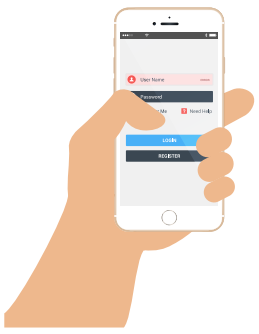
รู้ก่อนโหลด ก่อนเงินหมดบัญชี

กระบวนการทำงานของมิจฉาชีพ APP ดูดเงินแบบ REMOTE ACCESS มีดังนี้



1. SMS ลิงค์แปลก ๆ ให้กดเพิ่มเพื่อนใน Line

จุดเริ่มต้นของกระบวนการส่วนมากคือการคลิก Line ที่มาในรูปแบบ SMS หรือข้อความชวนเชื่อผ่านกลุ่ม Line หรือช่องทาง Social Media ต่าง ๆ เช่น แจกเงิน โปรโมชั่นลดสินค้า การกู้เงินดอกต่ำ เป็นต้น โดย Link ที่ติดมาเมื่อคลิกเข้าไปจะเด้งไปที่หน้า App Line เพื่อให้กดเพิ่มเพื่อนเกือบจะ 100%

2. หลอกล่อสร้างสถานการณ์ ให้โหลด App เพื่อส่งข้อมูลส่วนตัว

เมื่อเพิ่มเพื่อนแล้ว มิจฉาชีพก็จะหลอกล่อพูดคุย เพื่อให้เหยื่อหลงเชื่อ โดยจะสร้างสถานการณ์ตามกระแสช่วงนั้น ๆ เช่น ช่วงใกล้เสียภาษี ก็จะมาในรูปแบบของสรรพากร โดยการส่ง Link Applications มาให้โหลด เพื่อเหยื่อจะได้กรอกข้อมูลส่วนตัวลงไป

3. โหลด App นอก Store

App ที่ส่งมาให้โหลดนั้น จะเป็นแอปนอก Store ซึ่งเหยื่ออาจจะไม่ทราบ เพราะมิจฉาชีพทำออกมาหน้าตาเหมือนแอปที่อยู่บน Store ให้สังเกตถ้ามีการถามว่าจะโหลด App ต่อไหม แล้วเป็นไฟล์ .apk ให้ระวังว่า ไม่ใช่ App ดีแน่นอน ถ้าโหลดไปแล้วในส่วนนี้จะยังถอนตัวทัน

4. การให้ข้อมูลส่วนตัว ตั้งรหัสพินเหมือน App ธนาคาร

หลังจากติดตั้ง App เสร็จมิจฉาชีพจะให้กรอกข้อมูลส่วนตัวลงไป ซึ่งส่วนมากก็จะมีชื่อ เบอร์โทร และที่สำคัญคือ รหัสผ่านหรือพิน 6 ตัว ซึ่งส่วนมากเหยื่อจะตั้งรหัสพินเหมือนกันเกือบทุก App ไม่เว้นแม้แต่ App ธนาคาร ซึ่งจุดนี้จะทำให้มิจฉาชีพทราบว่ารหัสผ่านระบบต่าง ๆ ของเราคืออะไร รวมถึงมิจฉาชีพอาจจะหลอกขอพินโดยตรงจากเหยื่อได้เช่นกัน

5. การเข้าถึง การช่วยเหลือพิเศษ หรือ Accessibility

เมื่อมีการให้ข้อมูลต่าง ๆ แล้ว ขั้นตอนถัดไปที่สำคัญ คือ หลอกให้เหยื่อกดอนุญาตการเข้าถึงโทรศัพท์ แบบ Remote Access หรือการควบคุมทางไกล ซึ่งข้อความที่ขึ้นให้เราเห็นผ่านหน้า App ปลอมจะเป็นข้อความทั่ว ๆ ไป จนเราไม่ทันสังเกตว่านั่นคือการขอเข้าถึงทางไกล ที่เป็นฟีเจอร์ในมือถือ มีไว้เพื่อช่วยเหลือคนทุพพลภาพนั่นเอง ซึ่งส่วนนี้เหยื่อหลาย ๆ คน จะไม่ค่อยได้อ่านว่าที่กดอนุญาตไปนั้นคืออะไร ส่วนมากก็จะกดอนุญาตตามที่มิจฉาชีพบอก ซึ่ง ณ ตอนนี้ มิจฉาชีพสามารถควบคุมมือถือของเราได้ทั้งหมดแล้ว ซึ่งส่วนนี้ ทางเหยื่อจะเห็นเป็นภาพรอการทำงานขึ้นมา เช่น กรุณารอสักครู่ระบบกำลังทำรายการ หรือเป็นการเคาน์ดาวน์เวลานาน ๆ และห้ามใช้มือถือ ซึ่งบางครั้งเหยื่อก็มักจะวางมือถือทิ้งไว้ แล้วไปทำอย่างอื่นไม่ได้มองจออยู่ตลอด มิจฉาชีพก็จะเข้าสู่แอปต่าง ๆ ของเราในตอนนี้ แม้แต่เรานั่งมองจอ ก็จะไม่ทราบว่าเขาทำอะไรอยู่เบื้องหลัง เพราะมีภาพมากั้นไว้ ถ้าใครเก็บรหัสต่าง ๆ ไว้ในมือถือ มิจฉาชีพก็จะเข้า App โอนเงินออกไปในขั้นตอนนี้ พอทำเสร็จ จะมีการทำลายหลักฐานต่าง ๆ ทั้งสลิปการโอน และลบแอปออกทันที ซึ่งเหยื่อก็จะไม่รู้ตัว จนกว่าจะไปเช็คยอดเงิน

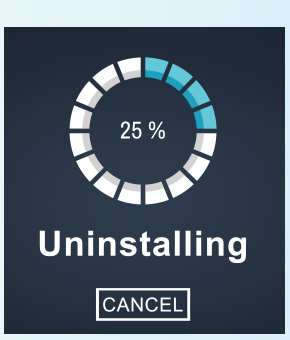
6. การขออนุญาตส่งสัญญาณภาพไปที่อื่น

ในส่วนนี้ มิจฉาชีพจะหลอกให้กดแต่จริง ๆ แล้วเขาสามารถกดเองได้เพียงแต่ทำเหมือนว่าเราทำ ซึ่งจะเกิดขึ้นเร็วมาก ๆ จนมองไม่ทัน โดยจะเป็นการส่งสัญญาณหน้าจอมือถือเราไปที่จอภาพของมิจฉาชีพ เขาก็จะเห็นแล้วว่าหน้าตาการใช้งานมือถือเราเป็นอย่างไร มี App อะไรบ้าง

7. ค้นข้อมูล โอนเงินออก โดยใช้ภาพหน้าจอหลอก

ต้องทำอย่างไร หากสังเกตว่ากำลังโดนมิจฉาชีพขโมยเงิน

1



2

3

4

หากเพียงแค่คลิก Link ยังไม่มีการโหลด App
ส่วนนี้ยังปลอดภัย ถ้ายังไม่ไว้ใจ สามารถให้ผู้เชี่ยวชาญตรวจสอบได้

หากโหลด App แล้ว ให้รีบถอนการติดตั้ง
หากทำไม่เป็น ให้ปิดเครื่องก่อนแล้วให้ผู้เชี่ยวชาญทำให้

อนุญาตการเข้าถึงไปแล้ว
หากนึกได้ว่าโดนหลอก ในขั้นตอนนี้ให้รีบตัดสัญญาณอินเทอร์เน็ต พร้อมทั้งถอด WIFI ปิดสัญญาณ 5G/4G โดยเปิด Airplane Mode หากกดไม่ได้ให้ปิดเครื่อง หรือถอดซิมออกพร้อมถอนการติดตั้งภายหลัง

หากตกเป็นเหยื่อแล้ว
- รีบแจ้งความดำเนินคดี
- รีบติดต่อธนาคารเพื่ออายัดบัญชีปลายทาง รวมทั้งบัญชีตัวเองทั้งหมด
- รีบอายัดบัตรเครดิต เปลี่ยนรหัสผ่าน
- นำมือถือไปให้ร้าน Reset

วิธีป้องกันและสังเกต App อันตราย

- อย่าดาวน์โหลด App นอก Store
- Update Sofeware และ App ธนาคาร อยู่เสมอ
- อ่านทุกอย่างให้ละเอียด ก่อนจะกดอนุญาต
- อย่า Click จาก SMS E-mail หรือ Line Group ที่ส่งจากผู้ส่งที่ไม่รู้จัก
- ติดตามข้อมูลข่าวสารอยู่เสมอ

การจัดการความรู้ KNOWLEDGE MANAGEMENT

จัดทำโดย กลุ่มพัฒนาระบบบริหาร

ที่มา : https://droidsans.com/malware-app-how-does-it-work/