



แนวทางปฏิบัติในการป้องกันไวรัสคอมพิวเตอร์ของกรมที่ดิน

ความรู้เกี่ยวกับไวรัสคอมพิวเตอร์

ไวรัสคอมพิวเตอร์ คือโปรแกรมที่มีผู้เขียนขึ้นมาเพื่อขัดขวางการทำงานของคอมพิวเตอร์ เช่น ขัดขวางการเข้าถึง (access) ข้อมูลในหน่วยความจำ ขัดขวางการอ่านเพิ่มข้อมูลจากฮาร์ดดิสก์ ขัดขวางการใช้งานอุปกรณ์ต่อพ่วง เช่น พรินเตอร์ สแกนเนอร์ ทำให้เสมือนว่าใช้งานกับคอมพิวเตอร์ไม่ได้ จนกระทั่งทำลายแฟ้มข้อมูล หรือทำให้คอมพิวเตอร์ทำงานผิดปกติไปจากเดิม

ความเสียหายที่เกิดจากไวรัส หากเครื่องคอมพิวเตอร์ของท่านมีอาการดังต่อไปนี้ ให้สันนิษฐานไว้ก่อนว่าเครื่องคอมพิวเตอร์ของท่านอาจติดไวรัสแล้ว เช่น

- การทำงานของคอมพิวเตอร์ช้ากว่าปกติ
- คอมพิวเตอร์หยุดทำงานโดยไม่ทราบสาเหตุ
- ข้อมูลหายไปโดยไม่ทราบสาเหตุ
- ส่งเสียง หรือมีการรันโปรแกรม หรือมีข้อความแปลกๆแสดงขึ้นมา
- ไดรฟ์ต่าง ๆ เม้าส์ คีย์บอร์ดหรือฮาร์ดดิสก์หยุดทำงานโดยไม่ทราบสาเหตุ
- ไฟล์ในแผ่นดิสก์ หรือฮาร์ดดิสก์ถูกเปลี่ยนเป็นขยะ
- เครื่องคอมพิวเตอร์ไม่สามารถ Boot ขึ้นมาใช้งานได้
- ใช้เวลานานผิดปกติในการเรียกโปรแกรมต่าง ๆ ขึ้นมาทำงาน
- ขนาดของโปรแกรมใหญ่ขึ้น
- วันเวลาของโปรแกรมเปลี่ยนไป
- ไฟแสดงสถานะ การทำงานของดิสก์ติดค้างนานกว่าที่เคยเป็น
- ขนาดของหน่วยความจำเหลือน้อยผิดปกติโดยหาเหตุผลไม่ได้
- เครื่องบูทตัวเองโดยไม่ได้สั่ง



วิธีการป้องกันไวรัสคอมพิวเตอร์

1. ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตข้อมูลไวรัสอยู่เสมอ
2. ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสบนเครื่องคอมพิวเตอร์อย่างน้อย 1 ครั้งต่อสัปดาห์
3. ระมัดระวังจากการเปิดไฟล์จากสื่อบันทึกข้อมูล (Media) ต่าง ๆ
 - เช่น แผ่นซีดี แผ่นบันทึกข้อมูลแบบ USB เป็นต้น
 - สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
 - ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลก ๆ ที่น่าสงสัย เช่น .pif เป็นต้น รวมทั้งไฟล์ที่มีนามสกุลซ้อนกัน เช่น .jpg.exe, .gif.scr, .txt.exe เป็นต้น
 - ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา
4. ใช้ความระมัดระวังในการเปิดอ่าน e-mail
 - อย่าเปิดไฟล์ที่แนบมากับ e-mail จนกว่าจะรู้ที่มา
 - อย่าเปิดอ่าน e-mail ที่มี Subject ที่เป็นข้อความจูงใจ เช่น ภาพเด็ด รหัสผ่าน เป็นต้น
 - ลบ e-mail ที่ไม่ทราบแหล่งที่มาทั้งหมดเพื่อตัดปัญหาทั้งปวง
 - อัปเดตโปรแกรมที่ใช้อ่าน e-mail เช่น Outlook Express, Microsoft Outlook เป็นต้น
5. ตระหนักถึงความเสี่ยงของไฟล์ที่ดาวน์โหลด หรือได้รับจากทางอินเทอร์เน็ต
 - ไม่ควรเปิดไฟล์ที่แนบมากับโปรแกรมที่ใช้สนทนา เช่น ICQ, MSN เป็นต้น หรือแลกเปลี่ยนไฟล์ โดยเฉพาะไฟล์ที่สามารถรันได้ เช่น ไฟล์ที่มีนามสกุล .exe, .pif, .com, .bat, .vbs เป็นต้น โดยไม่ได้ตรวจสอบแหล่งที่มาก่อน
 - ไม่ควรเข้าเว็บไซต์ที่มากับ e-mail หรือโปรแกรมสนทนาต่าง ๆ รวมทั้งโฆษณาชวนเชื่อ หรือหน้าเว็บที่ปรากฏขึ้นมาโดยไม่ได้ตั้งใจ
 - ไม่ดาวน์โหลดไฟล์ต่าง ๆ จากเว็บไซต์ที่ไม่มั่นใจ หรือไม่น่าเชื่อถือ
 - ติดตามข่าวสารข้อมูลการแจ้งเตือนไวรัสจากแหล่งข้อมูลด้านความปลอดภัยอยู่เสมอ
 - หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น ถ้าต้องแชร์ไฟล์ ควรแชร์แบบอ่านอย่างเดียวและตั้งรหัสผ่านด้วย
 - หลีกเลี่ยงโปรแกรมประเภทที่ใช้แชร์ไฟล์แบบ Peer-to-Peer เช่น KaZaa เนื่องจากมีความปลอดภัยต่ำ



สำนักเทคโนโลยีสารสนเทศ

6. กำหนดนโยบายด้านการบริหารจัดการไวรัสคอมพิวเตอร์ของหน่วยงาน

- ให้ปฏิบัติตาม ระเบียบกรมที่ดินว่าด้วยการรักษาความมั่นคงปลอดภัย พ.ศ. ๒๕๕๔ หมวด ๒
- สำรองข้อมูลไว้เสมอ
- ควรจำกัดจำนวนผู้ใช้งานเครื่องคอมพิวเตอร์แต่ละเครื่อง
- ให้ทำการสแกน e-mail เพื่อตรวจสอบหาไวรัส ก่อนส่งเข้าสู่ระบบ
- ห้ามหรือควบคุมการรับ-ส่ง เอกสารที่ลงท้ายด้วย .exe .bat .com .vbs ฯลฯ ในองค์กร
- ถ้าสงสัยว่าเครื่องติดไวรัสและไม่สามารถดำเนินการเองได้ ให้สอบถามเจ้าหน้าที่ดูแลระบบ หรือผู้ที่เกี่ยวข้องดำเนินการโดยด่วน
- ตรวจสอบการดาวน์โหลดไฟล์ และการนำโปรแกรมต่าง ๆ มาใช้ในองค์กร

ติดต่อสำนักเทคโนโลยีสารสนเทศ กรมที่ดิน

เว็บไซต์ Intranet สำนักเทคโนโลยีสารสนเทศ <http://172.29.3.11>

เว็บไซต์มาตรการด้านความมั่นคงปลอดภัยระบบสารสนเทศ กรมที่ดิน
<http://dolwms.dol.go.th:8081/dolsurvey/dolsecure>

ฝ่าย /กลุ่ม /ส่วน	Voice (ADSL VPN)	โทรศัพท์
ฝ่ายปฏิบัติการคอมพิวเตอร์	000001-000003	0-2503-3369 0-2984-0860
ส่วนระบบงานคอมพิวเตอร์		
- กลุ่มระบบงานคอมพิวเตอร์ด้านทะเบียน	000004-000007	0-2503-2110-9 ต่อ 502-503
- กลุ่มระบบงานคอมพิวเตอร์ด้านแผนที่	000009	0-2984-0819
ส่วนสารสนเทศ		
	000008	0-2503-2110-9 ต่อ 507-508, 512