# คิดก่อน Click

**นางสาวภัทรรัตน์ หอมกระจ่าง**
**นักนิติวิทยาศาสตร์ชำนาญการ**
**กลุ่มตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์**
**กองตรวจพิสูจน์ทางวิทยาศาสตร์**

ปัจจุบันมิจฉาชีพสามารถหลอกดูดเงินจากเหยื่อได้ง่ายขึ้น อย่างที่เราพบเห็นในข่าวบ่อย ๆ ก็มักจะมาในรูปแบบของแก๊งคอลเซ็นเตอร์ที่หลอกให้เหยื่อโอนเงิน หรือหลอกให้ติดตั้งแอปพลิเคชั่นลงมือถือแล้วจัดการโอนเงินออกจากบัญชี ซึ่งมีทั้งมาในรูปแบบหลอกเป็นเจ้าหน้าที่รัฐจากหน่วยงานต่างๆ หรือ ส่งข้อความการถูกรางวัลมาทาง SMS ให้ผู้เสียหายโดยตรง แล้วหลอกลวงให้ผู้เสียหายหลงเชื่อติดตั้งแอปฯดังกล่าว และบอกข้อมูลส่วนบุคคล ข้อมูลทางการเงิน เช่น ชื่อนามสกุล วันเดือนปีเกิด เบอร์โทรศัพท์ หมายเลขบัตรประชาชน เลขบัญชีธนาคาร เลขบัตรเดบิตหรือเครดิต รหัสหลังบัตร 3 หลัก รหัส OTP เป็นต้น จากนั้นมิจฉาชีพจะทำการควบคุมโทรศัพท์มือถือของเหยื่อ แล้วดำเนินการโอนเงินออกจากบัญชี โดยข้อมูลจากการตรวจพิสูจน์โทรศัพท์มือถือของผู้เสียหาย ของกองบัญชาการตำรวจสอบสวนกลาง CIB พบว่า มิจฉาชีพได้สิทธิเข้าถึงฟังชั่นต่างๆในโทรศัพท์ได้ถึง 23 สิทธิ เช่น

- สิทธิค้นหา application
- สิทธิการเข้าถึงรายชื่อบุคคลทั้งในโทรศัพท์ และสื่อ social
- การใช้งาน internet
- การเข้าถึงกล้องถ่ายรูป/ อัดเสียง ซึ่งมิจฉาชีพจะนำไปเข้าฐานข้อมูล AI แล้วเอาไปใช้ในการหลอกบุคคลที่เรารู้จัก

**วิธีสังเกตมือถือตนเองว่ามีแอปฯ ดูดเงินแฝงอยู่**

- แอปฯ ต่าง ๆ อาจค้างหรือหยุดทำงานแบบไม่มีเหตุผล
- เครื่องมีอาการช้าและอืดกว่าเดิมมาก
- แบตเตอรี่หมดเร็วกว่าปกติ เพราะแอปฯ ดูดเงินจะใช้ทรัพยากรในเครื่องหนักขึ้น เป็นต้น

- ***ถ้ารู้ตัวว่ากำลังถูกดูดเงิน ให้ตัดการเชื่อมต่ออินเตอร์เนต โดย***

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

- ***ถ้าถูกดูดเงินไปแล้ว รู้ตัวภายหลัง ให้ปฏิบัติดังนี้***

- ค้นหาแอปดูดเงินในโทรศัพท์แล้วลบทิ้ง

- รวบรวมหลักฐานการสนธนา หรือทำธุรกรรมทางการเงิน ติดต่อธนาคารเพื่ออายัดบัครเครดิต บัญชีธนาคาร
- แจ้งความเจ้าหน้าที่ตำรวจ หรือแจ้งความออนไลน์ที่ www.thaipoliceonline.com

**วิธีการตรวจสอบโทรศัพท์มือถือ**

***ระบบ iOS***

1. เข้าไปที่เมนู การตั้งค่า (Settings) และเลือกไปที่เมนู แบตเตอรี่ แล้วดูว่ามีแอปฯ ใดที่ใช้งานหนักเกินการใช้งานจริง
2. เข้าไปดูแอปฯ ทั้งหมดบน iPhone ว่ามีแอปฯ ไหนแปลกปลอม ถ้ามีให้กดลบทันที
3. สำคัญคือควรเปิดการเตือนเว็บหลอกลวงบน Safari โดยเข้าไปที่ การตั้งค่า -> Safari จากนั้นให้กดเปิดสวิตช์ **“คำเตือนเว็บไซต์หลอกลวง”** รวมไปถึงการลบปฏิทินสแปมบนแอปปฏิทินด้วย

***ระบบ Android***

1. เข้าไปที่เมนู การตั้งค่า (Settings) และเลือกไปที่เมนู แอป (Apps)
2. กดที่ปุ่มตัวเลือก (จุด 3 จุดมุมขวาบน) เพื่อเลือกเมนูย่อย (มือถือ Android บางรุ่นต้องเข้าไปที่เมนู Apps อีกครั้งก่อนหรือมีอยู่ในเมนู ไม่ต้องกดจุด 3 จุดมุมขวาบน)
3. เลือกไปที่ การเข้าถึงพิเศษ (Special access) ถ้าหากว่าเข้าได้ปกติก็แสดงว่ามือถือเรายังปกติดีอยู่ แต่ถ้าหากเข้าไม่ได้โดยหน้าจอจะเด้งออกไปที่หน้าหลัก แสดงว่ามือถือเครื่องนั้นถูกฝังแอพรีโมทดูดเงินเรียบร้อยแล้ว

**การดำเนินการของธนาคารเมื่อทราบว่าลูกค้าถูกมิจฉาชีพหลอกลวง**

1. ผู้เสียหายแจ้งไปยัง Call Center หรือสาขาธนาคารที่มีบัญชีอยู่ทันที
2. เมื่อธนาคารได้รับแจ้งจากผู้เสียหาย ธนาคารจะระงับธุรกรรมชั่วคราวทันที และจะแจ้งให้ธนาคารปลายทางทำการตรวจสอบ และระงับธุรกรรมชั่วคราวทันที 72 ชั่วโมง
3. ธนาคารที่ผู้เสียหายมีบัญชีจะออก Bank Case ID เพื่อให้ผู้เสียหายนำไปแจ้งความกับพนักงานสอบสวนที่สถานีตำรวจใดก็ได้ที่สะดวก
4. พนักงานสอบสวนจะรับพิจารณาร้องทุกข์ แล้วแจ้งธนาคารเพื่อ ขยายระยะเวลาระงับธุรกรรมเป็น 7 วัน เพื่อรอการตรวจสอบ และออกหมายต่อไป

**การป้องกันภัยจากมิจฉาชีพ**

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

**ที่มา**

- ข้อมูลจากรายการ Big story ช่อง ไทยพีบีเอส ออกอากาศวันที่ 5 ส.ค. 2566
- https://money.kapook.com/view264412.html
- กองบัญชาการตำรวจสอบสวนกลาง
- สมาคมธนาคารไทย