ตระหนักรู้ภัยออนไลน์รอบตัวคุณ

พันตำรวจโท ธนัทพัชร์ นวลศรี
อาจารย์ (สบ ๒) กลุ่มงานอาจารย์ ศูนย์ฝึกอบรมตำรวจภูธรภาค ๙

การเปลี่ยนแปลงทางเศรษฐกิจและสังคมของประเทศไทยในช่วงทศวรรษที่ผ่านมาถูกขับเคลื่อนโดยการขยายตัวของเทคโนโลยีดิจิทัลอย่างมีนัยสำคัญ การเข้าถึงอินเทอร์เน็ตที่รวดเร็วและการแพร่หลายของสมาร์ตโฟนได้ปรับเปลี่ยนพฤติกรรมการใช้ชีวิตและการทำธุรกรรมของประชาชนอย่างสิ้นเชิง ไม่ว่าจะเป็นการซื้อขายสินค้าออนไลน์ การโอนเงินผ่านแอปพลิเคชันธนาคาร หรือการใช้สื่อสังคมออนไลน์ในการติดต่อสื่อสารอย่างไรก็ตาม การเปลี่ยนแปลงนี้มาพร้อมกับความเสี่ยงด้านอาชญากรรมไซเบอร์โดยเฉพาะการหลอกลวงทางออนไลน์ที่ทวีความรุนแรงและซับซ้อนมากขึ้น

ข้อมูลจากศูนย์รับเรื่องร้องเรียนภัยออนไลน์ สำนักงานตำรวจแห่งชาติ (๒๕๖๗) ระบุว่ามีผู้เสียหายจากการหลอกลวงออนไลน์กว่า ๔๐๐,๐๐๐ ราย ในปีเดียว และมีมูลค่าความเสียหายรวมหลายหมื่นล้านบาท ตัวเลขนี้สะท้อนให้เห็นว่าปัญหานี้ไม่ได้เป็นเพียงเหตุการณ์เฉพาะราย แต่ได้กลายเป็นภัยสาธารณะที่ส่งผลกระทบต่อความมั่นคงทางเศรษฐกิจและความเชื่อมั่นในระบบดิจิทัลของประเทศ นอกจากนี้ กลโกงยังมีการปรับเปลี่ยนรูปแบบอย่างต่อเนื่อง จากการหลอกผ่านโทรศัพท์ (Vishing) และข้อความสั้น (Smishing) ไปสู่การใช้เทคโนโลยีขั้นสูงอย่างการใช้ AI ในการปลอมเสียงหรือใบหน้าในการสนทนาหลอกเหยื่อ

ประวัติศาสตร์ของการหลอกลวงในประเทศไทยไม่ได้จำกัดอยู่เพียงในยุคดิจิทัลเท่านั้น ประเทศไทยเคยมีกรณีแชร์ลูกโซ่ที่สร้างความเสียหายมหาศาล เช่น แชร์แม่ชม้อย(พ.ศ.๒๕๒๗)และแชร์ยูฟัน (พ.ศ. ๒๕๕๘) ซึ่งสะท้อนความเปราะบางของสังคมไทยต่อการลงทุนที่ให้ผลตอบแทนสูงผิดปกติ เมื่อก้าวเข้าสู่ยุคดิจิทัล ความเปราะบางเหล่านี้กลับถูกขยายขอบเขตด้วยเทคโนโลยีที่ทำให้การเข้าถึงเหยื่อทำได้ง่ายและรวดเร็วยิ่งขึ้น บทความฉบับนี้ผู้เขียนได้ศึกษาค้นคว้ารวบรวมข้อมูลที่เกิดขึ้นในปัจจุบันที่เกิดขึ้นกับสังคมไทยจึงมีวัตถุประสงค์สำคัญ ๕ ประการ ได้แก่ ๑. ทฤษฎีที่เกี่ยวข้อง ๒. กรณีศึกษา ๓. ประเภทของการหลอกลวงในปัจจุบัน ๔. มาตรการป้องกัน ๕. แนวทางการดำเนินการเมื่อประสบภัย

๑. ทฤษฎีที่เกี่ยวข้อง

การทำความเข้าใจปรากฏการณ์การหลอกลวงในยุคดิจิทัลต้องอาศัยกรอบแนวคิดและงานวิจัยที่เกี่ยวข้องทั้งในระดับทฤษฎีงานศึกษาในประเทศไทยและงานศึกษาระดับสากล

๑.๑ ทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory) ทฤษฎีนี้อธิบายว่าอาชญากรรมจะเกิดขึ้นได้เมื่อมีเงื่อนไขครบ ๓ ประการ คือ ๑. ผู้กระทำผิดที่มีแรงจูงใจ (Motivated Offender) ๒. เหยื่อที่เหมาะสม (Suitable Target) เช่น ผู้ที่ไม่ทันระวังหรือมีข้อมูลที่ถูกล่อใจ และ ๓. ขาดผู้พิทักษ์ที่มีประสิทธิภาพ (Absence of Capable Guardianship) เช่น ไม่มีระบบรักษาความปลอดภัยหรือกฎหมายที่เข้มงวด ตัวอย่างในประเทศไทย คือกรณี SMS ปลอมพัสดุที่แพร่หลายในปี พ.ศ. ๒๕๖๕–๒๕๖๗ ที่ประชาชนได้รับข้อความว่ามีพัสดุค้างชำระ เมื่อกดลิงก์แล้วกรอกข้อมูลบัตรเครดิตมิจฉาชีพสามารถนำข้อมูลไปใช้ได้ทันทีซึ่งสะท้อนว่าเหยื่อ (โดยเฉพาะผู้สูงอายุ) ไม่ระวังผู้ร้ายมีแรงจูงใจและไม่มีระบบเตือนภัยล่วงหน้าทำให้ก่ออาชญากรรมได้สำเร็จ

๑.๒ ทฤษฎีการรับรู้ความเสี่ยง (Risk Perception Theory) ทฤษฎีนี้ระบุว่ามนุษย์มักมีแนวโน้มที่จะ "มองข้ามความเสี่ยง" เมื่อมีผลตอบแทนสูงเข้ามาล่อใจ หรือเชื่อว่าตนเองจะไม่ตกเป็นเหยื่อ เช่น คดี Forex-3D ในประเทศไทยเป็นตัวอย่างที่ชัดเจน โดยมีการโฆษณาว่าลงทุนในตลาดแลกเปลี่ยนเงินตราต่างประเทศให้ผลตอบแทนสูงถึง ๖๐–๘๐% ต่อปี ทั้งที่ไม่มีการลงทุนจริงทำให้ผู้เสียหายนับพันรายสูญเงินกว่า ๒๐,๐๐๐ ล้านบาท สะท้อนว่าคนจำนวนมากเชื่อในผลตอบแทนที่สูงและประเมินความเสี่ยงต่ำกว่าความเป็นจริง

๑.๓ กรอบการจัดการความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) หน่วยงานวิจัย National Institute of Standards and Technology (NIST) ได้เสนอกรอบการป้องกันภัยไซเบอร์ที่หลายประเทศรวมถึงประเทศไทยนำมาใช้ ซึ่งประกอบด้วย ๕ ขั้นตอนหลัก ได้แก่ ๑. ระบุสิ่งที่ต้องปกป้อง (Identify) ๒. ป้องกัน (Protect) ๓. ตรวจจับ (Detect) ๔. ตอบสนอง (Respond) และ ๕. ฟื้นฟู (Recover) ตัวอย่างในประเทศไทย ธนาคารพาณิชย์ใช้กรอบนี้ในการสร้างระบบยืนยันตัวตนแบบหลายชั้น และการตรวจจับธุรกรรมผิดปกติ เช่น เมื่อมีการโอนเงินต่างประเทศเกินวงเงินปกติระบบจะหยุดธุรกรรมและแจ้งลูกค้าทันที

๑.๔ ทฤษฎีการเรียนรู้ของ AI (Artificial Intelligence(AI)) ในการตรวจจับ Phishing งานวิจัยสากลระบุว่าการเรียนรู้เชิงลึก (Deep Learning) สามารถตรวจจับเว็บไซต์และอีเมลหลอกลวง (Phishing) ได้แม่นยำมากกว่า ๙๐% เนื่องจากสามารถวิเคราะห์ทั้งโครงสร้างเว็บไซต์ พฤติกรรมผู้ใช้และเนื้อหาที่ผิดปกติ ในต่างประเทศ บริษัทใหญ่ๆ อย่าง Google และ Microsoft ใช้ AI ตรวจจับอีเมลหลอกลวง ทำให้สามารถป้องกัน Phishing ได้หลายพันล้านครั้งต่อปี อย่างไรก็ตามสำหรับประเทศไทยแม้ธนาคารพาณิชย์จะเริ่มใช้ AI ในการเฝ้าระวังธุรกรรม แต่การใช้ AI เพื่อตรวจจับ Deepfake และการหลอกลวงด้วยวิดีโอปลอมยังอยู่ในช่วงเริ่มต้น

๒.กรณีศึกษา

๒.๑ งานศึกษาในประเทศไทย มีงานศึกษาที่สะท้อนสถานการณ์และผลกระทบของการหลอกลวงออนไลน์ในประเทศไทย เพื่อทำความเข้าใจการหลอกลวงที่เกิดขึ้นในประเทศไทยจะขอนำเสนอกรณีศึกษาที่สำคัญที่ประชาชนสนใจติดตาม

- **คดี Forex-3D** เป็นโครงการระดมทุนแบบ Ponzi scheme หรือแชร์ลูกโซ่ที่เสนอผลตอบแทนสูงเกินจริงถึง ๖๐–๘๐% ต่อปี จากการเทรดแลกเปลี่ยนเงินตราผ่านเว็บไซต์ Forex- 3D.com เพื่อดึงดูดประชาชนให้ลงทุน โครงการนี้เริ่มในปี ๒๕๕๘ โดยอภิรักษ์ โคตธี จากข้อมูลของ DSI (๒๕๖๔) มีผู้เสียหายอย่างน้อย ๘,๔๓๖ ราย มูลค่าความเสียหายเกินกว่า ๒,๐๐๐ ล้านบาท แต่แหล่งข่าวอื่น ๆ ระบุว่าความเสียหายรวมอาจสูงถึง ๒.๕ หมื่นล้านบาท และมีผู้แจ้งความเกินกว่า ๙,๐๐๐ ราย มีการใช้บุคคลมีชื่อเสียง ดารา นักแสดง มาช่วยโปรโมตเพื่อสร้างความน่าเชื่อถือ คดีสิ้นสุดที่ศาลอาญากรุงเทพฯ เมื่อ ๒๖ ธันวาคม ๒๕๖๗ โดยศาลพิพากษาจำคุกจำเลยบางรายเป็นระยะเวลาเกือบ ๕๐,๐๐๐ ปี (แต่ลด เหลือ ๒๐ ปีตามกฎหมายสูงสุด) และสั่งชดเชยให้ผู้เสียหายรวม ๒.๔ พันล้านบาท **บทเรียนสำคัญ** การขาดความรู้ทางการเงินดิจิทัลและการควบคุมดูแลการลงทุนที่ไม่ได้รับอนุญาต ทำให้ประชาชนตกเป็นเหยื่อในวงกว้าง

- **คดีแก๊งคอลเซ็นเตอร์ (Call Center Scams)** แก๊งคอลเซ็นเตอร์เป็นกลโกงที่แพร่หลายอย่างต่อเนื่อง โดยเฉพาะช่วงปี ๒๕๖๔–๒๕๖๖ โดยมิจฉาชีพอ้างเป็นเจ้าหน้าที่รัฐ เช่น ตำรวจ, ธนาคาร, กสทช. ข่มขู่ว่าผู้เสียหายมีคดีความหรือทำผิดด้านการเงิน เพื่อหลอกให้โอนเงินเข้า "บัญชีม้า" เพื่อพิสูจน์ความบริสุทธิ์ ในปี ๒๕๖๖ และ ๒๕๖๗ มีผู้เสียหายหลายหมื่นราย มูลค่าความเสียหายหลายพันล้านบาท หน่วยงานที่เกี่ยวข้องได้ออกมาตรการ "อายัดบัญชีต้องสงสัยภายใน ๒๔ ชั่วโมง" เพื่อตัดเส้นทางการเงิน **บทเรียนสำคัญ** การใช้จิตวิทยาและความหวาดกลัวเป็นเครื่องมือทำให้ผู้เสียหายตัดสินใจโดยไม่ทันตรวจสอบ

- **ปัญหาบัญชีม้า (Mule Accounts)** บัญชีม้าคือบัญชีธนาคารที่บุคคลนำไปขายหรือให้ผู้อื่นใช้เพื่อทำธุรกรรมผิดกฎหมาย เช่น รับโอนเงินจากการหลอกลวงออนไลน์ มักมีการชักชวนผ่านออนไลน์เพื่อ "ให้เช่าบัญชี รับเงินตอบแทน" ในปี ๒๕๖๖ พบการตรวจสอบบัญชีม้ากว่า ๕๐,๐๐๐ บัญชี ทั่วประเทศและสถิติจากธนาคารแห่งประเทศไทย (๒๕๖๖) พบว่ามีการอายัดบัญชีต้องสงสัยกว่า ๖๐,๐๐๐ บัญชี ปัญหาบัญชีม้าทำให้ยากต่อการติดตามเส้นทางการเงิน ธนาคารแห่งประเทศไทยและสำนักงานตำรวจแห่งชาติได้ดำเนินมาตรการเข้มงวด เช่น ปิดบัญชีทันทีหากพบพฤติกรรมผิดปกติ และติดตามเอาผิดกับเจ้าของบัญชีตามกฎหมาย **บทเรียนสำคัญ** แม้ผู้ครอบครองบัญชีจะอ้างว่าไม่รู้เรื่อง แต่กฎหมายถือว่ามีความผิดเพราะมีส่วนร่วมอำนวยความสะดวกให้กับอาชญากรรม

- **กลโกงขายสินค้าออนไลน์** เป็นการหลอกขายสินค้าผ่าน Facebook หรือ LINE โดยใช้ภาพสินค้าจริง แต่เมื่อโอนเงินแล้วไม่ส่งของ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA, ๒๕๖๗) รายงานว่าปัญหานี้ติดอันดับ ๑ ของการร้องเรียนออนไลน์ ตัวอย่างที่พบเห็นได้บ่อยครั้ง เช่น ผู้เสียหายพบโพสต์ขายโทรศัพท์มือถือสมาร์ตโฟนรุ่นยอดนิยมในราคา ๒๐,๐๐๐ บาท ซึ่งดูน่าสนใจและคุ้มค่า จึงตัดสินใจสั่งซื้อและโอนเงินเต็มจำนวน แต่ท้ายที่สุดกลับไม่ได้รับสินค้า เมื่อพยายามทวงถามก็พบว่าไม่สามารถติดต่อผู้ขายได้อีก ทำให้สูญเสียเงินก้อนใหญ่ไปอย่างเปล่าประโยชน์ **บทเรียนสำคัญ** อาศัยความเชื่อใจ การจูงใจด้วยเทคนิคการขายการเสนอราคาสินค้าที่ต่ำกว่าความเป็นจริงในท้องตลาด หากพบเห็นสินค้าที่ราคาถูกกว่าปกติมาก ให้ตั้งข้อสงสัยไว้ก่อนเสมอ และควรตรวจสอบชื่อ-นามสกุล รวมถึงเลขที่บัญชีธนาคารของผู้ขายบนเว็บไซต์เตือนภัยมิจฉาชีพออนไลน์ก่อนทำการโอนเงินทุกครั้ง

- **การใช้ Deepfake และ AI Scams** เป็นการใช้ AI ปลอมเสียงและใบหน้าผู้บริหารบริษัทสั่งพนักงานโอนเงิน สถานการณ์ในไทยเริ่มพบการใช้ Deepfake ในการโทรหลอกลวง โดยอ้างเสียงเป็นผู้จัดการฝ่ายการเงินเพื่อขอรหัส OTP แม้ยังไม่มีสถิติชัดเจนแต่แนวโน้มสูงขึ้นตามรายงานของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES, ๒๕๖๗) พัฒนาการของ Deepfake Scam ในประเทศไทย นอกจากเป้าหมายระดับองค์กร (Corporate) แล้ว ในระดับบุคคลทั่วไปตามรายงานของหน่วยงานไทย (เช่น สอท. และศูนย์ AOC ๑๔๔๑) เราพบรูปแบบนี้มากขึ้น

วิดีโอคอลปลอมเป็นตำรวจ/เจ้าหน้าที่รัฐ แก๊งคอลเซ็นเตอร์เพิ่มความสามารถจากการโทรศัพท์ธรรมดาเป็นการเปิดกล้องวิดีโอคอล โดยใช้ AI สวมทับใบหน้า (Face Swapping) เป็นตำรวจขยับปากตามเสียงพูด (Lip-syncing) พร้อมฉากหลังที่เป็นสถานีตำรวจ ทำให้เหยื่อตื่นตระหนกและยอมโอนเงินง่ายขึ้น

การปลอมเป็นคนรู้จัก/คนในครอบครัว แฮ็กบัญชี LINE หรือ Facebook แล้วใช้วิดีโอคอลสั้นๆ หรือส่งข้อความเสียงปลอมเพื่อขอยืมเงินด่วน

๒.๒ งานศึกษาในระดับสากล ในระดับสากล ภัยคุกคามจากการหลอกลวงออนไลน์ก็เป็นประเด็นสำคัญ

- **Europol (๒๐๒๓) และ Interpol (๒๐๒๓)** ทั้งสองหน่วยงานเตือนว่า Deepfake และ AI-generated scams เป็นภัยใหม่ที่หลายประเทศรวมถึงยุโรปเผชิญเนื่องจากปลอมแปลงเสียงและภาพได้แม่นยำยิ่งขึ้น

- **Operation First Light (๒๐๒๔)** เป็นการระดมกำลังระดับโลก (ดำเนินการโดย ๖๑ ประเทศ ร่วมกับ Europol) สามารถจับกุมผู้กระทำผิดออนไลน์ ๓,๙๕๐ คน ยึดทรัพย์สินรวม ๒๕๗ ล้านดอลลาร์สหรัฐ และอายัดบัญชีถึง ๖,๗๔๕ บัญชี นับเป็นมาตรการสำคัญในการป้องกันออนไลน์ระหว่างประเทศ

- **สถานการณ์ในภูมิภาคเอเชียตะวันออกเฉียงใต้** มีรายงานกรณีถูกหลอกไปทำงานในศูนย์แก๊ง scammer ในประเทศเมียนมา เช่น ดาราจีน “Wang Xing” ถูกลักพาตัวไปยังศูนย์หลอกลวงก่อนได้รับความช่วยเหลือซึ่งส่งผลระยะยาวต่อความเชื่อมั่นของนักท่องเที่ยว

๓. ประเภทของการหลอกลวงในปัจจุบัน รูปแบบของการหลอกลวงมีการพัฒนาและหลากหลาย ดังนี้

๓.๑ ฟิชชิ่ง (Phishing) คือการปลอมแปลงอีเมลหรือเว็บไซต์ให้เหมือนของจริงเพื่อหลอกขโมยข้อมูลสำคัญ เช่น รหัสผ่านหรือข้อมูลบัญชีธนาคาร ตัวอย่าง มิจฉาชีพส่งอีเมลปลอมที่ดูเหมือนมาจากธนาคารแจ้งว่า "บัญชีของคุณถูกล็อก" พร้อมลิงก์ให้รีเซ็ตรหัสผ่านเมื่อคลิกลิงก์ปลอมนี้ข้อมูลทั้งหมดจะถูกส่งไปถึงอาชญากรทันที

๓.๒ สมิชชิ่ง / วิชชิ่ง (Smishing / Vishing) Smishing คือการหลอกผ่าน SMS ส่วน Vishing คือการหลอกผ่านโทรศัพท์เสียง ในปี ๒๐๒๔ บริษัท Whoscall พบว่ามีสายโทรและ SMS หลอกลวงในไทยสูงถึง ๑๖๘ ล้านสาย เพิ่มขึ้นถึง ๑๑๒ % จาก ๗๙ ล้านสายในปี ๒๐๒๓ ตัวอย่างคือ หลอกว่า "คุณได้รับเงินคืนจาก กยศ." พร้อมลิงก์ปลอมให้กรอกข้อมูล โดยใช้วิธีสร้างความน่าเชื่อถือจากข้อมูลเฉพาะตัวของเหยื่อ

๓.๓ ดีปเฟค / กลโกงสร้างด้วย (AI Deepfake / AI-generated scams) ใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) สร้างภาพหรือเสียงปลอม เช่น คลิปผู้บริหารหรือคนในครอบครัวที่สั่งให้โอนเงิน ตัวอย่างต่างประเทศคือ มิจฉาชีพสร้างเสียงปลอม CEO เพื่อสั่งโอนเงินด่วน ทำให้บริษัทถูกหลอกโอนหลายล้านบาทในเวลาไม่นาน

๓.๔ วิศวกรรมสังคม (Social Engineering) ใช้วิธีจิตวิทยาหลอกล่อ เช่น สร้างความกลัวหรือความกดดันให้เหยื่อตัดสินใจโดยไม่คิด ตัวอย่างในไทยคือ การโทรมาอ้างว่าเป็นเจ้าหน้าที่ตำรวจหรือ DSI มีหมายจับให้โอนเงินเพื่อ "ยกเลิกคดี" ทำให้หลายรายโอนเงินให้โดยไม่ตรวจสอบ

๓.๕ กลโกงแบบผสม (Hybrid Scams) เป็นการผสมผสานหลายวิธีเข้าด้วยกัน เช่น โทรหลอกผ่านเสียงแล้วส่ง SMS หรืออีเมลปลอมต่อเนื่อง ตัวอย่างคือ มิจฉาชีพโทรอ้างว่าเป็นธนาคารแล้วส่ง SMS ลิงก์ปลอมให้ตรวจสอบบัญชี พร้อมหน้าต่างเว็บหลอกให้กรอกข้อมูลทำให้เหยื่อเชื่อว่าเป็นขั้นตอนปกติ

๔. มาตรการป้องกัน

การรับมือกับการหลอกลวงออนไลน์ในประเทศไทยอาศัยทั้งเทคโนโลยีสมัยใหม่ กฎหมายและนโยบายของรัฐ และการสร้างความตระหนักรู้แก่ประชาชน ซึ่งมาตรการเหล่านี้ทำงานควบคู่กันเพื่อป้องกันไม่ให้มิจฉาชีพมีช่องโหว่ในการก่ออาชญากรรม

๔.๑ มาตรการทางเทคโนโลยี (Technological Measures)

- **การยืนยันตัวตนหลายขั้นตอน (Multi-Factor Authentication (MFA))** เป็นกลไกสำคัญในการตรวจจับและป้องกันอาชญากรรมออนไลน์ โดยเฉพาะในธุรกรรมทางการเงิน ธนาคารพาณิชย์ในไทยกำหนดให้ผู้ใช้งานต้องยืนยันตัวตนมากกว่าหนึ่งวิธี เช่น การใช้รหัสผ่าน (Password) ร่วมกับรหัส OTP (One-Time Password) หรือการสแกนใบหน้า เพื่อเพิ่มระดับความปลอดภัยและลดความเสี่ยงจากการถูกแฮกบัญชีโดยตรง ตัวอย่างเช่น ธนาคารไทยพาณิชย์ (SCB) บังคับใช้การยืนยันแบบ ๒ ชั้นทุกครั้งที่โอนเงินข้ามธนาคาร

- **ระบบตรวจจับการทุจริต (Fraud Detection System)** สถาบันการเงินจำนวนมากได้ลงทุนพัฒนาระบบตรวจจับธุรกรรมผิดปกติ (FDS) โดยใช้ Machine Learning วิเคราะห์พฤติกรรมของผู้ใช้งาน เช่น รูปแบบการโอนเงิน เวลาที่ทำธุรกรรมและสถานที่ หากพบความผิดปกติ ระบบจะระงับการทำธุรกรรมชั่วคราวและแจ้งเตือนลูกค้า ตัวอย่าง กรณีที่มีผู้ถูกแฮกบัญชีพยายามโอนเงิน ๓๐๐,๐๐๐ บาทไปต่างประเทศในเวลา ๐๓.๐๐ น. ระบบตรวจจับของธนาคารหยุดการโอนและโทรแจ้งลูกค้าทันที

- **ระบบยืนยันตัวตนดิจิทัลแห่งชาติ (National Digital ID (NDID))** ประเทศไทยได้พัฒนาแพลตฟอร์ม NDID สำหรับการพิสูจน์และยืนยันตัวตนดิจิทัล ซึ่งช่วยลดความเสี่ยงจากการสวมรอยเปิดบัญชี (Identity Theft) และปัญหา "บัญชีม้า" ในปี ๒๕๖๗ NDID เริ่มถูกใช้โดยหลายธนาคาร เช่น ธนาคารกสิกรไทยและธนาคารกรุงไทย ในการเปิดบัญชีใหม่

- **ระบบชีวมิติ (Biometrics)** ธนาคารและผู้ให้บริการโทรคมนาคมเริ่มบังคับใช้การยืนยันตัวตนด้วยลายนิ้วมือและการสแกนใบหน้า โดยเฉพาะในการเปิดบัญชีใหม่หรือทำธุรกรรมที่มีความเสี่ยงสูง ตัวอย่างคือ กรณีผู้สูงอายุในต่างจังหวัดถูกกดดันให้โอนเงิน ธนาคารเรียกใช้การยืนยันด้วย "สแกนใบหน้า" จึงหยุดการโอนของมิจฉาชีพได้

- **บล็อกเชน (Blockchain)** แม้ยังอยู่ในช่วงเริ่มต้น แต่บางหน่วยงานได้ทดลองใช้ Blockchain เพื่อเพิ่มความโปร่งใสและตรวจสอบย้อนกลับของธุรกรรม เช่น การโอนเงินระหว่างธนาคารและการจัดเก็บข้อมูลที่สำคัญ ตัวอย่างคือ ตลาดซื้อขายคริปโทเคอร์เรนซีในไทยใช้บล็อกเชนในการตรวจสอบธุรกรรม ทำให้ติดตามเส้นทางการเงินได้ง่ายขึ้น

๔.๒ มาตรการทางกฎหมาย

๔.๒.๑ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (Personal Data Protection Act (PDPA)) กฎหมายฉบับนี้มีผลบังคับใช้เมื่อวันที่ ๑ มิถุนายน ๒๕๖๕ มีสาระสำคัญคือการคุ้มครองข้อมูลส่วนบุคคลของประชาชน และไม่สามารถนำไปใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม มาตรา ๕ กำหนดว่ากฎหมายครอบคลุมการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทั้งที่อยู่ในและนอกประเทศไทย มาตรา ๑๙ ห้ามใช้ข้อมูลอ่อนไหว (Sensitive Data) เว้นแต่ได้รับความยินยอมชัดแจ้งและมาตรา ๔๐ กำหนดให้ผู้ประมวลผลข้อมูลต้องปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูลและจัดให้มีมาตรการป้องกันการเข้าถึงหรือรั่วไหล หากเกิดการละเมิดต้องแจ้งผู้ควบคุมข้อมูลทันที PDPA มีโทษทั้งอาญา (จำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิน ๑ ล้านบาท) โทษทางแพ่ง (ชดใช้ค่าเสียหายรวมถึงเชิงลงโทษไม่เกิน ๒ เท่า) และโทษปกครอง (ปรับสูงสุด ๕ ล้านบาท) ตัวอย่างคือ กรณีบริษัทโทรศัพท์ขายข้อมูลเบอร์โทรลูกค้าให้แก๊งคอลเซ็นเตอร์หากพิสูจน์ได้ว่าเป็นการกระทำโดยไม่ได้รับความยินยอม บริษัทอาจถูกปรับตาม PDPA.

๔.๒.๒ พระราชบัญญัติคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และแก้ไขเพิ่มเติม (Computer Crime Act) เป็นกฎหมายที่ใช้บังคับกับการกระทำความผิดที่เกี่ยวข้องกับระบบคอมพิวเตอร์หรือเครือข่ายอินเทอร์เน็ต มาตราสำคัญที่เกี่ยวข้องกับการหลอกลวงออนไลน์ ได้แก่ มาตรา ๕ (ผู้ใดเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ) มาตรา ๙ (ผู้ใดแก้ไข ทำลาย หรือเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ) และมาตรา ๑๔ (ผู้ใดนำข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ที่อาจทำให้ผู้อื่นเสียหายเช่น สร้างเว็บไซต์ธนาคารปลอมตัวอย่างคือ การสร้างเว็บไซต์ "ธนาคารปลอม" หลอกให้ประชาชนกรอก User และ Password สามารถเอาผิดตาม มาตรา ๑๔ ของ พ.ร.บ.คอมพิวเตอร์

๔.๓ มาตรการนโยบาย (Legal and Policy Measures)

การสร้างความตระหนักรู้และการศึกษา (Awareness and Education)

- โครงการรู้ทันกลโกงออนไลน์ โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) จัดทำคู่มือและสื่อประชาสัมพันธ์เพื่อเตือนภัยกลโกงรูปแบบต่าง ๆ เช่น SMS ปลอม เว็บไซต์ปลอมและการโทรหลอกลวง รวมถึงการเรียนรู้ที่เน้นการลงมือทำจริงให้ประชาชน โดยเฉพาะผู้สูงอายุ

- **การรณรงค์ผ่านสื่อสังคมออนไลน์** ธนาคารพาณิชย์และสำนักงานตำรวจแห่งชาติใช้ Facebook, LINE, และ YouTube เป็นช่องทางเผยแพร่ความรู้และกรณีตัวอย่าง เช่น "อย่ากดลิงก์ SMS" หรือ "ไม่โอน ไม่บอก ไม่คลิก" เพื่อให้ประชาชนรับรู้และป้องกันตัวเองได้ทันท่วงที

- **การอบรม Cyber Literacy (ความรู้เท่าทันดิจิทัล)** หน่วยงานรัฐร่วมมือกับโรงเรียนมหาวิทยาลัยและองค์กรปกครองส่วนท้องถิ่น เพื่อจัดอบรม Cyber Literacy โดยเฉพาะกลุ่มผู้สูงอายุและเกษตรกรที่มีความเสี่ยงสูงในการตกเป็นเหยื่อ ตัวอย่างจริงคือ โครงการฝึกอบรมผู้สูงอายุในหลายจังหวัดให้เรียนรู้การตั้งรหัสผ่านที่ปลอดภัยและวิธีตรวจสอบข่าวปลอม

๕. แนวทางการดำเนินการเมื่อประสบภัย

มาตรการของประเทศไทยมีความก้าวหน้าแต่ยังเผชิญความท้าทายใหม่ ๆ ที่ต้องจัดการอย่างจริงจัง จึงขอยกตัวอย่างเสนอแนวทางป้องกันจากกรณีที่เกิดขึ้นปรากฏทางสื่อในปัจจุบัน

๕.๑ กรณีถูกหลอกลงทุน (เช่น Forex-3D)

สิ่งที่ควรทำทันที เก็บหลักฐานทั้งหมด เช่น สัญญาการลงทุน ข้อความสนทนา หลักฐานการโอนเงินแจ้งความต่อ กรมสอบสวนคดีพิเศษ (DSI) และสำนักงานตำรวจแห่งชาติ ลงทะเบียนเป็นผู้เสียหายผ่านเว็บไซต์ DSI Online หรือสายด่วน ศูนย์ Anti Online Scam Operation Center (AOC) หรือศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ ตั้งสายด่วน ๑๔๔๑ ให้บริการแบบ One Stop Service ตลอด ๒๔ ชั่วโมง ช่วยระงับ/อายัดบัญชีมิจฉาชีพได้ทันทีภายใน ๑ ชั่วโมง พร้อมติดตามสถานะคดีและให้คำปรึกษาภัยออนไลน์ (เพื่อระงับบัญชี, รับคำปรึกษา, ติดตามผล)

การป้องกันในอนาคต ตรวจสอบรายชื่อบริษัทลงทุนกับ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ก่อนลงทุน

๕.๒ กรณีถูกแก๊งคอลเซ็นเตอร์หลอกให้โอนเงิน

สิ่งที่ควรทำทันที หากเพิ่งโอนเงินรีบโทรไปที่สายด่วนธนาคาร ๑๕๕๑ หรือเบอร์สายด่วนของธนาคารนั้นๆ เพื่ออายัดบัญชี แจ้งความที่สถานีตำรวจใกล้เคียง หรือ Police Cyber Hotline ๑๔๔๑ หรือ thaipoliceonline.go.th ซึ่งจะมีระบบอายัดบัญชี ๒๔ ชั่วโมง เก็บข้อมูลสายโทร/ข้อความที่ได้รับเพื่อส่งต่อให้ตำรวจ และกสทช.

การป้องกันในอนาคต ไม่บอกรหัส OTP หรือข้อมูลบัญชีแก่ใครทางโทรศัพท์เพราะหน่วยราชการจริงจะไม่ใช้วิธีนี้ (หลอกให้โอนเงิน)

๕.๓ กรณีบัญชีถูกใช้เป็น “บัญชีม้า”

สิ่งที่ควรทำทันที หากถูกจ้างให้เปิดบัญชีรีบแจ้งธนาคารเพื่อปิดบัญชีแจ้งตำรวจเพื่อป้องกันไม่ให้ถูกดำเนินคดีฐานฟอกเงิน หากพบว่าบัญชีถูกใช้ในทางผิดร่วมมือกับเจ้าหน้าที่ให้ข้อมูลทั้งหมด

การป้องกันในอนาคต ห้ามให้ผู้อื่นใช้บัญชีหรือเช่าบัญชี เพราะอาจถูกดำเนินคดีตาม พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน

๕.๔ กรณีซื้อสินค้าออนไลน์แล้วถูกโกง

สิ่งที่ควรทำทันที เก็บหลักฐาน เช่น สลิปโอนเงิน แชท ข้อมูลผู้ขายแจ้งความที่สถานีตำรวจหรือผ่านระบบ thaipoliceonline.com.แจ้งเรื่องกับ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ศูนย์ ๑๒๑๒ OCC (Online Complaint Center) โดย ETDA เป็นศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์ตลอด ๒๔ ชั่วโมง ทั้งเรื่องซื้อขายออนไลน์ เว็บไซต์ผิดกฎหมายภัยคุกคามไซเบอร์ และ Call Center ให้บริการผ่านสายด่วน ๑๒๑๒ อีเมล 1212@mdes.go.th เว็บไซต์ www.1212occ.com และ Facebook ข้อมูลข่าวสาร 1212 OCC

การป้องกันในอนาคต ใช้ระบบชำระเงินที่มีการคุ้มครองผู้ซื้อ เช่น บริการเก็บเงินปลายทาง (COD)

๕.๕ กรณีถูกหลอกด้วย Deepfake หรือ AI-generated Scams

สิ่งที่ควรทำทันที บันทึกวิดีโอ/ไฟล์เสียงที่สงสัยว่าเป็น Deepfake แจ้งหน่วยงานที่เกี่ยวข้อง เช่น MDES (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม) หรือ ETDA ผ่านช่องทางศูนย์ ๑๒๑๒ OCC หากเกี่ยวข้องกับการโอนเงินรีบติดต่อธนาคารเพื่ออายัดบัญชี

การป้องกันในอนาคต ตรวจสอบข้อมูลผ่านหลายช่องทางก่อนทำธุรกรรมใด ๆ (เช่น มีการโทรเข้ามาหากเกิดความไม่แน่ใจกับสิ่งที่พบเจอหรือเป็นเบอร์ที่ไม่รู้จักให้รีบทำการโทรยืนยันกับตัวบุคคลจริงก่อนทำการโอนเงินหรือหากอยู่ตามลำพังให้รีบปรึกษาคนใกล้ตัวในขณะนั้นโดยทันที)

ปรากฏการณ์การหลอกลวงในยุคดิจิทัลเป็นผลพวงจากความซับซ้อนของพฤติกรรมมนุษย์และวิวัฒนาการทางเทคโนโลยี ซึ่งสามารถอธิบายได้ด้วยทฤษฎีกิจวัตรประจำวันที่ชี้ให้เห็นว่าอาชญากรรมจะสำเร็จเมื่อผู้ร้ายที่มีแรงจูงใจพบกับเหยื่อที่มีช่องโหว่ในขณะที่ระบบป้องกันหย่อนยาน โดยมักใช้จิตวิทยาการรับรู้ความเสี่ยงที่ต่ำกว่าความเป็นจริงมาล่อลวงด้วยผลตอบแทนที่สูงเกินจริง ดังที่ปรากฏในกรณีศึกษาการฉ้อโกงครั้งใหญ่ เช่น คดี Forex-3D หรือขบวนการแก๊งคอลเซ็นเตอร์ที่สร้างความกลัวเพื่อบีบบังคับให้เหยื่อโอนเงินผ่านบัญชีม้าซึ่งยากต่อการติดตามเส้นทางการเงิน นอกจากนี้ มิจฉาชีพยังพัฒนาเครื่องมือไปสู่ระดับวิศวกรรมสังคมที่แยบยลทั้งการทำ Phishing เพื่อขโมยข้อมูลส่วนบุคคล และการใช้เทคโนโลยี Deepfake ปลอมแปลงใบหน้าและเสียงที่เริ่มระบาดอย่างหนักในปัจจุบัน อย่างไรก็ตามประเทศไทยได้วางรากฐานการป้องกันผ่านเกราะคุ้มกันสามชั้น ได้แก่ มาตรการทางเทคโนโลยีอย่างการยืนยันตัวตนหลายชั้น (MFA) และระบบซีวมิติ มาตรการทางกฎหมายที่เข้มงวดอย่าง PDPA และ พ.ร.บ.คอมพิวเตอร์ รวมถึงการสร้างความตระหนักรู้แก่ประชาชนในระดับนโยบาย ซึ่งหัวใจสำคัญของการรับมือเมื่อประสบเหตุคือความรวดเร็วในการติดต่อสายด่วน ๑๔๔๑ เพื่อระงับธุรกรรมภายในหนึ่งชั่วโมงแรก ควบคู่ไปกับการมีทักษะความรู้เท่าทันดิจิทัลเพื่อตรวจสอบข้อมูลทุกครั้งก่อนการตัดสินใจทำธุรกรรมใดๆ ในโลกออนไลน์

สุดท้ายในวันที่เทคโนโลยีก้าวล้ำจนมิจฉาชีพสามารถปลอมแปลงได้แม้กระทั่งใบหน้าและเสียง มาตรการทางกฎหมายและระบบรักษาความปลอดภัยทางเทคโนโลยีจึงเป็นเพียงเกราะชั้นนอกเท่านั้น แต่เกราะป้องกันที่แข็งแกร่งที่สุดคือ “สติและความรู้เท่าทัน” ของตัวผู้ใช้งานเองการ หมั่นตรวจสอบข้อมูล ไม่หลงเชื่ออะไรง่ายๆ และรู้วิธีจัดการเมื่อเกิดเหตุจะเป็นหัวใจสำคัญที่ช่วยให้เราใช้ชีวิตในโลกดิจิทัลได้อย่างปลอดภัยและมั่นคง

บรรณานุกรม

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (๒๕๖๖, ๒๐ พฤศจิกายน). คู่มือรู้เท่าทันกลโกงออนไลน์. https://www.mdes.go.th.

ธน หาพิพัฒน. (๒๕๖๗, ๒๖ กันยายน). การศึกษาสถานการณ์การถูกหลอกลวงผ่านช่องทางออนไลน์ กรณีศึกษาประชาชนอายุ ๑๕-๗๙ ปีไปทั่วทุกภูมิภาคของประเทศ. https://shorturl.asia/bW๗k๙

ธนาคารแห่งประเทศไทย. (๒๕๖๖, ๑๕ ธันวาคม). รายงานเสถียรภาพระบบการเงินไทย. https://www.bot.or.th.

สภาองค์การผู้บริโภค. (ม.ป.ป.). คู่มือรู้เท่าทันภัยมิจฉาชีพออนไลน์. https://shorturl.asia/l๙vna.

สำนักงาน กสทช. (๒๕๖๗, ๕ กุมภาพันธ์). รายงานการระงับบัญชีม้าและซิมการ์ดที่เกี่ยวข้องกับการหลอกลวงออนไลน์. https://www.nbtc.go.th

สำนักงานตำรวจแห่งชาติ. (๒๕๖๗, ๑๐ กุมภาพันธ์). รายงานสถิติการร้องเรียนภัยออนไลน์ประจำปี ๒๕๖๗. https://www.thaigov.go.th/news/contents/details/๙๐๐๐๒

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA). (๒๕๖๗, ๑๒ มกราคม). สถิติการร้องเรียนปัญหาออนไลน์ประจำปี ๒๕๖๗. https://www.etda.or.th

สำนักนายกรัฐมนตรี. (๒๕๖๗, ๓ ธันวาคม). รายงานสถิติการอายัดบัญชีและคดีอาชญากรรมออนไลน์สะสม. https://www.thaigov.go.th

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (๒๕๖๘, ๖ กุมภาพันธ์). ETDA โชว์สถิติร้องเรียนปัญหาออนไลน์ ปี ๖๗. https://shorturl.asia/๔eXaL