การป้องกันไวรัสสำหรับระบบเครือข่าย

กำหนดมาตรการป้องกันไวรัสที่มีประสิทธิภาพสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น การติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น การปกป้องระบบเครือข่าย สิ่งที่สำคัญอย่างยิ่ง คือ ผู้ใช้งานในระบบจะต้องคอยดูแล และป้องกันไม่ให้ตนเองเป็นช่องทางผ่านของ Hacker ผู้ดูแลระบบจะต้องคอยติดตามและหาวิธีการป้องกัน และแก้ไขจุดบกพร่องของซอฟต์แวร์ที่ใช้งาน เพราะไม่มีระบบเครือข่ายใดที่ปลอดภัยสมบูรณ์แบบ ดังนั้นจึงต้องมีระบบป้องกันที่ดีโดยมีวิธีการ ดังนี้

- ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ
  - ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสม
  - สร้างแผ่น Emergency Disk เพื่อใช้ในการกู้ระบบ
  - อัพเดตข้อมูลไวรัสของโปรแกรมทุกครั้งที่เครื่องเตือนให้อัพเดต
  - เปิดใช้งาน Auto Protect
  - ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือบันทึกข้อมูลต่างๆ
  - ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

- การป้องกันจากการเปิดไฟล์จากสื่อบันทึกข้อมูล (Media) ต่างๆ
  - แผ่น CD , เทปต่างๆ
  - สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
  - ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่น่าสงสัย เช่น .pif เป็นต้น
  - ไม่ใช้สื่อบันทึกที่ไม่ทราบแหล่งที่มา

- การป้องกันจากการเปิด E-Mail
  - อย่าเปิดไฟล์ E-Mail จากผู้ส่งที่ไม่รู้จัก และไม่ทราบที่มา
  - อย่าเปิดอ่าน E-Mail ที่มีหัวเรื่องเป็นข้อความไม่ปกติ
  - ลบ E-Mail ที่ไม่ทราบแหล่งที่มาทิ้งทันที
  - อัพเดตโปรแกรม E-Mail สม่ำเสมอ

- การป้องกันจากการดาวน์โหลดจาก Internet
  - ไม่ควรเปิดไฟล์ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น MSN
  - ไม่ควรเข้า Website ที่มากับ E-Mail
  - ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่มั่นใจหรือไม่น่าเชื่อถือ
  - ติดตามข้อมูลการแจ้งเตือนจากแหล่งข้อมูลด้านความปลอดภัยเสมอ
  - หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น
  - หลีกเลี่ยงการแชร์ไฟล์ประเภท Peer to Peer เนื่องจากมีโอกาสติดไวรัสสูง