เทรนด์ไมโครเตือนผู้ใช้อินสตาแกรมระวังมัลแวร์รูปแบบใหม่

รายงานบทความพิเศษโดยคาร์ลา อากรีกาโอ นักวิเคราะห์ภัยคุกคาม ศูนย์วิจัยเทรนด์แล็บส์ บริษัท เทรนด์ไมโคร ระบุว่า “อินสตาแกรม (Instagram) แอพพลิเคชั่นแชร์รูปภาพที่กำลังได้เป็นที่นิยม และเป็นเว็บไซต์เครือข่ายสังคมล่าสุดที่ตกเป็นเป้าหมายการหลอกลวงที่เรียกว่า “Survey Scams” อย่างที่เคยพบบนเฟซบุ๊ก และ ทวิตเตอร์ เราพบว่าการหลอกลวงโดยให้ผู้ใช้ร่วมตอบแบบสอบถามนี้จะทำให้ผู้ใช้ดาวน์โหลดแอนดรอยด์มัลแวร์ติดเข้ามาในอุปกรณ์ต่างๆ ด้วย”

ปัจจุบันเราจะพบว่ามีผู้ติดตามที่สนใจอยากจะติดตาม (follow) เราในอินสตาแกรม ซึ่งถือเป็นเรื่องปกติที่อินสตาแกรม แอคเค้าท์ของคุณจะต้องมีการตั้งค่าเป็น “ส่วนตัว” (private) และในขณะที่ตรวจสอบการร้องขอเหล่านี้ นักวิจัยระบบรักษาความปลอดภัยของเทรนด์ไมโครพบบางสิ่งที่ผิดปกติในหลายๆ รายชื่อที่ติดต่อเข้ามา เราจึงเข้าไปตรวจสอบหน้าเพจของอินสตาแกรม แอคเค้าท์เหล่านั้น และพบว่าพวกเขาเหล่านั้นโพสต์รูปภาพที่มีข้อความว่า “Get Free Followers!” โพสต์นี้ทำให้เรานึกถึงพินเทอเรสต์ (Pinterest) ที่เคยตรวจพบว่ามีการหลอกลวงในรูปแบบรายการโปรโมชั่นฟรี และเทรนด์ไมโครเคยบล็อกไปเมื่อเร็วๆ นี้

นอกจากนี้สิ่งอื่นที่เราพบว่าน่าสงสัยก็คือว่าผู้ติดตามอินสตาแกรมเหล่านี้มักจะใช้ชื่อที่ซ้ำๆ กัน เช่น “Tawna Tawna” และ “Concetta Concetta” เมื่อได้รับสัญญาณที่น่าสงสัย เทรนด์ไมโครจึงตรวจสอบรูปภาพ “Get Free Followers” และนำไปสู่หน้าเว็บที่มีแอพพลิเคชั่น “Get Followers” ซึ่งตรวจพบว่าเป็นมัลแวร์ ANDROIDOS_GCMBOT.A ที่จะหลอกให้ผู้ใช้เปิดหน้าเว็บที่เป็นอันตรายหรือส่ง SMS จากอุปกรณ์ต่างๆ ได้ ซึ่งบริษัทเทรนด์ไมโครสามารถปกป้องผู้ใช้จากภัยคุกคามนี้โดยการปิดกั้น URL ที่เกี่ยวข้องได้

อาชญากรไซเบอร์จะได้ประโยชน์จากแบบสอบถามหลอกลวง (Survey scams) ผ่านทางเว็บไซต์ ad-tracking หากผู้ใช้ที่ไม่ระมัดระวังและดาวน์โหลดแอพพลิเคชั่นดังกล่าว ผู้ใช้จะถูกเปลี่ยนเส้นทางไปก่อนหน้า Survey Page ของจริงและถูกนำไปสู่เว็บไซต์ที่เป็นอันตรายในที่สุด อีกทั้งคนร้ายยังสามารถใช้ข้อมูลที่รวบรวมมาจากการหลอกลวงเหล่านี้ไปเร่ขายให้กับกลุ่มอาชญากรรมอื่น ๆ หรือใช้ข้อมูลนี้เพื่อแผนการในอนาคตได้

ปัจจุบันอาชญากรไซเบอร์ที่อยู่เบื้องหลังการหลอกลวงเหล่านี้จะเข้าถึงทุกๆ เว็บไซต์เครือข่ายที่เป็นนิยม ไม่ว่าจะเป็น เฟซบุ๊ก พินเทอเรสต์ และอินสตาแกรม ดังนั้นเพื่อปกป้องตนเองจากการหลอกลวงเหล่านี้ ผู้ใช้งานจะต้องหมั่นตรวจสอบโพสต์ในบัญชีรายชื่อของคุณ แม้ว่าพวกเขาจะมาจากเพื่อน สมาชิกในครอบครัวหรือคนรู้จัก การระวังตัว

คือการป้องกันที่ดีที่สุดสำหรับคุณ