



ภูมิทัศน์ภัยการเงินในประเทศไทย

No. 4

กันยายน 2568

ฐิติ ทศบวร

กฤษฎ์เลิศ สัมพันธรักษ์

เทคโนโลยีทางการเงินที่ก้าวหน้าอย่างรวดเร็วได้สร้างความสะดวกสบาย แต่ในขณะเดียวกันก็เปิดช่องให้ ‘ภัยการเงิน’ ทวีความรุนแรง และสร้างความเสียหายในวงกว้าง บทความนี้นำเสนอกรอบคิดเชิงเศรษฐศาสตร์เพื่อทำความเข้าใจภูมิทัศน์ของปัญหาภัยการเงิน อย่างรอบด้าน โดยวิเคราะห์ตั้งแต่ปัจจัยที่ทำให้คนตัดสินใจเป็นมิชฌาชีพและตกเป็นเหยื่อ บทบาทของเทคโนโลยีที่ทำให้การฉ้อโกง ทำได้ง่ายขึ้น ไปจนถึงมาตรการ การออกแบบนโยบายที่จะมาช่วยลดความเสียหายตลอดห่วงโซ่ภัยการเงิน ทั้งการป้องกันก่อนเกิดเหตุ และการติดตามหลังเกิดความเสียหาย และชี้ให้เห็นว่าหัวใจสำคัญของการแก้ปัญหาภัยการเงินนั้น คือการลด “ความไม่สมมาตรของ ข้อมูล” และการสร้างแรงจูงใจที่เหมาะสม เพื่อให้ทุกภาคส่วนที่เกี่ยวข้อง ตั้งแต่ผู้เสียหาย แพลตฟอร์ม สถาบันการเงิน และผู้บังคับใช้ กฎหมาย ร่วมมือกันแลกเปลี่ยนข้อมูล เพื่อสร้างสมดุลระหว่างความปลอดภัยและประโยชน์จากนวัตกรรมทางการเงินในระบบ เศรษฐกิจ

NOTE

ผลการศึกษาบางส่วนที่อ้างถึงในรายงานนี้มาจากการวิเคราะห์ข้อมูลอาชญากรรมทางเทคโนโลยีร่วมกันระหว่างกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) และ ธนาคารแห่งประเทศไทย ความเห็นและข้อสรุปในรายงานนี้เป็นของคณะผู้วิจัย และไม่ถือเป็นความเห็นของหน่วยงานที่คณะผู้วิจัยสังกัดและหน่วยงานอื่น ๆ สำหรับรายละเอียดการวิเคราะห์ ดูได้ที่ Amarase et al. (forthcoming)

1. บทนำ

1.1. ภัยการเงินหมายถึงอะไร

ศัพท์บัญญัติที่ใกล้เคียงที่สุดของคำว่า “ภัยการเงิน” น่าจะเป็นคำว่า “ฉ้อโกง” ซึ่งราชบัณฑิตยสถานให้ความหมายไว้ว่าเป็นการหลอกลวงผู้อื่นโดยทุจริต เพื่อให้ได้ทรัพย์สินจากผู้ถูกหลอกลวงหรือจากบุคคลที่สาม ซึ่งเป็นความผิดอาญาที่มีมาตั้งแต่มีการประกาศใช้กฎหมายลักษณะอาญาฉบับแรกขึ้นใน ร.ศ. 127 (ปี ค.ศ. 1908)

“ภัยการเงิน” หรือ การหลอกลวงเพื่อให้ได้มาซึ่งทรัพย์สินของบุคคลอื่น เป็นสิ่งที่อยู่คู่กับมนุษย์มาโดยตลอด ในหนังสือสุภาษิตในคัมภีร์ฮีบรู ซึ่งเขียนขึ้นเมื่อกว่า 1000 ปีก่อนคริสตกาล มีการห้ามไม่ให้ใช้ตาซึ่งที่ “ขี้โกง” เพราะจะเป็นที่ไม่พอพระทัยของพระเจ้า ในกรีกโบราณเมื่อ 300 ปีก่อนคริสตกาล มีการบันทึกการพยายามจมน้ำเรือบรรทุกสินค้าเพื่อฉ้อโกงบริษัทประกัน หรือตั้งแต่ช่วงกลางศตวรรษที่ 15 ในยุโรป ก็มีนักต้มตุ๋นเดินทางไกลให้คนเล่นเกมทายบอลได้ถ้วย¹ มิจฌาชีพปลอมตัวเป็นเจ้าของหน้าที่ตำรวจเพื่อที่จะริดเอาทรัพย์สินจากเหยื่อ มาจนสมัยที่โทรศัพท์เริ่มเป็นที่แพร่หลายในช่วงหลังของศตวรรษที่ 20 มิจฌาชีพก็หันไปใช้โทรศัพท์เพื่อหลอกเหยื่อให้ซื้อสินค้าหรือลงทุน

จะเห็นได้ว่าไม่ว่าจะเป็นยุคสมัยใด ภัยการเงินล้วนเกิดจากการที่เหยื่อรู้ไม่เท่าทันกลโกงของมิจฌาชีพ ความรู้ที่ไม่เท่าทันนี้ในทางเศรษฐศาสตร์เรียกว่า ความไม่สมมาตรของข้อมูล (information asymmetry) ที่ฝ่ายหนึ่ง (มิจฌาชีพ) มีข้อมูลมากกว่าอีกฝ่ายหนึ่ง (เหยื่อ) เพียงแต่ช่องทางที่มิจฌาชีพใช้ในการหลอกลวงเหยื่อได้เปลี่ยนแปลงตามเทคโนโลยีที่พัฒนาไปเรื่อย ๆ ตามกาลเวลา

1.2 ประเภทของภัยการเงิน

ภัยการเงินมีความหมายที่กว้างและสามารถแบ่งออกเป็นประเภทต่างๆ ได้ในหลายมิติ

มิติที่หนึ่ง แบ่งตามความสัมพันธ์ระหว่างมิจฌาชีพกับเหยื่อ ได้แก่

1. การฉ้อโกงที่เหยื่อและมิจฌาชีพรู้จักกัน เคยพบตัวตนหรือมีความสัมพันธ์กันในชีวิตจริง เช่น กรณีที่คนรู้จักหลอกให้ร่วมลงทุน หรือ
2. การฉ้อโกงที่เหยื่อไม่รู้จักตัวตนจริงของมิจฌาชีพ เช่น การหลอกลวงเหยื่อผ่านโทรศัพท์หรือในโลกออนไลน์

มิติที่สอง แบ่งตามประเภทการให้ความยินยอมของเจ้าของเงิน ซึ่งได้แก่

1. การฉ้อโกงที่เจ้าของเงินไม่ให้ความยินยอม (unauthorized) แต่มีจฉฉฉสามารถเข้าถึงบัญชีและทำธุรกรรมแทนเจ้าของบัญชีได้ หรือ
2. การฉ้อโกงที่เจ้าของเงินให้ความยินยอม (authorized) เช่น เจ้าของบัญชีเงินฝากยืนยันตัวตน เป็นผู้กรอกรายละเอียดของบัญชีปลายทาง และอนุมัติการโอนเงินด้วยตนเอง

มิติที่สาม แบ่งตามผู้เริ่มต้นทำธุรกรรม ได้แก่

1. การฉ้อโกงที่ผู้รับเงิน เป็นผู้เริ่มต้นทำธุรกรรม (pull transaction) เช่น ร้านค้าที่เป็นมีจฉฉฉตัดเงินชำระสินค้าจากบัญชีธนาคารหรือบัตรเครดิตของเจ้าของเงิน หรือ
2. การฉ้อโกงที่ผู้ส่งเงินเป็นผู้เริ่มต้นทำธุรกรรม (push transaction) เช่น การที่เจ้าของเงินโอนเงินจากบัญชีของตนเพื่อชำระค่าสินค้าและบริการให้แก่ร้านค้าที่เป็นมีจฉฉฉ

มิติที่สี่ แบ่งตามความเร็วของธุรกรรมทางการเงิน ได้แก่

1. การฉ้อโกงที่ธุรกรรมการชำระเงินผ่านระบบ fast payment ซึ่งเกิดขึ้นและสิ้นสุด (finality) ทันทีหรือรวดเร็ว เมื่อโอนแล้วไม่สามารถยกเลิกธุรกรรมหรือดึงเงินกลับมาได้ เช่น การโอนเงินผ่านช่องทางดิจิทัล
2. การฉ้อโกงที่ธุรกรรมการชำระเงินใช้เวลานานกว่าจะสิ้นสุด เช่น การชำระเงินด้วยเช็ค

บทความนี้มุ่งศึกษาเฉพาะภัยการเงินที่เกิดจากการหลอกลวงเหยื่อออนไลน์โดยใช้ธุรกรรม authorized push payment (APP) ผ่านระบบ fast payment เนื่องจากเป็นภัยการเงินในรูปแบบที่เหยื่อโอนเงินผ่านช่องทางดิจิทัลออกจากบัญชีของตนไปให้มีจฉฉฉที่ไม่ได้รู้จักกันในชีวิตจริงเป็นภัยการเงินที่เป็นปัญหามากที่สุดในปัจจุบัน ดังที่เห็นได้จากการสำรวจที่ครอบคลุมกลุ่มตัวอย่างเกือบ 60,000 คนของ GASA (Global Anti-Scam Alliance) ที่ประเมินว่า ในปี 2024 มีความเสียหายจากการหลอกลวงออนไลน์ถึง 1 ล้านล้านดอลลาร์สหรัฐ ซึ่งมีขนาดพอ ๆ กับ GDP ของประเทศสวิตเซอร์แลนด์เลยทีเดียว

สำหรับประเทศไทยเอง มีปัจจัยพิเศษที่ทำให้การหลอกลวงออนไลน์สร้างผลกระทบในวงกว้าง เนื่องจากเศรษฐกิจไทยมีอัตราการเข้าถึงระบบ fast payment สูง ในขณะที่ประชากรจำนวนมากยังขาดภูมิคุ้มกันทางการเงิน เห็นได้จากตัวเลขอัตราการเข้าถึงอินเทอร์เน็ตที่สูงกว่า 90% หรืออัตราการใช้ระบบ fast payment ที่สูงเป็นอันดับต้น ๆ ของโลก แต่จากสถิติของกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) พบว่า นับตั้งแต่เดือนมีนาคม 2022 ที่มีการเก็บสถิติ มีผู้แจ้งความคดีออนไลน์แล้วถึง 1 ล้านคดี รวมมูลค่าความเสียหายกว่า 9.8 หมื่นล้านบาท เฉลี่ยความเสียหาย 77 ล้านบาทต่อวัน สะท้อนให้เห็นถึงขนาดของปัญหา และความเสี่ยงที่เพิ่มขึ้นต่อประชาชนทุกคน

2. กรอบความคิดทางเศรษฐศาสตร์ว่าด้วยภัยการเงิน

บทความในส่วนจะนำเสนอกรอบแนวคิดทางเศรษฐศาสตร์ที่ใช้อธิบายว่าการฉ้อโกงเกิดขึ้นได้จากปัจจัยอะไรบ้าง ทำไมเทคโนโลยีที่ก้าวหน้ามากขึ้นจึงทำให้การฉ้อโกงทางการเงินทวีความรุนแรงมากยิ่งขึ้นเมื่อเทียบกับการฉ้อโกงประเภทอื่นๆ และทำไมการป้องกันและปราบปรามภัยการเงินจึงเกิดขึ้นได้ยากหากไม่มีการแทรกแซงจากภาครัฐ

2.1. เศรษฐศาสตร์ว่าด้วยการฉ้อโกง

ในทางเศรษฐศาสตร์นั้น ภัยการเงินถือเป็นการฉ้อโกงประเภทหนึ่ง ซึ่งการฉ้อโกงสามารถอธิบายได้ด้วยกรอบความคิดทางเศรษฐศาสตร์ที่ประกอบด้วย (1) ปัจจัยที่ทำให้คนตัดสินใจเป็นมีจฉฉฉ (2) ปัจจัยที่ทำให้คนตกเป็นเหยื่อ และ (3) ระบบเศรษฐกิจที่เอื้อให้การฉ้อโกงเกิดขึ้นได้

2.1.1. มิจลาชีพ

มนุษย์ทุกคนไม่ได้เป็นมิจลาชีพโดยกำเนิด แต่การเป็นมิจลาชีพที่ก่ออาชญากรรมต่าง ๆ ซึ่งรวมถึงการฉ้อโกงนั้น เป็นกิจกรรมทางเศรษฐศาสตร์อย่างหนึ่ง ที่ผ่านการตัดสินใจโดยคำนึงถึงผลตอบแทนและต้นทุน เช่นเดียวกับการซื้อของ การลงทุน หรือการตัดสินใจเลือกอาชีพอื่น ๆ นั้นเอง ซึ่งงานชิ้นสำคัญของ Ehrlich (1996) ได้นำเสนอแบบจำลองที่ payoff ของการก่ออาชญากรรมว่าจะขึ้นอยู่กับ

ผลตอบแทนที่คาดว่าจะได้รับจากการเป็นมิจลาชีพ - ต้นทุนที่เกิดขึ้นจากการก่อเหตุ - โอกาสที่เสียไปจากการไม่ทำงานสุจริต
(โอกาสในการถูกจับกุม x โทษที่จะได้รับ)

ผลตอบแทนที่คาดว่าจะได้รับจากการเป็นมิจลาชีพ

ผลตอบแทนจากการเป็นมิจลาชีพขึ้นอยู่กับปัจจัยหลาย ๆ อย่างรวมกัน ทั้งจำนวนเหยื่อที่หลอก ปริมาณเงินที่คาดว่าจะหลอกได้จากเหยื่อ และโอกาสที่จะหลุดรอดระบบป้องกันต่าง ๆ ที่ได้กล่าวมาข้างต้น จนนำเงินออกไปนอกกระบวนการได้

ในช่วง 10 ปีที่ผ่านมา ความนิยมของการใช้บริการธนาคารผ่านโทรศัพท์มือถือ (mobile banking) เพิ่มขึ้นอย่างมาก โดยเฉพาะอย่างยิ่งในช่วงการแพร่ระบาดของโควิด 19 ทำให้มีความพยายามลดการสัมผัสเงินสด หรือมาตรการช่วยเหลือของรัฐที่กระตุ้นให้คนหันมาใช้ e-Payment มากขึ้น Tosborvorn et al. (2023) ประเมินว่าระหว่างเดือน ก.ค. 2020 ถึงเดือน ธ.ค. 2021 มีผู้ใช้บริการ e-Payment เพิ่มขึ้นถึงเกือบ 5 ล้านคน ความนิยม e-Payment ที่เพิ่มขึ้นนี้ ส่งผลให้จำนวนผู้ที่อาจตกเป็นเหยื่อเพิ่มขึ้นอย่างรวดเร็ว นอกจากนี้ จากธรรมชาติของการหลอกลวงที่มีจลาชีพสามารถพยายามหลอกเหยื่อได้หลายรายพร้อม ๆ กัน มีส่วนทำให้ผลตอบแทนที่คาดว่าจะได้จากการก่อเหตุสูงขึ้น

การลดการใช้ e-Payment ไม่ใช่แนวทางการลดภัยการเงินที่เหมาะสม เนื่องจาก e-Payment มีประโยชน์หลาย ๆ อย่างต่อพัฒนาการทางการเงิน ความสะดวกสบาย การเข้าถึงบริการทางการเงินของครัวเรือนและธุรกิจ ดังนั้น การแก้ไขจึงต้องมุ่งเน้นไปที่การทำให้คนในสังคมที่มีภูมิคุ้มกัน ตระหนัก และระมัดระวังภัยการเงิน มีอัตราส่วนมากขึ้น ผ่านการให้ความรู้ทางการเงิน หรือการมีมาตรการต่าง ๆ เพื่อเพิ่มประสิทธิภาพส่วนต่าง ๆ ที่ได้กล่าวไปข้างต้น ตั้งแต่การตรวจจับ แจ้งเตือน ของแพลตฟอร์มและผู้ให้บริการทางการเงิน การติดตามเส้นทางการเงินและป้องกันไม่ให้เงินออกนอกกระบวนการ

ต้นทุนที่เกิดขึ้นจากการก่อเหตุ

การก่อเหตุผ่านช่องทางออนไลน์มีต้นทุนที่น้อยกว่ามากเมื่อเปรียบเทียบกับ การก่อเหตุกับทรัพย์สินแบบอื่น เช่น การฉกชิงวิ่งราว การปล้น ทั้งจากต้นทุนทางตรง (เช่น ค่าใช้จ่ายในการซื้ออาวุธ ยานพาหนะ) และความเสี่ยงที่อาจเกิดขึ้นระหว่างก่อเหตุ (เช่น การถูกเหยื่อหรือเจ้าหน้าที่รักษาความปลอดภัยทำร้ายร่างกาย) ที่ต่ำกว่า

ในขณะเดียวกัน มิจลาชีพก็มีค่าใช้จ่ายอย่างอื่นเข้ามาแทนที่ เช่น ค่าใช้จ่ายในการซื้อบัญชีม้า ค่าใช้จ่ายเกี่ยวกับอุปกรณ์สื่อสาร การทำหลักฐานหรือสภาพแวดล้อมเพื่อมาหลอกเหยื่อ ค่าใช้จ่ายในการเปิดบริษัทเพื่อมาทำหน้าที่เป็นบัญชีม้าแบบนิติบุคคล สิ่งเหล่านี้ หากนโยบายสามารถทำให้มีต้นทุนที่สูงขึ้นได้ ก็เป็นปัจจัยลบที่ทำให้การก่ออาชญากรรมออนไลน์น่าดึงดูดน้อยลง เนื่องจากเป็นต้นทุนในการดำเนินการของมิจลาชีพนั่นเอง

โอกาสที่เสียไปจากการไม่ทำงานอื่น

การที่คนคนหนึ่งตัดสินใจที่จะเป็นมิจลาชีพ หมายความว่าคนคนนั้นจะเสียโอกาสที่จะได้ทำงานอื่น (หรือมีโอกาที่จะเสียรายได้เหล่านั้นหากถูกจับได้) ถ้าเราเทียบกันระหว่างคนที่มีงานประจำ มีรายได้สูง กับคนที่รายได้ต่ำหรือตกงาน คนที่มีรายได้สูงย่อมมี “ต้นทุน” ในการผันตัวมาเป็นมิจลาชีพที่สูงกว่า เนื่องจากจะต้องยอมเสียรายได้ประจําวันไปด้วย สถิติชี้ให้เห็นว่า อาชญากรรมต่อทรัพย์สินจะเพิ่มขึ้นเมื่อเศรษฐกิจไม่ดี และมิจลาชีพโดยทั่วไปมักเป็นผู้ไม่มีงานทำ (Piehl, 1998, Fagan & Freeman, 1999) ผ่านกลไกของค่าเสียโอกาส (opportunity cost) ดังกล่าว ดังนั้น การแก้ปัญหาเศรษฐกิจ ซึ่งรวมไปถึงการส่งเสริมการพัฒนาทักษะที่จำเป็นต่อการประกอบอาชีพสุจริต จึงเป็นการแก้ปัญหาที่ต้นเหตุที่สำคัญ

โทษที่คาดว่าจะได้รับ

โทษที่คาดว่าจะได้รับขึ้นอยู่กับโอกาสในการถูกจับกุมมาดำเนินคดี (certainty of punishment) กับโทษที่จะได้รับเมื่อถูกจับกุม (severity of punishment) ซึ่งเมื่อเปรียบเทียบระหว่างสองปัจจัยนี้แล้ว การศึกษาในอดีตหลายชิ้นพบว่า การเพิ่มโอกาสที่จะถูกจับกุม ส่งผลให้จำนวนอาชญากรรมลดลงได้มากกว่าการเพิ่มโทษ (Paternoster, 1987, Grogger, 1991, Nagin, 2013) นอกจากนี้ Waldo & Chiricos (1972) พบว่า สิ่งที่มีผลต่อจำนวนอาชญากรรมคือ “การรับรู้” (perception) ของคนเกี่ยวกับโอกาสที่จะถูกจับกุม หรือโทษที่จะได้รับ

มาตรการต่าง ๆ ที่ส่งผลต่อปัจจัยเหล่านี้ สามารถทำให้คนเปลี่ยนใจในการเลือกหรือไม่เลือกที่จะเป็นมิจฉาชีพได้

2.1.2. เหยื่อ

มนุษย์ทุกคนไม่ได้มีภูมิคุ้มกันต่อการหลอกลวงมาตั้งแต่เกิด ซึ่งปัจจัยที่ทำให้คนบางคนมีหรือไม่มีภูมิคุ้มกันภัย และตกเป็นเหยื่อของมิจฉาชีพสามารถแบ่งได้เป็นสองประเภทใหญ่ ๆ ได้แก่

- **ปัจจัยเชิงบุคคล (dispositional factors)** คือ ปัจจัยที่เฉพาะเจาะจงกับบุคคลใดบุคคลหนึ่ง ส่วนใหญ่มักเป็นปัจจัยที่ติดตัวบุคคลมาตั้งแต่เกิด หรือเป็นสิ่งที่เปลี่ยนแปลงได้ยาก และอาจส่งผลต่อการตัดสินใจ หรือพฤติกรรมในภาพรวม ปัจจัยเชิงบุคคล ยังสามารถแบ่งย่อยออกได้อีกเป็นสองประเภท คือ
 - **ปัจจัยที่สังเกตได้จากภายนอก** โดยทั่วไปหมายถึง ข้อมูลส่วนบุคคล (demographic variables) ต่าง ๆ เช่น อายุ เพศ ระดับการศึกษา อาชีพ เชื้อชาติ
 - **ปัจจัยที่สังเกตจากภายนอกได้ยาก** หมายถึง ลักษณะนิสัยส่วนบุคคล (psychological variables) เช่น ความเสี่ยงที่ยอมรับได้ (risk aversion) ความเชื่อใจผู้อื่น หรือความสามารถในการคิดวิเคราะห์และการตัดสินใจ (cognitive ability)

ในภาพรวม ปัจจุบันค่อนข้างยอมรับกันว่าไม่มีปัจจัยเชิงบุคคลหรือลักษณะของคนแบบใดแบบหนึ่งที่ทำให้คนคนนั้นมีโอกาสตกเป็นเหยื่อของการหลอกลวงออนไลน์ง่ายกว่าคนอื่น ไม่ว่าจะเป็นอายุ เพศ การศึกษา ฐานะทางการเงิน สถานภาพ การสมรส หรือแม้แต่ลักษณะนิสัยส่วนบุคคล (Whitty, 2020, Hanoch & Wood, 2021) และดูเหมือนว่าคนทุกประเภทต่างสามารถตกเป็นเหยื่อของการหลอกลวงออนไลน์ทั้งสิ้น

- **ปัจจัยเชิงสถานการณ์ (situational factors)** ซึ่งเปลี่ยนแปลงได้ในเวลาอันสั้นกว่า เช่น ความเหนื่อยล้า เพิ่งตกงานหรือได้รับข่าวร้าย การตกอยู่ในสถานที่ที่ไม่คุ้นเคย หรือสถานการณ์ที่ต้องตัดสินใจเร่งด่วน ซึ่งส่วนหนึ่ง ก็เป็นสถานการณ์ที่มีมิจฉาชีพสร้างขึ้น ซึ่งเมื่อเปรียบเทียบกับปัจจัยเชิงบุคคลแล้ว การศึกษาเกี่ยวกับปัจจัยเชิงสถานการณ์มีผลที่สอดคล้องกันมากกว่า

ความท้าทายในการศึกษาผู้เสียหาย

การศึกษาเกี่ยวกับปัจจัยเสี่ยงที่จะทำให้ตกเป็นเหยื่อของการหลอกลวงออนไลน์ ส่วนใหญ่เป็นการทำแบบสอบถามให้กลุ่มตัวอย่างตอบ โดยมีตัวแปรต้นเป็นลักษณะเชิงบุคคล หรือลักษณะอุปนิสัยที่สนใจ ส่วนตัวแปรตามนั้น คือประสบการณ์การถูกหลอกลวง ซึ่งอาจวิพากษ์กลุ่มตัวอย่างว่าเคยถูกหลอกหรือตกเป็นผู้เสียหายในช่วงเวลาที่ผ่านมาหรือไม่ แต่ด้วย underreporting bias ทำให้งานศึกษาลักษณะดังกล่าวมีข้อจำกัด เนื่องจากผู้ที่เคยโดนหลอกอาจปฏิเสธที่จะเปิดเผยว่าเคยโดนหลอก² เพื่อก้าวข้ามข้อจำกัดนี้ งานศึกษาบางชิ้นใช้วิธีการทดลองให้ผู้ตอบแบบสอบถามเจอการหลอกลวงที่ผู้วิจัยสร้างขึ้น (mock scam) เพื่อดูว่าผู้ตอบแบบสอบถามจะหลงเชื่อหรือไม่ ซึ่งงานศึกษาประเภทนี้ก็พบข้อจำกัดอีกประการหนึ่ง คือการที่ผู้ตอบแบบสอบถามอาจจะรู้ตัวว่ากำลังทำแบบสอบถามเกี่ยวกับภัยการเงินอยู่ ทำให้ระมัดระวังมากกว่าปกติ

ความท้าทายดังกล่าวชี้ให้เห็นถึงความสำคัญของการเก็บรวบรวมข้อมูลที่ดีกว่าที่เป็นอยู่ในปัจจุบัน การเชื่อมโยงเส้นทางการเงิน (ที่จะชี้ให้เห็นว่าบัญชีไหนเป็นบัญชีของมิจฉาชีพ ธุรกิจไหนน่าจะเป็นธุรกิจที่เหยื่อออนไลน์ให้มิจฉาชีพ) เข้ากับข้อมูลรายบุคคลที่ภาคการธนาคารมีอยู่ จะทำให้เราสามารถทำการศึกษาปัจจัยเสี่ยงที่แท้จริง โดยก้าวข้ามข้อจำกัดของการวิจัยจากการสำรวจแบบสอบถามทั่วไปได้ กระนั้นก็ตาม จนกว่าที่เราจะมีข้อมูลที่บ่งชี้สถานะของผู้เสียหายและผู้ที่ไม่ตกเป็นผู้เสียหายได้ดีกว่านี้ งานศึกษาเหล่านี้ก็เป็นสิ่งที่ทำได้ดีที่สุดในปัจจุบัน ภายใต้ข้อจำกัดที่มีอยู่

2.1.3. ธุรกรรมการฉ้อโกง

ธุรกรรมการฉ้อโกงเกิดขึ้นเมื่อมีฉ้อฉลหรือหลอกลวงเกิดขึ้น ซึ่งเงื่อนไขในการเกิดธุรกรรมนี้ ได้แก่ (1) เหยื่อไม่รู้เท่าทัน มีฉ้อฉล (2) ผลประโยชน์ที่มีฉ้อฉลคาดว่าจะได้รับจากการฉ้อโกงมีมูลค่าสูงกว่าต้นทุนในการหลอกลวง และ (3) เหยื่อและ มีฉ้อฉลมีช่องทางในการมาเจอกันเพื่อทำธุรกรรม ซึ่งการรู้ไม่เท่าทันมีฉ้อฉลของเหยื่อขึ้นอยู่กับภูมิคุ้มกันต่อการถูกหลอกลวงของ เหยื่อ ผลประโยชน์ที่มีฉ้อฉลคาดว่าจะได้รับขึ้นอยู่กับมูลค่าของธุรกรรมและโอกาสในการหลอกลวงเหยื่อได้สำเร็จ ส่วนต้นทุนในการฉ้อโกง ของมีฉ้อฉล ได้แก่ เงินทุนที่ใช้ในการก่อเหตุ เวลาและโอกาสที่เสียไปจากการไม่ทำงานอื่น และโทษที่คาดว่าจะได้รับ

ดังนั้น ระบบเศรษฐกิจที่เอื้อให้มีฉ้อฉลหรือหลอกลวงเหยื่อได้สำเร็จจึงมักมีลักษณะดังต่อไปนี้

1. ผู้คนในระบบเศรษฐกิจขาดภูมิคุ้มกันต่อการถูกหลอกลวง ตกเป็นเหยื่อได้ง่าย เนื่องจากตัดสินใจทำธุรกรรมโดยรู้ไม่เท่าทัน เล่ห์กลของมีฉ้อฉล อาจจะเพราะขาดข้อมูลประกอบการตัดสินใจที่เพียงพอ หรือตัดสินใจภายใต้แรงกดดันหรืออคติโดยไม่ พิจารณาข้อมูลประกอบให้ถี่ถ้วน เช่น ตัดสินใจด้วยความเร่งรีบ ความกลัว ความโลภ หรือความหลง ซึ่งรวมถึงความมั่นใจใน ตัวเองที่สูงเกินไป
2. มีฉ้อฉลมีช่องทางที่ใช้ในการหลอกลวงเหยื่อได้ง่าย เช่น ผ่านแพลตฟอร์มออนไลน์และระบบการชำระเงินที่ขาดการคัด กรองมีฉ้อฉลออกจากผู้ประกอบการที่สุจริต
3. มีฉ้อฉลไม่ได้รับการลงโทษที่รุนแรงพอเมื่อเทียบกับผลประโยชน์ที่คาดว่าจะได้รับ เนื่องจากการชี้ตัวและจับกุมมีฉ้อฉล ทำได้ยาก การบังคับใช้กฎหมายไม่เข้มแข็ง และบทลงโทษไม่สูงพอ

โดยปกติแล้ว การฉ้อโกงเป็นปรากฏการณ์ที่พบเห็นได้ทั่วไป เพราะการซื้อขายแลกเปลี่ยนสินค้าและบริการแทบทั้งหมดในระบบ เศรษฐกิจแบบตลาดนั้นเกิดขึ้นระหว่างผู้คนที่ไม่ได้รู้จักกันและไม่ทราบข้อมูลของอีกฝ่ายหนึ่งอย่างถูกต้องสมบูรณ์ ทำให้เหยื่อไม่รู้เท่า ทันมีฉ้อฉล

การที่เหยื่อไม่รู้เท่าทันมีฉ้อฉลเป็นสถานการณ์ที่วงวิชาการเศรษฐศาสตร์เรียกว่าการมีข้อมูลที่ไม่สมมาตร (asymmetric information) นั่นคือ มีฉ้อฉลมีข้อมูลมากกว่าเหยื่อ เหยื่อไม่ทราบเจตนาและเล่ห์กลในการทำธุรกรรมที่ทุจริตของมีฉ้อฉล ซึ่งข้อมูล ที่ไม่สมมาตรนี้ก่อให้เกิดการบิดเบือนแรงจูงใจในการประกอบธุรกรรมของผู้คนในระบบเศรษฐกิจ เนื่องจาก

1. มีฉ้อฉลมีแรงจูงใจที่จะฉวยโอกาสหลอกลวงเหยื่อ เช่น ผู้ขาย (มีฉ้อฉล) ไม่ส่งมอบสินค้าหรือบริการตามที่โฆษณาไว้ให้แก่ ลูกค้า (เหยื่อ) เมื่อได้รับชำระเงินแล้ว หรือผู้ซื้อ (มีฉ้อฉล) ชำระค่าสินค้าเป็นธนบัตรปลอมหรือเช็คแดงให้แก่ผู้ขาย (เหยื่อ) หลัง จากได้รับสินค้าหรือบริการแล้ว ปรากฏการณ์เหล่านี้ในทางเศรษฐศาสตร์เรียกว่า moral hazard
2. การฉ้อโกงยอมทำให้ผู้คนที่บริสุทธิ์ที่อาจตกเป็นเหยื่อของมีฉ้อฉลขาดแรงจูงใจในการทำธุรกรรม เพราะกลัวโดนหลอก ในระดับจุลภาค ตลาดที่มีการฉ้อโกงมากย่อมซบเซาหรือล่มสลาย ในระดับมหภาค หากระบบเศรษฐกิจเต็มไปด้วยมีฉ้อฉล ความเชื่อใจ (trust) ที่เป็นสิ่งจำเป็นพื้นฐานของระบบเศรษฐกิจแบบตลาดย่อมเสื่อมถอยลง เพราะคนบริสุทธิ์สิ่งเลวที่จะทำ ธุรกรรมกับผู้คนในตลาดที่เป็นคนแปลกหน้า ปรากฏการณ์นี้ในทางเศรษฐศาสตร์เรียกว่า adverse selection

ดังนั้น นอกจากการฉ้อโกงจะสร้างความเสียหายให้แก่เหยื่อแล้ว ยังทำให้การจัดสรรทรัพยากรในระบบเศรษฐกิจขาด ประสิทธิภาพอีกด้วย เนื่องจาก (1) ธุรกรรมที่ควรเกิดขึ้นกลับไม่เกิดขึ้นเพราะผู้บริสุทธิ์กลัวตกเป็นเหยื่อ และ (2) ระบบเศรษฐกิจ ต้องหมดเปลืองทรัพยากรไปกับการป้องกันการฉ้อโกง การตรวจสอบธุรกรรมที่ต้องสงสัย การตามจับและดำเนินคดีกับมีฉ้อฉล ตลอดจนการติดตามทรัพย์สินเพื่อชดเชยความเสียหายให้แก่เหยื่อ

เนื่องจากการฉ้อโกงสะท้อนถึงความล้มเหลวของตลาด (market failure) ในการจัดสรรทรัพยากรที่เกิดจากความไม่สมมาตร ของข้อมูล นโยบายภาครัฐที่ช่วยลดการฉ้อโกงจึงไม่เพียงแต่ช่วยป้องกันและบรรเทาความเสียหายให้แก่เหยื่อ แต่ยังช่วยลดผล เสียที่เกิดขึ้นต่อระบบเศรษฐกิจโดยรวมอีกด้วย

2.2. บทบาทของเทคโนโลยีต่อการเงิน

ถึงแม้ว่าการฉ้อโกงจะมีหลายรูปแบบ แต่การฉ้อโกงทางการเงินหรือภัยทางการเงินนั้นได้ทวีความรุนแรงขึ้นอย่างมากใน ปัจจุบันเมื่อเทียบกับการฉ้อโกงประเภทอื่น ๆ เนื่องจากเทคโนโลยีการเงินดิจิทัลที่พัฒนาอย่างก้าวกระโดดในช่วงทศวรรษที่ผ่านมา

เทคโนโลยีเหล่านี้ทำให้การทำธุรกรรมต่างๆ สะดวกขึ้น รวดเร็วขึ้น ต้นทุนต่ำลง และเข้าถึงผู้คนในระบบเศรษฐกิจมากขึ้น แต่ก็มาพร้อมกับความเสี่ยงภัยการเงินในรูปแบบใหม่ที่มากขึ้นเช่นกัน

ภัยการเงินจากการทำธุรกรรม authorized push payment (APP) ผ่านระบบ fast payment หรือ APP fraud เป็นตัวอย่างหนึ่งของพัฒนาการทางเทคโนโลยีทางการเงินที่มีประโยชน์ต่อผู้คนมากมาย แต่ก็มีความเสี่ยงภัยการเงินจากการโดนฉ้อโกงที่สูง กรอบแนวคิดทางเศรษฐศาสตร์ว่าด้วยการฉ้อโกงข้างต้น สามารถนำมาประยุกต์เพื่ออธิบายสาเหตุว่า ทำไมเทคโนโลยีที่ก้าวหน้ามากขึ้น จึงทำให้การฉ้อโกงทางการเงินทวีความรุนแรงมากยิ่งขึ้นเมื่อเทียบกับการฉ้อโกงประเภทอื่นๆ ได้แก่

1. **ผู้คนจำนวนมากขาดภูมิคุ้มกันต่อการหลอกลวงในรูปแบบใหม่** ทำให้ตัดสินใจทำธุรกรรมโดยรู้ไม่เท่าทันเล่ห์กลของมิจฉาชีพที่นำเทคโนโลยีใหม่ๆ เช่น Artificial Intelligence (AI) และข้อมูลออนไลน์มาสร้างสถานการณ์ที่เหมือนจริง หลอกให้เหยื่อหลงเชื่อได้ง่ายขึ้นมาก
2. **มิจฉาชีพใช้แพลตฟอร์มออนไลน์และใช้การชำระเงินผ่านระบบ fast payment** ทำให้มิจฉาชีพสามารถเข้าถึงเหยื่อจำนวนมากได้ด้วยต้นทุนที่ต่ำ การชำระเงินหรือโอนเงินด้วยระบบดิจิทัล เช่น PromptPay ยังทำให้เงินโอนออกจากบัญชีของเหยื่อทันทีและมีการโอนต่อไปบัญชีอื่นเป็นทอดๆ อีกหลายทอด จนออกจากระบบธนาคารและไม่สามารถเรียกเงินคืนกลับมาได้
3. **การซื้อตัวและจับกุมมิจฉาชีพทำได้ยากเนื่องจากเป็นธุรกรรมออนไลน์** มิจฉาชีพสามารถเปิดปิดบัญชีได้ง่าย มีการซื้อขายบัญชีปลอม แอปซ่อนธุรกรรมทุจริตได้ ในขณะที่ผู้บังคับใช้กฎหมายเผชิญข้อจำกัดหลายด้าน เพราะอาชญากรรมทางการเงินดิจิทัลเกี่ยวข้องกับหลายหน่วยงาน ทั้งภาครัฐและเอกชน ทำให้ต้องมีการประสานงานกัน แลกเปลี่ยนข้อมูลกัน รวมถึงการขาดการพัฒนาวิธีการติดตามมิจฉาชีพที่ก้าวหน้าอาชญากรรมทางดิจิทัล ทำให้กระบวนการแจ้งความ อาศัยบัญชี และติดตามเงินล่าช้าเมื่อเปรียบเทียบกับจำนวนคดีที่พุ่งสูงขึ้นอย่างรวดเร็ว

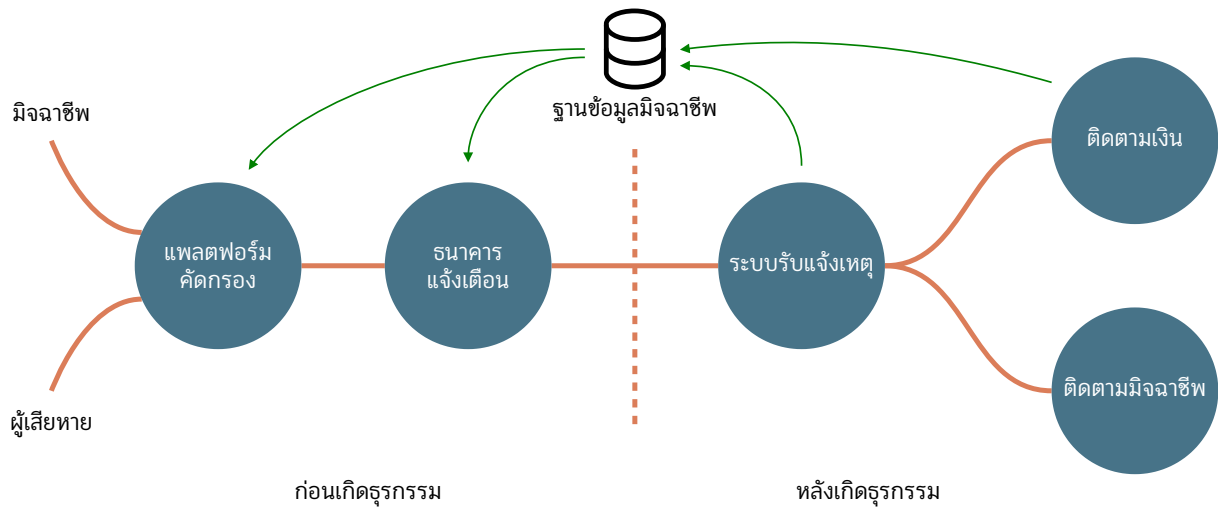
2.3. ข้อมูลและแรงจูงใจ กับการป้องกันและปราบปรามภัยการเงิน

การป้องกันและปราบปรามภัยการเงินต้องประกอบด้วยการลดโอกาสที่เหยื่อถูกหลอกลวงโดยมิจฉาชีพ ทั้งก่อนและหลังจากที่ธุรกรรมการฉ้อโกงเกิดขึ้น ได้แก่ (1) การให้ความรู้แก่ผู้ใช้บริการทางการเงินเพื่อให้รู้เท่าทันมิจฉาชีพ (2) การคัดกรองผู้ประกอบการบนแพลตฟอร์ม (3) การเตือนและการตรวจจับธุรกรรมที่ผิดปกติโดยสถาบันการเงิน ส่วนมาตรการหลังเกิดความเสียหาย ได้แก่ (1) การพัฒนาระบบรับแจ้งเหตุ (2) การพัฒนาระบบติดตามเส้นทางการเงินและป้องกันการนำเงินออกนอกกระบบ และ (3) การดำเนินคดีกับผู้กระทำผิด

การป้องกันและปราบปรามภัยการเงินเหล่านี้ล้วนมีจุดประสงค์ในการลดช่องว่างของข้อมูลข่าวสารตลอดห่วงโซ่ภัยการเงิน เพื่อให้ผู้เกี่ยวข้องทั้งหมดรู้เท่าทันมิจฉาชีพ ทั้งช่องว่างระหว่างเหยื่อกับมิจฉาชีพ และช่องว่างระหว่างแพลตฟอร์ม ธนาคาร และผู้บังคับใช้กฎหมาย กับมิจฉาชีพ

การลดช่องว่างของข้อมูลข่าวสารจำเป็นต้องมีการบูรณาการข้อมูลที่เกี่ยวข้องให้มากที่สุดและใช้ประโยชน์จากข้อมูลให้เกิดประสิทธิภาพมากที่สุด โดยมี การแลกเปลี่ยนข้อมูล การวิเคราะห์ข้อมูล การนำข้อมูลและผลการวิเคราะห์ไปใช้ในการคัดกรอง ตรวจสอบ และดำเนินคดีกับมิจฉาชีพ ตลอดจนใช้ในการสร้างภูมิคุ้มกันให้กับผู้มีโอกาสตกเป็นเหยื่อ ดังที่แสดงในรูปที่ 1

รูปที่ 1: กรอบความคิดทางเศรษฐศาสตร์ว่าด้วยภัยการเงินในห่วงโซ่ภัยการเงิน (fraud chain)



ถึงแม้ว่าผู้ที่เกี่ยวข้องในห่วงโซ่การเงินอาจมีความปรารถนาในการช่วยกันป้องกันและปราบปรามภัยการเงิน แต่อุปสรรคต่าง ๆ ในระบบเศรษฐกิจทำให้ขาดแรงจูงใจที่เพียงพอในการแลกเปลี่ยนและใช้ข้อมูลอย่างทันทั่วถึงและมีประสิทธิภาพ เช่น หย่อนขาดแรงจูงใจในการแจ้งความเพราะโอกาสที่จะได้รับเงินคืนต่ำเมื่อเทียบกับต้นทุนในการแจ้งความ แพลตฟอร์มและธนาคารขาดแรงจูงใจในการคัดกรองและตรวจจับธุรกรรมที่ต้องสงสัย เพราะแต่ละแพลตฟอร์มและแต่ละธนาคารไม่มีข้อมูลที่ไม่เพียงพอต่อการชี้ตัวมีจลาชีพที่แม่นยำ มีโอกาสผิดพลาดสูง ซึ่งส่งผลต่อชื่อเสียงและผลประโยชน์ ส่วนผู้บังคับใช้กฎหมายก็อาจจะขาดแรงจูงใจในการติดตามเส้นทางการเงินและป้องกันการนำเงินออกนอกระบบอย่างทันทั่วถึงเพราะระบบ เทคโนโลยี และกระบวนการทำงานไม่ทันสมัย ทำให้โอกาสในการติดตามเงินและจับกุมมีจลาชีพได้สำเร็จต่ำ เมื่อเทียบกับการดำเนินคดีอื่น ๆ

ดังนั้น มาตรการภาครัฐจึงเป็นสิ่งจำเป็นในการสร้างแรงจูงใจที่เหมาะสม เพื่อให้ผู้เกี่ยวข้องทั้งหมดร่วมกันแลกเปลี่ยนและใช้ข้อมูลในการป้องกันและปราบปรามภัยการเงินอย่างมีประสิทธิภาพมากที่สุด ส่วนที่ 3 และ 4 ของบทความนี้ จะนำเสนอมาตรการต่าง ๆ ที่หน่วยงานที่เกี่ยวข้องได้ดำเนินการอยู่ ตลอดจนมาตรการอื่น ๆ ที่สามารถนำมาใช้เพิ่มเติมได้ในอนาคต

3. มาตรการเพื่อป้องกันภัยการเงิน

ผู้มีโอกาสตกเป็นเหยื่อ แพลตฟอร์ม และภาคการเงิน เป็นปราการสำคัญที่สามารถเข้ามามีส่วนในการป้องกันภัยการเงินได้ ผ่านการสร้างภูมิคุ้มกันการเงิน การคัดกรองผู้ประกอบการธุรกรรม การแจ้งเตือน และการตรวจจับธุรกรรมที่ต้องสงสัย ซึ่งหัวใจของการดำเนินมาตรการเหล่านี้ นอกจากจะต้องบูรณาการข้อมูลในระบบเศรษฐกิจให้สมบูรณ์ที่สุดแล้ว ยังต้องใช้ข้อมูลให้เกิดประสิทธิภาพสูงสุดในการลดความรู้ไม่เท่าทันมีจลาชีพด้วย

3.1. การสร้างภูมิคุ้มกันการเงินให้กับผู้มีโอกาสตกเป็นเหยื่อ

การสร้างภูมิคุ้มกันการเงินสามารถลดโอกาสการตกเป็นเหยื่อของมีจลาชีพได้ ถึงแม้ว่าทุกคนล้วนมีความเสี่ยงต่อภัยการเงิน โดยเฉพาะเมื่อมีจลาชีพปรับเปลี่ยนกลยุทธ์เพื่อเจาะจงจุดอ่อนเฉพาะของแต่ละบุคคล และไม่มีใครที่ "มีภูมิคุ้มกัน" ต่อการหลอกลวงอย่างสมบูรณ์ก็ตาม

ข้อมูล เป็นสิ่งจำเป็นในการสร้างภูมิคุ้มกันทางการเงิน ซึ่ง (1) ข้อมูลจะต้องทันสมัย เท่าทันเล่ห์เหลี่ยมของมีจลาชีพที่เปลี่ยนแปลงไปอยู่เสมอ (2) ข้อมูลที่แก่ผู้มีความเสี่ยงต้องตรงกลุ่ม เนื่องจากมีจลาชีพมีการใช้เล่ห์เหลี่ยมที่แตกต่างกันไปตามกลุ่มเป้าหมายที่ต้องการหลอกลวง และ (3) ข้อมูลต้องนำเสนอให้แก่ผู้มีความเสี่ยงด้วยวิธีที่มีประสิทธิภาพ

3.1.1. การให้ข้อมูลที่ทันสมัยและเท่ากันมีจอาชีพ

การเตรียมตัวล่วงหน้าก่อนเผชิญมีจอาชีพ

การป้องกันภัยการเงินที่มีประสิทธิภาพจึงต้องดำเนินการก่อนที่จะจะถูกนำเข้าสู่สถานการณ์ที่มีจอาชีพกดดันให้เหยื่อตัดสินใจอย่างรีบเร่งหรือด้วยอารมณ์ ซึ่งบั่นทอนความสามารถในการคิดอย่างมีเหตุผล ดังนั้น เช่น

1. การติดตั้งแอปพลิเคชันการเตือน เช่น Whoscall ที่ช่วยตรวจสอบกับฐานข้อมูลว่าเบอร์ที่โทรเข้าเป็นเบอร์ที่เคยถูกรายงานหรือไม่
2. โปรแกรมตรวจจับเว็บไซต์ปลอม ที่สามารถแจ้งเตือนผู้ใช้เมื่อพวกเขา กำลังเยี่ยมชมเว็บไซต์ที่มีลักษณะคล้ายกับการ phishing
3. การตั้งค่าความปลอดภัยล่วงหน้า เช่น การกำหนดวงเงินโอนประจำวัน หรือการตั้งค่าให้ต้องยืนยันตัวตนเพิ่มเติมสำหรับธุรกรรมที่มีมูลค่าสูง

การลดต้นทุนของการตรวจสอบและรายงาน

ในช่วงที่ผ่านมา ประเทศไทยได้มีการพัฒนาเครื่องมือมาเตือนผู้ใช้ เช่น เว็บไซต์ Blacklistseller ที่เป็นแพลตฟอร์มที่จัดทำขึ้นโดยภาคประชาชน ให้ผู้เสียหายจากการซื้อของออนไลน์เข้ามารายงาน “เพื่อเตือนภัยสังคม แล้วจะไม่มีใครถูกหลอกเป็นครั้งที่สอง” หรือเว็บไซต์ฉลาดโอน ที่มีลักษณะการทำงานคล้ายกันแต่มีองค์กรรัฐเข้ามาร่วมด้วย เว็บไซต์ในลักษณะดังกล่าวจะช่วยป้องกันการฉ้อโกงได้ในกรณีที่ผู้ซื้อเข้ามาตรวจสอบบัญชีปลายทางก่อนที่จะโอน และนับว่าเป็นแพลตฟอร์มที่ช่วยทำให้การตรวจสอบประวัติเบื้องต้นสะดวกขึ้นสำหรับลูกค้ากลุ่มนั้น สำหรับตัวอย่างจากต่างประเทศนั้น ในสิงคโปร์ ได้มีการพัฒนาแอปพลิเคชัน ScamShield ที่ให้ใช้งานสามารถตรวจสอบเว็บไซต์ที่ตนเองสงสัย โดยการใช้ AI ได้ นอกจากนี้ ยังมีช่องทางให้ผู้ใช้งานรายงานเว็บไซต์ของมีจอาชีพ เพื่อให้เจ้าหน้าที่ตรวจสอบต่อไปด้วย

3.1.2. การให้ข้อมูลที่ตรงกับกลุ่ม

การให้ความรู้ที่ตรงตามความเสี่ยงเฉพาะกลุ่ม

การให้ความรู้ผ่านข้อความเตือนให้ระมัดระวังการถูกหลอกลวงออนไลน์แบบทั่วไปมีผลค่อนข้างจำกัด (Kubilay et al., 2023, Junger et al., 2017) ส่วนการให้ความรู้เกี่ยวกับการหลอกลวงออนไลน์ที่เฉพาะเจาะจง มุ่งเป้าไปที่กลุ่มเสี่ยงของการหลอกลวงแต่ละประเภท มีประสิทธิภาพมากกว่า (DeLiema et al., 2023) เช่น การให้ความรู้กับข้าราชการที่กำลังจะเกษียณ เกี่ยวกับการหลอกลวงที่เกี่ยวข้องกับเงินบำนาญ การให้ความรู้กับผู้ที่ย้ายมาหางานกับกรมจัดหางานเกี่ยวกับภัยการเงินที่มาจากการพยายามหางานทำ เพราะผลการศึกษาชี้ให้เห็นว่าการหลอกลวงแต่ละประเภทมีโอกาสประสบความสำเร็จกับคนบางกลุ่มมากเป็นพิเศษ

นโยบายป้องกันขั้นพื้นฐานที่ปรับเปลี่ยนได้

การมีนโยบายพื้นฐานที่อาจเฉพาะเจาะจงกับลักษณะของผู้ใช้บริการช่วยป้องกันหรือจำกัดมูลค่าความเสียหายได้ ซึ่งเป็นแนวทางที่หลายประเทศเลือกใช้ เช่น การจำกัดวงเงินโอนสูงสุดต่อวัน การกำหนดมาตรการเพิ่มเติมสำหรับการทำธุรกรรมวงเงินสูง (World Bank Group, 2023) แต่เนื่องจากความจำเป็นในการทำธุรกรรมของแต่ละคนแตกต่างกันไป นโยบายดังกล่าวจึงควรรองรับการปรับเปลี่ยนวงเงินที่สะท้อนการยอมรับความเสี่ยงของลูกค้าแต่ละกลุ่ม แต่ในขณะเดียวกัน ก็ปกป้องการล่อลวงจากมีจอาชีพที่จะนำไปสู่การปรับวงเงินอย่างไม่ตั้งใจด้วย

3.1.3. การให้ข้อมูลด้วยวิธีที่มีประสิทธิภาพ

แคมเปญที่มากกว่าการให้ความรู้

การศึกษาที่ผ่านมาพบว่า การให้ความรู้ผ่านข้อความเตือนในลักษณะการชี้ “จุดสังเกต” ของการหลอกลวงออนไลน์ได้ผลค่อนข้างจำกัด ส่วนหนึ่งเนื่องจากมีงานวิจัยที่เห็นข้อความเตือนเหล่านั้นและปรับตัวเช่นกัน (Kubilay et al., 2023) นอกจากนี้ ผู้ได้รับข้อความเตือนดังกล่าวยังอาจตกเป็นเหยื่อได้ง่ายขึ้น เนื่องจากมีความเชื่อว่าตนเองมีความรู้เท่าทันมิจฉาชีพแล้ว หรือที่ Whitty (2015) เรียกว่า “illusion of invulnerability” ก็เป็นไปได้

การศึกษายังพบว่า ผู้ที่ตกเป็นเหยื่อส่วนใหญ่เคยทราบเรื่องการหลอกลวงที่ตนเองตกเป็นเหยื่อมาก่อนแล้ว ดังนั้นปัญหาส่วนหนึ่งเกิดจากการที่ผู้เสียหายไม่สามารถดึงเอาความรู้ที่มีอยู่ มาใช้ในสถานการณ์จริงได้ (Chugh & Narang, 2023, Salathong et al., 2024) ซึ่งส่วนหนึ่งก็เป็นผลมาจากเทคนิคของมิจฉาชีพที่พยายามสร้างสถานการณ์หรือเงื่อนไข ที่ทำให้ความสามารถในการใช้เหตุผลของเหยื่อต่ำลงนั่นเอง (Lu et al., 2020, Liu et al., 2025)

ในระยะหลัง มีงานวิจัยที่พยายามศึกษาถึงวิธีการเตือนภัยการเงิน ว่าข้อความประเภทไหนมีประสิทธิภาพ ซึ่งมีหลายงานที่บ่งชี้ว่าข้อความเตือนที่ทำงานกับอารมณ์ของผู้รับสาร หรือให้ผู้รับสารรับรู้ถึงอารมณ์ของตนเอง (ซึ่งอาจขึ้นกับลักษณะของผู้รับสารด้วย) จะทำให้ผู้รับสารสามารถดึงเอาความรู้เกี่ยวกับภัยการเงินที่มีมาใช้ได้ (Lu et al., 2020, Wen et al., 2022, Fitrah et al., 2025, Malkin et al., 2017) กระนั้นก็ตาม ผลที่ได้อาจแตกต่างกันไปตามบริบทของสังคม

3.2. การคัดกรองผู้ประกอบการโดยแพลตฟอร์ม

เนื่องจากธุรกรรมเริ่มต้นที่แพลตฟอร์มซึ่งเป็นพื้นที่กลางให้คนซื้อและคนขายเข้ามาพบปะกัน แพลตฟอร์มจึงสามารถช่วยคัดกรองมิจฉาชีพออกได้ โดยแพลตฟอร์มในที่นี้ หมายรวมถึงแพลตฟอร์มขายของออนไลน์ แพลตฟอร์ม social media ต่าง ๆ แพลตฟอร์มส่งข้อความออนไลน์ หรือผู้ให้บริการโทรศัพท์³

ปัจจุบัน แพลตฟอร์มต่าง ๆ ตระหนักถึงบทบาทของตนเองที่มีในการป้องกันภัยการเงินมากขึ้น และมีมาตรการต่าง ๆ เพื่อป้องกันปัญหาดังกล่าว

- **แพลตฟอร์มขายของออนไลน์** โดยทั่วไปจะทำหน้าที่เป็น escrow คือบุคคลที่สามที่ทำหน้าที่ดูแลเงินให้ผู้ที่ทำธุรกรรมอยู่แล้ว โดยจะรับเงินมาจากผู้ซื้อแต่ยังไม่โอนเงินต่อไปยังผู้ขายจนกว่าผู้ซื้อจะยืนยันว่าได้สินค้าแล้ว เราจึงพบว่ากรณีการหลอกลวงที่เกี่ยวข้องกับแพลตฟอร์มขายของออนไลน์มีน้อยมาก หรือในกรณีที่มี ก็เป็นการหลอกลวงให้ทำการซื้อขายกันนอกแพลตฟอร์ม หรือการเชิญชวนให้ทำธุรกรรมอื่น ๆ โดยอ้างชื่อแพลตฟอร์ม
- **แพลตฟอร์ม social media** จากเดิมที่เป็นพื้นที่แลกเปลี่ยนความคิดเห็นกันของบุคคลทั่วไป ถูกใช้เป็นช่องทางติดต่อของธุรกิจต่าง ๆ ไม่ว่าจะเป็นเล็กหรือใหญ่ เกิดเป็น social commerce คือการซื้อขายกันผ่านแพลตฟอร์ม social media มากขึ้น โดยเป็นช่องทางการซื้อขายที่มีอัตราการเติบโตสูงกว่าปีละ 28% ในช่วงปี 2021-2024 (PayNXT360, 2025) ทำให้ถูกใช้เป็นช่องทางหลอกลวงได้ แม้ว่าแพลตฟอร์มเหล่านี้จะมีมาตรการป้องกันต่าง ๆ เช่น ระบบยืนยันตัวตนที่ช่วยให้ผู้ใช้บริการสามารถประเมินความน่าเชื่อถือของบัญชีผู้ใช้งานได้ในเบื้องต้น ว่ากำลังติดต่อกับบุคคลดังกล่าว หรือร้านค้าจริง ๆ หรือช่องทางให้ผู้ให้บริการแจ้งปัญหาบัญชีปลอมที่แอบอ้างบุคคลหรือบริษัทอื่น
- **แพลตฟอร์มส่งข้อความออนไลน์** หรือที่รู้จักกันในชื่อ instant messaging service เป็นช่องทางหลักที่มิจฉาชีพใช้ในการหลอกผู้เสียหาย เนื่องจากเป็นช่องทางส่วนตัวที่มิจฉาชีพสามารถใช้ข้อความในการชักจูง จูงใจเหยื่อได้ โดยเฉพาะหากถูกทำให้เชื่อว่าเป็นคนรู้จัก บริษัท หรือองค์กรที่น่าเชื่อถือ แพลตฟอร์มเหล่านี้พยายามแก้ปัญหาด้วยการเพิ่มระบบยืนยันตัวตนของบัญชีทางการ (official accounts) การให้ผู้ใช้งานปิดกั้น (block) และรายงานบัญชีที่ต้องสงสัยได้

การเชื่อมโยงข้อมูลระหว่างตำรวจและภาคการเงินเข้ากับแพลตฟอร์ม จะทำให้แพลตฟอร์มมีข้อมูลมากขึ้นเพื่อมาใช้ในการประเมินความเสี่ยงของบัญชีผู้ใช้งานแต่ละบัญชี ตัวอย่างหนึ่งที่เห็นได้ชัดเจน คือมาตรการของ Meta (บริษัทแม่ของ Facebook) ที่ จะตรวจสอบข้อความที่ผู้ใช้งานส่งหากัน ว่ามีการส่งเลขที่บัญชีที่มีอยู่ในฐานข้อมูลของตำรวจสอบสวนกลางหรือไม่ หากมีก็จะแจ้งเตือนผู้ใช้งาน นอกจากนี้ ยังมีการกำหนดให้ผู้ลงโฆษณารายใหม่ ต้องยืนยันหมายเลขโทรศัพท์ก่อน เนื่องจากการลงโฆษณาเป็นช่องทางที่มิจฉาชีพมักใช้ในการเข้าถึงเหยื่อได้เป็นจำนวนมาก

แม้ว่าแพลตฟอร์มจะมีความพยายามในการช่วยป้องกันภัยการเงินอยู่แล้วในปัจจุบัน แต่แพลตฟอร์มยังสามารถมีมาตรการอื่น ๆ เพิ่มเติมได้ในอีกหลายด้าน โดยเฉพาะการตรวจสอบและระงับบัญชีที่มีการรายงานโดยผู้ใช้ หรือบัญชีที่ถูกแจ้งความแล้ว นอกจากนี้

การยกระดับความเข้มข้น ก็ควรเกิดขึ้นในแพลตฟอร์มอื่น ๆ ด้วย ไม่ว่าจะเป็นการขอความร่วมมือ หรือกำหนดเป็นนโยบายที่แพลตฟอร์มจำเป็นต้องปฏิบัติ เหมือนในหลาย ๆ ประเทศ มิฉะนั้น มิฉฉาจะปรับตัวตามระดับความเข้มข้นของมาตรการ และย้ายไปแพลตฟอร์มที่มีมาตรการที่เข้มข้นน้อยกว่า

3.3. การเตือนและการตรวจจับธุรกรรมผิดปกติโดยสถาบันการเงิน

เมื่อผู้ขายกับผู้ซื้อตกลงที่จะทำธุรกรรมกันแล้ว ขั้นตอนถัดไปเป็นหน้าที่ของภาคการเงินในการที่จะเตือนผู้ให้บริการให้รับทราบความเสี่ยงที่มีอยู่สำหรับธุรกรรมนั้น ๆ และตรวจจับความผิดปกติ ก่อนจะเกิดธุรกรรมขึ้น แม้ว่าการตรวจจับธุรกรรมที่ผิดปกติโดยภาคการเงินจะเป็นสิ่งที่มาเป็นเวลานานแล้ว เช่น การตรวจสอบลายเซ็นเพื่อป้องกันการปลอมแปลงเช็ค แต่ในช่วงก่อนหน้านี้ เทคโนโลยีการตรวจจับความผิดปกติแบบทันที (real-time) นั้นกระจุกตัวอยู่เกือบจะเฉพาะในกลุ่มผลิตภัณฑ์บัตรเครดิตและเครดิตเท่านั้น

เมื่อระบบ fast payment เริ่มเข้ามามีบทบาทในการใช้จ่ายในชีวิตประจำวันของประชาชนมากขึ้น ระบบการตรวจจับธุรกรรมผิดปกติของภาคการเงินเองจำเป็นต้องปรับตัวตามด้วย ถึงแม้ว่าระบบ fast payment จะอำนวยความสะดวก ลดการใช้เงินสด แต่ก็เปิดทางให้มิฉฉาหันเข้ามาใช้ช่องทางนี้ในการหลอกลวงคนมากขึ้นและทำให้การติดตามเงินคืนยากขึ้นเพราะเมื่อโอนเงินแล้วไม่สามารถยกเลิกธุรกรรมหรือดึงเงินกลับมาได้ (World Bank Group, 2023)

การดำเนินการในช่วงที่ผ่านมา

การขึ้นข้อความเตือน

ในช่วงหลายปีที่ผ่านมา แอปพลิเคชัน mobile banking ได้ใช้มาตรการแสดงข้อความเตือนภัยจากมิฉฉาก่อนการทำทุก ๆ ธุรกรรม อย่างไรก็ตาม การแสดงคำเตือนในทุก ๆ ธุรกรรม นำไปสู่ความเคยชินต่อคำเตือน ซึ่งเป็นปรากฏการณ์ทางจิตวิทยาที่เรียกว่า “warning fatigue” โดยงานศึกษาพบว่าผู้ใช้ที่เคยเห็นข้อความเตือนเดิมซ้ำ ๆ มีโอกาสจะเพิกเฉยต่อข้อความเตือนนั้นสูงขึ้น (Daryanani, 2011, Ban et al., 2021) ส่งผลให้ประสิทธิภาพของมาตรการเตือนภัยผ่านข้อความดังกล่าวอาจไม่ได้ผลมากนัก

การตรวจจับธุรกรรมผิดปกติของเหยื่อ

ในช่วงก่อนหน้านี้ การตรวจจับธุรกรรมการโอนเงินที่ผิดปกติของเหยื่อ จะเป็นการดำเนินการโดยธนาคารต้นทางเอง แต่การดำเนินการดังกล่าวยังมีข้อจำกัด เนื่องจากธนาคารต้นทางจะไม่ทราบข้อมูลของบัญชีปลายทางที่อยู่ต่างธนาคาร การดำเนินการต่าง ๆ จึงอาศัยการสังเกตความผิดปกติในการทำธุรกรรมของลูกค้านั้นเองเท่านั้น

ในปี 2023 มีการพัฒนาระบบ Central Fraud Registry (CFR) ขึ้น ซึ่งเป็นระบบแลกเปลี่ยนข้อมูลระหว่างธนาคารเกี่ยวกับบัญชีต้องสงสัยที่อยู่ในเส้นทางการเงินของมิฉฉา ทำให้ธนาคารมีข้อมูลเกี่ยวกับบัญชีปลายทางต่างธนาคารมากขึ้น และสามารถระบุธุรกรรมของเหยื่อได้หากบัญชีปลายทางถูกเคยรายงานว่าเป็นบัญชีที่เคยใช้ในการก่อเหตุหรืออยู่ในเส้นทางการเงิน

เกี่ยวกับการเตือนของบัตรพลาสติก

อาจมีคำถามว่า เราสามารถนำระบบการตรวจจับธุรกรรมผิดปกติของบัตรพลาสติก (บัตรเครดิต/เดบิต) มาใช้กับการโอนเงินได้หรือไม่ มีข้อแตกต่างอย่างน้อย 3 ประการที่ทำให้ระบบตรวจจับธุรกรรมที่ผิดปกติสำหรับ fast payment โดยเฉพาะในบริบทของประเทศไทย แตกต่างออกไปจากธุรกรรมอื่น

1. ปริมาณธุรกรรมในระบบ fast payment สูงกว่ามาก จากสถิติของธนาคารแห่งประเทศไทย มีการโอนเงินผ่าน mobile banking กว่าเดือนละ 3.2 พันล้านธุรกรรม ขณะที่ธุรกรรมจากบัตรพลาสติกมีเพียง 100 ล้านธุรกรรมต่อเดือนเท่านั้น นอกจากนี้ ระบบ fast payment ที่จำเป็นต้องมีความรวดเร็ว และธุรกรรมเสร็จสิ้นทันที ทำให้การตรวจจับความผิดปกติเป็นไปได้ยากขึ้น เทียบกับบัตรพลาสติกที่มีการ settle กันช้าวัน

2. ระบบบัตรเครดิต/เดบิต เป็นแบบ pull payment คือ ปลายทางเป็นฝ่ายเรียกเก็บเงิน ซึ่งหมายความว่าคนมีสิทธิ์เรียกเก็บเงิน (มีเครื่องรูดบัตร) จะต้องมียี่ห้ออยู่ในระบบของธนาคาร ชำระค่าบริการรายเดือน ฯลฯ ทำให้เปิดใช้ยากกว่ามาก
3. ในระบบบัตรเครดิตนั้น ธนาคารจึงมีแรงจูงใจที่จะเพิ่มทรัพยากรมาเพื่อดูแลการทุจริตในส่วนนี้ เพราะผู้ให้บริการได้ค่าธรรมเนียมจากทุก ๆ ธุรกรรมที่เกิดขึ้น รวมถึงเงินที่ชำระให้ร้านค้ายังคงถือว่าเป็นเงินของธนาคารอยู่ (ธนาคารไปเรียกเก็บเงินจากเจ้าของบัตรภายหลัง) ในทางกลับกัน ในระบบ fast payment ธนาคารเองไม่ได้รายได้จากการโอน รวมถึงเงินที่ชำระให้ร้านค้าก็เป็นเงินของผู้ทำธุรกรรม ทำให้การตรวจสอบธุรกรรม หรือการลงทุนในโครงสร้างพื้นฐานเพื่อตรวจสอบธุรกรรมที่ผิดปกติเป็นค่าใช้จ่ายที่ผู้ให้บริการทางการเงินต้องแบกรับไว้

สิ่งที่ทำได้เพิ่มเติม

การมีระบบ CFR เพื่อแลกเปลี่ยนข้อมูลบัญชีต้องสงสัยข้ามธนาคาร (อันเนื่องมาจากการถูกแจ้งความ หรืออยู่ในเส้นทางการเงิน) เป็นจุดเริ่มต้นที่ดีที่ช่วยให้ระบบมีข้อมูลเกี่ยวกับบัญชีปลายทางที่ต้องสงสัยมากขึ้น แต่ตัวเลขความเสียหายในทุก ๆ วันนี้ แสดงให้เห็นว่ามีธุรกรรมที่บัญชีปลายทางเป็นบัญชีม้าที่ยังไม่มีประวัติอยู่ในระบบ CFR เป็นจำนวนมาก ขณะเดียวกัน การขึ้นข้อความเตือนที่ทำการแจ้งเตือนทั่วไป ทุกธุรกรรม ก็อาจไม่มีประสิทธิภาพมากนัก

การประเมินความเสี่ยงที่แม่นยำขึ้น

การเลือกแสดงข้อความเตือนเฉพาะธุรกรรมที่มีความเสี่ยงสูงสามารถช่วยลดความไม่สนใจจากการเตือนที่มากเกินไปลงได้ เนื่องจากปัจจุบันธนาคารมีข้อมูลของลูกค้าของตนเอง รวมถึงข้อมูลเบื้องต้นของบัญชีปลายทาง (เช่น ชื่อบัญชี) อยู่แล้วหากธนาคารนำข้อมูลดังกล่าวมาประกอบเพื่อประเมินความเสี่ยงของธุรกรรม เช่น การทำธุรกรรมมูลค่าสูงกว่าที่ลูกค้าคนนั้น ๆ ใช้อยู่ปกติ บัญชีปลายทางที่ไม่เคยโอนเงินให้มาก่อน จะสามารถเลือกแสดงข้อความเตือนเฉพาะธุรกรรมที่มีความเสี่ยงสูง ก็จะช่วยลด warning fatigue ลงได้

การนำข้อมูลอื่น ๆ เข้ามาร่วมประเมินความเสี่ยง จะช่วยให้ภาคธนาคารสามารถประเมินความเสี่ยงได้ดียิ่งขึ้น นอกจากข้อมูลที่ธนาคารมีเกี่ยวกับลูกค้าตัวเอง รวมไปถึง CFR ที่มีอยู่ในปัจจุบันแล้ว ข้อมูลอื่น ๆ ได้แก่ ข้อมูลของบัญชีปลายทาง เช่น อายุบัญชี ลักษณะธุรกรรมในอดีต รวมถึงจำนวนบัญชีที่เพิ่งเปิดใหม่ของเจ้าของบัญชี เป็นต้น

การแชร์ข้อมูลข้ามสถาบันการเงินดังกล่าว ทำได้หลายรูปแบบ ตั้งแต่การส่งข้อมูลระหว่างกันของธนาคารต้นทางกับปลายทาง ไปจนถึงการให้ผู้ดำเนินการระบบชำระเงิน (fast payment system operator: FPS operator) ซึ่งมีข้อมูลธุรกรรมระหว่างธนาคารทั้งหมด นำข้อมูลมาประมวลผลเป็นความเสี่ยงของธุรกรรมนั้น ๆ ดังเช่นที่ทำใน ฝรั่งเศส อินเดีย แอฟริกาใต้ (World Bank Group, 2023)

ความท้าทายหลักของการแลกเปลี่ยนข้อมูลคือการคำนึงถึงความสมดุลระหว่างความปลอดภัย ความเป็นส่วนตัวของข้อมูลผู้ใช้บริการ หรือความลับทางการค้าของสถาบันการเงิน

ข้อความเตือนที่มีประสิทธิภาพมากขึ้น

การศึกษาพบว่า ข้อความเตือนที่ตั้งคำถามหรืออธิบายปัจจัยเสี่ยงที่เฉพาะเจาะจงกับสถานการณ์นั้น ๆ ทำให้ผู้ใช้งานมีโอกาสนับจะปฏิบัติตามคำเตือนมากกว่าข้อความเตือนทั่วไป ตัวอย่างข้อความที่เฉพาะเจาะจง เช่น “คุณรู้จัก (ชื่อเจ้าของบัญชี) เป็นส่วนตัวหรือไม่” หรือ “คุณกำลังโอนเงินจำนวนมากไปยังบัญชีที่คุณไม่เคยโอนมาก่อน”) ส่วนตัวอย่างข้อความเตือนทั่วไป เช่น “โปรดระวังมิฉ้อฉล” (Wen et al., 2022, Roy et al., 2025)

นอกจากนี้ ธนาคารอาจเพิ่มขั้นตอนเล็กน้อย เพื่อให้ผู้ใช้งานมีโอกาสหยุดคิดก่อนจะตัดสินใจยืนยันธุรกรรม หรือที่เรียกว่า “positive friction” นอกเหนือจากข้อความเตือนที่แสดงในขั้นตอนการยืนยันธุรกรรมแล้ว (Whitley & Pujadas, 2018)

ตัวอย่าง POSITIVE FRICTION ของ ZELLE

Zelle เป็นผู้ให้บริการเครือข่ายการชำระเงินแบบ peer-to-peer (P2P) ในสหรัฐอเมริกา และได้รับแรงกดดันจากจำนวนการร้องเรียนที่ลูกค้าถูกละเมิดมากขึ้น นำไปสู่การเพิ่มมาตรการป้องกันต่าง ๆ หนึ่งในนั้น คือการเพิ่มขั้นตอนการโอนเงินเพื่อเป็น positive friction โดยผู้ใช้บริการจะถูกถามว่าจุดประสงค์ในการโอนเงินครั้งนี้คืออะไร (เช่น โอนให้เพื่อนหรือครอบครัว โอนชำระค่าสินค้าและบริการ โอนเพื่อลงทุน) เมื่อผู้ใช้ระบุวัตถุประสงค์ในการโอนเงิน ระบบจะทำการแสดงข้อความเตือนที่เกี่ยวข้องกับการโอนเงินในกรณีนั้น ๆ เพื่อให้ผู้ใช้ได้พิจารณาอีกครั้งก่อนที่จะยืนยันการทำธุรกรรม เช่น เตือนเกี่ยวกับ romance scam ในกรณีที่ผู้ใช้ตอบว่าโอนให้เพื่อนหรือครอบครัว และยังทำปุ่มสำหรับยกเลิกการทำธุรกรรมให้เด่นกว่าปุ่มสำหรับการทำธุรกรรมต่อ เพื่อช่วยป้องกันการกดปุ่มจากความเคยชินอีกด้วย

ในกรณีที่ธนาคารประเมินแล้วว่าธุรกรรมมีความเสี่ยงสูงมาก ธนาคารอาจมีมาตรการอื่น ๆ นอกเหนือจากการขึ้นข้อความเตือน เช่น การยืนยันความต้องการทำธุรกรรมกับบุคคลในครอบครัว การทวนเวลาธุรกรรม การทวนเวลาการโอนเงินออกจากบัญชีปลายทาง ไปจนถึงการระงับธุรกรรม

4. มาตรการหลังเกิดความเสียหายจากภัยการเงิน

เมื่อผู้เสียหายรู้ตัวแล้วว่าถูกละเมิด (ซึ่งอาจกินเวลาระยะหนึ่งหลังจากโอนเงินเสร็จ) ต้องติดต่อธนาคารเพื่อแจ้งเหตุ และแจ้งเจ้าหน้าที่ตำรวจ เพื่อขอหมายอายัดต่อไป หรือหากเงินถูกโอนออกจากบัญชีดังกล่าวแล้ว ก็ต้องติดตามเส้นทางการเงิน เพื่อป้องกันไม่ให้เงินออกนอกระบบธนาคาร นอกจากการป้องกันไม่ให้เงินออกไปนอกระบบธนาคารแล้ว ในทางกฎหมายเอง ตำรวจก็ยังมีส่วนในการติดตามจับกุมผู้กระทำความผิดมาดำเนินคดี รับโทษต่อไปด้วย

ในระหว่างนั้น มิจฉาชีพจะโอนเงินผ่านบัญชีม้า ก่อนที่จะนำเงินดังกล่าวไป “ฟอก” เพื่อไม่ให้ตรวจสอบเส้นทางการเงินได้ บัญชีม้าคือบัญชีที่จ้างผู้อื่นเปิด แลกกับผลตอบแทน โดยมีจุดประสงค์เพื่ออำพรางเส้นทางการเงินไม่ให้ถูกติดตามได้ง่าย ก่อนที่มิจฉาชีพจะนำเงินดังกล่าวไป “ฟอก” ซึ่งโดยทั่วไปเป็นการนำเงินออกจากระบบธนาคารชั่วคราว ผ่านช่องทางต่าง ๆ เช่น การถอนเงินสด การซื้อขายสินทรัพย์ดิจิทัล (World Bank Group, 2023) ก่อนที่จะนำเงินที่ไม่สามารถตรวจสอบเส้นทางแล้ว เข้ามาในระบบธนาคารอีกครั้ง

ทั้งสองฝั่งแข่งกับเวลา หากเหยื่อสามารถแจ้งความ ยื่นหมายอายัด หรือภาคการเงินสามารถตรวจจับธุรกรรมที่ต้องสงสัยของมิจฉาชีพและระงับไว้ ก่อนที่มิจฉาชีพจะนำเงินออกนอกระบบธนาคารได้ ก็มีโอกาที่จะได้เงินคืนมา แต่ถ้ามิจฉาชีพสามารถนำเงินออกนอกระบบได้ก่อน โอกาสที่จะติดตามเงินกลับมาได้ก็มีค่อนข้างน้อย

ทั้งนี้ ภาคการเงิน สามารถเข้ามามีส่วนได้ตั้งแต่ที่เหยื่อยังไม่รู้ตัวว่าถูกละเมิด ผ่านการตรวจจับธุรกรรมที่ต้องสงสัยของบัญชีปลายทาง เช่น บัญชีที่ไม่เคยมีการเคลื่อนไหวเลย แต่กลับมีเงินเข้ามาปริมาณมาก และมีความพยายามที่จะโอนต่อไปภายในเวลาสั้น ๆ โดยมีจุดมุ่งหมายคือการระงับธุรกรรมของมิจฉาชีพ และป้องกันไม่ให้เงินออกนอกระบบธนาคาร

หัวใจของการดำเนินการเหล่านี้ ก็คือการแบ่งปันข้อมูลระหว่างกัน ทั้งจากผู้เสียหายไปยังภาคการเงินและเจ้าหน้าที่ตำรวจในรูปแบบของการแจ้งเหตุ ระหว่างภาคการเงินด้วยกันเองเพื่อให้การติดตามเส้นทางการเงินเป็นไปได้อย่างมีประสิทธิภาพ และระหว่างภาคการเงินกับเจ้าหน้าที่ตำรวจ เพื่อการติดตามผู้กระทำความผิด

4.1. ระบบรับแจ้งเหตุ

ระบบรับแจ้งเหตุ เป็นจุดเชื่อมต่อแรกของผู้เสียหายหลังจากเกิดธุรกรรมและรู้ตัวว่าถูกละเมิด ระบบรับแจ้งเหตุที่ดี คือระบบรับแจ้งเหตุที่รวดเร็ว ส่งต่อข้อมูลทันเวลา และไม่ก่อให้เกิดต้นทุนต่อเหยื่อมากเกินไป เพราะการรับแจ้งเหตุ ไม่ได้ทำประโยชน์ให้เหยื่อเท่านั้น แต่ยังเป็นการส่งต่อข้อมูลของบัญชีต้องสงสัยเข้าในระบบ ซึ่งอาจช่วยป้องกันไม่ให้คนอื่นตกเป็นเหยื่อได้

การดำเนินการในช่วงที่ผ่านมา

ก่อนหน้านี้ กระบวนการแจ้งความ อาศัย มักกินเวลานาน เพราะเหยื่อต้องไปแจ้งความที่สถานีตำรวจ เพื่อให้ตำรวจสอบปากคำ ลงบันทึกประจำวัน และออกหมายอาัยให้ เหยื่อต้องนำหมายอาัยดังกล่าวไปให้ธนาคารของมิจฉาชีพ สาขานาการจึงส่งเรื่องไปที่สำนักงานใหญ่ และพยายามอาัยบัญชีของมิจฉาชีพ ไม่ให้ถอนเงินออกจากบัญชีดังกล่าวได้ กระบวนการทั้งหมดนี้มักกินเวลาหลายวัน หรือถ้าเหยื่ออยู่ในที่ที่เดินทางไม่สะดวก อาจใช้เวลาหลายสัปดาห์

เมื่อคดีหลอกลวงออนไลน์มีมากขึ้น สำนักงานตำรวจแห่งชาติจึงจัดตั้งศูนย์รับแจ้งความออนไลน์คดีทางเทคโนโลยี คือ thaipoliceonline.go.th (TPO) ขึ้นในปี 2022 โดยอยู่ในความดูแลของกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (สอท.) ระบบดังกล่าว ช่วยอำนวยความสะดวกให้ผู้เสียหายแจ้งความเบื้องต้นได้รวดเร็วและสะดวกขึ้น

สถิติและข้อสังเกต

ความเร็วของการแจ้งความ

เหยื่อใช้เวลาที่ค่อนข้างนานกว่าจะแจ้งความ ทำให้การอาัยบัญชีโดยอาศัยการโทรแจ้งของผู้เสียหายเพียงอย่างเดียวแทบจะไม่มีโอกาสเกิดขึ้นได้เลย จากข้อมูลของ สอท. พบว่า โดยเฉลี่ย เหยื่อใช้เวลาถึง 18 ชั่วโมงหลังจากการโอนเงินครั้งสุดท้ายก่อนจะแจ้งเข้ามาในระบบ เมื่อเปรียบเทียบกับสถิติการโอนเงินออกจากบัญชีม้าแฉวแรก ซึ่งใช้เวลาเฉลี่ยเพียง 2 นาทีหลังจากที่เหยื่อโอนเข้าเท่านั้น (Amarase et al., forthcoming)

กระนั้นก็ตาม การแจ้งเหตุของผู้เสียหาย ไม่ได้เปล่าประโยชน์ เนื่องจากการแจ้งเหตุ จะช่วยให้ระบบธนาคารมีข้อมูลเกี่ยวกับบัญชีของมิจฉาชีพ ทำให้ระงับธุรกรรมที่เกิดขึ้นกับบัญชีนั้นในภายหลังได้

โอกาสที่เหยื่อจะแจ้งความ

เหยื่อจำนวนมากไม่แจ้งความ งานศึกษาที่ผ่านมาในหลายประเทศพบว่าผู้เสียหายเพียง 10-15% เท่านั้นที่เข้าไปแจ้งความ (Whitty, 2015, Service statistique ministériel de la sécurité intérieure (SSMSI), 2019, U.S. Attorney's Office, Western District of Washington, 2025, Smith, 2007) สำหรับประเทศไทย การสำรวจของ Hapipat (2024) ได้ประเมินไว้ว่า มีผู้เสียหายเพียง 10% เท่านั้นที่เข้าแจ้งความ

การศึกษาถึงสาเหตุที่เหยื่อเลือกที่จะไม่ไปแจ้งความมีความสำคัญ แต่ก็มีความท้าทายค่อนข้างมาก การแจ้งเหตุช่วยเพิ่มประสิทธิภาพของระบบตรวจจับธุรกรรมผิดปกติ และช่วยให้ทราบถึงรูปแบบการหลอกลวงใหม่ ๆ เพื่อไปแจ้งเตือนประชาชน แต่โดยทั่วไป ทางกรมจะมีข้อมูลของผู้ที่ไปแจ้งความเท่านั้น การหาสาเหตุที่เหยื่อไม่ไปแจ้งความจึงต้องอาศัยการสัมภาษณ์ประสบการณ์ของผู้ที่เคยตกเป็นผู้เสียหายแล้ว (victimization study) เป็นหลัก

ในมุมมองของเศรษฐศาสตร์ การแจ้งความเป็น “กิจกรรมทางเศรษฐกิจ” อย่างหนึ่ง ผู้เสียหายจะเลือกที่จะแจ้งความ ก็ต่อเมื่อคาดว่าประโยชน์ที่ได้จากการแจ้งความ มากกว่าต้นทุนที่ต้องเสียไป เราจึงสามารถแบ่งเหตุผลที่ผู้เสียหายไม่แจ้งความเป็นสองกลุ่มใหญ่ ๆ ด้วยกัน

- ต้นทุนในการแจ้งความสูง

- **อับอาย และกลัวการถูกตีตราจากสังคม** ผู้เสียหายจำนวนมากอับอาย และความกลัวว่าคนรอบข้างจะมองว่าตนเป็นคนไม่ฉลาด สาเหตุนี้เป็นสาเหตุสำคัญที่งานศึกษาหลายชิ้นกล่าวถึง (Whitty, 2015, Cross, 2015, Parti & Tahir, 2023) Oak & Shafiq (2025) สัมภาษณ์ผู้ที่เคยตกเป็นเหยื่อของ pig-butcher scam จำนวน 26 รายจาก 5 ประเทศ และพบว่าผู้เสียหายส่วนใหญ่รู้สึกอับอายที่จะไปเล่ารายละเอียดของการถูกโกง โดยเฉพาะกรณีที่เป็น romance scam นอกจากนี้ ในการศึกษาดังกล่าว ผู้เสียหายเกือบ 1 ใน 4 ต้องการปกปิดเรื่องที่ถูกรังแกเป็นความลับเพราะไม่อยากให้คนรอบตัวรู้ Cross (2015) เปิดประเด็นที่น่าสนใจว่า งานศึกษาประเภท victimology study ที่พยายามเชื่อมโยงบุคลิกภาพของเหยื่อ (เช่น ผู้ที่ตกเป็นผู้เสียหายส่วนใหญ่มีความโลภ เชื่อคนง่าย) อาจยังทำให้ความรูสึกอับอาย (stigma) ของการเป็นเหยื่อรุนแรงขึ้น และยังส่งผลให้เหยื่อรู้สึกอับอาย ไม่กล้าแจ้งความหรือบอกคนรอบข้างขึ้นไปอีก Mason &

Benson (1996) พบว่าผู้เสียหายจากอาชญากรรมทางการเงิน (white collar crime) มีโอกาสที่จะแจ้งความเพิ่มขึ้นหากผู้เสียหายได้รับการสนับสนุนจากครอบครัว

- ไม่มีข้อมูลช่องทางการแจ้งความ หรือรู้สึกว่าการแจ้งความยุ่งยากเกินไป ผู้เสียหายหลายรายให้ความเห็นว่าระบบการแจ้งเหตุยังมีความซับซ้อนและสับสน หรือใช้เวลานาน (Cross et al., 2016, Cross, 2015, Button et al., 2013) นอกจากนี้ การที่ผู้เสียหายต้องเล่าเหตุการณ์การถูกหลอกลวงซ้ำไปซ้ำมาให้เจ้าหน้าที่ฟัง ก็เป็นอีกปัจจัยหนึ่งที่ผู้เสียหายบางส่วนเลือกที่จะไม่แจ้งความ (HM Government, 2023)
- ผลประโยชน์ที่คาดว่าจะได้รับต่ำ
 - คิดว่าการแจ้งความไม่ช่วยให้เอาเงินหรือจับกุมผู้กระทำความผิดได้ ผู้เสียหายบางส่วนไม่คิดว่าการแจ้งความจะทำให้เกิดผลใด ๆ ขึ้น (Whitty, 2015, Service statistique ministériel de la sécurité intérieure (SSMSI), 2019, Oak & Shafiq, 2025) ความคิดดังกล่าว เกิดได้จากการรับรู้ผ่านกระแสข่าวในสังคม คนใกล้ชิด หรืออาจเคยประสบด้วยตัวเอง
 - ขาดสิ่งจูงใจอื่น ๆ หากการแจ้งความยึดโยงกับการช่วยเหลือบางอย่างที่ผู้เสียหายจะได้รับ ก็เป็นไปได้ที่ผู้เสียหายจะมีแรงจูงใจที่จะแจ้งความมากขึ้น บางประเทศ เช่น การมีแนวทางการให้ผู้ให้บริการมีส่วนรับผิดชอบชัดเจน โดยมีข้อแม้ว่าผู้เสียหายต้องแจ้งความภายในเวลาที่กำหนด (Service statistique ministériel de la sécurité intérieure (SSMSI), 2019) หรือการให้ความรู้และเพิ่มมาตรการดูแลผู้ที่เคยตกเป็นเหยื่อแล้วเพื่อไม่ให้เป็นเหยื่อซ้ำอีก (HM Government, 2023)

สิ่งที่ทำได้เพิ่มเติม

การแจ้งความ มีประโยชน์ไม่เพียงแต่ต่อผู้เสียหายโดยตรงจากโอกาสที่จะตามอายัดเงินได้ทัน แต่ยังมีประโยชน์ต่อผู้อื่นที่อาจตกเป็นเหยื่อในอนาคตอีกด้วย ผ่านการเพิ่มข้อมูลบัญชีต้องสงสัยเข้าในฐานข้อมูลกลาง ในทางเศรษฐศาสตร์ กล่าวได้ว่าการแจ้งความเป็นกิจกรรมที่ส่งผลกระทบภายนอกทางบวกต่อสังคม (positive externality) ซึ่งสังคมโดยรวมจะได้ประโยชน์ถ้าผู้เสียหายแจ้งความมากขึ้น เมื่อเราย้อนกลับมาดูข้อมูล จะพบว่า หากผู้เสียหายแจ้งความภายใน 1 ชั่วโมงหลังจากที่มีการทำธุรกรรมครั้งสุดท้าย และมีการอายัดบัญชีไปเป็นทอด ๆ จะสามารถช่วยลดความเสียหายของผู้เสียหายคนอื่นได้ถึง 25% หรือกว่า 3.7 พันล้านบาท (Amarase et al., forthcoming)

สิ่งที่จะทำให้คนแจ้งความมากขึ้น ก็คือการเพิ่มประโยชน์ที่ผู้เสียหายคาดว่าจะได้รับ และลดต้นทุนในการแจ้งความ ซึ่งหมายรวมถึงการลดความสับสนและขั้นตอนของระบบการแจ้งความ การลดการบรรยาย (narrative) ในลักษณะที่เป็นการทำให้เหยื่ออับอาย หรือการยึดโยงการแจ้งความเข้ากับการดูแลคุ้มครองผู้เสียหายอื่น ๆ เป็นต้น

4.2. ระบบติดตามเส้นทางการเงิน และป้องกันการนำเงินออกนอกระบบ

หลังจากผู้เสียหายแจ้งเหตุแล้ว หน้าที่ของระบบธนาคารคือการตามเส้นทางการเงินให้ทัน ก่อนที่จะเงินจะออกไปนอกระบบธนาคาร โดยหากยังไม่มีเงินโอนออกไปจากบัญชีของมิจลาชีพ ก็จะต้องอายัดบัญชีไว้ นอกจากประโยชน์ในการพยายามยับยั้งเงินไม่ให้ออกนอกระบบแล้ว การติดตามเส้นทางการเงิน ยังเป็นการเพิ่มบัญชีที่อยู่ในเส้นทางการเงินเข้าไปในระบบ ว่าเป็นบัญชีที่ต้องสงสัย ซึ่งจะเป็นประโยชน์กับการตรวจจับธุรกรรมผิดปกติของเหยื่อ ที่ได้กล่าวถึงไปแล้วในส่วนที่ 3.3 ด้วย

การดำเนินการในช่วงที่ผ่านมา

ในอดีต หากธนาคารปลายทางที่ได้รับเงินโอนจากผู้เสียหายโดยตรงอายัดบัญชีของมิจลาชีพไว้ไม่ทัน ก็จะแจ้งกลับไปยังเจ้าหน้าที่ยืนยันว่าไม่สามารถอายัดได้ กระบวนการติดตามเส้นทางการเงินเป็นทอด ๆ จะเกิดขึ้นเฉพาะในกรณีที่เกี่ยวข้องกับการคดีฟอกเงินเท่านั้น

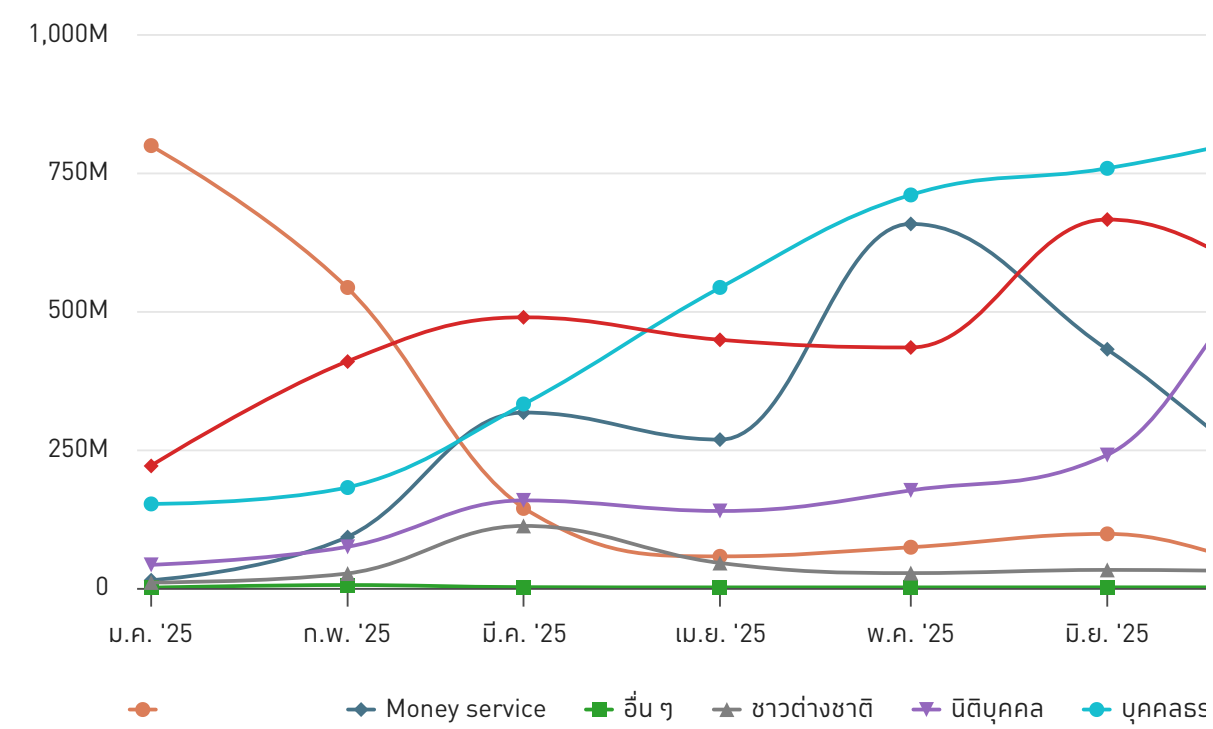
จนในปี 2023 คณะรัฐมนตรี ได้ผ่านพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ หรือที่รู้จักกันในนาม “พรก. โขเบอร์” ซึ่งกำหนดให้สถาบันการเงินและผู้ประกอบธุรกิจ มีหน้าที่ “เปิดเผยหรือแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าที่เกี่ยวข้องในระหว่างสถาบันการเงินและผู้ประกอบธุรกิจนั้นผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูล” อันนำไปสู่การพัฒนาระบบ Central Fraud Registry (CFR) ขึ้นมานั่นเอง

ระบบ CFR ทำให้การส่งต่อข้อมูลเพื่อการติดตามเส้นทางการเงินระหว่างธนาคารเป็นไปได้สะดวกขึ้น โดยเมื่อธนาคารได้รับแจ้งจากผู้เสียหายแล้ว ธนาคารก็จะตรวจสอบเส้นทางการเงินของบัญชีของมีجازชีพว่ามีเงินโอนต่อไปยังบัญชีอื่นหรือไม่ ในกรณีที่มีการโอนออกไปแล้ว ธนาคารจะนำข้อมูลธุรกรรมใส่ในระบบ CFR เพื่อให้ธนาคารปลายทางติดตามเส้นทางการเงินและระบุธุรกรรมต่อไป

สถิติและข้อสังเกต

มีجازชีพมักอาศัยจุดอ่อนของระบบธนาคารในการเชื่อมต่อข้อมูลระหว่างผู้ให้บริการทางการเงิน ตัวอย่างที่เห็นได้ชัดจนที่สุด คือช่องทางที่มีجازชีพใช้ในการนำเงินออกจากระบบธนาคาร

รูปที่ 2: ประเภทของบัญชีปลายทางเส้นทางการเงิน



หมายเหตุ: ข้อมูลจากระบบ CFR ผ่าน บช.สอท. ช่วงเดือนมกราคม-สิงหาคม 2025 สามารถอ่านรายละเอียดเพิ่มเติมได้จาก Amarase et al. (forthcoming)

รูปที่ 2 แสดงช่องทางที่มีجازชีพใช้ในการนำเอาเงินออกนอกระบบในช่วงเดือนมกราคมถึงสิงหาคม 2025 จะเห็นได้ว่า ในช่วงต้นปี การนำออกผ่านช่องทางสินทรัพย์ดิจิทัล (digital asset) เป็นช่องทางที่มีجازชีพใช้มากที่สุด ต่อมาเมื่อมีการขยายวงการต่อเส้นเงินให้รวมผู้ประกอบการสินทรัพย์ดิจิทัลแล้ว มีجازชีพก็หันมาใช้ช่องทางผู้ให้บริการ e-Money แทน และท้ายที่สุดเมื่อมีการขยายวงการต่อเส้นเงินให้ครอบคลุมผู้ให้บริการ e-Money แล้ว มีجازชีพก็หันไปใช้ช่องทางการนำเงินออกผ่านบัญชีธนาคาร ทั้งบุคคลธรรมดาและนิติบุคคล โดยอาศัยการไปถอนเงินที่สาขาธนาคาร หรือกดเงินสดจากตู้ ATM

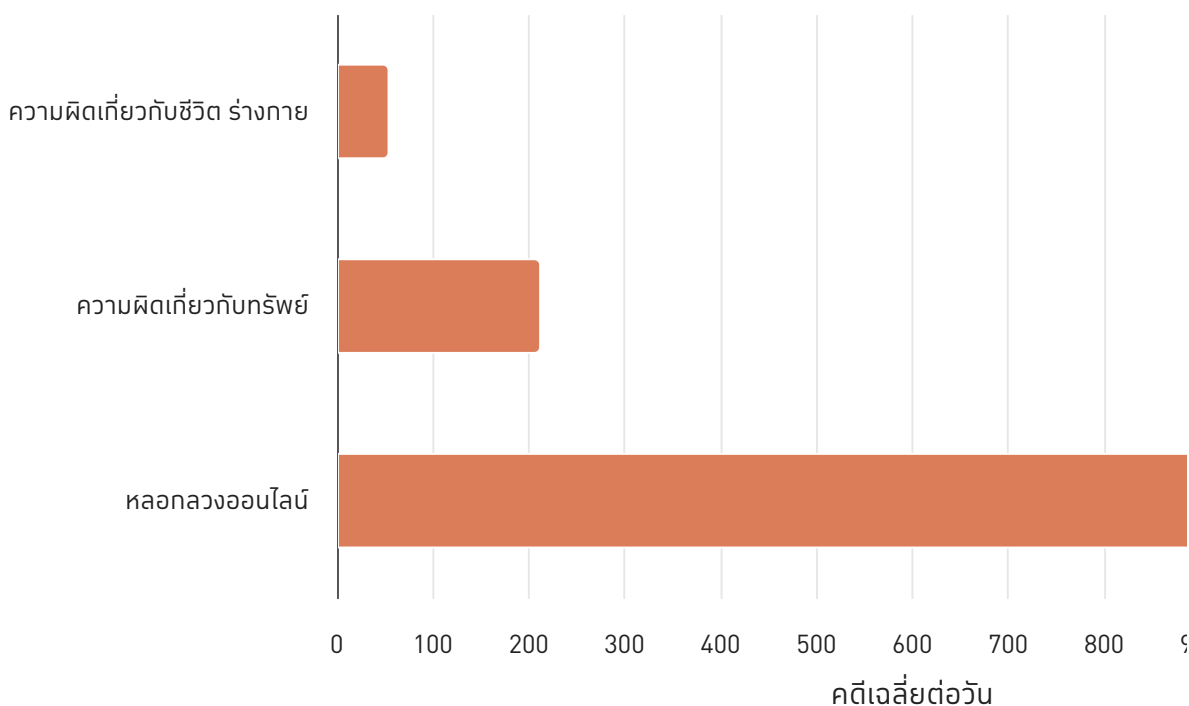
ระบบ CFR ที่ภาคการเงินพัฒนาขึ้นมาช่วยให้เกิดการต่อเส้นเงิน อันนำไปสู่การศึกษาพฤติกรรมของมีجازชีพและปรับนโยบายให้เท่าทัน กระนั้นก็ตาม ตัว CFR เองยังมีข้อจำกัดบางประการ เช่น ในการต่อเส้นเงิน ธนาคารจะเห็นเพียงธุรกรรมที่อยู่ในเส้นทางการเงินก่อนหน้า และธุรกรรมของบัญชีลูกค้าต้นเองเท่านั้น ขณะที่ระบบในบางประเทศ เช่น PayNet ของมาเลเซีย ระบบจะเปิดเผยธุรกรรมทั้งหมดของบัญชีในเส้นทางการเงินให้กับธนาคารและเจ้าหน้าที่ตำรวจโดยอัตโนมัติ

4.3. การดำเนินคดีกับผู้กระทำความผิด

นอกจากการติดตามเส้นทางเงินเพื่อป้องกันการนำเงินออกนอกประเทศแล้ว เจ้าหน้าที่ตำรวจก็ต้องสืบสวน และนำผู้กระทำความผิดมาดำเนินคดี โดยในปัจจุบัน เมื่อได้รับเรื่องร้องเรียนแล้ว แต่ละคดีความ ก็จะมีสารวัตรสืบสวนเจ้าของคดี ที่มีหน้าที่รวบรวมพยานหลักฐาน สอบปากคำ เพื่อทำหนังสืออายัด และทำสำนวนฟ้องส่งต่อไปให้อัยการต่อไป

ระบบดังกล่าวอาจจะใช้ได้ดีกับคดีอาญาในอดีต เช่น การทำร้ายร่างกาย การฉกชิงวิ่งราว แต่ภัยการเงินเป็นอาชญากรรมในรูปแบบที่ต่างออกไปมาก เนื่องจากเทคโนโลยีทำให้มีฉาชีพเข้าถึงเหยื่อได้หลาย ๆ คนพร้อม ๆ กัน นอกจากนี้ยังสามารถกระทำความผิดข้ามเขตพื้นที่ได้ เมื่อดูจากจำนวนคดีความเฉลี่ยต่อวัน จะพบว่าเมื่อเทียบกับคดีที่เป็นคดีอาญาทั่วไปแล้ว คดีหลอกลวงออนไลน์มีมากกว่าหลายเท่าตัว

รูปที่ 3: ปริมาณคดีเฉลี่ยต่อวัน แยกตามประเภทความผิด



หมายเหตุ: สถิติคดีอาญาเกี่ยวกับชีวิต ร่างกาย และเกี่ยวกับทรัพย์สิน จากกองแผนงานอาชญากรรม สำนักงานตำรวจแห่งชาติ เฉลี่ยระหว่าง 1 ต.ค. 2024 – 16 ก.ย. 2025; ข้อมูลคดีหลอกลวงออนไลน์ จาก ThaiPoliceOnline เฉลี่ยช่วงเดือน ส.ค. 2025

ในเมื่อเทคโนโลยีดิจิทัลทำให้มีฉาชีพทำงานได้รวดเร็วขึ้น ระบบกระบวนการยุติธรรมก็จำเป็นต้องปรับตัวตามโดยอาศัยเทคโนโลยีเช่นกัน ไม่ว่าจะเป็นด้วยการเชื่อมระบบของตำรวจเข้ากับระบบการชำระเงินให้ใกล้ชิดกันขึ้น (เช่นตัวอย่างของ PayNet ของมาเลเซีย) หรือใช้การวิเคราะห์เครือข่ายจากข้อมูลระดับธุรกรรม เพื่อรวบรวมคดีที่มีลักษณะเป็นเครือข่ายเดียวกันเข้ามาดำเนินการด้วยกัน

5. ประเด็นทางนโยบาย

บทความนี้ได้ชี้ให้เห็นว่าภัยการเงินเป็นปรากฏการณ์ทางเศรษฐศาสตร์ที่เกิดขึ้นในภาวะที่เหยื่อและหน่วยงานที่เกี่ยวข้องมีข้อมูลเกี่ยวกับมีฉาชีพที่ไม่สมบูรณ์ ซึ่งนอกจากจะทำให้เหยื่อได้รับความเสียหายแล้ว ยังทำให้ความเชื่อใจกันในระบบเศรษฐกิจสั่นคลอน ระบบการเงินไม่สามารถทำงานได้อย่างเต็มศักยภาพ ส่งผลให้การจัดสรรทรัพยากรขาดประสิทธิภาพ

ในสถานการณ์เช่นนี้ มาตรการจากหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้องสามารถลดความรุนแรงของปัญหาได้ ซึ่งหลักการสำคัญคือการแก้ไขปัญหาเรื่องข้อมูล โดยใช้ความรู้เกี่ยวกับภัยการเงินที่มีอยู่ทั้งหมดในระบบเศรษฐกิจให้เกิดประโยชน์สูงสุดตลอดห่วงโซ่ภัยการเงิน เพื่อให้เหยื่อ แพลตฟอร์ม ธนาคาร ผู้กำกับนโยบาย และผู้บังคับใช้กฎหมาย รู้เท่าทันมีฉาชีพมากยิ่งขึ้น ซึ่งมีประเด็นทางนโยบายที่สำคัญดังนี้

5.1. ข้อมูลที่สมบูรณ์มากขึ้นสามารถช่วยสร้างความปลอดภัยทางการเงินให้แก่ระบบเศรษฐกิจ

มาตรการต่าง ๆ ในการป้องกันและปราบปรามภัยการเงินที่มีประสิทธิผล ลดความรู้ไม่เท่าทันมีฉาชีพ ต้องมีข้อมูลที่สมบูรณ์และถูกต้อง ซึ่งเกิดจากการแลกเปลี่ยนข้อมูลกันระหว่างผู้ที่เกี่ยวข้อง และการนำข้อมูลไปใช้ให้เกิดประโยชน์สูงสุดตลอดห่วงโซ่ภัยการเงิน

การแลกเปลี่ยนข้อมูลระหว่างผู้เกี่ยวข้อง เริ่มตั้งแต่การแจ้งความโดยเหยื่อ การแลกเปลี่ยนข้อมูลระหว่างแพลตฟอร์ม ธนาคาร และตำรวจ เพื่อให้ฐานข้อมูลกลางในระบบ CFR สมบูรณ์มากยิ่งขึ้น สามารถตรวจจับภัยการเงินได้ดีขึ้น

นอกจากข้อมูลจะสามารถใช้ตรวจจับธุรกรรมฉ้อโกงได้ทันการณ์และแม่นยำมากขึ้นแล้ว ยังนำไปใช้วิเคราะห์ความเสี่ยงภัยการเงิน (risk assessment) และสร้างคะแนนความเสี่ยง (risk scoring) เพื่อใช้ในการป้องกันภัยการเงินได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ตลอดจนการประชาสัมพันธ์ให้กลภัยการเงินในรูปแบบใหม่ ๆ กลับไปให้สาธารณะชนทราบเพื่อสร้างภูมิคุ้มกันทางการเงินแก่ประชาชนให้เท่าทันเล่ห์เหลี่ยมของมีฉาชีพ

ประเด็นทางนโยบายคือ เราต้องการข้อมูลใดบ้างในการลดภัยการเงิน ใครมีข้อมูลอะไร และจะนำข้อมูลไปใช้อะไรได้บ้าง อย่างไร เพื่อให้เกิดประโยชน์สูงสุด

5.2. เทคโนโลยีที่ก้าวหน้าไปอย่างรวดเร็วทำให้รูปแบบภัยการเงินเปลี่ยนแปลงไป ด้วย กระบวนการป้องกันและปราบปรามภัยการเงินต้องปรับเปลี่ยนเพื่อให้เท่าทัน

ในด้านหนึ่งนั้น เทคโนโลยีที่ก้าวหน้าไปอย่างรวดเร็วทำให้การรู้เท่าทันมีฉาชีพทำได้ยากขึ้น นั่นคือ เทคโนโลยีทำให้ปัญหาความไม่สมมาตรของข้อมูลมีความรุนแรงมากขึ้น เทคโนโลยีสมัยใหม่ที่ก้าวหน้าไปอย่างรวดเร็วทำให้ภัยทางการเงินขยายวงกว้างมากขึ้น เร็วขึ้น ตรวจจับได้ยากขึ้น และติดตามมีฉาชีพได้ยากขึ้น กระบวนการป้องกันและปราบปรามภัยจากอาชญากรรมแบบดั้งเดิมขาดประสิทธิภาพในการจัดการกับภัยการเงินที่เกิดจาก APP บนระบบ fast payment

ในอีกด้านหนึ่งนั้น เทคโนโลยีสมัยใหม่สามารถช่วยให้ผู้เกี่ยวข้องกับภัยการเงินรู้เท่าทันมีฉาชีพได้มากขึ้น นั่นคือ เราสามารถใช้เทคโนโลยีเพื่อลดปัญหาความไม่สมมาตรของข้อมูลได้ โดยเฉพาะอย่างยิ่งการใช้เทคโนโลยีดิจิทัล เพื่อป้องกันและปราบปรามภัยการเงินที่เกิดบนแพลตฟอร์มดิจิทัลและการชำระเงินผ่านระบบ fast payment รวมถึงการใช้เทคโนโลยีในการสร้างภูมิคุ้มกันทางการเงินให้แก่ผู้ที่มีความเสี่ยง การแจ้งความที่สะดวก การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องที่รวดเร็ว การวิเคราะห์ข้อมูลการฉ้อโกงที่แม่นยำ การอายัดและถอนอายัดที่ถูกต้องมากขึ้นและผิดพลาดน้อยลง และการติดตามเส้นทางเงินของมีฉาชีพที่รวดเร็วทันการณ์

ประเด็นทางนโยบายคือ ขั้นตอนใดในห่วงโซ่ภัยการเงินที่เทคโนโลยีสามารถช่วยให้กระบวนการป้องกันและปราบปรามสามารถก้าวทันมีฉาชีพและภัยการเงินที่เปลี่ยนแปลงไปอย่างรวดเร็วได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

5.3. การแลกเปลี่ยนและการใช้ประโยชน์จากข้อมูลเพื่อลดภัยการเงินต้องอาศัยแรงจูงใจที่เหมาะสม

การดำเนินมาตรการเพื่อจัดการกับภัยการเงินต่าง ๆ ต้องได้รับความร่วมมือจากผู้เกี่ยวข้องทั้งหมดในห่วงโซ่ภัยการเงิน แต่มาตรการต่าง ๆ มีต้นทุนที่ผู้เกี่ยวข้องต้องแบกรับ การดำเนินมาตรการต่าง ๆ จึงจำเป็นต้องสร้างแรงจูงใจที่เหมาะสมให้แก่ผู้เกี่ยวข้อง เช่น แรงจูงใจให้เหยื่อแจ้งความกับตำรวจแม้ว่าโอกาสที่จะได้เงินคืนต่ำมากก็ตาม ในขณะที่แพลตฟอร์ม ธนาคาร และตำรวจ

ต้องมีแรงจูงใจในการแลกเปลี่ยนข้อมูลกันเพื่อตรวจจับและยับยั้งธุรกรรมที่ปกติ และเพื่อติดตามเส้นทางเงินและจับกุมมิฉฉาหลังธุรกรรมเกิดขึ้นแล้ว

แรงจูงใจอาจมาจากความรับผิดชอบต่อความเสียหายจากภัยการเงินที่เกิดขึ้นจากความบกพร่องของผู้ที่ได้รับมอบหมายให้ดำเนินมาตรการ แต่การกำหนดผู้ที่ต้องรับผิดชอบกับความเสียหายจากภัยการเงินก็อาจทำให้ผู้เกี่ยวข้องอื่น ๆ มีแรงจูงใจที่จะป้องกันและปราบปรามภัยการเงินน้อยลง ทำให้เกิดปัญหา moral hazard ขึ้นได้ เช่น ในกรณีที่ธนาคารเป็นผู้รับผิดชอบต่อความเสียหายทั้งหมด เหยื่อย่อมไม่มีแรงจูงใจในการป้องกันตนเองมากเท่าที่ควร ผู้บังคับใช้กฎหมายก็อาจไม่มีแรงจูงใจเพียงพอในการติดตามมิฉฉา หรือในกรณีที่เหยื่อย่อมมีแรงจูงใจต่อความเสียหายเองทั้งหมด ธนาคารอาจไม่มีแรงจูงใจในการตรวจจับธุรกรรมที่ต้องสงสัย โดยเฉพาะอย่างยิ่ง หากต้องตรวจจับโดยอาศัยข้อมูลที่ไม่สมบูรณ์ที่อาจมีข้อผิดพลาดและส่งผลกระทบต่อชื่อเสียงและผลประโยชน์ของธนาคาร

แรงจูงใจที่เหมาะสมจึงอาจมาจากความรับผิดชอบความสูญเสียร่วมกันของผู้เกี่ยวข้องทั้งหมดตลอดห่วงโซ่การเงิน (shared responsibility) โดยมีจุดประสงค์เพื่อลดปัญหา moral hazard ที่อาจเกิดขึ้นหากไม่ต้องรับผิดชอบความสูญเสีย ทำให้ภาคส่วนที่เกี่ยวข้องมีแรงจูงใจในการร่วมกันแลกเปลี่ยนข้อมูลที่ตนมี และใช้ข้อมูลที่ได้รับให้เกิดประสิทธิภาพต่อการลดภัยการเงินมากที่สุด

ประเด็นทางนโยบายที่ต้องถกเถียงกันคือ ใครควรเป็นผู้รับผิดชอบในการดำเนินมาตรการสร้างความปลอดภัยทางการเงินบ้าง ต้นทุนของมาตรการต่าง ๆ ตลอดจนความเสียหายจากภัยการเงินจะแบ่งกันรับผิดชอบอย่างไร ในสัดส่วนเท่าไร เพื่อให้เกิดแรงจูงใจที่เหมาะสมกับผู้ที่เกี่ยวข้อง

5.4. มาตรการสร้างความปลอดภัยทางการเงินที่เหมาะสมอาจไม่ใช่มาตรการที่ทำให้ภัยการเงินหมดสิ้นลงอย่างสมบูรณ์ แต่เป็นมาตรการที่สร้างสมดุลระหว่างความปลอดภัยทางการเงินกับประโยชน์จากเทคโนโลยีทางการเงิน

ในภาพรวมแล้ว จะเห็นได้ว่ามาตรการสร้างความปลอดภัยทางการเงินต่าง ๆ ล้วนมีต้นทุนต่อระบบเศรษฐกิจ ไม่เพียงแต่ทรัพยากรทางการเงินและบุคลากรจากหน่วยงานที่เกี่ยวข้องเท่านั้น แต่ยังรวมถึงความสะดวกสบาย ความรวดเร็ว ความเป็นส่วนตัว และความสามารถในการเข้าถึงบริการทางการเงินของผู้คนในระบบเศรษฐกิจ เช่น การจำกัดปริมาณและมูลค่าธุรกรรมทางการเงิน ความเข้มงวดในการตรวจสอบธุรกรรม รวมถึงการอายัดธุรกรรมหรือบัญชีที่ต้องสงสัย ย่อมสร้างความไม่สะดวกสบายให้กับผู้ใช้บริการทางการเงิน หรือ การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่างๆ ย่อมทำให้ความเป็นส่วนตัวของผู้ใช้บริการทางการเงินลดลง

มาตรการสร้างความปลอดภัยทางการเงินที่เหมาะสมจึงเป็นมาตรการที่สร้างสมดุลระหว่างความปลอดภัยทางการเงินกับประโยชน์ที่ได้จากเทคโนโลยีทางการเงิน ซึ่งจุดสมดุลนี้ย่อมแตกต่างกันไปในแต่ละสังคมว่าครัวเรือนและธุรกิจสามารถรับความเสี่ยงจากภัยการเงินได้มากน้อยเพียงใด

ประเด็นทางนโยบายคือ จุดสมดุลระหว่างความปลอดภัยทางการเงินกับประโยชน์จากเทคโนโลยีทางการเงินสำหรับประเทศไทยควรอยู่ที่ใด

เอกสารอ้างอิง

- Amarase, N., Chantararat, S., Choedpasuporn, S., Devahastin Na Ayudhya, C., Maneesilp, S., Tosborvorn, T., Treerat, N., & Yousub, W. (forthcoming). *Thailand's Fraud Landscape* [Discussion Paper]. Puey Ungphakorn Institute for Economic Research.
- Ban, T., Samuel, N., Takahashi, T., & Inoue, D. (2021). Combat Security Alert Fatigue with AI-Assisted Techniques. *Proceedings of the 14th Cyber Security Experimentation and Test Workshop*, 9–16.
- Button, M., Tapley, J., & Lewis, C. (2013). The 'fraud justice network' and the infra-structure of support for individual fraud victims in England and Wales. *Criminology & Criminal Justice*, 13(1), 37–61.
- Chugh, B., & Narang, L. (2023). *Are Fraud-awareness Campaigns Effective?*. Technical report, Dvara Research.

- Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21(2), 187–204.
- Cross, C., Smith, R. G., & Richards, K. (2016). The reporting experiences and support needs of victims of online fraud. *Trends & Issues in Crime and Criminal Justice*, 518.
- Daryanani, M. (2011). *Desensitizing the User* [Phdthesis]. University of Oxford.
- DeLiema, M., Li, Y., & Mottola, G. (2023). Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type. *International Journal of Consumer Studies*, 47(3), 1042–1059.
- Ehrlich, I. (1996). Crime, Punishment, and the Market for Offenses. *Journal of Economic Perspectives*, 10(1), 43–67.
- Fagan, J., & Freeman, R. B. (1999). Crime and Work. *Crime and Justice*, 25, 225–290.
- FINRA Investor Education Foundation. (2007). *Senior Fraud Risk Survey*. FINRA Investor Education Foundation.
- Fitrah, M. S., Ramadhani, S., & Syakir, A. (2025). The Vulnerability Level of University Students Using Digital Banking Services to Phishing Banking Attacks. *Journal of Social Commerce*, 5(2), 157–166.
- Grogger, J. (1991). Certainty vs. Severity of Punishment. *Economic Inquiry*, 29(2), 297–309.
- Hanoch, Y., & Wood, S. (2021). The Scams Among Us: Who Falls Prey and Why. *Current Directions in Psychological Science*, 30(3), 260–266.
- Hapipat, T. (2024). การศึกษาสถานการณ์การถูกหลอกลวงผ่านช่องทางออนไลน์: กรณีศึกษาประชาชนอายุ 15-79 ปีไปทั่วทุกภูมิภาคของประเทศ. Chulalongkorn University, Faculty of Economics.
- HM Government. (2023). *Fraud Strategy: Stopping Scams and Protecting the Public*. HM Government.
- Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66, 75–87.
- Kubilay, E., Raiber, E., Spantig, L., Cahliková, J., & Kaaria, L. (2023). *Financial fraud in developing countries: Common scam detection tips do not help distinguish scam from non-scam messages*. ECONtribute Policy Brief.
- Liu, X. F., Ai, Y., Jiang, L. C., Wang, X., & Wu, Y. (2025). Understanding the human element in scams: a multidisciplinary approach. *Journal of Information Technology Case and Application Research*, 27(1), 9–24.
- Lu, H. Y., Chan, S., Chai, W., Lau, S. M., & Khader, M. (2020). Examining the influence of emotional arousal and scam preventive messaging on susceptibility to scams. *Crime Prevention and Community Safety*, 22(4), 313–330.
- Malkin, N., Mathur, A., Harbach, M., & Egelman, S. (2017). Personalized security messaging: Nudges for compliance with browser warnings. *2nd European Workshop on Usable Security*.
- Mason, K. A., & Benson, M. L. (1996). The effect of social support on fraud victims' reporting behavior: A research note. *Justice Quarterly*, 13(3), 511–524.
- Nagin, D. S. (2013). Deterrence in the Twenty-First Century. *Crime and Justice*, 42(1), 199–263.
- Oak, R., & Shafiq, Z. (2025). *"Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams*.
- Parti, K., & Tahir, F. (2023). "If We Don't Listen to Them, We Make Them Lose More than Money:" Exploring Reasons for Underreporting and the Needs of Older Scam Victims. *Social Sciences*, 12(5), 264.
- Paternoster, R. (1987). The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues. *Justice Quarterly*, 4(2), 173–217.
- PayNXT360. (2025). *Thailand Social Commerce Market Intelligence and Future Growth Dynamics Databook - 50+ KPIs on Social Commerce Trends by End-Use Sectors, Operational KPIs, Retail Product Dynamics, and Consumer Demographics - Q2 2025 Update*. ResearchAndMarkets.com.
- Piehl, A. M. (1998). Economic Conditions, Work, and Crime. In M. Tonry (Ed.), *The Handbook of Crime & Punishment*. Oxford University Press.

- Roy, S. S., Torres, C., & Nilizadeh, S. (2025). *“Explain, Don’t Just Warn!” – A Real-Time Framework for Generating Phishing Warnings with Contextual Cues.*
- Salathong, J., Silanoi, W., Kankaew, J., & Rattanapong, S. (2024). *เสียงของผู้เสียหายจากอาชญากรรมออนไลน์สู่ข้อเสนอแนะในการรับมือ และสร้างการรู้เท่าทัน.* Chulalongkorn University, Faculty of Economics.
- Service statistique ministériel de la sécurité intérieure (SSMSI). (2019). *Enquête « Cadre de vie et sécurité » (CVS) 2018.* Institut national de la statistique et des études économiques (INSEE).
- Smith, R. G. (2007). Consumer scams in Australia: an overview. *Trends & Issues in Crime and Criminal Justice*, 331.
- Tosborvorn, T., Treeratpituk, P., Wasi, N., & Laimek, R. (2023). *เจาะลึกพฤติกรรมการใช้ e-Payment ของคนไทย (aBRIDGED NaN/2023).* Puey Ungphakorn Institute for Economic Research.
- U.S. Attorney’s Office, Western District of Washington. (2025). *Financial Fraud Crime Victims.* U.S. Department of Justice.
- Vititanon, N. (2024). *SMS ลวงหลอก: ภัยคุกคามออนไลน์กับมาตรการในต่างประเทศ.* Chulalongkorn University, Faculty of Economics. [ฉันทนา%20SMS%20ลวงหลอก-final.pdf](#)
- Waldo, G. P., & Chiricos, T. G. (1972). Perceived Penal Sanction and Self-Reported Criminality: A Neglected Approach to Deterrence Research*. *Social Problems*, 19(4), 522–540.
- Wen, X., Xu, L., Wang, J., Gao, Y., Shi, J., Zhao, K., Tao, F., & Qian, X. (2022). Mental States: A Key Point in Scam Compliance and Warning Compliance in Real Life. *International Journal of Environmental Research and Public Health*, 19(14).
- Whitley, E. A., & Pujadas, R. (2018). *Report on a study of how consumers currently consent to share their financial data with a third party.* Financial Conduct Authority.
- Whitty, Monica T. (2015). Mass-Marketing Fraud: A Growing Concern. *IEEE Security & Privacy*, 13(4), 84–87.
- Whitty, Monica Therese. (2020). Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims. *European Journal on Criminal Policy and Research*, 26(3), 399–409.
- World Bank Group. (2023). *Fraud Risks in Fast Payments* [Focus Note]. The World Bank.

1. เกมทายบอลได้ถ้วย คือการหลอกลวงที่ผู้แสดงจะสลับถ้วยหรือภาชนะอื่น เช่น เปลือกหอย สามใบ ใบหนึ่งครอบลูกบอลอยู่ แล้วให้คนดูทายว่าลูกบอลอยู่ในถ้วยใบไหน มีโดยมี “หนาม้า” มาแสดงเป็นคนที่ทายแล้วถูก เพื่อชักชวนให้เหยื่อลงเงินพนัน
2. ตัวอย่างเช่น รายงานของ [FINRA Investor Education Foundation \(2007\)](#) พบว่า จากการสอบถามผู้เสียหายที่มีรายชื่ออยู่ในรายชื่อผู้เสียหายจากการถูกหลอกลวงทุนของเจ้าหน้าที่ตำรวจ มีเพียงครึ่งหนึ่งที่ยอมรับว่าตนเองถูกหลอก
3. ในช่วงก่อนหน้านี้นี้ เทคนิคการหลอกลวงที่พบเห็นได้มาก คือการทำ SMS phishing หรือที่เรียกว่า smishing คือ การสวมรอยเป็นบุคคลอื่น เช่น ธนาคาร บริษัทขนส่ง หน่วยงานรัฐ ส่งข้อความ SMS หาเหยื่อ เพื่อให้เหยื่อคลิกไปยังเว็บไซต์ปลอม เพื่อหลอกเอาข้อมูลหรือรหัสผ่าน หรือให้เหยื่อลงแอปพลิเคชันของมิจฉาชีพ อันจะนำไปสู่การหลอกลวงแบบ unauthorized fraud แต่มาตรการต่าง ๆ ของทั้งภาครัฐและเอกชน ก็ช่วยป้องกันปัญหาดังกล่าวได้มาก (สำหรับภาพรวมของปัญหา SMS phishing อ่านเพิ่มเติมได้ที่ [Vititanon \(2024\)](#)) กระนั้น การหลอกลวงผ่านการโทรศัพท์ หรือที่เรียกกันติดปากว่า “call center” ก็ยังมีให้เห็นอยู่



จิติ ทศบวร
สถาบันวิจัยเศรษฐกิจป๋วย อึ๊งภากรณ์



นฤกุลเลิศ สัมพันธรักษ์
University of California San Diego

ข้อคิดเห็นที่ปรากฏในบทความนี้เป็นความเห็นของผู้เขียน ซึ่งไม่จำเป็นต้องสอดคล้องกับความเห็นของสถาบันวิจัยเศรษฐกิจป๋วย อึ๊งภากรณ์