



ใบความรู้ที่ 15 เรื่อง การติดตั้งซอฟต์แวร์จากอินเทอร์เน็ต



การติดตั้งซอฟต์แวร์จากอินเทอร์เน็ตเป็นการติดตั้งโปรแกรมหรือชุดคำสั่งโดยการนำซอฟต์แวร์ที่อยู่บนอินเทอร์เน็ตมาติดตั้งบนอุปกรณ์เทคโนโลยี ซึ่งในบางครั้งอาจทำให้อุปกรณ์เทคโนโลยีนั้นเกิดความเสียหายได้



1.

อันตรายจากการติดตั้งซอฟต์แวร์

การติดตั้งซอฟต์แวร์ที่อยู่บนอินเทอร์เน็ตมาลงบนเครื่องคอมพิวเตอร์ มักพบโปรแกรมที่เรียกว่า มัลแวร์ (Malicious Software : Malware) ซึ่งเป็นเครื่องมือสำหรับการก่อปัญหาอาชญากรรมทางอินเทอร์เน็ตที่แฝงมากับซอฟต์แวร์ที่ติดตั้ง โดยมัลแวร์ที่พบในปัจจุบันมีหลายประเภท



1. ไวรัสคอมพิวเตอร์ (Computer Virus)

เป็นโปรแกรมที่เขียนขึ้นเพื่อขัดขวาง การทำงานของคอมพิวเตอร์ ทำให้ผู้ใช้งานเกิดความรำคาญ ก่อให้เกิดความเสียหายต่อข้อมูลหรือระบบการทำงานของคอมพิวเตอร์โดยไวรัสคอมพิวเตอร์มักติดมากับไฟล์งานต่าง ๆ และจะทำงานเมื่อมีการเปิดใช้งานไฟล์นั้นขึ้นมา

4. โปรแกรมโฆษณา หรือ แอดแวร์

(Advertising Supported Software:

Adware)

เป็นโปรแกรมที่แฝงมากับโปรแกรมทั่วไป ทำหน้าที่แสดงโฆษณาอย่างต่อเนื่องหรือดาวน์โหลดโฆษณาอัตโนมัติ ก่อให้เกิดความรำคาญแก่ผู้ใช้

2. หนอนอินเทอร์เน็ต หรือ วอร์ม (Worm)

เป็นโปรแกรมอันตรายที่ใช้วิธีหาจุดอ่อนของระบบรักษาความปลอดภัย แล้วแพร่กระจายไปสู่คอมพิวเตอร์เครื่องอื่น ๆ ในระบบเครือข่ายได้ด้วยตนเองอย่างรวดเร็ว ทำให้คอมพิวเตอร์และระบบเครือข่ายเกิดความเสียหายที่รุนแรง

5. โปรแกรมเรียกค่าไถ่ (Ransomware)

เป็นโปรแกรมที่ขัดขวางการเข้าถึงไฟล์ข้อมูลภายในอุปกรณ์เทคโนโลยีด้วยการเข้ารหัสจนกว่าผู้ใช้จะจ่ายเงินให้ผู้เรียกค่าไถ่จึงจะได้รับรหัสผ่านเพื่อเข้าใช้งานไฟล์ดังกล่าว

3. โปรแกรมดักจับข้อมูล หรือสปายแวร์

(Spyware)

เป็นโปรแกรมที่แอบขโมยข้อมูลของผู้ใช้ระหว่างใช้งานคอมพิวเตอร์ เพื่อนำไปใช้แสวงหาผลประโยชน์ต่าง ๆ เช่น เก็บข้อมูลพฤติกรรมการใช้งานอินเทอร์เน็ต เพื่อนำไปใช้ในการโฆษณา

6. ม้าโทรจัน (Trojan Horse)

เป็นโปรแกรมที่หลอกลวงผู้ใช้ให้ติดตั้งและเรียกใช้งาน แต่เมื่อเรียกใช้งานแล้วจะเริ่มทำงานเพื่อสร้างปัญหาตามที่ผู้เขียนกำหนด เช่น ลักลอบส่งออกข้อมูลส่วนตัวของผู้ใช้งาน ทำลายระบบ



2. แนวทางในการตรวจสอบและป้องกันมัลแวร์

1) สังเกตความเร็วของอุปกรณ์เทคโนโลยี
อินเทอร์เน็ต

2) ตรวจสอบความเร็วของเครือข่าย

3) สังเกตความผิดปกติในการใช้งาน

4) เรียกใช้งานโปรแกรมตรวจจับมัลแวร์

