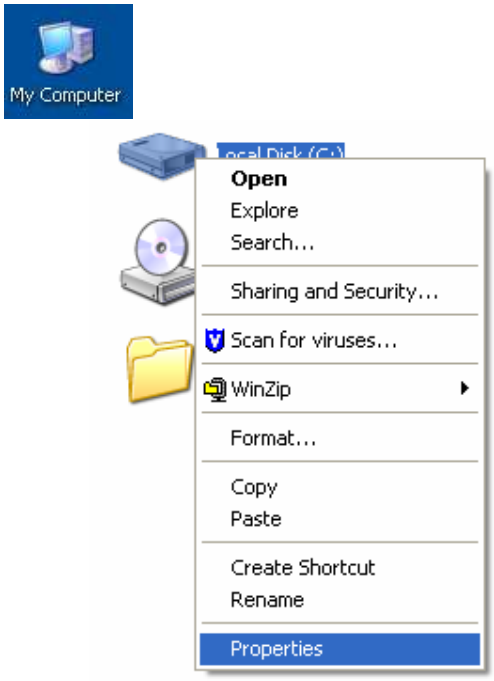
ตอนที่ 1
การแก้ปัญหาเครื่องคอมพิวเตอร์ขั้นพื้นฐาน

การสำรองระบบและการสำรองข้อมูล

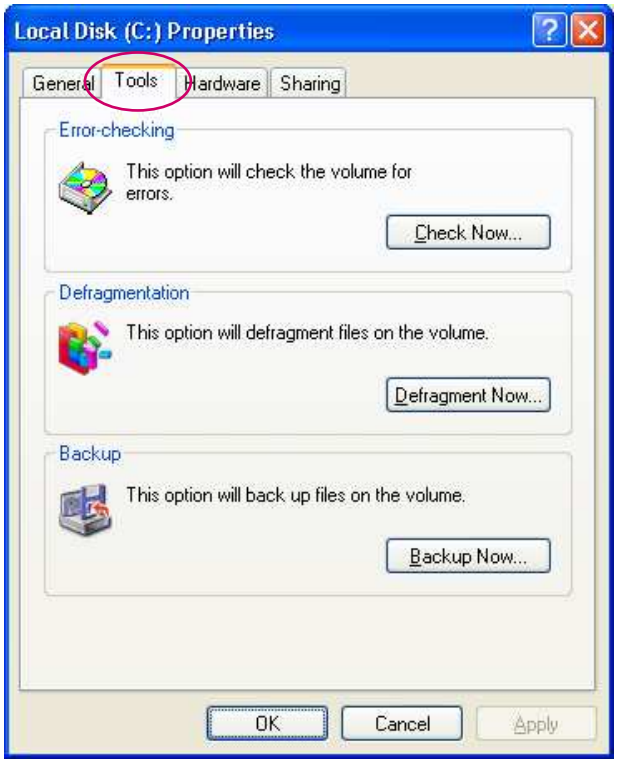
ในการใช้งานคอมพิวเตอร์นั้นเมื่อเกิดปัญหาต่างๆ ขึ้นผู้ใช้ต้องทำการบำรุงรักษาหรือแก้ไขเพื่อให้คอมพิวเตอร์สามารถใช้งานต่อไปได้ แต่บางครั้งข้อมูลต่างๆ ก็อาจเสียหายหรือเกิดความสูญหายได้ ดังนั้น จึงควรมีการสำรองระบบและสำรองข้อมูลเอาไว้เพื่อให้สามารถนำข้อมูลที่ต้องการกลับมาใช้งานได้อีกครั้ง โดยมีขั้นตอนดังนี้

1. ดับเบิลคลิกที่ My Computer
2. คลิกขวาที่ไดร์ฟที่ต้องการ → เลือกคำสั่ง **Properties**



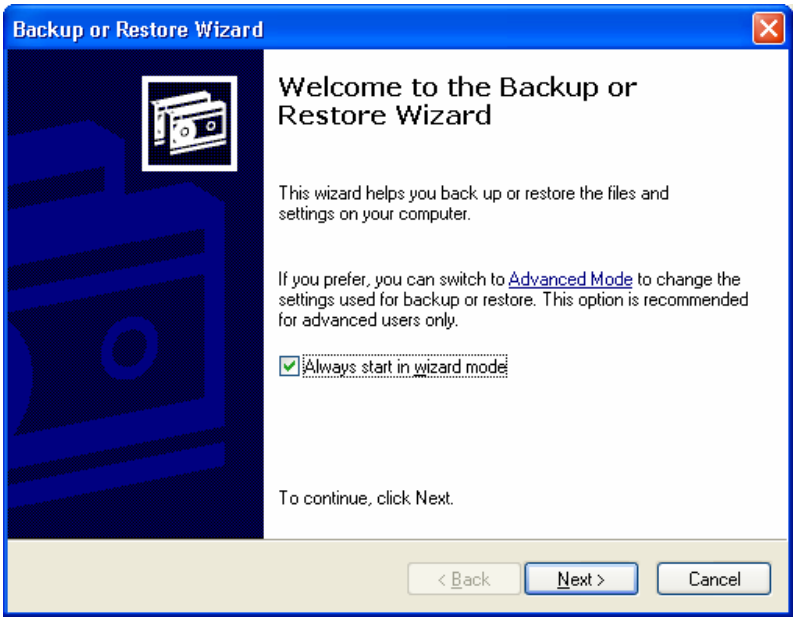
ภาพที่ 1-1 แสดงขั้นตอนการสำรองระบบและการสำรองข้อมูล

3. คลิกเลือกป้าย **Tools**
4. คลิกปุ่ม **Backup Now**



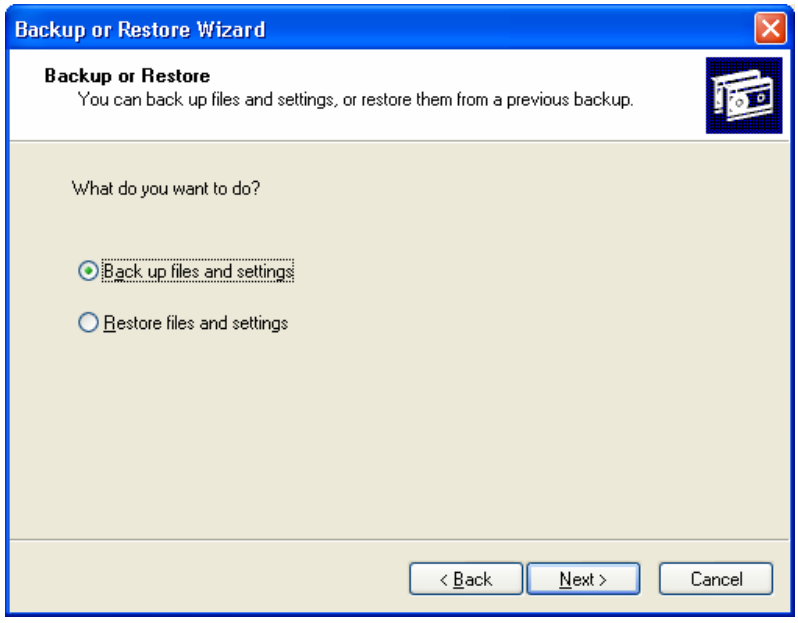
ภาพที่ 1-2 แสดงขั้นตอนการสำรองระบบและการสำรองข้อมูล (ต่อ)

5. จะปรากฏหน้าต่าง **Welcome…**
6. คลิกปุ่ม **Next**



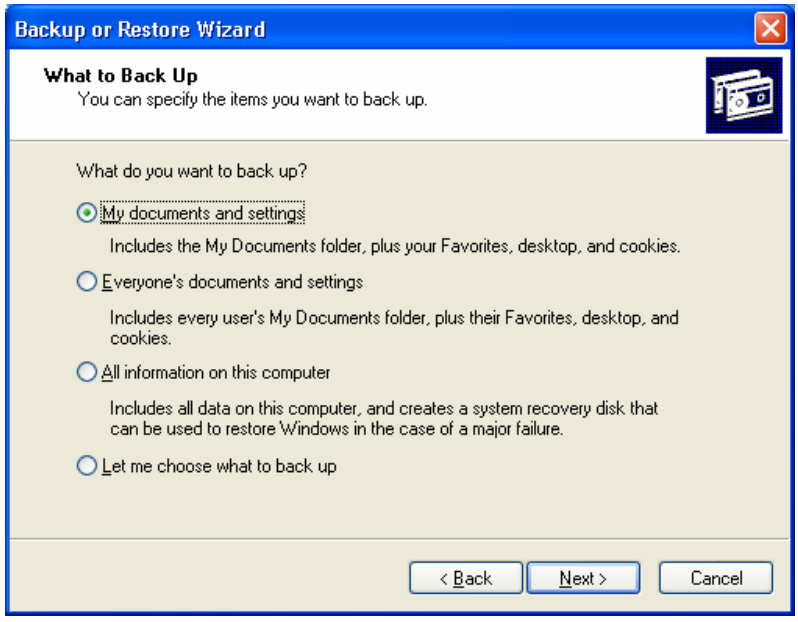
ภาพที่ 1-3 แสดงขั้นตอนการสำรองระบบและการสำรองข้อมูล (ต่อ)

7. เลือกทางเลือกการทำงาน
   - Backup files and setting
   - Restore files and setting
8. คลิกปุ่ม **Next**



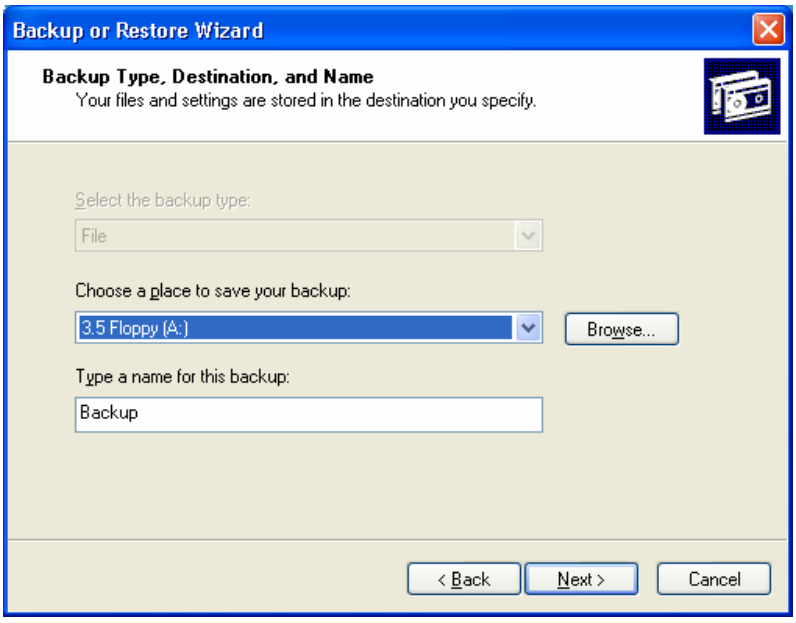
ภาพที่ 1-4 แสดงทางเลือการทำงานในการสำรองระบบและสำรองข้อมูล

9. เลือกรูปแบบการ **Back Up**
10. คลิกปุ่ม **Next**



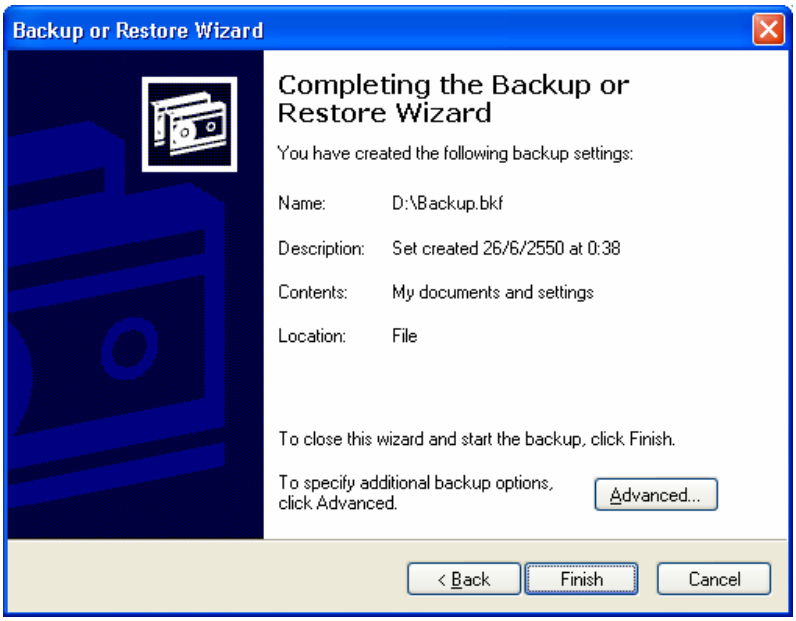
ภาพที่ 1-5 แสดงรูปแบบในการสำรองระบบและสำรองข้อมูล

11. เลือกไดร์ฟที่ต้องการเก็บข้อมูล
12. ตั้งชื่อไฟล์
13. คลิกปุ่ม **Next**



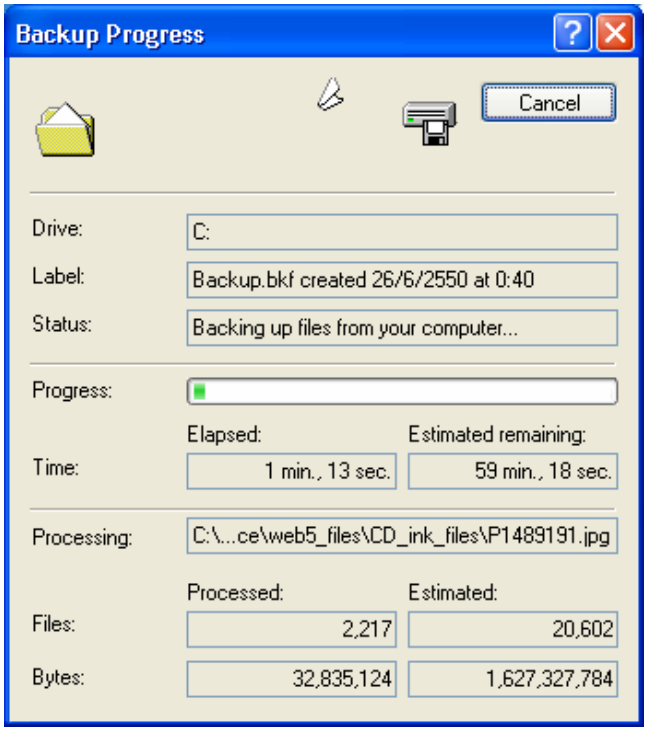
ภาพที่ 1-6 การเลือกไดร์ฟและตั้งชื่อไฟล์ในการสำรองระบบและสำรองข้อมูล

14. คลิกปุ่ม **Finish**



ภาพที่ 1-7 แสดงรายละเอียดในการสำรองระบบและสำรองข้อมูล

15. จะปรากฏหน้าต่างการทำ Backup ให้รอจนกระทั่งทำเสร็จ



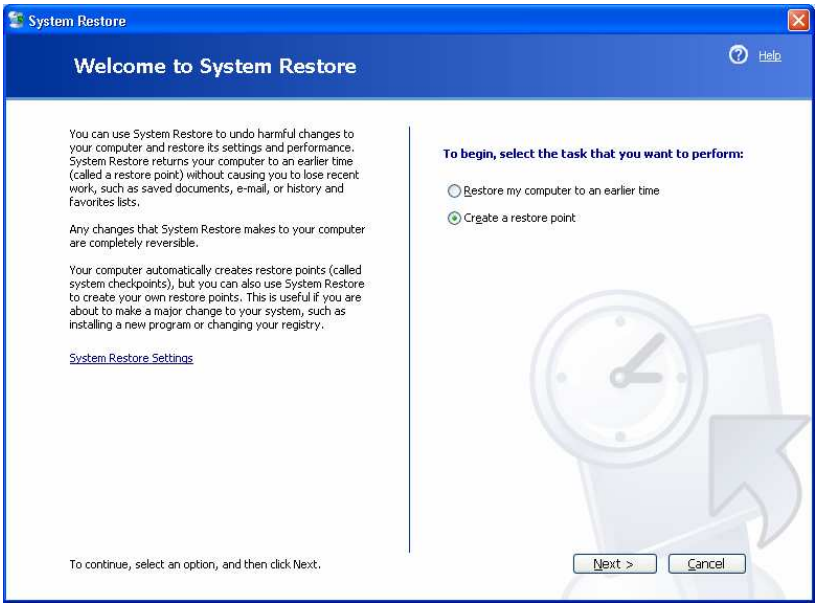
ภาพที่ 1-8 แสดงการสำรองระบบและสำรองข้อมูล

การใช้งาน System Restore

ปกติทั้ง Windows XP และ Windows ME จะมีเครื่องมือชื่อว่า System Restore ให้มาด้วย โดยจะทำหน้าที่เหมือนโกดังเก็บข้อมูลต่างๆ เกี่ยวกับการทำงานของ Windows และไฟล์แอพพลิเคชันต่างๆ ที่ติดตั้งในระบบ เมื่อคุณต้องการเรียกคืนสถานภาพการทำงานในช่วงเวลาก่อนหน้านี้ให้กับระบบก็สามารถทำได้ด้วยการเลือกวันที่ต้องการย้อนกลับไป และนี่คือหน้าที่ของ System Restore ของ Windows System Restore จะสามารถสร้างจุดในการเรียกคืนระบบ (restore point) ได้หลายวิธีด้วยกัน ซึ่งปกติจะมีการสร้างข้อมูลที่ใช้ในการเรียกคืนระบบทุกๆ 24 ชั่วโมง ในกรณีที่คอมพิวเตอร์เปิดทำงานตลอดเวลา แต่ถ้าเครื่องคอมพ์ปิดอยู่ การทำ restore point จะถูกสร้างขึ้นเมื่อคุณเปิดเครื่องขึ้นทำงาน นอกจากนี้ restore point ยังอาจถูกสร้างขึ้นตอนที่คุณติดตั้งโปรแกรม หรือบางทีก็ตอนติดตั้งอุปกรณ์ใหม่ เพิ่มเข้าไปอย่างเช่น เครื่องพิมพ์ เป็นต้น อย่างไรก็ดี คุณสามารถสร้าง restore point เองได้ด้วย

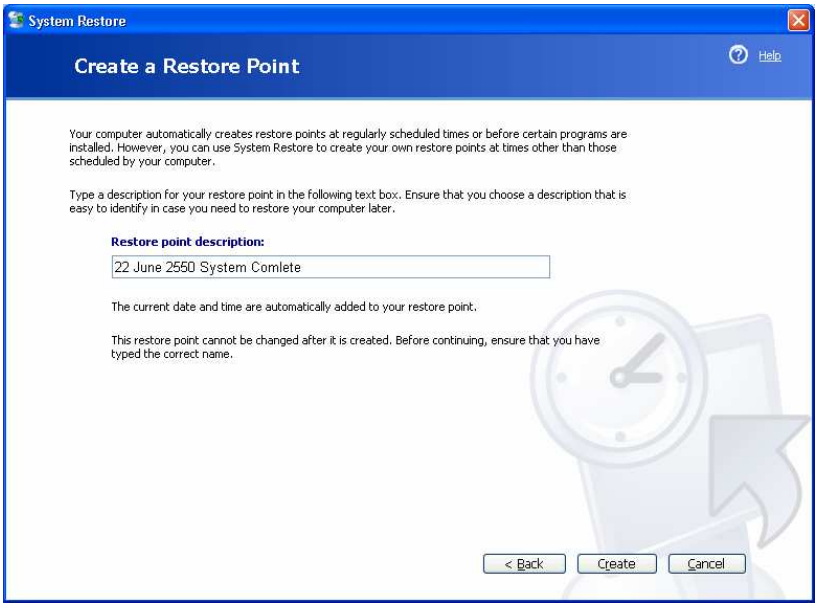
การเรียกใช้งาน System Restore

1. คลิกปุ่ม **Start** → เลือก **Programs** → เลือก **Accessories** → เลือก **System Tools** → เลือก **System Restore**
2. คลิกเลือกทางเลือก **Create a restore point**
3. คลิกปุ่ม **Next**



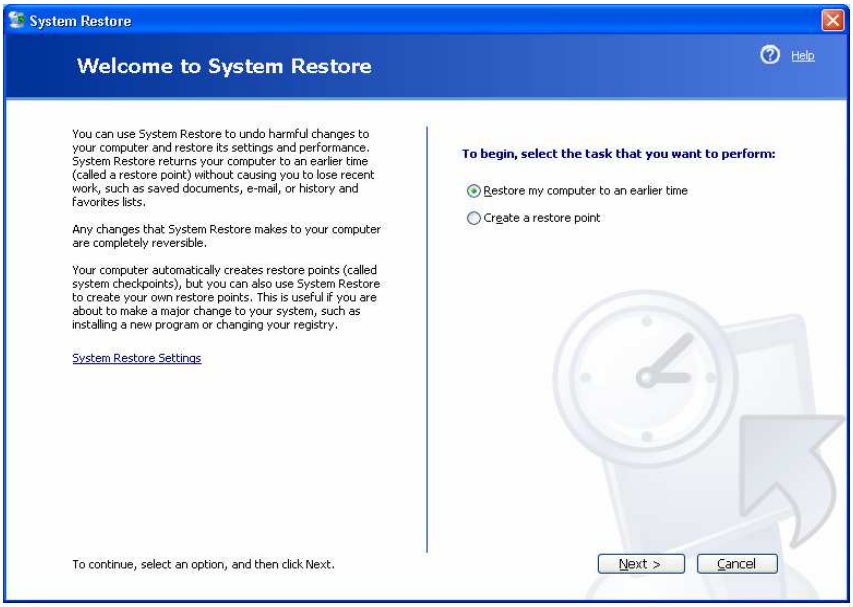
ภาพที่ 1-9 แสดงการกำหนดจุดสร้างระบบ

4. กำหนดรายละเอียด (ตั้งชื่อ)
5. คลิกปุ่ม **Create**



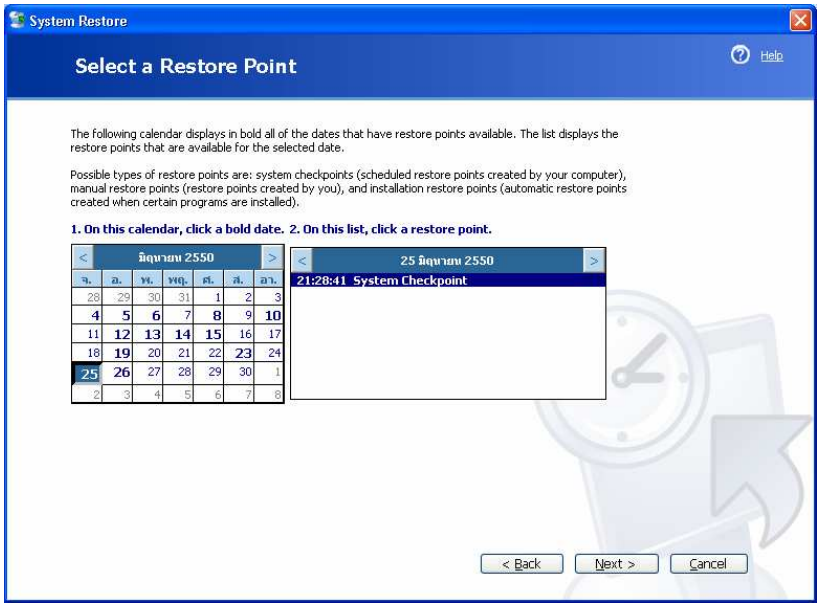
ภาพที่ 1-10 แสดงการกำหนดจุดสร้างระบบ (ต่อ)

6. ที่หน้าต่าง System Restore เลือกทางเลือก **Restore my computer to an earlier time**



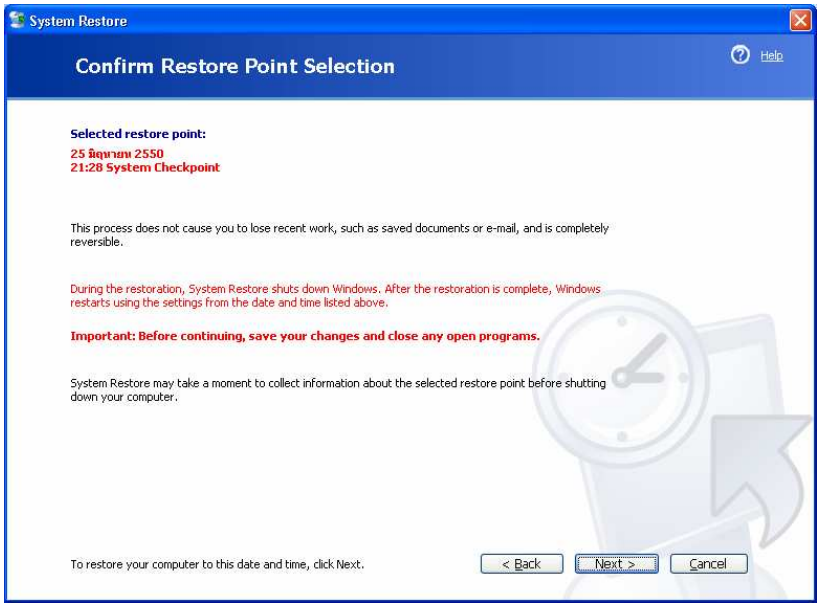
ภาพที่ 1-11 แสดงการกู้ระบบคืน

7. คลิกปุ่ม **Next**
8. คลิกเลือกวันที่ที่ต้องการจะกู้คืน จากช่องปฏิทิน
9. คลิกเลือกจุดที่จะกู้คืน จากชื่อ **Restore Point**
10. คลิกปุ่ม **Next**



ภาพที่ 1-12 แสดงการเลือกวันที่ที่ต้องการกู้ระบบคืน

11. คลิกปุ่ม **Next** เพื่อยืนยัน



ภาพที่ 1-13 แสดงยืนยันการกู้ระบบคืน

ไวรัสคอมพิวเตอร์

ปัญหาของการใช้งานคอมพิวเตอร์ที่สำคัญอย่างหนึ่งก็คือ ปัญหาจากไวรัสคอมพิวเตอร์ ดังนั้น เราควรทำความรู้จักและหาวิธีป้องกัน เพื่อไม่ให้ไวรัสคอมพิวเตอร์เข้ามาสร้างความเสียหายกับระบบคอมพิวเตอร์ของเรา

ในสมัยก่อนเมื่อได้ยินคำว่าไวรัสคอมพิวเตอร์ก็เริ่มสงสัยว่าเป็นอย่างไร เหมือนกับไวรัสที่เป็นพวกเชื้อโรคที่ทำให้เราเป็นหวัดหรือไม่ แต่พอได้ยินคำว่าไวรัสคอมพิวเตอร์มันเป็นไวรัสชนิดใหม่หรืออย่างไรหลายท่านอาจจะสงสัย ดังนั้นเรามาทำความรู้จักกับไวรัสคอมพิวเตอร์กันดีกว่า

ไวรัสคอมพิวเตอร์คืออะไร

ไวรัสคอมพิวเตอร์เป็นโปรแกรมชนิดหนึ่ง ไวรัสคอมพิวเตอร์ถูกสร้างจากโปรแกรมเมอร์ที่มีความชำนาญในการเขียนโปรแกรม โดยปกติไวรัสจะทำงานด้วยตัวมันเอง โดยที่ไม่ต้องรับคำสั่งจากผู้ใช้เมื่อเปิดเครื่องที่มีไวรัสคอมพิวเตอร์มันจะเริ่มทำงานโดยอัตโนมัติ

การทำงานของไวรัสคอมพิวเตอร์ส่วนใหญ่จะอาศัยการลักลอบเข้าไปในคอมพิวเตอร์ต่อจากนั้นก็เริ่มแพร่กระจายโดยฝังตัวติดไปกับไฟล์ต่างๆ ที่อยู่ภายในเครื่องคอมพิวเตอร์ เช่น ไฟล์โปรแกรมต่างๆ หรือไฟล์ระบบ เช่น บู๊ตเซ็กเตอร์ เมื่อทำการบู๊ตเครื่องไวรัสคอมพิวเตอร์ก็จะเริ่มทำงานและเริ่มโหลดตัวเองลงสู่หน่วยความจำ จากนั้นมันก็จะเริ่มปฏิบัติภารกิจของมันก็คือทำลายไฟล์โปรแกรมต่างๆ เช่น ไฟล์เอกสาร ไฟล์ระบบ เป็นต้น

การที่เราเรียกโปรแกรมประเภทนี้ว่า ไวรัสคอมพิวเตอร์ เพราะว่าโปรแกรมมีขนาดเล็กและสามารถแพร่กระจายไปยังเครื่องคอมพิวเตอร์เครื่องอื่นได้ นอกจากนั้นยังทำความเสียหายให้กับ

ระบบอีกด้วย ทั้งหมดที่กล่าวมามีลักษณะคล้ายกับไวรัสในทางชีววิทยาจึงทำให้โปรแกรมเมอร์เรียกโปรแกรมประเภทนี้ว่า *"ไวรัสคอมพิวเตอร์"*

ไวรัสคอมพิวเตอร์ทำงานอย่างไร

การทำงานของไวรัสคอมพิวเตอร์จะมีลักษณะคือ พยายามรวมตัวเองเข้ากับไฟล์โปรแกรม เมื่อใดที่โปรแกรมเริ่มทำงานไวรัสคอมพิวเตอร์ก็จะเริ่มทำงาน สมัยก่อนวิธีแพร่กระจายของไวรัสคอมพิวเตอร์จะอาศัยแผ่นฟล็อปปี้ดิสก์ เมื่อนำแผ่นฟล็อปปี้ดิสก์ที่มีไวรัสคอมพิวเตอร์ไปใช้งานก็จะเริ่มแพร่กระจายลงสู่หน่วยความจำและฝังตัวอยู่กับไฟล์ต่างๆ ในเครื่อง

ในปัจจุบันเทคโนโลยีทางด้านอินเทอร์เน็ตเข้ามามีบทบาทในชีวิตประจำวันมากขึ้น ซึ่งอันตรายที่ตามมาหลังจากการใช้งานอินเทอร์เน็ตก็คือ การแพร่กระจายของไวรัสคอมพิวเตอร์ที่ได้อาศัยช่องทางจากอินเทอร์เน็ต โดยไวรัสจะอาศัยการแนบไฟล์มากับอีเมล์ หรือว่าโปรแกรมต่างๆ ที่เราดาวน์โหลดมา เพราะฉะนั้นเมื่อเราต้องอ่านจดหมายอิเล็กทรอนิกส์ที่มีไฟล์แนบมา ควรจะแน่ใจว่าไม่มีไวรัส หรือไฟล์ที่เราต้องการดาวน์โหลดก็ควรตรวจสอบไวรัสเสียก่อน

โดยปกติเวลาที่เราเช็คเมล์ถ้าไม่มีไฟล์ที่แนบมาด้วยไวรัสจะไม่สามารถฝังตัวอยู่ได้ แต่ถ้าเมล์ที่เรารับมามีการแนบไฟล์มาด้วยไวรัสจะอาศัยอยู่ในไฟล์ที่แนบมา เมื่อทำการอ่านไฟล์ที่แนบมาไวรัสก็จะเริ่มปฏิบัติภารกิจทันที

ไวรัสคอมพิวเตอร์จะมีการทำงานบนระบบปฏิบัติการหลายแบบ ทั้งระบบ DOS, Windows หรือ Linux เป็นต้น ซึ่งการทำงานของไวรัสคอมพิวเตอร์จะไม่เหมือนกัน แต่โดยส่วนใหญ่ไวรัสคอมพิวเตอร์จะทำงานอยู่ 2 รูปแบบ คือ

1. ไม่ทำความเสียหายให้กับระบบ แต่จะคอยสร้างความรำคาญให้กับผู้ใช้ เช่น สั่งเครื่อง Shutdown เป็นต้น
2. ทำลายความเสียหายให้กับระบบ ไวรัสคอมพิวเตอร์ประเภทนี้จะทำลายไฟล์ข้อมูลต่าง ๆ เช่น ลบข้อมูล, ฟอร์แมตฮาร์ดดิสก์ เป็นต้น

ประเภทของไวรัสคอมพิวเตอร์

ไวรัสคอมพิวเตอร์ที่พบบ่อยๆ ในปัจจุบันเราสามารถแบ่งออกได้เป็น 7 ประเภท คือ

1. ไวรัสโปรแกรม (Program Virus)

เป็นไวรัสคอมพิวเตอร์ที่ทำงานบนระบบปฏิบัติการ Dos และ Windows เป็นหลัก หากมีการเรียกใช้งาน โปรแกรมที่ติดไวรัสก็จะทำให้มีการกระจายไปยังไฟล์อื่นในระบบของเรา

2. ไวรัสบู๊ต (Boot Virus)

เป็นไวรัสที่คอยฝังตัวอยู่ในส่วนของการบู๊ตเครื่องส่วนใหญ่จะเป็น Boot Sector เมื่อมีการเรียกใช้งานก็จะเริ่มโหลดตัวเองลงสู่ระบบ ปัญหาที่มักเกิดเมื่อติดไวรัสจำพวกนี้ก็คือ เมื่อเปิดเครื่องจะไม่สามารถเข้าสู่วินโดวส์ได้เพราะว่าไวรัสฝังตัวอยู่ในส่วนของการบู๊ตเครื่อง

3. ไวรัสมาโคร (Macro Viruses)

ไวรัสคอมพิวเตอร์ชนิดนี้ตอนนี้กำลังได้รับความนิยมอย่างมาก เนื่องจากโปรแกรมเมอร์สามารถพัฒนาไวรัสชนิดนี้ได้ง่าย หน้าที่ของไวรัสประเภทมาโครส่วนใหญ่จะคอยทำลายไฟล์เอกสารต่างๆ เช่น .doc, .xls ของไมโครซอฟต์ออฟฟิศ เป็นต้น

4. ไวรัสเลียนแบบ (Companion Virus)

ไวรัสชนิดนี้มีหลักการทำงานที่แปลกจากหลักการทำงานของไวรัสทั่วๆ ไป นั่นคือไวรัสทั่วไปจะอาศัยการแฝงไปตามไฟล์ต่างๆ แต่ไวรัสเลียนแบบจะทำการสร้างไฟล์ขึ้นมาใหม่แล้วเลียนแบบไฟล์โปรแกรมที่มีอยู่ในระบบดอส จากนั้นจึงหลอกให้ดอสเรียกไฟล์ที่เลียนแบบขึ้นมาทำงานซึ่งจะทำให้เครื่องติดไวรัสทันที

5. ไวรัสหลบหลีก (Stealth Virus)

เป็นไวรัสที่มีความฉลาดในการหลบหลีกการตรวจจับ หรือการกำจัดจากโปรแกรมป้องกันไวรัส เนื่องจากไวรัสชนิดนี้จะทำการขัดขวางการทำงานของโปรแกรมบางประเภทที่มีการป้องกันไวรัสด้วยวิธีการก๊อปปี้ไฟล์ข้อมูลเดิมไว้ก่อน ถ้าไฟล์ข้อมูลนั้นเกิดมีปัญหาในการติดไวรัสโปรแกรมนั้นก็จะเลือกไฟล์ข้อมูลเดิมที่ได้ก๊อปปี้ไว้มาทำงานแทนไฟล์ที่ติดไวรัส และ Stealth นั้นสามารถทำการเปลี่ยนชื่อไฟล์หรือไดเร็กทอรี่ให้กับไฟล์ที่ติดไวรัสได้ ซึ่งจะทำให้โปรแกรมป้องกันไวรัสคิดว่าไฟล์นั้นไม่ได้ติดไวรัสนั่นเอง

6. ไวรัสหลอกลวง (Polymorphic Viruses)

เป็นไวรัสที่เมื่อทำการแพร่กระจายเชื้อไปตามไฟล์ต่างๆ แล้วจะทำการแสดงผล เหมือนกับมีไวรัสอยู่หลายตัวในเครื่อง ซึ่งจะทำให้มีความยากในการตรวจสอบ

7. ไวรัสสองหน้า (Multipartite Virus)

ไวรัสชนิดนี้มีความสามารถพิเศษกว่าไวรัสชนิดอื่น ตรงที่สามารถทำการแพร่ได้ทั้งโปรแกรม และ Boot Sector ได้พร้อมๆ กันการทำงานของไวรัสขั้นตอนแรกจะทำการฝังตัวอยู่ในหน่วยความจำของ Boot Sector ก่อนจากนั้นจึงทำการแพร่กระจายเชื้อไปตามไฟล์ต่างๆ

อาการของเครื่องคอมพิวเตอร์ที่ติดไวรัส

เราสามารถสังเกตการทำงานของเครื่องคอมพิวเตอร์ ถ้าหากว่าเครื่องของคุณมีอาการดังต่อไปนี้ อาจเป็นไปได้ว่าได้มีไวรัสเข้าไปติดอยู่ในเครื่องแล้วอาการที่ว่านั้น ได้แก่

- ใช้เวลานานผิดปกติในการเรียกโปรแกรมขึ้นมาทำงาน
- ขนาดของโปรแกรมใหญ่ขึ้น
- วันเวลาของโปรแกรมเปลี่ยนไป
- ข้อความที่ปกติไม่ค่อยได้เห็นกลับถูกแสดงขึ้นมาบ่อย ๆ
- เกิดอักษรหรือข้อความประหลาดบนหน้าจอ
- เครื่องส่งเสียงออกทางลำโพงโดยไม่ได้เกิดจากโปรแกรมที่ใช้อยู่
- แป้นพิมพ์ทำงานผิดปกติหรือไม่ทำงานเลย

- ขนาดของหน่วยความจำที่เหลือลดน้อยกว่าปกติ โดยหาเหตุผลไม่ได้
- ไฟล์แสดงสถานะการทำงานของดิสก์ติดค้างนานกว่าที่เคยเป็น
- ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้อยู่ๆ ก็หายไป
- เครื่องทำงานช้าลง
- เครื่องบูตตัวเองโดยไม่ได้สั่ง
- ระบบหยุดทำงานโดยไม่ทราบสาเหตุ
- เซกเตอร์ที่เสียมีจำนวนเพิ่มขึ้นโดยมีการรายงานว่าจำนวนเซกเตอร์ที่เสียมีจำนวนเพิ่มขึ้นกว่าแต่ก่อนโดยที่ ยังไม่ได้ใช้โปรแกรมใดเข้าไปตรวจหาเลย

ถ้าหากว่าเครื่องของท่านมีอาการดังที่กล่าวมาข้างต้น ก็ถึงเวลาแล้วที่ท่านควรจะสงสัยและตรวจหาไวรัสในเครื่องของท่านก่อนที่เหตุการณ์จะบานปลาย จนถึงขั้นที่ไวรัสไปทำลายข้อมูลและไฟล์ระบบในเครื่องของท่านจนท่านต้องสูญเสียข้อมูลอันมีค่าในเครื่องของท่านไป และในยามปกติก็ควรที่จะหาโปรแกรมป้องกัน และกำจัดไวรัสมาไว้ในเครื่องของท่านเพื่อความปลอดภัย

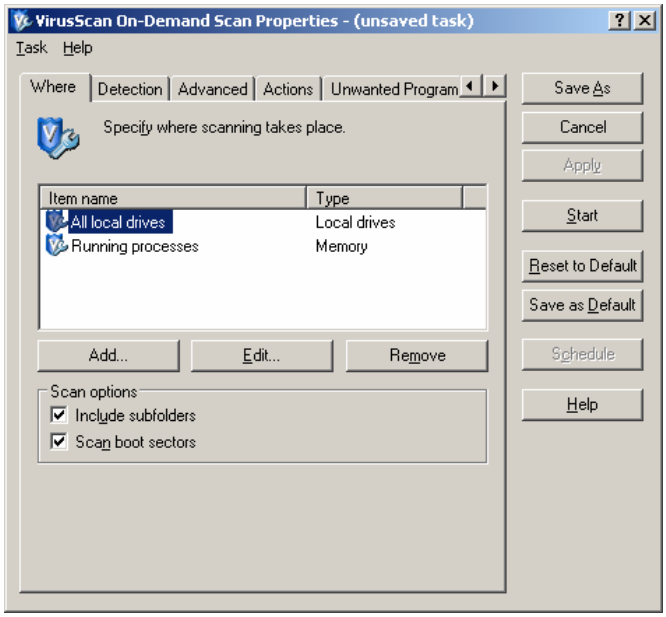
การใช้งานโปรแกรมป้องกันไวรัส McAfee Virus Scan

โปรแกรมป้องกันไวรัสในปัจจุบันมีอยู่มากมายหลายบริษัท ไม่ว่าจะเป็น MacAfee Scan Virus, Norton Anti-Virus, AVG หรือ PC Cilin เป็นต้น แต่โปรแกรมป้องกันไวรัส Mcafee Scan Virus จากบริษัท Network Associate ถือว่าเป็นโปรแกรมป้องกันไวรัสที่นิยมใช้กันมากตัวหนึ่งตั้งแต่ระบบปฏิบัติการ DOS จนถึงปัจจุบัน ด้วยความสามารถใหม่ๆ ของ McAfee อย่างเช่น การทำแผ่นดิสก์ฉุกเฉิน การอัปเดทข้อมูลไวรัสผ่านทางอินเทอร์เน็ต การสแกนไวรัสจากอีเมล์ เป็นต้น รวมไปถึงการพัฒนารูปแบบให้สวยงาม จึงทำให้โปรแกรม McAfee เป็นที่นิยมใช้ในปัจจุบัน

หลังจากที่ทำการติดตั้งโปรแกรมเสร็จเรียบร้อยแล้วจะมีการสแกนหาไวรัสให้อัตโนมัติอยู่แล้ว แต่ถ้าต้องการสแกนหาไวรัสในครั้งต่อไปเราสามารถทำได้ดังนี้

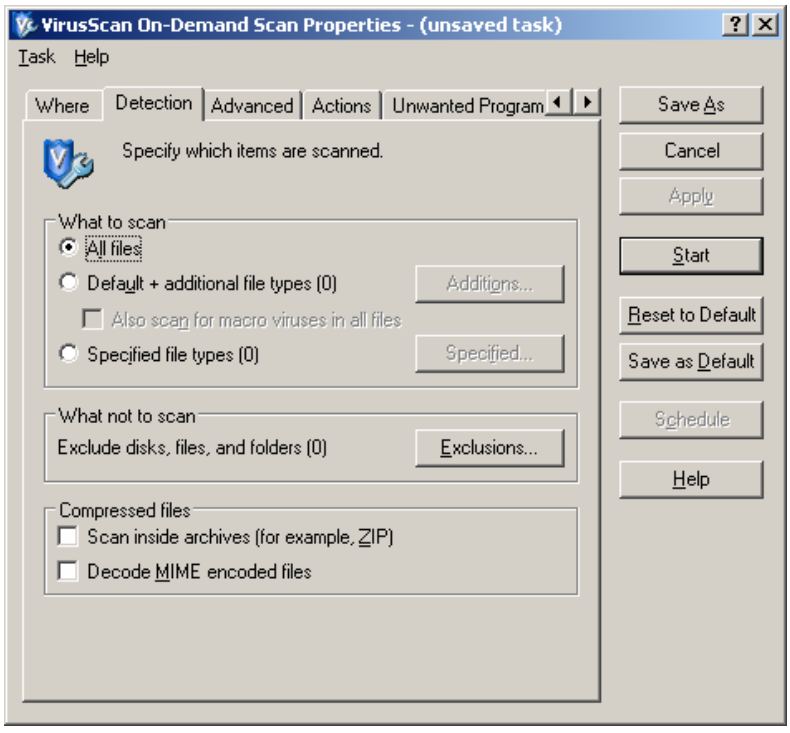
การเรียกใช้โปรแกรม

1. คลิกที่ปุ่ม **Start → Programs →Network Associates → Virus Scan On-Demand Scan** จะปรากฏหน้าต่างโปรแกรม McAfee คลิกเลือกไดร์ฟ หรือโฟล์เดอร์ที่ต้องการสแกน



ภาพที่ 1-14 แสดงหน้าต่างของโปรแกรม McAfee VirusScan.Enterprisev8.0

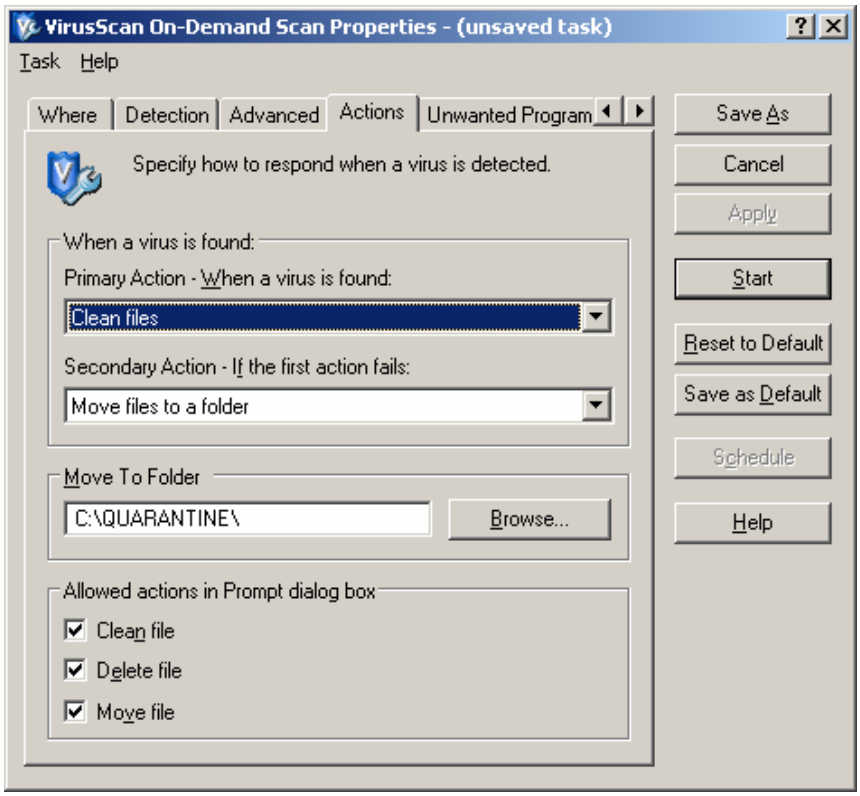
2. คลิกที่ป้าย **Detection** เพื่อกำหนดรายละเอียดการสแกน



ภาพที่ 1-15 แสดงหน้าจอสำหรับกำหนดรายละเอียดการสแกน

- **All Files** กำหนดให้ทำการสแกนไวรัสทุกไฟล์ที่อยู่ในไดร์ฟ และโฟลเดอร์ที่เราเลือกไว้
- **Default Files** กำหนดให้ทำการสแกนไวรัสในส่วนที่เป็นไฟล์พื้นฐานของระบบ ซึ่งจะเป็นไฟล์ระบบทั่วไปของ Windows
- **User Specified Files** กำหนดให้ทำการสแกนไวรัสเฉพาะไฟล์ที่ผู้ใช้งานเลือกไว้
- **Compress Files** กำหนดให้ทำการสแกนไวรัสในไฟล์ที่มีการบีบอัดไว้

3. คลิกที่ป้าย **Actions** เพื่อกำหนดรายละเอียดการสแกน



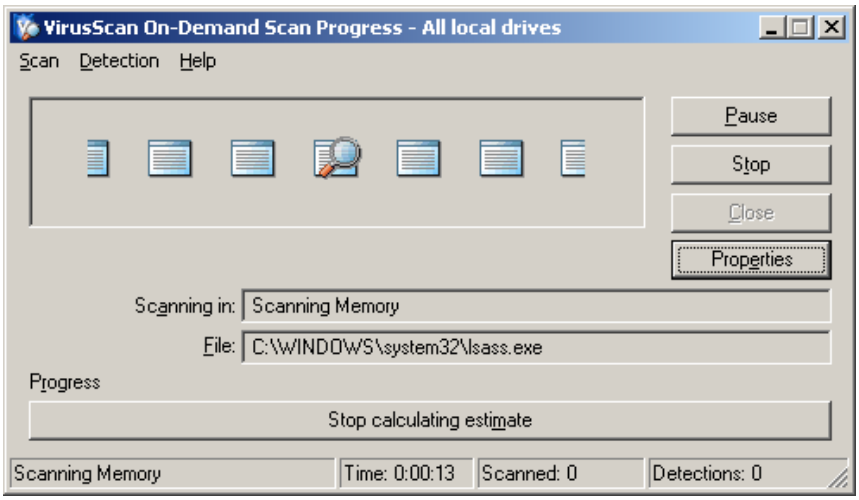
ภาพที่ 1-16 แสดงหน้าจอสำหรับกำหนดรายละเอียดการสแกน

ในหัวข้อ **When a virus is found** เป็นการกำหนดค่าเมื่อโปรแกรมสแกนพบไวรัสแล้วจะให้ทำงานอย่างไร ซึ่งจะมีรายการให้เราเลือกดังนี้

- **Prompt for user action** แสดงข้อความเพื่อให้ผู้ใช้เลือกว่าต้องการทำอย่างไรกับไฟล์ที่ติดไวรัส
- **Clean infected files automatically** กำหนดให้โปรแกรมกำจัดไวรัสโดยอัตโนมัติทันทีที่พบไวรัส

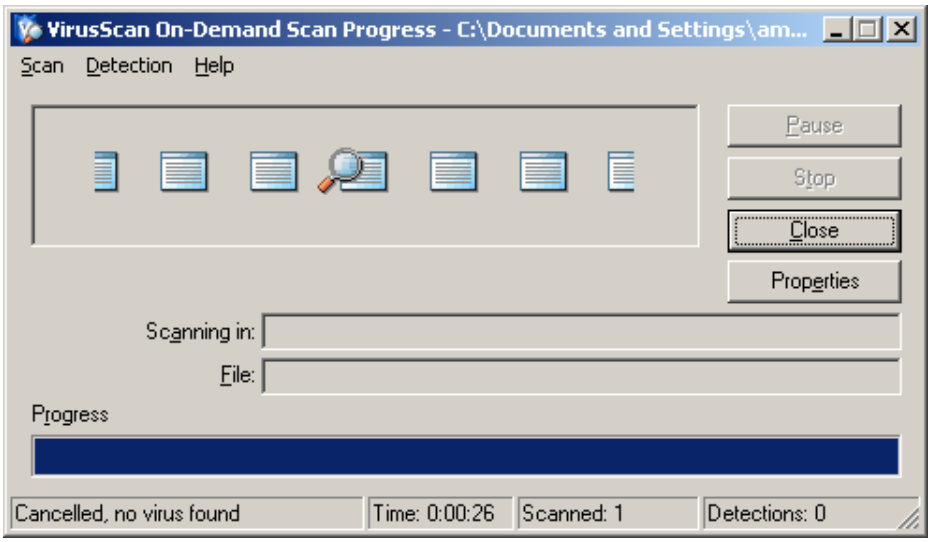
- **Delete infected files automatically** กำหนดให้โปรแกรมทำการลบไฟล์ข้อมูลที่ติดไวรัสโดยอัตโนมัติ
- **Quarantine** กำหนดให้โปรแกรมทำตรึงหรือกักขังไวรัสไว้ไม่ให้แพร่หลายไปสู่ไฟล์ข้อมูลอื่น
- **Continue Scanning** กำหนดให้โปรแกรมทำการสแกนหาไวรัสต่อไป

4. เมื่อเรากำหนดรายละเอียดการสแกนเสร็จเรียบร้อยให้คลิกปุ่ม **Start**



ภาพที่ 1-17 แสดงหน้าจอขณะทำการสแกนไวรัส

5. เมื่อสแกนหาไวรัสเสร็จสิ้นแล้วจะแสดงผลการสแกนดังภาพ



ภาพที่ 1-18 แสดงหน้าจอผลการตรวจสอบไวรัส

ในกรณีที่ผู้ใช้งานไม่มีเวลาที่จะทำการสแกนหาไวรัสได้ด้วยตัวเอง ก็สามารถกำหนดตารางการทำงานไว้ล่วงหน้าได้ ซึ่งเราอาจจะสร้างตารางเวลาในการสแกนไวรัสขึ้นเองจากโปรแกรม McAfee Virus Scan เองหรือจะสร้างโดยใช้โปรแกรม Schedules Task ใน Accessories ก็ได้ เมื่อถึงเวลาโปรแกรมก็จะทำงานอัตโนมัติ เพื่อให้เครื่องคอมพิวเตอร์ของเราทำงานตอบสนองความต้องการได้อย่างราบรื่น และเราก็จะมีความสุขในการทำงานอีกด้วย

ขั้นตอนในการป้องกันไวรัส

หลังจากที่เราได้ทราบถึงความยุ่งยาก และความร้ายกาจของไวรัสแล้ว ก่อนที่จะสูญเสียข้อมูลที่สำคัญขอแนะนำขั้นตอนพื้นฐานในการป้องกันไวรัสคอมพิวเตอร์เบื้องต้น โดยขั้นตอนต่างๆ ดังจะกล่าวต่อไปนี้ ซึ่งจะช่วยทำให้ผู้ใช้งานคอมพิวเตอร์ไม่ต้องประสบกับปัญหาตามมาภายหลัง

ขั้นตอนที่ 1 เตรียมโปรแกรมป้องกันไวรัส

การที่เครื่องของเราติดตั้งโปรแกรมป้องกันไวรัส ก็จะช่วยให้เราสามารถจับการทำงานของไวรัสได้ ถ้าหากว่าตอนนี้ท่านใดยังไม่ได้ติดตั้งโปรแกรมป้องกันไวรัส ท่านควรจะหาโปรแกรมป้องกันไวรัสมาติดตั้งเสียก่อน ซึ่งโปรแกรมก็สามารถจะหาซื้อได้ตามร้านขาย Software หรืออาจจะทำการดาวน์โหลดโปรแกรมทางอินเทอร์เน็ต ตามเว็บไซต์ที่มีให้บริการฟรีดาวน์โหลด เช่น www.download.com, www.thaiware.com เป็นต้น

ขั้นตอนที่ 2 อัปเดตข้อมูลไวรัสบ่อยๆ

ควรทำการปรับปรุงข้อมูลของไวรัสใหม่ๆ ให้กับโปรแกรมป้องกันไวรัสบ่อยๆ ซึ่งโปรแกรมป้องกันไวรัสเวอร์ชันใหม่ๆ นั้นจะมีคุณสมบัติที่สามารถเชื่อมต่อกับเว็บไซต์ของผู้ผลิตได้โดยอัตโนมัติเพื่อทำการปรับปรุงข้อมูลไวรัสใหม่ๆ ให้กับโปรแกรมป้องกันไวรัสนั้นเอง

ขั้นตอนที่ 3 ทำการสแกนไวรัสอย่างสม่ำเสมอ

ควรกำหนดรายละเอียดในการสแกนอย่างสม่ำเสมอ เพื่อที่จะแน่ใจได้ว่าเครื่องจะปลอดภัยจากไวรัสเสมอ

ขั้นตอนที่ 4 ตรวจสอบอีเมล์ที่ได้รับ

หากเป็นคนที่ต้องติดต่อสื่อสารผ่านอีเมล์เป็นประจำให้ระมัดระวังเมล์ และไฟล์ที่แนบมากับอีเมล์ เพราะอาจจะได้รับไวรัสคอมพิวเตอร์โดยไม่รู้ตัวทางที่ดีควรทำการสแกนไฟล์ที่แนบมาพร้อมกับอีเมล์ทุกครั้ง

ขั้นตอนที่ 5 พยายามตรวจสอบข้อมูลไวรัส

รู้หรือไม่ว่าไวรัสแต่ละตัวจะทำงานวันไหน ฉะนั้นต้องเก็บข้อมูลเกี่ยวกับวันที่ไวรัสจะทำงาน และตรวจสอบวิธีการทำงานของไวรัส รวมถึงเตรียมพร้อมในการป้องกันและวิธีกำจัดเพื่อจะได้รับมือได้ทัน

ขั้นตอนที่ 6 ควรตรวจสอบแผ่นดิสก์ทุกแผ่นที่นำมาใช้

ทุกครั้งที่มีการนำแผ่นดิสก์มาใช้งานก่อนใช้ทุกครั้ง ต้องตรวจสอบแผ่นให้แน่ใจว่าไม่มีไวรัส เพราะการแพร่กระจายไวรัสทางแผ่นก็เป็นที่นิยมอีกวิธีหนึ่ง