101PUB
POLICY
INSIGHTS

ปราบมิจฯ ให้อยู่หมัด ต้องมอบหน้าที่ให้ธุรกิจร่วมรับผิดชอบ

กัลป์ กรุยรุ่งโรจน์

Highlights

- มิจฉาชีพปรับตัวหลบเลี่ยงมาตรการของรัฐอยู่เสมอ ส่งผลให้มาตรการที่ภาครัฐใช้อยู่ในปัจจุบัน (กฎหมายลงโทษผู้เกี่ยวข้อง อายัดบัญชีม้าชิมผี ให้ความรู้ประชาชน) ไม่เพียงพอป้องกันการหลอกลวงออนไลน์

- ในต่างประเทศจึงมอบหน้าที่ให้เอกชนช่วยป้องกันไม่ให้ประชาชนถูกหลอกลวง โดย 1. ให้เอกชนเป็นผู้ป้องกันหน้างาน 2. ให้เอกชนร่วมป้องกันทั้งต้นน้ำและปลายน้ำ 3. มีกลไกความรับผิดชอบหากเอกชนไม่ทำหน้าที่ป้องกัน

- ประเทศออสเตรเลียเป็นประเทศตัวอย่างที่ดึง ค่ายมือถือ-บริษัทแพลตฟอร์ม-สถาบันการเงิน มาป้องกันไม่ให้ประชาชนถูกหลอกลวงให้โอนเงิน ในขณะที่ประเทศสิงคโปร์เป็นประเทศตัวอย่างที่ดึงค่ายมือถือ-สถาบันการเงิน มาช่วงป้องกันไม่ให้ประชาชนถูกโกงจากแอปพลิเคชั่นดูดเงิน

ฉบับที่ 57
พฤศจิกายน 2024


ที่มา: Freepik

ทุกวันนี้มีข่าวคนไทยถูกมิจฉาชีพหลอกกันแทบไม่เว้นวัน ทั้งโดนหลอกให้ลงทุนในสินทรัพย์ที่ไม่มีอยู่จริงบ้าง ถูกแก๊งคอลเซ็นเตอร์หลอกบ้าง โดนหลอกให้ลงแอปดูดเงินบ้าง หรือกระทั่งโดนหลอกให้ลงเงินกับธุรกิจเครือข่ายอย่างกรณีดิไอคอนบ้าง จนแทบจะเรียกได้ว่า ‘การโดนหลอก’ กลายเป็น ‘นิวนอร์มอล’ ของคนไทยไปแล้ว

หลายคนจึงเกิดคำถามว่า “ทำไมคนไทยถึงถูกหลอกง่ายขนาดนี้” บางคนชี้ว่าก็เพราะคนไทยนั้นไร้เดียงสาขาดความรู้เชื่อคนง่าย (เพราะฉะนั้นรัฐควรต้องเร่งให้ความรู้ประชาชน) ส่วนบางคนชี้ว่าก็เพราะคนไทยนั้นมีกิเลส โลภ โดนมิจฉาชีพล่อลวงหน่อยก็ติดกับแล้ว

ในขณะที่บางคนอาจขยับไปมองอีกมุมหนึ่งและตั้งคำถามว่า หรือรัฐไทยยังจัดการมิจฉาชีพไม่ดีพอ?

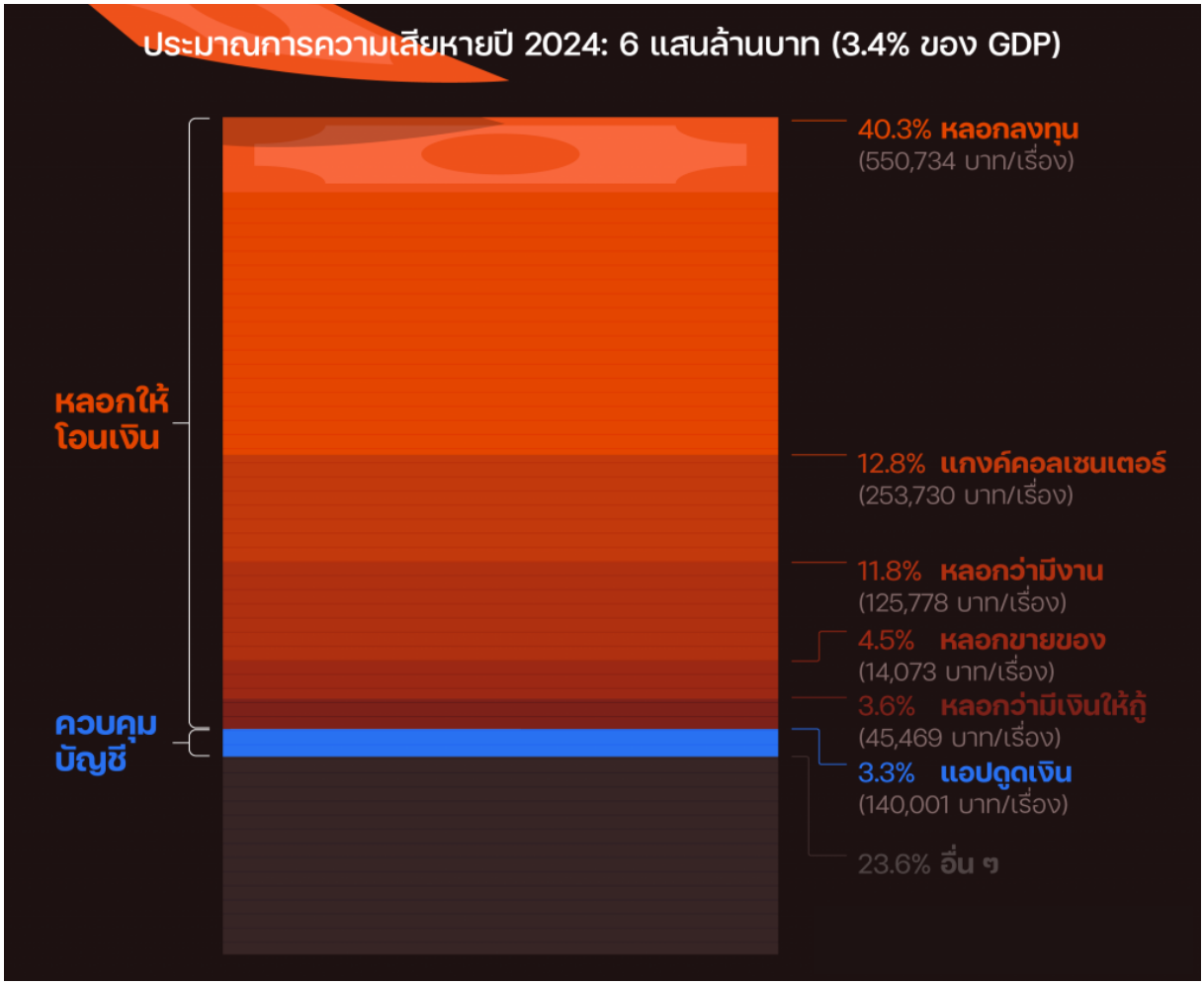
101 PUB ชวนผู้อ่านทุกท่านไปสำรวจว่าประเทศอื่นนั้นมีมาตรการจัดการกับมิจฉาชีพออนไลน์อย่างไร? เพื่อชี้ให้เห็นว่าสถานการณ์การระบาดของการหลอกลวงนั้นไม่ได้ขึ้นอยู่กับคุณสมบัติของคนในชาติเพียงอย่างเดียว แต่ที่สำคัญคือขึ้นกับระบบการป้องกันด้วย

บทความนี้เริ่มต้นจากการอธิบายให้เห็นวิธีการหลอกลวงของมิจฉาชีพ ตามมาด้วยการพูดถึงแนวทางการจัดการของรัฐไทย และสุดท้ายจะพาไปสำรวจแนวทางที่หลายประเทศใช้เพื่อยกระดับการป้องกันการหลอกลวงออนไลน์

ประเทศไทยเสียหาย จากการถูกหลอกลวง ออนไลน์แค่ไหน?

ข้อมูลการสำรวจสถานการณ์การโกงออนไลน์ในไทยปี 2024 ประมาณการว่า คนไทยสูญเสียจากการถูกหลอกลวงออนไลน์เกือบ 600,000 ล้านบาท คิดเป็นประมาณ 3.4% ของ GDP[1] สัดส่วนความเสียหายนี้นับว่าสูงเป็นอันดับต้นๆ ของโลก โดยอาจมีคนไทยมากถึงราว 18-20 ล้านคนที่เคยสูญเสียทรัพย์สินจากการถูกหลอกลวงทางออนไลน์[2]

ความสูญเสียที่เกิดขึ้นเกิดจากการหลอกลงทุนมากที่สุด คิดเป็น 40.3% ของมูลค่าความ



ที่มา
สำนักงานตำรวจแห่งชาติ (3 มี.ค. 2567); GASA (2024)

เสียหาย ตามสถิติการแจ้งความออนไลน์สำนักงานตำรวจแห่งชาติ รองลงมาคือการหลอกลวงด้วยการข่มขู่ (แก๊งคอลเซ็นเตอร์) คิดเป็น 12.8% ของมูลค่าความเสียหาย อันดับสามคือการหลอกลวงให้โอนเงินเพื่อทำงาน คิดเป็น 11.8% ของมูลค่าความเสียหาย อันดับสี่คือการหลอกขายของคิดเป็น 4.5% ของมูลค่าความเสียหาย[3]

มิจฉาชีพในไทยมีกลยุทธ์ในการหลอกลวงเอาเงินจากเหยื่ออย่างไร?

ถึงแม้ว่ามิจฉาชีพจะมีวิธีการสารพัดเพื่อหลอกลวงดูดเอาเงินจากเหยื่อ แต่เมื่อพิจารณาจากแนวทางการหลอกลวงแล้วสามารถแบ่งออกมาได้เป็น 2 ประเภทหลักๆ คือ การหลอกลวงให้เหยื่อโอนเงิน (Authorized Push Payment – APP Scam) กับการหลอกลวงยึดบัญชีเหยื่อ (Account Takeover – ATO scam)


ที่มา: Freepik

หลอกลวงให้เหยื่อโอนเงิน (APP Scam)

ด้วยวิธีการนี้ มิจฉาชีพจะเกลี้ยกล่อมจูงใจเหยื่อด้วยข้อมูลอันเป็นเท็จ เพื่อให้ตัวเหยื่อโอนเงินไปที่บัญชีของมิจฉาชีพเอง หรือมอบข้อมูลส่วนบุคคลที่มิจฉาชีพสามารถนำไปใช้ประโยชน์ได้ในอนาคต[4] เช่น การเปิดบัญชีหรือซิมโทรศัพท์เพื่อใช้ในการหลอกลวงผู้อื่น เป็นต้น มิจฉาชีพต้องอาศัยกลยุทธ์การหลอกลวงที่สอดคล้องกับบริบทความต้องการของคนในสังคม โดยมีแนวทางในการหลอกลวงหลัก ดังนี้[5]

การหลอกลงทุน: มิจฉาชีพจะชักชวนเหยื่อผ่านการโฆษณาผลิตภัณฑ์การลงทุนที่สัญญาว่าจะให้ผลตอบแทนสูง เช่น หุ้น คริปโตฯ ทองคำ สกุลเงินต่างประเทศ ฯลฯ ผ่านโซเชียลมีเดียหรือ SMS[6] เมื่อเหยื่อสนใจลงทุน มิจฉาชีพจะติดต่อเข้าไปพูดคุยกับเหยื่อโดยทำให้รู้สึก ‘โลภ’ และ ‘เชื่อใจ’ มากขึ้น เช่น ดึงเข้ากลุ่มไลน์ที่มีกูรูสอนให้ลงทุนพร้อมให้ข้อมูลวงใน[7] ในช่วงแรกๆ เหยื่อจะระวังตัวและลงทุนในจำนวนเงินน้อยๆ ในขั้นตอนนี้มิจฉาชีพก็จะมอบผลตอบแทนให้ตามที่โฆษณาไว้ เพื่อจูงใจให้เหยื่อลงทุนเพิ่มขึ้น แต่เมื่อเหยื่อลงเงินก้อนใหญ่แล้ว มิจฉาชีพจะหลบหนีหายไปพร้อมกับเงินของผู้ลงทุน

การข่มขู่: มิจฉาชีพมักจะติดต่อเหยื่อผ่านการโทรหาโดยตรง แล้วอ้างตัวว่าเป็นเจ้าหน้าที่ เช่น ตำรวจ เจ้าหน้าที่การประปา เจ้าหน้าที่ธนาคาร เพื่อแจ้งว่าเหยื่อมีความผิดบางอย่าง[8] อาทิ มีชื่อในขบวนการฟอกเงิน เมื่อเหยื่อเกิดความ ‘กลัว’ แล้ว มิจฉาชีพก็จะเสนอความช่วยเหลือให้ โดยให้เหยื่อโอนเงินเข้าบัญชีของเจ้าหน้าที่ (ปลอม) เพื่อดำเนินการตรวจสอบที่มาทางการเงินและรับรองความบริสุทธิ์ให้ ซึ่งเมื่อเหยื่อโอนเงินให้แล้วมิจฉาชีพจะตัดการติดต่อทันที

หลอกว่ามีงานให้ทำ: มิจฉาชีพชักชวนเหยื่อด้วยการโฆษณารับสมัครงานรายได้ดีผ่านช่องทางโซเชียลมีเดีย โดยมิจฉาชีพจะหลอกให้เหยื่อมีความ ‘หวัง’ ที่จะมีรายได้ด้วยการมอบภารกิจให้ทำ โดยเริ่มจากทำงานง่าย ๆ เช่น กดไลก์โปรโมตเพจ ตามมาด้วยการให้ช่วยกดสั่งซื้อสินค้าจำนวนน้อย ๆ เพื่อกระตุ้นยอดขายแล้วมิจฉาชีพจะให้เงินคืน แต่เงินที่เหยื่อได้รับคืนจะไม่สามารถถอนออกมาได้จนกว่าจะโปรโมตได้ตามเป้า เพื่อหลอกล่อให้เหยื่อโอนเงินซื้อสินค้ามาก ๆ

หลอกว่ามีเงินให้กู้: มิจฉาชีพโฆษณาตามช่องทางโซเชียลมีเดียเชิญชวนให้คนมากู้เงิน เมื่อเหยื่อสมัครเพื่อขอกู้เงิน มิจฉาชีพจะติดต่อเหยื่อในช่องทางส่วนตัวเพื่อแจ้งให้โอนค่าธรรมเนียม ค่ามัดจำ หรือค่าปลดล็อกเพื่อให้กู้ได้มากขึ้น ซึ่ง

ต่อให้เหยื่อโอนเงินค่าดำเนินการเหล่านี้ไปก็ไม่ได้รับเงินกู้อยู่ดี

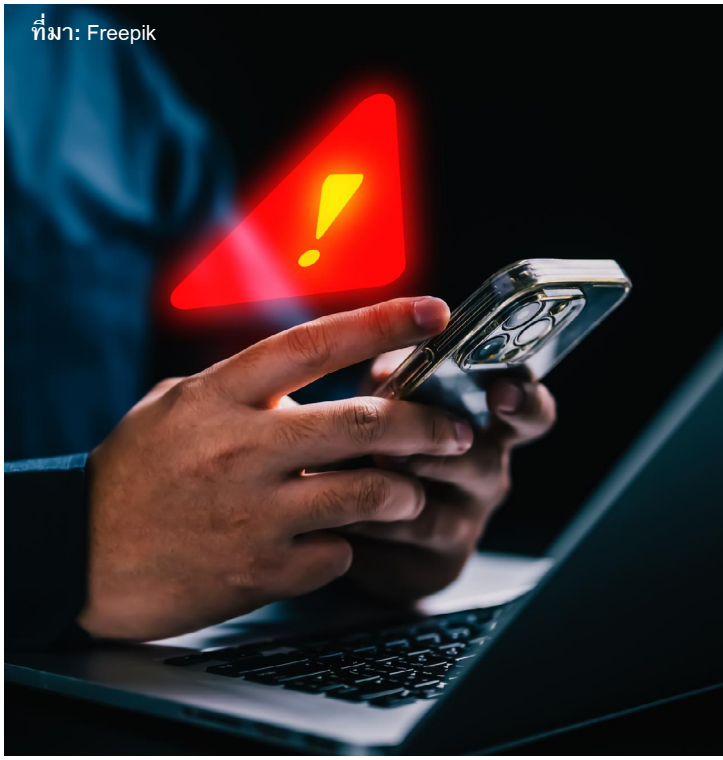
โดยสรุปแล้ว การหลอกให้เหยื่อโอนเงินเริ่มต้นจากการที่มิจฉาชีพเข้าถึงเหยื่อด้วยการโทรหาเหยื่อโดยตรง ส่งข้อความ SMS หรือประกาศชักชวนในช่องทางโซเชียลมีเดีย โดยให้ข้อเสนอต่างๆ ที่ทำให้ ‘อารมณ์’ ครอบงำ ทั้งอาจสับสน กลัว หรือโลภ แล้วบีบให้เหยื่อโอนเงินเข้าบัญชีของมิจฉาชีพ

การหลอกลวงให้โอนเงินเป็นอาชญากรรมทางออนไลน์ที่ภาครัฐต้องให้ความสำคัญเนื่องจากสร้างความเสียหายมหาศาล โดยการหลอกลวง 4 ประเภทที่ยกตัวอย่างไปสร้างความเสียหายรวมกันเกือบ 70% ของมูลค่าความเสียหายที่เกิดจากการหลอกลวงออนไลน์ทั้งหมด การจะยับยั้งไม่ให้ประชาชนถูกหลอกให้โอนเงินจำเป็นต้องหาวิธีที่จะช่วยเตือนในหลายขั้นตอน เพื่อไม่ให้ประชาชนถูกหลอกลวงได้ง่าย

การหลอกลวงยึดบัญชีเหยื่อ (ATO Scam)

ในวิธีการนี้ มิจฉาชีพจะหาวิธีการเจาะระบบออนไลน์ของธนาคาร เพื่อเข้าไปควบคุมบัญชีของเหยื่อ ก่อนที่จะทำธุรกรรมโอนเงินออกจากบัญชีเหยื่อเข้าบัญชีของมิจฉาชีพ โดยกระบวนการในต่างประเทศมักเริ่มต้นจากการที่มิจฉาชีพจะหาข้อมูลบัญชีและรหัสผ่านของเหยื่อในที่ซื้อขายกันในเว็บเถื่อน ก่อนที่จะใช้ข้อมูลดังกล่าวเป็นจุดตั้งต้นเพื่อแฮ็กระบบธนาคาร (อาจจะใช้ bot ร่วมด้วย) เพื่อทำให้เกิดธุรกรรม[9]

ในกรณีของประเทศไทย แอปดูดเงินคือประเภทการหลอกลวงแบบยึดบัญชีเหยื่อ โดยมิจฉาชีพมักจะใช้วิธีการส่งลิงก์ให้เหยื่อผ่าน SMS และหลอกให้เหยื่อโหลดแอปพลิเคชันปลอม[10] เมื่อเหยื่อติดตั้งแอปพลิเคชันแล้วจะต้องลงทะเบียนด้วยการกรอกข้อมูลส่วนบุคคล ตั้งค่ารหัสผ่าน 6 หลัก (PIN) รวมถึงให้สแกนใบหน้า ส่งผลให้มิจฉาชีพซึ่งเป็นเจ้าของแอปพลิเคชันปลอมนี้ได้ข้อมูลส่วนบุคคลสำคัญทั้งหมดสำหรับการทำธุรกรรมทางการเงิน รวมถึงมีวิดีโอบันทึกภาพใบหน้าเพื่อใช้ปลดล็อกแอปพลิเคชันด้วย[11] นอกจากนี้ แอปพลิเคชันปลอมเหล่านี้จริงๆ แล้วเป็นแอปพลิเคชันสำหรับการควบคุมมือถือทางไกล ส่งผลให้มิจฉาชีพสามารถเข้าควบคุมมือถือของเหยื่อได้ทันทีหลังลงทะเบียนเสร็จ ซึ่งมิจฉาชีพก็จะใช้ข้อมูลส่วนบุคคลที่ได้มาจากเหยื่อทำธุรกรรมโอนเงินออกจากบัญชีของเหยื่อเข้าบัญชีที่มิจฉาชีพจัดเตรียมไว้


ที่มา: Freepik

จากกระบวนการทั้งหมดจะเห็นได้ว่า การหลอกลวงประเภท ‘แอปฯ ดูดเงิน’ นั้นแตกต่างจากการหลอกลวงประเภทอื่น กล่าวคือ ธุรกรรมที่เกิดขึ้นไม่ได้เกิดจากการที่เหยื่อโอนเงินให้มิจฉาชีพด้วยตัวเอง แต่เกิดจากการที่มิจฉาชีพอาศัยช่องว่างของระบบธุรกรรมออนไลน์เข้ามาฉวยเงินออกจากบัญชีของเหยื่อ[12]

ในการรับมือกับการหลอกลวงประเภทแอปฯ ดูดเงิน ผู้ที่เกี่ยวข้องจำเป็นต้องทำให้ระบบการทำธุรกรรมออนไลน์มีความปลอดภัยมากขึ้น ปิดช่องโหว่ต่างๆ ที่อาจทำให้มิจฉาชีพใช้ประโยชน์ขโมยเงินจากเหยื่อได้

รัฐบาลไทยจัดการการหลอกลวงออนไลน์อย่างไร?

ที่ผ่านมาภาครัฐมองเห็นว่าการหลอกลวงออนไลน์เป็นปัญหาสำคัญและได้ผลักดันมาตรการต่างๆ เพื่อยับยั้งป้องกันไม่ให้คนไทยถูกหลอกลวงออนไลน์ โดยสามารถแบ่งออกเป็น 3 แนวทางหลัก

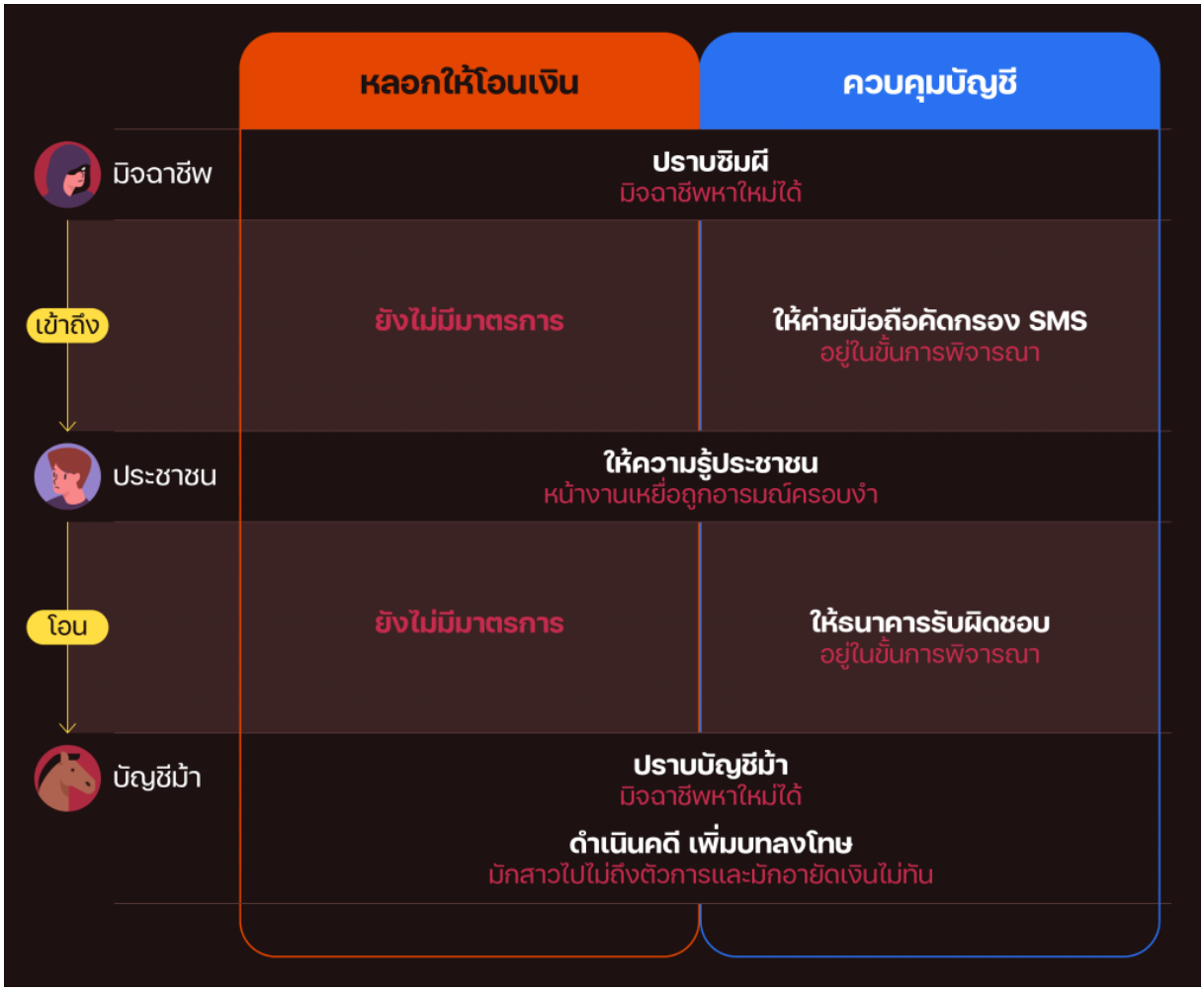
มาตรการปราบปรามผู้ที่มีส่วนเกี่ยวข้องกับการก่ออาชญากรรม

ในปี 2023 รัฐบาลไทยได้ผลักดันกฎหมายเพิ่มอำนาจให้ตำรวจจัดการกับอาชญากรรมออนไลน์ โดยกำหนดโทษผู้ที่มีส่วนเกี่ยวข้อง และกำหนดให้ภาคธุรกิจต้องเปิดเผยข้อมูลกับเจ้าหน้าที่รัฐ เพื่อระงับเหตุได้ทันท่วงที[13]

ถึงแม้ว่าทางเจ้าหน้าที่จะมีอำนาจในการดำเนินการมากขึ้น แต่การตามจับมิจฉาชีพหลังก่อเหตุนั้นมีข้อจำกัดอย่างมาก เนื่องจากมิจฉาชีพที่หลอกลวงประชาชนจำนวนมากมีฐานปฏิบัติการในต่างประเทศ[14] ซึ่งอยู่นอกขอบเขตอำนาจของรัฐบาลไทย นอกจากนี้ มิจฉาชีพมักใช้บัญชีที่จดทะเบียนในชื่อผู้อื่น (บัญชีม้า) เป็นบัญชีรับเงิน[15] ส่งผลให้เจ้าหน้าที่มักสาวไปไม่ถึงตัวการก่อเหตุ

ยิ่งไปกว่านั้น ต่อให้เจ้าหน้าที่จับมิจฉาชีพได้ ก็ไม่สามารถนำเงินที่หลอกลวงคืนกลับมาได้ เนื่องจากมิจฉาชีพจะโอนเงินที่หลอกมาได้ออกจากบัญชีม้ากระจายไปหลายบัญชีและโอนออกต่อเนื่องเป็นทอดๆ ภายในเพียงไม่กี่นาที[16] ที่ผ่านมาจึงสามารถอายัดคืนได้เพียง 15% ของจำนวนที่แจ้งอายัดเท่านั้น[17]

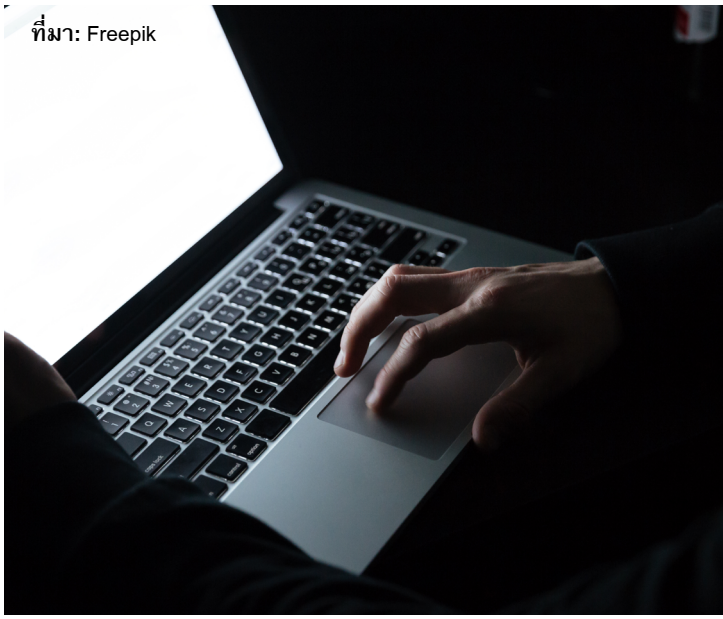

ที่มา: AFP



มาตรการปราบปรามซิมผีและบัญชีม้า

โดยปกติแล้ว มิจฉาชีพมักหลีกเลี่ยงการถูกจับกุมด้วยการใช้เบอร์และบัญชีธนาคารที่ลงทะเบียนในชื่อผู้อื่น (ซิมผีและบัญชีม้า) ในการโจรกรรม ภาครัฐจึงมองว่าการปราบปรามซิมผีและบัญชีม้าจะมีผลทำให้มิจฉาชีพทำงานยากมากขึ้น และคาดว่าการหลอกลวงจะลดน้อยลง

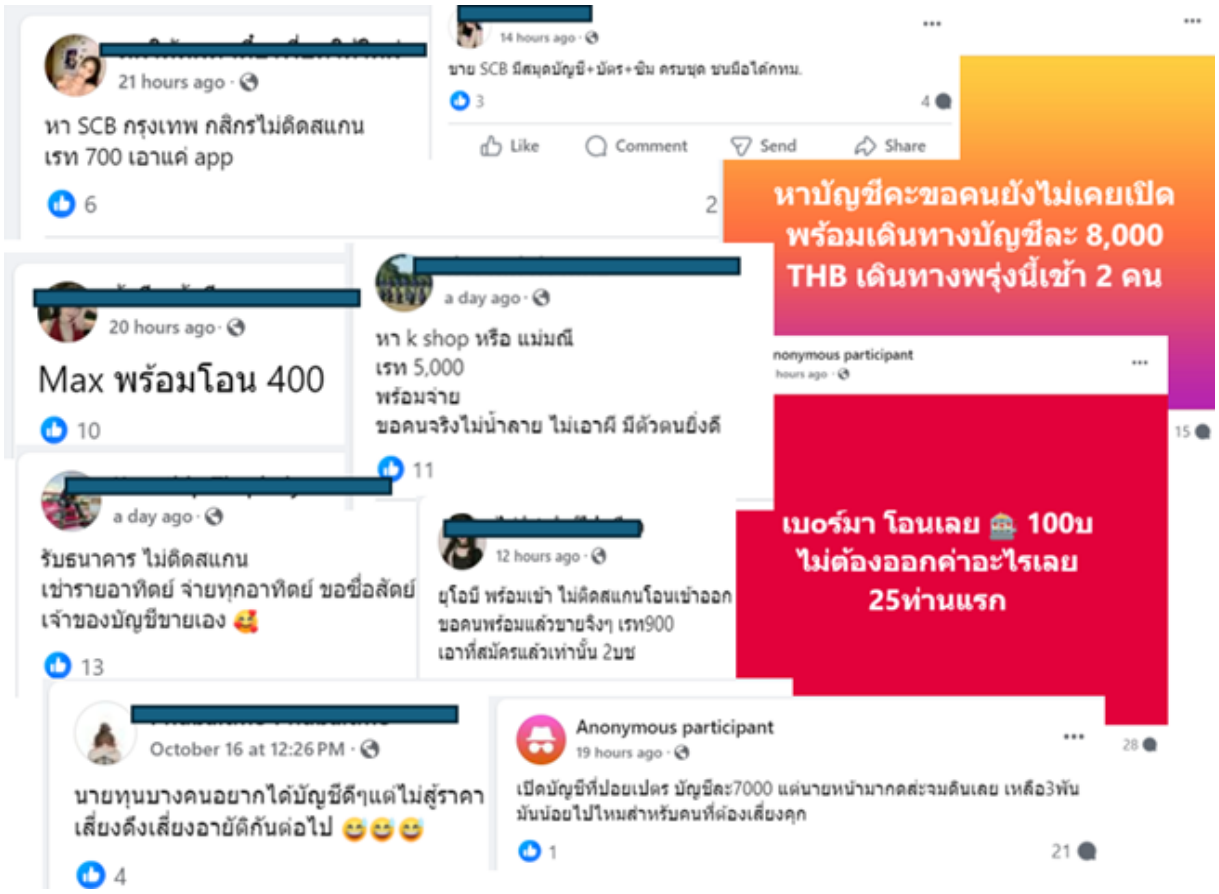
ในการปราบปรามซิมผีนั้น ภาครัฐสามารถอายัดหมายเลขโทรศัพท์รวมกันได้ประมาณ 2.9 ล้านหมายเลข[18] จากซิมของผู้ที่ครอบครองซิมมือถือตั้งแต่ 6 ซิมขึ้นไปแล้วไม่ได้ไปยืนยัน


ที่มา: Freepik

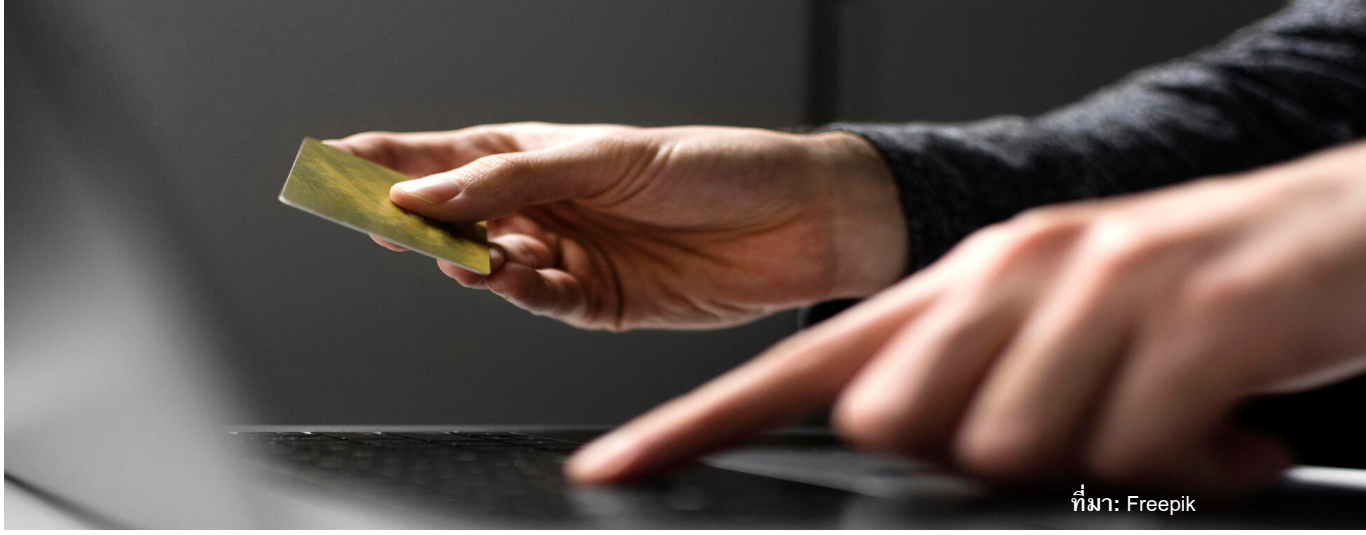
ตัวตน[19] ซิมที่โทรออกเกิน 100 ครั้งต่อวัน และซิมของผู้ที่มีชื่อลงทะเบียนซิมไม่ตรงกับชื่อในบัญชี Mobile Banking

ส่วนการปราบปรามบัญชีม้านั้น ในปัจจุบันภาครัฐสามารถระงับการทำธุรกรรมออนไลน์ของบัญชีม้าได้กว่า 1 ล้านบัญชี[20] โดยให้ธนาคารพาณิชย์ต้องระงับการทำธุรกรรมออนไลน์ของบุคคลที่มีรายชื่อในฐานข้อมูล[21] ของสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) และ Central Fraud Register (CFR)[22] รวมทั้งให้ธนาคารพาณิชย์สร้างมาตรฐานร่วมกันในตรวจจับบัญชีต้องสงสัย

อย่างไรก็ตาม ถึงแม้ว่าการปราบปรามบัญชีม้าและซิมผีจะทำให้มิจฉาชีพทำงานได้ยากขึ้น แต่มิจฉาชีพเองก็สามารถปรับตัวหาเครื่องมืออันใหม่มาทดแทน ทั้งการหาซื้อบัญชีม้าและซิมผีทางอินเทอร์เน็ต[23] หันไปเข้าถึงเหยื่อผ่านช่องทางออนไลน์แทนการโทร หรือหันไปใช้กระเป๋าเงินดิจิทัลรับเงินแทนการใช้บัญชีม้า[24] การปราบปรามจึงไม่สามารถทำให้มิจฉาชีพหมดไปได้



ตัวอย่างการซื้อขายบัญชีม้า ซิมผี รวมถึงกระเป๋าเงินดิจิทัล ในกลุ่มเฟสบุ๊ก (สืบค้นวันที่ 24 ตุลาคม 2024)



ที่มา: Freepik

มาตรการสร้างภูมิคุ้มกันให้ประชาชน

ในเชิงอุดมคติ หากประชาชนมีความรู้คอยระวังตัวตลอดเวลา ไม่เชื่อคนง่าย ไม่รีบโอนเงิน มิจฉาชีพก็คงจะไม่สามารถหลอกเอาเงินจากเหยื่อได้ รัฐบาลจึงให้ความสำคัญกับการเผยแพร่ความรู้เพื่อสร้างภูมิคุ้มกันให้ประชาชน โดยได้จัดทำฐานข้อมูลความรู้ของทางราชการเพื่อผลิตสื่ออธิบายการโกงแต่ละประเภท[25] ทำงานประสานกับภาคธุรกิจให้ความรู้ประชาชนที่ใช้บริการของตน[26] นอกจากนี้ สื่อสารมวลชนทั้งทางโทรทัศน์ วิทยุ และอินเทอร์เน็ตเองก็ลงข่าวเกี่ยวกับการหลอกลวงออนไลน์กันโดยตลอด กล่าวได้ว่าทุกภาคส่วนของสังคมต่างผลักดันเรื่องการให้ความรู้เพื่อป้องกันการหลอกลวงออนไลน์กันอย่างขยันขันแข็ง

อย่างไรก็ตาม การเผยแพร่ความรู้ให้ประชาชนก็ยังเป็นวิธีการป้องกันที่มีข้อจำกัด เนื่องจาก 1. มิจฉาชีพใช้วิธีการที่หลากหลายมีความซับซ้อน และยังพัฒนาสรรหาวิธีใหม่ๆ ที่น่าเชื่อถือมากขึ้นมาหลอกลวงประชาชนอยู่เสมอ[27] จึงเป็นไปได้ยากที่จะทำให้ทุกคนรู้เท่าทันการหลอกลวงจากมิจฉาชีพในทุกวิธี 2. มิจฉาชีพมักใช้เทคนิคกระตุ้นอารมณ์ที่ถึงแม้ว่าเราจะมีความรู้ประมาณหนึ่งก็ตกเป็นเหยื่อได้[28] โดยใช้ข้อเสนอที่ดึงดูด เร่งรัดให้เหยื่อรีบตัดสินใจในระยะเวลาอันสั้น[29] และกล่อมให้เหยื่อตัดสินใจด้วยตัวเองคนเดียว[30] ส่งผลให้ถึงแม้ว่าเหยื่อจะตามข่าวรับรู้กลลวงของมิจฉาชีพมาบ้าง แต่เมื่อเจอสถานการณ์จริงก็หลงกลตกเป็นผู้เสียหายอยู่ดี

เห็นได้ว่ามิจฉาชีพเองก็ปรับตัวหาวิธีหลีกเลี่ยงการควบคุมจากภาครัฐอยู่เสมอ ส่งผลให้มาตรการที่ภาครัฐผลักดันทั้ง 3 แบบยังไม่เพียงพอต่อการควบคุมการระบาด รัฐจึงหันไปผลักดันมาตรการเพิ่มเติมที่จะดึงภาคเอกชนเข้ามาร่วมป้องกัน โดยเริ่มกำหนดให้ธนาคารและค่ายมือถือมีหน้าที่บางอย่างเพื่อป้องกันการหลอกลวง

ในฝั่งของธนาคาร ปัจจุบันภาครัฐโดยธนาคารแห่งประเทศไทย กำลังศึกษาจัดทำแนวปฏิบัติ (guideline) ที่กำหนดหน้าที่ให้ธนาคารพาณิชย์ต้องหาทางป้องกันไม่ให้ประชาชนโดนโกงจากแอปฯ ดูดเงิน โดยหากละเลยหน้าที่ ธนาคารต้องรับผิดชอบชดเชยความเสียหายให้เหยื่อทั้งหมด 100%[31]

ในฝั่งของค่ายมือถือ ภาครัฐเริ่มกำหนดให้เครือข่ายมือถือต้องลงทะเบียนผู้ที่จะส่ง SMS ที่มีการแนบลิงก์ เพื่อให้ผู้ให้บริการได้ตรวจสอบลิงก์ก่อน[32]

ต่างประเทศจัดการการโกงออนไลน์อย่างไร?

แนวทางของภาครัฐไทยที่เริ่มมอบหน้าที่ให้ภาคเอกชนเข้าร่วมป้องกันนั้นสอดรับกับแนวโน้มการป้องกันภัยออนไลน์ในต่างประเทศ ที่หันมามอบบทบาทหน้าที่ให้ธุรกิจที่เกี่ยวข้องมาร่วมป้องกันภัยออนไลน์ อย่างไรก็ตาม แนวทางของไทยยังขาดการวางแนวทางป้องกันที่เชื่อมโยงกันเป็นระบบและยังไม่ครอบคลุมการหลอกลวงในทุกรูปแบบ ในส่วนต่อไปจึงชวนสำรวจแนวทางที่ต่างประเทศดึงภาคเอกชนเข้ามาร่วมป้องกัน

ปี 2024 เป็นปีที่รัฐบาลในหลายประเทศหันมากำหนดให้ภาคเอกชนมีหน้าที่ป้องกันการหลอกลวงออนไลน์ทั้ง ญี่ปุ่น[33] อังกฤษ[34] ไต้หวัน[35] มาเลเซีย[36] สิงคโปร์[37] ออสเตรเลีย[38] ฯลฯ เนื่องจากมองว่ามิจฉาชีพมักใช้บริการของภาคเอกชนเป็นเครื่องมือในการหลอกลวง หากเอกชนผู้ให้บริการช่วยยับยั้งจะทำให้การหลอกลวงออนไลน์ลดลงได้

การออกแบบให้ภาคเอกชนเข้ามามีส่วนร่วมช่วยยับยั้งการหลอกลวงออนไลน์มีหลักการสำคัญ 3 ประการ

ประการแรก ภาครัฐต้องกระจายหน้าที่ให้ธุรกิจช่วยดูแลหน้างานให้ เนื่องจากธุรกิจรับรู้พฤติกรรมการใช้งานของมิจฉาชีพทำให้สามารถพอจะคาดเดาได้ว่าผู้ใช้งานคนไหนต้องสงสัย นอกจากนี้ ธุรกิจเป็นผู้ที่ให้บริการระหว่างเกิดเหตุ จึงสามารถช่วยยับยั้งการหลอกลวงในช่วงที่มิจฉาชีพกำลังก่อเหตุได้ ซึ่งจะมีประสิทธิผลกว่าการตามจับหลังเกิดเหตุ และหากมิจฉาชีพมีการปรับตัวใช้วิธีหลอกลวงใหม่ๆ ภาคธุรกิจก็มีความคล่องตัวสูงในการเรียนรู้ปรับตัวเพื่อรับมือได้อย่างรวดเร็ว

ประการที่สอง รัฐต้องแบ่งหน้าที่ให้ธุรกิจดูแลตั้งแต่ต้นน้ำจนถึงปลายน้ำของกระบวนการหลอกลวง การที่มิจฉาชีพจะหลอกลวงเอาเงินมาจากเหยื่อได้ต้องพึ่งพาหลายบริการจากภาคธุรกิจ ทั้งบริการการสื่อสารเพื่อติดต่อเข้าหาเหยื่อ (ต้นน้ำ) ตลอดจนบริการทางการเงินเพื่อรับเงินโอนจากเหยื่อ (ปลายน้ำ) ดังนั้น จึงต้องให้ธุรกิจแต่ละส่วนช่วยป้องกัน

ในขั้นต้นน้ำ ค่ายมือถือและธุรกิจแพลตฟอร์ม เช่น โซเชียลมีเดีย ต้องทำหน้าที่เป็นด่านแรกในการป้องกันไม่ให้มิจฉาชีพเข้าถึงเหยื่อได้ โดยต้องทำระบบคัดกรองไม่ให้มิจฉาชีพใช้บริการของตนเพื่อติดต่อหลอกลวงเหยื่อ รวมถึงต้องคอยตรวจสอบและให้แจ้งเตือนผู้ใช้บริการหากตกอยู่ในความเสี่ยงที่จะเผชิญกับมิจฉาชีพ

ที่มา: Freepik

ในขั้นปลายน้ำ หากมิจฉาชีพฝ่าด่านแรกเข้าถึงประชาชน และหลอกลวงให้ประชาชนโอนเงิน (หรือหลอกให้โหลดแอปดูดเงิน) ธนาคารต้องทำหน้าที่ป้องกันไม่ให้มิจฉาชีพได้รับเงินจากเหยื่อ โดยธนาคารต้องช่วยเตือนภัยในกรณีต้องสงสัยว่ามีโอกาสเป็นการโอนเงินเข้าบัญชีมิจฉาชีพ รวมถึงต้องทำระบบป้องกันไม่ให้มิจฉาชีพที่สามารถควบคุมมือถือเหยื่อสามารถโอนเงินออกได้

ประการที่สาม รัฐต้องสร้างกลไกรับผิดชอบของธุรกิจในแต่ละส่วนให้ชัดเจน หลายประเทศได้กำหนดบทลงโทษหากธุรกิจยังปล่อยให้ประชาชนถูกหลอก เพื่อกระตุ้นให้ธุรกิจเข้มงวดในการทำหน้าที่ รวมถึงช่วยกระตุ้นให้ธุรกิจคิดหานวัตกรรมใหม่ๆ ที่จะช่วยป้องกันไม่ให้ประชาชนถูกหลอกลวงได้ง่าย เช่น การนำเทคโนโลยีมาช่วยตรวจจับพฤติกรรมของมิจฉาชีพ[39]

ประเทศที่ประสบความสำเร็จในการควบคุมการโกงออนไลน์ทำอย่างไร?

ออสเตรเลียและสิงคโปร์คือประเทศตัวอย่างที่ประสบความสำเร็จในการควบคุมการระบาดของการหลอกลวงออนไลน์ โดยเสียหายจากการหลอกลวงไม่ถึง 0.5% ของ GDP[40] ซึ่งประเทศเหล่านี้ได้ยกระดับวางแนวทางความรับผิดชอบให้กับภาคเอกชนอย่างเป็นระบบ

ผู้วิจัยเห็นว่าประเทศออสเตรเลียเป็นตัวอย่างที่ดีในการกำหนดให้ภาคเอกชนต้องมีหน้าที่ช่วยไม่ให้ประชาชนถูกหลอกให้โอนเงิน ในขณะที่ประเทศสิงคโปร์มีแนวทางที่ดีในการกำหนดให้ภาคเอกชนต้องมีส่วนรับผิดชอบไม่ให้ประชาชนถูกโกงจากกลโกงควบคุมบัญชี

ที่มา
The Australian Treasury (2023); MAS and IMDA (2023)

ออสเตรเลีย – บทบาทแต่ละภาคส่วน (Industry Codes) เพื่อป้องกันการหลอกให้โอนเงิน

ภายหลังจากที่ประเทศออสเตรเลียสูญเสียให้กับการถูกหลอกลวงออนไลน์จำนวนมาก รัฐบาลออสเตรเลียจึงผลักดันชุดมาตรการใหม่ที่ได้กำหนดแนวทางขั้นต่ำที่ภาคเอกชนต้องปฏิบัติ (Industry Codes) เพื่อป้องกัน (Prevention) สอดส่อง (Detection) ยับยั้ง (Disrupt) และรายงาน (Report) การหลอกลวงออนไลน์ที่เกิดขึ้น[41] โดยมาตรการใหม่จะบังคับใช้ในอนาคตอันใกล้

จุดเด่นสำคัญของแนวทางออสเตรเลียคือการออกแบบที่กำหนดหน้าที่ความรับผิดชอบที่กระจายตัวไปหลายภาคส่วน ซึ่งครอบคลุมทั้งค่ายมือถือ บริษัทแพลตฟอร์ม และสถาบันการเงิน

หน้าที่ของค่ายมือถือ

แนวทางตรวจจับและการป้องกัน: 1. ให้ความรู้ประชาชนเกี่ยวกับลักษณะพฤติกรรมในการโทรและการส่ง SMS ของมิจฉาชีพ แนวทางในการรับมือ รวมถึงช่องทางแจ้งเรื่องหากพบเจอมิจฉาชีพ 2. ทำระบบลงทะเบียนผู้ที่สามารถโทรหรือส่งข้อความ SMS ได้ 3. คอยตรวจหาการโทรหรือข้อความที่เข้าข่ายว่าเป็นมิจฉาชีพและตามหาต้นตอผู้ใช้งาน

แนวทางยับยั้ง: 1. หากตรวจพบเบอร์ที่ไม่ลงทะเบียนที่น่าสงสัยต้องระงับการใช้งานและส่งข้อมูลให้กับหน่วยงานกำกับดูแล 2. ระงับสัญญาณทันทีหากระบุได้ว่าเป็นเบอร์ที่มิจฉาชีพใช้งาน

แนวทางรายงาน: แจ้งให้หน่วยงานกำกับดูแลทราบภายใน 20 วันหลังจากระงับสัญญาณเบอร์ของมิจฉาชีพ

หน้าที่ของบริษัทแพลตฟอร์ม

แนวทางป้องกัน: 1. ทำระบบระบุตัวตนของผู้ที่จะลงโฆษณาในแพลตฟอร์ม 2. ตรวจหาปฏิสัมพันธ์ที่เข้าข่ายเสี่ยงว่าจะเป็นการหลอกลวงเพื่อแจ้งเตือนหรือบล็อกการติดต่อ 3. ป้องกันไม่ให้มิจฉาชีพแฮ็กบัญชีส่วนบุคคลไปใช้หลอกลวงคนในเครือข่ายสังคมของเจ้าของบัญชี

แนวทางตรวจจับและยับยั้ง: 1. แลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับพฤติกรรมของมิจฉาชีพกับผู้ให้บริการแพลตฟอร์มอื่นและผู้กำกับดูแล 2. หากได้รับแจ้งเบาะแสมิจฉาชีพต้องดำเนินการอายัดบัญชีทันที

แนวทางดูแลผู้ใช้งาน: 1. ต้องมีช่องทางที่ผู้ใช้งานสามารถรายงานการถูกหลอกลวงที่ใช้ง่าย (user-friendly) 2. หากผู้กำกับดูแลขอข้อมูลต้องส่งให้ภายในระยะเวลาที่กำหนด

หน้าที่ของสถาบันการเงิน

แนวทางการป้องกัน: 1. นำมาตรการระบุชื่อผู้รับ (Identity of Payee) มาใช้[42] 2. หากตรวจพบว่าผู้ใช้งานมีพฤติกรรมเสี่ยงว่ากำลังถูกหลอก สถาบันการเงินต้องดำเนินการเพิ่มเติมก่อนที่จะปล่อยให้เหยื่อโอนเงิน[43] 3. ต้องมีมาตรการประเมินตรวจจับธุรกรรมที่เสี่ยง เพื่อแจ้งเตือนผู้ใช้งานหรืออายัดธุรกรรมนั้นไว้ก่อน

แนวทางตรวจจับและยับยั้ง: 1. ธนาคารต้องแบ่งปันข้อมูลบัญชีที่สงสัยว่าเป็นบัญชี

มิจฉาชีพให้ธนาคารอื่นรับรู้ 2. หากได้รับแจ้งถึงธุรกรรมที่เข้าข่ายว่าถูกหลอกลวงต้องระงับธุรกรรมทันที และต้องร่วมมือกับธนาคารผู้รับโอนในการจัดการด้วย (ในกรณีที่โอนเข้าบัญชีปลายทางแล้ว)

แนวทางดูแลผู้ใช้งาน: 1. ต้องมีช่องทางที่ผู้ใช้งานสามารถรายงานความเสี่ยงในการถูกหลอกลวงที่ใช้ง่าย (user-friendly) 2. ต้องช่วยให้ผู้ถูกหลอกได้รับเงินคืนได้ง่าย เช่น ให้ธนาคารปลายทางต้องยกเลิกธุรกรรมภายใน 24 ชั่วโมงหลังจากธนาคารของผู้เสียหายร้องขอ 3. หากผู้กำกับดูแลขอข้อมูลต้องส่งให้ภายในระยะเวลาที่กำหนด

หากเอกชนผู้มีส่วนเกี่ยวข้องปล่อยปละละเลยจนมีผู้เสียหาย เอกชนที่ไม่ทำหน้าที่ต้องเสียค่าปรับเป็นจำนวนสามเท่าของกำไรที่ได้รับในช่วงที่ฝ่าฝืนไม่ทำตามมาตรฐาน หรือ 30% ของรายได้ของธุรกิจในช่วงที่ฝ่าฝืนไม่ทำตามมาตรฐาน โดยไม่เกิน 50 ล้านดอลลาร์ออสเตรเลีย (ประมาณ 1,280 ล้านบาท)

ทั้งนี้ กรอบมาตรการได้รับการออกแบบไว้ให้มีความยืดหยุ่นสามารถปรับเปลี่ยนไปตามความเหมาะสมของสถานการณ์ โดยเปิดช่องให้ธุรกิจในภาคอื่นต้องเข้ามาร่วมมีหน้าที่ป้องกันในอนาคต หากมิจฉาชีพปรับยุทธศาสตร์ไปใช้บริการของธุรกิจอื่นเป็นเครื่องมือ นอกจากนี้ หน้าที่ที่กำหนดไว้นี้ยังเป็นหน้าที่เบื้องต้นเท่านั้น ในแต่ละปีภาคธุรกิจที่เกี่ยวข้องต้องจัดทำรายงานประสิทธิภาพการป้องกันส่งให้ผู้กำกับดูแลด้วย เพื่อประเมินความเหมาะสมในการทำหน้าที่ที่เอกชนต้องรับผิดชอบ สุดท้าย จะต้องมีมาตรการที่เปิดพื้นที่ให้ผู้เสียหายสามารถร้องเรียนให้ผู้ให้บริการชดเชยความเสียหายได้ และหากธุรกิจสามารถเจรจาชดเชยให้ผู้เสียหายพึงพอใจได้แล้วก็ไม่ต้องเข้าสู่กระบวนการสอบสวนเพื่อให้เอกชนต้องจ่ายค่าปรับให้แก่รัฐ

สิงคโปร์ – กรอบความรับผิดชอบร่วม (Shared Responsible Framework – SRF) เพื่อป้องกันการควบคุมบัญชี

รัฐบาลสิงคโปร์ได้ผลักดันมาตรการที่กำหนดให้ทั้งสถาบันการเงิน ค่ายมือถือ และผู้บริโภคร่วมรับผิดชอบความเสียหายที่เกิดจากการหลอกลวงประเภทการควบคุมบัญชี (แอปฯ ดูดเงิน) เพื่อผลักดันให้ภาคเอกชนยกระดับระบบป้องกันภัยของระบบการเงิน ความน่าสนใจของกรณีสิงคโปร์คือ การสร้างความปลอดภัยของระบบการเงินของสิงคโปร์นั้นไม่ได้พึ่งพาเพียงแต่สถาบันการเงินอย่างเดียว แต่ดึงให้ค่ายมือถือมีส่วนช่วยรับผิดชอบป้องกันภัยคุกคามจากมิจฉาชีพด้วย

โดยภาครัฐได้มีข้อเสนอที่จะกำหนดให้ค่ายมือถือ และสถาบันทางการเงินมีหน้าที่ดังนี้[44]

หน้าที่ของค่ายมือถือ

• ทำระบบลงทะเบียนหมายเลขที่สามารถส่ง SMS ได้

• บล็อกไม่ให้หมายเลขที่ไม่ได้ลงทะเบียนส่ง SMS ได้

• ตรวจหา SMS ที่ส่งมาจากมิจฉาชีพ โดยเฉพาะ SMS ที่มีลิงก์ประกอบ

หน้าที่ของสถาบันการเงิน

• หน่วงเวลาการใช้งานบัญชีธนาคารออนไลน์ 12 ชั่วโมง หลังจากลงแอปพลิเคชันธนาคารใหม่ (ทำให้เวลามิจฉาชีพได้ข้อมูลสำคัญจากเหยื่อไป แล้วจะไปลงแอปพลิเคชันธนาคารเพื่อโอนเงินออก ทำได้ช้าลง)

• แจ้งเตือนหากมีการลงแอปพลิเคชันธนาคารใหม่ หรือเกิดธุรกรรมที่มีความเสี่ยงสูง

• แจ้งเตือนเมื่อมีเงินออกจากบัญชีในทันที

• มีช่องทางให้เหยื่อแจ้งล็อกบัญชี (Kill Switch) ทันทีได้ตลอด 24 ชั่วโมง

หากเหยื่อยังเสียหายจากการถูกมิจฉาชีพควบคุมบัญชี มาตรการกรอบความรับผิดชอบร่วม (SRF) ได้แบ่งสัดส่วนการรับผิดชอบความเสียหายที่ชัดเจนระหว่าง ค่ายมือถือ สถาบันการเงิน และตัวเหยื่อ ซึ่งสามารถแบ่งได้เป็น 3 กรณี

1. หากมีข้อบ่งชี้ว่า สถาบันทางการเงินไม่ทำตามหน้าที่ สถาบันทางการเงินต้องรับผิดชอบชดเชยความเสียหายให้กับเหยื่อทั้งหมด

2. หากมีข้อบ่งชี้ว่า สถาบันทางการเงินทำตามหน้าที่แล้ว แต่ความเสียหายเกิดขึ้นจากการที่ค่ายมือถือไม่ทำตามหน้าที่ ค่ายมือถือต้องรับผิดชอบความเสียหายให้กับเหยื่อทั้งหมด

3. หากมีข้อบ่งชี้ว่า ทั้งสถาบันการเงินและค่ายมือถือทำตามหน้าที่แล้ว เหยื่อต้องแบกรับความเสียหายที่เกิดขึ้นเอง

เมื่อหันกลับมาพิจารณาแนวทางของไทย จะพบว่า ภาครัฐไทยผลักดันให้เอกชนเข้ามามีส่วนร่วมในการป้องกันการหลอกลวงออนไลน์ตามแนวทางของประเทศสิงคโปร์ โดยเน้นที่การป้องกันภัยจากแอปดูดเงิน ทั้งการผลักดันให้ธนาคารต้องรับผิดชอบความเสียหายจากแอปฯ ดูดเงิน 100% รวมถึงมาตรการที่ค่ายมือถือต้องลงทะเบียนผู้ส่ง SMS ที่แนบลิงก์

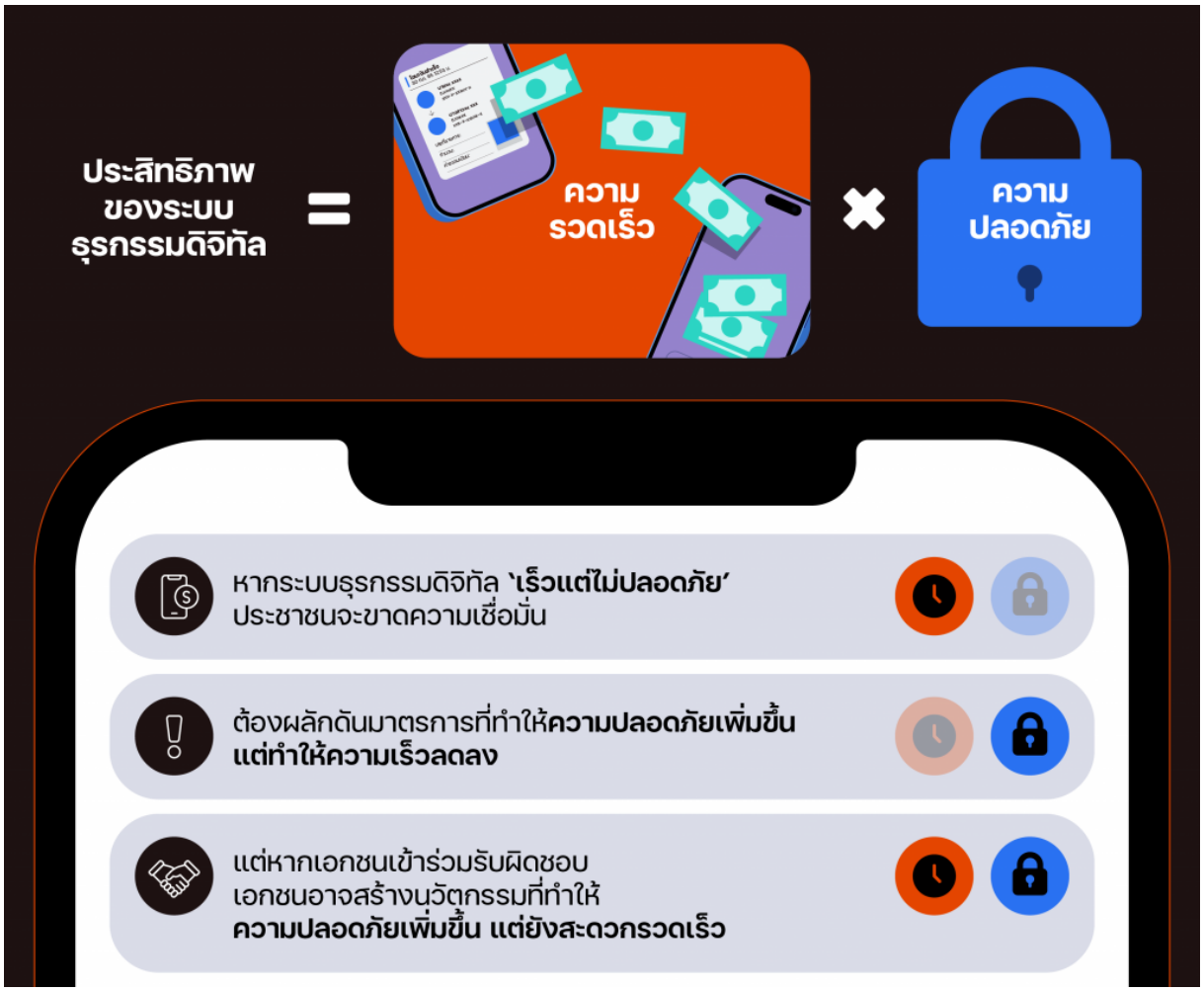
อย่างไรก็ตามเมื่อเทียบกับประเทศต้นแบบแล้ว ไทยยังไม่ได้กำหนดแนวทางความรับผิดชอบร่วมซึ่งเป็นหลักการหัวใจของประเทศสิงคโปร์ กล่าวคือถึงแม้ว่าจะกำหนดความรับผิดชอบของธนาคารพาณิชย์แล้ว แต่ภาครัฐก็ยังไม่ได้กำหนดให้ค่ายมือถือต้องรับผิดชอบความเสียหายหากไม่ทำตามหน้าที่ รวมถึงยังไม่ได้แบ่งขอบเขตความรับผิดชอบที่ชัดเจนระหว่างสถาบันการเงิน ค่ายมือถือ และประชาชน

นอกจากนี้ ถึงแม้ว่ารัฐไทยจะให้เอกชนเข้ามาร่วมป้องกันการหลอกลวงออนไลน์ประเภทควบคุมบัญชีแล้ว แต่ยังไม่ได้กำหนดหน้าที่ความรับผิดชอบของเอกชนให้ช่วยป้องกันการหลอกลวงออนไลน์ประเภทหลอกให้โอนเงินอย่างเป็นรูปธรรม ทั้งที่ยังคงระบาดและความเสียหายอย่างรุนแรงต่อคนไทย

มาตรการยับยั้งการโกงออนไลน์ มีผลข้างเคียงอย่างไร?

หากมองในภาพที่กว้างขึ้น การระบาดของมิจฉาชีพออนไลน์นั้นมีผลกระทบต่อความเชื่อมั่นในระบบเศรษฐกิจดิจิทัลด้วย เนื่องจากการหลอกลวงที่เกิดขึ้นในทุกวันมีผลทำให้เหยื่อและผู้เกี่ยวข้องหวาดระแวงไม่กล้าใช้บริการดิจิทัล ตั้งแต่การไม่กล้ารับโทรศัพท์ที่เบอร์ไม่คุ้นเคย ไปจนถึงการใช้บริการทางการเงิน ซึ่งหากประชาชนขาดความเชื่อมั่นและใช้บริการในระบบเศรษฐกิจดิจิทัลลดลง ธุรกิจดิจิทัลของไทยจะมีข้อจำกัดในการเติบโต ทำให้ประเทศไทยเสียโอกาสที่จะนำระบบดิจิทัลมาช่วยส่งเสริมให้เศรษฐกิจเติบโตได้อย่างเต็มประสิทธิภาพ

หากต้องการทำให้ประชาชนกลับมาเชื่อมั่น กล้าใช้บริการในระบบดิจิทัล ก็ต้องทำให้บริการในระบบดิจิทัลปลอดภัยจากมิจฉาชีพ อย่างไร



ก็ตาม หลายมาตรการที่ถูกออกแบบมาเพื่อป้องกันการหลอกลวงออนไลน์นั้นส่งผลให้ความรวดเร็วของบริการนั้นลดลง เช่น มาตรการลงทะเบียนเพื่อส่ง SMS หรือยิงโฆษณาสร้างความยุ่งยากให้กับธุรกิจที่ต้องการสื่อสารกับเป้าหมายในวงกว้าง มาตรการเพิ่มขั้นตอนก่อนโอนเงินและมาตรการหน่วงเงิน[45] ส่งผลให้การทำธุรกรรมออนไลน์ช้าลง[46]

อย่างไรก็ตาม หากผู้ให้บริการมีส่วนร่วมในการป้องกันการหลอกลวงออนไลน์ ผู้ให้บริการภาคเอกชนก็อาจมีนวัตกรรมที่ทำให้บริการของตนปลอดภัยมากขึ้นโดยไม่ทำให้ความเร็วในการใช้งานลดลงมากนัก[47] เช่น สถาบันการเงินจะมีระบบตรวจจับความเสี่ยงที่แม่นยำมากขึ้น สามารถทำนายได้ว่าธุรกรรมไหนเสี่ยงที่จะเป็นการโอนเงินให้มิจฉาชีพ สถาบันการเงินนั้นจึงบังคับใช้มาตรการเพิ่มขั้นตอนการโอนเงินหรือหน่วงเงินเฉพาะกรณีเสี่ยงสูงเท่านั้น ทำให้มีผลกระทบต่อธุรกรรมทั่วไปอย่างจำกัด

เอกชนร่วมรับผิดชอบ = ประชาชนไม่ต้องรับผิดชอบ?

การให้ภาคเอกชนร่วมชดเชยความเสียหาย ไม่ได้แปลว่าภาระในการป้องกันการหลอกลวงออนไลน์ตกอยู่กับภาคเอกชนทั้งหมด ประชาชนเองก็ต้องระมัดระวังตัวเองอยู่ดี

ในโมเดลของออสเตรเลียและสิงคโปร์ได้กำหนดขอบเขตหน้าที่ที่ภาคเอกชนต้องปฏิบัติไว้ชัดเจน หากภาคเอกชนทำหน้าที่แจ้งเตือนช่วยป้องกันอย่างเต็มที่แล้ว แต่เหยื่อยังประมาทไม่ดำเนินการตามที่ตนควรทำเพื่อป้องกันการถูกหลอกหลังได้รับการแจ้งเตือน ภาคเอกชนก็ไม่มีหน้าที่ชดเชยความเสียหายให้กับเหยื่อ

นอกจากนี้ หากผู้เสียหายต้องการได้รับเงินชดเชย ผู้เสียหายก็มีต้นทุนที่ต้องดำเนินการเพื่อให้ได้รับการชดเชยเงินคืน ผู้เสียหายต้องแจ้งเรื่องเพื่อเข้าสู่กระบวนการสืบสวน ซึ่งต้องใช้เวลาหลายเดือนถึงจะได้รับการชดเชยเยียวยา และก็ไม่ได้การันตีว่าผู้เสียหายจะได้รับเงินคืน 100% ด้วย นั่นหมายความว่าไม่มีใครอยากถูกหลอกแล้วต้องเข้าสู่กระบวนการเรียกร้องชดเชยเงินคืนหากไม่มีความจำเป็น

เชิงอรรถ

1. https://www.gasa.org/_files/ugd/7bdaac_0facba990813403a9f41ce9713577619.pdf

2. https://www.hfocus.org/content/2024/05/30458

3. https://www.prachachat.net/ict/news-1514260

4. https://www.forbes.com/uk/advisor/personal-finance/what-is-app-fraud/

5. ทางสำนักงานตำรวจแห่งชาติได้รวบรวมกรณีศึกษาที่ประชาชนถูกหลอกลวง และจัดแบ่งประเภทไว้สามารถอ่านเพิ่มเติมได้ https://24hicarecenter.com/pctpr

6. หลายครั้งมิจฉาชีพจะสร้างความน่าเชื่อถือด้วยการปลอมแปลงเป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์หรือบุคคลที่มีชื่อเสียง

7. ในกลุ่มไลน์มักมีหน้าม้า ที่แกล้งทำเป็นลงทุนตามที่กูรูแนะนำและได้ผลตอบแทนที่สูง เพื่อสร้างความน่าเชื่อถือและกดดันเหยื่อให้ลงทุน

8. มิจฉาชีพมีการกลยุทธ์ในการสร้างความน่าเชื่อถือด้วยการแอบอ้างเป็นบุคคลที่มีอยู่จริง รวมถึงใช้ข้อมูลส่วนตัวของเหยื่อที่หลุดมาจากฐานข้อมูลของภาครัฐในการข่มขู่ด้วย https://pdpathailand.com/pdpa-news/%E0%B8%AA%E0%B8%A3%E0%B8%B8%E0%B8%9B%E0%B9%80%E0%B8%AB%E0%B8%95%E0%B8%B8%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%B8%93%E0%B9%8C-%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%A3%E0%B8%B1/

9. https://www.imperva.com/learn/application-security/account-takeover-ato/#:~:text=Account%20Takeover%20(ATO)%20is%20an,data%20breaches%20and%20phishing%20attacks.

10. หลอกว่าเหยื่อยังไม่ได้ชำระค่าไฟฟ้าให้โหลดแอปการไฟฟ้าในลิงก์เพื่อจ่ายเงิน ซึ่งแอปการไฟฟ้านั้นเป็นแอปปลอมที่มิจฉาชีพสร้างขึ้นมาให้มีหน้าตาคล้ายแอปการไฟฟ้าจริง ๆ https://24hicarecenter.com/pctpr

11. สามารถทำความเข้าใจวิธีการการทำงานของแอปดูดเงินได้ที่ https://www.youtube.com/watch?v=yLB72G_whmg

12. การหลอกลวงประเภทนี้อาศัยช่องโหว่ของระบบการทำธุรกรรมออนไลน์ รัฐบาลไทยจึงจัดให้การหลอกลวงประเภทแอปดูดเงินเป็นภัยคุกคามระดับร้ายแรง https://www.infoquest.co.th/2024/412105 ถึงแม้ว่าจะสร้างความเสียหายเพียงแค่ 3% ของมูลค่าความเสียหายจากการหลอกลวงเท่านั้น

13. พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี 2566

14. https://www.bbc.com/thai/articles/cgxg7lqnv4no

15. หลายครั้งเจ้าของบัญชีม้าไม่รู้เห็นต่อการหลอกลวง เนื่องจากมิจฉาชีพขโมยข้อมูลไปเปิดบัญชี https://www.bangkokbiznews.com/news/news-update/1142664 สามารถทำความเข้าใจปัญหาของบัญชีม้าโดยละเอียดได้ที่ https://www.youtube.com/watch?v=ANgDX-FszUg

16. https://thaipublica.org/2023/03/electronic-crime-law-effective-now-01/

17. https://www.prachachat.net/ict/news-1514260 ซึ่งต่อให้อายัดได้ก็ต้องผ่านกระบวนการพิสูจน์ความเป็นเจ้าของอีก ผู้เสียหายจึงมีโอกาสที่จะได้รับคืนต่ำ

18, 20. รองนายกเร่งกวาดบัญชีม้า

19. https://www.pptvhd36.com/news/%E0%B9%84%E0%B8%AD%E0%B8%97%E0%B8%B5/220912

21. https://www.bot.or.th/th/news-and-media/news/news-20240613.html

22. ระบบที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ธนาคารแห่งประเทศไทย สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ และสำนักงานป้องกันและปราบปรามการฟอกเงิน ใช้ในการแลกเปลี่ยนข้อมูลกัน https://www.tba.or.th/en/%E0%-B8%94%E0%B8%B5%E0%B8%AD%E0%B8%B5%E0%B9%80%E0%B8%AD%E0%B8%AA-%E0%B8%88%E0%B8%B1%E0%B8%9A%E0%B8%A1%E0%B8%B7%E0%B8%AD-5-%E0%B8%AB%E0%B8%99%E0%B9%88%E0%B8%A7%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99/

23. https://www.prachachat.net/ict/news-1538913

24. https://www.uni.net.th/index.php/news/9445/

25. https://24hicarecenter.com/pctpr

26. ร่วมมือกับ tiktok https://www.infoquest.co.th/2024/416933 และร่วมมือกับ whoscall https://www.infoquest.co.th/2024/430364 รวมถึงที่ค่ายมือถือและธนาคารต่างๆ จัดทำสื่อความรู้เกี่ยวกับการโกงของตนเอง

27. ตัวอย่างเช่น กลยุทธ์ใหม่ในเดือนตุลาคม 2567 อ้างเป็นคนของสถาบันคุ้มครองเงินฝากหลอกให้แสกนใบหน้าเพื่อยกระดับความปลอดภัยในการคุ้มครองเงินฝาก เพื่อนำไปใช้ปลดล็อคธุรกรรมออนไลน์ในอนาคต https://www.bangkokbiznews.com/news/news-update/1150460

28. อ่านเพิ่มเติมเรื่องจิตวิทยาและพฤติกรรมศาสตร์ของเหยื่อที่ถูกหลอกลวงออนไลน์ได้ใน https://www.the101.world/nattavudh-powdthavee-scammers-interview/ และ https://plus.thairath.co.th/topic/politics&society/104327

29. เหยื่อเกินกว่าครึ่งตัดสินใจโอนเงินภายในไม่กี่ชั่วโมง https://www.gasa.org/_files/ugd/7bdaac_0facba990813403a9f41ce9713577619.pdf

30. เหยื่อ 80% ตัดสินใจคนเดียวตอนถูกหลอก https://www.gasa.org/_files/ugd/7bdaac_0facba990813403a9f41ce9713577619.pdf

31. https://www.tba.or.th/%E0%B8%98%E0%B8%9B%E0%B8%97-%E0%B8%AD%E0%B8%A2%E0%B8%B9%E0%B9%88%E0%B8%A3%E0%B8%B0%E0%B8%AB%E0%B8%A7%E0%B9%88%E0%B8%B2%E0%B8%87%E0%B8%A8%E0%B8%B6%E0%B8%81%E0%B8%A9%E0%B8%B2%E0%B8%81%E0%B8%B2%E0%B8%A3/

32. https://www.infoquest.co.th/2024/439681

33. รัฐบาลญี่ปุ่นกำหนดให้บริษัทดิจิทัลแพลตฟอร์มต้องมีแนวทางในการปราบปรามโฆษณาของมิจฉาชีพ และต้องเปิดเผยแนวทางในการปราบปราม https://japannews.yomiuri.co.jp/politics/politics-government/20240618-192893/

34. รัฐบาลอังกฤษกำหนดให้ธนาคารต้องรับผิดชอบความเสียหายให้กับผู้เสียหาย 100% ในกรณีที่ถูกหลอกให้โอนเงิน https://www.moneysavingexpert.com/news/2023/12/banks-scam-fraud-compensation-rules-confirmed/

35. รัฐบาลไต้หวันกำหนดให้บริษัทดิจิทัลแพลตฟอร์มต้องกำจัดโฆษณาและการส่งข้อความเพื่อการหลอกลวงในแพลตฟอร์มของตน https://focustaiwan.tw/society/202405090017

36. รัฐบาลมาเลเซียผลักดันกฎหมายที่กำหนดให้ธนาคารต้องรับผิดชอบความเสียหายหากเหยื่อถูกหลอกลวงออนไลน์ ยกเว้นจะพิสูจน์ได้ว่าธนาคารป้องกันเต็มที่แล้วแต่ผู้เสียหายไม่ป้องกันตัวเองอย่างเพียงพอ https://www.businesstoday.com.my/2024/07/09/banks-cannot-hold-customers-responsible-for-online-banking-fraud-losses-under-present-regulations-lim/

37. รัฐบาลสิงคโปร์กำหนดให้ค่ายมือถือและธนาคารต้องร่วมรับผิดชอบความเสียหายหากประชาชนเสียหายจากแอปดูดเงิน https://www.tookitaki.com/blog/what-is-singapores-shared-responsibility-framework-to-combat-phishing

38. รัฐบาลออสเตรเลียกำหนดให้ค่ายมือถือ บริษัทแพลตฟอร์มดิจิทัล และธนาคารช่วยประชาชนไม่ให้ถูกหลอก https://www.biocatch.com/blog/australia-scams-code-framework

39, 47. https://www.biocatch.com/blog/future-of-scam-detection

40. GASA. (2023). The Global State of Scams—2023. SCAMADVISER.

41. The Australian Treasury, 2023, Scams-Mandatory Industry Codes Consultation Paper https://treasury.gov.au/consultation/c2023-464732

42. ก่อนจะโอนเงินผู้โอนต้องกรอกชื่อของเจ้าของบัญชีปลายทางให้ถูกต้อง หากชื่อที่ผู้โอนกรอกกับชื่อเจ้าของบัญชีปลายทางไม่ตรงกัน ธนาคารสามารถยับยั้งได้ มาตรการนี้มีไว้ป้องกันหากปลอมแปลงเป็นบุคคลอื่น โดยใช้ชื่อที่ใกล้เคียงกัน https://www.bottomline.com/resources/what-confirmation-payee

43. ธนาคารออสเตรเลียใช้ระบบตรวจจับการใช้งานของผู้บริโภคเพื่อประเมินความเสี่ยงหากผู้บริโภคถูกหลอกลวง เช่น หากผู้ใช้งานมีพฤติกรรมแปลกๆ อย่างการกดมือถือย้ำๆ เพื่อโอนเงินอย่างรวดเร็ว อาจบ่งบอกได้ว่าผู้ใช้งานตกอยู่ภายใต้การกดดันของมิจฉาชีพ https://

biocatch.com/blog/scam-safe-banking-searching-for-clues-in-both-victim-and-recipient-behavior

44. MAS and IMDA, 2023, Guideline on Share Responsibility Framework, https://www.mas.gov.sg/publications/consultations/2023/consultation-paper-on-proposed-shared-responsibility-framework

45. สภาผู้บริโภคของไทยมีข้อเสนอที่ต้องการให้การโอนเงินปลอดภัยมากขึ้นด้วยการหน่วงเงินธุรกรรมที่มีมูลค่า 1 หมื่นบาทขึ้นไป เป็นเวลา 1 ชั่วโมง https://www.tcc.or.th/slow-payment/

46. แนวโน้มในระดับโลกเริ่มหันไปชะลอความเร็วในการทำธุรกรรมทางการเงิน เพื่อสร้างความปลอดภัยมากขึ้น https://www.biocatch.com/blog/faster-payments-sand-in-the-gears

ผู้วิจัยหลัก
กัลป์ กรุยรุ่งโรจน์
ติดต่อ
kanlapa.23.kan@gmail.com
contact.101pub@gmail.com

นักวิจัยนโยบายสาธารณะ 101 PUB สนุกกับการเห็นประสบการณ์ของต่างประเทศ และสนุกกับการเห็นความเป็นไปได้ใหม่ๆ ของสังคมไทย

101 PUB หรือ 101 Public Policy Think Tank - ศูนย์ความรู้นโยบายสาธารณะเพื่อการเปลี่ยนแปลง มุ่งทำงานวิจัยด้านนโยบายสาธารณะไทยในบริบทโลกใหม่ เราทำงานวิเคราะห์ ออกแบบ ขับเคลื่อน และสื่อสารนโยบายสาธารณะ บนฐานวิชาการ ฐานการพัฒนา และฐานประชาธิปไตย

www.101pub.org
101PUB
@101_PUB
@101_pub
contact.101pub@gmail.com