คำนำ

ในยุคปัจจุบันระบบเทคโนโลยีสารสนเทศที่มีความทันสมัยเข้ามามีอิทธิพลในชีวิตการทำงานและชีวิตประจำวันเป็นอย่างมาก แต่ขณะเดียวกันผู้ใช้คอมพิวเตอร์และระบบสารสนเทศผ่านอุปกรณ์ที่มีความทันสมัยยังคงพบมหันตภัยร้ายจากไวรัสคอมพิวเตอร์ที่เป็นภัยคุกคามที่ก่อให้เกิดความเสียหาย ที่หลายท่านอาจประสบพบเจอมาด้วยตนเอง หรือได้ยินได้ฟังมาบ้าง ทำให้เกิดความกลัวความเสียหายที่อาจเกิดขึ้นจากการถูกโจมตี และอาจมีคำถามเกิดขึ้นว่า การป้องกันไวรัสควรจะเป็นหน้าที่ของใคร ผู้ดูแลระบบหรือผู้ใช้เครื่องที่เป็นผู้ดูแลเอง และจะเลือกวิธีการใดในการป้องกันเพื่อให้การใช้งานมีความปลอดภัยและน่าเชื่อถือมากยิ่งขึ้น จำเป็นจะต้องทราบถึงประเภทของไวรัสมีกี่กลุ่มกี่สายพันธุ์ วิธีการสังเกตอาการของการทำงานที่ผิดปกติจากการถูกโจมตี พฤติกรรม และลักษณะการทำงานของไวรัส เพื่อเข้าถึงการทำงานของไวรัส และสร้างความเข้าใจที่ถูกต้อง เพื่อประโยชน์ในการหาวิธีป้องกันระบบให้ปลอดภัยจากไวรัสคอมพิวเตอร์

สำนักงานทรัพยากรน้ำภาค ๑๐ หวังเป็นอย่างยิ่งว่า หนังสือ “ภัยคุกคามและการรักษาความปลอดภัยระบบคอมพิวเตอร์” ฉบับนี้ จะเป็นประโยชน์ต่อผู้ใช้ระบบงานคอมพิวเตอร์ทุกท่าน ซึ่งได้รวบรวมถึงรายละเอียด องค์ความรู้ที่เป็นประโยชน์ในการดูแลป้องกันไวรัสคอมพิวเตอร์ไว้อย่างครอบคลุม ที่สามารถนำไปสู่การยกระดับการรักษาความปลอดภัยในการใช้งานได้อย่างมีประสิทธิภาพและประสิทธิผล และยั่งยืนต่อไป

คณะทำงานการจัดการความรู้ ปี 2555
สำนักงานทรัพยากรน้ำภาค 10

สารบัญ

สารบัญ

บทที่ 1
ความรู้ทั่วไปเรื่องภัยคุมคามคอมพิวเตอร์

ในปัจจุบันเรื่องของความปลอดภัยของข้อมูลและระบบสารสนเทศในการทำงานทั้งภาครัฐและเอกชนถือเป็นส่วนสำคัญของการนำระบบสารสนเทศเข้ามาใช้ในองค์กร เนื่องจากระบบสารสนเทศนั้นใช้คอมพิวเตอร์ในการเก็บรักษาข้อมูล และใช้ระบบเครือข่ายเป็นสื่อกลางในการติดต่อสื่อสาร และด้วยเหตุผลดังกล่าว จึงเป็นการง่ายต่อการคุกคามข้อมูลจากผู้ไม่ประสงค์ดี ดังนั้น การนำระบบสารสนเทศเข้ามาใช้ จึงมีความจำเป็นที่จะต้องเพิ่มเติมในเรื่องของการรักษาความปลอดภัยของข้อมูลควบคู่ไปด้วยอย่างหลีกเลี่ยงไม่ได้

ประกอบกับในปัจจุบันอินเตอร์เน็ต และอีเมล์ก้าวเข้ามาเป็นส่วนหนึ่งในชีวิตของเรา จึงทำให้ภัยอันตรายและความเสี่ยงอีกมากมายเพิ่มขึ้นตามไปด้วยดังนั้นผู้ใช้จึงจำเป็นต้องมั่นใจได้ว่ามีความรู้พื้นฐาน พอที่จะสามารถสังเกตุเห็นความผิดปกติและแก้ไขปัญหาในเบื้องต้นได้ เมื่อเผชิญหน้ากับผู้บุกรุก, ไวรัสคอมพิวเตอร์, ความผิดพลาดของซอฟต์แวร์, อุบัติภัย และความผิดพลาดในขั้นตอนการทำงานของระบบคอมพิวเตอร์

1.1 รู้จักภัยคุกคามทางคอมพิวเตอร์

ภัยคุกคามด้านความปลอดภัยของระบบคอมพิวเตอร์ และข้อมูลนั้นนับวันยิ่งทวีความซับซ้อนและทวีความรุนแรงเพิ่มมากขึ้น เราอาจสังเกตุได้จากสถิติของสำนักวิจัยหลายสำนักที่ได้ทำการวิเคราะห์ภัยคุมคามต่างๆ ที่เป็นปัญหาใหญ่ของผู้ดูแลระบบความปลอดภัย ภัยคุกคามเหล่านี้ล้วนเป็นอุปสรรคที่กระทบต่อการปฏิบัติงานขององค์กร เพราะในปัจจุบันระบบสารสนเทศ และเครือข่ายอินเตอร์เน็ตนั้นมีบทบาทสำคัญในการขับเคลื่อนการทำงานทั้งภาครัฐ และภาคธุรกิจ ดังนั้นหากระบบสารสนเทศขององค์กรไม่มีความปลอดภัยที่ดีพอ และยังจัดการกับปัญหาที่เกิดขึ้นได้ไม่ถูกทางหรือไม่ถูกจุด ทำให้ปัญหาต่างๆ ยังคงอยู่ถึงแม้ว่ามีการลงทุนกับระบบรักษาความปลอดภัยขององค์กรไปมากมายก็ตาม ดังนั้นเราควรทำความเข้าใจและศึกษาวิเคราะห์ปัญหาภัยคุกคามทางคอมพิวเตอร์เหล่านั้นเพื่อที่จะได้วางแผน แก้ไขปัญหาเพื่อปลอดภัยได้อย่างถูกต้องตรงกับปัญหา เพื่อความ

ปลอดภัยและเสถียรภาพที่ดีขึ้นของระบบคอมพิวเตอร์ในองค์กร รวมไปจนถึงคอมพิวเตอร์ที่เราใช้อยู่เป็นส่วนตัวในลักษณะ Home User อีกด้วย โดยเราสามารถแบ่งประเภทของภัยคุกคามได้ดังนี้

1.2 ประเภทของภัยคุกคาม

ภัยคุกคาม เป็นภัยภิบัติที่เกิดขึ้นกับระบบ (Disaster) เป็นความเสียหายทั้งทางด้านกายภาพและด้านข้อมูล ที่เกิดขึ้นกับระบบคอมพิวเตอร์ Hardware Programs แฟ้มข้อมูล และอุปกรณ์อื่น ๆ ถูกทำลายให้ให้เกิดความเสียหาย ซึ่งที่ร้ายแรงที่สุดอาจก็คือการที่ภัยนั้นทำให้ระบบล่มไม่สามารถใช้งานได้ โดยประเภทของภัยคุกคามที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่ายนั้นสามารถจำแนกได้ 2 ประเภทหลัก ๆ ดังนี้

1. ภัยคุกคามทางตรรกะ (Logical) หมายถึง ภัยคุกคามทางด้านข้อมูล
2. ภัยคุกคามทางกายภาพ (Physical) หมายถึง ภัยที่เกิดกับตัวเครื่องและอุปกรณ์ เช่น ภัยภิบัติจากธรรมชาติ และภัยจากการกระทำของมนุษย์ที่ทำความเสียหายให้กับตัวเครื่องและอุปกรณ์

1.3 ภัยคุกคามทางด้านข้อมูล

Hacker คือ ผู้ที่แอบเข้าใช้งานระบบคอมพิวเตอร์ของหน่วยงานหรือองค์กรอื่น โดยมิได้รับอนุญาต แต่ไม่มีประสงค์ร้าย หรือไม่มีเจตนาที่จะสร้างความเสียหายหรือสร้างความเดือดร้อนให้แก่ใครทั้งสิ้น แต่เหตุผลที่ทำเช่นนั้นอาจเป็นเพราะต้องการทดสอบความรู้ความสามารถของตนเองก็เป็นไปได้

Cracker คือ ผู้ที่แอบเข้าใช้งานระบบคอมพิวเตอร์ของหน่วยงานหรือองค์กรอื่น โดยมีเจตนาร้ายอาจจะเข้าไปทำลายระบบ หรือสร้างความเสียหายให้กับระบบ Network ขององค์กรอื่นหรือขโมยข้อมูลที่เป็นความลับทางธุรกิจ

ไวรัส (Viruses) คือ โปรแกรมคอมพิวเตอร์ประเภทหนึ่งที่เขียนขึ้นโดยความตั้งใจของ Programmer ถูกออกแบบมาให้แพร่กระจายตัวเองจากไฟล์หนึ่งไปยังไฟล์อื่นๆ ภายในเครื่องคอมพิวเตอร์ ไวรัสจะแพร่กระจายตัวเองอย่างรวดเร็วไปยังทุกไฟล์ภายในคอมพิวเตอร์ หรืออาจจะทำให้ไฟล์เอกสารติดเชื้ออย่างช้าๆ แต่ไวรัสจะไม่สามารถแพร่กระจายจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งได้ด้วยตัวมันเอง โดยทั่วไปแล้วจะเกิดจากการที่ผู้ใช้ใช้สื่อจัดเก็บข้อมูลเช่น Diskette คัดลอกไฟล์ข้อมูลลง Disk และติดไวรัสเมื่อนำไปใช้กับเครื่องอื่น หรือไวรัสอาจแนบมากับไฟล์เมื่อมีการส่ง E-mail ระหว่างกัน

หนอนอินเตอร์เน็ต (Worms) มีอันตรายต่อระบบมาก สามารถทำความเสียหายต่อระบบได้จากภายใน เหมือนกับหนอนที่กัดกินผลไม้จากภายใน หนอนร้ายเป็นโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้สามารถแพร่กระจายตัวเองจากเครื่องคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งโดยอาศัยระบบเน็ตเวิร์ค (ผ่านสาย Cable) ซึ่งการแพร่กระจายสามารถทำได้ด้วยตัวของมันเองอย่าง

รวดเร็วและรุนแรงกว่าไวรัส เมื่อไรก็ตามที่คุณสั่ง Share ไฟล์ข้อมูลผ่าน Network เมื่อนั้น Worms สามารถเดินไปกับสายสื่อสารได้

Spam mail คือ การส่งข้อความที่ไม่เป็นที่ต้องการให้กับคนจำนวนมาก ๆ จากแหล่งที่ผู้รับไม่เคยรู้จักหรือติดต่อมาก่อน โดยมากมักอยู่ในรูปของ E-mail ทำให้ผู้รับรำคาญใจและเสียเวลาในการลบข้อความเหล่านั้นแล้ว Spam mail ยังทำให้ประสิทธิภาพการขนส่งข้อมูลบนอินเทอร์เน็ตลดลงด้วย

1.4 ภัยคุกคามในการทำธุรกิจ E- Commerce

ในการทำธุรกิจบนระบบพาณิชย์อิเล็กทรอนิกส์ อาจจะเกิดภัยคุกคามต่อเว็บไซต์ได้ จึงเป็นสิ่งสำคัญที่เราทุกคนควรจะรู้ว่ามีภัยคุกคามใดบ้างที่อาจเกิดขึ้นกับระบบ เพื่อเตรียมพร้อมสำหรับการป้องกันล่วงหน้า ตัวอย่างภัยคุกคามที่ควรระวังสำหรับพาณิชย์อิเล็กทรอนิกส์ เช่น

1. การเข้าสู่เครือข่ายโดยไม่ได้รับอนุญาต เช่น มีบุคคลอื่นแอบอ้างในการใช้ชื่อ Login Name และ Password ในการเข้าไปทำธุรกรรมซื้อขายบน Web site แทนตัวเราเอง

2. การทำลายข้อมูลและเครือข่าย เช่น Cracker เจาะระบบเข้าไปทำลาย file และข้อมูลภายในเครื่อง Server ของ Web site ผู้ขาย ทำให้ข้อมูลสมาชิกหรือลูกค้าของระบบเกิดความเสียหาย

3. การเปลี่ยนแปลง การเพิ่ม หรือการดัดแปลงข้อมูล เช่น การส่ง Order หรือจดหมายอิเล็กทรอนิกส์ในการสั่งซื้อสินค้า หรือการที่จดหมายถูกเปิดอ่านระหว่างทาง ทำให้ข้อมูลไม่เป็นความลับ และผู้เปิดอ่านอาจเปลี่ยนแปลง แก้ไข หรือเพิ่มเติมข้อความในจดหมาย เช่น การแก้ไขจำนวนยอดของการสั่งซื้อสินค้า เป็นต้น

4. การเปิดเผยข้อมูลแก่ผู้ที่ไม่ได้รับอนุญาต เมื่อเราสมัครเป็นสมาชิกไว้ใน Web site ใด ๆ Server ของเจ้าของ Web site จะเก็บข้อมูลส่วนตัวของเราไว้ หากเจ้าของ Web Site ขาดจริยธรรมในการทำธุรกิจอาจนำข้อมูลส่วนตัวของเราไปขายให้องค์กรอื่น เช่น ขายข้อมูลให้กับบริษัทบัตร Credit เป็นต้น

5. การทำให้ระบบบริการของเครือข่ายหยุดชะงัก เช่น การที่ Cracker เข้ามาทำลายระบบเครือข่าย และส่งผลให้เครื่อง Server ของเจ้าของ Web site ไม่สามารถให้บริการแก่ลูกค้าของเขาได้จนกว่าระบบนั้นจะถูกแก้ไข ดังนั้น เมื่อระบบล่มเป็นระยะเวลานานหลายชั่วโมง หรืออาจจะนานหลายวันก็จะส่งผลต่อยอดขายสินค้าบน Web ด้วย

6. การขโมยข้อมูล เมื่อตัวเราเองเป็นผู้ให้ข้อมูลไว้กับ Web site ที่เราจะซื้อขายสินค้า ข้อมูลนั้นอาจถูกขโมยจากเจ้าของ Web site จากผู้ดูแล Web หรือจาก Cracker ที่นำไปใช้ประโยชน์ต่อเขาเหล่านั้น แต่ส่งผลเสียกับตัวเรา เพราะการเปิดเผยข้อมูลส่วนตัวเขาของเราโดยไม่ได้รับอนุญาตถือเป็นการขโมย

7. การปฏิเสธการบริการที่ได้รับ เช่น ปฏิเสธว่าไม่ได้เข้าไปกรอกรายการสั่งซื้อที่ Web site โดยใช้ชื่อนี้หรืออ้างว่าสั่งซื้อสินค้าแล้วแต่ไม่ได้รับการจัดส่งสินค้าจาก web site ดังกล่าวเพื่อใช้เป็นข้ออ้างในการชำระเงินค่าสินค้าส่วนที่เหลือ

8. การอ้างว่าได้ให้บริการ หรือ อ้างว่าได้ส่งมอบสินค้าและบริการแล้ว

9. Virus ที่แอบแฝงมากับผู้ที่เข้ามาใช้บริการ ส่งผลทำให้เครื่อง Server ของเจ้าของ web site ได้รับความเสียหาจากการที่ Virus ทำลายข้อมูลและ file ต่าง ๆ ภายในระบบ

1.5 ภัยคุกคามบน Internet

อันตรายหนึ่งที่คาดไม่ถึงจากอินเทอร์เน็ตที่ส่งผลกระทบโดยตรงต่อเยาวชนไทย เพราะอินเทอร์เน็ตยังเป็นสื่อ Electronic ที่มาตรการการควบคุมสิทธิเสรีภาพของผู้ใช้ยังไม่ดีนัก ดังนั้นการกระทำใด ๆ ในห้องสนทนา (Chat) และ เว็บบอร์ด (Web board) จึงเกิดขึ้นได้อย่างไร้ขอบเขต จนกลายเป็นที่ระบายออกซึ่งอารมณ์และความรู้สึกของผู้ใช้

ในห้องสนทนา ทุกคนสามารถคุยอะไรกับใครก็ได้ รายละเอียดต่างๆไม่มีการเปิดเผย รู้เพียงแต่ชื่อที่ใช้ในการสนทนาเท่านั้น ดังนั้นจึงไม่มีทางรู้ได้เลยว่า เรากำลังพูดคุยอยู่กับใคร สิ่งที่คนนั้นพูดอยู่เป็นความจริงหรือไม่ ดังจะเห็นตามหน้าหนังสือพิมพ์ที่อาชญากรรมที่เกิดกับวัยรุ่นสมัยนี้บางครั้งมีจุดเริ่มต้นมาจากการพูดคุยกันในห้องสนทนา (Chat Room) บนอินเทอร์เน็ต

บทที่ 2
ไวรัสบนเครื่องคอมพิวเตอร์

ในปัจจุบันไวรัสคอมพิวเตอร์ยังถือว่ายังคงเป็นปัญหาหลักของผู้ใช้คอมพิวเตอร์ส่วนบุคคล ตลอดจนภาครัฐ และองค์กรธุรกิจ โดยไวรัสคอมพิวเตอร์สามารถสร้างความเสียหายในรูปแบบของข้อมูลที่มีค่าขององค์กร และในปัจจุบันมีองค์กรจำนวนมากที่ต้องสูญเงินจำนวนมากต่อปีเพื่อป้องกันอันตรายที่เกิดจากไวรัส และกู้คืนข้อมูลระบบที่ถูกทำลาย

2.1 ไวรัสคอมพิวเตอร์ คืออะไร

ไวรัสคอมพิวเตอร์ คือ โปรแกรมคอมพิวเตอร์หรือชุดคำสั่งเล็กๆ ที่เขียนขึ้นเพื่อให้รบกวนการทำงาน หรือทำลายไฟล์ข้อมูล ตลอดจนไฟล์โปรแกรมต่างๆ ในระบบคอมพิวเตอร์ โดยคุณสมบัติพิเศษของไวรัสคอมพิวเตอร์ก็คือ ไวรัสคอมพิวเตอร์สามารถหลบหลีกซ่อนตัวอยู่ในเครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง และหาโอกาสทำสำเนาคัดลอกเพื่อแพร่กระจายตัวเองไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ได้ และเครื่องที่ติดไวรัสคอมพิวเตอร์เข้าไปแล้วก็จะเกิดอาการแปลกๆ ตามแต่ชุดคำสั่งที่เขียนไว้ในโปรแกรมไวรัสคอมพิวเตอร์นั่นเอง ซึ่งไวรัสอาจทำลายโปรแกรมหรือข้อมูลอื่น ๆ ที่อยู่ในเครื่องคอมพิวเตอร์ หรือ เพียงแค่รบกวนการทำงานโดยการแสดงข้อความวิ่งไปมาบนหน้าจอ

2.2 ที่มาของไวรัสคอมพิวเตอร์

ความเป็นมาของไวรัสคอมพิวเตอร์ตั้งแต่อดีตจนปัจจุบันและเหตุการณ์การแพร่ระบาดที่สำคัญๆ มีดังนี้

ปี พ.ศ. 2492 John Von Neumann ได้เขียนทฤษฎีเกี่ยวกับโปรแกรมคอมพิวเตอร์ที่สามารถสร้างตัวเองได้ ชื่อ “Theory and Organization of Complicated Automata”

ปี พ.ศ. 2524 Richard Skrenta ได้พัฒนาไวรัสบนเครื่องไมโครคอมพิวเตอร์ตัวแรก ชื่อ “Elk Cloner”

ปี พ.ศ. 2525 Joe Deliinger พัฒนาไวรัสบนเครื่อง Apple II ชื่อ Apple และได้พัฒนาโปรแกรมกำจัดไวรัสชนิดนี้ไว้ด้วย

ปี พ.ศ. 2526 Fred Cohen เสนอทฤษฎีชื่อ “Computer Virus”-Theory and

Experiments” และนิยามความหมายของคำว่าไวรัสคอมพิวเตอร์

ปี พ.ศ. 2529 สองพี่น้องชาวปากีสถานได้สร้างไวรัสชื่อ Brain เพื่อป้องกันการคัดลอกทำสำเนาโปรแกรมของพวกเขาโดยไม่จ่ายเงิน

ปี พ.ศ. 2530 ไวรัส Jerusalem เป็นไวรัสตัวแรกที่ลบไฟล์ได้ตามประสงค์และกระจายตัวในวงกว้าง และยังมีไวรัส Stoned ที่สามารถฝังตัวเองที่ Master Boot Record (MBR)

ปี พ.ศ. 2531 John Mcafee ได้พัฒนาโปรแกรมป้องกันไวรัส ชื่อ Virus Scan เป็นคนแรก และในปีนี้เองได้เกิดหนอนอินเทอร์เน็ตตัวแรก ชื่อ Morris ซึ่งถูกพัฒนาโดย Robert Morris Jr.

ปี พ.ศ. 2533 บริษัท Symantec เริ่มจำหน่ายโปรแกรมป้องกันไวรัสชื่อ Norton Anti-virus

ปี พ.ศ. 2534 Tequila เป็นไวรัสตัวแรกที่เป็น Polymorphic เป็นการอาศัยการเปลี่ยนแปลงรูปแบบของไวรัส มีการแบ่งรหัสของตัวไวรัสเป็นส่วนย่อยแทรกอยู่ระหว่างแฟ้มข้อมูล เมื่อแฟ้มข้อมูลทำงานรหัสไวรัสจะถูกนำไปรวมกันในหน่วยความจำ การใช้การเข้ารหัสและการถอดรหัสก่อนการทำงานด้วยคีย์เฉพาะ ทำให้ยากต่อการตรวจสอบจากรหัสลายเซ็นไวรัส (Virus Signature เป็นรหัสเฉพาะของไวรัสที่ผู้เขียนโปรแกรมป้องกันไวรัสได้ทำการถอดรหัสออกมาซึ่งไวรัสแต่ละตัวก็จะมีรูปแบบของข้อมูลที่แตกต่างกัน)

ปี พ.ศ. 2535 ไวรัส Michelagelo มีการทำงานวันที่ 6 มีนาคม

ปี พ.ศ. 2537 Hoax ตัวแรกที่แพร่กระจายตัวผ่านอินเทอร์เน็ตโดยใช้อีเมล์ ชื่อ Good Times

ปี พ.ศ. 2538 มาโครไวรัสตัวแรกที่ชื่อ Concept มีผลต่อโปรแกรม Microsoft Word Basic

ปี พ.ศ. 2540 ไวรัสเริ่มแพร่ระบาดใน Chat forum

ปี พ.ศ. 2541
- มาโครไวรัสตัวแรกบน MS Access
- StrangeBrew ไวรัสตัวแรกที่ติดไฟล์จาวา
- Cherbobyl เป็นไวรัสตัวแรกที่ทำลายไบออสเครื่องคอมพิวเตอร์

ปี พ.ศ. 2542
- ไวรัส Tristate เป็นมาโครไวรัสที่ผลกับโปรแกรม Word Excel รวมทั้ง Powerpoint ด้วย
- หนอน ชื่อ Melisa ที่แพร่ระบาดทางอีเมล์จำนวนมาก
- ค้นพบไวรัส Funlove, 4099

ปี พ.ศ. 2543
- จดหมายรักถูกส่งออกมาพร้อมกับไวรัส VBS.LoveLetter
- ม้าโทรจันบนระบบปฏิบัติการ Palm OS ตัวแรก ชื่อ Plam.Liberty.A

ปี พ.ศ. 2544 - ค้นพบไวรัส VBSWG.J หรือรู้จักกันในชื่อ Anna Kournikova
- เซอร์เวอร์ IIS ถูก Code Red โจมตี
- หนอน Sircam ระบาดผ่านอีเมล์ และการแชร์ไฟล์
- หนอน Nimda โจมตีโดยอาศัยประตูลับที่หนอน Code Red II เปิดไว้
- หนอน BadTrans ระบาด

ปี พ.ศ. 2545 - หนอน Klez ระบาดรุนแรงมาก
- Bugbear ที่มีข่าวออกมาว่ารุนแรงกว่า Klez ระบาด

ปี พ.ศ. 2546 - หนอน Slammer ถูกปล่อยออกมา ทำให้เครือข่ายอินเทอร์เน็ตทั่วโลกหยุดให้บริการ
- Bugbear.B ถกปล่อยมาเพื่อขโมยข้อมูลทางการเงิน
- Blaster แล Nachi ที่มุ่งโจมตีช่องโหว่ DCOM RPC นอกจากนี้ยัง Sobig.F ที่ว่ากันว่าเป็นหนอนที่ระบาดทางอีเมล์เร็วที่สุด
- Swen.A เป็นหนอนที่ส่งอีเมล์คล้ายกับบริษัทไมโครซอฟต์เป็นผู้ส่งข้อมูลมา

ปี พ.ศ. 2547 - Bagle.A และ Mydoom ระบาดทางอีเมล์
- สายพันธ์ Bagle และ Netsky เริ่มระบาดอย่างต่อเนื่อง
- หนอน Sasser ออกมาโจมตีผ่านช่องโหว่ LSASS นอกจากนี้ยังมี Rugrat เป็นหนอนที่โจมตีผ่านวินโดว์ส 64 บิตตัวแรก
- ไวรัส Cabir เป็นไวรัสที่โจมตีผ่านโทรศัพท์มือถือเป็นตัวแรก
- ไวรัส Dust.A เป็นไวรัสโจมตีผ่าน Windows CE บน Pocket PC เป็นตัวแรก

ไวรัสคอมพิวเตอร์ที่เกิดขึ้นจากอดีตจนถึงปัจจุบันนี้มีมากกว่า 67,946 ตัว โดยมีไวรัสคอมพิวเตอร์ประมาณ 200-300 ตัวที่พบแพร่ระบาดอยู่ในปัจจุบัน และในแต่ละวันๆ จะมีไวรัสคอมพิวเตอร์เกิดขึ้นใหม่ๆ อีกนับร้อยตัวแต่ที่ตรวจสอบพบอาจจะพบเพียงวันละ 1-2 ตัว

2.3 ช่องทางการแพร่กระจายของไวรัสคอมพิวเตอร์

ช่องทางในการแพร่กระจายไวรัสคอมพิวเตอร์มี 2 ช่องทางคือ

1) หน่วยความจำสำรอง

โปรแกรมไวรัสคอมพิวเตอร์ติดอยู่ในฮาร์ดิสก์ของเครื่องคอมพิวเตอร์จะคัดลอกตัวเองผ่านทางแผ่นฟลอปปีดิสก์ เมื่อแผ่นฟลอปปีดิสก์ที่มีไวรัสติดอยู่ถูกนำไปใช้งานข้ามเครื่องก็จะคัดลอกตัวเองเข้าไปอยู่ในฮารด์ดิสก์ของเครื่องต่อไป

2) ระบบเครือข่าย

เนื่องจากการเติบโตของเครือข่ายคอมพิวเตอร์ ทำให้ไวรัสคอมพิวเตอร์ยุคหลังๆ มีความสามารถในการทำสำเนาคัดลอกและแพร่กระจายตัวเองผ่านระบบเครือข่ายมากขึ้น โดยเฉพาะอย่างยิ่งการแพร่กระจายผ่านเครือข่ายอินเทอร์เน็ตผ่านโปรแกรมรับ-ส่งจดหมายอิเล็กทรอนิกส์ หรืออีเมล์ต่างๆ

2.4 ไวรัสติดต่อกันได้อย่างไร

การแพร่กระจายของไวรัสนั้นสาเหตุที่สำคัญมาจากการที่เราแบ่งปันข้อมูลการทำงานหรือเพื่อความบันเทิงในลักษณะต่างๆ เช่น เพลง ภาพยนต์ โปรแกรม เกมส์ เป็นต้น โดยการคัดลอกผ่านสื่อบันทึกข้อมูลมาจากแหล่งอื่น รวมถึงการดาวน์โหลดผ่านระบบอินเตอร์เน็ต หากข้อมูลที่คัดลอก หรือดาวน์โหลดเข้ามาใรเครื่องติดไวรัสมาจากเครื่องใดเครื่องหนึ่งแล้ว เจ้าไวรัสก็จะทำการหลบซ่อนอยู่ในหน่วยความจำของเครื่องคอมพิวเตอร์เพื่อรอโอกาส เมื่อเรานำสื่อบันทึกข้อมูลอื่นไปใช้กับเครื่องที่ติดไวรัสนั้น ไวรัสจะทำการคัดลอกตัวเองจากหน่วยความจำของเครื่องลงมาติดส่วนต่างๆ ของสื่อบันทึกข้อมูลตามลักษณะการทำงานที่ไวรัสชนิดนั้นๆ ถูกสร้างขึ้นมาเช่นในโรงพยาบาลที่มีการใช้ระบบเครือข่ายคอมพิวเตอร์ร่วมกัน มีอัตราเสี่ยงที่จะติดไวรัสได้ง่ายมากโดยเฉพาะอย่างยิ่งเครื่องที่มีฮาร์ดดิสก์นั้นมีคุณสมบัติของการเป็นตัวการในการแพร่ไวรัสชั้นดี โดยไวรัสที่ติดมากับผู้ใช้คนใดคนหนึ่งในโรงพยาบาล ทั้งผ่านระบบเครือข่ายภายใน หรือการแลกเปลี่ยนข้อมูลผ่านสื่อบันทึกข้อมูล จะด้วยความตั้งใจหรือไม่ก็ตามไวรัสก็มีโอกาส

2.5 ความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์

อาการ และความเสียหายของคอมพิวเตอร์เมื่อถูกไวรัสแต่ละตัวจู่โจม จะมีความแตกต่างกันไปตามวัตถุประสงค์ของผู้เขียน หรือผู้ที่สร้างไวรัสนั้นขึ้นมา เช่น ทำลายระบบปฏิบัติการ โปรแกรมสำเร็จรูปหรือข้อมูลอื่นๆ ที่อยู่ในคอมพิวเตอร์ หรือรบกวนการทำงาน เช่น การบูตระบบช้าลง เรียกใช้โปรแกรมได้ไม่สมบูรณ์ หรือเกิดอาการค้าง (แฮงก์ไม่ทราบสาเหตุ) เกิดข้อความวิ่งไปมาที่

หน้าจอ หรือกรอบข้อความเตือนไม่ทราบสาเหตุ เป็นต้น ซึ่งสามารถแบ่งลักษณะการสร้างความเสียหายให้กับระบบ 2 ลักษณะ ดังนี้

1) Time Bomb เป็นการสร้างความเสียหายเมื่อถึงเวลาใดเวลาหนึ่ง

2) Logic Bomb เป็นการสร้างความเสียหายเมื่อเงื่อนไขใดเงื่อนไขหนึ่งในระบบเกิดขึ้น

2.6 ประเภทของไวรัส

เพื่อให้สะดวกในการป้องกันและกำจัดไวรัส จึงมีการแบ่งไวรัสคอมพิวเตอร์ออกเป็นหมวดหมู่ดังนี้

1) บูตเซกเตอร์ไวรัส (Boot Sector or Boot Infector Viruses) คือไวรัสที่เก็บตัวเองอยู่ในบูตเซกเตอร์ของดิสก์ เมื่อเครื่องคอมพิวเตอร์เริ่มทำงานขึ้นมาตอนแรก เครื่องจะเข้าไปอ่านโปรแกรมบูตระบบที่อยู่ในบูตเซกเตอร์ก่อน ถ้ามีไวรัสเข้าไปฝังตัวอยู่ในบูตเซกเตอร์ในบริเวณที่เรียกว่า Master Boot Record (MBR) ในทุกครั้งที่เราเปิดเครื่อง ก็เท่ากับว่าเราไปปลุกให้ไวรัสขึ้นมาทำงานทุกครั้งก่อนการเรียกใช้โปรแกรมอื่นๆ

2) โปรแกรมไวรัส (Program or File Infector Viruses) เป็นไวรัสอีกประเภทหนึ่งที่มักจะระบาดด้วยการติดไปกับไฟล์โปรแกรมที่มีนามสกุลเป็น com, exe, sys, dll สังเกตได้จากไฟล์โปรแกรมจะมีขนาดที่โตขึ้นจากเดิม บางชนิดอาจจะสำเนาตัวเองไปทับบางส่วนของโปรแกรมซึ่งไม่อาจสังเกตจากขนาดของไฟล์ได้ การทำงานของไวรัสจะเริ่มขึ้นเมื่อไฟล์โปรแกรมที่ติดไวรัสถูกเรียกมาทำงาน ไวรัสจะถือโอกาสไปฝังตัวในหน่วยความจำทันทีแล้วจึงให้โปรแกรมนั้นทำงานต่อไป เมื่อมีการเรียกโปรแกรมอื่นๆ ขึ้นมาทำงานไวรัสก็จะสำเนาตัวเองให้ติดไปกับโปรแกรมตัวอื่นๆ ต่อไปได้อีกเรื่อยๆ

3) มาโครไวรัส (Macro Viruses) เป็นไวรัสสายพันธุ์ที่ก่อกวนโปรแกรมสำนักงานต่างๆ เช่น MS Word, Excel, PowerPoint เป็นชุดคำสั่งเล็กๆ ทำงานอัตโนมัติ ติดต่อด้วยการสำเนาไฟล์จากเครื่องหนึ่งไปยังเครื่องหนึ่ง มักจะทำให้ไฟล์มีขนาดใหญ่ขึ้นผิดปกติ การทำงานหยุดชะงักโดยไม่ทราบสาเหตุ หรือทำให้ไฟล์เสียหาย ขัดขวางกระบวนการพิมพ์ เป็นต้น

4) สคริปต์ไวรัส (Scripts Viruses) ไวรัสสายพันธุ์นี้เขียนขึ้นมาจากภาษาที่ใช้ในการเขียนโปรแกรม เช่น VBScript, JavaScript ซึ่งไวรัสคอมพิวเตอร์เหล่านี้จะทำงานเมื่อผู้ใช้เปิดหรือเรียกใช้งานไฟล์นามสกุล .vbs, .js ที่เป็นไวรัส ซึ่งอาจจะติดมาจากการเรียกดูไฟล์ HTML ในหน้าเว็บเพจบนเครือข่ายอินเทอร์เน็ต

5) ม้าโทรจัน (Trojan Horses) เป็นไวรัสประเภทสปาย (SPY) ที่จะคอยล้วงความลับจากเครื่องของเราส่งไปให้ผู้เขียนโปรแกรม ระบาดกันมากบนอินเทอร์เน็ต ความลับที่ม้าโทรจันจะส่งกลับไปยังผู้เขียนโปรแกรมได้แก่ Username, Password หรือเลขที่บัตรเครดิต สำหรับท่านที่ชอบ

ปิ้งออนไลน์ โดยโปรแกรมพวกนี้จะสามารถจับการกดคีย์ใดๆ บนคีย์บอร์ดแล้วจัดเก็บเป็นไฟล์ข้อความขนาดเล็กส่งกลับไปยังผู้เขียนโปรแกรม

6) ไวรัสประเภทกลายพันธุ์ หมายถึง ไวรัสในยุคปัจจุบันนี้ที่มีความสามารถในการแพร่กระจายตัวเองได้อย่างรวดเร็ว เปลี่ยนแปลงลักษณะตัวเองไปเรื่อยๆ เพื่อหลีกเลี่ยงการตรวจจับและซ่อนแอบอยู่ได้ในระบบคอมพิวเตอร์ ที่รู้จักกันมากได้แก่ประเภทหนอน (Worm) ชนิดต่างๆ ซึ่งสามารถแพร่กระจายผ่านเครือข่ายอินเทอร์เน็ตด้วยการแฝงตัวไปกับอีเมล์ กับไฟล์สคริปต์ที่ให้บริการบนอินเทอร์เน็ต ตัวอย่างของไวรัสประเภทนี้ที่รู้จักกันดีก็ได้แก่ Love bug จะแพร่กระจายผ่านทางอีเมล์ เมื่อผู้รับเปิดอ่านจดหมายนั้นไวรัสจะแฝงตัวเข้าในเครื่องและค้นหารายชื่อที่อยู่อีเมล์ใน Addrees book โดยเฉพาะผู้ใช้งาน Outlook Express แล้วทำการส่งจดหมายไปยังผู้รับตามรายชื่อพร้อมไฟล์ไวรัสนั้นด้วย

2.7 ไวรัสสามารถสร้างความเสียหายได้ในระดับใด

ไวรัสคอมพิวเตอร์สามารถติดไปกับโปรแกรมต่างๆที่สามารถทำงานได้ เช่นเวิร์ดโปรแซสซิ่ง สเปรดชีต หรือ โปรแกรมระบบปฏิบัติการ ไวรัส สามารถติดไปกับส่วนต่างๆ ของดิสก์ หรือส่วนที่เฉพาะเจาะจงของระบบดิสก์ได้ เช่น Boot Record ได้ซึ่งมันจะถูกเรียกให้ทำงานทันทีที่มีการนำแผ่นดิสก์ที่มีไวรัสไปใช้งาน หรือมีการบูตระบบให้ทำงาน และจะเริ่มกระบวนการแพร่กระจาย แต่ไวรัสคอมพิวเตอร์ จะไม่สามารถสร้างความเสียหายให้เกิดขึ้นกับระบบที่เป็นฮาร์ดแวร์ได้ เช่นจอภาพ หรือคีย์บอร์ด แต่บางครั้งการทำงานของไวรัสทำให้เราเข้าใจผิดพลาด ว่าระบบฮาร์ดแวร์มีปัญหา ที่เป็นเช่นนั้นเพราะว่าไวรัสเข้าไปทำการควบคุมโปรแกรมที่ทำหน้าที่ควบคุมการทำงานของจอภาพ และคีย์บอร์ด เช่นการทำให้เกิดตัวอักษรแปลกๆ หรือตัวอักษรร่วงหล่นจากจอภาพ และไวรัสจะไม่สามารถทำให้ดิสก์เสียหายได้ เพียงแต่จะอาศัยอยู่ในดิสก์เท่านั้น และยังสามารถติดกับไฟล์ได้หลายๆประเภท และมันจะทำให้เกิดความผิดพลาดในการทำงานกับโปรแกรมหรือข้อมูลนั้นๆ เท่านั้น

2.8 การแก้ไขระบบที่ติดไวรัสคอมพิวเตอร์

การแก้ไขระบบที่ถูกไวรัสคอมพิวเตอร์คุกคามนั้นแตกต่างกันไปขึ้นอยู่กับไวรัสที่เข้ามาคุกคามระบบ ดังนั้นก่อนอื่นจะต้องทราบก่อนว่าไวรัสอะไรเข้ามาอยู่บนระบบ ส่วนใหญ่ระบบที่ถูกไวรัสคอมพิวเตอร์คุกคามคือระบบที่ไม่มีการใช้งานโปรแกรม Anti-virus หรือมีการใช้งานโปรแกรม Anti-virus แต่ไม่ได้ทำการ update ฐานข้อมูลไวรัส ดังนั้นการจะทราบถึงว่าไวรัสอะไรอยู่ในระบบได้นั้น ซึ่งสามารถเลือกใช้วิธีการต่อไปนี้

- นำเครื่องคอมพิวเตอร์อื่นที่มีซอฟต์แวร์ Anti-virus ติดตั้งอยู่และได้รับการ update ฐานข้อมูลไวรัสให้ทันสมัยและผ่านการตรวจสอบแล้วว่าระบบปราศจากไวรัส

คอมพิวเตอร์ เข้ามาช่วยในการตรวจสอบว่าระบบถูกไวรัสอะไรคุกคาม (สำหรับรายละเอียดเกี่ยวกับวิธีการตรวจสอบไวรัสโดยอาศัยเครื่องคอมพิวเตอร์อื่นด้วยการเชื่อมต่อคอมพิวเตอร์ทั้งสองเครื่องผ่านเครือข่าย (หรือการต่อสาย Cross) สามารถปรึกษาผู้เชี่ยวชาญได้ เช่น ThaiCERT ฯ)

- ใช้บริการระบบตรวจหาไวรัสคอมพิวเตอร์ผ่านเว็บ (ฟรี) เช่น http://housecall.trendmicro.com/housecall/ หรือ http://www.pandasoftware.com/products/activescan/ เป็นต้น จุดอ่อนของวิธีนี้คือการตรวจสอบอาจทำได้ไม่เร็วนักเนื่องจากความล่าช้าของเครือข่าย นอกจากนั้นระบบเหล่านี้อาจไม่ทำงานบนระบบที่มีซอฟต์แวร์ Anti-virus ยี่ห้ออื่นติดตั้งอยู่ และยิ่งไปกว่านั้น ไวรัสบางชนิดทำให้ระบบไม่สามารถใช้งานเครือข่ายได้เลย

บางครั้งอาจสงสัยว่าทำไมไม่ใช้วิธีติดตั้งซอฟต์แวร์ Anti-virus และ/หรือ update ฐานข้อมูลไวรัส และเรียกใช้งานโปรแกรมดังกล่าว เพื่อทำการตรวจหาไวรัสบนระบบ จุดอ่อนของวิธีนี้คือเมื่อระบบถูกไวรัสคุกคาม ไวรัสอาจทำการปิดกั้นหรือขัดขวางระบบทำให้ท่านไม่สามารถติดตั้งหรือเรียกใช้งานซอฟต์แวร์ดังกล่าวได้ หรืออาจทำให้ซอฟต์แวร์ Anti-virus ทำงานขัดข้องหรือบกพร่องได้ เมื่อทราบว่าระบบติดไวรัสชนิดใดแล้ว ให้ทำการจัดหาโปรแกรมสำหรับกำจัดไวรัสคอมพิวเตอร์ตัวนั้นๆ (Fix Tool) มาใช้กำจัดไวรัสบนระบบ ซึ่งสามารถ download โปรแกรม Fix Tool เหล่านี้มาใช้งานได้ฟรีจากเว็บไซต์ต่างๆเช่น http://www.pandasoftware.com/download/utilities/ เป็นต้น โดยอาจจะต้องทำให้ระบบปฏิบัติการทำงานใน Safe Mode (ปรึกษาผู้เชี่ยวชาญ) เพื่อที่จะให้โปรแกรม Fix Tool เหล่านี้ทำงานได้อย่างมีความถูกต้องสูงสุด

เมื่อกำจัดไวรัสบนระบบหมดแล้ว ให้ทำการตรวจสอบว่าระบบปฏิบัติการมีช่องโหว่ที่ critical อยู่หรือไม่ ถ้ามี ให้ทำการแก้ไข ซึ่งการตรวจสอบและแก้ไข โดยปกติทำได้โดยการ browse ไปที่ http://windowsupdate.microsoft.com/ เมื่อแก้ไขช่องโหว่ของระบบปฏิบัติการเสร็จแล้ว ให้ทำการติดตั้งโปรแกรม Anti-virus และ/หรือ update ฐานข้อมูลไวรัสให้ทันสมัยที่สุด และเรียกใช้งานโปรแกรมดังกล่าวเพื่อทำการตรวจสอบระบบโดยละเอียดอีกครั้งหนึ่งว่าปราศจากไวรัสคอมพิวเตอร์แล้ว โดยสรุปแล้ว ขั้นตอนคร่าวๆ ในการแก้ไขระบบที่ติดไวรัสคอมพิวเตอร์ คือ

1. ตรวจสอบว่าระบบติดไวรัสอะไร โดยการใช้โปรแกรมสำหรับตรวจสอบไวรัสซึ่งอาจทำได้โดยการอาศัยเครื่องคอมพิวเตอร์อีกเครื่องหนึ่งเข้ามาต่อพ่วงเพื่อช่วยในการตรวจสอบ หรืออาศัยระบบการตรวจสอบไวรัสคอมพิวเตอร์ผ่านทางเว็บ (Web-based virus scan engine)
2. Download โปรแกรมสำหรับแก้ไขไวรัสที่ตรวจพบมาใช้กำจัดไวรัส

3. อุดช่องโหว่ของระบบปฏิบัติการ
4. Update ฐานข้อมูลไวรัสของโปรแกรม Anti-virus แล้วตรวจหาไวรัสอีกครั้ง

บทที่ 3
สาเหตุ และอาการของคอมพิวเตอร์การติดไวรัส

3.1 สาเหตุของการติดไวรัสคอมพิวเตอร์

ไวรัสคอมพิวเตอร์สามารถติดหรือแพร่กระจายจากเครื่องคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องคอมพิวเตอร์อีกเครื่องหนึ่งได้หลายวิธี เช่น การแลกเปลี่ยนข้อมูลโดยการใช้อุปกรณ์บันทึกข้อมูลสำรอง จากเครื่องคอมพิวเตอร์ไปอีกเครื่องหนึ่ง การดาวน์โหลดข้อมูลหรือโปรแกรมคอมพิวเตอร์ที่ติดไวรัส จากเครือข่ายหรือระบบอินเทอร์เน็ต การเปิดข้อมูลเอกสารที่แนบมากับอีเมล์หรือการแชท (Chat) โดยข้อมูลที่แนบมากับอีเมล์หรือการแชทมักจะถูกตั้งชื่อไฟล์ให้น่าสนใจ เช่น เว็บแคม 004 (webcam_004), ไวรัสเอ็มเอสเอ็น (virus_msn), เลิฟมี (love_me), เซ็กซี่เบดรูม (sexy_bedroom) โดยผู้จัดทำได้ทำการรวบรวมสาเหตุหลักๆ ในการใช้งานคอมพิวเตอร์ที่อาจเป็นสาเหตุทำเครื่องคอมพิวเตอร์ของท่านติดไวรัสได้ดังต่อไปนี้

- ทางอีเมล์ ไวรัสที่มากับอีเมล์และไฟล์ที่แนบมากับอีเมล์ส่วนใหญ่จะเป็นไวรัสประเภทโทรจัน เกิดจากอีเมล์ที่ระบุแหล่งที่มาไม่ชัดเจนหรือผู้ที่เราไม่รู้จัก อาจจะมีลักษณะเป็นภาษาต่างดาว และที่สำคัญจะไม่ระบุชื่อผู้รับโดยตรง และกินเนื้อที่ค่อนข้างมาก
- การดูดอีเมล์จาก pop3 server ด้วยโปรแกรมอย่าง Outlook Express ส่วนใหญ่จะเป็นพวกหนอนอินเตอร์เน็ตประเภท mass-mailing worm เช่น Netsky, Beagle, Mydoom
- จากช่องโหว่ (vulnerability) ของระบบปฏิบัติการหรือของโปรแกรม โดย network worm, mass-mailing worm ที่โจมตีช่องโหว่ของ Windows เช่น Blaster, Sasser, Bobax ซึ่งต่อไปอาจจะเป็นกรณีของ zero-day attack
- จากการเข้าไปในเว็บที่มี malicious script/malware ซ่อนอยู่ก็อย่างเว็บโป๊ เว็บ crack ทั้งหลาย เช่นพวก dialer, trojan downloader, spyware, browser hijacker
- จากการเข้าไปในเว็บธรรมดาที่ติดไวรัสเช่น VBS/Redlof
- จากการเคลื่อนย้ายไฟล์จากเครื่องหนึ่งไปยังอีกเครื่อ งหนึ่งผ่านทางแผ่นดิสก์เช่น macro virus ที่อยู่ในไฟล์ของ MS Office
- การดาวโหลดไฟล์จากเครือข่าย P2P อย่างเช่น KaZaA เช่น P2P worm และโทรจันทั้งหลาย
- จากการดาวโหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถืออย่างเช่นเว็บ crack, warez ส่วนใหญ่จะเป็นพวก private/modified Trojan
- จากการเล่นหรือรับไฟล์จากโปรแกรมประเภท Instant Message เช่น MSN, ICQ

- จากการเล่นโปรแกรมประเภท IRC เช่น Pirch98 เช่น IRC Worm และอื่นๆ Instant messaging (IM) เช่น MSN ICQ, QQ , yahoo messenger , skype , IRC เป็นโปรแกรมส่งข้อความข้าม ระบบเน็ตเวิร์ค แบบทันทีทันใด การใช้งาน MSN Messenger แค่มี E-mail ของ hotmail หรือ MSN คุณก็สามารถเล่น MSN ได้ทันที พร้อมทั้งยังทำงานร่วมกับ E-mail ของเราด้วย โดยที่ เมื่อใดก็ตามที่มีเมล์ เข้ามาถึงเรา เจ้า MSN มันก็จะแจ้ง ให้ทราบทันที นอกจากนั้น ความเร็วของการ รับและส่งข้อความระหว่างกัน ก็ทำได้อย่างรวดเร็ว ซึ่งภัยร้ายที่แอบแฝงมาพร้อมกับการรับข้อมูลระหว่างกันก็คือไวรัสนั่นเอง การแพร่กระจายไวรัสทาง MSN จะแพร่กระจายอย่างเป็นเครือข่าย กล่าวคือ เมื่อมีผู้ใดผู้หนึ่งติดไวรัส

- การดาวน์โหลดไฟล์ต่าง ๆ จากอินเทอร์เน็ต ไม่ว่าจะเป็น ภาพพักหน้าจอ ภาพลามก เพลง ภาพการ์ตูน โปรแกรม Crack ต่าง ๆ และไฟล์อื่น ๆ อีกมากมาย มีโอกาสติดไวรัสทั้งสิ้น เพราะไวรัสมักจะแฝงตัวอยู่กับไฟล์หรือภาพต่าง ๆ เหล่านั้น เมื่อเราดาวน์โหลดไฟล์มาไว้ในเครื่องคอมพิวเตอร์ของเรา ก็จะทำให้ติดไวรัสได้

- แชร์ไฟล์ หมายถึง ไฟล์ที่สามารถให้ผู้อื่นในเครือข่ายเดียวกันสามารถเข้าถึงได้ การเปิดแชร์ไฟล์ ก็เป็นการให้ผู้อื่นใช้งานไฟล์จากเครื่องคอมพิวเตอร์ของเราโดยผ่านเครื่อง คอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่ายเดียวกัน ซึ่งการใช้งานแบบแชร์ไฟล์ก็มีโอกาสเสี่ยงที่จะติดหรือแพร่ไวรัส Folder ที่เปิดแชร์ไว้

3.2 ลักษณะของเครื่องคอมพิวเตอร์เมื่อติดไวรัสคอมพิวเตอร์

ลักษณะของเครื่องคอมพิวเตอร์เมื่อติดไวรัสคอมพิวเตอร์มีหลายลักษณะขึ้นอยู่กับประเภทของไวรัสคอมพิวเตอร์นั้น โดยมีลักษณะผิดปกติเพียงเล็กน้อยจนกระทั่งไม่สามารถใช้งานเครื่องคอมพิวเตอร์ได้ ซึ่งเราสามารถแบ่งอาการผิดปกติของเครื่องคอมพิวเตอร์ได้ 2 ลักษณะ คือ

3.2.1 อาการที่เกิดกับฮาร์ดแวร์ คือ ความผิดปกติต่างๆ ที่ส่งผลกับอุปกรณ์คอมพิวเตอร์ ได้แก่

- เครื่องคอมพิวเตอร์รีสตาร์ทตัวเองโดยไม่ได้สั่งงาน
- เครื่องคอมพิวเตอร์ทำงานช้าลง จนกระทั่งหยุดทำงานโดยไม่ทราบสาเหตุ
- ฮาร์ดดิสก์แจ้งว่ามีแบดเซกเตอร์เพิ่มขึ้น ทั้งที่ไม่ได้สั่งให้ตรวจสอบแบดเซกเตอร์นั้น
- เครื่องส่งเสียงดังออกทางลำโพงโดยไม่ได้เกิดจากโปรแกรมที่เปิดใช้งานอยู่
- แป้นพิมพ์ทำงานผิดปกติ เช่น พิมพ์ตัวอักษรหนึ่งแต่ปรากฏบนหน้าจออีกตัวอักษรหนึ่งจนถึงขั้นไม่สามารถใช้งานแป้นพิมพ์ได้เลย
- เมื่อตรวจเช็คขนาดของหน่วยความจำ จะปรากฏว่าเหลือน้อยกว่าปกติ
- ฮาร์ดดิสก์เสีย ไม่สามารถบันทึกข้อมูลได้ เนื่องจากไวรัสเข้าไปทำลายระบบ

3.2.2 อาการที่เกิดกับซอฟต์แวร์หรือโปรแกรม ทั้งโปรแกรมระบบซึ่งเป็นโปรแกรมหลักในการใช้งานเครื่องคอมพิวเตอร์และโปรแกรมประยุกต์ซึ่งแตกต่างกันไปตามเครื่องคอมพิวเตอร์ จะมีอาการที่แสดงว่าติดไวรัสคอมพิวเตอร์แตกต่างกัน เช่น

•โปรแกรมที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์มีขนาดใหญ่ขึ้นหรือต้องการพื้นที่การทำงานในฮาร์ดดิสก์มากยิ่งขึ้น

•วันและเวลาของโปรแกรมเปลี่ยนแปลงไป ไม่ตรงกับที่ตั้งไว้และไม่ว่าจะแก้ไขอย่างไรก็ตาม วันและเวลาของโปรแกรมก็จะเปลี่ยนแปลงไปเสมอ

•ซอฟต์แวร์ระบบไม่ทำงานหรือหยุดทำงานโดยไม่ทราบสาเหตุ

•ปรากฏแฟ้มข้อมูลที่ไม่ได้สร้างและแฟ้มข้อมูลบางแฟ้มถูกทำลายเป็นประจำไม่ว่าจะสร้างกี่ครั้งก็ตามตัวอักษรหรือข้อความในโปรแกรมปรากฏลักษณะที่ไม่ได้ติดตั้งโปรแกรม เช่น เกิดตารางสี่เหลี่ยมในโปรแกรมไมโครซอฟต์เวิร์ดและไม่สามารถเปลี่ยนเป็นลักษณะตัวอักษรแบบอื่นๆ ได้

•ซอฟต์แวร์หรือโปรแกรมที่ติดตั้งไว้หายไปจากโปรแกรมระบบไม่สามารถเปิดใช้งานโปรแกรมบางโปรแกรมได้

ทั้งนี้ผลกระทบที่เกิดขึ้นอาจมีลักษณะแตกต่างกันไป ขึ้นอยู่กับประเภทของไวรัสนั้นๆ เช่น

- ทำลายบูตเซกเตอร์ ทำให้ฮาร์ดดิสก์หรือแผ่นดิสก์ที่มีระบบ บูตไม่ได้
- ทำลายไฟล์ข้อมูล โดยลบไฟล์ข้อมูลแล้วกู้กลับคืนมาไม่ได้
- ทำลาย FAT ของแผ่นดิสก์
- ทำให้ไฟล์ข้อมูลมีขนาดเพิ่มขึ้นเอง โดยไวรัสจะสร้างข้อมูลขึ้นมาเอง ทำให้ไฟล์ข้อมูลมีลักษณะแปลกหูแปลกตาเกิดขึ้น
- ทำให้ความเร็วของเครื่องช้าลง การเรียกใช้โปรแกรมเสียเวลามากขึ้น
- การเรียกใช้บางโปรแกรม จะเกิดอาการเครื่องขัดข้อง (hang – up) ต้องเปิด – ปิดเครื่องบ่อย ๆ ทำให้ผู้ใช้เสียอารมณ์
- ฟอร์แมตแผ่นให้เราใหม่ โดยไม่ได้สั่ง
- หน่วยความจำของเครื่องมีขนาดเล็กลง
- ทำลายค่าที่ติดตั้งของระบบ เช่น ทำลายไฟล์ CONFIG.SYS ทำให้เมื่อเราเริ่มเปิดเครื่อง เครื่องจะไม่ทำงานในส่วนนี้
- ส่งข้อความแปลกประหลาด ออกทางหน้าจอหรือทางเครื่องพิมพ์แล้วแต่จังหวะโดยที่ผู้ใช้ไม่ได้สั่งการ

บทที่ 4
วิธีป้องกันตัวเองให้ปลอดภัยจากไวรัสคอมพิวเตอร์

อย่างที่ได้เกริ่นนำในบทในบทที่ผ่านมาทำให้เรามีความเข้าใจภัยมืดที่คอยคุกคามผู้ใช้งานระบบคอมพิวเตอร์ ซึ่งก็คงหนีไม่พ้น “ไวรัสคอมพิวเตอร์” ที่ทำให้ผู้ใช้งานคอมพิวเตอร์โดยทั่วไปต่างวิตกกังวล และเกรงกลัวว่าเครื่องคอมพิวเตอร์ที่ใช้งานอยู่จะติดเชื้อไวรัส จึงมีคำถามตามมาว่า แล้วพอมีวิธีการใดบ้างหรือไม่ที่จะใช้ป้องกันเครื่องคอมพิวเตอร์ และข้อมูลของตนเองให้ปลอดภัยจากไวรัสคอมพวิเตอร์ เช่นเริ่มต้นด้วยการจัดการภายในเครื่องเช่น การติดตั้งโปรแกรมป้องกันไวรัส ตลอดจนการใช้งานโปรแกรมที่มีการเชื่อมต่อไปยังอินเตอร์เน็ตเช่น โปรแกรมเว็บเบราเซอร์ โปรแกรมอ่าน E-Mail และ โปรแกรม Social Network อื่นๆ เป็นต้น

ในบทนี้จึงมุ่งเน้นให้เกิดประโยชน์ทั้งสำหรับผู้ใช้งานคอมพิวเตอร์ทั่วไป ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ ตลอดจนผู้บริหารที่จะสามารถวิธีการป้องกันเหล่านี้ไปใช้ประกอบในการร่างนโยบายการรักษาความปลอดภัยของคอมพิวเตอร์ภานในหน่วยงานด้วย และวิธีการที่กล่าวทั้งหมดต่อไปนี้เป็นเพียงวิธีการเบื้องต้นในการป้องกันตนเองเท่านั้น แต่ไม่สามารถป้องกันไวรัสได้ 100% โดยการป้องกันอาจทำได้ดังนี้

1. ตัดการเชื่อมต่อเครือข่ายก่อนการติดตั้งระบบปฏิบัติการ เป็นขั้นตอนที่สำคัญมากก่อนการติดตั้งระบบปฏิบัติการต้องทำการถอดสายแลนก่อน จนกระทั่งเมื่อติดตั้งโปรแกรมป้องกันไวรัสเสร็จแล้วจะต้องทำการปรับปรุงฐานข้อมูลของโปรแกรมป้องกันไวรัส เพื่อป้องกันการโจมตีจากไวรัสหรือผู้บุกรุกก่อนที่จะปรับแต่งให้เครื่องมีความแข็งแกร่งเพียงพอ

2. การฉีดวัคซีนคุ้มกัน ก็คือการติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์นั่นเอง ไม่ใช่ว่าเพียงแค่ติดตั้งโปรแกรมป้องกันไวรัสก็จะปลอดภัยจากไวรัสคอมพิวเตอร์ได้ ดังนั้นหลักการปฏิบัติเกี่ยวกับการใช้งานโปรแกรมป้องกันไวรัสเพื่อให้เครื่องปลอดภัยมีดังนี้

- เลือกใช้โปรแกรมป้องกันไวรัสที่เหมาะสมหรือตามที่องค์กรกำหนด
- สร้างแผ่นบูต emergency disk เพื่อใช้ช่วยในการกู้ระบบ การสร้างแผ่น emergency disk หรือบางครั้งอาจเรียกว่า Rescure disk นั้นมีความจำเป็นอย่างยิ่ง ถ้าเครื่องติดไวรัสที่ไม่สามารถจะกำจัดได้โดยผ่านระบบปฏิบัติการวินโดวส์ หรือผลกระทบของไวรัสที่ทำให้เครื่องไม่

สามารถบูตได้ตามปกติ เราก็สามารถใช้แผ่น emergency disk มาช่วยในการกู้ข้อมูลและกำจัดไวรัสออกจนทำให้บูตเครื่องได้ตามปกติ

- ปรับปรุงฐานข้อมูลไวรัสทุกวันหรืออย่างน้อยอาทิตย์ละครั้ง ขั้นตอนนี้เปรียบเสมือนหัวใจของการใช้งานโปรแกรมป้องกันไวรัส เนื่องจากไวรัสคอมพิวเตอร์ถูกพัฒนาออกมาใหม่ทุกวัน ดังนั้นจึงควรที่จะสอนโปรแกรมป้องกันไวรัสให้รู้จักไวรัสชนิดใหม่ๆ ด้วย โดยการปรับปรุงฐานข้อมูลไวรัสที่ใช้งานนั่นเอง

- ก่อนเปิดไฟล์จากแผ่นที่นำมาใช้จากที่อื่นให้สแกนหาไวรัสก่อน แผ่นดิสก์ที่นำไปใช้ที่อื่นแล้วนำกลับมาเปิดที่เครื่อง จะมั่นใจได้อย่างไรว่าแผ่นนั้นไม่มีไวรัสอยู่ ดังนั้นควรจะตรวจหาไวรัสในแผ่นก่อนที่จะเปิดอ่านข้อมูลที่ถูกบรรจุในแผ่นดิสก์ดังกล่าว

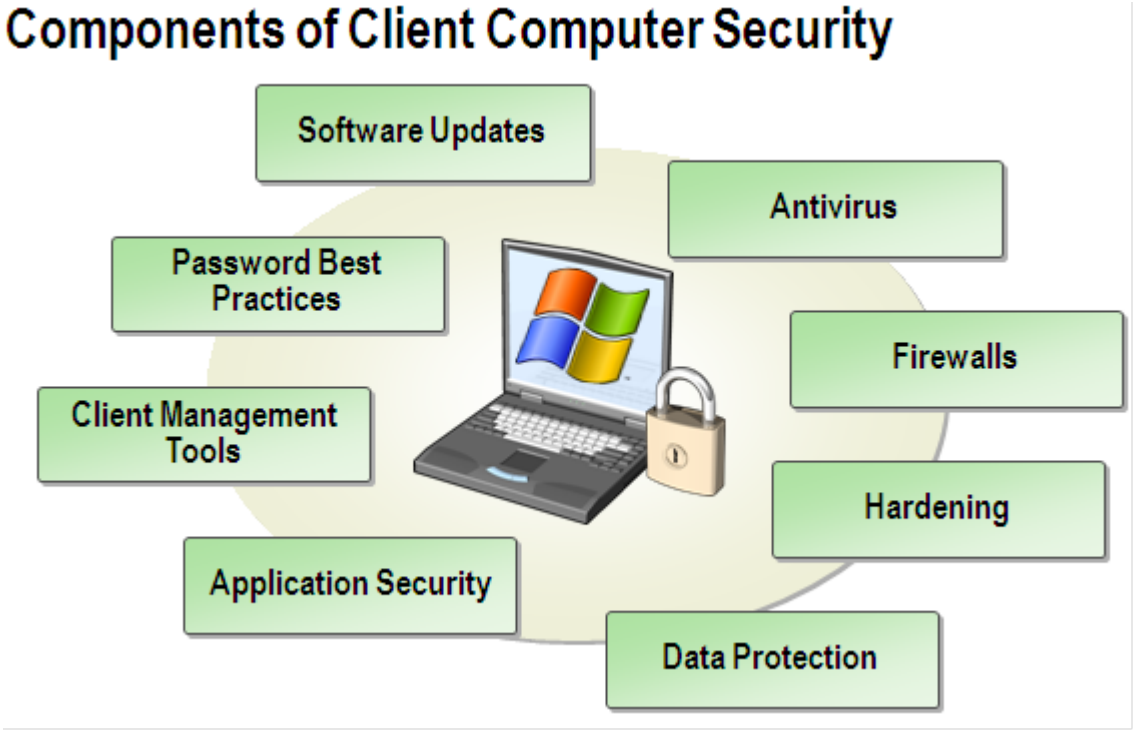
- ทำการตรวจหาไวรัสทุกสัปดาห์ ในแต่ละสัปดาห์แน่นอนว่ามีไฟล์ที่ผ่านเข้าออกเครื่องมากมาย ไม่ว่าจะเป็น อี-เมล์ที่ได้รับ ไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ตลอดจนไฟล์ชั่วคราวของโปรแกรมเว็บบราวเซอร์ที่เก็บในแต่ละครั้งที่เข้าเยี่ยมชมเว็บไซต์ แล้วจะแน่ใจได้อย่างไรว่าไฟล์เหล่านั้นไม่มีไวรัสแฝงตัวมา ดังนั้นจึงควรที่จะทำการตรวจหาไวรัส โดยการสแกนหาทั้งระบบ อาจจะเป็นทุกเย็นของวันศุกร์ก่อนกลับบ้านก็เป็นได้

3. การแชร์ไฟล์ และการรับ-ส่งไฟล์ต่างๆ การแชร์ไฟล์นั้นมีประโยชน์ในการรับ-ส่งไฟล์มากภายในองค์กร เนื่องจากทั้งรวดเร็วและเสียค่าใช้จ่ายน้อย แต่ทราบหรือไม่ว่าจากประโยชน์นี้ก็แฝงไว้ด้วยอันตรายที่น่าสะพรึงกลัวของไวรัสคอมพิวเตอร์ด้วย ดังนั้นการแชร์ไฟล์ควรกระทำด้วยความระมัดระวัง เป็นไปได้ก็ไม่ควรที่จะแชร์ไฟล์ แต่ถ้าในการใช้งานจริงๆ มีความจำเป็นที่จะต้องแชร์ไฟล์ก็ควรที่จะแชร์เป็นประเภทอ่านอย่างเดียว และควรตั้งรหัสผ่านด้วย

4. สำรองข้อมูลไว้ เมื่อเกิดเหตุการณ์ที่ไม่คาดคิดกับเครื่องที่ใช้งานอยู่ เป็นต้นว่าไฟฟ้าตก หรือไวรัสแพร่กระจายไปยังไฟล์สำคัญ อาจส่งผลให้เครื่องนั้นไม่สามารถใช้งานได้ตามปกติหรือใช้งานไฟล์บางไฟล์ไม่ได้ ซึ่งอาจจะส่งผลให้เจ้าของเครื่องดังกล่าวสูญเสียข้อมูลสำคัญๆ ได้ ดังนั้นถ้าเรามีการสำรองข้อมูลไว้ ปัญหาที่ผู้ใช้งานจะสูญเสียข้อมูลก็จะลดลงได้มากพอสมควร ในการสำรองข้อมูลเพื่อใช้ในการกู้ระบบคืนนั้นควรกระทำบ่อยๆ อย่างน้อยประมาณ 1 ครั้งต่อสัปดาห์ และสิ่งที่ควรจะทำการสำรองไว้บ่อยๆ คือ

5. ติดตามข่าวสารต่างๆ เนื่องด้วยในวันหนึ่งๆ จะมีไวรัสคอมพิวเตอร์ออกมาใหม่เป็นจำนวนมาก ดังนั้นการรับรู้ข้อมูลข่าวสารที่รวดเร็วและหาทางป้องกันจึงนับเป็นหนทางที่ดีที่สุดวิธีหนึ่งในการป้องกันไวรัสคอมพิวเตอร์ ไม่ว่าจะเป็นผู้ใช้ทั่วๆ ไปหรือแม้กระทั่งผู้ดูแลระบบเอง จึงควรที่จะหาช่องทางในการรับรู้ข่าวสารเกี่ยวกับไวรัสคอมพิวเตอร์และข่าวสารเกี่ยวกับความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้วย

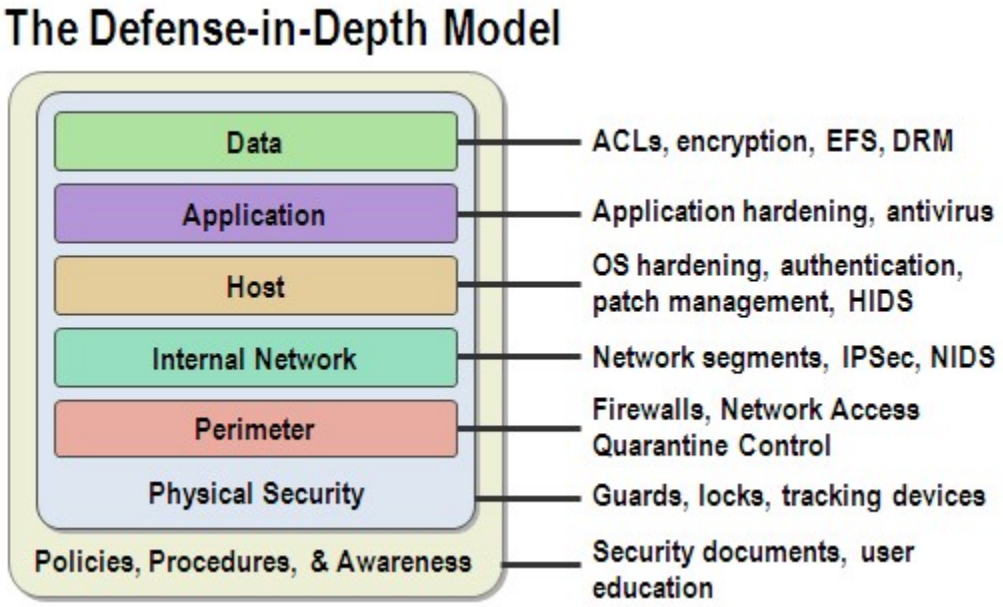
4.1 รู้จักกับฮาร์ดเดนนิง (Hardening) และการเพิ่มความปลอดภัยให้กับคอมพิวเตอร์ส่วนตัว



ข้อมูลสารสนเทศที่เก็บไว้ในคอมพิวเตอร์ส่วนตัวที่เราใช้งานอยู่ ไม่ว่าจะเป็นข้อมูลส่วนตัวหรือ ข้อมูลขององค์กร มีความเสี่ยงที่อาจได้รับการคุกคามจากหลายแหล่งอาทิเช่น การแพร่กระจายของไวรัส หรือถูกเครื่องมือ Hack Tools ที่มีแจกจ่ายอยู่ในโลก Internet มาทำการค้นข้อมูลภายในเครื่อง ทำให้เครื่องคอมพิวเตอร์ของเรามีปัญหา และอาการแปลก ๆ และอาจนำไปสู่ความเสียหายที่ประเมินค่ามิได้ซึ่งหลายท่านอาจเคยได้พบเจอมาแล้ว

ทั้งนี้อาจมาจากการที่ระบบปฏิบัติการที่เราใช้มีช่องโหว่ โดยเฉพาะ Windows XP และภัยคุกคามที่มีการแพร่หลายอย่างรวดเร็วได้ในปัจจุบัน ทำให้ทั้งองค์กร ผู้เชี่ยวชาญด้านไอที และผู้ใช้งานทั่วไปที่มีความรู้ด้านไอที มักจะแสวงหาการลงทุนเรื่อง Hardware / Software เพื่อปกป้องภัยคุกคามต่าง ๆ ที่อาจจะเกิดขึ้นกับระบบคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ที่ใช้งาน

รูปด้านล่างแสดงถึงการลงทุนมหาศาลด้านเทคโนโลยีสารสนเทศเพื่อสร้างความปลอดภัยให้กับองค์กร หรือคอมพิวเตอร์ส่วนตัว โดยที่ทางซ้ายมือของท่านผู้อ่านเป็นส่วนที่มีความเสี่ยงจะถูกภัยคุกคาม และด้านขวามือแสดงถึงเครื่องมือต่าง ๆ ที่ใช้เป็นแนวทางในการปกป้องภัยคุกคาม



ภาพแนวทางการเลือกใช้เพื่อเพิ่มความปลอดภัยให้กับเทคโนโลยีสารสนเทศบริษัท Microsoft

ภาพดังกล่าวแสดงถึงค่าใช้จ่ายจำนวนมหาศาลเพื่อการป้องกันภัยคุกคามด้านสารสนเทศ แต่มีอยู่ช่องทางหนึ่งวที่เป็นการเพิ่มความปลอดภัยให้สูงขึ้นโดยไม่เพิ่มค่าใช้จ่าย

“นั่นคือการทำ ฮาร์ดเดนนิง (Hardening)”

การฮาร์ดเดนนิงระบบปฏิบัติการ (Operating System Hardening) เป็นกระบวนการของการกำหนดค่า (Parameter) บนระบบปฏิบัติการเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตป้องกันผู้บุกรุก แฮกเกอร์ และช่องโหว่ด้านความปลอดภัยอื่น ๆ OS ทำให้ระบบคอมพิวเตอร์เชื่อถือได้มากขึ้น มีความปลอดภัย และช่วยเพิ่มประสิทธิภาพการทำงานเนื่องจากใช้หลักการ "ลดสิ่งที่ไม่ได้ใช้ออกไปจากระบบ" นั่นเอง

โดยหลักหารของ Hardening คือ การลดความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้น ที่เป็นผลมาจากการควบคุมของผู้ใช้เองให้ได้มากที่สุดซึ่งวิธีดังกล่าวเป็นวิธีการเพิ่มความปลอดภัยให้คอมพิวเตอร์โดยการควบคุมระบบปฏิบัติการที่เราใช้อยู่ ที่ผ่านมาวิธีดังกล่าวเป็นวิธีการที่มักถูกมองข้ามแต่ได้ผลโดยผู้ใช้ไม่จำเป็นต้องสูญเงินไปกับการซื้อ Software ราคาแพงเพื่อเพิ่มขีดความสามารถด้านการรักษาความปลอดภัย ก็สามารถเพิ่มความปลอดภัยให้กับคอมพิวเตอร์ได้ เพียงแต่เราใส่ใจนำเอา Security Best Practice ของระบบปฏิบัติการที่ใช้อยู่มาลงมือปฏิบัติกับระบบปฏิบัติการที่เราใช้ ซึ่งโดยส่วนใหญ่

บรรดาผู้ผลิต Software ระบบปฏิบัติการ แจกจ่ายให้แก่ลูกค้าผู้ใช้ผลิตภัณฑ์อยู่แล้วแต่มักถูกมองข้ามหรือให้ความสนใจนำมาใช้เป็นประโยชน์เพียงบางกลุ่มเท่านั้น

หากเรามองในมุมขององค์กร หรือหน่วยงานแล้ว กระบวนการในการทำ Hardening เป็นหนึ่งในส่วนสำคัญในการสร้างมาตรฐานการรักษาความปลอดภัยข้อมูลอย่างเป็นระบบและมีประสิทธิภาพ

จากภาพ แสดงการทำ Hardening เป็นส่วนหนึ่งในกระบวนการสำคัญในการบริหารจัดการระบบรักษาความปลอดภัยของข้อมูลอย่างเป็นระบบและมีประสิทธิภาพ

4.2วิธีการ Hardening อย่างง่ายที่สามารถเพื่อมความปลอดภัยให้กับคอมพิวเตอร์ของท่าน

1. <u>เลือกใช้ระบบไฟล์ NTFS</u>
   ระบบไฟล์ NTFS ช่วยให้ข้อมูลที่อยู่บนเครื่องของเรามีการพิสูจน์สิทธิก่อนการเข้าถึงควรตรวจสอบระบบการจัดเก็บบน Harddisk ให้เป็นแบบ NTFS
2. <u>ปิดการใช้งาน Autorun (Disable Autorun)</u>
   Autorun เป็นปัญหาหลักที่ช่วยให้ไวรัสแพร่กระจายได้อย่างรวดเร็ว เพราะทุกครั้งที่เราทำการ double click USB Drive ที่เรานำมาใช้งาน ไวรัสหรือไฟล์ที่ execute ต่าง ๆ ก็สามารถทำงานได้ทันที วิธีการปิด Autorun คือ Start > Run > ใช่คำสั่ง GPEDIT.MSC > จากนั้นไปที่ Computer Configuration > Administrative Templates > System > หาคำว่า Turn autoplay off ให้เลือกเป็น Enable

3. <u>เลือกใช้งานรหัสผ่านสำหรับ Screen Saver (Password Protect for Screen Saver)</u>
   หลังจากที่เราเพิ่มการป้องกันเครื่องคอมพิวเตอร์ของเราด้วยการตั้งรหัสผ่านเรียบร้อยแล้ว การเพิ่มความปลอดภัยโดยการตั้งให้ Screen Saver ทำงานพร้อมกับมีการถามรหัสผ่านสำหรับการกลับเข้าสู่ระบบเสมอวิธีการปรับแต่งคือคลิกขวาที่ Desktop แล้วเลือก Properties จากนั้นไปที่ TAB Screen Saver เลือกเช็ค Box ให้ On Resume, display Welcome screen
4. <u>ปิดการใช้งานรีโมท (Disable Remote Desktop)</u>
   Remote Desktop เป็น Service ที่ทำให้คอมพิวเตอร์ของเราเปิด Port ไว้มากขึ้นเป็นการเพิ่ม Attack Surface ให้กับระบบ หากไม่มีความจำเป็นต้องใช้งานควรปิดการใช้งานฟังก์ชันนี้
5. <u>เลือกใช้งาน Internet Explorer เวอร์ชัน ล่าสุดเสมอ</u>
   Internet Explorer Version ที่ออกมาสามารถรองรับการทำงานบน Windows ได้อย่างไม่มีปัญหาการปรับปรุงความปลอดภัยที่เพิ่มขึ้นเป็นสิ่งที่น่าพิจารณารีบดาวน์โหลดมาใช้งานกัน
6. <u>อย่าลืม Windows Update และ Windows Service Pack</u>
7. <u>ตั้งรหัสผ่านเสมอสำหรับทุก Users ที่มีอยู่บนเครื่องคอมพิวเตอร์</u>
   เนื่องจาก Windows XP ยอมให้มีการใช้งานโดย Users ไม่จำเป็นต้องตั้งรหัสผ่านใดๆ ดังนั้นมันจึงเป็นช่องโหว่ที่สำคัญของการใช้งานระบบ โดยเฉพาะความเสี่ยงที่ หลายคนเก็บข้อมูลส่วนบุคคล และข้อมูลทางการเงินบนคอมพิวเตอร์ส่วนตัว การตั้งรหัสผ่านควรตั้งให้ยากต่อการคาดเดาด้วยนะครับ
8. <u>ลบ หรือ Disable Users ที่ไม่จำเป็นใช้งานออกจากระบบ</u>
   อาจมี User ที่เราเผลอสร้างขึ้นมาหลังจากทดลองใช้งาน หรือติดมากับ Application ต่างๆ หากแน่ใจว่าไม่มีความจำเป็นต้องใช้งานควรลบ Users นั้น ๆ ออกจากระบบ หรือเลือก Disable ชั่วคราวหากยังไม่แน่ใจ โดยเฉพาะ User Guest ควรจะ Disable ก่อนเป็นอันดับแรก
9. <u>ระมัดระวังการแชร์ไฟล์ผ่านระบบเครือข่าย</u>
   ตรวจสอบอยู่เสมอถึงการแชร์ไฟล์บนเครื่องของเราว่ามีการกรองการเข้าถึงที่ดีหรือยัง (Access Control + Assign Permission) โดยเฉพาะข้อมูลสำคัญของบริษัท ข้อมูลส่วนบุคคล และข้อมูลทางการเงินที่เก็บไว้บนคอมพิวเตอร์ส่วนตัว

การ Hardening ที่ได้แนะนำเป็นเป็นเพียงบางส่วน เป็นวิธีการที่ไม่สลับสลับซับซ้อนมากนัก โดยเราสามารถติดตามวิธีการในการตั้งค่า หรือปรับแต่งระบบปฏิบัติการของเครื่องคอมพิวเตอร์ให้มีความปลอดภัยมากยิ่งขึ้นโดยวิธีการต่างๆ สามารถติดตามได้จากแหล่งชุมนุมของเหล่ากูรู ที่มักนำเทคนิควิธีการ และเทคนิคใหม่ๆ มาแบ่งปันกันบนโลกออนไลน์ การติดตามข้อมูลความรู้เหล่านี้ก็สามารถที่จะช่วยให้การใช้งานคอมพิวเตอร์ของท่านมีความปลอดภัยมากขึ้น และที่สำคัญคือมีค่าใช้จ่ายต่ำ และสามารถทำได้เอง

บทที่ 5
โปรแกรมป้องกันไวรัส

โปรแกรม Antivirus นั้นเป็นโปรแกรมที่ถูกเขียนขึ้นมาเพื่อป้องกันไวรัสที่จะเข้ามาสร้างความเสียหายแก่ข้อมูลและระบบคอมพิวเตอร์ เปรียบเหมือนในชีวิตคนเราแน่นอนว่าไวรัสเป็นตัวก่อกำเนิดโรคภัยต่างๆ ในคอมพิวเตอร์ก็เช่นกันครับไวรัสนั้นก็เป็นตัวที่ทำให้คอมพิวเตอร์ของเรานั้นเสียหายจนอาจจะถึงขั้นป่วยหนัก และถึงขั้นไม่สามารถเปิดคอมพิวเตอร์เลยก็เป็นได้ โดยโปรแกรม Antivirus จุดประสงค์เพื่อที่จะฆ่าหรือป้องกันไวรัสที่จะเข้ามาทำร้ายเครื่องคอมพิวเตอร์ ถ้าหากเปรียบเทียบก็คงเหมือนดั่งวัคซีน หรือยาบรรเทา เพื่อรักษาอาการความผิดปกติ และความเสียหายที่เกิดขึ้น

โปรแกรม Antivirus นั้นมีอยู่มากมายในโลกนี้ครับแต่ก็ไม่มีตัวใดที่ดีที่สุด เพราะของที่ดีที่สุดอยู่ที่เราพอใจมันรึไม่ แต่โปรแกรม Antivirus ที่ดีจะต้องมีคุณสมบัติดังต่อไปนี้

5.1คุณสมบัติโปรแกรม Antivirus ที่ดี คือ

1. ใช้ทรัพยากรเครื่องที่น้อย หรือพูดง่ายๆใช้พื้นในการติดตั้งน้อย ไม่กินแรมจนทำให้เครื่องอืด
2. สามารถตรวจสอบสายพันธุ์ไวรัสได้จำนวนมาก แม่นยำ และฉับไว
3. มีการ Update ฐานข้อมูลของสายพันธุ์ ไวรัสตลอดเวลา ถ้าหากจะให้ดีอัพเดตตลอดทุกวันเพราะว่าไวรัสนั้นเกิดขึ้นใหม่ทุกวัน
4. สามารถจัดการเจ้าไวรัสนั้นได้ก่อนที่มันจะมาทำลายข้อมูลงานของเราและยังสามารถที่จะซ่อมไฟล์ที่ถูกไวรัสนั้นแทรกซึมบางส่วนให้กลับมาเป็นปกติได้ครับ
5. มีหน้าตาที่ใช้งานง่าย เข้าใจง่าย

ถ้าหากว่ากำลังมองหาโปรแกรม Antivirus อยู่ละก็สามารถที่จะใช้เกณฑ์คุณสมบัตินี้ในการเลือกเพราะถือว่าเป็นเกณฑ์มาตรฐานที่เอาไว้ดูโปรแกรม Antivirus ที่มีประสิทธิภาพ ซึ่งช่วยให้เรานั้นสามารถที่จะเลือกโปรแกรม Antivirus เพื่อใช้งานได้อย่างเหมาะสมมากยิ่งขึ้น

ปัจจุบันได้มีโปรแกรมป้องกันไวรัสหลากหลายในท้องตลอดให้ผู้ใช้ได้เลือกสรร โดยแต่ละค่ายมีจุดเด่นและจุดด้อย แตกต่างกัน ตามความต้องการและความชอบส่วนตัว ซึ่งไวรัสที่เป็นที่นิยมในปัจจุบัน คือ

- Kaspersky Antivirus
- Nod 32 Antivirus
- Avast Antivirus
- Norton Antivirus
- Mcafree Antivirus
- Bitdefender Antivirus
- AVG Antivirus
- Avira Antivirus
- Panda Antivirus

โดยข้อมูลอ้างอิงผลการจัดลำดับ 10 สุดยอดโปรแกรมป้องกันไวรัสที่ดีที่สุดสำหรับปี 2012 จากเว็บไซต์ TopTenReviews โดยอันดับหนึ่งนั้นก็คือ Bitdefender Antivirus Plus ตามมาด้วย Kaspersky Anti-Virus ส่วนอันดับสามเป็น Panda Antivirus Pro ซึ่งไม่มีความแตกต่างกันมากนักจากการจัดลำดับปี 2011 เพราะโปรแกรมที่เข้าวินส่วนใหญ่นั้นก็มาจากค่ายเดิมๆ ซึ่งแสดงถึงความน่าเชื่อถือของโปรแกรม Antivirus ค่ายต่างๆ ที่มีผู้นิยมเลือกใช้

Rank	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
★★★★ Excellent ★★★☆ Very Good ★★☆☆ Good ★☆☆☆ Fair ☆☆☆☆ Poor	Bitdefender Antivirus Plus	Kaspersky Anti-Virus	Panda Antivirus Pro	F-Secure Anti-Virus	AVG Anti-Virus	Avast! Pro Antivirus	G Data AntiVirus	BullGuard Antivirus	Avira AntiVir Premium	ESET NOD32 Antivirus
Reviewer Comments	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review
Lowest Price	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now
	$29.95	$59.95	$39.99	$39.99	$34.99	$39.99	$29.95	$29.95	$23.49	$39.99
Overall Rating	★★★★	★★★★	★★★½	★★★½	★★★½	★★★☆	★★★☆	★★★☆	★★★☆	★★★☆
Ratings										
Performance	★★★★	★★★★	★★★½	★★★½	★★★☆	★★★☆	★★★½	★★★☆	★★★☆	★★★☆
Features	★★★★	★★★★	★★★½	★★☆☆	★★★★	★★★★	★★★☆	★★★★	★★★½	★★★★
Help & Support	★★★★	★★★★	★★☆☆	★★★★	★★★★	★★★☆	★★★☆	★★★★	★★★★	★★★☆

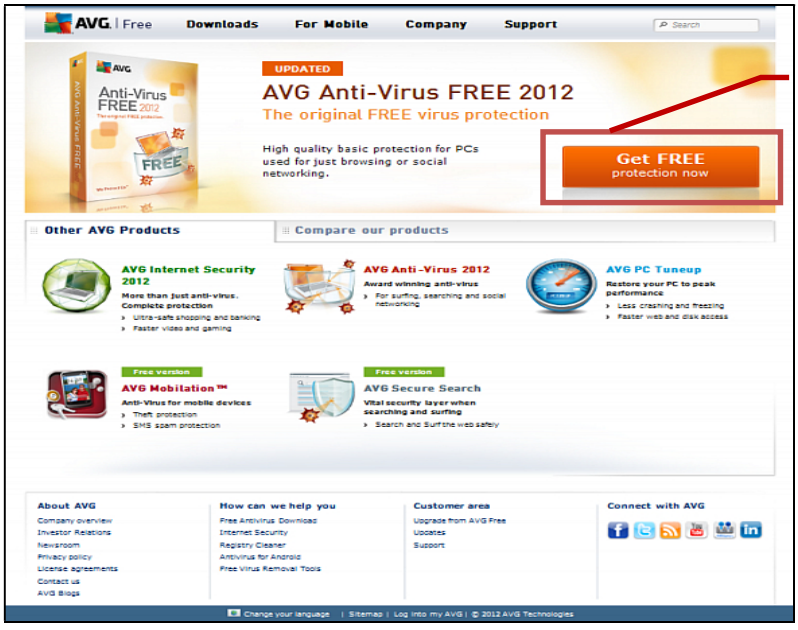
ภาพแสดงผลการจัดอันดับ 10 สุดยอดโปรแกรมป้องกันไวรัสที่ดีที่สุดสำหรับปี 2012" จากเว็บไซต์ TopTenReviews

ในช่วงที่ผ่านมานั้นเรามักได้ยินข่าวการแพร่ระบาดของไวรัสอย่างต่อเนื่อง เพื่อเป็นประโยชน์แก่ผู้ศึกษาการจัดการความรู้ฉบับนี้ ผู้จัดทำจึงขอแนะนำโปรแกรมป้องกันไวรัสที่ดีมากอีกค่ายหนึ่ง ที่ติดอันดับ 10 สุดยอดโปรแกรมป้องกันไวรัสที่ดีที่สุดสำหรับปี 2012 คือ AVG Anti – Virus Free 2012

ซึ่งเป็นโปรแกรม Antivirus เวอร์ชันล่าสุดจากค่าย AVG ซึ่งแจกให้ใช้ฟรีและดีมากๆ ตัวหนึ่งมีผู้ใช้ทั่วโลกมากมายและเป็นฟรี Antivirus ชั้นแนวหน้าของโลกอีกด้วย โดยคุณสมบัติหลักที่ให้มานั้นก็คือการผ้องกันไวรัสและสปายแวร์ทั้งหลายที่จะเข้ามาทำร้ายหรือดักจับข้อมูลในเครื่องคอมพิวเตอร์ เรื่องประสิทธิภาพการทำงาน Antivirus ที่จะนำมาแนะนำกันนี้ดับรางวัลเป็นเครื่องการันตีมากมาย ไม่ว่าจะเป็น อันดับที่ 5 จากผลการจัดลำดับอันดับ 10 สุดยอดโปรแกรมป้องกันไวรัสที่ดีที่สุดสำหรับปี 2012 และได้รับคำชื่นชมจากผู้ใช้บนโลกออนไลน์มากมายในช่วงที่ผ่านมา

5.2 ขั้นตอนการติดตั้ง AVG Anti – Virus Free 2012

1. เปิด web browser และไปยังเว็บ AVG.com เพื่อทำการดาวน์โหลด Application : AVG Anti – Virus Free 2012 (http://free.avg.com/ww-en/free-downloads) จะ เข้าสู่หน้า เว็บเพจดังภาพ แล้วทำการ Click ขวา ตามรูปภาพเพื่อเข้าสู่ขั้นตอนการ Download Program



Click ขวา เพื่อดาวน์โหลดโปรแกรม AVG Anti – Virus Free 2012

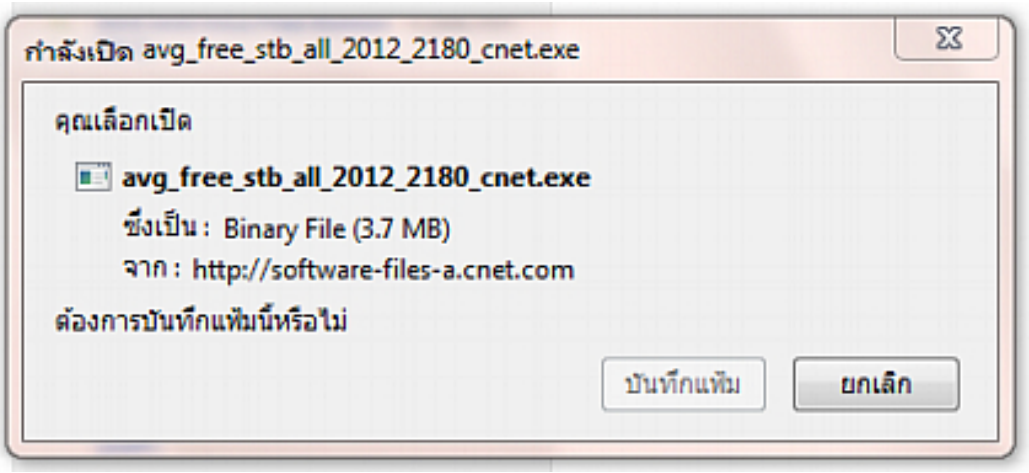
2. จากขั้นตอนที่ 1 จะเข้ามาสู่เว็บเพจดังภาพ จากนั้นให้ทำการเลือกดาวน์โหลด AVG Anti – Virus 2012 Free Version ตามภาพด้านล่าง

Click ขวา เพื่อดาวน์โหลด โปรแกรม AVG Anti – Virus Free Version

3. จะเข้ามาสู่เว็บเพจดังภาพ จากนั้นให้ทำการเลือก Download Now

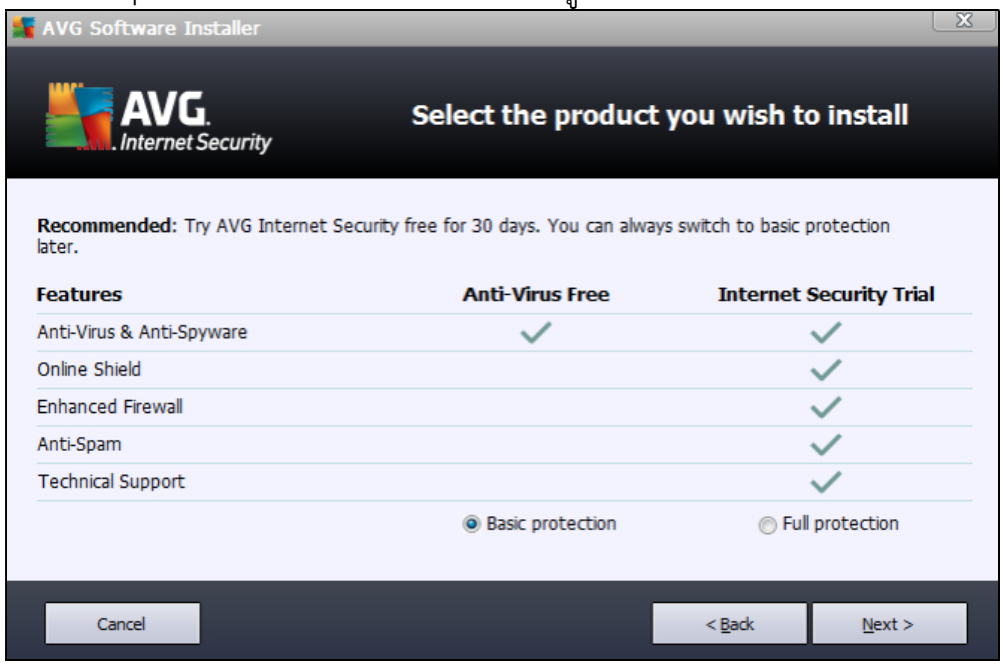
Click ที่ Download Now
เพื่อเริ่มต้น Download

4. ขั้นตอนนี้ระบบจะถามว่าต้องการบันทึก หรือยกเลิกการดาวน์โหลด ให้เลือก “บันทึกแฟ้ม” เพื่อบันทึกโปรแกรมลงในเครื่องคอมพิวเตอร์ และรอจนกว่าการดาวน์โหลดโปรแกรมเสร็จสิ้น

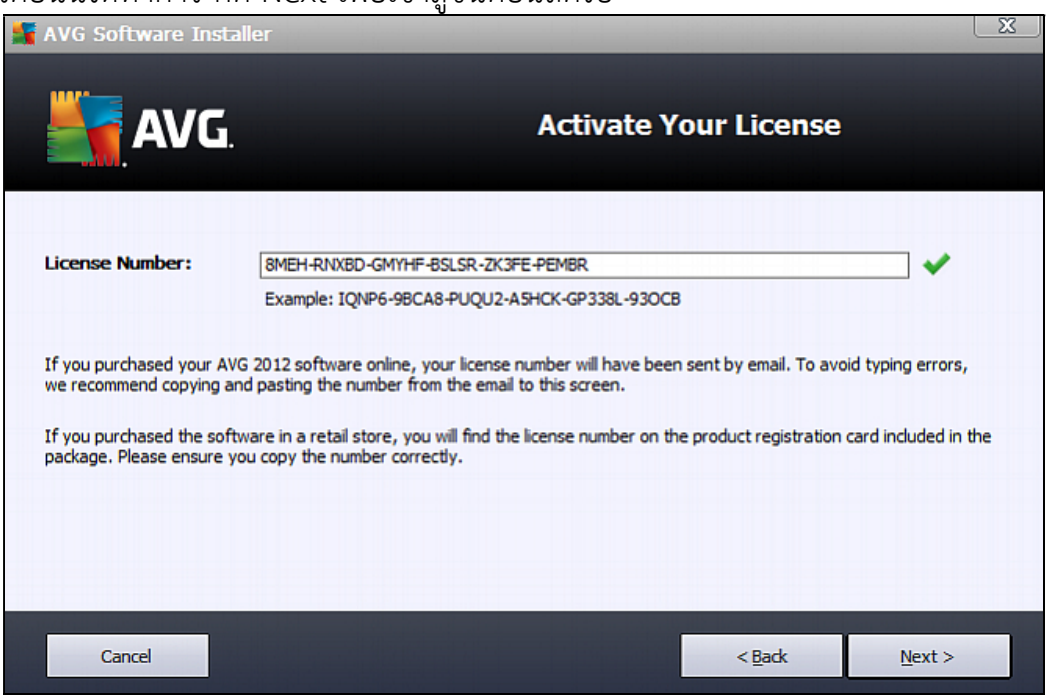


5. เมื่อโปรแกรมที่ทำการดาวน์โหลดเสร็จสมบูรณ์ ให้ทำการ Double Click เพื่อเริ่มเข้าสู่ขั้นตอนการติดตั้งจะปรากฏดังภาพ ในขั้นตอนนี้ให้เลือก Accept

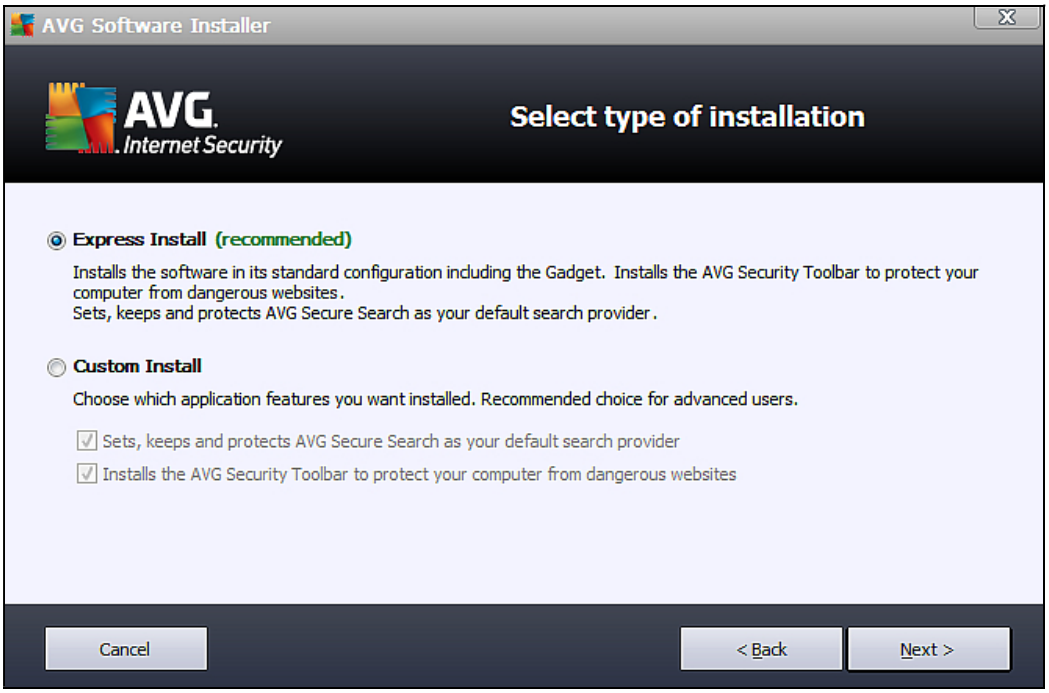
6. จากนั้นโปรแกรม จะให้ทำการเลือกระหว่าง Basic protection และ Full protection ให้เลือก Basic protection และกด Next เพื่อเข้าสู่ขั้นตอนถัดไป



7. ในขั้นตอนนี้ให้ทำการ กด Next เพื่อเข้าสู่ขั้นตอนถัดไป

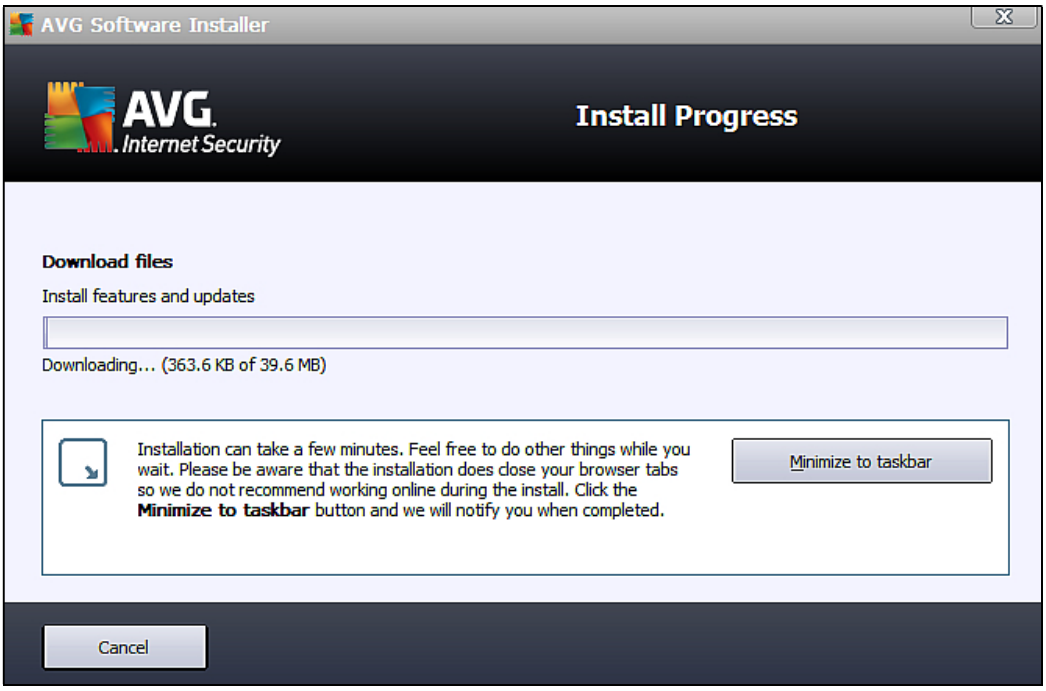


8. จากนั้นโปรแกรมจะมีตัวเลือกระหว่าง Express Install และ Custom Install ให้เลือก Express Install และกด Next เพื่อเข้าสู่ขั้นตอนถัดไป



9. จากนั้นโปรแกรมจะเริ่มทำการ Download และติดตั้ง AVG Anti – Virus 2012

ในขั้นตอนนี้ให้รอจนโปรแกรมดำเนินการติดตั้งจนเสร็จสิ้น

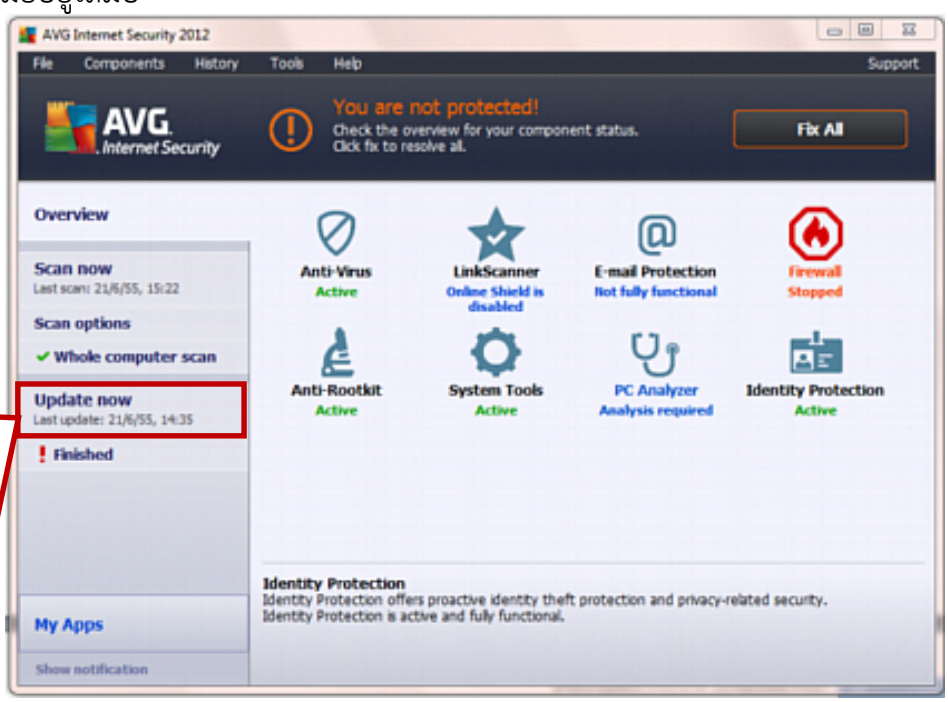


10. เมื่อโปรแกรมทำการติดตั้งแล้วเสร็จโปรแกรมจะเริ่มทำงาน ดังภาพที่ปรากฏ ถึงขั้นตอนนี้แสดงว่าการติดตั้งโปรแกรมสำเร็จ และสามารถทำงานได้อย่างสมบูรณ์

11. หลังจากนั้นให้ทำการ Update ข้อมูล เพื่อทำให้ฐานข้อมูลที่จะเป็นภูมิคุ้มกันไวรัสให้

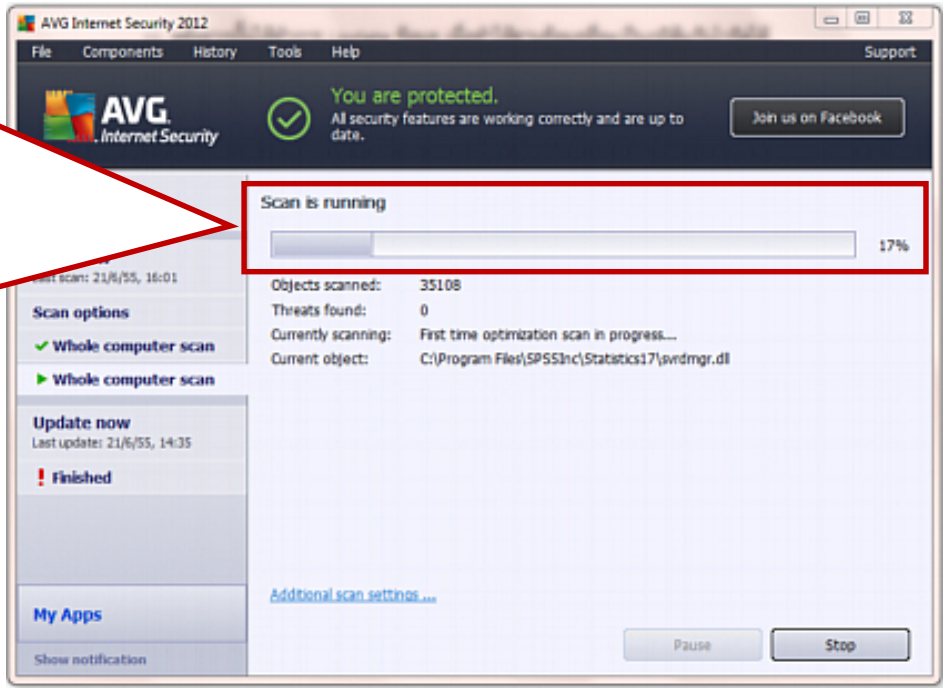
กับเรามีความทันสมัยอยู่เสมอ

เลือก Update now เพื่อทำโปรแกรมรู้จักไวรัสที่เกิดขึ้นมาใหม่ โดยขั้นตอนนี้ควรทำการUpdateเป็นประจำทุกอาทิตย์ เพื่อให้โปรแกรมรู้จักไวรัสใหม่ๆ อยู่เสมอ



12. จากนั้นเริ่มทำการตรวจสอบหาไวรัสที่ทำงานและซ่อนตัวอยู่ในเครื่องคอมพิวเตอร์ โดยเลือกคำสั่ง Scan now เพื่อเริ่มขั้นตอนการค้นหาและทำลายไวรัสในเครื่องคอมพิวเตอร์

เมื่อเริ่มคำสั่ง Scan now แล้วปล่อยให้โปรแกรมทำการ Scan ไวรัสในเครื่องจน Scan is running ครบ 100 %



บทที่ 6

รู้จัก และป้องกันคอมพิวเตอร์จาก Spyware

6.1 รู้จัก Spyware

Spyware คือ โปรแกรมคอมพิวเตอร์ที่แอบทำการติดตั้งลงบนเครื่องคอมพิวเตอร์โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่ยินยอม โปรแกรมนี้จะเข้าขัดขวางการทำงานหรือทำให้คอมพิวเตอร์ทำงานผิดปกติไป ซึ่งการระบาดของ spyware ทำให้มีผู้สร้างโปรแกรม Anti-spyware ขึ้นมา ซึ่งผู้ใช้คอมพิวเตอร์ควรจะติดตั้งโปรแกรมนี้ลงในคอมพิวเตอร์ของตน

6.2 ประวัติความเป็นมาของ Spyware

มีการใช้คำว่า spyware ครั้งแรกในวันที่ 16 ตุลาคม ค.ศ.1995 ในหนังสือ Usenet ซึ่งกล่าวถึง spyware ตัวแรก ที่ถูกสร้างขึ้นมา โดยมีวัตถุประสงค์เพื่อเป็นการจารกรรมข้อมูล

ในต้นปีค.ศ. 2000 ผู้ก่อตั้ง Zone Labs ที่ชื่อ Gregor Freund ได้ตีพิมพ์โดยใช้คำนี้เพื่อหมายถึง ZoneAlarm Personal Firewall และตั้งแต่นั้นมาก็เริ่มมีการใช้คำนี้กันอย่างแพร่หลาย ในปีค.ศ.2005 AOL และ National Cyber-Security Alliance ได้ทำการสำรวจผู้ใช้คอมพิวเตอร์และพบว่า

61% ของผู้ใช้คอมพิวเตอร์มี spyware ในเครื่องคอมพิวเตอร์ของตน

92% ของผู้ใช้คอมผิวเตอร์ที่มี spyware ในเครื่องคอมพิวเตอร์ของตน ไม่ทราบว่ามี spyware อยู่

และ 91% ของผู้ใช้คอมผิวเตอร์ที่มี spyware ในเครื่อง ไม่ได้ยินยอมให้มีการติดตั้ง spyware ลงในเครื่องของตน

ในปีค.ศ.2006 spyware กลายเป็น Malware ที่มีการระบาดมากเป็นอันดับต้นๆ โดยมุ่งโจมตีระบบปฏิบัติการของ Microsoft Windows โดยมี IE เป็นตัวช่วยในการแพร่กระจาย spyware เนื่องจากมีช่องโหว่ของ IE ในส่วนของ ActiveX ซึ่งพบว่า 9 ใน 10 ของผู้ใช้คอมพิวเตอร์มี spyware อยู่ในเครื่องคอมพิวเตอร์

6.3 วิธีที่ Spyware เข้าสู่เครื่องคอมพิวเตอร์

Spyware นั้นไม่ได้ใช้วิธีการเดียวกับ virus และ worm ในการเข้าสู่เครื่องคอมพิวเตอร์ กล่าวคือ โดยปกติแล้วเครื่องคอมพิวเตอร์ที่ติด Spyware จะไม่สามารถแพร่กระจาย Spyware ที่มีในเครื่อง ไปยังเครื่องคอมพิวเตอร์เครื่องอื่นได้ ดังนั้น Spyware จึงอาศัยการหลอกล่อหรือทำให้ผู้ใช้คอมพิวเตอร์เข้าใจผิด หรืออาจจะเข้าสู่เครื่องคอมพิวเตอร์ โดยอาศัยช่องโหว่ของระบบ

Spyware ส่วนใหญ่จะถูกติดตั้งลงในเครื่องคอมพิวเตอร์โดยที่ผู้ใช้ไม่รู้ตัว แต่ผู้ใช้ส่วน

ใหญ่เมื่อทราบว่าเครื่องคอมพิวเตอร์ของตนมี spyware อยู่ในระบบ มักจะใช้โปรแกรมช่วยในการขัดขวางการทำงานของ Spyware ซึ่ง Spyware จะทำการขัดขวางขั้นตอนการติดตั้งโปรแกรมนั้นๆ นอกจากนี้ Spyware ยังมีวิธีการหลอกล่อผู้ใช้คอมพิวเตอร์ โดยใช้โปรแกรมที่น่าสนใจเป็นตัวดึงดูดให้ผู้ใช้คอมพิวเตอร์ดาวน์โหลดโปรแกรม แต่ในความเป็นจริงโปรแกรมนั้นมี Spyware แนบมาด้วย และติดตั้งโปรแกรม Spyware ลงในเครื่องของตน เช่น โปรแกรม Anti-spyware ปลอม หรือที่เรียกว่า "rougue"

การติด Spyware นั้น บางครั้งอาจเกิดจากการที่ผู้ใช้คอมพิวเตอร์เข้า websites ที่ตนเองไม่รู้จัก คลิ๊กลิ้งค์ใน website เหล่านั้น ทำให้มีหน้าต่างโฆษณาปรากฏขึ้นมาบนหน้าจอ ซึ่งมีลักษณะคล้าย dialog box ของ Windows และอาจมีปุ่มให้เลือกกด แต่ไม่ว่าผู้ใช้คอมพิวเตอร์จะกดปุ่มใดก็ตาม Spyware ก็จะสามารถถูกดาวน์โหลดเข้ามายังเครื่องคอมพิวเตอร์นั้นได้ ดังนั้นผู้ใช้คอมพิวเตอร์จึงไม่ควรคลิ๊กลิ้งค์ใดๆ ก็ตาม ที่ไม่มีความน่าเชื่อถือหรือไม่แน่ใจว่าปลอดภัยหรือไม่ อันที่จริงโปรแกรม IE นั้นได้ถูกออกแบบมาเพื่อป้องกันปัญหาที่เกิดจากจุดนี้แล้ว คือ เมื่อผู้ใช้คอมพิวเตอร์เปิด Website จะไม่มีการดาวน์โหลดโดยอัตโนมัติ ผู้ใช้คอมพิวเตอร์จะต้องเป็นผู้ออกคำสั่งว่าต้องการจะดาวน์โหลดหรือไม่ ในปัจจุบันโปรแกรม IE ได้ ทำการพัฒนาโปรแกรมเรื่อยๆ เพื่อป้องกันปัญหาในจุดนี้ และนอกจากนี้ Spyware อาจจะอาศัย virus หรือ worm ช่วยในการติดตั้งตัวมันลงไปในระบบก็ได้

6.4 พฤติกรรมของ Spyware

Spyware มักจะไม่อยู่เป็นโปรแกรมเดี่ยวๆ ในคอมพิวเตอร์ (มันสามารถแพร่กระจายไปยังส่วนต่างๆได้อย่างรวดเร็ว) ผู้ใช้คอมพิวเตอร์ส่วนใหญ่จะสังเกตเห็นอาการของคอมพิวเตอร์ที่มีประสิทธิภาพในการทำงานลดลง Spyware จะรบกวนคอมพิวเตอร์โดยการทำให้ CPU ทำงานผิดปกติไปจากเดิม เนื่องจากมีการใช้ทรัพยากรหน่วยความจำของเครื่องมากขึ้น และทำให้การเชื่อมต่อกับเครือข่ายล้มเหลว ซึ่งสาเหตุที่กล่าวมานี้ เป็นสาเหตุที่ทำให้คอมพิวเตอร์ทำงานช้าลง Spyware จะแทรกแซงการทำงานของ networking software ซึ่งทำให้ยากต่อการเชื่อมต่ออินเตอร์เน็ต

Spyware มักจะไม่ปรากฏตัวให้ผู้ใช้คอมพิวเตอร์ทราบว่ามีการติด spyware แล้ว ซึ่งผู้ใช้คอมพิวเตอร์ต้องสันนิษฐานหาสาเหตุเอาเองว่า ที่เครื่องคอมพิวเตอร์ของตนมีความผิดปกติเกิดขึ้นนั้น เกิดจาก hardware ผิดปกติ, ปัญหาระหว่างการติดตั้ง Windows หรือเกิดจากไวรัสเป็นต้นเหตุ โดยการแก้ปัญหานั้น ผู้ใช้คอมพิวเตอร์บางคนจะพึ่งพาช่างเทคนิค หรืออาจจะถึงขั้นซื้อคอมพิวเตอร์ใหม่ เนื่องจากเครื่องคอมพิวเตอรีนั้นทำงานได้ช้าเกินไป การติดไวรัสนั้นมักแก้ไขได้โดยการลบและติดตั้งโปรแกรมใหม่ทั้งหมด เพื่อให้เครื่องคอมพิวเตอร์กลับมาทำงานได้ตามปกติอีกครั้ง

ผลกระทบที่เกิดจาก spyware อาจแสดงอาการออกมา โดยผู้ใช้คอมพิวเตอร์สามารถ

สังเกตเองได้ เช่น คอมพิวเตอร์ทำงานได้ช้ากว่าปกติมาก เพราะมีโปรแกรมกำลังงานอยู่บนคอมพิวเตอร์หลายโปรแกรมพร้อมๆ กัน ยิ่งกว่านั้น Spyware บางประเภทจะปิดการทำงานของ firewall และโปรแกรม anti-virus และปรับระบบรักษาความปลอดภัยของ browser ด้วย ดังนั้นจะทำให้มีโอกาสที่จะติดไวรัสต่างๆ มากขึ้น เสมือนกับว่าเป็นโรคขาดภูมิคุ้มกันนั่นเอง. Spyware บางประเภทจะปิดการทำงานหรือลบโปรแกรม spyware คู่แข่งออก เพราะรบกวนการทำงานของตัว Spyware เอง ซึ่งภายหลังผู้สร้างโปรแกรม spyware ทั้งสองค่ายได้ตั้งข้อตกลงว่าจะไม่ปิดการทำงานของกันและกัน

6.5 แนะนำโปรแกรมแอนติ้สปายแวร์ (anti-spyware)

1. Spybot Search & Destroy: เป็นหนึ่งในโปรแกรมป้องกัน และกำจัดสปายแวร์ฟรี ที่ได้ครับความนิยมอย่างแพร่หลาย ซึ่งเครื่องมือตัวนี้ สามารถสแกน ค้นหาสปายแวร์ แอดแวร์ ไฮแจ๊คเกอร์ และโปรแกรมมัลแวร์ทั้ง หลาย อีกทั้งยังสามารถเคลียร์ ทำความสะอาด tracking ต่างๆ ได้ ทั้งนี้ สามารถรองรับวินโดวส์วิสต้า อีกทั้งยังสนับสนุนการใช้งานได้หลายภาษาอีกด้วย

2. SpywareBlaster: เป็นเครื่องมือฟรี สำหรับป้องกันเครื่องของคุณ จากสปายแวร์ แอดแวร์ เบราเซอร์ไฮแจ๊คเกอร์ และทรีทต่างๆที่เกิดขึ้นอย่างมากมายในอินเตอร์เน็ตทุกวันนี้ ทั้งนี้สามารถป้องกันการติดตั้งพวก ActiveX Object ต่างๆของสปายแวร์ได้อีกด้วย

3. SpywareGuard: เป็นอีกโปรแกรมที่ช่วยป้องกันคุณจากสปายแวร์แบบ เรียลไทม์ ซึ่งเป็นเครื่องมือที่ทำงานร่วมกับ SpwareBlaster ได้อย่างมีประสิทธิภาพ ซึ่งสามารถรีลไทม์ป้องกัน spayware และ bowser hijacking ในขณะที่เราดาวน์โหลดโปรแกรมหรือท่องอินเตอร์เน็ตได้อีกด้วย

4. Spyware Terminator: เป็นฟรีโปรแกรมป้องกัน สปายแวร์ที่สามารถทำงานได้แบบเรียลไทม์ 100% สามารถกำจัด ลบ สปายแวร์ แอดแวร์ โทรจันต่างๆ โปรแกรมจำพวกคีย์ล็อกเกอร์ ง่ายต่อการใช้งาน สามารถตั้ง schedule ในการรันสแกนได้อัตโนมัติด้วย

5. Windows Defender: เป็นฟรีโปรแกรมป้องกันสปายแวร์จากทางค่ายไมโครซอร์ฟ ที่ช่วยป้องกันเครื่องคอมพิวเตอร์ของคุณจาก ป๊อปอัพ แบนเนอร์ต่างๆ สปายแวร์ที่ ทำให้การทำงานของเครื่องมีประสิทธิภาพต่ำ ซีเคียวริตี้ทรีทต่างๆ สามารทำงานได้ในโหมดเรียลไทม์ ทั้งนี้ ก่อนทำการดาวน์โหลดจะมีการเช็ค Windows Genuine ด้วย ถ้าไม่สามารถดาวน์โหลดได้ สามารถดูวิธีได้ที่บทความ มาทำ Windows XP ของคุณให้เป็น Window$ Genuine ด้วย Trick ง่ายๆ

6. Ad Aware: เป็นเครื่องมือฟรีป้องกันและกำจัดสปายแวร์ แอดแวร์ มัลแวร์ โทรจัน อินเตอร์เน็ตแทรกกิ้งต่างๆ ซึ่งเป็นโปรแกรมที่ได้รับความนิยมกันอย่างแพร่หลายใน ทั่วโลกอีกตัวหนึ่ง ซึ่งสามารถป้องกันการขโมยข้อมูลธนาคาร รหัสผ่าน เลขที่บัตรเครดิตการ์ด ทั้งนี้ในเวอร์ชั่นฟรีนี้ จะไม่มีโหมดเรียลไทม์โปรเทคชั่น

7. WinPooch: เรียกได้ว่าเป็นโปรแกรมสุนัขเฝ้าวินโดวส์เลยก็ว่าได้ ซึ่งเป็นโปรแกรม

ฟรีทั้งซอร์สโค้ดและตัวติดตั้งใช้งาน ที่ป้องกันได้ทั้งสปายแวร์และโทรจัน สามารถทำการสแกนได้ในโหมดเรียลไทม์ด้วย สามารถทำงานได้ควบกับโปรแกรมป้องกันไวรัส Clamwin

8. Malwarebytes' Anti-Malware: มัลแวร์ และสปายแวร์ที่ดังมากอีกตัวหนึ่งในขณะนี้ ด้วยยอดการดาวน์โหลดกว่า 2 ล้าน ดาวน์โหลดจากเวป download.com ซึ่งสามารถหยุดหรือกำจัดมัลแวร์นั้นๆ ก่อนที่มันจะเริ่มทำงานได้ อีกทั้งยังสามารถค้นหา ป้องกันและกำจัดมัลแวร์ ที่โปรแรกมตรวจจับไวรัส หรือแอนติไวรัส ไม่สามารถตรวจจับและกำจัดได้ นอกจากนี้ยังสามารถทำงานในโหมดเรียลไทม์สแกนได้ ทำให้อุ่นใจได้ ว่าเครื่องของคุณจะปลอดภัยจากการคุกคามของเหล่าสปายแ วร์ มัลแวร์ โทรจันได้

9. SUPERAntiSpyware: ตัวสุดท้ายกำลังเป็นที่นิยมใช้กันอย่างมากในขณะนี้ SUPERAntiSpyware เป็นโปรแกรมฟรี เอาไว้สำหรับ remove และ กำจัดสปายแวร์ มัลแวร์และโทรจัน ซึ่งเจ้าโปรแกรม SUPERAntiSpyware นี้ สามารถทำการ remove และ กำจัดสปายแวร์ มัลแวร์และโทรจันได้มากกว่า 1 ล้านตัวเลยทีเดียว ยกตัวอย่างเช่น VirusRay, AntiVirGear,VirusProtectPro, DriveCleaner, SmitFraud, Vundo, WinFixer, SpyAxe, SpyFalcon, WinAntiVirus, AntiVermins, AntiSpyGolden และอื่นๆอีกมากมายโดยโปรแกรม SUPERAntiSpyware นี้ สามารถทำการ remove และ กำจัดสปายแวร์ มัลแวร์และโทรจันเหล่านั้น ได้อย่างง่ายดาย

ซึ่งการการจัดการความรู้เล่มนี้ขอเสนอการใช้งานโปรแกรมในการป้องกัน Spyware ที่แนะนำกันเป็นตัวสุดท้ายคือ SUPERAntiSpyware เนื่องจากมีคุณสมบัติและความสามารถที่โดดเด่นดังนี้ คือ

1. สามารถเลือกสแกน กำจัดสปายแวร์ มัลแวร์และโทรจัน ได้ทั้ง 3 โหมด คือ Quick, Complete และ Custom Scan ซึ่งสามารถสแกน ค้นหา และกำจัดสปายแวร์ มัลแวร์และโทรจัน ได้ทั้งใน Hard Drives, Removable Drives, Memory, Registry และโฟลเดอร์อื่นๆที่ต้องการ
2. สามารถทำการค้นหา ตรวจจับ และกำจัด Spyware, Adware, Malware, Trojans, Dialers, Worms, KeyLoggers, HiJackers, Parasites, Rootkits และอื่นๆ
3. ตัวโปรแกรมน้อย ไม่กินทรัพยากรระบบ ซึ่งไม่ทำให้เครื่องอืด ช้า เหมือนกับโปรแกรมในกลุ่ม ประเภทเดียวกัน
4. สามารถทำการซ่อมแซมค่าต่างๆของระบบได้ เช่น ค่า Internet Setting, Desktop,

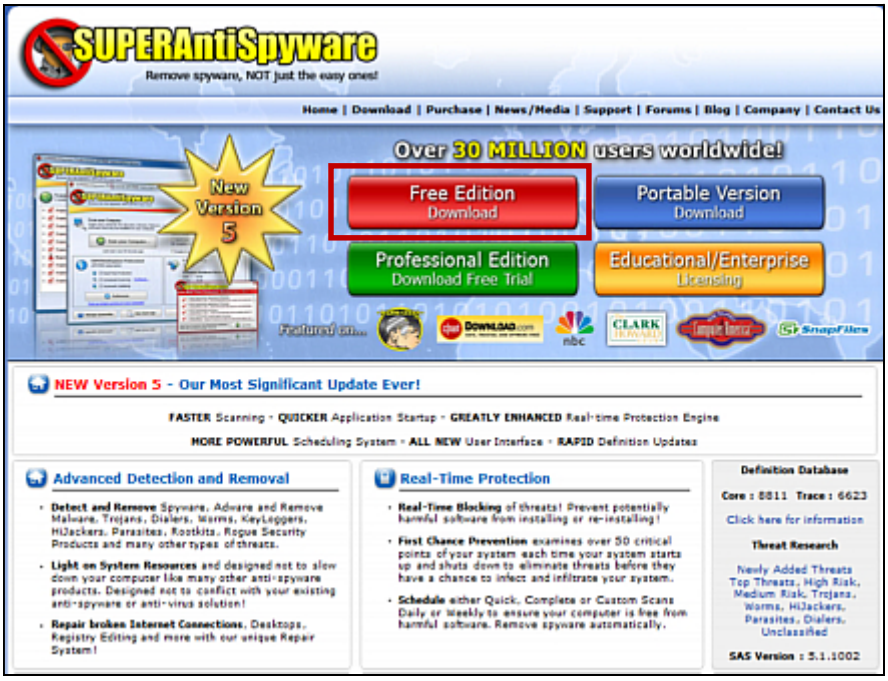
Registry ต่างๆ

5. เป็นพันธมิตรกับโปรแกรมในกลุ่ม ประเภทเดียวกัน กล่าวคือ สามารถติดตั้งร่วมกับโปรแกรมกำจัดสปายแวร์ มัลแวร์และโทรจันอื่นๆได้

6. มี Context Menu(เมนูคลิกเม้าส์ขวา นั่นเอง) ทำให้สะดวกและง่ายต่อการสแกนไดรว์ ไฟล์หรือโฟลเดอร์ใดๆ

6.6 วิธีใช้งานโปรแกรม SUPERAntiSpyware

1. ดาวน์โหลดและติดตั้งโปรแกรม SuperAntispyware ซึ่งสามารถดาวน์โหลดตามที่อยู่ www.superantispyware.com โดยให้ทำการเลือก Download Version Free Edition ดังภาพ

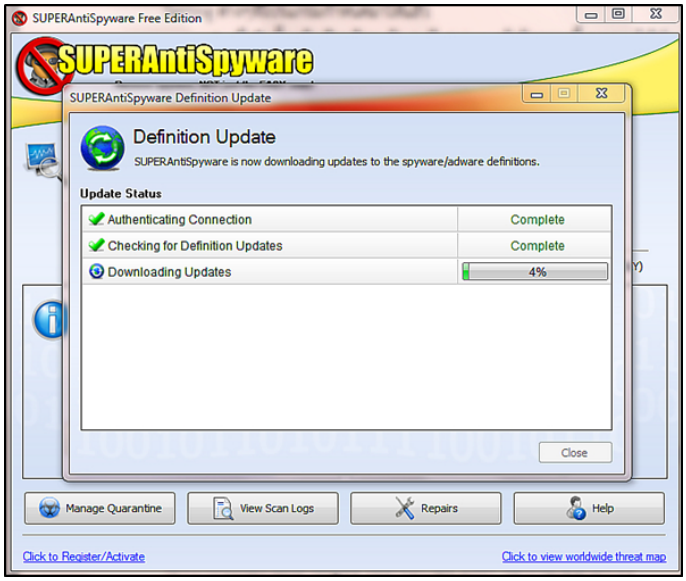


2. เมื่อดาวน์โหลดเสร็จเรียบร้อยแล้ว ให้ทำการปิดโปรแกรมต่างๆออกให้หมด จากนั้นทำการติดตั้งโปรแกรม SuperAntispyware โดยดับเบิ้ลคลิกที่ไฟล์ SUPERAntiSpyware.exe และทำการขั้นตอน คำแนะนำ คำสั่งการติดตั้งอย่างเคร่งครัด และห้ามทำการเปลี่ยนค่า Setting ต่างๆที่โปรแกรมกำหนดมาให้แล้ว

3. เมื่อติดตั้งเสร็จเรียบร้อยแล้ว จะมี dialog แจ้งข้อความขึ้นมาถามให้ทำการอัพเดท

ให้คลิกที่ปุ่ม Yes เพื่อทำการอัพเดทโปรแกรม

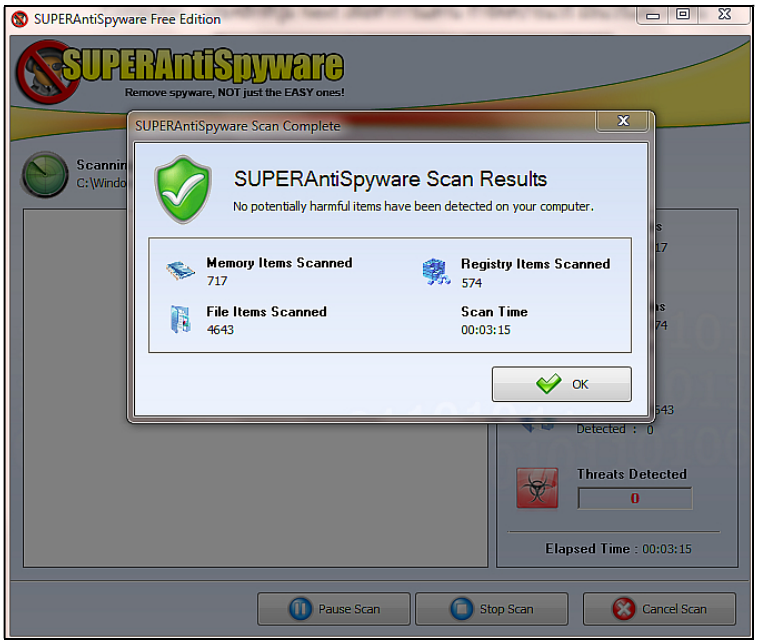
4. และเมื่อโปรแกรม SUPERAntiSpyware ทำการอัพเดทตัวเองเสร็จเรียบร้อยแล้ว ให้คลิกที่ปุ่ม Finish เพื่อสิ้นสุดขั้นตอนการติดตั้ง



5. จากนั้นก็เรียกใช้งานโปรแกรมตามปกติ โดยเมื่อจะสแกนให้คลิกที่ปุ่ม Scan your

Computer... และคลิกที่ปุ่ม Next เพื่อทำการสแกน กำจัดสปายแวร์ มัลแวร์และโทรจัน

6. และเมื่อโปรแกรมทำการสแกนเสร็จเรียบร้อย ก็จะแสดงหน้าต่าง dialog แสดงผลของการสแกนให้ดู ให้คลิกที่ปุ่ม OK



7. ในกรณีที่โปรแกรมตรวจพบ Spyware โปรแกรมจะแสดงรายการ Spyware ที่

ตรวจพบ หลังจากนั้นคลิกปุ่ม Next เพื่อทำการ Remove กำจัดสปายแวร์ มัลแวร์และโทรจันที่ตรวจจับได้

7. ถ้าโปรแกรม SUPERAntiSpyware มีข้อความ dialog ขึ้นมาถาม ให้เราทำการ Reboot เครื่อง โดยการคลิกที่ปุ่ม Yes เพื่อตกลง Reboot เครื่องใหม่อีกครั้ง

การใช้โปรแกรมป้องกัน Spyware SUPERAntiSpyware ที่ได้นำมาแนะนำนี้ เป็นเพียงทางเลือกหนึ่งในหลายๆ โปรแกรมที่เป็นทางเลือกในการป้องกันภัยคุกคาม Spyware ที่มีให้เลือกใช้ทั้ง Freeware และ Shareware ให้ทดลองใช้และถ้าหากว่าผู้ใช้รู้สึกพอใจในประสิทธิภาพก็อาจจะต้องจ่ายเงินซื้อ Software Anti-spyware ซึ่งมีราคาค่อนข้างสูง โดยแต่ละค่ายต่างมีข้อดี และข้อด้อยแตกต่างกันไปขึ้นอยู่กับความต้องการ และความชอบส่วนบุคคลของผู้ใช้และงบประมาณเป็นสำคัญ และในบางครั้งการจ่ายเงินเพื่อซื้อ Software Anti-Spyware หลายตัวก็ใช่ว่าจะได้มาตรฐานความปลอดภัยที่ที่ดีกว่า Free Anti-Spyware บางตัวโดยเฉพาะตัวที่นำมาแนะนำในการจัดการความรู้ฉบับนี้

เอกสารอ้างอิง

กิตติพงศ์ กลิ่นจันทร์. (2552). วิธีป้องกันตนเองให้ปลอดภัยจากไวรัสคอมพิวเตอร์. วันที่ค้นหาข้อมูล 2 มิถุนายน 2555, จากฟิสิกส์ราชมงคล 5 เว็บไซต์ :http://www.neutron.rmutphsics.com/news/index.php?option=com_content&task=view&id=1128&ltemid=3&Limit=1&limitstart=1

สัญญา คล่องในวัย. (2553). การป้องกันไวรัสในองค์กร. วันที่ค้นหาข้อมูล 2 มิถุนายน 2555, จากมหาวิทยาลัยขอนแก่น เว็ปไซต์ : http://std.kku.ac.th/4830503638/virus/12.%2520virus.doc

สุทธิพันธ์ ภัสสร. (2554). รู้จักกับ ฮาร์ดเดนนิง (Hardening) : ปกป้องความปลอดภัยให้กับคอมพิวเตอร์แบบง่าย ๆ ค่าใช้จ่ายต่ำ และทำได้เอง. วันที่ค้นหาข้อมูล 2 มิถนายน 2555, จากเว็บไซต์ : http://mvpskill.com/blogs/kb/archive/2011/03/17/hardening.aspx

มหาวิทยาลัยอีสเทิร์นเอเชีย. (2554). Lesson11ไวรัสคอมพิวเตอร์. วันที่ค้นหาข้อมูล 4 มิถุนายน 2555, จากเว็บไซต์ : http://course.eau.ac.th/course/Download/0000713/Lesson11

http://www.no-poor.com. (2550). ภัยคุกคามและการรักษาความปลอดภัยบนระบบคอมพิวเตอร์. วันที่ค้นหาข้อมูล 8 มิถุนายน 2555, จากเว็บไซต์ : http://www.nopoor.com/inttotoComandcomapp/chapter7-comapp.html

การจัดการความรู้ ประจำปี 2555

สำนักงานทรัพยากรน้ำภาค 10 กรมทรัพยากรน้ำ

คณะที่ปรึกษา

1.	นายสัญญา	มัณฑางกูร	ผู้อำนวยการสำนักงานทรัพยากรน้ำภาค 10
2.	นายธีระสาร	เขตอนันต์	ผู้อำนวยการส่วนพัฒนาและฟื้นฟูแหล่งน้ำ
3.	นายไพศาส	ศรีเกตุ	ผู้อำนวยการส่วนประสานและบริหารจัดการลุ่มน้ำตาปี
4.	นายสุชาติ	เกตุแก้ว	ผู้อำนวยการส่วนวิชาการ
5.	นางจารี	เลิศปรัชญานนท์	ผู้อำนวยการส่วนอำนวยการ
6.	นายภาณุพล	ภิโสรมย์	ผู้อำนวยการส่วนประสานและบริหารจัดการลุ่มน้ำภาคใต้ฝั่งตะวันออกส่วนที่ 1
7.	นายชาญวุฒิ	สันติราชัย	ผู้อำนวยการส่วนประสานและบริหารจัดการลุ่มน้ำภาคใต้ฝั่งตะวันตกส่วนที่ 1
8.	นายวิเชียร	ไข่มุกข์	ผู้อำนวยการส่วนบริหารจัดการน้ำ
9.	นายวินัย	กิติพงษ์วัฒนา	ผู้อำนวยการส่วนอุทกวิทยา

คณะผู้จัดทำ

1.	นายอนนท์	รื่นพานิช	ประธานคณะทำงานการจัดการความรู้
2.	นายดุลยธรรม	ทวิชสังข์	วิศวกรโยธาชำนาญงาน
3.	นายศักดิ์ชัย	ตันติวิวัฒน์	นายช่างโยธาอาวุโส
4.	นายนิกร	ช่วยชาติ	นายช่างโยธาอาวุโส
5.	นายสมศักดิ์	วัจนสาร	นายช่างโยธาชำนาญงาน
6.	นายธเนศ	การพร้อม	นายช่างโยธาชำนาญงาน
7.	นางณปภัช	โพธิ์แก้ว	นักวิเคราะห์นโยบายและแผนชำนาญการ
8.	นางวัฒนา	หนูแก้ว	นักวิเคราะห์นโยบายและแผนชำนาญการ
9.	นางพรรณรัตน์	ยิ้มประเสริฐ	นักวิเคราะห์นโยบายและแผนชำนาญการ
10.	นายวิเชียร	ทองบัว	นักวิเคราะห์นโยบายและแผนชำนาญการ
11.	นายธงไทย	สมเกียรติกุล	นักวิเคราะห์นโยบายและแผนปฏิบัติการ