

ก้าวสู่โลกออนไลน์ที่ปลอดภัยสำหรับทุกคน ไทย-อียูร่วมสร้างเกราะไซเบอร์



โลกดิจิทัลกับความเสี่ยงที่ซ่อนอยู่

ทุกคลิก ทุกการเปิดลิงก์ หรือแม้แต่เสียงแจ้งเตือนเล็กๆ บนโทรศัพท์มือถืออาจซ่อนภัยเงียบที่คาดไม่ถึง โลกดิจิทัลที่เคยสร้างความสะดวกสบาย กลับกลายเป็นกับดักที่โหดร้ายที่สุด จาก SMS และลิงก์ปลอม ไปจนถึงแอปพลิเคชันหลอกลวงและโซเชียลมีเดียที่ทุกคนใช้เป็นประจำที่นำตกใจคือ ในจำนวนคนไทยทุกๆ 10 คน จะมีจำนวน 5 คนที่เคยถูกละเมิดทางออนไลน์ โดยปัญหาภัยไซเบอร์ไม่ใช่เพียงอาชญากรรมทั่วไป แต่เป็น “ปัญหาข้ามพรมแดน” ที่ดำเนินการในลักษณะอุตสาหกรรม และที่น่าห่วงยิ่งไปกว่านั้นคือการที่มิจฉาชีพจำนวนไม่น้อยถูกบังคับเข้าสู่ขบวนการค้ายาเสพติด

เพื่อเตรียมรับมือกับภัยทางไซเบอร์ที่ซับซ้อนดังกล่าว เมื่อเร็วๆ นี้ กระทรวงการต่างประเทศไทยร่วมกับสหภาพยุโรป (อียู) ได้จัดการสัมมนา “Safeguarding Digital Societies: Scam Prevention and Cybercrime” ขึ้น เพื่อสร้างความตระหนักรู้ในหมู่ประชาชน ผู้ให้บริการโทรคมนาคม และหน่วยงานรัฐผ่านการแลกเปลี่ยนแนวปฏิบัติที่ดี และเพื่อเน้นย้ำว่าภัยไซเบอร์นี้เป็นภัยที่ทุกประเทศกำลังเผชิญร่วมกันและเป็นวาระเร่งด่วนของรัฐบาล

เป้าหมายเดิม วิธีการใหม่

ตั้งแต่อดีตจนถึงปัจจุบัน เป้าหมายของมิจฉาชีพคือการหลอกลวงผู้คนเพื่อผลประโยชน์ทางการเงิน สิ่งที่เปลี่ยนไปคือวิธีการและเครื่องมือที่ใช้ จากจดหมายและการหลอกลวงตัวต่อตัวในอดีต ปัจจุบันมิจฉาชีพใช้ระบบอัตโนมัติ ดิจิทัล และโทรคมนาคม ทำให้สามารถโจมตีได้ตลอดเวลาทุกสถานที่ โดยเทคนิคหลักที่ใช้คือการหลอกล่อให้เหยื่อตัดสินใจผิดพลาด กระบวนการอาจเริ่มจากการส่ง Phishing ผ่าน SMS หรืออีเมลที่ส่งลิงก์ปลอมเลียนแบบหน้าธนาคารหรือแพลตฟอร์มซื้อขายสินค้า หากผู้ใช้เผลอคลิก ข้อมูลบัญชีและรหัส OTP จะถูกดักจับทันที ขณะเดียวกัน Social Engineering บนโซเชียลมีเดียกำลังแพร่หลาย โดยมีมิจฉาชีพสร้างบัญชีปลอมเข้ามาสร้างความสัมพันธ์และความไว้วางใจจากผู้ใช้ ก่อนหลอกให้โอนเงินหรือเปิดเผยข้อมูลสำคัญ และที่อันตรายไม่แพ้กันคือ Malware ผ่านแอปพลิเคชันปลอม ซึ่งแฝงตัวในรูปแอปพลิเคชันธนาคารหรือแพลตฟอร์มซื้อขายของออนไลน์ เมื่อถูกติดตั้งแล้วมัลแวร์จะเข้าควบคุมอุปกรณ์ ดักจับข้อมูล และส่งโอนเงินโดยอัตโนมัติ

ภัยไซเบอร์โหดร้ายกว่าที่คิด

หลายคนมองว่าเป็นเรื่องไกลตัว แต่แท้จริงแล้วข้อมูลส่วนบุคคล บัญชีธนาคาร และความไว้วางใจของผู้ใช้อินเทอร์เน็ตคือเป้าหมายหลักของมิจฉาชีพ การคลิกเพียงครั้งเดียวอาจนำไปสู่ความเสียหายมหาศาล

ในประเทศไทย มีผู้ใช้จำนวนมากถูกละเมิดให้โอนเงินช่วยเหลือฉุกเฉิน หรือซื้อสินค้าที่ไม่มีอยู่จริง บางรายสูญเสียเงินหลายแสนบาท ขณะที่ในระดับโลก Online Scam สร้างมูลค่าความเสียหายมหาศาลถึงหมื่นล้านดอลลาร์สหรัฐต่อปี เทียบเท่า GDP ของบางประเทศ โดยผลกระทบไม่ได้หยุดอยู่แค่เรื่องการเงิน แต่ยังบั่นทอนความเชื่อใจและความปลอดภัยทางจิตใจของผู้ใช้ด้วย ในยุโรปก็เช่นเดียวกัน บริษัทเทคโนโลยีรายใหญ่ต้องจัดตั้งทีมฉุกเฉินเพื่อรับมือการโจมตีไซเบอร์ ขณะที่รัฐบาลหลายประเทศกำลังเร่งออกกฎหมายใหม่เพื่อเพิ่มโทษอาชญากรรมออนไลน์และคุ้มครองประชาชน

ไทยเดินทางป้องกันภัยไซเบอร์

ประเทศไทยไม่ได้นิ่งดูดายต่อปัญหาการหลอกลวงออนไลน์ หน่วยงานรัฐและผู้ให้บริการโทรคมนาคมกำลังเดินหน้ารื้อสร้างระบบป้องกันหลายชั้น กสทช. ร่วมกับผู้ให้บริการเครือข่ายมือถือ



เช่น True และ AIS ได้ใช้ AI ตรวจสอบกิจกรรมผิดปกติแบบเรียลไทม์ หากพบพฤติกรรมเสี่ยงระบบจะสกัดกั้นกิจกรรมทันทีและแจ้งเตือนผู้ใช้นอกจากนี้ ยังมีการจัดตั้งศูนย์ปฏิบัติการแก้ไขปัญหายาเสพติดออนไลน์ (AOC 1441) เพื่อเยียวยาเหยื่อและระบุตัวตนผู้กระทำผิด ซึ่งเป็นกุญแจสำคัญในการแก้ปัญหาดังกล่าว นอกจากนี้ ธนาคารแห่งประเทศไทยและสำนักงาน ก.ล.ต. ได้เพิ่มมาตรการตรวจสอบบัญชีม้าและธุรกรรมที่ผิดปกติอย่างต่อเนื่อง พร้อมระบบเตือนภัยล่วงหน้าและการประสานงานกับแพลตฟอร์มโซเชียลอย่างทั่วถึงที่ มาตรการเชิงรุกอื่นๆ ได้แก่ แคมเปญให้ความรู้แก่ประชาชนเกี่ยวกับ Phishing Malware และ Social Engineering การจัดฝึกอบรมหน่วยงานรัฐและภาคเอกชนในการตรวจจับภัยไซเบอร์และการร่วมมือกับแพลตฟอร์มโซเชียลเพื่อสกัดโพสต์หลอกลวงแบบเร่งด่วน ซึ่งช่วยลดความเสียหายไปได้กว่า 90%

ถอดบทเรียนมาตรการเข้มข้นในอียู

ฝรั่งเศส เยอรมนี และโปรตุเกสได้ออกมาตรการเข้มงวดในการรับมืออาชญากรรมไซเบอร์ โดยฝรั่งเศสมีแพลตฟอร์ม Pharos ที่สามารถลบเนื้อหาอันตรายได้อย่างทันทีทั่วทั้งสื่อดิจิทัลกับหลักการของ Europol ที่ย้ำว่า “ความเร็วคือชีวิต” เนื่องจากหากสามารถติดตามธุรกรรมที่ผิดพลาดภายใน 48 ชั่วโมง ก็ยังมีโอกาสกู้คืนได้

กรณีศึกษาในเยอรมนี ทีม Cyber Response ของธนาคารใหญ่สามารถยับยั้งการโอนเงินที่เป็นผลจาก Phishing ได้ภายในไม่กี่ชั่วโมง

ส่วนในโปรตุเกส แพลตฟอร์มโซเชียลร่วมกับหน่วยงานรัฐสามารถสกัดบัญชีปลอมและลบเนื้อหาหลอกลวงได้ทันทีเช่นกัน

นอกจากนี้ อียูยังได้ออกกฎหมายบริการดิจิทัล (EU Digital Services Act: DSA) ซึ่งมีผลบังคับใช้ตั้งแต่กลางเดือนกรกฎาคมที่ผ่านมา มุ่งเน้นไปที่การสร้างแนวทางปฏิบัติที่เป็นมาตรฐานเดียวกันและการปกป้องเหยื่อที่เปราะบาง (ผู้เยาว์)

บทบาทนำของไทยในการสร้างโลกดิจิทัลที่ไม่ทอดทิ้งใครไว้ข้างหลัง

การสัมมนาครั้งนี้สะท้อนภาพลักษณ์ของไทยในฐานะ “ศูนย์กลางความร่วมมือไซเบอร์ในอาเซียน” และชี้ชัดว่าความปลอดภัยทางไซเบอร์ไม่ใช่หน้าที่ของรัฐหรือภาคธุรกิจเพียงฝ่ายเดียว แต่เป็นการกิจร่วมกันของทุกคน เพื่อให้ไม่มีใครถูกทิ้งไว้ข้างหลัง พร้อมเรียกร้องให้มีการปฏิรูปกฎหมาย การทำงานเชื่อมโยงระหว่างสถาบันและการบังคับใช้ที่เข้มแข็งเพื่อป้องกันและปราบปรามภัยไซเบอร์อย่างจริงจัง

ไทยและอียูยังเห็นว่า “ความเชื่อมั่นของผู้บริโภค” คือหัวใจของเศรษฐกิจดิจิทัล เพราะหากผู้ใช้ไม่มั่นใจในความปลอดภัยของข้อมูลก็จะไม่กล้าก้าวเข้าสู่โลกออนไลน์ ดังนั้น กฎหมายอย่าง GDPR และ PDPA จึงไม่ใช่เพียงข้อบังคับ แต่เป็นเครื่องมือสร้างความไว้วางใจและขีดความสามารถในการแข่งขันบนเวทีโลก

การแลกเปลี่ยนแนวปฏิบัติที่ตรงระหว่างไทย-อียูในครั้งนี้ จึงไม่เพียงเพิ่มเกราะป้องกันทางไซเบอร์ผ่านในการสร้างกฎระเบียบและการบังคับใช้ที่เข้มแข็ง การพัฒนาเทคโนโลยีที่ก้าวหน้าควบคู่ไป

กับการสร้างความตระหนักรู้ต่อสาธารณชนเพื่อสร้างสภาพแวดล้อมของสังคมดิจิทัลที่ปลอดภัยต่อทุกคนอย่างครอบคลุมและยั่งยืนเท่านั้น แต่ยังคงยกระดับไทยสู่บทบาทผู้นำในการขับเคลื่อนภูมิภาคอาเซียนสู่โลกดิจิทัลที่ปลอดภัย นับเป็นกลไกสนับสนุนนโยบายการทูตเพื่อประชาชนอย่างแท้จริง

เส้นทางสู่อนาคต: ไทย-อียูพนักกำลังสร้างโลกไซเบอร์ที่ปลอดภัย

ไทยและอียูได้เห็นหน้าความร่วมมืออย่างเข้มข้นภายใต้กรอบ Enhancing Security Cooperation in and with Asia and the Indo-Pacific (ESIWA+) ที่มุ่งเน้นความร่วมมือกับเอเชียเพื่อสร้างเครือข่ายป้องกันภัยไซเบอร์ระหว่างสองภูมิภาคผ่านการแลกเปลี่ยนข้อมูลอย่างทันทั่วทั้ง การพัฒนาฐานข้อมูลร่วมเพื่อระบุเทคนิคการโจมตีรูปแบบใหม่ การอบรมเจ้าหน้าที่และภาคเอกชนให้ตรวจจับและสกัดกั้นภัยไซเบอร์ได้อย่างมีประสิทธิภาพ พร้อมทั้งวางมาตรฐานความปลอดภัยไซเบอร์เพื่อคุ้มครองประชาชนทุกคนทั้งในระดับชาติ ภูมิภาค และนานาชาติ

ประเทศไทยได้แสดงบทบาทนำในระดับภูมิภาคอย่างชัดเจนตั้งแต่การจัดตั้งคณะทำงาน ASEAN Working Group on Anti-Online Scam (WG-AS) ไปจนถึงการมีส่วนร่วมอย่างโดดเด่นบนเวทีนานาชาติในกรอบองค์การว่าด้วยความมั่นคงและความร่วมมือในยุโรป (OSCE) ในฐานะประเทศหุ้นส่วนเพียงหนึ่งเดียวจากอาเซียนและล่าสุด การจัดสัมมนาครั้งนี้ได้ยกระดับความร่วมมือไทย-อียูด้านความมั่นคง โดยจะต่อยอดสู่การเป็นเจ้าภาพ Asian Conference ของไทยในปีหน้า ซึ่งจะหยิบยก “ความปลอดภัยทางไซเบอร์” เป็นวาระหลัก พร้อมขยายความร่วมมือสู่ประเด็นความมั่นคงทางไซเบอร์ทางทะเลภายใต้กรอบ ESIWA+ ร่วมกับอียูต่อไป อันเป็นประเด็นร้อนท่ามกลางภูมิรัฐศาสตร์โลกที่ผันผวน

ในโลกที่มีการพัฒนาของเทคโนโลยีอย่างรวดเร็ว การสร้างความปลอดภัยทางไซเบอร์ผ่านความร่วมมือระหว่างประเทศจึงเป็นพันธกิจสำคัญของกระทรวงการต่างประเทศ ความร่วมมือไทย-อียูครั้งนี้เปรียบเสมือนการประกาศต่อประชาคมโลกถึงความมุ่งมั่น ความไว้วางใจ และความเห็นอกเห็นใจ เพื่อร่วมกันสร้างสังคมดิจิทัลที่ปลอดภัย เป็นพื้นที่แห่งโอกาส ความเท่าเทียม และอนาคตที่มั่นคงสำหรับทุกคน

วิจิต จันท์แก้ว นันทิภา แก้วเกตุทอง