Thai

เคล็ดลับสำคัญ 10 ข้อในการรักษาความเป็นส่วนตัว

1. แฮ็กเกอร์ใช้อีเมลหลอกลวงเพื่อล้วงข้อมูลที่คุณเก็บไว้อย่างปลอดภัย โปรดระวังข้อความทั้งหมดที่คุณได้รับ และหากคุณคิดว่าอีเมลนั้นน่าสงสัย อย่าคลิกลิงก์ใด ๆ หรือเปิดไฟล์แนบใด ๆ

2. เพิ่มความปลอดภัยของคุณโดยตั้งการยืนยันตัวตนสองขั้นตอน การเพิ่มขั้นตอนการยืนยันตัวตนอีกขั้นจะทำให้ผู้เจาะข้อมูลเข้าถึงข้อมูลของคุณได้ยากขึ้น

3. โปรดอย่าเปิดพิกัดที่ตั้งตลอดเวลา เว็บไซต์ต่าง ๆ มักขอให้คุณแชร์พิกัดของคุณในการทำเช่นนี้ เว็บไซต์เหล่านั้นรวบรวมข้อมูลเกี่ยวกับพิกัดและความสนใจของคุณ โปรดตั้งพิกัดที่ตั้งของคุณเองแทนแบบอัตโนมัติ เพื่อปกป้องข้อมูลของคุณให้ปลอดภัยยิ่งขึ้น

4. ติดตั้งตัวบล็อกโฆษณา — โฆษณาอาจติดตามคุณอยู่เบื้องหลัง โปรดใช้ตัวบล็อกโฆษณาเพื่อปิดกั้นการติดตามและการวิเคราะห์ข้อมูลจากบุคคลที่สองและสาม

5. โปรดระวังเครือข่าย Wi-Fi สาธารณะ เครือข่ายเหล่านี้มักปลอดภัยน้อยกว่าเครือข่ายทั่วไป และอนุญาตให้เข้าถึงข้อมูลของคุณมากเกินความจำเป็นเมื่อให้บริการเชื่อมต่ออินเทอร์เน็ต

6. คุณมีสิทธิที่จะสอบถามเหตุผลในการเก็บรวบรวมข้อมูลใด ๆ เกี่ยวกับคุณ ซึ่งรวมถึงหน่วยงานภาครัฐในระดับรัฐ และองค์กรอื่น ๆ เป็นต้น นโยบายความเป็นส่วนตัวของหน่วยงานและองค์กรเหล่านี้อาจระบุข้อมูลนี้ไว้

7. เก็บรักษาเอกสารและไฟล์ข้อมูลของคุณให้ปลอดภัยหากเอกสารเหล่านี้ระบุข้อมูลสำคัญหรือข้อมูลส่วนบุคคล พิจารณาใช้การเข้ารหัสเพื่อล็อกฮาร์ดไดร์ฟและยูเอสบีที่พกพาได้ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตหากวางอุปกรณ์เหล่านี้ไว้ผิดที่

8. เก็บรักษารหัสผ่าน รหัส PINs และโค้ดอื่น ๆ ในการเข้าใช้ให้ปลอดภัยและเป็นความลับ การใช้โปรแกรมจัดการรหัสผ่านเป็นวิธีที่ดีที่จะเก็บรักษารหัสผ่านและรายละเอียดในการลงชื่อเข้าใช้ให้ปลอดภัย เนื่องจากรหัสผ่านและรายละเอียดเหล่านี้จะได้รับการเก็บรักษาไว้ในฐานข้อมูลที่เข้ารหัส

9. ตั้งค่าความเป็นส่วนตัวและตรวจการตั้งค่าเหล่านี้เป็นประจำเมื่อใช้โซเชียลมีเดียและเว็บไซต์สร้างเครือข่ายออนไลน์ (เช่น เฟซบุ๊ก ทวิตเตอร์) และควรพิจารณาตั้งค่าโปรไฟล์โซเชียลมีเดียของคุณเป็นแบบส่วนตัว

10. ทำลายจดหมายที่ระบุข้อมูลส่วนบุคคลไว้โดยใช้วิธีที่รัดกุม (เช่น ใช้เครื่องย่อยเอกสาร) อย่านำเอกสารสำคัญที่ระบุข้อมูลส่วนบุคคลของคุณไปทิ้งในถังขยะรีไซเคิลโดยเด็ดขาด