

LINE ขอยืมเงิน ผู้สูงอายุต้องทำอะไร ก่อนโอน

โดย เอกสยาม ชัยศรี

บริษัท เอกสยาม แอนด์ पार्टเนอร์ส จำกัด

เนื้อหานี้เป็นข้อมูลทั่วไปสำหรับผู้สูงอายุและครอบครัว ไม่ใช่คำแนะนำเฉพาะกรณี ข้อเท็จจริงของแต่ละครอบครัวแตกต่างกัน ควรตรวจกับหน่วยงานหรือผู้เชี่ยวชาญที่เกี่ยวข้องก่อนตัดสินใจ ฉบับออนไลน์ที่ปรับปรุงล่าสุดอยู่ที่ <https://www.sukjaiwaikao.com/article-line-scam.html>

ในบรรดาดีหลอกหลวงออนไลน์ที่น้องเฝ้าพบในช่วงหลายปีที่ผ่านมา มีคดีหนึ่งที่ยังติดอยู่ในใจไม่หาย คุณป้าท่านหนึ่งอายุ 67 ปี โอนเงิน 80,000 บาทให้ "ลูกสาว" ผ่าน LINE เพราะลูกสาวบอกว่าอยู่ต่างจังหวัดแล้วกระเป๋าสตางค์หาย เมื่อโทรกลับหาลูกสาวตัวจริง ลูกสาวตอบว่าไม่รู้เรื่อง: ชื่อและรูปโปรไฟล์ LINE นั้นมีฉฉาฟสร้างขึ้นเอง

เหตุการณ์แบบนี้เกิดขึ้นทุกวันทั่วประเทศ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) รายงานว่าในปี 2566 มีผู้เสียหายจากอาชญากรรมออนไลน์มากกว่า 300,000 ราย โดยรูปแบบ "แอบอ้างเป็นคนรู้จักทาง LINE" ติดอันดับต้นๆ ที่พบบ่อยที่สุด^[1]

300,000+ ผู้เสียหายอาชญากรรมออนไลน์ ปี 2566 (ข้อมูล ETDA)

72 ชม. กรอเวลาตาม พ.ร.ก. 2566 ต้องแจ้งความภายในเวลานี้

1441 สายด่วนรับแจ้ง อาชญากรรมทางเทคโนโลยี 24 ชม.

LINE กลายเป็นเป้าหมายของฉฉาฟได้อย่างไร

LINE เป็นแอปที่คนไทยใช้ตกท้ายกันมากที่สุด: ทั้งครอบครัว เพื่อน และชุมชน วัยเก๋าส่วนใหญ่ไว้วางใจข้อความที่มาจาก LINE มากกว่าโทรศัพท์หรือ SMS เพราะ "เห็นหน้าเห็นชื่อชัดเจน" และความไว้วางใจนี้เองคือจุดที่ฉฉาฟนำมาใช้ประโยชน์



มีงานวิจัยว่าถ้าสามารถทำให้ "ข้อความดูมาจากลูกหลาน" ได้ โอกาสที่ท่านจะโอนเงินโดยไม่ตรวจสอบก็สูงมาก พวกเขาจึงลงทุนเวลาในการสร้างบัญชีปลอมที่เหมือนจริงทุกรายละเอียด

3 เทคนิคโคลนบัญชี LINE ที่มีงานวิจัยใช้

ก่อนจะป้องกันได้ ต้องรู้ก่อนว่าเขาทำอะไร มีงานวิจัยใช้วิธีหลักๆ 3 แบบ:

โคลนโปรไฟล์จาก Facebook

ดึงรูปโปรไฟล์และชื่อจริงจาก Facebook ของลูกหลานที่ตั้งค่าสาธารณะ แล้วสร้างบัญชี LINE ใหม่ที่มีหน้าตาเหมือนกันทุกอย่าง

พบบ่อยมาก

พิชิ่ง QR Code

ส่งลิงก์หรือ QR Code ให้เหยื่อกด เมื่อกดแล้วจะได้รหัส OTP ของ LINE แล้วมีงานวิจัยนำไปใช้เข้าควบคุมบัญชีตัวจริง

อันตรายสูง

วิศวกรรมสังคม (Social Engineering)

หาข้อมูลส่วนตัวจากโซเชียลมีเดีย เช่น ชื่อลูกหลาน อาชีพ ที่อยู่ แล้วสร้างบทสนทนาที่ฟังดูน่าเชื่อถืออย่างมาก

พบบ่อย

ลองดูตัวอย่างบทสนทนาที่มีงานวิจัยใช้ เพื่อให้ท่านเห็นภาพว่ามันหน้าตาเป็นอย่างไร:

ลูกชาย (บัญชีปลอม) กำลังออนไลน์

แม่ครับ อยู่ใหม่เนี่ย รีบหน่อยนะ

09:14

อยู่ๆ มีอะไรเหรอลูก



กระเป๋ายาหยาบครับ ตำรวจก็ยุ่งอยู่ ต้องจ่ายค่าโรงแรมก่อน โอนมาให้ 5,000 ได้มั้ยครับ คินนี้จะคินให้เลย ตอนนี้นี้แบตจะหมดแล้ว

09:16

โอนมาที่ xxx-x-xxxxx-x นะครับ ชื่อ นาย ก. ข. ค. รับผิดชอบ

09:16

นี่คือรูปแบบมาตรฐานของการหลอกลวง: เร่งรัด, บัญชีปลายทางเป็นชื่อคนแปลกหน้า, อ้างว่าแบตจะหมด (เพื่อไม่ให้โทรกลับ)

สัญญาณอันตราย 5 ข้อที่ต้องหยุดทันที

ถ้าเจอสัญญาณเหล่านี้ อย่าเพิ่งโอนเด็ดขาด

- ขอเร่งรัด: "รับผิดชอบ" "ด่วนมาก" "แบตจะหมดแล้ว" สัญญาณคลาสสิกที่สุดเพื่อไม่ให้ท่านมีเวลาคิด
- ชื่อบัญชีปลายทางไม่ตรง: ถ้าลูกชื่อ ก. แต่บัญชีที่ให้โอนไปชื่อ ข.: หยุดทันที
- ห้ามโทรหา: อ้างว่า "โทรไม่ได้ อยู่ในที่ประชุม / สัญญาณไม่ดี / แบตจะหมด"
- ขอโอนก่อนแล้วจะคืนทีหลัง: ลูกหลานจริงๆ จะไม่ขอแบบนี้กับพ่อแม่ผ่านแชท
- ขอข้อมูลส่วนตัวเพิ่มเติม: เลขบัญชี, รหัส OTP: ไม่ว่าใครก็ตามขอ ห้ามให้เด็ดขาด

หากอีกฝ่ายเร่งรัดมาก นั่นคือสัญญาณที่ชัดที่สุดว่าท่านต้อง "ช้าลง": มีงานวิจัยพบว่าท่านจะมีเวลาไตร่ตรอง

หลัก THINK: 5 ขั้นตอนก่อนโอนทุกครั้ง

น้องเอ๋ขอแนะนำหลักง่ายๆ ที่ตอบทุกกรณีได้ เรียกว่า **THINK** ใช้ได้ทุกครั้งที่มีคนขอเงินผ่าน LINE ไม่ว่าจะ เป็นลูกหลาน เพื่อน หรือคนรู้จัก:

T



Talk: โทรด้วยเสียงก่อนเสมอ

โทรหาหมายเลขโทรศัพท์จริงที่บันทึกไว้ในมือถือ **ไม่ใช่**โทรในแอป LINE เพราะมีจาชีพควบคุม LINE ของเหยื่อได้ ถ้าโทรไม่ได้ ให้ส่งข้อความถามเรื่องที่รู้กันเฉพาะสองคน

H

History: ย้อนดูประวัติการสนทนา

เปิดดูการสนทนาหน้า บัญชีโคลนมักไม่มีประวัติการคุยกันเลย หรือมีแค่ไม่กี่ข้อความ บัญชีจริงจะมีประวัติยาวนานย้อนหลัง

I

Identity: ขอยืนยันตัวตนด้วยวิดีโอ

ขอ Video Call ทันที ถ้าปฏิเสธหรืออ้างสารพัดข้อแก้ตัว นั่นคือสัญญาณชัดว่าเป็นมิจฉาชีพ ลูกหลานจริงๆ ยินดีรับสายวิดีโอเสมอเมื่อรู้ว่าพ่อแม่ต้องการยืนยัน แต่ปัจจุบันมิจฉาชีพบางรายใช้ภาพและเสียงปลอมที่สร้างด้วย AI ในวิดีโอคอลได้ จึงควรโทรกลับเบอร์เดิมที่บันทึกไว้ในเครื่องประกอบด้วยเสมอ

N

Number: ตรวจสอบบัญชีปลายทาง

ชื่อบัญชีที่ให้โอนต้องตรงกับชื่อลูกหลานที่ขอ ถ้าไม่ตรง แม้จะอ้างว่า "ยืมบัญชีเพื่อน" ก็ ห้ามโอนเด็ดขาด นี่คือนสัญญาณอันตรายระดับสูงสุด

K

Known: ถามเรื่องที่รู้กันเฉพาะสองคน

ถามเรื่องที่มีเฉพาะลูกหลานจริงๆ เท่านั้นที่รู้ เช่น "ชื่อสุนัขที่บ้านเราชื่ออะไร" "วันเกิดของพ่อคือวันอะไร" มิจฉาชีพตอบไม่ได้แน่นอน



พิมพ์ THINK แปะไว้ที่โทรศัพท์ได้เลย

เขียนตัวอักษร T-H-I-N-K ใส่กระดาษเล็กๆ แล้วแปะไว้ข้างโทรศัพท์ หรือตั้งเป็นวอลเปเปอร์โทรศัพท์ เพราะเวลาตื่นตื่นหรือตกใจ เราต้องการ "ตัวเตือน" มากกว่าความจำ

ความระมัดระวังก่อนโอนเงินสักไม่ก็นาที คุ่มค่ากว่าเสียใจที่หลังมาก (ภาพ: Unsplash)

โอนไปแล้ว: ทำอะไรให้ทันใน 72 ชั่วโมง

ถ้าเกิดเหตุขึ้นแล้ว อย่าเสียเวลาโทษตัวเอง สิ่งที่สำคัญที่สุดคือ **ความเร็ว** พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 กำหนดกรอบเวลาไว้ชัดเจน: เมื่อรับแจ้ง ธนาคารมีหน้าที่ระงับธุรกรรมไว้ชั่วคราว และแจ้งให้ท่านไปร้องทุกข์ต่อพนักงานสอบสวนภายใน **72 ชั่วโมง**:

1. ทันทีที่รู้ตัว

โทรธนาคารของท่านทันที: ขอร้องระงับธุรกรรม

โทรหาเบอร์หลังบัตรเดบิต/เครดิต หรือ Call Center ธนาคาร แจ้งว่าถูกหลอกให้โอนเงิน ขอให้ "ระงับการทำธุรกรรมชั่วคราว" ตาม พ.ร.ก. 2566 ธนาคารมีหน้าที่ต้องดำเนินการทันที

2. ภายใน 1 ชั่วโมง

โทร 1441: ศูนย์ปฏิบัติการต่อต้านอาชญากรรมออนไลน์ (AOC)

สายด่วน 1441 เปิด 24 ชั่วโมง จะช่วยประสานกับธนาคารและหน่วยงานที่เกี่ยวข้องให้อีกช่องทางหนึ่ง เตรียม: เลขที่บัญชีปลายทาง, จำนวนเงิน, เวลาที่โอน, และ screenshot การสนทนา LINE

3. ภายใน 72 ชั่วโมง

แจ้งความที่สถานีตำรวจ: สำคัญมาก

ตามมาตรา 7 แห่ง พ.ร.ก. 2566 เมื่อธนาคารระงับธุรกรรมไว้ชั่วคราวแล้ว จะแจ้งให้ท่านไปร้องทุกข์ต่อพนักงานสอบสวนภายใน 72 ชั่วโมง เมื่อร้องทุกข์แล้ว พนักงานสอบสวนต้องพิจารณาดำเนินการกับบัญชีภายใน 7 วัน หากไม่มีคำสั่งให้ระงับต่อ ธนาคารจะยกเลิกการระงับ จึงควรไปแจ้งความให้เร็วที่สุด

4. ระหว่างทำเรื่อง

รวบรวมหลักฐานให้ครบ

Screenshot บทสนทนา LINE ทั้งหมด, สลิปโอนเงิน, เลขบัญชีปลายทาง, ชื่อและรูปโปรไฟล์ของบัญชีปลอม ยังมีหลักฐานมาก ตำรวจยังสามารถติดตามได้เร็วขึ้น



5. หลังแจ้งความ

ยื่นคำร้องต่อธนาคารปลายทาง

นำหลักฐานและใบแจ้งความไปยื่นต่อธนาคารของผู้รับเงินด้วย เพื่อขอให้ตรวจสอบบัญชีดังกล่าวและอายัดเงินที่ยังเหลือ บางกรณีสามารถได้เงินคืนบางส่วนหรือทั้งหมดได้

อย่ารอ: ทุกนาทีมีความหมาย

มิฉะพียงจะรีบโอนเงินออกจากบัญชีในทันทีที่ได้รับ มักโอนผ่านบัญชีม้าหลายบัญชีภายในชั่วโมงเดียว ยิ่งแจ้งธนาคารช้า โอกาสอายัดเงินยิ่งน้อยลงเรื่อยๆ

กฎหมายที่คุ้มครองท่าน: พ.ร.ก. อาชญากรรมทางเทคโนโลยี 2566

ประเทศไทยมีกฎหมายที่แข็งแกร่งรองรับเหตุการณ์แบบนี้โดยเฉพาะ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 วางกรอบชัดเจนทั้งสิทธิของเหยื่อและโทษของผู้กระทำผิด (ปัจจุบันมีพระราชกำหนดฉบับที่ 2 พ.ศ. 2568 แก้ไขเพิ่มเติม ใช้บังคับตั้งแต่ 13 เมษายน 2568 ข้อความด้านล่างยกจากฉบับ พ.ศ. 2566):

มาตรา 7

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

สิทธิของผู้เสียหาย: ระบุธุรกรรมและกรอบ 72 ชั่วโมง

"ในกรณีที่สถาบันการเงินหรือผู้ประกอบการได้รับแจ้งจากผู้เสียหาย... ให้สถาบันการเงินหรือผู้ประกอบการดังกล่าว มีหน้าที่ระบุการทำธุรกรรม นั้นไว้ชั่วคราว... และ แจ้งให้ผู้เสียหายไป ร้องทุกข์ ต่อ พนักงานสอบสวน ภายในเจ็ดสิบสองชั่วโมง"

สิทธิของท่าน: เมื่อแจ้งธนาคาร ธนาคารมีหน้าที่ระบุธุรกรรมไว้ชั่วคราว และท่านควรไปร้องทุกข์ต่อพนักงานสอบสวนภายใน 72 ชั่วโมง

มาตรา 9

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

โทษสำหรับ "บัญชีม้า": การปล่อยให้คนอื่นใช้บัญชี

"ผู้ใดเปิดหรือยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของตน ทั้งนี้ โดยประการที่รู้หรือควรรู้ว่า จะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด..."

โทษ: จำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ



มาตรา 10

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

โทษสำหรับผู้เป็นธุระจัดหาให้มีการซื้อขาย ให้เช่า หรือให้ยืมบัญชี

"ผู้ใดเป็นธุระจัดหา โฆษณา หรือโฆษณาโดยประการใด ๆ เพื่อให้มีการซื้อ ขาย ให้เช่า หรือให้ยืมบัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ เพื่อใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทาง เทคโนโลยีหรือความผิดทางอาญาอื่นใด"

โทษ: จำคุกตั้งแต่ 2 ปีถึง 5 ปี หรือปรับตั้งแต่ 200,000 บาทถึง 500,000 บาท หรือทั้งจำทั้งปรับ

มาตรา 9 และ 10 สำคัญมากสำหรับลูกหลานและคนรู้จักด้วย บางคนอาจถูกชักชวนให้ "ให้บัญชียืม" โดยไม่รู้ว่าผิดกฎหมาย: กรุณาแชร์ข้อมูลนี้ให้คนในครอบครัวรับทราบด้วย

ตั้งค่าป้องกัน LINE 3 อย่างทำวันนี้ได้เลย

ทำสิ่งเหล่านี้ได้เลย ใช้เวลาไม่เกิน 5 นาที

- ปิด "อนุญาตให้เพิ่มโดยใช้ ID": ไปที่ LINE → ตั้งค่า → ความเป็นส่วนตัว → ปิดตัวเลือก "อนุญาตให้ค้นหา โดย ID" เพื่อไม่ให้คนแปลกหน้าค้นพบบัญชีของท่านได้โดยง่าย
- เปิดล็อก LINE ด้วย Face ID / ลายนิ้วมือ: ตั้งค่า → ความเป็นส่วนตัว → ล็อกแอป ถ้าโทรศัพท์หายหรือถูกขโมย คนอื่นเข้า LINE ไม่ได้
- ไม่ลิงก์ LINE กับ Facebook แบบสาธารณะ: ตรวจสอบว่าโปรไฟล์ Facebook ของท่านและลูกหลานไม่ได้ ตั้งเป็นสาธารณะ (Public) เพราะมีจิวาซีฟใช้รูปและชื่อจาก Facebook ในการโคลนบัญชี LINE

การถูกหลอกไม่ได้แปลว่าท่านไม่รอบคอบ มีจิวาซีฟตั้งใจวางกลอุบายให้ใครก็หลงเชื่อได้: และตอนนี้ท่านรู้ทันแล้ว แชร์บทความนี้ให้ลูกหลานด้วยนะครับ เพราะเขาก็อาจถูกแอบอ้างในชื่อของเขาด้วยเหมือนกัน

แหล่งอ้างอิง

1. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA). (2566). รายงานสถานการณ์ภัยออนไลน์ประจำปี 2566. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. www.etda.or.th
2. พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566. ราชกิจจานุเบกษา เล่ม 140 ตอนที่ 18 ก วันที่ 16 มีนาคม 2566. มาตรา 7, 9, 10.
3. กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.). (2566). สถิติคดีอาชญากรรมทางเทคโนโลยี ปี 2566. สำนักงานตำรวจแห่งชาติ. thaipoliceonline.go.th



4. กรมกิจการ ผู้สูงอายุ กระทรวง การพัฒนา สังคม และ ความมั่นคง ของ มนุษย์. (2566). คู่มือ รู้เท่าทัน ภัย ดิจิทัล สำหรับ ผู้สูงอายุ. www.dop.go.th
5. ธนาคารแห่งประเทศไทย. (2567). แนวทางป้องกันภัยทางการเงินออนไลน์สำหรับผู้บริโภค. www.bot.or.th

