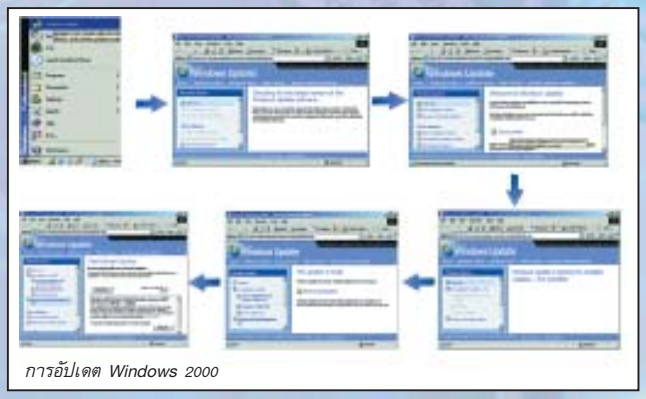
วิธีการป้องกัน ไวรัสคอมพิวเตอร์

1 ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตข้อมูลไวรัสอยู่เสมอ
- ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสม
- สร้างแผ่น Emergency disk เพื่อใช้ในการกู้ระบบ
- อัปเดตข้อมูลไวรัสของโปรแกรมทุกวัน หรือ ทุกครั้งที่โปรแกรมแจ้งเตือนให้อัปเดต
- เปิดใช้งาน auto-protect ถ้าโปรแกรมสนับสนุน
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่น หรือบันทึกข้อมูลต่างๆ
- ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสบนเครื่องคอมพิวเตอร์อย่างน้อย 1 ครั้ง ต่อสัปดาห์

2 ติดตั้งโปรแกรมอุดช่องโหว่ (patch) โดยการอัปเดตซอฟต์แวร์และโปรแกรมประยุกต์ต่างๆ ให้ใหม่อยู่เสมอ เช่น ระบบปฏิบัติการโปรแกรม Internet Explorer (IE) และ โปรแกรม Microsoft Office เป็นต้น



การอัปเดต Windows 2000

3 ปรับแต่งให้ซอฟต์แวร์ที่ใช้งานปลอดภัยสูงที่สุด
- ปรับ Security Zone ให้เป็น High Security

ภาพแสดงการปรับแต่งค่า Security Zone

- ปรับแต่งไม่ให้โปรแกรมที่ใช้อ่าน e-mail รันไฟล์แนบ (Attachment) โดยอัตโนมัติ
- ถ้าใช้ Microsoft Office ไม่ควรอนุญาตให้รันมาโคร (macro)
- ปิด Service ของระบบปฏิบัติการที่ไม่จำเป็น เช่น DCOM RPC เป็นต้น
- ตั้งค่าของระบบปฏิบัติการให้แสดงไฟล์ที่มีอยู่ทั้งหมด และแสดงนามสกุลของไฟล์ด้วย โดยปรับค่าการทำงานที่ Folder Options ใน Tools ของ Windows Explorer

4 ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูล (Media) ต่างๆ

- เช่น แผ่นฟล็อปปี้ดิสก์ แผ่นซีดี แผ่นดีวีดี เทปแบ็กอัป เป็นต้น
- สแกนหาไวรัสจากสื่อบันทึกข้อมูล ก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่น่าสงสัย เช่น .pif เป็นต้น รวมทั้งไฟล์ที่มีนามสกุลซ้อนกัน เช่น .jpg.exe, .gif.scr, txt.exe เป็นต้น ให้ลบไฟล์นั้นทิ้งทันที
- ไม่ใช้สื่อบันทึกข้อมูล ที่ไม่ทราบแหล่งที่มา

5 ใช้ความระมัดระวังในการเปิดอ่าน e-mail

- อย่าเปิดไฟล์ที่แนบมากับ e-mail จนกว่าจะรู้ที่มา
- อย่าเปิดอ่าน e-mail ที่มี Subject ที่เป็นข้อความจูงใจ เช่น ภาพเด็ด รหัสผ่าน เป็นต้น
- ลบ e-mail ที่ไม่ทราบแหล่งที่มาทิ้งทันที เพื่อตัดปัญหาทั้งปวง
- อัปเดตโปรแกรมที่ใช้อ่าน e-mail เช่น Outlook Express, Microsoft Outlook เป็นต้น

6 ตระหนักถึงความเสี่ยงของไฟล์ที่ดาวน์โหลด หรือได้รับจากทางอินเทอร์เน็ต
- ไม่ควรเปิดไฟล์ที่แนบมากับโปรแกรมที่ใช้สนทนา เช่น ICQ, MSN, IRC เป็นต้น หรือการแลกเปลี่ยนไฟล์ โดยเฉพาะไฟล์ที่สามารถรันได้ เช่น ไฟล์ที่มีนามสกุล .exe, .pif, .com, .bat, .vbs เป็นต้น โดยไม่ได้ตรวจสอบแหล่งที่มาก่อน
- ไม่ควรเข้าเว็บไซต์ที่มากับ e-mail หรือโปรแกรมสนทนาต่างๆ รวมทั้งโฆษณาชวนเชื่อ หรือหน้าเว็บที่ปรากฏขึ้นมาโดยไม่ได้ตั้งใจ
- ไม่ดาวน์โหลดไฟล์ต่างๆ จากเว็บไซต์ที่ไม่มั่นใจ หรือไม่น่าเชื่อถือ
- ติดตามข่าวสารข้อมูลการแจ้งเตือนไวรัสจากแหล่งข้อมูลด้านความปลอดภัยอยู่เสมอ

ตัวอย่าง e-mail ที่มีไฟล์หนอนแนบมา (W32.Bagle.H@mm)

- หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น ถ้าต้องแชร์ไฟล์ ควรแชร์แบบอ่านอย่างเดียว และตั้งรหัสผ่านด้วย
- หลีกเลี่ยงโปรแกรมประเภทที่ใช้แชร์ไฟล์แบบ Peer-to-Peer เช่น KaZaa เนื่องจากมีความปลอดภัยต่ำ

7 กำหนดนโยบายด้านการบริหารจัดการไวรัสคอมพิวเตอร์ขององค์กร
- สำรองข้อมูลสำคัญไว้เสมอ
- ควรจำกัดจำนวนผู้ใช้งานเครื่องคอมพิวเตอร์แต่ละเครื่อง
- ให้ทำการสแกน e-mail เพื่อตรวจสอบหาไวรัส ก่อนส่งเข้าสู่ระบบ
- ห้ามหรือควบคุมการรับ-ส่ง เอกสารที่ลงท้ายด้วย .exe .vbs ฯลฯ ในองค์กร
- ถ้าสงสัยว่าเครื่องติดไวรัสและไม่สามารถดำเนินการเองได้ ให้สอบถามเจ้าหน้าที่ดูแลระบบ หรือผู้ที่เกี่ยวข้องดำเนินการโดยด่วน
- ตรวจสอบการดาวน์โหลดไฟล์ และการนำโปรแกรมต่างๆ มาใช้ในองค์กร
- จัดการอบรมให้ความรู้เกี่ยวกับไวรัสแก่พนักงานในองค์กร

คาถาป้องกันไวรัส ไม่ใช้แผ่นมั่ว ไม่ซัวร์อย่าเปิด อย่าละเมิด Security (Policy) ติดตามข่าวสารไวรัสตีๆ มีการสำรองข้อมูลที่สำคัญ

แหล่งที่มา: วิธีป้องกันตนเองจากไวรัสคอมพิวเตอร์: http://www.thaicert.nectec.or.th/paper/virus/protectvirus.php

งานเทคโนโลยีสารสนเทศเพื่อความมั่นคง
ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT)
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
112 อุทยานวิทยาศาสตร์ประเทศไทย ถนนพหลโยธิน
ตำบลคลองหนึ่ง อำเภอคลองหลวง จังหวัดปทุมธานี 12120
โทรศัพท์ 02-564-6900 โทรสาร 02-564-6901..2

http://www.nectec.or.th/

สวทช NSTDA ECTI-21 NECTEC