คอมพิวเตอร์ไวรัสเป็นชื่อเรียกสำหรับโปรแกรมประเภทหนึ่งที่มีพฤติกรรมคล้ายๆ กับไวรัสที่เป็นเชื้อโรค ที่สามารถแพร่เชื้อได้และมักทำอันตรายต่อสิ่งมีชีวิตที่มันอาศัยอยู่ แต่ต่างกันตรงที่ว่าคอมพิวเตอร์ไวรัสเป็นแค่เพียงโปรแกรมเท่านั้น ไม่ใช่สิ่งมีชีวิต

## ไวรัสคืออะไร

ไวรัส คือ โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในระบบคอมพิวเตอร์ได้ และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่นๆ ซึ่งอาจเกิดจากการนำเอาดิสก์ที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือระบบสื่อสารข้อมูล ไวรัสก็อาจแพร่ระบาดได้เช่นกัน

การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงว่าไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำคอมพิวเตอร์เรียบร้อยแล้ว เนื่องจากไวรัสก็เป็นแค่โปรแกรมๆ หนึ่ง การที่ไวรัสจะเข้าไปอยู่ในหน่วยความจำได้นั้นจะต้องมีการถูกเรียกให้ทำงานได้นั้น ยังขึ้นอยู่กับประเภทของไวรัสแต่ละตัว ปกติผู้ใช้มักจะไม่รู้ตัวว่าได้ทำการปลุกคอมพิวเตอร์ไวรัสขึ้นมาทำงานแล้ว

จุดประสงค์ของการทำงานของไวรัสแต่ละตัวขึ้นอยู่กับตัวผู้เขียนโปรแกรมไวรัสนั้น เช่น อาจสร้างไวรัสให้ไปทำลายโปรแกรมหรือข้อมูลอื่นๆ ที่อยู่ในเครื่องคอมพิวเตอร์ หรือแสดงข้อความวิ่งไปมาบนหน้าจอ เป็นต้น

## ประเภทของไวรัส

### บูตเซกเตอร์ไวรัส

Boot Sector Viruses หรือ Boot Infector Viruses คือ ไวรัสที่เก็บตัวเองอยู่ในบูตเซกเตอร์ของดิสก์ การใช้งานของบูตเซกเตอร์คือเมื่อเครื่องคอมพิวเตอร์เริ่มทำงานขึ้นมาตอนแรก เครื่องจะเข้าไปอ่านบูตเซกเตอร์โดยในบูตเซกเตอร์จะมีโปรแกรมเล็กๆไว้ใช้ในการเรียกระบบปฏิบัติการขึ้นมาทำงานอีกทีหนึ่ง บูตเซกเตอร์ไวรัสจะเข้าไปแทนที่โปรแกรมดังกล่าว และไวรัสประเภทนี้ ถ้าไปติดอยู่ในฮาร์ดดิสก์ โดยทั่วไปจะเข้าไปอยู่บริเวณที่เรียกว่า Master Boot Sector หรือ Parition Table ของฮาร์ดดิสก์นั้น ถ้าบูตเซกเตอร์ของฮาร์ดดิสก์ใดมีไวรัสประเภทนี้ติดอยู่ ทุกๆ ครั้งที่บูตเครื่องขึ้นมาโดย พยายามเรียกดอสจากดิสก์นี้ ตัวโปรแกรมไวรัสจะทำงานก่อนและจะเข้าไปฝังตัวอยู่ในหน่วยความจำเพื่อเตรียมพร้อมที่จะทำงานตามที่ได้ถูกโปรแกรมมา แล้วตัวไวรัสจึงค่อยไปเรียกดอสให้ขึ้นมาทำงานต่อไป ทำให้เหมือนไม่มีอะไรเกิดขึ้น

### โปรแกรมไวรัส

Program Viruses หรือ File Intector Viruses เป็นไวรัสอีกประเภทหนึ่งที่จะติดอยู่กับโปรแกรม ซึ่งปกติก็คือ ไฟล์ที่มีนามสกุลเป็น COM หรือ EXE และบางไวรัสสามารถเข้าไปติดอยู่ในโปรแกรมที่มีนามสกุลเป็น sys และโปรแกรมประเภท Overlay Programs ได้ด้วย โปรแกรมโอเวอร์เลย์ปกติจะเป็นไฟล์ที่มีนามสกุลที่ขึ้นต้นด้วย OV วิธีการที่ไวรัสใช้เพื่อที่จะเข้าไปติดโปรแกรมมีอยู่ 2 วิธี คือ การแทรกตัวเข้าไปอยู่ในโปรแกรม ผลก็คือหลังจากที่โปรแกรมนั้นติดไวรัสไปแล้ว ขนาดของโปรแกรมจะใหญ่ขึ้น หรืออาจมีการสำเนาตัวเองเข้าไปทับส่วนของโปรแกรมที่มีอยู่เดิม ดังนั้นขนาดของโปรแกรมจะไม่เปลี่ยนและยากที่จะซ่อมให้กลับเป็นดังเดิม การทำงานของไวรัสโดยทั่วไป คือ เมื่อมีการเรียกโปรแกรมที่ติดไวรัสอยู่ ตัวไวรัสจะเข้าไปหาโปรแกรมตัวอื่นๆ ที่อยู่ในดิสก์เพื่อทำสำเนาตัวเองลงไปทันทีแล้วจึงค่อยให้โปรแกรมที่ถูกเรียกนั้น ทำงานตามปกติต่อไป

### ม้าโทรจัน

ม้าโทรจัน (Trojan Horse) เป็นโปรแกรมที่ถูกเขียนขึ้นมาให้ทำตัวเหมือนว่าเป็นโปรแกรมธรรมดาทั่วๆ ไป เพื่อหลอกล่อผู้ใช้ให้ทำการเรียกขึ้นมาทำงาน แต่เมื่อถูกเรียกขึ้นมาแล้ว ก็จะเริ่มทำลายตามที่โปรแกรมมาทันที ม้าโทรจันบางตัวถูกเขียนขึ้นมาใหม่ทั้งชุด โดยคนเขียนจะทำการตั้งชื่อโปรแกรมพร้อมชื่อรุ่นและคำอธิบายการใช้งานที่ดูสมจริง เพื่อหลอกให้คนที่จะเรียกใช้ตายใจ จุดประสงค์ของคนเขียนม้าโทรจันอาจจะเช่นเดียวกับคนเขียนไวรัส คือ เข้าไปทำอันตรายต่อข้อมูลที่มีอยู่ในเครื่อง หรืออาจมีจุดประสงค์เพื่อที่จะล้วงเอาความลับของระบบคอมพิวเตอร์

ม้าโทรจันนี้อาจจะถือว่าไม่ใช่ไวรัส เพราะเป็นโปรแกรมที่ถูกเขียนขึ้นมาโดดๆ และจะไม่มีการเข้าไปติดตั้งในโปรแกรมอื่นเพื่อสำเนาตัวเอง แต่จะใช้ความรู้เท่าไม่ถึงการของผู้ใช้เป็นตัวแพร่ระบาดซอฟต์แวร์ที่มีม้าโทรจันอยู่ในนั้นและนับว่าเป็นหนึ่งในประเภทของโปรแกรมที่มีความอันตรายสูง เพราะยากที่จะตรวจสอบและสร้างขึ้นมาได้ง่าย ซึ่งอาจใช้แค่แบตช์ไฟล์ก็สามารถโปรแกรมประเภทม้าโทรจันได้

### โพลีมอร์ฟิกไวรัส

Polymorphic Viruses เป็นชื่อที่ใช้ในการเรียกไวรัสที่มีความสามารถในการแปรเปลี่ยนตัวเองได้ เมื่อมีการสร้างสำเนาตัวเองเกิดขึ้นซึ่งอาจได้ถึงหลายร้อยรูปแบบ ผลก็คือ ทำให้ไวรัสเหล่านี้ยากต่อการถูกตรวจจับ โดยโปรแกรมตรวจหาไวรัสที่ใช้วิธีการสแกนอย่างเดียว ไวรัสใหม่ๆในปัจจุบันที่มีความสามารถนี้เริ่มมีจำนวนเพิ่มมากขึ้นเรื่อยๆ

### สทีลต์ไวรัส

Stealth Viruses เป็นชื่อเรียกไวรัสที่มีความสามารถในการพรางตัวต่อการตรวจจับได้ เช่น ไฟล์อินเฟกเตอร์ ไวรัสประเภทที่ไปติดโปรแกรมใดแล้วจะทำให้ขนาดของโปรแกรมนั้นใหญ่ขึ้น ถ้าโปรแกรมไวรัสนั้นเป็นแบบสทีลต์ไวรัส จะไม่สามารถตรวจดูขนาดที่แท้จริงของโปรแกรมที่เพิ่มขึ้นได้ เนื่องจากตัวไวรัสจะเข้าไปควบคุมดอส เมื่อมีการใช้คำสั่ง DIR หรือโปรแกรมใดก็ตามเพื่อตรวจดูขนาดของโปรแกรม ดอสก็จะแสดงขนาดเหมือนเดิมทุกอย่างราวกับว่าไม่มีอะไรเกิดขึ้น

## อาการของเครื่องที่ติดไวรัส

สามารถสังเกตุการทำงานของเครื่องคอมพิวเตอร์ถ้ามีอาการดังต่อไปนี้อาจเป็นไปได้ว่าได้มีไวรัสเข้าไปติดอยู่ในเครื่องแล้ว อาการที่ว่านั้น ได้แก่

- ใช้เวลานานผิดปกติในการเรียกโปรแกรมขึ้นมาทำงาน
- ขนาดของโปรแกรมใหญ่ขึ้น
- วันเวลาของโปรแกรมเปลี่ยนไป
- ข้อความที่ปกติไม่ค่อยได้เห็นกลับถูกแสดงขึ้นมาบ่อยๆ
- เกิดอักษรหรือข้อความประหลาดบนหน้าจอ
- เครื่องส่งเสียงออกทางลำโพงโดยไม่ได้เกิดจากโปรแกรมที่ใช้อยู่
- แป้นพิมพ์ทำงานผิดปกติหรือไม่ทำงานเลย
- ขนาดของหน่วยความจำที่เหลือลดน้อยกว่าปกติ โดยหาเหตุผลไม่ได้
- ไฟล์แสดงสถานะการทำงานของดิสก์ติดค้างนานกว่าที่เคยเป็น
- ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้อยู่ๆ ก็หายไป
- เครื่องทำงานช้าลง
- เครื่องบูตตัวเองโดยไม่ได้สั่ง
- ระบบหยุดทำงานโดยไม่ทราบสาเหตุ
- เซกเตอร์ที่เสียมีจำนวนเพิ่มขึ้นโดยมีการรายงานว่าจำนวนเซกเตอร์ที่เสียมีจำนวนเพิ่มขึ้นกว่าแต่ก่อนโดยที่
- ยังไม่ได้ใช้โปรแกรมใดเข้าไปตรวจหาเลย

## การตรวจหาไวรัส

### การสแกน

โปรแกรมตรวจหาไวรัสที่ใช้วิธีการสแกน (Scanning) เรียกว่า สแกนเนอร์ (Scanner) โดยจะมีการดึงเอาโปรแกรมบางส่วนของตัวไวรัสมาเก็บไว้เป็นฐานข้อมูล ส่วนที่ดึงมานั้นเราเรียกว่า ไวรัสซิกเนเจอร์ (VirusSignature) และเมื่อสแกนเนอร์ถูกเรียกขึ้นมาทำงานก็จะเข้าตรวจหาไวรัสในหน่วยความทรงจำ บูตเซกเตอร์และไฟล์โดยใช้ไวรัสซิกเนเจอร์ที่มีอยู่

**ข้อดี**ของวิธีการนี้ก็คือ เราสามารถตรวจสอบซอฟต์แวร์ที่มาใหม่ได้ทันทีเลยว่าติดไวรัสหรือไม่ เพื่อป้องกันไม่ให้ไวรัสถูกเรียกขึ้นมาทำงานตั้งแต่เริ่มแรก

แต่วิธีนี้มี**จุดอ่อน**หลายข้อ คือ

1. ฐานข้อมูลที่เก็บไวรัสซิกเนเจอร์จะต้องทันสมัยอยู่เสมอ และครอบคลุมไวรัสทุกตัวมากที่สุดเท่าที่จะทำได้
2. เพราะสแกนเนอร์จะไม่สามารถตรวจจับไวรัสที่ยังไม่มีซิกเนเจอร์ของไวรัสนั้นเก็บอยู่ในฐานข้อมูลได้
3. ยากที่จะตรวจจับไวรัสประเภทโพลีมอร์ฟิก เนื่องจากไวรัสประเภทนี้เปลี่ยนแปลงตัวเองได้
4. จึงทำให้ไวรัสซิกเนเจอร์ที่ใช้สามารถนำมาตรวจสอบได้ก่อนที่ไวรัสจะเปลี่ยนตัวเองเท่านั้น
5. ถ้ามีไวรัสประเภทสทีลต์ไวรัส ติดอยู่ในเครื่องตัวสแกนเนอร์อาจจะไม่สามารถตรวจหาไวรัสนี้ได้
6. ทั้งนี้ขึ้นอยู่กับความฉลาดและเทคนิคที่ใช้ของตัวไวรัสและของตัวสแกนเนอร์เองว่าใครเก่งกว่า
7. เนื่องจากไวรัสมีตัวใหม่ๆ ออกมาอยู่เสมอๆ ผู้ใช้จึงจำเป็นต้องหาสแกนเนอร์ตัวที่ใหม่ที่สุดมาใช้
8. มีไวรัสบางตัวจะเข้าไปติดในโปรแกรมทันทีที่โปรแกรมนั้นถูกอ่าน และถ้าสมมติ
9. ว่าสแกนเนอร์ที่ใช้ไม่สามารถตรวจจับได้ และถ้าเครื่องมีไวรัสนี้ติดอยู่ เมื่อมีการ
10. เรียกสแกนเนอร์ขึ้นมาทำงาน สแกนเนอร์จะเข้าไปอ่านโปรแกรมทีละโปรแกรมเพื่อตรวจสอบ
11. ผลก็คือจะทำให้ไวรัสตัวนี้เข้าไปติดอยู่ในโปรแกรมทุกตัวที่ถูกสแกนเนอร์นั้นอ่านได้
12. สแกนเนอร์รายงานผิดพลาดได้ คือ ไวรัสซิกเนเจอร์ที่ใช้บังเอิญไปตรงกับที่มี
13. อยู่ในโปรแกรมธรรมดาที่ไม่ได้ติดไวรัส ซึ่งมักจะเกิดขึ้นในกรณีที่ไวรัสซิกเนเจอร์ที่ใช้มีขนาดสั้นไป
14. จะทำให้โปรแกรมดังกล่าวใช้งานไม่ได้อีกต่อไป

### การตรวจการเปลี่ยนแปลง

การตรวจการเปลี่ยนแปลง คือ การหาค่าพิเศษอย่างหนึ่งที่เรียกว่า เช็คซัม (Checksum) ซึ่งเกิดจากการนำเอาชุดคำสั่งและข้อมูลที่อยู่ในโปรแกรมมาคำนวณ หรืออาจใช้ข้อมูลอื่นๆ ของไฟล์ ได้แก่ แอตริบิวต์ วันและเวลา เข้ามารวมในการคำนวณด้วย เนื่องจากทุกสิ่งทุกอย่าง ไม่ว่าจะเป็นคำสั่งหรือข้อมูลที่อยู่ในโปรแกรม จะถูกแทนด้วยรหัสเลขฐานสอง เราจึงสามารถนำเอาตัวเลขเหล่านี้มาผ่านขั้นตอนการคำนวณทางคณิตศาสตร์ได้ ซึ่งวิธีการ

คำนวณเพื่อหาค่าเช็คซัมนี้มีหลายแบบ และมีระดับการตรวจสอบแตกต่างกันออกไป เมื่อตัวโปรแกรมภายในเกิดการเปลี่ยนแปลง ไม่ว่าไวรัสนั้นจะใช้วิธีการแทรกหรือเขียนทับก็ตาม เลขที่ได้จากการคำนวณครั้งใหม่จะเปลี่ยนไปจากที่คำนวณได้ก่อนหน้านี้

**ข้อด**ของการตรวจการเปลี่ยนแปลงก็คือ สามารถตรวจจับไวรัสใหม่ๆ ได้ และยังมีความสามารถในการตรวจจับไวรัสประเภทโพลีมอร์ฟิกไวรัสได้อีกด้วย แต่ก็ยังยากสำหรับสทีลต์ไวรัส ทั้งนี้ขึ้นอยู่กับความฉลาดของโปรแกรมตรวจหาไวรัสเองด้วยว่า จะสามารถถูกหลอกโดยไวรัสประเภทนี้ได้หรือไม่ และมีวิธีการตรวจการเปลี่ยนแปลงนี้จะตรวจจับไวรัสได้ก็ต่อเมื่อไวรัสได้เข้าไปติดอยู่ในเครื่องแล้วเท่านั้น และค่อนข้างเสี่ยงในกรณีที่เริ่มมีการคำนวณหาค่าเช็คซัมเป็นครั้งแรก เครื่องที่ใช้ต้องแน่ใจว่าบริสุทธิ์พอ คือต้องไม่มีโปรแกรมใดๆ ติดไวรัส มิฉะนั้นค่าที่หาได้จากการคำนวณที่รวมตัวไวรัสเข้าไปด้วยซึ่งจะลำบากภายหลังในการที่จะตรวจหาไวรัสตัวนี้ต่อไป

## การเฝ้าดู

เพื่อที่จะให้โปรแกรมตรวจจับไวรัสสามารถเฝ้าดูการทำงานของเครื่องได้ตลอดเวลานั้น จึงได้มีโปรแกรมตรวจจับไวรัสที่ถูกสร้างขึ้นมาเป็นโปรแกรมแบบเรซิเดนท์หรือ ดีไวซ์ไดรเวอร์ โดยเทคนิคของการเฝ้าดูนั้นอาจใช้วิธีการสแกนหรือตรวจการเปลี่ยนแปลง หรือสองแบบรวมกันก็ได้ การทำงานโดยทั่วไป ก็คือ เมื่อซอฟแวร์ตรวจจับไวรัสที่ใช้วิธีนี้ถูกเรียกขึ้นมาทำงานก็จะเข้าไปตรวจในหน่วยความจำของเครื่องก่อนว่ามีไวรัสติดอยู่หรือไม่ โดยใช้ไวรัสซิกเนเจอร์ที่มีอยู่ในฐานข้อมูล จากนั้นจึงค่อยนำตัวเองเข้าไปฝังอยู่ในหน่วยความจำ และต่อไปถ้ามีการเรียกโปรแกรมใดขึ้นมาใช้งาน โปรแกรมเฝ้าดูนี้ก็จะเข้าไปตรวจโปรแกรมนั้นก่อนโดยใช้เทคนิคการสแกนหรือตรวจการเปลี่ยนแปลงเพื่อหาไวรัส ถ้าไม่มีปัญหาก็จะอนุญาตให้โปรแกรมนั้นขึ้นมาทำงานได้ นอกจากนี้โปรแกรมตรวจจับไวรัสบางตัวยังสามารถตรวจสอบขณะที่มีการคัดลอกไฟล์ได้อีกด้วย

**ข้อด**ของวิธีนี้ คือ เมื่อมีการเรียกโปรแกรมใดขึ้นมา โปรแกรมนั้นจะถูกตรวจสอบก่อนทุกครั้งโดยอัตโนมัติ ซึ่งถ้าเป็นการใช้สแกนเนอร์จะสามารถทราบได้ว่าโปรแกรมใดติดไวรัสอยู่ ก็ต่อเมื่อทำการเรียกสแกนเนอร์นั้นขึ้นมาทำงานก่อนเท่านั้น

**ข้อเสีย**ของโปรแกรมตรวจจับไวรัสแบบเฝ้าดูก็คือ จะมีเวลาที่เสียไปสำหรับการตรวจหาไวรัสก่อนทุกครั้ง และเนื่องจากเป็นโปรแกรมแบบเรซิเดนท์หรือดีไวซ์ไดรเวอร์ จึงจำเป็นจะต้องใช้หน่วยความจำส่วนหนึ่งของเครื่องตลอดเวลาเพื่อทำงาน ทำให้หน่วยความจำในเครื่องเหลือน้อยลง และเช่นเดียวกับสแกนเนอร์ ก็คือ จำเป็นจะต้องมีการปรับปรุงฐานข้อมูลของไวรัสซิกเนเจอร์ให้ทันสมัยอยู่เสมอ

## คำแนะนำและการป้องกันไวรัส

- สำรองไฟล์ข้อมูลที่สำคัญ
- สำหรับเครื่องที่มีฮาร์ดดิสก์ อย่าเรียกดอสจากฟลอปปีดิสก์
- ป้องกันการเขียนให้กับฟลอปปีดิสก์
- อย่าเรียกโปรแกรมที่ติดมากับดิสก์อื่น
- เสาะหาโปรแกรมตรวจหาไวรัสที่ใหม่และมากกว่าหนึ่งโปรแกรมจากคนละบริษัท
- เรียกใช้โปรแกรมตรวจหาไวรัสเป็นช่วงๆ
- เรียกใช้โปรแกรมตรวจจับไวรัสแบบเฝ้าดูทุกครั้ง
- เลือกคัดลอกซอฟแวร์เฉพาะที่ถูกตรวจสอบแล้วในบีบีเอส
- สำรองข้อมูลที่สำคัญของฮาร์ดิสก์ไปเก็บในฟลอปปีดิสก์
- เตรียมฟลอปปีดิสก์ที่ไว้สำหรับให้เรียกดอสก์ขึ้นมาทำงานได้
- เมื่อเครื่องติดไวรัส ให้พยายามหาที่มาของไวรัสนั้น

## การกำจัดไวรัส

เมื่อแน่ใจว่าเครื่องติดไวรัสแล้ว ให้ทำการแก้ไขด้วยความใคร่ครวญและระมัดระวังอย่างมาก เพราะบางครั้งตัวคนแก้เองจะเป็นตัวทำลายมากกว่าตัวไวรัสจริงๆ เสียอีก การฟอร์แมตฮาร์ดดิสกใหม่อีกครั้งก็ไม่ใช่วิธีที่ดีที่สุดเสมอไป ยิ่งแย่ไปกว่านั้นถ้าทำไปโดยยังไม่ได้มีการสำรองข้อมูลขึ้นมาก่อน การแก้ไขนั้นถ้าผู้ใช้มีความรู้เกี่ยวกับไวรัสที่กำลังติดอยู่ว่าเป็นประเภทใดก็จะช่วยได้อย่างมาก และข้อเสนอแนะต่อไปนี้อาจจะมีประโยชน์ต่อท่าน

## บูตเครื่องใหม่ทันทีที่ทราบว่าเครื่องติดไวรัส

เมื่อทราบว่าเครื่องติดไวรัสให้ทำการบูตเครื่องใหม่ทันที โดยเรียกดอสขึ้นมาทำงานจากฟลอปปีดิสก์ที่ได้เตรียมไว้ เพราะถ้าไปเรียกดอสจากฮาร์ดดิสก์ เป็นไปได้ว่าตัวไวรัสอาจกลับเข้าไปในหน่วยความจำได้อีก เมื่อเสร็จขั้นตอนการเรียกดอสแล้ว ห้ามเรียกโปรแกรมใดๆ ก็ตามในดิสก์ที่ติดไวรัส เพราะไม่ทราบว่าโปรแกรมใดบ้างที่มีไวรัสติดอยู่

## เรียกโปรแกรมไวรัสขึ้นมาตรวจหาและทำลาย

ให้เรียกโปรแกรมตรวจจับไวรัส เพื่อตรวจสอบดูว่ามีโปรแกรมใดบ้างติดไวรัส ถ้าโปรแกรมตรวจหาไวรัสที่ใช้อยู่สามารถกำจัดไวรัสตัวที่พบได้ก็ให้ลองทำดู แต่ก่อนหน้านี้ให้ทำการคัดลอกเพื่อสำรองโปรแกรมาที่ติดไวรัสไปเสียก่อน โดยโปรแกรมจัดการไวรัสบางโปรแกรมสามารถสั่งให้ทำสำรองโปรแกรมที่ติดไวรัสไปเป็นอีกชื่อหนึ่งก่อนที่จะกำจัดไวรัส เช่น MSAV ของดอสเอง เป็นต้น

การทำสำรองก็เพราะว่า เมื่อไวรัสถูกกำจัดออกจากโปรแกรมไป โปรแกรมนั้นอาจไม่สามารถทำงานได้ตามปกติหรือทำงานไม่ได้เลยก็เป็นไปได้

วิธีการตรวจขั้นต้น คือ ให้ลองเปรียบเทียบขนาดของโปรแกรมหลังจากที่ถูกกำจัดไวรัสไปแล้วกับขนาดเดิม ถ้ามีขนาดน้อยกว่าแสดงว่าไม่สำเร็จ หากเป็นเช่นนั้นให้เอาโปรแกรมที่ติดไวรัสที่สำรองไว้ แล้วหาโปรแกรมจัดการไวรัสตัวอื่นมาใช้แทน แต่ถ้ามีขนาดมากกว่าหรือเท่ากับของเดิม เป็นไปได้ว่าการกำจัดไวรัสอาจสำเร็จ โดยอาจลองเรียกโปรแกรมตรวจหาไวรัสเพื่อทดสอบโปรแกรมอีกครั้ง

หากผลการตรวจสอบออกมาว่าปลอดเชื้อ ก็ให้ลองเรียกโปรแกรมที่ถูกกำจัดไวรัสไปนั้นขึ้นมาทดสอบการทำงานดูอย่างละเอียดว่าเป็นปกติดีอยู่หรือไม่อีกครั้ง ในช่วงดังกล่าวควรเก็บโปรแกรมนี้ที่สำรองไปขณะที่ติดไวรัสอยู่ไว้ เผื่อว่าภายหลังพบว่าโปรแกรมทำงานไม่เป็นไปตามปกติ ก็สามารถลองเรียกโปรแกรมจัดการไวรัสตัวอื่นขึ้นมากำจัดต่อไปในภายหลัง แต่ถ้าแน่ใจว่าโปรแกรมทำงานเป็นปกติดี ก็ทำการลบโปรแกรมสำรองที่ยังติดไวรัสอยู่ทิ้งไปทันที เป็นการป้องกันไม่ให้มีการเรียกขึ้นมาใช้งานภายหลังเพราะความบังเอิญได้