5 วิธีปกป้องตนเองไม่ตกเป็นเหยื่อบนโลกออนไลน์

นำเสนอเมื่อ : 22 ก.พ. 2566

แนะ 5 วิธีปกป้องตนเองไม่ตกเป็นเหยื่อบนโลกออนไลน์

อุบัติการณ์ด้านการรักษาความปลอดภัยไซเบอร์ สร้างความเสียหายมากขึ้นต่อเนื่อง ด้วยการใช้เทคนิคการโจมตีที่ซับซ้อนและเรียกร้องกรรโชกกดดันอย่างหนัก เราเห็นข่าวผู้เสียหายสูญเสียเงินเกือบทุกวัน พาโล อัลโต้ เน็ตเวิร์กส์ แนะ 5 วิธีป้องกัน

ดร.ธัชพล โปษยานนท์ ผู้อำนวยการ ประจำประเทศไทยและอินโดจีน พาโล อัลโต้ เน็ตเวิร์กส์ เปิดเผยว่า ข้อมูลส่วนบุคคลมีความสำคัญ และเป็นความลับ จึงไม่ควรให้ข้อมูลส่วนตัวกับใคร การปรับเปลี่ยนพฤติกรรมเล็กๆ น้อยๆ บนอุปกรณ์และบัญชี สามารถดูแลปกป้องความเป็นส่วนตัวจากบุคคลที่ไม่ได้รับอนุญาตซึ่งพยายามแอบลักลอบเข้าถึงอุปกรณ์และข้อมูลส่วนตัวโดยไม่พึงประสงค์ เพื่อป้องกันภัยคุกคามทางไซเบอร์และข้อมูลออนไลน์ จึงได้แนะนำแนวปกป้องข้อมูลส่วนตัวบนโลกออนไลน์ด้วยวิธีการง่ายๆ 5 วิธี ประกอบด้วย

1. ปกป้องแอคเคานท์ของคุณ : การล็อกและปกป้องบัญชีของคุณเป็นเรื่องสำคัญ คุณไม่ควรเปิดเผยข้อมูลทางบัญชีที่อ่อนไหวกับบุคคลใดก็ตาม ทุกคนควรใช้โปรแกรมจัดการรหัสผ่านเพื่อสร้างและจดจำรหัสผ่านที่ซับซ้อนและแตกต่างกันในแต่ละแอคเคานท์และควรหลีกเลี่ยงการใช้รหัสผ่านที่คาดเดาได้ง่าย เช่น “password”, “1234” หรือใช้วันเกิดเป็นรหัสผ่าน หากเป็นเช่นนั้น ควรเปลี่ยนรหัสผ่านให้บ่อย อีกทั้งทุกคนควรใช้การยืนยันตัวตนแบบสองขั้นตอนกับทุกบัญชีออนไลน์ในทุกกรณีหากเป็นไปได้

2.ปกป้องการท่องเว็บ : เพื่อเป็นการยับยั้งโฆษณาที่แอบติดตามคุณ คุณควรปิดโฆษณาประเภทอิงตามความสนใจ ทั้งที่มาจาก Apple, Facebook, Google และ Twitter และยอมรับคุกกี้ของเว็บไซต์เฉพาะเท่าที่จำเป็น อีกทั้งยังแนะนำให้ใช้เครือข่ายส่วนตัวแบบเสมือน (VPN) หรือฮอตสปอตส่วนตัวแทนการเชื่อมต่อกับไว-ไฟสาธารณะ เมื่อต้องการท่องอินเทอร์เน็ต

3. ติดตั้งซอฟต์แวร์ป้องกันไวรัสบนคอมพิวเตอร์ : ซอฟต์แวร์ที่ประสงค์ร้ายที่แฝงอยู่กับคอมพิวเตอร์ของเราสามารถสร้างหายนะได้หลากหลายรูปแบบ ตั้งแต่การแสดงหน้าต่างโฆษณาไปจนถึงการแอบขุดบิตคอยน์ หรือกระทั่งสแกนหาข้อมูลส่วนตัวของคุณ หากคุณเสี่ยงต่อการคลิกลิงก์อันตรายหรือต้องใช้คอมพิวเตอร์ร่วมกันหลายคนในครอบครัว แนะนำให้ติดตั้งซอฟต์แวร์ป้องกันไวรัสโดยเฉพาะบนคอมพิวเตอร์ตระกูล Windows เพราะแฮกเกอร์มักใช้มัลแวร์หรือไวรัสเพื่อเข้าถึงคอมพิวเตอร์ของเหยื่อ ซึ่งซอฟต์แวร์ป้องกันไวรัสจะช่วยปกป้องคุณจากแฮกเกอร์ได้ในกรณีส่วนใหญ่

4. อัปเดตซอฟต์แวร์และอุปกรณ์ : ควรตรวจสอบให้แน่ใจว่าได้เปิดใช้การอัปเดตแบบอัตโนมัติบนระบบปฏิบัติการที่ใช้งานอยู่หรือไม่ ทั้งบนระบบ Windows, macOS หรือ Chrome OS ก็ตาม ผู้ใช้ควรตั้งค่าให้แอปบนอุปกรณ์มีการอัปเดตโดยอัตโนมัติ หากไม่พบตัวเลือกการอัปเดตอัตโนมัติ อาจจำเป็นต้องรีบูตอุปกรณ์ด้วยตนเองเป็นครั้งคราว (อาจตั้งรายการเตือนในปฏิทินเป็นประจำทุกเดือนก็ได้)

5. บุ่มเพาะนิสัยแห่ง ‘ซีโร่ทรัสต์’ หรือความไม่วางใจใดๆ :
เคล็ดลับข้อสุดท้ายเป็นเรื่องสำคัญที่สุด
โดยทั่วไปแฮกเกอร์มักไม่พอใจกับสิ่งที่ได้ตรงหน้าและมองหาลู่ทางเพิ่มเติมโดยตลอด
แฮกเกอร์ไม่ได้พอใจกับข้อมูลบริษัทเล็กๆ ที่ตนเองมีอยู่ในมือ เช่น โรงแรมต่างๆ
แต่มักพยายามลอบขโมยข้อมูลจากองค์กรขนาดใหญ่ องค์กรต่างๆ
สามารถรับมือปัญหาดังกล่าวได้โดยใช้แนวทางการรักษาความปลอดภัยไซเบอร์ที่เรียกว่า “ซีโรทรัสต์”
ซึ่งอนุมานว่าคนรายแฝงอยู่ในเครือข่ายองค์กรเรียบร้อยแล้ว ดังนั้นจึงไม่ควรไว้วางใจผู้ใดก็ตาม
ควรมีการตรวจสอบผู้ใช้ทุกคน ยืนยันอุปกรณ์ทุกเครื่อง จำกัดการเข้าถึงและสิทธิต่างๆ เฉพาะที่จำเป็น
และใช้ระบบแมชชีนเลิร์นนิ่งที่มีความอัจฉริยะซึ่งสามารถเรียนรู้และปรับเปลี่ยนการทำงานได้ตามพฤติกรรมผู้ใช้ที่เกิดขึ้น เพื่อจะได้ไม่กระทบต่อการทำงานของพนักงาน

ขอบคุณที่มาจาก เดลินิวส์