มิจฉาชีพเปลี่ยนรูปแบบหลอกหลอนชาวบ้านไม่พักเลย

สำนักงานตำรวจแห่งชาติ โดย พล.ต.ท.สมพงษ์ ชิงดวง ผู้ช่วย ผบ.ตร./หัวหน้าคณะทำงานสร้างเสริมภูมิคุ้มกันต้านภัยอาชญากรรมทางเทคโนโลยี พร้อมด้วยคณะทำงาน ได้ร่วมกันนำเสนอสถิติการรับแจ้งความออนไลน์รอบสัปดาห์และภัยที่เกิดขึ้นใหม่ เพื่อประชาสัมพันธ์ให้ประชาชนได้มีภูมิป้องกันภัยออนไลน์ ไม่ตกเป็นเหยื่อของมิจฉาชีพ โดยมีรายละเอียดดังนี้

ในรอบสัปดาห์ที่ผ่านมา (12-18 มี.ค.2566) **รวมทั้งสัปดาห์มีผู้แจ้งความ 4,291 เคส/351,191,412.31 บาท** สถิติการรับแจ้งลดลงจากสัปดาห์ที่แล้ว **1,496 เคส/26,093,473.69 บาท** โดยสถิติการรับแจ้งความคดีออนไลน์มากที่สุดยังเป็นคดีเดิมๆ 5 อันดับ ได้แก่ อันดับ 1) คดีหลอกลวงซื้อขายสินค้า 1,500 เคส/14,003,677.05 บาท 2) คดีหลอกลวงให้โอนเงินเพื่อหารายได้จากการทำกิจกรรม 578 เคส/71,469,279.03 บาท 3) คดีหลอกลวงทางโทรศัพท์ที่เป็นขบวนการ (call center) 529 เคส/65,547,808.73 บาท 4) คดีหลอกให้กู้เงินแต่ไม่ได้เงิน 429 เคส/17,113,573.64 บาท และ 5) คดีหลอกเป็นบุคคลอื่นเพื่อยืมเงิน 236 เคส/10,637,571.37 บาท

ภัยออนไลน์ที่น่าสนใจและเกิดขึ้นมากในรอบสัปดาห์ **<u>เรื่องที่ 1</u>** คือ คดีหลอกลวงซื้อขายสินค้า นม Thai-Denmark โดยมิจฉาชีพสร้างเพจ Facebook “Thai-Denmark **นมไทยแท้ ส่งทั่วไทย**” คล้ายของจริง เมื่อมีผู้หลงเชื่อมาสอบถามเพื่อขอซื้อนม เพจจะให้ผู้หลงเชื่อโอนเงินให้ก่อน แล้วปิดเพจหนีไป **จุดสังเกตุ ของปลอม** พบการกดปุ่มโกรธ (angry)จำนวนมาก สถานะของเพจเป็นอสังหาริมทรัพย์ เพิ่งเปิดเพจ และผู้จัดการเพจอยู่ต่างประเทศ ส่วน **ของแท้** เป็นธุรกิจท้องถิ่น และ เปิดมานานและผู้จัดการเพจอยู่ประเทศไทย จึงขอประชาสัมพันธ์ให้ประชาชนควรสงสัยไว้ก่อนว่าของดีและถูกเกินกว่าราคาตลาดมากๆ และบัญชีรับโอนเงินบุคคลธรรมดา น่าจะหลอกลวง

<u>เรื่องที่ 2</u> คดีแก๊งคอลเซนเตอร์ติดต่อร้านอาหารผ่านแอปพลิเคชันไลน์หลอกสั่งข้าวกล่อง และโอนมัดจำให้ร้านค้าก่อน วันต่อมา คนร้ายได้โทรศัพท์บอกให้ร้านอาหารสั่งชุดอาหารพิเศษเพิ่ม 7 ชุด และส่ง QR Code มาให้ร้านแอด และบอกว่าจ่ายเงินเพิ่มให้ภายหลัง และอ้างด้วยว่าเป็น QR Code แอดไลน์เท่านั้น แต่เมื่อแสกน QR Code พบว่า หน้าจอค้างเจ้าของโทรศัพท์จึงรีบเข้าแอปฯ ธนาคาร เพื่อโอนเงินออกไปบัญชีอื่นก่อน และปิดเครื่อง จึงขอประชาสัมพันธ์ให้ตรวจสอบแหล่งที่มาของ QR Code ให้ดีก่อนที่จะ Scan หรือโอนเงิน

<u>เรื่องที่ 3</u> คดีกลรักออนไลน์(Romance Scam) ถูกหลอกซ้ำซ้อน คือหลอกให้โอนเงิน 2 ครั้ง และหลอกให้ผู้เสียหายเปิดบัญชีม้าโดยไม่รู้ตัว เรื่องนี้คนร้ายได้ติดต่อพูดคุยกับผู้เสียหายทาง Facebook จากนั้นอ้างว่าอยากจะมาอยู่เมืองไทย มาใช้ชีวิตคู่กับผู้เสียหาย และส่งสินค้ามีค่ามาให้ โดยให้ผู้เสียหายโอนเงินชำระภาษี ถือเป็นการหลอกให้โอนเงินรอบแรก จากนั้นจะหลอกว่าต้องการทำธุรกิจร่วมกับผู้เสียหาย แล้วให้ผู้เสียหายเปิดบัญชีไว้สำหรับการลงทุน จากนั้นคนร้ายได้หลอกผู้เสียหายคนที่ 2 และให้โอนเงินเข้าบัญชีผู้เสียหายคนแรก และให้ผู้เสียหายคนแรก ซื้อเหรียญคลิปโตให้คนร้าย ทำให้ผู้เสียหายคนแรก กลายเป็นผู้ต้องหาในคดี จึงขอประชาสัมพันธ์ให้ประชาชนได้รับทราบ รู้เท่าทัน ไม่ตกเป็นเหยื่อของคนร้าย

ด้วยความปรารถนาดีจากสำนักงานตำรวจแห่งชาติ และศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (PCT)

คดีหลอกลวงซื้อขายผลิตภัณฑ์สินค้า

“Thai-Denmark นมไทยแท้ ส่งทั่วไทย”

กลโกง	จุดสังเกต	วิธีป้องกัน
1. สร้างเพจ Facebook ขึ้นมาโดยใช้ชื่อ รูปโปรไฟล์ รูปปก ที่อยู่ ข้อความแนะนำ ใกล้เคียงกับเพจ “Thai-Denmark” ที่เป็นของจริง 2. สร้างเป็นเพจ Facebook หรือซื้อโฆษณาเพจเพื่อให้คนเห็นได้จากระบบอินเตอร์เน็ต 3. เมื่อมีผู้หลงเชื่อมาสอบถามเพื่อขอซื้อ เพจจะให้ผู้หลงเชื่อโอนเงินให้ก่อน 4. เมื่อถึงวันรับสินค้า เหยื่อจะส่งข้อมูลไปสอบถาม คนร้ายจะถ่วงเวลา 5. เปลี่ยนเป็นเพจใหม่ เพื่อหลอกขายเช่นเดิมไปเรื่อยๆ	**ของปลอม** 1. พบการกดปุ่มโกรธ (angry)จำนวนมาก 2. สถานะของเพจเป็นอสังหาริมทรัพย์ 3. เพิ่งเปิดเพจ และผู้จัดการเพจอยู่ต่างประเทศ **ของแท้** 1.สถานะของเพจเป็นธุรกิจท้องถิ่น 2. เปิดมานานและผู้จัดการเพจอยู่ประเทศไทย	1. ตรวจสอบเพจ Facebook ให้แน่ใจก่อนซื้อ โดยกด “เกี่ยวกับ” “ความโปร่งใส” ก็จะเห็นว่าเปิดมานานเท่าใด ผู้จัดการเพจอยู่ประเทศไทยหรือไม่(อยู่ต่างประเทศ ควรหลีกเลี่ยง) 2. ดูช่องกดไลค์(มีเครื่องหมาย “โกรธ” ดูโพสต์เป็นหลัก อย่าดูด้านใต้ชื่อเพียงอย่างเดียว เพราะสามารถซื้อ “ไลค์” ได้ 3. ลองนำชื่อเพจนั้น ไปใส่ช่องค้นหาใน Facebook ว่ามีเพจอื่นอีกหรือไม่ แล้วนำมาเปรียบเทียบกันดูว่า เพจไหนจริง/ปลอม 4. “ของดีและถูกเกินกว่าราคาตลาดมากๆ” ให้สงสัยไว้ก่อนว่าหลอกลวง 5. บัญชีรับโอนเงินควรเป็นบัญชีชื่อร้าน หากเป็นบัญชีบุคคลธรรมดา ให้สงสัยไว้ก่อนว่าหลอกลวง

คอลเซ็นเตอร์หลอกสั่งข้าวกล่อง

(ให้ Scan QR Code เพื่อควบคุมเครื่อง)

กลโกง	จุดสังเกต	วิธีป้องกัน
1. คนร้ายติดต่อร้านอาหารผ่านแอปพลิเคชันไลน์ หลอกสั่งข้าวกล่องจำนวน 100 กล่อง เพื่อนำไปจัดเลี้ยงประชุม และโอนมัดจำมาก่อน 2,000 บาท 2. คนร้ายโทรศัพท์บอกให้ร้านอาหารสั่งชุดอาหารพิเศษเพิ่ม 7 ชุดและบอกว่าจะจ่ายเงินเพิ่มให้ภายหลัง จากนั้นส่ง QR Code มาให้ร้านแอด โดยอ้างว่าเป็น QR Code แอดไลน์เท่านั้น 3. เมื่อสแกน QR Code แล้ว คนร้ายจะควบคุมเครื่องโทรศัพท์ เพื่อถอนเงินหรือติดตามการทำงาน	1. บัญชีไลน์ที่ใช้ในการหลอก อาจมีผู้ใช้มากกว่า 1 คน เนื่องจากในแชทมีคำลงท้ายทั้งครับและค่ะ 2. QR Code ปลอมใช้โลโก้ไลน์แปะไว้ตรงกลาง ซึ่งทำให้มีผู้หลงเชื่อว่าเป็น QR Code ไลน์จริง จนสามารถหลอกผู้เสียหายได้ 3. QR Code ปลอมไม่ได้เชื่อมต่อเพื่อเพิ่มเพื่อนผ่านไลน์ แต่เป็นการแฝงลิงก์ดาวน์โหลดมัลแวร์แบบอัตโนมัติ	1. ใช้โปรแกรมหรือแอปพลิเคชั่นที่สามารถระบุได้ว่าเป็นลิงก์ปลอม 2. เมื่อสแกนแล้ว มีการปรากฏลิงก์แปลกปลอม หรือไม่น่าเชื่อถือ อย่ากดเข้าไป 3. หากเข้าเว็บแปลกปลอมหลังจากสแกนไปแล้ว ให้รีบออกทันที 4. มีสติ ปิดเครื่อง ตัดสัญญาณอินเทอร์เน็ตและมือถือทันที หากมีการติดตั้งแอปพลิเคชั่นที่เป็นอันตรายลงไป 5. ตรวจสอบให้แน่ใจว่าคู่บัญชีที่ทำธุรกรรมนั้น ได้ทำการซื้อขายสินค้าจริงหรือไม่

คดี Romance Scam หลอกซ้ำซ้อน

กลโกง	จุดสังเกต	วิธีป้องกัน
1. แก๊งกลรักออนไลน์ (Romance Scam) ได้ติดต่อพูดคุยกับผู้เสียหายทาง Facebook และเว็บไซต์หาคู่ จากนั้นอ้างว่าอยากจะมาอยู่เมืองไทย มาใช้ชีวิตคู่กับผู้เสียหาย จะส่งสินค้ามีค่ามาให้ 2. คนร้ายให้ผู้เสียหายโอนเงินเพื่อชำระภาษี และได้เงินจากผู้เสียหายรอบแรก 3. คนร้ายจะหลอกว่าต้องการทำธุรกิจร่วมกับผู้เสียหาย แล้วให้ผู้เสียหายเปิดบัญชีไว้สำหรับการลงทุน 4. คนร้ายไปหลอกผู้เสียหายคนที่ 2 และให้โอนเงินเข้าบัญชีผู้เสียหายคนแรก 5. คนร้ายให้ผู้เสียหายคนแรก ซื้อเหรียญคริปโตให้คนร้าย บัญชีผู้เสียหายคนแรก กลายเป็นบัญชีม้า (ใช้บัญชีผู้อื่นไปรับโอนเงินจากผู้กระทำผิด)	1. มิจฉาชีพมักจะใช้รูปโปรไฟล์ชาวต่างชาติที่มีหน้าตาดีหรือมีประวัติการทำงานที่ดีและมั่นคง ซึ่งข้อมูลและรูปเหล่านี้ได้มาจากหลายๆ แหล่งในอินเทอร์เน็ต 2. เมื่อมิจฉาชีพสามารถสร้างความเชื่อถือให้กับผู้เสียหายได้แล้ว ก็จะหลอกให้ผู้เสียหายเปิดบัญชีเพื่อลงทุนหรือเทรดเงินคริปโต 3. มิจฉาชีพที่ใช้กลโกงลักษณะนี้มักมีการหลอกให้โอนเงินโดยอ้างว่าชำระค่าภาษี	1. ต้องตรวจสอบตัวตนของคนในโลกโซเชียล เนื่องจากคนร้ายสามารถปลอมแปลงตัวตน รูปภาพ ฯลฯ เพื่อให้เหยื่อหลงเชื่อว่าเป็นของจริง อาจตรวจสอบโดยการโทรพูดคุยผ่าน messenger หรือโทรศัพท์ปกติ เพื่อสังเกตุสำเนียงการใช้ภาษาพูดว่าเป็นบุคคลที่กล่าวอ้างหรือไม่ 2.ถ้ามีการให้เปิดบัญชีเพื่อลงทุนหรือเทรดเงินคริปโตหลังจากสร้างความเชื่อมั่นในระยะเวลาไม่นาน ให้ปฏิเสธ และปิดกั้นการสนทนา 3. การหาคู่รักผ่านทางออนไลน์โอกาสประสบความสำเร็จในด้านความรักจริงน้อยกว่าแบบทั่วไป 4. ควรเรียนรู้และกระทำการลงทุนหรือเทรดเงินคริปโตด้วยตนเอง ไม่ต้องมีผู้ใดมาสอนให้ 5. ควรมีสติทุกครั้ง เวลากระทำการธุรกรรมใดๆ กับบุคคลที่สามที่ไม่รู้จัก

ตาม พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566

1. พ.ร.ก.นี้กำหนดให้ผู้เสียหายสามารถติดต่อธนาคารเพื่อระงับธุรกรรมของบัญชีต้องสงสัยชั่วคราวได้โดยตรงทันที จากนั้นจึงไปร้องทุกข์ต่อพนักงานสอบสวน

2. กรณีธนาคารพบธุรกรรมต้องสงสัย สามารถระงับธุรกรรมชั่วคราว แล้วส่งให้เจ้าหน้าที่ตำรวจตรวจสอบ

3. ผู้เสียหายจะร้องทุกข์ที่สถานีตำรวจใด หรือที่กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีก็ได้ และพนักงานสอบสวนผู้รับคำร้องทุกข์เป็นพนักงานสอบสวนผู้รับผิดชอบ โดยผู้เสียหายต้องแจ้งความร้องทุกข์ภายใน 72 ชม. และพนักงานสอบสวนจะรวบรวมพยานหลักฐานแจ้งกลับไปยังธนาคารของบัญชีนั้น ภายใน 7 วัน เพื่อยืนยันการระงับธุรกรรมของบัญชีนั้น

4. ให้อำนาจ เจ้าหน้าที่ตำรวจ DSI ปปง. มีอำนาจนำข้อมูลต้องสงสัยไปใช้ประโยชน์ได้โดยไม่เป็นความผิดตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

บทกำหนดโทษ

ฐานความผิด	อัตราโทษ
เปิดหรือยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก(บัญชีม้าหรือซิมม้า) โดยรู้หรือควรรู้ว่าจะนำไปใช้ ในการกระทำความผิด	มีโทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 300,000 บาท หรือ ทั้งจำทั้งปรับ
เป็นธุระ จัดหา โฆษณา หรือไขข่าว เพื่อให้มีการ ซื้อขายบัญชี(บัญชีม้าหรือซิมม้า) เพื่อใช้ในการกระทำความผิด	จำคุกตั้งแต่ 2 ถึง 5 ปี ปรับตั้งแต่ 200,000 ถึง 500,000 บาท หรือทั้งจำทั้งปรับ
เป็นธุระ จัดหา โฆษณา หรือไขข่าว เพื่อให้มีการ ซื้อขายหมายเลขโทรศัพท์ซึ่งลงทะเบียนในนามบุคคลอื่นแล้ว แต่ไม่สามารถระบุตัวผู้ใช้จริงได้	จำคุกตั้งแต่ 2 ถึง 5 ปี ปรับตั้งแต่ 200,000 ถึง 500,000 บาท หรือทั้งจำทั้งปรับ