บทที่ 9
ภัยที่มากับอินเทอร์เน็ตและวิธีป้องกัน

เวอร์ม (Worm)

เวอร์มหรือมาโครไวรัส (Macro Virus) หมายถึงโปรแกรมซึ่งเป็นอิสระจากโปรแกรมอื่นๆ โดยจะแพร่กระจายผ่านเครือข่ายไปยังคอมพิวเตอร์และอุปกรณ์ ที่อยู่บนเครือข่าย การแพร่กระจาย จะคล้ายกับตัวหนอนที่เจาะไซหรือซอกซอนไปยังเครื่องคอมพิวเตอร์อื่นๆ และแพร่พันธุ์ด้วยการคัดลอก (Copy) ตนเอง ออกและส่งต่อผ่านเครือข่ายออกไป เวอร์มเป็นไวรัสชนิดหนึ่งที่ใช้มาโครโปรแกรม (Macro programming) ที่อยู่ในโปรแกรมประยุกต์ในการกระจายหรือแพร่พันธุ์ตัวมันเอง เช่น มาโครในโปรแกรมไมโครซอฟต์ เวอร์ด (Microsoft Word) หรือไมโครซอฟต์เอ็กเซล (Microsoft Excel) ดังนัน เมื่อมีการรันโปรแกรมสคริปต์ หรือมาโคร เวอร์มจะทำการแพร่กระจายตนเอง ตัวอย่างเช่น เวอร์มที่แนบมากับแฟ้มในอีเมล เมื่อผู้รับเปิด แฟ้มดังกล่าว เวอร์มจะทำเริ่ม ทำงานทันทีโดยจะคัดลอกตนเองและจะถูกส่งไปกับอีเมลไปให้ผู้อื่นต่อๆ ไป

โลจิกบอมบ์ (Logic bombs) หรือ ม้าโทรจัน (Trojan Horses)

หมายถึงโปรแกรมซึ่งถูกออกแบบมาให้มีการทำงานในลักษณะถูกตั้งเวลาเหมือนระเบิดเวลา โลจิกบอมบ์ชนิดที่มีชื่อเสียงหรือมักกล่าวถึง มีชื่อว่า **ม้าโทรจัน** ซึ่งมีที่มาจากมหากาพย์เมืองทรอยใน อดีตของโฮมเมอร์ และถูกนำมาประยุกต์ใช้เป็นชื่อของโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้แฝง

ตัวเองเข้าไปในระบบและจะทำงานโดยการดักจับเอารหัสผ่านเข้าสู่ระบบต่างๆ และส่งกลับไปยังเจ้าของ
หรือผู้ส่ง เพื่อบุคคลดังกล่าวสามารถเข้าใช้หรือโจมตีระบบในภายหลัง
โปรแกรมม้าโทรจันสามารถแฝง
มาได้ในหลายรูปแบบ อาทิเช่น เกมส์ บัตรอวยพร หรือจดหมายอิเล็กทรอนิกส์
โปรแกรมม้าโทรจันจะดู
เสมือนว่าเป็นโปรแกรมที่มีประโยชน์
แต่ในความเป็นจริงม้าโทรจันมีวัตถุประสงค์เพื่อทำลายโปรแกรม
ต่างๆ ในระบบคอมพิวเตอร์ เรามักเรียกการทำงานของม้าโทรจันว่า
“ปฏิบัติการเพื่อล้วงความลับ” เมื่อ
โปรแกรมม้าโทรจันถูกโหลดเข้าไปในระบบคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง
ม้าโทรจันจะทำการดักจับ
รหัสผ่านหรือข้อมูลที่ใช้ในการ Login ของผู้ใช้ระบบฯ
เพื่อนำข้อมูลดังกล่าวไปใช้ในการเจาะเข้าไปในระบบ
คอมพิวเตอร์ต่อไป โปรแกรมม้าโทรจันไม่ได้ถูกออกแบบมาเพื่อทำลายระบบ
หรือสร้างความเสียหายต่อ
ระบบคอมพิวเตอร์ ม้าโทรจันต่างจากไวรัส
และหนอนคือมันไม่สามารถทำสำเนาตัวเองและแพร่กระจาย
ตัวเองได้ แต่มันสามารถที่จะอาศัยตัวกลาง ซึ่ง อาจเป็นโปรแกรมต่างๆ
จดหมายอิเล็กทรอนิกส์ หรือการไป
โหลดไฟล์จากแหล่งต่างๆ เมื่อเรียกใช้งานไฟล์เหล่านี้
โปรแกรมม้าโทรจันก็จะทำงานและจะเปิดช่องทาง
ต่างๆ ให้ผู้บุกรุกเข้าโจมตีระบบได้
ในทำนองเดียวเหตุการณ์ในอดีตที่ชาวกรีกทำกับชาวเมืองทรอย

ข่าวไวรัสหลอกลวง (Hoax)

เป็นไวรัสประเภทหนึ่งซึ่งมาในรูปของการสื่อสารที่ต้องการให้ผู้ใช้คอมพิวเต

อร์เข้าใจผิด มักถูกส่งมาในรูปแบบจดหมายอิเล็กทรอนิกส์
ข่าวไวรัสหลอกลวงมักมีผลต่อผู้ใช้คอมพิวเตอร์จำนวนมาก การส่ง
ข้อความต่อๆ กันไปผ่านทางโปรแกรมรับส่งข้อความ หรือห้องสนทนาต่างๆ
ซึ่งสามารถสร้างความวุ่นวาย
ให้เกิดขึ้น ได้มากหรือน้อยเพียงใดขึ้น กับ
เทคนิคและการวิธีการหรือจิตวิทยาของผู้สร้างข่าว โดยส่วนใหญ่
จดหมายอิเล็กทรอนิกส์ประเภทนี้จะมีหัวเรื่องที่น่าสนใจ
อาจมีการอ้างแหล่งข้อมูลซึ่งเป็นบริษัทหรือ
องค์กรขนาดใหญ่เพื่อสร้างความเชื่อมั่น
และเมื่อผู้รับจดหมายดังกล่าวทำการส่งต่อไปยังคนอื่นๆ ทำให้ดู
เหมือนมีความน่าเชื่อถือมากขึ้น
แนวทางในการป้องกันและแก้ไขไวรัสหลอกลวงได้แก่ เมื่อได้รับจดหมาย
ประเภทนี้ก็ ไม่ควรส่งต่อจดหมายอิเล็กทรอนิกส์ดังกล่าวไปถึงคนอื่นๆ
หรือควรตรวจสอบจากแหล่งข้อมูล
ที่ถูกต้องก่อนทำการส่งต่อไป

แนวทางหรือมาตรการในการป้องกัน (Security Measures)

1. การกำหนดแนวปฏิบัติหรือระเบียบปฏิบัติ(Procedures) และนโยบายทั่วๆ
ไปในองค์กร อาทิเช่น

- องค์กรมีนโยบายหรือมาตรการให้ผู้ใช้ระบบคอมพิวเตอร์ทุกคนต้องเปลี่ยนรหัสผ่าน
(Password) บ่อยๆ หรืออย่างน้อยปีละหนึ่งครั้ง
- มีการกำหนดสิทธิให้ผู้ใช้ระบบเข้าใช้ระบบในส่วนที่จำเป็นต้องเท่านั้น
- มีการกำหนดสิทธิให้ผู้ใช้ระบบสามารถเข้าถึงข้อมูลเฉพาะในส่วนของตนเองเท่านั้น
- องค์กรอาจมีการนำอุปกรณ์ตรวจจับทางชีวภาพ (Biometric devices) มาใช้ในการ
ควบคุมการเข้าใช้ระบบคอมพิวเตอร์

- มีการเข้ารหัสข้อมูลในระบบคอมพิวเตอร์
-
มีระเบียบปฏิบัติในการควบคุมอย่างชัดแจ้งในการใช้ระบบเทคโนโลยีสารสนเทศ
- ให้ความรู้อย่างสม่ำเสมอในเรื่องการรักษาความปลอดภัย
การเตรียมตัวและการป้องกัน
การบุกรุกของแฮกเกอร์(Hackers) หรือแครกเกอร์(Crakers)
รวมถึงขั้นตอนการดูแลรักษาระบบคอมพิวเตอร์เมื่อถูกบุกรุก
- องค์กรควรมีการดูแลและตรวจตราข้อมูล แฟ้มข้อมูล
รวมถึงการสำรองแฟ้มข้อมูลและ
ระบบคอมพิวเตอร์รวมถึงระบบเครือข่ายอย่างสม่ำเสมอ
- การเก็บข้อมูลหรือกิจกรรมต่างๆ
ที่เกิดขึ้นในระบบคอมพิวเตอร์ตลอดเวลา (Log files)
2. การป้องกันโดยซอฟต์แวร์ (Virus protection software)
ปัจจุบันมีซอฟต์แวร์ป้องกันไวรัสหลายชนิด
ทั้งแบบซอฟต์แวร์เชิงพาณิชย์และซอฟต์แวร์
ที่แจกฟรี อาทิเช่น
- ลายมือชื่ออิเล็กทรอนิกส์ (Digital signatures)
- การเข้าและถอดรหัส (Encryption)

ความรู้เบื้องต้นเกี่ยวกับ Phishing

Phishing ออกเสียงคล้ายกับ fishing
คือการหลอกลวงทางอินเทอร์เน็ตอย่างหนึ่ง โดยผู้ที่ทำการ
หลอกลวงซึ่ง เรียกว่า Phisher
จะใช้วิธีการปลอมแปลงอีเมลติดต่อไปยังผู้ใช้อินเตอร์เน็ต โดยหลอกให้
ผู้ใช้เข้าใจว่าเป็นจดหมายจากองค์กร หรือบริษัท
ห้างร้านที่ผู้ใช้ทำการติดต่อหรือเป็นสมาชิกอยู่ โดยใน
เนื้อหาจดหมายอาจเป็นข้อความหลอกว่ามีเหตุการณ์อย่างใดอย่างหนึ่งเกิดขึ้น
และต้องการให้ผู้ใช้ยืนยัน
ข้อมูลส่วนตัวอีกครั้ง ซึ่งก็จะเป็นข้อมูลส่วนตัวซึ่งเป็นความลับ และมีความสำคัญ
เช่น ชื่อผู้ใช้ระบบ

(Username) รหัสผ่าน(Password) หมายเลขบัตรประจำตัวประชาชน
ข้อมูลบัตรเครดิต ข้อมูลบัญชีธนาคาร
หากผู้ใช้ได้รับอีเมลลักษณะดังกล่าวและหลงเชื่อดำเนินการตามที่อีเมลดังกล่าวระบุ จะทำให้ผู้ที่สร้างอีเมล
หลอกลวงขึ้นมานี้ได้ข้อมูลความลับส่วนตัวของผู้ที่ตกเป็นเหยื่อไป
และสามารถนำข้อมูลดังกล่าวไป
ดำเนินการต่าง ซึ้งก็ให้เกิดความเสียหายต่อทรัพย์สินของผู้ที่ตกเป็นเหยื่อได้

ลักษณะของการหลอกลวงดังกล่าว สามารถทำให้ผู้ใช้หลงเชื่อได้ง่าย เนื่องจากผู้ใช้อาจเป็น
สมาชิกของบริษัทให้บริการอินเทอร์เน็ตหนึ่งๆ
หรืออาจเคยไปทำการสั่งซื้อสินค้าจากเว็บหนึ่งๆ หรืออาจ
เคยทำธุรกรรมใดเกี่ยวกับบัตรเครดิต หรือบัญชีธนาคารผ่านอินเทอร์เน็ต ซึ่งผู้หลอกลวงอาจส่งข้อมูลมา
แจ้งว่าจากการสั่งซื้อสินค้าที่เว็บใดเว็บหนึ่งที่ผู้ใช้สั่งไปติดปัญหาข้อมูลการชำระเงินและให้ผู้ใช้ยืนยันข้อมูล
บัตรเครดิตอีกครั้งโดยการหลอกลวงนี้ก็จะมีการสร้างลิงค์ไปยังเว็บที่ถูกสร้างเลียนแบบขึ้นมา (Spoofed Website) โดยมีลักษณะเหมือนกับเว็บของบริษัท
ห้างร้าน หรือองค์กรนั้น จริงๆ ซึ่งก็จะทำให้เหยื่อหลงเชื่อ ยิ่งขึ้น

วิธีป้องกันและรับมือกับ Phishing

1. ระวังอีเมลที่มีลักษณะในการขอให้ท่านกรอกข้อมูลส่วนตัวใดๆ หรือยืนยันข้อมูล
ส่วนตัวใดๆ โดยส่วนใหญ่เนื้อหาในจดหมายจะระบุว่าเป็นจดหมายเร่งด่วน ให้ดำเนินการกรอกข้อมูล
ส่วนตัวบางอย่าง หากพบอีเมลลักษณะดังกล่าว ให้ลบอีเมลดังกล่าวทันที และอาจใช้การโทรศัพท์ติดต่อกับ
ทางองค์กร บริษัทห้างร้านด้วยตนเองอีกทีหากมีข้อสงสัย
2. หากต้องการกระทำธุรกรรมใดๆ ควรไปที่_website โดยตรงโดยการพิมพ์ URL ใหม่

3. ไม่ควรคลิกที่ hyperlink ใดๆ หรือรันไฟล์ใดๆ ที่มากับอีเมล หรือโปรแกรมสนทนา
ต่างๆ จากบุคคลที่ไม่รู้จัก

4. ควรติดตั้ง โปรแกรมตรวจสอบไวรัส และ Firewall เพื่อป้องกันการรับอีเมลที่ไม่พึง
ประสงค์ หรือการสื่อสารจากผู้ที่ไม่ได้รับอนุญาต

5. ควรติดตั้ง โปรแกรมปรับปรุงช่องโหว่ (Patch) ของซอฟต์แวร์ต่างๆ ที่เราใช้งานอยู่
ตลอดเวลา

6. ในการกรอกข้อมูลส่วนตัวที่สำคัญใดๆ ที่เว็บไซต์หนึ่งๆ ควรตรวจสอบให้แน่ใจว่าเป็น
เว็บไซต์ที่ถูกต้องและปลอดภัย ซึ่งเว็บไซต์ที่ปลอดภัยจะใช้โปรโตคอล https:// แทน http://

7. ควรตรวจสอบข้อมูลบัญชีธนาคาร บัตรเครดิตต่างๆ ที่มีการใช้งานผ่านอินเทอร์เน็ต
เป็นประจำ

ความรู้เบื้องต้นเกี่ยวกับไฟร์วอลล์

มาตรการหนึ่งที่ใช้ต่อสู้กับไวรัสคือ ไฟร์วอลล์ อินเทอร์เน็ตมีความสำคัญต่อการดำเนินชีวิตของผู้คน
ในสังคมยุคโลกาภิวัตน์เป็นอย่างมาก โดยผู้คนเหล่านั้นต้องการเชื่อมต่อเครือข่ายของตนเองกับอินเตอร์เน็ต
เพื่อที่จะได้รับประโยชน์ต่าง ๆ เช่น เพื่อหาข้อมูล เพื่อทำการค้า แต่การกระทำดังกล่าวทำให้ใครก็ได้บน
อินเตอร์เน็ตสามารถเข้ามายังเครือข่ายนั้นๆ ได้ จึงเกิดปัญหาเรื่องความปลอดภัยของระบบเครือข่าย เช่น การถูกเจาะระบบ และขโมยข้อมูล

จากปัญหาดังกล่าวทำให้เราต้องมีวิธีการในการรักษาความปลอดภัย สิ่งที่สามารถช่วยลดความเสียงนี้ได้ก็คือ ไฟร์วอลล์

ไฟร์วอลล์ คือ รูปแบบของโปรแกรมหรืออุปกรณ์ที่ถูกจัดตั้ง
อยู่บนเครือข่ายเพื่อทำหน้าที่เป็น
เครื่องมือรักษาความปลอดภัยให้กับเครือข่ายภายใน (Intranet)
โดยป้องกันผู้บุกรุก(Intrusion) ที่มาจาก
เครือข่ายภายนอก (Internet)
หรือเป็นการกำหนดนโยบายการควบคุมการเข้าถึงระหว่างเครือข่ายสอง
เครือข่าย โดยสามารถกระทำได้โดยวิธีแตกต่างกันไป แล้วแต่ระบบ

ถ้าผู้บุกรุกมาจากจากเครือข่ายภายในระบบนี้จะป้องกันไม่ได้ สิงที่ป้องกัน
เช่น ไวรัสคอมพิวเตอร์
(Virus), หนอนคอมพิวเตอร์ (Worm), การโจมตีแบบ DoS (Denial of
Service), ม้าโทรจัน (Trojan Horse), ip spoofing ฯลฯ
โดยมีลักษณะการบุกรุก ดังนี้เช่น

- Virus จะแย่งใช้หรือทำลายทรัพยากรของคอมพิวเตอร์เช่น ไฟล์ข้อมูล,
แรม ฯ

- Worm จะแย่งใช้ทรัพยากรของคอมพิวเตอร์ เช่น
เขียนไฟล์ขยะลงบนฮาร์ดดีสก์ จนทำ
ให้ฮาร์ดดีสก์เต็ม

ไฟร์วอลล์ มีขีดความสามารถในการไม่อนุญาตการ Login
สำหรับผู้ใช้ที่ไม่มีสิทธิใPนการเข้าใช้งานในเครือข่าย
แต่ผู้ใช้ที่มีสิทธิ์ใช้งานจะมีสิทธิ์ใช้งานทั้ง ภายในและติดต่อภายนอกเครือข่ายได้
โดยจำกัด ข้อมูลจากภายนอกเครือข่าย ไม่ให้เข้ามาในเครือข่าย
นับเป็นจุดสังเกตการณ์ ตรวจจับและรักษาความ ปลอดภัยของเครือข่าย
เปรียบได้ดังยามที่ทำหน้าที่เฝ้าประตูเมือง

ความรู้เบื้องต้นเกี่ยวกับ Cookies

การทำงานของ Web Server ในบางครั้ง
ก็มีการบันทึกข้อมูลลงในเครื่องของผู้ใช้อีกฝั่งซึ่งเป็นไฟล์ที่
อ่านจะมีข้อมูลสำคัญ
จึงควรตระหนักถึงประเด็นนี้เพื่อปกป้องข้อมูลส่วนบุคคลให้ดี Cookie

คือแฟ้มข้อมูลชนิด Text ทีเว็บเซิร์ฟเวอร์
ทำการจัดเก็บไว้ที่ฮาร์ดดิสค์ของผู้ทีไปเรียกใช้งานเว็บเซิร์ฟเวอร์นั้น
ซึ่งข้อมูลที่อยู่ในไฟล์ Cookie
นี้จะเป็นข้อมูลที่เราเข้าไปป้อนข้อมูลหรือมีการทำธุระกรรม ต่างๆ
ทีเว็บไซต์นั้นแล้วเว็บไซต์นั้น ได้มีการจัดเก็บหรือบันทึกข้อมูล เช่น ข้อมูล ชื่อ
นามสกุล ที่อยู่ อีเมล ชื่อผู้ใช้ รหัสผ่าน หรือแม้แต่ รหัสบัตรเครดิตการ์ด
ของเราเอาไว้ที่ไฟล์นี้ ซึ่งแต่ละเว็บไซต์ก็มีการจัดเก็บข้อมูลที่ แตกต่างกันไป
ซึ่งข้อมูลใน Cookie นี้ก็จะเป็นประโยชน์สำหรับเว็บไซต์ เมื่อเราเข้าไปใช้งาน
เว็บไซต์ในครั้งถัดๆไป ก็สามารถดูข้อมูลจาก Cookie
นี้เพื่อให้ทราบว่าผู้ที่เข้าใช้เป็นใคร และมีข้อมูลส่วนตัว อะไรบ้าง

เว็บไซต์ใช้ Cookies เพื่ออะไร

- เว็บไซต์สามารถใช้ประโยชน์จาก Cookie
เพื่อให้ทราบจำนวนผู้ที่เข้ามาใช้งานเว็บไซต์
เพราะผู้ใช้แต่ละคนจะถูกกำหนดหมายเลขไว้จากเว็บไซต์
ซึ่งทางเว็บไซต์ก็สามารถทราบได้ ว่าเป็นผู้ใช้เก่า
หรือใหม่ และผู้ใช้แต่ละคนเข้าใช้เว็บไซต์บ่อยแค่ไหน
- เว็บไซต์ที่มีการซื้อ ขายสินค้าผ่านทางเว็บไซต์
สามารถที่จะตรวจสอบได้ว่าผู้ใช้เลือกซื้อสินค้าอะไรไปบ้าง
ซึ่งผู้ใช้อาจยังไม่ต้องการจัดการเรื่องการสั่งซื้อในวันนั้น
ข้อมูลสินค้าที่ผู้ใช้เลือกไว้ก็ สามารถถูกจัดเก็บไว้ที่ Cookie ก่อน
เมื่อผู้ใช้เข้าใช้งานในครั้งถัดไปข้อมูลสินค้าที่เลือกไว้ ก็จะปรากฏขึ้น
มาให้โดยไม่ต้องทำการเลือกใหม่อีก

ข้อควรระวังที่เกี่ยวกับ Cookies

เนื่องจากข้อมูลที่ถูกเก็บใน Cookie อาจมีข้อมูลที่สำคัญเช่น
ข้อมูลบัตรเครดิต ข้อมูลที่อยู่ ข้อมูล
อีเมล ชื่อผู้ใช้ รหัสผ่าน
ซึ้งข้อมูลเหล่านี้ถูกส่งกลับไปมาระหว่างเครื่องผู้ใช้และเว็บไซต์ ซึ่งอาจมีการขโมย

ข้อมูลจากบุคคลอื่นได้ในระหว่างการถ่ายโอนไฟล์
ซึ่งผู้ใช้ควรระมัดระวังในการให้ข้อมูลต่างๆ แก่เว็บไซต์

ความรู้เบื้องต้นเกี่ยวกับ Spyware

- โปรแกรมที่แฝงเข้ามาในคอมพิวเตอร์ขณะที่ท่องอินเตอร์เน็ต
  เป็นโปรแกรมที่ถูกเขียนขึ้นมาสอดส่อง (สปาย)
  หรือดักจับข้อมูลการใช้งานเครื่องคอมพิวเตอร์ นอกจากนี้อาจจะมีการสำรวจโปรแกรม และไฟล์ต่างๆ ในเครื่องด้วย
- สปายแวร์
  นี้จะทำการส่งข้อมูลดังกล่าวไปในเครื่องปลายทางที่โปรแกรมได้ระบุเอาไว้ดังนั้นข้อมูลต่าง ๆ ในเครื่องของคุณอาจไม่เป็นความลับอีกต่อไป สปายแวร์อาจเข้ามาเพื่อโฆษณาสินค้าต่าง ๆ
  บางตัวก็สร้างความรำคาญเพราะจะเปิดหน้าต่างโฆษณาบ่อย ๆ แต่บางตัวร้ายกว่านั้น คือ ทำให้คุณใช้อินเตอร์เน็ทไม่ได้เลย

ประเภทของ Spyware สปายแวร์มีอยู่หลายประเภท โดยแบ่งเป็นประเภทต่างๆ ได้ดังนี้

1. Adware
   เป็นสปายแวร์ที่จะคอยส่งแบนเนอร์โฆษณามาที่คอมพิวเตอร์ของเรา
   สาเหตุที่เราจัดให้ Adware
   เป็นสปายแวร์ก็เพราะมีส่วนประกอบของโปรแกรมที่ทำให้สามารถติดตามข้อมูลของผู้ใช้และส่ง ข้อมูลนั้นออกไปที่อื่นได้
2. Dialer เป็นแอพพลิเคชันที่สั่งให้โมเด็มตัดการเชื่อมต่อกับ ISP แล้วหมุนโมเด็มไปยังผู้ให้บริการต่างประเทศ ทำให้ค่าโทรศัพท์สูงขึ้น
3. Hijacker เป็นสปายแวร์ที่สามารถเปลี่ยนแปลง Start Page และ Bookmark บนเว็บบราวเซอร์ ต่างๆ
4. BHO (Browser Helper Objects)
   เป็นสปายแวร์ที่ยัดเยียดฟังก์ชั่นที่ไม่พึงประสงค์ให้บนเว็บ บราวเซอร์

5.Toolbar

บางอย่างก็จัดเป็นสปายแวร์ที่ยัดเยียดเครื่องมือที่ไม่พึงประสงค์ให้บนเว็บบราวเซอร์ด้วย

อาการของเครื่องที่ติดไวรัสและสปายแวร์

อาการของการติดไวรัสนั้นมีมากมายขึ้นอยู่กับชนิดของไวรัสด้วย

อาการที่สามารถสังเกตได้ว่าเครื่อง

คอมพิวเตอร์ติดไวรัสและสปายแวร์หรือไม่มีดังต่อไปนี้

1.

เครื่องมีการรีสตาร์ทหรือเครื่องปิดตัวเองลงขณะที่กำลังใช้งานอยู่หรือเมื่อเปิดเครื่องแล้วไม่ สามารถบูตเข้าสู่วินโดวส์ได้

2. เกิดไฟล์ขึ้นเองโดยไม่ได้สร้างขึ้น เช่น Autorun.inf หรือไฟล์นามสกุล .vbs ปรากฏตามไดรฟ์ต่างๆ

3. เนื่อที่ในฮาร์ดดิสก์ลดลงโดยไม่ทราบสาเหตุโดยไม่ได้ติดตั้งโปรแกรมหรือนำข้อมูลมาลงไว้

4. วินโดวส์แสดงไดอะล็อกบ๊อกซ์ข้อความโดยไม่ทราบสาเหตุหรือมีโปรแกรมบางตัวทำงานเองโดย ไม่ได้เรียกใช้งาน

5. คอมพิวเตอร์ทำงานช้าอย่างผิดปกติทั้งๆ ที่ไม่ได้เปิดใช้โปรแกรมใดๆ

6. ไฟล์ข้อมูลมีขนาดใหญขึ้นมากแบบผิดปกติทุกครั้งที่ใช้งาน

7. เครื่องคอมพิวเตอร์เกิดอาการแฮงค์ (Hang) โดยไม่ทราบสาเหตุ

8. โปรแกรมป้องกันไวรัสไม่สามารถเปิดได้หรือเปิดโปรแกรมต่างๆ ไม่ได้หรือบางครั้งโปรแกรมที่ใช้ ประจำหายไป

9. มี Pop up ขึ้นมาบ่อยๆ ในขณะที่เราเข้าเว็บ หรือถึงแม้จะไม่ได้ต่อ internet

10. toolbar มีแถบปุ่มเครื่องมือเพิ่มขึ้น โดยที่เราไม่ได้ติดตั้งอะไรเสริมเลย

11 หน้า Desktop มีไอคอนประหลาดๆ เพิ่มขึ้น

บรรณานุกรม

เอกสารประกอบการเรียนการสอนจากคณาจารย์คณะวิทยาการสารสนเทศ มหาวิทยาลัยบูรพา, “คอมพิวเตอร์และเทคโนโลยีสารสนเทศในชีวิตประจำวัน”, 2553.