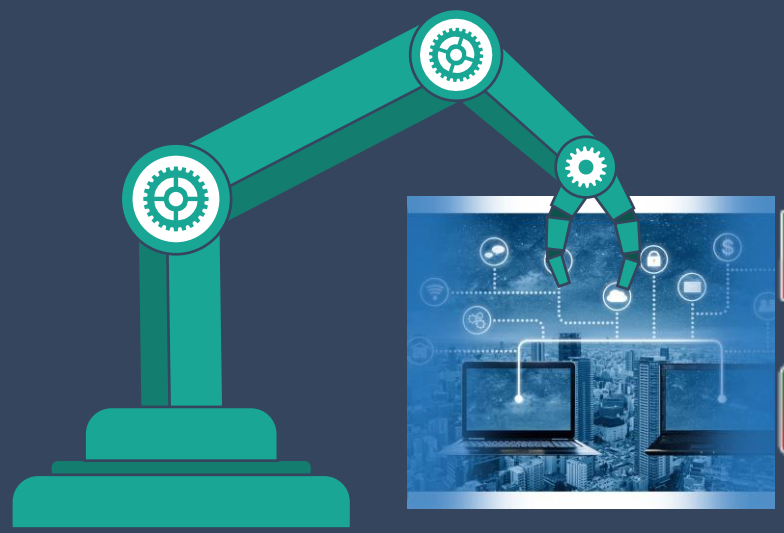
REG Network

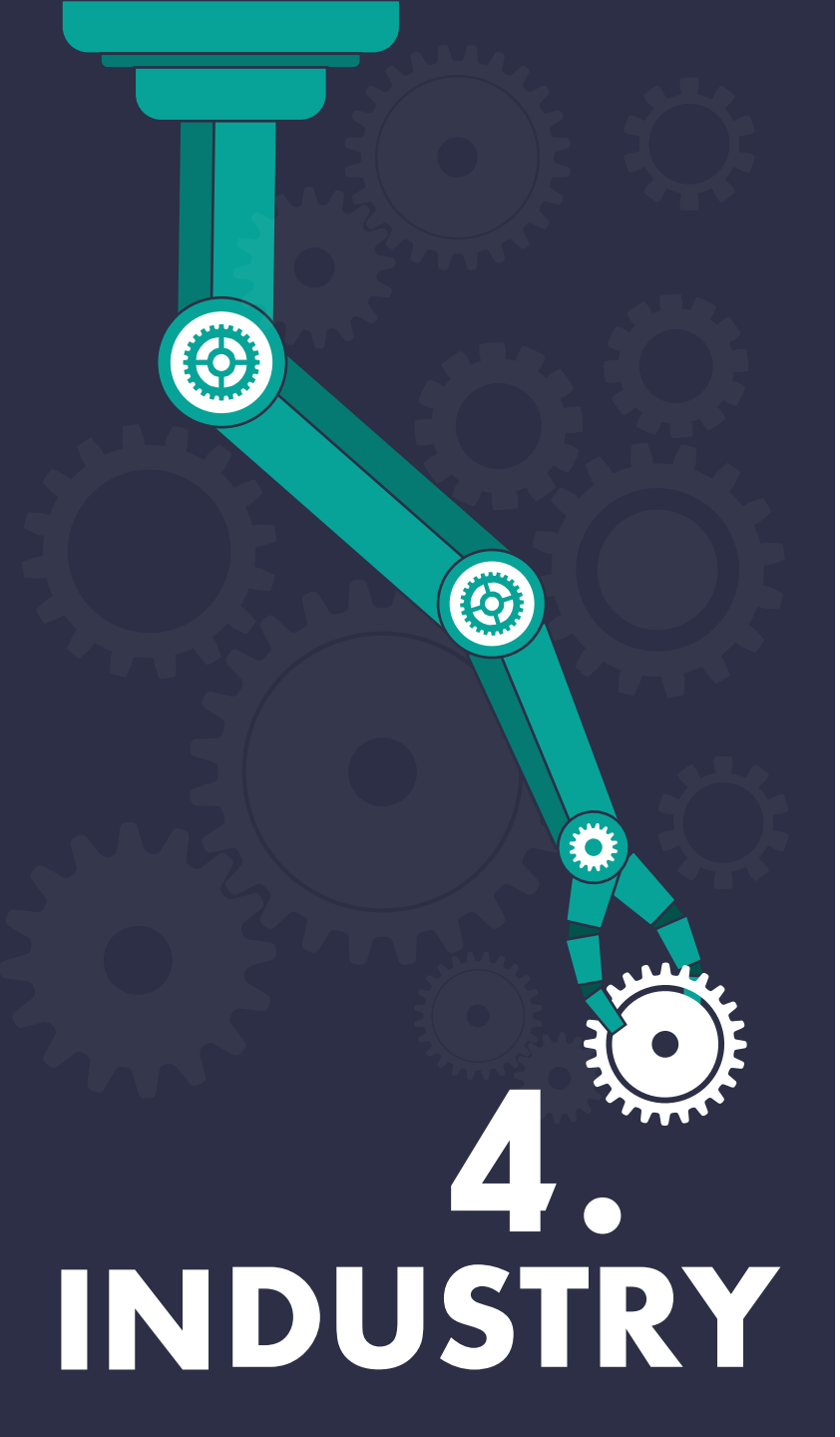
การดูแลรักษาระบบเครือข่ายและความปลอดภัยบนเครื่องคอมพิวเตอร์

network security and computer security



Network Security
Computer Security

การดูแลรักษาระบบเครือข่ายและความปลอดภัยบนเครื่องคอมพิวเตอร์



Network Security and Computer Security

01 ผังระบบแม่ข่าย และระบบเครือข่าย

02 ความเสี่ยงด้านระบบเครือข่าย

03 ภัยคุกคามต่อระบบคอมพิวเตอร์

04 การดูแลรักษาและความปลอดภัยบนระบบเครือข่าย

ความเสี่ยงด้านระบบเครือข่าย

ความเสี่ยงด้านระบบเครือข่าย หมายถึง ความเสี่ยงหรือภัยต่างๆที่เกิดขึ้นกับระบบเครือข่ายของ องค์กร ทั้งระบบอินทราเน็ต (Intranet)และอินเทอร์เน็ต (Internet) ซึ่งรวมถึงภัยที่มีสาเหตุมาจากปัญหาพื้นฐานของโพรโตคอล (Protocol) TCP/IP ด้วย เช่น ความเสี่ยงด้านกายภาพ ความเสี่ยงด้านระบบปฏิบัติการความเสี่ยงระบบแม่ข่าย ความเสี่ยงจากการบุกรุกระบบเครือข่าย และความเสี่ยงจากภัยคุกคามต่างๆ

ความเสี่ยงด้านระบบเครือข่าย

การบริหารจัดการความเสี่ยงด้านระบบเครือข่าย มีประเด็นหลัก ดังนี้

1. ความเสียหายที่เกิดจากระบบเครือข่าย การเฝ้าระวังและตรวจสอบระบบเครือข่าย และการจัดทำระบบการกำหนดสิทธิในการเข้าถึงระบบเครือข่ายได้การดำเนินการ ควรจัดให้มีระบบการติดตามและเฝ้าดูการใช้เครือข่ายภายในและการเข้าออก Internet ทุกวัน รวมทั้งการสร้าง Firewall เพื่อป้องกันการเข้าถึงและการโจมตีจากภายนอกให้ทุกเครื่องคอมพิวเตอร์ลูกข่าย(Client)ในเครือข่ายระบบฐานข้อมูล,ระบบ Web Server เป็นต้น

2. พัฒนาระบบงานด้านเครือข่าย โดยการพัฒนาบริหารควบคุม กำกับดูแล และบำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายสารสนเทศพื้นฐาน พัฒนาระบบการให้บริการเครือข่ายเพิ่มการรักษาและคุ้มครองความปลอดภัยข้อมูลผ่านระบบเครือข่าย

ความเสี่ยงด้านระบบเครือข่าย

การบริหารจัดการความเสี่ยงด้านระบบเครือข่าย (ต่อ)

3. เพิ่มประสิทธิภาพในการให้บริการระบบเครือข่ายคอมพิวเตอร์ให้มีความเสถียรและมีประสิทธิภาพรองรับกับปริมาณฐานข้อมูล และการเคลื่อนไหวของฐานข้อมูล

4. มีแผนการรักษาความปลอดภัยของระบบเครือข่าย (Network Security) วัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องไม่ให้เข้าถึง ล่วงรู้(access risk) หรือแก้ไขเปลี่ยนแปลง (integrity risk) ข้อมูล หรือ การทำงานของระบบเครือข่ายที่จะมีผลถึงระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง การป้องกันการบุกรุกผ่านระบบเครือข่าย มีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส มิให้เข้าถึงหรือสร้างความเสียหาย (availability risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหารายละเอียดเกี่ยวกับแนว ทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์เครื่องแม่ข่ายและระบบเครือข่าย

ภัยคุกคามต่อระบบคอมพิวเตอร์

ภัยคุกคามต่อระบบคอมพิวเตอร์ครอบคลุมทั้งการคุกคามทางระบบฮาร์ดแวร์ระบบซอฟต์แวร์และข้อมูล โดยสาเหตุของภัยคุกคามอาจจะมาจากทางกายภาพ เช่น อัคคีภัย ปัญหาวงจรไฟฟ้า ระบบสื่อสาร ความผิดพลาดของฮาร์ดแวร์ความผิดพลาดของซอฟต์แวร์หรือภัยคุกคามที่เกิดจากคน หรือผู้ใช้ระบบ เช่น การบุกรุกจากผู้ที่ไม่ได้รับอนุญาต หรือผู้ใช้ไม่เข้าใจระบบทำให้ระบบเกิดความเสียหาย ภัยคุกตามเหล่านี้เป็นสาเหตุให้ข้อมูลในระบบเสียหาย สูญหาย ถูกขโมย หรือแก้ไขบิดเบือน

ภัยคุกคามต่อระบบคอมพิวเตอร์

ภัยคุกคามต่อระบบคอมพิวเตอร์ยจำแนกภัยคุกคามทางระบบคอมพิวเตอร์แบ่งออกเป็น 3 ประเภท ดังนี้

1. ภัยคุกคามทางระบบฮาร์ดแวร์ (Hardware Security Threats) คือ ภัยที่มีต่อระบบการจ่ายไฟฟ้า ภัยที่เกิดจากการทำลายทางกายภาพโดยตรงต่อระบบคอมพิวเตอร์นั้นๆและภัยจากการลักขโมยโดยตรง

2. ภัยคุกคามทางระบบซอฟต์แวร์ (Software Security Threats) การลบซอฟต์แวร์หรือการลบเพียงบางส่วนของซอฟต์แวร์นั้น ๆ การขโมยซอฟต์แวร์ (Software Theft) การเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (Software Modification) และการขโมยข้อมูล (Information Leaks)

3.ภัยคุกคามที่มีต่อระบบข้อมูล (Data Threats) การที่ข้อมูลอาจถูกเปิดเผยโดยมิได้รับอนุญาต การที่ข้อมูลอาจถูกเปลี่ยนแปลงแก้ไขเพื่อผลประโยชน์โดยมิได้มีการตรวจสอบแก้ไข การที่ข้อมูลนั้นถูกทำให้ไม่สามารถนำมาใช้งานได้

ภัยคุกคามต่อระบบคอมพิวเตอร์

รูปแบบภัยคุกคามทางคอมพิวเตอร์

1. มัลแวร์ (Malware) คือความไม่ปกติทางโปรแกรม ที่สูญเสีย C (Confidentiality) I (Integrity) และ A (Availability) อย่างใดอย่างหนึ่ง หรือทั้งหมด สูญเสียความลับทางข้อมูล สูญเสียความไม่เปลี่ยนแปลงของข้อมูล สูญเสียเสถียรภาพของระบบปฏิบัติการ

2. ไวรัสคอมพิวเตอร์(Computer Virus) เป็นซอฟต์แวร์ประเภทที่มีเจตนาร้ายแฝงเข้ามาในระบบคอมพิวเตอร์โดยจะตรวจพบได้ยาก

3. หนอนคอมพิวเตอร์(computer worm) หนอนคอมพิวเตอร์จะแพร่กระจายโดยไม่ผ่านการใช้งานของผู้ใช้โดยมันจะคัดลอกและกระจายตัวมันเองข้ามเครือข่าย เช่น ระบบเครือข่าย หรืออินเทอร์เน็ต เป็นต้น

ภัยคุกคามต่อระบบคอมพิวเตอร์

4. ม้าโทรจัน (Trojan horse) โปรแกรมคอมพิวเตอร์ที่ถูกบรรจุเข้าไปในคอมพิวเตอร์เพื่อลอบเก็บข้อมูลของคอมพิวเตอร์เครื่องนั้น เช่น ข้อมูลชื่อผู้ใช้รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคลอื่น ๆ โดยส่วนใหญ่แฮกเกอร์จะส่งโปรแกรมเข้าไปในคอมพิวเตอร์เพื่อดักจับข้อมูลดังกล่าว แล้วนาไปใช้ในการเจาะระบบ

5. สปายแวร์(Spyware) ประเภทโปรแกรมคอมพิวเตอร์ที่บันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ

6. ประตูหลัง (Backdoor) รูรั่วของระบบรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ที่ผู้ออกแบบหรือผู้ดูแลระบบจงใจทิ้งไว้โดยเป็นกลไกล ลับทางซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้ข้ามผ่านการควบคุมความมั่นคงปลอดภัย แต่อาจเปิดทางให้ผู้ไม่ประสงค์ดีสามารถเข้ามาในระบบและก่อความเสียหายได้

ภัยคุกคามต่อระบบคอมพิวเตอร์

7. Rootkit โปรแกรมที่ออกแบบมาเพื่อซ่อนอ็อบเจ็กต์ต่างๆ เช่น กระบวนงาน ไฟล์หรือข้อมูล แม้จะเป็นโปรแกรมที่อาจไม่เป็นอันตรายเสมอไป แต่ก็ถูกนำมาใช้ในการซ่อนกิจกรรมที่เป็นอันตรายมากขึ้น

8. การโจมตีแบบ DoS/DDoS ความพยายามโจมตีเพื่อทาให้เครื่องคอมพิวเตอร์ปลายทางหยุดทางานหรือสูญเสียเสถียรภาพ หากเครื่องต้นทาง (ผู้โจมตี) มีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากผู้โจมตีมีมากและกระทำพร้อมๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่าการโจมตีแบบ Distributed Denial of Service (DDoS)

9. BOTNET ภัยคุกคามทางเครือข่ายคอมพิวเตอร์ด้วยมัลแวร์ทั้งหลายที่กล่าวในตอนต้นต้องการตัวนำทางเพื่อต่อยอดความเสียหาย และทำให้ยากแก่การควบคุมมากขึ้น ตัวนำทางที่ว่านี้ก็คือ Botnet ซึ่งก่อให้เกิดภัยคุกคามที่ไม่สามารถเกิดขึ้นได้เอง เช่น Spam, DoS/DDoS และ Phishing เป็นต้น

ภัยคุกคามต่อระบบคอมพิวเตอร์

10. Spam Mail หรืออีเมล์ขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ anti spam หรือหากใช้ฟรีอีเมล์เช่น hotmail, yahoo ก็จะมีโปรแกรมคัดกรองอีเมล์ขยะในชั้นหนึ่งแล้ว

11. Phishing คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิตโดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ตัวอย่างของการฟิชชิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทาให้คุณต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้น จะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง Phishing

ภัยคุกคามต่อระบบคอมพิวเตอร์

12. Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง

13. ข้อมูลขยะ (Spam) ภัยคุกคามส่วนใหญ่ที่เกิดจากอีเมล์หรือเรียกว่า อีเมล์ขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับโดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับ

14. Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์อาศัยโปรแกรมแฮก หลากรูปแบบ ที่หาได้ง่ายในโลกอินเทอร์เน็ต แถมยังใช้งานได้ง่าย ไม่ต้องเป็นผู้เชี่ยวชาญในคอมพิวเตอร์ก็สามารถเจาะระบบได้

15. ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกตามที่หนัก

ความปลอดภัยบนเครือข่าย

มาตรการความปลอดภัยขั้นพื้นฐาน (Basic Security Measures)

ระบบคอมพิวเตอร์ทุกระบบ จำเป็นต้องมีมาตรการความปลอดภัยขั้นพื้นฐาน ยกตัวอย่างง่าย ๆ เช่น คอมพิวเตอร์ที่ผู้คนส่วนใหญ่ใช้งาน มักจะมีโปรแกรมป้องกันไวรัสเพื่อป้องกันไวรัสเข้าสู่ระบบ และแพร่ระบาดบนเครือข่าย นอกจากนี้ อาจจำเป็นต้องล็อกเครื่องคอมพิวเตอร์เพื่อมิให้ผู้อื่นเข้ามาเปิดใช้งาน การล็อกกลอนประตู และการเข้ารหัสข้อมูล เพื่อป้องกันการลักลอยนำข้อมูลไปใช้งาน สิ่งเหล่านี้จัดเป็นการป้องกันความปลอดภัย ซึ่งก็มีหลายวีให้เลือกใช้งานตามความเหมาะสม อย่างไรก็ตาม สำหรับเนื้อหาต่อไปนี้จะทำให้เราๆได้ทราบถึงมาตรการด้านความปลอดภัยขั้นพื้น ฐานที่พึงมี ซึ่งแต่ละมาตรการก็จะมีเทคนิควิธีที่แตกต่างกันไป โดยสามารถแบ่งออกได้เป็น 7 ประเภทด้วยกันดังนี้

ความปลอดภัยบนเครือข่าย

มาตรการความปลอดภัยขั้นพื้นฐาน (Basic Security Measures)

1. ความปลอดภัยบนสภาพแวดล้อมภายนอก (External Security)
2. ความปลอดภัยด้านการปฏิบัติงาน (Operational Security)
3. การตรวจตราเฝ้าระวัง (Surveillance)
4. การใช้รหัสผ่านและระบบแสดงตัวตน (Passwords and ID Systems)
5. การตรวจสอบ (Auditing)
6. สิทธิ์การเข้าถึง (Access Rights)
7. การป้องกันไวรัส (Guarding Against Viruses)

การดูแลรักษาและความปลอดภัยบนระบบเครือข่าย

ในระบบเครือข่ายนั้นมีผู้ร่วมใช้เป็นจำนวนมาก ดังนั้นจึงมีทั้งผู้ที่ประสงค์ดีและประสงค์ร้ายควบคู่กันไป สิ่งที่พบเห็นกันบ่อยๆ ในระบบเครือข่ายก็คืออาชญากรรมทางด้านเครือข่ายคอมพิวเตอร์หลายประเภทด้วยกันเช่น พวกที่คอยดักจับสัญญาณผู้อื่นโดยการใช้เครื่องมือพิเศษจั๊มสายเคเบิลแล้วแอบบันทึกสัญญาณ พวกแคร๊กเกอร์(Crackers) ซึ่งได้แก่ ผู้ที่มีความรู้ความชำนาญด้านคอมพิวเตอร์แต่มีนิสัยชอบเข้าไปเจาะระบบคอมพิวเตอร์ผ่านเครือข่าย หรือไวรัสคอมพิวเตอร์ (Virus Computer)ซึ่งเป็นโปรแกรมคอมพิวเตอร์ที่เขียนขึ้นมาโดยมุ่งหวังในการก่อกวน หรือทำลายข้อมูลในระบบ

การดูแลรักษาและความปลอดภัยบนระบบเครือข่าย

การรักษาความปลอดภัยในระบบเครือข่ายมีวิธีการกระทำได้หลายวิธีคือ

1. ควรระมัดระวังในการใช้งาน การติดไวรัสมักเกิดจากผู้ใช้ไปใช้แผ่นดิสก์ร่วมกับผู้อื่น แล้วแผ่นนั้นติดไวรัสมา หรืออาจติดไวรัสจากการดาวน์โหลดไฟล์มาจากอินเทอร์เน็ต

2. หมั่นสำเนาข้อมูลอยู่เสมอ การป้องกันการสูญหายและถูกทำลายของข้อมูลที่ดีก็คือ การหมั่นสำเนาข้อมูลอย่างสม่ำเสมอ

3. ติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัส วิธีการนี้ สามารตรวจสอบ และป้องกันไวรัสคอมพิวเตอร์ได้ระดับหนึ่ง แต่ไม่ใช่เป็นการป้องกันได้ทั้งหมด เพราะว่าไวรัสคอมพิวเตอร์ได้มีการพัฒนาอยู่ตลอดเวลา

การดูแลรักษาและความปลอดภัยบนระบบเครือข่าย

4. การติดตั้งไฟร์วอลล์ (Firewall) ไฟร์วอลล์จะทำหน้าที่ป้องกันบุคคลอื่นบุกรุกเข้ามาเจาะเครือข่ายในองค์กรเพื่อขโมยหรือทำลายข้อมูล เป็นระยะที่ทำหน้าที่ป้องกันข้อมูลของเครือข่ายโดยการควบคุมและตรวจสอบการรับส่งข้อมูลระหว่างเครือข่ายภายในกับเครือข่ายอินเทอร์เน็ต

5. การใช้รหัสผ่าน (Username & Password) การใช้รหัสผ่านเป็นระบบรักษาความปลอดภัยขั้นแรกที่ใช้กันมากที่สุด เมื่อมีการติดตั้งระบบเครือข่ายจะต้องมีการกำหนดบัญชีผู้ใช้และรหัสผ่านหากเป็นผู้อื่นที่ไม่ทราบรหัสผ่านก็ไม่สามารถเข้าไปใช้เครือข่ายได้หากเป็นระบบที่ต้องการความปลอดภัยสูงก็ควรมีการเปลี่ยนรหัสผ่านบ่อย ๆ เป็นระยะๆ อย่างต่อเนื่อง

การดูแลรักษาและความปลอดภัยบนระบบเครือข่าย

อาการของเครื่องคอมพิวเตอร์เมื่อติดไวรัส

1. เครื่องทำงานช้าผิดปกติ
2. พื้นที่ในหน่วยความจำมีขนาดเล็กลงผิดปกติ
3. ไฟล์ข้อมูลมีขนาดใหญ่ผิดปกติ
4. ฮาร์ดดิสก์มีพื้นที่ลดลงอย่างไม่ทราบสาเหตุ
5. ใช้เวลาในการเรียกใช้โปรแกรมนานเกินไป
6. เครื่องคอมพิวเตอร์หยุดการทำงาน (Hang) โดยไม่ทราบสาเหตุ
7. บูทเครื่องจากฮาร์ดดิสก์ไม่ได้
8. เปิดไฟล์ข้อมูลไม่ได้
9. เปิดไฟล์ได้แต่เป็นภาษาแปลก ๆ
10. ไม่สามารถเรียกใช้โปรแกรมได้
11. เกิดอาการแปลก ๆตามคำสั่งของโปรแกรมไวรัส เช่น ปรากฏข้อความแปลก ๆ บนจอภาพ เป็นต้น

การดูแลรักษาและความปลอดภัยบนระบบเครือข่าย

การป้องกันไวรัส

1.ทุกครั้งที่นำซอฟต์แวร์ที่ไม่ทราบแหล่งที่ผลิตหรือได้รับแจกฟรีมาใช้ต้องตรวจสอบว่าปลอดไวรัสอย่างแน่นอนก่อนนำไปใช้เสมอ

2.ควรตรวจสอบทั้งฮาร์ดแวร์และซอฟต์แวร์อย่างสม่ำเสมออย่างน้อยวันละ1 ครั้ง

3.เตรียมแผ่นที่ไม่ได้ติดไวรัสไว้สำหรับบูทเครื่องเมื่อถึงคราวจำเป็น

4.ควรสำรองข้อมูลไว้เสมอ

5.พยายามสังเกตสิ่งผิดปกติที่เกิดขึ้นกับเครื่องอย่างสม่ำเสมอ เช่น การทำงานที่ช้าลง ขนาดของไฟล์ใหญ่ขึ้น ไดร์ฟมีเสียงผิดปกติ หรือหน้าจอแสดงผลแปลก ๆ

การดูแลรักษาและความปลอดภัยบนระบบเครือข่าย

การป้องกันไวรัส (ต่อ)

6.ไม่นำแผ่นดิสก์ไปใช้กับเครื่องคอมพิวเตอร์อื่น ถ้ายังไม่ได้ปิดแถบป้องกันการบันทึก (Write Protect)

7. ควรแยกแผ่นโปรแกรมและแผ่นข้อมูลออกจากกันโดยเด็ดขาด

8.ไม่อนุญาตให้คนอื่นมาเล่นเครื่องคอมพิวเตอร์ โดยปราศจากการควบคุมอย่างใกล้ชิด

9. ควรมีโปรแกรมป้องกันไวรัสใช้ตรวจสอบและป้องกัน

10. ควรใช้ฮาร์ดแวร์ป้องกันไวรัส

Thank You