คู่มือการจัดการความรู้(KM)
ไวรัสคอมพิวเตอร์และสปายแวร์

สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย

คำนำ

ปัญหาเรื่องเครื่องคอมพิวเตอร์ติดไวรัสคอมพิวเตอร์และสปายแวร์ เป็นปัญหาที่สำคัญอย่างยิ่งต่อการทำงาน อาจทำให้เกิดความเสียหายต่อข้อมูล หรือทำลายโปรแกรม การจัดการความรู้เรื่องไวรัสคอมพิวเตอร์และสปายแวร์ จึงเป็นสิ่งที่จำเป็นและมีประโยชน์อย่างยิ่งต่อมหาวิทยาลัย สำนักงานจัดการระบบเทคโนโลยีสารสนเทศ จึงได้จัดโครงการอบรมเชิงสัมมนาเรื่อง “การจัดการความรู้เรื่อง Antivirus, Anti Spam” ขึ้นทำให้ได้คู่มือเล่มนี้ ใช้เป็นแนวทางการป้องกันและแก้ไขปัญหาการติดไวรัสคอมพิวเตอร์และสปายแวร์

ทีมงานจัดการความรู้
สำนักบริหารเทคโนโลยีสารสนเทศ
จุฬาลงกรณ์มหาวิทยาลัย

สารบัญ

1. ไวรัสคอมพิวเตอร์และสปายแวร์

ก่อนอื่นเรามาทำความรู้จักไวรัสคอมพิวเตอร์และกับสปายแวร์กันก่อน

ไวรัสคอมพิวเตอร์(Virus)คืออะไร

ไวรัสคอมพิวเตอร์ เป็นโปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในระบบคอมพิวเตอร์ได้และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่น ๆ ซึ่งอาจเกิดจากการนำเอาดิสก์เก็ตที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือระบบสื่อสารข้อมูลไวรัสก็อาจแพร่ระบาดได้เช่นกัน เมื่อไวรัสเข้ามาอยู่ในคอมพิวเตอร์แล้ว อาจจะทำความเสียหายแก่ข้อมูลในฮาร์ดดิสก์ หรือรบกวนการทำงานของระบบปฏิบัติการ การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงว่าไวรัสได้เข้าไปผังตัวอยู่ในหน่วยความจำ คอมพิวเตอร์ เรียบร้อยแล้ว

ประเภทของไวรัส

ไวรัสมีอยู่หลายประเภท โดยแบ่งเป็นประเภทใหญ่ๆ ได้ดังนี้

1. ไฟล์ไวรัส (File virus) เป็นประเภทไวรัสที่ใหญ่ที่สุด โดยไวรัสประเภทนี้จะซ่อนตัวเองไปกับไฟล์ ซึ่งโดยมากมักเป็นไฟล์ประเภทโปรแกรมที่มีนามสกุลเป็น com, exe, sys, dll

2. บู๊ตเซ็กเตอร์ไวรัส (Boot Sector Virus) เป็นไวรัสประเภทที่ติดทางแผ่นดิสก์เก็ตและฮาร์ดดิสก์ ตัวไวรัสจะทำงานโหลดตัวเองขึ้นมาก่อนระบบปฏิบัติการ ทุกครั้งที่เราเปิดเครื่อง ก็เท่ากับว่าเราไปปลุกให้ไวรัสขึ้นมาทำงานทุกครั้งก่อนการเรียกใช้โปรแกรมอื่นๆ

3. มาโครไวรัส (Macro Virus) เป็นไวรัสประเภทใหม่ที่ก่อกวนโปรแกรมสำนักงานต่างๆ เช่น MS Word, Excel, PowerPoint ซึ่งจะใช้ลักษณะพิเศษของโปรแกรมที่มีการเขียนโปรแกรมด้วยมาโคร เป็นชุดคำสั่งเล็กๆ ทำงานอัตโนมัติ มักจะทำให้ไฟล์มีขนาดใหญ่ขึ้นผิดปกติ การทำงานหยุดชะงักโดยไม่ทราบสาเหตุ หรือทำให้ไฟล์เสียหาย ขัดขวางกระบวนการพิมพ์ เป็นต้น

4. หนอนไวรัส (Worm) โดยที่จริงแล้วหนอนไวรัสยังไม่ถือว่าเป็นไวรัสเสียทีเดียว เนื่องจากจะไม่ติดกับโปรแกรมใด ๆ หนอนไวรัสอาจจะเป็นโปรแกรมหนึ่ง หรือชุดคำสั่งโปรแกรม ซึ่งสามารถทำสำเนาได้เอง และจะติดกับคอมพิวเตอร์ในระบบเครือข่าย (Network) เป้าหมายของหนอนไวรัสคือ การโจมตีผ่านเครือข่าย ซึ่งมีตั้งแต่ขัดขวางการทำงานไปจนถึงทำให้เครือข่ายล่ม

5. โทรจัน (Trojan) มีลักษณะและพฤติกรรมไม่แพร่เชื้อไปติดไฟล์อื่นๆ ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆได้ โทรจันเป็นโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้แฝงตัวเองเข้าไปในระบบและจะทำงานโดยการดักจับเอารหัสผ่านเข้าสู่ระบบต่างๆ และส่งกลับไปยังผู้ประสงค์ร้าย เพื่อเข้าใช้หรือโจมตีระบบในภายหลัง ซึ่งแฝงมาในหลายๆ รูปแบบ เช่น โปรแกรม หรือ การ์ดอวยพร เป็นต้น เพื่อดักจับ ติดตาม หรือควบคุมการทำงานของเครื่องคอมพิวเตอร์ที่ถูกคุกคาม

สปายแวร์ (Spyware) คืออะไร

สปายแวร์ คือ โปรแกรมที่แฝงเข้ามาในคอมพิวเตอร์ขณะที่คุณท่องอินเตอร์เน็ต เป็นโปรแกรมที่ถูกเขียนขึ้นมาสอดส่อง (สปาย) หรือดักจับข้อมูลการใช้งานเครื่องคอมพิวเตอร์ของคุณ นอกจากนี้อาจจะมีการสำรวจโปรแกรม และไฟล์ต่าง ๆ ในเครื่องเราด้วย และ สปายแวร์ นี้จะทำการส่งข้อมูลดังกล่าวไปในเครื่อง

ปลายทางที่โปรแกรมได้ระบุเอาไว้ ดังนั้นข้อมูลต่าง ๆ ในเครื่องของคุณอาจไม่เป็นความลับอีกต่อไป สปายแวร์อาจเข้ามาเพื่อโฆษณาสินค้าต่าง ๆ บางตัวก็สร้างความรำคาญเพราะจะเปิดหน้าต่างโฆษณาบ่อย ๆ แต่บางตัวร้ายกว่านั้น คือ ทำให้คุณใช้อินเตอร์เน็ทไม่ได้เลย

ประเภทของสปายแวร์

สปายแวร์ มีอยู่หลายประเภท โดยแบ่งเป็นประเภทต่างๆ ได้ดังนี้

1. Adware เป็นสปายแวร์ที่จะคอยส่งแบนเนอร์โฆษณามาที่คอมพิวเตอร์ของเรา สาเหตุที่เราจัดให้ Adware เป็นสปายแวร์ก็เพราะมีส่วนประกอบของโปรแกรมที่ทำให้สามารถติดตามข้อมูลของผู้ใช้และส่งข้อมูลนั้นออกไปที่อื่นได้

2. Dialer เป็นสปายแวร์ที่เคยอยู่บนเว็บโป๊ต่างๆ และใช้โมเด็มเครื่องเหยื่อหมุนโทรศัพท์ทางไกลต่อไปยังต่างประเทศ

3. Hijacker เป็นสปายแวร์ที่สามารถเปลี่ยนแปลง Start Page และ Bookmark บนเว็บบราวเซอร์ต่างๆ

4. BHO (Browser Helper Objects) เป็นสปายแวร์ที่ยัดเยียดฟังก์ชั่นที่ไม่พึงประสงค์ให้บนเว็บบราวเซอร์

5. Toolbar บางอย่างก็จัดเป็นสปายแวร์ที่ยัดเยียดเครื่องมือที่ไม่พึงประสงค์ให้บนเว็บบราวเซอร์ด้วย

2. อาการของเครื่องที่ติดไวรัสและสปายแวร์

อาการของการติดไวรัสนั้นมีมากมายขึ้นอยู่กับชนิดของไวรัสด้วย อาการที่สามารถสังเกตได้ว่าเครื่องคอมพิวเตอร์ติดไวรัสและสปายแวร์หรือไม่มีดังต่อไปนี้

1. เครื่องมีการรีสตาร์ทหรือเครื่องปิดตัวเองลงขณะที่กำลังใช้งานอยู่ หรือเมื่อเปิดเครื่องแล้วไม่สามารถบูตเข้าสู่วินโดวส์ได้

2. เกิดไฟล์ขึ้นเองโดยไม่ได้สร้างขึ้น เช่น Autorun.inf หรือไฟล์นามสกุล .vbs ปรากฏตามไดรฟ์ต่างๆ

3. เนื่อที่ในฮาร์ดดิสก์ลดลงโดยไม่ทราบสาเหตุ โดยไม่ได้ติดตั้งโปรแกรม หรือนำข้อมูลมาลงไว้

4. วินโดวส์แสดงไดอะล๊อกบ๊อกซ์ข้อความโดยไม่ทราบสาเหตุ หรือมีโปรแกรมบางตัวทำงานเองโดยไม่ได้เรียกใช้งาน

5. คอมพิวเตอร์ทำงานช้าอย่างผิดปกติ ทั้งๆ ที่ไม่ได้เปิดใช้โปรแกรมใดๆ

6. ไฟล์ข้อมูลมีขนาดใหญขึ้นมากแบบผิดปกติทุกครั้งที่ใช้งาน

7. เครื่องคอมพิวเตอร์เกิดอาการแฮงค์ (Hang) โดยไม่ทราบสาเหตุ

8. โปรแกรมป้องกันไวรัสไม่สามารถเปิดได้ หรือเปิดโปรแกรมต่างๆ ไม่ได้ หรือบางครั้งโปรแกรมที่ใช้ประจำหายไป

9. มี Pop up ขึ้นมาบ่อยๆ ในขณะที่เราเข้าเว็บ หรือถึงแม้จะไม่ได้ต่อ internet

10. toolbar มีแถบปุ่มเครื่องมือเพิ่มขึ้น โดยที่เราไม่ได้ติดตั้งอะไรเสริมเลย

11, หน้า Desktop มีไอคอนประหลาดๆ เพิ่มขึ้น

12.เมื่อเปิด Internet Explorer หน้าเว็บแรกที่พบแสดงเว็บอะไรก็ไม่รู้ ไม่เคยเห็นมาก่อน

3. การตรวจหาไวรัสคอมพิวเตอร์และสปายแวร์

วิธีการตรวจหาไวรัสคอมพิวเตอร์มี 2 วิธีดังนี้

1. การสแกน

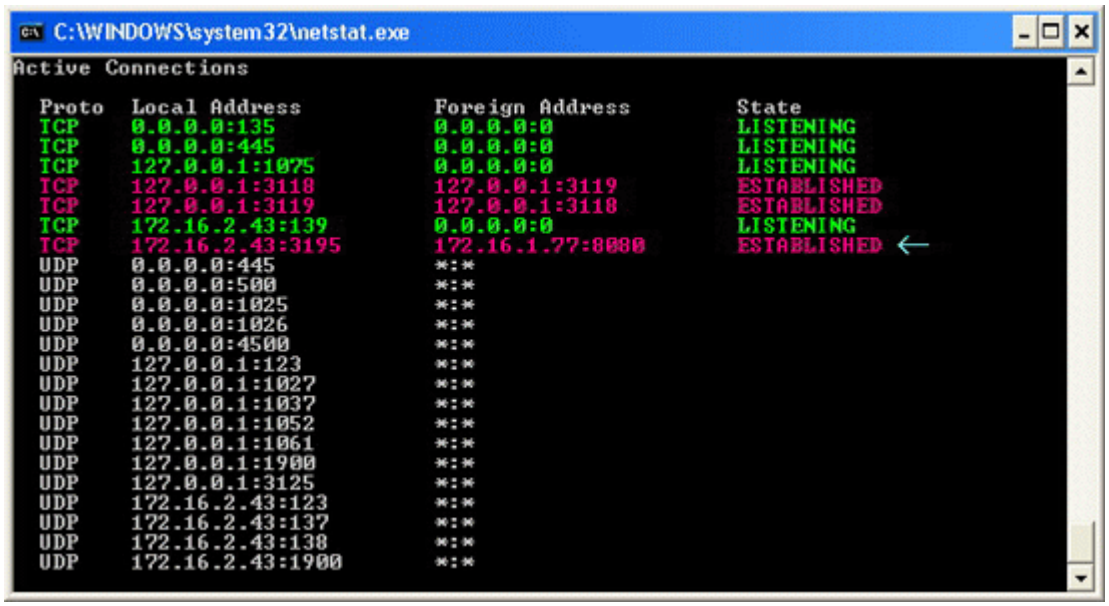
การใช้โปรแกรมในการตรวจหาไวรัส โดยการดึงโปรแกรมบางส่วนของตัวไวรัสมาเก็บไว้เป็นฐานข้อมูล ส่วนที่ดึงมานั้นเรียกว่าไวรัสซิกเนเจอร์ (Virus Signature) เมื่อโปรแกรมสแกนไวรัสถูกเรียกขึ้นมาทำงาน โปรแกรมจะเข้าไปตรวจหาไวรัสในหน่วยความจำ บู๊ตเซ็กเตอร์ และไฟล์โดยใช้ไวรัสซิกเนเจอร์ที่มีอยู่

จุดแข็ง สามารถตรวจสอบหาไวรัสที่มาใหม่ได้ทันที

จุดอ่อน ฐานข้อมูลที่เก็บไวรัสซิกเนเจอร์จะต้องทันสมัยอยู่เสมอ และครอบคลุดไวรัสทุกตัว และมากที่สุดด้วย ดังนี้การตรวจหาไวรัสแบบนี้จะขึ้นอยู่กับเทคนิคที่ใช้สร้างไวรัสกับโปรแกรมสแกนไววัสว่าแบบใดจะใช้ได้ผลมากกว่า

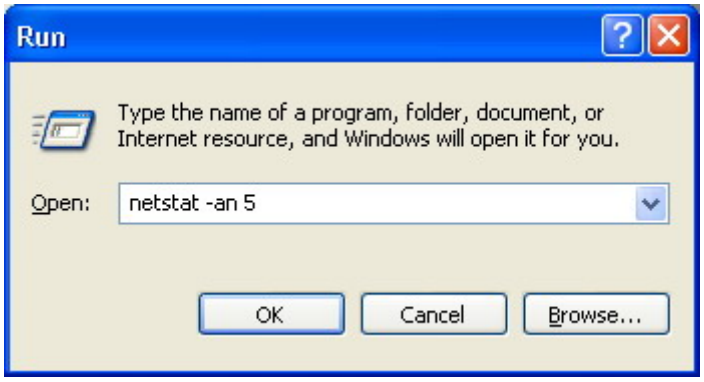
2. ใช้คำสั่ง netstat ที่มีในระบบปฏิบัติการ Windowa XP อยู่แล้ว ตรวจสอบ

netstat เป็นคำสั่งที่ใช้แสดงสถานะการเชื่อมต่อกับเครื่องคอมพิวเตอร์เตรื่องอื่นๆ โดยที่เราสนใจจะเป็นการเชื่อมต่ออินเทอร์เน็ตผ่านโปรโตคอล TCP/IP



สังเกตดูรูปคอลัมน์แรก (Proto) จะแสดงโปรโตคอลที่ใช้เชื่อมต่อ
คอลัมน์ที่สอง (Local Address) เป็น IP เครื่องเราเอง
คอลัมน์ที่สาม (Foreign Address) เป็น IP เครื่องอื่นที่ติดต่อกับเรา
คอลัมป์ที่สี่ (State) สถานะการเชื่อมต่อ ซึ่งจะมีหลายๆสถานะ แต่ที่จะขอกล่าวแบบง่ายๆมี 2 สถานะ
สถานะ LISTENING เป็นสถานะที่เปิดรอไว้ คอยคนอื่นมาเชื่อมต่อ
สถานะ ESTABLISHED เป็นสถานะที่กำลังเชื่อมต่ออยู่ ซึ่งสถานะนี้เองที่เราจะใช้ในการตรวจสอบโปรแกรม

ประเภท spyware โดยการดูว่ามีการเชื่อมต่อใดที่อยู่ในสถานะ ESTABLISHEDและเชื่อมต่อไปยังคอมพิวเตอร์เครื่องที่เราไม่รู้จัก (Foreign Address แปลกๆ) หรือไม่



เชื่อมต่ออินเทอร์เน็ต แล้วเรียกคำสั่ง netstat -an 5 จากหน้าจอ Run เพื่อตรวจสอบ Spyware ซึ่งถ้าจะโดนก็จะเห็นการเชื่อมต่อไปยังเครื่องแปลกๆ ที่เราไม่รู้จัก นั่นคือสัญญาณเตือนให้ทราบว่าขณะนี้เครื่องของคุณกำลังโดนดูดข้อมูลออกไป

4. เทคนิคการกำจัดไวรัสคอมพิวเตอร์และสปายแวร์

ใช้เครื่องมือในการกำจัดไวรัส Remove Tools

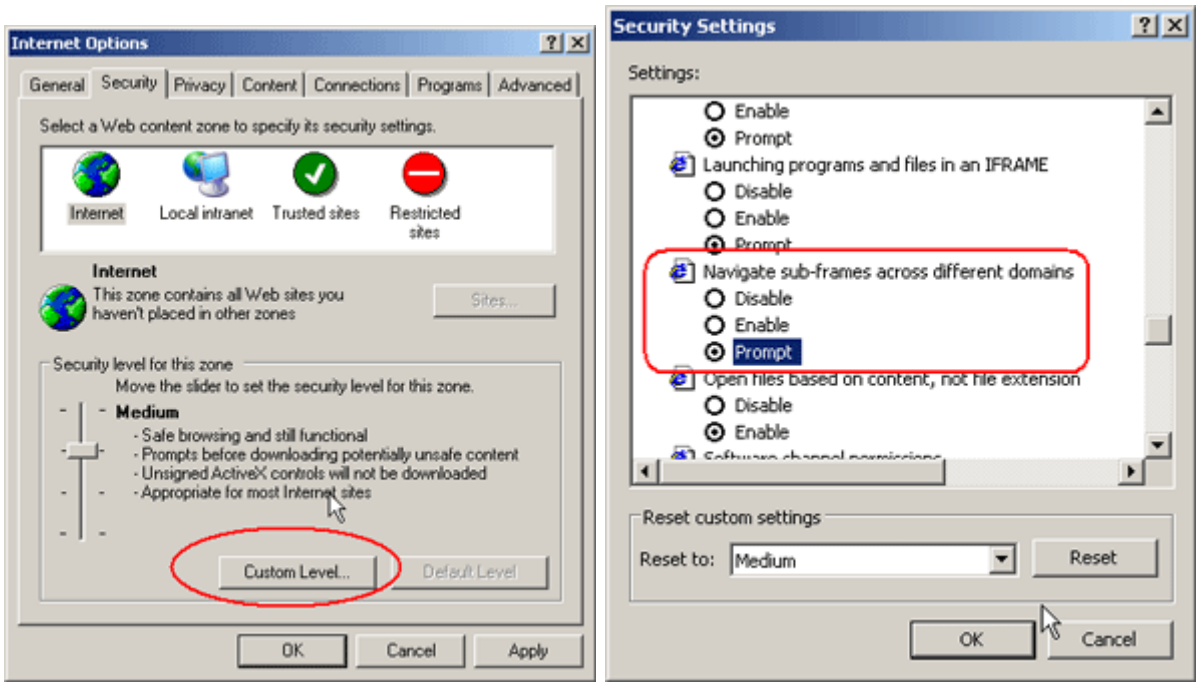
Remove Tools คือเครื่องมือในการกำจัดไวรัสในรูปแบบตัวต่อตัว หมายความว่า ถ้าเราทราบว่าไวรัสที่ติดนั้นคืออะไร แต่โปรแกรมเจ้ากรรมที่ใช้อยู่ ไม่สามารถกำจัดได้ ดังนั้น เราอาจจำเป็นต้อง download Remove Tools จากเว็บไซต์ค่ายๆ มาจัดการโดยเฉพาะ เช่น http://securityresponse.symantec.com/avcenter/tools.list.html

จุดแข็ง สามารถกำจัดไวรัสได้ด้วยโปรแกรมเฉพาะ และกำจัดได้หมด

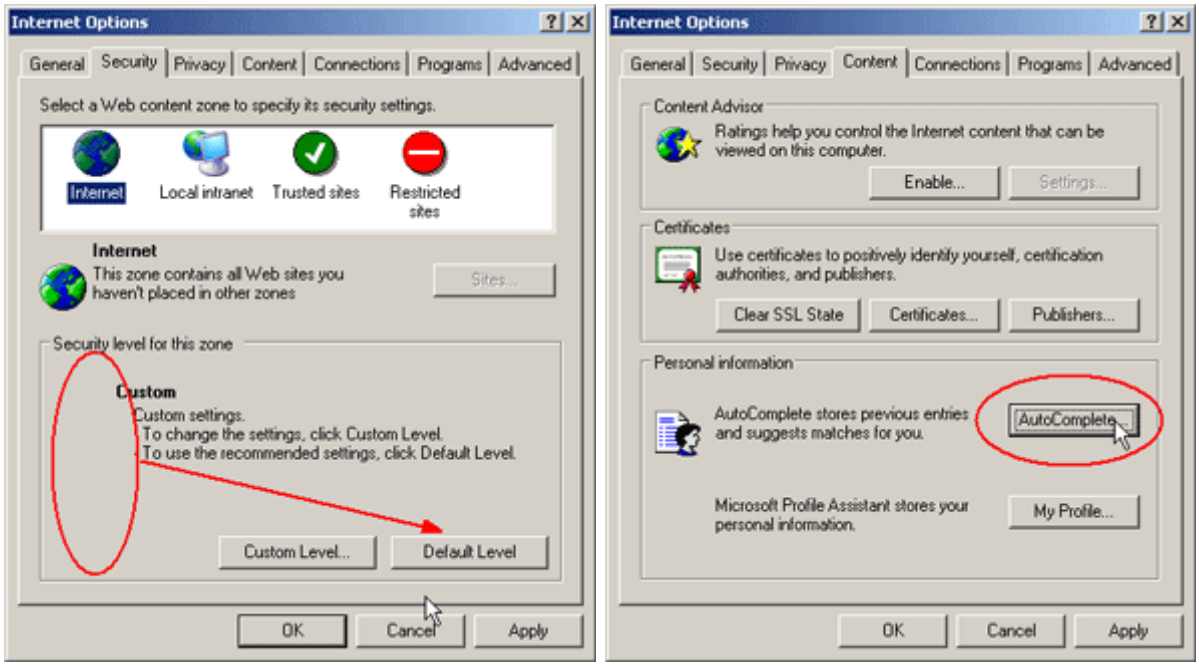
จุดอ่อน ไม่สามารถป้องกันไวรัสแบบ Real Time ได้ เพราะใช้สำหรับตรวจสอบไวรัสเป็นรายครั้ง ไม่มีการอัปเดทโปรแกรมผ่านทางอินเตอร์เน็ต ต้องเข้าไปเว็บไซต์นั้นๆ ใหม่ และ download มาใหม่ การกำจัดไวรัส บางครั้งจำเป็นต้องเข้าใน Windows Save Mode เท่านั้น และกำจัดไวรัสได้เฉพาะบางตัว จึงจำเป็นต้องรู้ชื่อไวรัสก่อนเพื่อจะได้เลือก download โปรแกรมที่ถูกต้อง และสามารถกำจัดให้หมดสิ้นได้

การตั้งค่าความปลอดภัยใน Internet Explorer

การตั้งค่าในบราวเซอร์ Internet Explorer เป็นสิ่งที่จำเป็นและมีความสำคัญ ปัญหาหลายๆ อย่างเกิดจากช่องโหว่เหล่านี้มากมายทีเดียว เพราะผู้เขียนโปรแกรมไวรัสและสปายแวร์มีความสามารถมากขึ้นจึงสามารถหารูโหว่เข้าโจมตีได้ง่ายขึ้น เราจะทำการปรับตั้งค่าบางส่วนได้ดังนี้ (ตัวอย่างนี้ใช้ IE 6.0 SP2)

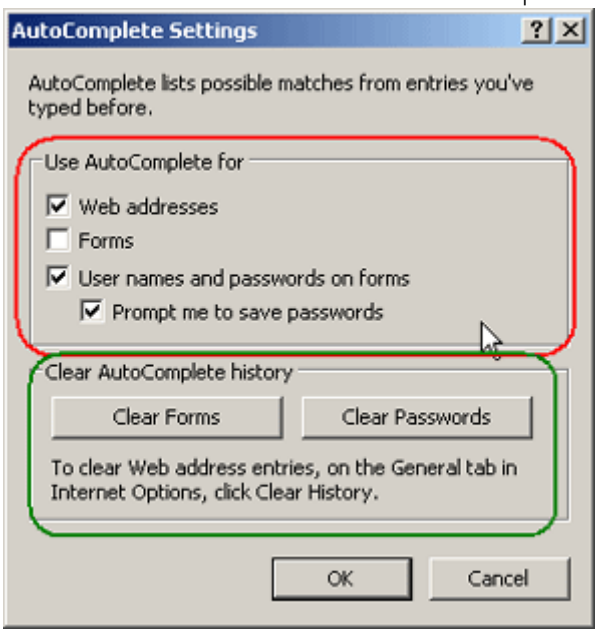


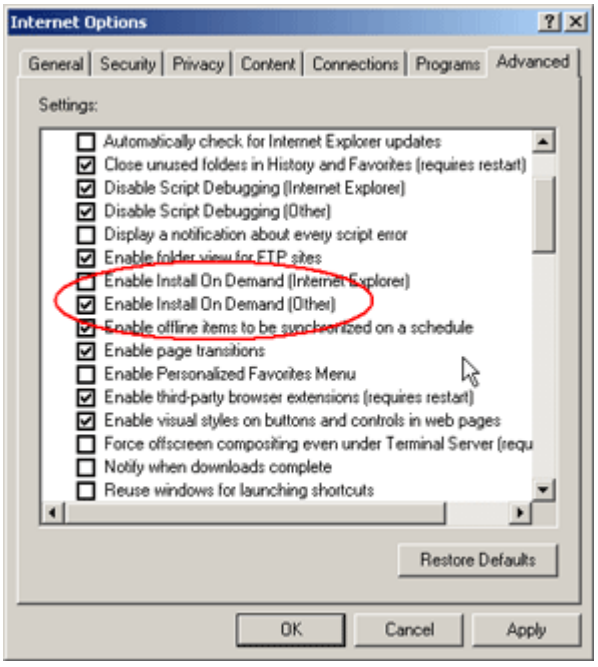
จากเมนูของ IE เลือก Tools --> Internet Options --> Security ค่าปกติของบราวเซอร์จะอยู่ที่ Medium ถ้าตั้งไว้สูงเป็น High อาจจะเข้าชมบางเว็บไม่ได้เลย ให้คลิกที่ปุ่ม Custom Level เพื่อการตั้งค่าดังรูปที่ 2 ทางขวามือ ให้เลื่อนรายละเอียดลงไปด้านล่างถึงหัวข้อ Navigate sub-frames across different domains ให้ตั้งค่าไว้ที่ Prompt แล้วคลิกปุ่ม OK เพื่อการเก็บค่านี้ไว้



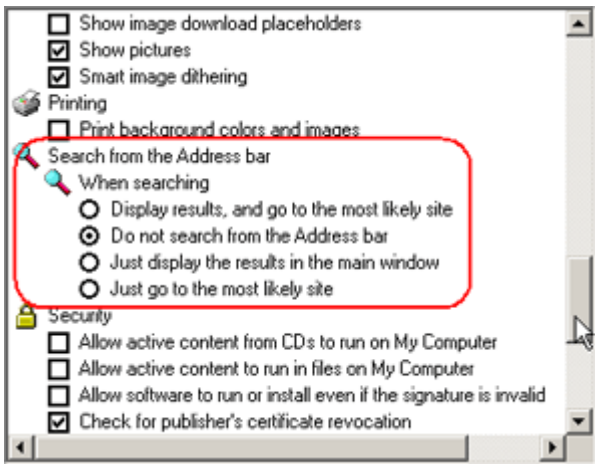
เมื่อตั้งค่าแล้วจะเห็นว่า สไลด์เลื่อนปรับค่า Security (ในวงกลมสีแดง) หายไป สามารถเรียกกลับคืนด้วยคลิกที่ปุ่ม Default Level ต่อไปเราจะปรับตั้งค่าในส่วน Content ที่วงกลมสีแดง AutoComplete... เพื่อการกำหนดค่าการจดจำรหัสผ่านและประวัติการท่องเว็บต่างๆ ดังภาพถัดไป

การกำหนดให้จำ URL และรหัสผ่านต่างๆ





ถ้ายกเลิกการ Check box ต่อไปบราวเซอร์จะไม่จำ URL ที่เคยไปมาก่อน และรหัสผ่านต่างๆ ที่เคยกรอกไว้เช่น รหัสผ่านในการรับ-ส่งอีเมล์ผ่านหน้าเว็บ การกรอกข้อมูลในฟอร์ม เมื่อยกเลิกแล้วอยากลบสิ่งที่โปรแกรมเคยบันทึกสามารถทำได้ด้วยการคลิกปุ่มในกรอบสีเขียวทั้งสองปุ่ม



ในกรอบขวามือบนเป็นการคลิกไปที่แท็ป Advanced เพื่อกำหนดให้ยกเลิก (เอาเครื่องหมายถูกออกจากหัวข้อที่วงไว้) การติดตั้งสคริปต์หรือโปรแกรมตามความต้องการอื่น เช่นพวก Browser hijacker ไปเปลี่ยนค่าในบราวเซอร์

ในด้านซ้ายมือเป็นการตั้งค่าไม่ให้บราวเซอร์ไปค้นหาเว็บไซต์ อื่นๆ ที่มีชื่อใกล้เคียงกัน แต่ให้แสดงเป็นหน้าว่างๆ แทน เพราะมีหนอนไวรัส หรือ สปายแวร์บางตัว จะอาศัยช่องโหว่ของการป้อนข้อมูล URL ผิดทำให้วิ่งตรงไปยังเว็บไซต์ที่โปรแกรมต้องการได้ จากนั้นก็จะพยายามติดตั้งหรือฝังตัวสคริปต์ลงในเครื่องของเราเพื่อการรับส่งข้อมูลนั่นเอง

เพียงขั้นตอนง่ายๆ อย่างนี้ ก็จะทำให้การใช้งานอินเทอร์เน็ตของเราเป็นเรื่องที่มีความเสี่ยงลดน้อยลงได้เมื่อใช้ร่วมกับโปรแกรมป้องกันอื่นๆ ที่จะนำเสนอต่อไปก็จะช่วยให้เรามีความปลอดภัยมากยิ่งขึ้น

5. แนวทางป้องกันไวรัสคอมพิวเตอร์และสปายแวร์

การติดไวรัสคอมพิวเตอร์สามารถได้มาจากหลายทางดังนี้

- ไวรัสจากอินเตอร์เน็ต
- ยูเอสบีแฟลวไดร์ฟ
- ไวรัสจากการเชื่อมต่อเครือข่าย
- ติดตั้งซอฟท์แวร์ผิดลิขสิทธิ์ แล้วโดนโปรแกรมประสงค์ร้ายแถมมา
- ถูกหลอก หรือรู้เท่าไม่ถึงการณ์ ติดตั้งโปรแกรมที่ไม่รู้จัก หรือคลิกลิงค์ที่เชื่อมต่อกับเว็บไซต์ที่เป็นไวรัส
- ติดไวรัสผ่านทางจดหมายอิเล็กทรอนิกส์ เนื่องจากตั้งรหัสผ่านที่สามารถเดาได้ง่าย หรือไวรัสใช้โปรแกรมสุ่มหารหัสผ่านเสี่ยงต่อการถูกแฮ็คจดหมายอิเล็กทรอนิกส์

หลักการทั่วไปของการป้องกันมีดังนี้

- จำกัดสิทธิ์ของผู้ใช้ (Least user privilege) หมายถึงไม่ควรใช้ Admin account ในการใช้งานคอมพิวเตอร์ เนื่องจากสิทธิ์ Admin เป็นสิทธิสูงสุดของคอมพิวเตอร์ เมื่อถูกไวรัสจู่โจมทำให้ไวรัสนั้นมีสิทธิเทียบเท่า Admin ไปด้วย ดังนั้นในการใช้งานทั่วไป ควรตั้งผู้ใช้งานของผู้ใช้แต่ละคนที่ใช้งานเครื่องคอมพิวเตอร์นั้น เช่น ชื่อผู้ใช้ Kanyarat ที่มีสิทธิการใช้งานเครื่องคอมพิวเตอร์ใกล้เคียงกับสิทธิ Admin เป็นต้น เมื่อถูกไวรัสจู่โจมสามารถกำจัดไวรัสได้ง่ายกว่า
- update Web browser บ่อยๆ รวมถึง update plugin
- update program สแกนไวรัสที่ติดตั้งบนเครื่องคอมพิวเตอร์ตามระยะเวลา
- ติดตั้งโปรแกรมที่มีลิขสิทธิ์ถูกต้อง
- ติดตั้งโปรแกรมป้องกันไวรัส สปายแวร์ มัลแวร์ โดยเฉพาะโปรแกรมป้องกันไวรัสเพียงอย่างใดอย่างหนึ่งเท่านั้น เพื่อป้องกันการทำงานข้าลงของเครื่องคอมพิวเตอร์
- รหัสผ่านที่ใช้สำหรับเข้าใช้งานแต่ละโปรแกรมไม่ควรใช้รหัสเดียวกัน เพื่อป้องกันการถูกแฮ็ค
- ควรติดตั้งเฉพาะโปรแกรมที่จำเป็นสำหรับการปฏิบัติงานเท่านั้น
- เมื่อจะเข้าใช้เว็บไซต์ใดให้สังเกตชื่อเว็บไซต์ (URL เช่น http://www.it.chula.ac.th) ว่าแปลกไปจากเดิมหรือไม่ เพราะอาจจะเข้าเว็บไซต์ที่เป็นไวรัสได้

วิธีการป้องกัน สปายแวร์

เพื่อที่จะป้องกันการเข้ามาติดตั้งสปายแวร์อย่างไม่ได้ตั้งใจ แนะนำให้ปฏิบัติตามวิธีการ ดังนี้

- ไม่คลิ้กลิ้งบนหน้าต่างเล็กๆ ที่ปรากฏขึ้นมาอัตโนมัติหรือโฆษณาที่ป๊อบอัพขึ้นมา เพราะป๊อบอัพเหล่านั้นมักจะมีตัวสปายแวร์ฝังอยู่ การคลิ้กลิ้งเหล่านั้นจะทำให้สปายแวร์ถูกนำเข้ามาติดตั้งบนเครื่องของคุณผ่านวินโดวส์ได้ในทันที โดยวิธีการปิดหน้าต่างป๊อบอัพเหล่านั้นควรคลิ้กที่ปุ่ม "X" บนแถบเมนู Title bar แทนที่จะปิดด้วยคำสั่ง close บนแถบแสดงเครื่องมือมาตรฐานของวินโดว์ (standard toolbar)
- ควรเลือกที่คำตอบ "No" ทุกครั้งที่มีคำถามต่างๆ ถามขึ้นมาจากป๊อบอัพเหล่านั้น คุณต้องระมัดระวังเป็นอย่างมากกับคำถามที่ปรากฏขึ้นมาเป็นไดอะล็อกบ๊อกซ์ต่างๆ แม้ว่าไดอะล็อกบ๊อกซ์เหล่านั้นจะ

เกิดขึ้นตอนคุณกำลังรันโปรแกรมเฉพาะที่คุณจะใช้งาน หรือใช้โปรแกรมอื่นอยู่ก็ตาม ควรปิดหน้าต่างป๊อบอัพเหล่านั้นด้วยวิธีคลิ้กที่ปุ่ม "X" บนแถบเมนู Title bar แทนที่จะปิดด้วยคำสั่ง close บนแถบแสดงเครื่องมือมาตรฐานของวินโดว์ (standard toolbar)

- ควรระมัดระวังอย่างมากในการดาวน์โหลดซอฟต์แวร์ที่จัดให้ดาวน์โหลดฟรี เพราะมีหลายเว็บไซต์ ที่จัดหาแถบเครื่องมือแบบที่ให้ผู้ใช้ปรับแต่งเองหรือมีคุณสมบัติอื่นๆ ที่เหมาะสำหรับผู้ใช้ให้ปรับแต่งเองไว้ให้ดาวน์โหลดบนอินเทอร์เน็ต สำหรับท่านที่ต้องการใช้คุณสมบัติของเครื่องมือเหล่านี้ ไม่ควรจะดาวน์โหลดเครื่องมือเหล่านี้มาจากเว็บไซต์ที่ไม่น่าเชื่อถือ และต้องตระหนักเสมอว่ามันเป็นการปล่อยให้สปายแวร์ผ่านเข้ามายังเครื่องคุณได้ด้วย

- ไม่ควรติดตามอีเมล์ลิ้งที่ให้ข้อมูลว่ามีการเสนอซอฟต์แวร์ป้องกันสปายแวร์ เหมือนกับอีเมล์ที่ให้ข้อมูลว่ามีการเสนอซอฟต์แวร์ป้องกันไวรัส ซึ่งอันที่จริงลิ้งเหล่านั้นจะนำไปสู่แนวทางที่ตรงกันข้าม คือเป็นการถามเพื่อให้คุณคลิ้กอนุญาตให้สปายแวร์เข้ามาดำเนินการติดตั้งในเครื่องโดยไม่ถูกขัดขวาง

วิธีการป้องกัน ไวรัสคอมพิวเตอร์

วิธีการที่ดีที่สุดในการป้องกันปัญหาไวรัสคอมพิวเตอร์ คือ ให้ติดตั้งโปรแกรมแอนตี้ไวรัสแล้วทำการอัพเดทไวรัสอย่างสม่ำเสมอ และให้ทำการสแกนไวรัสเป็นประจำ โดยสแกนแบบ Full

- ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตข้อมูลไวรัสอยู่เสมอ
- ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสมกับ OS ของเครื่อง
- สร้างแผ่น Emergency Disc หรือแผ่น boot CD/USB เพื่อใช้ในการกู้ระบบ
- อัปเดตข้อมูลไวรัสของโปรแกรมทุกวัน หรือ ทุกครั้งที่โปรแกรมแจ้งเตือนให้อัปเดต
- เปิดใช้งาน auto-protect ถ้าโปรแกรมสนับสนุน
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือสื่อบันทึกข้อมูลต่าง ๆ
- ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสบนเครื่องคอมพิวเตอร์อย่างน้อย 1 ครั้ง ต่อสัปดาห์

ติดตั้งโปรแกรมอุดช่องโหว่(patch) โดยการอัปเดตซอฟต์แวร์และโปรแกรมประยุกต์ต่าง ๆ ให้ใหม่อยู่เสมอ

- ระบบปฏิบัติการ(OS) Windows , โปรแกรม Internet Explorer (IE) และโปรแกรม Microsoft Office เป็นต้น

ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูล(Media) ต่าง ๆ

- เช่น แผ่นฟล็อปปี้ดิสก์ แผ่นซีดี แผ่นดีวีดี เทปแบ็กอัป หรือไม่ทราบแหล่งที่มา เป็นต้น
- สแกนหาไวรัสจากสื่อบันทึกข้อมูล ก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลก ๆ ที่น่าสงสัย เช่น .pifเป็นต้น รวมทั้งไฟล์ที่มีนามสกุลซ้อนกัน เช่น .jpg,.exe ,.gif.scr , txt.exe เป็นต้น ให้ลบไฟล์นั้นทิ้งทันที

ใช้ความระมัดระวังในการเปิดอ่าน E-mail

- อย่าเปิดไฟล์ที่แนบมากับ E-mail จนกว่าจะรู้ที่มา
- อย่าเปิดอ่าน E-mail ที่มี Subject ที่เป็นข้อความจูงใจ
- ลบ E-mail ที่ไม่ทราบแหล่งที่มาทิ้งทันที เพื่อตัดปัญหาทั้งปวง

ตระหนักถึงความเสี่ยงของไฟล์ที่ดาวน์โหลด หรือได้รับจากทางอินเตอร์เน็ต

- ไม่ควรเปิดไฟล์ที่แนบมากับโปรแกรมที่ใช้สนทนา Social Network เช่น ICQ, MSN, skype, facebook, twitter เป็นต้น หรือการแลกเปลี่ยนไฟล์ โดยเฉพาะไฟล์ที่สามารถรันได้ เช่น ไฟล์ที่มีนามสกุล .exe , .pif , .com , .bat , .vbsเป็นต้นโดยไม่ได้ตรวจสอบแหล่งที่มาก่อน
- ไม่ควรเข้าเว็บไซต์ที่มากับ E-mail หรือโปรแกรมสนทนาต่าง ๆรวมทั้งโฆษณาชวนเชื่อ หรือหน้าเว็บที่ปรากฏขึ้นมาโดยไม่ตั้งใจ
- ไม่ดาวน์โหลดไฟล์ต่าง ๆ จากเว็บไซต์ที่ไม่มั่นใจ หรือไม่น่าเชื่อถือ
- ติดตามข่าวสารข้อมูลการแจ้งเตือนไวรัสจากแหล่งข้อมูลด้านความปลอดภัยอยู่เสมอ

หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น ถ้าต้องการแชร์ไฟล์ ควรแชร์แบบอ่านอย่างเดียว และตั้งรหัสผ่านด้วย

6. คำแนะนำการจัดการไวรัสคอมพิวเตอร์และสปายแวร์

วิธีแก้ไวรัส ซ่อนไฟล์

เอามาประยุกต์ใช้กับ Card Reader หรือ ไดรฟ์อื่น ในเครื่องก็ได้นะ
หรือถ้าโดนไวรัส บล็อค Folder option ก็สามารถแก้ได้
เสียบแฟลชไดรฟ์ แล้ว สังเกตุว่า แฟลชไดรฟ์ คุณอยู่ที่ไดรฟ์ไหน
ยกตัวอย่างเช่น ของผม อยู่ไดรฟ์ H:
หลังจากนั้น เข้าไปที่ Command Propmt โดยการ
เข้าไปที่ Start —> Run ——> แล้วพิมคำว่า cmd แล้วกด Enter
หรืออีกวิธี
เข้าไปที่ Start —>Programs——>Acessories———>Command Propmt
จะเข้าหน้าจอดังนี้
C:\Document and Settings\Administrator> (บางคนอาจไม่เหมือนกัน แต่ไม่ต้องสนใจ)
ขั้นตอนที่ 2 ให้เราพิมพ์ คำสั่ง เพื่อสลับไปที่ ไดรฟ์แฟลชไดรฟ์ เช่น แฟลชไดรฟ์ผมอยู่ H:
G:\Document and Settings\Administrator> h: <—– พิม h: แล้วกด Enter
จะมาขึ้นดังนี้
H:\>
หลังจากนั้นเป็นส่วนสำคัญคือการ ใส่คำสั่งAttribute
H:\> attrib *.* -s -h -a -r /d /s (เว้น ช่องไฟด้วยนะครับ)
แล้วรอซักครู่ ให้มันทำงานจนกลับไปที่
H:\>
หลังจากนั้นให้กลับไปดูที่แฟลชไดรฟ์คุณ จะเห็นว่า ไฟล์ที่ซ่อนไว้ถูกแสดงหมด

Shift ปุ่มมหัศจรรย์ป้องกันไวรัส Autorun

ไวรัส Autorun
จะทำงานทันทีที่เราเสียบ External Media เช่น Flash
Drive / USB Hard disk เป็นต้น ผ่านพอร์ต USB ดังนั้น
ซึ่งไวรัสนี้จะทำการสร้างไฟล์ Autorun เข้าไปยัง drive
ในคอมพิวเตอร์ของเรา สำหรับวิธีการป้องกันไม่ให้ไวรัสทำงานทันทีที่เราเสียบ
Flash Drive เข้าไป นั่นก็คือการยกเลิกการสั่งรันอัตโนมัตินั่นเอง
แล้ว Shift Key บนแป้นพิมพ์ มีประโยชน์อย่างไร

Shift ปุ่มมหัศจรรย์ป้องกันไวรัส Autorun

ปุ่ม Shiftบนแป้นพิมพ์ของเราสามารถสั่งยกเลิกาการรัน หรือตรวจสอบ Flash Drive อัตโนมัติได้ เพียงคุณทำตามขั้นตอนดังต่อไปนี้

1. กดปุ่ม Shift ค้าง
2. เสียบ Flash Drive ในพอร์ต USB
3. กดปุ่ม Shift ค้างต่อประมาณ 3-5 วินาที

4. ปล่อยมือจากปุ่ม Shift
5. จากนั้นให้กดปุ่ม Windows Logo + E เพื่อเปิด My Computer
6. คลิกขวาไดร์ซของ Flash Drive เลือกคำสั่ง Scan Virus หรือชื่อใกล้เคียงนี้

ด้วยขั้นตอนดังกล่าว เราจะสามารถลดปัญหาไวรัส Autorun ได้ แต่อย่างไรก็ตาม แนะนำให้ตรวจสอบอุปกรณ์ที่จะมาเสียบกับพอร์ต USB ของเราเสมอเพื่อลดปัญหาไวรัส

7. แนะนำ Web site ที่รวบรวมวิธีแก้ไวรัสคอมพิวเตอร์และสปายแวร์

www.stopbadware.org/clearinghouse/search

file hippo

www.thaicert.or.th

virusdetail.blogspot.com

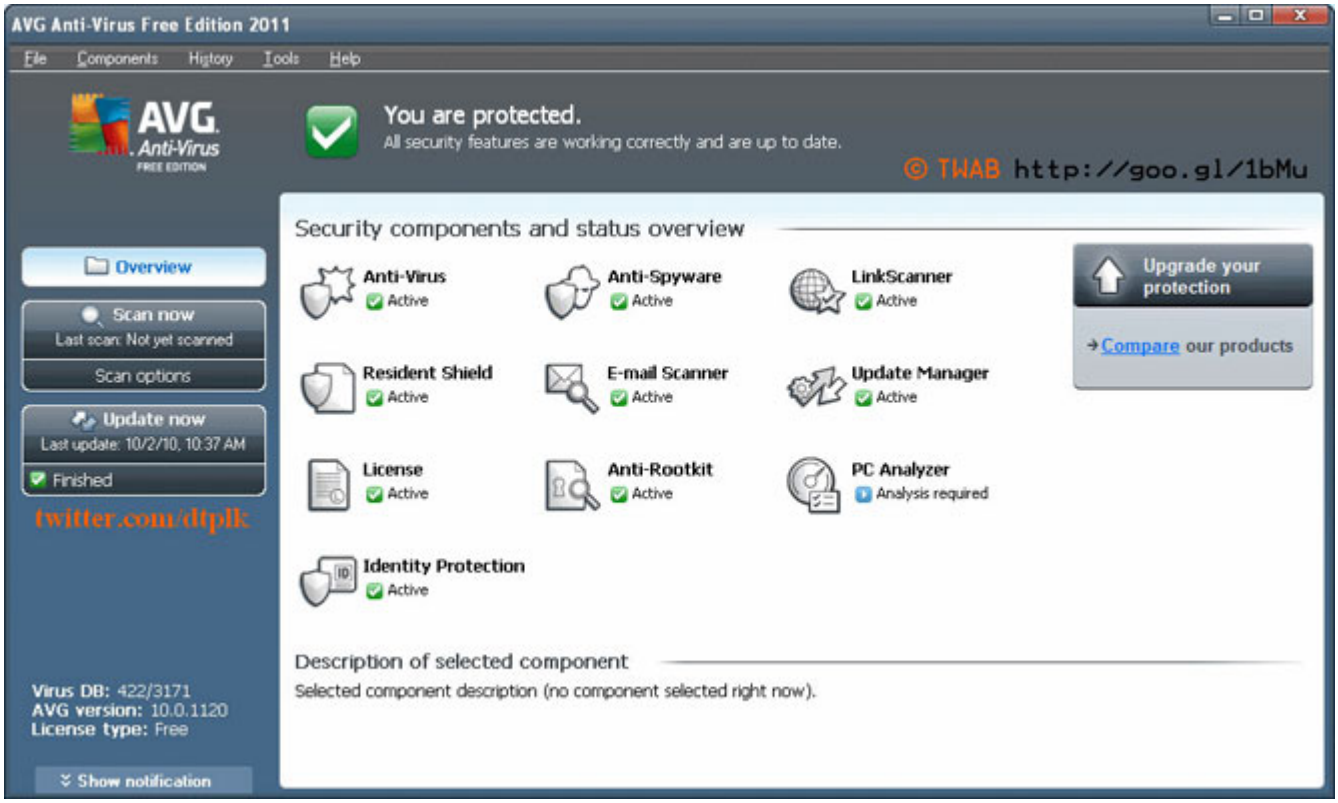
most.go.th

8. แนะนำแหล่งข้อมูล ข่าวแจ้งเตือนไวรัสคอมพิวเตอร์ และสปายแวร์

http://virus.thaiware.com/

9. แนะนำโปรแกรม antivirus และสปายแวร์

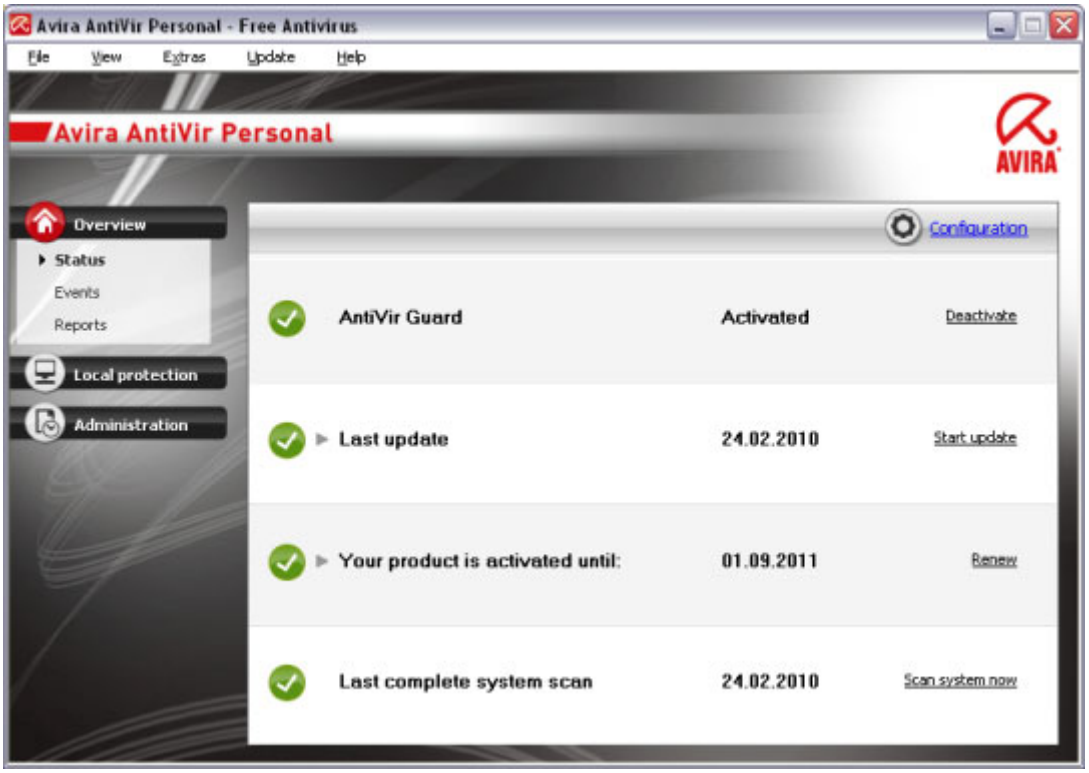
1. AVG Antivirus Free Edition 2011: เป็นโปรแกรมที่สามารถป้องกันไวรัสและสปายแวร์ ตัวใหม่ๆ ได้ เช่น ไวรัสที่มากับ E-mail เพราะทุกวันนี้ไวรัสและสปายแวร์จะมีการอัพเดทความสามารถในการทำลายอยู่ตลอด ดังนั้นเราก็ควรอัพเดทโปรแกรมที่มีอยู่และอัพเดทเวอร์ชั่นใหม่ๆ ของโปรแกรมอยู่ตลอด



Download free

http://free.avg.com/ww-en/free-antivirus-download

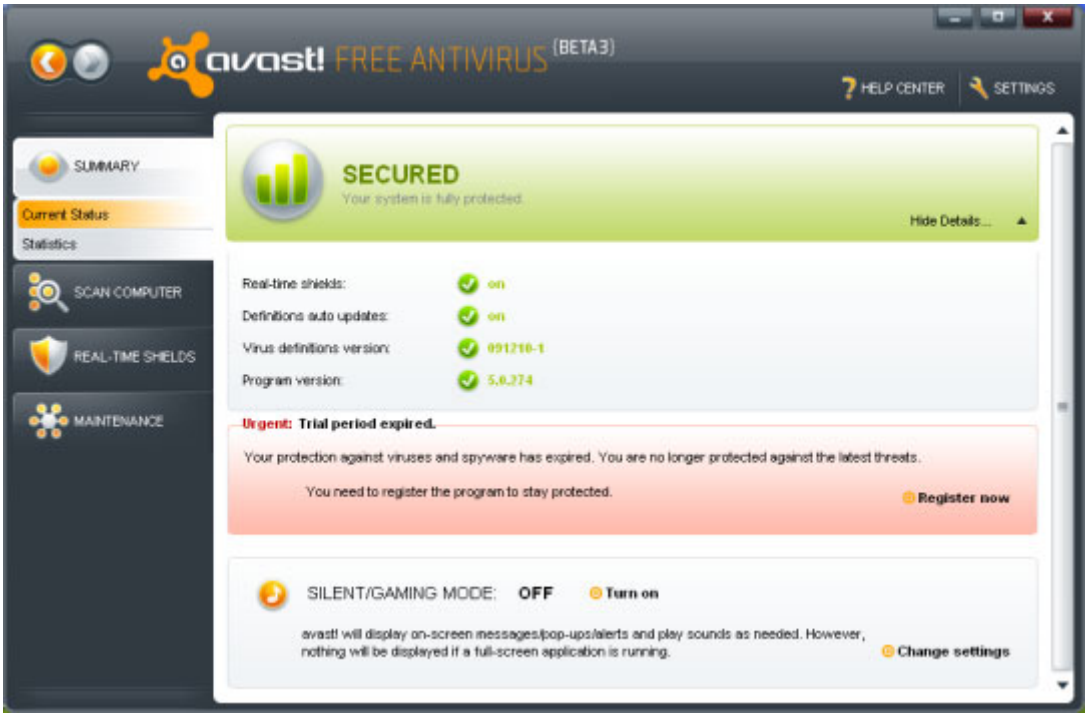
2. Avira AntiVir Personal Free Edition: สามารถกำจัดไวรัสได้มากว่า 300,000 ชนิด มีการอัพเดท ข้อมูลไวรัสในเครื่องของเราแบบอัตโนมัติ ทำให้โปรแกรมไม่ล้าหลัง และตามไวรัสตัวใหม่ๆ ได้ทัน โปรแกรมนี้เหมาะสำหรับคนที่ชอบเล่นอินเทอร์เน็ต และชอบดาวน์โหลด ทั้งหลาย แต่บางทีเวลาที่เราสแกนโปรแกรมก็ชอบลบข้อมูลบางอย่างออกไปด้วย และไม่ค่อยซับพอร์ตโปรแกรมอื่นเท่าไหร่



Download free

http://download.cnet.com/Avira-Free-Antivirus-2013/3000-2239_4-10322935.html?tag=contentMain;contentAux

3. Avast Free Antivirus: สามารถป้องกันไวรัส Spyware หรือ Malware ต่าง ๆ ที่แฝงตัวมากับเว็บไซต์ไม่ให้เข้ามาทำร้ายข้อมูลในเครื่องคอมพิวเตอร์ของเราได้ การสแกนสามารถสแกนได้ทั้งไฟล์ที่อยู่ในเครื่องคอมพิวเตอร์ และสแกนขณะที่บู๊ตเครื่องก็ได้ โดยโปรแกรมจะตรวจจับไวรัสและกำจัดไวรัสให้ทันทีที่พบ และในปัจจุบันโปรแกรมสามารถรองรับภาษาได้มากกว่า 19 ภาษา เป็นโปรแกรมที่มีขนาดเล็ก กระทัดรัด สามารถใช้งานได้ง่าย ที่สำคัญไม่หนักเครื่องด้วยนะจ๊ะ



Download free

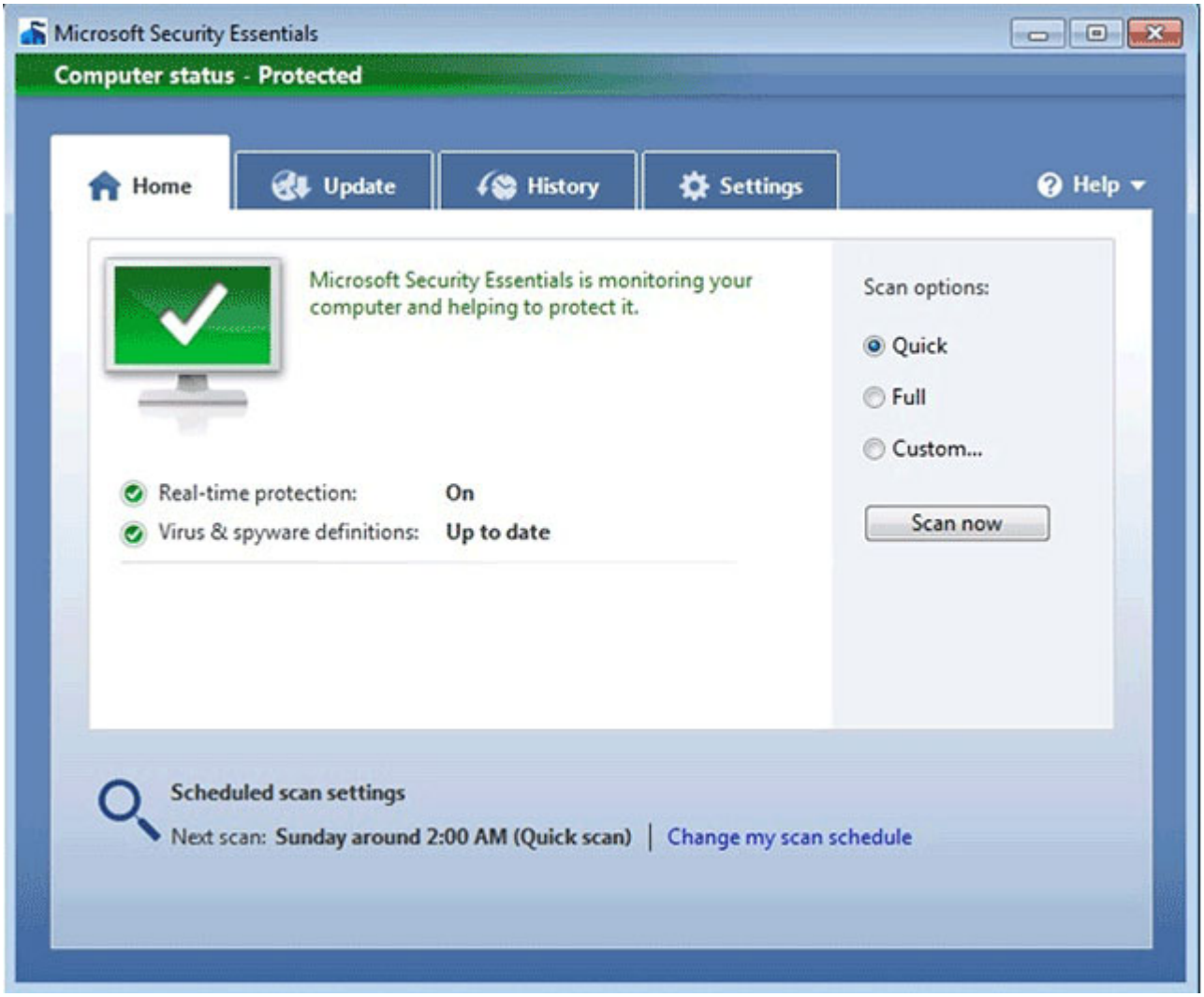
http://download.cnet.com/Avast-Free-Antivirus/3000-2239_4-10019223.html?tag=mncol;pop

4. PC Tools AntiVirus Free: โปรแกรมนี้ก็จะช่วยป้องกันเครื่องคอมพิวเตอร์ของเราไม่ให้ติดไวรัสได้ง่ายๆ ซึ่งเหมือนกับโปรแกรมสแกนไวรัสตัวอื่น ๆ สำหรับโปรแกรมนี้สามารถดาวน์โหลดมาใช้งานได้ฟรี แต่ขนาดของไฟล์อาจจะค่อนข้างใหญ่ และอาจทำให้หนักเครื่องอยู่บ้างนะค่ะ

Download free

http://download.cnet.com/PC-Tools-AntiVirus-Free/3000-2239_4-10625067.html?tag=mncol;pop

5. Microsoft Security Essentials: สำหรับโปรแกรมนี้ เป็นโปรแกรมที่สามารถตรวจสอบและกำจัดไวรัสหรือสปายแวร์ได้เกือบทุกรูปแบบ ไม่ว่าไวรัสจะเปลี่ยนสถานะในการเข้าถึงข้อมูลของเราเป็นอย่างไรก็ตาม โปรแกรมก็จะตรวจพบไวรัสได้อยู่ดี ถ้าใครยังไม่มีโปรแกรมสแกนไวรัสลองโหลดโปรแกรมตัวนี้ไปใช้ดูนะคะ เพราะเป็นโปรแกรมที่พัฒนาขึ้นมาโดยบริษัท Microsoft เองซึ่งน่าจะช่วยให้ผู้ที่ใช้งานคอมพิวเตอร์ในระบบปฏิบัติการ Windows อย่าลืมว่าในการติดตั้งโปรแกรมนี้ Windows ของคุณจะต้องเป็น Windows ที่ถูกลิขสิทธิ์ด้วย



Download free

http://windows.microsoft.com/th-th/windows/security-essentials-download

6. ThreatFire AntiVirus Free Edition: โปรแกรมป้องกันและกำจัดไวรัสตัวนี้มีความสามารถตรวจจับได้ทั้ง trojans, rootkits, hijackers, keyloggers และ Malware ตัวอื่นๆ แต่ว่าโปรแกรมสแกนไวรัสตัวนี้ไม่สามารถสแกนทีละ File หรือ Folder ได้ เพราะโปรแกรมจะบังคับให้สแกนทุกไดร์ฟพร้อมกันหมด

ThreatFire
Zero-day Malware Protection

Download free

http://download.cnet.com/ThreatFire-AntiVirus-Free-Edition/3000-2239_4-10726873.html

7. Emsisoft Anti-Malware 5.0: สำหรับโปรแกรมนี้ เป็นโปรแกรมที่ช่วยป้องกันไวรัสโทรจันประเภท Back Orifice และโปรแกรมนี้ยังสามารถตรวจหาไวรัสที่แนบมากับ E-Mail ที่เป็นตระกูล ZIP, ARJ, CAB หรือไฟล์ที่มาจากการดาวน์โหลดได้เช่นกัน และในโปรแกรมนี้ยังสามารถสแกนตัวโทรจันและระบุข้อมูลของไวรัสโทรจันแต่ละประเภทได้อีกด้วยหากคุณต้องการเรียนรู้เกี่ยวกับไวรัสโทรจันเหล่านี้ ถ้าใครคิดจะใช้โปรแกรมนี้คงต้องใช้เวลานานในการติดตั้ง เพราะโปรแกรมมีขนาดใหญ่พอสมควร

Download free

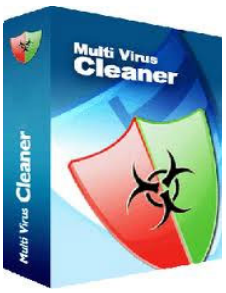
http://www.emsisoft.com/en/software/antimalware/

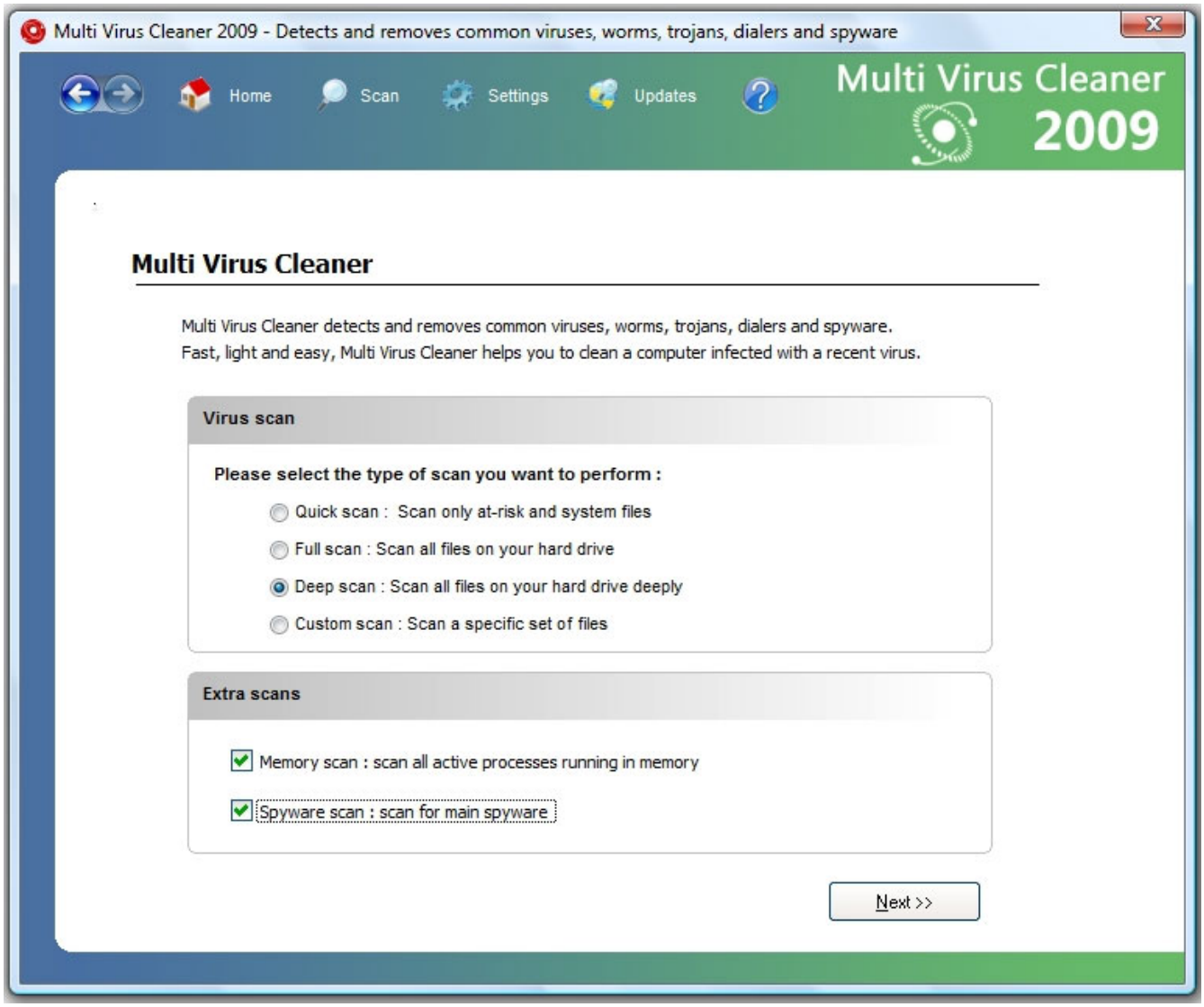
8. Panda Cloud Antivirus Free: เป็นโปรแกรมที่มีขนาดเล็ก ใช้พื้นที่ของเครื่องคอมพิวเตอร์น้อย สำหรับโปรแกรมนี้สามารถใช้งานง่าย เพราะมีไอคอนเพียงไม่กี่ปุ่ม ในการทำงานของโปรแกรมนี้จะทำการอัพเดทอัตโนมัติเมื่อเราเชื่อมต่ออินเทอร์เน็ต ทำให้สามารถสแกนไวรัสตัวใหม่ๆ ได้ อีกทั้งยังสแกนรวดเร็ว

Download free

http://download.cnet.com/Panda-Cloud-Antivirus-Free-Edition/3000-2239_4-10914099.html

9. Multi Virus Cleaner 2009: โปรแกรมตัวนี้เป็นโปรแกรมเอนกประสงค์ที่สามารถตรวจจับและกำจัดไวรัสหรือสปายแวร์ได้ และสามารถอัพเดทฐานข้อมูลไวรัสของตัวเองเพื่อให้โปรแกรมสามารถตรวจจับไวรัสชนิดใหม่ๆ ได้ โดยคุณสามารถดาวน์โหลดโปรแกรมตัวนี้มาใช้งานได้หากเครื่องของคุณมีปัญหา นอกจากนี้โปรแกรมสแกนไวรัส Multi Virus Cleaner 2009 ยังสามารถตรวจพบไวรัสได้มากถึง 6,400 ประเภทในแบบต่างๆกันได้อย่างไม่มีปัญหา

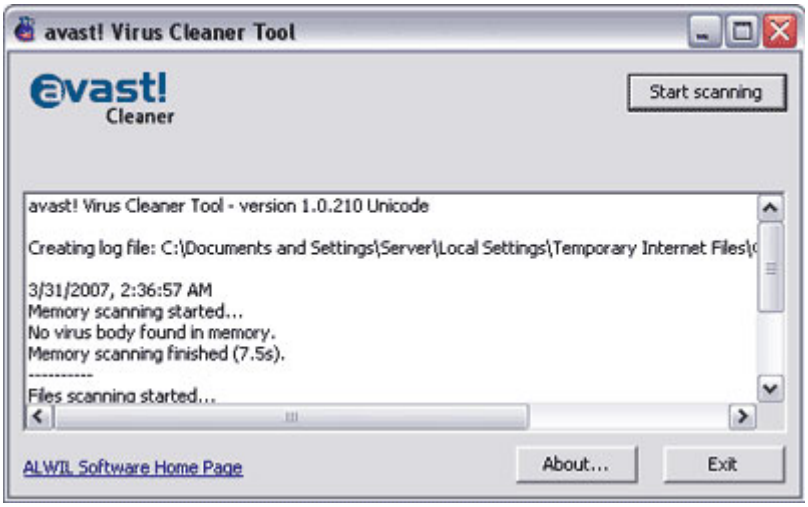




Download free

http://www.soft82.com/download/windows/multi-virus-cleaner/

10. Avast – Virus Cleaner and Worm Removal Tool: โปรแกรมนี้จะช่วยกำจัดไวรัส และหนอนต่างๆ ในเครื่องคอมพิวเตอร์ของคุณ ไม่ว่าจะเป็นการลบจาก Registry หรือ Start up สำหรับข้อเสียของโปรแกรมนี้ คือไม่สามารถกำจัดไวรัสได้ทุกตัว ส่วนข้อดี คือ โปรแกรมนี้ไม่จำเป็นต้องติดตั้งให้ยุ่งยาก เพียงแค่ดับเบิ้ลคลิกก็สามารถใช้งานได้ทันที และข้อดีอีกอย่าง โปรแกรมนี้สามารถพกพาได้ง่าย เพียงแค่เรา Save ใส่ Flash Drive ก็สามารถนำไปสแกนได้ทุกที่



Download free

http://www.download3000.com/download_45538.html