ในโลกดิจิทัล

สิ่งที่อันตรายที่สุด

อาจไม่ใช่ Hacker

แต่อาจเป็น

“การกดโดยไม่คิด” ของเราเอง

AI Scams

ภัยใหม่ที่
“แนบเนียน”ยิ่งกว่าเดิม

วิธีป้องกันตัวเอง

✅ อย่าดูแค่สลิป

สลิปต้องระบุว่า "ทำรายการสำเร็จ" เท่านั้น

✅ เช็กยอดเงินในแอปฯ ธนาคาร

ต้องมี “แจ้งเตือนเงินเข้าจริง” ก่อนยื่นเงินสด/สินค้าให้

✅ สแกน QR Code บนสลิป

ต้องขึ้น “ชื่อผู้โอน-ชื่อผู้รับ-ยอดเงิน-เวลาที่โอนจริง”

✅ ระมัดระวังเป็นพิเศษ

หากมีคนขอ “แลกเงินสดจำนวนมากผ่านการโอน”

DEEP FAKE

หน้าคุ้น
เสียงคุ้น

แต่...

ไม่ใช่ “คนจริง”

มิจฉาชีพใช้ AI สร้างวิดีโอ
อ้างเป็นคนมีชื่อเสียง
ชวนลงทุน อ้างกำไรสูง

หมายเหตุ: ภาพจำลองประกอบเนื้อหา

FAKE VOICE

คุณไม่ได้โดนหลอก
เพราะ AI

คุณโดนหลอก
เพราะ **“รีบเชื่อ”**

หมายเหตุ: ภาพจำลองประกอบเนื้อหา

!!!! เตือนภัยมิจฉาชีพ
ใช้ AI ปลอมเสียงมา

คุณพ่อโหวพริบดีมาก

ข่าวใหญ่

รายการนี้ดีมากเลยค่ะ เน้นๆทุกประเด็นข่าว

@Thaich8

LINE

ช่อง 8 27 LIVE
11:43:24

ที่มา : สำนักข่าวช่อง 8

AI Scams

พัฒนาต่อเนื่องทุกวินาที.. แล้วคุณล่ะ?

Phishing

มากกว่า...

“เว็บไซต์ปลอม”


ระวัง! เว็บบอลโลกปลอม
มิจฉาชีพอาจปลอมเว็บขายบัตร / แพ็กเกจท่องเที่ยว เพื่อหลอกเอาข้อมูลและเงิน
tickets-worldcup2026.com
WORLD CUP TICKETS
MATCHES
PACKAGES
TRAVEL
FAQ
FAKE
FINAL MATCH
VIP TICKET
฿ 29,990
BUY NOW
VIP TICKET
Card Number
**** **** **** 1234
CVV
***
Expiry Date
MM / YY

1 รูปแบบที่พบบ่อย

1 เว็บปลอมเลียนแบบเว็บขายบัตรหรือเว็บทางการ

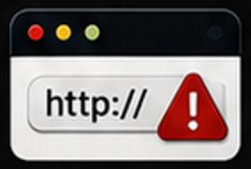
2 โฆษณาขายบัตรราคาถูกผิดปกติหรือโปรด่วนจำกัดเวลา

3 แพ็กเกจตั๋ว + โรงแรม + ทัวร์ดูคุ้มเกินจริง

4 ส่งลิงก์ผ่านโซเชียล แชต หรือ SMS ให้กดเข้าไปกรอกข้อมูล

5 ปลอมเป็นหน้าชำระเงินหรือหน้าล็อกอินเพื่อขโมยข้อมูลส่วนตัว

2 จุดสังเกตเว็บหลอก



1 URL แปลก สะกดผิด หรือโดเมนไม่น่าเชื่อถือ

2 ขอข้อมูลมากเกินจำเป็น เช่น รหัสผ่าน, OTP, CVV

3 เร่งให้จ้ายเงินทันที หรือกดดันว่าของมีจำนวนจำกัด

4 ดีไซน์เว็บไม่เรียบร้อย ภาพ/ข้อความผิดปกติหรือแปลกตา

5 ไม่มีข้อมูลติดต่อชัดเจน หรือไม่ใช่เงื่อนไขการซื้อขาย

6 ลิงก์หรือปุ่มกดพาไปหน้าผิดปกติ / รีวิวดูไม่น่าเชื่อถือ

จำง่าย: ก่อนจ่าย ต้องเช็ก URL ก่อนทุกครั้ง

อย่าให้รหัส OTP, CVV หรือรหัสผ่านกับเว็บไซต์ที่ไม่น่าเชื่อถือ

https://openew[.]app

OpenAI Research Products Business Developers

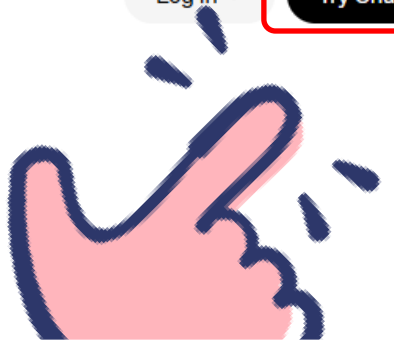
Log in Try ChatGPT ↗

จะโหลดอะไร...

โหลดจาก “เว็บจริง” เท่านั้น

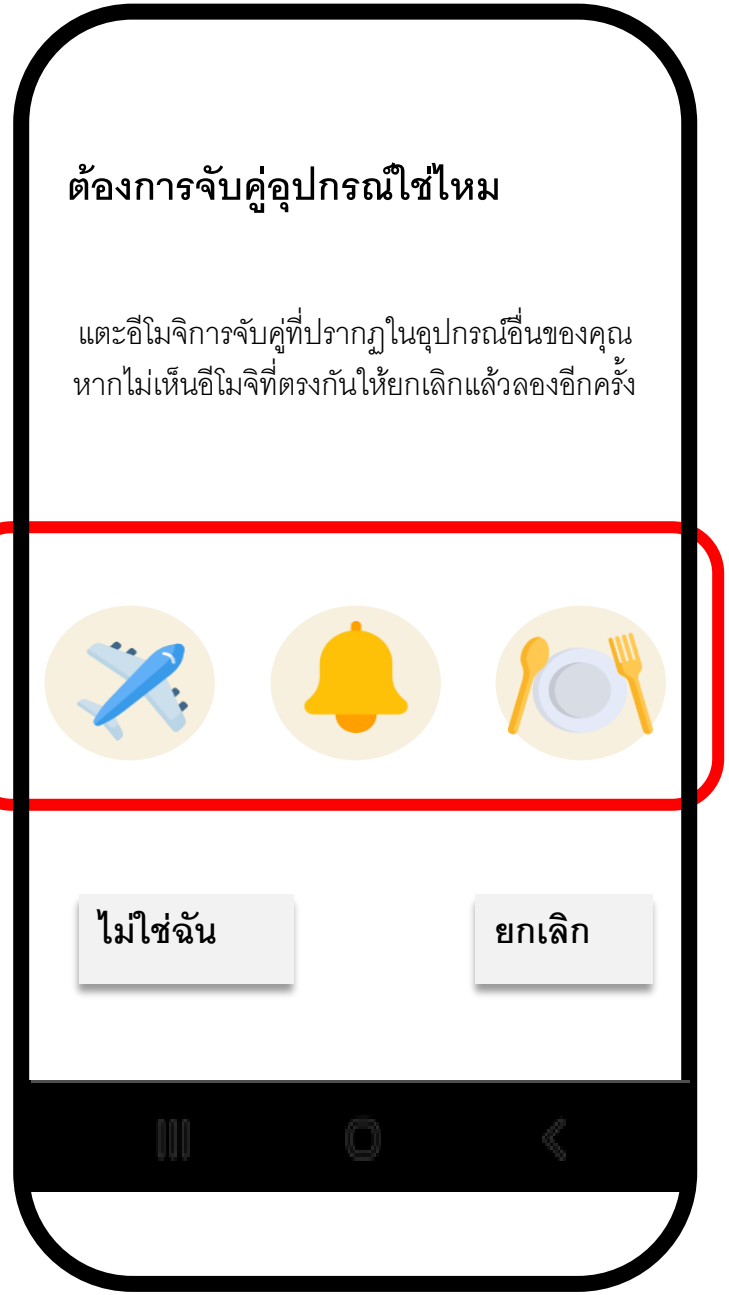
openai.com/chatgpt/desktop

openai.com/chatgpt/download



หมายเหตุ: ภาพจำลองประกอบเนื้อหา

Popup จับคู่อุปกรณ์



ไม่แน่ใจ..

อย่ากด“รับ”

หมายเหตุ: ภาพจำลองประกอบเนื้อหา

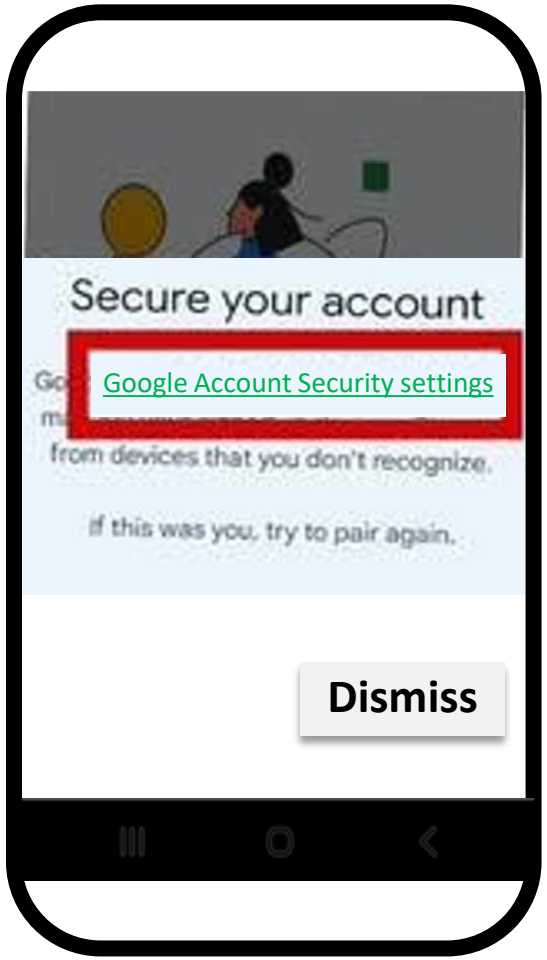
ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ห้ามกดบนภาพเด็ดขาด

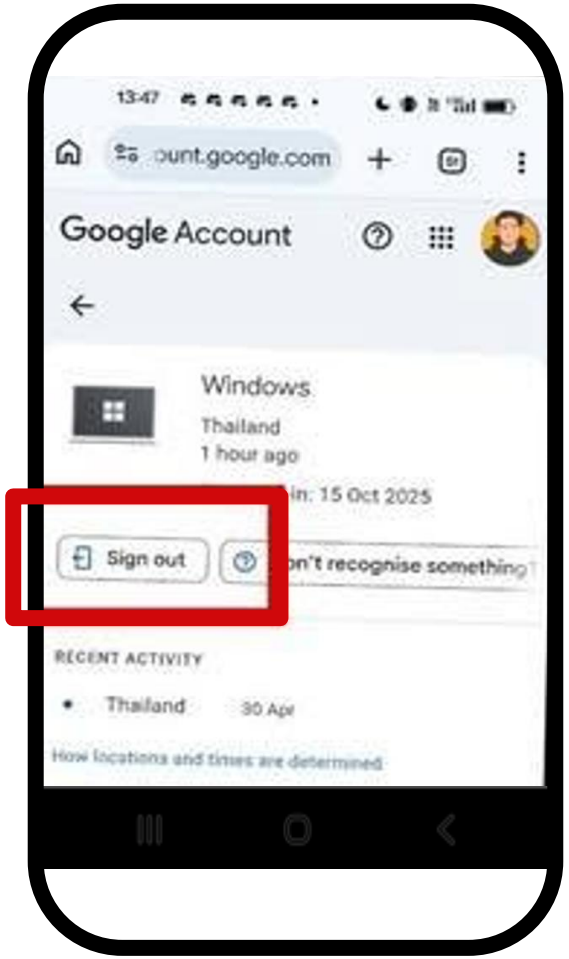
หากพบการแจ้งเตือนลักษณะดังกล่าว ให้ดำเนินการดังนี้

1 กดปุ่ม “ไม่ใช่ฉัน”

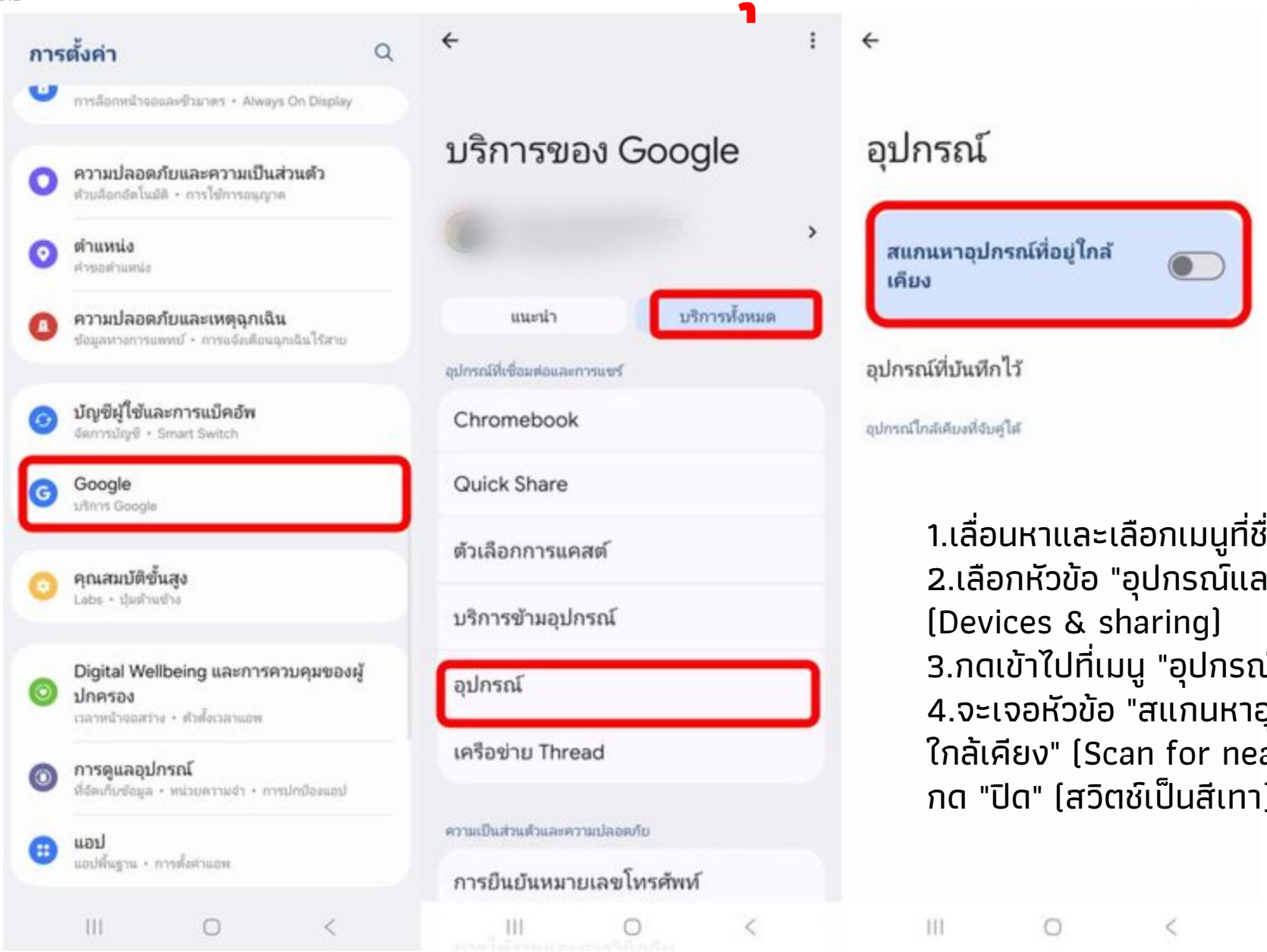
2 กดลิงก์ “Google Account Security settings”



3 ออกจากระบบ (Sign out) บนอุปกรณ์ที่น่าสงสัย

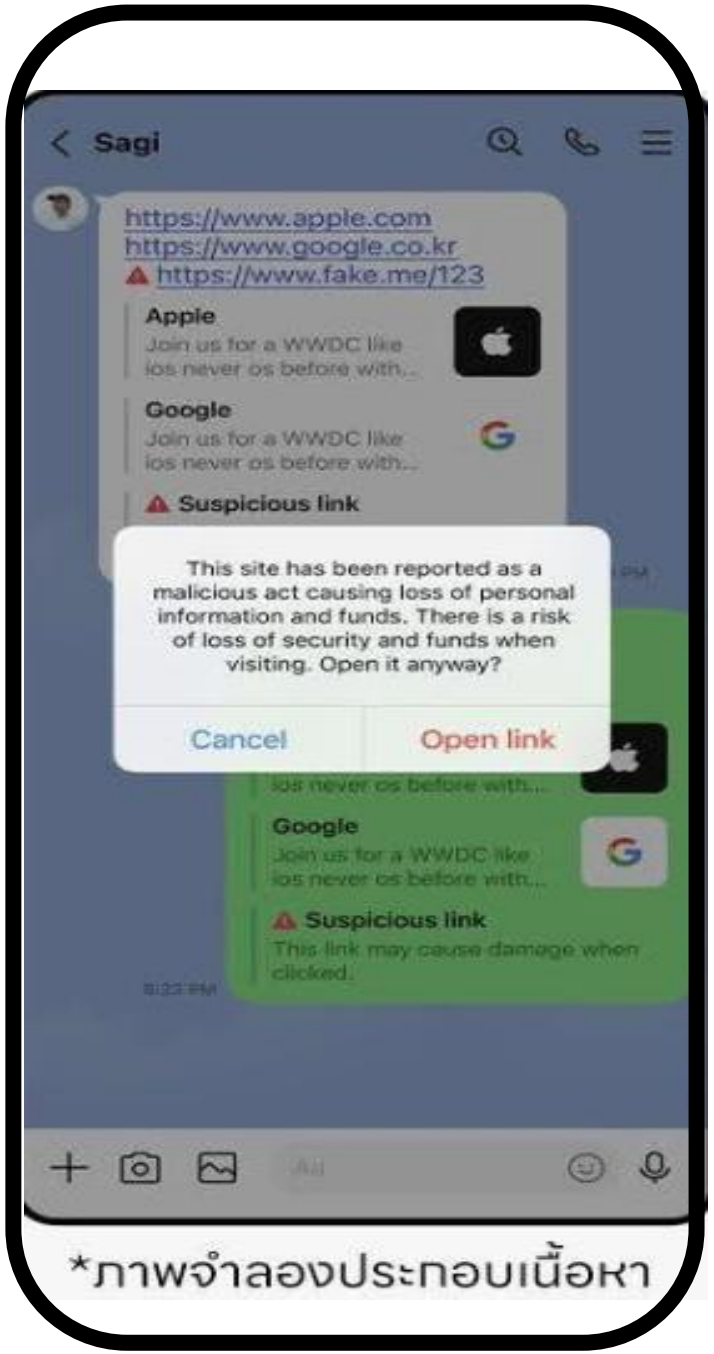


วิธีปิดการค้นหาอุปกรณ์ใกล้เคียง



1.เลื่อนหาและเลือกเมนูที่ชื่อว่า "Google"
2.เลือกหัวข้อ "อุปกรณ์และการแชร์" [Devices & sharing]
3.กดเข้าไปที่เมนู "อุปกรณ์" [Devices]
4.จะเจอหัวข้อ "สแกนหาอุปกรณ์ที่อยู่ใกล้เคียง" [Scan for nearby devices] ให้กด "ปิด" [สวิตช์เป็นสีเทา] ได้เลย

Link ทาง LINE



ไม่ชัวร์...

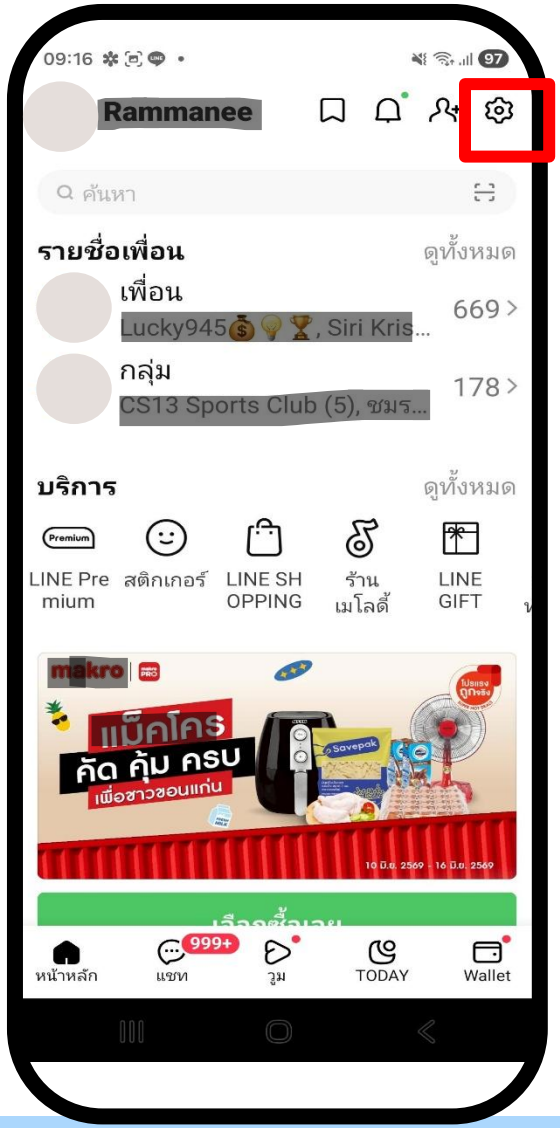
อย่า“กด link”

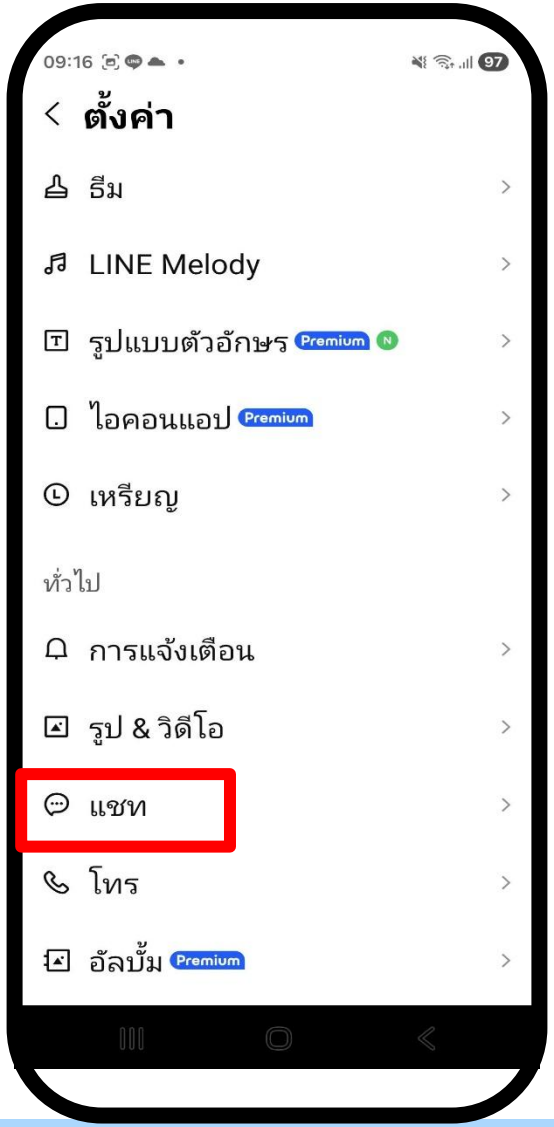
หมายเหตุ: ภาพจำลองประกอบเนื้อหา

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

Phishing Site Detection บน LINE

ระบบเตือนภัยลิงก์ปลอม ป้องกันผู้ใช้จากเว็บไซต์หลอกลวง





ช่องทางแจ้งเบาะแส / ร้องเรียน

เลือกแจ้งให้ตรงประเภท เพื่อให้ช่วยเหลือและดำเนินการได้เร็วขึ้น

1) อาชญากรรมออนไลน์ / แจ้งความ

1441

บช.สอท. ตำรวจไซเบอร์

2) สายโทร / ข้อความหลอกลวง

1200

กสทช.

3) แชร์ลูกโซ่ / หลอกลงทุน

1359 • 1202

1359 ศูนย์รับแจ้งการเงินนอกระบบ กระทรวงการคลัง

1202 กรมสอบสวนคดีพิเศษ (DSI)

สอบถาม / ขอคำปรึกษา: **1213** ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธปท.

คาถาป้องกันโจร

คิด

ก่อนที่คุณจะ..

คลิก
เชื่อ
โอน