บทที่ 9
การรักษาความปลอดภัยในระบบคอมพิวเตอร์

ความมุ่งหมายของบทเรียน

1. สามารถบอกถึงประเภทและลักษณะของอาชญากรรมคอมพิวเตอร์ได้
2. อธิบายถึงระบบการรักษาความปลอดภัย การตรวจสอบและการเข้าถึงข้อมูล
3. อธิบายถึงการกระทำผิดทางด้านกฎหมายลิขสิทธิ์
4. สามารถป้องกันการเกิดไวรัสคอมพิวเตอร์ต่อการใช้งานของตนเองได้
5. ปฏิบัติตามจรรยาบรรณของผู้ใช้อินเทอร์เน็ตและมีมารยาทในการใช้อินเทอร์เน็ต

เนื้อหาของบทเรียน

1. ความปลอดภัยและความเป็นส่วนตัวในระบบคอมพิวเตอร์
2. อาชญากรรมคอมพิวเตอร์ และทรัพย์สินทางปัญญา
3. การรักษาความปลอดภัยของข้อมูล (Data Security)
4. การป้องกันหนอนและไวรัส และการสำรองไฟล์ข้อมูล
5. จรรยาบรรณของนักคอมพิวเตอร์ และผู้ใช้อินเทอร์เน็ต

วิธีการสอนและกิจกรรม

1. บรรยาย
2. การศึกษาและค้นคว้าเพิ่มเติม
3. ทำแบบฝึกหัด

อุปกรณ์การสอน

1. เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบการนำเสนอ
2. ประมวลการสอน
3. เอกสารประกอบการสอน

การวัดและประเมินผล

1. การสังเกตพฤติกรรมผู้เรียน
2. การซักถาม
3. แบบฝึกหัด

ความปลอดภัยและความเป็นส่วนตัวในระบบคอมพิวเตอร์

ในอดีตเรื่องความปลอดภัย และความเป็นส่วนตัว สำหรับเครื่องคอมพิวเตอร์ เป็นสิ่งที่สามารถจัดการได้โดยง่าย เพียงแค่ใส่กุญแจประตู ห้องคอมพิวเตอร์ก็ถือว่าปลอดภัยแล้ว เพราะเนื่องจากในอดีตนั้น เครื่องคอมพิวเตอร์ ถูกติดตั้งและ ใช้งานในลักษณะระบบแบบรวมศูนย์ (Centralize)ซึ่งมีระบบการทำงานและเครื่องคอมพิวเตอร์อยู่เพียงหน่วยเดียว

แต่ปัจจุบัน ระบบคอมพิวเตอร์ได้เปลี่ยนแปลงไป ใครๆ ก็สามารถเชื่อมต่อไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ที่อยู่คนละสถานที่กัน ให้ติดต่อกันได้ อันเนื่องมาจาก ความสามารถของการสื่อสารข้อมูล ดังนั้นความปลอดภัย (Security) ของข้อมูลเป็นเรื่องที่สำคัญที่สุด ที่ควรคำนึงถึง เพราะว่าไฟล์ข้อมูลจำนวนมาก ที่จัดเก็บอยู่ในเครื่องคอมพิวเตอร์ ต้องได้รับการดูแล ให้ปลอดภัยจากการถูกทำลาย ความเสียหายที่เกิดจากอุบัติเหตุ ขโมยหรือแม้แต่การจารกรรม อันเนื่องมาจากการสื่อสารที่เข้าถึงกันได้อย่างสะดวกและง่ายดาย

จุดประสงค์ในการรักษาความปลอดภัย

ในการรักษาความปลอดภัยของระบบคอมพิวเตอร์มีจุดประสงค์สำคัญ 3 ประการคือ

1. การรักษาความลับของข้อมูล (Confidentiality)

เป็นการเก็บรักษาข้อมูลมิให้ถูกล่วงรู้โดยบุคคลที่ไม่ได้รับอนุญาต หรือสามารถเข้าถึงข้อมูลได้เฉพาะตามสิทธิที่ได้รับเท่านั้น

2. การรักษาความถูกต้องของข้อมูล (Integrity)

เป็นการเก็บรักษาข้อมูลมิให้ถูกเปลี่ยนแปลง แก้ไขโดยมิได้รับอนุญาต หรือเปลี่ยนแปลงโดยไม่สามารถตรวจสอบได้

3. การพร้อมใช้งานอย่างเต็มประสิทธิภาพ (Availability)

เป็นการทำให้ระบบคอมพิวเตอร์มีความสามารถพร้อมทำงานได้ตรงตามวัตถุประสงค์ ปริมาณ และเวลาที่ต้องการ ตามกรอบของการทำงานที่กำหนดไว้

อาชญากรรมคอมพิวเตอร์

แฮกเกอร์ (Hackers) หรือแครกเกอร์ (Cracker) คือ บุคคลที่พยายามเชื่อมต่อเข้าสู่ระบบคอมพิวเตอร์อย่างผิดกฎหมาย คำว่า แฮกเกอร์แต่เดิมนั้นมีความหมายในเชิงบวกคือหมายถึงบุคคลที่มีความเชี่ยวชาญอย่างมากทางด้านคอมพิวเตอร์ สามารถเข้าถึงระบบต่างๆ ได้ด้วยความสามารถเฉพาะตัว ส่วนคำว่า แครกเกอร์ จะเป็นความหมายในเชิงลบ คือมุ่งเน้นการทำลายระบบจริงๆ แต่ปัจจุบันความหมายของ แฮกเกอร์ ได้มีความ เข้าใจไปในทางลบด้วย คือถือว่าเป็นอาชญากรคอมพิวเตอร์ด้วย เพราะตามปกติ ผู้ที่เข้าถึงระบบของผู้อื่น คงไม่เป็นผู้ที่ประสงค์ดีต่อระบบนั้น หรือถ้าเป็นคนดีจริงทำไมจะต้องลอบเข้าไปในระบบอื่นด้วย

แต่สำหรับผู้ที่เป็น แฮกเกอร์จริงๆ ก็จะไม่ยอมรับตนเองว่าเป็น แครกเกอร์ ไปด้วยเพราะถือว่าศักดิ์ศรีต่างกัน อย่างไรก็ตามแล้ว ก็จะเรียกแฮกเกอร์ว่าเป็น นักเจาะระบบ

ลักษณะของอาชญากรรมคอมพิวเตอร์

1.การฉ้อโกงบัตรเครดิต (Credit Card Fraud)

2. การฉ้อโกงในการสื่อสารข้อมูล (Data Communications Fraud)

3. การเข้าถึงไฟล์ข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Access to Computer File)

4. การทำสำเนาซอฟต์แวร์คอมพิวเตอร์อย่างผิดกฎหมาย (Unlawful Copying of Copyright Software)

ความปลอดภัย

ความปลอดภัย (Security) เป็นระบบป้องกันที่ถูกออกแบบ เพื่อปกป้องระบบคอมพิวเตอร์และข้อมูลจากความเสียหาย ทั้งโดยเจตนาหรือโดยบังเอิญ หรือจากการเข้าใช้ระบบโดยบุคคลที่ไม่ได้รับอนุญาต การระบุตัวผู้ใช้ระบบและการเข้าถึงข้อมูล
โดยอาศัยวิธีการระบุตัวผู้ใช้ระบบและการเข้าถึงข้อมูล 4 ประเภทใหญ่ๆ ดังนี้

1. สิ่งที่คุณมี (What you have?)

2. สิ่งที่คุณรู้ (What you know?)

3. สิ่งที่คุณทำ (What you do?)

4. สิ่งที่คุณเป็น (What you are?)

ทรัพย์สินทางปัญญากับระบบคอมพิวเตอร์

ในระบบคอมพิวเตอร์นั้น ทรัพย์สินทางปัญญาที่มีความเกี่ยวข้องมากที่สุด คือ ลิขสิทธิ์ซอฟต์แวร์คอมพิวเตอร์ ซึ่งลิขสิทธิ์นั้น หมายถึง สิทธิแต่เพียงผู้เดียวของผู้สร้างสรรค์งานที่จะกระทำการใดๆ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น ผลงานเหล่านั้นเกิดจากการใช้สติปัญญาความสามารถและความวิริยะอุตสาหะในการสร้างสรรค์ขึ้น จึงควรได้รับการคุ้มครองตามกฎหมาย

นโยบายการให้ความคุ้มครองด้านลิขสิทธิ์ของประเทศไทยมีจุดมุ่งหมายเพื่อ

1. เพื่อคุ้มครองสิทธิประโยชน์อันชอบธรรมของผู้สร้างสรรค์

2. เพื่อกระตุ้นให้มีการสื่อสารหรือถ่ายทอดความคิด ความรู้ และข้อมูลในสังคมมากที่สุด

3. เพื่อกำหนดกฎเกณฑ์หรือ กติกาในการแสวงหาประโยชน์ ทางเศรษฐกิจการค้า จากผลงานสร้างสรรค์ด้านลิขสิทธิ์ทั้งในระดับ ภายในประเทศและระหว่างประเทศ

4. เพื่อส่งเสริมและรักษาผลงานสร้างสรรค์อันเป็นมรดกทางวัฒนธรรมของประเทศ

การรักษาความปลอดภัยของข้อมูล (Data Security)

1. การรักษาความปลอดภัยของขยะข้อมูล (Secured Waste)
2. การควบคุมในระบบคอมพิวเตอร์ (Internal Controls)
3. การตรวจสอบ (Auditor Checks)
4. การตรวจสอบประวัติผู้สมัครงาน (Applicant Screening)
5. การใช้รหัสผ่าน (Passwords)
6. ตัวป้องกันในซอฟต์แวร์ (Built-in Software Protection)

การป้องกันหนอนและไวรัส

หนอน (Worm) เป็นโปรแกรมที่ถ่ายเทตัวเอง จากคอมพิวเตอร์หนึ่ง ไปยังคอมพิวเตอร์อีกเครื่องหนึ่ง ผ่านทาง ระบบเครือข่าย และบันทึกตัวเองเป็นไฟล์ข้อมูล แยกต่างหากลงในที่เก็บข้อมูลเดียวกัน โปรแกรมนี้สามารถ เพิ่มจำนวนได้เอง อย่างควบคุมไม่ได้ ทำให้พื้นที่เก็บข้อมูลเต็มจนกระทั่งคอมพิวเตอร์ไม่สามารถทำงานต่อได้

ไวรัส (Virus) เป็นโปรแกรมที่สามารถดัดแปลงแก้ไขโปรแกรมอื่นๆ หรือส่งผ่านตัวเองจากโปรแกรมหนึ่งไปสู่อีก โปรแกรมหนึ่งเมื่อใช้งานโปรแกรมร่วมกันได้ นอกจากนี้ไวรัสยังสามารถเปลี่ยนหรือลบไฟล์ข้อมูล หรือขยายขนาดของไฟล์ข้อมูล หรือแสดงข้อความแปลกๆ ออกมาบนหน้าจอ หรือทำให้ภาพบนหน้าจอเกิดความผิดปกติ

แอนตี้ไวรัส (Antivirus) เป็นโปรแกรมคอมพิวเตอร์ที่หยุดการกระจายและกำจัดไวรัส แต่ก็มีโปรแกรม Retrovirus ที่สามารถต้านทานและอาจลบแอนตี้ไวรัส ได้ ปัจจุบันได้มีผู้พัฒนาโปรแกรมแอนตี้ไวรัส ขึ้นมาหลายตัว อาทิเช่น Norton Antivirus หรือ McAfee VirusScan เป็นต้น

วิธีการป้องกัน

1. ไม่ติดตั้งโปรแกรมจากแผ่นฟลอปปีดิสก์ที่ไม่ได้มาจากผู้ขายโดยตรง
2. ให้ระวังในการใช้ซอฟต์แวร์ที่มาจากบริษัทอื่นที่ไม่ได้ทำธุรกิจร่วมกัน
3. ใช้ซอฟต์แวร์ตรวจสอบไวรัส เพื่อตรวจสอบไฟล์ข้อมูลและเอกสารอื่นๆ ก่อนใช้งานหรือบันทึกข้อมูลลงในฮาร์ดดิสก์ทุกครั้ง
4. ถ้านำแผ่นฟลอปปีดิสก์ หรือ แฟลตเมมโมรีไปใช้กับเครื่องคอมพิวเตอร์เครื่องอื่นที่ไม่เคยใช้ ก็ต้องตรวจสอบไวรัสก่อนด้วย
5. ควรติดตั้งแอนตี้ไวรัส เพื่อใช้สแกนฮาร์ดดิสก์ทุกครั้งที่เปิดเครื่อง หรือตามระยะเวลาที่กำหนด ไม่เปิดอีเมล์นั้นดูหากไม่แน่ใจว่าใครเป็นผู้ส่งมาและให้ลบทิ้งไปทันที

การสำรองไฟล์ข้อมูล

ถึงแม้ว่าองค์กรทั้งหลาย ตระหนักถึงความสำคัญของข้อมูล และมีมาตรการในการสำรองข้อมูลอยู่เสมอ แต่ผู้ใช้ เครื่องคอมพิวเตอร์ส่วนบุคคล กลับมองข้ามสิ่งเหล่านี้ไป ซึ่งถ้าใช้ซอฟต์แวร์อย่างไม่ถูกต้อง หรือใส่ข้อมูลผิดพลาด อาจเป็นเวลานานกว่าจะทราบข้อผิดพลาด แต่บางครั้งซอฟต์แวร์เองก็ทำให้ข้อมูลเสียหาย บางครั้งฮาร์ดแวร์เอง ก็ทำงานผิดพลาด ทำให้ ไม่สามารถอ่านข้อมูลได้ หรืออาจเกิดอุบัติภัย เช่นไฟไหม้ น้ำท่วม หรืออาจลบไฟล์ข้อมูลโดยไม่ได้ตั้งใจ ในการแก้ไข ก็ต้องย้อนกลับไป ยังเวลาที่ข้อมูลยังถูกต้องอยู่

เพื่อเป็นการป้องกัน ข้อผิดพลาดต่างๆ ก็ควรสำรองข้อมูลอยู่เสมอ วิธีการสำรองข้อมูลอย่างง่ายๆ ทำได้โดยคัดลอก ไฟล์ข้อมูลต่างๆ จากฮาร์ดดิสก์ลงในแผ่นฟลอปปีดิสก์ หรืออาจใช้อีกวิธีที่ดีกว่าคือ การคัดลอกไฟล์ข้อมูลทั้งหมด ลงบนเทป ซึ่งจะปลอดภัย และรวดเร็วกว่า ในปัจจุบันหากไฟล์ข้อมูลที่มีขนาดใหญ่ ก็จะนิยมบันทึกลงแผ่นซีดีรอม ซึ่งปัจจุบัน มีราคาถูกลงมาก รวมทั้งอาจใช้ซอฟต์แวร์สำรองไฟล์ข้อมูลแบบอัตโนมัติหรือแบบวันต่อวันหรือตามต้องการก็ได้

นอกจากนี้อาจคัดลอกไฟล์ข้อมูลทั้งหมด ที่มีอยู่ในฮาร์ดดิสก์ตัวที่ใช้งานอยู่เป็นประจำ ลงบนฮาร์ดดิสก์อีกตัวหนึ่งที่เรียกว่า Mirror Hard Disk ก็ได้ แต่จะเสียค่าใช้จ่ายสูงพอสมควร

จรรยาบรรณของนักคอมพิวเตอร์

จรรยาบรรณของนักคอมพิวเตอร์ ประกอบด้วยข้อพึงปฏิบัติ และกฎข้อบังคับ แต่กฎข้อบังคับนั้นผูกมัดผู้ที่เป็นสมาชิกของ ACM (Association of Computer Machinery) หลักการทั่วไปมีดังนี้

1. สมาชิกจะต้องประพฤติตนอย่างซื่อสัตย์ตรงไปตรงมา เช่น จะต้องไม่นำข้อมูลข่าวสารใดๆ ที่เป็นความลับของนายจ้างหรือลูกค้า ไม่ว่าอดีตหรือปัจจุบันไปใช้โดยไม่ได้รับอนุญาตล่วงหน้า

2. สมาชิกควรพยายามเพิ่มพูนความรู้ ความสามารถของตน และศักดิ์ศรีของวิชาชีพ เช่น สมาชิกพยายามออกแบบ และพัฒนาระบบที่ทำงาน ตามที่ต้องการได้อย่างเพียงพอ และตรงต่อความจำเป็นในเชิงปฏิบัติของนายจ้างหรือลูกค้า

3. สมาชิกจะต้องรับผิดชอบในงานของตนเอง เช่น สมาชิกจะต้องไม่พยายามที่จะ ประกาศหรือจำกัดตัวเอง ออกจากความรับผิดชอบ ต่อลูกค้าในความผิดพลาดที่ตนได้ก่อขึ้น

4. สมาชิกจะต้องปฏิบัติตัวด้วยความรับผิดชอบทางวิชาชีพ

จรรยาบรรณของผู้ใช้อินเทอร์เน็ต

จรรยาบรรณของผู้ใช้อินเทอร์เน็ต ที่ควรปฏิบัติและถือเป็นมารยาทในการใช้อินเทอร์เน็ตมีอยู่ 10 ประการ ดังนี้

1. ต้องไม่ใช้คอมพิวเตอร์ทำร้ายหรือละเมิดผู้อื่น
2. ต้องไม่รบกวนการทำงานของผู้อื่น
3. ต้องไม่สอดแนมหรือแก้ไขเปิดดูในไฟล์ของผู้อื่น
4. ต้องไม่ใช้คอมพิวเตอร์เพื่อการโจรกรรมข้อมูลข่าวสาร
5. ต้องไม่ใช้คอมพิวเตอร์สร้างหลักฐานที่เป็นเท็จ
6. ต้องไม่คัดลอกโปรแกรมผู้อื่นที่มีลิขสิทธิ์
7. ต้องไม่ละเมิดการใช้ทรัพยากรคอมพิวเตอร์โดยที่ตนเองไม่มีสิทธิ์
8. ต้องไม่นำเอาผลงานของผู้อื่นมาเป็นของตน
9. ต้องคำนึงถึงสิ่งที่จะเกิดขึ้นกับสังคมอันติดตามมาจากการกระทำ
10. ต้องใช้คอมพิวเตอร์โดยเคารพกฎระเบียบ กติกามารยาท

บรรณานุกรม

Forouzan B. A , *Data Communication and Networking* , 4 rd Edition, MeGrow-Hill.

http://web.ku.ac.th/schoolnet/f-snet1.htm เข้าถึงเมื่อวันที่ 31 สิงหาคม 2550

http://www.moc.go.th/opscenter/cr/lic1.htm เข้าเมื่อวันที่ 25 มกราคม 2552

แบบฝึกหัดท้ายบท

1. Hacker แตกต่างจาก Cracker อย่างไร
2. การรักษาความปลอดภัยของข้อมูลประกอบด้วยวิธีการใดบ้าง
3. จงอธิบายถึงความแตกต่างระหว่างหนอนและไวรัสคอมพิวเตอร์
4. จงยกตัวอย่างการป้องกันไวรัสคอมพิวเตอร์
5. การสำรองข้อมูลมีความสำคัญอย่างไร
6. จรรยาบรรณของนักคอมพิวเตอร์มีความแตกต่างจากจรรยาบรรณของผู้ใช้อินเทอร์เน็ตอย่างไร