คู่มือการปฏิบัติงาน
การป้องกันไวรัสคอมพิวเตอร์

<u>บทนำ</u>

ในปัจจุบันการนำเทคโนโลยีคอมพิวเตอร์มาใช้ในการดำเนินกิจกรรมในชีวิตประจำวัน ทั้งในการทำงาน การเรียน การพักผ่อน ตลอดจนการติดต่อสื่อสาร เป็นไปอย่างแพร่หลายไปทั่วทุกผืนดินของโลกไปจนถึงอวกาศ แต่อย่างไรก็ตามในปัจจุบันมีภัยมืดที่คุกคามโลกไซเบอร์ซึ่งมีความน่ากลัวเป็นอันดับต้นๆ ก็คงหนีไม่พ้น “ไวรัสคอมพิวเตอร์” ผู้ใช้งานคอมพิวเตอร์ทั่วไปต่างหวาดวิตกและเกรงว่าเครื่องคอมพิวเตอร์ที่ใช้งานอยู่นั้นจะติดไวรัสคอมพิวเตอร์จอมวายร้าย แล้วพอจะมีวิธีใดบ้างไหมที่จะช่วยให้รอดพ้นจากไวรัสคอมพิวเตอร์นี้ คู่มือนี้จะกล่าวถึงเรื่องต่าง ๆ ที่เกี่ยวข้องกับไวรัสคอมพิวเตอร์ วิธีการต่างๆ ที่จะใช้ป้องกันตัวเองให้ปลอดภัยจากไวรัสคอมพิวเตอร์ เริ่มต้นด้วยการจัดการภายในเครื่องเช่น การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ตลอดจนการใช้งานโปรแกรมที่มีการเชื่อมต่อไปยังอินเทอร์เน็ต เช่นโปรแกรมเว็บเบราเซอร์ โปรแกรมที่ใช้อ่านอี-เมล์ เป็นต้น

<u>ความหมายของไวรัสคอมพิวเตอร์</u>

ไวรัสคอมพิวเตอร์ คือ โปรแกรมที่มีลักษณะการทำงานเหมือนกับโปรแกรมทั่ว ๆ ไปแต่จะแตกต่างกันตรงที่โปรแกรมอื่นๆนั้นจะก่อให้เกิดประโยชน์ต่อมนุษย์ ส่วนไวรัสคอมพิวเตอร์จะมีวัตถุประสงค์เพื่อทำลายข้อมูลและโปรแกรมอื่น ๆ เป็นโปรแกรมคอมพิวเตอร์ที่ถูกสร้างขึ้นมาจากภาษาระดับล่างโดยมีการออกแบบมาทางลบคือ ให้มีคุณสมบัตินำตัวเองไปติดปะปนกับ โปรแกรมอื่นที่อยู่ในระบบ ได้รับการเขียนขึ้นมาเพื่อให้จัดการกับตัวมันเอง โดยมีลักษณะเลียนแบบสิ่งมีชีวิต คือ เจริญเติบโตเองได้ ขยายและแพร่กระจายเองได้ สามารถอยู่รอดได้ มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในระบบคอมพิวเตอร์ได้และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่น ๆ เขียนขึ้นมาเพื่อขัดขวางการทำงานของคอมพิวเตอร์ เช่น ขัดขวางการเข้าถึงข้อมูลในหน่วยความจำ ขัดขวางการอ่านแฟ้มข้อมูลจากฮาร์ดดิสก์ ขัดขวางการใช้งานอุปกรณ์ต่อพ่วง เช่น พรินเตอร์ สแกนเนอร์ ทำให้เสมือนว่าใช้งานกับคอมพิวเตอร์ไม่ได้ จนกระทั่งทำลายแฟ้มข้อมูล หรือทำให้คอมพิวเตอร์ทำงานผิดปกติไปจากเดิม

ไวรัสคอมพิวเตอร์เข้าไปอยู่ในระบบคอมพิวเตอร์ได้ โดยผ่านทางแผ่นฟลอปปีดิสก์ เครือข่ายคอมพิวเตอร์ ซึ่งอาจเกิดจากการนำเอาดิสก์ที่ติดไวรัสคอมพิวเตอร์จากเครื่องหนึ่งไปใช้อีก

เครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือระบบสื่อสารข้อมูลไวรัสคอมพิวเตอร์ก็อาจแพร่ระบาดได้เช่นกัน การที่คอมพิวเตอร์ใดติดไวรัสคอมพิวเตอร์ หมายถึงว่าไวรัสคอมพิวเตอร์ได้เข้าไปผังตัวอยู่ในหน่วยความจำ คอมพิวเตอร์ เรียบร้อยแล้ว เนื่องจากไวรัสคอมพิวเตอร์ก็เป็นแค่โปรแกรม ๆ หนึ่ง การที่ไวรัสคอมพิวเตอร์จะเข้าไปอยู่ ในหน่วยความจำได้นั้นจะต้องมีการถูกเรียกให้ทำงานได้นั้นยังขึ้นอยู่กับประเภทของไวรัสคอมพิวเตอร์ แต่ละตัวปกติผู้ใช้มักจะไม่รู้ตัวว่าได้ทำการปลุกคอมพิวเตอร์ไวรัสคอมพิวเตอร์ขึ้นมาทำงานแล้ว

จุดประสงค์ของการทำงานของไวรัสแต่ละตัวขึ้นอยู่กับตัวผู้เขียนโปรแกรมไวรัสนั้น เช่น อาจสร้างไวรัสให้ไปทำลายโปรแกรมหรือข้อมูลอื่น ๆ ที่อยู่ในเครื่องคอมพิวเตอร์ หรือ แสดงข้อความวิ่งไปมาบน หน้าจอ รบกวนการทำงานของคอมพิวเตอร์ หรือทำลายแฟ้มข้อมูลและโปรแกรมต่างๆ ในระบบคอมพิวเตอร์ และหลบซ่อนตัวเพื่อติดต่อไปยังแผ่นดิสก์หรือฮาร์ดดิสก์อื่นๆ ได้เมื่อถึงเวลาที่เหมาะสม การที่ไวรัสคอมพิวเตอร์ ทำงานได้ด้วยเงื่อนไขลักษณะใดลักษณะหนึ่งหลายลักษณะ จึงทำให้ผู้ใช้ไม่รู้ว่าเครื่องคอมพิวเตอร์ของตนติดไวรัสคอมพิวเตอร์หรือไม่ พอเปิดเครื่องใช้ก็อาจพบว่าระบบคอมพิวเตอร์ของตนถูกไวรัสคอมพิวเตอร์ทำลายเสียแล้ว ไวรัสคอมพิวเตอร์บางตัวไม่เพียงทำลาย ลบ ล้าง ย้ายข้อมูลของเรา โดยไม่ได้รับอนุญาตเท่านั้น แต่ยังสามารถทำลายโปรแกรมอื่น ๆได้อีกด้วยโดยสังเกตได้จากการที่หน้าจอแสดงผลแปลก ๆ ไวรัสคอมพิวเตอร์จะทำงานเฉพาะในหน่วยความจำของระบบเท่านั้น และจะอยู่จนกว่าจะมีการปิดเครื่อง เมื่อเปิดเครื่องไวรัสคอมพิวเตอร์ก็จะถูกกำจัดออกจากหน่วยความจำด้วยเช่นกัน แต่นั่นไม่ได้หมายความว่าได้กำจัดไวรัสคอมพิวเตอร์ออกจากระบบ เมื่อมีการใช้คอมพิวเตอร์ในครั้งต่อไปไวรัสคอมพิวเตอร์ก็จะทำงานด้วย และมันจะทำการแพร่กระจายไปยังโปรแกรมอื่นๆ ด้วยก่อให้เกิดความเสียหายต่อข้อมูลที่อยู่ในดิสก์หรือฮาร์ดดิสก์ หรือเกิดการทำงานที่ผิดเพี้ยนไป หรือการทำงานที่ไม่พึงประสงค์ เช่น การลบไฟล์ที่อยู่ในฮาร์ดดิสก์ หรืออาจฟอร์แมตฮาร์ดดิสก์ เป็น

<u>กลุ่มของไวรัสคอมพิวเตอร์</u>

ในปัจจุบันไวรัสคอมพิวเตอร์มีอยู่หลายกลุ่มด้วยกัน โดยพิจารณาจากการทำงานหรือลักษณะการทำงาน โดยสามารถจัดเป็นกลุ่มได้ดังนี้

1. Macro Virus เป็นไวรัสคอมพิวเตอร์ที่เกิดขึ้นใหม่โดยถูกสร้างจากภาษาไมโครซอฟต์เวิร์ด (Word Basic) ซึ่งจะทำงานและแพร่กระจายไปถึงไฟล์ข้อมูลประเภทเอกสาร โดยเฉพาะโปรแกรม Microsoft Word ซึ่งตัวไวรัสคอมพิวเตอร์จะฝังตัวและเข้าไปทำลายแฟ้มนามสกุล .dot และ .doc ไวรัสคอมพิวเตอร์จะเข้าไปทำลายไฟล์ระบบของไมโครซอฟต์เวิร์ดทำให้เวลาพิมพ์รายงาน เครื่องจะเกิดอาการแฮงก์บ้างหรือเปิดไฟล์ไม่ได้บ้าง หรือเปิดไฟล์เอกสารได้แต่เป็นภาษาฮิ

ปบรูปมา ไวรัสคอมพิวเตอร์มาโครเวิร์ดเป็นไวรัสคอมพิวเตอร์ที่อันตรายพอสมควร ได้แก่ ไวรัสคอมพิวเตอร์ชื่อ Word_cab และไวรัสคอมพิวเตอร์ชื่อ Wont_Johnny ไวรัสประเภททำลายเฉพาะไฟล์ ไวรัสคอมพิวเตอร์ประเภทนี้เกาะติดไฟล์โปรแกรมไปเรื่อย ๆ และเมื่อพบไฟล์ที่ต้องการก็จะเริ่มทำงานไม่ว่าจะเป็นการแก้ไข การทำลาย การเคลื่อนย้าย เป็นไวรัสคอมพิวเตอร์ที่ร้ายแรงต่อเศรษฐกิจมากกว่าไวรัสคอมพิวเตอร์ประเภทอื่น ๆ กว่าจะพิสูจน์ได้ว่าติดไวรัสคอมพิวเตอร์แล้วข้อมูลที่สำคัญของผู้ใช้ก็อาจหายไปหมดแล้ว

2. Command Virus เป็นไวรัสคอมพิวเตอร์ทั่ว ๆ ไป ที่ไม่ได้หวังผลในการทำลายระบบหรือแฟ้มข้อมูลเป็นการทำให้เกิดความกลัว และสร้างความรำคาญให้กับผู้ใช้เครื่องคอมพิวเตอร์ ไวรัสคอมพิวเตอร์ประเภทนี้ง่ายต่อการตรวจสอบและการกำจัด ไวรัสคอมพิวเตอร์ที่เกาะตามไฟล์ส่วนมากจะเกาะติดไฟล์ที่มีสกุล .COM และ .EXE คือเมื่อมีการใช้งานโปรแกรม .COM .EXE ไวรัสคอมพิวเตอร์ประเภทนี้จะแยกตัวไปซ่อนอยู่ในหน่วยความจำ แล้วหาทางเกาะติดไฟล์ที่มีนามสกุลดังกล่าว ที่เก็บไว้ในแผ่นดิสก์

3. Program Virus ไวรัสคอมพิวเตอร์ประเภทนี้เป็นไวรัสคอมพิวเตอร์ประเภทที่สามารถแพร่กระจายได้เมื่อมีการเรียกใช้โปรแกรมที่มีไวรัสคอมพิวเตอร์ทำงานอยู่ และสามารถกระจายไปสู่โปรแกรมอื่นอย่างรวดเร็ว Program Viruses หรือ File Intector Viruses เป็นไวรัสคอมพิวเตอร์อีกประเภทหนึ่งที่จะติดอยู่กับโปรแกรม ซึ่งปกติก็คือ ไฟล์ที่มีนามสกุลเป็น COM หรือ EXE และบางไวรัสคอมพิวเตอร์สามารถเข้า ไปติดอยู่ในโปรแกรมที่มีนามสกุลเป็น sys และโปรแกรมประเภท Overlay Programsได้ด้วย โปรแกรมโอเวอร์เลย์ปกติจะเป็นไฟล์ที่มีนามสกุลที่ขึ้นต้นด้วย OV วิธีการที่ไวรัสคอมพิวเตอร์ใช้เพื่อที่จะ เข้าไปติดโปรแกรมมีอยู่สองวิธี คือ การแทรกตัวเองเข้าไปอยู่ในโปรแกรมผลก็คือหลังจากที่โปรแกรมนั้นติดไวรัสคอมพิวเตอร์ไปแล้ว ขนาดของโปรแกรมจะใหญ่ขึ้น หรืออาจมีการสำเนาตัวเองเข้าไปทับส่วนของโปรแกรมที่มีอยู่เดิมดังนั้นขนาดของโปรแกรมจะไม่เปลี่ยนและยากที่ จะซ่อมให้กลับเป็นดังเดิม การทำงานของไวรัสคอมพิวเตอร์ โดยทั่วไป คือ เมื่อมีการเรียกโปรแกรมที่ติดไวรัสคอมพิวเตอร์ ส่วนของไวรัสคอมพิวเตอร์จะทำงานก่อนและจะถือโอกาสนี้ฝังตัวเข้าไปอยู่ในหน่วยความจำทันทีแล้วจึงค่อยให้โปรแกรมนั้นทำงานตามปกติต่อไป เมื่อไวรัสคอมพิวเตอร์เข้าไปฝังตัวอยู่ในหน่วยความจำแล้วหลัง จากนี้ไปถ้ามีการเรียกโปรแกรมอื่น ๆ ขึ้นมาทำงานต่อ ตัวไวรัสคอมพิวเตอร์ก็จะสำเนาตัวเองเข้าไป ในโปรแกรมเหล่านี้ทันที เป็นการแพร่ระบาดต่อไป

วิธีการแพร่ระบาดของโปรแกรมไวรัสอีกแบบหนึ่งคือ เมื่อมีการเรียกโปรแกรมที่มีไวรัสคอมพิวเตอร์ติดอยู่ ตัวไวรัสคอมพิวเตอร์จะเข้าไปหาโปรแกรมอื่น ๆ ที่อยู่ในดิสก์เพื่อทำสำเนาตัวเองลงไปทันทีแล้วจึงค่อยให้โปรแกรมที่ถูกเรียก นั้นทำงานตามปกติต่อไป

4. boot Virus ไวรัสคอมพิวเตอร์ประเภทนี้เป็นไวรัสคอมพิวเตอร์ประเภทที่สามารถแฝงตัวเองและสามารถกระจายในส่วนที่เป็นพื้นที่เฉพาะของดิสก์ หรือฮาร์ดดิสก์ คือในส่วนของบูตเรก

คอร์ด (Boot Record) หรือมาสเตอร์บูตเรกคอร์ด (Master Boot Record) เป็นไวรัสคอมพิวเตอร์ที่ฝังตัวอยู่ตามบูตเซ็กเตอร์ของแผ่นดิสก์และตารางพาร์ติชัน ทุกครั้งที่ทำการเปิดเครื่อง ระบบจัดการของคอมพิวเตอร์จะอ่านข้อมูลจากบูตเซ็กเตอร์ และโหลดเข้าไปในหน่วยความจำก่อน ทำให้ไวรัสคอมพิวเตอร์ประเภทนี้ถูกโหลดไปหลบซ่อนในหน่วยความจำเพื่อรอจังหวะแพร่กระจายต่อไปยังแผ่นดิสก์ไวรัสคอมพิวเตอร์ประเภท ไม่สามารถทำลายได้โดยการเปิดเครื่องใหม่ เพราะมันจะเริ่มอยู่ในหน่วยความจำตั้งแต่เปิดเครื่อง และจะทำงานตลอดเวลานับจากนั้น

ในบูตเซกเตอร์จะมีโปรแกรมเล็ก ๆ ไว้ใช้ในการเรียกระบบ ปฏิบัติการขึ้นมาทำงานอีกทีหนึ่ง บูตเซกเตอร์ไวรัสจะเข้าไปแทนที่โปรแกรมดังกล่าว และไวรัส ประเภทนี้ถ้าไปติดอยู่ในฮาร์ดดิสก์ โดยทั่วไป จะเข้าไปอยู่บริเวณที่เรียกว่า Master Boot Sector หรือ Parition Table ของฮาร์ดดิสก์นั้น ถ้าบูตเซกเตอร์ของดิสก์ใดมีไวรัสคอมพิวเตอร์ประเภทนี้ติดอยู่ ทุก ๆ ครั้งที่บูตเครื่องขึ้นมาโดย พยายามเรียก ดอสจากดิสก์นี้ ตัวโปรแกรมไวรัสคอมพิวเตอร์จะทำงานก่อนและจะเข้าไปฝังตัวอยู่ใน หน่วยความจำเพื่อเตรียมพร้อมที่ จะทำงานตามที่ได้ถูกโปรแกรมมา แล้วตัวไวรัสคอมพิวเตอร์จึงค่อยไป เรียกดอสให้ขึ้นมาทำงานต่อไป ทำให้เหมือนไม่มีอะไรเกิดขึ้น

5. Stealth Virus เป็นไวรัสคอมพิวเตอร์ที่มีความสามารถในการหลบซ่อน สามารถซ่อนตัวเองจากการตรวจสอบได้ ทำให้ยากแก่การตรวจสอบ และการกำจัด สทีลต์ไวรัสเป็นไวรัสคอมพิวเตอร์ประเภทที่ไปติดโปรแกรมใดแล้วจะทำให้ขนาดของ โปรแกรมนั้นใหญ่ขึ้น ถ้าโปรแกรมไวรัสคอมพิวเตอร์นั้นเป็นแบบสทีลต์ไวรัส จะไม่สามารถตรวจดูขนาดที่แท้จริง ของโปรแกรมที่เพิ่มขึ้นได้ เนื่องจากตัว ไวรัสคอมพิวเตอร์จะเข้าไปควบคุมดอส เมื่อมีการใช้คำสั่ง DIR หรือโปรแกรมใดก็ตามเพื่อตรวจดูขนาดของโปรแกรม ดอสก็จะแสดงขนาดเหมือนเดิม ทุกอย่างราวกับว่าไม่มีอะไรเกิดขึ้น

6. Polymorphic Viruses เป็นไวรัสคอมพิวเตอร์ที่มีลักษณะการทำงานหลายรูปแบบในตัวเอง มีรูปแบบที่แตกต่างกันในการแพร่กระจายแต่ละครั้ง ทำให้ยากแก่การตรวจสอบ มีความสามารถในการแปรเปลี่ยนตัวเอง ได้เมื่อมีสร้างสำเนาตัวเองเกิดขึ้น ซึ่งอาจได้ถึงหลายร้อยรูปแบบ ผลก็คือ ทำให้ไวรัสคอมพิวเตอร์เหล่านี้ยากต่อการถูกตรวจจับ โดยโปรแกรมตรวจหาไวรัสคอมพิวเตอร์ที่ใช้วิธีการสแกนอย่างเดียว ไวรัสคอมพิวเตอร์ใหม่ ๆ ในปัจจุบันที่มีความสามารถนี้เริ่มมีจำนวนเพิ่มมากขึ้นเรื่อย ๆ

7. Mullipartite Viruses เป็นไวรัสคอมพิวเตอร์แบบผสมที่รวมเอาการทำงานของไวรัสคอมพิวเตอร์หลายๆ แบบไว้ในตัวของมัน สามารถแพร่กระจายได้ในไฟล์และในโปรแกรม

8. Trojan Horse เป็นโปรแกรมที่ถูกเขียนขึ้นมาให้ทำตัวเหมือนว่าเป็น โปรแกรมธรรมดาทั่ว ๆ ไป เพื่อหลอกล่อผู้ใช้ให้ทำการเรียกขึ้นมาทำงาน แต่เมื่อ ถูกเรียกขึ้นมาแล้ว ก็จะเริ่มทำลายตามที่โปรแกรมมาทันที ม้าโทรจันบางตัวถูกเขียนขึ้นมาใหม่ทั้ง ชุด โดยคนเขียนจะทำการตั้งชื่อโปรแกรมพร้อมชื่อรุ่นและคำอธิบายการใช้งานที่ดูสมจริง เพื่อหลอกให้คนที่จะเรียกใช้ตายใจ

จุดประสงค์ของคนเขียนม้าโทรจันอาจจะเช่นเดียวกับคนเขียนไวรัสคอมพิวเตอร์ คือ เข้าไปทำอันตรายต่อข้อมูลที่มีอยู่ในเครื่อง หรืออาจมีจุดประสงค์เพื่อที่จะล้วงเอาความลับของระบบคอมพิวเตอร์ ม้าโทรจันนี้อาจจะถือว่าไม่ใช่ไวรัสคอมพิวเตอร์ เพราะเป็นโปรแกรมที่ถูกเขียนขึ้นมาโดด ๆ และจะไม่มีการเข้าไปติดในโปรแกรมอื่นเพื่อสำเนาตัวเอง แต่จะใช้ความรู้เท่าไม่ถึงการณ์ของ ผู้ใช้เป็นตัวแพร่ระบาดซอฟต์แวร์ที่มีม้าโทรจันอยู่ในนั้นและนับว่าเป็นหนึ่งในประเภทของโปรแกรม ที่มีความอันตรายสูง เพราะยากที่จะตรวจสอบและสร้างขึ้นมาได้ง่าย ซึ่งอาจใช้แค่แบตซ์ไฟล์ก็สามารถโปรแกรมประเภทม้าโทรจันได้

<u>สาเหตุของการติดไวรัสคอมพิวเตอร์และการแพร่กระจายของไวรัสคอมพิวเตอร์</u>

การแพร่กระจายของไวรัสคอมพิวเตอร์ มีลักษณะคล้ายกับการแพร่กระจายของเชื้อโรคทั่วไป กล่าวคือ ต้องมีพาหะ หรือตัวกลาง เช่น อากาศ น้ำ และพาหะอื่น ๆ ส่วนโลกของคอมพิวเตอร์พาหะที่ว่านั้นก็คือ แผ่นดิสก์ อุปกรณ์บันทึกข้อมูลประเภทต่าง ๆ สายเคเบิลเพื่อสื่อสารข้อมูล โดยเฉพาะเครื่องคอมพิวเตอร์ที่มีผู้ใช้หลายคน และแต่ละคนก็ต่างมีแผ่นดิสก์ของตนเอง รวมทั้งมีการก๊อปปี้แผ่นดิสก์กันโดยไม่มีเงื่อนไขด้วยแล้ว ยังมีโอกาสติดไวรัสคอมพิวเตอร์มากขึ้น สาเหตุสำคัญที่ทำให้เครื่องคอมพิวเตอร์ติดไวรัสคอมพิวเตอร์ ก็คือ ผู้ใช้เครื่องคอมพิวเตอร์นำแผ่นดิสก์หรือแผ่นซีดีที่มีไวรัสคอมพิวเตอร์อยู่ ซึ่งอาจเป็นแผ่นเกมส์ หรือแผ่นโปรแกรมอื่นๆ มาใช้งานกับเครื่องคอมพิวเตอร์ ไวรัสคอมพิวเตอร์จะเข้าไปฝังตัวอยู่ในหน่วยความจำของเครื่องตั้งแต่เริ่มต้นการทำงาน ไวรัสคอมพิวเตอร์จะสามารถสร้างความเสียหายให้กับเครื่องโดยสามารถติดไปกับส่วนต่างๆของดิสก์ ฮาร์ดดิสก์ หรือ Boot Record ซึ่งมักจะถูกเรียกให้ทำงานทันทีที่มีการนำแผ่นดิสก์ที่ติดไวรัสคอมพิวเตอร์ไปใช้งาน การทำงานของไวรัสคอมพิวเตอร์บางครั้งอาจทำให้เข้าใจผิดว่าฮาร์ดดิสก์มีปัญหา เพราะว่าไวรัสคอมพิวเตอร์เข้าไปควบคุมโปรแกรมที่ทำหน้าที่ควบคุมการทำงานของจอภาพ เช่น การทำให้เกิดตัวอักษรแปลกๆ หรือตัวอักษรร่วงหล่นจากจอภาพ เป็นต้น จากการศึกษาพบว่ามีสาเหตุของการติดไวรัสคอมพิวเตอร์และการแพร่กระจายดังต่อไปนี้

1. มีการเรียกใช้งานไฟล์ที่มีไวรัสคอมพิวเตอร์ฝังตัวอยู่

ในส่วนของสาเหตุจากการที่ผู้ใช้คอมพิวเตอร์เรียกใช้งานไฟล์ที่มีไวรัสคอมพิวเตอร์ฝังตัวอยู่แล้วทำให้ ระบบถูกไวรัสคอมพิวเตอร์เข้ามาคุกคามได้นั้นเป็นสาเหตุซึ่งเป็นที่รู้จัก กันดี นอกจากการฝังตัวอยู่กับไฟล์ของผู้ใช้งานซึ่งเป็นรูปแบบของไวรัสคอมพิวเตอร์แบบยุคต้นๆ แล้วนั้น ในปัจจุบันไวรัสคอมพิวเตอร์มักจะใช้หลักจิตวิทยาที่เรียกว่า Social Engineering เพื่อทำการล่อลวงให้ผู้ใช้งานเรียกเปิดไฟล์ที่เป็นไวรัส เช่น แฝงมาในรูปแบบของโปรแกรมการ์ดอวยพร หรือ โปรแกรม screen saver หรือ แฝงอยู่ใน ไฟล์ที่ได้รับมาจากบุคคลที่ผู้ใช้รู้จัก ซึ่งผู้ใช้อาจจะได้รับมาทางอี-เมล์ที่มีการปลอมแปลงว่ามาจากบุคคลที่ผู้ใช้รู้จัก หรือไวรัสอาจแฝงอยู่ในรูปแบบของ link ในอี-เมล์หรือเว็บไซต์ต่างๆ ที่หลอกลวงให้ผู้ใช้ click เพื่อเรียกใช้งาน เป็นต้น

2. ระบบที่ไม่มีการใช้งานโปรแกรม Anti-Virus หรือมีการใช้งานโปรแกรม Anti-Virus แต่ไม่ได้ทำการ Update ฐานข้อมูลไวรัส

สำหรับสาเหตุหลักอีกสาเหตุหนึ่งของการที่ระบบถูกไวรัสคอมพิวเตอร์คุกคามคือการที่ระบบไม่มีการใช้ งานโปรแกรม Anti-Virus หรือมีการใช้งานโปรแกรม Anti-Virus แต่ไม่ได้ทำการ update ฐานข้อมูลไวรัสให้ทันสมัยอยู่เสมอ ซอฟต์แวร์ Anti-Virus ส่วนใหญ่จะสามารถต่อต้านการคุกคามจากไวรัสคอมพิวเตอร์ที่โปรแกรมรู้จักซึ่งจะได้ รับการจัดเก็บอยู่ในฐานข้อมูลไวรัส

คอมพิวเตอร์ คอมพิวเตอร์ (Virus Definition Database) ซึ่งจำเป็นต้องมีการ Update ฐานข้อมูลดังกล่าวนี้ให้ทันสมัยอยู่เสมอเพื่อ ให้โปร-แกรมรู้จักและสามารถต่อต้านไวรัสคอมพิวเตอร์ตัวใหม่ๆ ได้ บางท่านอาจมีความเชื่อที่ผิดๆ ว่าหากมีการติดตั้งซอฟต์แวร์ Anti-virus บนระบบแล้ว ไวรัสคอมพิว- เตอร์จะไม่สามารถเข้ามาคุกคามระบบได้ ในความเป็นจริงแล้วถึงแม้ระบบจะมีการติดตั้งซอฟต์แวร์ดังกล่าวอยู่ แต่หากไม่มีการ update ฐานข้อมูลไวรัสให้ทันสมัยอยู่เสมอ หรือ ไม่มีการใช้งานซอฟต์แวร์ Anti-virus เพื่อตรวจสอบโดยละเอียดว่าระบบปราศจากไวรัสคอมพิวเตอร์อย่างสม่ำเสมอแล้วนั้นไวรัสคอมพิวเตอร์ก็ยังอาจสามารถเข้ามา คุกคามระบบได้ ยิ่งไปกว่านั้นถึงแม้ซอฟต์แวร์ Anti-virus จะได้รับการติดตั้งและใช้งานอย่างเหมาะสมทุกประการ แต่ระบบก็ยังอาจมีความเสี่ยงต่อการถูกคุมคามอยู่หาก ระบบมีช่องโหว่ (Vulnerbilities) ซึ่งจะกล่าวถึงในช่วงต่อไป

3. ระบบปฏิบัติการหรือซอฟต์แวร์ที่ทำงานอยู่บนระบบมีช่องโหว่ (Vulnerbilities) พร้อมทั้งระบบมีการเชื่อมต่อกับเครือข่าย

สำหรับสาเหตุในส่วนของการที่ระบบมีช่องโหว่นั้นยังไม่ค่อยเป็นที่เข้าใจและตระหนักถึงกันอย่างถ่องแท้มากนัก ในความเป็นจริง ระบบปฏิบัติการและซอฟต์แวร์ที่ทำงาน อยู่บนระบบมักจะมีช่องโหว่อยู่ทั้งสิ้น ซึ่งมักจะมีผู้ค้นพบช่องโหว่ใหม่ๆ ของระบบอยู่เรื่อยๆ อย่างต่อเนื่อง ช่องโหว่ (vulnerbilities) มีความหมายคล้ายๆ กับ จุดบกพร่อง (Bugs) ของระบบ โดยรวมๆ ช่องโหว่หมายถึง การที่ ระบบมีช่องทางให้ผู้โจมตีสามารถเข้ามาครอบครอง ควบคุมการทำงาน นำไวรัสคอมพิวเตอร์มาเรียกใช้งาน หรือ ทำการบางอย่าง บนระบบได้ ในกรณีที่ท่านใช้ระบบปฏิบัติการ Microsoft Windows ท่านสามารถตรวจสอบว่าระบบของท่านมีช่องโหว่อะไรบ้างได้ โดยการเรียกใช้งาน Windows Update หรือ browse ไปที่ http://windowsupdate.microsoft.com/ ท่านอาจพบว่าระบบ ของท่านมีช่องโหว่ที่ร้ายแรงมากมาย ซึ่งช่องโหว่ เหล่านี้เป็นช่องทางให้ไวรัสคอมพิวเตอร์หรือผู้ไม่ประสงค์ดีสามารถเข้ามาในระบบ ของท่านผ่านเครือข่ายได้การที่ระบบมีช่องโหว่เป็นสาเหตุที่ทำให้เกิดเหตุการณ์ที่เรียก ได้ว่า "อยู่ดีๆ ก็ติดไวรัส" นั่นเอง นอกจากนี้ การใช้งานระบบปฏิบัติการหรือซอฟต์แวร์ในบางลักษณะก็ทำให้เกิดช่องโหว่ได้ เช่น การให้โปรแกรมเปิดอ่านอี-เมล์และไฟล์ที่แนบ มาโดยอัตโนมัติ การอนุญาตให้บุคคลอื่นนำไฟล์มาติดตั้งบนระบบได้ (Full-Right File Sharing) เป็นต้น

<u>อาการของเครื่องคอมพิวเตอร์ที่ติดไวรัสคอมพิวเตอร์</u>

เราสามารถสังเกตการทำงานของเครื่องคอมพิวเตอร์ที่ใช้ว่าเข้าข่ายติดไวรัสหรือไม่ จะปรากฏอาการดังต่อไปนี้

อาการที่เกิดขึ้นกับระบบคอมพิวเตอร์ขณะทำงาน

1. การโหลด (Load) โปรแกรมเข้าสู่หน่วยความจำใช้เวลานานขึ้นและใช้เวลานานผิดปกติในการเรียกโปรแกรมขึ้นมาทำงาน

2. ขนาดของหน่วยความจำที่เหลือลดน้อยลงกว่าปกติ โดยไม่ทราบสาเหตุ

3. ไฟแสดงสถานะการทำงานของฮาร์ดิสก์ติดค้างนานกว่าที่เคยเป็นแม้จะไม่เรียกโปรแกรมทำงานก็กระพริบตลอด

4. เครื่องทำงานช้าลงหรือหยุดทำงานโดยไม่ทราบสาเหตุ รวมทั้งเกิดอาการรีบูตตัวเองโดยไม่ได้สั่ง

5. แป้นพิมพ์หรือเมาส์ทำงานผิดปกติหรือไม่ทำงานเลย

6. เครื่องคอมพิวเตอร์มีการกระทำที่แปลกๆ สุดแต่ผู้เขียนโปรแกรมไวรัสจะกำหนดมา เช่น อาจส่งเสียงพิสดารต่างๆ หรือกดอักษร A หนึ่งครั้งก็แสดงอักษร A ออกมาได้หลายสิบตัว

อาการที่เกิดขึ้นกับแฟ้มข้อมูล ข้อมูล ฮาร์ดดิสก์และอุปกรณ์บันทึกข้อมูล

1. ขนาดของโปรแกรมหรือไฟล์ใหญ่ขึ้น (เพิ่มจากปกติอย่างผิดสังเกต)

2. เซกเตอร์ที่เสียมีจำนวนเพิ่มขึ้น โดยมีการรายงานว่ามีจำนวนเซกเตอร์ที่เสียเพิ่มขึ้นทั้งๆ ที่ยังไม่ได้ใช้โปรแกรมใดๆ เข้าไปตรวจหาเลย ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้งานอยู่ๆ ก็หายไป

3. เนื้อที่ในฮาร์ดดิสก์ลดลงโดยไม่ทราบสาเหตุ

4. เปิดไฟล์เอกสารไม่ได้ หรือเปิดได้แต่เป็นตัวอักษรประหลาดๆ ปนมาด้วย 15. ทำลายไฟล์ข้อมูล โดยลบไฟล์ข้อมูลแล้วกู้กลับคืนมาไม่ได้

5. ทำลาย FAT ของแผ่นดิสก์

6. มีแฟ้มข้อมูลที่เราไม่ได้สร้างปรากฏบนดิสก์ เนื่องจากไวรัสบางชนิดสามารถที่จะเขียนแฟ้มข้อมูลของตนเองลงไปในดิสก์ ทำให้เนื้อที่ ๆ สามารถใช้งานได้ลดน้อยลงไป

7. ข้อมูลทั่วไปสูญหายเป็นลักษณะของการสูญหายกับทุกแฟ้มข้อมูล ไวรัสบางตัวจะลบแฟ้มข้อมูลทุกครั้งที่โปรแกรมที่มีไวรัสนั้นอยู่ถูกเรียกใช้งาน บางชนิดก็ต้องถูกกระตุ้นหลายๆ ครั้งจึงจะทำลายข้อมูลทีหนึ่ง และบางครั้งไวรัสก็ถูกโปรแกรมให้อยู่เฉยๆ เป็นเวลานานกว่าจะเริ่มการทำลาย กว่าจะทราบว่าติดไวรัสนั้นก็ได้แพร่กระจายไปเป็นจำนวนมาก

8. ดิสก์เสียไวรัสเข้าไปทำลายระบบการจัดเก็บข้อมูลดิสก์ ทำให้ดิสก์ใช้งานไม่ได้ทำลายค่าที่ติดตั้งของระบบ เช่น ทำลายไฟล์ CONFIG.SYS ทำให้เมื่อเราเริ่มเปิดเครื่อง เครื่องจะไม่ทำงานในส่วนนี้

9. เปิดเครื่องคอมพิวเตอร์แล้วบูตเครื่องจากฮาร์ดดิสก์ไม่ได้ทำลายบูตเซกเตอร์ ทำให้ฮาร์ดดิสก์หรือแผ่นดิสก์ที่มีระบบ บูตไม่ได้

10. ฟอร์แมตแผ่นให้เราใหม่ โดยไม่ได้สั่ง

11. วันเวลาของโปรแกรมหรือไฟล์ข้อมูลเปลี่ยนไปโดยไม่ได้มีการแก้ไขหรือเรียกใช้งาน

<u>การป้องกันไวรัสคอมพิวเตอร์</u>

การป้องกันไวรัสคอมพิวเตอร์มีแนวทางในการป้องกันหลายวิธีด้วยการ สามารถจำแนกได้เป็น 2 แนวทาง คือ การป้องกันทางกายภาพและการป้องกันทางเทคนิค ดังรายละเอียดต่อไปนี้

1. การป้องกันทางกายภาพ เป็นการป้องกันที่เน้นในด้านการตรวจสอบสื่อบันทึกข้อมูลตลอดจนการสำรองข้อมูล

1.1 ตรวจสอบแผ่นดิสก์ ควรมีการตรวจสอบก่อนว่ามีไวรัสคอมพิวเตอร์ติดมาด้วยหรือไม่

1.2 ตรวจสอบฮาร์ดดิสก์ ควรมีการตรวจสอบฮาร์ดดิสก์ของเครื่องอย่างสม่ำเสมอ

1.3 ตรวจสอบ Bad Sector ควรมีการตรวจสอบ Bad Sector ในฮาร์ดดิสก์บ่อยๆ ว่ามีเนื้อที่ที่เป็น Bad Sector เพิ่มขึ้นหรือไม่

1.4 ทำการสำรองข้อมูล ควรมีการสำรอง (Backup) ข้อมูลที่มีความสำคัญไว้อย่างสม่ำเสมอเมื่อมีการปรับปรุงข้อมูล

2. การป้องกันทางเทคนิค เป็นการป้องกันทางด้านเทคนิค โดยอาศัยฮาร์ดแวร์หรือซอฟต์แวร์มาช่วยในการป้องกัน

2.1 ใช้ฮาร์ดแวร์พิเศษป้องกัน ฮาร์ดแวร์พิเศษ ก็คือ ชิ้นส่วนภายนอกที่ใช้ต่อร่วมกับตัวเครื่องคอมพิวเตอร์ มีลักษณะเป็นการ์ด ซึ่งเสียบลงบนสล็อตในเมนบอร์ดของเครื่องคอมพิวเตอร์ เช่น การ์ด AVC-4000 เป็นผลิตภัณฑ์ของบริษัท R&D โดยใช้ Hardware ผสม Software โดยใช้ Card เสียบเข้าไปในเครื่องคอมฯ และใช้โปรแกรมสนับสนุน หรือการ setup ที่ BIOS ใน CPU การใช้ Card ต้องลงทุนสูงสักหน่อย สามารถหาซื้อได้ตามร้านคอมฯ ทั่วไป การติดตั้งง่ายไม่ยุ่งยาก ตอนนี้คงมีรุ่นใหม่ AVC5000 ของ บ. R&D ออกมาจำหน่ายนิยมมากที่สุด เท่าที่

ลองใช้ดู ประสิทธิภาพค่อนข้างสูงมาก แต่ก็ต้องคอย Update ข้อมูลไวรัสด้วย ส่วนการ setup ที่ BIOS ถือว่าประสิทธิภาพพอใช้ได้ระดับหนึ่ง

2.2 ใช้ซอฟต์แวร์กำจัดไวรัส เป็นโปรแกรมที่ทำหน้าที่ปกป้องคุ้มครองข้อมูลให้รอดพ้นจากการทำลายของไวรัสคอมพิวเตอร์ทั้งหลาย โปรแกรมกำจัดไวรัสบางตัวจะฝังตัวอยู่ในหน่วยความจำซึ่งเป็นประเภท Resident Program และจะตรวจสอบการทำงานของระบบอยู่ตลอดเวลา เมื่อใดที่มีการเรียกใช้โปรแกรมทำงานใดๆ โปรแกรมนี้จะทำการตรวจสอบหาไวรัสที่รู้จักและถ้าพบก็จะร้องเตือน โปรแกรมกำจัดไวรัสที่นิยมใช้กันโดยทั่วไป ได้แก่ PC-Cillin Nortorn Anti Virus หรือ McAfee Scan Virus ซึ่งโปรแกรมเหล่านี้สามารถดาวน์โหลดมาใช้ได้จากระบบอินเทอร์เน็ต ซึ่งผู้ใช้คอมพิวเตอร์ควรจะทำการอัพเกรดโปรแกรมอยู่บ่อยๆ โดยการโหลดโปรแกรมกำจัดไวรัสเวอร์ชั่นใหม่ๆ มาใช้งาน เนื่องจากไวรัสก็มีการพัฒนารุ่นใหม่ๆ ออกมา 2. โดยใช้ Software หาซื้อหรือ Download ตาม website ต่างๆ ได้เข้าไปติดตั้งในเครื่องคอมฯ และต้อง update ข้อมูลไวรัสสม่ำเสมอด้วย เป็นที่นิยมกันมากเพราะลงทุนน้อยหรือฟรี ต้องมาดูว่าจะมาใช้โปรแกรมอะไรดี ซึ่งมีหลายโปรแกรมด้วยกัน เช่น McAfee (Scan) , Norton (NAV) , ThunderBYTE (TBAV) , Dr.Solomon และ PC-Cillin ท่านสามารถเข้าไป download ตาม website ต่างๆ หรือตามบริษัทผู้ผลิตโปรแกรมนั้นๆ ซึ่งจะเป็นชุดทดลอง ใช้ฟรีก่อนตัดสินใจซื้อจริง ส่วนประสิทธิภาพถือว่าดีระดับหนึ่ง ให้ผลการป้องกันและฆ่าได้ดี แต่ต้องคอย update ข้อมูลไวรัสสม่ำเสมอจาก website ผู้ผลิต (ดูในหัวข้อ การ update หรือจะ Download)

3. การป้องกันโดยอาศัยมาตรการเข้มงวดสำหรับสื่อต่าง ๆ

การป้องกันแบบนี้จะโหดสักหน่อย คือห้ามนำสื่อจากภายนอกเข้ามาใช้ภายในเครื่อง เช่น แผ่น CD , แผ่น diskette หรือจะเป็นเข้าระบบ Network LAN, Intranet หรือ Internet ซึ่งการป้องกันแบบนี้คงจะทำได้ ยากมากๆ