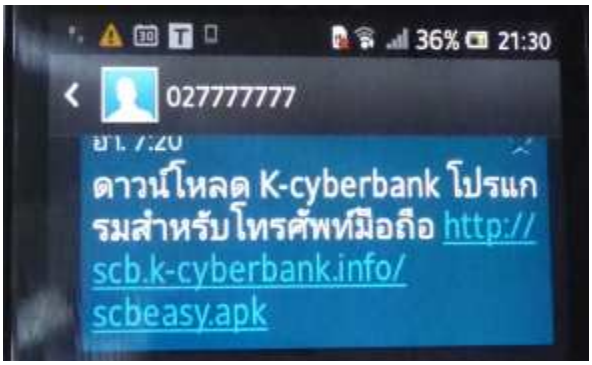
ตัวอย่างการโจรกรรมข้อมูลผ่านทางลิงค์ที่ส่งมาใน SMS โดยหลอกให้ติดตั้งโปรแกรมเพื่อดักข้อมูล Username และ Password ของบริการ SCB Easy Net จากโทรศัพท์ Android

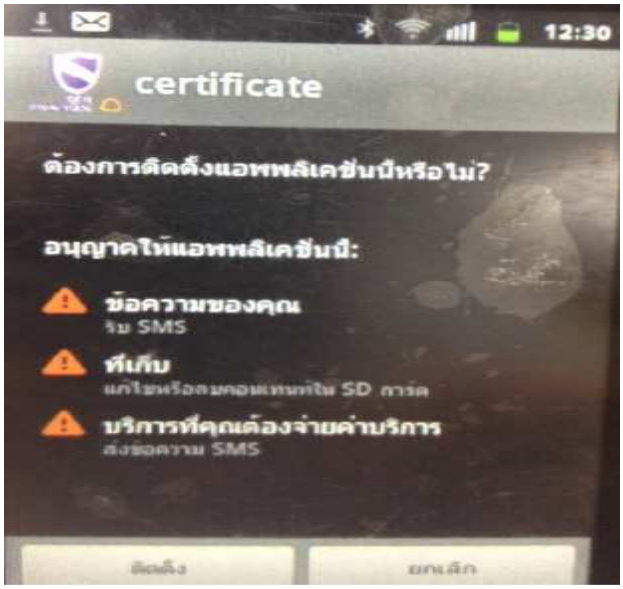
1. เหยื่อจะได้รับ Phishing SMS จากคนร้ายที่ปลอมแปลงหมายเลขผู้ส่งเป็น 02-777-7777 ซึ่งจะมีลิงค์ในข้อความล่อลวงให้ดาวน์โหลดโปรแกรมจาก URL http://scb.k-cyberbank.info/scbeasy.apk



2. หากหลงเชื่อคลิกลิงค์เพื่อดาวน์โหลดโปรแกรม จะเข้าสู่ขั้นตอนการติดตั้งโปรแกรมดักจับ Username และ Password ของคนร้าย ซึ่งระบบปฏิบัติการ Androidจะแจ้งเตือนว่าโปรแกรมดังกล่าวไม่ปลอดภัย เพราะไม่ได้มากจาก Android Market

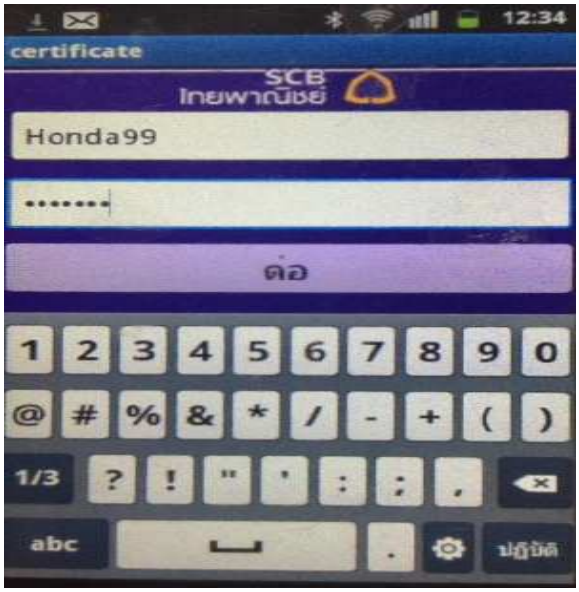
3. หากยืนยันที่จะดำเนินการต่อโดยกดปุ่ม “การตั้งค่า” โทรศัพท์จะดาวน์โหลดโปรแกรมจาก URL ปลอมดังกล่าวของคนร้ายทันที

4. เมื่อคลิกเปิดโปรแกรม จะแสดงหน้าจอยืนยันการติดตั้งแอพพลิเคชันอีกครั้งโดยแอบอ้างโลโก้ธนาคารและระบบรักษาความปลอดภัยเพื่อความน่าเชื่อถือ

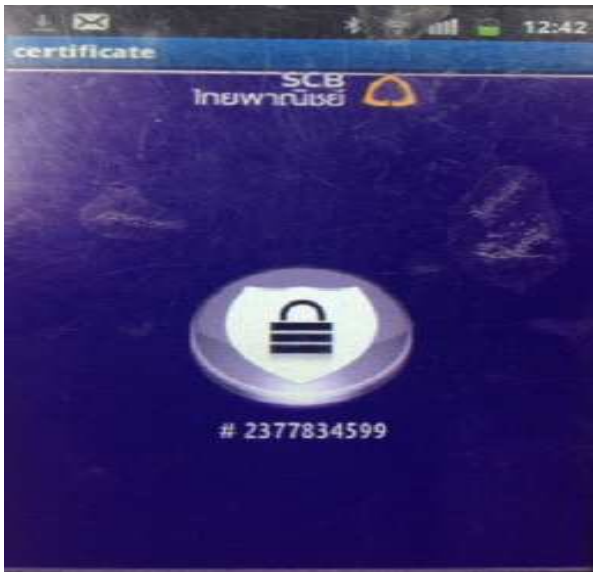


5. เมื่อติดตั้งโปรแกรมเสร็จจะถูกบังคับให้เปิดแอพพลิเคชันทันทีไม่ว่าจะกดปุ่ม “เปิด” หรือ “ปฏิบัติ”

6. เมื่อเปิดโปรแกรม จะแสดงหน้าแอพพลิเคชันพร้อมโลโก้ธนาคารปลอม ล่อลวงให้ใส่ Username และ Password ของ SCB Easy Net หากเหยื่อหลงเชื่อใส่ข้อมูลจริง และกดปุ่ม “ต่อ” ข้อมูล SCB Easy Net ของเหยื่อจะตกเป็นของคนร้ายทั้งหมดทันที



7. หน้าจอโทรศัพท์จะค้าง ไม่สามารถทำรายการใดๆ ต่อไปได้อีก เหยื่อจะไม่ได้รับ OTP หรือ SMS แจ้งเตือนใดๆ จาก SCB Easy Net อีกต่อไปเพราะแอพพลิเคชันปลอมดักจับไว้หมดแล้ว



หากพบข้อความลักษณะข้างต้น อย่าคลิกลิงค์ใดๆ ในข้อความ และโปรดแจ้ง SCB Call Center 02-777-6780 ทันที