



กลไกมิจาชีพ
หลอกติดตั้งแอปพลิเคชันดูดเงิน
และ การยกระดับมาตรการป้องกัน
ร่วมกับหน่วยงานต่าง ๆ

ภาพรวม ขั้นตอนของมิจฉาชีพ กรณีใช้แอปดูดเงิน สร้างความเสียหายต่อประชาชน

1. หลอกลวง ล่อเหยื่อ



Call Center

- หลอกรื่องภาชี เช่น คั้นภาชี หลีกเลี้ยงภาชี ตรวจสอบภาชี
- หลอกรื่องคดีความ ฟ้องร้อง
- หลอกให้บริการเงินกู้
- หลอกรื่องอื่นๆ



SMS

- ใช้ชื่อ Sender name เหมือนหน่วยงานต่างๆ
- ใช้ชื่อ Sender name คล้ายหน่วยงานต่างๆ
- ใช้เบอร์โทรทั่วไปหลอกลวง



Social Media

- หลอกให้บริการเงินกู้
- หลอกให้เงินรางวัล ตัวเครื่องบิน
- หลอกรื่องอื่นๆ



Add LINE Account

- หลอกให้เพิ่ม (Add) บัญชีไลน์ปลอม (Fake LINE Account) ของมิจฉาชีพ

2. หลอกให้ติดตั้งโปรแกรม



Installation

- ชวนพูดคุย หลอกขอข้อมูลเหยื่อ
- ใช้เอกสารปลอม เพื่อเพิ่มความน่าเชื่อถือ เช่น บัตรประชาชน รูปถ่าย ใบจดทะเบียนธุรกิจการค้า
- หลอกให้เหยื่อทำตามเพื่อติดตั้ง Mobile Application ปลอม (ไฟล์ติดตั้งนามสกุล .apk) โดยใช้ความสามารถของ Accessibility Service ของระบบปฏิบัติการ Android ในการควบคุมมือถือของเหยื่อ

3. ควบคุมเครื่องและใช้ประโยชน์



Action on Objectives

- Mobile Application ปลอม เชื่อมต่อกลับไปยังเครื่องของมิจฉาชีพ Command-and-Control (C2) server และควบคุมมือถือของเหยื่อ
- โอนเงิน, ขโมยข้อมูลส่วนบุคคล, ขโมยบัญชี Social, ขโมยรูปถ่าย, แบล็คเมล ฯลฯ

3 รูปแบบหลักของแอปดูดเงิน

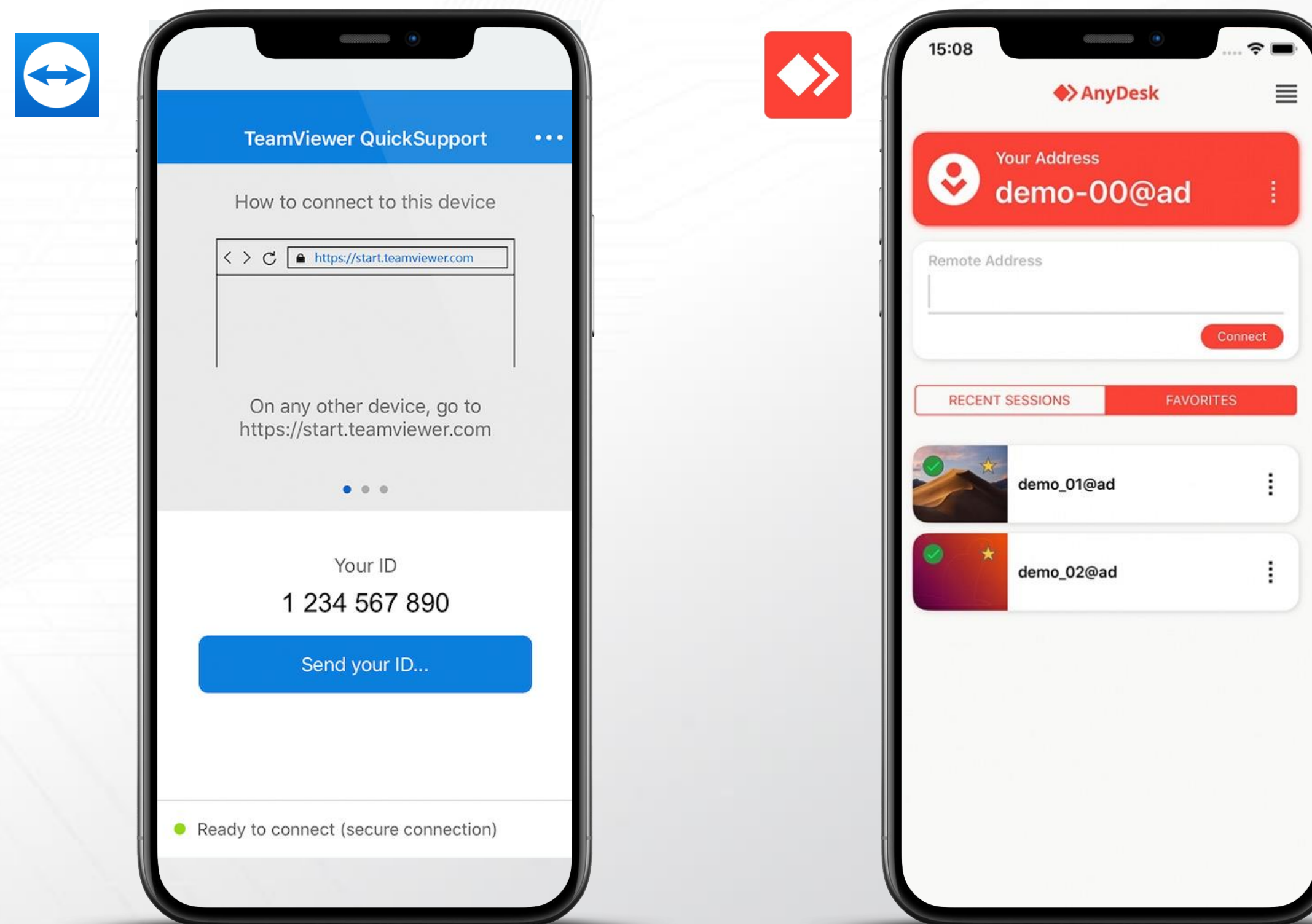
ที่มีจจาซีฟใช้หลอกประชาชน

1. หลอกให้เหยื่อติดตั้งโปรแกรมจำพวกรีโมท เช่น  TeamViewer,  AnyDesk แล้วควบคุมโทรศัพท์ของเหยื่อแบบรีโมทเพื่อโอนเงินออกทันที (เกิดขึ้นมากในช่วงกลางปี 2565)
2. หลอกให้เหยื่อทำตามเพื่อติดตั้งแอปพลิเคชันอันตราย (.apk) แล้วจอมือถือของเหยื่อจะค้าง และโจรจะรีโมทมาควบคุมมือถือของเหยื่อ และโอนเงินออกทันที เช่นกรณี DSI, สรรพากร, Lion-Air, ไทยประกันชีวิต, กระทรวงพาณิชย์ (ยังคงเป็นรูปแบบที่มีจจาซีฟใช้มากที่สุด)
3. หลอกให้เหยื่อทำตามเพื่อติดตั้งแอปพลิเคชันอันตราย (.apk) เพื่อควบคุมมือถือของเหยื่อ แต่โจรจะยังไม่โอนเงินทันที และรอประชาชนเพลอ แล้วแอบโอนเงินออกภายหลัง เช่น กรณีแอปหาคู่  Bumble,  Snapchat (ยังคงเป็นรูปแบบที่มีจจาซีฟใช้)

* ในปัจจุบันพบเฉพาะประชาชนที่ใช้โทรศัพท์ ระบบปฏิบัติการ Android ที่ได้รับผลกระทบ

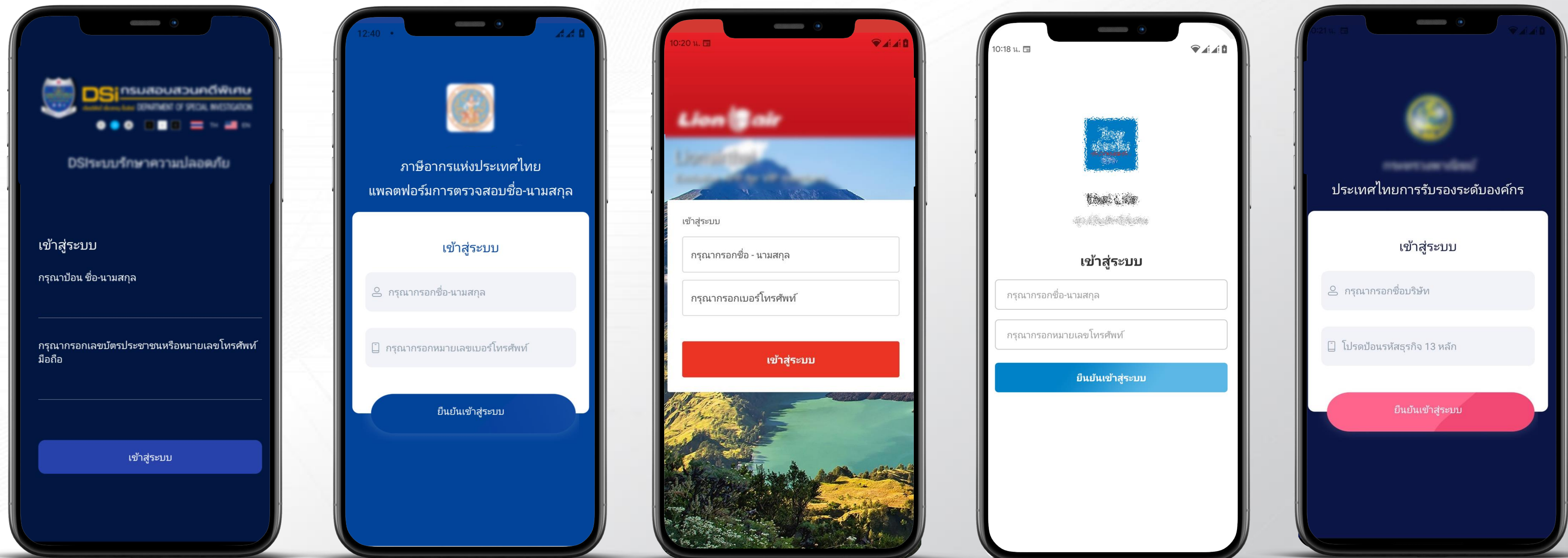
รูปแบบหลักของแอปดูเงิน (หน้า 1/3)

1. หลอกให้เหยื่อติดตั้งโปรแกรมจำพวกรีโมท เช่น TeamViewer, AnyDesk แล้วควบคุมโทรศัพท์ของเหยื่อแบบรีโมทเพื่อโอนเงินออกทันที (เกิดขึ้นมากในช่วงกลางปี 2565)



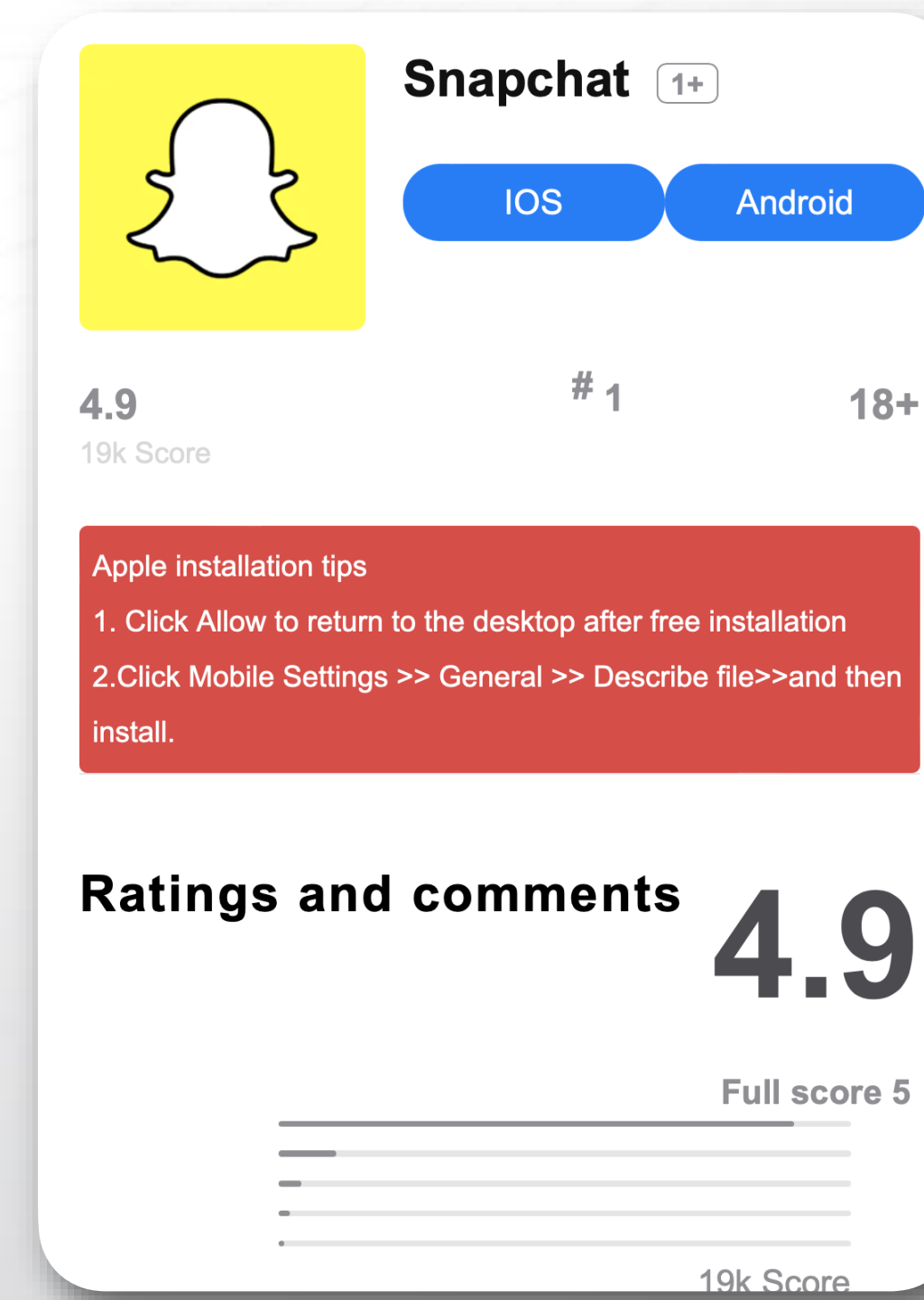
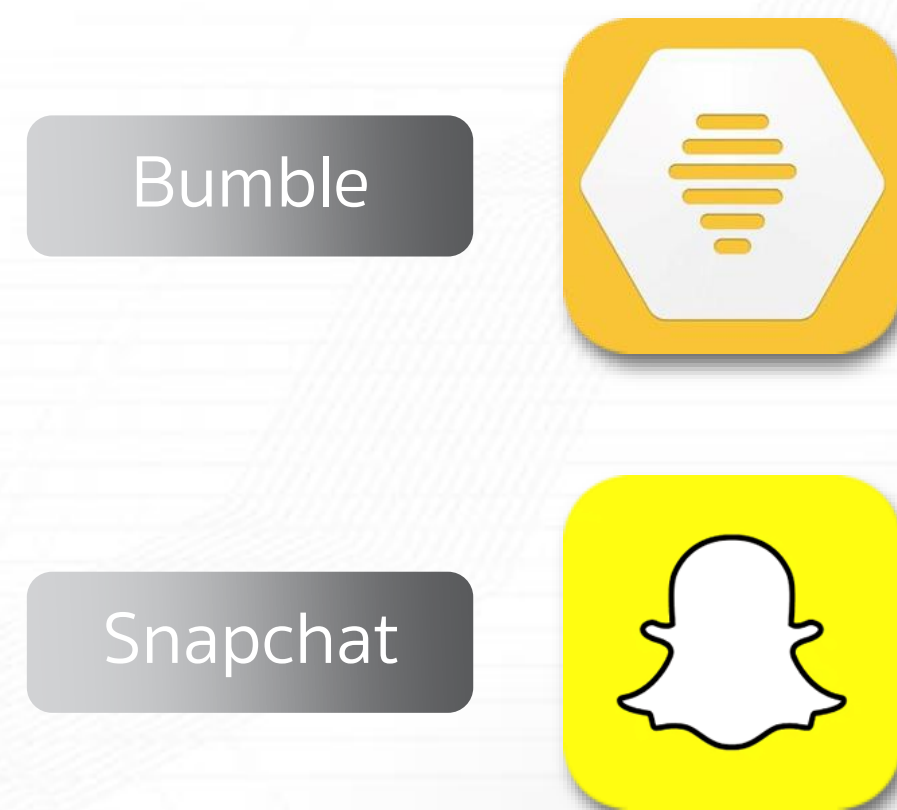
รูปแบบหลักของแอปดูเงิน (หน้า 2/3)

2. หลอกให้เหยื่อทำตามเพื่อติดตั้งแอปพลิเคชันอันตราย (.apk) แล้วจอมือถือของเหยื่อจะค้าง และโจรจะรีโมทมาควบคุมมือถือของเหยื่อ และโอนเงินออกทันที เช่นกรณี DSI, สรรพากร, Lion-Air, ไทยประกันชีวิต, กระทรวงพาณิชย์ (ยังคงเป็นรูปแบบที่มีจาชิปใช้มากที่สุด)

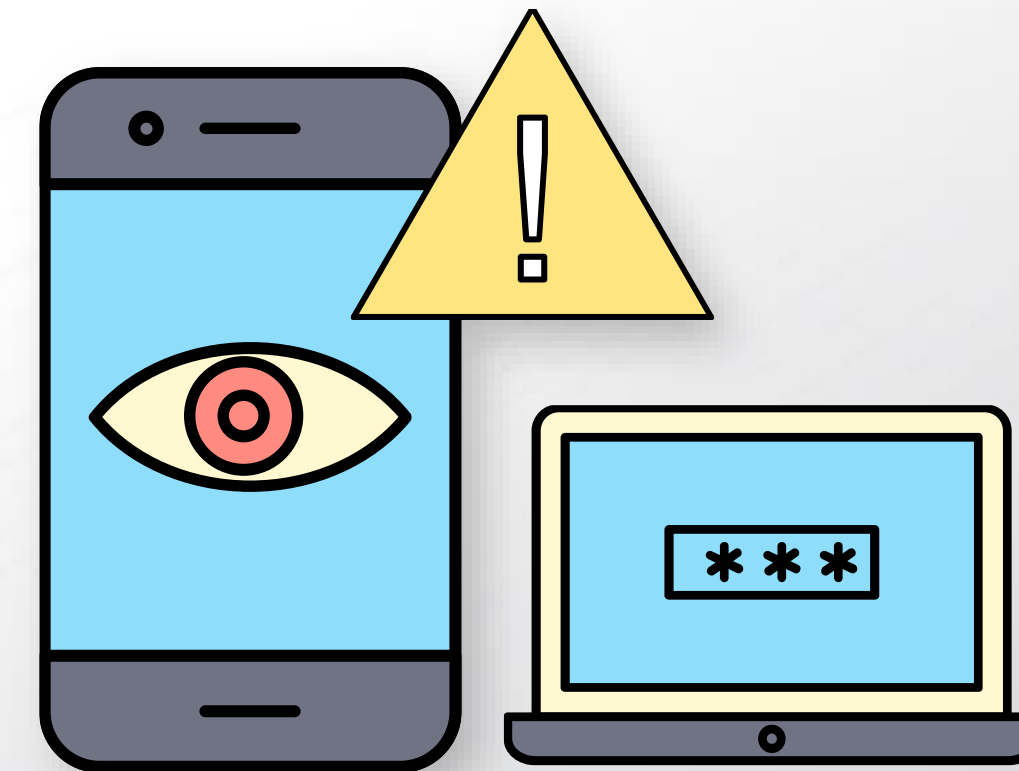
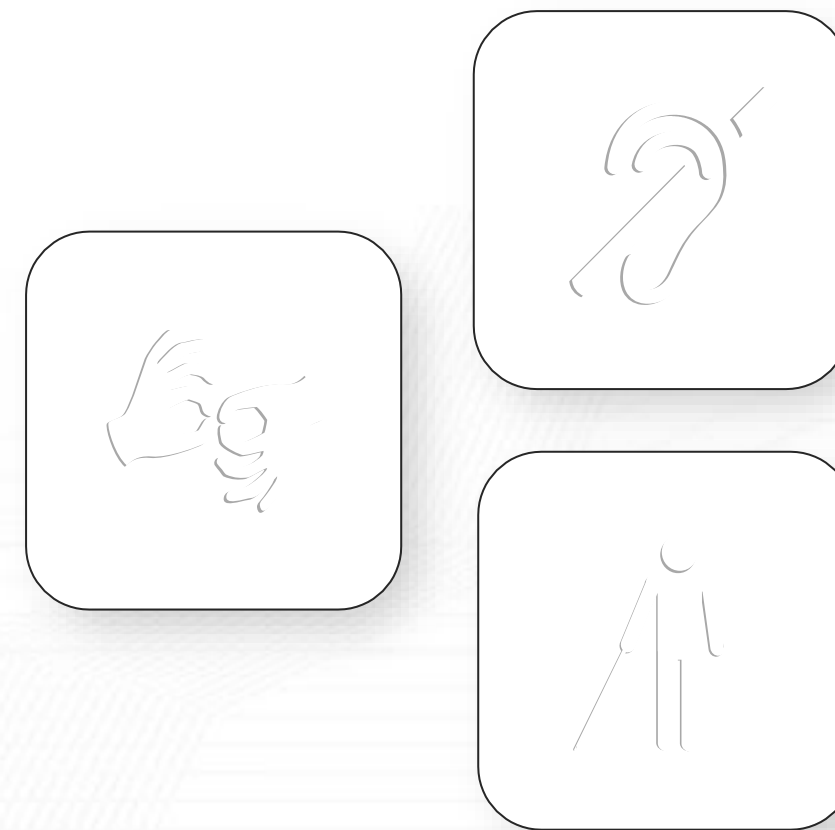


รูปแบบหลักของแอปดูดเงิน (หน้า 3/3)

3. หลอกให้เหยื่อทำตามเพื่อติดตั้งแอปพลิเคชันอันตราย (.apk) เพื่อควบคุมมือถือของเหยื่อ แต่โจรจะยังไม่โอนเงินทันที และรอประชาชนเผลอ แล้วแอบโอนเงินออกภายหลัง เช่น กรณีแอปหลอก Bumble, Snapchat (ยังคงเป็นรูปแบบที่มีจาชฟใช้)



มีจดาชีพใช้ การเข้าถึงแบบพิเศษ (Accessibility Service) เป็นกลไกหลัก

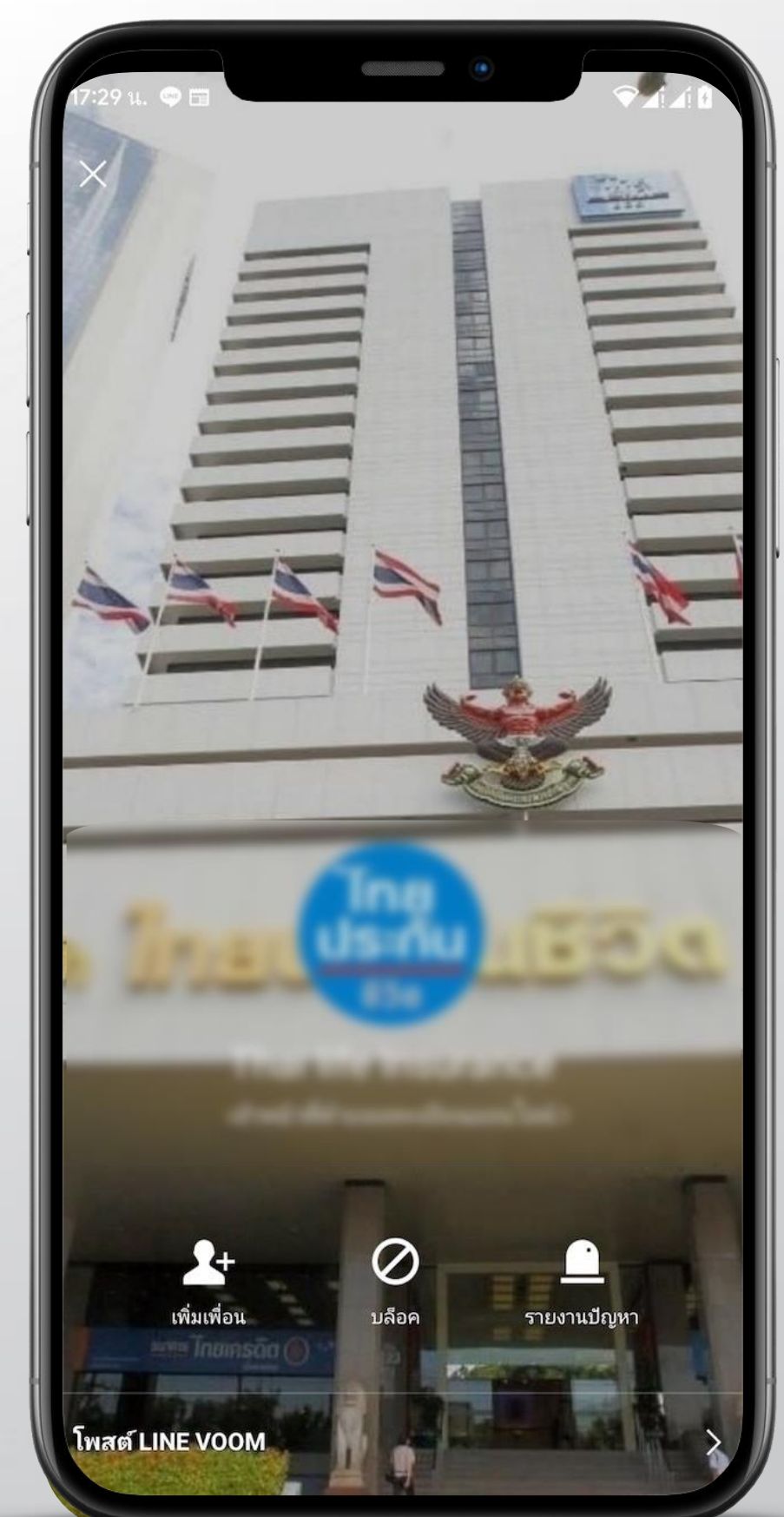
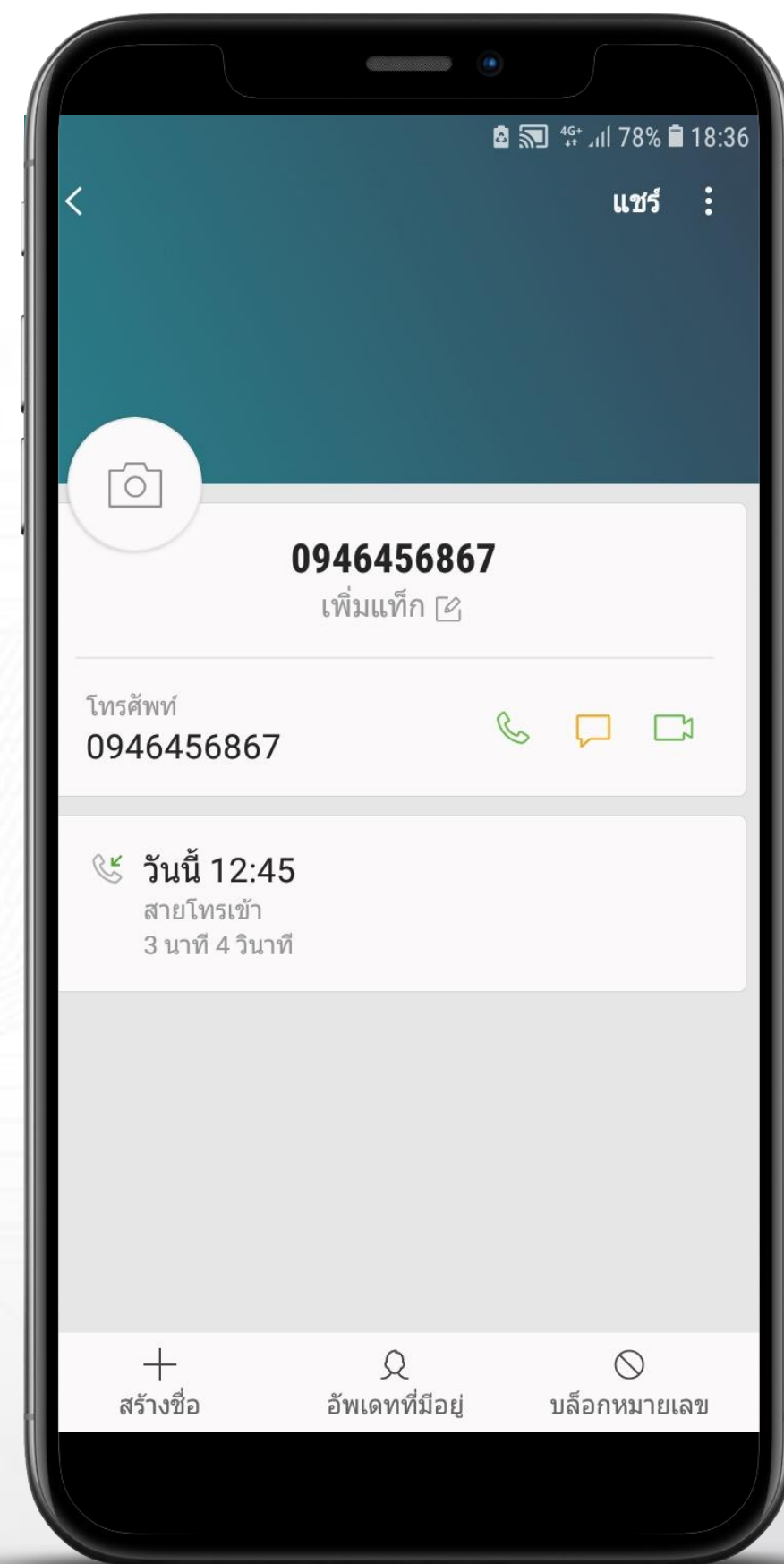


- Accessibility Service เป็นความสามารถพิเศษของระบบปฏิบัติการมือถือที่ เมื่อแอปพลิเคชันใด ๆ ได้รับอนุญาตให้ทำงานภายใต้ Accessibility Service แล้วจะสามารถเข้าถึงและควบคุมการส่งงานมือถือแทนผู้ใช้งานได้
- จริงๆ แล้ว Accessibility Service ถูกออกแบบมาเพื่อใช้ในการช่วยเหลือคนพิการหรือผู้ที่มีปัญหาในการสั่งการตามปกติ เช่น ช่วยอ่านเนื้อหาอีเมลให้ฟัง เขียนอีเมลให้ตามคำบอก สั่งการโปรแกรมประยุกต์ต่าง ๆ ด้วยเสียง เป็นต้น
- การที่มีจดาชีพจะควบคุมมือถือของเหยื่อได้ **มีจดาชีพจึงใช้วิธีการส่งแอปพลิเคชันปลอมเข้าเครื่องเหยื่อ** โดยการชวนเหยื่อพูดคุย และให้เหยื่อคลิกลิงก์เพื่อ download และ ติดตั้งแอปพลิเคชันของมีจดาชีพให้สามารถทำงานภายใต้ Accessibility Service บนมือถือของเหยื่อ หลังจากนั้นมีจดาชีพก็จะสามารถเข้ามาอ่านเนื้อหาที่แสดงบนหน้าจอของเหยื่อ แอบดักการพิมพ์ต่างๆ รวมถึงรหัสผ่านได้ทั้งหมด รวมถึงสามารถสั่งการกดหน้าจอแทนผู้ใช้งานได้โดยสมบูรณ์

ขั้นตอนการโจมตี Step by Step (หน้า1/9)

STEP

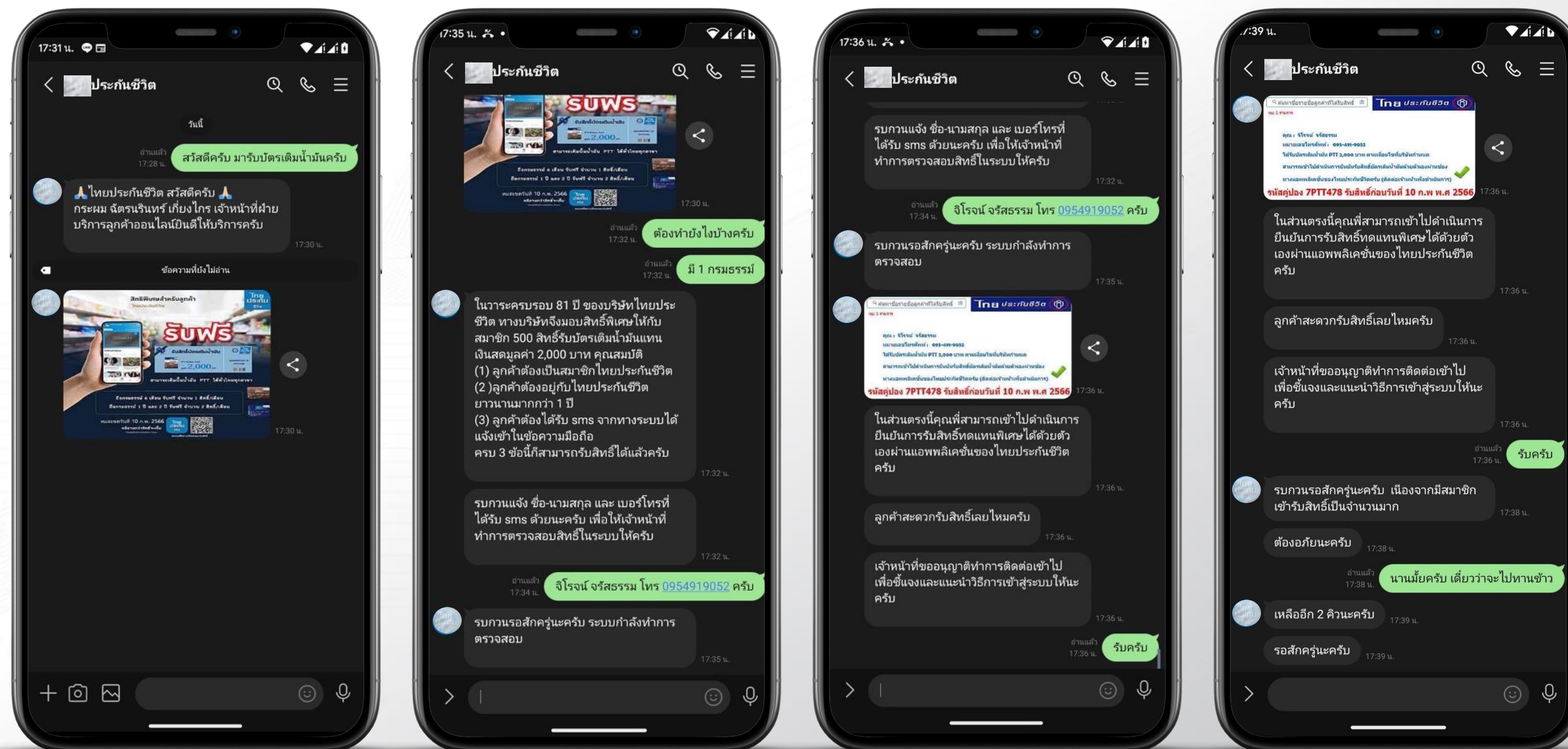
1. ติดต่อ ให้ตายใจ



ขั้นตอนการโจมตี Step by Step (หน้า 2/9)

STEP

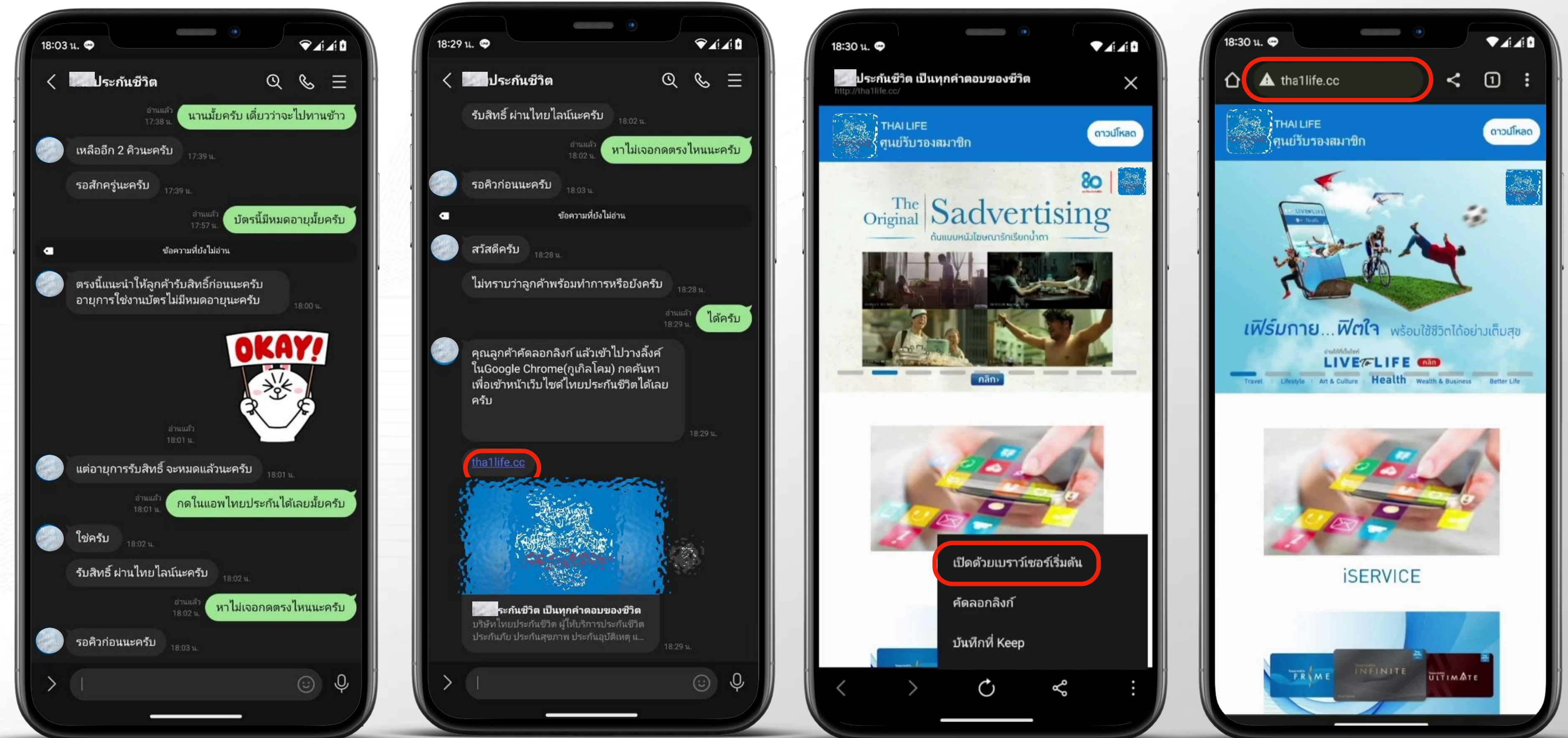
2. ชวนแอด ไลน์ไป คุยต่อ



ขั้นตอนการโจมตี Step by Step (หน้า 3/9)

STEP

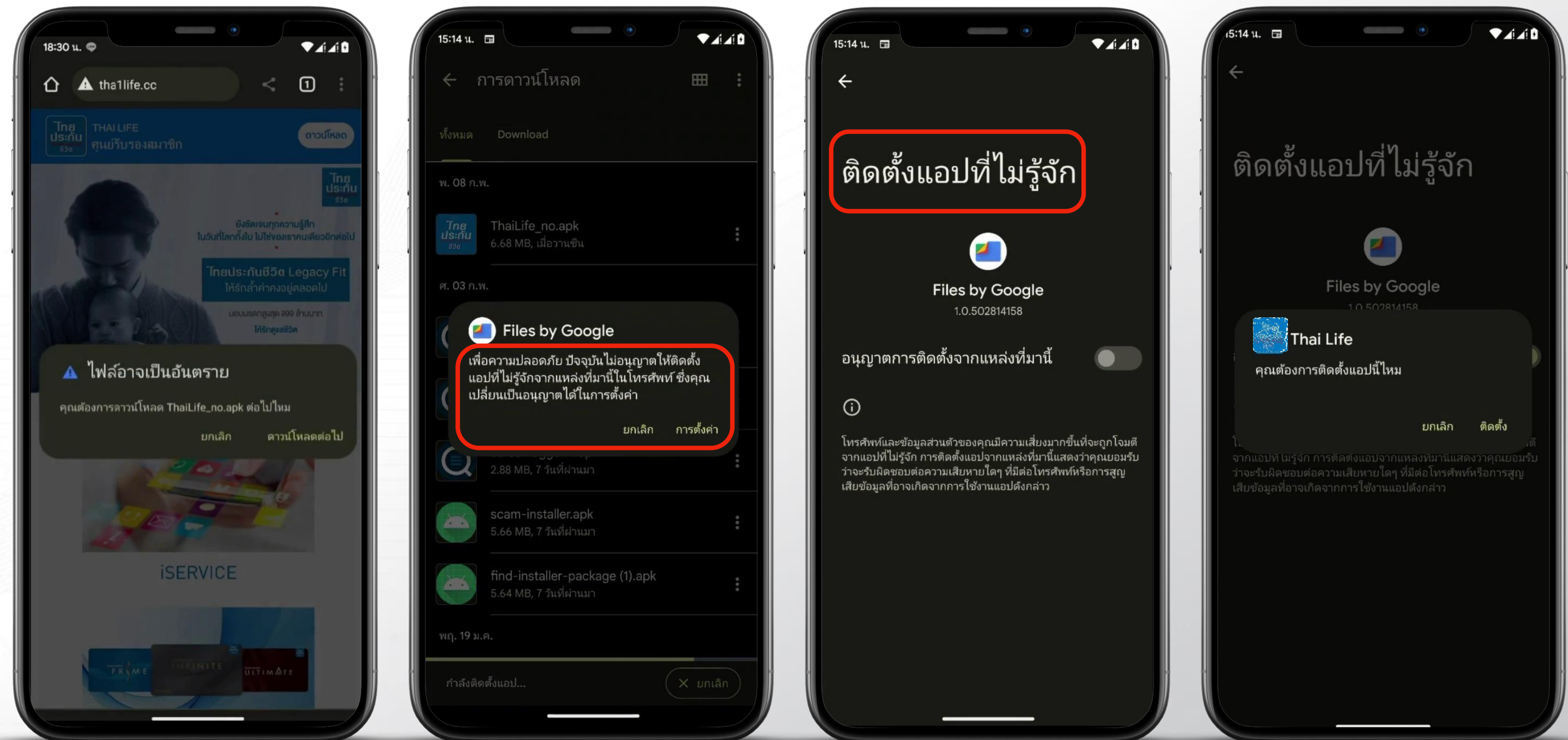
3. หลอกติดตั้งแอปโจร



ขั้นตอนการโจมตี Step by Step (หน้า 4/9)

STEP

3. หลอกติดตั้งแอปโจร

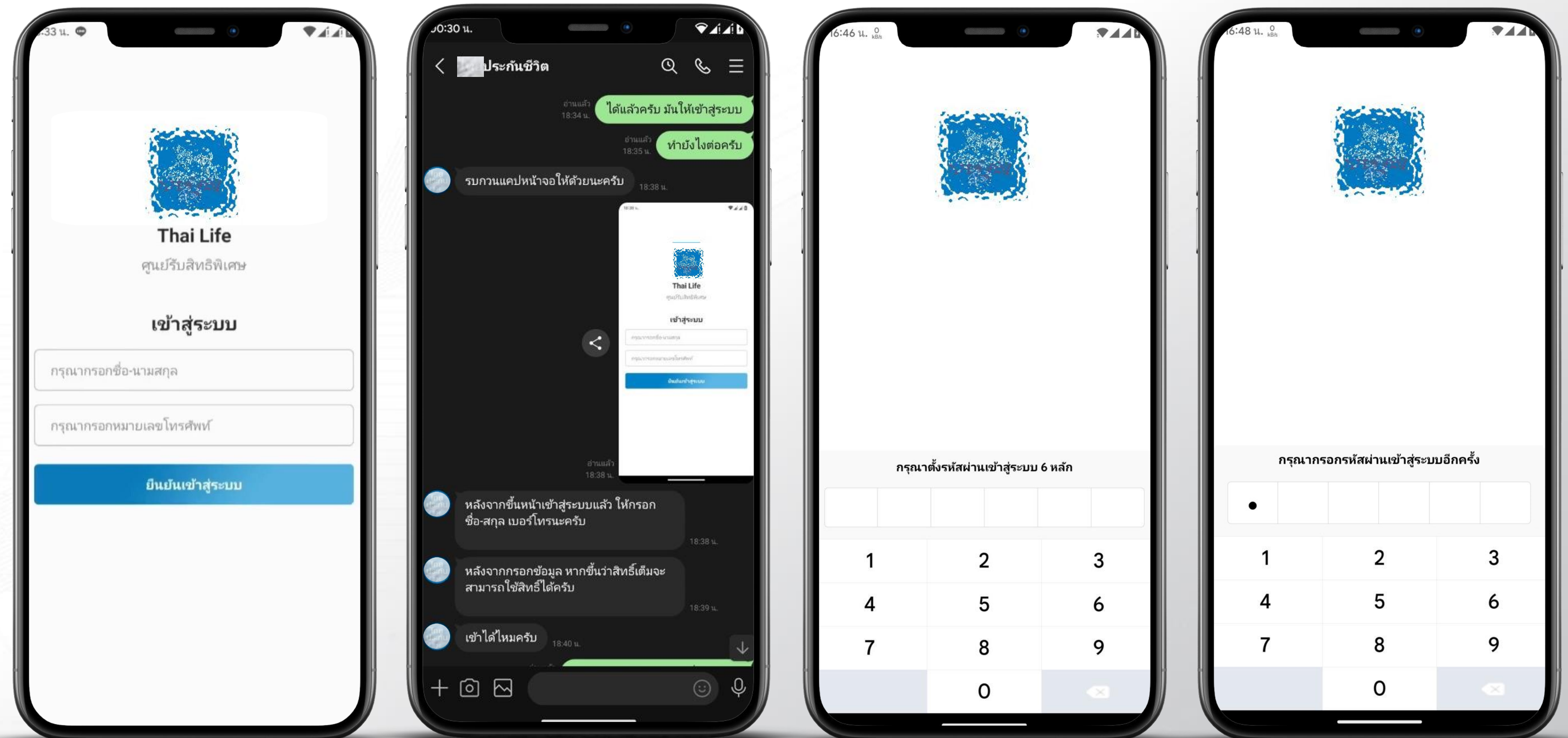


ขั้นตอนการโจมตี Step by Step (หน้า 5/9)

STEP

4.

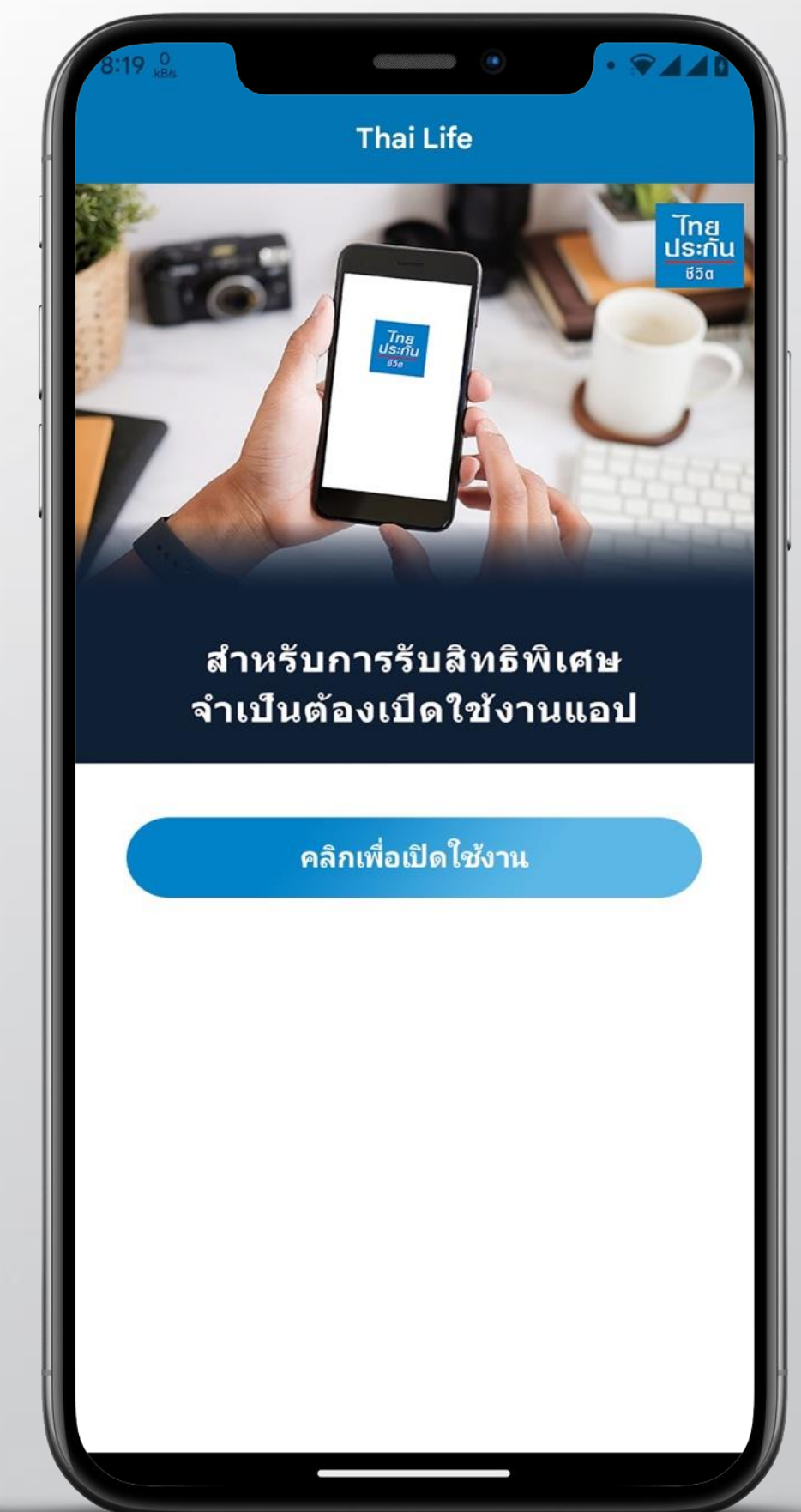
หลอกให้ตั้งรหัสผ่าน



ขั้นตอนการโจมตี Step by Step (หน้า 6/9)

STEP

4. คลอก ให้ตั้ง รหัสผ่าน



ขั้นตอนการโจมตี Step by Step (หน้า 7/9)

STEP

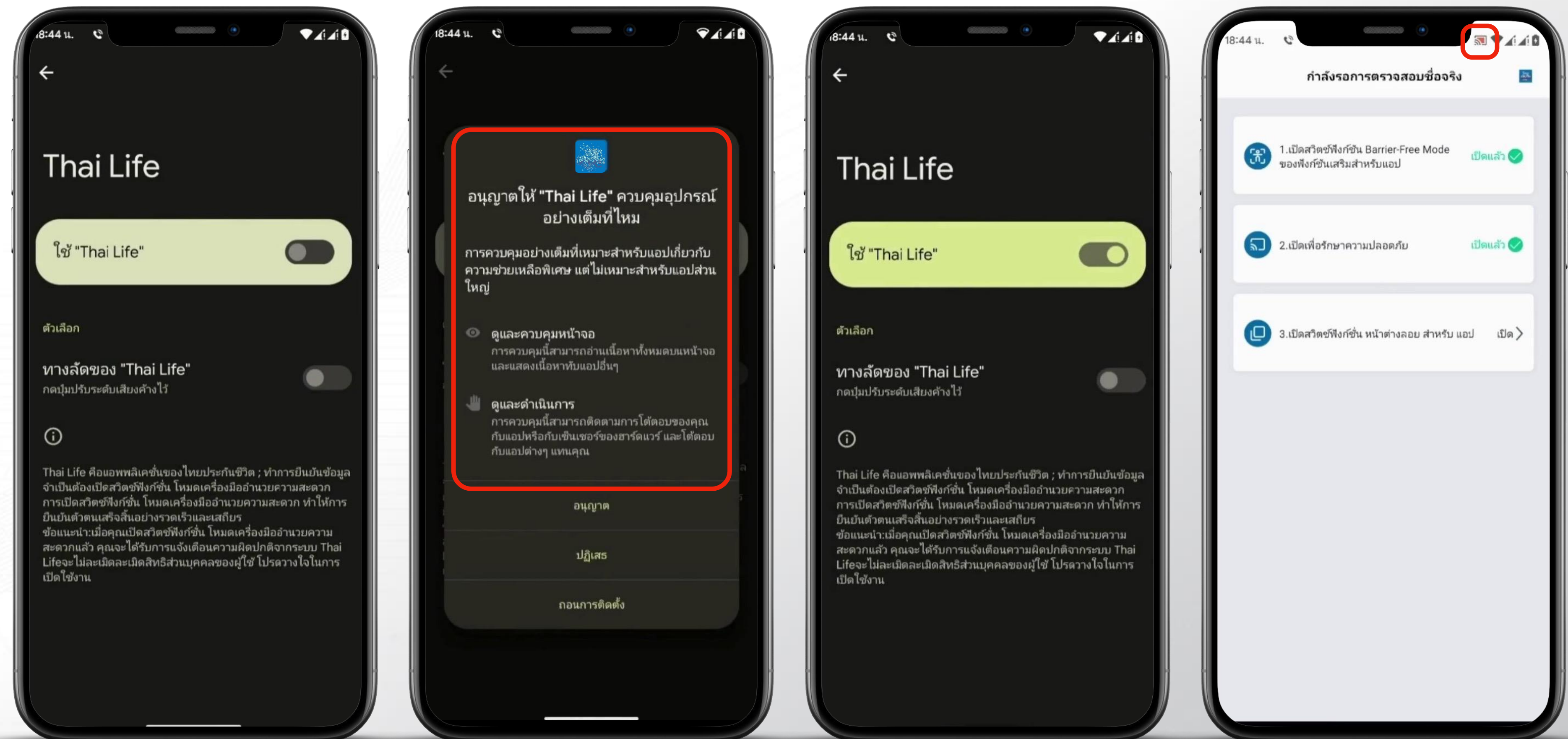
5. ขอสิทธิ์ควบคุมอุปกรณ์



ขั้นตอนการโจมตี Step by Step (หน้า 8/9)

STEP

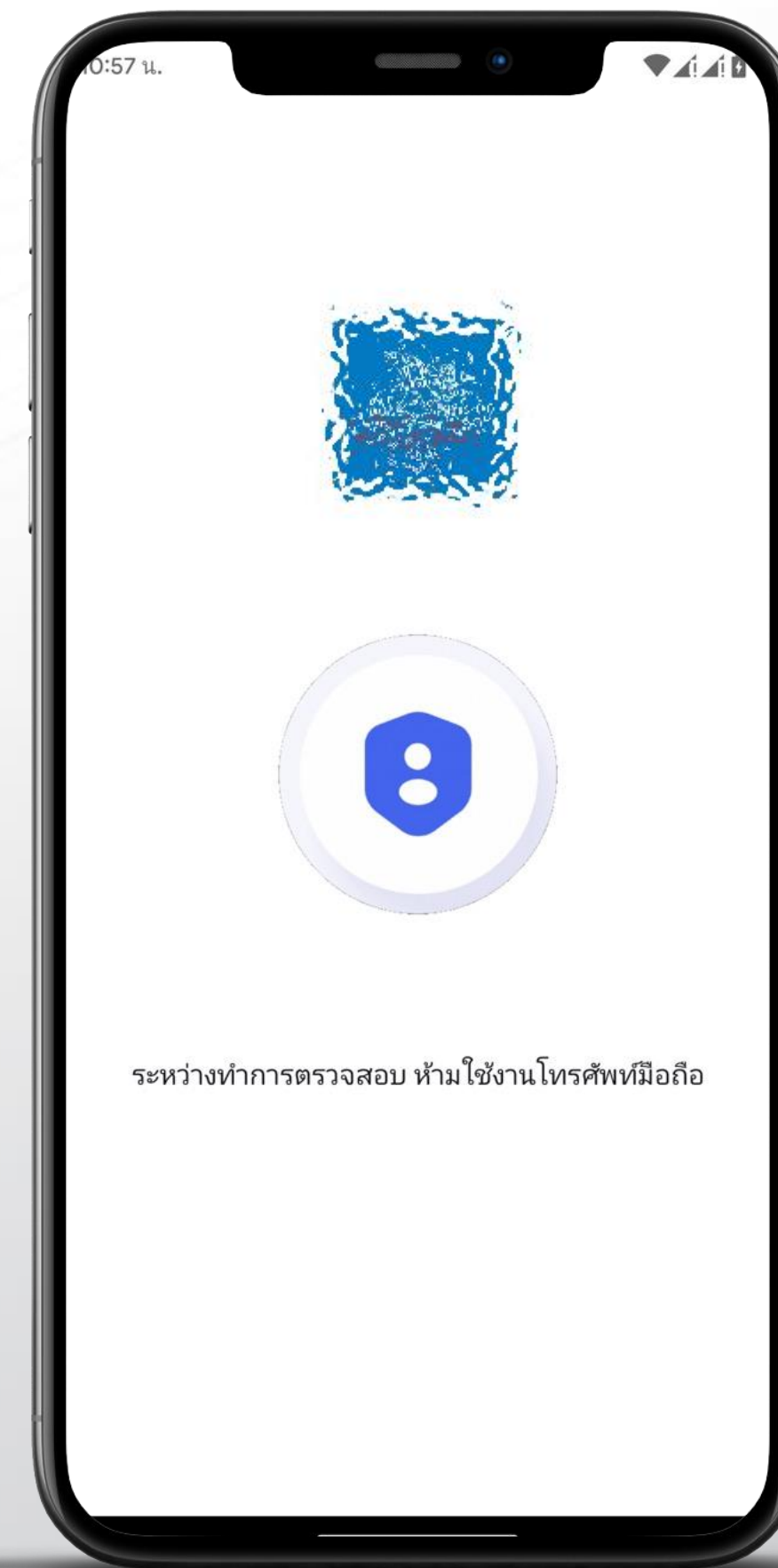
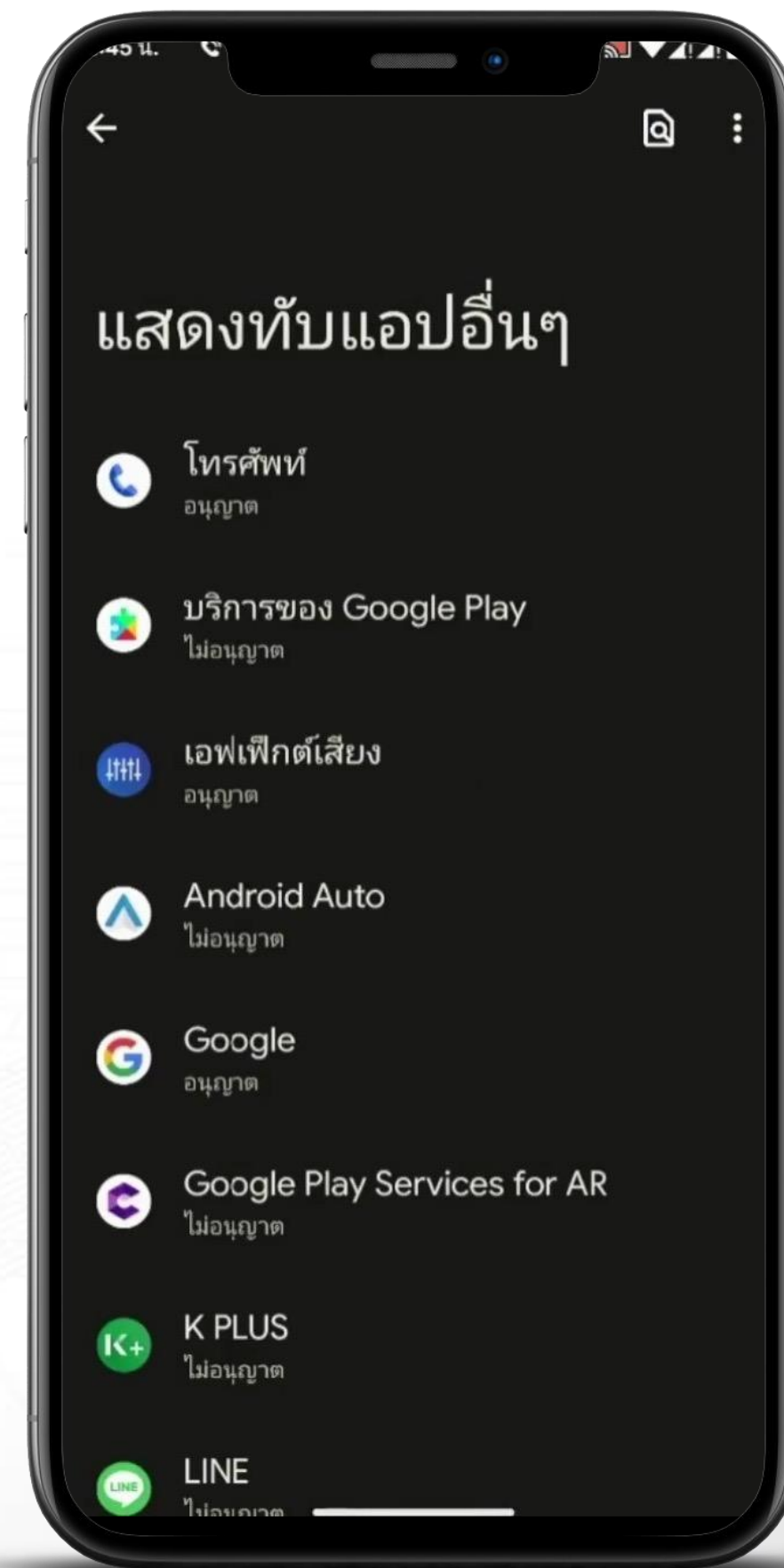
5. ขอสิทธิ์ควบคุมอุปกรณ์



ขั้นตอนการโจมตี Step by Step (หน้า 9/9)

STEP

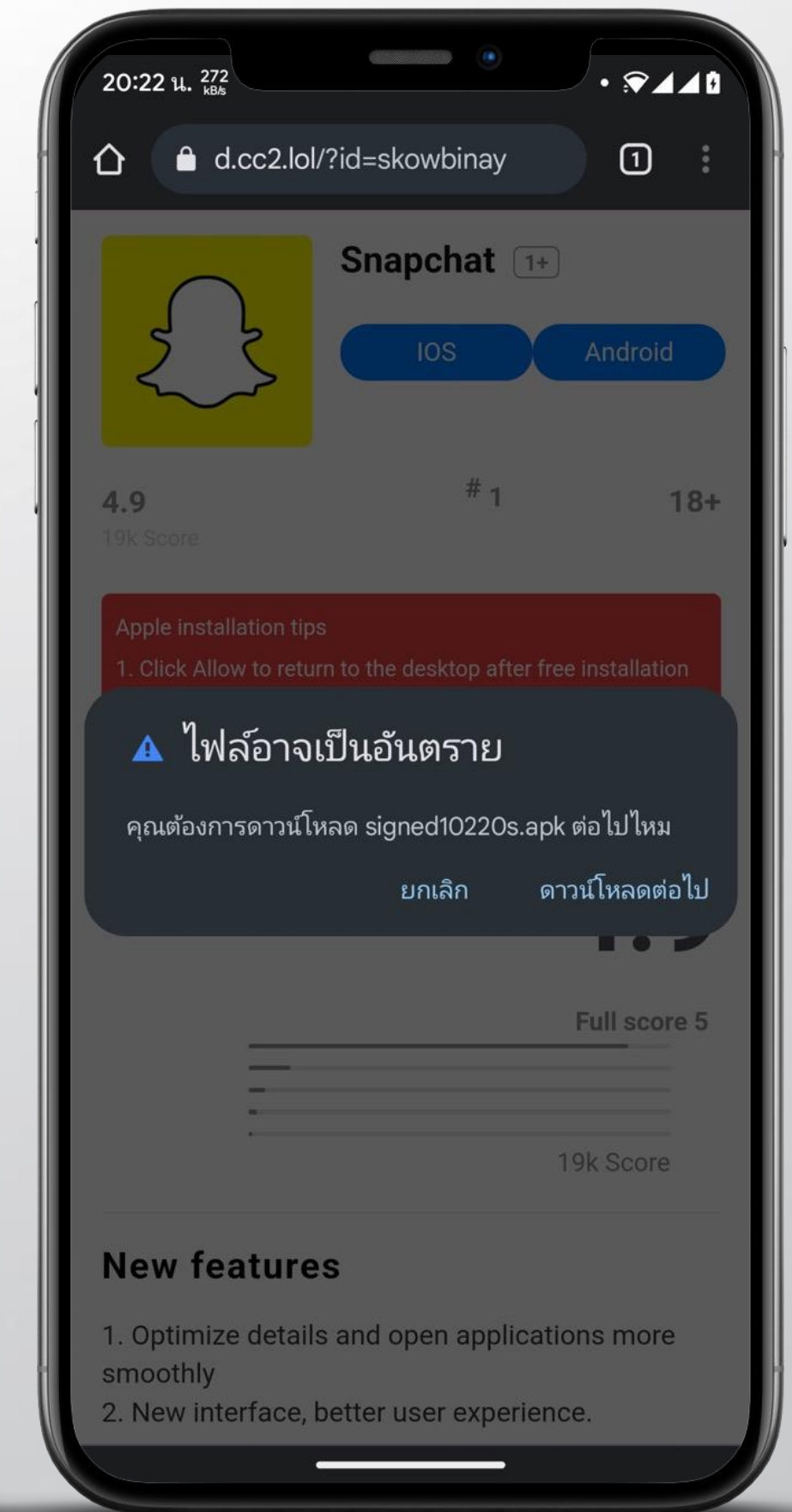
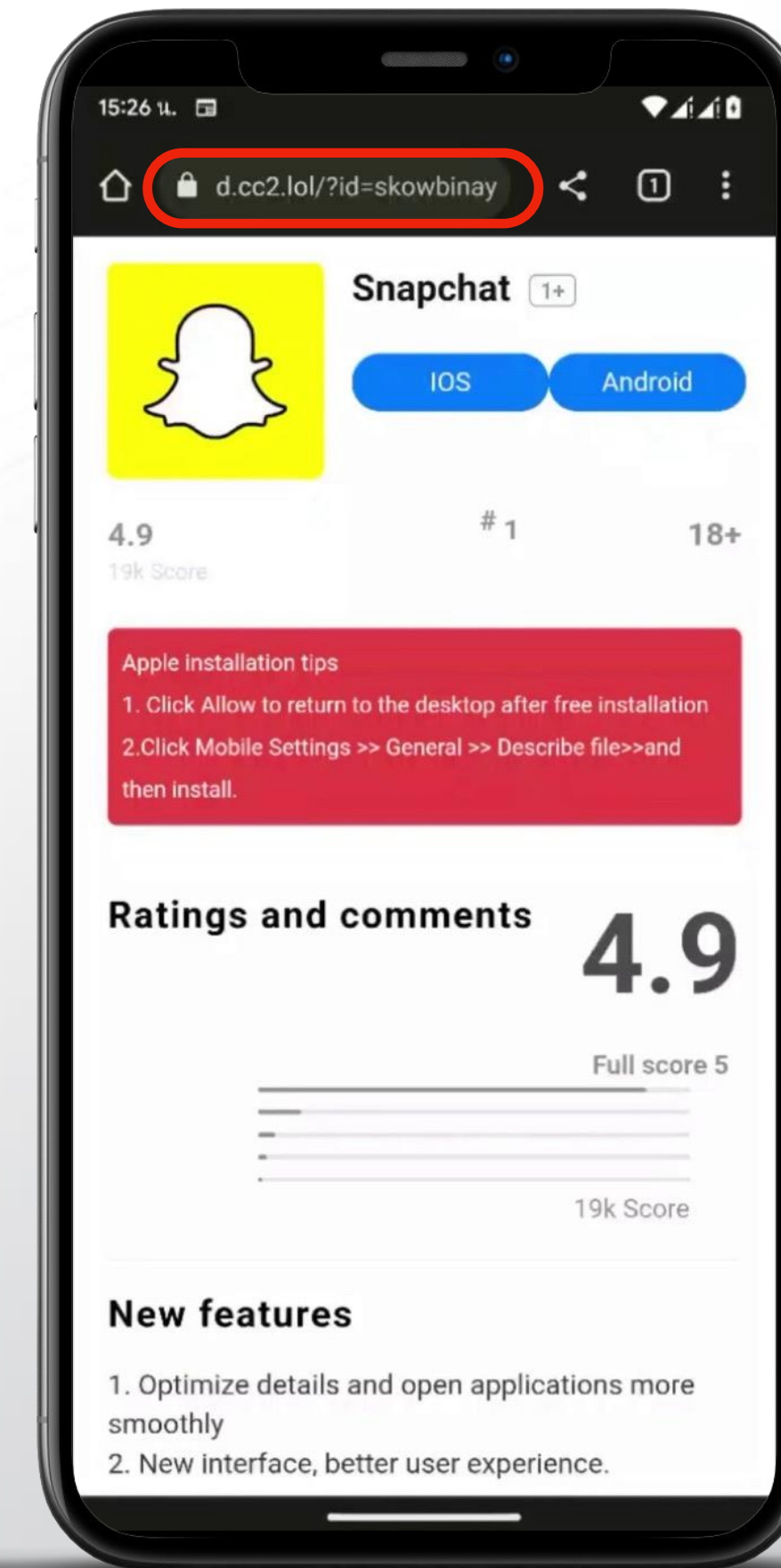
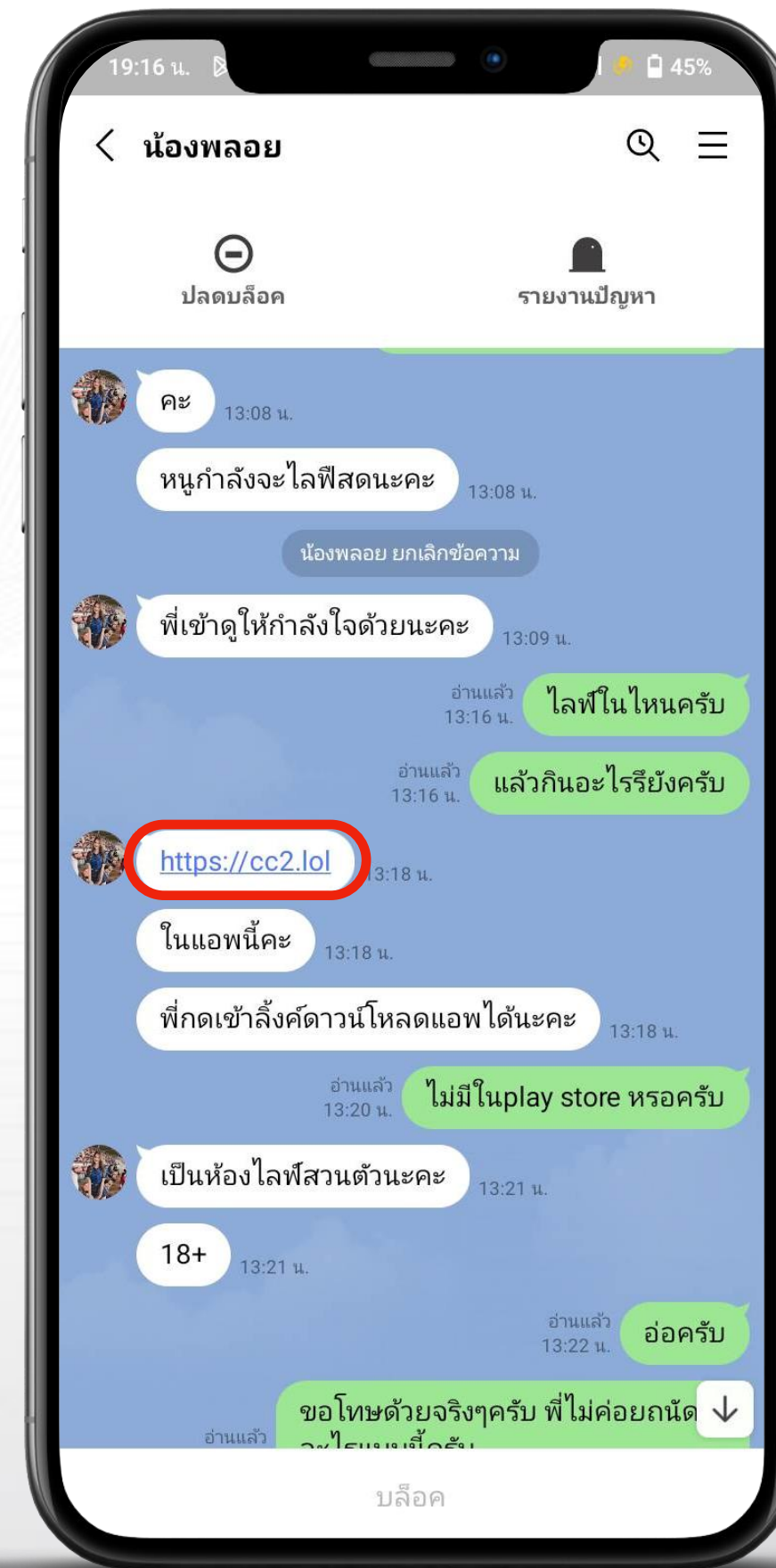
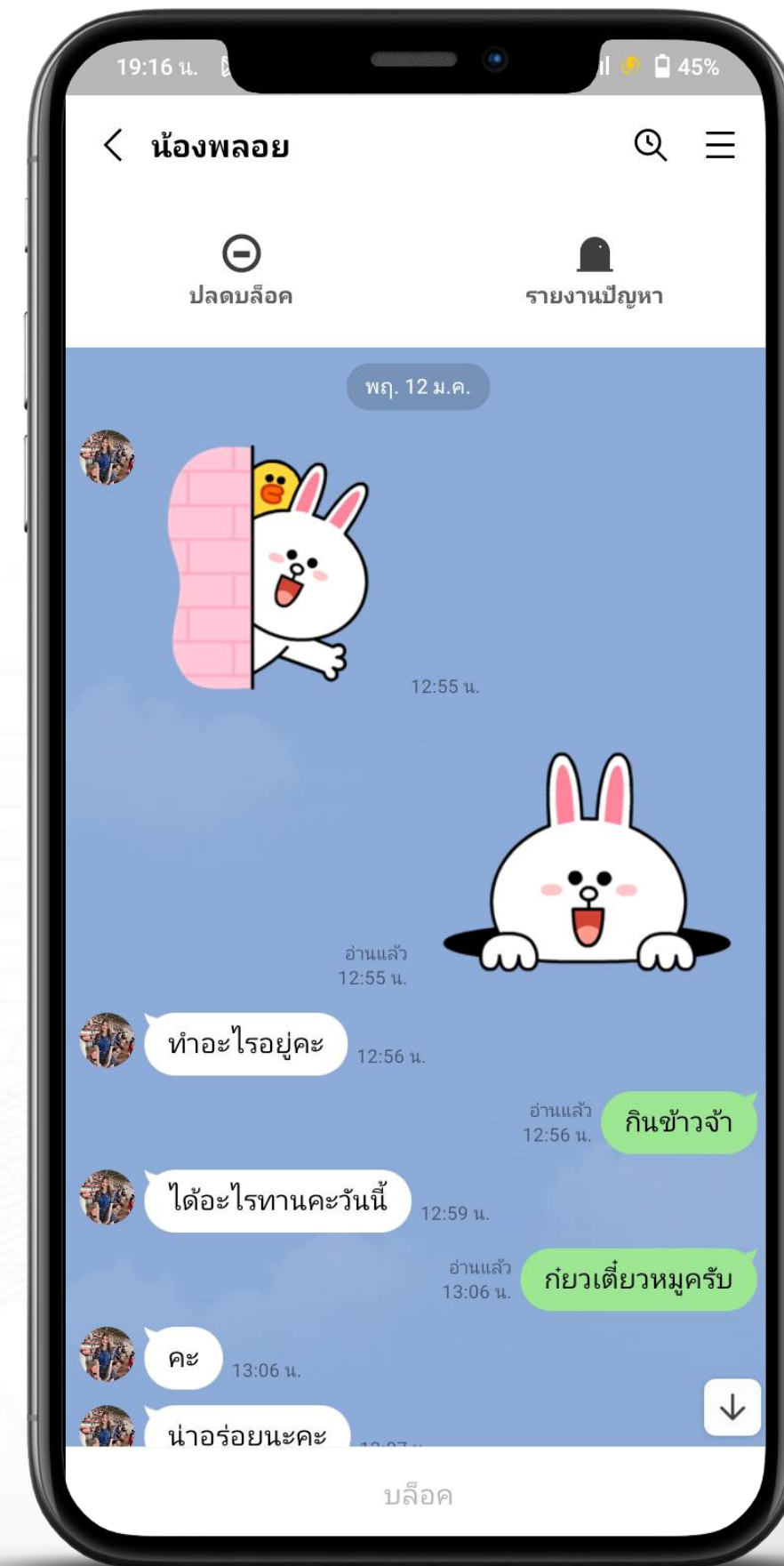
6.
ล็อกจอ
แล้ว
ขโมย
เงิน



ขั้นตอนการโจมตี (กรณีเป็นรูปแบบของแอปที่ไม่โอนเงินออกทันที หน้า1/4)

STEP

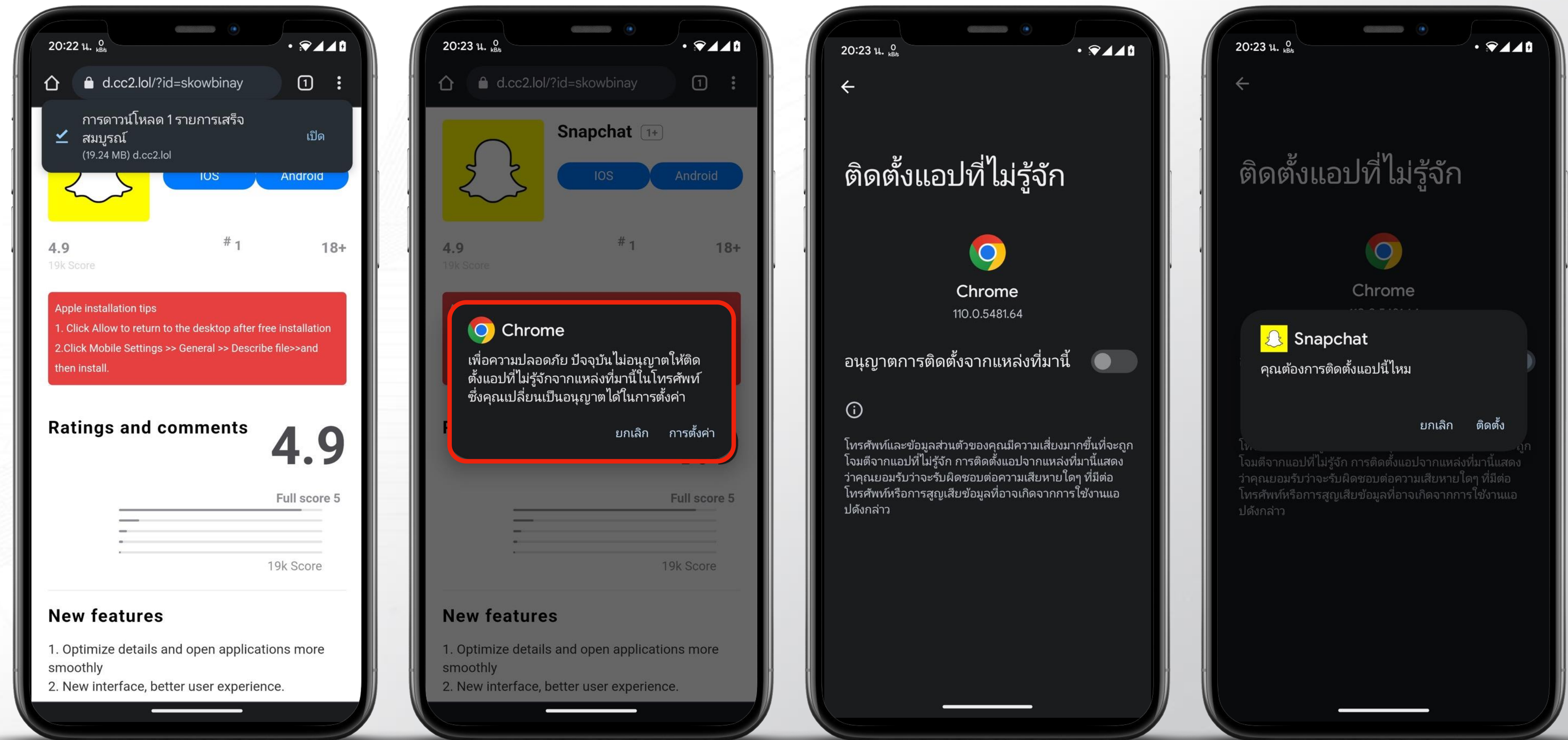
1. ติดต่อให้ตายใจ
2. ชวนแอดไลน์ไปคุยต่อ
3. หลอกติดตั้งแอปโจร



ขั้นตอนการโจมตี (กรณีเป็นรูปแบบของแอปที่ไม่โอนเงินออกทันที หน้า 2/4)

STEP

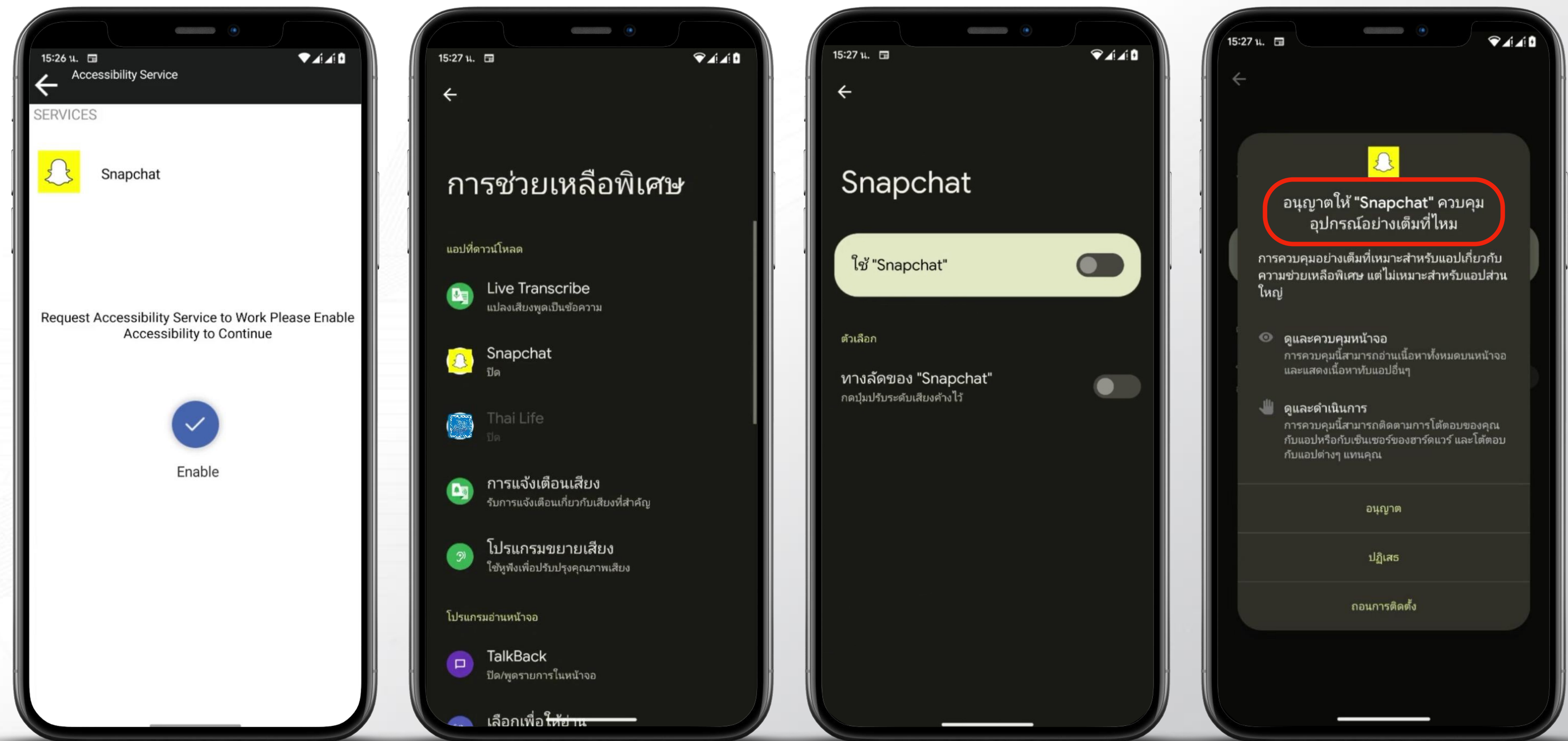
3. หลอกติดตั้งแอปโจร



ขั้นตอนการโจมตี (กรณีเป็นรูปแบบของแอปที่ไม่โอนเงินออกทันที หน้า3/4)

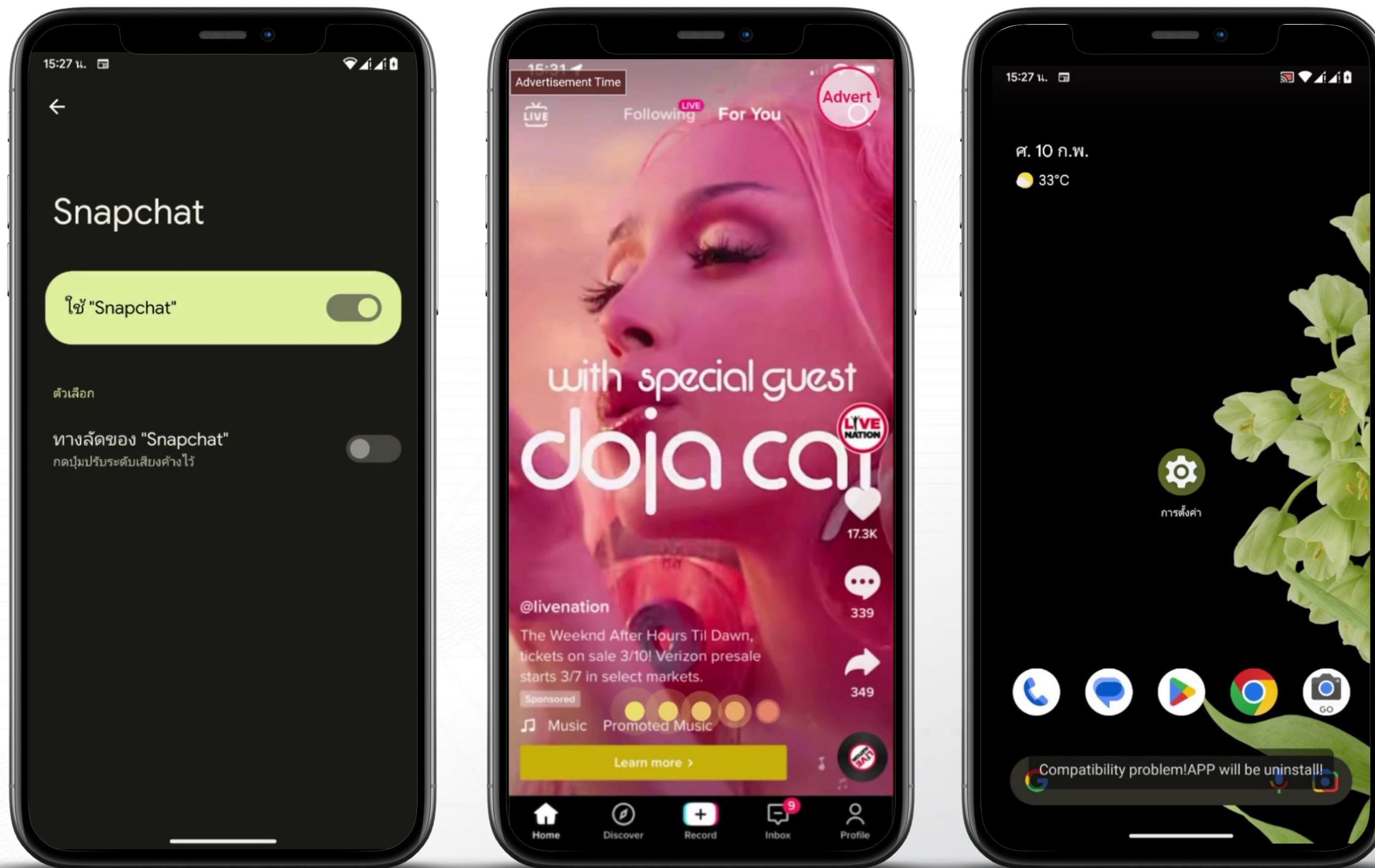
STEP

5. ขอสิทธิ์ ควบคุม อุปกรณ์



ขั้นตอนการโจมตี (กรณีเป็นรูปแบบของแอปที่ไม่โอนเงินออกทันที หน้า4/4)

ข้อสังเกต



✗ STEP 4.

ไม่มีหน้าจอหลอกให้
ผู้ใช้ตั้งรหัสผ่าน

✗ STEP 6.

แจ้งว่าติดตั้ง
ไม่สำเร็จ และจอค้าง

เหตุจูงใจหลัก ๆ ที่ทำให้หลอกล

- รัก หลอกให้รักและเชื่อใจ
- โลก หลอกล่อด้วยของแถม ของฟรี เงินคืน หรือ ลงทุนได้ผลตอบแทนดี
- กลัว หลอกให้กลัวว่าจะต้องถูกดำเนินคดี ถูกปรับ เคยหลบเลี่ยงภาษี ถ้าไม่ทำ ก็กลัวความผิดตามที่ถูกกล่าวอ้าง
- หลง หลอกให้หลง งมงายในกาม เช่น ให้อู live สด 18+

กลยุทธ์หรือยุทธวิธี
ที่มีจวิชาชีพใช้ประกอบการชักจูง



Urgency



Misdirection



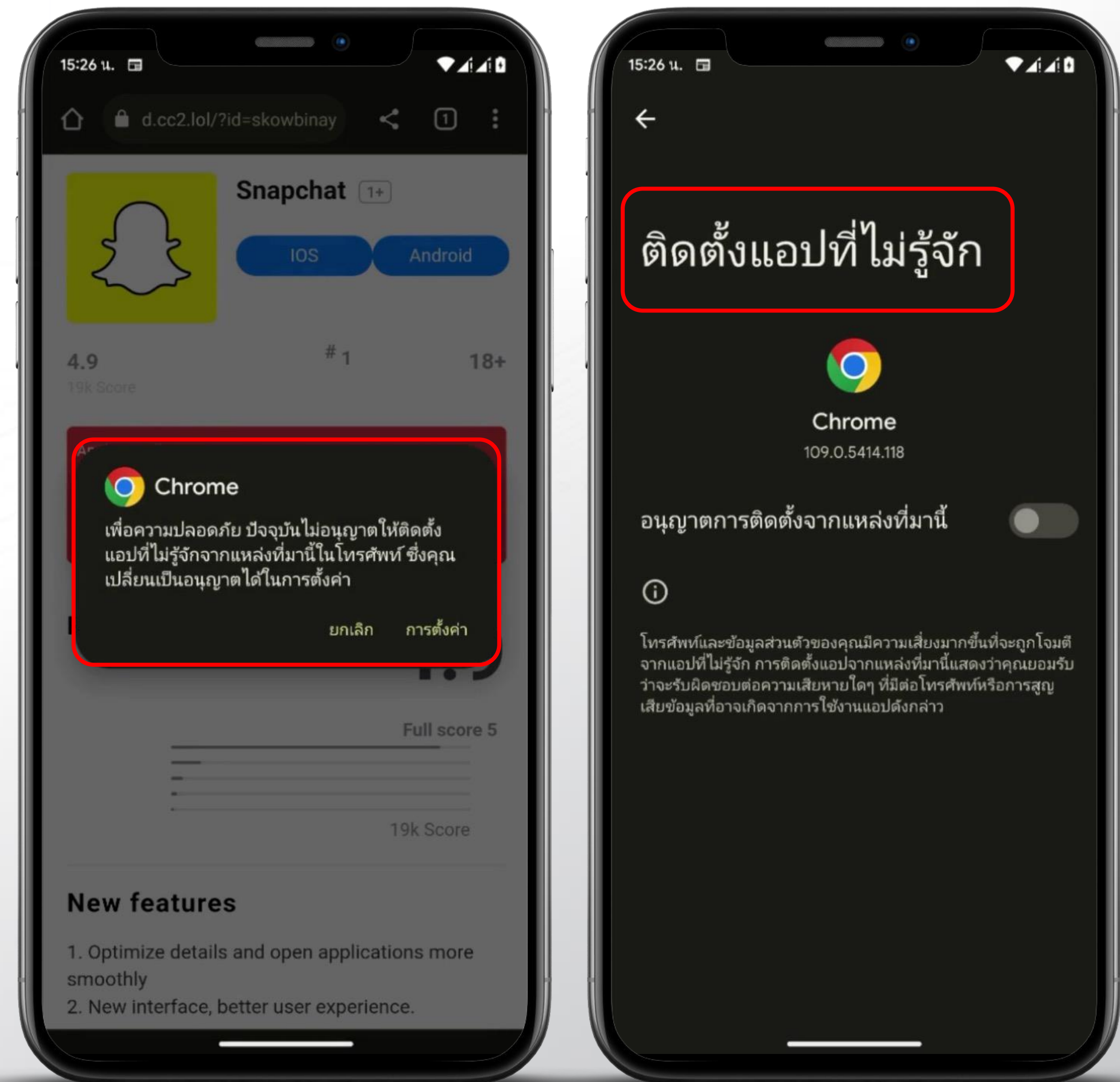
Sympathy



Authority

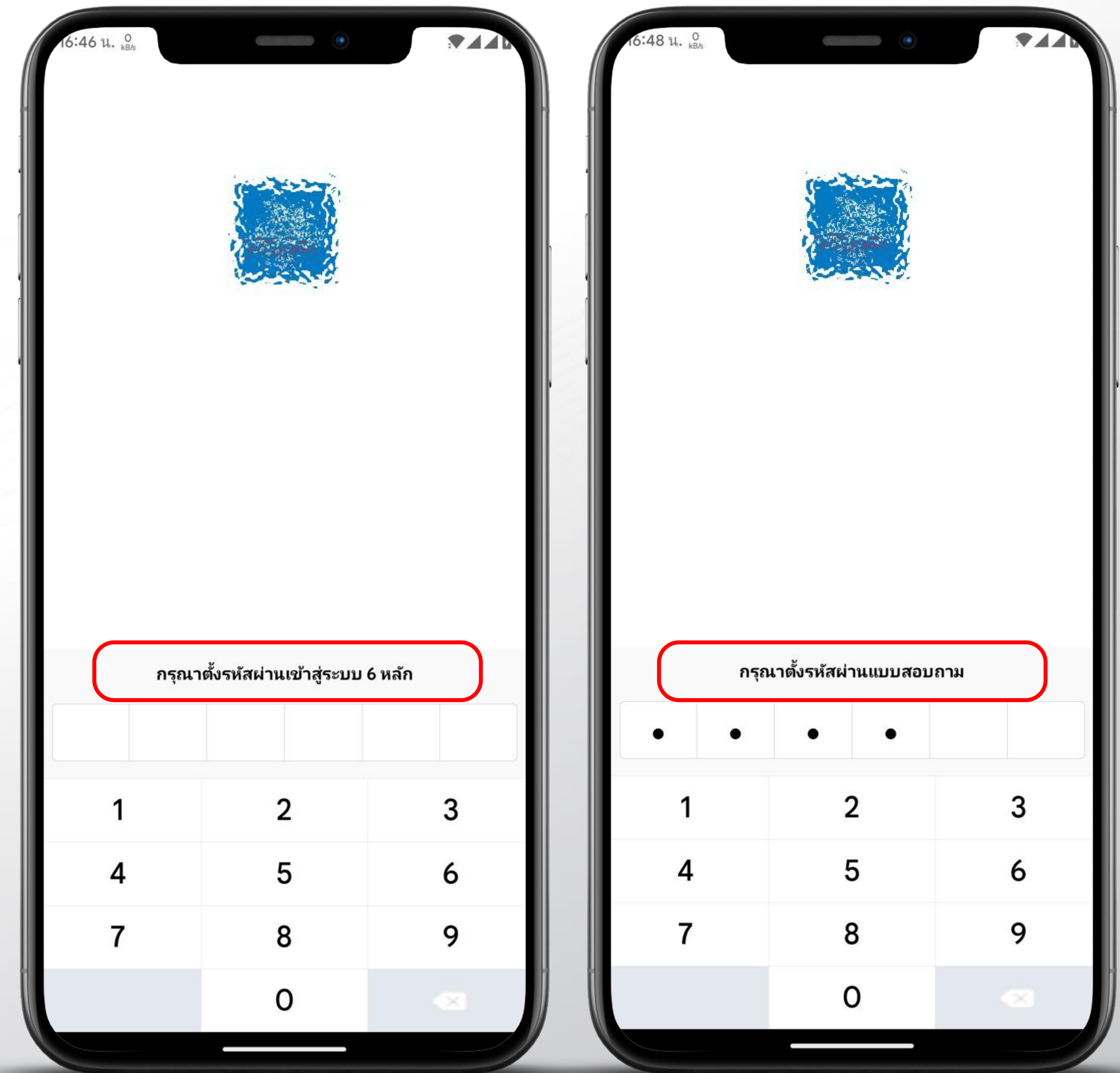
จุดสังเกตสำคัญ
ที่ต้องระวังไม่ให้หลงกล

2.
ขณะทำการติดตั้งโปรแกรม
จะต้องเปิดสิทธิ์ในการ
ติดตั้งแอปที่ไม่รู้จัก



จุดสังเกตสำคัญ
ที่ต้องระวังไม่ให้หลงกล

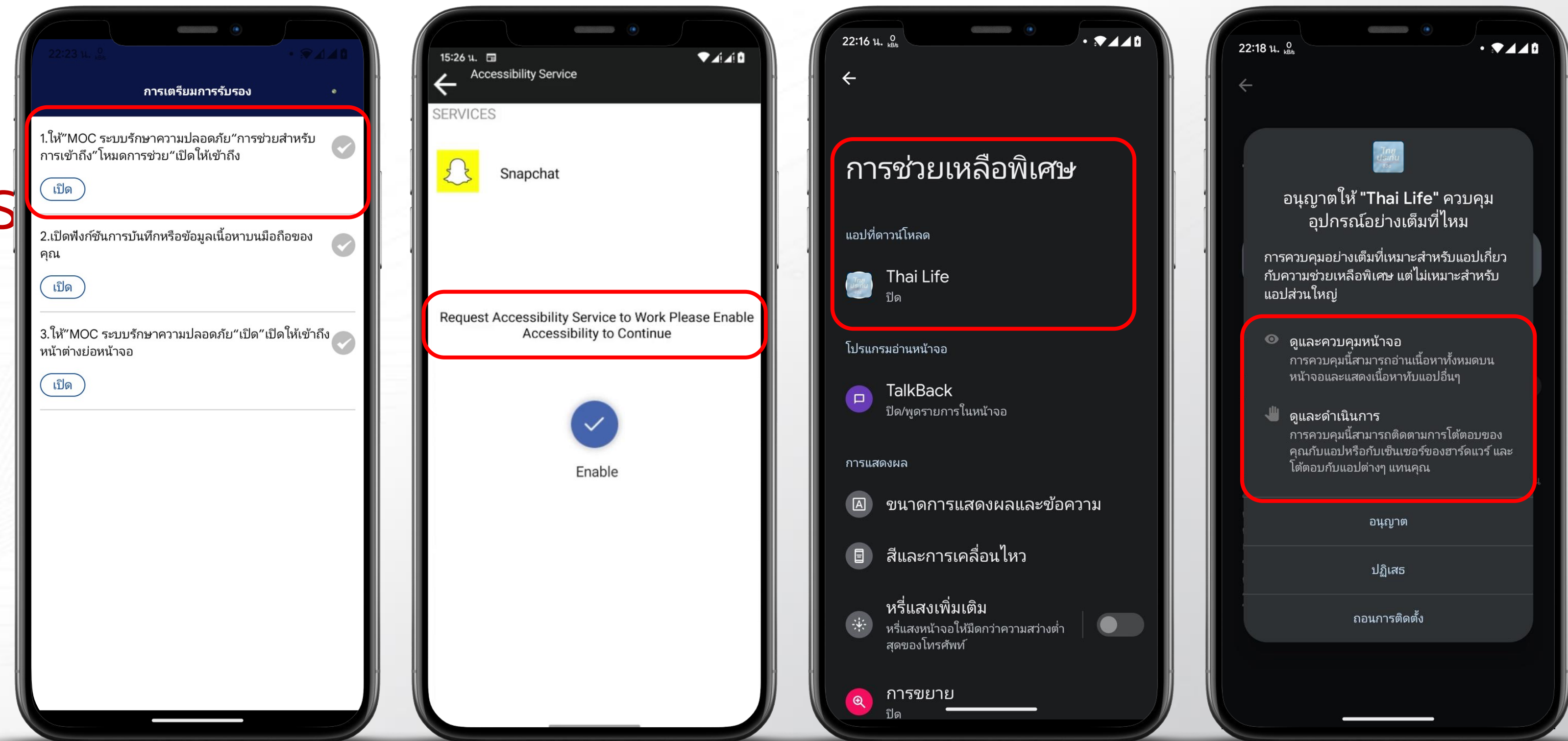
3.
มีจาชีพพยายามให้ตั้ง
PIN หลายครั้ง หวังให้
เหยื่อเผลอตั้ง PIN ชำ
กับรหัสผ่านธนาคาร



จุดสังเกตสำคัญ ที่ต้องระวังไม่ให้หลงกล

4.

หลอกให้เหยื่อเปิดสิทธิ์ การ
 ช่วยเหลือพิเศษ
 (Accessibility)
 โดยชวนคุย
 จนเหยื่อหลงเชื่อ

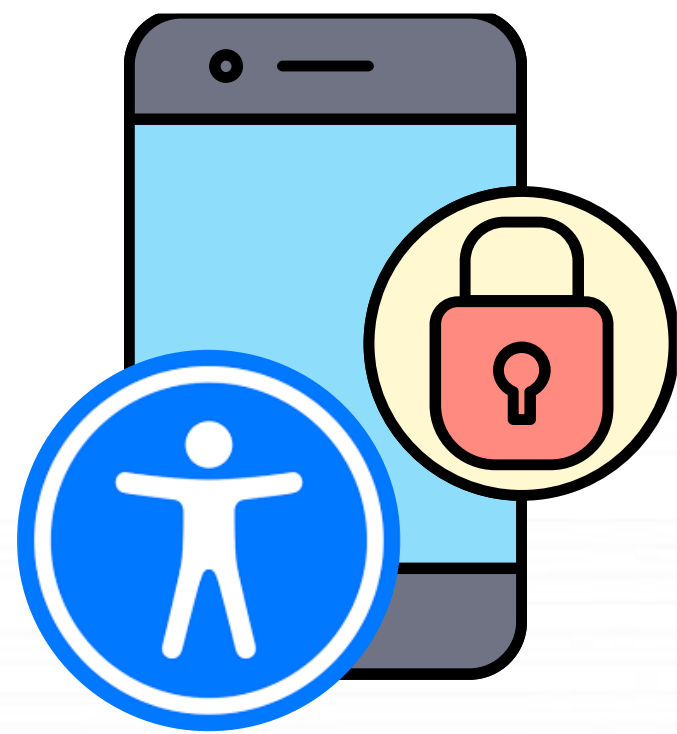


จุดสังเกตสำคัญ ที่ต้องระวังไม่ให้หลงกล

1. ต้องการ Download App ให้ทำจาก app store หรือ play store เท่านั้น 
2. หากเราไม่ได้เกี่ยวข้องกับเรื่องที่ถูกกล่าวอ้างก็ไม่ต้องสนใจสิ่งที่เค้ากำลังขู่เรา
3. ของฟรีไม่มีในโลก ดังนั้นอย่าหลงกลเชื่อว่าจะได้ของแถมของฟรี หรือคูปองส่วนลด
4. ส่วนใหญ่จะให้ Add  หรือ ช่องทาง chat อื่น ๆ เช่น whatsapp, viber หรือ อื่น ๆ เพื่อคุยสร้างความน่าเชื่อถือ ดังนั้น ห้าม add line หรือช่องทาง chat อื่น ๆ คุยกับคนแปลกหน้า
5. มิจฉาชีพจะพยายามสร้างความน่าเชื่อถือโดยการอ้างอิงข้อมูลของเรา ซึ่งปัจจุบันข้อมูลส่วนตัวเราน่าจะกระจายอยู่ทั่ว
6. มิจฉาชีพจะพยายามสร้างความน่าเชื่อถือโดยการอ้างอิงข้อมูลของหน่วยงานนั้น เช่น หมายเลข ID ของผู้ให้บริการ, ใบธุรกิจการค้า, ใบภพ 20 เป็นต้น

** ส่วนใหญ่คนที่เป็นเหยื่อในรุ่นแรก ๆ คือ มีบางอย่างเกี่ยวข้องกับสิ่งที่มิจฉาชีพแอบอ้าง อย่างเช่น แม่ค้าขายของหรือร้านค้าที่ไม่เสียภาษี หรือเสียภาษีบางส่วน พอมีมิจฉาชีพโทรมา (ส่มโทร) บังเอิญเป็นเราพอดีที่เกี่ยวกับเรื่องนี้ ก็จะตกเป็นเหยื่อเชื่อมิจฉาชีพและหลงทำตาม

วิธีการตรวจสอบว่ามือถือเรา ปลอดภัยจากแอปดูดเงินหรือไม่

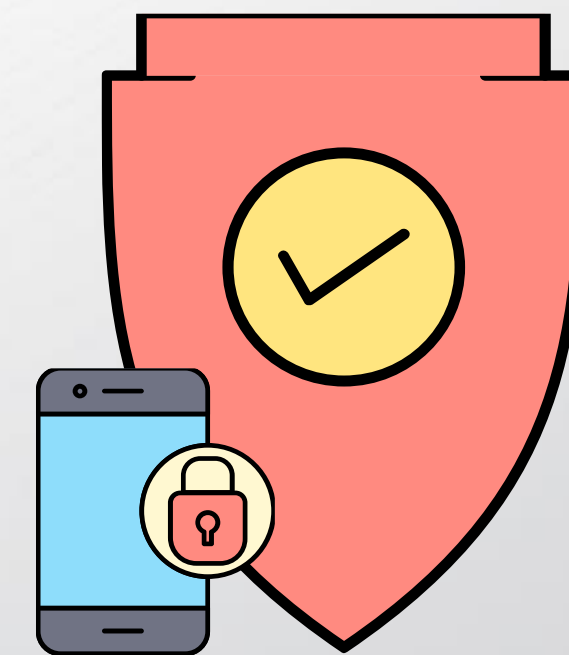


1. ตรวจสอบว่ามีเปิดแอปพลิเคชันที่ทำงานภายใต้ Accessibility Service ที่เราไม่ได้ตั้งใจจะเปิดใช้หรือไม่



Google Play
Protect

2. ใช้ Google Play Protect ในการ scan หาแอปพลิเคชันอันตรายอยู่เสมอ

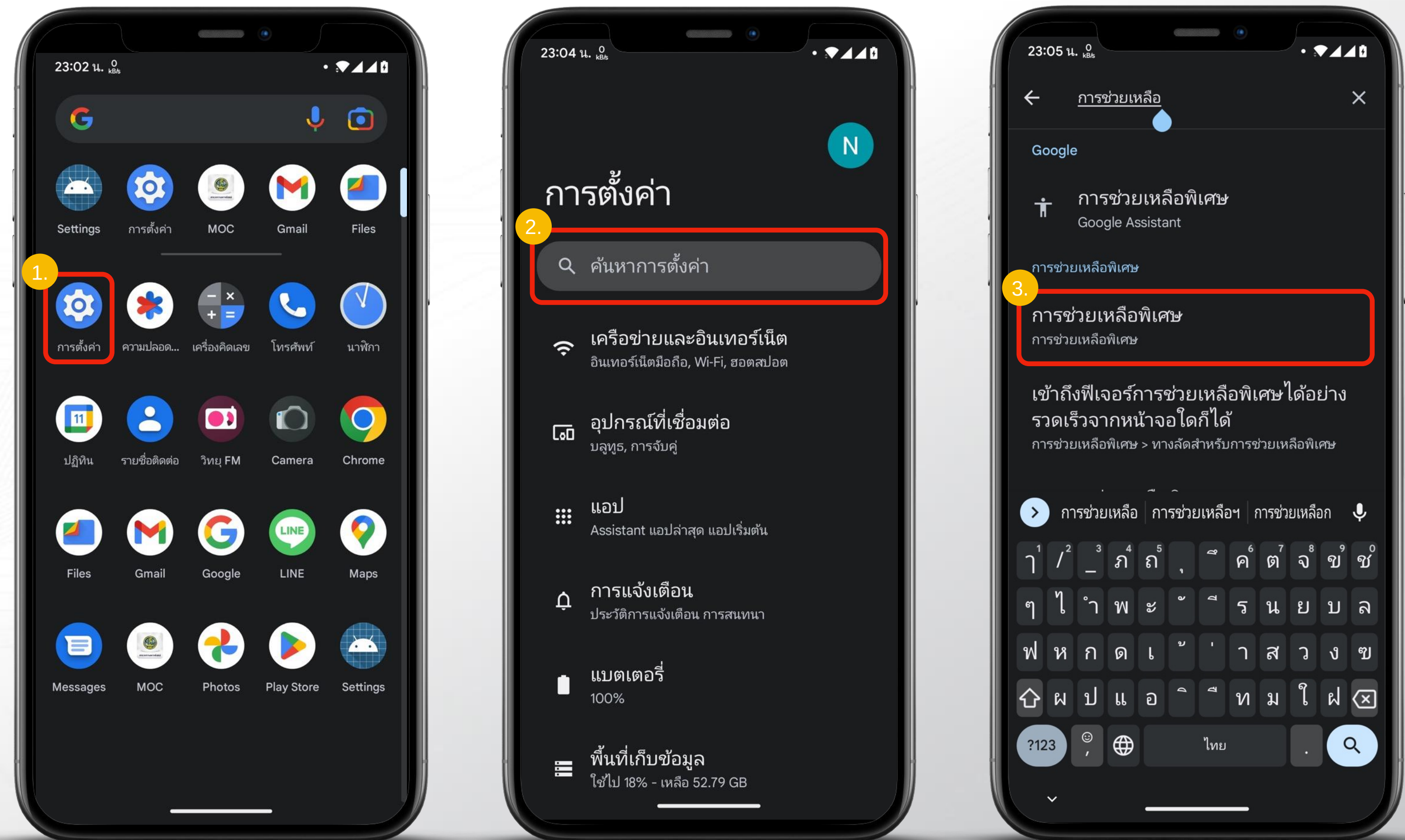


3. มือถือมีการติดตั้ง End Point Protection /Antivirus หรือไม่ หากไม่มีแนะนำให้ติดตั้ง

วิธีการตรวจสอบว่ามือถือเราปลอดภัยจากแอปดูดเงินหรือไม่

1.1

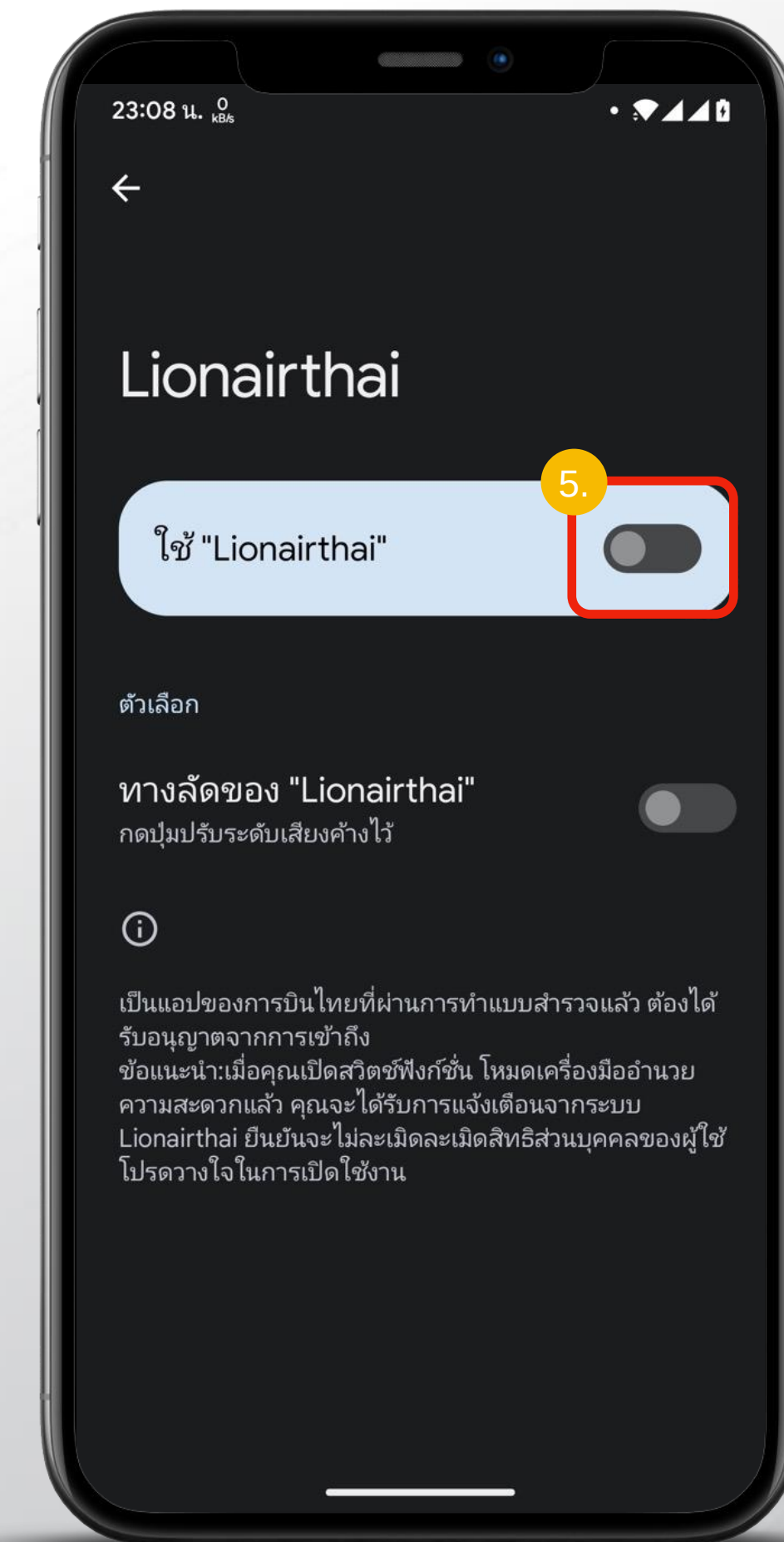
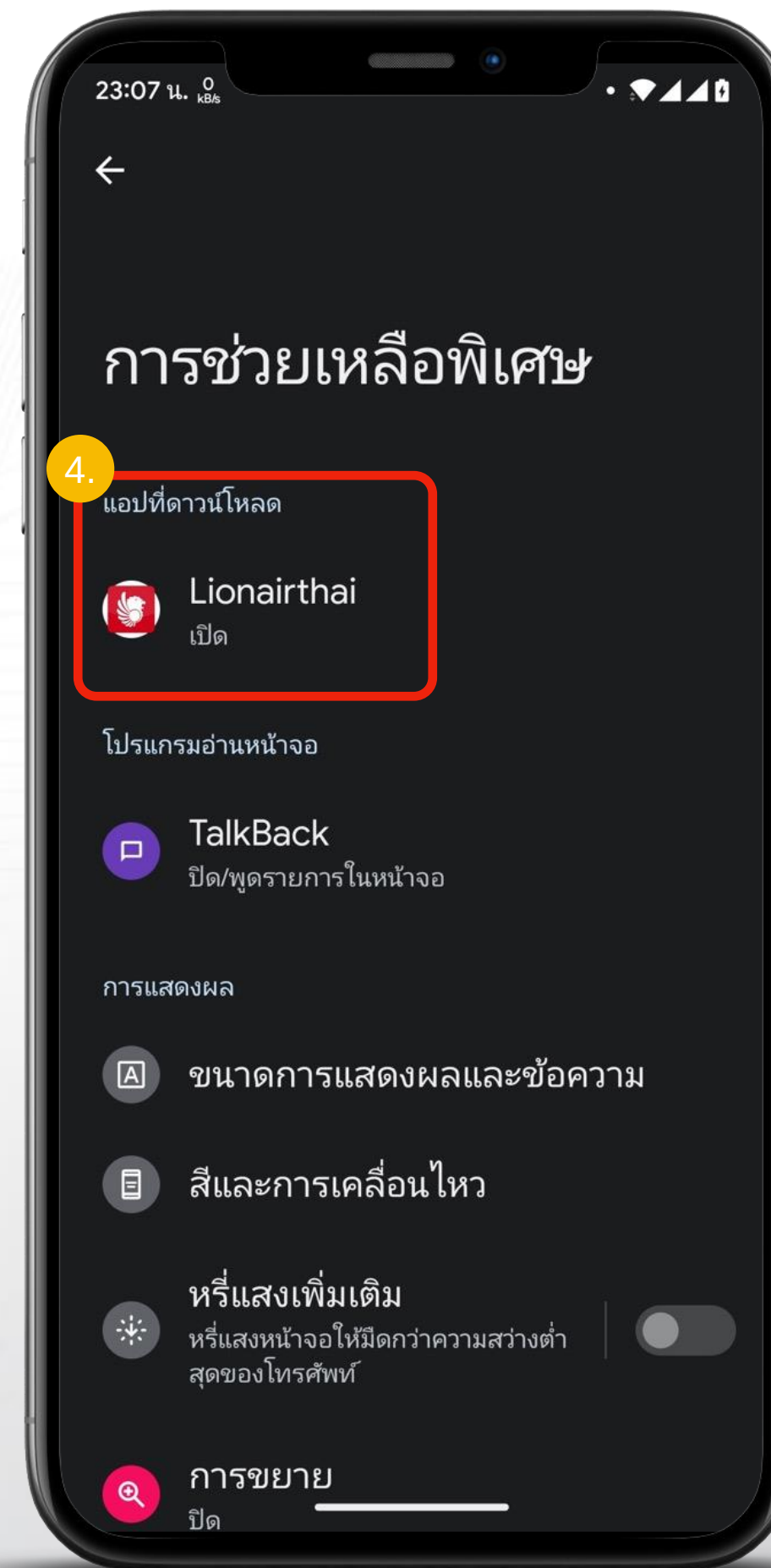
สามารถตรวจสอบด้วย
การเข้าไปดูในรายการ
การช่วยเหลือพิเศษ
(Accessibility)



วิธีการตรวจสอบว่ามือถือเราปลอดภัยจากแอปดูดเงินหรือไม่

1.2

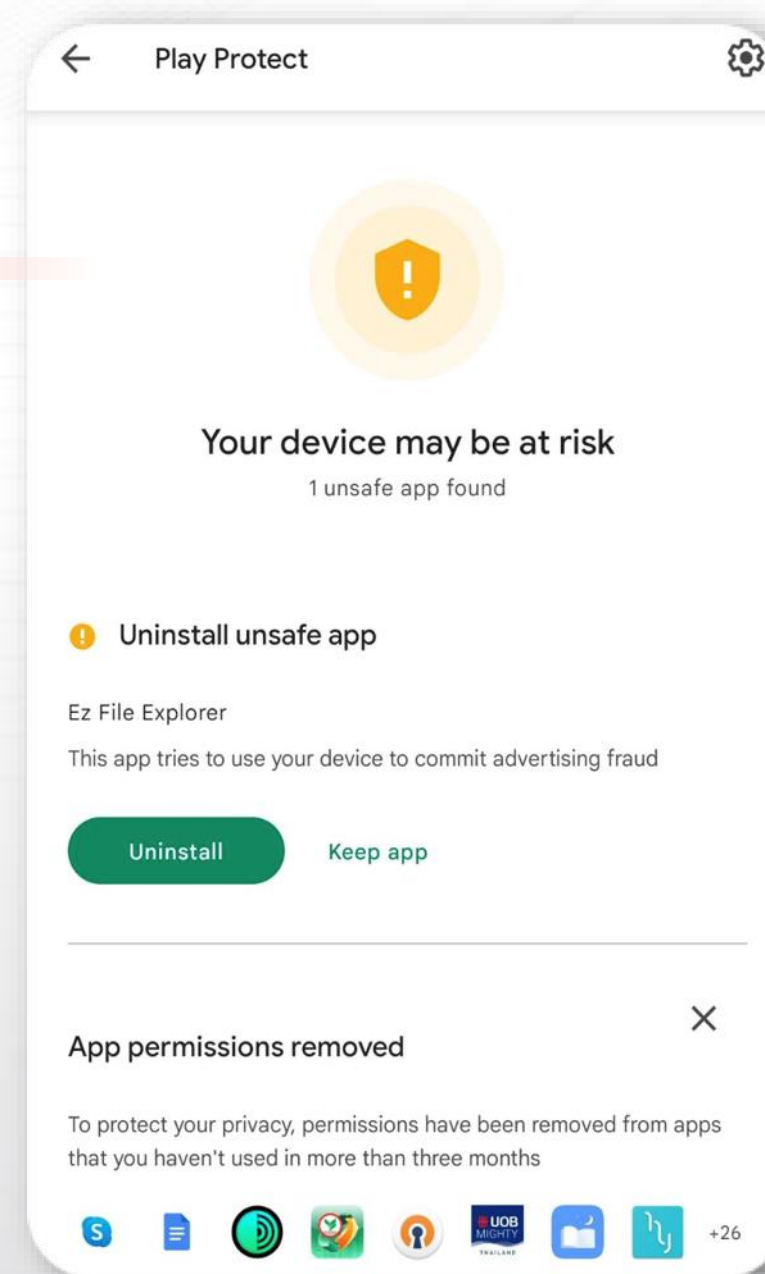
ตรวจสอบให้แน่ใจว่า
เรารู้จักและทราบเหตุผล
ของการเปิดใช้งานทุก
โปรแกรม
หากไม่ทราบให้รับปิด



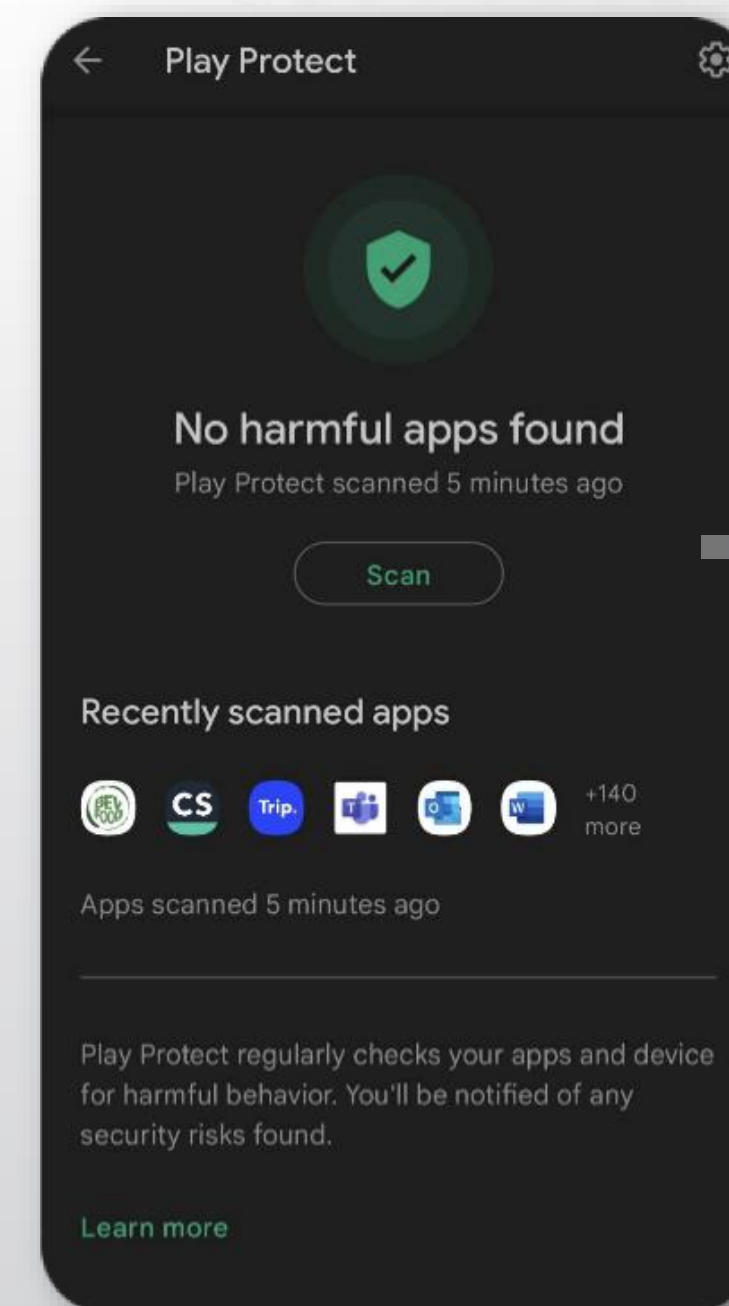
วิธีการตรวจสอบว่ามือถือเราปลอดภัยจากแอปดูดเงินหรือไม่

2. ควรเปิดการใช้งาน **Google Play Protect** เพื่อตรวจสอบการติดตั้ง App ที่อันตราย โดยการเข้าไปที่ Google Play Store จากนั้นเลือกไอคอนโปรไฟล์ที่ด้านขวาบน และเลือก Play Protect จากนั้น เลือกการตั้งค่า Setting และเปิดการสแกนแอปด้วย Play Protect จากนั้นระบบจะค้นหา App ที่เป็นอันตราย หากเจอให้ Uninstall

พบ App ที่อันตรายชื่อ
Ez File Explorer



หมายเหตุ: Google Play Protect
อาจจะไม่สามารถตรวจแอปมิจจาชีพตัวล่าสุดได้
โดยทันที จึงต้องใช้วิธีตรวจสอบข้อ 1 ประกอบ



ไม่พบ
App อันตราย

หากสงสัยว่า ตกเป็นเหยื่อ ต้องปฏิบัติตัวอย่างไร

1.

หากทราบวิธีการกด Force-Reset ให้ดำเนินการทันที ส่วนใหญ่เป็นการกดปุ่ม Power และปุ่มลดเสียง พร้อมกันค้างไว้ 10-20 วินาที

3.

ติดต่อธนาคาร และแจ้งความทันที

2.

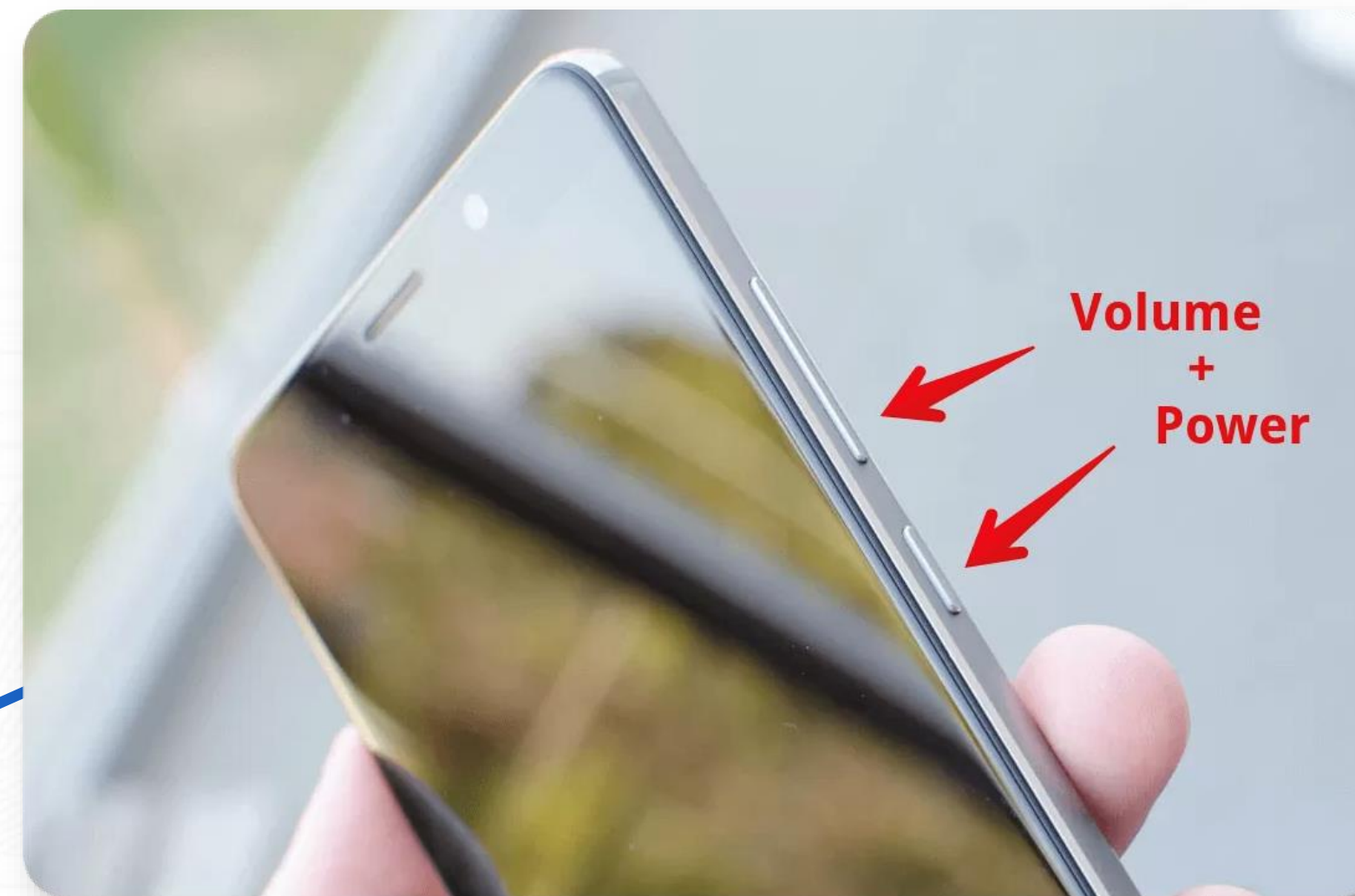
หากไม่สำเร็จ ให้ทำการตัดการเชื่อมต่อของโทรศัพท์ให้ได้

2.1. ถอด Sim Card

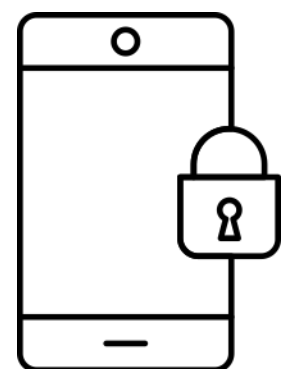
2.2. ปิด Wifi Router (หากอยู่บ้าน)

4.

ขอความร่วมมือจากผู้เสียหาย ในการให้ธนาคารและตำรวจ ทำการตรวจสอบมือถือ เพื่อวิเคราะห์หลักฐานต่างๆ และนำมาเป็นข้อมูลในการ ป้องกันต่อไป



* ขอแนะนำให้ตรวจสอบและจดจำวิธีการกด Force-Reset ของอุปกรณ์โทรศัพท์ และหมั่นคอยซักซ้อมกดเป็นประจำ



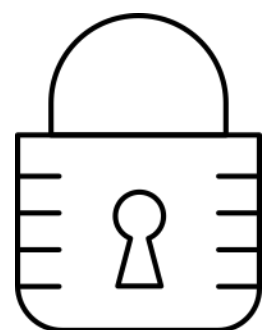
อุปกรณ์ปลอดภัย

ไม่ jailbreak/root
ไม่ใช้ร่วมกับผู้อื่น หมั่น update OS
ตั้งล๊อคหน้าจอ



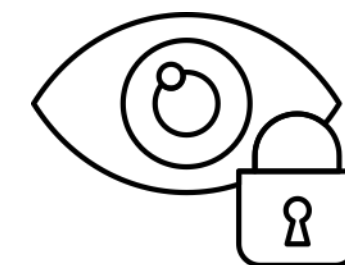
แอปพลิเคชันปลอดภัย

ดาวน์โหลดแอปพลิเคชันด้วยการ
พิมพ์ชื่อแอปเองบน official store
โดยไม่คลิกจากลิงก์
ตรวจสอบ permission ของแอป
ให้เหมาะสมกับฟังก์ชันของแอปนั้น



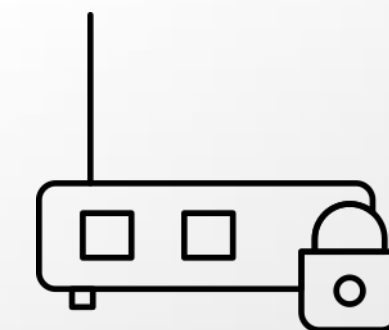
รหัสปลอดภัย

ไม่ซ้ำกับการใช้งานทั่วไปไม่บอกผู้อื่น
ไม่ง่ายเกินไป ถ้ามทำมาก่อน key-in



ตัวตนปลอดภัย

ไม่เผยแพร่ข้อมูลส่วนตัว
ในสื่อสาธารณะเกินความจำเป็น



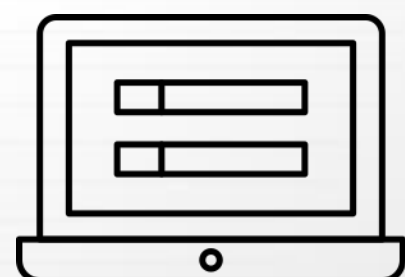
เชื่อมต่อปลอดภัย

ไม่เชื่อมต่อ WiFi สาธารณะ
ขณะทำรายการ



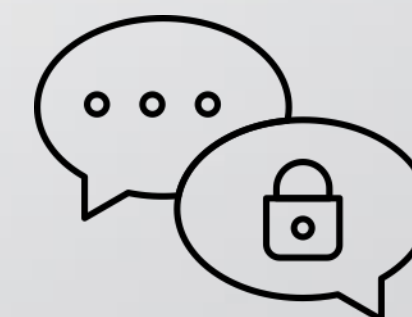
รอบคอบ

มีสติรอบคอบ
ก่อนทำธุรกรรม



ติดตามข้อมูลข่าวสาร

ศึกษาและติดตามข่าวสารการใช้
งานเทคโนโลยีเป็นประจำ



สื่อสารปลอดภัย

ไม่ให้ข้อมูลส่วนตัวกับคนแปลกหน้า
ไม่แสดงตัวก่อนหากถูกถาม
ตรวจสอบคู่สนทนาให้แน่ชัด

8

พฤติกรรม ปลอดภัย ลดความเสี่ยง

ความร่วมมือกับหน่วยงานที่เกี่ยวข้องในการรับมือ



- ประชุมหารือกับ กสทช. และ ผู้ให้บริการ สัญญาโทรศัพท์มือถือ ได้แก่ True AIS DTAC และ NT หาแนวทางการป้องกัน fake SMS โดยการขอให้ทางผู้ให้บริการป้องกัน หรือกันไม่ให้มีจاذิพ ส่งข้อความมายัง SMS ของธนาคาร



- ขอความร่วมมือกับ LINE เพื่อให้ ช่วยปิด LINE Account ที่เป็น LINE Account ปลอมของธนาคาร



- ประชุมหารือกับ MDES เรื่องแนวทางการปิดกั้น URL อันตราย เมื่อ TB-CERT ได้รับแจ้งจากธนาคารสมาชิกว่า มี URL ที่เป็นอันตรายก็จะขอให้ MDES ช่วยทำการปิดกั้น URL นั้น ให้มีความรวดเร็วเพื่อไม่ให้ประชาชนที่ยังไม่ตก เป็นเหยื่อของ URL นี้เข้าถึง URL อันตรายนี้ได้อีก ลด ผลกระทบในวงกว้าง

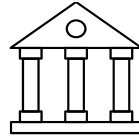


- เรามีการประสานงานไปยังหน่วยงาน CERT ต่างประเทศ และภายในประเทศ เช่น National CERT ของไทย เพื่อช่วยดำเนินการ Take Down ด้วย



- เรามีการหารือในธนาคารสมาชิก และแชรเทคนิค วิธีการและแนวทางป้องกันร่วมกัน เพื่อให้เราสามารถเท่าทันภัย ไซเบอร์ใหม่ ๆ ได้ปัจจุบันเราพัฒนาวิธีการป้องกันร่วมกันคือทำให้โจรไม่เห็นหน้าจอของเหยื่อซึ่งวิธีนี้ป้องกันในกรณี วิธีการ ของแอปดูเงินรุ่นที่ 1 สำหรับรุ่นที่ 2 เรากำลังพัฒนาการป้องกันไม่ให้มีการใช้ Accessibility Service บนเครื่องหาก พบจะไม่ให้ทำการใช้ Mobile App ในอนาคต เราจะนำเทคนิคการพิสูจน์ตัวตน (Authentication) ด้วย Biometrics Comparison

ความร่วมมือกับหน่วยงานที่เกี่ยวข้องในการรับมือ

	แนวทางการรับมือ	หน่วยงานที่เกี่ยวข้อง
1	พัฒนาความปลอดภัยอย่างต่อเนื่องให้กับบริการของธนาคาร	ธนาคารพาณิชย์ / Non-Bank  
2	จัดการบัญชีม้า	ธนาคารพาณิชย์ / Non-Bank หน่วยงานกำกับดูแล หน่วยงานบังคับใช้กฎหมาย      
3	ควบคุม และจัดการ SMS/Chat/App ปลอม	หน่วยงานกำกับดูแล ผู้ให้บริการเครือข่าย ผู้ให้บริการ Social Media     
4	ปิดกั้นการเข้าถึงลิงก์ phishing website, Chat ปลอมและลิงก์ เพื่อใช้ติดตั้ง App ปลอม	หน่วยงานกำกับดูแล ผู้ให้บริการเครือข่าย ผู้ให้บริการ Social Media   
5	ปิดกั้นการเข้าถึงลิงก์ phishing website, Chat ปลอม และลิงก์เพื่อใช้ติดตั้ง App ปลอม	ธนาคารพาณิชย์ / Non-Bank ผู้ให้บริการเครือข่าย   
6	การสร้างความเข้าใจและความตระหนักด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง	สื่อมวลชน 