

แนวทางปฏิบัติในการป้องกันไวรัสคอมพิวเตอร์ ศูนย์สนับสนุนบริการสุขภาพที่ ๑

ไวรัสคอมพิวเตอร์ (Computer Virus)

คือ โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในเครื่องคอมพิวเตอร์ และถ้ามีโอกาสก็สามารถแทรกเข้าไปติดอยู่ในระบบคอมพิวเตอร์อื่นๆ ซึ่งอาจเกิดจากการนำเอาแผ่นดิสก์ หรือ แฟลชไดรฟ์ที่ติดไวรัสจากเครื่องหนึ่งไปใช้กับอีกเครื่องหนึ่ง การที่คอมพิวเตอร์ใดติดไวรัส หมายความว่าไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำคอมพิวเตอร์เครื่องนั้นเรียบร้อยแล้ว การที่ไวรัสจะเข้าไปอยู่ในหน่วยความจำได้นั้นจะต้องมีการถูกเรียกใช้ให้ทำงาน ซึ่งโดยปกติแล้วผู้ใช้มักจะไม่รู้ตัวเลยว่า ขณะที่ตนเรียกใช้โปรแกรมหรือเปิดไฟล์ใดๆ ขึ้นมาทำงาน ก็ได้เรียกไวรัสขึ้นมาทำงานด้วย จุดประสงค์การทำงานของไวรัสแต่ละตัวขึ้นอยู่กับผู้เขียนโปรแกรมไวสนั้น เช่น อาจสร้างไวรัสให้ไปทำลายโปรแกรมหรือข้อมูลอื่นๆ ที่อยู่ในเครื่องคอมพิวเตอร์ หรือ แสดงข้อความวิ่งไปมาบนหน้าจอคอมพิวเตอร์ เป็นต้น (<http://th.wikipedia.org/wiki/ไวรัสคอมพิวเตอร์>)

ผลกระทบจากไวรัสคอมพิวเตอร์ (Computer Virus Affected)

เครื่องคอมพิวเตอร์เมื่อติดไวรัสคอมพิวเตอร์แล้ว มักจะมีการทำงานที่ผิดปกติไปจากเดิม ซึ่งอาการของเครื่องคอมพิวเตอร์ที่มักจะเกิดขึ้นเมื่อติดไวรัส มีดังต่อไปนี้

- ✓ คอมพิวเตอร์ทำงานช้าผิดปกติ
- ✓ มีข้อความแปลกๆ แสดงขึ้นมาให้เห็นอยู่ประจำ
- ✓ คอมพิวเตอร์หยุดทำงานบ่อยครั้ง โดยไม่ทราบสาเหตุ
- ✓ ข้อมูลหายหรือถูกซ่อนโดยไม่ทราบสาเหตุ
- ✓ มีการเปิดโปรแกรมที่ไม่รู้จักขึ้นมาทำงานอัตโนมัติ
- ✓ อุปกรณ์ต่อพ่วงหยุดทำงานโดยไม่ทราบสาเหตุ
- ✓ ไฟล์ในสื่อบันทึกข้อมูล หรือ Hard Disk ถูกเปลี่ยนเป็นไฟล์ขยะ
- ✓ เครื่องคอมพิวเตอร์ไม่สามารถ Boot ได้ (เช่น เปิดเครื่องแล้วจอดำ ไม่ยอมเข้าหน้าวินโดว)
- ✓ ใช้เวลานานผิดปกติในการเรียกโปรแกรมต่างๆ ขึ้นมาทำงาน
- ✓ หน่วยความจำหลัก (Ram) หรือหน่วยประมวลผลกลาง (CPU) ทำงานหนักอยู่ตลอดเวลา
- ✓ นามสกุลของไฟล์ต่างๆ มีการเปลี่ยนแปลง เช่น test.jpg --> test.exe

วิธีการป้องกันไวรัสคอมพิวเตอร์(Computer Virus Protection)

๑. ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตฐานข้อมูลไวรัสใหม่ๆ อยู่เสมอ (Install Antivirus Program)
๒. สแกนไวรัสในเครื่องคอมพิวเตอร์อย่างน้อย ๑ ครั้งต่อสัปดาห์ โดยใช้โปรแกรมจากข้อ ๑ (Scan Virus at least ๑ time/week)
๓. 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
 - ไม่ใช่สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา
๔. ใช้ความระมัดระวังในการเปิดอ่าน E-mail
 - อย่างเปิดไฟล์ที่แนบมากับ E-mail จนกว่าจะรู้ที่มา
 - อย่าเปิดอ่าน E-mail ที่มี Subject ที่มีข้อความจูงใจ
 - ลบ E-mail ที่ไม่ทราบแหล่งที่มาทิ้งทันที เพื่อตัดปัญหาทั้งปวงที่มาจากผู้ไม่หวังดี
๕. ตระหนักถึงความเสี่ยงของไฟล์ที่ดาวน์โหลด หรือได้รับจากทางอินเทอร์เน็ต
 - ไม่ควรเปิดไฟล์ที่แนบมากับโปรแกรมที่ใช้สนทนา เช่น Skype, Facebook, ICQ, Web Chat ต่างๆ ที่มีการแลกเปลี่ยนไฟล์ โดยเฉพาะไฟล์ที่สามารถรันได้ เช่น ไฟล์ที่มีนามสกุล .exe, .pif, .com, .bat, .vbs เป็นต้น (โดยไม่ทราบแหล่งที่มา)
 - ไม่ควรเข้าเว็บไซต์ที่มากับ E-mail หรือโปรแกรมสนทนาต่างๆ รวมทั้งโฆษณาชวนเชื่อ หรือหน้าเว็บที่ปรากฏขึ้นมาโดยไม่ได้ตั้งใจ
 - ไม่ดาวน์โหลดไฟล์ต่างๆ จากเว็บไซต์ที่ไม่มั่นใจ หรือไม่น่าเชื่อถือ
 - หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น ถ้าต้องการแชร์ไฟล์ ควรตั้งค่าการแชร์แบบอ่านอย่างเดียว (Read only) หรืออาจตั้งรหัสผ่านด้วยก็ได้

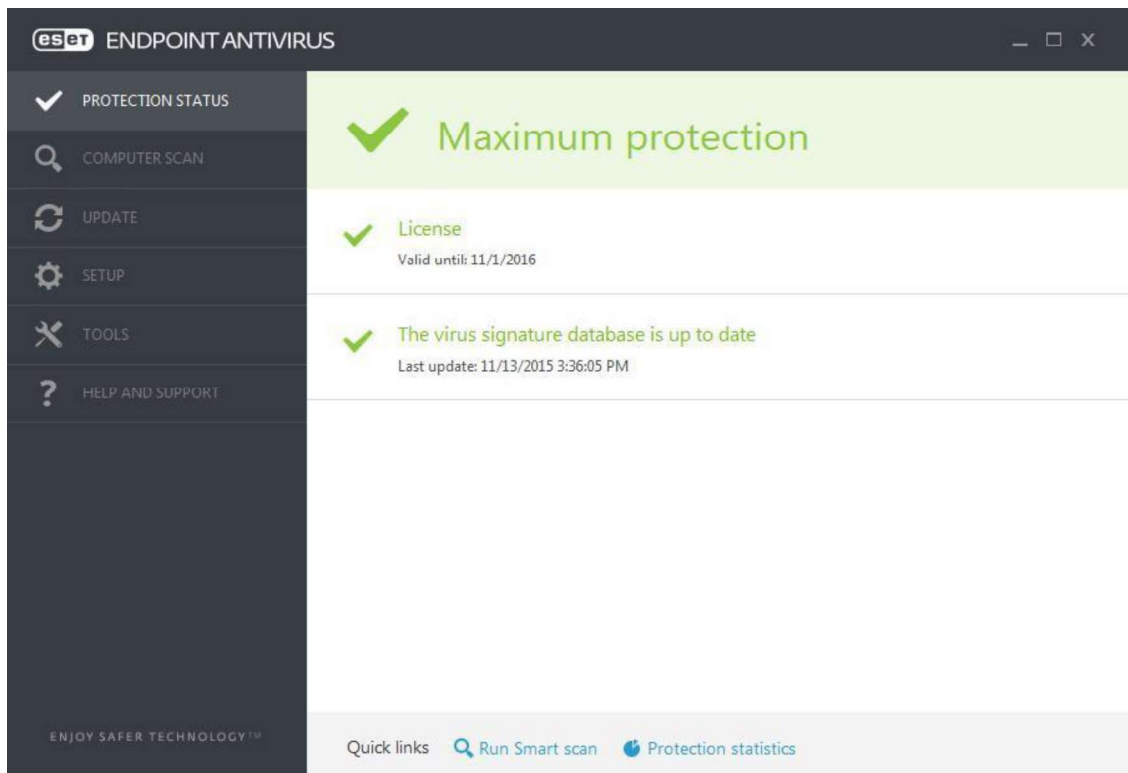
ข้อมูลโปรแกรมป้องกันไวรัส (Virus Program)

โปรแกรมป้องกันไวรัสที่ทางศูนย์สนับสนุนบริการสุขภาพที่ ๑ ได้ติดตั้งใช้งาน คือ ESET Endpoint Antivirus

วิธีการใช้งานโปรแกรมป้องกันไวรัส Antivirus ESET Endpoint Antivirus

1. คำอธิบายเมนูหน้าต่างหลักของโปรแกรม

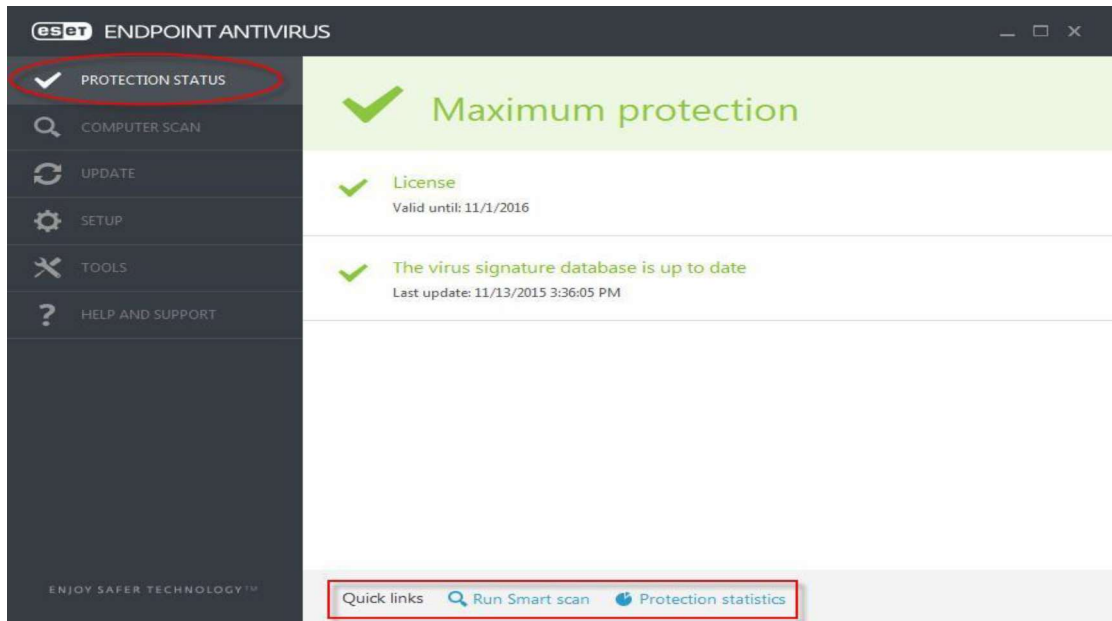
- Protection status แสดงข้อมูลเกี่ยวกับสถานะการป้องกันของ ESET Endpoint Antivirus
- Computer scan ตัวเล็กลูกนี้จะช่วยให้คุณสมารถกำหนดค่าและเริ่มต้นการสแกนแบบสมาร์ท การสแกนแบบกำหนดเอง หรือการสแกนสื่อที่ถอดเข้าออกได้ คุณยังสามารถทำการสแกนล่าสุดซ้ำได้
- Update แสดงข้อมูลเกี่ยวกับการอัปเดตฐานข้อมูลไวรัส
- Setup ปรับตั้งค่าการรักษาความปลอดภัยสำหรับคอมพิวเตอร์, เว็บและอีเมล
- Tools การเข้าถึงไฟล์ บันทึก, สถิติการป้องกัน, กระบวนการที่ทำงานอยู่, ติดตามการทำงาน, ตัววางกำหนดการ, กักเก็บไฟล์ไวรัส, ESET SysInspector (เครื่องมือช่วยตรวจสอบข้อมูลในเครื่อง), ESET SysRescue (สร้างซีดีบูตอัพ) และการส่งไฟล์ตัวอย่างไปวิเคราะห์
- Help and support เรียกดูการเข้าถึงไฟล์วิธีใช้, ฐานความรู้ของ ESET และเว็บไซต์ของ ESET นอกจากนี้ยังมีลิงค์เพื่อเปิดคำร้องขอรับการสนับสนุนจากฝ่ายดูแลลูกค้า เครื่องมือสนับสนุนและข้อมูลเกี่ยวกับการเปิดใช้งานผลิตภัณฑ์



หน้าจอสถานะการป้องกันจะแจ้งให้คุณทราบเกี่ยวกับระดับความปลอดภัยและการป้องกันในปัจจุบันของ คอมพิวเตอร์ สถานะการป้องกันสูงสุดสีเขียว แสดงว่ามีการป้องกันสูงสุด

2. การทำงานของหน้าต่างหลักของโปรแกรม ESET Endpoint Antivirus

1. Protection status (สถานะการป้องกัน) เมนูนี้จะแจ้งให้ทราบเกี่ยวกับระดับการรักษาความปลอดภัยและการป้องกันในปัจจุบันของคอมพิวเตอร์, ใบอนุญาต และสถานะการอัปเดตฐานข้อมูลไวรัสหากสถานะเป็นสีเขียวแสดงว่ามีการป้องกันขั้นสูงสุดและตัวโปรแกรมทำงานปกติ นอกจากนี้หน้าต่างสถานะยังแสดงเมนูที่ใช้อยู่ในโปรแกรม ESET Endpoint Antivirus ดังภาพ



หน้าต่างสถานะยังแสดงข้อมูลเกี่ยวกับการอัปเดตล่าสุด และมีลิงก์ด่วนไปยังคุณลักษณะที่ใช้อยู่ใน ESET Endpoint Antivirus

2. Computer scan (การสแกนคอมพิวเตอร์)

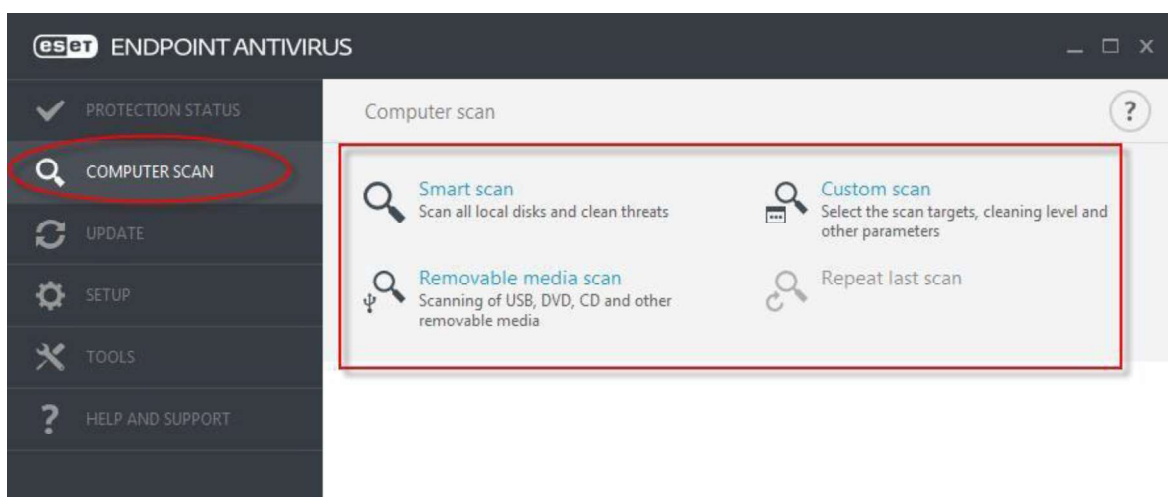
หลังจากการติดตั้งเสร็จสมบูรณ์แล้ว ESET Endpoint Antivirus จะดำเนินการสแกนคอมพิวเตอร์โดยอัตโนมัติเพื่อตรวจหาภัยคุกคาม นอกจากนี้ผู้ใช้งานยังสามารถสั่งสแกนคอมพิวเตอร์ได้ด้วยตัวเอง โดยสามารถเลือกการสแกนจาก 4 ตัวเลือกลงนี้

- **Smart scan** การสแกนแบบสมาร์ทจะช่วยให้คุณเริ่มต้นการสแกนคอมพิวเตอร์และกำจัดไฟล์ที่ติดไวรัสได้อย่างรวดเร็ว โดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ ข้อดีของการสแกนแบบสมาร์ท คือ ใช้งานง่าย และไม่ต้องมีการกำหนดค่าการสแกนโดยละเอียด การสแกนแบบสมาร์ทจะตรวจสอบทุกไฟล์ในไดรฟ์ในระบบรวมทั้งกำจัดหรือลบการแฝงตัวที่ตรวจพบโดยอัตโนมัติ

- **Custom scan** การสแกนที่กำหนดเองเป็นโซลูชันที่เหมาะสม หากคุณต้องการระบุพารามิเตอร์การสแกน เช่น เป้าหมายการสแกน และวิธีการสแกน ข้อดีของการสแกนที่กำหนดเอง คือ คุณสามารถกำหนดพารามิเตอร์ในรายละเอียดได้ คุณสามารถบันทึกการกำหนดค่าไว้ไปยังโปรไฟล์การสแกนที่ผู้ใช้กำหนดซึ่งเป็ประโยชน์ถ้ามีการสแกนซ้ำโดยใช้พารามิเตอร์เดียวกัน (เป็นการสแกนโดยเลือกไดรฟ์, ไฟล์ หรืออุปกรณ์)

- **Removable media scan** การสแกนสื่อที่ถอดเข้าออกได้ เช่น ซีดี/ดีวีดี/USB เมื่อมีการเชื่อมต่อ อุปกรณ์ USB กับคอมพิวเตอร์ คุณสามารถสั่งสแกนได้ทันที

- **Repeat last scan** ทำการสแกนครั้งล่าสุดซ้ำอีกครั้ง



3. Update (การอัปเดต)

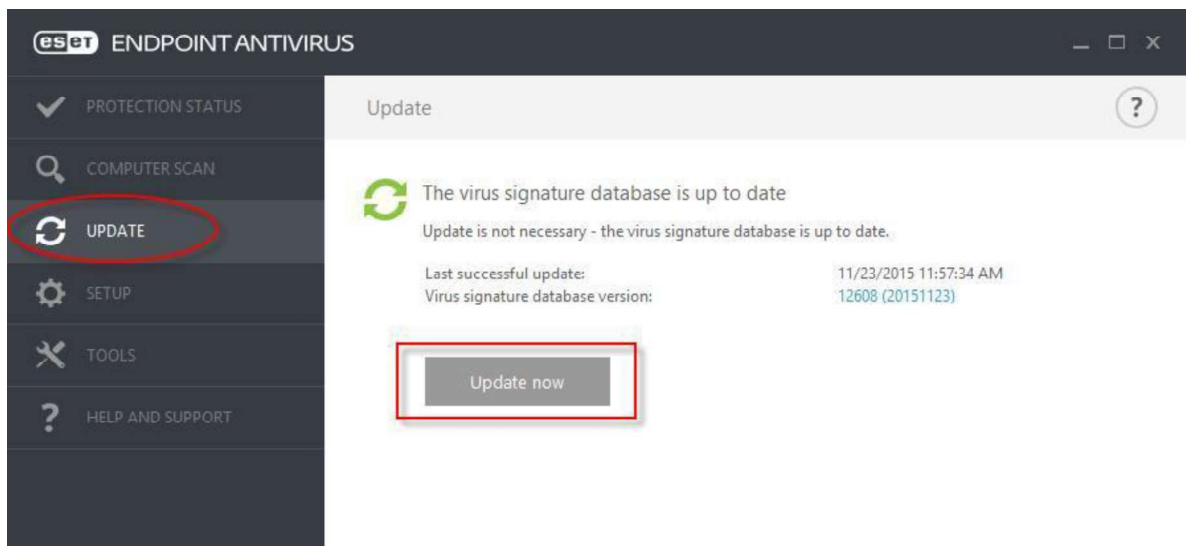
การอัปเดตเป็นประจำ เป็นวิธีการที่ดีที่สุดเพื่อให้คอมพิวเตอร์ มีระดับการรักษาความปลอดภัยสูงสุด โมดูลการอัปเดตจะทำให้มั่นใจว่าโปรแกรม ESET Endpoint Antivirus มีความทันสมัยอยู่เสมอโดยใช้ 2 วิธี คือ

- การอัปเดตฐานข้อมูลไวรัส
- การอัปเดตองค์ประกอบของโปรแกรม

เมื่อคลิกเมนู Update ในหน้าต่างโปรแกรมหลัก จะพบสถานะการอัปเดตในปัจจุบัน รวมถึงวันที่และเวลาของการอัปเดตที่สำเร็จครั้งล่าสุด และแสดงว่าจะต้องมีการอัปเดตหรือไม่หน้าต่างหลักจะมีเวอร์ชันของ ฐานข้อมูลไวรัส เมื่อคลิกตัวเลขนี้จะลิงค์ไปยังเว็บไซต์ของ ESET ซึ่งจะแสดงฐานข้อมูลทั้งหมดที่เพิ่มขึ้นมา

- Last successful update – วันที่และเวลาล่าสุดที่อัปเดตฐานข้อมูล
- Version signature database version – หมายเลขฐานข้อมูลไวรัสที่อัปเดตไว้ล่าสุด ซึ่งเมื่อคลิกจะลิงค์ไปยังเว็บไซต์ของ ESET เพื่อดูรายการของฐานข้อมูลที่เพิ่มขึ้นมา

a. คลิกปุ่ม “Update now” เพื่อตรวจสอบการอัปเดตฐานข้อมูลไวรัสล่าสุด



b. กระบวนการอัปเดต หลังจากคลิก “Update now” กระบวนการดาวน์โหลดจะเริ่มต้น ทำงานจะแสดงแถบความคืบหน้าการดาวน์โหลด หากต้องการยกเลิกการอัปเดตให้คลิกปุ่ม “Cancel update”

