

ลวงซัดๆ! ภัยเอสเอ็มเอส

- ล้วงดับข้อมูลส่วนตัวกู้เงิน
- อย่าเชื่อ 'ติดตั้งแอปเถื่อน'

รายงานข่าวจาก สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) เปิดเผยว่า ขณะนี้ได้มีมิจฉาชีพได้ส่งข้อความสั้นหรือเอสเอ็มเอส หลอกหลวงไปยังโทรศัพท์มือถือของประชาชน เช่น ธนาคารแจ้งการอัปเดตระบบ โปรดอัปเดตทันที หรือ บัญชีของคุณถูกแจ้งปิดการใช้งาน คลิกเพื่อตรวจสอบ และ คุณมีเงินเข้าแล้ว 100,000 บาท โดยทุกข้อความจะมีลิงก์ยูอาร์แอลให้กดเข้าไป เพื่อให้กรอกข้อมูลส่วนตัว ยูสเซอร์เนม และพาสเวิร์ด เมื่อหลงเชื่อพิมพ์ข้อมูลไปก็จะถูกนำข้อมูลดังกล่าวไปใช้ หรือถูกแฮกเกอร์นำข้อมูลไปใช้ทำธุรกรรมออนไลน์ต่าง ๆ จึงขอเตือนประชาชน เมื่อมีข้อความลักษณะนี้ส่งเข้ามาไม่ต้องคลิกหรือกดเข้าไปเพื่อลดความเสี่ยงในการถูกหลอกหลวง และหากสงสัยให้ติดต่อธนาคารโดยตรง

ด้านรายงานข่าวจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ หรืออีดีต้า กล่าวว่าไทยเซิร์ตได้รับแจ้งเกี่ยวกับข้อความหลอกหลวงทางเอสเอ็มเอส มีจุดประสงค์เพื่อชักชวนติดตั้งแอปพลิเคชันนอกเพลย์ สโตร์ และขอข้อมูลส่วนบุคคลสำหรับสมัครกู้เงิน โดยหลังจากที่ผู้ใช้งานคลิกลิงก์ในเอสเอ็มเอสจะถูกเชิญให้แอดบัญชีไลน์ชื่อ We Cash 2001 ซึ่งจะส่งข้อความชักชวนให้กดลิงก์เพื่อติดตั้งแอปพลิเคชัน

ซึ่งในกรณีที่เครื่องที่ใช้งานเป็นระบบปฏิบัติการไอโอเอส ลิงก์ดังกล่าวจะพาไปยังเว็บไซต์เพื่อชักชวนให้ดาวน์โหลดและติดตั้งโปรไฟล์ส่งผลให้ผู้ไม่หวังดีได้รับข้อมูล เช่น ข้อมูลของอุปกรณ์ รายการแอปพลิเคชันที่ติดตั้ง และหากในกรณีที่เครื่องที่ใช้งานเป็นระบบปฏิบัติการแอนดรอยด์ เว็บไซต์จะชักชวนให้ติดตั้งแอปพลิเคชันชื่อ Quick Loan (QuickLoan1.2.1-0411.apk) ซึ่งจะขอสิทธิที่ส่งผลกระทบต่อความเป็นส่วนตัว เช่น สิทธิเข้าถึงกล้อง ไฟลีนในเครื่อง รวมถึงสิทธิการบันทึกเสียง ฯลฯ



ทั้งนี้เมื่อเรียกใช้งานแอปพลิเคชัน จะแสดงผลหน้าสำหรับลงทะเบียนและล็อกอินเพื่อกู้เงิน โดยขั้นตอนการลงทะเบียนจะต้องใช้หมายเลขโทรศัพท์สำหรับการยืนยันตัวตนที่ หลังจากลงทะเบียนเสร็จ แอปพลิเคชันจะขอข้อมูลส่วนบุคคลในการยืนยันตัวตนก่อนเข้าใช้งาน อาทิ ชื่อจริง หมายเลขบัตรประชาชน การศึกษา รายได้ต่อปี ข้อมูลบัตรธนาคาร บัญชีธนาคาร และหมายเลขโทรศัพท์รับรอง ฯลฯ ซึ่งไทยเซิร์ตอยู่ระหว่างการประสานหน่วยงานที่เกี่ยวข้องเพื่อแก้ไขโดเมนดังกล่าวแล้ว

อย่างไรก็ตามขอแนะนำเบื้องต้นในการป้องกัน ให้หลีกเลี่ยงการคลิกลิงก์ในข้อความนำส่งจากผู้ส่งที่ไม่รู้จัก ซึ่งถูกส่งผ่านเอสเอ็มเอส ไลน์ และอีเมล โดยอาจพิจารณาบล็อกผู้

ส่งดังกล่าวเพื่อลดความเสี่ยงและหลีกเลี่ยงการติดตั้งโปรไฟล์ บนไอโอเอส และควรเลือกติดตั้งแอปพลิเคชันจากแหล่งน่าเชื่อถือ เช่น กูเกิล เพลย์ สโตร์ หรือ แอป สโตร์ และกรณีที่ติดตั้งแอปแล้วให้ถอนการติดตั้งจากเครื่องทันที.