เมื่อ Online Scam กลายเป็นวาระหลักของโลก

- เมื่อการฉ้อโกงกลายเป็นภัยคุกคามของผู้บริโภค และอาชญากรมักใช้เครื่องมือทางออนไลน์เลือกเฟ้นเหยื่อ ถอดบทเรียนจากประเทศต่าง ๆ ในการกำกับดูแลปัญหาการฉ้อโกงออนไลน์ -

ปฏิเสธไม่ได้เลยว่าเทคโนโลยีดิจิทัลในทุกวันนี้ช่วยให้ชีวิตเราสะดวกสบายเป็นอย่างมาก การจัดการธุระประจำวันที่สามารถทำผ่านออนไลน์ได้ผ่านระบบอินเทอร์เน็ต และแอปพลิเคชั่น ช่วยลดค่าใช้จ่ายในการเดินทาง และประหยัดเวลาไปทำอย่างอื่นได้มากมาย แต่ไม่ใช่แค่ผู้บริโภคอย่างเราเท่านั้นที่ใช้เทคโนโลยีในการทำสิ่งต่าง ๆ เท่านั้น มิจฉาชีพผู้ที่จ้องจะเล่นงานเราก็ใช้เทคโนโลยีแบบเดียวกันในการขโมยทั้งข้อมูลส่วนตัว และดูดเงินจากบัญชีของเราไปหน้าตาเฉย แบบหาตัวจับไม่ได้อีกด้วย และแน่นอนว่าปัญหาแบบนี้ไม่ได้เกิดในประเทศไทยเท่านั้น แต่เป็นปัญหาที่ทั่วโลกต่างต้องเผชิญ และยังคิดไม่ตกว่าจะรับมือกับมิจฉาชีพพวกนี้อย่างไรดี

จากรายงาน The Global State of Scam Report 2023 ของ The Global Anti-Scam Alliance (GASA) พบว่าในปี 2566 มีการฉ้อโกงทั่วโลกเพิ่มขึ้นถึงร้อยละ 10.2 เมื่อเทียบกับปีก่อนหน้า และมีมูลค่าความเสียหายทางการเงินกว่า 55,000 ล้านเหรียญสหรัฐ หรือประมาณ 2 ล้านล้านบาท โดยเทคโนโลยีที่มีการนำมาใช้ในการหลอกลวงมากที่สุดคือ Generative AI อาทิ ChatGPT และ DeepFake ซึ่งสามารถใช้เทคโนโลยีการโคลนนิ่ง โดยวิเคราะห์เสียงที่ได้จากออนไลน์เพื่อสร้างเสียงสังเคราะห์ที่มีความใกล้เคียงกับเสียงของบุคคลเป้าหมายมากที่สุด เพื่อแอบอ้างเป็นบุคคลใกล้ชิด และหลอกให้มีการโอนเงินหรือให้ข้อมูลที่เป็นความลับ

นอกจากนี้ รายงานเรื่อง “It’s Prime Time for Real-Time 2023” ของ ACI Worldwide ซึ่งเป็นผู้ให้บริการการชำระเงินผ่านระบบอิเล็กทรอนิกส์แบบเรียลไทม์ระดับโลก พบว่า 1 ใน 5 ของผู้บริโภคที่ถูกสำรวจในปี 2565 เคยตกเป็นเหยื่อของการฉ้อโกงการชำระเงิน ขณะที่ประเทศที่ใช้ระบบการเงินแบบโอนและรับเงินได้ทันทีตลอด 24 ชั่วโมง จะมีแนวโน้มการถูกคุกคามทางการเงินสูงขึ้นตามอัตราที่มีการใช้งาน ซึ่ง 3 ประเทศที่มีการทำธุรกรรมแบบเรียลไทม์มากที่สุดในปี 2565 ได้แก่ (1) อินเดีย (89,500 ล้านรายการ) มีอัตราการหลอกลวงที่ร้อยละ 44.6 (2) บราซิล (29,000 ล้านรายการ) มีอัตราการหลอกลวงที่ร้อยละ 22.5 (3) จีน

(17,600 ล้านรายการ) มีอัตราการหลอกลวงที่ร้อยละ 10.7 และ ไทย (16,500 ล้านรายการ) มีอัตราการถูกหลอกลวงเป็นอันดับที่ 6 ของโลกที่ร้อยละ 25.7 โดยวิธีการที่พบคล้ายคลึงกันคือ ใช้รูปแบบการหลอกเหยื่อให้หลงเชื่อและโอนเงิน (Authorized Push Payment: APP) การหลอกให้ชำระค่าสินค้าปลายทาง (cash on delivery: COD) โดยลูกค้าไม่ได้สั่งซื้อสินค้า การสวมรอยเป็นคนอื่น (identity theft) เพื่อนำข้อมูลไปใช้แบบผิดกฎหมาย และ Social engineering หรือการหลอกให้ทำธุรกรรมหรือส่งข้อมูลส่วนตัวให้โดยการส่งอีเมล์หรือข้อความที่มีลิงก์ปลอม และการปลอมเป็นหน่วยงานที่น่าเชื่อถือและให้ตรวจสอบข้อมูลโดยการคลิกเข้าไปในลิงก์ปลอมเพื่อเจาะระบบเข้าสู่บัญชีธนาคารของเหยื่อ เป็นต้น

		ปริมาณการทำรายการ	อัตราการถูกหลอกลวง
	อินเดีย	(89.5 พันล้านรายการ)	44.6%
	บราซิล	(29.2 พันล้านรายการ)	22.6%
	จีน	(17.6 พันล้านรายการ)	10.7%
	ไทย	(16.5 พันล้านรายการ)	25.7%
	เกาหลีใต้	(8.0 พันล้านรายการ)	6.2%

ที่มา: https://www.bot.or.th

<u>ถอดบทเรียนมิจฉาชีพออนไลน์จากรอบโลก</u>

❖ **สหราชอาณาจักร**

ในปี 2565 การหลอกลวงเกี่ยวกับการชำระเงินมีสัดส่วนมากถึงร้อยละ 57 จากกรณีการถูกฉ้อโกงทั้งหมดที่เกิดขึ้นในสหราชอาณาจักร และสร้างความเสียหายกว่า 422 ล้านปอนด์ หรือ 19,000 ล้านบาท ซึ่งส่วนใหญ่เป็นการชักจูงแบบ APP คือหลอกให้หลงเชื่อแล้วโอนเงินไปให้ และเงินดังกล่าวก็จะถูกโอนไปยังบัญชีม้า เพื่ออำพรางเงินและหลบเลี่ยงการตรวจสอบของเจ้าหน้าที่

เพื่อแก้ไขปัญหาที่เกิดขึ้นจึงได้มีการจัดตั้งหน่วยงานกลางชื่อ The National Fraud Intelligence Bureau ขึ้นเพื่อเป็นศูนย์กลางด้านการตรวจสอบการฉ้อโกงและอาชญากรรมไซเบอร์ของสหราชอาณาจักร โดยมีหน้าที่ประสานงานกับตำรวจและหน่วยงานที่เกี่ยวข้องเพื่อแก้ปัญหาภัยการเงินแบบรวมศูนย์ นอกจากนี้ ยังมีการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาช่วยธนาคารพาณิชย์ในการตรวจสอบและยับยั้งการโจรกรรมทางการเงิน โดยสามารถตรวจจับการเคลื่อนไหวทางธุรกรรมทางการเงินที่เข้าข่ายผิดปกติ เช่น โอนเงินไปยังบัญชีที่อาจเป็นธุรกิจปลอมหรือผิดกฎหมาย โดย AI สามารถตรวจสอบข้อมูลการทำธุรกรรมแบบบัญชีต่อบัญชี (account-to-account) และช่วยวิเคราะห์ข้อมูลที่สำคัญ รวมถึงความเป็นไปได้ที่บัญชีผู้รับเงินอาจเกี่ยวข้องกับการโจรกรรมได้

ล่าสุด สหราชอาณาจักร ร่วมกับบริษัท BigTech 11 บริษัท ได้แก่ Amazon, eBay, Facebook, Google, Instragram, LinkedIn, Match Group, Microsoft, Snap, Tiktok, X, Youtube, techUK และ HM Government ร่วมกันจัดทำกฎบัตรการฉ้อโกงออนไลน์ (Online Fraud Charter) ขึ้น เพื่อใช้เป็นเครื่องมือสำหรับการกำกับดูแล การติดตาม ตรวจสอบ และแก้ไขปัญการฉ้อโกงออนไลน์ โดยกำหนดหน้าที่ให้กับบริษัท BigTech ที่เข้าร่วมต้องมีหน้าที่สอดคล้องดูแลเนื้อหาที่เข้าข่ายและทำการถอดเนื้อหาดังกล่าวออกจากเว็บไซต์หรือแอปพลิเคชั่น รวมถึงให้มีการตรวจสอบและบล็อคการเข้าถึงลิงก์หรือเนื้อที่ผิดปกติหรือคาดว่าจะก่อให้เกิดการหลอกลวงด้วย

❖ **ออสเตรเลีย**

ในปี 2565 ออสเตรเลียเกิดความเสียหายจากกรณีการฉ้อโกงออนไลน์มูลค่ากว่า 3 พันล้านเหรียญออสเตรเลีย หรือประมาณ 6.9 หมื่นล้านบาท โดยการหลอกลวงออนไลน์ที่พบมากที่สุด ได้แก่ (1) การหลอกให้ลงทุน ซึ่งมีสัดส่วนถึงร้อยละ 66 ของความเสียหายทั้งหมด (2) โรแมนซ์สแกม (Romance Scam) โดยปลอมแปลงตัวตนหรือใช้รูปภาพบุคคลอื่นหลอกให้เหยื่อหลงรักและเชื่อใจ และหลอกให้โอนเงินหรือทรัพย์สินให้ (3) การหลอกเรียกเก็บเงิน เช่น เก็บค่าสินค้าปลายทางจากสินค้าที่ไม่ได้สั่ง (4) การหลอกลวงทางอินเทอร์เน็ต เช่น ลิงก์ปลอมหรือแอปพลิเคชั่นดูดเงิน และการขโมยข้อมูลส่วนบุคคลผ่านอีเมล์หรือ QR Codeและ (5) การหลอกให้กดลิงก์หรือดาวน์โหลดแอปพลิเคชั่นเพื่อควบคุมโทรศัพท์มือถือจากระยะไกล (remote access scam)

เพื่อแก้ไขปัญหาที่เกิดขึ้น ออสเตรเลียได้จัดทำแพลตฟอร์ม Fraud Reporting Exchange ในการช่วยเหลือธนาคารรับเรื่องร้องเรียน สื่อสาร ติดตาม และระงับธุรกรรมที่เป็นการฉ้อโกงแบบเรียลไทม์ และได้จัดตั้งศูนย์ต่อต้านการฉ้อโกงทางออนไลน์แห่งชาติ (National Anti-Scam Center) เพื่อแก้ไขปัญหาเรื่องร้องเรียน ประสานงานหน่วยงานที่เกี่ยวข้อง ส่งต่อข้อมูลฉ้อโกงให้หน่วยงานที่เกี่ยวข้อง ประชาชนผู้ประกอบการรายอื่นรับทราบ เพื่อหยุดการทำธุรกรรม ตลอดจนทำระบบแจ้งเบาะแส แจ้งเตือนภัยประชาสัมพันธ์และให้ความรู้ผู้บริโภค นอกจากนี้ยังให้หน่วยงานที่เกี่ยวกับการสื่อสารและเทคโนโลยีติดตามตรวจสอบและป้องกัน Call Center และข้อความหลอกลวงด้วย แต่ยังไม่มีแนวทางการเยียวยาความเสียหายแก่ผู้บริโภค

❖ **สิงคโปร์**

ในปี 2565 เกิดกรณีการหลอกลวงขึ้นในสิงคโปร์มูลค่ารวมกว่า 660.7 ล้านเหรียญสิงคโปร์ (ประมาณ 17,000 ล้านบาท) และมีการฟ้องร้องดำเนินคดีถึง 31,728 คดี โดยกรณีที่พบมากในช่วงที่ผ่านมา คือ การหลอกให้สแกน QR Code เพื่อกรอกแบบสำรวจแลกกับชานมไข่มุก 1 แก้ว โดยมิจฉาชีพได้ฝังลิงก์เพื่อเจาะเข้าสู่ระบบโทรศัพท์มือถือของเหยื่อผ่าน QR Code ทำให้สามารถเข้าถึงข้อมูลทุกอย่างที่อยู่ในโทรศัพท์มือถือได้ แต่ที่น่าประหลาดใจคือ กลุ่มผู้เสียหายไม่ใช่ผู้สูงอายุที่ไม่รู้เท่าทันเทคโนโลยีแบบกรณีทั่วไป แต่กลับเป็นกลุ่มวัยรุ่น และวัยทำงานที่มีช่วงอายุ 20 – 39 ปี ซึ่งเป็นกลุ่มที่มีความรู้ด้านเทคโนโลยีค่อนข้างดีและมีอัตราการใช้สื่อสังคมออนไลน์สูง โดยปัจจุบันชาวสิงคโปร์วัยเรียนและวัยทำงานส่วนใหญ่จะนิยมอ่านข่าวออนไลน์ และชอบคลิกลิงก์ต่าง ๆ ที่อยู่บนแพลตฟอร์ม และข้อความจากหน่วยงานต่าง ๆ เพื่ออ่านข้อมูล จึงเห็นได้ว่ากลุ่มมิจฉาชีพมีการศึกษาข้อมูลและพฤติกรรมของเหยื่อมาเป็นอย่างดี และเลือกใช้เทคโนโลยีและกลโกงที่แตกต่างกันไปในแต่ละกลุ่มด้วย ดังนั้น เราจึงจำเป็นต้องรอบคอบก่อนที่จะคลิกลิงก์ต่างๆ และที่สำคัญอย่าแลกข้อมูลเพื่อชานมไข่มุกเพียงแก้วเดียว

เพื่อจัดการปัญหาการหลอกลวงออนไลน์ สิงคโปร์ได้จัดตั้งศูนย์ต่อต้านการหลอกลวงแห่งชาติ (National Anti-Scam Center) ขึ้น เพื่อแก้ปัญหาและดูแลเหยื่อที่ได้รับความเสียหายอย่างครบวงจร

ไทยกำลังทำอะไรเพื่อแก้ไขปัญหาในเรื่องนี้บ้าง

จากข้างต้นตามสถิติไทยเป็นประเทศที่มีกรณีอาชญากรรมออนไลน์ด้านการเงินมากที่สุดเป็นอันดับที่ 6 ของโลก โดยพบว่าประเภทคดีที่มีสถิติการแจ้งความออนไลน์มากที่สุดในปี 2566 ได้แก่ หลอกให้ซื้อขายสินค้าหรือบริการ หลอกให้โอนเงินเพื่อทำงาน หลอกให้กู้เงิน หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ และการข่มขู่ทางโทรศัพท์ ซึ่งมีความคล้ายคลึงกันกับประเทศอื่น ๆ ที่พบปัญหาเรื่องการหลอกลวงออนไลน์

ปัจจุบัน ไทยได้มีการจัดตั้งศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ หรือโทรสายด่วน 1441 ขึ้น เพื่อให้เหยื่อผู้ได้รับความเดือดร้อนสามารถแจ้งและยื่นเรื่องขอความช่วยเหลือได้แบบเบ็ดเสร็จในจุดเดียว โดยศูนย์ปฏิบัติการดังกล่าว จะทำงานร่วมมือกับธนาคาร และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน อาทิ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ และผู้ให้บริการมือถือ

สำหรับมิติทางด้านกฎหมาย ได้มีการประกาศบังคับใช้ พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยได้เพิ่มโทษของผู้กระทำความผิดโดยการเปิดบัญชีม้า จำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ

<u>บทวิเคราะห์</u>

ปัจจุบันการฉ้อโกงทางออนไลน์เกิดขึ้นทั่วโลก และเป็นปัญหาที่ดูเหมือนจะไม่มีทางแก้ไข ยิ่งเทคโนโลยีมีการพัฒนามากขึ้นเท่าไหร่ เทคนิคและกลโกงของมิจฉาชีพยิ่งมีความซับซ้อนมากขึ้นเท่านั้น นอกจากจะได้เปรียบในทางเทคโนโลยีแล้ว มิจฉาชีพเหล่านี้ยังได้เปรียบอีกสองต่อ คือ

(1) เราไม่สามารถระบุตัวตนที่แท้จริงของคนเหล่านี้ได้ การใช้ IP address ปลอม หรือใช้เบอร์โทรศัพท์ที่โทรผ่านเครือข่ายอินเทอร์เน็ตทำให้ไม่สามารถตรวจสอบตัวตนได้ และ

(2) ไม่มีแหล่งที่อยู่ที่สามารถระบุได้อย่างชัดเจน อีกทั้งส่วนใหญ่ที่ตรวจสอบพบล้วนเป็นอาชญากรรมข้ามชาติ คือ มีแหล่งที่ตั้งการกระทำความผิดนอกเขตแดนของไทย ทำให้ยากต่อการตรวจสอบ เนื่องจากจำเป็นต้องมีความร่วมมือระหว่างประเทศกับหน่วยงานที่เกี่ยวข้องเพื่อดำเนินการร่วมกันในเรื่องดังกล่าว และเมื่อตรวจสอบไม่ได้ และไม่ได้รับโทษทางการกระทำ จึงอาจเป็นช่องโหว่ที่คนเหล่านี้มองว่าเป็นโอกาสในการกระทำความผิดไปเรื่อย ๆ ส่งผลให้มีผู้เสียหายเพิ่มมากขึ้นหากเรายังไม่มีเครื่องมือในการกำกับดูแลเรื่องนี้อย่างมีประสิทธิภาพ

กรณีของไทยปัญหาที่พบส่วนใหญ่ คือ มิจฉาชีพหลอกเหยื่อผ่านแอปพลิเคชั่นไลน์ (LINE) และการโทรศัพท์โดยแอบอ้างเป็นบุคคลที่เรารู้จัก รวมถึงเทคนิคอื่น ๆ อาทิ การปลอมชื่อหน่วยงานไม่ว่าจะเป็นธนาคาร หรือหน่วยงานภาครัฐ เพื่อเพิ่มความน่าเชื่อถือ โดยมีการส่งข้อความมายังโทรศัพท์มือ โดยหลอกให้กดลิงก์เพื่อควบคุม วิธีนี้เรียกว่า False Base Station (FBS) Attack โดยหมายเลขโทรศัพท์ที่ใช้โทรหรือส่งข้อความเหล่านี้ไม่ได้ส่งผ่านเครือข่ายผู้ให้บริการ แต่เป็นการส่งผ่านช่องทางอินเทอร์เน็ต ทำให้ไม่สามารถระบุแหล่งที่มาของเบอร์โทรศัพท์ ซึ่งหน่วยงานที่เกี่ยวข้องกับการกำกับดูแล อาทิ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) หรือ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.) อาจพิจารณาแนวทางของสหราชอาณาจักรในการร่วมมือกับผู้ให้บริการโครงข่ายหรือแพลตฟอร์มออนไลน์ ในการแก้ไขปัญหาดังกล่าว ด้วยการจัดทำความตกลงร่วมกัน และกำหนดหน้าที่ที่ชัดเจนให้แก่ผู้ให้บริการในการสอดส่องดูแลแพลตฟอร์ม และโครงข่ายของตนเอง ว่ามีเนื้อหา ข้อความ ลิงก์ หรือปัจจัยเสี่ยงที่จะนำไปสู่อาชญากรรมออนไลน์หรือไม่

ปัญหาเรื่องการหลอกลวงออนไลน์ไม่ได้เพียงกระตุ้นให้เกิดการตื่นตัวภายในประเทศเท่านั้น แต่ในเวทีระหว่างประเทศได้เริ่มมีการหารือเพื่อสร้างความร่วมมือระหว่างกันในการรับมือกับปัญหาการ

หลอกลวงข้ามชาติ ซึ่งจะช่วยแก้ไขข้อจำกัดเรื่องการกระทำผิดนอกอาณาเขตของประเทศได้ อาทิ ในกรอบ APEC ซึ่งไทยโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ริเริ่มการผลักดันให้มีการหารือแนวทางการรับมือและกำกับดูแลในเรื่องดังกล่าว นอกจากนี้ ในการเจรจาจัดทำบทเศรษฐกิจดิจิทัล/การค้าดิจิทัลภายใต้ FTA ในปัจจุบัน อาทิ ภายใต้กรอบ IPEF ยังได้มีการเสนอให้มีความร่วมมือเพื่อกำกับดูแลปัญหาการฉ้อโกงออนไลน์ระหว่างประเทศภาคี และแนวทางการกำกับดูแลเทคโนโลยีปัญญาประดิษฐ์ที่อาจกลายเป็นเครื่องมือของมิจฉาชีพในการก่ออาชญากรรมด้วย

เหรียญย่อมมีสองด้านฉันใด เทคโนโลยีก็นำพามาทั้งด้านดีและด้านเสียด้วยเช่นเดียวกันฉันนั้น จะเห็นได้ว่าการพัฒนาทางเทคโนโลยีแม้จะมีประโยชน์ต่อเราในหลายแง่มุม แต่ในอีกด้านกลับเป็นปัจจัยหลักในการนำภัยคุกคามมาถึงตัวเราอย่างแยบยล การใช้เทคโนโลยีจึงต้องมีสติ รอบคอบ และรู้เท่าทันจึงจะเกิดประสิทธิภาพสูงสุด และตัวผู้บริโภคเองก็ต้องมีความรู้ความเข้าใจในการใช้เทคโนโลยี (digital literacy) เพื่อให้สามารถเท่าทันเหตุการณ์ด้วย ปัญหาการถูกหลอกลวงทางออนไลน์จะได้เบาบางลง

บทความโดย: นางสาวยุวจุฑา แก้วประทีป
นักวิชาการพาณิชย์ชำนาญการ
สำนักเจรจาการค้าบริการและการลงทุน
กรมเจรจาการค้าระหว่างประเทศ
มีนาคม 2567

แหล่งที่มาของข้อมูล:

-https://news.sky.com/story/uk-to-launch-an-online-fraud-charter-with-11-major-tech-companies-including-tiktok-snapchat-and-youtube-13019307
-https://www.callsign.com/knowledge-insights/scams-global-legislation-and-approaches-to-liability
-https://www.bot.or.th/th/research-and-publications/articles-and-publications/bot-magazine/Phrasiam-66-3/globaltrend_financialfraud.html
-https://www.gov.uk/government/publications/online-fraud-charter-2023/online-fraud-charter-2023-accessible#governance
-https://www.tcijthai.com/news/2023/09/scoop/13355