



คิดก่อน Click

By: Phatararat Homkrajang
Digital Forensic Section
Division of Forensic Investigation

กรรมที่คืน

- ✗ ไม่โทรหา
- ✗ ไม่ขอแอคไลน์
- ✗ ไม่มีหน้าที่เก็บภาษีที่ดินและสิ่งปลูกสร้าง

ระวัง! มีจาชัพ หลอกดูดเงิน

เจอ แจ้ง จบ

Call center นรท.คืน 0 2141 5555

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 1441

กรรมที่คืน Fanpage
 กรรมที่คืน
 กรรมที่คืน Channel
 @DL-PR
 @SmartLands

เตือนภัย

เว็บแจ้งความออนไลน์ปลอม

DSI ไม่มี Line Official

แจ้งเบาะแส DSI สายด่วน 1202
หรือ www.dsi.go.th เท่านั้น

ปลอม

ตำรวจไซเบอร์ไม่มี Line Official

สามารถแจ้งความออนไลน์ได้ที่
www.thaipoliceonline.com

#ตำรวจไซเบอร์เตือนภัย

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี
CYBER CRIME INVESTIGATION BUREAU

ตำรวจไซเบอร์

เตือนภัยมุกใหม่มีจาชัพ

ส่ง "รทรปลอม" หลอกให้กดลิงก์

SMS

แอบอ้าง M-FLOW ของกรมทางหลวง

M-FLOW

ส่ง SMS แจ้งให้รีบ
ชำระยอดค้างด่วน
พร้อมแนบลิงก์ปลอม

ประชาชนสามารถชำระค่าธรรมเนียมผ่านทาง
M-FLOW ได้ 3 ช่องทางเท่านั้น ได้แก่

1. เว็บไซต์ WWW.MFLOWTHAI.COM
2. แอปพลิเคชัน MFLOWTHAI
3. LINE OA : @MFLOWTHAI

ไม่เชื่อ ไม่รับ ไม่โอน

#ตำรวจไซเบอร์เตือนภัย

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี
CYBER CRIME INVESTIGATION BUREAU

ตำรวจไซเบอร์

← Google Play 🔍 ⋮

 **ลงทะเบียนรับเงินดิจิทัล 10000**

Myspirit24
มีโฆษณา

↓ 6.7 MB | 3+ | 3+ ⓘ

ติดตั้ง

เกี่ยวกับแอปนี้ →

แนะนำการลงทะเบียนรับเหรียญดิจิทัล วอลเล็ต 10000 ล่วงหน้าตามนโยบายเพื่อไทย

← Google Play 🔍 ⋮

 **รับสิทธิเงินดิจิทัล 10000**

Lodner Official
มีโฆษณา

↓ 11 MB | 3+ | 3+ ⓘ

ติดตั้ง

← Google Play 🔍 ⋮

 **ลงทะเบียนรับเงินดิจิทัล 10000**

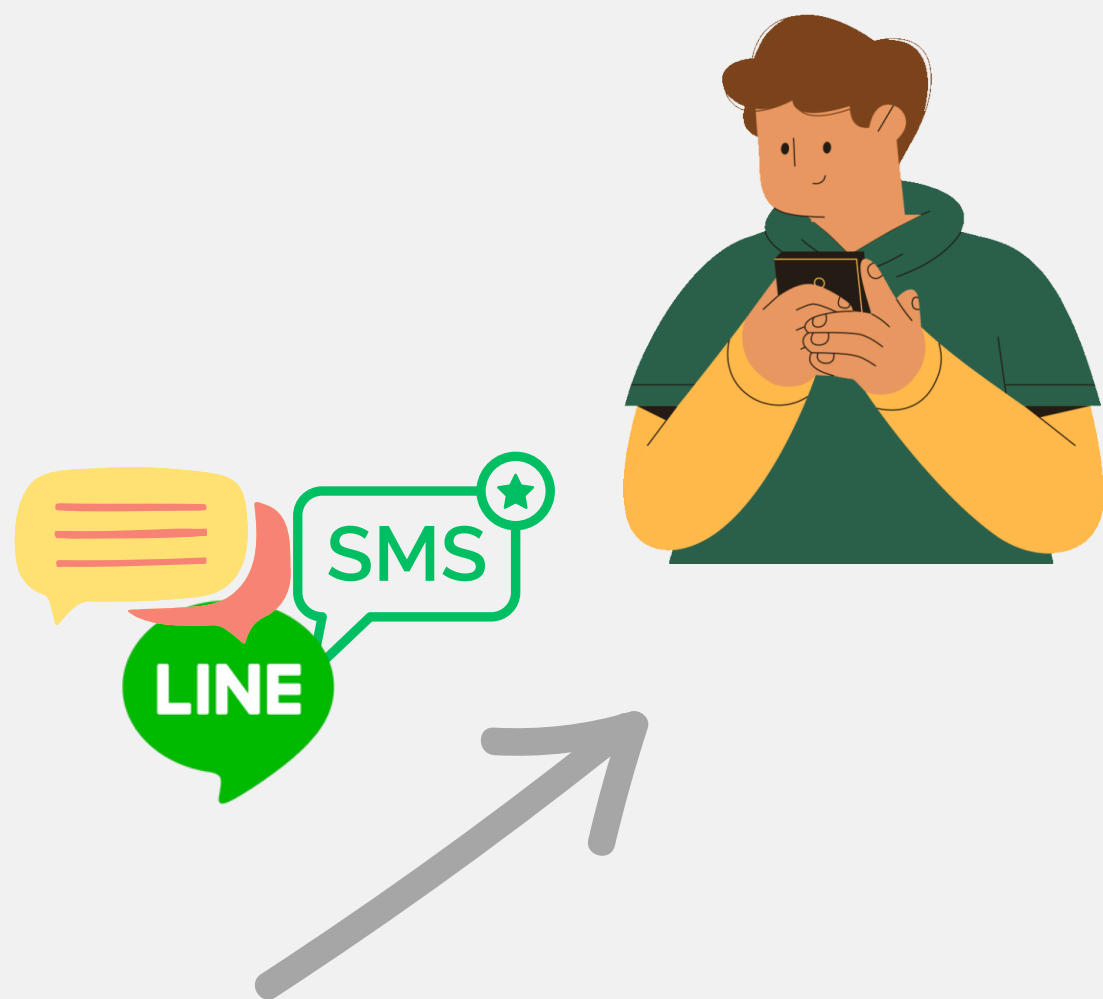
Myspirit24
มีโฆษณา

↓ 6.7 MB | 3+ | 3+ ⓘ

ติดตั้ง

เตือนภัย! มีจาชิปส่ง SMS

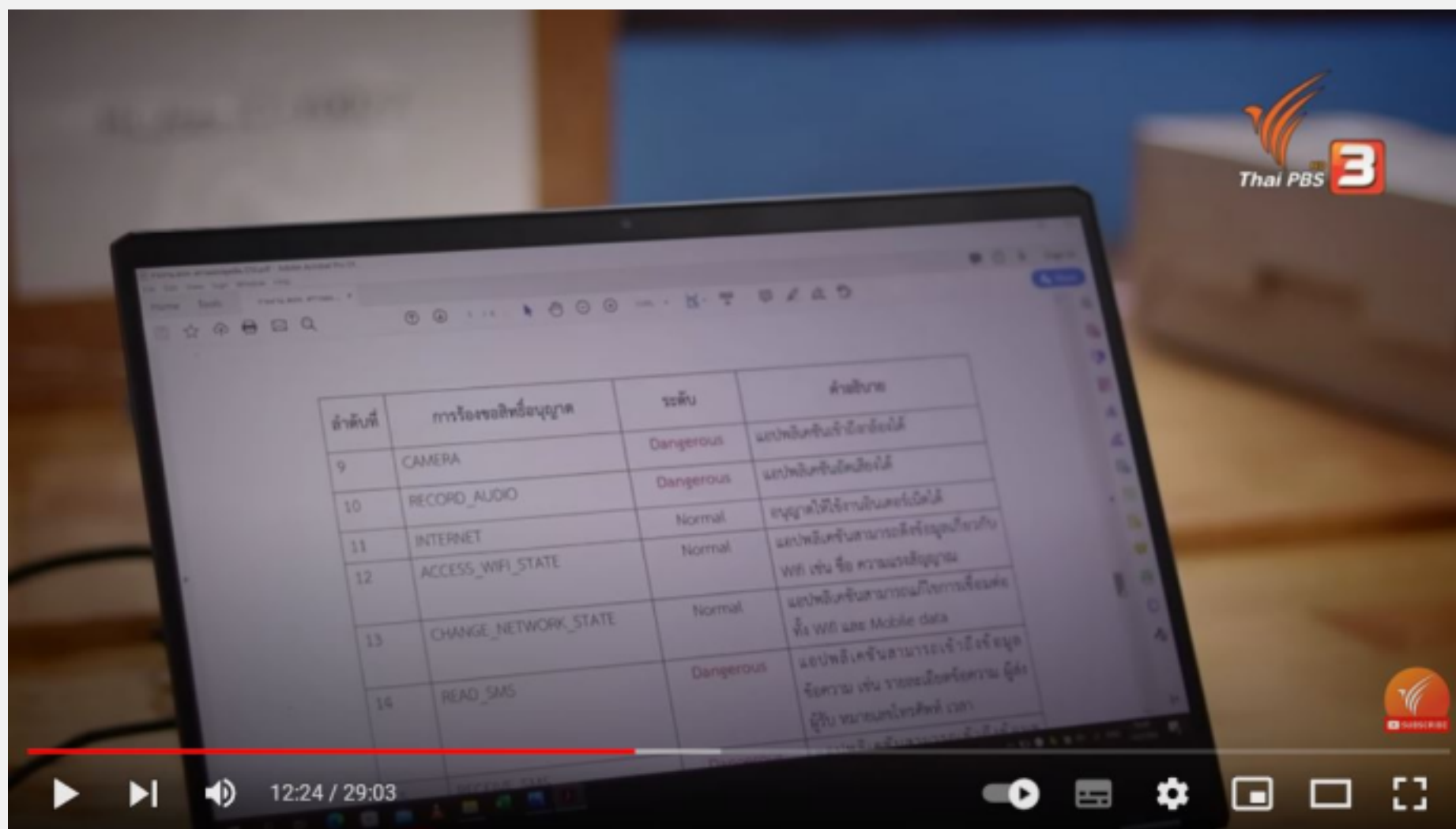
▲ แจ้งได้รับเงินดิจิทัล 10,000 หลอกติดตั้งแอปดูดเงิน



ข้อมูลส่วนบุคคล และข้อมูลทางการเงิน

เช่น ชื่อ นามสกุล วันเดือนปีเกิด
เบอร์โทรศัพท์ เลขบัญชีธนาคาร
เลขบัตรประชาชน รหัส OTP
เลขบัตรเดบิต หรือ บัตรเครดิต
รหัสหลังบัตร 3 หลัก





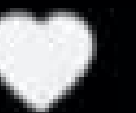
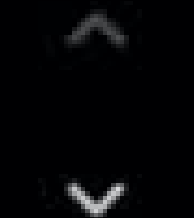
ข้อมูลจากการตรวจพิสูจน์โทรศัพท์
มือถือของผู้เสียหายของกองบัญชาการ
ตำรวจสอบสวนกลาง **CIB** พบว่า
มีจอสายฟได้สิทธิเข้าถึงฟังก์ชันต่างๆ
ในโทรศัพท์ได้ถึง **23** สิทธิ เช่น

- สิทธิค้นหา **application**
- สิทธิการเข้าถึงรายชื่อบุคคลทั้งใน
โทรศัพท์ และสื่อ **social**
- การใช้งาน **Internet**
- การเข้าถึงกล้องถ่ายรูป อัดเสียง
ซึ่งมีจอสายฟจะนำไปเข้าฐานข้อมูล **AI**
แล้วเอาไปใช้ในการหลอกลวงบุคคลที่เรารู้จัก

ที่มา: ข้อมูลจากรายการ *Big story* ช่อง ไทยพีบีเอส ออกอากาศวันที่ 5 ส.ค. 2566



เมื่อมิจฉาชีพควบคุมโทรศัพท์ทางไกลได้
แะอีก รหัส Facebook , แอปธนาคาร ?
วิชา มิจฉาชีพออนไลน์



288.6K

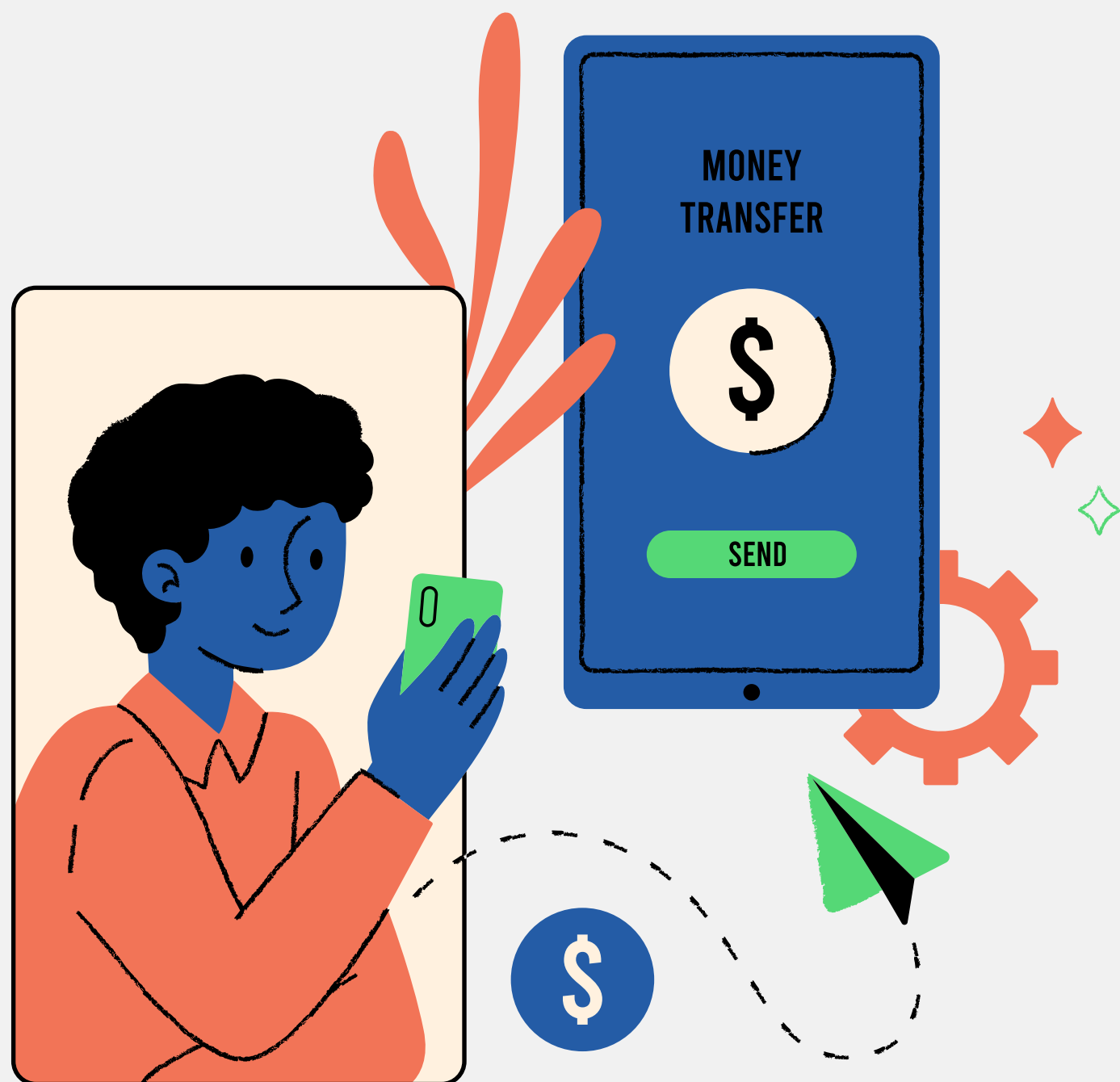


5293



39.9K





How to know ???

ถ้าหากในมือถือมี**แอปดูดเงิน**แฝงอยู่ เราจะมีวิธีสังเกตได้หลายอย่าง ได้แก่

- แอปต่างๆ อาจค้างหรือหยุดทำงาน แบบไม่มีเหตุผล
- เครื่องมีอาการช้าและอืดกว่าเดิมมาก
- แบตเตอรี่หมดเร็วกว่าปกติ เพราะแอปดูดเงินจะใช้ทรัพยากรในเครื่องหนักขึ้น เป็นต้น

ถ้ารู้ตัวว่า กำลังถูกดูดเงิน

- เปิดโหมดเครื่องบิน (Airplane mode หรือ Flight mode)
- ปิด router / wifi ในบ้าน
- ดึงซิมการ์ดออกจากโทรศัพท์



ถ้าถูกดูดเงินไปแล้ว รู้ตัวภายหลัง

- ค้นหาแอปดูดเงินในโทรศัพท์แล้วลบทิ้ง
- รวบรวมหลักฐานการสนทนา หรือทำธุรกรรมทางการเงิน ติดต่อธนาคารเพื่อยกบัญชีเครดิต บัญชีธนาคาร
- แจ้งความเจ้าหน้าที่ตำรวจ หรือแจ้งความออนไลน์ที่ www.thaipoliceonline.com

วิธีการตรวจสอบมือถือระบบ **ios**

1. การตั้งค่า --> **แบตเตอรี่** และดูว่ามีแอปไหนที่ใช้งานหนักเกินการใช้งานจริง
2. เข้าไปดูแอปทั้งหมดบน iPhone ว่ามีแอปไหนแปลกปลอมติดมาหรือเปล่า ถ้ามีให้กดลบทันที
3. สำคัญคือควรเปิดการเตือนเว็บหลอกลวงบน Safari โดยเข้าไปที่ **การตั้งค่า --> Safari** จากนั้นให้กดเปิดสวิตช์ “คำเตือนเว็บไซต์หลอกลวง” รวมไปถึงการลบปฏิทินสแปมบนแอปปฏิทินด้วย



ที่มา : กองบัญชาการตำรวจสอบสวนกลาง

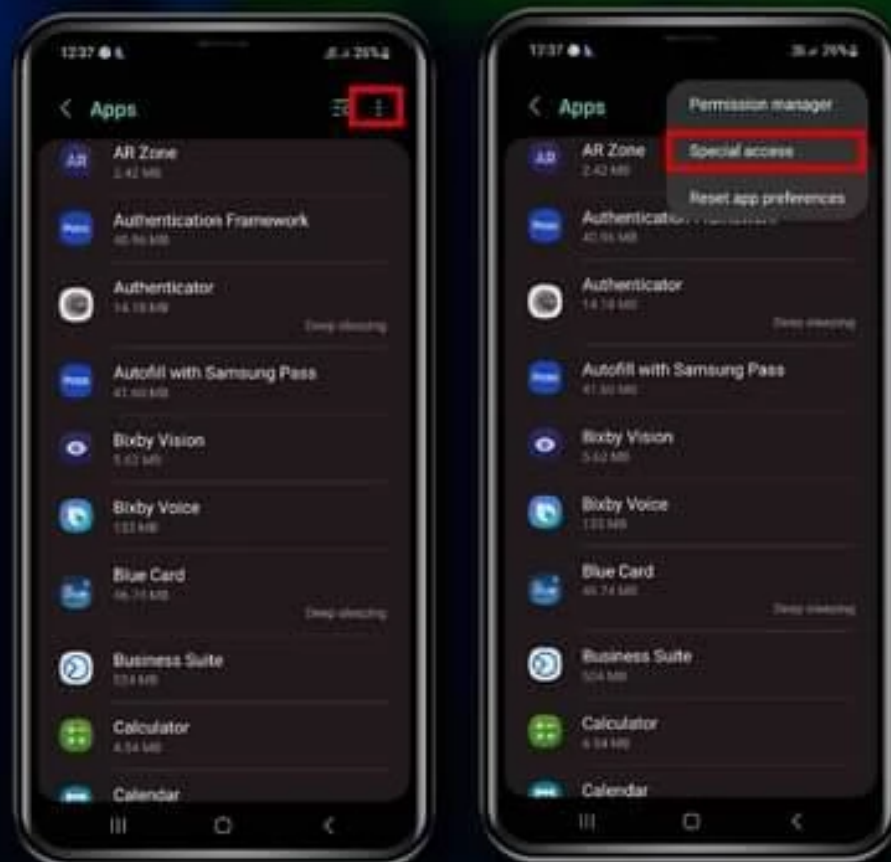
Android

1. เข้าไปที่เมนู การตั้งค่า (Settings) และเลือกไปที่เมนู แอป (Apps)



2. กดที่ปุ่มตัวเลือก (จุด 3 จุดมุมขวาบน) เพื่อเลือกเมนูย่อย

3. เลือกไปที่การเข้าถึงพิเศษ (Special access) ถ้าหากเข้าไม่ได้หน้าจอจะเด้งออกไปที่หน้าหลัก แสดงว่ามือถือเครื่องนั้นถูกฝังแอปรีโมทดูเงินเรียบร้อยแล้ว



วิธีการตรวจสอบมือถือระบบ **Android**

1. เข้าไปที่เมนู **การตั้งค่า** --> **แอป**

2. กดที่ปุ่ม**ตัวเลือก** (จุด 3 จุดมุมขวาบน) เพื่อเลือกเมนูย่อย (มือถือ Android บางรุ่นต้องเข้าไปที่เมนู Apps อีกครั้งก่อนหรือมืออยู่ในเมนู ไม่ต้องกดจุด 3 จุดมุมขวาบน)

1. เลือกไปที่ **การเข้าถึงพิเศษ (Special access)** ถ้าหากว่า  **เข้าได้ปกติ** ก็แสดงว่ามือถือเรายังปกติดีอยู่

 **หากเข้าไม่ได้** โดยหน้าจอจะเด้งออกไปที่หน้าหลัก

แสดงว่ามือถือเครื่องนั้นถูก**ฝังแอปรีโมท**ดูเงินเรียบร้อยแล้ว
ให้**รีบตัดการเชื่อมต่ออินเทอร์เน็ตทันที** แล้ว**สำรองข้อมูล**ที่สำคัญ และให้**รีบล้างเครื่องโดยรีเซ็ต**เครื่องกลับสู่ค่าเริ่มต้นที่มาจากโรงงานทันที

การดำเนินการของธนาคารเมื่อลูกค้าทราบว่า ถูกมิจฉาชีพหลอกลวง



1. ผู้เสียหาย**แจ้งไปยัง Call Center หรือสาขาธนาคาร**ที่มีบัญชีอยู่ที่



2. เมื่อธนาคารได้รับแจ้งจากผู้เสียหาย ธนาคาร**จะระงับธุรกรรมชั่วคราวทันที** และจะแจ้งให้ธนาคารปลายทางทำการตรวจสอบและ**ระงับธุรกรรมชั่วคราวทันที 72 ชั่วโมง**



3. ธนาคารที่ผู้เสียหายมีบัญชีจะออก **Bank Case ID** เพื่อให้ผู้เสียหายนำไปแจ้งความกับ พนักงานสอบสวนที่สถานีตำรวจใดก็ได้ที่สะดวก

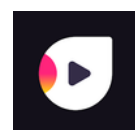


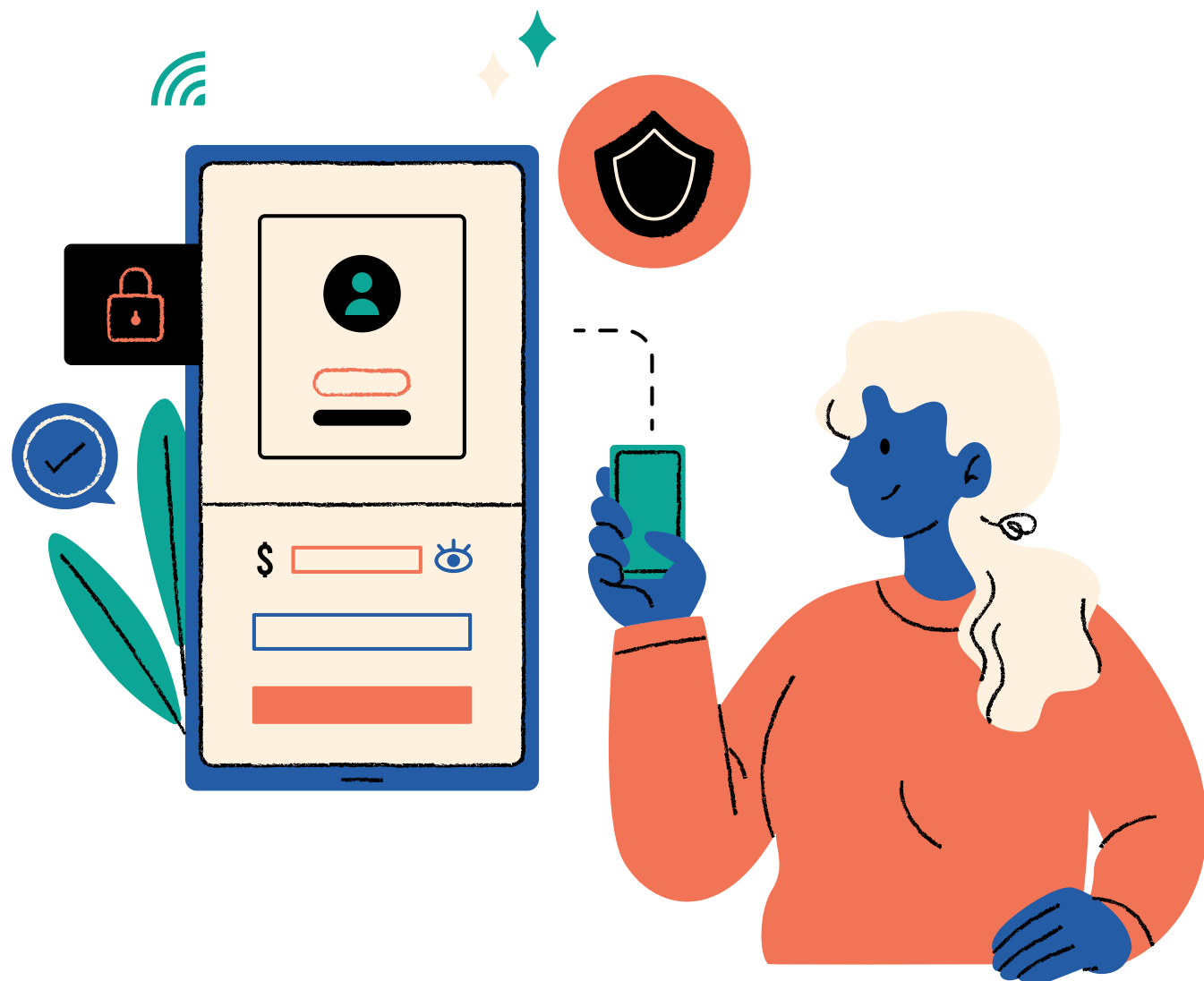
4. พนักงานสอบสวนจะรับพิจารณาร้องทุกข์ แล้วแจ้งธนาคารเพื่อ **ขยายระยะเวลาการระงับธุรกรรม เป็น 7 วัน** เพื่อรอการตรวจสอบ และออกหมายต่อไป

วันที่ 4 สิงหาคม 2566 มีรายงานว่า แพนเพจ **สำรวจสอบสวนกลาง** ได้เผยแพร่เรื่องราวเตือนภัย **แอปพลิเคชันอันตราย** โดยระบุข้อความว่า ขณะนี้ตรวจพบ **แอปที่มีมัลแวร์ดักข้อมูลแฝงอยู่** ซึ่งบางแอปถูกถอดจาก Playstore แล้ว แต่ยังสามารถติดตั้งผ่านช่องทางแอปพลิเคชันอื่นได้อยู่ และบางแอปจะอยู่ในรูปแบบ Mini-Game ที่ให้ผู้ใช้เข้ามาเล่นเพื่อรับรางวัล



โดยมี **10** แอปฯ อันตรายดังนี้

	Noizz	แอปฯ ตัดต่อวิดีโอพร้อมเพลง (100,000,000 downloads)
	Zapya	แอปฯ แชร์ไฟล์ ย้ายไฟล์ (100,000,000 downloads)
	VFly	แอปฯ สร้างวิดีโอ (50,000,000 downloads)
	MVBit	แอปฯ ตัดต่อวิดีโอ (50,000,000 downloads)
	Biugo	แอปฯ ตัดต่อวิดีโอ (50,000,000 downloads)
	Crazy Drop	แอปฯ เล่นเกม รับรางวัล (10,000,000 downloads)
	Cashzine	แอปฯ เล่นเกม รับรางวัล (10,000,000 downloads)
	Fizzo Novel	แอปฯ อ่านหนังสือออนไลน์ (10,000,000 downloads)
	CashEM	แอปฯ รับรางวัล (5,000,000 downloads)
	Tick	แอปฯ ดูวิดีโอเพื่อรับรางวัล (5,000,000 downloads)



การป้องกันภัยจากมิจฉาชีพ

1. ไม่กดลิงค์ หรือ ดาวน์โหลดแอปพลิเคชันที่แนบมากับข้อความ SMS / Application chat
2. ไม่ให้ข้อมูลส่วนตัว เมื่อรับสายที่ไม่รู้จัก
3. โทรสอบถามจากเบอร์กลางของหน่วยงานที่ถูกต้อง
4. ไม่ใช้รหัส หรือ PIN เดียวกันในทุกแอปพลิเคชัน
5. ปรับวงเงินในบัญชี/บัตรเครดิตให้ลดลง
6. ยกเลิกการผูกบัญชีผ่านช่องทางต่างๆ

Do you have any questions?

