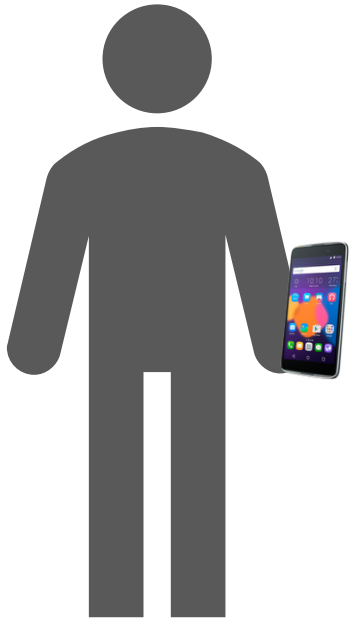
360

100,000

o

15,000



โลกข้อมูลส่วนบุคคลในโทรศัพท์

รู้ทันกลโกงออนไลน์
(Online Scam Awareness)

ถอดรหัสกลโกง ถอดเทคนิคมิจฉาชีพ การปกป้องตนเอง และขั้นตอนการรับมือเมื่อตกเป็นผู้เสียหาย

พ.ต.อ. เกรียงไกร พุทไธสง | ผู้กำกับการกลุ่มงานสนับสนุนทางไซเบอร์ บก.ตอท.

09.00 - 10.30

ภาพรวมสถานการณ์กลโกง

Scam Trends, รู้ทันตัวเอง และรู้ทันกลโกงจิตวิทยา 3 รูปแบบ

10.45 - 12.00

เจาะลึกแคสแอปดูดเงิน

กระบวนการติดมัลแวร์ ตั้งแต่ SMS จนถึงเงินถูกดูดออกจากบัญชี

13.00 - 14.30

รู้ทันเทคโนโลยี

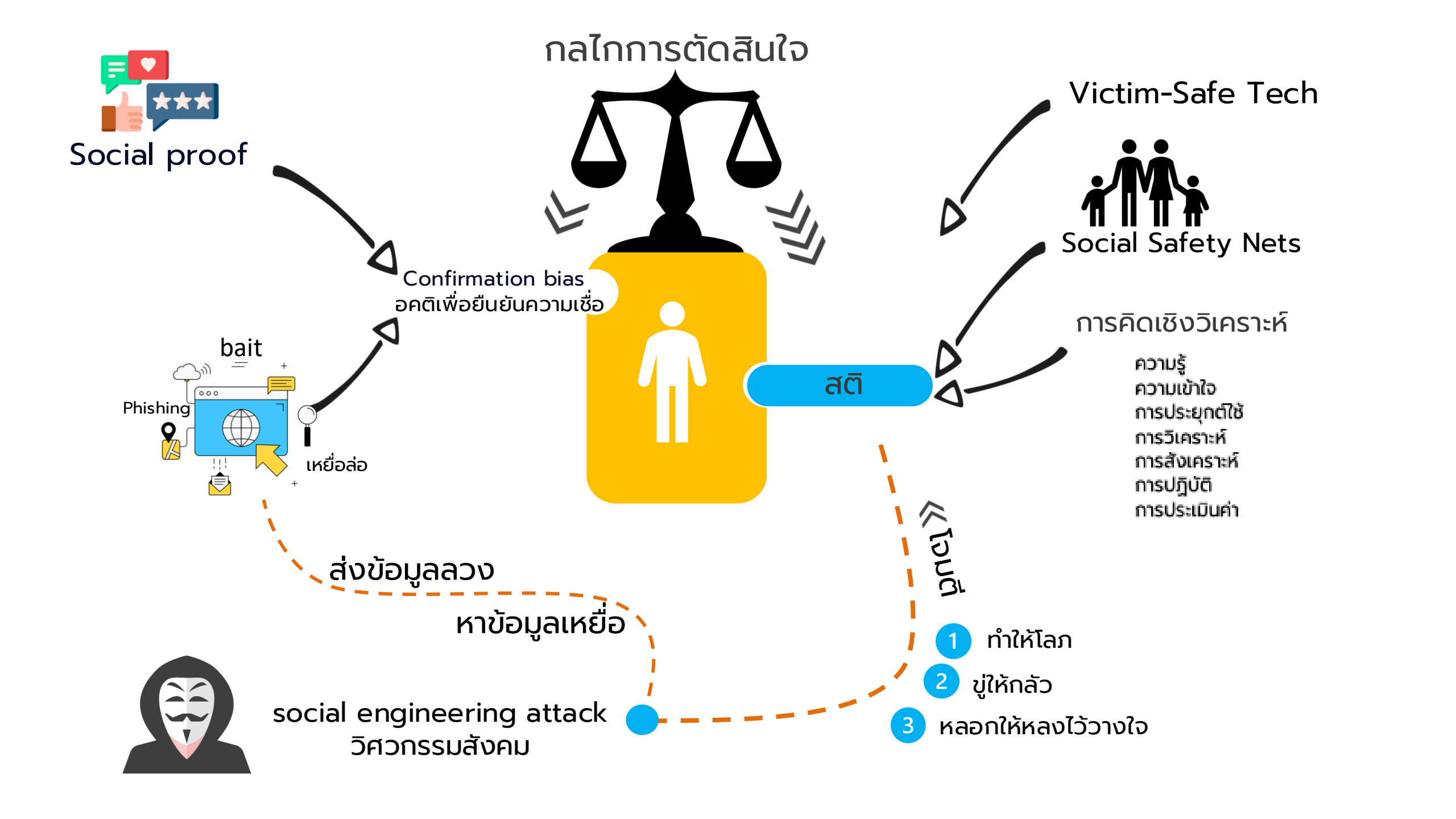
การปกป้องอุปกรณ์ และฝึกปฏิบัติใช้แอป Police Care ตรวจมิจฉาชีพ

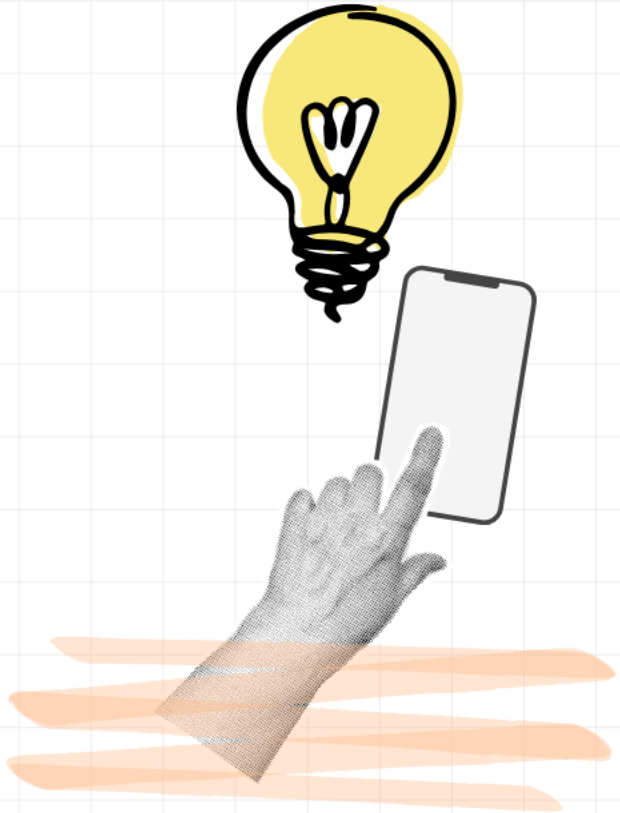
14.45 - 16.30

กระบวนการเมื่อเกิดเหตุ

การเตรียมหลักฐาน แจ้งความออนไลน์ และทดสอบวัคซีนไซเบอร์


12:58:12
LIVE
โหนกระแส
"ชาล็อต" เสียท่า ถูกมิจฉี้อ้างเป็นตำรวจ หลอกโอนเงิน 4 ล้าน


กลไกการตัดสินใจ
Social proof
Confirmation bias
อคติเพื่อยืนยันความเชื่อ
bait
Phishing
เหยื่อล่อ
Victim-Safe Tech
Social Safety Nets
การคิดเชิงวิเคราะห์
สติ
ความรู้
ความเข้าใจ
การประยุกต์ใช้
การวิเคราะห์
การสังเคราะห์
การปฏิบัติ
การประเมินค่า
ส่งข้อมูลลวง
หาข้อมูลเหยื่อ
social engineering attack
วิศวกรรมสังคม
โจมตี
1 ทำให้โลภ
2 ขู่ให้กลัว
3 หลอกให้หลงไว้วางใจ



ภัยไซเบอร์ปัจจุบัน (CURRENT CYBER THREATS)

ภัยคุกคามไร้พรมแดนที่ยกระดับเป็นขบวนการอาชญากรรมข้ามชาติ มีความซับซ้อนสูงและปรับเปลี่ยนรูปแบบอย่างรวดเร็ว โดยผสานการใช้จิตวิทยา (เช่น แผนประทุษกรรมแบบ Hybrid Scam ที่หลอกให้รักแล้วชวนลงทุน) เข้ากับเทคโนโลยีขั้นสูง (เช่น การใช้ AI หรือ Deepfake เพื่อสร้างความน่าเชื่อถือ) มุ่งเป้าหมายโจมตีเหยื่ออย่างเจาะจง เพื่อสร้างความเสียหายทางการเงินมูลค่ามหาศาล

มีสติ

Mindfulness

การหยุดคิดทบทวนและควบคุมอารมณ์ก่อนตัดสินใจทำธุรกรรม หรือให้ข้อมูลส่วนบุคคล ไม่ตื่นตระหนกไปกับสถานการณ์บีบบังคับหรือคำขู่ และไม่หลงเชื่อความโลภจากผลตอบแทนที่สูงเกินจริง เพื่อตัดวงจรความเร่งรีบที่มิจฉาชีพจงใจสร้างขึ้น

รู้ทันกลโกง

Understanding Modus Operandi

การทำความเข้าใจแผนประทุษกรรมและรูปแบบการหลอกลวงที่ปรับเปลี่ยนอยู่เสมอ เช่น การหลอกให้รักแล้วชวนลงทุน การหลอกให้ทำภารกิจ หรือกลฉ้อโกงออนไลน์ต่างๆ เพื่อให้สามารถสังเกตเห็นจุดผิดปกติ และรู้พฤติกรรมของคนร้ายได้ทันท่วงที

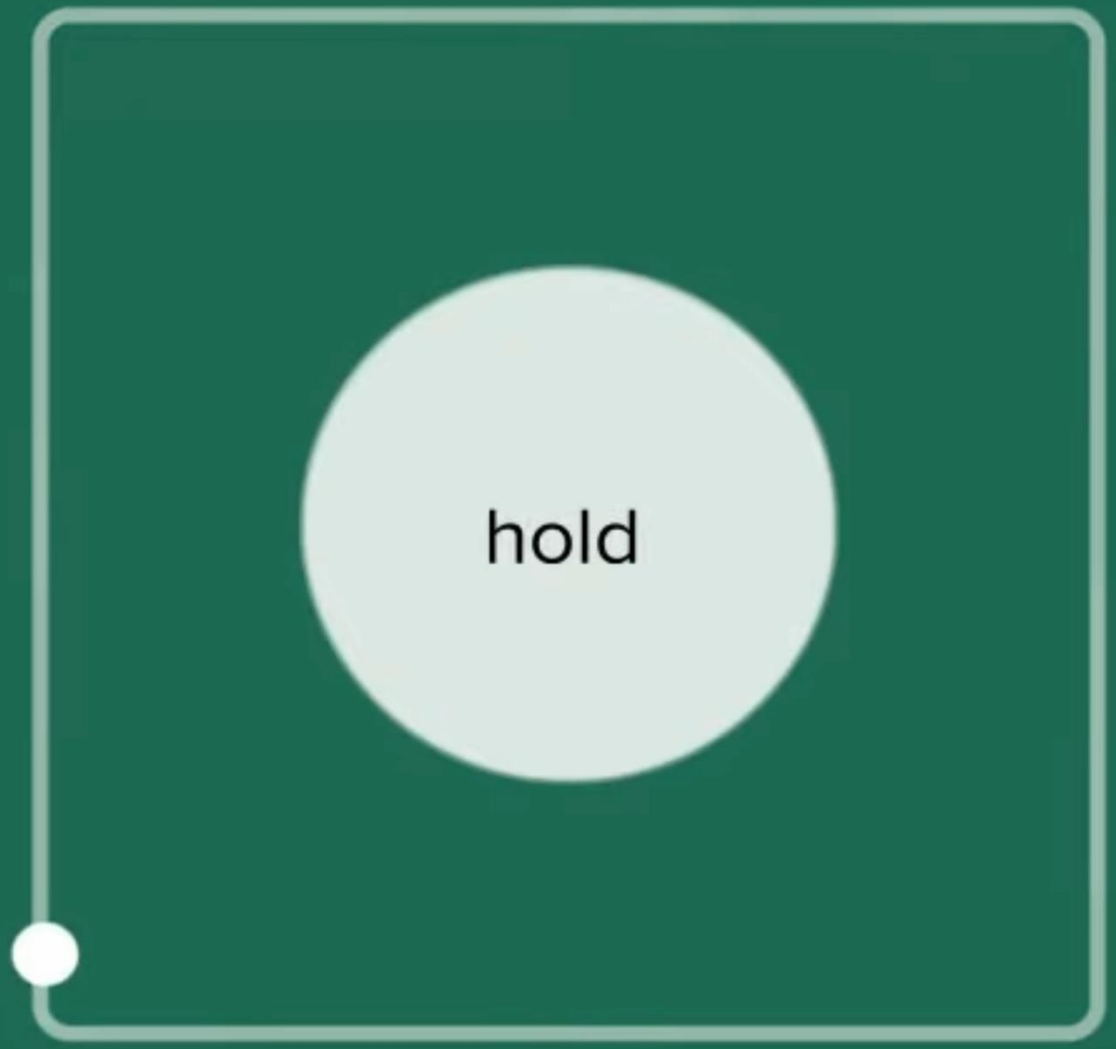
เท่าทันเทคโนโลยี

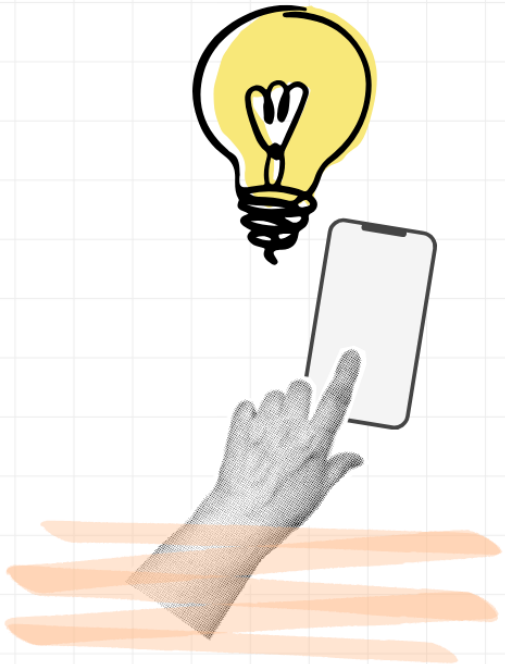
Technological Literacy

การอัปเดตความรู้เกี่ยวกับเครื่องมือดิจิทัลและภัยคุกคามรูปแบบใหม่ เช่น การใช้ AI โคลนเสียงและสร้างภาพปลอม (Deepfake) หรือแอปพลิเคชันแฝงมัลแวร์ดูดเงิน รวมถึงรู้วิธีการป้องกันตัวเองเบื้องต้น เช่น การตั้งค่าความเป็นส่วนตัว การไม่กดลิงก์อันตราย และการตรวจสอบแหล่งที่มาของข้อมูล

การสร้างความตระหนักรู้

“การข่มขู่ทางโทรศัพท์ Call Center”


hold



ภัยไซเบอร์ปัจจุบัน (CURRENT CYBER THREATS)

ภัยคุกคามไร้พรมแดนที่ยกระดับเป็นขบวนการอาชญากรรมข้ามชาติ มีความซับซ้อนสูงและปรับเปลี่ยนรูปแบบอย่างรวดเร็ว โดยผสานการใช้จิตวิทยา (เช่น แผนประทุษกรรมแบบ Hybrid Scam ที่หลอกให้รักแล้วชวนลงทุน) เข้ากับเทคโนโลยีขั้นสูง (เช่น การใช้ AI หรือ Deepfake เพื่อสร้างความน่าเชื่อถือ) มุ่งเป้าหมายโจมตีเหยื่ออย่างเจาะจง เพื่อสร้างความเสียหายทางการเงินมูลค่ามหาศาล

มีสติ

Mindfulness

การหยุดคิดทบทวนและควบคุมอารมณ์ก่อนตัดสินใจทำธุรกรรมหรือให้ข้อมูลส่วนบุคคล ไม่ตื่นตระหนกไปกับสถานการณ์บีบบังคับหรือคำขู่ และไม่หลงเชื่อความโลภจากผลตอบแทนที่สูงเกินจริง เพื่อตัดวงจรความเร่งรีบที่มิจฉาชีพจงใจสร้างขึ้น

รู้ทันกลโกง

Understanding Modus Operandi

การทำความเข้าใจแผนประทุษกรรมและรูปแบบการหลอกลวงที่ปรับเปลี่ยนอยู่เสมอ เช่น การหลอกให้รักแล้วชวนลงทุน การหลอกให้ทำภารกิจ หรือกลฉ้อโกงออนไลน์ต่างๆ เพื่อให้สามารถสังเกตเห็นจุดผิดปกติ และรู้พฤติกรรมของคนร้ายได้ทันท่วงที

เท่าทันเทคโนโลยี

Technological Literacy

การอัปเดตความรู้เกี่ยวกับเครื่องมือดิจิทัลและภัยคุกคามรูปแบบใหม่ เช่น การใช้ AI โคลนเสียงและสร้างภาพปลอม (Deepfake) หรือแอปพลิเคชันแฝงมัลแวร์ดูดเงิน รวมถึงรู้วิธีการป้องกันตัวเองเบื้องต้น เช่น การตั้งค่าความเป็นส่วนตัว การไม่กดลิงก์อันตราย และการตรวจสอบแหล่งที่มาของข้อมูล

Cyber Support Unit

แนวโน้มรูปแบบกลโกง

กลโกง

ล่อลวงด้วยความโลภ

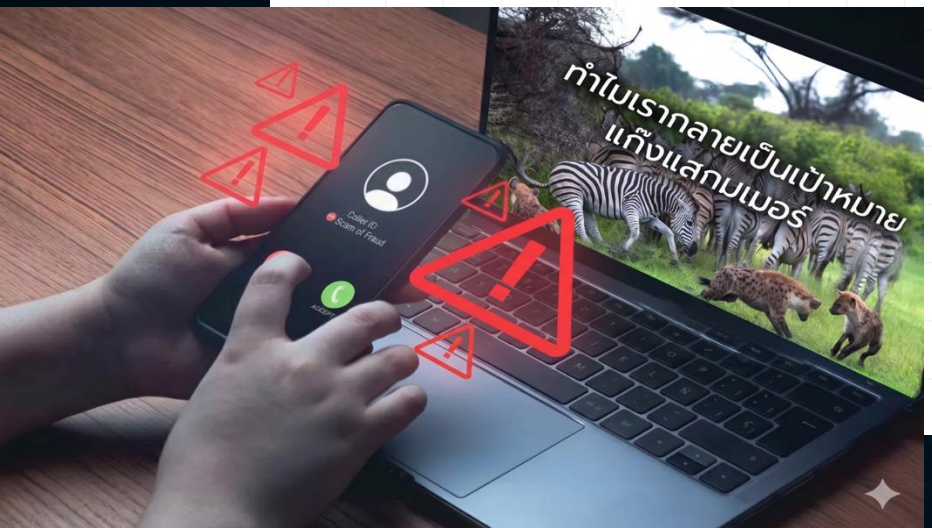
- หลอกทำภารกิจ
- หลอกขายของออนไลน์
- หลอกลงทุนแอบอ้างคนดัง
- หลอกคืนเงินค่าสินค้า

ข่มขู่ให้หวาดกลัว

- ทวงเงินกู้โดยข่มขู่คนรอบข้าง
- การแบล็กเมล์ ข่มขู่ด้วยภาพลับ หรือข้อมูลส่วนตัว
- อ้างเป็นเจ้าหน้าที่ขู่ว่าพัวพันคดีฟอกเงินหรือพัสดุผิดกฎหมาย

หลอกให้หลงไว้วางใจ

- หลอกให้รักแล้วส่งของหรือทางผ่านบัญชี
- หลอกให้รักแล้วลงทุน Pig-Butchering
- ติดตั้งแอปปลอม/ดูดเงินในบัญชี/เก็บข้อมูล



รู้ทันกลโกง E-commerce Scams: หลอกผู้ซื้อ vs หลอกผู้ขาย

2.1 ฝั่งหลอกผู้ซื้อ (Fake Sellers)

- เปิดเพจปลอม/ร้านปลอม
- เมื่อเหยื่อโอนเงินแล้วจะบล็อกหนี ส่งกล่องเปล่า ส่งของไม่ตรงปก

2.2 ฝั่งหลอกผู้ขาย (Fake Buyers)

- ทำทีมาขอซื้อสินค้า จากนั้นส่ง "สลิปโอนเงินปลอม" หรือโอนเงินเกินยอดจริงแล้วขอให้แม่ค้าโอนเงินทอนคืน
- ทำทีมาขอซื้อสินค้า และชวนไปเปิดร้านขายออนไลน์เพื่อเพิ่มยอดขายหรือส่ง link ให้กด

2. การเข้าถึงตัวเหยื่อ (Contact Method)

- ยิงแอดโฆษณา (Sponsored)
- ทักแชท (Inbox) โดยตรงหาร้านค้า หรือทักส่วนตัวหาคนที่โพสต์ขายของมือสอง

3. จุดอุกที่คนร้ายใช้ (The Hook)

ราคาถูกเกินจริง

ความเร่งรีบ โอนด่วน!

- “เช็คก่อนโอน”
- ตรวจ: “ความเป็นโปรงไสของเพจ”
- ตรวจ: การยืนยันตัวตน

- ยึดแอปธนาคารเป็นหลัก
- ไม่กด link แปลกปลอมที่ไม่รู้แหล่งที่มา

Cyber Support Unit

ข้อสังเกตประกอบการสืบสวน

เพจมีเครื่องหมายยืนยัน (Verified) ไม่ได้หมายความว่าปลอดภัยแสมอไป

กรณีตรวจสอบเพจขายสินค้าใน Facebook จำเป็นต้องตรวจสอบข้อมูลอื่นเพิ่มเติม

ข้อมูลเพจที่ตรวจสอบ

เจ๊หน่อย ปูม้าระยอง & เนื้อปูแกะ ทั้งปลีก-ส่ง

พบเครื่องหมายยืนยันจากระบบ

ผู้ติดตาม 4.8 พัน คน

ขายส่งอาหาร ฿฿

2 ข้อสังเกตเบื้องต้น

1. พบผู้เสียหายหลายรายแจ้งว่า สั่งซื้อสินค้าแล้ว **ไม่ได้รับสินค้า**
2. ค้นหาเพจดังกล่าวใน Facebook พบว่าเพจมีเครื่องหมายยืนยัน (Verified)
3. อย่างไรก็ตาม ยังต้องตรวจสอบข้อมูลอื่นประกอบ **ไม่ควรเชื่อถือจากเครื่องหมายยืนยันเพียงอย่างเดียว**

3 ประวัติการเปลี่ยนชื่อเพจ

ข้อสังเกต: มีการเปลี่ยนชื่อเพจเรื่อยมา

24 เมษายน 2026	เจ๊หน่อย ปูม้าระยอง & เนื้อปูแกะ ทั้งปลีก-ส่ง
26 พฤศจิกายน 2025	เจ๊จุ เนื้อปูแกะ & ปูม้าระยอง พร้อมเสิร์ฟถึงหน้าบ้าน ทั้งปลีก-ส่ง
30 กรกฎาคม 2024	เจ๊หน่อยระยอง ปูม้า & เนื้อปูแกะ พร้อมเสิร์ฟถึงหน้าบ้าน ทั้งปลีก-ส่ง

4 ตำแหน่งของผู้จัดการเพจ

ข้อสังเกต: ผู้จัดการเพจอยู่หลายประเทศ

Myanmar	(3)
India	(1)
Japan	(1)

อ้างอิงข้อมูลจาก Facebook Page Transparency

5 ประเด็นที่ควรตรวจสอบเพิ่มเติม

- ประวัติการเปลี่ยนชื่อเพจ
- ประเทศ/ภูมิภาคของผู้จัดการเพจ
- รีวิว คำร้องเรียน หรือข้อมูลผู้เสียหาย
- บัญชีรับชำระเงินและช่องทางติดต่อ
- รูปแบบการโฆษณาและพฤติการณ์การขาย

สรุป: เครื่องหมาย Verified เป็นเพียงข้อมูลหนึ่งในการพิจารณา ไม่ใช่หลักฐานยืนยันความน่าเชื่อถือทั้งหมด

แผนประทุษกรรม: กลโกงสามเส้า (ABC Scam) แบบไฮบริด (Hybrid) - กรณีขายรถมือสอง

Phase 1: ONLINE

ขั้นที่ 1: ขั้นตอนออนไลน์ (Online)

สร้างเหยื่อ

1. มิจฉาชีพ (B) สวมรอยเป็นผู้ซื้อ

A. เจ้าของรถจริง (A) หรให้วิรายละเอียนละรูป และรูวาเหยานกัน

B. มิจฉาชีพ (B)

2. มิจฉาชีพ (B) นำรูปและข้อมูลไปโพสต์ขาย ถูกกว่าท้องตลาด

C. ผู้ซื้อจริง (C) ถูกตับสนใจ

Phase 2: ON-SITE & CLOSING

ขั้น: 2A: หลอกลวงทุกฝ่าย (ABC แท้)

3. นัดดูรถหน้างาน (On-site)

- **หลอกสับขาหลอก**
  - บอก A: เดี๋ยวแฟน/ลูกน้อง (คือ C) ไปดูแทน
  - บอก C: เดี๋ยวพี่ชาย/ญาติ (คือ A) เอารถไปให้ดู

4. ทำสัญญา & โอนเงิน

C โอนเงิน → บัญชีม้า (ของ B)

ผลลัพธ์: มิจฉาชีพหนี -> A ไม่ปล่อยรถ -> C ไม่ได้รถ

2B: ร่วมมือกัน (Collusion / จัดฉาก)

3. นัดดูรถและตรวจสภาพหน้างาน

มิจฉาชีพร่วมมือกับเจ้าของรถหรือจัดฉาก

4. ทำสัญญา

5. กุลอุบายโอนอีกบัญชีหนึ่ง

* อ้างบัญชีเดิมมีปัญหา สรรพากรตรวจอยู่

* โอนเข้าบัญชีบุคคลที่สาม (คือ บัญชีม้า)

บัญชีม้า (ของ B)

ข้อสังเกตและข้อควรระวัง

- ✓ **ตรวจสอบ:** ชื่อคนขาย = ชื่อในเล่มทะเบียน = ชื่อในสัญญา = ชื่อบัญชีธนาคาร (บุคคลเดียวกัน)
- ✓ **ระวัง!:** หากผู้จัดการหรือเจ้าของรถตัวจริงให้โอนเงินเข้าบัญชีบุคคลอื่นโดยอ้างเหตุผลสารพัด
- ✓ **ห้าม!:** โอนเงินเข้าบัญชีคนอื่นเด็ดขาด

Cyber Support Unit

รู้ทันกลโกง: หลอกทำภารกิจ (Task Scams)

1. วิธีการ/รูปแบบ (Modus Operandi)

เริ่มต้น: งานง่ายๆ (กดไลก์/รีวิว/แชร์) ได้เงินจริงทันที (หลักร้อย)

ต่อมา: ดึงเข้า **“กลุ่ม VIP”** ผลตอบแทนสูงขึ้น

สุดท้าย: บังคับ **“สำรองเงินล่วงหน้า”** ถอนเงินไม่ได้ (อ้างผิดขั้นตอน/ภาษี)

2. การเข้าถึงตัวเหยื่อ (Contact Method)

- **โฆษณาโซเชียลมีเดีย:** รับสมัครงาน Work from Home/พาร์ทไทม์
- **ส่ง SMS/LINE ตรง:** อ้างเป็นฝ่ายบุคคลบริษัทดัง

3. จุดฮุกที่คนร้ายใช้ (The Hook)

"เงินง่าย ได้จริงตอนแรก": สร้างความเชื่อใจ (Trust)

"หน้าม้าในกลุ่ม": ส่งสลิปปลอม โชว์กำไร กระตุ้นความโลภ

จัดทำโดย เมษา เจ้าหน้าที่สืบสวนอาชญากรรมทางเทคโนโลยี

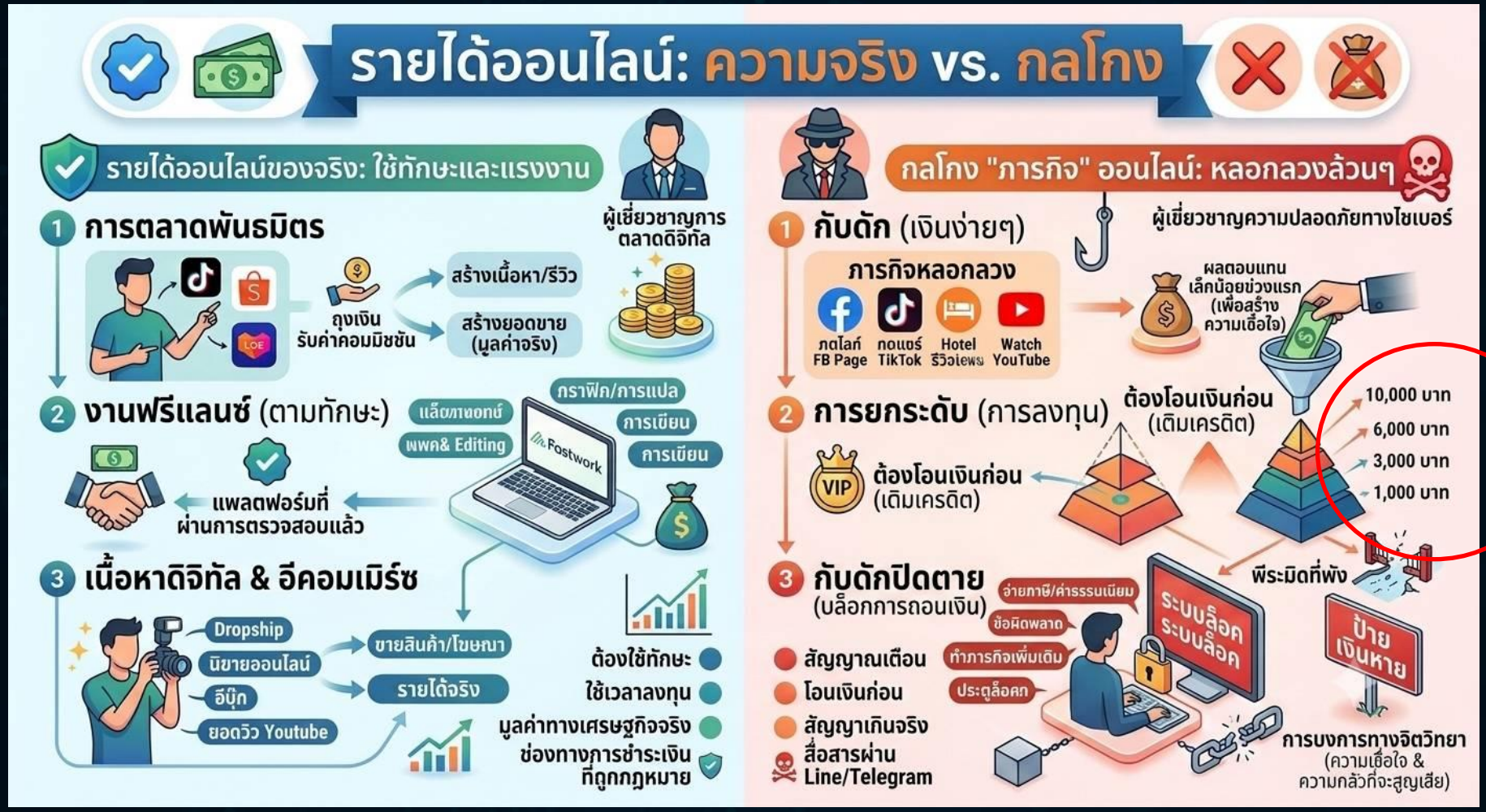
4. จุดที่จะทำให้เหยื่อรอดพ้น (Survival Point)

โล่ป้องกัน

- **ทางรอด:** จำประโยคทอง! **"งานจริง ต้องได้เงิน ไม่ใช่เสียเงิน!"**
- **คำต้องห้าม:** "สำรองจ่าย / เติมเงิน / เปิดพอร์ต" = โจร 100%
- **"เช็กบัญชี":** โอนเข้า/ออก หลายชื่อ บัญชีบุคคล = บัญชีม้า เสี่ยงสูง!


แผนประทุษกรรม! กลโกงสวมรอยบริษัทจริง หลอกโอนเงิน 2 ต่อ
ระวัง! ถูกสั่งให้โอนเข้าบัญชีบุคคลธรรมดาหลังโอนเข้าบริษัท
STEP 1
1. เพจปลอม ก๊อปเหมือน 100%
AD
Ice Maker Machine
999 บาท
ยิงโฆษณาขายของราคาถูกผิดปกติ
STEP 2
2. โอนครั้งแรก "บัญชีบริษัทจริง"
บริษัทจำกัด
เพื่อให้เหยื่อตายใจว่าไม่โดนโกง
STEP 3
3. ล่อเข้าไลน์ "ทำภารกิจ"
LINE
เข้ากลุ่มรับของแถม/เงินคืน
STEP 4
4. โอนครั้งที่ 2 "บัญชีม้า"
บัญชีบุคคลธรรมดา
ยอดสูงหลักหมื่น! ไม่โอนอดได้สินค้า
STEP 5
5. บริษัทจริงกลายเป็น "จำเลย"
POLICE
ถูกแจ้งความและอายัดบัญชี
คนร้ายลอยนวลพร้อมเงิน
NotebookLM


แผนร้าย "หลอกขายเครื่องทำน้ำแข็ง": รู้ทันก่อนหมดตัว!
1. ก๊อปปี้เพจเนียน 100%
บริษัทจริง
เพจปลอม
ใช้ชื่อและรูปโปรไฟล์เหมือนบริษัทจริงทุกกระเบียดนิ้ว แล้วระดมยิงโฆษณาหาเหยื่อ
2. ล่อซื้อด้วยราคา 999 บาท
999 บาท
ตั้งราคาถูกผิดปกติเพื่อกระตุ้นให้เหยื่อรีบตัดสินใจโอนเงิน
3. ใช้บัญชีบริษัทจริงเป็น "ทางผ่าน"
โอนเงินยอดแรก
บัญชีบริษัทจริง
TRUSTED
ให้เหยื่อโอนเงินยอดแรกเข้าบัญชีบริษัทจริงๆ เพื่อสร้างความน่าเชื่อถือว่าไม่ได้โกง
4. ล่อเข้า Line ไปเชือดเพิ่ม
LINE
ภารกิจ
กิจกรรม
โอนเงินเพิ่มหลักหมื่น!
อ้างว่าต้องทำกิจกรรม/ภารกิจก่อนส่งของ สุดท้ายหลอกให้โอนเงินเพิ่มเป็นหลักหมื่น
NotebookLM


รายได้ออนไลน์: ความจริง vs. กลโกง
รายได้ออนไลน์ของจริง: ใช้ทักษะและแรงงาน
ผู้เชี่ยวชาญการตลาดดิจิทัล
1 การตลาดพันธมิตร
ถุงเงิน
รับค่าคอมมิชชัน
สร้างเนื้อหา/รีวิว
สร้างยอดขาย (มูลค่าจริง)
2 งานฟรีแลนซ์ (ตามทักษะ)
กราฟิก/การแปล
การเขียน
การเขียน
แพลตฟอร์มที่ผ่านการตรวจสอบแล้ว
Fastwork
3 เนื้อหาดิจิทัล & อีคอมเมิร์ซ
Dropship
นิขายออนไลน์
อีบุ๊ก
ยอดวิว Youtube
ขายสินค้า/โฆษณา
รายได้จริง
ต้องใช้ทักษะ
ใช้เวลาลงทุน
มูลค่าทางเศรษฐกิจจริง
ช่องทางการชำระเงินที่ถูกกฎหมาย
กลโกง "ภารกิจ" ออนไลน์: หลอกลวงล้วนๆ
ผู้เชี่ยวชาญความปลอดภัยทางไซเบอร์
1 กับดัก (เงินง่ายๆ)
ภารกิจหลอกลวง
กดไลก์ FB Page
กดแชร์ TikTok
Hotel รีวิวโรงแรม
Watch YouTube
ผลตอบแทนเล็กน้อยช่วงแรก (เพื่อสร้างความเชื่อใจ)
2 การยกระดับ (การลงทุน)
ต้องโอนเงินก่อน (เติมเครดิต)
VIP
ต้องโอนเงินก่อน (เติมเครดิต)
10,000 บาท
6,000 บาท
3,000 บาท
1,000 บาท
พีระมิดที่พัง
3 กับดักปิดตาย (บล็อกการถอนเงิน)
สัญญาณเตือน
โอนเงินก่อน
สัญญาเกินจริง
สื่อสารผ่าน Line/Telegram
ค่าธรรมเนียม
ข้อผิดพลาด
ทำภารกิจเพิ่มเติม
ประตูล็อค
ระบบล็อค
ระบบล็อค
ป้าย เงินหาย
การบงการทางจิตวิทยา (ความเชื่อใจ & ความกลัวที่จะสูญเสีย)

รู้ทันกลโกง: หลอกลงทุนแอบอ้างคนดัง (Fake endorsement)

1. วิธีการ/รูปแบบ (Modus Operandi)

ชักชวนให้ลงทุนในหุ้น
คริปโทฯ หรือกองทุนรวม
โชว์กราฟพอร์ตสวยหรู

จ่ายปันผลจริง
ในเดือนแรกๆ

แต่พอลงเงินก้อนใหญ่
ระบบจะปิดตัวหนี

2. การเข้าถึงตัวเหยื่อ (Contact Method)

ยิงแอดโฆษณาบนโซเชียล หรือสร้าง
เพจข่าวปลอม (Fake News)

ชวนเข้ากลุ่ม LINE โอเพนแชท ที่มี
"อาจารย์/โค้ช" คอยนำเทรด

3. จุดฮุกที่คนร้ายใช้ (The Hook)

ความน่าเชื่อถือปลอม
Phony profile

การันตีผลตอบแทนสูงลิ่ว
(เช่น ได้กำไร 20-30% ต่อเดือน)

AI

จัดทำโดย เนษา เจ้าหน้าที่สืบสวนอาชญากรรมทางเทคโนโลยี

4. จุดที่จะทำให้เหยื่อรอด (Survival Point)

โล่ป้องกัน

- การลงทุนที่การันตีผลตอบแทนสูง = หลอกลวง
- หน่วยงานรัฐหรือบุคคลที่มีชื่อเสียง ไม่มีทาง ชักชวนให้ประชาชนโอนเงินลงทุน เข้า "บัญชีบุคคลธรรมดา (บัญชีม้า)" หรือสอนเทรดผ่านกลุ่ม LINE
- การลงทุนมีความเสี่ยง : ตรวจสอบทุกขั้นตอนการลงทุนเสมอ

Check First

Diyabundesert

Cyber Support Unit

AI

Real-time Face Swap

Deepfake

วิจารณญาณ

Cyber Support Unit

ระวัง! กลโกงหลอกคืนสินค้า / หลอกคืนเงิน (Fake Refunds & Recovery Scams)

1. วิธีการ/รูปแบบ (Modus Operandi)

แอบอ้างบริษัทดัง:
อ้างเป็นพนักงาน Shopee, Lazada, HomePro

สินค้ามีปัญหา:
อ้างสินค้าชำรุดต้องการคืนเงิน

หลอกให้สแกน QR Code หรือกดลิงก์:
หลอกว่าโอนเงินเกิน:

2. การเข้าถึงตัวเหยื่อ (Contact Method)

โทรศัพท์มาหาโดยตรง
ส่ง SMS แนบลิงก์

3. จุดฮุกที่คนร้ายใช้ (The Hook)

ความหวังที่จะได้เงินคืน (Hope)

เชื่อมโยงกับเรื่องจริงที่เหยื่อซื้อสินค้านั้นๆ

อย่าสแกน QR Code: ห้ามสแกน QR Code ที่คนแปลกหน้าส่งมาให้เพื่อรับเงินเด็ดขาด เพราะโดยปกติการรับเงินคืนเพียงแค่บอกเลขบัญชีหรือเบอร์พร้อมเพย์ก็เพียงพอแล้ว

ตรวจสอบแอปพลิเคชันโดยตรง: หากมีการอ้างว่าคืนเงินจากแอปช้อปปิ้ง ให้ตรวจสอบสถานะการสั่งซื้อและคุยกับเจ้าหน้าที่ผ่าน แชทในแอปพลิเคชันหลัก เท่านั้น

กลโกง

ล่อลวงด้วยความโลภ

- หลอกทำภารกิจ
- หลอกขายของออนไลน์
- หลอกลงทุนแอบอ้างคนดัง
- หลอกคืนเงินค่าสินค้า

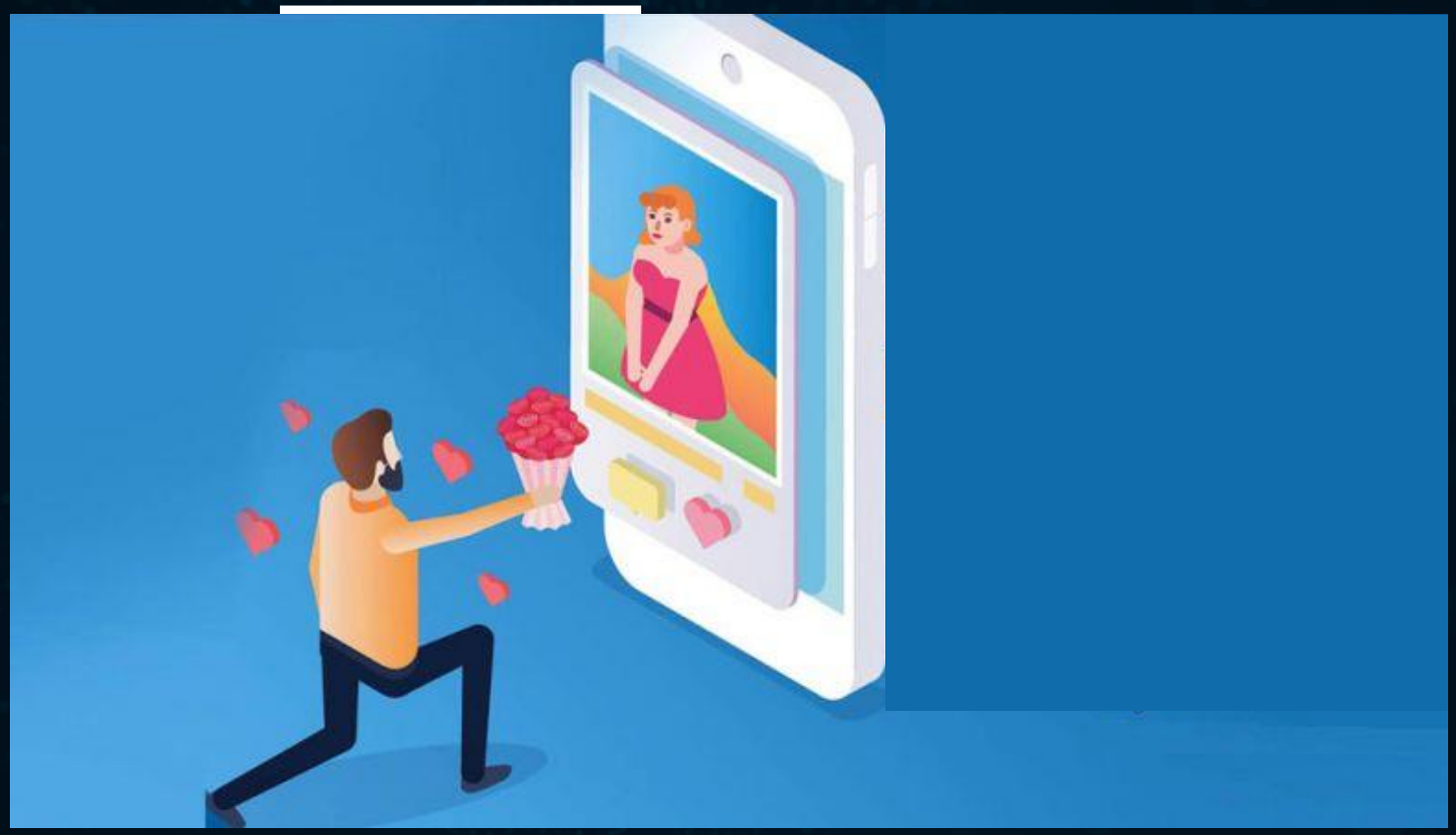
ข่มขู่ให้หวาดกลัว

- ทวงเงินกู้โดยข่มขู่คนรอบข้าง
- การแบล็กเมล์ ข่มขู่ด้วยภาพลับ หรือข้อมูลส่วนตัว
- อ้างเป็นเจ้าหน้าที่ขู่ว่าพัวพันคดีฟอกเงินหรือพัสดุผิดกฎหมาย

หลอกให้หลงไว้วางใจ

- หลอกให้รักแล้วส่งของหรือทางผ่านบัญชี
- หลอกให้รักแล้วลงทุน Pig-Butchering
- ติดตั้งแอปปลอม/ดูดเงินในบัญชี/เก็บข้อมูล

Cyber Support Unit



Sextortion

Cyber Support Unit

สคริปต์คำพูดมาตรฐาน

01

โยนความผิด (สายที่ 1 - พนักงานธนาคาร/ค่ายมือถือ/ไปรษณีย์)

สวัสดีค่ะ ติดต่อจากธนาคาร.../ค่ายมือถือ... ตรวจสอบพบว่ามีการนำชื่อและบัตรประชาชนของคุณไปเปิดบัญชี/เปิดเบอร์มือถือที่จังหวัด... (มักเป็นจังหวัดไกลๆ) และถูกนำไปใช้ฉ้อโกงประชาชน/ฟอกเงิน คุณทราบเรื่องนี้ไหมคะ?

ข้อมูลส่วนตัวตรง

02

เสนอตัวช่วยเหลือและโอนสาย (การสร้างความตระหนก)

ถ้าคุณไม่ได้ทำ คุณต้องรีบไปแจ้งความที่ สภ. (จังหวัดที่อ้างถึง) ภายใน 2 ชั่วโมงนะคะ ไม่อย่างนั้นบัญชีของคุณทุกธนาคารจะถูกอายัด... คุณสะดวกเดินทางไปไหมคะ? ถ้าไม่สะดวกเดี๋ยวทางเราจะบริการ 'โอนสาย' ให้คุยกับร้อยเวรโดยตรงค่ะ

03

ตำรวจรับแจ้งความ (สายที่ 2 - ตำรวจระดับปฏิบัติการ)

สภ... ยินดีรับใช้ครับ ขอทราบชื่อนามสกุล... เดี๋ยวผมเช็กประวัติในระบบให้ (ทำทีเป็นพิมพ์คอมพิวเตอร์/มีเสียงวิทยุสื่อสารแทรก) ...โอ้โห! คุณมีรายชื่อเป็นผู้ต้องสงสัยพัวพันคดีฟอกเงินรายใหญ่ร่วมกับนาย... (ชื่อสมมติ) ตอนนี้ศาลออกหมายจับแล้วนะครับ!

สร้างสภาพแวดล้อมการทำงาน

04

ข่มขู่และแยกเหยื่อ (สายที่ 3 - ตำรวจระดับสูง/สารวัตร)

ผมสารวัตร... เป็นหัวหน้าชุดสืบสวน คดีนี้เป็นคดีลับสุดยอด ห้ามคุณบอกใครเด็ดขาด ให้คุณเดินไปหาที่เงียบๆ อยู่คนเดียว ล็อกประตู และห้ามวางสายผมแอดไลน์ สภ. มา เดี๋ยวผมจะส่งหมายศาลให้ดู" (จากนั้นจะส่งภาพหมายจับ/หมายเรียกปลอมที่มีชื่อและเลขบัตรประชาชนของเหยื่อครบถ้วน)

ข้อมูลปลอม

05

ปิดจ๊อบดูดเงิน (THE EXTORTION)

เพื่อแสดงความบริสุทธิ์ใจ คุณต้องโอนเงินจากทุกบัญชีที่คุณมี มาที่ 'บัญชีกลางของ ปปง. / ธนาคารแห่งประเทศไทย' เพื่อให้เจ้าหน้าที่ตรวจสอบเส้นทางการเงินว่าไม่มีส่วนเกี่ยวข้องกับยาเสพติด หากตรวจสอบแล้วว่าบริสุทธิ์ จะโอนคืนให้ภายใน 24 ชั่วโมง" (หากเหยื่อเชื่อและโอนเงิน มิจฉาชีพจะหลอกให้กู้เงินเพิ่ม/เอาเงินพ่อแม่

แยกเหยื่อความเร่งด่วน

Cyber Support Unit

กลโกง

ล่อลวงด้วยความโลภ

- หลอกทำภารกิจ
- หลอกขายของออนไลน์
- หลอกลงทุนแอบอ้างคนดัง
- หลอกคืนเงินค่าสินค้า

ข่มขู่ให้หวาดกลัว

- ทวงเงินกู้โดยข่มขู่คนรอบข้าง
- การแบล็กเมล์ ข่มขู่ด้วยภาพลับ หรือข้อมูลส่วนตัว
- อ้างเป็นเจ้าหน้าที่ขู่ว่าพัวพันคดีฟอกเงินหรือพัสดุผิดกฎหมาย

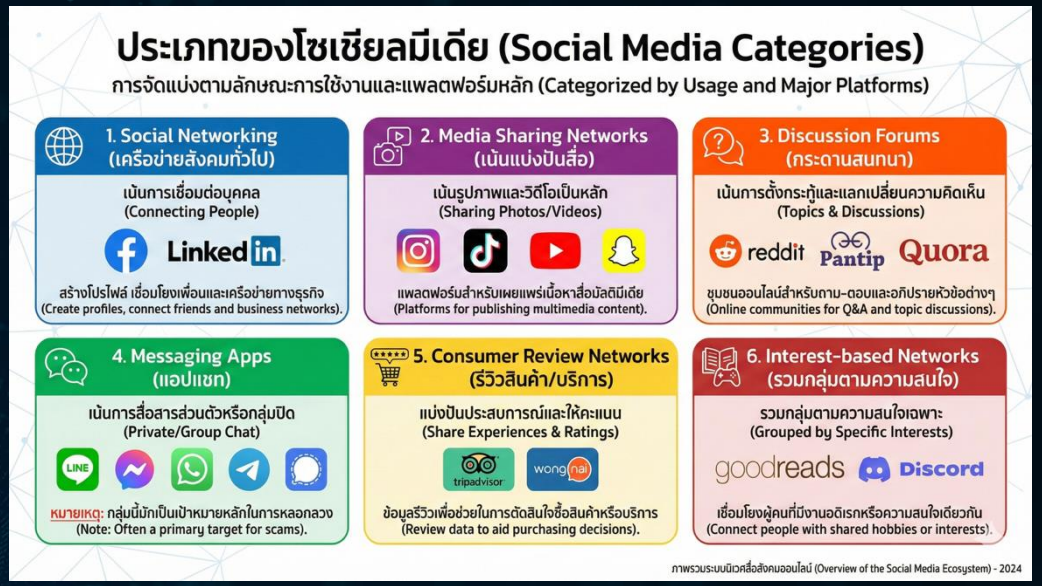
หลอกให้หลงไว้วางใจ

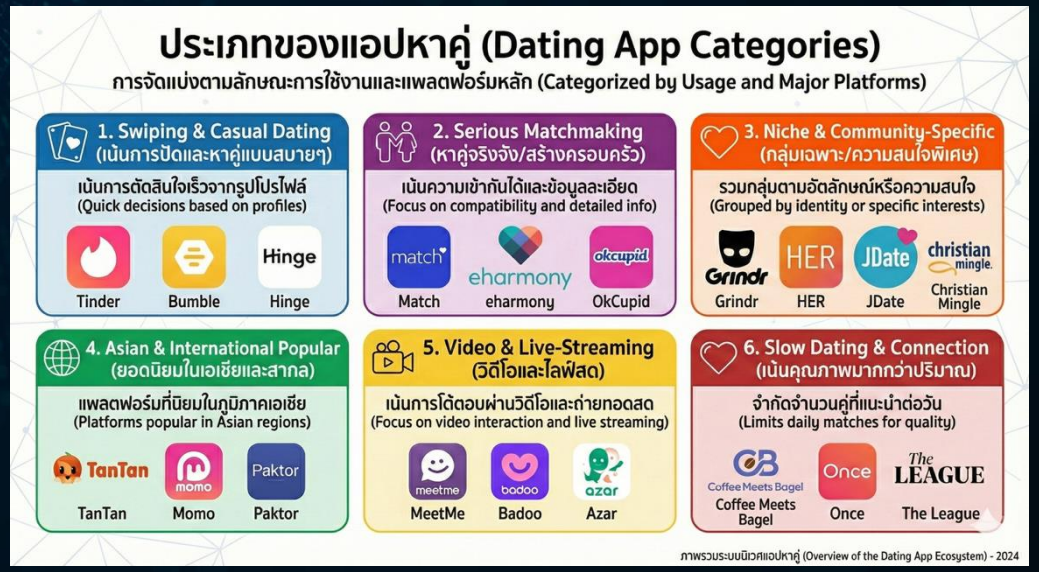
- หลอกให้รักแล้วส่งของหรือทางผ่านบัญชี
- หลอกให้รักแล้วลงทุน Pig-Butchering
- ติดตั้งแอปปลอม/ดูดเงินในบัญชี/เก็บข้อมูล

Cyber Support Unit

ทางแยก

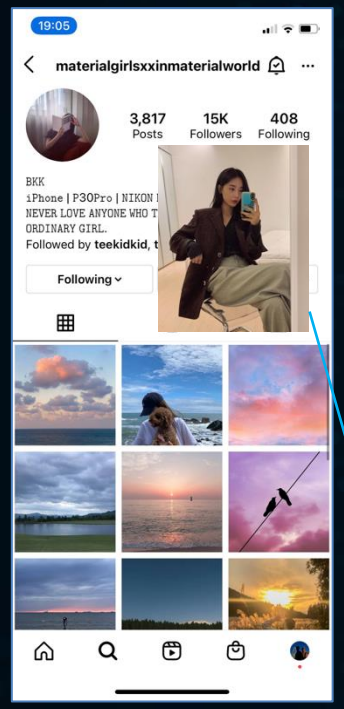
FAKE RICH
Sadfishing
Faith-based

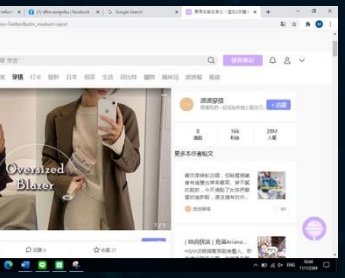


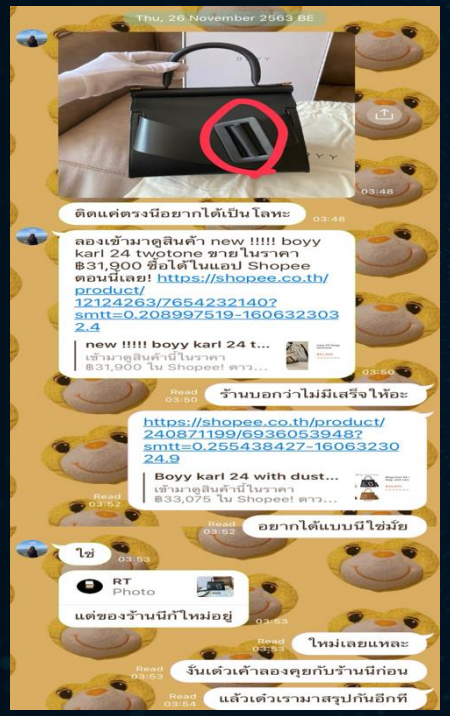


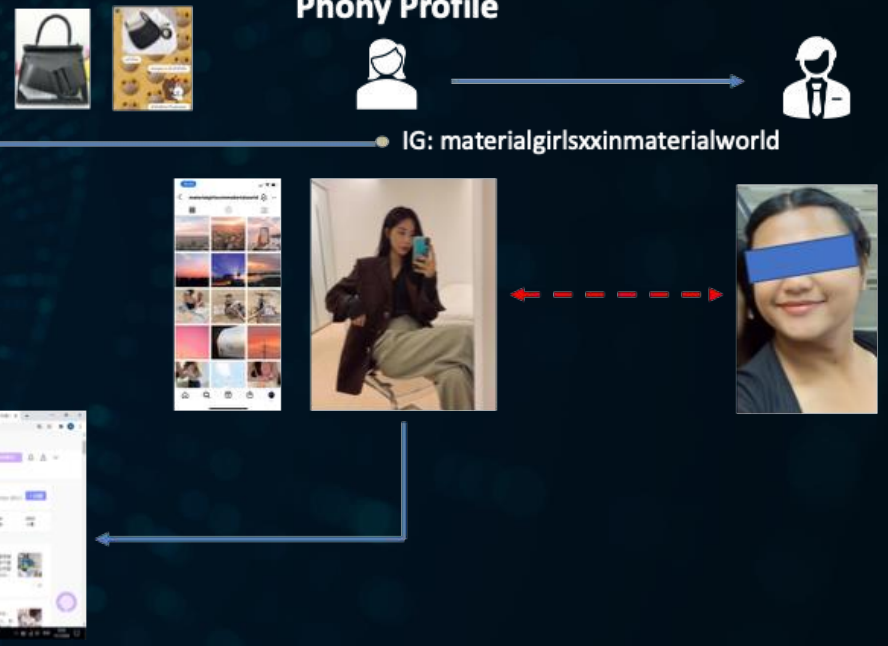
Cyber Support Unit

Relationship and Trust Fraud

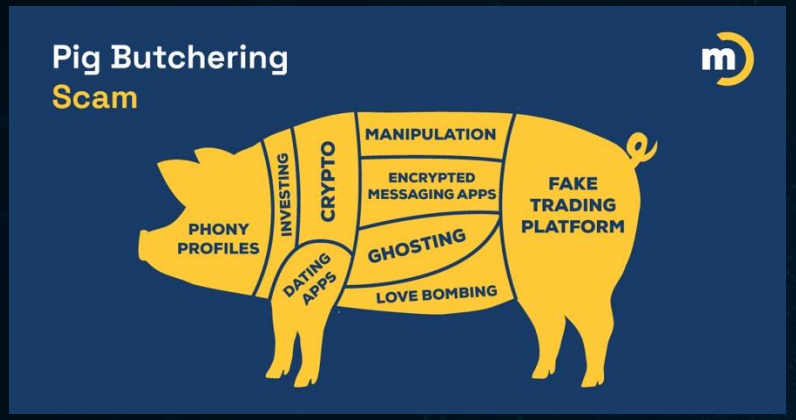








Cyber Support Unit



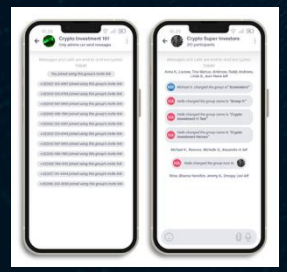
- Letting you speak first
- Giving you no time to decide
- Moving Goalposts

Phony Profile

Social Engineering

AI

กลุ่มใหญ่



ห้องเชือด

09.00 - 10.30

ภาพรวมสถานการณ์กลโกง

Scam Trends, รู้ทันตัวเอง และรู้ทันกลโกงจิตวิทยา 3 รูปแบบ

10.45 - 12.00

เจาะลึกแคสแอปดูดเงิน

กระบวนการติดมัลแวร์ ตั้งแต่ SMS จนถึงเงินถูกดูดออกจากบัญชี

13.00 - 14.30

รู้ทันเทคโนโลยี

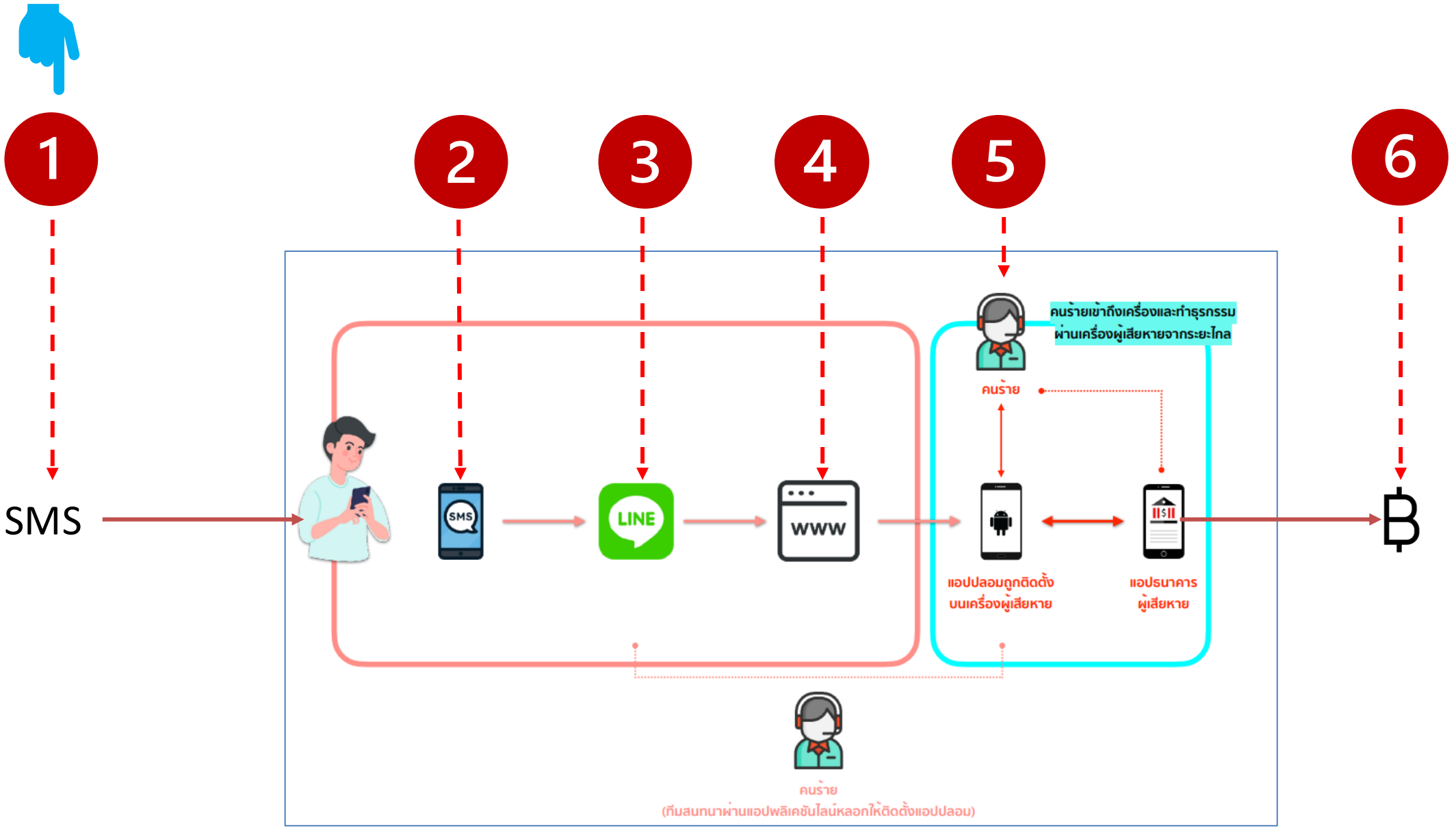
การปกป้องอุปกรณ์ และฝึกปฏิบัติใช้แอป Police Care ตรวจมิจฉาชีพ

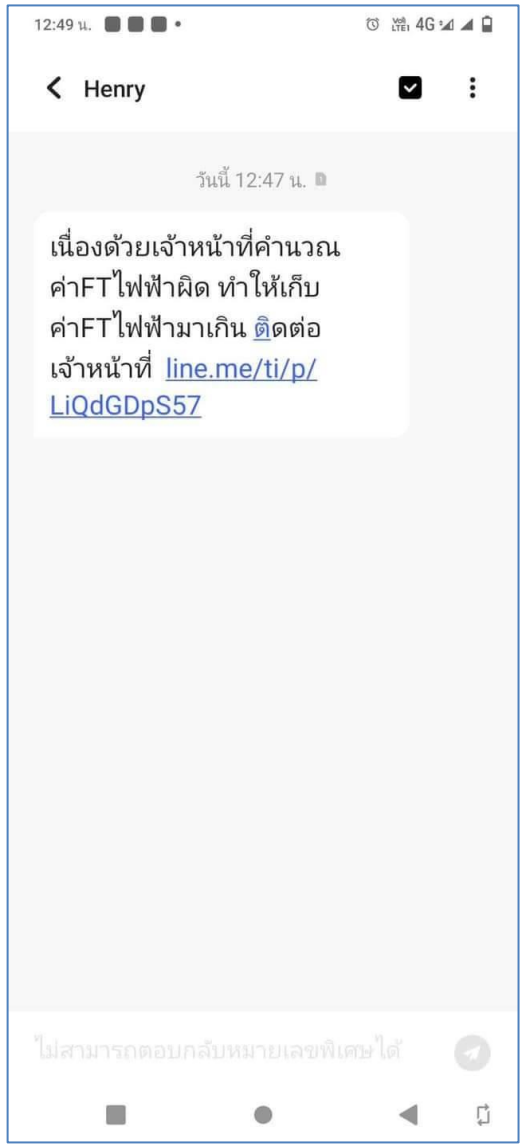
14.45 - 16.30

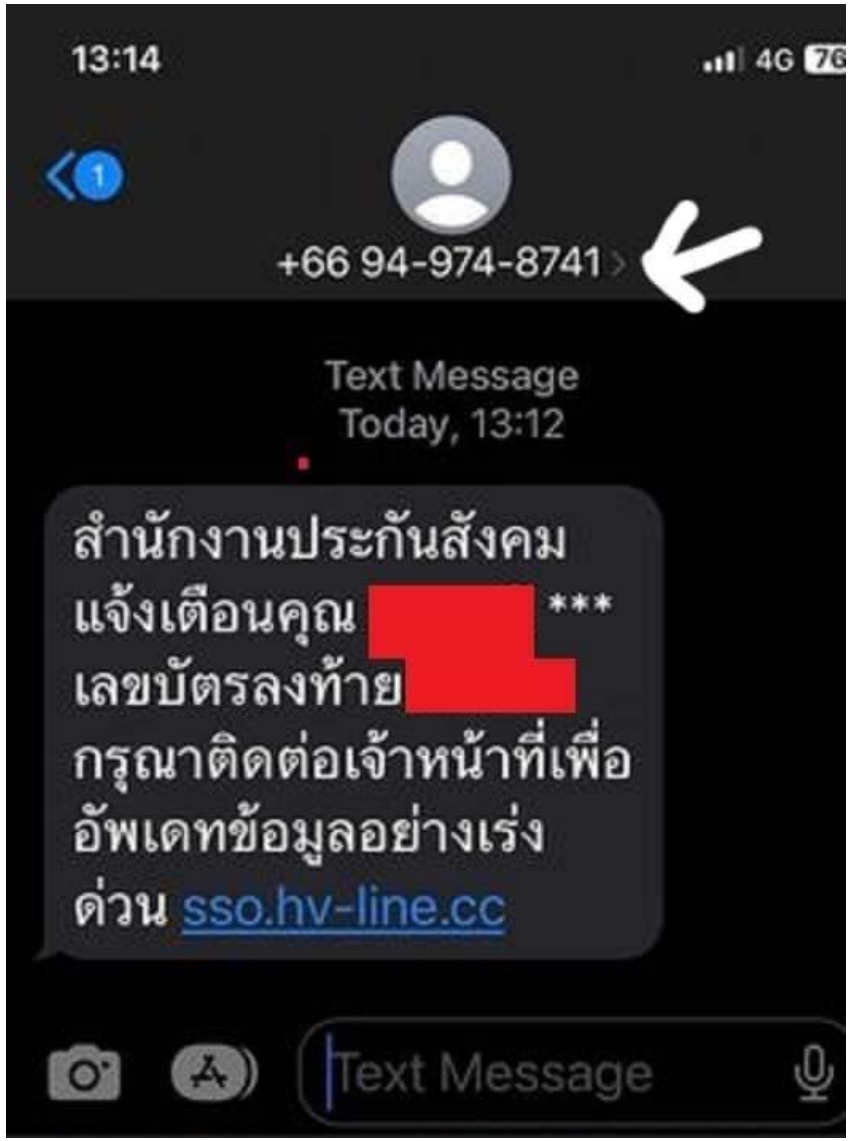
กระบวนการเมื่อเกิดเหตุ

การเตรียมหลักฐาน แจ้งความออนไลน์ และทดสอบวัคซีนไซเบอร์

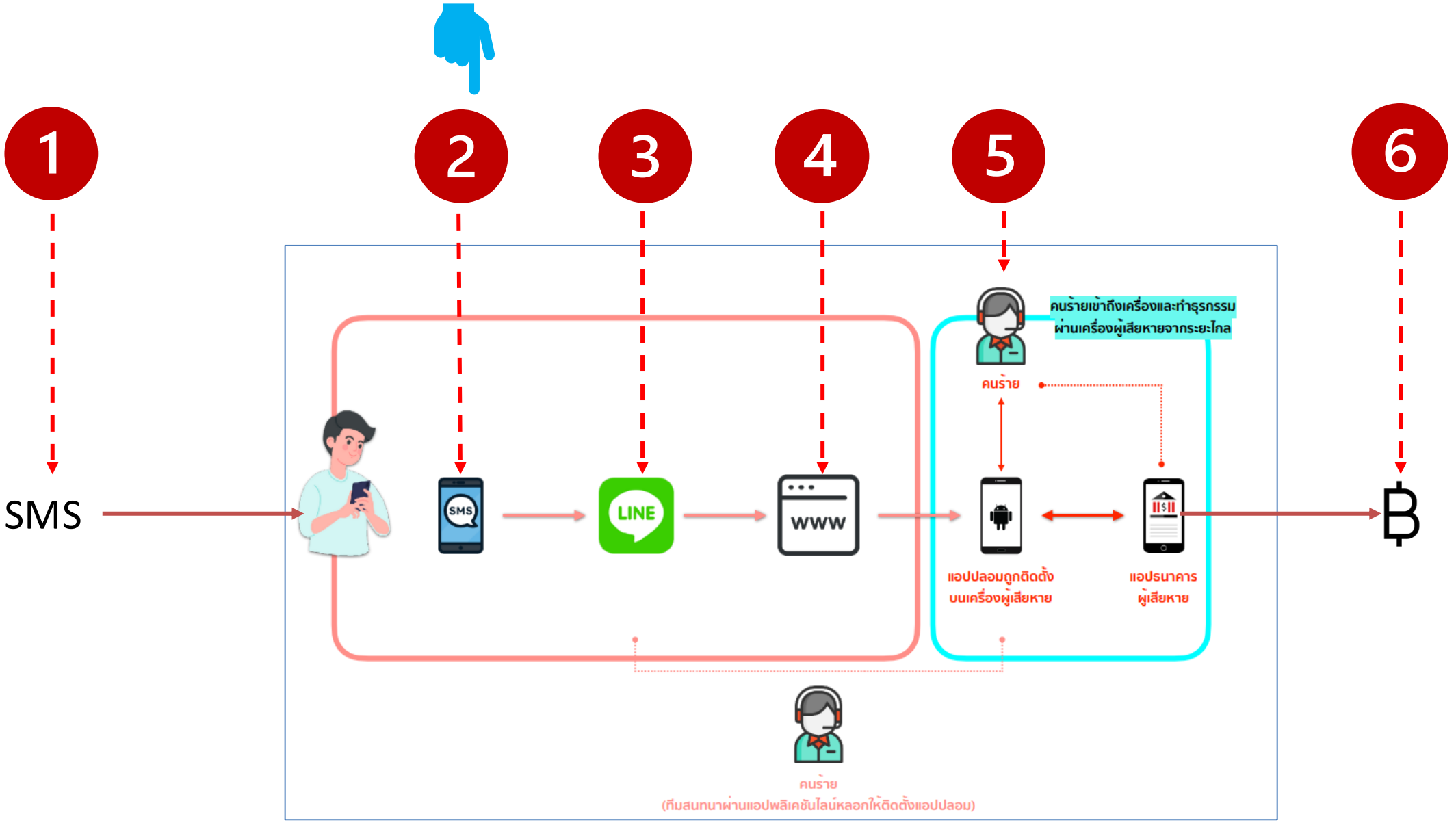

TikTok
chuicom07

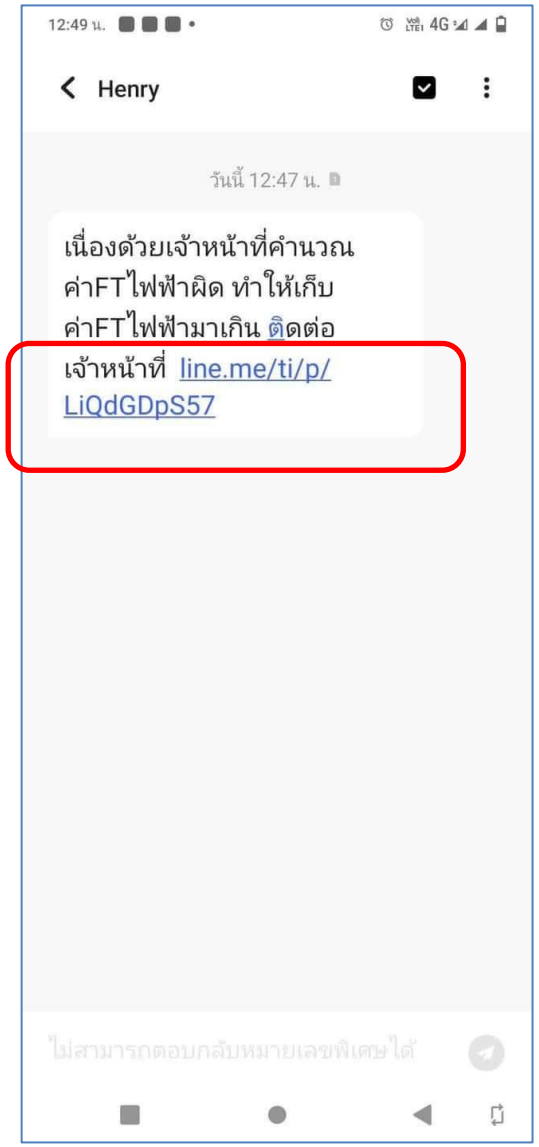

1
2
3
4
5
6
SMS
SMS
LINE
WWW
คนร้ายเข้าถึงเครื่องและทำธุรกรรม
ผ่านเครื่องผู้เสียหายจากระยะไกล
คนร้าย
แอปปลอมถูกติดตั้ง
บนเครื่องผู้เสียหาย
แอปธนาคาร
ผู้เสียหาย
คนร้าย
(ทีมสนทนาผ่านแอปพลิเคชันไลน์หลอกให้ติดตั้งแอปปลอม)

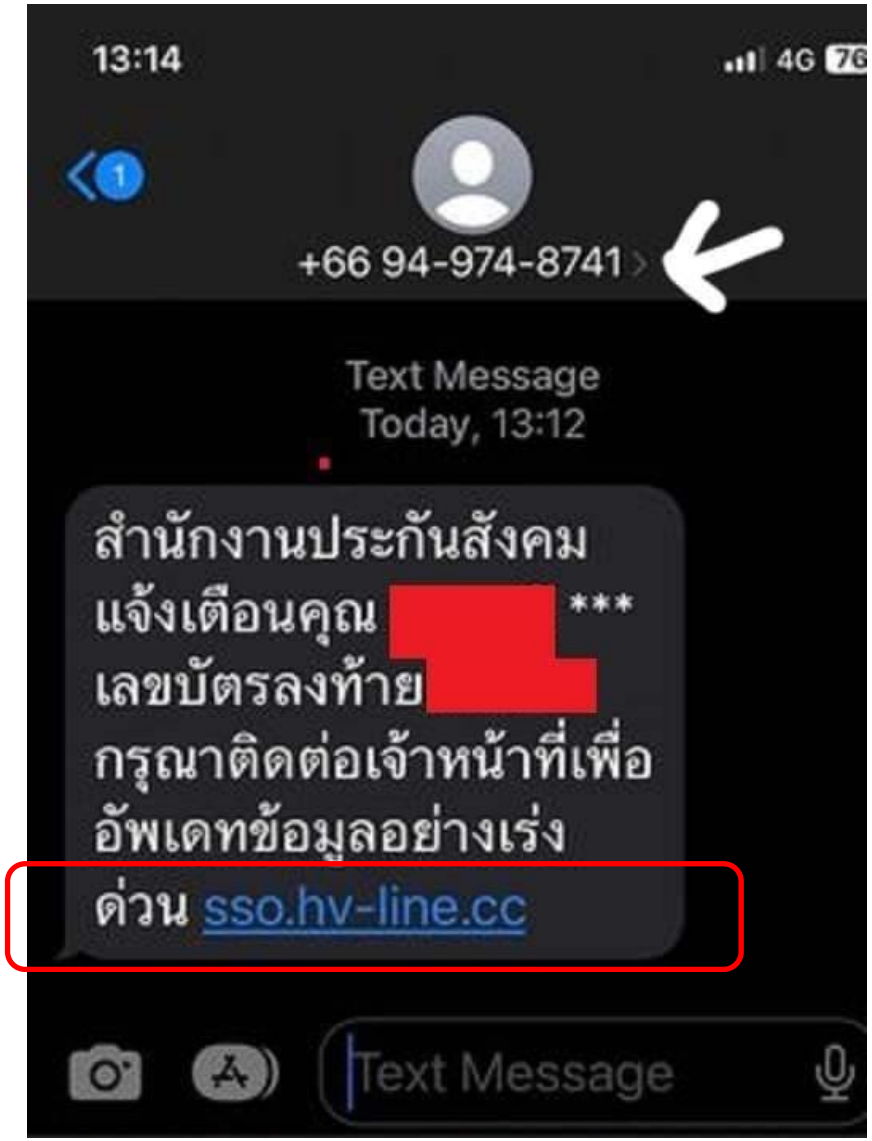




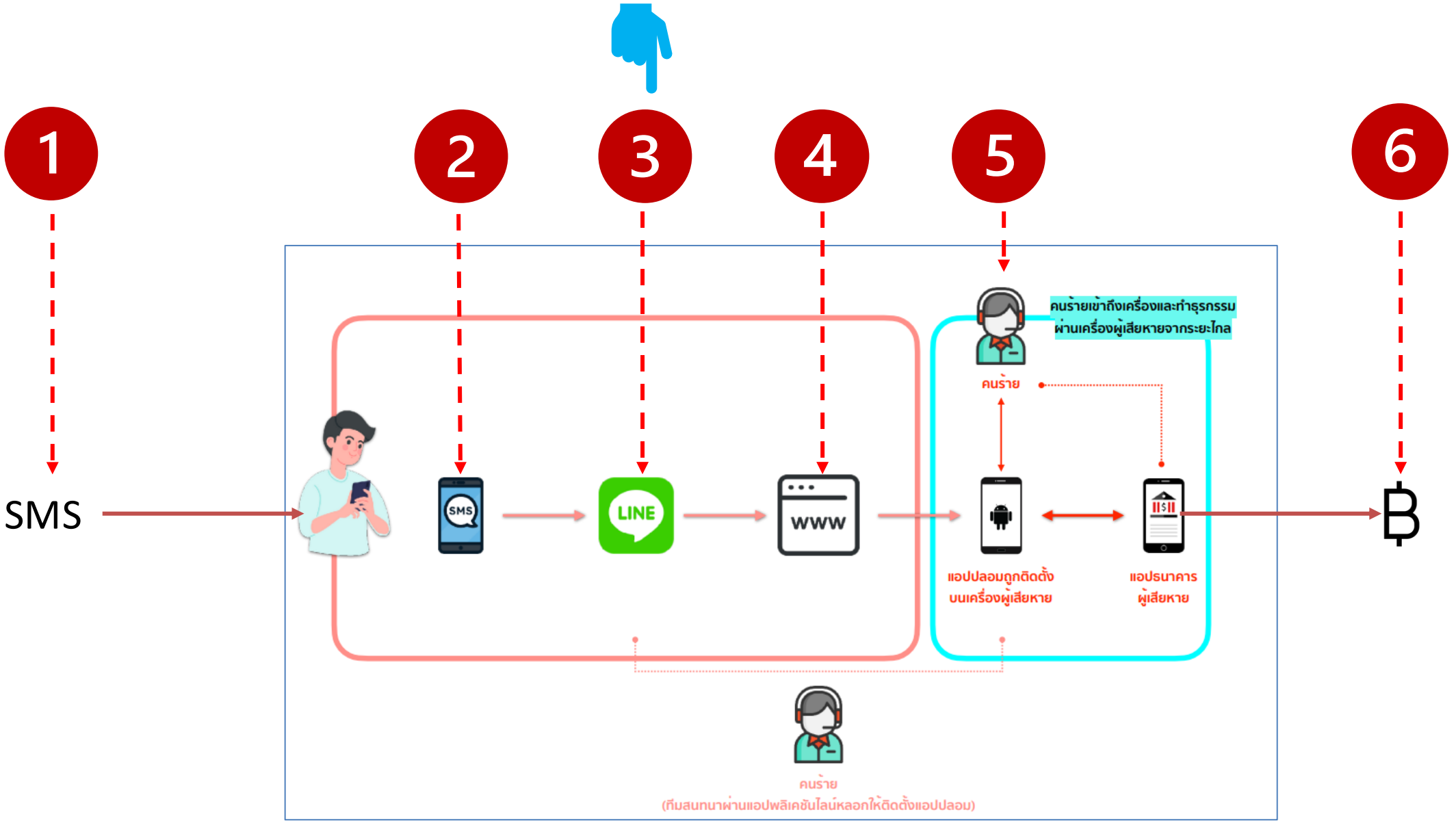
Smishing Phishing


1
2
3
4
5
6
SMS
SMS
LINE
WWW
คนร้ายเข้าถึงเครื่องและทำธุรกรรม
ผ่านเครื่องผู้เสียหายจากระยะไกล
คนร้าย
แอปปลอมถูกติดตั้ง
บนเครื่องผู้เสียหาย
แอปธนาคาร
ผู้เสียหาย
คนร้าย
(ทีมสนทนาผ่านแอปพลิเคชันไลน์หลอกให้ติดตั้งแอปปลอม)





Smishing Phishing


1
2
3
4
5
6
SMS
SMS
LINE
WWW
คนร้ายเข้าถึงเครื่องและทำธุรกรรม
ผ่านเครื่องผู้เสียหายจากระยะไกล
คนร้าย
แอปปลอมถูกติดตั้ง
บนเครื่องผู้เสียหาย
แอปธนาคาร
ผู้เสียหาย
คนร้าย
(ทีมสนทนาผ่านแอปพลิเคชันไลน์หลอกให้ติดตั้งแอปปลอม)

LINE Official Account (LINE OA)

บัญชีทั่วไป

บัญชีรับรอง

บัญชีพรีเมียม

Lotus's - โลตัส

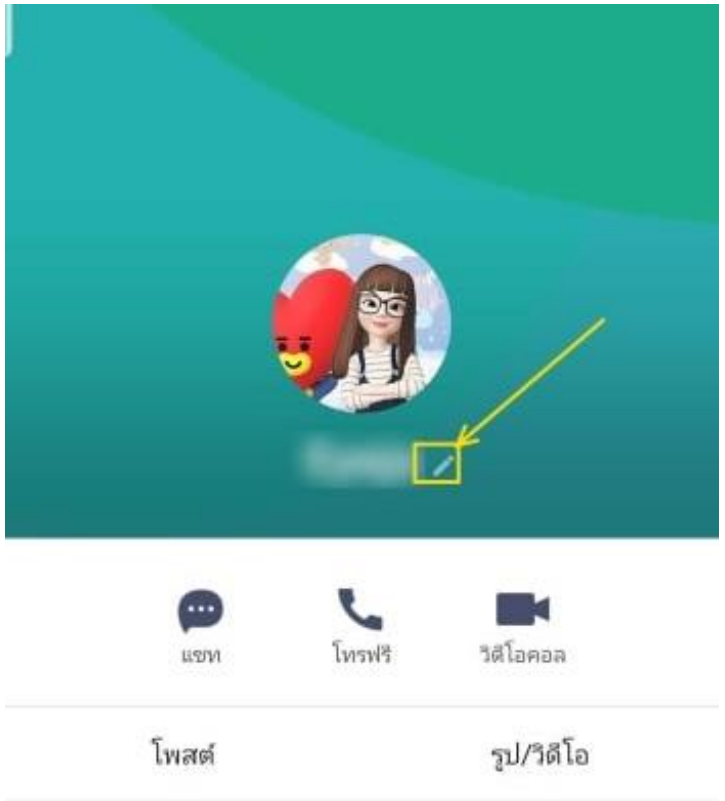
Friends 34,050,586

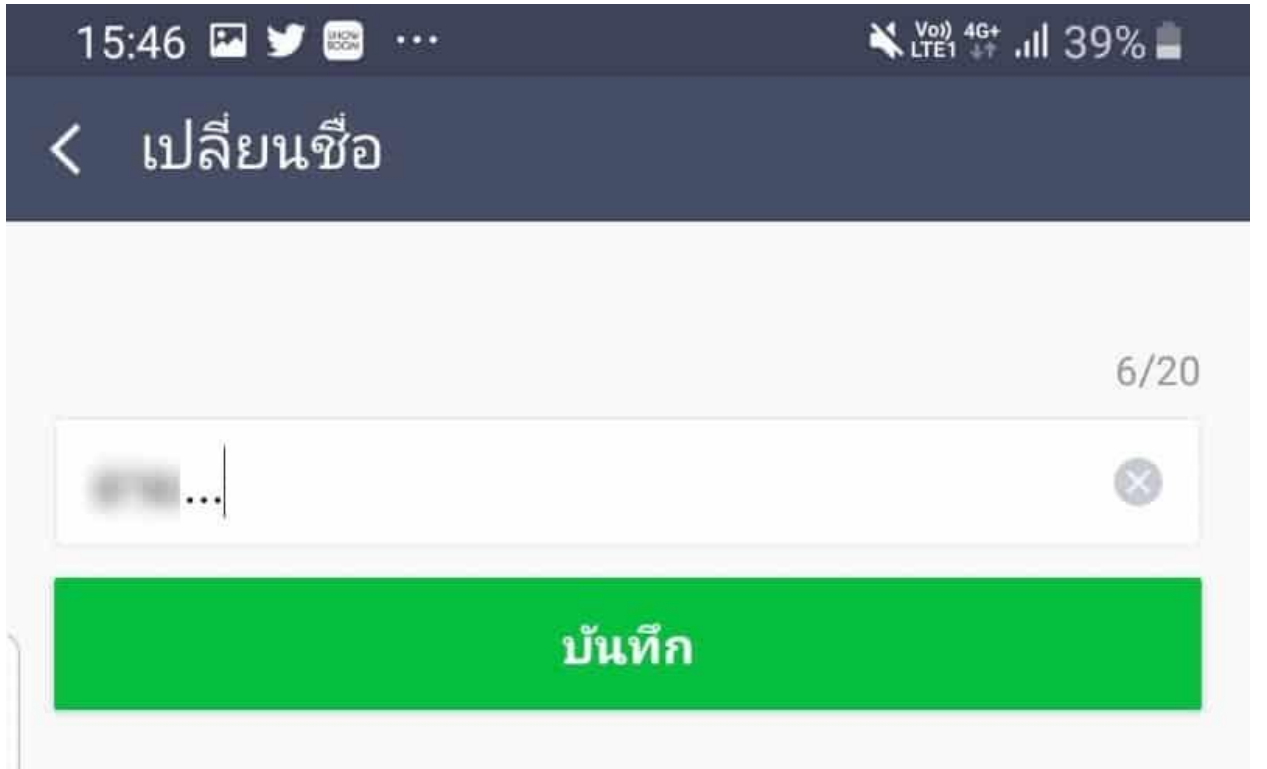
See basic info >

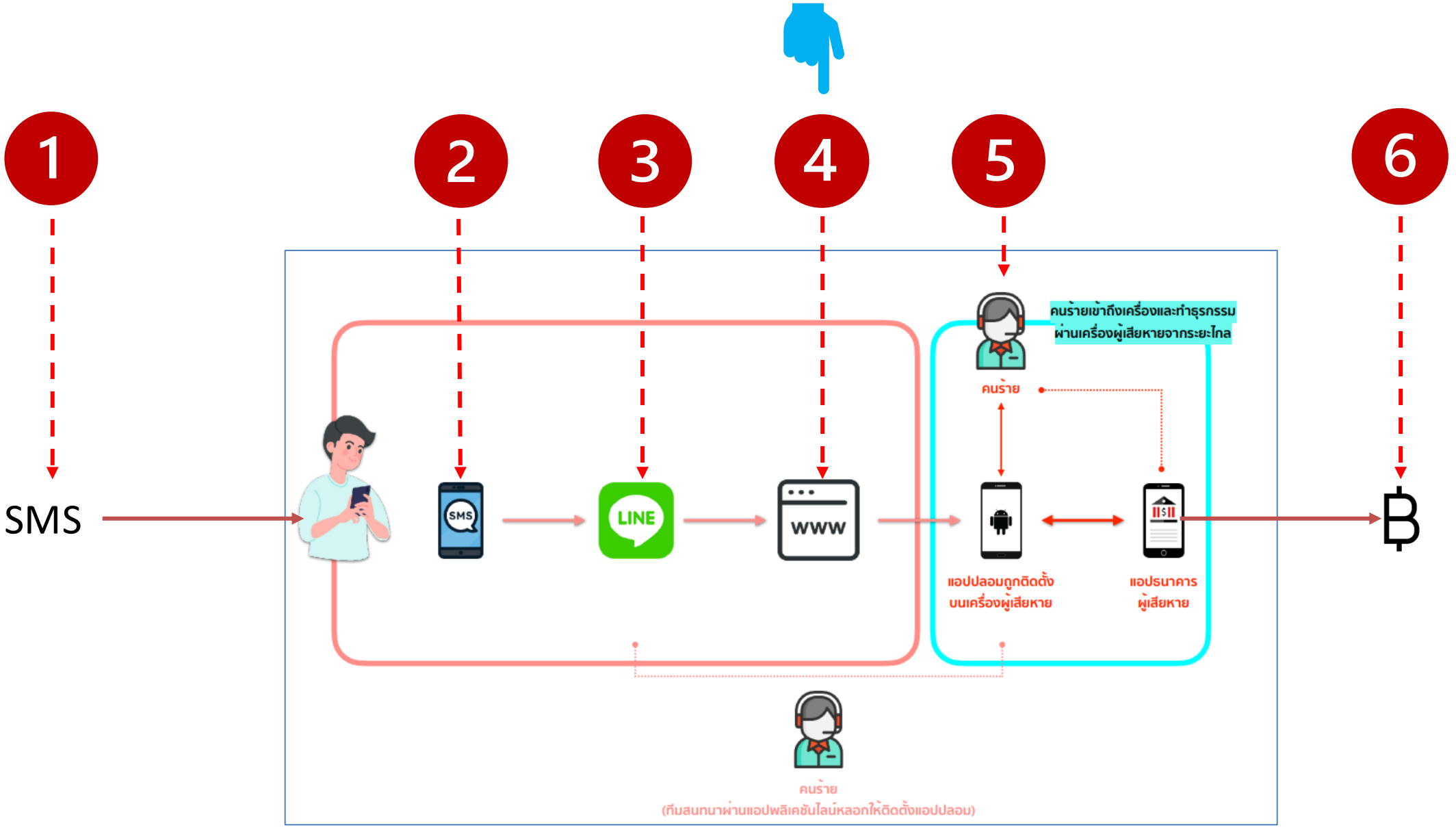
AirAsia MOVE

Friends 27,877,235

Travel More For Less


แชท
โทรฟรี
วิดีโอคอล
โพสต์
รูป/วิดีโอ


15:46
39%
เปลี่ยนชื่อ
6/20
บันทึก


1
2
3
4
5
6
SMS
SMS
LINE
WWW
คนร้ายเข้าถึงเครื่องและทำธุรกรรม
ผ่านเครื่องผู้เสียหายจากระยะไกล
คนร้าย
แอปปลอมถูกติดตั้ง
บนเครื่องผู้เสียหาย
แอปธนาคาร
ผู้เสียหาย
คนร้าย
(ทีมสนทนาผ่านแอปพลิเคชันไลน์หลอกให้ติดตั้งแอปปลอม)

https://afdw7.com

กรมสรรพากร
THE REVENUE DEPARTMENT

ยื่นภาษีเงินได้บุคคลธรรมดา ครึ่งปี (ภ.ง.ด.94) '65

ตั้งแต่วันนี้ - 10 ต.ค. 65

ยื่นออนไลน์ →

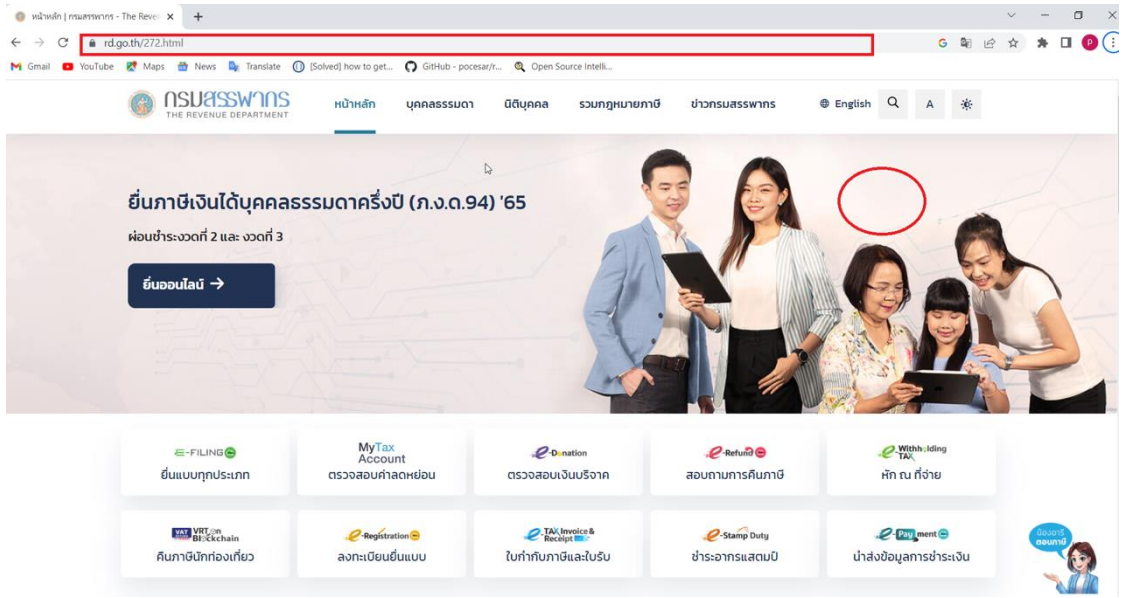
E-FILING
ยื่นแบบทุกประเภท

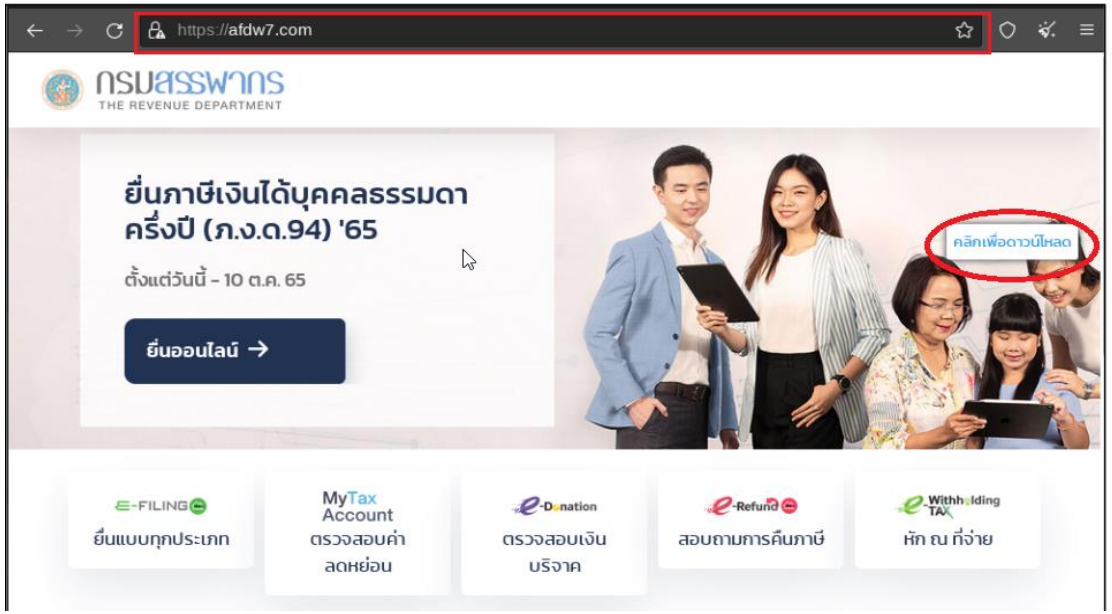
MyTax Account
ตรวจสอบค่าลดหย่อน

e-Donation
ตรวจสอบเงินบริจาค

e-Refund
สอบถามการคืนภาษี

e-Withholding TAX
หัก ณ ที่จ่าย


rd.go.th/272.html
กรมสรรพากร
THE REVENUE DEPARTMENT
หน้าหลัก
บุคคลธรรมดา
นิติบุคคล
รวมกฎหมายภาษี
ข่าวกรมสรรพากร
English
ยื่นภาษีเงินได้บุคคลธรรมดาครึ่งปี (ภ.ง.ด.94) '65
ผ่อนชำระงวดที่ 2 และ งวดที่ 3
ยื่นออนไลน์ →
e-Filing
ยื่นแบบทุกประเภท
MyTax Account
ตรวจสอบค่าลดหย่อน
e-Donation
ตรวจสอบเงินบริจาค
e-Refund
สอบถามการคืนภาษี
e-Withholding Tax
หัก ณ ที่จ่าย
VAT Refund on Blockchain
คืนภาษีนักท่องเที่ยว
e-Registration
ลงทะเบียนยื่นแบบ
e-Tax Invoice & Receipt
ใบกำกับภาษีและใบรับ
e-Stamp Duty
ชำระอากรแสตมป์
e-Payment
นำส่งข้อมูลการชำระเงิน


https://afdw7.com
กรมสรรพากร
THE REVENUE DEPARTMENT
ยื่นภาษีเงินได้บุคคลธรรมดา
ครึ่งปี (ภ.ง.ด.94) '65
ตั้งแต่วันนี้ - 10 ต.ค. 65
ยื่นออนไลน์ →
คลิกเพื่อดาวน์โหลด
e-Filing
ยื่นแบบทุกประเภท
MyTax Account
ตรวจสอบค่าลดหย่อน
e-Donation
ตรวจสอบเงินบริจาค
e-Refund
สอบถามการคืนภาษี
e-Withholding Tax
หัก ณ ที่จ่าย

MOC Account
สมัครบัญชีผู้ใช้งานกลาง
กระทรวงพาณิชย์

สำหรับ
ประชาชนทั่วไป

สำหรับ
ผู้ประก

คลิกเพื่อดาวน์โหลด

คู่มือประชาชน

รายงานประจำปี

NEWS ล้านดอลลาร์สหรัฐ เพิ่มขึ้น 15.62 % (YoY) ประเทศไทยขาดดุลการค้ามูลค่า 853.17 ล้านดอลลาร์สหรัฐ ดัชนีราคาผู้บริโภค เดือนกันยายน 2565 เท่ากับ 107.70 หรือ อัตราเงินเฟ้อทั่วไป อยู่ที่ร้อยละ 6.41 (YoY) กระทรวงพาณิชย์ แถลงข่าวภาวะการค้าระ

บริการแบบเบ็ดเสร็จ ณ จุดเดียว ด้วยระบบ
บริการด้าน
ทะเบียนธุรกิจ
บริการด้าน
ทรัพย์สินทางปัญญา
บริการด้าน
การค้าระหว่างประเทศ
บริการด้าน
การค้าภายในประเทศ
บริการ
สารสนเทศและกิจกรรม

MOC Account
สมัครบัญชีผู้ใช้งานกลาง กระทรวงพาณิชย์

สำหรับ ประชาชนทั่วไป >

สำหรับ ผู้ประกอบการ >

คู่มือประชาชน

รายงานประจำปี

NEWS กระทรวงพาณิชย์ แถลงข่าวภาวะการค้าระหว่างประเทศของไทยเดือน ต.ค.65 ส่งออกมูลค่า 21,772.37 ล้านดอลลาร์สหรัฐ ลดลง 4.41 % (YoY) นำเข้ามูลค่า 22,368.78 ล้านดอลลาร์สหรัฐ ลดลง 2.07 % (YoY) ประเทศไทยขาดดุลการค้ามูลค่า 596.41 ล้านดอลลาร์สหรั


https://www.moc-co-th.com
กระทรวงพาณิชย์
Ministry of Commerce
หน้าแรก
เกี่ยวกับกระทรวง
SMART MOC :
ค้นหาตามชื่อ, Keyword ตามที่ต้องการ
ค้นหา
NEWS
เว็บไซต์นี้มีการใช้งานคุกกี้เพื่อให้ท่านสามารถใช้บริการได้อย่างต่อเนื่องและ
เนื้อหาตรงตามความต้องการของท่าน โดยสามารถศึกษารายละเอียดเพิ่ม
บริการแบบเบ็ดเสร็จ ณ จุดเดียว ด้วยระบบ
บริการด้าน


https://www.moc.go.th/th/page/item/index/id/1
กระทรวงพาณิชย์
Ministry of Commerce
หน้าแรก
เกี่ยวกับกระทรวง
SMART MOC :
เชี่ยวชาญการค้า ก้าวหน้านวัตกรรม
เป็นธรรมโปร่งใส ใส่ใจประชาชน
ค้นหาตามชื่อ, Keyword ตามที่ต้องการ
ค้นหา
NEWS
กระทรวงพาณิชย์ แถลงข่าวภาวะการค้าระหว่างประเทศของไทยเดือน ต.ค.65 ส่งออกมูลค่า 21,772.37 ล้านดอ
เว็บไซต์นี้มีการใช้งานคุกกี้เพื่อให้ท่านสามารถใช้บริการได้อย่างต่อเนื่องและอำนวยความ
เนื้อหาตรงตามความต้องการของท่าน โดยสามารถศึกษารายละเอียดเพิ่มเติมได้ใน

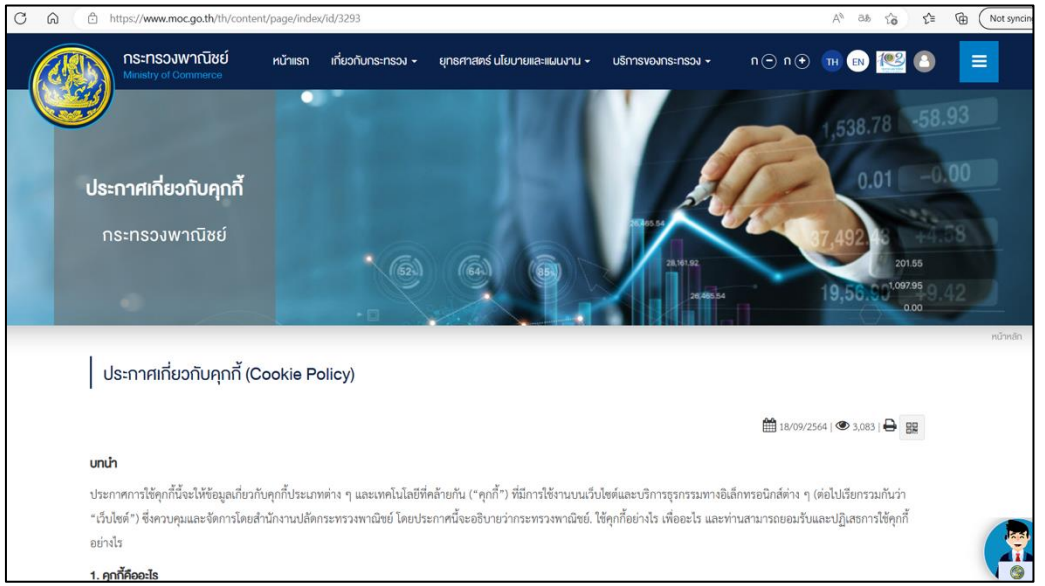
ปลอม

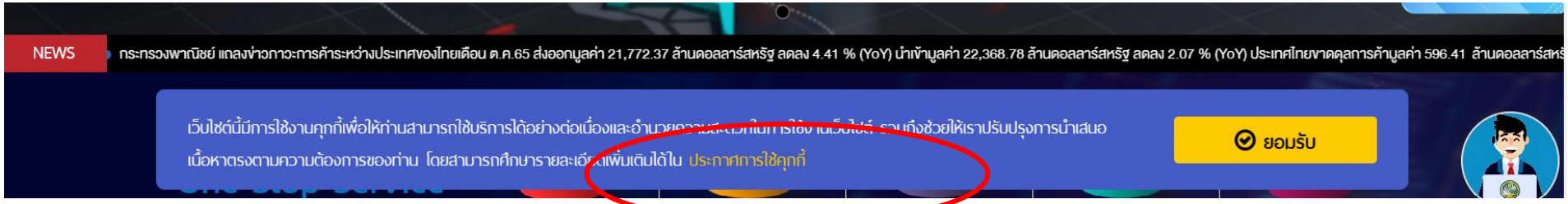
จริง

https://www.moc-co-th.com/content/page/index/id/3293

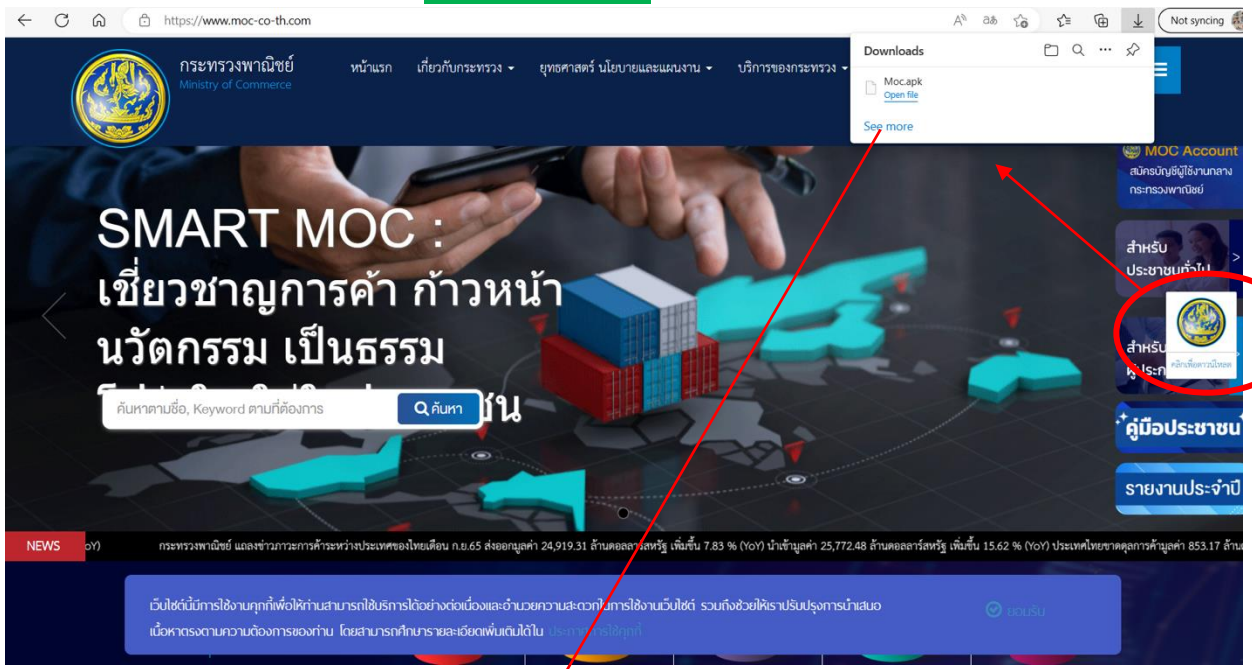
404 Not Found

nginx

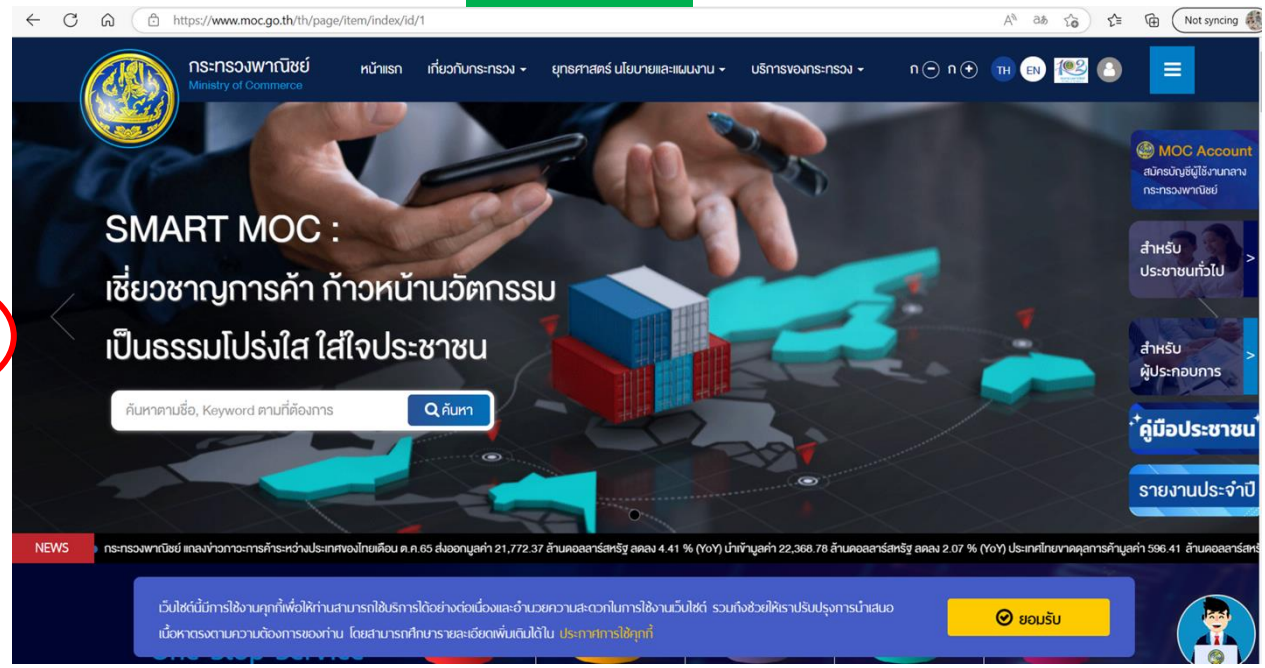


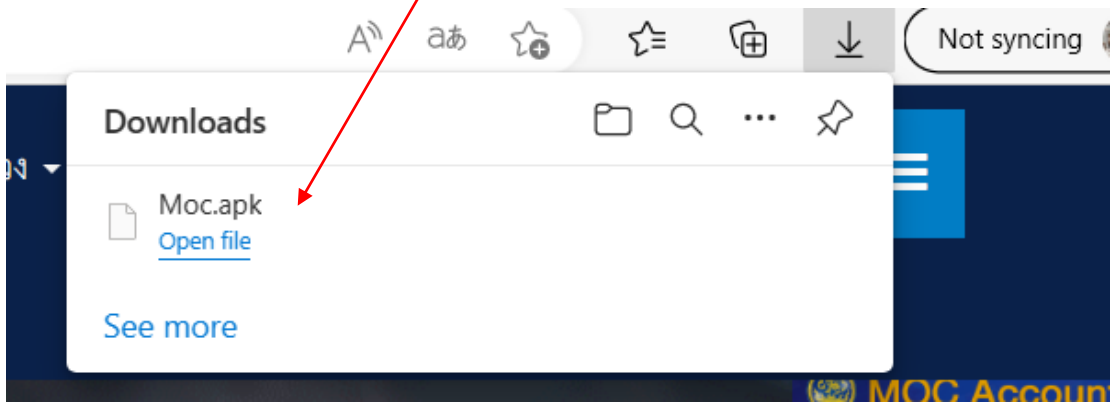


ปลอม



จริง



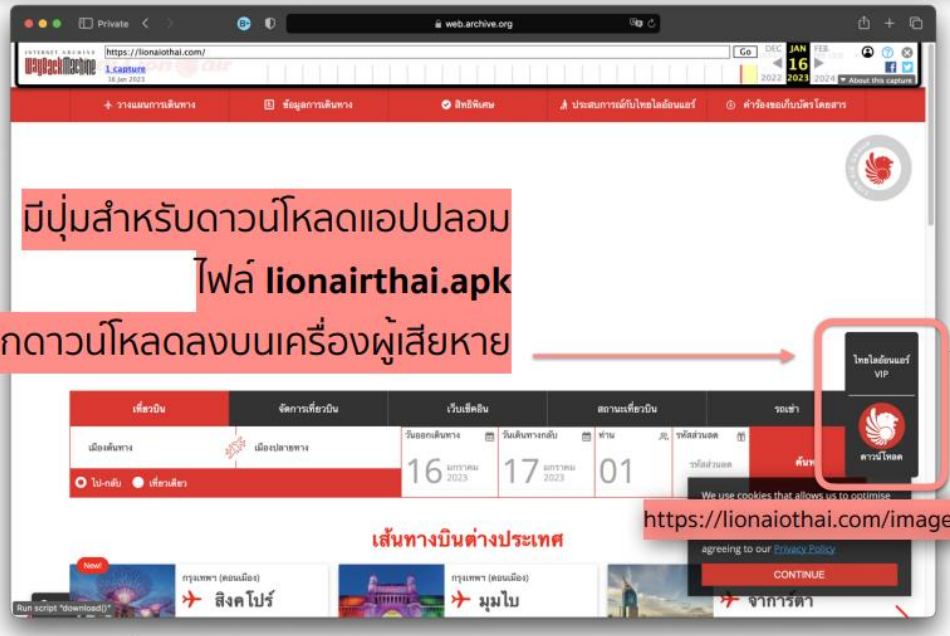


moc.apk

ประวัติหน้าเว็บไซต์ https://lionaiothai.com เมื่อวันที่ 16 ม.ค. 66

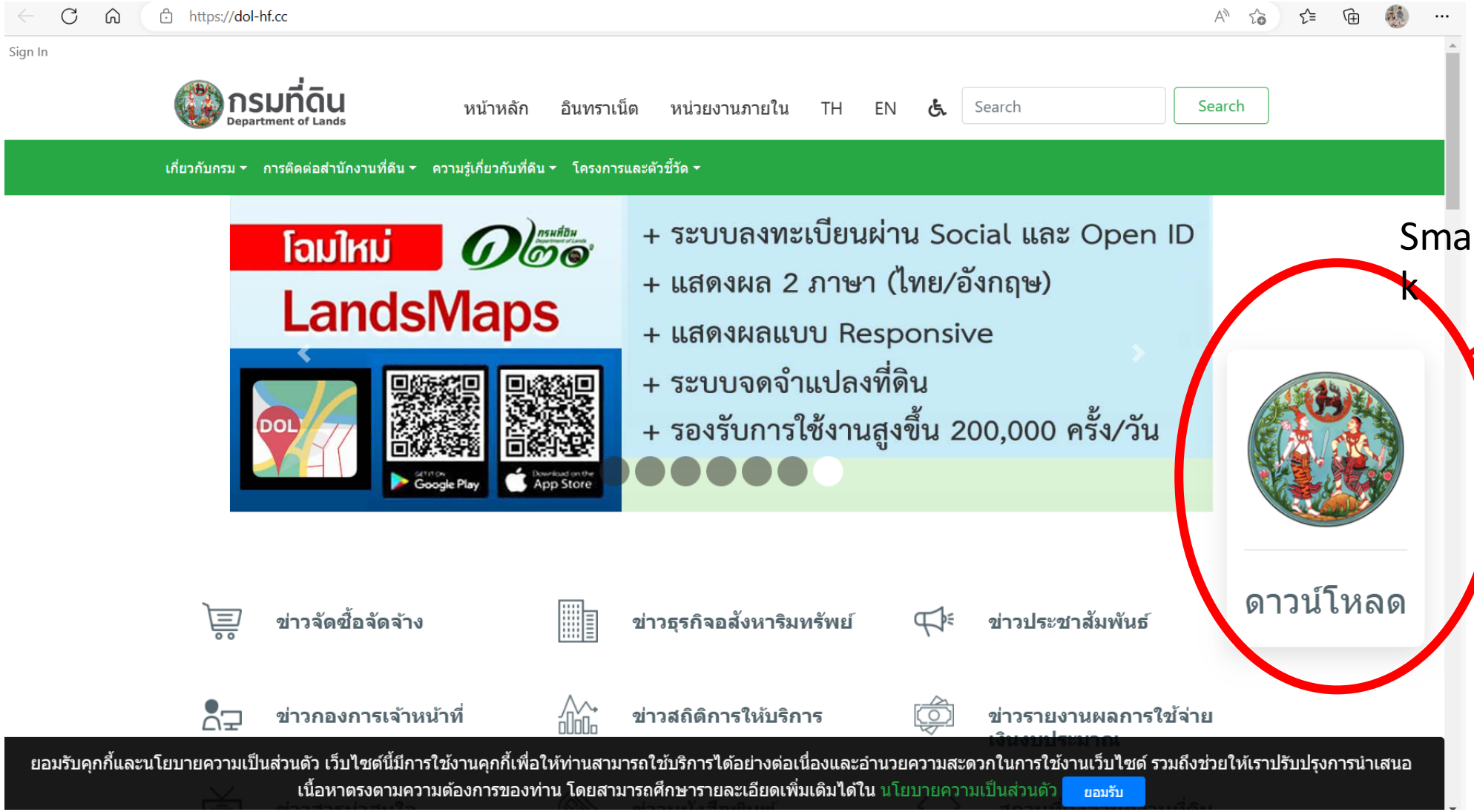
ที่มา : https://web.archive.org/web/20230116070255/https://lionaiothai.com/

ประวัติหน้าเว็บไซต์ https://lionaiothai.com เมื่อวันที่ 16 ม.ค. 66



ที่มา : https://web.archive.org/web/20230116070255/https://lionaiothai.com/

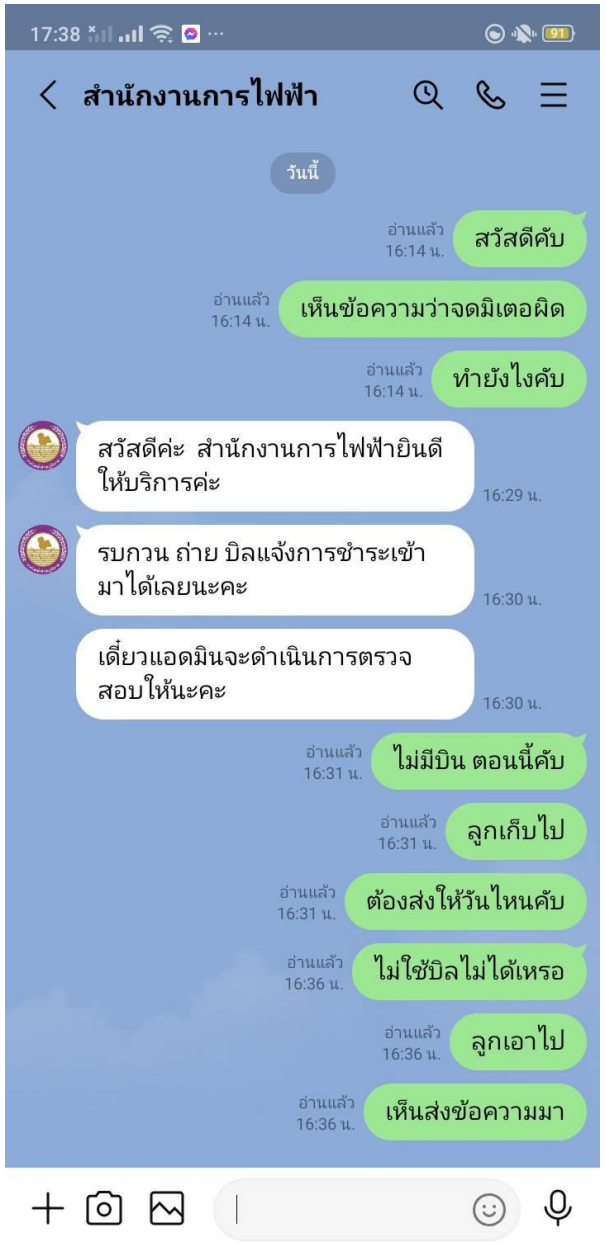
http://lionairthai.com)



Smartland.apk

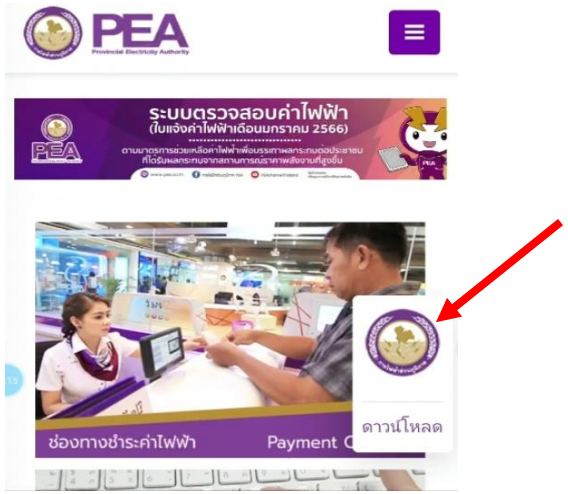
https://dol-hf.cc/
https://dol.trth.cc

→ https://www.dol.go.th/



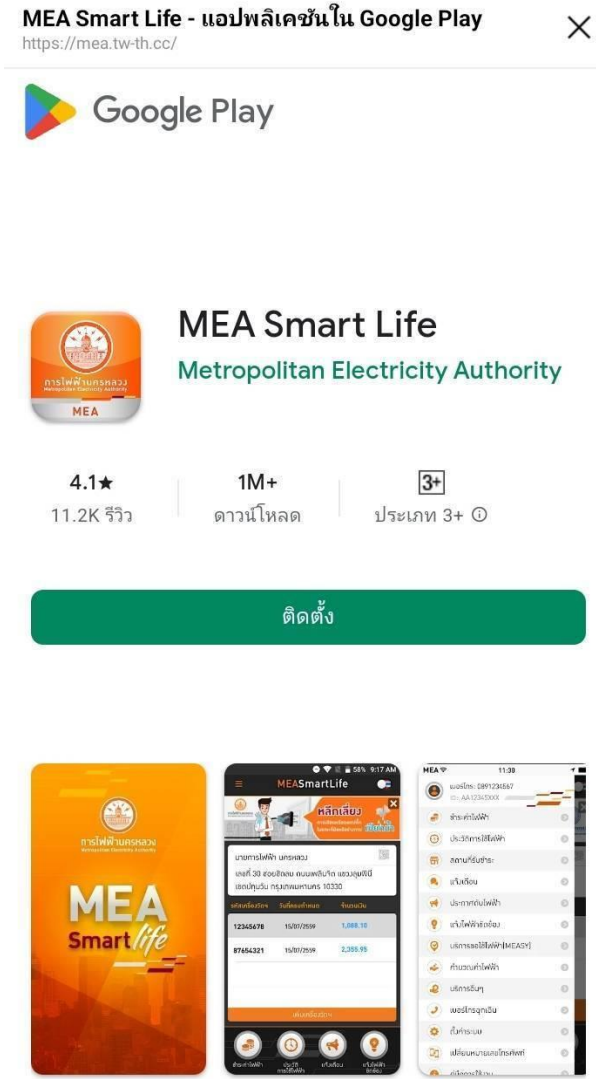
ปลอม

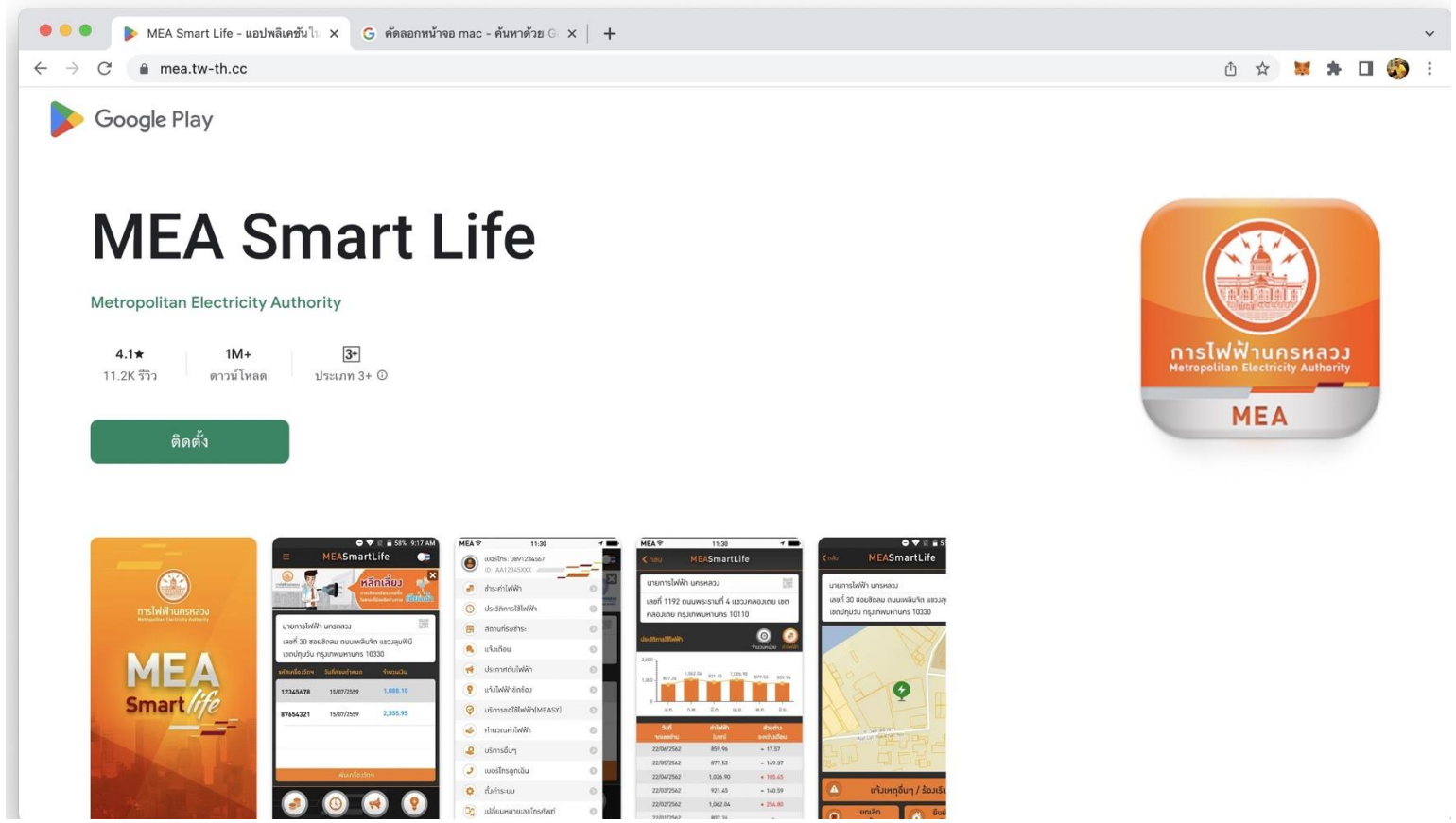
http://pea-ty-th.cc



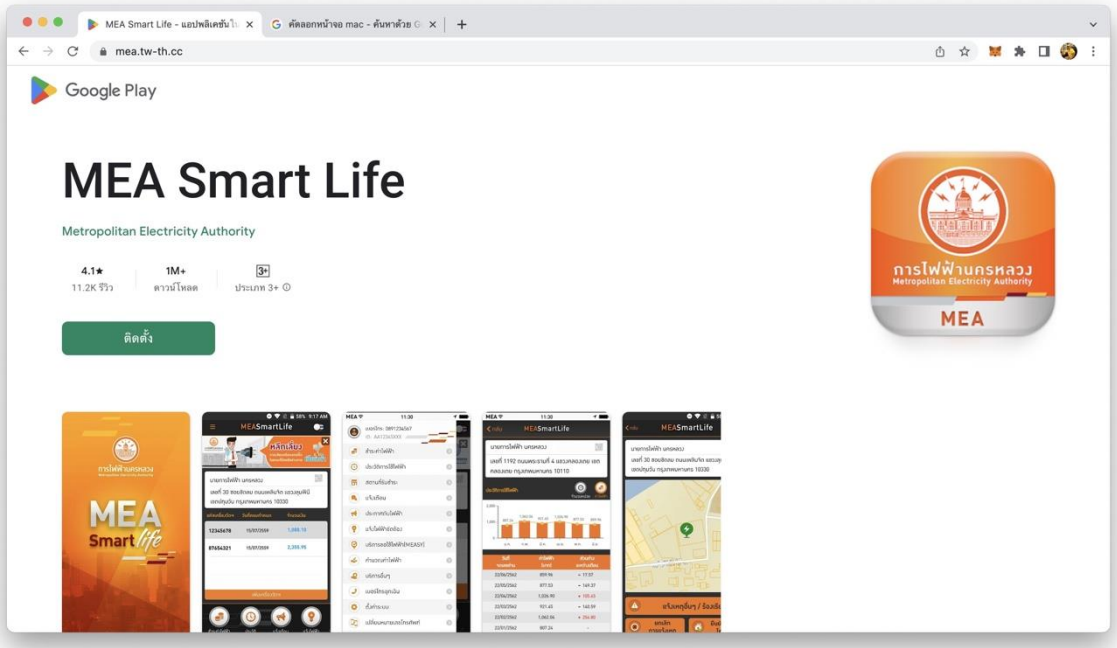
จริง

https://www.pea.co.th

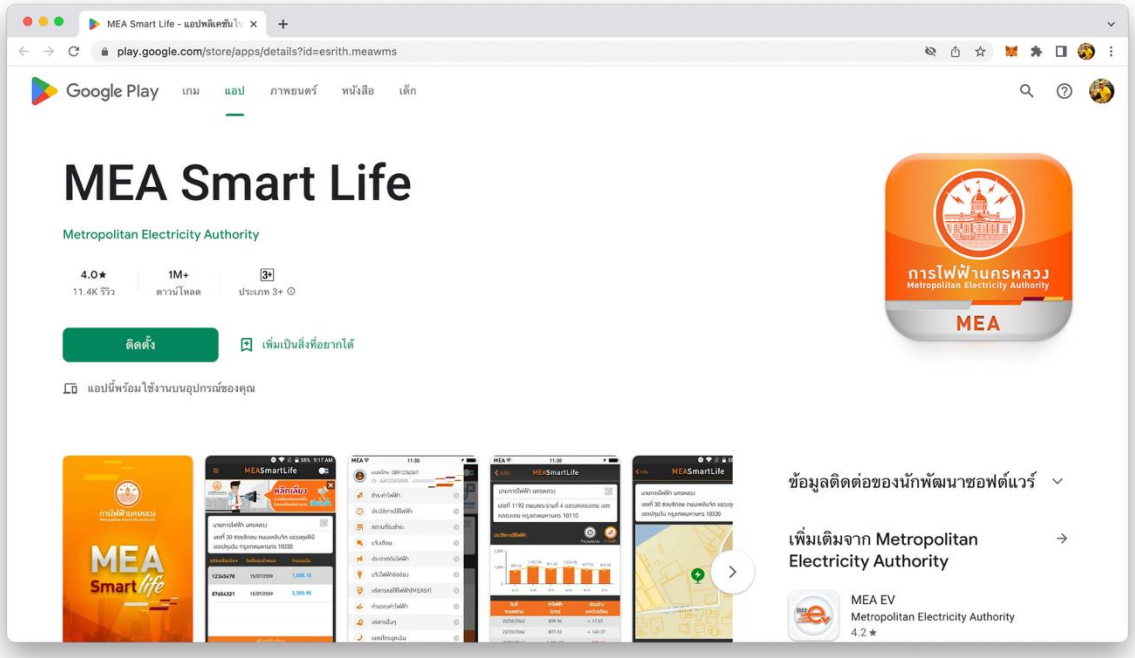




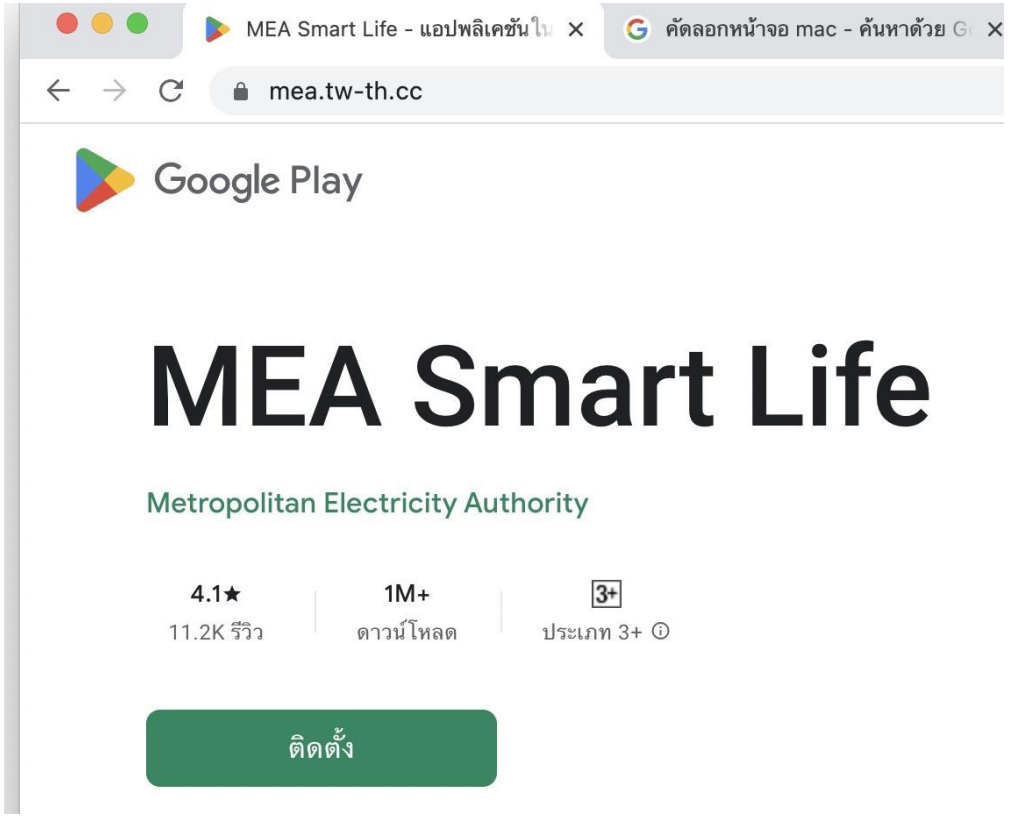
http://mea.tw-th.cc/



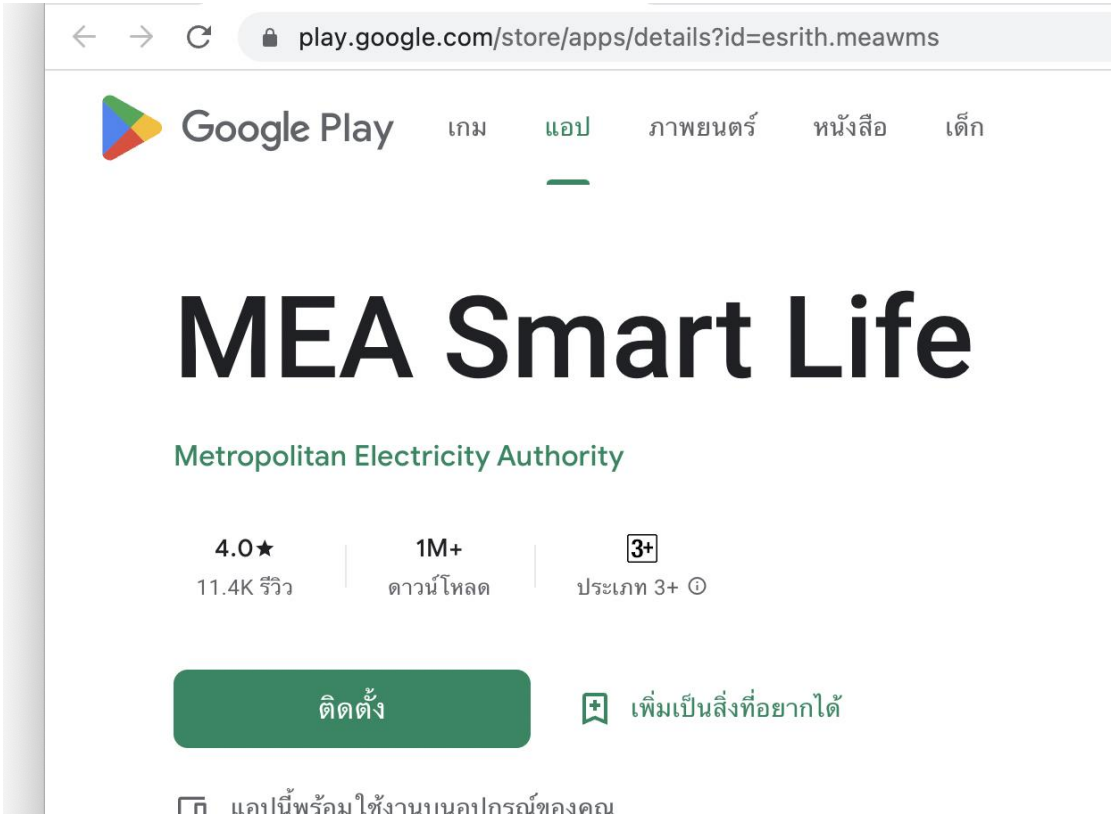
http://mea.tw-th.cc/



https://play.google.com/store/apps/details?id=esrith.meawms



http://mea.tw-th.cc/



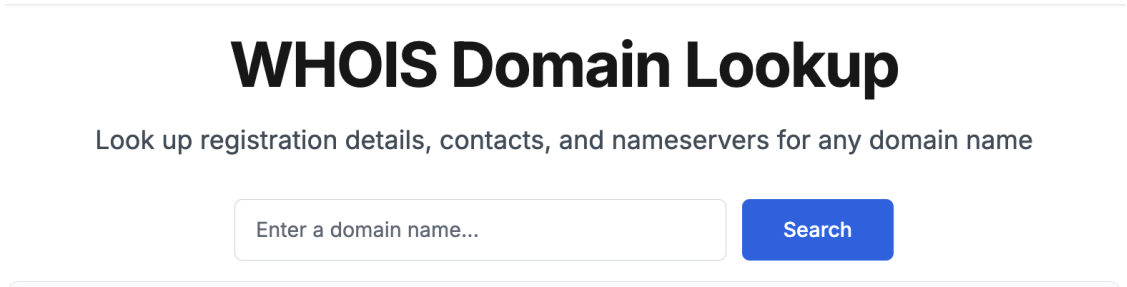
https://play.google.com/store/apps/details?id=esrith.meawms

วิธีจับสังเกตเว็ปไซด์จริง หรือปลอม

สังเกต HTTPS และ Certificate
•เว็บไซต์จริงของหน่วยงานจะขึ้นต้นด้วย https:// (มี S = Secure)
•กดไอคอน 🔒 ดูใบรับรอง (Certificate) ได้ ว่าจดโดยใคร

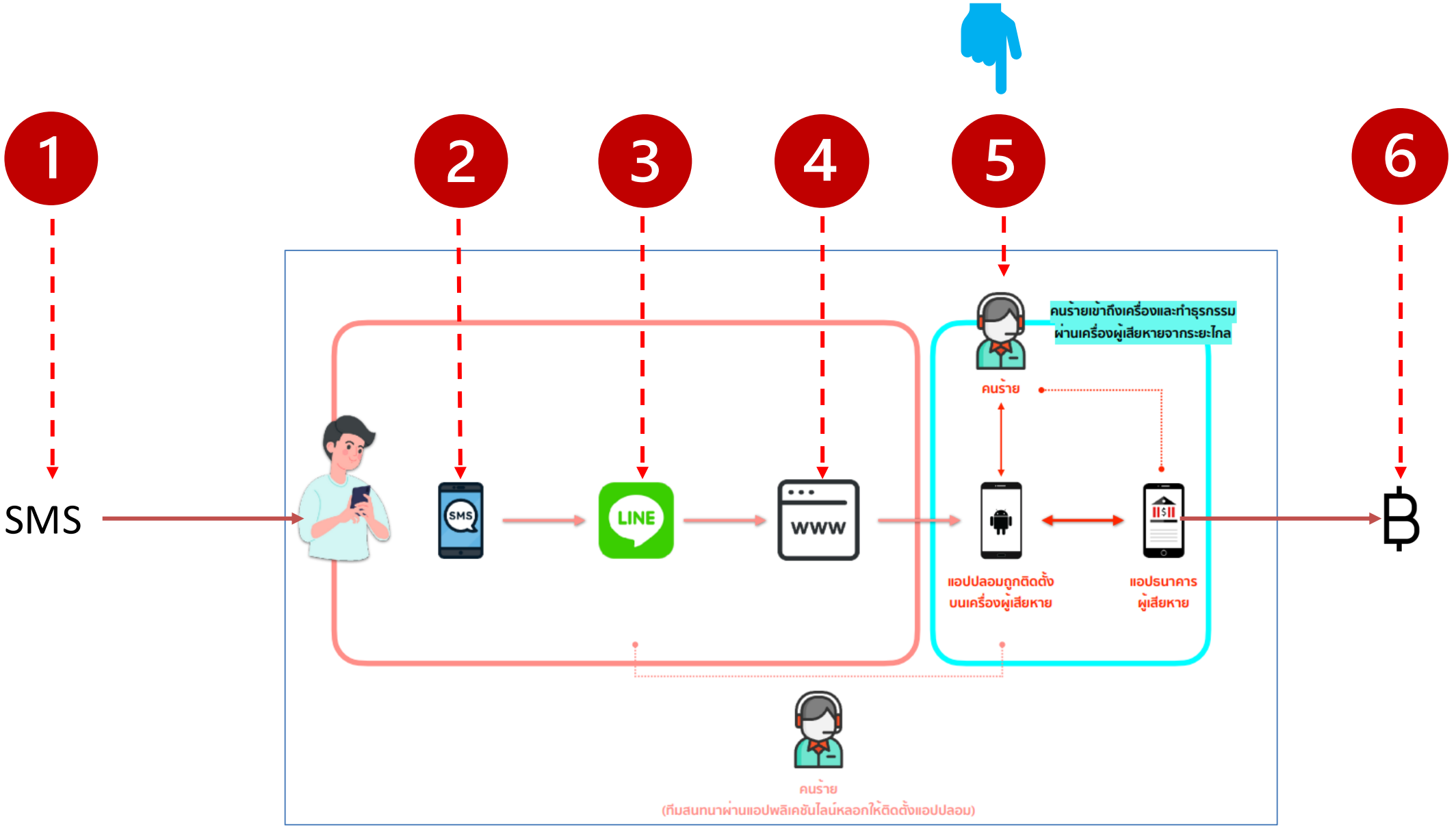
สังเกตุชื่อโดเมนหลัก (Domain Name)
•โดเมนหลักคือชื่อก่อน .go.th, .com, .org, .ac.th
•ควร **ตรงกับชื่อหน่วยงาน** อย่างเป็นทางการ

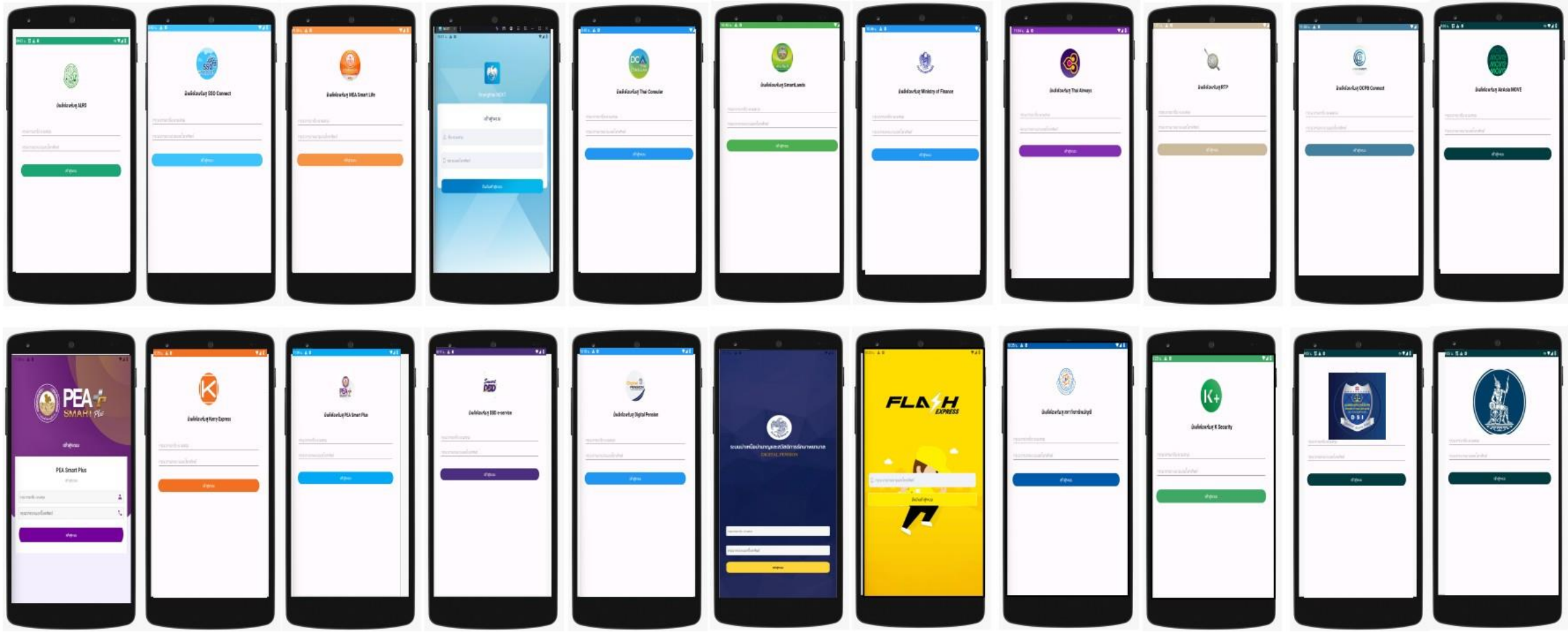
ตรวจสอบการจดโดเมนเนม จาก https://who.is/



ประเภทของนามสกุลโดเมน:

.com: เป็นที่นิยมใช้สำหรับเว็บไซต์เชิงพาณิชย์และองค์กรต่างๆ.
.net: สำหรับเว็บไซต์ที่เกี่ยวข้องกับเครือข่ายและอินเทอร์เน็ต.
.org: สำหรับองค์กรไม่แสวงผลกำไร เช่น มูลนิธิ, สมาคม.
.go.th: สำหรับหน่วยงานราชการของประเทศไทย.
.ac.th: สำหรับสถาบันการศึกษาในประเทศไทย.
.co.th: สำหรับธุรกิจที่จดทะเบียนในประเทศไทย.
.in.th: สำหรับบุคคลทั่วไปและหน่วยงานทุกประเภทในประเทศไทย.
.or.th: สำหรับองค์กรไม่แสวงผลกำไรในประเทศไทย.


1
2
3
4
5
6
SMS
SMS
LINE
WWW
คนร้ายเข้าถึงเครื่องและทำธุรกรรม
ผ่านเครื่องผู้เสียหายจากระยะไกล
คนร้าย
แอปปลอมถูกติดตั้ง
บนเครื่องผู้เสียหาย
แอปธนาคาร
ผู้เสียหาย
คนร้าย
(ทีมสนทนาผ่านแอปพลิเคชันไลน์หลอกให้ติดตั้งแอปปลอม)

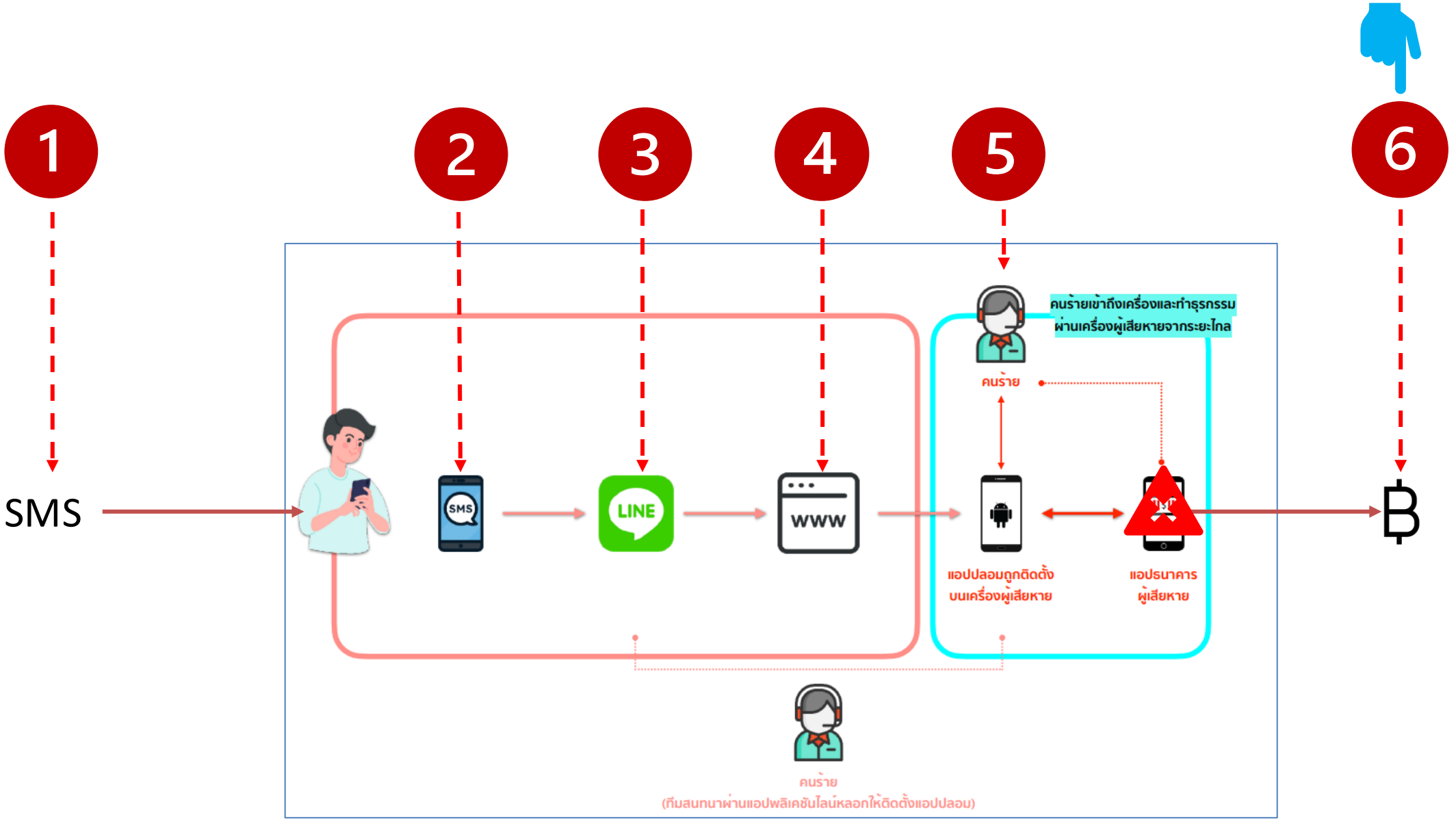

PEA
SMART Plus
PEA Smart Plus
FLASH
EXPRESS

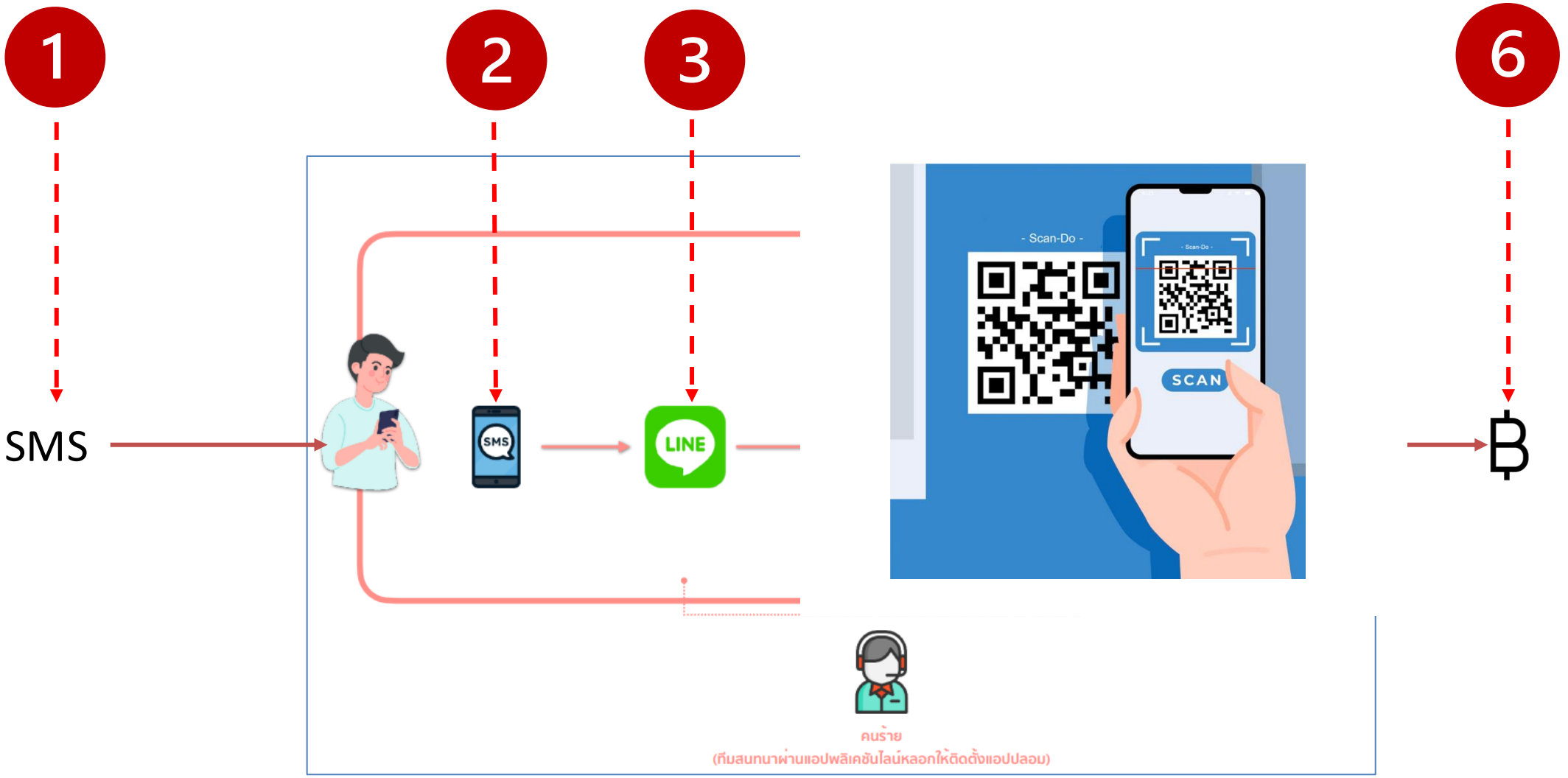
วิเคราะห์ไฟล์ **lionairthai.apk**

- **Requested Permissions**
  - android.permission.BIND_ACCESSIBILITY_SERVICE โหมดคนพิการ
  - android.permission.REQUEST_DELETE_PACKAGES ลบแอป
  - android.permission.QUERY_ALL_PACKAGES ค้นหาแอป
  - android.permission.GET_INSTALLED_APPS ติดตั้งแอป
  - android.permission.ACCESS_NETWORK_STATE เข้าถึงเครือข่าย
  - android.permission.FOREGROUND_SERVICE ให้แอปใช้งาน
  - android.permission.READ_PHONE_STATE เข้าถึงสถานะเครือข่าย
  - android.permission.WRITE_EXTERNAL_STORAGE ก็บข้อมูลภายนอก
  - android.permission.CAMERA เข้าใช้งานกล้อง
  - android.permission.RECORD_AUDIO บันทึกเสียง
  - android.permission.INTERNET ใช้งานอินเตอร์เน็ต
  - android.permission.ACCESS_WIFI_STATE การเชื่อมโยง WIFI
  - android.permission.CHANGE_NETWORK_STATE เปลี่ยนสถานะเชื่อมโยงเครือข่าย

- **Requested Permissions**
  - android.permission.READ_SMS อ่าน SMS
  - android.permission.RECEIVE_SMS ลบ SMS
  - android.permission.SEND_SMS ส่ง SMS
  - android.permission.SYSTEM_ALERT_WINDOW แจ้งเตือนบนหน้าจอ
  - android.permission.SYSTEM_OVERLAY_WINDOW ซ้อนทับหน้าจอ
  - android.permission.MOUNT_UNMOUNT_FILESYSTEMS ติดตั้ง ยกเลิก ระบบไฟล์
  - android.permission.READ_EXTERNAL_STORAGE อ่านข้อมูลจากหน่วยจัดเก็บภายนอก
  - android.permission.MODIFY_AUDIO_SETTINGS แก้ไขการตั้งค่าเสียง
  - android.permission.WRITE_SETTINGS อ่านหรือเขียนตั้งค่าระบบ
  - android.permission.ACCESS_NOTIFICATION_POLICY เข้าถึงการแจ้งเตือน

กรณีที่แอปต้องการเข้าถึงทรัพยากรหรือความสามารถต่างๆ ของอุปกรณ์ แอปจะต้องขอสิทธิ์จากผู้ใช้จึงจะทำได้
สิทธิ์บางอย่างจะมอบให้โดยผู้ใช้เมื่อติดตั้งแอป และบางอย่างจำเป็นต้องได้รับการยืนยันเพิ่มเติมในขณะที่แอปกำลังทำงาน
สิทธิ์การเข้าถึงที่ถูกร้องขอ จะมีการประกาศสิทธิ์ในไฟล์ AndroidManifest.xml ของแอปนั้นๆ


1
2
3
4
5
6
SMS
SMS
LINE
WWW
คนร้ายเข้าถึงเครื่องและทำธุรกรรม
ผ่านเครื่องผู้เสียหายจากระยะไกล
คนร้าย
แอปปลอมถูกติดตั้ง
บนเครื่องผู้เสียหาย
แอปธนาคาร
ผู้เสียหาย
คนร้าย
(ทีมสนทนาผ่านแอปพลิเคชันไลน์หลอกให้ติดตั้งแอปปลอม)


1
2
3
6
SMS
SMS
LINE
- Scan-Do -
SCAN
฿
คนร้าย
(ทีมสนทนาผ่านแอปพลิเคชันไลน์หลอกให้ติดตั้งแอปปลอม)

09.00 - 10.30

ภาพรวมสถานการณ์กลโกง

Scam Trends, รู้ทันตัวเอง และรู้ทันกลโกงจิตวิทยา 3 รูปแบบ

10.45 - 12.00

เจาะลึกเคสแอปดูดเงิน

กระบวนการติดมัลแวร์ ตั้งแต่ SMS จนถึงเงินถูกดูดออกจากบัญชี

13.00 - 14.30

รู้ทันเทคโนโลยี

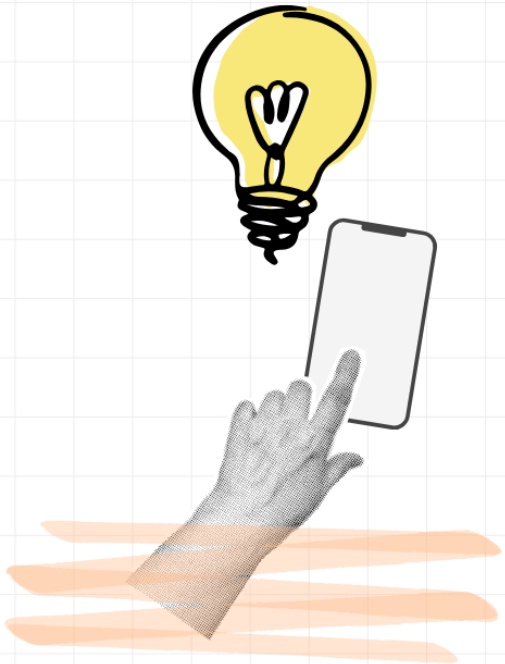
การปกป้องอุปกรณ์ และฝึกปฏิบัติใช้แอป Police Care

ตรวจมิจฉาชีพ

14.45 - 16.30

กระบวนการเมื่อเกิดเหตุ

การเตรียมหลักฐาน แจ้งความออนไลน์ และทดสอบวัคซีนไซเบอร์



ภัยไซเบอร์ปัจจุบัน (CURRENT CYBER THREATS)

ภัยคุกคามไร้พรมแดนที่ยกระดับเป็นขบวนการอาชญากรรมข้ามชาติ มีความซับซ้อนสูงและปรับเปลี่ยนรูปแบบอย่างรวดเร็ว โดยผสานการใช้จิตวิทยา (เช่น แผนประทุษกรรมแบบ Hybrid Scam ที่หลอกให้รักแล้วชวนลงทุน) เข้ากับเทคโนโลยีขั้นสูง (เช่น การใช้ AI หรือ Deepfake เพื่อสร้างความน่าเชื่อถือ) มุ่งเป้าหมายโจมตีเหยื่ออย่างเจาะจง เพื่อสร้างความเสียหายทางการเงินมูลค่ามหาศาล

มีสติ

Mindfulness

การหยุดคิดทบทวนและควบคุมอารมณ์ก่อนตัดสินใจทำธุรกรรมหรือให้ข้อมูลส่วนบุคคล ไม่ตื่นตระหนกไปกับสถานการณ์บีบบังคับหรือคำขู่ และไม่หลงเชื่อความโลภจากผลตอบแทนที่สูงเกินจริง เพื่อตัดวงจรความเร่งรีบที่มิจฉาชีพจงใจสร้างขึ้น

รู้ทันกลโกง

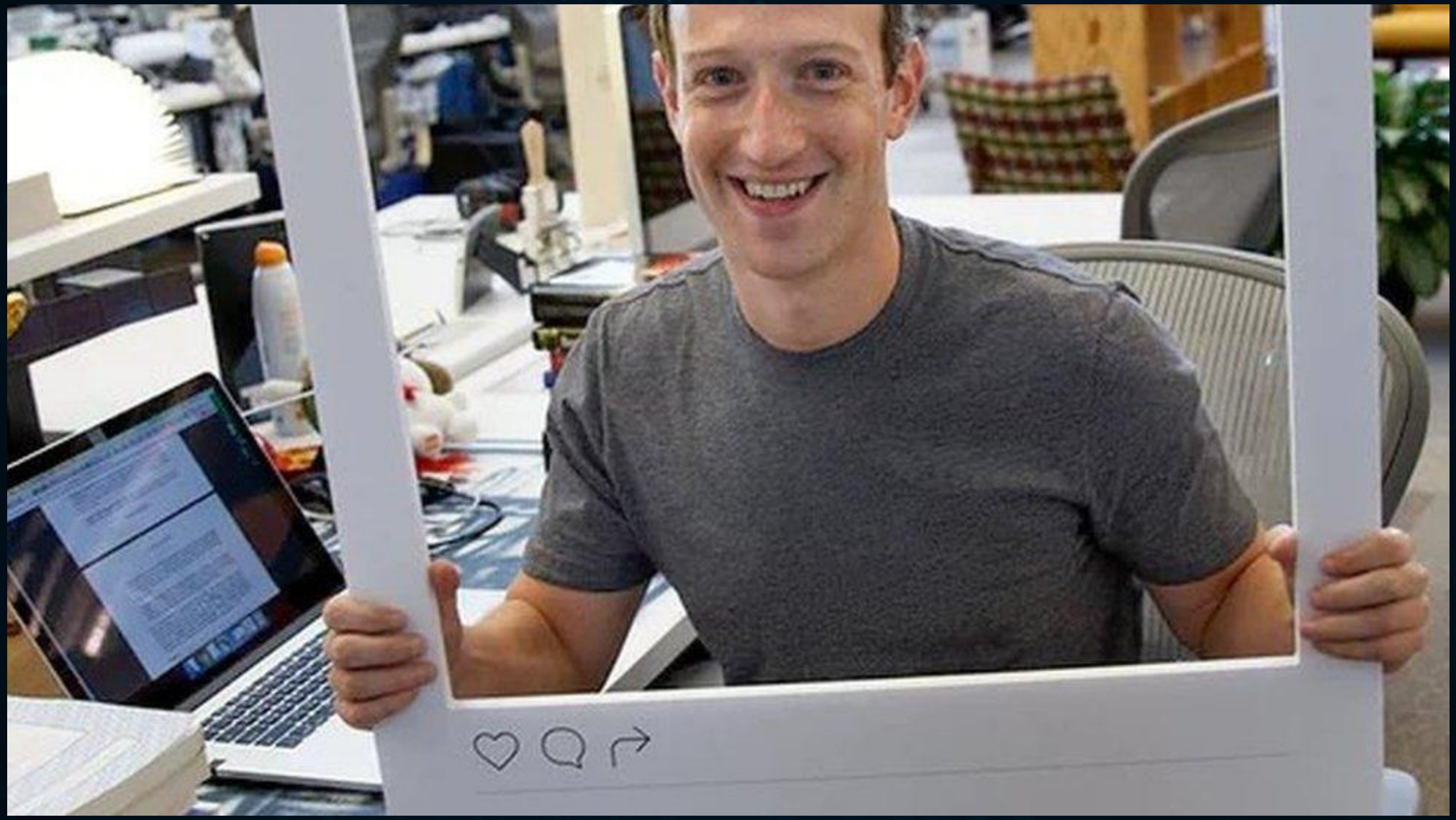
Understanding Modus Operandi

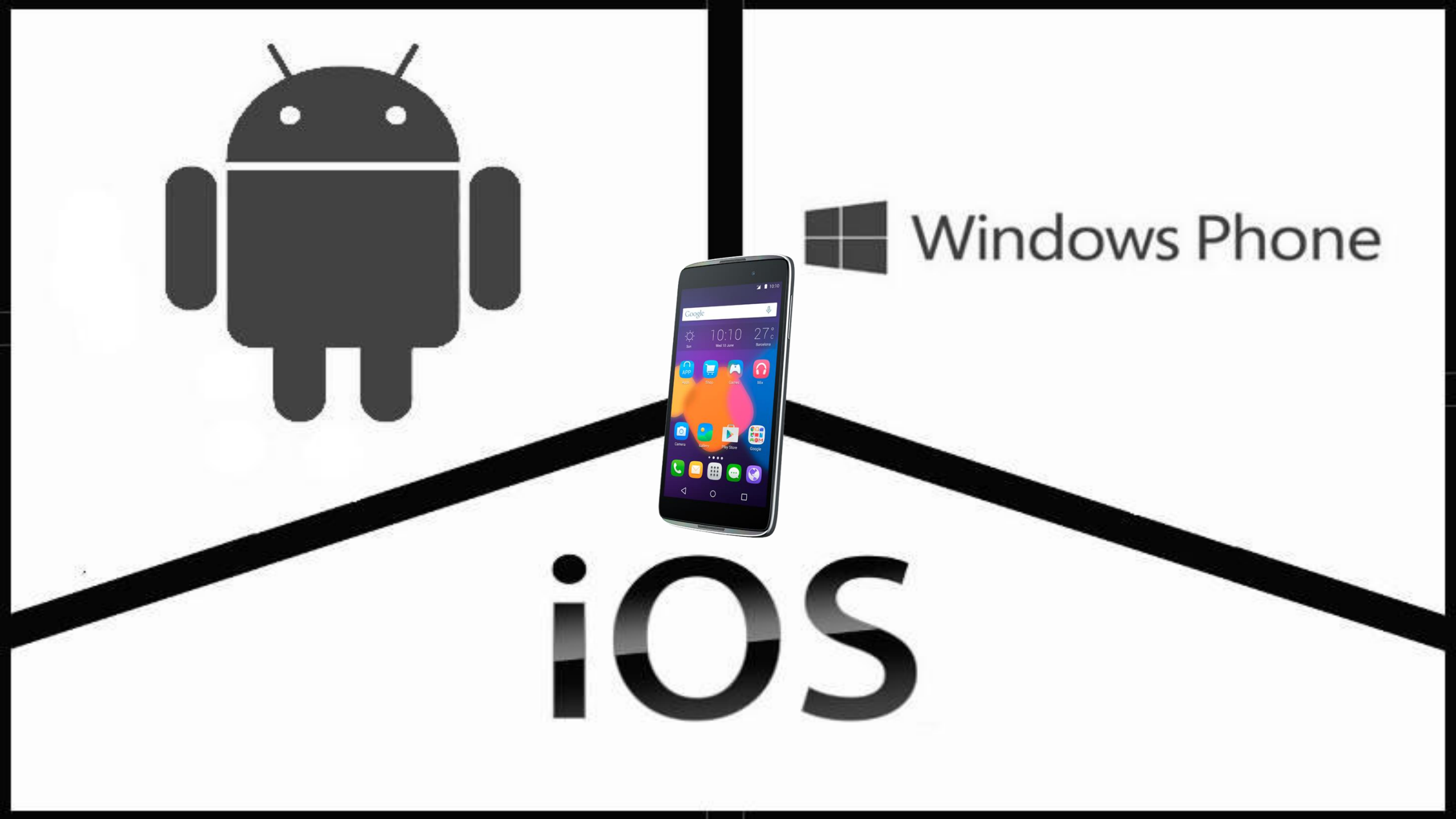
การทำความเข้าใจแผนประทุษกรรมและรูปแบบการหลอกลวงที่ปรับเปลี่ยนอยู่เสมอ เช่น การหลอกให้รักแล้วชวนลงทุน การหลอกให้ทำภารกิจ หรือกลล้อโกงออนไลน์ต่างๆ เพื่อให้สามารถสังเกตเห็นจุดผิดปกติ และรู้พฤติกรรมของคนร้ายได้ทันท่วงที

เท่าทันเทคโนโลยี

Technological Literacy

การอัปเดตความรู้เกี่ยวกับเครื่องมือดิจิทัลและภัยคุกคามรูปแบบใหม่ เช่น การใช้ AI โคลนเสียงและสร้างภาพปลอม (Deepfake) หรือแอปพลิเคชันแฝงมัลแวร์ดูดเงิน รวมถึงรู้วิธีการป้องกันตัวเองเบื้องต้น เช่น การตั้งค่าความเป็นส่วนตัว การไม่กดลิงก์อันตราย และการตรวจสอบแหล่งที่มาของข้อมูล




Windows Phone
iOS

SMARTPHONE SECURITY BEST PRACTICES

5 กฎเหล็ก...

พื้นฐานความปลอดภัยสมาร์ทโฟน

1

Strong Screen Lock

ตั้งล็อกหน้าจอด้วย PIN 6 หลัก ขึ้นไป, สแกนนิ้ว, หรือใบหน้า

หลีกเลี่ยง Pattern (ลากเส้น) เพราะเดายากง่าย

2

Update OS & Apps Always

อัปเดตระบบและแอป ให้เป็นเวอร์ชันล่าสุดเสมอ

เพื่ออุดช่องโหว่ความปลอดภัย

3

Download Only from Official Stores

ติดตั้งแอปผ่าน App Store หรือ Google Play Store เท่านั้น

ห้ามโหลด .APK จากแหล่งภายนอก

4

Check App Permissions

ตรวจสอบสิทธิ์การเข้าถึง (กล้อง, รายชื่อ, SMS)

ปฏิเสธ “Accessibility Services” สำหรับแอปทั่วไป

5

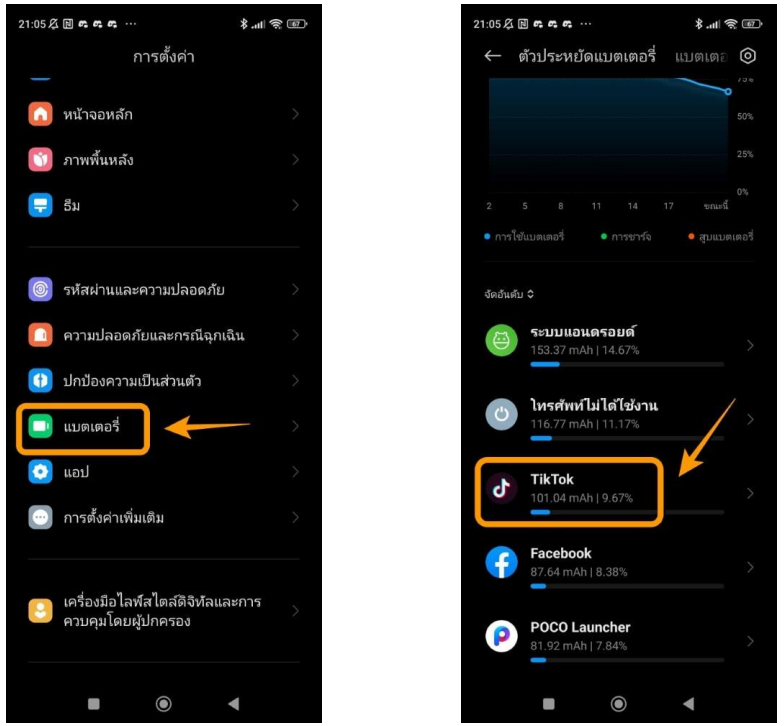
Beware of SMS & Links

ระวัง SMS หรือ ลิงก์ที่น่าสงสัย

ธนาคารยกเลิกส่งลิงก์ผ่าน SMS ห้ามกด!

ตรวจเช็คการใช้งานแบตเตอรี่

IOS

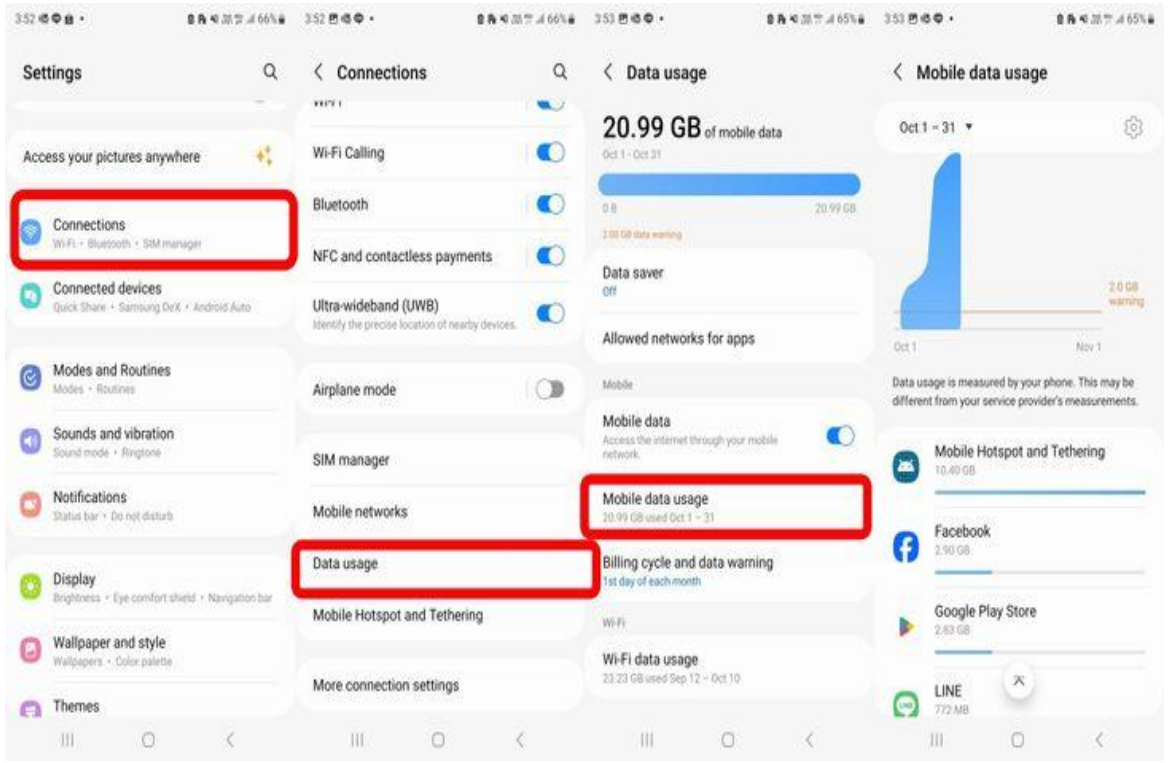


Android

ตรวจเช็คการใช้ข้อมูล

IOS

หน้าตั้งค่า (Settings) > เครือข่ายมือถือ (Cellular) > กดที่ซิมที่คุณต้องการ > การใช้งานข้อมูล



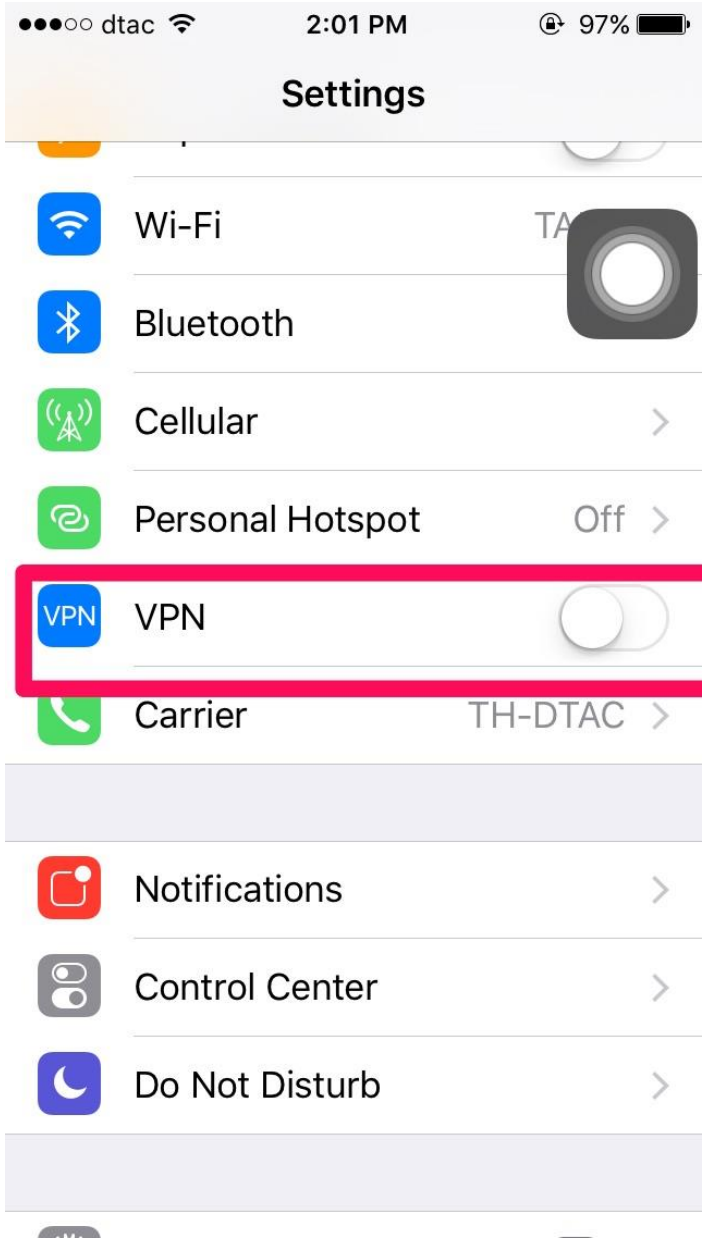
Android

หน้าตั้งค่า (Setting) > การเชื่อมต่อ (Connections) > การใช้ข้อมูล (Data Usage)

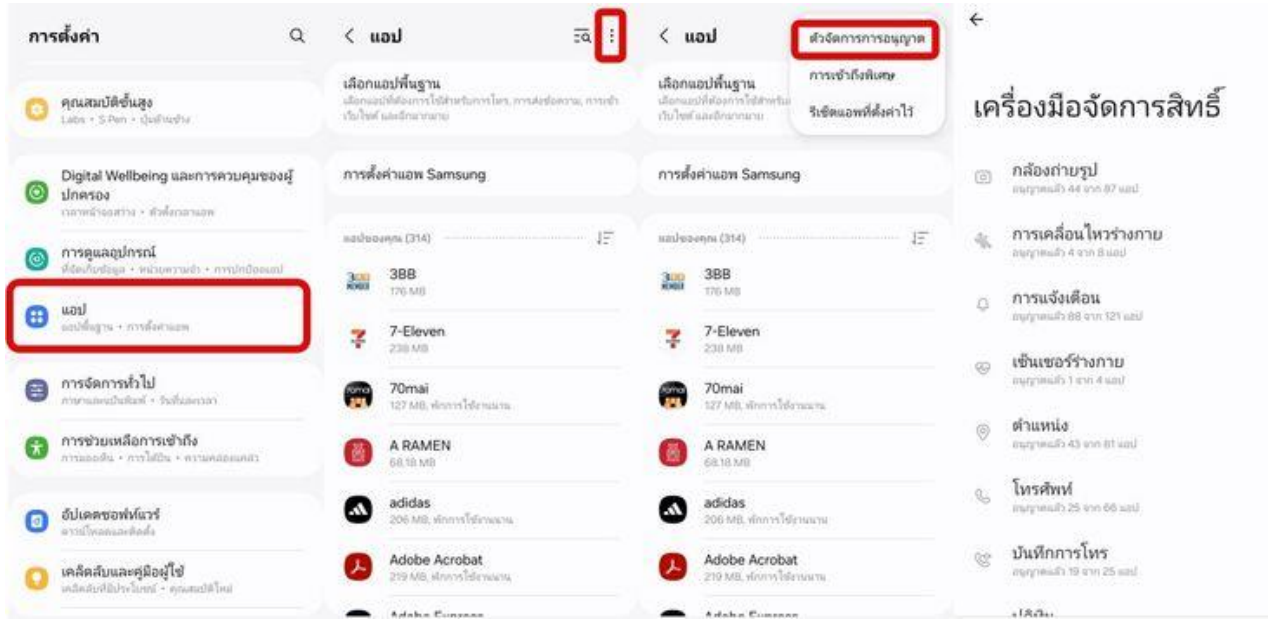
เพิ่มเติมสำหรับ ระบบ IOS

การตั้งค่า > ทั่วไป > VPN & การจัดการอุปกรณ์

หากมี VPN ที่กำหนดค่าไว้ จะแสดงอยู่ในรายการ หากมีการเชื่อมต่อ VPN อยู่ สถานะการเชื่อมต่อจะแสดงอยู่ใต้ชื่อ VPN นั้นๆ



ตรวจเช็คการขอสิทธิ์การเข้าถึง



Android

1.เปิดแอป "การตั้งค่า" ในอุปกรณ์
2.แตะ "แอป"
3.เลือกแอปที่ต้องการตรวจสอบ หากไม่พบ ให้แตะ "ดูแอปทั้งหมด"
4.แตะ "สิทธิ์"

- ในหน้านี้ คุณจะเห็นรายการสิทธิ์ทั้งหมดที่แอปนั้นร้องขอ เช่น ตำแหน่งที่ตั้ง ไมโครโฟน กล้อง
- สิทธิ์ที่อนุญาตแล้วจะแสดงเป็น "อนุญาต"
- สิทธิ์ที่ไม่อนุญาตจะแสดงเป็น "ไม่อนุญาต" หรือ "ถามทุกครั้ง"

5.หากต้องการเปลี่ยนการตั้งค่าสิทธิ์ ให้แตะสิทธิ์นั้นแล้วเลือก "อนุญาต" หรือ "ไม่อนุญาต" หรือ "ถามทุกครั้ง" (ถ้ามี)

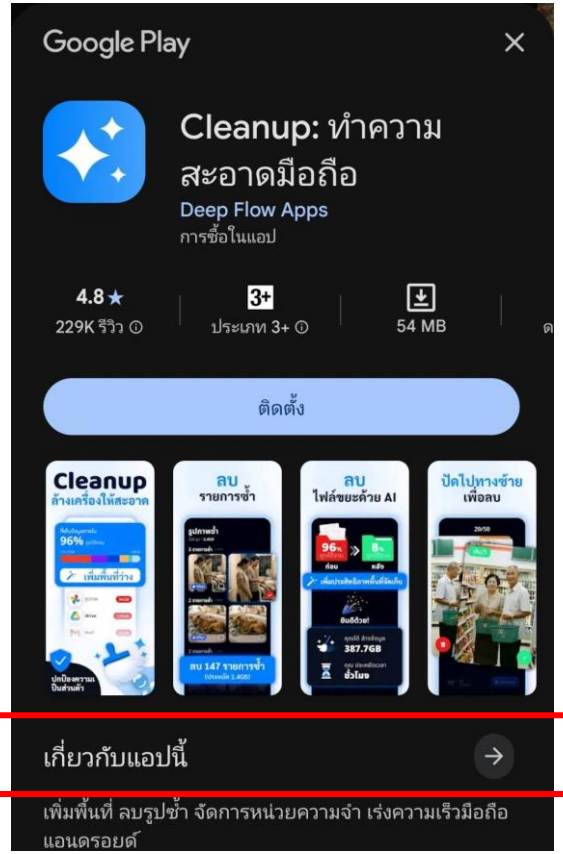
ตรวจเช็คการขอสิทธิ์การเข้าถึง

IOS

1.เปิดแอป "การตั้งค่า"
2.เลื่อนลงมา แล้วแตะ "ความเป็นส่วนตัว"
3.เลือกประเภทข้อมูล ที่คุณต้องการตรวจสอบ เช่น ตำแหน่งที่ตั้ง, ไมโครโฟน, กล้อง, รายชื่อ
4.ในแต่ละประเภทข้อมูล คุณจะเห็นรายชื่อแอปที่ขอสิทธิ์เข้าถึงข้อมูลนั้นๆ

- แอปที่เข้าถึงข้อมูลได้ จะแสดงสัญลักษณ์สีเขียว
- แอปที่ถูกปิดกั้นการเข้าถึง จะแสดงเป็นสีเทา

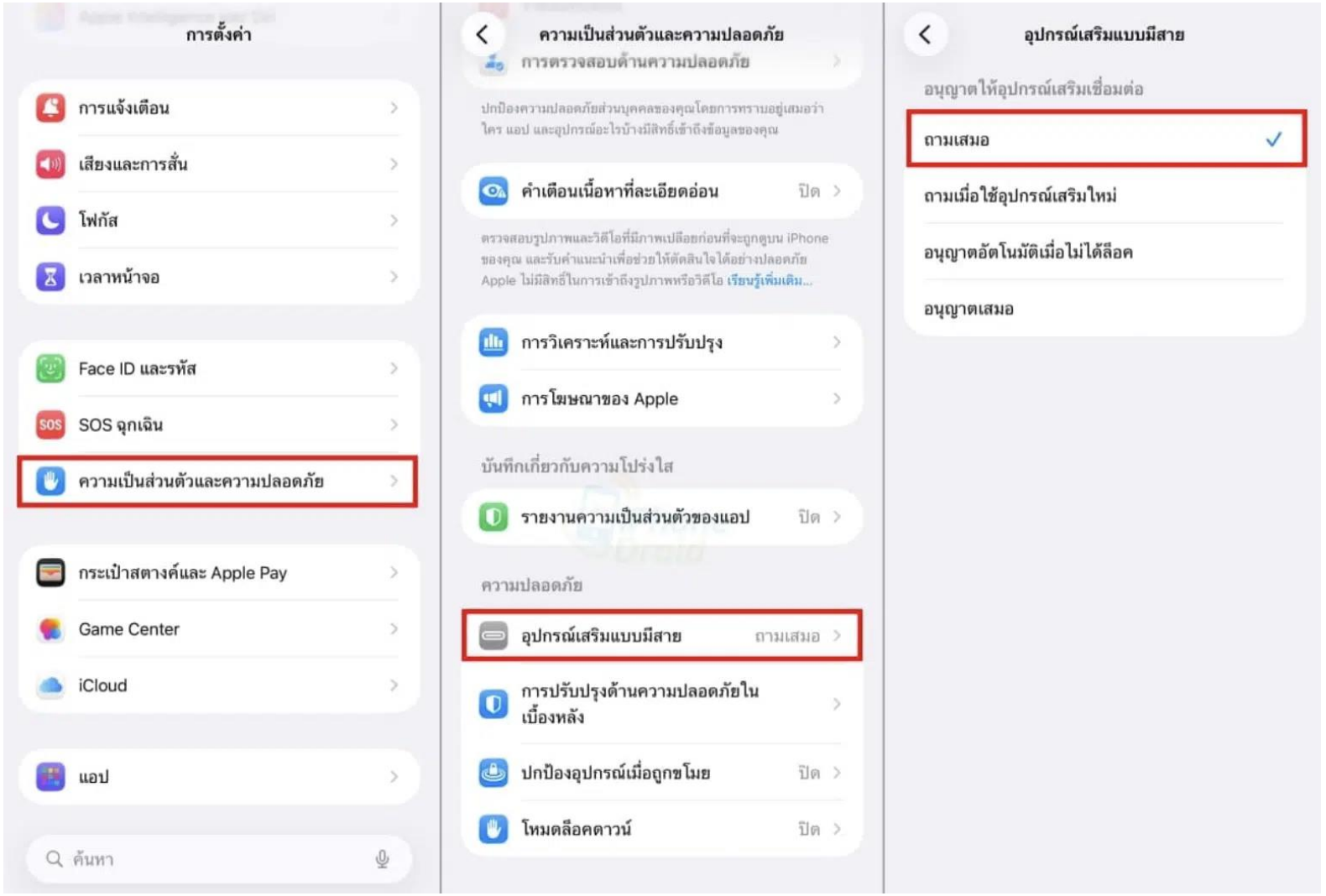
5.หากต้องการเปลี่ยนการตั้งค่าสิทธิ์ ให้แตะที่แอปนั้น แล้วเลือกตัวเลือกที่ต้องการ


Google Play
Cleanup: ทำความสะอาดมือถือ
Deep Flow Apps
การซื้อในแอป
4.8★
229K รีวิว
3+
ประเภท 3+
54 MB
ติดตั้ง
Cleanup
ล้างเครื่องให้สะอาด
ลบ
รายการซ้ำ
ลบ
ไฟล์ขยะด้วย AI
ปัดไปทางซ้าย
เพื่อลบ
เกี่ยวกับแอปนี้
เพิ่มพื้นที่ ลบรูปซ้ำ จัดการหน่วยความจำ เร่งความเร็วมือถือแอนดรอยด์


Cleanup: ทำความสะอาดมือถือ
สิทธิ์ของแอป
เวอร์ชัน 1.3.8 อาจขอสิทธิ์ในการเข้าถึง
รายชื่อติดต่อ
• อ่านผู้ติดต่อของคุณ
• แก้ไขผู้ติดต่อของคุณ
พื้นที่เก็บข้อมูล
• แก้ไขหรือลบเนื้อหาในพื้นที่จัดเก็บข้อมูลที่ใช้ร่วมกัน
อื่นๆ
• เข้าถึง AdServices Custom Audience API
• อ่านไฟล์วิดีโอจากพื้นที่เก็บข้อมูลที่แชร์
• สิทธิ์ในการรับรหัสโฆษณา
• อ่านไฟล์ภาพจากพื้นที่เก็บข้อมูลที่แชร์
• ควบคุมการสั่นเตือน
• เข้าถึง AdServices Topics API
• บริการเรียกเก็บเงินของ Google Play
• ทำงานเมื่อเริ่มต้น
• การตรวจสอบใบอนุญาตของ Google Play
• มีสิทธิ์เข้าถึงเครือข่ายเต็มรูปแบบ
• ใช้ฮาร์ดแวร์ชีวมิติ
• ดูการเชื่อมต่อเครือข่าย
• ป้องกันไม่ให้โทรศัพท์เข้าโหมดสลีป
• Play Install Referrer API
• เข้าถึง Adid API
• เข้าถึง AdServices Attribution API
• ดูการเชื่อมต่อ WiFi
• ใช้ฮาร์ดแวร์ลายนิ้วมือ
• แสดงการแจ้งเตือน
• รับข้อมูลจากอินเทอร์เน็ต

Android

IOS



1.ไปที่ **การตั้งค่า (Settings)**
2.เลือก **ความเป็นส่วนตัวและความปลอดภัย (Privacy & Security)**
3.เลือกเมนู **อุปกรณ์เสริมแบบมีสาย (Wired Accessories)**
4.เปลี่ยนตัวเลือกเป็น **"ถามเสมอ" (Always Ask)** หรือ **"ถามเมื่อใช้อุปกรณ์เสริมใหม่" (Ask for New Accessories)**


13:30
TikTok
@cyberpolice_th
ตำรวจไซเบอร์

IOS

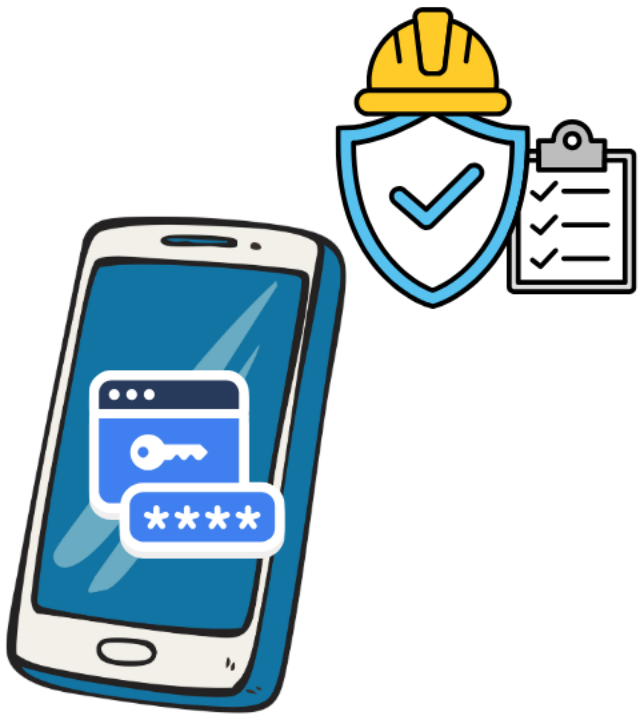

TikTok
@cyberpolice_th
ตำรวจไซเบอร์

android


****
AWARENESS
ABOUT
ONLINE
PRIVACY
#SAFERINTERNET #DIGITALSAFETY


พื้นฐานความปลอดภัยในการใช้งานคอมพิวเตอร์
UPDATE
Windows/macOS
การดูแลระบบปฏิบัติการ
(OS & Software Updates)
หมั่นอัปเดต Windows, macOS หรือโปรแกรมต่างๆ
ให้เป็นปัจจุบันเสมอ เพื่อปิดช่องโหว่
(Vulnerabilities) ที่ผู้ไม่หวังดีอาจใช้โจมตี
SCAN
การติดตั้งโปรแกรมป้องกันไวรัส
(Antivirus/Anti-Malware)
เปิดใช้งานระบบป้องกันพื้นฐาน (เช่น Windows
หรือโปรแกรมความปลอดภัยที่น่าเชื่อถือ
และสแกนเครื่องอย่างสม่ำเสมอ
การใช้อุปกรณ์เชื่อมต่อภายนอก
(USB Safety)
ระวังการนำ Flash Drive หรือ External
Hard Drive ที่ไม่ทราบที่มามาเสียบใช้งาน
เพราะอาจมีมัลแวร์ซ่อนอยู่
การล็อกหน้าจอ
(Screen Lock)
ล็อกหน้าจอเครื่องทุกครั้งเมื่อลุกออกจากโต๊ะทำงาน
(Win + L บน Windows หรือ Cmd + Ctrl + Q บน Mac)
ความปลอดภัยเริ่มต้นที่คุณ!

ระหัสผ่าน
PASSWORD



Cyber Support Unit

User Name
Password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	24 mins
7	Instantly	Instantly	3 hours	12 hours	1 day
8	Instantly	43 mins	1 weeks	1 month	3 months
9	Instantly	18 hours	1 year	5 years	16 years
10	Instantly	3 weeks	56 years	325 years	1k years
11	20 mins	1 year	2k years	20k years	76k years
12	3 hours	37 years	151k years	1m years	5m years
13	1 day	962 years	7m years	77m years	375m years
14	2 weeks	25k years	409m years	4bn years	26bn years
15	5 months	650k years	21bn years	298bn years	1tn years
16	4 years	16m years	1tn years	18tn years	128tn years
17	39 years	439m years	57tn years	1qd years	9qd years
18	388 years	11bn years	2qd years	71qd years	631qd years

https://www.hivesystems.com/password-table?hl=th-TH

2FA

Passkey: อนาคตการล็อกอินที่ไร้รหัสผ่าน

ทำความรู้จักและเปรียบเทียบกับรหัสผ่านแบบเดิม

Passkey คืออะไร?

ระบบยืนยันตัวตนใหม่ที่ปลอดภัยกว่า
ไม่ต้องใช้รหัสผ่าน

COMPUTER AS TARGET
THE KEY CONCEPT
APT Zero-Day

รหัสผ่านแบบเดิม
(Old Passwords)

- ต้องจำรหัสผ่านยาวและยาก
- เสี่ยงจากการถูก Phishing
- เสี่ยงต่อการเดารหัส (Brute Force)

Passkey แบบใหม่
(New Passkeys)

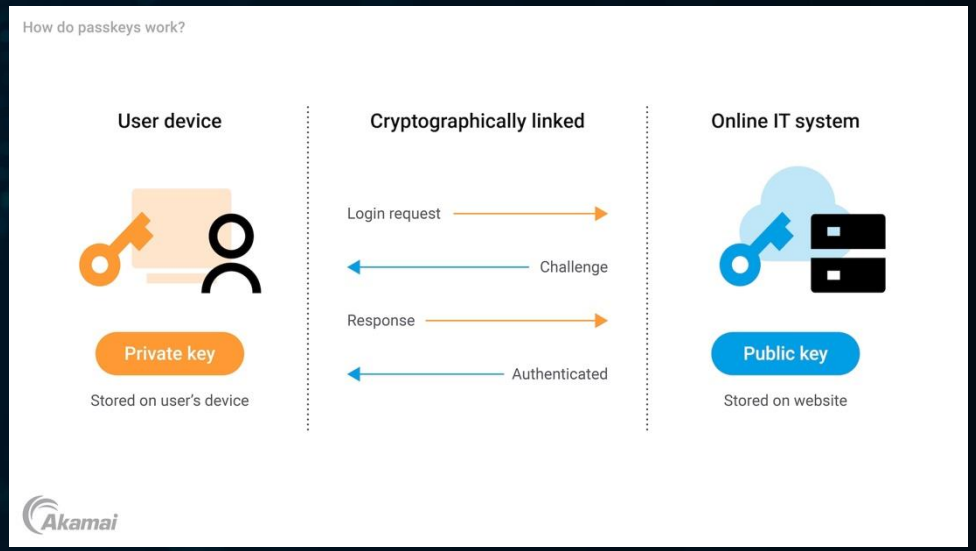
- ไม่ต้องจำรหัสผ่าน
- ใช้การสแกนลายนิ้วมือ, ใบหน้า, หรือ PIN
- ป้องกันการ Phishing 100% (ระดับสูงสุด)

ความปลอดภัยสูง
ยากต่อการโจมตี

สะดวกสบาย
รวดเร็วในการเข้าสู่ระบบ

ป้องกัน Phishing
ปกป้องจากการหลอกลวง

ใช้งานง่าย
เข้าถึงง่ายบนทุกอุปกรณ์



รวมเทคนิคการตั้งรหัสผ่านระดับสากล: ยุคเทคโนโลยีและปลอดภัย

เคล็ดลับจากผู้เชี่ยวชาญเพื่อป้องกันการโจรกรรมข้อมูล

1. เทคนิค “Passphrase”

ใช้ประโยคยาวๆ
ผสมคำที่ไม่เกี่ยวข้องกัน

เช่น:

Coffee-Rain-Running-Spaghetti

2. เทคนิค “ย่อประโยคจำใจความ”

เลือกประโยคที่ชอบ
เอาตัวอักษรแรกของคำมาตั้ง

I like to eat Pizza
-> IlteP!

3. เทคนิค “ต่อเติมท้าย” (The Matrix)

ตั้ง “รหัสหลัก” ที่แข็งแกร่ง

SuperSafe2026

แล้วเติมโค้ดลับของเว็บ

@FB
@GM
@NL

4. เทคนิค “รหัสไทยบนแป้นอังกฤษ”

พิมพ์ภาษาไทยบนแป้นอังกฤษ
แฮกเกอร์เดาไม่ออก

แมวบิน → lv[:lv

เทคนิคเสริมความปลอดภัยเพิ่มเติม

- ห้ามใช้รหัสซ้ำ
- เปลี่ยนเมื่อจำเป็นเท่านั้น
- เปิดใช้ 2FA เสมอ

ที่มา: รวบรวมโดย เมษา - ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์

อัปเดต: พ.ศ. 2569

อัปเดต: พ.ศ. 2569


1
Gmail (gmail.com)
พื้นที่เก็บข้อมูลฟรี : 15GB
2
Outlook (outlook.live.com)
พื้นที่เก็บข้อมูลฟรี : 15GB
3
Yahoo mail (mail.yahoo.com)
พื้นที่เก็บข้อมูลฟรี : 1TB
4
Zoho Mail (zoho.com)
พื้นที่เก็บข้อมูลฟรี : 5GB
5
AOL Mail (aolmail.com)
พื้นที่เก็บข้อมูลฟรี : 25MB
6
Mail.com
พื้นที่เก็บข้อมูลฟรี : 2GB
7
Protonmail (protonmail.com)
พื้นที่เก็บข้อมูลฟรี : 500MB
8
GMX Mail (gmx.com)
พื้นที่เก็บข้อมูลฟรี : 2GB
9
ICloud Mail (cloud.com)
พื้นที่เก็บข้อมูลฟรี : 5GB
10
10 อันดับอีเมลฟรี ปี 2019 มาแรง
Yandex.Mail (mail.yandex.com)
พื้นที่เก็บข้อมูลฟรี : 10GB

EMAIL SECURITY BEST PRACTICES

5 กฎเหล็ก... พื้นฐานการใช้อีเมลให้ปลอดภัย ป้องกันภัยคุกคามไซเบอร์

1

Strong & Unique Password

ตั้งรหัสผ่านให้รัดกุม และไม่ซ้ำใคร

ยาว 12+ ตัวอักษร ผสมอักษร-ใหญ่ ตัวเลย และ สัญสลักษณ์ ตัวเลย และ ลัญลักษณ์ ห้ามใช้บัญชีอื่นเต็ดาด

2

Enable 2FA / MFA

เปิดการยืนยันตัวตน 2 ชั้น

เกราะป้องยันขั้นที่อง ป้องการเยีกเข้าพืบบบบอ่างได้ มากกว่า 99% แม้รห้น่านะธัวไหล

3

Verify Sender & Links (Phishing Awareness)

เช็กผู้ส่งและลิงก์ก่อนคลิกเสมอ

ลังกผู้ส่งโอเบบผู้ส่องอ่างที่ถ้วน (เขีน paypal.com vas paypa1.com) และเน่าาลิ์ไบ่วางเหนีสัจก์ (Hover) เฟัลตู URL จรังท่อนกด

4

Beware of Urgent Urgency & Attachments

น๊อะะ อย่าหลงกลคำขู่ และระวังไฟล์แนบ

มือจาพิพพักสร้างความตกใจ เช่น "บัญชีวะ๓ะโดมระถับใน 24 ชน." และห้านเปิดไฟล์แบบยบระเทกภ .em..exe, zip หรังไฟล์ก์ไม่ไม่รู้จัก

5

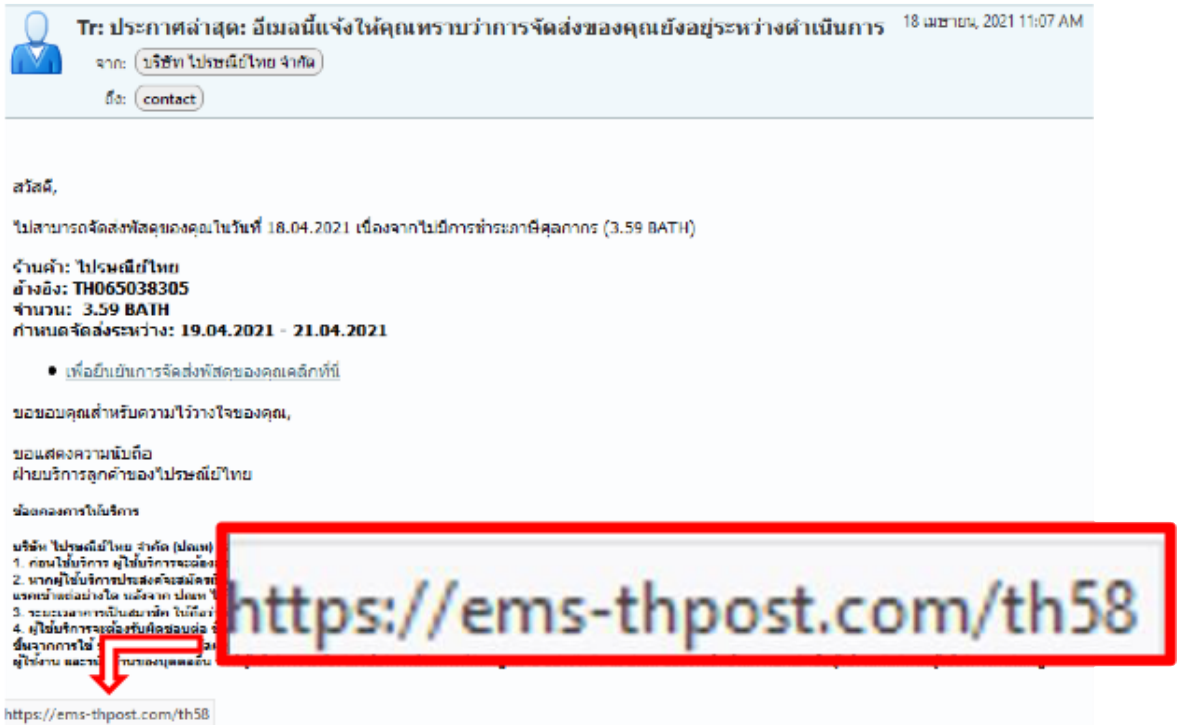
Monitor Sign-in Activity

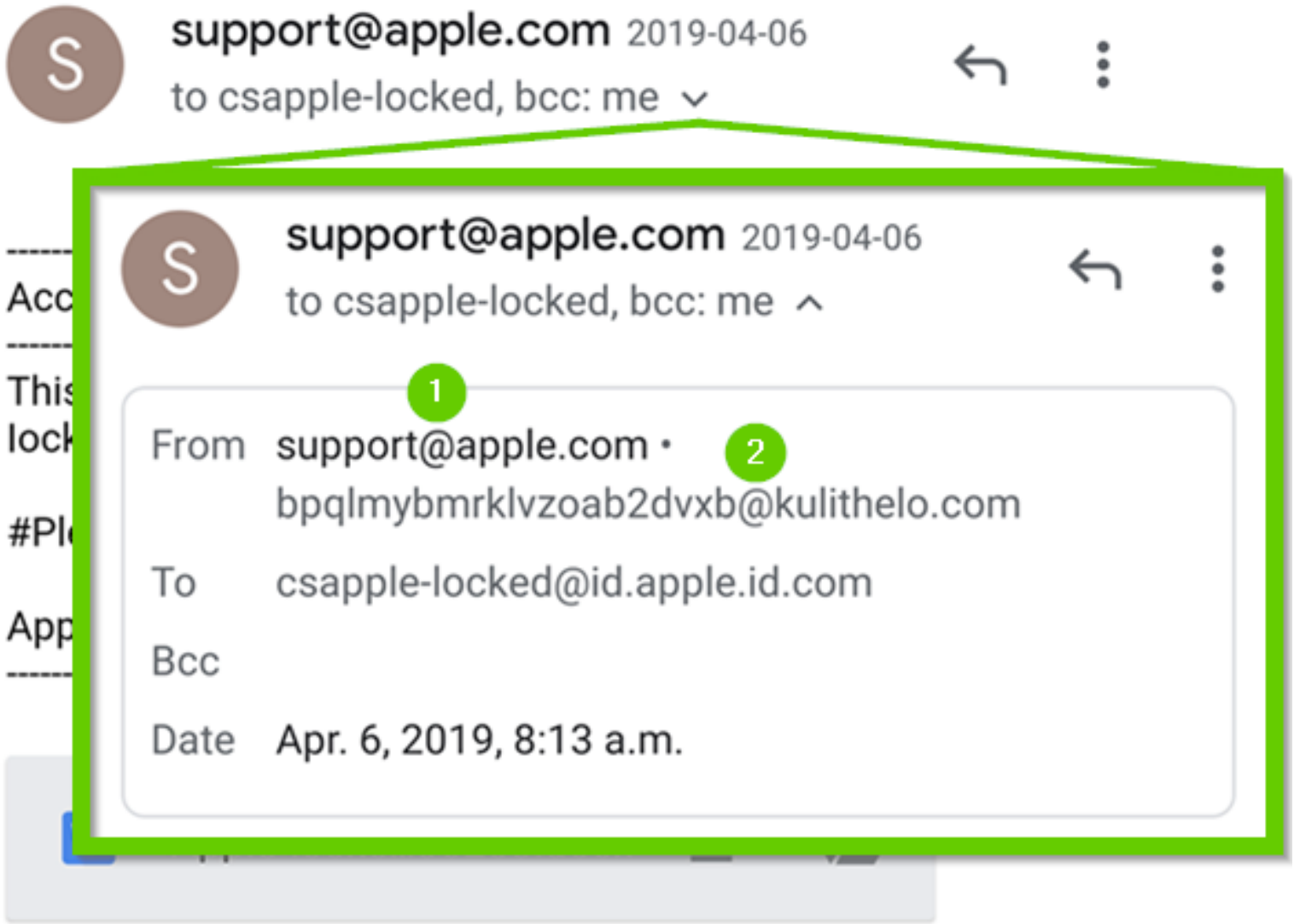
ตรวจสอบประวัติการเข้าใช้งาน

หนึ่บเล็กตั้งทำความปลอดกัดยิเตา ม่มีขุปกรณ์แปลกปลอบลือกอีนอยู่ หรือไม่ หากพบความผิอปกทิให้าติ Log Out All Devices ทันที

Remember: "ความประมาทเพียงคลิกเดียว อาจสร้างความเสียหายให้ทั้งองค์กร" หากพบอีเมลสงสัยว่าจะเป็น Phishing ให้แจ้งทีม IT / Security ทันที

ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน




S
support@apple.com 2019-04-06
to csapple-locked, bcc: me
S
support@apple.com 2019-04-06
to csapple-locked, bcc: me
1
2
From support@apple.com •
bpqlmybmrklvzoab2dvxb@kulithelo.com
To csapple-locked@id.apple.id.com
Bcc
Date Apr. 6, 2019, 8:13 a.m.

เจรจาเรื่องความร่วมมือ External Inbox ×

Starlink live <starlinklive.web3@gmail.com> 2:46 PM (6 hours ago)

to contact

สวัสดียินดีที่ได้รู้จัก.
ฉันเป็นผู้เชี่ยวชาญด้านการประชาสัมพันธ์แอปพลิเคชันวิดีโอสั้น starlinklive บริษัทดำเนินธุรกิจด้านการลงทุนและการจัดการทางการเงินเป็นหลัก การลงทุนมีเสถียรภาพและให้ผลกำไร และโครงการการลงทุนที่ให้ผลตอบแทนสูง ฉันพบคุณผ่านวิดีโอ YouTube สาธารณะของคุณ และต้องการเชิญคุณให้โปรโมตพวกเขา ไลน์ไอดีของฉัน: starlinklive02
หากคุณสนใจที่จะร่วมมือโปรดติดต่อฉันขอบคุณ

ตอบกลับ ตอบกลับทั้งหมด ส่งต่อ

ส. 9/6/2560 12:26

ธนาคารกสิกรไทย (KASIKORN BANK) <nooriebook@hanmail.net>

การโอนเงินที่น่าสงสัย / suspicious fund transfer ref: 2332 // 988 (มิถุนายน 9, 2017)

ถึง [redacted]

คลิกที่นี่เพื่อดาวน์โหลดรูปภาพ เพื่อป้องกันความเป็นส่วนตัวของคุณ Outlook ได้หลีกเลี่ยงการดาวน์โหลดรูปภาพบางรูปโดยอัตโนมัติในข้อความนี้
Outlook ได้บล็อกไม่ให้เข้าถึงสิ่งที่แนบมาที่มีแนวโน้มว่าไม่ปลอดภัยดังต่อไปนี้: การโอนเงินที่น่าสงสัย (มิถุนายน 9, 2017) ref_ 2332-988.jar.

เรียน ลูกค้า

เรา ได้ รับ การ โอน เงิน ที่ น่า สงสัย จาก บัญชี ธนาคาร ของ คุณ เป็น จำนวน เงิน 19,890 บาท โดย มี รหัส การ ทำ ธุรกรรม 2332 // 988

โปรด ดู ราย ละเอียด การ ชำระ เงิน ที่ แนบ มา เพื่อ ยืนยัน

ฝ่าย บัญชี
ธนาคาร กสิกร ไทย

.....-

แม้ว่า ข้อมูล นี้ เป็น สิ่ง ที่ สำคัญ สำหรับ ทุก คน ใน ปัจจุบัน เพื่อ ให้ บริการ ลูกค้า เป็น ความ ลับ ของ เรา

ธนาคารกสิกรไทย (KASIKORN BANK) ไม่มีราบการ

Subject: ยืนยันการชำระเงิน

สวัสดีตอนเช้า
โปรดยืนยันการชำระเงินที่แนบมาและส่งใบแจ้งยอดบัญชีของคุณ
ด้วยความนับถือ:

1 attachment: การชำระเงิน 00252021-01.7z 533 KB

การชำระเงิน 00252021-01.7z 533 KB

.7z

Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan

การชำระเงิน 00252021-01.7z - 7-Zip archive, unpacked size 1,247,744 bytes

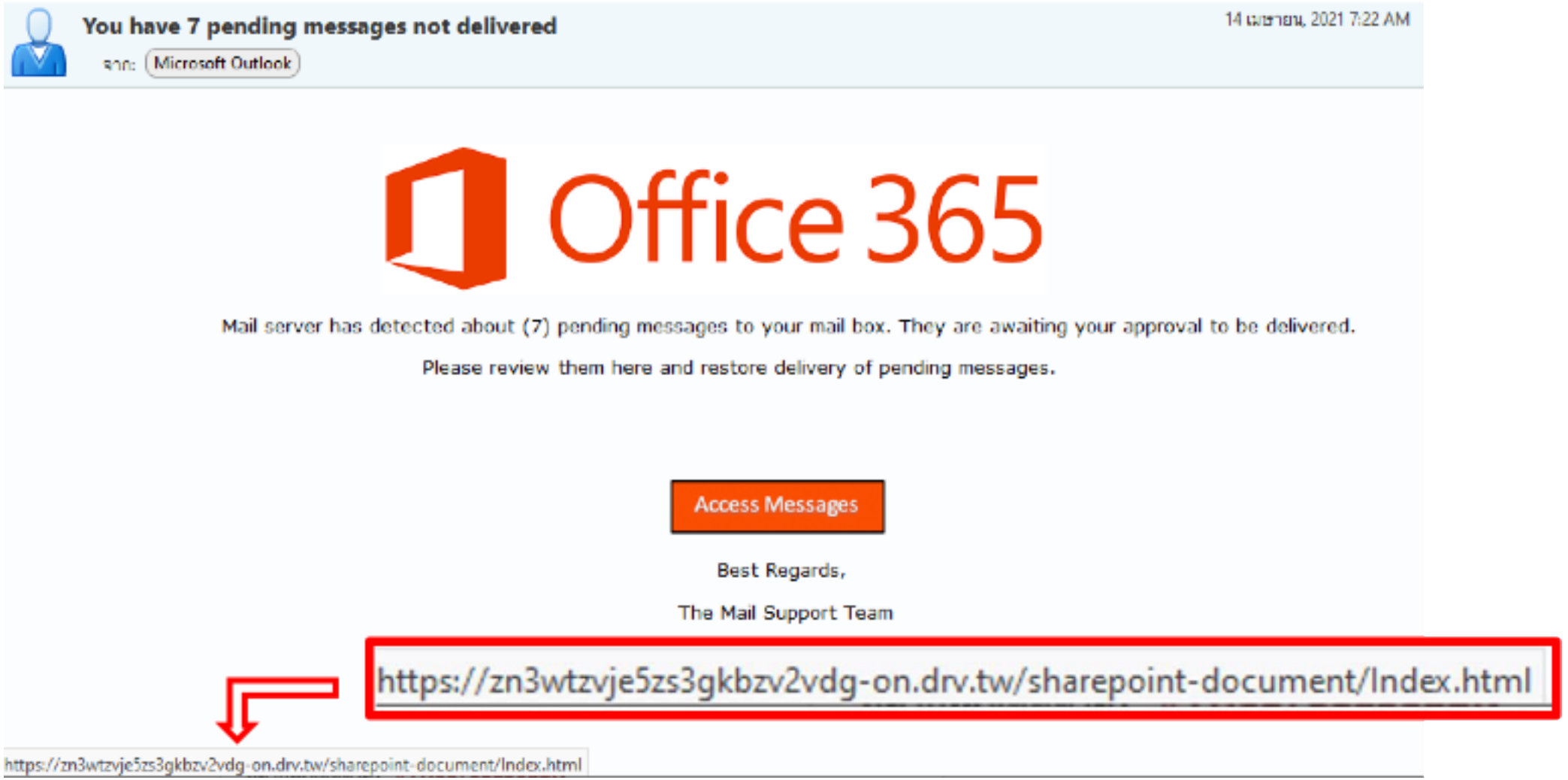
Name	Size	Packed	Type	Modified
..			File folder	
agreement.pdf.....exe	0	0	Application	2021-01-25 20:12
การชำระเงิน 00252021-01.exe	1,247,744	545,417	Application	2021-01-25 07:29

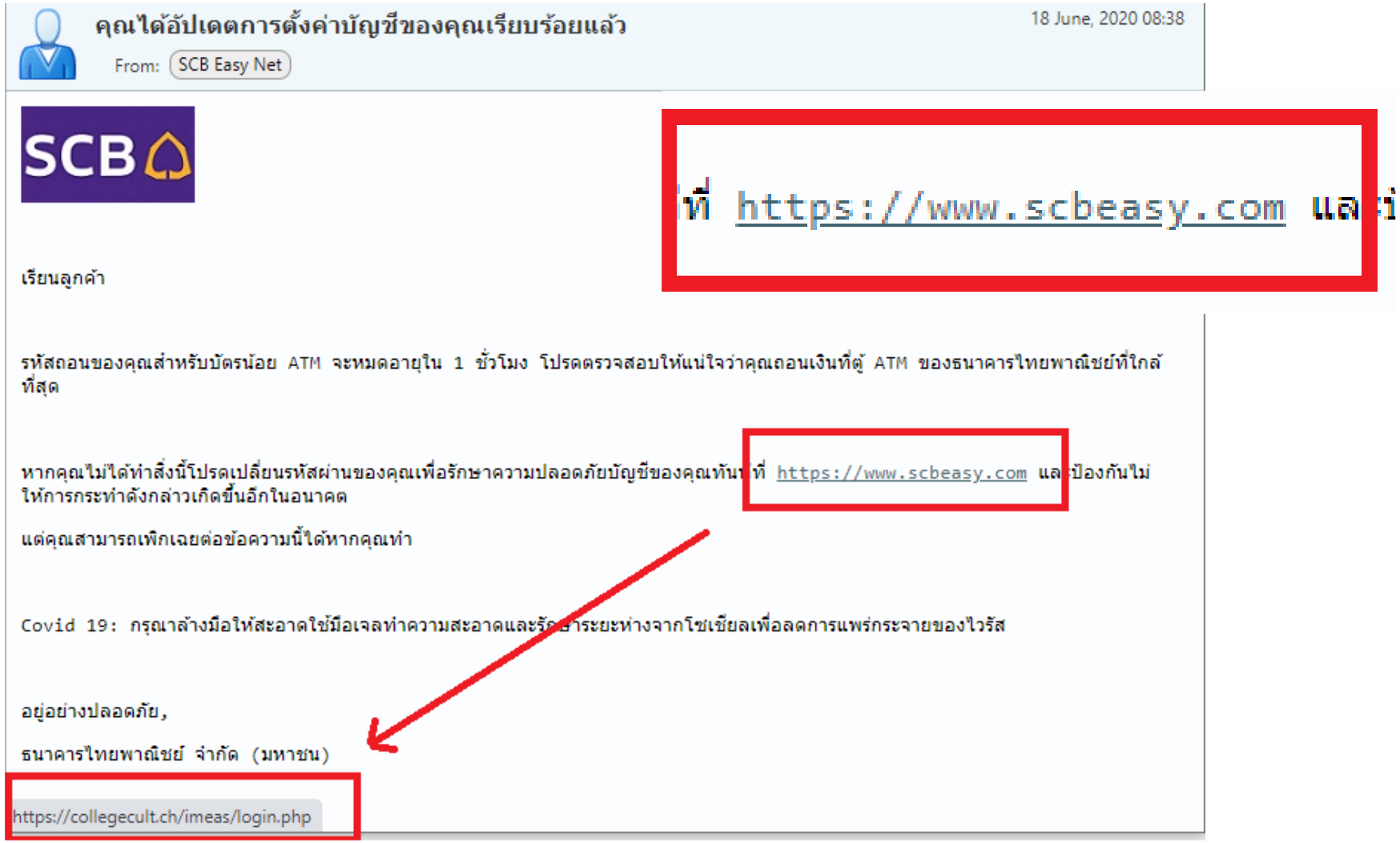
ตัวอย่างไฟล์อันตราย

iReallyHost.com

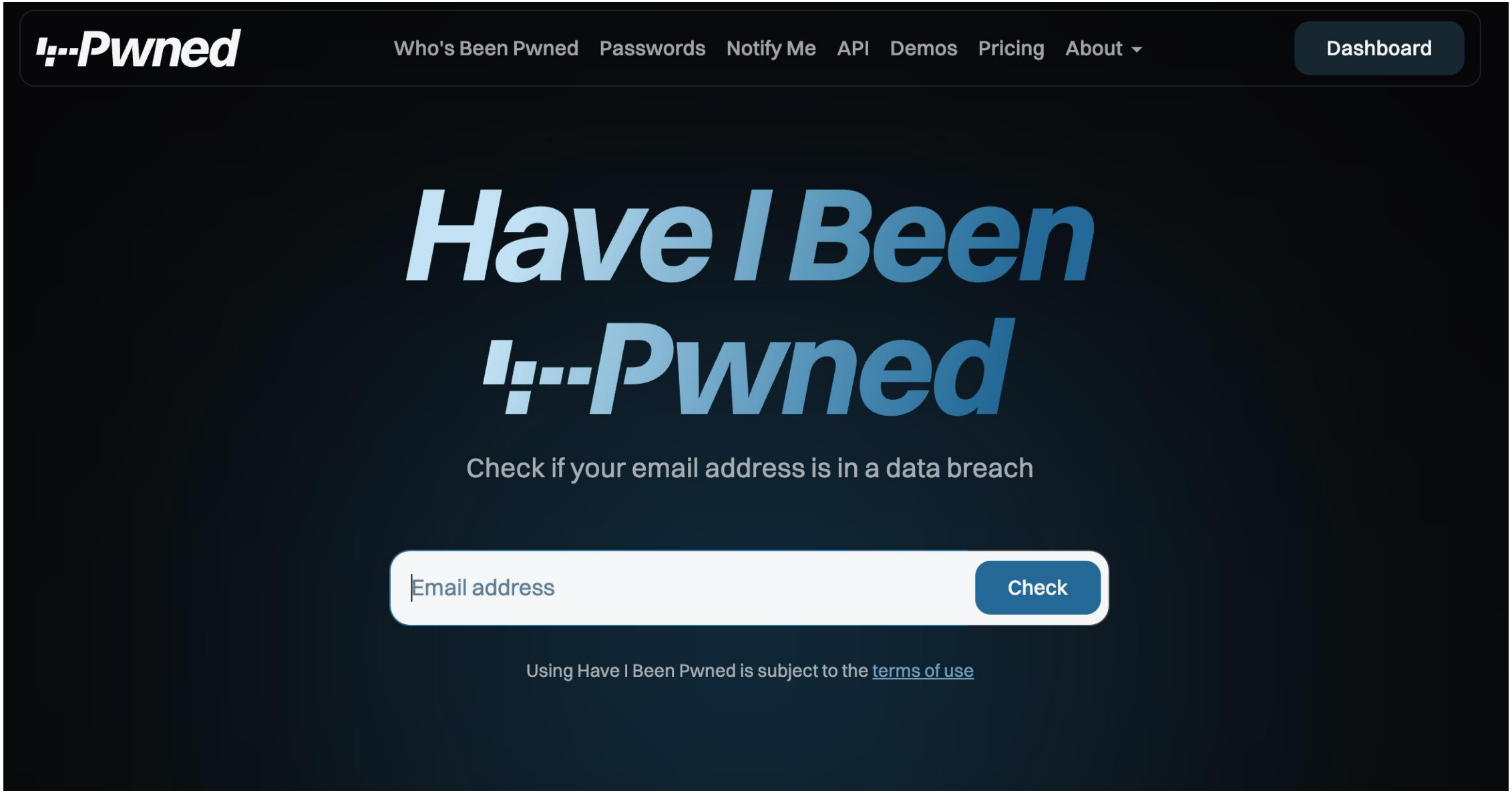
มักลงด้ายด้วย .exe , .bin , .reg

Total 1,247,744 bytes in 2 files

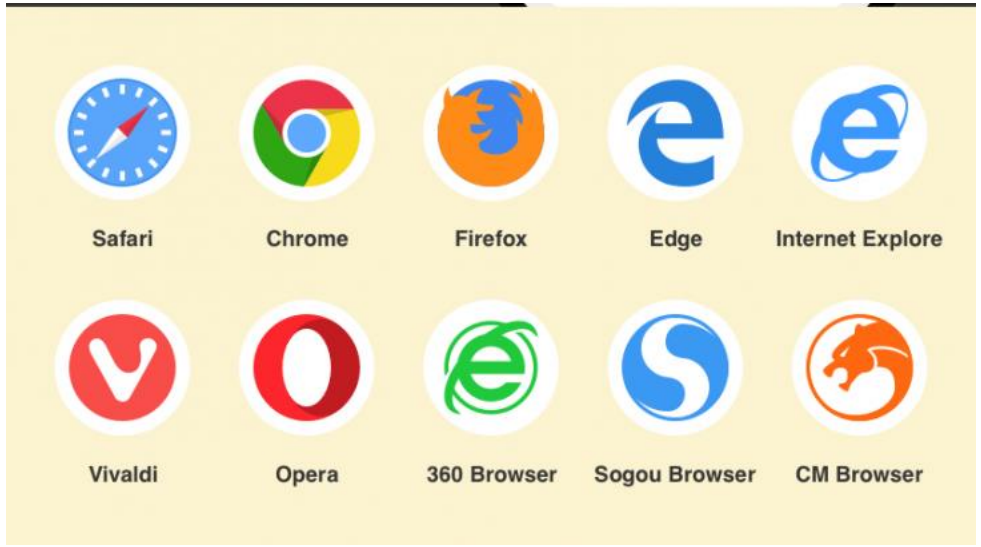

You have 7 pending messages not delivered
จาก: Microsoft Outlook
14 เมษายน, 2021 7:22 AM
Office 365
Mail server has detected about (7) pending messages to your mail box. They are awaiting your approval to be delivered.
Please review them here and restore delivery of pending messages.
Access Messages
Best Regards,
The Mail Support Team
https://zn3wtzvje5zs3gkbzv2vdg-on.drv.tw/sharepoint-document/Index.html
https://zn3wtzvje5zs3gkbzv2vdg-on.drv.tw/sharepoint-document/Index.html


คุณได้อัปเดตการตั้งค่าบัญชีของคุณเรียบร้อยแล้ว
18 June, 2020 08:38
From: SCB Easy Net
SCB
ที่ https://www.scbeasy.com และ
เรียนลูกค้า
รหัสถอนของคุณสำหรับบัตรน้อย ATM จะหมดอายุใน 1 ชั่วโมง โปรดตรวจสอบให้แน่ใจว่าคุณถอนเงินที่ตู้ ATM ของธนาคารไทยพาณิชย์ที่ใกล้ที่สุด
หากคุณไม่ได้ทำสิ่งนี้โปรดเปลี่ยนรหัสผ่านของคุณเพื่อรักษาความปลอดภัยบัญชีของคุณทันที ที่ https://www.scbeasy.com และป้องกันไม่ให้การกระทำดังกล่าวเกิดขึ้นอีกในอนาคต
แต่คุณสามารถเพิกเฉยต่อข้อความนี้ได้หากคุณทำ
Covid 19: กรุณาล้างมือให้สะอาดใช้มือเจลทำความสะอาดและรักษาระยะห่างจากโซเชียลเพื่อลดการแพร่กระจายของไวรัส
อยู่อย่างปลอดภัย,
ธนาคารไทยพาณิชย์ จำกัด (มหาชน)
https://collegecult.ch/imeas/login.php

https://haveibeenpwned.com/



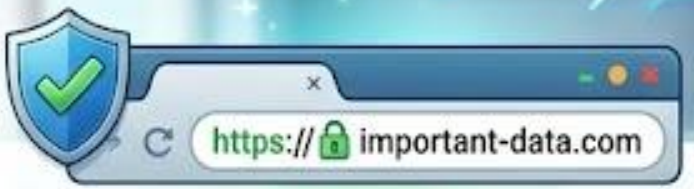
Web Browser



Website

ความปลอดภัยในการใช้งานเว็บไซต์และเบราว์เซอร์

เบราว์เซอร์คือประตูเปิดไปสู่โลกอินเทอร์เน็ต
ซึ่งเป็นช่องทางหลักที่มัลแวร์และเว็บไซต์หลอกลวงใช้โจมตี



HTTPS / Secure Connection

1. สังเกตการเข้ารหัสข้อมูล (HTTPS)

ตรวจสอบว่า URL เริ่มต้นด้วย https:// และมีสัญลักษณ์
รูปกุญแจล็อก ก่อนกรอกข้อมูลสำคัญเสมอ

2. ตรวจสอบชื่อโดเมน (Domain Name Verification)

สังเกตตัวสะกดของ URL อย่างละเอียด
เช่น google.com กับ g00gle.com
เพื่อป้องกันการตกเป็นเหยื่อ Phishing Website

3. การจัดการส่วนขยาย (Browser Extensions)

ติดตั้งเฉพาะส่วนขยายที่จำเป็นจาก
Official Store เท่านั้น และลบส่วนขยาย
ส่วนขยายที่ไม่รู้จักหรือไม่ได้ใช้ออกทันที

4. การจัดการคุกกี้ และประวัติการใช้งาน

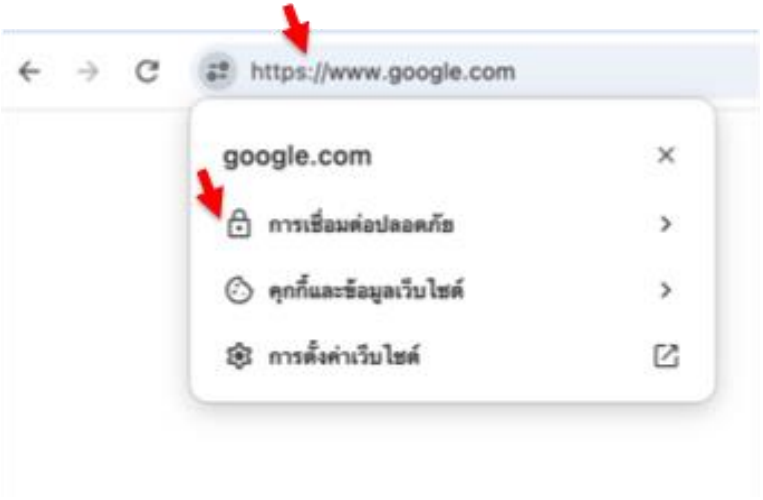
ล้าง Cache, Cookies และ Session การเข้าสู่ระบบเป็นประจำ
โดยเฉพาะเมื่อใช้งานคอมพิวเตอร์สาธารณะหรือคอมพิวเตอร์ที่ใช้ร่วมกับผู้อื่น

ความปลอดภัยเริ่มต้นที่คุณ!

- นักวิจัยด้านความปลอดภัยไซเบอร์เคยตรวจพบว่า เมื่อเราใช้งานฟีเจอร์ Password Manager บน Microsoft Edge (รวมถึงเว็บบราวเซอร์กลุ่ม Chromium อื่นๆ ในลักษณะใกล้เคียงกัน) ในขณะที่บราวเซอร์กำลังประมวลผลหรือกรอกรหัสผ่านให้อัตโนมัติ รหัสผ่านนั้นจะถูกดึงเข้ามาพักไว้ใน **RAM (Memory)** ของเครื่องชั่วคราว
- ในช่วงเวลาที่อยู่ใน RAM ข้อมูลรหัสผ่านนั้นจะอยู่ในรูปแบบข้อความธรรมดา (Plain Text) ไม่ได้เข้ารหัสไว้

เงื่อนไขสำคัญที่ต้องเกิดก่อนถึงจะโดน Hack ได้:

- แฮกเกอร์ **ไม่สามารถ** ดึงรหัสผ่านออกไปจากระยะไกลได้ทันทีเพียงแค่เราใช้ Edge
- เครื่องคอมพิวเตอร์ของคุณ **ต้องถูกฝังมัลแวร์ (Infostealer / Malware)** หรือมีผู้ไม่หวังดีสิทธิ์ Administrator เข้าถึงเครื่องได้แล้วเท่านั้น ถึงจะสามารถรันคำสั่งดึงข้อมูลจาก RAM (Memory Dump) ออกไปได้
- หมายความว่า หากเครื่องปลอดภัย ไม่มีมัลแวร์ติดอยู่ รหัสผ่านใน RAM นั้นก็ไม่ได้หลุดออกไปไหน

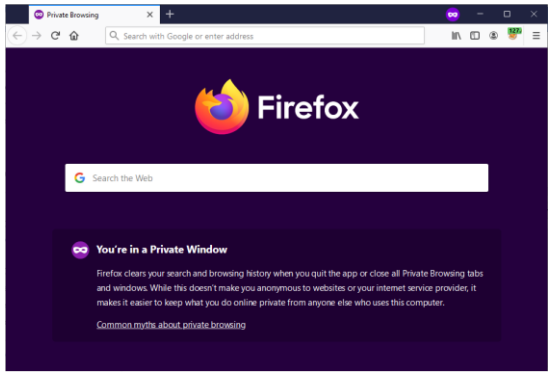

https://www.google.com
google.com
การเชื่อมต่อปลอดภัย
คุกกี้และข้อมูลเว็บไซต์
การตั้งค่าเว็บไซต์


DEV
http://www.example.com
password: abc123
HTTP
https://www.example.com
password: abc123
HTTPS
HTTP
& HTTPS
เหมือนจะต่างกันแค่ตัว S
แต่ความปลอดภัยคนละเรื่องเลย

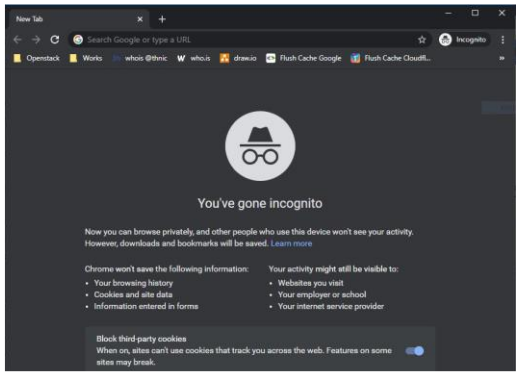

Without password encryption
Hacker see "abc123"


With password encryption
Hacker see "XyaeRXbya"

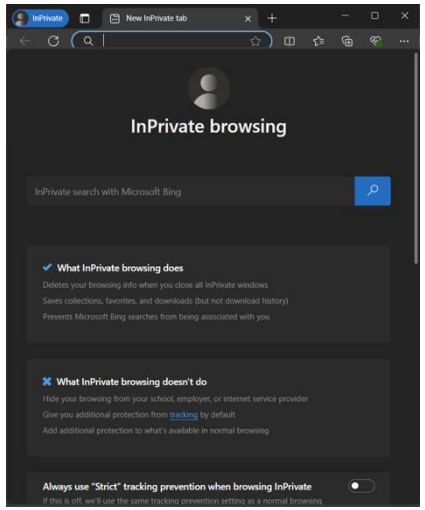
ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัว ควรใช้งาน Browser ในโหมด Safe Web Browsing



Private Windows



Incognito mode
โหมดแบบไม่ระบุตัวตน



InPrivate browsing
โหมดแบบไม่ระบุตัวตน

- ไม่บันทึกประวัติการท่องเว็บ
- ไม่บันทึกคุกกี้และเซสชันการเข้าสู่ระบบ
- ไม่บันทึกข้อมูลการกรอกฟอร์มและรหัสผ่าน
- แยกการทำงานออกจากส่วนขยายแปลกปลอม

⚠ **ข้อควรระวังเพิ่มเติม (โหมดความเป็นส่วนตัวไม่ได้ป้องกัน 100%)**

- **โหมดนี้ป้องกันเฉพาะข้อมูลในตัวบราวเซอร์บนเครื่องนั้นเท่านั้น** แต่ผู้ดูแลเครือข่าย (Admin), Wi-Fi สาธารณะ, หรือโปรแกรมดักจับระดับเครื่อง (เช่น Keylogger / Malware) ยังอาจเห็นการเคลื่อนไหวหรือสิ่งที่พิมพ์ได้
- **หลีกเลี่ยงการทำธุรกรรมทางการเงิน** (เช่น Internet Banking หรือกรอกบัตรเครดิต) บนเครื่องที่ไม่ใช่ของเราเด็ดขาด
- **เมื่อใช้งานเสร็จ ให้ปิดหน้าต่างโหมดความเป็นส่วนตัวทุกหน้าต่างทันที** เพื่อสั่งให้ระบบทำการลบข้อมูลชั่วคราวออกทั้งหมด

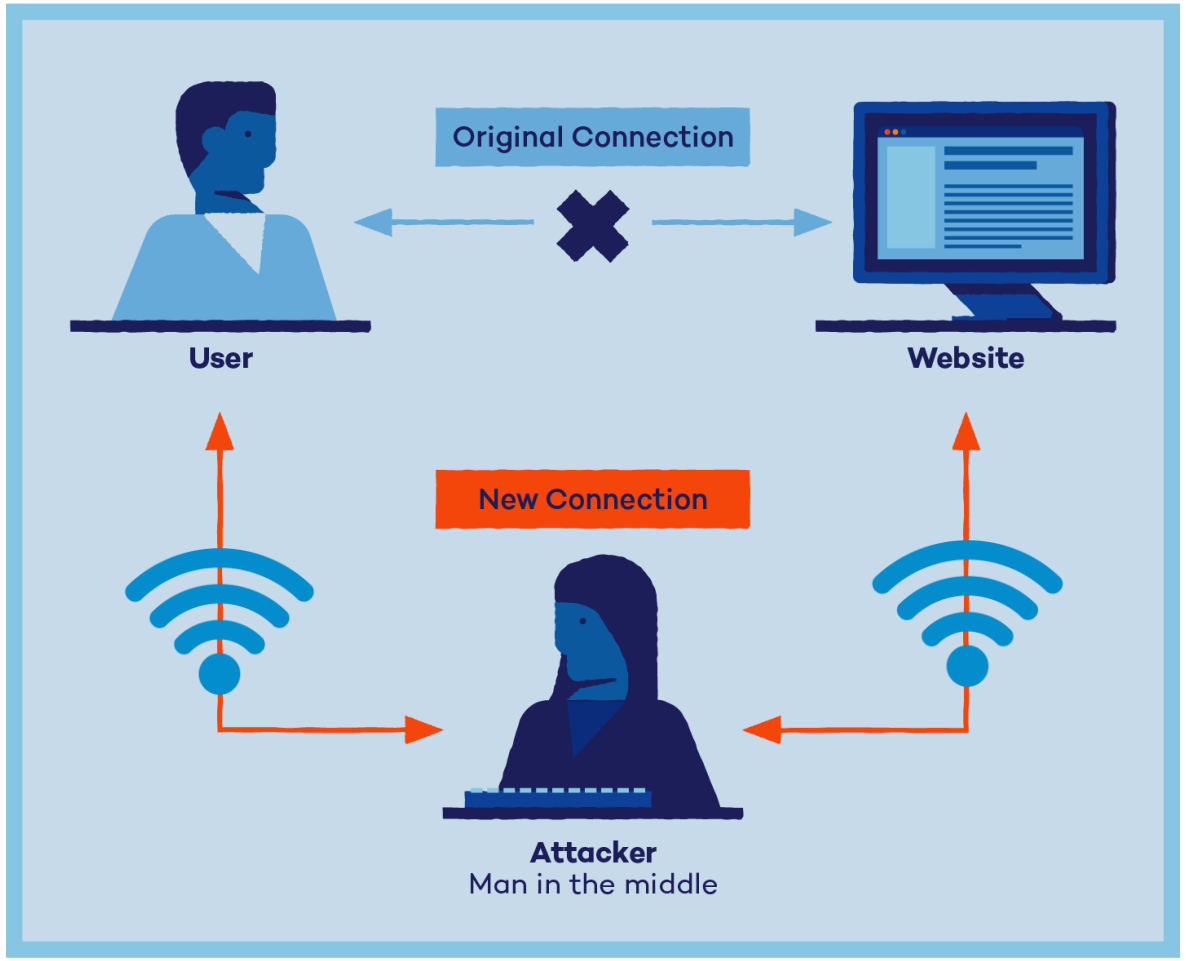
ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัว

เข้าใช้งานโดย QR

ห้ามบันทึกรหัสผ่านไว้


Wi
Fi
TM

1. ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
2. หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ



Wi-Fi ที่บ้าน: ตั้งค่ายังไงให้ปลอดภัย?

1. **อย่าใช้รหัสตั้งต้นจากโรงงาน:** รหัสผ่านสำหรับเข้าตั้งค่ากล่อง Wi-Fi (Router) มักจะเป็น admin/admin ให้เปลี่ยนทันทีตั้งแต่วันแรก
2. **ตั้งรหัสผ่าน Wi-Fi ให้เดายาก:** ยาวอย่างน้อย 12 ตัวอักษร ผสมตัวเลขและอักษรพิเศษ (อย่าใช้เบอร์โทร หรือวันเกิด)
3. **เปิด Wi-Fi สำหรับผู้มาเยือน (Guest Wi-Fi):** เวลาเพื่อนมาบ้าน ให้เชื่อมต่อช่องนี้ เพื่อแยกอุปกรณ์ของเพื่อนออกจากทีวี กล้องวงจรปิด หรือคอมพิวเตอร์ทำงานของเรา
4. **ปิดระบบ WPS:** ปุ่มกดเชื่อมต่อแบบง่ายๆ (WPS) บนกล่อง Wi-Fi คือช่องโหว่ที่แฮกเกอร์ชอบใช้เจาะรหัสผ่าน ให้ปิดไว้ปลอดภัยที่สุด

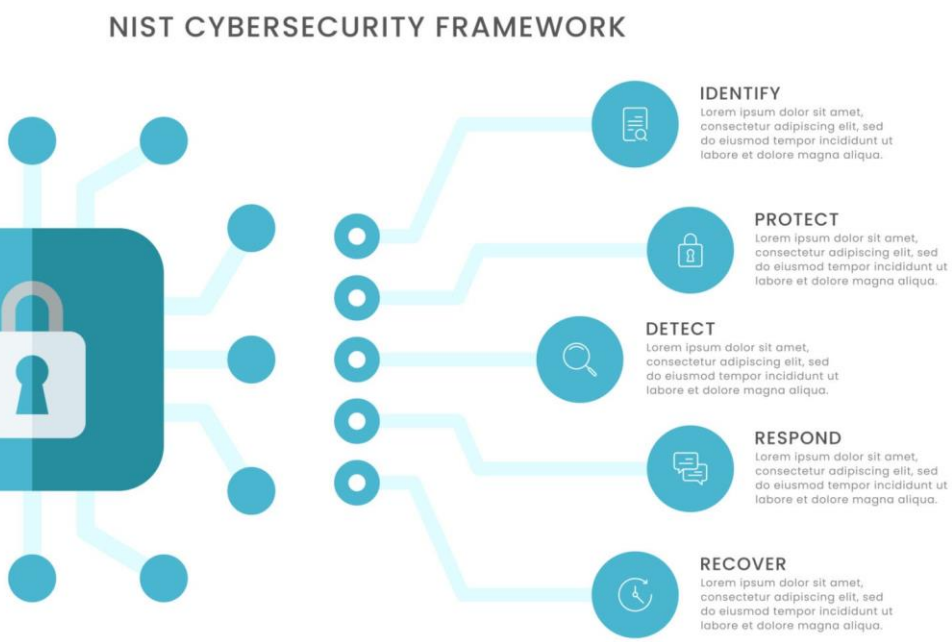
☕ **2. Wi-Fi สาธารณะ (ร้านกาแฟ / สนามบิน / โรงแรม): ใช้งานอย่างไรไม่ให้โดนแฮก?**

- **ห้ามทำธุรกรรมการเงิน:** ไม่เข้าแอปธนาคาร ไม่โอนเงิน ไม่กรอกเลขบัตรเครดิตขณะเชื่อมต่อ Wi-Fi ฟรี
- **ใช้ VPN ช่วยล็อกข้อมูล:** หากจำเป็นต้องทำงาน ให้เปิดแอป VPN เพื่อสร้างท่อส่งข้อมูลที่เข้ารหัสปลอดภัย
- **ปิดระบบเชื่อมต่ออัตโนมัติ (Auto-Connect):** ตั้งค่ามือถือ/โน้ตบุ๊กไม่ให้แอบต่อ Wi-Fi สาธารณะเองเมื่อเดินผ่าน

Internet of things

AIOT

Physical AI



1. การบริหารจัดการสิทธิ์และการยืนยันตัวตน (Authentication & Access Control)
2. การแยกเครือข่ายใช้งาน (Network Segmentation)
3. การอัปเดตเฟิร์มแวร์และพัตช์ (Firmware & Patch Management)
4. การเข้ารหัสข้อมูล (Data Encryption)
5. การกำหนดโครงสร้างและปิดช่องทางที่ไม่จำเป็น (Hardening & Service Minimization)

การเลือกซื้ออุปกรณ์ **IoT (Internet of Things)**

ยี่ห้อและแบรนด์ที่น่าเชื่อถือ (Brand & Ecosystem)

- **มีชื่อเสียงด้านความปลอดภัย:** เลือกร้านค้าหรือแบรนด์ที่มีชื่อคุ้นหู มีช่องทางติดต่อชัดเจน หลีกเลี่ยงอุปกรณ์โนเนมราคาถูกผิดปกติที่ไม่มีระบุชื่อผู้ผลิต
- **อยู่ในระบบนิเวศ (Ecosystem) มาตรฐาน:** อุปกรณ์ที่รองรับแพลตฟอร์มหลัก เช่น Google Home, Apple Home, Samsung SmartThings หรือแอปยอดนิยมอย่าง Tuya/Smart Life มักจะผ่านการตรวจสอบมาตรฐานความปลอดภัยในระดับหนึ่ง
- **มองหาโลโก้ "Matter":** หากอุปกรณ์รองรับมาตรฐาน **Matter** จะช่วยเรื่องความปลอดภัย การทำงานร่วมกันระหว่างแบรนด์ และการเชื่อมต่อในบ้านได้เสถียรยิ่งขึ้น

การเลือกซื้ออุปกรณ์ **IoT (Internet of Things)**

ตรวจสอบ "ฉลาก" หรือ "ระบบความปลอดภัย" ข้างกล่อง
เวลาพลิกดูข้างกล่อง หรืออ่านรายละเอียดสินค้า ให้มองหาคำเหล่านี้:

- **การเข้ารหัสข้อมูล (Encryption):** มีคำว่า **AES-128**, **AES-256**, **TLS** หรือ **HTTPS** เพื่อให้มั่นใจว่าข้อมูล ภาพ หรือคำสั่งจะไม่ถูกดักจับระหว่างทาง
- **End-to-End Encryption (E2EE):** โดยเฉพาะ **กล้องวงจรปิด** หรือ **กริ่งประตู** ควรเลือกที่มี E2EE ซึ่งหมายความว่ามีแค่เราเท่านั้นที่ดูภาพได้ แม้แต่ผู้ให้บริการคลาวด์ก็แอบดูไม่ได้
- **มาตรฐาน Wi-Fi:** อุปกรณ์ต้องรองรับ **WPA2** ขึ้นไป (หรือ **WPA3** จะดีที่สุด) ไม่ควรซื้ออุปกรณ์ที่รองรับแค่ระบบ WEP เพราะแฮกง่ายมาก

การเลือกซื้ออุปกรณ์ **IoT (Internet of Things)**

มีระบบอัปเดตความปลอดภัย (Security Updates & Firmware)

- **นโยบายการอัปเดต:** ตรวจสอบดูว่าผู้ผลิตมีประวัติออกอัปเดต "เฟิร์มแวร์" (Firmware) สม่ำเสมอไหม หากเป็นไปได้ ให้เลือกแบรนด์ที่ระบุชัดเจนว่าจะสนับสนุนการอัปเดตความปลอดภัยอย่างน้อย 2-5 ปี
- **รองรับการอัปเดตอัตโนมัติ (Auto Update):** ช่วยให้อุปกรณ์ปิดช่องโหว่ความปลอดภัยใหม่ๆ ได้เองโดยที่เราไม่ต้องคอยกดอัปเดตเองบ่อยๆ

บังคับให้เปลี่ยนรหัสผ่านทันที (No Default Password)

- **ปฏิเสธรหัสผ่านกลาง:** หลีกเลี่ยงอุปกรณ์ที่ใช้รหัสผ่านเริ่มต้นแบบง่ายๆ เหมือนกันหมดทุกเครื่อง เช่น 123456 หรือ admin โดยที่ระบบไม่ยอมให้เราเปลี่ยน
- **อุปกรณ์ที่ดี:** เมื่อเปิดใช้งานครั้งแรก ระบบจะต้อง **บังคับ** ให้เราตั้งรหัสผ่านใหม่ หรือกำหนดรหัสผ่านเฉพาะตัวมาให้ตั้งแต่โรงงาน (Unique Password)

การเลือกซื้ออุปกรณ์ **IoT (Internet of Things)**

มีระบบอัปเดตความปลอดภัย (Security Updates & Firmware)

- **นโยบายการอัปเดต:** ตรวจสอบดูว่าผู้ผลิตมีประวัติออกอัปเดต "เฟิร์มแวร์" (Firmware) สม่ำเสมอไหม หากเป็นไปได้ ให้เลือกแบรนด์ที่ระบุชัดเจนว่าจะสนับสนุนการอัปเดตความปลอดภัยอย่างน้อย 2-5 ปี
- **รองรับการอัปเดตอัตโนมัติ (Auto Update):** ช่วยให้อุปกรณ์ปิดช่องโหว่ความปลอดภัยใหม่ๆ ได้เองโดยที่เราไม่ต้องคอยกดอัปเดตเองบ่อยๆ

บังคับให้เปลี่ยนรหัสผ่านทันที (No Default Password)

- **ปฏิเสธรหัสผ่านกลาง:** หลีกเลี่ยงอุปกรณ์ที่ใช้รหัสผ่านเริ่มต้นแบบง่ายๆ เหมือนกันหมดทุกเครื่อง เช่น 123456 หรือ admin โดยที่ระบบไม่ยอมให้เราเปลี่ยน
- **อุปกรณ์ที่ดี:** เมื่อเปิดใช้งานครั้งแรก ระบบจะต้อง **บังคับ** ให้เราตั้งรหัสผ่านใหม่ หรือกำหนดรหัสผ่านเฉพาะตัวมาให้ตั้งแต่โรงงาน (Unique Password)

แอปพลิเคชันและการจัดการความเป็นส่วนตัว (App & Privacy)

- **รองรับการยืนยันตัวตน 2 ชั้น (2FA / MFA):** แอปพลิเคชันที่ใช้ควบคุมอุปกรณ์ต้องรองรับการส่งรหัส OTP หรือกดรับรองในมือถืออีกขั้นก่อนเข้าใช้งาน
- **ขอสิทธิ์ตามจริง:** ตอนติดตั้งแอป สังเกตว่าแอปขอสิทธิ์มือถือเกินความจำเป็นไหม เช่น แอปควบคุมหลอดไฟ แต่กลับขอเข้าถึง "รายชื่อติดต่อ" หรือ "SMS" ในมือถือ ถือว่าน่าสงสัย

09.00 - 10.30

ภาพรวมสถานการณ์กลโกง

Scam Trends, รู้ทันตัวเอง และรู้ทันกลโกงจิตวิทยา 3 รูปแบบ

10.45 - 12.00

เจาะลึกแคสแอปดูดเงิน

กระบวนการติดมัลแวร์ ตั้งแต่ SMS จนถึงเงินถูกดูดออกจากบัญชี

13.00 - 14.30

รู้ทันเทคโนโลยี

การปกป้องอุปกรณ์ และฝึกปฏิบัติใช้แอป Police Care

ตรวจมิจฉาชีพ

14.45 - 16.30

กระบวนการเมื่อเกิดเหตุ

การเตรียมหลักฐาน แจ้งความออนไลน์ และทดสอบวัคซีนไซเบอร์

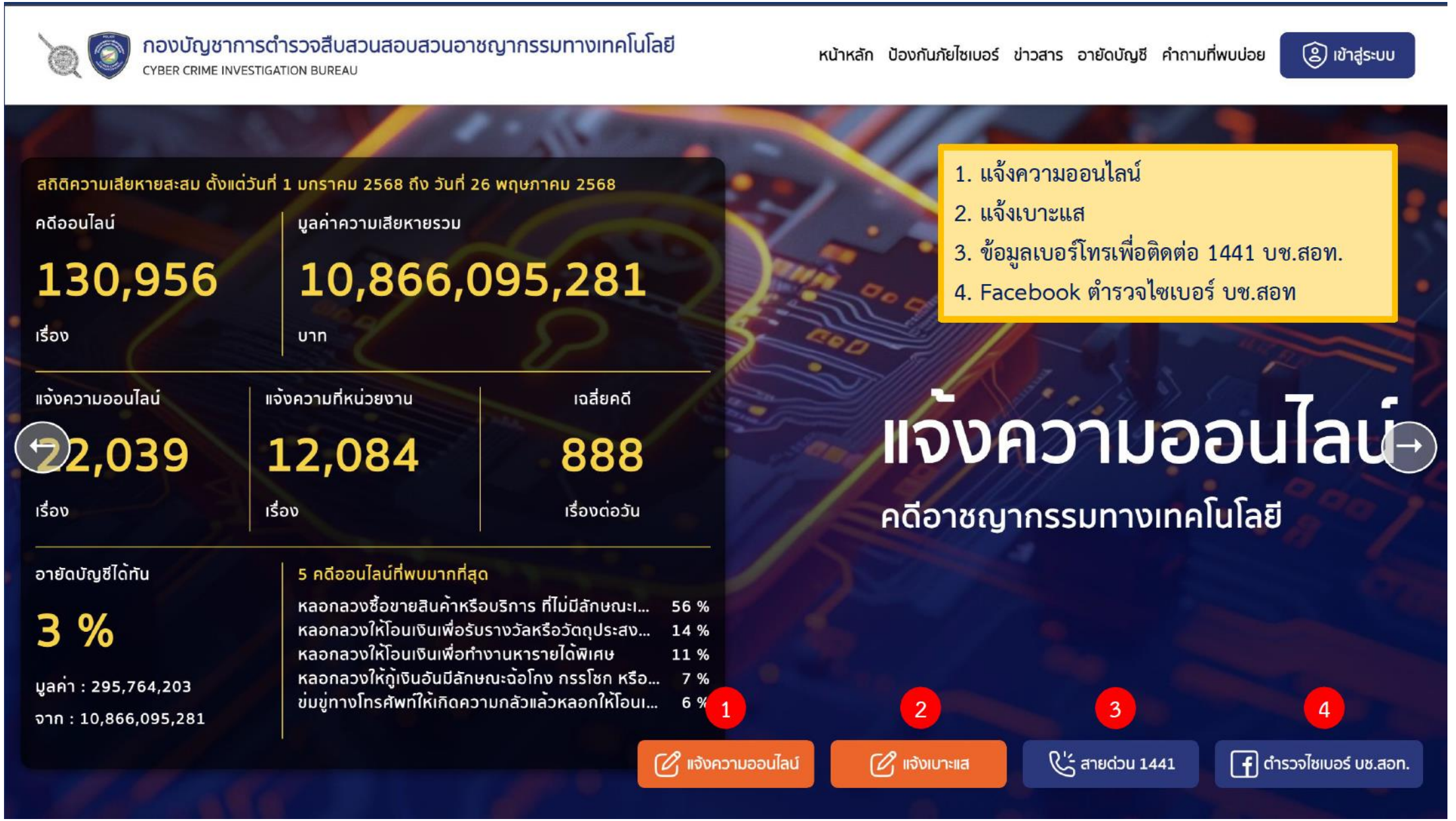
กระบวนการรับมือเมื่อตกเป็นผู้เสียหาย

ขั้นตอนการแจ้งความออนไลน์ การเตรียมหลักฐานสำคัญ

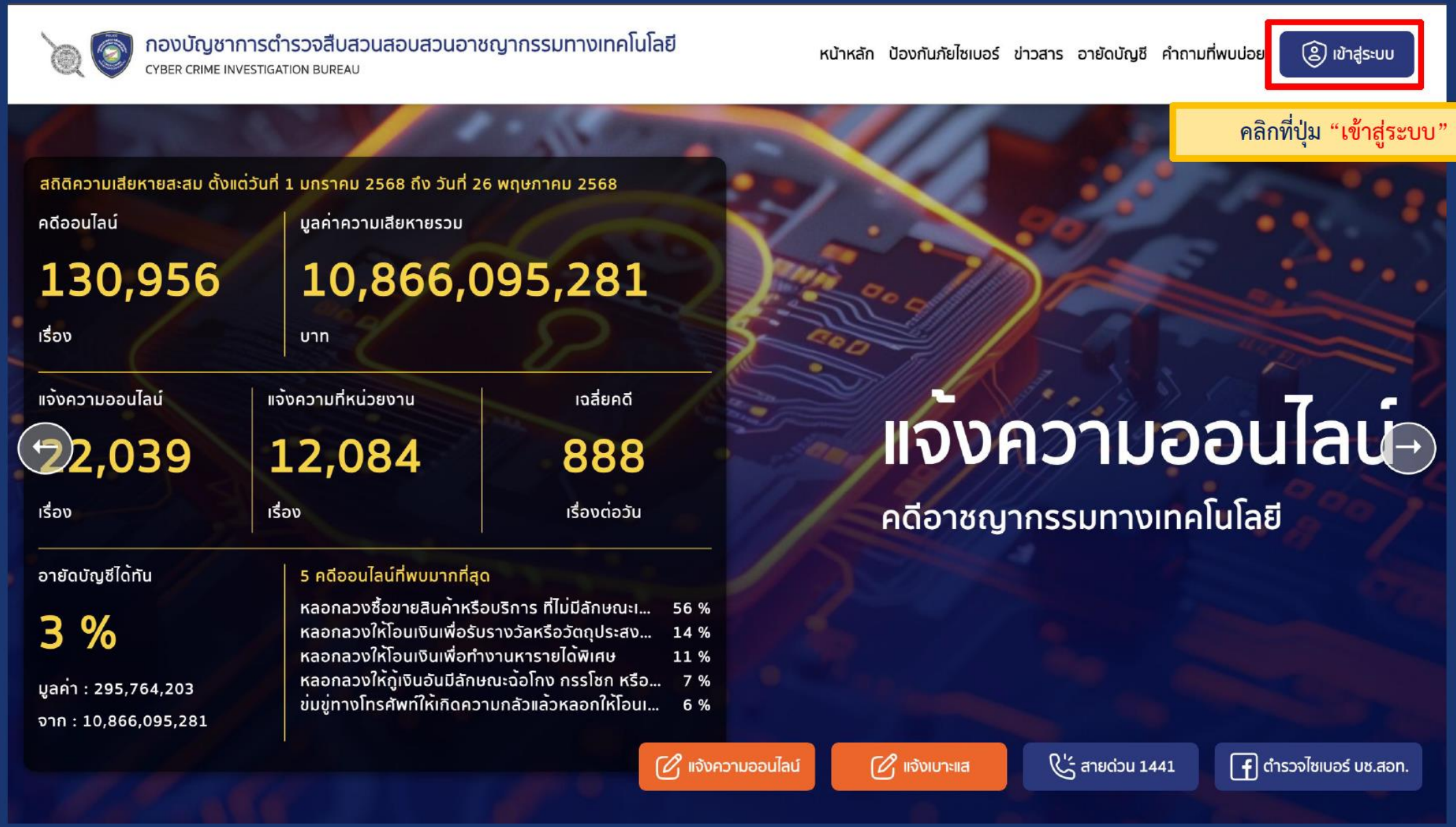
ช่องทางการแจ้งความออนไลน์

1. https://www.thaipoliceonline.go.th/
2. โทร. 1441
3. สถานีตำรวจ

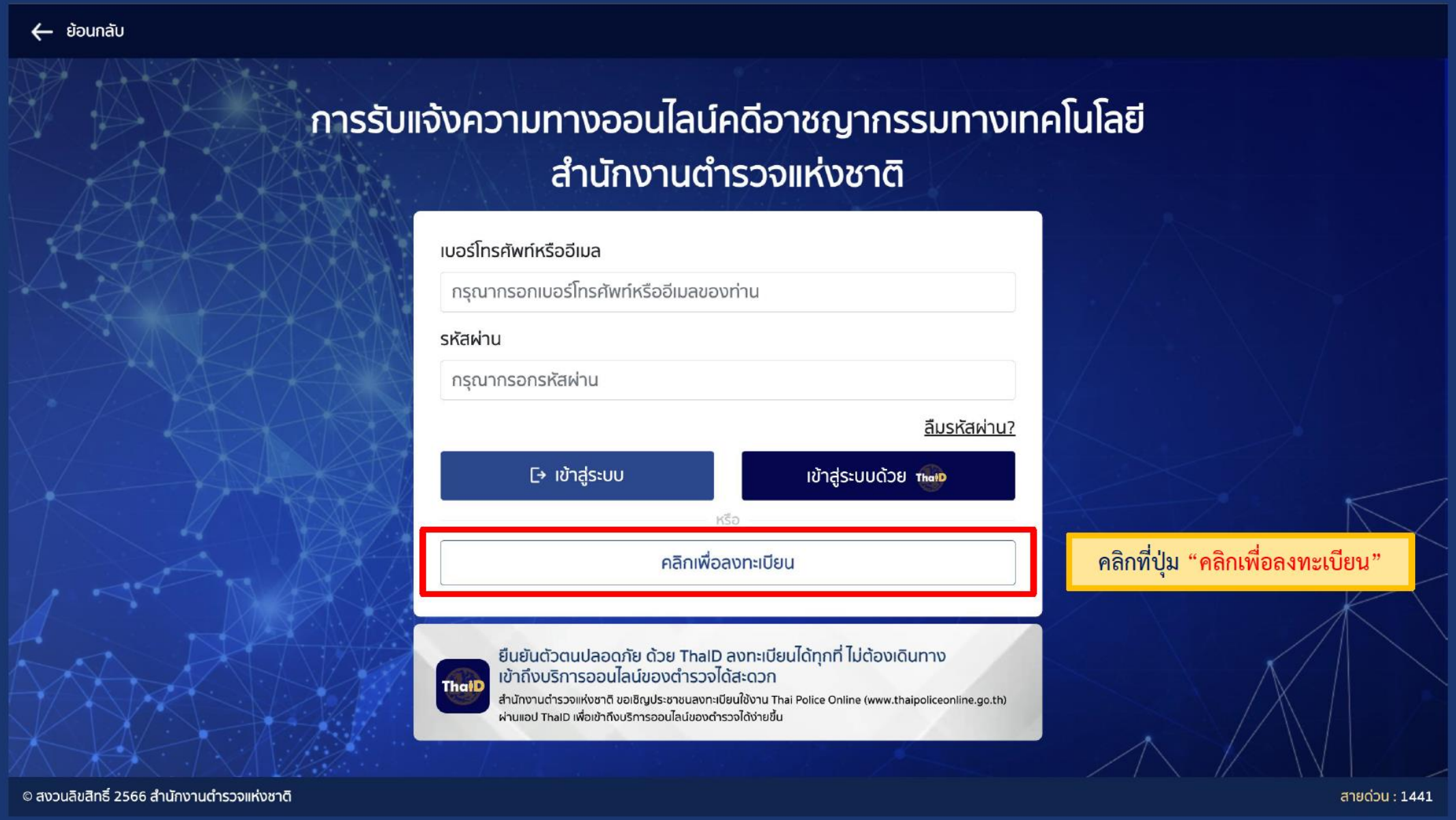
https://www.thaipoliceonline.go.th/



ขั้นตอนการลงทะเบียนเข้าใช้งาน



ขั้นตอนการลงทะเบียนเข้าใช้งาน



คลิกที่ปุ่ม “คลิกเพื่อลงทะเบียน”

ขั้นตอนการลงทะเบียนเข้าใช้งาน

ย้อนกลับ

การรับแจ้งความทางออนไลน์คดีอาชญากรรมทางเทคโนโลยี
สำนักงานตำรวจแห่งชาติ

1 ข้อมูลผู้ใช้ — 2 ยืนยันรหัส OTP

คำนำหน้า:* | ชื่อภาษาไทย:* | นามสกุลภาษาไทย:*

เบอร์โทรศัพท์:* | อีเมล: | วัน/เดือน/ปีเกิด:*

เลขประจำตัวประชาชน: *

Laser Code หลังบัตรประจำตัวประชาชน: *

คำแนะนำในการกรอก Laser Code

สำนักงานตำรวจแห่งชาติ ยกระดับการรักษาความปลอดภัย ข้อมูลของผู้ใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลของท่าน ด้วยการตรวจสอบ Laser Code หลังบัตรประจำตัวประชาชน

เลือกรหัสผู้ใช้งาน:*

เบอร์โทรศัพท์ อีเมล

รหัสผู้ใช้งาน (เบอร์โทรศัพท์ หรือ อีเมล):* | รหัสผ่าน:* | ยืนยันรหัสผ่าน:*

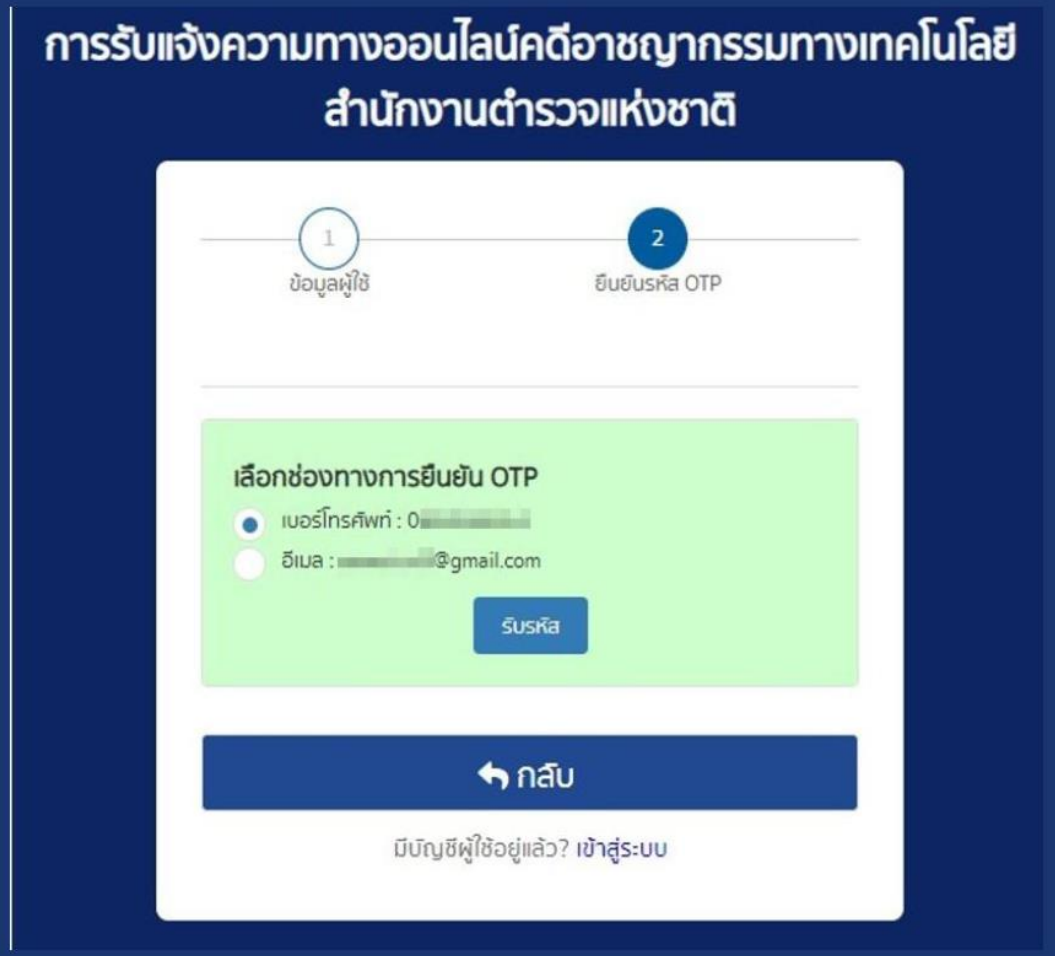
→ ถัดไป

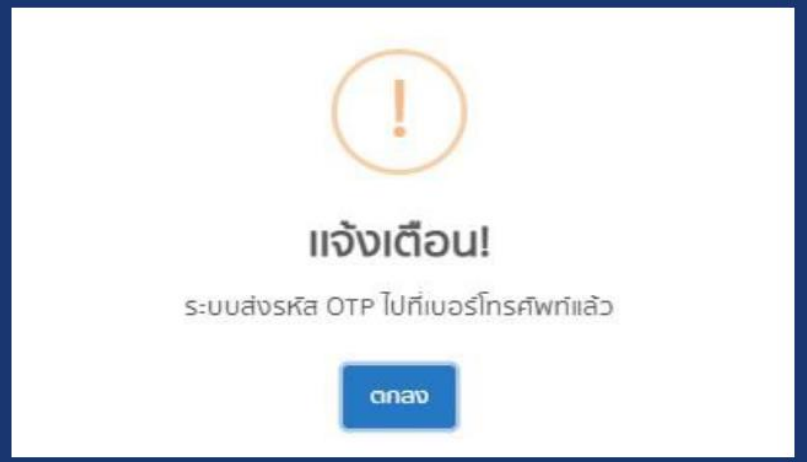
มีบัญชีผู้ใช้อยู่แล้ว? เข้าสู่ระบบ

กรอกข้อมูลให้ครบถ้วน และคลิกที่ปุ่ม “ถัดไป”

สายด่วน : 1441

ขั้นตอนการลงทะเบียนเข้าใช้งาน





เลือกช่องทางการยืนยัน OTP และคลิกที่ปุ่ม “รับรหัส”
ระบบจะทำการส่งรหัส OTP ไปยังช่องทางที่ท่านเลือก
จากนั้นกรอกรหัสที่ได้รับมา

การดาวน์โหลด ThaiD และขั้นตอนการลงทะเบียนด้วยตัวเอง

สามารถดาวน์โหลดแอปพลิเคชัน **ThaID** ได้ที่

Download on the Google Play

Download on the App Store

ขั้นตอนการลงทะเบียนด้วยตนเอง

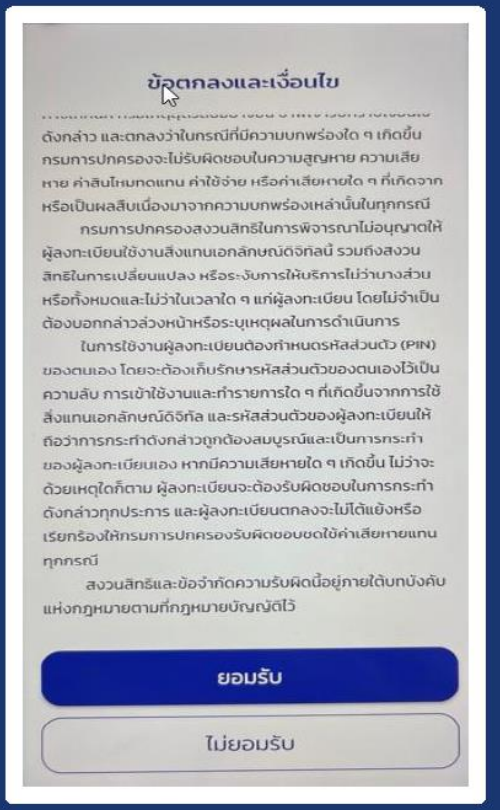
1. เลือกหัวข้อลงทะเบียนด้วยตนเอง
2. ยอมรับข้อตกลงและเงื่อนไขการใช้บริการเพื่อทำการลงทะเบียนสิ่งแทนเอกลักษณ์ดิจิทัล
3. ถ่ายรูปหน้าบัตรประจำตัวประชาชน เมื่อเสร็จแล้วให้ตรวจสอบความชัดเจนและกดปุ่มยืนยันหรือถ่ายใหม่
4. ถ่ายรูปหลังบัตรประจำตัวประชาชน เมื่อเสร็จแล้วให้ตรวจสอบความชัดเจนและกดปุ่มยืนยันหรือถ่ายใหม่
5. ตรวจสอบข้อมูลบัตรประจำตัวประชาชน หากถูกต้องให้กดยืนยัน
6. ถ่ายรูปภาพใบหน้าตนเอง
7. ตั้งค่ารหัสผ่านเหมือนกัน 2 ครั้งโดยต้องไม่เรียงกัน และไม่ซ้ำกันเกิน 4 ตัว เช่น 1234, 1111
8. ระบบแจ้งเตือนขอความยินยอมโดยระบุรหัสผ่านอีกครั้งเพื่อเข้าใช้งานแอปพลิเคชันครั้งแรก
9. เมื่อลงทะเบียนเสร็จสิ้น หน้าจอจะแสดงรูปบัตรประจำตัวประชาชน

*กรณีลืมรหัสผ่าน สามารถรีเซ็ตรหัสผ่านได้ โดยการถ่ายรูปภาพใบหน้าตนเองเพื่อขอสร้างรหัสผ่านให้

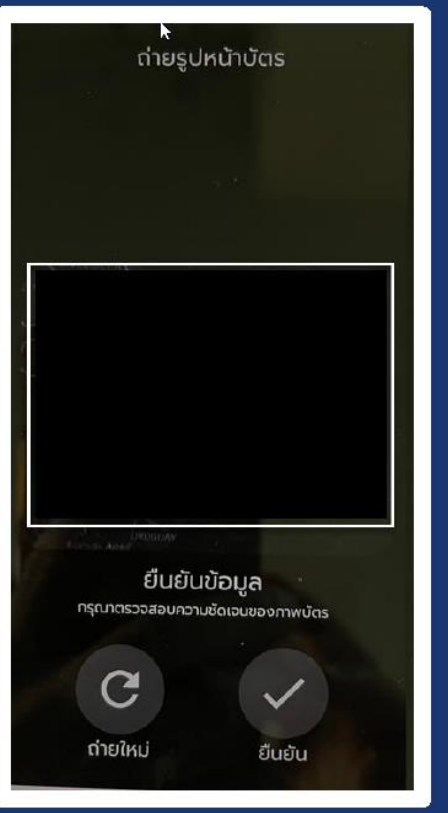
ขั้นตอนการลงทะเบียนเข้าใช้งาน ThaiD

กดเริ่มต้นการใช้งาน

เลือกหัวข้อ ลงทะเบียนด้วยตนเอง



กดยอมรับข้อตกลงและ
เงื่อนไขการใช้บริการ
เพื่อทำการลงทะเบียน



ถ่ายรูปหน้าบัตรประชาชน
ตรวจสอบความชัดเจน
แล้วกดปุ่ม ยืนยัน

ขั้นตอนการลงทะเบียนเข้าใช้งาน ThaiD

ถ่ายรูปหลังบัตรประชาชน
ตรวจสอบความชัดเจน
แล้วกดปุ่ม ยืนยัน

ตรวจสอบข้อมูล
บัตรประชาชน
หากถูกต้องให้ กดยืนยัน

ถ่ายรูปใบหน้าตนเอง
ตรวจสอบความชัดเจน
และ กดยืนยัน

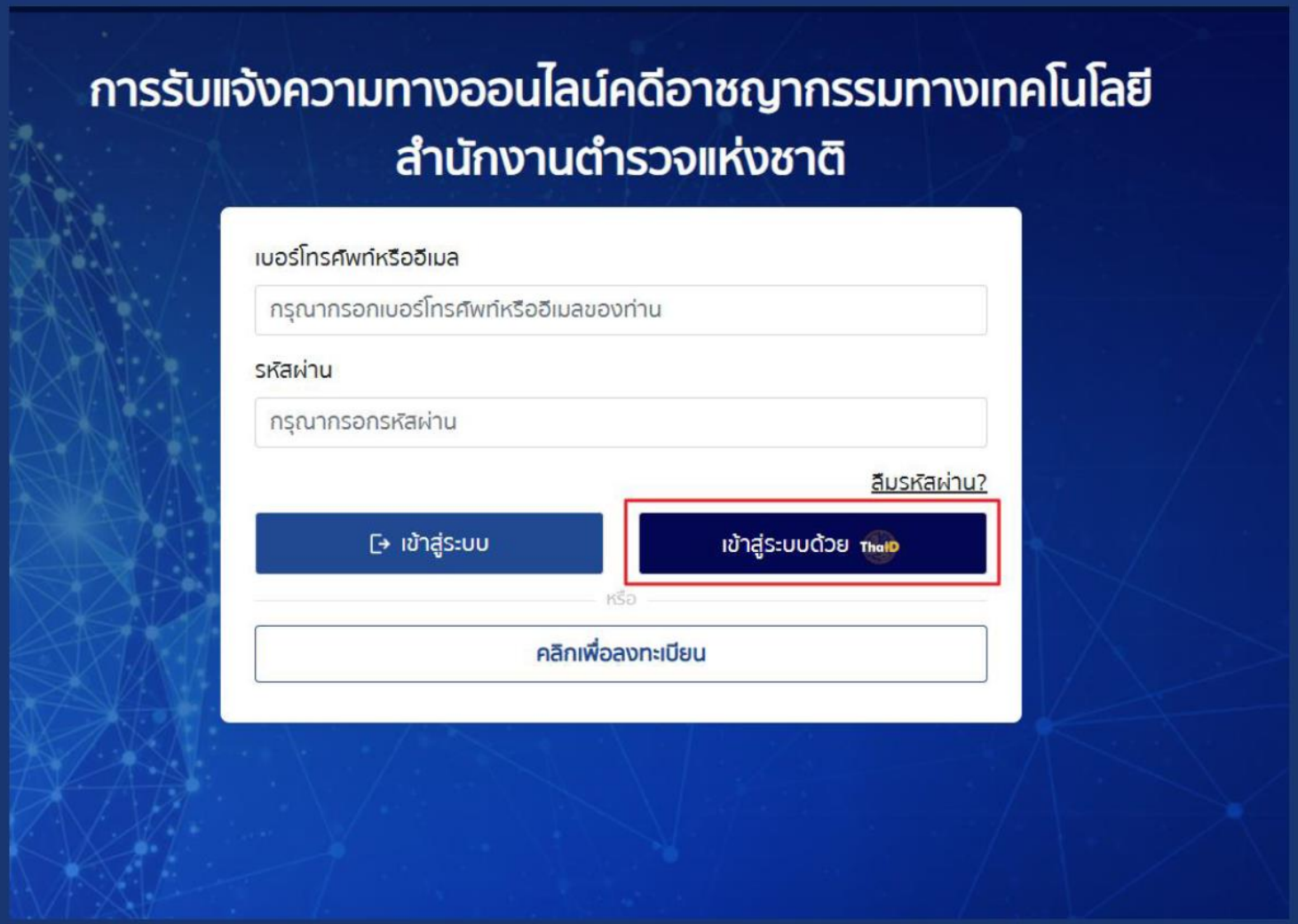
สร้างรหัสผ่าน 8 หลัก
โดยจะต้องไม่เรียงกัน และไม่ซ้ำ
กันเกิน 4 ตัว และ กดยืนยัน

ขั้นตอนการลงทะเบียนเข้าใช้งาน ThaiD

ระบบจะแจ้งเตือน
<u>กดยินยอม</u>

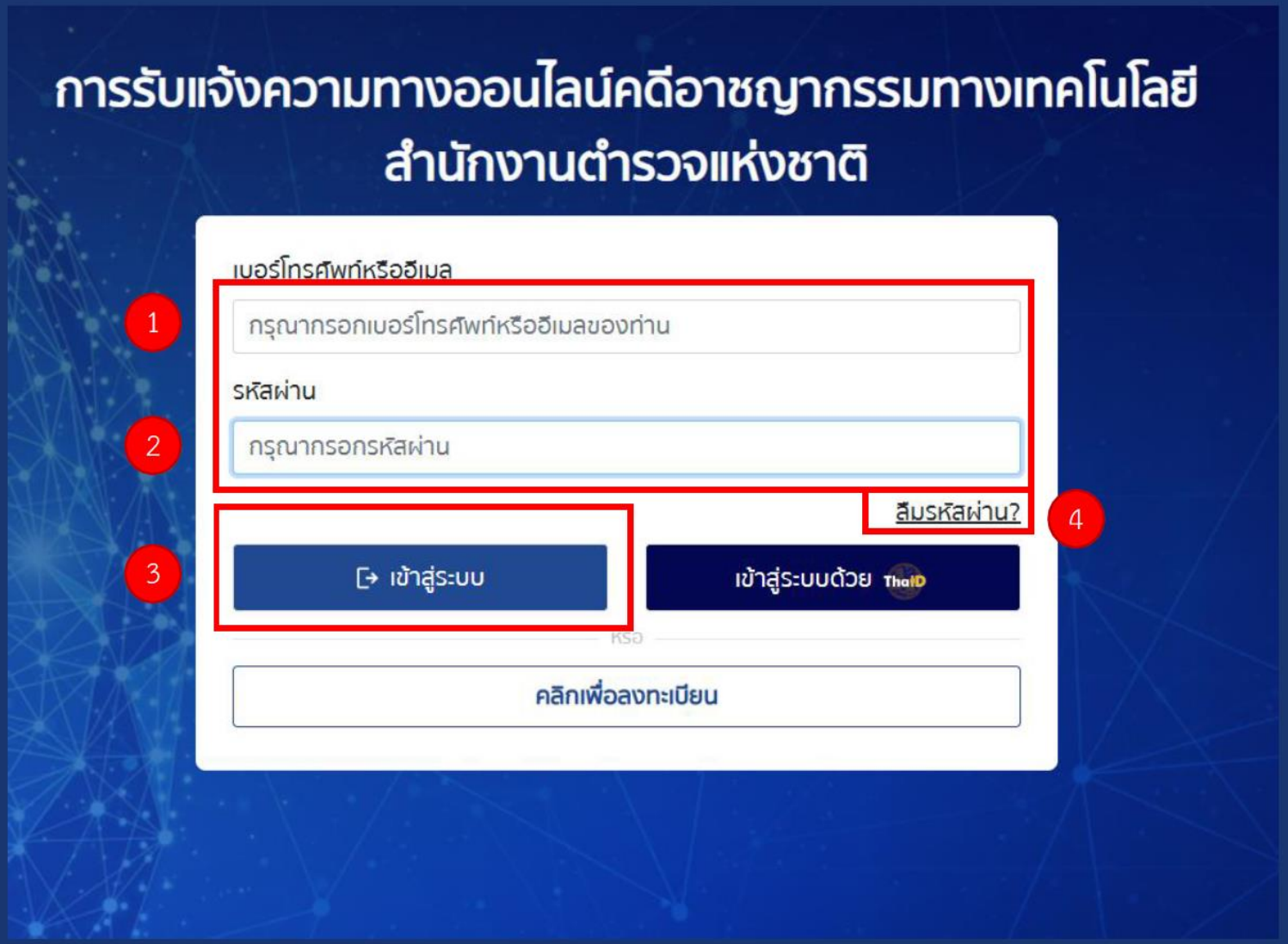
กดคำว่าสแกน
เพื่อเข้าไปสแกน QR Code
ThaiD

ขั้นตอนการเข้าสู่ระบบ Thaipoliceonline ด้วย ThaiD



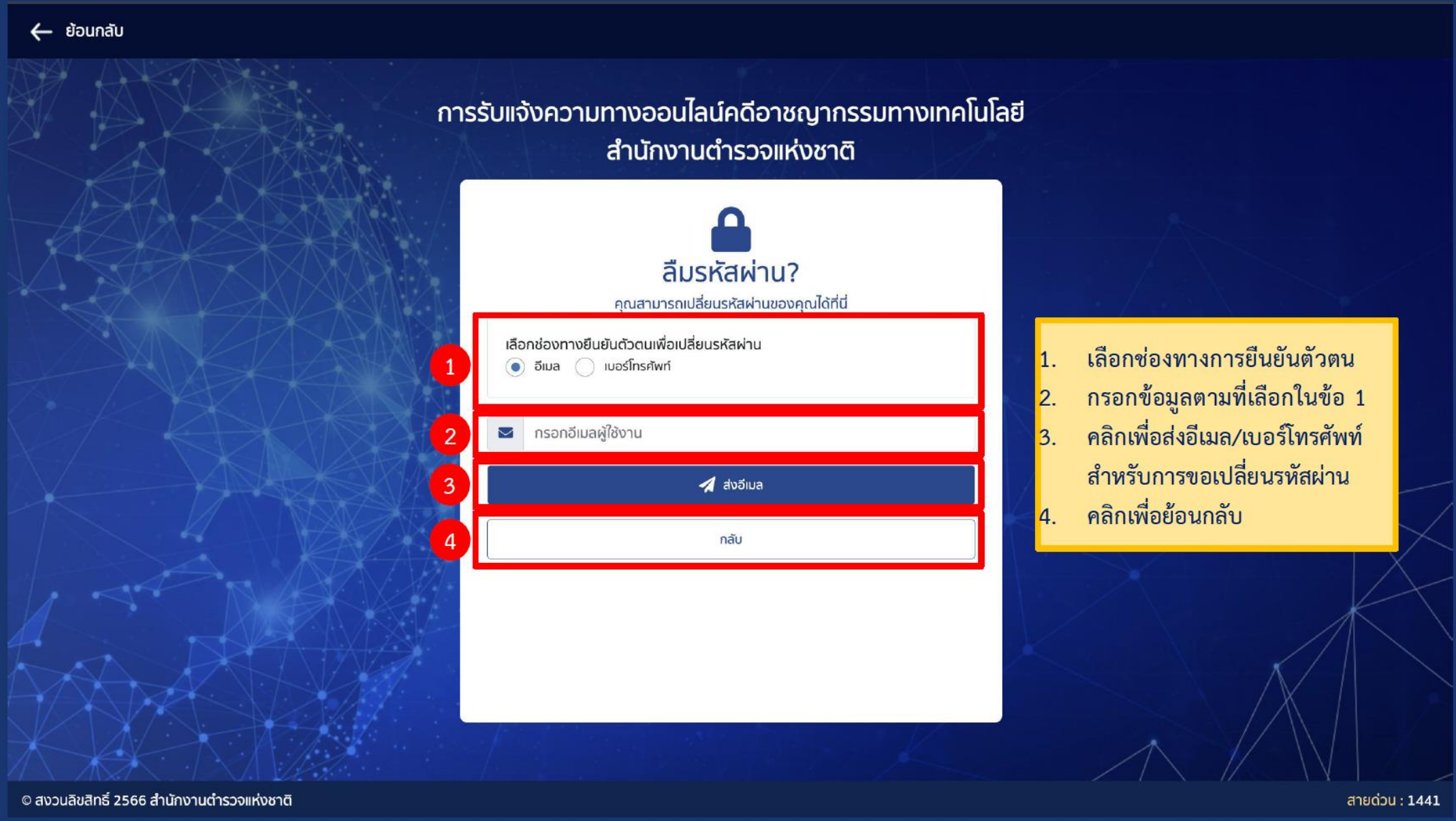
คลิกที่ปุ่ม “เข้าสู่ระบบด้วย ThaiD” จากนั้น สแกน QR Code เพื่อยืนยันตัวตน เข้าระบบ ThaiD

ขั้นตอนการเข้าสู่ระบบ Thaipoliceonline

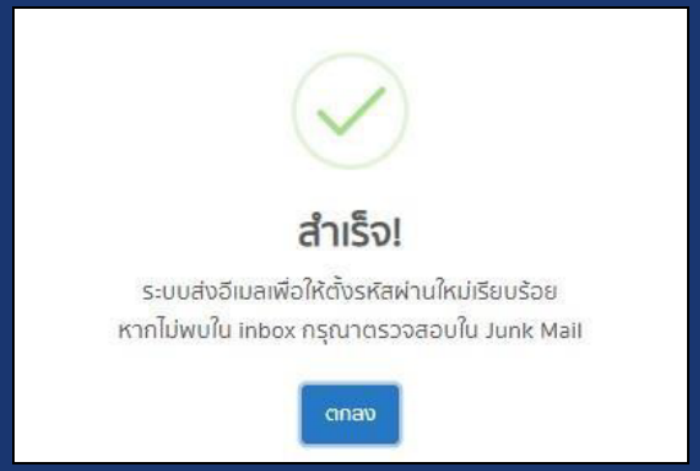


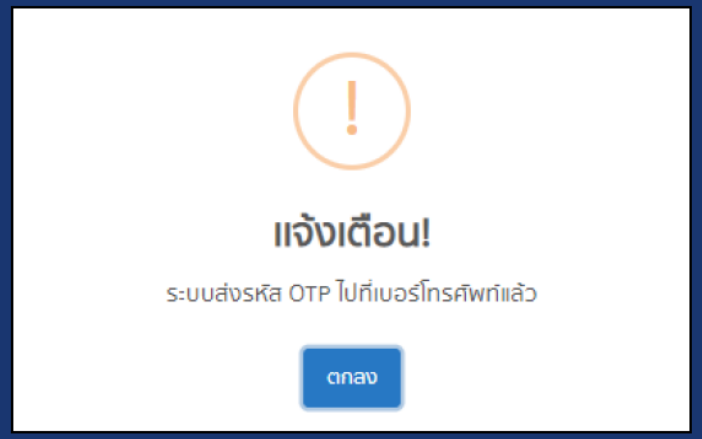
1. กรอกเบอร์โทรศัพท์หรืออีเมลที่ลงทะเบียนไว้
2. กรอกรหัสผ่านที่ตั้งไว้
3. คลิกเพื่อเข้าสู่ระบบ
4. หากลืมรหัส ให้กด “ลืมรหัสผ่าน”

ขั้นตอนกรณีลืมรหัสผ่าน

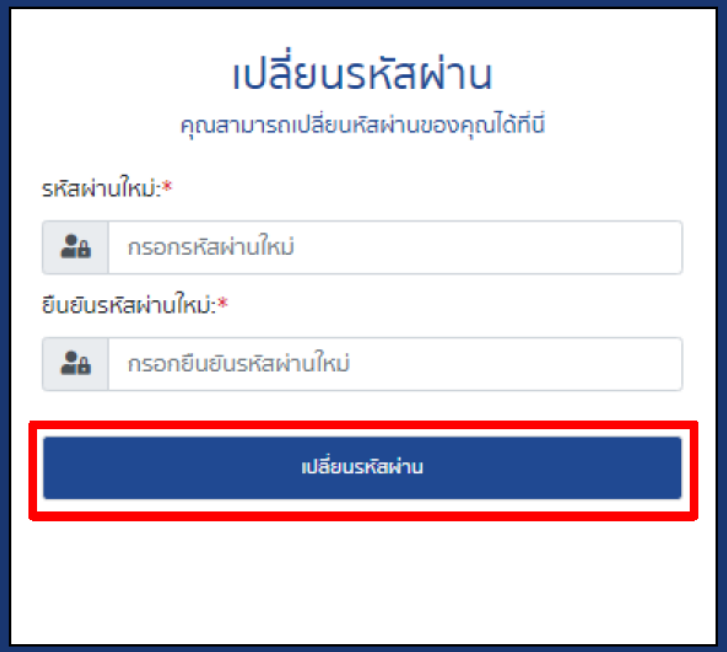


ขั้นตอนกรณีลืมรหัสผ่าน

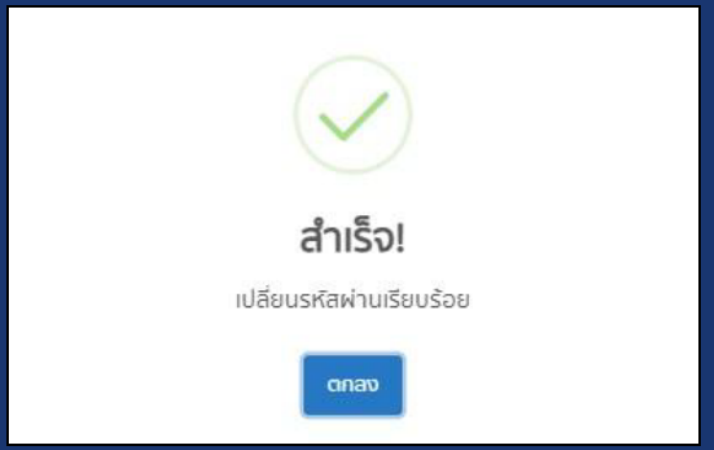




แจ้งเตือนการส่งอีเมลหรือ OTP สำเร็จ

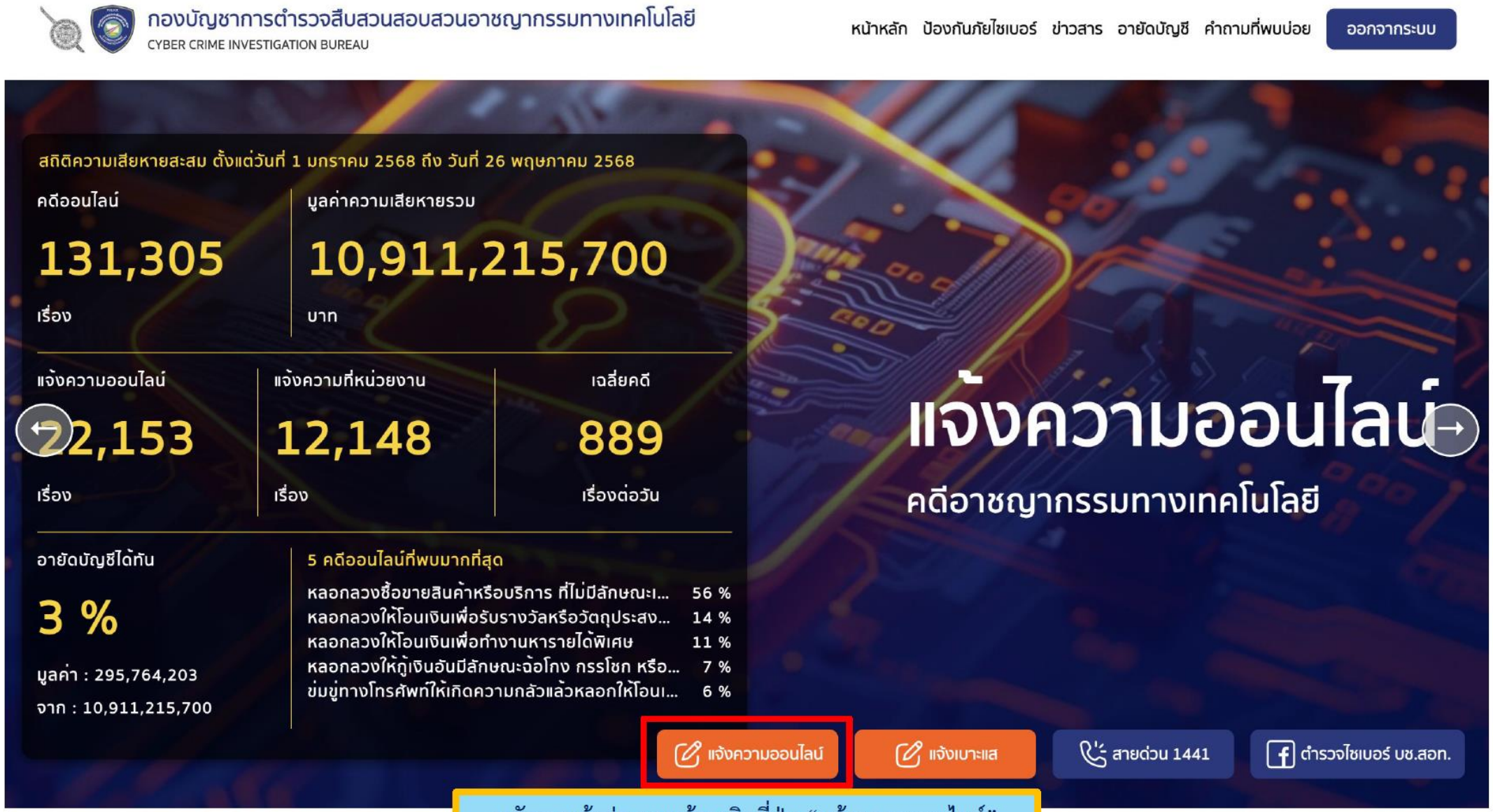


หน้าจอแสดงการเปลี่ยนรหัสผ่าน
คลิกเพื่อยืนยันการเปลี่ยนรหัสผ่าน

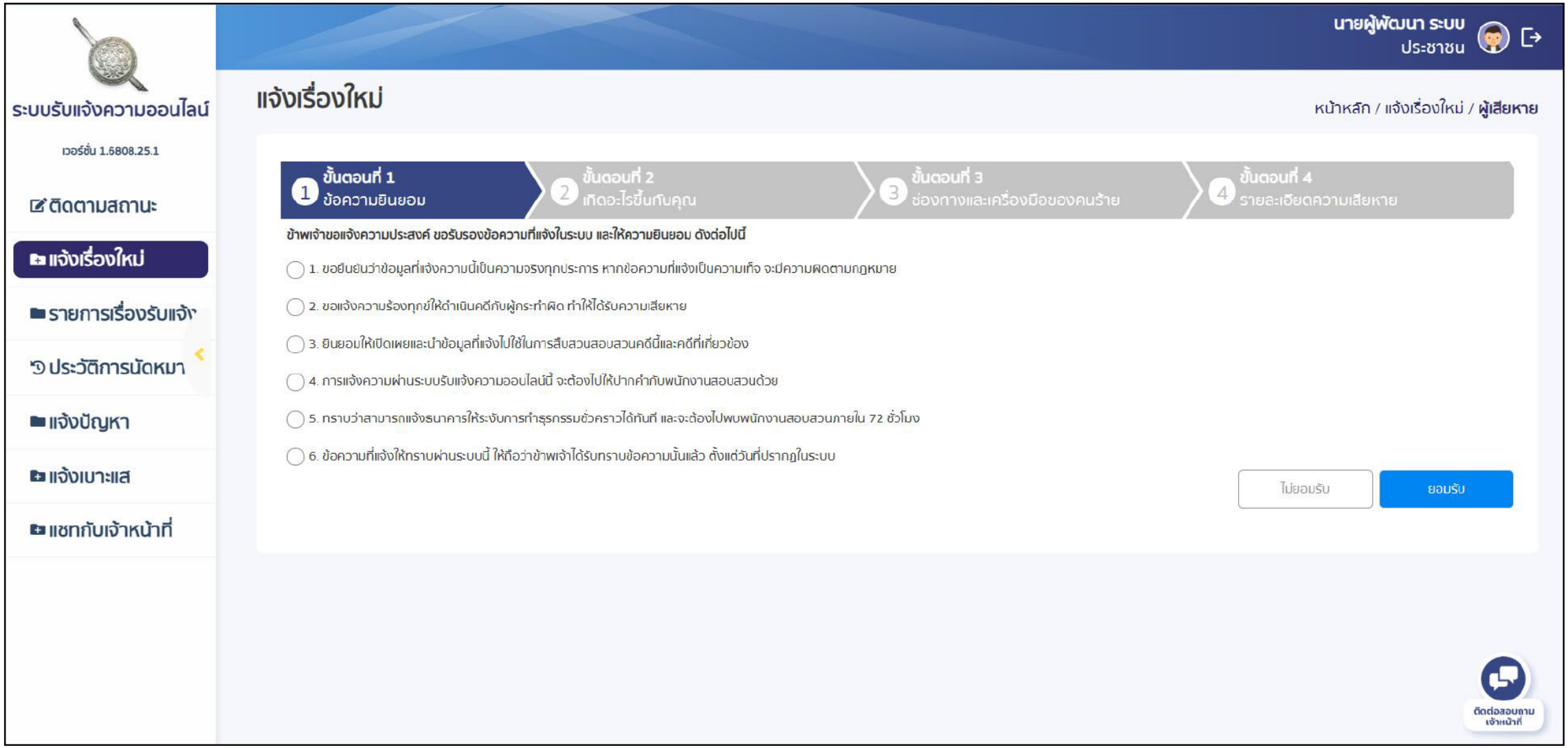


แจ้งเตือนการเปลี่ยนรหัสผ่านสำเร็จ

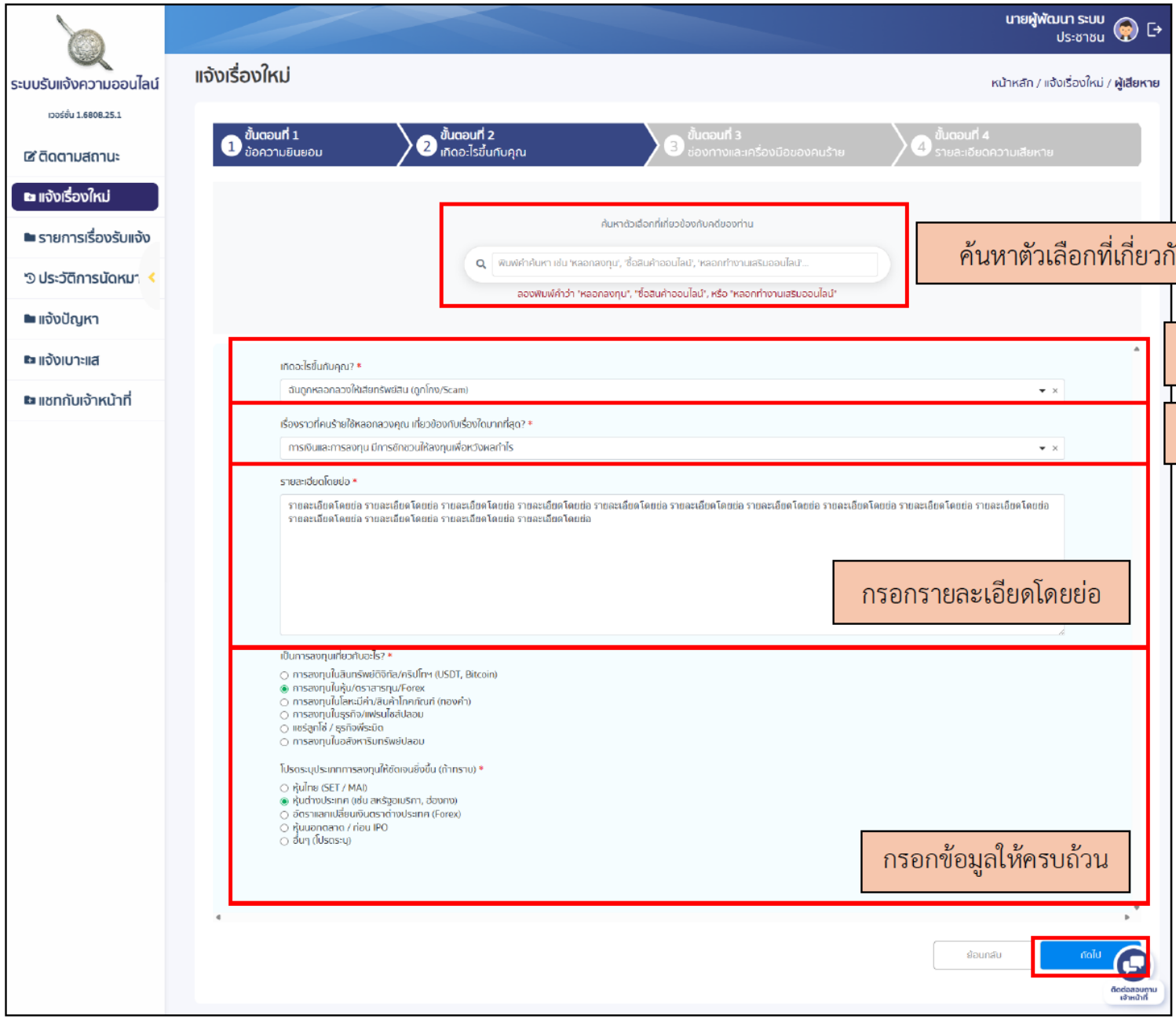
ขั้นตอนการแจ้งความออนไลน์



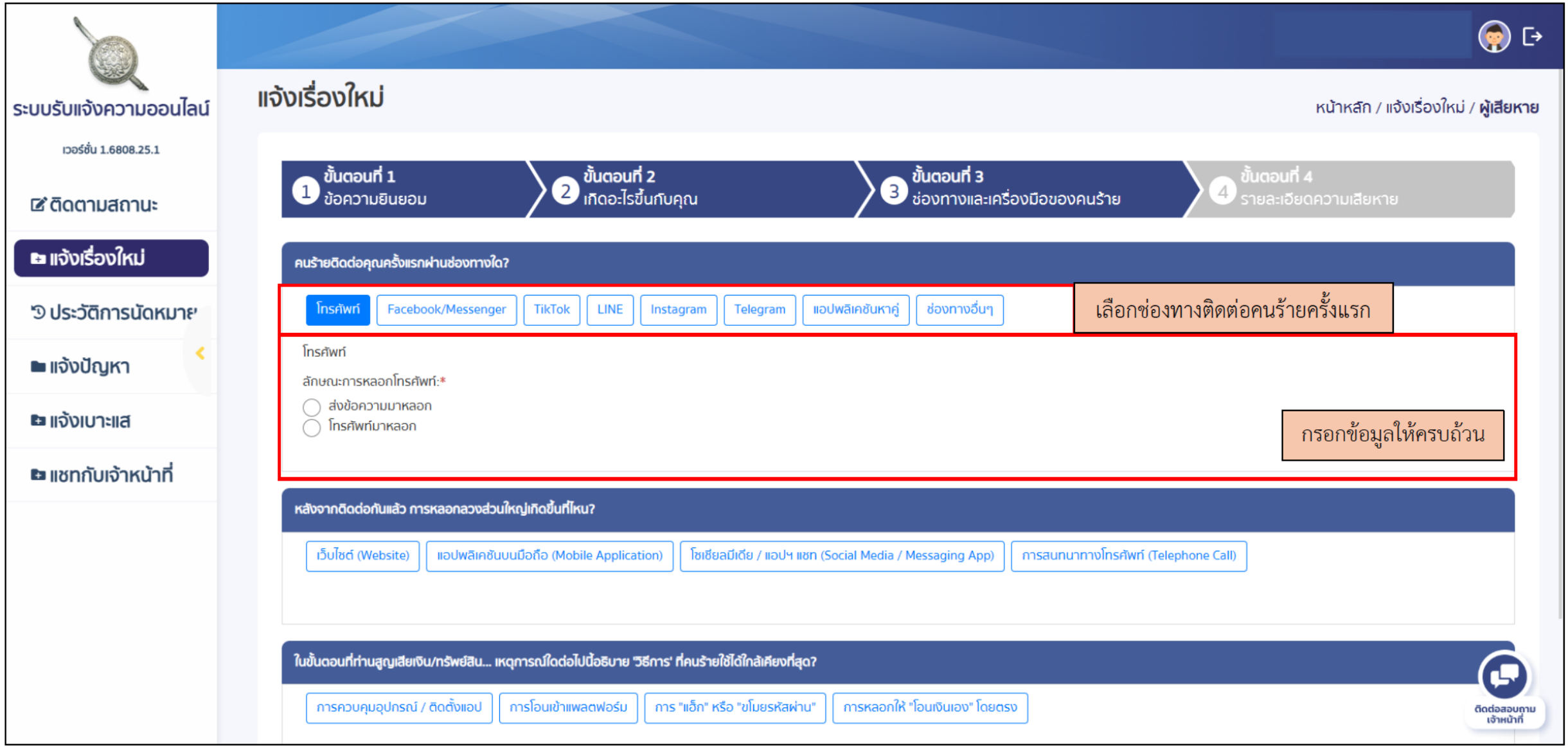
หลังจากเข้าสู่ระบบแล้ว คลิกที่ปุ่ม “แจ้งความออนไลน์”



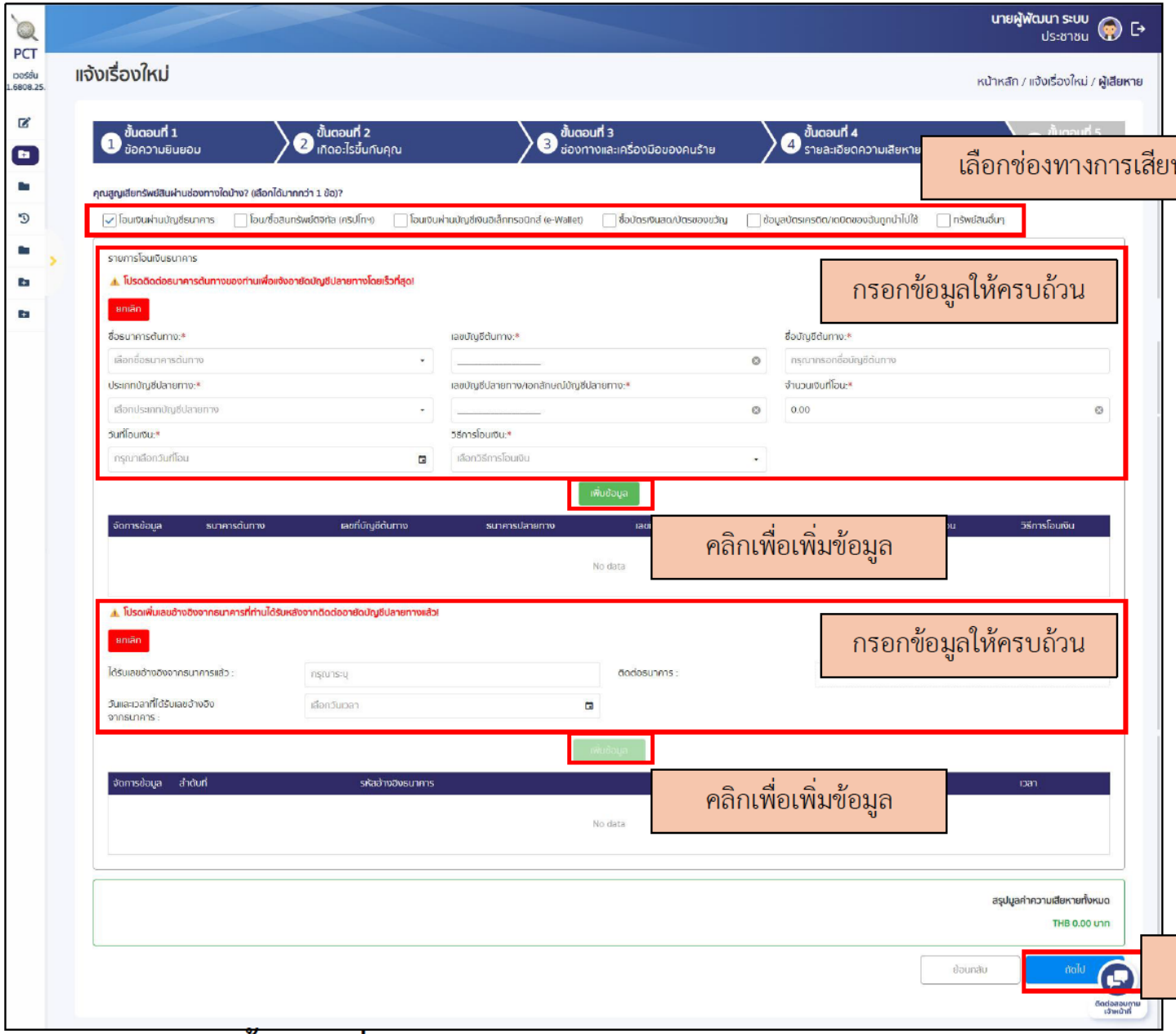
ขั้นตอนที่ 1 การขอรับรองข้อความที่แจ้งในระบบ และให้ความยินยอม



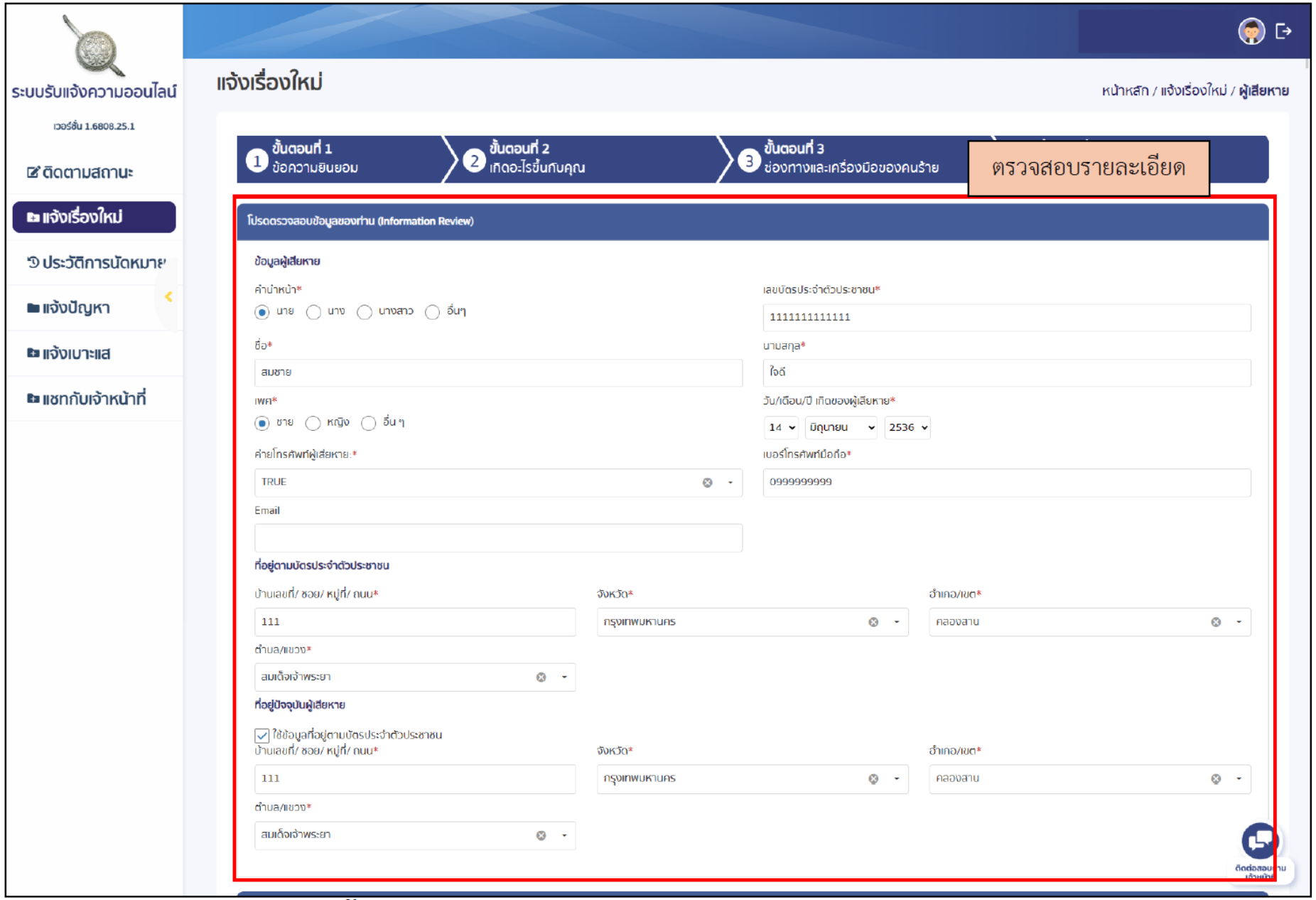
ขั้นตอนที่ 2 กรอกข้อมูลรายละเอียดเหตุการณ์ที่เกิดขึ้น



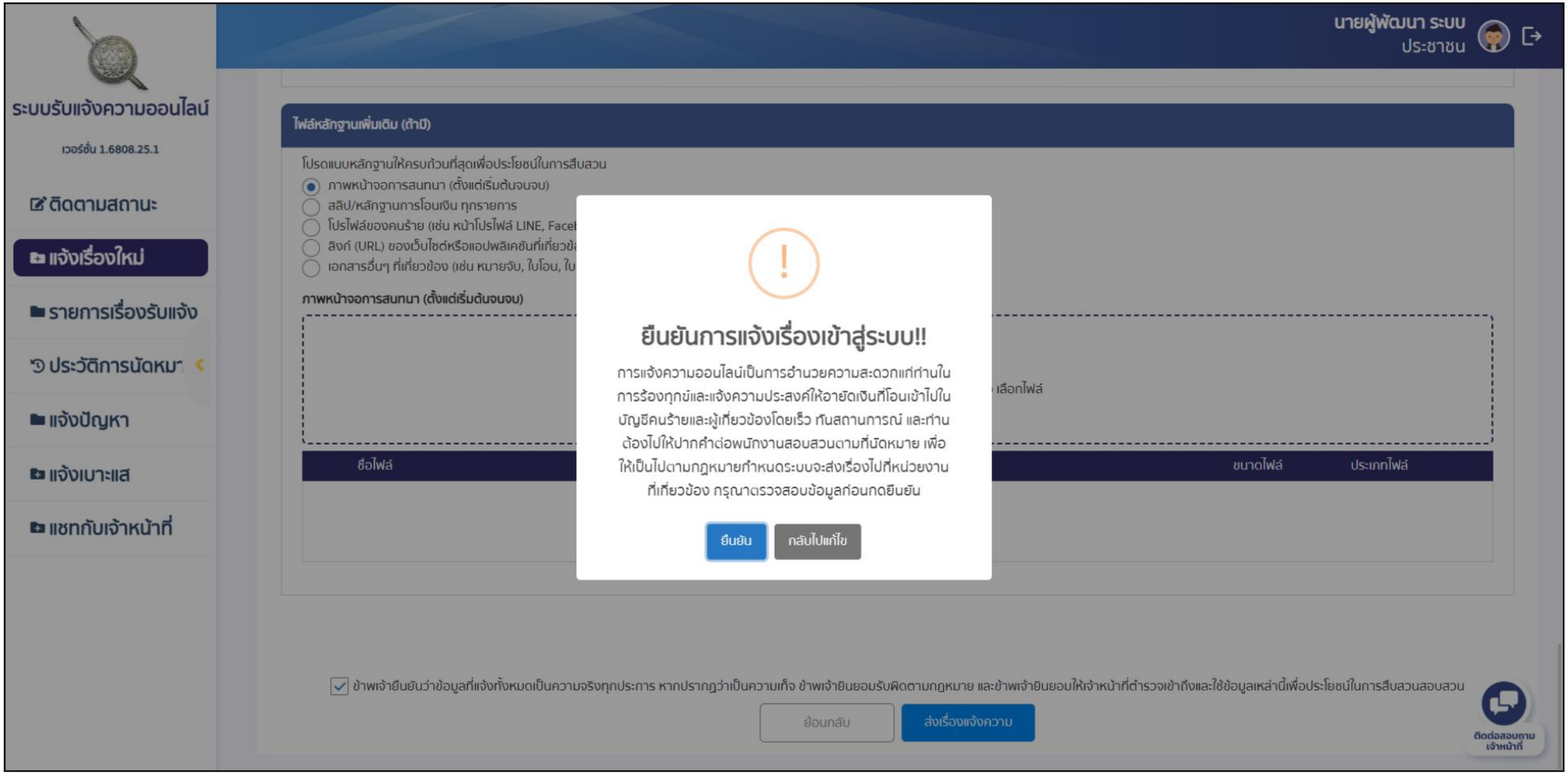
ขั้นตอนที่ 3 กรอกข้อมูลช่องทางติดต่อและเครื่องมือของคนร้าย



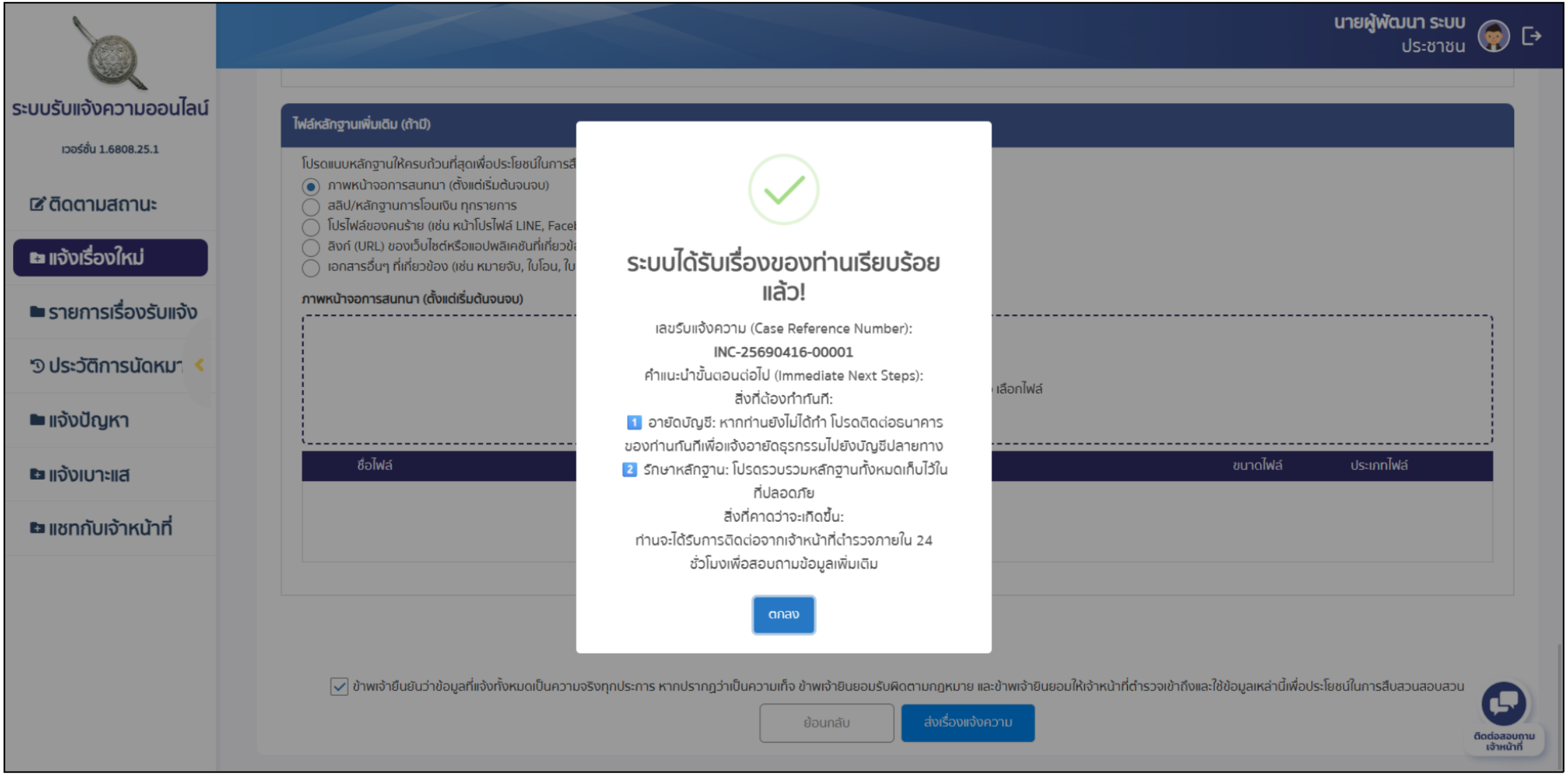
ขั้นตอนที่ 4 กรอกข้อมูลรายละเอียดความเสียหาย



ขั้นตอนที่ 5 ตรวจสอบรายละเอียด (ข้อมูลผู้เสียหาย)



ขั้นตอนที่ 5 ตรวจสอบรายละเอียด พร้อมกดส่ง “ส่งเรื่องแจ้งความ” (ต่อ)



ขั้นตอนที่ 5 ตรวจสอบรายละเอียด พร้อมกดส่ง “ส่งเรื่องแจ้งความ” (ต่อ)

SESSION_END // Q&A STATUS: COMPLETED

Q&A & Conclusion

กลุ่มงานสนับสนุนทางไซเบอร์ บก.ตอท. | พ.ต.อ. เกรียงไกร พุทไธสง