาธนาคารแห่งประเทศไทย (ธปท.) ให้ความสำคัญกับการกำกับดูแลให้สถาบันการเงินดำเนินการตามแนวปฏิบัติความปลอดภัยด้านเทคโนโลยีสารสนเทศและบัญชีม้าอยู่แล้ว อย่างไรก็ตาม คณะวิจัยมีข้อเสนอว่า ธปท. ควรยกระดับการกำกับดูแลสถาบันการเงินให้มีความเข้มข้นมากขึ้น เพื่อให้ทันต่อระดับความรุนแรงและเร่งด่วนของปัญหา ดังนี้

1) ควรพิจารณาและศึกษาความเป็นไปได้ในการทบทวนและปรับปรุงแนวปฏิบัติของสถาบันการเงินให้มีความเข้มงวดมากขึ้นในการตรวจสอบข้อมูลและยืนยันตัวตนในการเปิดบัญชี และการทำธุรกรรมทางการเงินต่าง ๆ เช่น

- การตรวจสอบพฤติกรรมก่อนอนุมัติการเปิดบัญชี เช่น การวิเคราะห์ข้อมูลพฤติกรรมทางการเงินของบุคคลที่มาขอเปิดบัญชี หากมีแนวโน้มเป็นบัญชีม้า ควรมีการตรวจสอบเพิ่มเติมก่อนอนุมัติ
- การจำกัดจำนวนบัญชีที่บุคคลใดบุคคลหนึ่งสามารถเปิดได้ เพื่อป้องกันไม่ให้มิจฉาชีพใช้ตัวตนเดียวเปิดหลายบัญชี แล้วนำไปใช้ในกิจกรรมผิดกฎหมาย

ทั้งนี้ การศึกษาความเป็นไปได้ในการทบทวนและปรับปรุงแนวปฏิบัติดังกล่าว ควรเปิดให้มีการรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องและครอบคลุมทุกกลุ่ม เพื่อให้มีข้อมูลที่ครบถ้วน เพียงพอ และสามารถรักษาสมดุลระหว่างการยกระดับมาตรการความปลอดภัยกับความสะดวกของประชาชนได้ โดยมีแนวทางปฏิบัติ ดังนี้

ตารางที่ 8 แนวปฏิบัติด้านความเข้มงวดในการตรวจสอบและยืนยันตัวตน

มาตรการ	รายละเอียด	หน่วยงานที่เกี่ยวข้อง	กฎหมายที่เกี่ยวข้อง	ผลที่คาดว่าจะได้รับ
1.1 การตรวจสอบประวัติ / พฤติกรรมก่อนอนุมัติเปิดบัญชี	- พิจารณาใช้ข้อมูลเชิงวิเคราะห์ / พฤติกรรมทางการเงินของผู้ขอเปิดบัญชี เช่น ตรวจสอบประวัติบัญชีที่เคยปิดกะทันหัน หรือการเคยถูกขึ้นบัญชีดำ - หากพบความเสี่ยงสูง ควรตรวจสอบเชิงลึกเพิ่มเติม (Enhanced Due Diligence)	- ธปท. - สถาบันการเงิน	- พระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 (พ.ร.บ. สถาบันการเงินฯ) - พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566	- ลดการเปิดบัญชีม้าที่มิจฉาชีพใช้ - สกัดการเปิดหลายบัญชีในชื่อเดียวกันโดยไม่มีเหตุอันควร
1.2 การจำกัดจำนวนบัญชีต่อคน / เฝ้าระวังหลายบัญชีผิดปกติ	- กำหนดแนวปฏิบัติร่วมกันในการจำกัดจำนวนบัญชีที่บุคคลหนึ่งสามารถเปิดได้ภายในช่วงระยะเวลาที่กำหนด (เช่น 3 หรือ 6 เดือน) - หากตรวจพบ “เปิดบัญชีหลายสิบบัญชี” ในชื่อเดียว อาจเข้าข่ายบัญชีม้า ควรแจ้งเตือน/ตรวจสอบเป็นพิเศษ	- สถาบันการเงิน - สมาคมธนาคารไทย	- พ.ร.บ. สถาบันการเงินฯ	- ป้องกันมิจฉาชีพใช้ตัวตนเดียวเปิดบัญชีจำนวนมาก
1.3 การเพิ่มความเข้มงวดในการยืนยันตัวตนแบบ 2FA	- กำหนดให้ลูกค้าใช้วิธียืนยันตัวตนหลายวิธีร่วมกัน เช่น การใช้รหัสผ่านร่วมกับรหัส OTP เมื่อทำธุรกรรม โดยเฉพาะรายการสำคัญหรือบัญชีต้องสงสัย เช่น การโอนเงิน หรือการเพิ่มบัญชีผู้รับโอน - ให้ระบบตรวจสอบว่า OTP ถูกใช้จริงจากอุปกรณ์ที่ผ่านการลงทะเบียน	- สถาบันการเงิน - ผู้ให้บริการ e-Payment	- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ (สำหรับกรณีแฮ็ก) - ข้อกำหนด ธปท. เรื่อง มาตรฐานความปลอดภัยทางเทคโนโลยีสารสนเทศ	- ลดความเสี่ยงที่มิจฉาชีพจะเข้าถึงและควบคุมบัญชีผู้ใช้ได้โดยง่าย - ป้องกัน Phishing ที่ทำโดยใช้รหัสผ่านเพียงอย่างเดียว
1.4 ระบบแจ้งเตือนเรียลไทม์ (Real-time Alerts)	- เมื่อมีการโอนเงินหรือทำธุรกรรมทุกครั้ง ให้ส่ง SMS / Push Notification แจ้งลูกค้าทันที - หากเป็นรายการผิดปกติ (เช่น มูลค่าสูง หรือการโอนเงินต่างประเทศ) ควรแจ้งเตือนพิเศษ หรือให้ลูกค้ากดยืนยันซ้ำ เพื่อชะลอความเร็วในการทำธุรกรรม	- สถาบันการเงิน	- แนวปฏิบัติ ธปท. ด้าน E-Payment - ประกาศ ธปท. เกี่ยวกับแนวทางป้องกันและแก้ไขปัญหาการทุจริตทางการเงิน	- ลูกค้าธนาคารเห็นทันทีที่มีรายการแปลกปลอม - ลูกค้าสามารถระงับธุรกรรมต้องสงสัยได้ทันเวลา
1.5 ระบบแจ้งเตือนการเปลี่ยนแปลงข้อมูลลูกค้า	หากมีการเปลี่ยนแปลงข้อมูลสำคัญ อาทิ หมายเลขโทรศัพท์ อีเมล หรือที่อยู่ ธนาคารต้องส่งแจ้งเตือนไปยังข้อมูลเดิมของลูกค้าด้วย	- สถาบันการเงิน	- แนวปฏิบัติ ธปท. ด้าน E-Payment - ประกาศ ธปท. เกี่ยวกับแนวทางป้องกันและแก้ไขปัญหาการทุจริตทางการเงิน	- ลูกค้าเห็นทันทีที่เกิดการเปลี่ยนแปลงข้อมูลโดยบุคคลที่สาม - ลูกค้าสามารถแจ้ง

มาตรการ	รายละเอียด	หน่วยงานที่เกี่ยวข้อง	กฎหมายที่เกี่ยวข้อง	ผลที่คาดว่าจะได้รับ
				ความผิดปกติได้เร็วขึ้น
1.6 การรับฟังความคิดเห็นสาธารณะและผู้มีส่วนได้ส่วนเสีย	- จัดกระบวนการรับฟังความเห็นสาธารณะ และกระบวนการปรึกษาหารือกับผู้บริโภค / สมาคมธนาคารไทย / สถาบันวิจัย อย่างสม่ำเสมอ เพื่อประเมินผลกระทบของมาตรการเข้มงวดในการเปิดบัญชี และชั่งน้ำหนักระหว่าง “ความสะดวก” กับ “ความปลอดภัย” - สามารถใช้แพลตฟอร์มออนไลน์หรือเวทีสาธารณะในการระดมความคิดเห็น	- ธปท. - สถาบันการเงิน	- พ.ร.บ. คุ้มครองผู้บริโภค - มติคณะกรรมการนโยบายสถาบันการเงิน (หากกำหนดเป็นนโยบาย)	- การมีส่วนร่วมช่วยวางหลักประกันได้ว่ามาตรการใหม่จะมีความเหมาะสม ไม่ลิดรอนสิทธิส่วนบุคคล และไม่เพิ่มภาระเกินจำเป็น - การมีส่วนร่วมของทุกฝ่ายช่วยเพิ่มความตระหนักรู้ต่อปัญหาในสังคมได้

2) ควรพิจารณาทบทวนและปรับปรุงแนวปฏิบัติของสถาบันการเงินให้สามารถเฝ้าระวังและตรวจสอบพฤติกรรมผิดปกติในระบบได้ก่อนที่จะเกิดเหตุการณ์ขึ้น เช่น

- การกำหนดให้สถาบันการเงินพัฒนาและใช้เทคโนโลยี AI และ machine learning ที่สามารถวิเคราะห์พฤติกรรมของบัญชีธนาคารและธุรกรรมที่ผิดปกติ โดยระบบสามารถแจ้งเตือนและระงับธุรกรรมชั่วคราวหากพบพฤติกรรมผิดปกติ
- การกำหนดให้สถาบันการเงินพัฒนาระบบแจ้งเตือนอัตโนมัติเมื่อมีการทำธุรกรรมที่มีความเสี่ยงสูง และอนุญาตให้ผู้ใช้สามารถระงับการทำธุรกรรมได้เองในช่วงระยะเวลาหนึ่ง เป็นต้น

ทั้งนี้ ควรพิจารณาทบทวนและปรับปรุงแนวปฏิบัติของสถาบันการเงินให้เฝ้าระวังและตรวจสอบพฤติกรรมผิดปกติในระบบก่อนเกิดเหตุ โดยมีแนวทางปฏิบัติ ดังนี้

ตารางที่ 9 แนวปฏิบัติด้านการเฝ้าระวังและตรวจสอบพฤติกรรมผิดปกติของบัญชีและธุรกรรม

มาตรการ	รายละเอียด	หน่วยงานที่เกี่ยวข้อง	กฎหมายที่เกี่ยวข้อง	ผลที่คาดว่าจะได้รับ
2.1 ใช้ AI / Machine Learning เฝ้าระวังธุรกรรมผิดปกติ	- สถาบันการเงินควรพัฒนา Fraud Detection System ด้วยเทคโนโลยี AI วิเคราะห์พฤติกรรมบัญชี เช่น จำนวนครั้งการโอน ยอดเงิน เวลาที่โอน หากพบ “ผิดปกติ” ให้ระงับชั่วคราวหรือแจ้งเตือนลูกค้า - บูรณาการข้อมูล “บัญชีต้องสงสัย”	- ธปท. - สถาบันการเงิน - สมาคมธนาคารไทย	- ประกาศแนวปฏิบัติ ธปท. ด้าน IT Risk - พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน (พ.ร.บ. ปปง.)	- ตรวจจับธุรกรรมเป้าหมายได้ก่อนเงินหาย - เพิ่มโอกาสกู้คืนทรัพย์และอายัดบัญชีได้ทันท่วงที

มาตรการ	รายละเอียด	หน่วยงานที่เกี่ยวข้อง	กฎหมายที่เกี่ยวข้อง	ผลที่คาดว่าจะได้รับ
	ร่วมกันระหว่างธนาคาร เพื่อยับยั้งก่อนจะฟอกเงินผ่านบัญชีม้า			
2.2 ระบบแจ้งเตือนธุรกรรมเสี่ยง และ "ระงับได้เอง" (Transaction Pause)	- เมื่อพบธุรกรรมมูลค่าสูง หรือรูปแบบผิดปกติ ให้แอปธนาคารแจ้งเตือนพิเศษ และให้ลูกค้าสามารถ กด "Pause / Cancel" ธุรกรรมนั้นได้เองภายในเวลาที่กำหนด เช่น 5–10 นาที - ถ้าลูกค้าถูกหลอกกดโอน แต่ยังไม่แน่ใจ สามารถหยุดได้ก่อนเงินถูกโอนออกไป	- สถาบันการเงิน	- ประกาศแนวปฏิบัติ ธปท. ว่าด้วยมาตรการป้องกัน / แก้ไขการทุจริต - มาตรฐานการให้บริการ e-Payment	- ลดเคส Phishing ที่เหยื่อรู้ตัวทันทีหลังโอน - สร้างความอุ่นใจให้ผู้ใช้ว่าหากโอนโดยไม่ตั้งใจ ยังมีเวลาระงับ
2.3 การชะลอธุรกรรมที่มีลักษณะผิดปกติ	กำหนดระยะเวลาชะลอการโอนเงินเมื่อพบว่าธุรกรรมนั้นเข้าข่ายผิดปกติ โดยระงับชั่วคราว 12-24 ชั่วโมง และแจ้งให้ลูกค้ายืนยันตัวตนก่อนดำเนินการต่อ	- ธปท. - สถาบันการเงิน	- พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	ป้องกันการโอนเงินผิดกฎหมาย และช่วยให้มีเวลาตรวจสอบเพิ่มเติม
2.4 ระบบรอหากเปิดใช้งาน E-Banking บนเครื่องใหม่ (Cooling-off Period)	- หากลูกค้าขอ "ลงทะเบียนอุปกรณ์ / Token" ใหม่ ต้องใส่ ระยะเวลารอ (12 ชม. หรือมากกว่า) ก่อนจะทำธุรกรรมมูลค่าสูงได้ - แจ้งเตือนลูกค้าต้นฉบับทันทีเมื่อมีการเปิด Token ที่เครื่องใหม่	- สถาบันการเงิน	- ประกาศแนวปฏิบัติ ธปท. หรือออกเป็นมาตรฐานสมาคมธนาคารได้	- ป้องกัน SIM Swap Fraud หรือกรณีมิจฉาชีพเพิ่มอุปกรณ์ตนเองแล้วรีบโอนเงิน - ลูกค้ามีเวลารู้ตัวก่อนเกิดธุรกรรมต้องสงสัย

3) ควรดำเนินการเชิงรุกในการผลักดันให้เกิดความร่วมมือกับหน่วยงานอื่นที่เกี่ยวข้อง ดังนี้

- การสร้างระบบแบ่งปันข้อมูลบัญชีม้าแบบเรียลไทม์ ซึ่งจะทำให้เข้าถึงข้อมูลธุรกรรมต้องสงสัยได้เร็วขึ้น และยกระดับการป้องกันและติดตามเส้นทางการเงินของบัญชีม้าได้อย่างมีประสิทธิภาพมากขึ้น
- การจัดตั้งคณะทำงานร่วมเพื่อศึกษาความเป็นไปได้ในการปรับปรุงกฎหมายเพื่อทลายข้อจำกัดของสถาบันการเงินในการจัดการบัญชีม้า อาทิ การเพิ่มอำนาจของธนาคารในการอายัดบัญชีได้โดยไม่ต้องรอคำสั่งจากตำรวจ หรือสามารถขยายระยะเวลาการระงับบัญชีต้องสงสัยได้ (ปัจจุบันระยะเวลาการระงับบัญชีอยู่ที่ 72 ชั่วโมง) หากมีหลักฐานเพียงพอว่าบัญชีดังกล่าวอยู่ในฐานข้อมูลบัญชีม้าหรือมีพฤติกรรมผิดปกติ และการปรับปรุงแนวปฏิบัติในกระบวนการดำเนินคดี โดยกำหนดให้หน่วยงานภาครัฐและธนาคารต้องให้ความช่วยเหลือทางกฎหมายแก่ผู้เสียหาย โดยไม่ต้องรอให้ผู้เสียหายดำเนินการด้วยตนเอง

- การจัดตั้งคณะทำงานร่วมเพื่อจัดทำแผนและดำเนินการสื่อสาร ประชาสัมพันธ์ และสร้างความตระหนักรู้ให้กับประชาชน เกี่ยวกับภัยคุกคามทางไซเบอร์ การรับมือกลลวงของมิจฉาชีพ โทษจากการมีส่วนร่วมในการเปิดบัญชีม้า รวมถึงการประชาสัมพันธ์ศูนย์ AOC ให้เป็นที่รู้จักในฐานะศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ที่สามารถดำเนินการได้แบบเบ็ดเสร็จ โดยดำเนินการเชิงรุกในลักษณะแผนการสื่อสารประชาสัมพันธ์ที่เป็นวาระแห่งชาติ มีช่องทางการสื่อสารที่หลากหลาย เข้าถึงประชาชนทุกกลุ่ม โดยเฉพาะกลุ่มเปราะบาง โดยมีแนวทางปฏิบัติดังนี้

ตารางที่ 10 แนวปฏิบัติด้านการผลักดันให้เกิดความร่วมมือกับหน่วยงานที่เกี่ยวข้อง

มาตรการ	รายละเอียด	หน่วยงานที่เกี่ยวข้อง	กฎหมายที่เกี่ยวข้อง	ผลที่คาดว่าจะได้รับ
3.1 แบ่งปันข้อมูลบัญชีม้าแบบเรียลไทม์	- จัดตั้งแพลตฟอร์มกลางให้ธนาคารทุกแห่งส่งข้อมูลบัญชีต้องสงสัยแบบเรียลไทม์ เพื่อช่วยกันบล็อกหรือเฝ้าระวัง - บูรณาการฐานของมูลของหมายเลขโทรศัพท์เพื่อตรวจสอบ	- ธปท. - สถาบันการเงิน - สำนักงานตำรวจแห่งชาติ	- พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน - พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566	- ติดตามและสกัดบัญชีม้าได้รวดเร็ว - ลด “Chain Transfer” ตามเส้นทางเงิน
3.2 ปรับปรุงกฎหมายให้ธนาคาร “อายัดบัญชี” ได้ทันที	- ตั้งคณะทำงานร่วมระหว่างธนาคาร ธปท. สตช. ปปง. เพื่อศึกษาความเป็นไปได้ในการเพิ่มอำนาจธนาคารในการอายัดบัญชีต้องสงสัยโดยไม่ต้องรอคำสั่งตำรวจ (ภายใต้เงื่อนไข / หลักฐานเพียงพอ) - ขยายเวลาระงับเกิน 72 ชั่วโมง หากตรวจพบเป็นบัญชีม้าจริง	- ธปท. - สถาบันการเงิน - สมาคมธนาคารไทย - สตช. - ปปง.	- พ.ร.บ. ฟอกเงิน - พ.ร.บ. สถาบันการเงินฯ	- สามารถหยุดการโอน/ถอนในบัญชีม้าได้เร็วขึ้น - ประสิทธิผลการปราบปรามแก๊งคอลเซ็นเตอร์สูงขึ้น
3.3 จัดตั้งคณะทำงาน “แผนประชาสัมพันธ์วาระแห่งชาติ”	- รัฐร่วมกับสถาบันการเงิน ตำรวจ ผู้ให้บริการโทรคมนาคม ผู้ให้บริการแพลตฟอร์ม / Marketplace จัดโครงการสื่อสารเชิงรุก ให้ประชาชนตระหนักรู้ถึงอาชญากรรมไซเบอร์ โทษการเปิดบัญชีม้า ศูนย์ AOC และวิธีป้องกันฟิชชิง-แก๊งคอลเซ็นเตอร์ - เข้าถึงกลุ่มเปราะบางผ่านสื่อต่าง ๆ	- ธปท. - กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม - สตช. - ผู้ให้บริการโทรคมนาคม - ผู้ให้บริการแพลตฟอร์ม / marketplace	- พ.ร.บ. คุ้มครองผู้บริโภคฯ - มติคณะรัฐมนตรี (หากจัดเป็นวาระแห่งชาติ)	- คนทั่วไปตื่นตัวกับกลโกงใหม่ ๆ - ลดจำนวนเหยื่อ - ศูนย์ AOC เป็นที่รู้จัก ช่วยเหลือผู้เสียหายได้เบ็ดเสร็จ

4) ควรพิจารณาจัดทำหลักเกณฑ์ แนวปฏิบัติ และความรับผิดชอบของสถาบันการเงินในการเยียวยาผู้เสียหายที่มีความชัดเจนมากยิ่งขึ้น โดยอย่างน้อยควรพิจารณาประเด็นดังต่อไปนี้

- การจัดทำหลักเกณฑ์ในการชดเชยเยียวยาผู้เสียหายที่มีความชัดเจนมากขึ้น โดยเฉพาะในกรณีที่ผู้เสียหายถูกมิจฉาชีพหลอกลวงให้ทำธุรกรรมเอง (authorized fraud)
- การกำหนดมาตรฐานการชดเชยเยียวยาที่เป็นธรรม โดยผู้เสียหายควรได้รับการชดเชยเยียวยาภายในระยะที่เหมาะสม หลังจากที่สามารถพิสูจน์ได้ว่าถูกมิจฉาชีพหลอกลวง และสถาบันการเงินควรต้องชดเชยเยียวยา หรือ “คืนเงินโดยอัตโนมัติ” โดยไม่ต้องให้ผู้เสียหายดำเนินการทางกฎหมายเอง

โดยมีแนวทางปฏิบัติ ดังนี้

ตารางที่ 11 แนวปฏิบัติด้านการจัดทำหลักเกณฑ์ แนวปฏิบัติ และความรับผิดชอบของสถาบันการเงินในการเยียวยาผู้เสียหาย

มาตรการ	รายละเอียด	หน่วยงานที่เกี่ยวข้อง	กฎหมายไทยที่เกี่ยวข้อง	ผลที่คาดว่าจะได้รับ
4.1 กำหนดเกณฑ์ชดเชยสำหรับผู้เสียหายที่ถูกหลอกทำธุรกรรมเอง	- จัดทำ “หลักเกณฑ์การชดเชยกรณีผู้เสียหายถูกมิจฉาชีพหลอกลวงให้ทำธุรกรรมเอง” (authorized fraud) ชัดเจน เช่น มีข้อกำหนดว่าหากมีหลักฐานว่าลูกค้าถูกหลอกลวงจริง ธนาคารอาจพิจารณาชดเชยบางส่วนหรือเต็มจำนวน - กำหนดเพดานหรือเงื่อนไข เช่น ผู้เสียหายต้องแจ้งภายใน 24 ชั่วโมง หรือแสดงหลักฐานว่าถูกหลอก - กำหนด “ระยะเวลาการคืนเงิน” ที่เหมาะสม	- ธปท. - สถาบันการเงิน - สมาคมธนาคารไทย	- ประกาศแนวปฏิบัติ ธปท.	- ผู้เสียหาย authorized fraud ได้ความช่วยเหลือ - สร้างบรรทัดฐานและสถาปนาความเป็นธรรมในการชดเชย
4.2 มาตรฐานการคืนเงินอัตโนมัติ (Fast Refund) กรณีพิสูจน์แล้วว่าเป็น phishing	- ในกรณีเป็น “unauthorized transaction” เพราะฟิชชิงแน่ชัด และ เกิดจากความบกพร่องของธนาคาร เช่น ไม่ได้แจ้งเตือนธุรกรรมที่มีความเสี่ยง ลูกค้าควรได้ “คืนเงินอัตโนมัติ” โดยไม่ต้องฟ้องร้อง - อาจกำหนดกรอบวัน เช่น “ภายใน 5 วันทำการ”	- ธปท. - สถาบันการเงิน	- ประกาศแนวปฏิบัติ ธปท. ด้าน e-Payment	- ลดภาระที่ผู้เสียหายต้องไปฟ้องคดีเอง - หากธนาคารยอมรับผิด ชดเชยทันที ช่วยสร้างความเชื่อมั่นระยะยาวต่อระบบการเงิน

มาตรการ	รายละเอียด	หน่วยงานที่เกี่ยวข้อง	กฎหมายไทยที่เกี่ยวข้อง	ผลที่คาดว่าจะได้รับ
4.3 ปรับปรุงกระบวนการร้องเรียน-พิสูจน์ให้โปร่งใส	- จัดทำระบบให้ลูกค้าตรวจสอบสถานะคำร้องเรียนได้ว่าอยู่ขั้นไหน, เหตุใดล่าช้า - มีคณะกรรมการกลางหรือกลไกระงับข้อพิพาทที่อยู่นอกกระบวนการศาล (เทียบ FIDReC สิงคโปร์)	- ธปท. - สถาบันการเงิน - สมาคมธนาคารไทย - สคบ.	- พ.ร.บ. คุ้มครองผู้บริโภค - ยกร่างกฎหมาย / กฎระเบียบเฉพาะ	- เพิ่มความโปร่งใสเหยื่อทราบขั้นตอนทุกระยะ - ลดข้อพิพาทยืดเยื้อ

5) ควรพิจารณาทบทวนประสิทธิผลของมาตรการที่ผ่านมาของ ธปท. อย่างน้อยปีละ 1 ครั้ง เนื่องจากมิจฉาชีพเปลี่ยนแปลงเทคนิคการหลอกลวงอยู่เสมอมาตรการที่เคยได้ผลในอดีตอาจไม่จำเป็น หรือได้ประโยชน์ไม่คุ้มค่ากับต้นทุนหรือความเสี่ยงอีกต่อไป ตัวอย่างเช่น มาตรการสแกนใบหน้าทุกครั้งที่โอนเงินขั้นต่ำ 50,000 บาท สร้างภาระให้กับผู้ใช้บริการ เพิ่มความเสี่ยงที่ข้อมูลชีวมิติ (biometric) อาจรั่วไหลจากสถาบันการเงิน ในขณะเดียวกันก็ไม่สามารถแก้ปัญหาการหลอกลวงของมิจฉาชีพปัจจุบันที่ใช้วิธีล่อหลอกให้ผู้ใช้บริการทำธุรกรรมด้วยตัวเอง มิได้สวมรอยเป็นผู้ใช้แต่อย่างใด

ตารางที่ 12 แนวปฏิบัติด้านทบทวนประสิทธิผลมาตรการของธนาคารแห่งประเทศไทย

มาตรการ	รายละเอียด	หน่วยงานหลัก	กฎหมายไทยที่เกี่ยวข้อง	ผลที่คาดว่าจะได้รับ
5.1 ประเมินซ้ำความคุ้มค่า / ประสิทธิผลของมาตรการ	- กำหนดรอบประเมินมาตรการที่เกี่ยวข้องอย่างน้อยปีละ 1 ครั้ง เพื่อตรวจสอบว่ามาตรการใดใช้ได้ผลจริง หรือมีต้นทุนสูงแต่ได้ผลน้อย เช่น บังคับสแกนใบหน้าทุกครั้งอาจไม่คุ้มค่า เป็นต้น - มีระบบรวบรวมข้อมูลจากสถิติการร้องเรียน ข้อเสนอแนะประชาชน มุมมองผู้เชี่ยวชาญ	- ธปท. - สถาบันการเงิน - สมาคมธนาคารไทย	- ประกาศแนวปฏิบัติ ธปท.	- ทำให้มาตรการมีความคล่องตัว - เท่าทันต่อเทคนิคของมิจฉาชีพที่เปลี่ยนแปลงตลอดเวลา - ลดภาระผู้ใช้หากมาตรการบางอย่างล้าสมัย
5.2 ปรับปรุง / ยกเลิกมาตรการที่ไม่ตอบโจทย์	- หากพบว่ามาตรการปัจจุบัน เช่น ระดับเกณฑ์สแกน Biometric โอน 50,000 บาท สร้างภาระและไม่แก้ปัญหาจริง ควรพิจารณาปรับเปลี่ยนเงื่อนไข ลดภาระ หรือใช้เทคโนโลยีใหม่	- ธปท. - สถาบันการเงิน - สมาคมธนาคารไทย	- กฎหมายเฉพาะที่เกี่ยวโยง เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) เรื่องการเก็บข้อมูลชีวมิติ (biometric)	- ผู้บริโภคได้มาตรการที่ “ทันสมัย” และ “ได้ผล” จริง - ไม่เกิดการเก็บข้อมูลส่วนเกินที่ไม่จำเป็น เพิ่มความเสี่ยงที่ข้อมูลจะรั่วไหล

4.2 ข้อเสนอแนะสำหรับหน่วยงานอื่น ๆ นอกเหนือจาก ธปท.

1) การเพิ่มความเข้มงวดในการลงทะเบียนซิมโทรศัพท์

ซิมม้าเป็นช่องโหว่สำคัญที่มิจฉาชีพใช้ในการเข้าถึงระบบธนาคาร เนื่องจากเป็นขั้นตอนสุดท้ายของการยืนยันตัวตนของผู้ใช้บริการ ดังนั้น กสทช. ในฐานะหน่วยงานกำกับดูแลผู้ให้บริการโทรคมนาคม ควรพิจารณาและศึกษาความเป็นไปได้ในการทบทวนและปรับปรุงแนวปฏิบัติของผู้ให้บริการโทรคมนาคมให้มีความเข้มงวดมากขึ้นในการตรวจสอบข้อมูลและยืนยันตัวตนในการเปิดซิม เช่น ให้เจ้าของซิมต้องกดยืนยันความเป็นเจ้าของทุก 3 เดือน เป็นต้น

นอกจากนี้ ควรจัดทำหลักเกณฑ์ในการตรวจสอบและสุ่มตรวจหมายเลขโทรศัพท์ที่มีพฤติกรรมผิดปกติ เช่น หมายเลขที่ใช้ทำธุรกรรมที่มีความเสี่ยงสูง และกำหนดให้ผู้ให้บริการโทรคมนาคมรายงานผลการตรวจสอบเป็นประจำ รวมถึงเผยแพร่ผลการตรวจสอบต่อสาธารณะ ทั้งนี้ ควรเปิดรับฟังความเห็นสาธารณะก่อนบังคับใช้ เพื่อไม่ให้ผู้ใช้บริการเดือดร้อนเกินจำเป็น โดยมีแนวปฏิบัติ ดังนี้

ตารางที่ 13 แนวปฏิบัติในการดูแลของผู้ให้บริการโทรคมนาคม

มาตรการ	รายละเอียด	หน่วยงานที่เกี่ยวข้อง	กฎหมายที่เกี่ยวข้อง	ผลที่คาดว่าจะได้รับ
1. ป้องกัน SIM Swap Fraud	- กำหนดให้ผู้ให้บริการโทรคมนาคมตรวจสอบตัวตนเข้มงวด เมื่อลูกค้าขอออกซิมใหม่ / ย้ายซิม เช่น การสแกนใบหน้า การขอเอกสารฉบับจริง เพื่อตรวจสอบเทียบหมายเลขชิป ฯลฯ - ถ้า “ตัวแทน” หรือ “ร้านสะดวกซื้อ” รับออกซิม ต้องมีระบบ e-KYC	- กสทช. - ผู้ให้บริการโทรคมนาคม	- พ.ร.บ. โทรคมนาคมฯ - ประกาศ กสทช. ว่าด้วยการลงทะเบียนซิม - พ.ร.ก. มาตรการฯ ป้องกันบัญชีม้า 2566 (อาจใช้สกัดการเปิดเบอร์ม้า)	- ลดการปลอมเอกสารขอซิมใหม่ ป้องกันกรณีมิจฉาชีพขโมย OTP ผ่านการย้ายซิม
2. ระบบ Block SMS ที่ไม่ได้รับอนุญาต / ตั้ง SMS Sender ID Registry	- ผู้ให้บริการโทรคมนาคมต้องมีระบบลงทะเบียน Sender ID ให้กับผู้ที่ซื้อ SMS ส่งปริมาณสูง โดยอาจต้องเป็นหน่วนงานที่มีการรับรองหรือถูกต้องตามกฎหมาย - หากมี SMS ที่อ้าง Sender ID แต่ไม่อยู่ในระบบ registry ให้บล็อกหรือติดป้าย “Likely SCAM”	- กสทช. - ผู้ให้บริการโทรคมนาคม	- พ.ร.บ. การประกอบกิจการโทรคมนาคมฯ - ประกาศแนวปฏิบัติ กสทช. เรื่องประกาศร่วมมือผู้ให้บริการโทรคมนาคมสกัด SMS หลอกลวง	- ป้องกันการสวมชื่อธนาคาร หรือองค์กรต่าง ๆ - ลด SMS ฟิชชิงที่ปลอมชื่อผู้ส่ง

มาตรการ	รายละเอียด	หน่วยงานที่เกี่ยวข้อง	กฎหมายที่เกี่ยวข้อง	ผลที่คาดว่าจะได้รับ
	- ผู้ให้บริการโทรคมนาคมต้องติดตั้งระบบ AI-based Filtering เพื่อตรวจสอบและบล็อก SMS ที่มีลิงก์ฟิชชิงหรือข้อความน่าสงสัย ก่อนถึงลูกค้า			
3. ระบบยืนยันตัวตนของเลขหมาย Caller ID Authentication	- ใช้เทคโนโลยีตรวจหมายเลขโทรเข้าต้นทาง - ถ้าตรวจพบ Caller ID ปลอม ให้ขึ้นเตือนหรือบล็อก	- กสทช. - ผู้ให้บริการโทรคมนาคม	- ประกาศแนวปฏิบัติ กสทช. เรื่องการป้องกัน Caller ID spoofing (ถ้ามีการบังคับใช้) - พ.ร.บ. โทรคมนาคมฯ	- ลดแก๊งคอลเซ็นเตอร์ที่ปลอมหมายเลขเป็นหน่วยงานราชการ / ธนาคาร - ช่วยผู้บริโภคไม่หลงเชื่อสายปลอม
4. การยืนยันตัวตนผู้ใช้งาน SIM เป็นระยะ (Periodic ID Verification)	- กำหนดให้มี “Re-Verify” หรือ “Re-KYC” เป็นประจำ เช่น ทุก 3 เดือน หรือ 12 เดือน สำหรับเบอร์ที่ใช้งานอยู่ผ่านการแจ้งเตือนผู้ใช้ผ่าน SMSหรือแอปฯ เพื่อยืนยันตัวตน ผ่าน e-KYC หรือระบบยืนยันตัวตนอื่นๆ ภายในระยะเวลาที่กำหนด - หากผู้ใช้ไม่ดำเนินการหรือยืนยันตัวตนไม่ผ่านในระยะเวลาที่กำหนด ผู้ให้บริการโทรคมนาคมอาจระงับการโทรออกหรือระงับข้อมูลชั่วคราว จนกว่าจะมีการยืนยันตัวตน - กรณีตรวจพบว่าผู้ใช้เป็น “บุคคลอันตราย” หรือใช้เอกสารปลอม ควรบันทึกเป็นบัญชีดำร่วมกันในเครือข่าย	- กสทช. - ผู้ให้บริการโทรคมนาคม	- พ.ร.บ. การประกอบกิจการโทรคมนาคม พ.ศ. 2544 - ประกาศแนวปฏิบัติ กสทช. เรื่องการลงทะเบียนซิม / การคุ้มครองผู้ใช้บริการโทรคมนาคม - กฎหมาย / ประกาศเสริมเกี่ยวกับ e-KYC และการคุ้มครองข้อมูลส่วนบุคคล (PDPA)	- ป้องกันกรณี “เบอร์ผี” หรือ “ซิมม้า” ที่มีการใช้งานยาวนานแต่ไม่เคยยืนยันตัวตน - ลดโอกาสที่มิจฉาชีพนำเบอร์ที่ลงทะเบียนแบบหลวม ๆ มาทำ SIM Swap หรือหลอกลวงทางโทรศัพท์ได้ง่าย - ทำให้ผู้ให้บริการโทรคมนาคมมีข้อมูลอัปเดตของผู้ใช้ช่วยสืบสวนเมื่อเกิดคดีอาชญากรรม

2) การยกระดับการป้องกันการใช้แพลตฟอร์มออนไลน์ในการหลอกลวง

มิจฉาชีพจำนวนมากใช้แพลตฟอร์มออนไลน์ในการหลอกลวงเหยื่อ ไม่ว่าจะเป็นการลงทุนปลอม การหลอกขายของออนไลน์ หรือการปลอมตัวเป็นหน่วยงานราชการ ดังนั้น หน่วยงานที่เกี่ยวข้องควรกำหนดมาตรการเพื่อยกระดับการป้องกันการใช้แพลตฟอร์มออนไลน์ในการหลอกลวง อาทิ การกำหนดแนวปฏิบัติให้ผู้ให้บริการแพลตฟอร์มออนไลน์ต้องมีมาตรการตรวจสอบตัวตนผู้ใช้ที่ทำธุรกรรมทางการเงิน เช่น การลงทะเบียนบัญชีธุรกิจโดยใช้เอกสารราชการ การพัฒนาระบบยืนยันตัวตนของผู้ขายที่เข้มงวดขึ้น เพื่อลดการใช้บัญชีปลอมในการขายของหลอกลวง การจัดทำ “บัญชีขาว” (White List) สำหรับบัญชีที่สามารถทำธุรกรรมทางการเงินได้ และเปิดให้ธนาคารสามารถตรวจสอบความน่าเชื่อถือของบัญชีปลายทางก่อนอนุมัติการโอนเงินได้ เป็นต้น

ทั้งนี้ ควรเปิดรับฟังความเห็นสาธารณะก่อนบังคับใช้ เพื่อไม่ให้ผู้ใช้บริการเดือดร้อนเกินจำเป็น โดยมีแนวปฏิบัติ ดังนี้

ตารางที่ 14 แนวปฏิบัติในการกำกับดูแลของ Marketplace/Platform

มาตรการ	รายละเอียด	หน่วยงานหลัก	กฎหมายที่เกี่ยวข้อง	ผลที่คาดว่าจะได้รับ
1. การยืนยันตัวตนร้านค้า	- Marketplace ควรบังคับยืนยันตัวตนผู้ขายอย่างเข้มงวด เช่น อัปโหลดบัตรประชาชนหรือรูปถ่ายตัวเอง (selfie) หรือ e-KYC - หากมีการโอนเงินภายในแพลตฟอร์ม ควรบันทึกข้อมูลบัญชีธนาคารที่ชัดเจน และไม่เปิดช่องให้ใช้เกิดบัญชีร้านค้าแบบไม่มีการยืนยันตัวตน	- Marketplace - กระทรวงพาณิชย์ (พณ.) - ETDA	- พ.ร.บ. ว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ - พ.ร.บ.คุ้มครองผู้บริโภค	- ลดร้านค้าปลอมหลอกให้ลูกค้าโอนนอกระบบ - ตามหาตัวผู้ขายได้ง่ายขึ้นถ้าเกิดปัญหา
2. มีระบบรายงานร้านฉ้อโกง / Review & Ban	- สร้าง ปุ่มรายงาน (Report) ให้ผู้บริโภคร้องเรียนร้านค้าน่าสงสัยได้ - ตั้งทีมตรวจสอบเร่งด่วน หากพบหลักฐานฉ้อโกงจะต้องแบน / ระงับร้านหรือบัญชี หรืออายัดเงินค้างในระบบ ทันที	- ETDA - Marketplace	- พ.ร.บ.คอมพิวเตอร์ฯ (กรณีฉ้อโกงผ่านระบบ) - พ.ร.บ.คุ้มครองผู้บริโภค	- ลดระยะเวลาที่ร้านปลอมอยู่ในระบบ - ผู้บริโภคคนอื่นไม่ตกเป็นเหยื่อซ้ำ

มาตรการ	รายละเอียด	หน่วยงานหลัก	กฎหมายที่เกี่ยวข้อง	ผลที่คาดว่าจะได้รับ
3. แจ้งเตือนผู้ซื้อ “ระวังลิงก์ภายนอก”	- หากมีคนร้ายส่งลิงก์นอกระบบ Marketplace (เช่น เว็บธนาคารปลอม) ผ่านช่องแชท ระบบควรเตือนการกดลิงก์นอกระบบเสี่ยงโดนหลอกลวง - หากตรวจพบลิงก์ซ้ำที่เคยถูกรายงานหลอกลวง ให้บล็อกหรือแจ้งเตือนล่วงหน้า	- Marketplace	- พ.ร.บ.คุ้มครองผู้บริโภค	- ผู้ซื้อรู้ตัวก่อนกดลิงก์ปลอม - ยับยั้งการฟิชชิงใน Marketplace ได้เร็ว

บรรณานุกรม

1. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (1 พฤศจิกายน 2566). เข้าถึงได้จาก https://www.mdes.go.th/news/detail/7535-
2. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (1 เมษายน 2567). เข้าถึงได้จาก https://www.mdes.go.th/news/detail/7974-AOC-1441-%E0%B9%80%E0%B8%95%E0%B8%B7%E0%B8%AD%E0%B8%99%E0%B8%A0%E0%B8%B1%E0%B8%A2%E0%B8%A3%E0%B8%B0%E0%B8%A7%E0%B8%B1%E0%B8%87%E0%B8%96%E0%B8%B9%E0%B8%81%E0%B8%AB%E0%B8%A5%E0%B8%AD%E0%B8%81%E0%B9%82%E0%B8%AD%E0%B8%9
3. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (ม.ป.ป.). *พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562*. เข้าถึงได้จาก กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม: https://www.mdes.go.th/uploads/tinymce/source/NCSA/Document/PPT%20CYBER-publish.pdf
4. กลต. (ม.ป.ป). เข้าถึงได้จาก https://market.sec.or.th/public/ipos/IPOSGetFile.aspx?TransID=395861&TransFileSeq=7
5. กสทช. (15 กรกฎาคม 2567). เข้าถึงได้จาก https://www.nbtc.go.th/News/Information/66726.aspx?lang=th-TH
6. ฐานเศรษฐกิจ. (2566). เข้าถึงได้จาก https://www.thansettakij.com/finance/financial-banking/557755
7. ไทยโพสต์. (9 กรกฎาคม 2567). *ดีอี ประกาศแอปดูดเงิน เป็นภัยคุกคามทางไซเบอร์ระดับร้ายแรง*. เข้าถึงได้จาก ไทยโพสต์: https://www.thaipost.net/economy-news/617357/
8. ธนาคารกรุงไทย. (2024). *ความปลอดภัยทางไซเบอร์*. เข้าถึงได้จาก krungthai: https://krungthai.com/th/sustainability/esg-policy/governance/cyber-security
9. ธนาคารกรุงศรีอยุธยา. (2024). *ด้านธรรมาภิบาล*. เข้าถึงได้จาก krungsri: https://www.krungsri.com/th/esg/sustainable-banking/esg/governance
10. ธนาคารกสิกรไทย. (2020). *Documents.* เข้าถึงได้จาก kasikornbank: https://www.kasikornbank.com/th/News/Documents/KBank%20Vision%202020_News%20Release_TH.docx
11. ธนาคารกสิกรไทย. (2024). *sustainable development*. เข้าถึงได้จาก kasikornbank: https://www.kasikornbank.com/th/sustainable-development/goal/Pages/dataprivacy.aspx

12. ธนาคารทหารไทยธนชาต. (2024). *ความมั่นคงปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล*. เข้าถึงได้จาก ttb: https://www.ttbbank.com/th/sustainability/corporate-governance-and-business-ethics/cybersecurity-and-data-privacy
13. ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร. (2024). *นโยบายสำคัญ*. เข้าถึงได้จาก baac: https://www.baac.or.th/th/content-cg.php?content_group_sub=0009&id_cg=15
14. ธปท. (13 มิถุนายน 2567). *ธปท. ยกระดับมาตรการจัดการภัยทุจริตทางการเงิน*. เข้าถึงได้จาก ธปท.: https://www.bot.or.th/th/news-and-media/news/news-20240613.html
15. ธปท. (14 เมษายน 2565). เข้าถึงได้จาก https://www.bot.or.th/content/dam/bot/documents/th/research-and-publications/reports/payment-report/bi-monthly-report/Bi-monthly_report_Vol14-2022_April.pdf
16. ธปท. (18 พฤศจิกายน 2562). *ประกาศธนาคารแห่งประเทศไทย ที่ สนส.21/2566 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลนยีสารสนเทศของสถาบันการเงิน และแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก* . เข้าถึงได้จาก ธปท.: https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2562/ThaiPDF/25620272.pdf
17. ธปท. (2 ธันวาคม 2567). *(ร่าง) ประกาศธนาคารแห่งประเทศไทย เรื่อง การรักษาความมั่นคงปลอดภัยของการให้บริการและการชำระเงินบนอุปกรณ์เคลื่อนที่*. เข้าถึงได้จาก ธปท.: https://www.bot.or.th/content/dam/bot/documents/th/laws-and-rules/hearing/public-hearing-20241202.pdf
18. ธปท. (2024 มิถุนายน 2567). เข้าถึงได้จาก https://www.bot.or.th/content/dam/bot/documents/th/news-and-media/news/2024/news-th-20240613-attach1.pdf
19. ธปท. (22 สิงหาคม 2562). *แนวทางการเปิดเผยข้อมูลสถิติระบบเทคโนโลยีสารสนเทศขัดข้องที่กระทบต่อการให้บริการสำคัญของธนาคารพาณิชย์.* เข้าถึงได้จาก ธปท.: https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2562/ThaiPDF/25620181.pdf
20. ธปท. (24 กุมภาพันธ์ 2563). *การรายงานชุดข้อมูล (Data Set) ที่เกี่ยวข้องกับการบริหารจัดการด้านเทคโนโลยีสารสนเทศของธนาคารพาณิชย์* . เข้าถึงได้จาก ธปท.: https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2563/ThaiPDF/25630042.pdf

21. ธปท. (2562 กันยายน 2562). *แนวปฏิบัติการทดสอบระบบแบบ Intelligence-Iced (iPentest).* เข้าถึงได้จาก ธปท.: https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2562/ThaiPDF/25620192.pdf
22. ธปท. (2566 พฤศจิกายน 2566). *ประกาศธนาคารแห่งประเทศไทย ที่ สกช. 5/2566 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ.* เข้าถึงได้จาก ธปท.: https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2566/ThaiPDF/25660202.pdf
23. ธปท. (2566). เข้าถึงได้จาก https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2566/ThaiPDF/25660066.pdf
24. ธปท. (27 ธันวาคม 2562). *แนวนโยบายการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security).* เข้าถึงได้จาก ธปท.: https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2562/ThaiPDF/25620311.pdf
25. ธปท. (30 ธันวาคม 2564). *กรอบการประเมินความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Assessment Framework: CRAF).* เข้าถึงได้จาก ธปท.: https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2565/ThaiPDF/25650007.pdf
26. ธปท. (9 มีนาคม 2566). *ธปท. ออกมาตรการจัดการภัยทุจริตทางการเงิน*. เข้าถึงได้จาก ธปท.: https://www.bot.or.th/th/news-and-media/news/news-20230309.html
27. ธปท. (ม.ป.ป.). *รายงานข้อมูลสถิติระบบเทคโนโลยีสารสนเทศขัดข้องที่กระทบต่อการให้บริการสำคัญของธนาคารพาณิชย์*. เข้าถึงได้จาก ธปท.: https://www.bot.or.th/th/statistics/system-failure-disclosure.html
28. บมจ. ธนาคารกรุงไทย. (2564). เข้าถึงได้จาก https://krungthai.com/Download/aboutKTB/MediaFile_252WhistleBlowingPolicy.PDF
29. บมจ. ธนาคารกรุงไทย. (ม.ป.ป.). เข้าถึงได้จาก https://krungthai.com/th/sustainability/esg-policy/governance/cyber-security
30. ปปง. (9 May 2024). *ประชาสัมพันธ์*. เข้าถึงได้จาก amlo: https://amlo.go.th/index.php/th/news/detail/15643

31. ประชาชาติธุรกิจ. (5 เมษายน 2567). เข้าถึงได้จาก https://www.prachachat.net/ict/news-1538102#:~:text=%E2%80%9C%E0%B8%9A%E0%B8%B1%E0%B8%8D%E0%B8%8A%E0%B8%B5%E0%B8%A1%E0%B9%89%E0%B8%B2%E0%B9%80%E0%B8%94%E0%B8%B4%E0%B8%A1%E0%B9%83%E0%B8%AB%E0%B9%89%E0%B8%8A%E0%B8%B2%E0%B8%A7,%E0%B8%81%E0%B8%A3%E0%B8%93%E0%
32. พงศกร เส้งสุย, และ พินิจ ทิพย์มณี. (2566). ความรับผิดทางแพ่งของธนาคารพาณิชย์และธนาคารแห่งประเทศไทย: ศึกษากรณีเงินฝากสูญหาย. *วารสารบัณฑิตศึกษา มหาวิทยาลัยธุรกิจบัณฑิตย์ ปีที่ 12 ฉบับที่ 1*, 178-191.
33. พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566. (9 มีนาคม 2566). เข้าถึงได้จาก https://www.mdes.go.th/law/detail/6664-%E0%B8%9E%E0%B8%A3%E0%B8%B0%E0%B8%A3%E0%B8%B2%E0%B8%8A%E0%B8%81%E0%B8%B3%E0%B8%AB%E0%B8%99%E0%B8%94%E0%B8%A1%E0%B8%B2%E0%B8%95%E0%B8%A3%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%9B%E0%B9%89%E0%B8%AD%E0%B8%87%E0%B8%81%E0%B8%B1
34. มติชนออนไลน์. (3 May 2567). *economy*. เข้าถึงได้จาก matichon: https://www.matichon.co.th/economy/news_4557615
35. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข. (ม.ป.ป.). *ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564*. เข้าถึงได้จาก ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข: https://ict.moph.go.th/th/extension/1011
36. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ. (ม.ป.ป.). *เกี่ยวกับ ThaiCERT*. เข้าถึงได้จาก ThaiCERT: https://www.thaicert.or.th/about-us/
37. ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร. (2566). *Annual Report 2023.* เข้าถึงได้จาก TBA: https://www.tba.or.th/wp-content/uploads/2024/04/TB-CERT-Annual-Report-2023.pdf
38. สตช. (24 ธันวาคม 2565). เข้าถึงได้จาก https://human.police.go.th/2022/12/18crime/
39. สตช. (29 กรกฎาคม 2567). เข้าถึงได้จาก https://www.facebook.com/story.php/?story_fbid=911325844361541&id=100064524017126&_rdr
40. สภาองค์กรของผู้บริโภค. (1 September 2024). เข้าถึงได้จาก https://www.tcc.or.th/financial-disaster/

41. สภาองค์กรของผู้บริโภค. (2024). เข้าถึงได้จาก https://www.tcc.or.th/slow-payment/
42. สภาองค์กรของผู้บริโภค. (26 November 2024). เข้าถึงได้จาก https://www.tcc.or.th/cybercrime_policy/
43. สภาองค์กรของผู้บริโภค. (29 สิงหาคม 2567). *เปิดภัยไซเบอร์ ในเวทีอาเซียน+3 อินโดฯ ข้อมูลบุคคลรั่ว ใช้เอไอสร้างข่าวปลอมป่วนเลือกตั้ง*. เข้าถึงได้จาก สภาองค์กรของผู้บริโภค : https://www.tcc.or.th/asean3-consumerprotection-cybercrime/?utm_source=chatgpt.com
44. สำนักงานคณะกรรมการ ก.ล.ต. (2567). *ภาคผนวก 2 : การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance) (แนบท้ายประกาศที่ สธ. 38/2565)*. เข้าถึงได้จาก สำนักงานคณะกรรมการ ก.ล.ต.: https://capital.sec.or.th/webapp/nrs/nrs_search.php?chk_frm=1&ref_id=9905&cat_id=1346
45. สำนักงานคณะกรรมการ ก.ล.ต. (2567). *ภาคผนวก 3 : การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security) (แนบท้ายประกาศ สธ. 33/2567)*. เข้าถึงได้จาก สำนักงานคณะกรรมการ ก.ล.ต.: https://capital.sec.or.th/webapp/nrs/nrs_search.php?chk_frm=1&ref_id=9905&cat_id=1346
46. สำนักงานคณะกรรมการ ก.ล.ต. (2567). *ภาคผนวก 4 : การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit) (แนบท้ายประกาศ สธ. 33/2567)*. เข้าถึงได้จาก สำนักงานคณะกรรมการ ก.ล.ต.: https://capital.sec.or.th/webapp/nrs/nrs_search.php?chk_frm=1&ref_id=9905&cat_id=1346
47. สำนักงานคณะกรรมการ ก.ล.ต. (28 กันยายน 2565). *ประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ สธ. 38/2565*. เข้าถึงได้จาก สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์: https://capital.sec.or.th/webapp/nrs/nrs_search.php?chk_frm=1&ref_id=9905&cat_id=1346
48. สำนักงานคณะกรรมการ ก.ล.ต. (ม.ป.ป.). *คำอธิบายประกอบการจัดทำแบบรายงานผล IT Audit [รอบปี 2567]*. เข้าถึงได้จาก สำนักงานคณะกรรมการ ก.ล.ต.: https://capital.sec.or.th/webapp/nrs/nrs_search.php?chk_frm=1&ref_id=9905&cat_id=1346
49. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ . (ม.ป.ป.). *สถิติภัยคุกคามทางไซเบอร์*. เข้าถึงได้จาก สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ : https://www.ncsa.or.th/service-statistics.html
50. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ . (ม.ป.ป.). *คำแนะนำ เรื่อง แนวทางปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทาง*

สารสนเทศ. เข้าถึงได้จาก สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ : https://drive.ncsa.or.th/s/GXEamHQin9JaWZB

51. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (ม.ป.ป.). *หน้าที่และอำนาจของสำนักงานฯ*. เข้าถึงได้จาก สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ: https://www.ncsa.or.th/functions-and-powers-of-the-office.html
52. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ . (27 กรกฎาคม 2566). *“กฎหมาย DPS” มีแล้วใครได้ประโยชน์ เจาะอินไซต์ที่ ผู้ใช้บริการแพลตฟอร์มดิจิทัล ต้องอ่าน!* เข้าถึงได้จาก Knowledge Sharing: https://www.etda.or.th/th/Useful-Resource/dps_inside.aspx
53. สำนักงานส่งเสริมเศรษฐกิจดิจิทัล. (18 ธันวาคม 2566). *ประกาศสำนักงานส่งเสริมเศรษฐกิจดิจิทัล เรื่อง หลักเกณฑ์ในการขึ้นทะเบียนผู้ประกอบการในอุตสาหกรรมดิจิทัล เพื่อสนับสนุนการประยุกต์ใช้เทคโนโลยีดิจิทัลในภาคธุรกิจอุตสาหกรรม ประจำปี พ.ศ. 2567*. เข้าถึงได้จาก สำนักงานส่งเสริมเศรษฐกิจดิจิทัล: https://www.depa.or.th/storage/app/media/uploaded-files/Digital%20Provider%2067.pdf
54. องค์การรักษาความปลอดภัยฝ่ายพลเรือน สำนักข่าวกรองแห่งชาติ. (12 July 2024). *อินโดนีเซียเร่งคุมเข้มความปลอดภัยทางไซเบอร์หลังถูกแรนซัมแวร์โจมตี*. เข้าถึงได้จาก องค์การรักษาความปลอดภัยฝ่ายพลเรือน สำนักข่าวกรองแห่งชาติ: https://www.secnia.go.th/2024/07/อินโดนีเซียเร่งคุมเข้ม
55. ACCC. (n.d.). เข้าถึงได้จาก https://www.scamwatch.gov.au/
56. AFCA. (2018). เข้าถึงได้จาก https://www.afca.org.au/what-to-expect/the-process-we-follow
57. Alexander Stronell. (2020). เข้าถึงได้จาก https://www.iiss.org/ar-BH/online-analysis/online-analysis/2020/09/csfc-brazils-cyber-security-strategy/
58. American Bankers Association . (2020, February 27). *Money Mule Scams*. Retrieved from American Bankers Association : https://www.aba.com/news-research/analysis-guides/money-mule-scams
59. Anti-Cybercrime Group. (2023). เข้าถึงได้จาก Anti-Cybercrime Group: https://acg.pnp.gov.ph/?fbclid=IwY2xjawHbDDZleHRuA2FlbQIxMAABHakKBLXryyxSqqLfoAlH4BuZKuu2BmtbD3yAbNnuBNgvaB9PZte1UdpavA_aem_yRuPwuBAKZ0-JT3yZNpd4w
60. Anti-Fake News Center Thailand . (14 พฤศจิกายน 2022). *wi-fi-สาธารณะ-ใช้อย่างไรให้ปลอดภัย*. เข้าถึงได้จาก ศูนย์ต่อต้านข่าวปลอม ประเทศไทย : https://www.antifakenewscenter.com/คลังความรู้/wi-fi-สาธารณะ-ใช้อย่างไรให้ปลอดภัย/

61. Asia Pacific Solidarity Network. (17 November 2023). *BSSN records 361 million cyber attacks in Indonesia.* เข้าถึงได้จาก Asia Pacific Solidarity Network: https://www.asia-pacific-solidarity.net/index.php/news/2023-11-17/bssn-records-361-million-cyber-attacks-indonesia.html?utm_source=chatgpt.com
62. Attorney-General's Chambers. (2020). *Computer Misuse Act (Cap. 50A)*. เรียกใช้เมื่อ December 2024 จาก https://sso.agc.gov.sg/Act/CMA1993
63. AWS. (ม.ป.ป.). *การยืนยันตัวตนโดยใช้หลายปัจจัย (MFA) คืออะไร*. เข้าถึงได้จาก AWS: https://aws.amazon.com/th/what-is/mfa/#:~:text=%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A2%E0%B8%B7%E0%B8%99%E0%B8%A2%E0%B8%B1%E0%B8%99%E0%B8%95%E0%B8%B1%E0%B8%A7%E0%B8%95%E0%B8%99%E0%B9%82%E0%B8%94%E0%B8%A2%E0%B9%83%E0%B8%8A%E0%B9%89%E0%B8%AB%E0%B8%A5%E0%B8%B2%
64. Banco Central do Brasil. (2018). เข้าถึงได้จาก https://www.bcb.gov.br/ingles/norms/resolution%204658.pdf
65. Banco Central Do Brazil. (2021). เข้าถึงได้จาก bcb: https://www.bcb.gov.br/content/about/legislation_norms_docs/BCB_Resolution_No_85_2021.pdf
66. Bangko Sentral ng Pilipinas. (31 October 2018). เข้าถึงได้จาก morb.bsp.gov.ph: https://morb.bsp.gov.ph/appendix-77/
67. Bank of Thailand. (31 july 2024). *statistics*. เข้าถึงได้จาก bot: https://app.bot.or.th/BTWS_STAT/statistics/BOTWEBSTAT.aspx?reportID=949&language=TH
68. Cervantes Mikee Filane. (2022). เข้าถึงได้จาก https://www.pna.gov.ph/articles/1173364
69. CFPB. (n.d.). เข้าถึงได้จาก https://www.consumerfinance.gov/
70. Chambers and Partners. (2024). เข้าถึงได้จาก https://practiceguides.chambers.com/practice-guides/cybersecurity-2024/singapore
71. Comply Advantage. (2024). เข้าถึงได้จาก https://complyadvantage.com/insights/australias-new-scam-code-to-make-banks-telcos-and-social-media-responsible-for-fraud-safety/
72. comply advantage. (27 April 2023). *Insights*. เข้าถึงได้จาก complyadvantage: https://complyadvantage.com/insights/singapore-proposes-tougher-laws-to-crack-down-on-money-mules/

73. CPA Canada. (2019). เข้าถึงได้จาก https://www.cpacanada.ca/_site_cpa-app/news/canada/2019-12-06-credit-card-fraud
74. DataBleach. (n.d.). เข้าถึงได้จาก https://data-breach.com/#:~:text=If%20you%20suffered%20financial%20losses,be%20reimbursed%20this%20lost%20money.
75. DFS. (n.d.). *Cybersecurity Resource Center*. Retrieved from Department of Financial Services: https://www.dfs.ny.gov/industry_guidance/cybersecurity
76. Digital Watch newsletters. (February 2024). *Philippines' National Cybersecurity Plan (NCSP) 2023-2028* . เข้าถึงได้จาก Digital Watch newsletters: https://dig.watch/resource/philippines-national-cybersecurity-plan-ncsp-2023-2028?
77. Entreprendre Service Public. (2023). เข้าถึงได้จาก https://entreprendre.service-public.fr/actualites/A16531?lang=en
78. ETDA. (12 มิถุนายน 2561). *Knowledge Sharing*. เข้าถึงได้จาก ETDA: https://www.etda.or.th/th/Useful-Resource/knowledge-sharing/articles/ความมนคงปลอดภย/การหลอกลวงทางอนเทอรเนต-(Scam).aspx
79. FATF. (2023). เข้าถึงได้จาก FATF: https://www.fatf-gafi.org/en/publications/Mutualevaluations/Brazil-mer-2023.html
80. FDIC. (2018). เข้าถึงได้จาก https://www.fdic.gov/consumers/consumer/news/october2018.html
81. Federal Register of Legislation. (1995). เรียกใช้เมื่อ December 2024 จาก Criminal Code Act 1995.: https://www.legislation.gov.au/Details/C2023C00274
82. FEDERAL TRADE COMMISSION. (n.d.). *Report to help fight fraud!* Retrieved from FEDERAL TRADE COMMISSION: https://reportfraud.ftc.gov
83. FFIEC. (ม.ป.ป.). *Cybersecurity and Resilience Against Cyber Attacks*. เข้าถึงได้จาก Federal Financial Institutions Examination Council: https://www.ffiec.gov/press/PDF/FFIECCyberSecurityBrochure.pdf
84. FFIEC. (n.d.). *About the FFIEC*. Retrieved from The Federal Financial Institutions Examination Council (FFIEC): https://www.ffiec.gov/about.htm
85. FFIEC. (n.d.). *CAT Sunset Statement*. Retrieved from Federal Financial Institutions Examination Council: https://www.ffiec.gov/press/pdf/CAT_Sunset_Statement_FFIEC_Letterhead.pdf

86. FRB. (n.d.). เข้าถึงได้จาก https://www.federalreserve.gov/boarddocs/caletters/2008/0807/08-07_attachment.pdf
87. FSF. (2021). เข้าถึงได้จาก https://www.bsp.gov.ph/Media_And_Research/Banking%20Advisories/FSF-Consumer_Protection_Guidelines.pdf
88. FTC. (n.d.). เข้าถึงได้จาก https://reportfraud.ftc.gov/
89. Gatekeeper. (n.d.). *FFIEC IT Examination Handbook*. Retrieved from Gatekeeper: https://www.gatekeeperhq.com/glossary/ffiec-it-examination-handbook
90. GBG and The Asian Banker. (2020).
91. GDPR. (n.d.). เข้าถึงได้จาก https://gdpr-info.eu/
92. Government of Canada. (2024). เข้าถึงได้จาก https://www.canada.ca/en/financial-consumer-agency.html
93. Government of India. (2000). *The Information Technology Act, 2000*. เรียกใช้เมื่อ December 2024 จาก Ministry of Electronics and Information Technology.: https://www.indiacode.nic.in/handle/123456789/1999
94. ICO. (n.d.). เข้าถึงได้จาก https://ico.org.uk/for-the-public/data-protection-and-journalism/taking-your-case-to-court-and-claiming-compensation/#:~:text=The%20GDPR%20gives%20you%20a,e.g.%20you%20have%20suffered%20distress).
95. imperva. (ม.ป.ป.). *Phishing attacks*. เข้าถึงได้จาก imperva: https://www.imperva.com/learn/application-security/phishing-attack-scam/#:~:text=Phishing%20is%20a%20type%20of,instant%20message%2C%20or%20text%20message
96. International Telecommunication Union ITU. (1 1 2020). *Cybersecurity*. เรียกใช้เมื่อ 2020 จาก ITU: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
97. International Telecommunication Union. (2024). *Global Cybersecurity Index 2024 5th Edition.* Retrieved from International Telecommunication Union: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf
98. iT24Hrs. (12 ตุลาคม 2567). *Vishing คืออะไร? คำศัพท์ IT ที่น่ารู้* . เข้าถึงได้จาก iT24Hrs: *https://it24hrs.com/2024/vishing-online-scams/?utm_source=chatgpt.com*

99. Joyce Lee. (10 September 2024). Reuters. เข้าถึงได้จาก https://www.reuters.com/world/asia-pacific/south-korea-summit-target-blueprint-using-ai-military-2024-09-09/?taid=66de64c107f6440001c93a70&utm_campaign=trueAnthem:+Trending+Content&utm_medium=trueAnthem&utm_source=twitter
100. Kartina Sury. (2021). เข้าถึงได้จาก https://techforgoodinstitute.org/blog/expert-opinion/indonesias-cyber-resilience-at-the-epicenter-of-asean-digital-economy-growth/
101. Legislation.gov.uk. (2006). Fraud Act 2006. เรียกใช้เมื่อ December 2024 จาก https://www.legislation.gov.uk/ukpga/2006/35
102. Mastercard Canada. (2024). เข้าถึงได้จาก https://www.mastercard.ca/en-ca/vision/who-we-are/terms-of-use/zero-liability-terms-conditions.html
103. MGR Online. (24 April 2024). *ข่าวอาชญากรรม* . เข้าถึงได้จาก mgronline: https://mgronline.com/crime/detail/9670000035517#google_vignette
104. Microsoft. (2024). *What is phishing?* เรียกใช้เมื่อ December 2024 จาก Microsoft: https://www.microsoft.com/th-th/security/business/security-101/what-is-phishing?utm_source=chatgpt.com
105. Monetary Authority of Singapore. (2023). เข้าถึงได้จาก https://www.mas.gov.sg/news/media-releases/2023/mas-and-imda-consult-on-shared-responsibility-framework-for-phishing-scams
106. Monetary Authority of Singapore. (2024). เข้าถึงได้จาก https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidelines/pso/guidelines-on-shared-responsibility-framework/guidelines-on-shared-responsibility-framework.pdf
107. Monetary Authority of Singapore. (January 2021). *regulation.* เข้าถึงได้จาก mas: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf
108. MRG ONLINE. (3 สิงหาคม 2567). *“โทรจันธนาคารมือถือ” ภัย Mobile Banking อันตรายสูงสุด! (Cyber Weekend)*. เข้าถึงได้จาก MRG ONLINE: https://mgronline.com/cyberbiz/detail/9670000070194

109. Natasha Teja. (2023). เข้าถึงได้จาก https://fticybersecurity.com/wp-content/uploads/2023/01/Indonesias-OJK-issues-new-cybersecurity-rules-after-attacks-escalate-Global-Banking-Regulation-Review.pdf
110. NT cyfence. (30 กรกฎาคม 2019). *รู้ทัน!! คนโกงในโลกออนไลน์ และ วิธีป้องกันไม่ให้เป็นเหยื่อ*. เข้าถึงได้จาก บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน): https://www.cyfence.com/article/how-to-protect-yourself-from-online-fraud/?utm_source=chatgpt.com
111. OJK. (April 2024). เข้าถึงได้จาก https://ojk.go.id/en/berita-dan-kegiatan/info-terkini/Documents/Pages/Cybersecurity-Guidelines-for-Financial-Sector-Technology-Innovation-FSTI-Providers/2024.07.26%20Cybersecurity%20Guidelines%20for%20Financial%20Sector%20Technology%20Innovation%20Provide
112. OpenGov Asia. (27 October 2017). *Department of Information and Communications Technology Philippines releases National Cybersecurity Plan 2022*. เข้าถึงได้จาก OpenGov Asia: https://opengovasia.com/2017/10/27/department-of-information-and-communications-technology-philippines-releases-national-cybersecurity-plan-2022/
113. PagBrazil. (2024). เข้าถึงได้จาก https://www.pagbrasil.com/blog/news/file-chargeback-brazil/
114. Philippine government. (8 February 2024). *PBBM approves National Cybersecurity Plan to fortify PH against various threats*. เข้าถึงได้จาก Philippine government: https://pco.gov.ph/news_releases/pbbm-approves-national-cybersecurity-plan-to-fortify-ph-against-various-threats/?utm_source=chatgpt.com&__cf_chl_tk=d2dA4BJbz5AviSWxpks.F7vmEQ1lEmwrDwXaLcE.4Lg-1735274667-1.0.1.1-cXi60KmWKbPo6iDfKtbX0uMklOk5K7KN6k6trZqoB.8
115. Pimlapat Phansuathong. (25 October 2023). *ฟิชชิง (Phishing) คืออะไร รู้เท่าทันภัย 9 ประเภทบนโลกออนไลน์*. เข้าถึงได้จาก Primal: https://www.primal.co.th/th/seo/what-is-phishing/?utm_source=chatgpt.com
116. proofpoint. (ม.ป.ป.). *What Is a Data Leak?* เข้าถึงได้จาก proofpoint: https://www.proofpoint.com/us/threat-reference/data-leak

117. Republic of the Philippines. (2012). *Official Gazette.* เรียกใช้เมื่อ December 2024 จาก Cybercrime Prevention Act of 2012: https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/
118. Secureframe. (2024, February 22). *A Guide to the NYDFS NYCRR 500 Cybersecurity Regulation + Compliance Checklist [2024]* . Retrieved from Secureframe: https://secureframe.com/blog/nydfs-nycrr-500
119. SkySoft. (2022, November 18). *วิธีการตรวจสอบ และอุดช่องโหว่ขั้นพื้นฐาน*. Retrieved from SkySoft: https://skysoft.co.th/blog/vulnerability-assessment/
120. Society, Ministry of Digital Economy and. (2017). *พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*. เข้าถึงได้จาก Ministry of Digital Economy and Society: https://www.mdes.go.th/uploads/files/2017/TH/ComputerCrimeAct_No2_BE_2560_Eng.pdf
121. The MATTER. (27 May 2024). *Brief*. เข้าถึงได้จาก thematter: https://thematter.co/brief/226537/226537
122. THE STANDARD. (2023, March 24). *'นิวยอร์ก' รั้งเบอร์ 1 เมืองศูนย์กลางการเงินโลก 5 ปีซ้อน 'แอลเอ' แซงหน้าเซี่ยงไฮ้ขึ้นอันดับ 6 ส่วน 'กรุงเทพฯ' ร่วงไปอยู่ที่ 71*. Retrieved from THE STANDARD: https://thestandard.co/new-york-number-1-world-financial-center/
123. The Straitstimes. (2024). เข้าถึงได้จาก https://www.straitstimes.com/singapore/at-a-glance-duties-of-telcos-and-banks-under-singapores-scam-liability-framework
124. Today Online. (2024). เข้าถึงได้จาก https://www.todayonline.com/singapore/banks-telcos-losses-regulations-anti-scam-consumers-2290181
125. Toki Kawase. (28 July 2024). *สถานะปัจจุบันของกฎหมายที่ควบคุม AI คืออะไร? การเปรียบเทียบและจุดสำคัญในการรับมือระหว่างญี่ปุ่นและสหภาพยุโรป*. เข้าถึงได้จาก Monolith Law: https://monolith.law/th/it/ai-law-regulation
126. Trend Micro. (ม.ป.ป.). *Ransomware*. เข้าถึงได้จาก https://www.trendmicro.com/vinfo/th/security/definition/ransomware.
127. U.S. Bank. (2024). เข้าถึงได้จาก https://www.usbank.com/credit-cards/benefits/personal-credit-card-benefits.html#:~:text=U.S.%20Bank%20provides%20Zero%20Fraud,conditions%20and%20limitations%20may%20apply.&text=You%20agree%20to%20be%20responsible,User%20makes%20on%20your%20account.

128. U.S. Department of Justice. (2021, December 3). *Blogs Photo Galleries Podcasts Press Releases Speeches Videos Archived News Para Notícias en Español PRESS RELEASE U.S. Law Enforcement Targets Fraud Facilitators, Doubling Last Year's Enforcement*. Retrieved from Office of Public Affairs U.S. Department of Justice: https://www.justice.gov/opa/pr/us-law-enforcement-targets-fraud-facilitators-doubling-last-year-s-enforcement
129. Uchenna Jerome Orji. (2019). Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria. *TILBURG LAW REVIEW*, 105-124.
130. United States Code. (2012). *Crimes and Criminal Procedure*. เรียกใช้เมื่อ December 2024 จาก https://www.govinfo.gov/content/pkg/USCODE-2011-title18/html/USCODE-2011-title18-partI-chap47-sec1030.htm
131. Visa. (2024). เข้าถึงได้จาก https://usa.visa.com/pay-with-visa/visa-chip-technology-consumers/zero-liability-policy.html#When_can_I_expect_to_get_a_refund_for_an_unauthorized_transaction_-726159271