10 ข้อควรรู้ที่จะช่วยให้คุณรับมือกับภัยทางไซเบอร์ได้ดีขึ้น

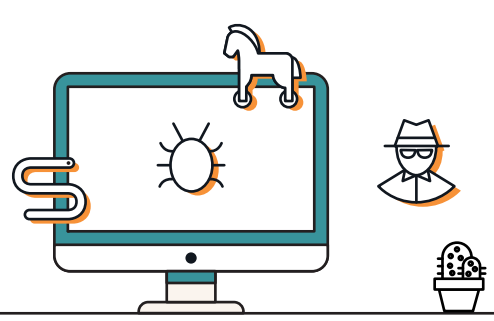
1

ปรับความเข้าใจเบื้องต้นว่าคอมพิวเตอร์และเครื่องมือเชื่อมต่อทางอินเตอร์เน็ตทุกประเภท อาจไม่ได้ถูกติดตั้งการรักษาความปลอดภัยมาตั้งแต่แรก ฉะนั้นเราควรติดตั้งซอฟท์แวร์หรือแอปพลิเคชันที่ใช้ป้องกันภัยจากมัลแวร์และไม่ควรใช้ซอฟท์แวร์ปลอมหรือแอปพลิเคชันที่ไม่น่าเชื่อถือ

2

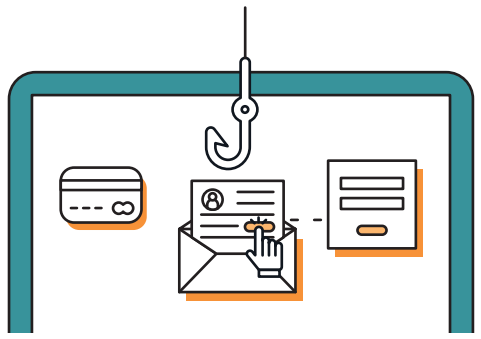
อ่านข้อตกลงและนโยบายความเป็นส่วนตัวทุกครั้ง ก่อนติดตั้งซอฟท์แวร์ในคอมพิวเตอร์หรือแอปพลิเคชันใดๆลงในอุปกรณ์เชื่อมต่ออินเตอร์เน็ต เพราะหลังการติดตั้ง ข้อมูลทุกอย่างที่เกี่ยวข้องกับคุณและการใช้งานจะถูกส่งไปยังผู้ผลิตอุปกรณ์ ซอฟท์แวร์ และแอปพลิชันเสมอ

3



ภัยทางไซเบอร์ที่เข้าโจมตีผ่านทางคอมพิวเตอร์เรียกว่ามัลแวร์หรือ Malicious Software เป็นซอฟท์แวร์ที่เข้าสู่ระบบโดยที่ผู้ใช้ไม่ได้อนุญาต มีหลายชนิด ได้แก่ ไวรัสคอมพิวเตอร์ หนอนคอมพิวเตอร์ โทรจัน สปายแวร์ ฯลฯ การติดมัลแวร์แต่ละชนิดมีที่มาไม่เหมือนกัน มัลแวร์แต่ละตัวมีรูปแบบวิธีการจู่โจมเป้าหมาย การทำงาน และให้ผลเสียแตกต่างกัน

4



นอกจากมัลแวร์แล้วคุณควรรู้จักการโจมตีในรูปแบบของการปลอมแปลงอีเมลเพื่อทำการหลอกลวงเหยื่อด้วย เช่น Phishing และ Business Email Compromise (BEC) เพราะรูปแบบการหลอกลวงแม้จะคล้ายกันอยู่บ้าง แต่วิธีและเป้าหมายการทำงานแตกต่างกัน ที่สำคัญคือสร้างผลเสียเป็นมูลค่ามหาศาลให้แก่เหยื่อ โดยที่ไม่สามารถแก้ไขได้

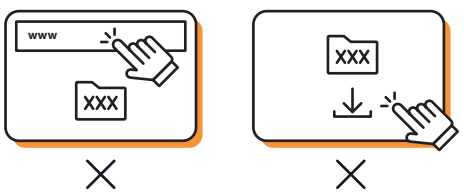
5

เมื่อได้รับอีเมล แม้เป็นอีเมลจากผู้ที่เคยติดต่อกันมาก่อน ควรเช็คการสะกดชื่อของ Email Address ให้ถูกต้องทุกครั้งก่อนตอบกลับเพื่อป้องกันการหลอกลวงจากผู้ไม่หวังดี หรือหากได้รับอีเมลจากผู้ที่ไม่เคยติดต่อกันมาก่อน ไม่ควรเปิดอ่านถ้าหัวข้อและเนื้อหาตอนต้นของอีเมลไม่มีความเกี่ยวข้องเชื่อมโยงกับเรา ไม่ควรเปิดไฟล์แนบในกรณีที่ไม่ได้มีการตกลงกันมาก่อน และเมื่อมีการรับส่งอีเมลสำคัญ ควรมีการยืนยันข้อมูลรับส่งกับผู้รับปลายทางด้วยวิธีอื่นด้วย เช่น การโทรหา การส่งข้อความทางมือถือ การนัดเจอ เป็นต้น

6

คุณควรตั้งรหัสผ่านการใช้บริการอินเทอร์เน็ตบ่อยๆและไม่ควรตั้งรหัสผ่านเหมือนกันทุกระบบ เพราะหากคุณโดนแฮกเกอร์เจาะระบบสำเร็จในระบบอื่นๆก็อาจถูกเจาะไปด้วย

7

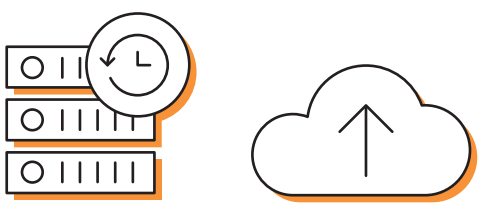


หลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสมเพื่อหลีกเลี่ยงการติดมัลแวร์ และไม่ควรดาวน์โหลดไฟล์ ซอฟท์แวร์ หรือโปรแกรมจากเว็บไซต์ที่ไม่น่าเชื่อถือ

8

สแกนคอมพิวเตอร์อาทิตย์ละครั้ง รวมถึงสแกนอุปกรณ์เก็บข้อมูลทั้ง USB CD หรือ DVD ทุกครั้งก่อนใช้งาน เพื่อลดความเสี่ยงในการติดมัลแวร์

9



ควรมีการแบคอัพข้อมูลหรือไฟล์ที่สำคัญอยู่เสมอ เพราะหากแก้ไขไม่ได้เลย อย่างน้อยคุณยังมีไฟล์สำรองที่ยังสามารถดึงข้อมูลมาใช้ได้

10

ควรอัพเดทแพทช์และซอฟท์แวร์ป้องกันมัลแวร์อย่างสม่ำเสมอ และติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์จากแหล่งข่าวที่น่าเชื่อถือ

Aware

+66 5326 3350 info@aware.co.th www.aware.co.th