

คดีหลอกลวงซื้อขายผลิตภัณฑ์สินค้า
“Thai-Denmark นมไทยแท้ ส่งทั่วโลก”

กลโกง	จุดสังเกต	วิธีป้องกัน
<p>1. สร้างเพจ Facebook ขึ้นมา โดยใช้ชื่อ รูปโปรไฟล์ รูปปก ที่อยู่ ข้อความแนะนำ ใกล้เคียงกับเพจ “Thai-Denmark” ที่เป็นของจริง</p> <p>2. สร้างเป็นเพจ Facebook หรือ ชื่อโฆษณาเพจเพื่อให้คนเห็นได้จากระบบอินเทอร์เน็ต</p> <p>3. เมื่อมีผู้หลงเชื่อมาสอบถามเพื่อขอซื้อ เพจจะให้ผู้หลงเชื่อโอนเงินให้ก่อน</p> <p>4. เมื่อถึงวันรับสินค้า เขี่ยจะส่งข้อมูลไปสอบถาม คนร้ายจะถ่วงเวลา</p> <p>5. เปลี่ยนเป็นเพจใหม่ เพื่อหลอกลวงขายเช่นเดิมไปเรื่อยๆ</p>	<p>ของปลอม</p> <p>1.พบการกดปุ่มโกรธ (angry)จำนวนมาก</p> <p>2.สถานะของเพจเป็น อสังหาริมทรัพย์</p> <p>3. เพิ่งเปิดเพจ และผู้จัดการเพจ อยู่ต่างประเทศ</p> <p>ของแท้</p> <p>1.สถานะของเพจเป็นธุรกิจท้องถิ่น</p> <p>2. เปิดมานานและผู้จัดการเพจอยู่ประเทศไทย</p>	<p>1. ตรวจสอบเพจ Facebook ให้แน่ใจก่อนซื้อ โดยกด “เกี่ยวกับ” “ความโปร่งใส” ก็จะเห็นว่าเปิดมานานเท่าใด ผู้จัดการเพจอยู่ประเทศไทยหรือไม่(อยู่ต่างประเทศ ควรหลีกเลี่ยง)</p> <p>2. ดูช่องกดไลค์(มีเครื่องหมาย “โกรธ” ดูโพสต์เป็นหลัก อย่าดูด้านใต้ชื่อเพียงอย่างเดียว เพราะสามารถซื้อ “ไลค์” ได้</p> <p>3. ลองนำชื่อเพจนั้น ไปใส่ช่องค้นหาใน Facebook ว่ามีเพจอื่นอีกหรือไม่ แล้วนำมาเปรียบเทียบกันดูว่า เพจไหนจริง/ปลอม</p> <p>4. “ของดีและถูกเกินกว่าราคาตลาดมากๆ” ให้สงสัยไว้ก่อนว่าหลอกลวง</p> <p>5. บัญชีรับโอนเงินควรเป็นบัญชีชื่อร้าน หากเป็นบัญชีบุคคลธรรมดา ให้สงสัยไว้ก่อนว่าหลอกลวง</p>

คอลเซ็นเตอร์หลอกสั่งข้าวกล่อง
(ให้ Scan QR Code เพื่อควบคุมเครื่อง)

กลโกง	จุดสังเกต	วิธีป้องกัน
<p>1. คนร้ายติดต่อร้านอาหารผ่านแอปพลิเคชันไลน์ หลอกสั่งข้าวกล่องจำนวน 100 กล่อง เพื่อนำไปจัดเลี้ยงประชุม และโอนมัดจำมาก่อน 2,000 บาท</p> <p>2. คนร้ายโทรศัพท์บอกให้ร้านอาหารสั่งชุดอาหารพิเศษเพิ่ม 7 ชุดและบอกว่าจะจ่ายเงินเพิ่มให้ภายหลัง จากนั้นส่ง QR Code มาให้ร้านแอด โดยอ้างว่าเป็น QR Code แอดไลน์เท่านั้น</p> <p>3. เมื่อสแกน QR Code แล้ว คนร้ายจะควบคุมเครื่องโทรศัพท์ เพื่อถอนเงินหรือติดตามการทำงาน</p>	<p>1. บัญชีไลน์ที่ใช้ในการหลอก อาจมีผู้ใช้มากกว่า 1 คน เนื่องจากในเซทมีคำลงท้ายทั้งครับและค่ะ</p> <p>2. QR Code ปลอมใช้โลโก้ไลน์แปะไว้ตรงกลาง ซึ่งทำให้มีผู้หลงเชื่อว่าเป็น QR Code ไลน์จริง จนสามารถหลอกผู้เสียหายได้</p> <p>3. QR Code ปลอมไม่ได้เชื่อมต่อเพื่อเพิ่มเพื่อนผ่านไลน์ แต่เป็นการแฝงลิงก์ดาวน์โหลดมัลแวร์แบบอัตโนมัติ</p>	<p>1. ใช้โปรแกรมหรือแอปพลิเคชันที่สามารถระบุได้ว่าเป็นลิงก์ปลอม</p> <p>2. เมื่อสแกนแล้ว มีการปรากฏลิงก์แปลกปลอม หรือไม่น่าเชื่อถืออย่ากดเข้าไป</p> <p>3. หากเข้าเว็บแปลกปลอมหลังจากสแกนไปแล้ว ให้รีบออกทันที</p> <p>4. มีสติ ปิดเครื่อง ตัดสัญญาณอินเทอร์เน็ตและมีมือถือทันที หากมีการติดตั้งแอปพลิเคชันที่เป็นอันตรายลงไป</p> <p>5. ตรวจสอบให้แน่ใจว่าคุณบัญชีที่ทำธุรกรรมนั้น ได้ทำการซื้อขายสินค้าจริงหรือไม่</p>

คดี Romance Scam หลอกซ้ำซ้อน

กลโกง	จุดสังเกต	วิธีป้องกัน
<p>1. แก๊งกรักออนไลน์ (Romance Scam) ได้ติดต่อพูดคุยกับผู้เสียหายทาง Facebook และเว็บไซต์หาคู่ จากนั้นอ้างว่าอยากมาอยู่เมืองไทย มาใช้ชีวิตคู่กับผู้เสียหาย จะส่งสินค้ามีค่ามาให้</p> <p>2. คนร้ายให้ผู้เสียหายโอนเงินเพื่อชำระภาษี และได้เงินจากผู้เสียหายรอบแรก</p> <p>3. คนร้ายจะหลอกว่าต้องการทำธุรกิจร่วมกับผู้เสียหาย แล้วให้ผู้เสียหายเปิดบัญชีไว้สำหรับการลงทุน</p> <p>4. คนร้ายไปหลอกผู้เสียหายคนที่ 2 และให้โอนเงินเข้าบัญชีผู้เสียหายคนแรก</p> <p>5. คนร้ายให้ผู้เสียหายคนแรก ซื้อเหรียญคริปโตให้คนร้าย บัญชีผู้เสียหายคนแรก กลายเป็นบัญชีม้า (ใช้บัญชีผู้อื่นไปรับโอนเงินจากผู้กระทำผิด)</p>	<p>1. มิฉฉาซีพีมักจะใช้รูปโปรไฟล์ชาวต่างชาติที่มีหน้าตาดีหรือมีประวัติการทำงานที่ดีและมั่นคง ซึ่งข้อมูลและรูปเหล่านี้ได้มาจากหลายๆ แหล่งในอินเทอร์เน็ต</p> <p>2. เมื่อมิฉฉาซีพีสามารถสร้างความเชื่อให้กับผู้เสียหายได้แล้ว ก็จะหลอกให้ผู้เสียหายเปิดบัญชีเพื่อลงทุนหรือเทรดเงินคริปโต</p> <p>3. มิฉฉาซีพีที่ใช้กลโกงลักษณะนี้ มักมีการหลอกให้โอนเงินโดยอ้างว่าชำระค่าภาษี</p>	<p>1. ต้องตรวจสอบตัวตนของคนในโลกโซเชียล เนื่องจากคนร้ายสามารถปลอมแปลงตัวตนรูปภาพ ฯลฯ เพื่อให้เหยื่อหลงเชื่อว่าเป็นของจริง อาจตรวจสอบโดยการโทรพูดคุยผ่าน messenger หรือโทรศัพท์ปกติ เพื่อสังเกตสำเนียงการใช้ภาษาพูดว่าเป็นบุคคลที่กล่าวอ้างหรือไม่</p> <p>2. ถ้ามีการให้เปิดบัญชีเพื่อลงทุนหรือเทรดเงินคริปโตหลังจากสร้างความเชื่อมั่นในระยะเวลายาวนาน ให้ปฏิเสธ และปิดกั้นการสนทนา</p> <p>3. การหาคู่รักผ่านทางออนไลน์ โอกาสประสบความสำเร็จในด้านความรักจริงน้อยกว่าแบบทั่วไป</p> <p>4. ควรเรียนรู้และกระทำการลงทุนหรือเทรดเงินคริปโตด้วยตนเอง ไม่ต้องมีผู้ใดมาสอนให้</p> <p>5. ควรมีสติทุกครั้ง เวลากระทำการธุรกรรมใดๆ กับบุคคลที่สามที่ไม่รู้จัก</p>

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(บัญชีมาหรือซิมม้า) โดยรูหรือควรรูว่าจะนำไปใช้ ในการกระทำความผิด	มีโทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 300,000 บาท หรือ ทั้งจำทั้งปรับ
เปนธุระ จัดหา โฆษณา หรือโฆษณา เพื่อให้มีการ ซื้อขายบัญชี(บัญชีมาหรือซิมม้า) เพื่อใช้ในการกระทำความผิด	จำคุกตั้งแต่ 2 ถึง 5 ปี ปรับตั้งแต่ 200,000 ถึง 500,000 บาท หรือทั้งจำทั้งปรับ
เปนธุระ จัดหา โฆษณา หรือโฆษณา เพื่อให้มีการ ซื้อขายหมายเลขโทรศัพท์ซึ่งลงทะเบียนในนามบุคคลอื่นแล้ว แต่ไม่สามารถระบุตัวผู้โฆษณาจริงได้	จำคุกตั้งแต่ 2 ถึง 5 ปี ปรับตั้งแต่ 200,000 ถึง 500,000 บาท หรือทั้งจำทั้งปรับ

