บทที่ 8
ความปลอดภัยและจริยธรรมทางด้านคอมพิวเตอร์

1. หัวข้อเนื้อหาประจำบท

8.1 แนวคิดเกี่ยวกับระบบรักษาความปลอดภัยในระบบคอมพิวเตอร์

8.2 การรักษาความปลอดภัยในองค์กร

8.3 การรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ต

8.4 การรักษาความปลอดภัยของข้อมูลส่วนบุคคลแนวโน้มของระบบรักษาความปลอดภัยในอนาคต

8.5 แนวโน้มของระบบรักษาความปลอดภัยในอนาคต

8.6 จริยธรรมทางด้านคอมพิวเตอร์

2. วัตถุประสงค์เชิงพฤติกรรม

1. อธิบายแนวคิดเกี่ยวกับระบบรักษาความปลอดภัยในระบบคอมพิวเตอร์
2. อธิบายบทบาทของระบบรักษาความปลอดภัยในองค์กร และ เครือข่ายอินเตอร์เน็ต ข้อมูลส่วนบุคคลแนวโน้มของระบบรักษาความปลอดภัยในอนาคต
3. อธิบายจริยธรรมทางด้านคอมพิวเตอร์

3. วิธีการสอนและกิจกรรมการเรียนการสอนประจำบท

1. วิธีการสอนแบบบรรยาย
2. วิธีการสอนแบบอภิปราย
3. ให้นักศึกษาทำแบบฝึกหัดท้ายบท

4. สื่อการเรียนการสอน

1. เอกสารประกอบการสอนวิชาเทคโนโลยีคอมพิวเตอร์และนวัตกรรมสื่อร่วมสมัย
2. สื่อประกอบการสอน Power Point
3. คำถามทบทวนและแบบฝึกหัด

5. การวัดผลและการประเมินผล

1. การทดสอบความรู้เบื้องต้นด้านเทคโนโลยีสารสนเทศ และคอมพิวเตอร์ก่อนเรียน
2. สังเกตจากการตอบคำถาม การซักถามและการอภิปราย
3. การตรวจการทำแบบฝึกหัดท้ายบท

บทที่ 8
ความปลอดภัยและจริยธรรมทางด้านคอมพิวเตอร์

ในปัจจุบันเทคโนโลยีต่างๆ ได้มีการพัฒนาขึ้นเป็นอย่างมาก ทั้งนี้เพื่ออำนวยความสะดวกสบายให้แก่มนุษย์ ซึ่งในเทคโนโลยีเหล่านั้นได้รวมไปถึงเทคโนโลยีการสื่อสารที่ทำให้ระยะทางและเวลาไม่เป็นอุปสรรคอีกต่อไป แต่ถึงแม้ว่าปัญหาเก่าๆ จะหมดสิ้นไป ปัญหาใหม่ที่เกิดขึ้นมากลับมีความรุนแรงมากกว่าปัญหาเดิมหลายเท่า ได้แก่ ปัญหาเกี่ยวกับความปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศ ซึ่งปัจจุบันเว็บไซต์หรือองค์กรธุรกิจส่วนใหญ่จะต้องมีระบบรักษาความปลอดภัยที่มีประสิทธิภาพมากยิ่งขึ้น เพื่อป้องกันภัยคุกคามจากผู้ประสงค์ร้ายต่อธุรกิจ ข้อมูลที่เป็นความลับขององค์กร หรือข้อมูลส่วนตัวของบุคคลทั่วไปที่องค์กรนั้นมีอยู่ มีปัญหาดังกล่าวเป็นผลเนื่องมาจากการขาดจริยธรรมในการใช้งานคอมพิวเตอร์ของบุคคลผู้มีความสามารถในด้านนี้ โดยนำไปใช้ในทางที่ผิด ดังนั้น เนื้อหาในบทนี้จึงขอกล่าวถึงความปลอดภัยในระบบคอมพิวเตอร์และจริยธรรมทางด้านคอมพิวเตอร์

8.1 แนวคิดเกี่ยวกับระบบรักษาความปลอดภัยในระบบคอมพิวเตอร์

แนวคิดเกี่ยวกับระบบรักษาความปลอดภัยในระบบคอมพิวเตอร์ เกิดขึ้นเนื่องจากบุคคลที่มีเจตนาร้ายเข้ามาทำลายข้อมูลภายในระบบคอมพิวเตอร์ด้วยรูปแบบแตกต่างกันไป ไม่ว่าจะเป็นการส่งไวรัสเข้าสู่ระบบคอมพิวเตอร์ซึ่งมีผลทำให้ข้อมูลต่างๆ เกิดความเสียหาย หรือการโจรกรรมข้อมูลที่เป็นความลับซึ่งมีความสำคัญด้านการแข่งขันทางธุรกิจ และความมั่นคงของชาติ หรือการละเมิดข้อมูลส่วนบุคคลของผู้อื่น เป็นต้น ดังนั้นตัวบุคคลและองค์กรต่างๆ จึงต้องมีการเพิ่มความสามารถในการรักษาความปลอดภัยให้กับระบบคอมพิวเตอร์ของตนให้มากขึ้น รวมถึงต้องตระหนักถึงหน้าที่และความรับผิดชอบในการใช้งานคอมพิวเตอร์ของตนเองที่มีต่อผู้อื่นด้วย

ผู้ที่มีความสามารถผ่านระบบรักษาความปลอดภัยเข้ามาได้มี 2 ประเภท ได้แก่ Hacker และ Cracker โดยจะมีวิธีในการเข้าใช้ระบบหลายวิธีด้วยกัน แต่โดยทั่วไปจะเข้าสู่ระบบโดยใช้การ Log In แบบผู้ใช้ทั่วๆ ไป ข้อแตกต่างระหว่าง Hacker และ cracker ก็คือ จุดประสงค์ของการลักลอบเข้าสู่ระบบคอมพิวเตอร์ผู้อื่น ดังนี้

Hacker คือ ผู้เชี่ยวชาญที่มีความรู้ความสามารถในการถอดรหัส หรือเจ้ารหัสของระบบรักษาความปลอดภัยของเครื่องคอมพิวเตอร์คนอื่นได้ โดยมีวัตถุประสงค์เพื่อทดสอบขีดความสามารถของระบบและของตนเองเท่านั้น หรืออาจจะทำไปตามหน้าที่ โดยไม่มีเจตนาที่จะลักลอบข้อมูลหรือมีเจตนาร้ายแต่อย่างใด เช่น ผู้ที่มีหน้าที่เกี่ยวข้องกับระบบรักษาความปลอดภัยของเครือข่ายหรือองค์กร เพื่อทำการทดสอบประสิทธิภาพของระบบว่ามีจุดบกพร่องใดเพื่อแก้ไขต่อไปเท่านั้น เป็นต้น

Cracker คือ ผู้เชี่ยวชาญที่มีความรู้ความสามารถในการถอดรหัส หรือเจาะรหัสของระบบรักษาความปลอดภัยของเครื่องคอมพิวเตอร์คนอื่นได้ โดยมีวัตถุประสงค์เพื่อบุกรุกระบบหรือเข้าสู่เครื่องคอมพิวเตอร์คนอื่นเพื่อขโมยข้อมูลหรือทำลายข้อมูลคนอื่นโดยผิดกฎหมาย

โดยภัยคุกคามที่เกิดขึ้นกับระบบรักษาความปลอดภัยของคอมพิวเตอร์สามารถแบ่งออกได้ 5 รูปแบบ ดังนี้

1. ภัยคุกคามแก่ระบบ

เป็นภัยคุมคามจากผู้มีเจตนาร้ายเข้ามาทำการปรับเปลี่ยน แก้ไข หรือลบไฟล์ข้อมูลสำคัญภายในระบบคอมพิวเตอร์ แล้วส่งผลให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ ทำให้ไม่สามารถใช้งานได้ ตัวอย่างเช่น Cracker แอบเจาะเข้าไปในระบบเพื่อลบไฟล์ระบบปฏิบัติการ เป็นต้น

2. ภัยคุกคามความเป็นส่วนตัว

เป็นภัยคุกคามที่ Cracker เข้ามาทำการเจาะข้อมูลส่วนบุคคล หรือติดตามร่องรอยพฤติกรรมของผู้ใช้งานแล้วส่งผลให้เกิดความเสียหายขึ้น ตัวอย่างเช่น การใช้โปรแกรมสปาย (Spyware) ติดตั้งบนเครื่องคอมพิวเตอร์ของบุคคลอื่น และส่งรายงานพฤติกรรมของผู้ใช้ผ่านทางระบบเครือข่ายหรือทางอีเมล์ไปยังบริษัทขายสินค้า เพื่อใช้เป็นข้อมูลในการส่งโฆษณาขายสินค้าต่อไป เป็นต้น

3. ภัยคุกคามต่อทั้งผู้ใช้และระบบ

เป็นภัยคุมคามที่ส่งผลเสียหายให้แก่ผู้ใช้งาน และเครื่องคอมพิวเตอร์เป็นอย่างมาก ตัวอย่างเช่น ใช้ Java Script หรือ Java Applet ทำการล็อคเครื่องคอมพิวเตอร์ไม่ให้ทำงาน หรือบังคับให้ผู้ใช้งานปิดโปรแกรมบราวเซอร์ขณะใช้งานอยู่ เป็นต้น

4. ภัยคุกคามที่ไม่มีเป้าหมาย

เป็นภัยคุกคามที่ไม่มีเป้าหมายแน่นอน เพียงแต่ต้องการสร้างจุดสนใจ โดยปราศจากความเสียหายที่จะเกิดขึ้น ตัวอย่างเช่น ส่งข้อความหรืออีเมล์มารบกวนผู้ใช้งานในระบบหลาย ๆ คน ในลักษณะที่เรียกว่า “Spam” เป็นต้น

5. ภัยคุกคามที่สร้างความรำคาญ

เป็นภัยคุกคามที่สร้างความรำคาญ โดยปราศจากความเสียหายที่จะเกิดขึ้น ตัวอย่างเช่น แอบเปลี่ยนการตั้งค่าคุณลักษณะในการทำงานต่างๆ ของเครื่องคอมพิวเตอร์ จากเดิมที่เคยกำหนดไว้โดยไม่ได้รับอนุญาต เป็นต้น

จากความสำคัญของข้อมูล และภัยคุกคามต่างๆ เหล่านี้ ทำให้สามารถแบ่งลักษณะการรักษาความปลอดภัยบนคอมพิวเตอร์ตามลักษณะการใช้งานได้ 3 ลักษณะ คือ การรักษาความปลอดภัยในองค์กร การรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ต และการรักษาความปลอดภัยของข้อมูลส่วนบุคคล

8.2 การรักษาความปลอดภัยในองค์กร

บุคคลผู้ไม่ประสงค์ดีต่อองค์กรมีอยู่ 2 กลุ่ม คือ ผู้ที่ทำงานอยู่ภายในองค์กรเอง และผู้ที่เป็นบุคคลภายนอกการรักษาความปลอดภัยของข้อมูลและระบบคอมพิวเตอร์ภายในองค์กรจึงต้องป้องกันผู้บุกรุกทั้ง 2 กลุ่มนี้ให้ได้ โดยมีวิธีการที่บุคคลเหล่านี้ใช้มีด้วยกันหลายวิธี แต่สามารถแบ่งเป็นประเภทได้ 2 ประเภท ได้แก่

1. การบุกรุกทางกายภาพ (เข้าถึงระบบได้โดยตรง) เช่น การเข้ามาคัดลอกข้อมูลใส่แผ่นดิสก์กลับไป การขโมยฮาร์ดดิสก์ออกไป การสร้างความเสียหายโดยตรงกับฮาร์ดแวร์ต่างๆ หรือการติดตั้งซอฟต์แวร์ที่ดักจับ Password ของผู้อื่นแล้วส่งไปให้ผู้บุกรุก เป็นต้น

2. การบุกรุกทางเครือข่ายคอมพิวเตอร์ เช่น การปล่อยไวรัสคอมพิวเตอร์เข้ามาทำลายระบบ หรือใช้ Spyware เพื่อขโมยข้อมูลส่วนตัวของผู้ใช้ ตลอดจนการเจาะเข้ามาทางช่องโหว่ของระบบปฏิบัติการโดยตรงเพื่อขโมย Password หรือข้อมูล เป็นต้น

ระบบรักษาความปลอดภัยที่ใช้ป้องกันการบุกรุกทางกายภาพที่นิยมใช้ คือ ระบบ Access Control ส่วนระบบที่ป้องกันการบุกรุกทางเครือข่าย คือ Firewall นอกจากนี้ยังใช้วิธีการ Backup ข้อมูลที่สำคัญเก็บเอาไว้ เพื่อใช้ในกรณีที่ข้อมูลเกิดความเสียหายจากสาเหตุใดๆ ก็ตาม

Access Control

Access Control คือ ระบบควบคุมการเข้าใจงาน เป็นวิธีการที่คิดค้นขึ้นมาเพื่อป้องกันการโจรกรรมข้อมูลจากบุคคลที่ไม่มีสิทธิ์ในการเข้าใช้ข้อมูลหรือระบบ (Unauthorized) โดยผู้ที่สามารถเข้าใช้ระบบโดยผ่านระบบ Access Control นี้ได้ จะต้องได้รับการอนุญาตหรือได้รับสิทธิ์ในการเข้าใช้งานก่อน (Authorize) แต่จะมีสิทธิ์ในการเข้าใช้ระบบไม่เท่ากัน เช่น บางคนอาจได้สิทธิ์เพียงเรียกใช้ข้อมูล แต่บางคนสามารถแก้ไขข้อมูลได้ เป็นต้น เมื่อได้รับสิทธิ์แล้ว หากต้องการเข้าใช้ระบบจะต้องมีการพิสูจน์ด้วยว่าบุคคลที่อ้างสิทธิ์นั้นเป็นผู้ที่ได้รับสิทธิ์จริงหรือไม่ วิธีการนี้เรียกว่า “Authentication” หากพิสูจน์แล้วปรากฏว่าบุคคลผู้นั้นเป็นผู้ที่ได้รับสิทธิจริง จึงจะสามารถเข้าใช้งานได้

ระบบควบคุมการเข้าใช้งานได้รับความนิยมในปัจจุบันนี้ แบ่งออกได้เป็น 3 รูปแบบ ดังนี้

ชื่อผู้ใช้และรหัสผ่าน (User Name and Password)

ชื่อผู้ใช้ (User Name หรือ User ID) คือ ตัวอักษรหรือตัวเลขซึ่งบ่งบอกว่าผู้ใช้เป็นใคร **ส่วน รหัสผ่าน (Password)** เป็นรหัสลับเฉพาะเพื่อเข้าใช้ระบบ ซึ่งเปรียบเสมือนกุญแจ (Key) ที่ใช้เปิดประตู การจะเข้าใช้คอมพิวเตอร์ที่มีระบบควบคุมการเข้า

ใช้งานในลักษณะนี้ ผู้ใช้จะต้องบอกชื่อผู้ใช้ซึ่งเป็นชื่อที่ขึ้นทะเบียนไว้กับระบบคอมพิวเตอร์ ระบบจะตรวจสอบข้อมูลของผู้ใช้เหล่านั้นจากบัญชีที่ผู้ใช้กรอกข้อมูลไว้เมื่อเริ่มต้น

โดยชื่อผู้ใช้จะต้องไม่ซ้ำกัน ซึ่งนั่นทำให้คอมพิวเตอร์สามารถบ่งบอกความแตกต่างของผู้ใช้แต่ละคนได้หลังจากกรอกชื่อผู้ใช้แล้วต้องป้อนรหัสผ่านด้วย หากชื่อผู้ใช้และรหัสผ่านไม่ตรงกับที่มีอยู่ในทะเบียน ระบบจะปฏิเสธการเข้าใช้งานทันที หรือหากมีการป้อนชื่อผู้ใช้หรือรหัสผ่านซ้ำกันในเวลาเดียวกัน จะมีผู้ใช้เพียงคนเดียวเท่านั้นที่สามารถใช้ระบบได้

โดยทั่วไปคอมพิวเตอร์จะอนุญาตให้ผู้ใช้และรหัสผ่านได้ด้วยตนเอง ซึ่งรหัสผ่านที่มีประสิทธิภาพในการป้องกันการเข้าใช้นั้นต้องประกอบไปด้วยลักษณะ 2 ประการ คือ

1. จำนวนของตัวอักษร หรือตัวเลขที่ประกอบกันเป็นรหัสผ่านนั้นต้องมีความยาวที่เหมาะสม คือไม่ต่ำกว่า 6 ตัวอักษร
2. รหัสผ่านที่ตั้งนั้นไม่ควรจะเป็นคำที่ผู้อื่นคาดเดาได้ง่าย เช่น วันเกิด หรือชื่อเล่น เป็นต้น หากรหัสผ่านมีคุณสมบัติทั้ง 2 ข้อนี้แล้วก็เป็นการยากที่ผู้บุกรุกจะสามารถเข้าใช้ระบบได้ ดังภาพที่ 8.1

ภาพที่ 8.1 แสดงภาพการป้อนชื่อผู้ใช้และรหัสผ่าน

Possessed Object รูปแบบหนึ่งในการควบคุมการเข้าใช้ระบบที่นิยมกันมากในปัจจุบัน การเข้าใช้คอมพิวเตอร์ที่มีระบบเช่นนี้ต้องใช้กุญแจ (Key) ซึ่งกุญแจในที่นี้จะหมายถึงวัตถุที่คอมพิวเตอร์อนุญาตให้ใช้ในการเข้าระบบได้ เช่น บัตร ATM หรือ KeyCard กุญแจเหล่านี้จะมี Personal Identification Number (PIN) หรือ รหัสตัวเลขซึ่งบ่งบอกว่ากุญแจเหล่านั้นเป็นของใคร และต้องมีรหัสผ่านคอยควบคุมการเข้าใช้ระบบ เช่น บัตร ATM เป็นตัวอย่างที่แสดงการทำงานของ PIN ได้ดีที่สุด การใช้บัตร ATM ต้องกดรหัสตัวเลข 4 ตัว เพื่อใช้งาน ซึ่งตัวเลขเหล่านั้นเป็นรหัสส่วนบุคคล เป็นต้น

อุปกรณ์ Biometric อุปกรณ์รักษาความปลอดภัยซึ่งใช้ลักษณะส่วนบุคคลเป็นรหัสผ่าน เช่น ลายนิ้วมือ ขนาดของฝ่ามือ หรือดวงตา เป็นต้น อุปกรณ์ลักษณะนี้จะแปลงลักษณะเฉพาะส่วนบุคคลเป็นรหัสตัวเลข (Digital Code) เพื่อเปรียบเทียบรหัสตัวเลขนั้นกับข้อมูลที่เก็บไว้ หากไม่ตรงกันคอมพิวเตอร์จะปฏิเสธการเข้าใช้ระบบ

อุปกรณ์สแกนนิ้วมือเป็นตัวอย่างของอุปกรณ์ Biometric ที่ใช้กันอย่างแพร่หลายในปัจจุบัน เครื่องสแกนลายนิ้วมือจะใช้การตรวจสอบความโค้งและรอยบากของลายนิ้วมือ ซึ่งแต่ละคนจะมีลักษณะไม่เหมือนกัน ทำให้ตรวนสอบได้ว่าเจ้าของลายนิ้วมือเป็นใคร มีสิทธิ์เข้าใช้ระบบหรือไม่ และที่สำคัญอุปกรณ์ชนิดนี้มีราคาถูกจึงได้รับความนิยมอย่างมาก ดังภาพที่ 8.2

ภาพที่ 8.2 แสดงการสแกนลายนิ้วมือเพื่อเข้าสู่ระบบ

นอกจากระบบควบคุมการเข้าใช้ข้อมูลดังกล่าวแล้ว ยังสามารถเลือกใช้ซอฟต์แวร์และผู้ให้บริการ ที่มีความสามารถในการตรวจจับและป้องกันการบุกรุกได้ดังต่อไปนี้

ซอฟต์แวร์ตรวจจับการบุกรุก (Intrusion Detection Software : IDS)

ซอฟต์แวร์ตรวจจับการบุกรุก จะคอยจับตาดูระบบและทรัพยากรของเครือข่าย แล้วรายงานให้ผู้ดูแลรักษาความปลอดภัยทราบเมื่อมีความเป็นไปได้ว่าจะมีผู้บุกรุกเข้ามา ตัวอย่างพฤติกรรมที่น่าสงสัยว่ามีผู้บุกรุกเข้ามา เช่น มีผู้พยายาม Log In เข้าใช้ข้อมูลหลายครั้ง แต่ไม่สามารถเข้าใช้ระบบได้ โดยพฤติกรรมดังกล่าวจะเกิดในช่วงเวลาที่ผิดปกติ เป็นต้น การใช้ IDS นี้ เป็นการเพิ่มการป้องกันอีกชั้นหนึ่งในกรณีที่ผู้บุกรุกได้ผ่านระบบรักษาความปลอดภัยชั้นนอก เช่น รหัสผ่าน ไฟร์วอลล์ เป็นต้น) เข้ามาแล้ว

ผู้ให้บริการจัดการความปลอดภัย (Managed Security Service Provider : MSSP)

ผู้ให้บริการจัดการความปลอดภัย จะคอยจับตาดูผู้บุกรุกและดูแลรักษาฮาร์ดแวร์และซอฟต์แวร์ ตลอดจน รักษาความปลอดภัยของเครือข่ายให้ เหมาะสำหรับองค์กรขนาดเล็กขนาดกลาง เนื่องจากต้นทุนในการจ้างผู้เชี่ยวชาญด้านการรักษาความปลอดภัยบนเครือข่ายเพื่อปกป้องการดำเนินงานทางธุรกิจอาจจะสูงเกินไป

การป้องกันและกำจัดไวรัสคอมพิวเตอร์ นอกจากการป้องกันผู้มีเจตนาร้ายที่ต้องการลักลอบเข้าสู่ระบบคอมพิวเตอร์ภายในองค์กรแล้ว องค์กรยังต้องรับมือกับ “ไวรัสคอมพิวเตอร์” ที่เกิดจากการใช้งานอินเตอร์เน็ตและการใช้งานโดยทั่วไปของบุคลากรในองค์กรเองอีกด้วย เป็นที่ทราบกันดีแล้วว่า ไวรัสคอมพิวเตอร์นั้นสามารถแพร่กระจายเข้าสู่คอมพิวเตอร์ได้อย่างง่ายดาย จากพฤติกรรมการใช้งานอินเตอร์เน็ต เช่น การดาวน์โหลดไฟล์ การรับ-ส่งอีเมล์และไฟล์ข้อมูล เป็นต้น พฤติกรรมดังกล่าวเกิดขึ้นโดยไม่ระมัดระวังประกอบกับหากไม่มีการติดตั้งโปรแกรม Anti-Virus ไว้ที่เครื่องคอมพิวเตอร์ของบุคลากรในองค์กรแล้ว ระบบคอมพิวเตอร์ในองค์กรย่อมมีความเสี่ยงต่อการติดไวรัสสูงมาก

สำหรับรายละเอียดของไวรัสคอมพิวเตอร์และการป้องกันนั้น สามารถศึกษาได้จากบทที่ 8 “ไว้รัสคอมพิวเตอร์และการป้องกัน”

ไฟร์วอลล์ (Firewall) ไฟร์วอลล์ คือ ระบบป้องกันภัยทางเครือข่าย (Network) เพื่อป้องกันมิให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาในระบบหรือส่งแพ็คเกจเข้ามาโจรกรรมข้อมูล สอดแนม หรือทำลายความมั่นคงในระบบเครือข่ายได้

ไฟร์วอลล์เป็นซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ที่จัดว่าเป็นทางผ่านในการเข้า – ออกของข้อมูล เพื่อป้องกันการแปลกปลอมของผู้ที่ไม่ได้รับสิทธิ์ในการเข้าถึงข้อมูล หรือเข้ามาในเครือข่ายขององค์กร นอกจากนี้ ยังใช้ในการควบคุมการใช้งานภายในเครือข่ายโดยกำหนดสิทธิ์ของแต่ละบุคคลได้อีกด้วย ระบบไฟร์วอลล์จึงเป็นสิ่งสำคัญในการใช้ป้องกันและรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ขององค์กร โดยกำหนดให้คอมพิวเตอร์เครื่องหนึ่งทำหน้าที่เป็นไฟร์วอลล์จากนั้นจึงเชื่อมต่อเครือข่ายอินทราเน็ตเข้ากับอินเตอร์เน็ต เพื่อตรวจสอบการเข้า – ออกของบุคคล

การป้องกันข้อมูลจากภาวะระบบล้มเหลว (System Failure) ระบบล้มเหลว หรือที่เรียกกันทั่วไปว่า “ระบบล่ม” สามารถสร้างความเสียหายให้แก่อุปกรณ์ และซอฟต์แวร์คอมพิวเตอร์ได้เป็นอย่างมาก ทั้งสามารถทำลายข้อมูลที่เก็บไว้ได้ ปัญหานี้มีที่มาจากหลายสาเหตุ เช่น ความบกพร่องของอุปกรณ์ต่างๆ ภัยธรรมชาติ หรือความผิดพลาดของมนุษย์ เป็นต้น

ปัญหาจากกระแสไฟฟ้า เป็นหนึ่งในสาเหตุสำคัญที่ทำให้ระบบล้มเหลว ทำให้เกิดความเสียหายแก่อุปกรณ์และข้อมูลรวมไปถึงระบบเครือข่ายด้วย ปัญหาจากกระแสไฟฟ้ามี 3 ลักษณะ ดังนี้

1. **ไฟฟ้ากระตุก (Noise)** เป็นอาการที่ไฟฟ้าเข้าสู่เครื่องคอมเตอร์ไม่สม่ำเสมอ เนื่องจากมีการใช้อุปกรณ์ไฟฟ้าอื่น ๆ ปัญหานี้เป็นเพียงการสร้างความรำคาญแก่ผู้ใช้คอมพิวเตอร์เท่านั้น
2. **ไฟฟ้าไม่เพียงพอ (Undervoltage)** โดยทั่วไปปัญหานี้จะทำให้ข้อมูลสูญหาย แต่ไม่สร้างความเสียหายแก่อุปกรณ์ อย่างไรก็ตาม สิ่งสำคัญของการทำงานก็คือ ข้อมูล จึงนับว่าเป็นความเสียหายที่ไม่ต้องการให้เกิดขึ้น
3. **ไฟฟ้ามากเกินไป (Overvoltage)** เกิดจาการที่ไฟฟ้าเข้าสู่เครื่องคอมพิวเตอร์มากเกินไป เช่น ฟ้าผ่า ปัญหาชนิดนี้จะสร้างความเสียหายแก่ข้อมูล ซอฟต์แวร์ และอุปกรณ์เป็นอย่างมาก

การสำรองข้อมูล (Backup)

การสร้างแฟ้มข้อมูลสำรอง เป็นวิธีการป้องกันความเสียหายของข้อมูลที่มีสาเหตุมาจากระบบล้มเหลว เนื่องจากเมื่อระบบล้มเหลวแล้วข้อมูลเกิดสูญหาย ก็สามารถนำข้อมูลที่ได้สำรองไว้นี้มาใช้แทนได้ สื่อหรืออุปกรณ์ที่ใช้ทำสำเนาข้อมูลควรเป็นวัสดุที่มีคุณภาพดีและมีความจุสูง เช่น CD-RW, Magnetic Tape, DVD-RW หรือ Zip Disk เป็นต้น

วัสดุที่เก็บสำเนาข้อมูลนั้นควรเก็บไว้ให้ไกลจากความร้อน ไฟ และควรห่างจากอุปกรณ์คอมพิวเตอร์ทุกชนิดในปัจจุบันนี้มีบริการเก็บรักษาสำเนาข้อมูลผ่านระบบเครือข่าย หรือเก็บในระบบอินเตอร์เน็ต โดยเมื่อครบ 1 ปี ผู้ให้บริการจะส่ง CD-ROM สำเนาข้อมูลมาให้ การทำสำเนาข้อมูลแบ่งออกเป็น 3 ระดับได้แก่

1. **Full Backup หรือ Archival Backup** เป็นการทำสำเนาทุกโปรแกรมและทุกแฟ้มข้อมูลที่มีอยู่ในคอมพิวเตอร์ การทำสำเนาข้อมูลแบบนี้เป็น

การป้องกันความเสียหายของข้อมูลที่ดีที่สุด แต่ใช้เวลาในการทำสำเนานานที่สุด

2. **Differential Backup** เป็นการทำสำเนาข้อมูลเฉพาะแฟ้มข้อมูลที่มีความเปลี่ยนแปลงหลังจากทำ Full Backup
3. **Incremental Backup** เป็นการทำสำเนาเฉพาะแฟ้มข้อมูลที่มีการเปลี่ยนแปลงหลังจากการทำ Incremental Backup ครั้งสุดท้าย

โดยทั่วไปจะทำ Full Backup ในทุกสุดสัปดาห์ หรือทุกสิ้นเดือน และในช่วงที่ไม่มีการทำ Full Backup ควรมีการทำ Differential Backup หรือ Incremental Backup ไว้ด้วย

8.3 การรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ต

ถึงแม้ว่าการใช้งานเครือข่ายอินเตอร์เน็ตจะมีประโยชน์สูง แต่ก็มีอันตรายแฝงอยู่มากมายหลายรูปแบบเช่นกัน เนื่องจากว่าทุกคนมีสิทธิ์ในการใช้งานเท่าเทียมกัน ทำให้มีบุคคลหลายประเภทเข้ามาใช้งาน และจุดประสงค์ของแต่ละบุคคลก็แตกต่างกัน รวมถึงผู้ที่มีความสามารถแต่มีจุดประสงค์ไปในทางไม่ดีด้วย (Cracker) ทำให้บนเครือข่ายอินเตอร์เน็ตจำเป็นจะต้องมีการรักษาความปลอดภัยที่มีประสิทธิภาพสูงเพื่อป้องกันการบุกรุกในรูปแบบต่างๆ รวมไปถึงการโจรกรรมข้อมูลด้วย

หัวใจสำคัญของการรักษาความปลอดภัยบนอินเตอร์เน็ต ก็คือ การรักษาข้อมูลต่างๆ ของผู้ใช้ ที่เข้ามาใช้บริการบนอินเตอร์เน็ต ดังนั้นจึงสามารถนำระบบรักษาความปอลดภัยในองค์กรเข้ามาประยุกต์ใช้ได้ แต่ก็ต้องมีการเพิ่มระบบรักษาความปลอดภัยบางอย่างเพื่อเพิ่มความมั่นใจให้แก่ผู้ใช้งาน เช่น การป้องกันเครื่องเซิร์ฟเวอร์จากการถูกโจมตี การเข้ารหัสข้อมูลที่รับ – ส่งบนเครือข่ายเพื่อไม่ให้ผู้อื่นรู้ข้อความที่ส่งติดต่อกัน เป็นต้น

ความปลอดภัยของเครื่องเซิร์ฟเวอร์

การโจมตีประเภทสั่งให้เซิร์ฟเวอร์ปฏิเสธการให้บริการ เป็นการโจมตีรูปแบบหนึ่ง ซึ่งจะส่งผลให้เครื่องคอมพิวเตอร์หรือระบบหยุดการทำงานโดยไม่ทราบสาเหตุ หรืออาจจะให้การทำงานเครื่องเพิ่มมากขึ้นจนกระทั่งผู้ใช้ไม่สามารถใช้งานได้ เช่น วิธีการโจมตีแบบ Distributed Denial of Service (DDoS) คือ การที่ผู้บุกรุกติดตั้ง “Agent” (ส่วนใหญ่มักเป็นโปรแกรมประเภท Trojan) ให้ทำงานในเครื่องที่ตนเองได้รับสิทธิ์เข้าใช้งาน เพื่อให้คอมพิวเตอร์เครื่องนั้นพร้อมที่จะรับคำสั่งต่อไป หลังจากที่ผู้บุกรุกสร้างเครื่องที่จะทำหน้าที่เป็น Agent ได้ตามจำนวนที่ต้องการแล้ว จะมีคอมพิวเตอร์อีกเครื่องหนึ่งทำหน้าที่เป็น “Handler” ทำการสั่งให้เครื่องที่เป็น Agent ทั้งหมดทำการโจมตีแบบ Denial of Service ไปยังระบบอื่นโดยเครื่อง Agent จะสร้างข้อมูลขยะขึ้นมาแล้วส่งไปที่เครื่องหรือระบบเป้าหมาย ดังนั้น เป้าหมายสุดท้ายของการโจมตีจึงไม่ใช้เครื่องคอมพิวเตอร์ของผู้ใช้โดยตรง แต่

เป็นคอมพิวเตอร์เครื่องอื่น โดยเครื่องคอมพิวเตอร์ของผู้ใช้เป็นเพียงเครื่องช่วยขยายขอบเขตในการโจมตีเท่านั้น

สามารถตรวจสอบการโจมตีแบบ DoS ได้ด้วยการใช้ไฟร์วอลล์ (Firewall) หรือซอฟต์แวร์ประเภทตรวจสอบการบุกรุก (Intrusion Detection System : IDS) เพื่อรายงานสภาวะการบุกรุกของการโจมตีดังกล่าวได้

ความปลอดภัยในการส่งข้อมูลผ่านเครือข่ายอินเตอร์เน็ต (Securing Internet Transactions)

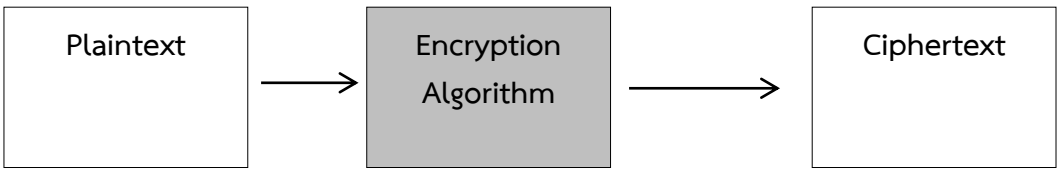
การรักษาความปลอดภัยของข้อมูลที่ส่งผ่านเครือข่ายอินเตอร์เน็ตที่นิยมใช้งานกันมากที่สุด คือ “การเข้ารหัส (Encryption)” ซึ่งระดับความปลอดภัยของการสื่อสารข้อมูลจะมีความแตกต่างกันขึ้นอยู่กับความสำคัญของข้อมูลนั้นการเข้ารหัสข้อมูลมีระดับความปลอดภัยหลายระดับ ตั้งแต่ 40-bit Encryption จนถึง 128-bit Encryption โดยที่จำนวนบิตในการเข้ารหัสยิ่งสูงจะทำให้ข้อมูลมีความปลอดภัยสูงขึ้นตามไปด้วย ดังนั้นข้อมูลที่มีความสำคัญมากๆ เช่น ข้อมูลทางการเงิน จะเข้ารหัสแบบ 128-bit Encryption

เว็บไซต์ที่ใช้วิธีการเข้ารหัสเพื่อป้องกันข้อมูลจะใช้ Digital Certification ร่วมกับ Security Protocol เพื่อทำให้ความปลอดภัยสูงขึ้น ซึ่งโดยทั่วไปโปรโตคอลที่นิยมใช้งานมีอยู่ 2 ชนิด คือ Secure Socket Layer (SSL) และ Secure HTTP (SHTTP) แต่ยังมีโปรโตคอล Secure Electronic Transaction (SET) อีกหนึ่งโปรโตคอลที่มีผู้คิดค้นขึ้นเพื่อความปลอดภัยในการชำระเงินด้วยบัตรเครดิตทางอินเตอร์เน็ต

การเข้ารหัส (Encryption)

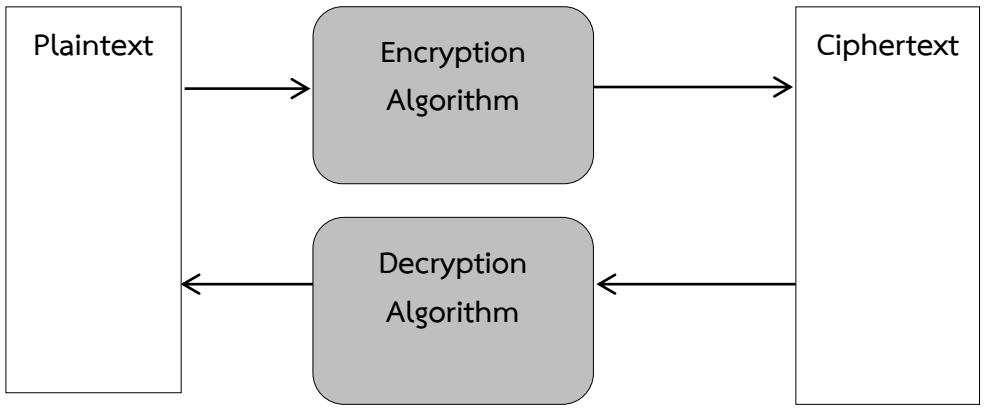
การเข้ารหัส เป็นวิธีการป้องกันข้อมูลจากการถูกโจรกรรมในขณะที่มีการรับและส่งข้อมูลผ่านทางเครือข่ายวิธีการนี้มีความน่าเชื่อถือได้มากกว่าการควบคุมการเข้าใช้งาน เนื่องจากข้อมูลทั้งหมดจะถูกแปลงเป็นรหัสที่ไม่สามารถอ่านได้ด้วยวิธีการปกติ (เรียกว่า “เข้ารหัส หรือ “Encrypt”) ดังนั้นแม้ว่าจะมีผู้โจรกรรมข้อมูลไปได้ แต่หากไม่สามารถถอดรหัส (Decrypt) ได้ ก็ไม่สามารถเข้าใจในข้อมูลเหล่านั้น

กระบวนการเข้ารหัสเพื่อป้องกันการโจรกรรมข้อมูล เริ่มต้นด้วยการแปลงข้อมูลในรูปของ Plaintext ให้กลายเป็น Ciphertext (ข้อมูลที่ถูกเข้ารหัสเรียบร้อยแล้ว) โดยใช้อัลกอริธึมอย่างใดอย่างหนึ่ง แล้วจึงส่งออกไปบนเครือข่าย ดังรูป 8.3



ภาพที่ 8.3 แสดงการเข้ารหัสแบบทางเดียว (One-way Encryption)

จากภาพที่ 8.3 เป็นการเข้ารหัสแบบทางเดียว (One-way Encryption) นิยมใช้กับรหัสผ่าน (Password) เนื่องจาก การส่งรหัสผ่านที่เป็น Plaintext ไปในเครือข่ายนั้นไม่มีความปลอดภัย จึงต้องการมีการเข้ารหัสเป็น Ciphertext ไว้ และที่เครื่องเซิร์ฟเวอร์ก็จะมี Ciphertext ที่เหมือนกันอยู่เพื่อใช้เปรียบเทียบว่าตรงกันหรือไม่โดยไม่ต้องทำการถอดรหัสแต่อย่างใด นอกจากนี้ ยังมีการเข้ารหัสอีกวิธีหนึ่ง ซึ่งต้องมีการถอดรหัส (Decryption) ก่อนใช้งาน เรียกว่า “การเข้ารหัสแบบสองทาง (Two-way Encryption)” แสดงได้ดังภาพที่ 8.4



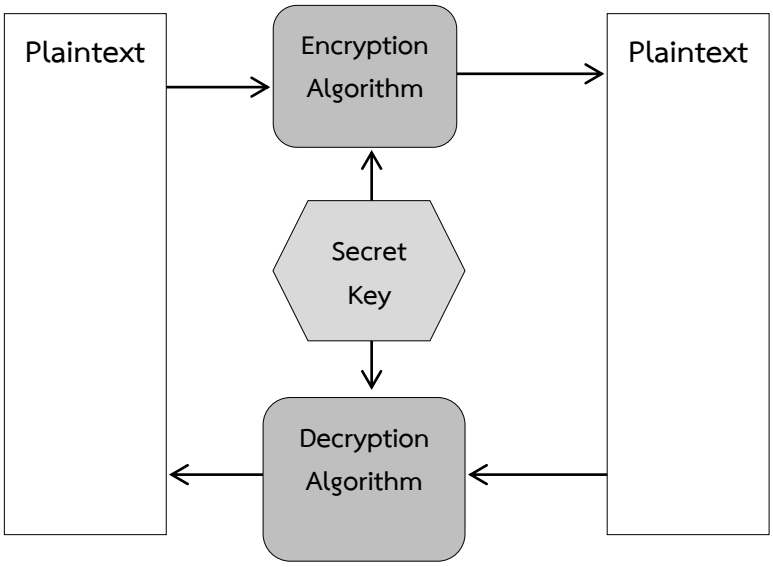
ภาพที่ 8.4 แสดงการเข้ารหัสแบบสองทาง (Two-way Encryption)

วิธีการเข้ารหัสที่ใช้โดยทั่วไปมีอยู่ 2 วิธี คือ การเข้ารหัสด้วยกุญแจที่เหมือนกัน (Symmetric Key Encryption) และการเข้ารหัสด้วยกุญแจที่ต่างกัน (Asymmetric Key Encryption)

การเข้ารหัสด้วยกุญแจที่เหมือนกัน (Symmetric Key Encryption)

การเข้ารหัสด้วยกุญแจที่เหมือนกัน หรือเรียกว่า “การเข้ารหัสด้วยกุญแจลับ (Secret Key Encryption)” เป็นการเข้ารหัสและถอดรหัสด้วยกุญแจตัวเดียวกัน ดังนั้นกุญแจที่ใช้จึงต้องเป็น “กุญแจลับ (Secret Key)” ที่ไม่มีใครรู้ นอกจากผู้ส่งและผู้รับเท่านั้น โดยการเข้ารหัสจะเริ่มจากผู้ส่งใช้กุญแจลับในการเข้ารหัส Plaintext ให้เป็น Ciphertext แล้วส่งไปยังผู้รับ เมื่อผู้รับได้รับ

Ciphertext แล้ว จะใช้กุญแจลับตัวนั้นในการถอดรหัสให้กลายเป็น Plaintext เพื่อให้สามารถอ่านข้อมูลที่ถูกส่งมาได้ ดังภาพที่ 8.5



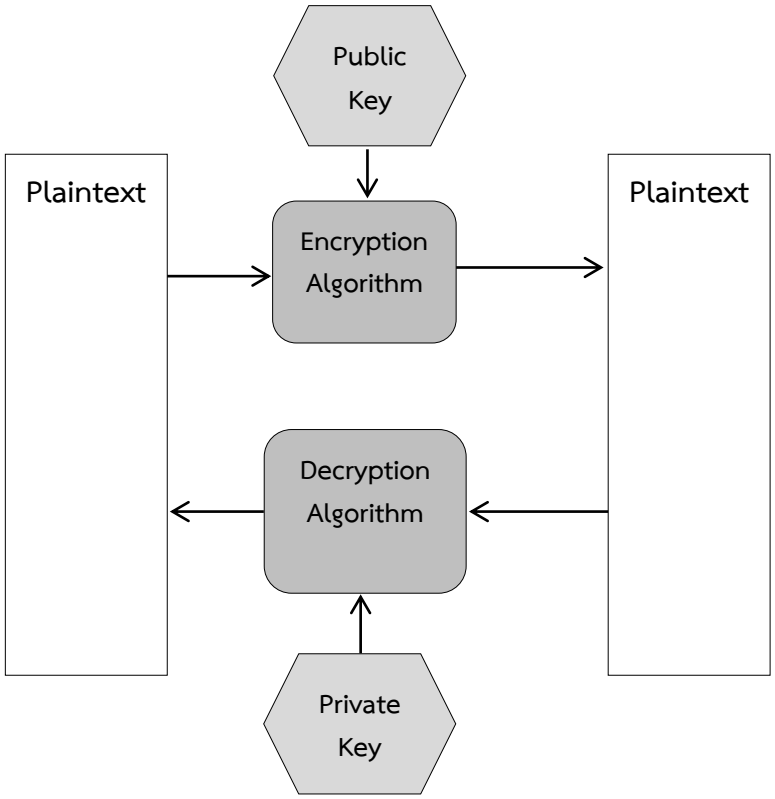
ภาพที่ 8.5 แสดงการเข้ารหัสด้วยกุญแจลับ (Secret Key Encryption)

วิธีการเข้ารหัสด้วยกุญแจลับที่นิยมใช้กัน คือ “Data Encryption Standard (DES)” ซึ่งได้รับการพัฒนาโดยบริษัท IBM แต่ในปัจจุบันถือว่าล้าสมัยไปแล้ว เนื่องจาการเข้ารหัสแบบ DES เริ่มไม่เพียงพอต่อการรักษาความปลอดภัยอีกต่อไป โดยมีวิธีการอื่นๆ เข้ามาแทนที่แต่ก็ยังคงใช้แนวความคิดแบบนี้อยู่

การเข้ารหัสด้วยกุญแจลับมีข้อเสีย คือ ต้องทำการแลกเปลี่ยนกุญแจระหว่างผู้รับกับผู้ส่ง ซึ่งหากส่งไปในเครือข่ายอินเตอร์เน็ตจะเสี่ยงต่อการถูกขโมยไปได้ และไม่สะดวกต่อการเดินทางไปแลกเปลี่ยนด้วยตนเองด้วย

การเข้ารหัสด้วยกุญแจที่ต่างกัน (Asymmetric Key Encryption)

การเข้ารหัสด้วยกุญแจที่ต่างกัน หรือเรียกว่า “การเข้ารหัสด้วยกุญแจสาธารณะ (Public Key Encryption)” เป็นการเข้ารหัสและถอดรหัสด้วยกุญแจที่แตกต่างกัน โดยใช้ “กุญแจสาธารณะ (Public Key)” ซึ่งเป็นกุญแจที่เปิดเผยให้ผู้อื่นรู้ได้ และ “กุญแจส่วนตัว (Private Key)” ซึ่งเป็นกุญแจที่ไม่สามารถเปิดเผยให้ผู้อื่นรู้ได้ เริ่มจาก ผู้ส่งทำการเข้ารหัส Plaintext ให้กลายเป็น Ciphertext ด้วยกุญแจสาธารณะของผู้รับ แล้วส่งไปให้ผู้รับ เมื่อผู้รับได้รับ Ciphertext แล้ว ก็จะใช้กุญแจส่วนตัวของตนเองในการถอดรหัส Ciphertext ให้กลายเป็น Plaintext เพื่ออ่านข้อมูล ดังภาพที่ 8.6



ภาพที่ 8.6 แสดงการเข้ารหัสด้วยกุญแจสาธารณะ (Public Key; Encryption)

กุญแจส่วนตัวที่ใช้ในการถอดรหัส ต้องเป็นกุญแจที่คู่กับกุญแจสาธารณะนั้นๆ เท่านั้น ไม่สามารถนำกุญแจส่วนตัวอื่นมาถอดรหัสได้ เนื่องจากกุญแจทั้ง 2 เชื่อมโยงกันด้วยสูตรทางคณิตศาสตร์ ดังนั้นแม้ผู้อื่นจะได้รหัสที่เป็น Ciphertext ไป แต่จะไม่สามารถถอดรหัสเหล่านั้นได้หากไม่มีกุญแจส่วนตัวของผู้รับ วิธีการนี้จึงมีความปลอดภัยสูงกว่าวิธีแรก แต่ในทางกลับกันก็มีความซับซ้อนมากกว่าด้วย จึงทำให้ต้องใช้เวลาในการเข้ารหัสนานกว่า

วิธีการเข้ารหัสด้วยกุญแจสาธารณะที่นิยมใช้กัน คือ RSA Encryption (Rivest-Shamir-Adelman Encryption) ซึ่งถูกพัฒนาโดย Ron Rivest, Ado Shamir และ Leonard Adleman การเข้ารหัสแบบ RSA นี้ให้ความปลอดภัยสูงมาก ดังนั้นในปัจจุบันจึงมีโปรแกรมเข้ารหัสจำนวนมากใช้เทคโนโลยีนี้เพื่อรักษาความปลอดภัย เช่น Pretty Good Privacy (PGP), Netscape Navigator หรือแม้แต่ Microsoft Internet Explore เป็นต้น

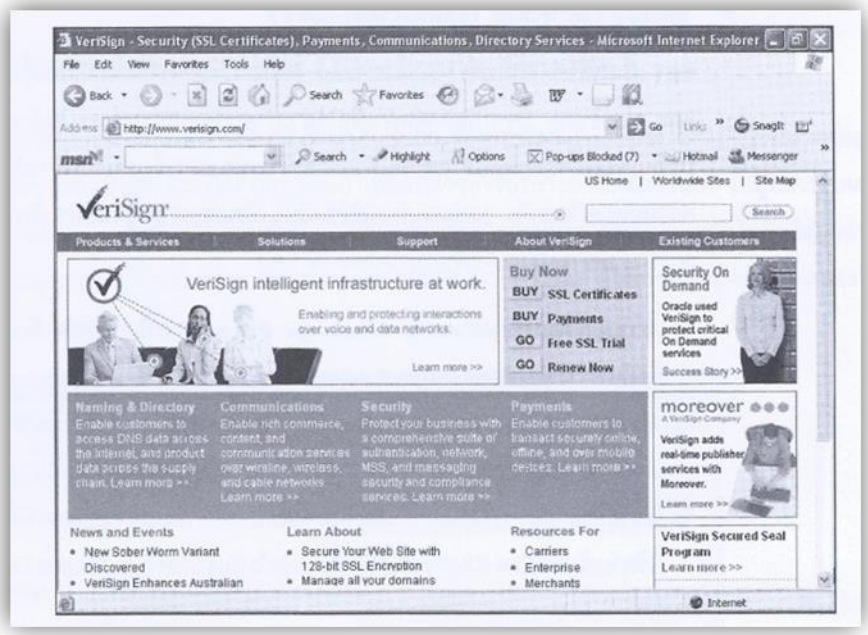
Secure Socket Layer (SSL)

จากปัญหาการโจรกรรมข้อมูลในขณะที่ข้อมูลส่งผ่านระบบเครือข่าย ทำให้ Netscape ได้คิดค้นและพัฒนาโปรโตคอล ขึ้นใหม่ในปี พ.ศ. 2538 คือ Secure Socket Layer Protocol (SSL) เพื่อใช้สำหรับเข้ารหัสด้วยกุญแจสาธารณะแก่ข้อมูล ก่อนที่ข้อมูลนั้นจะถูกส่งไปบนเครือข่ายอินเตอร์เน็ต โดยการเข้ารหัสมี 2 ระดับ คือ 40-bit Enceyption และ 128-bit Encryption

SSL นั้นได้รับการยอมรับอย่างกว้างขวางบน World Wide Web เพื่อใช้สำหรับตรวจสอบและเข้ารหัสของการติดต่อสื่อสารระหว่างไคลเอนท์กับเซิร์ฟเวอร์ โดยกลไกของการรักษาความปลอดภัยด้วยโปรโตคอล SSL มีดังนี้

- **ความปลอดภัยของข้อความ (Message Privacy)** เกิดจากการเข้ารหัสทั้ง 2 แบบ คือ ใช้การเข้ารหัสด้วยกุญแจสาธารณร่วมกับการเข้ารหัสด้วยกุญแจลับ เพื่อให้สามารถเข้ารหัสและถอดรหัสได้อย่างรวดเร็วและมีความปลอดภัยสูง
- **ความสมบูรณ์ของข้อความ (Message Integrity)** มั่นใจได้ว่าข้อมูลจะไม่ถูกแก้ไขระหว่างการรับ-ส่งข้อมูลของไคลเอนท์กับเซิร์ฟเวอร์ โดยอาศัย “Hash Function” คือ เมื่อป้อนข้อมูลขนาดความยาวที่กำหนดลงไปในฟังก์ชัน ก็จะได้ผลลัพธ์ออกมาเป็นรหัสที่จำกัด เรียกว่า “Message Digest” ของข้อมูลต้นฉบับ และการเข้ารหัสประกอบกัน เพื่อใช้ในการตรวจสอบเมื่อข้อความถึงผู้รับว่ามีขนาดเพิ่มขึ้นหรือลดลงหรือไม่
- **ความน่าเชื่อถือ (Matual Authentication)** เครื่องไคลเอนท์สามารถตรวจสอบใบรับรองดิจิตอล (Digital Certificate) ของเซิร์ฟเวอร์ได้ และหากผู้ใช้ทางฝั่งไคลเอนท์มีใบรับรองดิจิตอล ทางเซิร์ฟเวอร์ก็สามารถตรวจสอบข้อมูลของผู้ใช้ได้ด้วยเช่นกัน

ใบรับรองดิจิตอล (Digital Certificate หรือ Digital ID) เป็นสิ่งที่บ่งบอกว่าผู้ใช้เป็นใครหรือองค์กรใด มีข้อมูลส่วนตัวหรือข้อมูลขององค์กรเป็นอย่างไร มี Public Key ที่ใช้ในการถอดรหัสเป็นอย่างไร โดยได้รับการรับรองจากองค์กรหรือหน่วยงานกลางที่มีความน่าเชื่อถือ เรียกองค์กรนี้ว่า “Certification Authority (CA)” เช่น Thawte และ VeriSign ดังภาพที่ 8.7 เป็นต้น โดยการเข้ารหัสใบรับรองดิจิตอลนี้จะใช้การเข้ารหัสแบบกุญแจสาธารณะ



ภาพที่ 8.7 แสดงองค์กร Certification Authority (CA) ชื่อ VeriSign

Secure Hypertext Transport Protocol (S-HTTP)

S-HTTP เป็นส่วนของโปรโตคอล HTTP ทำหน้าที่ตรวจสอบสิทธิ์ผู้ใช้ที่มีต่อเซิร์ฟเวอร์ ซึ่งจะเข้ารหัสการลงลายเซ็นดิจิตอล (Digital Signature) การตรวจสิทธิ์สนับสนุนมาตรฐาน PKCS-7 และ PEM ซึ่งพัฒนาโดย RSA

ผู้ใช้สามารถเลือกระดับความซับซ้อนของการเข้ารหัสได้ แต่ระบบนี้จะอนุญาตให้ผู้ใช้และเซิร์ฟเวอร์ติดต่อกันได้เมื่อทั้ง 2 ฝ่ายได้รับใบรับรองดิจิตอล (Digital Certificate) การใช้ระบบรักษาความปลอดภัยรูปแบบนี้มีการจัดการระบบที่ยุ่งยากกว่า SSL แต่มีความปลอดภัยมากกว่า ระบบนี้นิยมใช้ในวงการธุรกิจการเงินและเศรษฐศาสตร์ที่มีข้อมูลความลับเป็นจำนวนมาก

ลายเซ็นดิจิตอล (Digital Signature) เป็นข้อความที่ประกอบด้วยตัวอักษรและตัวเลขจำนวนหนึ่งซึ่งใช้การเข้ารหัสด้วยกุญแจสาธารณะ แล้วส่งไปพร้อมกับเอกสารอิเล็กทรอนิกส์ เพื่อยืนยันว่าเอกสารที่ส่งไปนั้นเป็นตนจริง ๆ เสมือนหนึ่งว่าตนเป็นผู้เซ็นชื่อลงไปบนเอกสารนั้น ทำให้ใช้เป็นหลักฐานในการทำธุรกรรมบนอินเตอร์เน็ตได้

Secure Electronic Transaction (SET)

SET เป็นโปรโตคอลที่ทาง Visa และ Mastercard เป็นผู้คิดค้นและพัฒนาขึ้น โดยร่วมมือกับ Microsoft และ Netscape มีจุดประสงค์หลักเพื่อใช้สำหรับตรวจสอบการชำระเงินด้วยบัตรเครดิตอย่างปลอดภัยบนอินเตอร์เน็ตและเครือข่ายต่าง ๆ ด้วยการสร้างรหัส SET ซึ่งเป็นการเข้ารหัสด้วยกุญแจสาธารณะ ที่มีความปลอดภัยระดับ 128-bit โดยใช้ร่วมกับโปรโตคอลมาตรฐานอื่นๆ อีกหลายโปรโตคอล ข้อดีของการรักษาความปลอดภัยด้วยโปรโตคอล SET คือ

- **ความปลอดภัยของข้อความ (Message Privacy)** สามารถรักษาข้อมูลที่รับ – ส่งให้เป็นความลับได้ โดยการเข้ารหัสด้วยกุญแจสาธารณะ
- **ความสมบูรณ์ของข้อความ (Message Integrity)** สามารถรักษาความถูกต้องของข้อมูลที่ส่งผ่าน โดยข้อมูลจะไม่ถูกแก้ไขระหว่างทางด้วยการใช้ลายเซ็นดิจิตอล (Digital Signature)
- **ความน่าเชื่อถือ (Matual Authentication)** สามารถตรวจสอบการมีสิทธิ์ของผู้เกี่ยวข้องด้วยการใช้ลายเซ็นดิจิตอล (Digital Signature) และใบรับรองดิจิตอล (Digitla Certificate)

ความปลอดภัยของอีเมล์หรือจดหมายอิเล็กทรอนิกส์ (Securing E-Mail Messages)

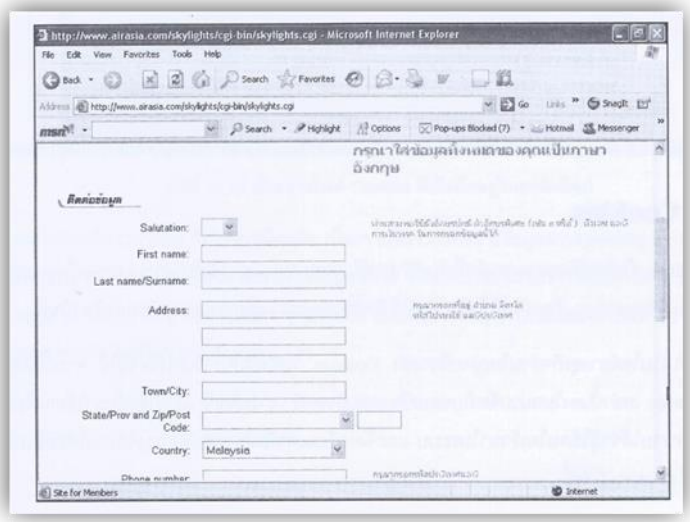
การส่งอีเมล์หรือจดหมายอิเล็กทรอนิกส์ผ่านเครือข่ายอินเตอร์เน็ตนั้นมีความเปิดเผยมาก จดหมายเหล่านั้นอาจถูกผู้อื่นเปิดอ่านได้ และหาข้อมูลในจดหมายเป็นข้อมูลที่มีความสำคัญจะเกิดความเสียหายเป็นอย่างมาก ดังนั้นการส่งข้อมูลในรูปของอีเมล์ไปบนอินเตอร์เน็ตจึงต้องมีการป้องกัน วิธีการป้องกันการโจรกรรมข้อมูลในจดหมายอิเล็กทรอนิกส์ที่ใช้ในปัจจุบันมี 2 วิธี คือ

1. ใช้โปรแกรมเข้ารหัส ซึ่งเป็นวิธีที่นิยมมากในปัจจุบัน เช่น Pretty Good Privacy (PGP) สามารถ Download โปรแกรมเหล่านี้ได้จากอินเตอร์เน็ตโดยไม่เสียค่าลิขสิทธิ์
2. ใช้ Digital Signature หรือ Digital Certificate

8.4 การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

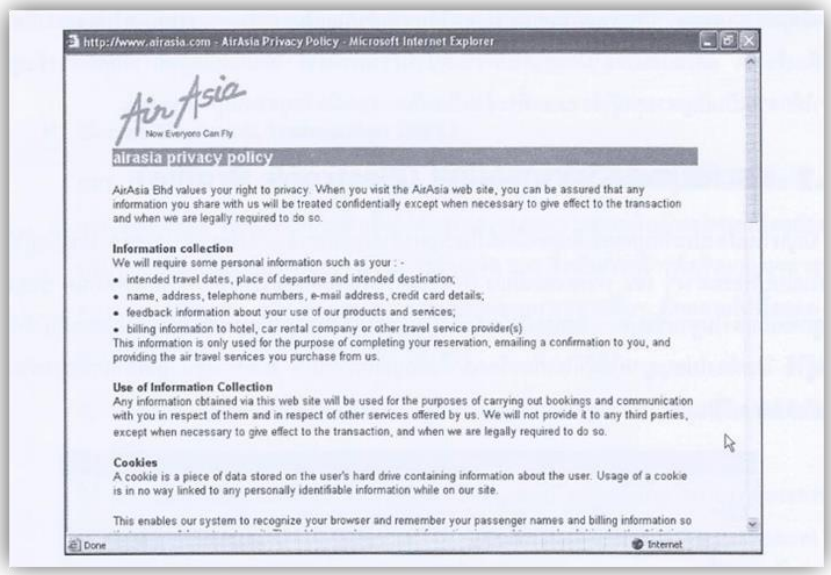
ข้อมูลส่วนบุคคล เป็นเรื่องที่ในต่างประเทศให้ความสำคัญเป็นอย่างมาก หากผู้ใดไปล่วงละเมิดผู้เสียหายก็สามารถฟ้องร้องได้ แต่ในเมืองไทยไม่ค่อยได้รับความสนใจมากเท่าที่ควร ทั้งยังไม่มีกฎหมายที่คุ้มครองข้อมูลส่วนบุคคลอีกด้วย ทำให้กลายเป็นปัญหาของผู้ใช้เองที่จะต้องป้องกันการละเมิดข้อมูลส่วนบุคคลของตน

ประวัติบุคคลอิเล็กทรอนิกส์ (Electronic Profile) ปัญหาในเรื่องประวัติบุคคลอิเล็กทรอนิกส์เป็นปัญหาสำคัญที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยเมื่อผู้ใช้กรอกข้อมูลส่วนตัวลงในแบบฟอร์มต่างๆ เช่น การลงทะเบียน (Register) เพื่อสมัครขอใช้บริการทางอินเตอร์เน็ต ข้อมูลส่วนบุคคลเหล่านี้จะถูกจัดเก็บลงในฐานข้อมูล ซึ่งทางเว็บไซต์หรือผู้ดูแลเว็บไซต์จะต้องมีระบบรักษาความปลอดภัยให้กับข้อมูลส่วนบุคคลของผู้ใช้ โดยต้องไม่อนุญาตให้ผู้ที่ไม่เกี่ยวข้องเข้าถึงข้อมูลเหล่านั้นได้ ตัวอย่างเช่น ผู้ใช้กรอกข้อมูลส่วนบุคคลลงในแบบฟอร์มการลงทะเบียนออนไลน์ ดังภาพที่ 8.8



ภาพที่ 8.8 ตัวอย่างการกรอกข้อมูลส่นตัวลงในแบบฟอร์มต่างๆ

โดยที่ทุกเว็บไซต์ต้องมีการแสดงนโยบายสิทธิส่วนบุคคล (Privacy Policy) ให้ผู้ใช้ทราบ และต้องมีการยืนยันการเก็บรักษาข้อมูลส่วนบุคคล เงื่อนไข และข้อตกลงในการให้บริการ ดังภาพที่ 8.9

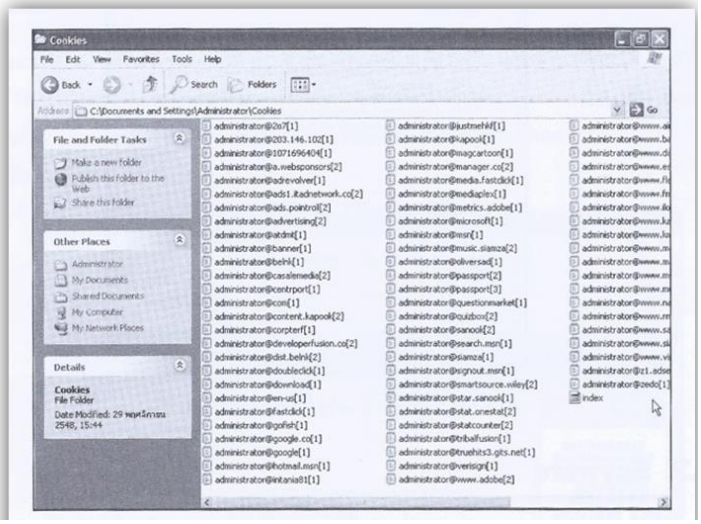


ภาพที่ 8.9 ตัวอย่างเว็บไซต์ที่มีการกำหนดนโยบายสิทธิส่วนบุคคล (Privacy Policy) ให้ผู้ใช้ทราบ

Cookies เป็นไฟล์ข้อมูลขนาดเล็กที่เว็บเซิร์ฟเวอร์ (Web Server) ใช้เก็บข้อมูลลงบนเครื่องคอมพิวเตอร์ของผู้ใช้ไฟล์ Cookies จะมีข้อมูลต่างๆ เกี่ยวกับผู้ใช้ เช่น ชื่อผู้ใช้ สิทธิพิเศษต่างๆ หรือหมายเลขบัตรเครดิต เป็นต้น

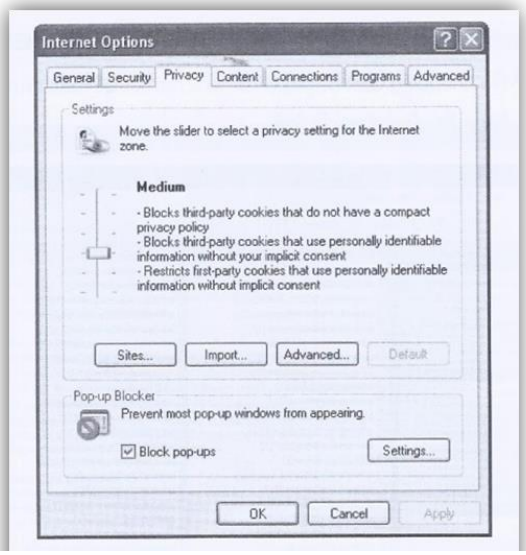
สำหรับเว็บไซต์ทางธุรกิจส่วนใหญ่จะมีการส่ง Cookies ไปยังเว็บบราวเซอร์ของผู้ใช้ จากนั้นคอมพิวเตอร์จะทำการจัดเก็บ Cookies เหล่านั้นลงในหน่วยจัดเก็บของเครื่องคอมพิวเตอร์ (ฮาร์ดดิสก์) เมื่อผู้ใช้กลับมาใช้งานเว็บไซต์ที่เว็บเพจนั้นอีกครั้งจะทำให้ทราบได้ว่าผู้ใช้คนใดเข้ามาในระบบ และจัดเตรียมเพจที่เหมาะสมกับการใช้งานให้อัตโนมัติ วัตถุประสงค์ของเว็บไซต์ที่ใช้ Cookies มีดังรูป

- เว็บไซต์ส่วนใหญ่จะอนุญาตให้ผู้ใช้ที่เคยเข้ามายังเว็บไซต์นั้นแล้วเข้าใช้งานได้ทันที โดยตรวจสอบจาก Cookies ที่ถูจัดเก็บอยู่ในเครื่องของผู้ใช้
- บางเว็บไซต์จะใช้ Cookies ในการจัดเก็บรหัสผ่านของผู้ใช้
- เว็บไซต์ด้านการซื้อขายแบบออนไลน์ (Online Shopping Site) ส่วนใหญ่จะใช้ Cookies เพื่อเก็บข้อมูลการเลือกซื้อสินค้าใน Shopping Cart
- ใช้ในการเก็บข้อมูลเกี่ยวกับผู้เข้าชมเว็บไซต์



ภาพที่ 8.10 ตัวอย่างไฟล์ Cookies ที่บันทึกอยู่ในฮาร์ดดิสก์

แต่บางครั้งการเก็บ Cookies ก็มีโทษเหมือนกัน เนื่องจากใน Cookies มีข้อมูลส่วนบุคคลอยู่ หากมีผู้ไม่ประสงค์ดีเข้ามาโจรกรรมข้อมูลใน Cookies ไป ก็สามารถรับรู้ในข้อมูลนั้นได้ ดังนั้นเว็บบราวเซอร์จึงได้ให้ผู้ใช้สามารถกำหนดระดับการจัดเก็บ Cookies ได้ โดยอาจให้เว็บบราวเซอร์ทำการบันทึก Cookies ของทุกเว็บไซต์โดยอัตโนมัติ ไปจนถึงไม่อนุญาตให้มีการรับ Cookies จากเว็บไซต์ใดๆ เลย ดังภาพที่ 8.11



ภาพที่ 8.11 ตัวเลือกสำหรับกำหนดการจัดเก็บ Cookies

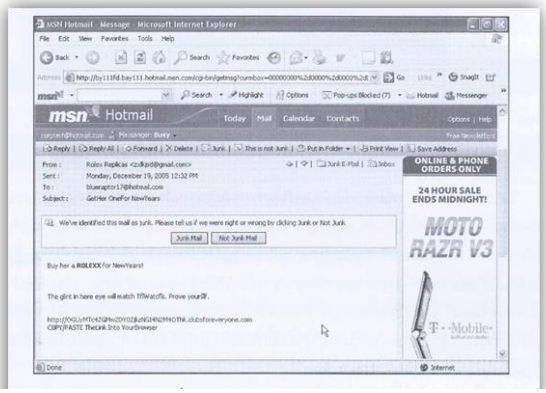
Spyware เป็นโปรแกรมคอมพิวเตอร์ที่ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์โดยที่ผู้ใช้ไม่รู้ตัว โดยจะเข้าโจมตีระบบรักษาความปลอดภัยของเครื่อง เพื่อเข้าถึงข้อมูลที่เป็นความลับ เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่นๆ เป็นต้น

จุดประสงค์หลักของ Spyware ก็คือ ติดตามและรวบรวมข้อมูลส่วนตัวหรือข้อมูลสำคัญของผู้ใช้คอมพิวเตอร์เพื่อส่งกลับไปให้บริษัทผู้ผลิต Spyware ที่มาตามเว็บไซต์นั้น จากนั้น บริษัทดังกล่าวจะนำข้อมูลส่วนตัว เช่น Username, Password, URL ที่เรียกใช้บ่อยๆ เป็นต้น ไปใช้ในการโฆษณาขายสินค้า สังเกตได้จาก ในบางครั้งเราอาจได้รับอีเมล์โฆษณาสินค้าโดยที่ไม่ได้ไปสมัครสมาชิกไว้แต่อย่างใด หรือทุกครั้งที่เชื่อมต่อเข้าอินเตอร์เน็ตจะปรากฏป้ายโฆษณาโดยที่ยังไม่ได้เปิด Web Browser

Spam คือ อีเมล์ลักษณะหนึ่งที่ผู้รับไม่ต้องการ ซึ่งส่วนใหญ่จะเป็นอีเมล์ที่เกี่ยวกับการขายสินค้าหรือบริการการส่งเสริมการขาย และการโฆษณาต่างๆ ทำให้ผู้ใช้เกิดความรำคาญ จุดประสงค์ของการใช้ Spam คือ การก่อกวนผู้รับเมล์เชิญชวนให้ซื้อสินค้า แนะนำเว็บทางการค้า หรือระบบเมล์ของเครือข่ายนั้นๆ โดยผู้สร้าง Spam อาจเป็น Hacker ที่เขียนโปรแกรมเพื่อการค้าหรือนักเจาะระบบมือสมัครเล่นที่ชอบทดลองก็ได้ ซึ่งการส่ง spam ถือว่าเป็นการละเมิดสิทธิส่วนบุคคล เนื่องจากมีการนำ E-mail Address ของผู้ใช้มาจากเว็บไซต์อื่นโดยไม่ได้รับอนุญาต

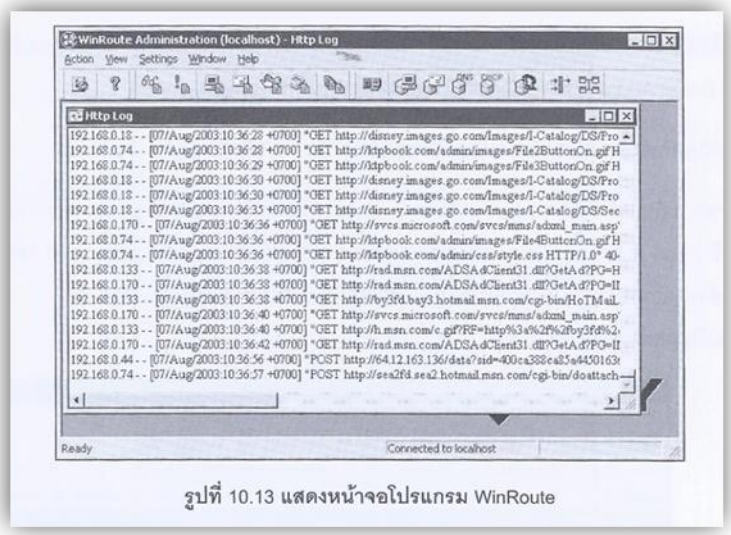
สามารถป้องกันปัญหาที่เกิดขึ้นจาก Spam ได้ดังนี้

- รายงานกับ ISP หรือ Provider ที่ใช้บริการ เพื่อให้สกัดอีเมล์ที่อาจเป็น Spam ที่มาจาก Domain นั้นๆ
- ใช้ Filter สำหรับการกรองหรือค้นหาคำหรือข้อความ เช่น Money, Promote, Sell หรือ Cash เป็นต้น แล้วทำการลบอีเมล์เหล่านั้นทิ้งที่เซิร์ฟเวอร์เพื่อจะได้ไม่ต้องเสียเวลาดาวน์โหลด
- ไม่เปิดเผยอีเมล์ส่วนตัวในวงกว้าง โดยไม่จำเป็น



ภาพที่ 8.12 แสดงภาพตัวอย่างเมล์ Spam

Employee Monitoring เป็นการติดตามการทำงานของพนักงาน โดยใช้โปรแกรมสำหรับสังเกตการณ์ บันทึกและตรวจสอบ การใช้งานคอมพิวเตอร์ในการติดต่อสื่อสาร เช่น การเช็คอีเมล์ซึ่งปกติผู้ดูแลระบบ (Administrator) สามารถเข้าไปอ่านเนื้อหาในอีเมล์ได้อยู่แล้ว การตรวจสอบการท่องเว็บไซต์ต่างๆ โดยใช้ซอฟต์แวร์ Win Route หรือ Microsoft Internet Security & Acceleration Server และการใช้ซอฟต์แวร์ในการเข้าถึงข้อมูลที่แสดงอยู่บนจอของลูกจ้างหรือพนักงานอย่างเช่น PC Anywhere เป็นต้น



รูปที่ 10.13 **แสดงหน้าจอโปรแกรม** WinRoute

ภาพที่ 8.13 แสดงหน้าจอโปรแกรม WinRoute

8.5 แนวโน้มของระบบรักษาความปลอดภัยในอนาคต

ในช่วงเริ่มต้นของการพัฒนาคอมพิวเตอร์และระบบเครือข่ายเมื่อหลายสิบปีที่ผ่านมา โปรแกรมที่สามารถสร้างความเสียหายแก่ข้อมูลหรือเครื่องคอมพิวเตอร์จะถูกพัฒนาขึ้นอย่างต่อเนื่องควบคู่กับวิวัฒนาการของคอมพิวเตอร์ โดยโปรแกรมเหล่านี้เป็นปัญหาสำหรับผู้ใช้คอมพิวเตอร์มาตลอด ผู้เชี่ยวชาญเกี่ยวกับคอมพิวเตอร์กล่าวถึงปัญหาเกี่ยวกับความปลอดภัยของคอมพิวเตอร์ในอนาคตว่า “บุคคลและองค์กรต่างๆ จะต้องใช้เงินจำนวนมากสำหรับการป้องกันอุปกรณ์ ซอฟต์แวร์และข้อมูลในคอมพิวเตอร์” แนวโน้มของอาชญากรรมคอมพิวเตอร์ในอนาคตจะมีความรุนแรงมากขึ้น มีการผลิตซอฟต์แวร์สำหรับเจาะเข้าสู่ระบบฐานข้อมูลเป็นจำนวนมาก โปรแกรมไวรัสสายพันธุ์เดิมต่างๆ ถูกพัฒนาออกเป็นหลากหลายพันธุ์มีความรุนแรงและการทำงานที่แตกต่างจากเดิม

ในปัจจุบันนี้รูปแบบของการโจมตีผ่านระบบเครือข่ายมีการพัฒนาขึ้น โดยมีรูปแบบที่ไม่มีใครรู้จักสำหรับผู้ดูแลระบบแล้วปัญหานี้เป็นเรื่องที่ยากจะแก้ไขหรือติดตามหาบุคคลที่พยายามบุกรุกระบบ

แนวทางสำหรับพัฒนาระบบรักษาความปลอดภัยของคอมพิวเตอร์ในปัจจุบัน สามารถจำแนกรูปแบบการรักษาความปลอดภัยออกเป็น ดังนี้

1. ระบบรักษาความปลอดภัยสำหรับเครื่องไคลเอนท์
2. ระบบป้องกันการโจรกรรมข้อมูล
3. เครื่องมือเข้ารหัส
4. ระบบป้องกันการเจาะข้อมูล
5. ระบบป้องกันแฟ้มข้อมูลส่วนบุคคล
6. ระบบรักษาความปลอดภัยสำหรับเครือข่าย
7. ระบบป้องกันไวรัส

ระบบต่างๆ เหล่านี้มีรูปแบบ และการทำงานที่แตกต่างกัน สามารถทำงานได้อย่างมีประสิทธิภาพ เนื่องจากมีหน้าที่ในแต่ละส่วนของระบบ ทำให้แยกกันทำงานและมีการเชื่อมโยงข้อมูลต่างๆ เกี่ยวกับการรักษาความปลอดภัยถึงกันได้

แนวโน้มในอนาคตคาดว่าระบบรักษาความปลอดภัยของคอมพิวเตอร์และระบบสารสนเทศจะถูกแยกการทำงานออกเป็นหลายส่วนด้วยกัน โดยจะทำงานแยกจากกันแต่สามารถเชื่อมโยงข้อมูลถึงกันได้ ผู้ผลิตซอฟต์แวร์สำหรับรักษาความปลอดภัยส่วนใหญ่ให้ความสนใจกับแนวคิดนี้ และบางรายพัฒนาซอฟต์แวร์รุ่นใหม่ของตนให้เป็นไปในรูปแบบนี้แล้ว เช่น Sybase ผู้ผลิต Norton AntiVirus และ Norton Utility เป็นต้น

8.6 จริยธรรมทางด้านคอมพิวเตอร์

จริยธรรม เป็นศาสตร์แขนงหนึ่งของปรัชญาที่เกี่ยวข้องกับหลักในการประพฤติปฏิบัติตนของมนุษย์ ที่มุ่งเน้นแต่การทำดี คิดดี ซึ่งทางด้านการใช้งานคอมพิวเตอร์แล้ว จริยธรรมเป็นสิ่งสำคัญประการหนึ่งที่ผู้ใช้คอมพิวเตอร์ทุกคนควรจะตระหนักถึงตลอดเวลา เพื่อไม่ให้มีการใช้ความสามารถในทางคอมพิวเตอร์ไปในทางที่ผิด อันจะก่อให้เกิดความเสียหายต่อบุคคลอื่นได้

8.6.1 จริยธรรมและกฎหมาย (Ethics and Laws)

ข้อกำหนดในการใช้คอมพิวเตอร์นั้นถูกกำหนดกฎเกณฑ์และสิทธิในการเข้าถึงข้อมูลไว้ด้วย 2 วิธี คือ กำหนดด้วยจริยธรรมและกำหนดด้วยกฎหมาย ซึ่งทั้ง 2 วิธีการนี้มีจุดประสงค์เดียวกันคือการสร้างความเป็นระเบียบและความเรียบร้อยรวมทั้งคุ้มครองสิทธิส่วนบุคคลในระบบสารสนเทศ แต่ทั้งจริยธรรมและกฎหมายนั้นมีความแตกต่างกันอย่างมากในหลายประเด็นซึ่งเกิดเป็นปัญหาขึ้น จริยธรรมอาจจะครอบคลุม หรือไม่ครอบคลุมโดยกฎหมายก็ได้ ดังรายละเอียดในตารางต่อไป

ตารางที่ 8.1 ความแตกต่างระหว่างกฎหมายและจริยธรรม

ความแตกต่างระหว่างกฎหมายและจริยธรรม		
หัวข้อ	**จริยธรรม**	**กฎหมาย**
หลักการพื้นฐาน	ไม่มีหลักการตายตัว และขึ้นอยู่กับจิตสำนึกของบุคคลในสังคม	เป็นหลักและกฎเกณฑ์ตายตัว เปลี่ยนแปลงได้ยาก มีความซับซ้อน
ผู้ติดสินความผิด	บุคคลผู้กระทำ	การตัดสินเป็นไปตามกระบวนการที่รัฐบาลกำหนดขึ้น
บทลงโทษ	การวิพากษ์วิจารณ์ หรือถูกรังเกียจจากผู้คนในสังคม	ปรับ หรือจำคุก หรือทั้งจำทั้งปรับ
การบังคับใช้	ขึ้นอยู่กับสังคมนั้น	ขึ้นอยู่กับสังคมนั้น

8.6.2 ประเด็นที่เกี่ยวข้องกับจริยธรรมทางด้านคอมพิวเตอร์

ในโลกนี้มีหลักจริยธรรมและหลักฐานกฎหมายที่เป็นแนวทางในการประพฤติปฏิบัติตนของมนุษย์อยู่มากมาย แตกต่างกันไปตามแต่ละประเทศ ขึ้นอยู่กับขนบธรรมเนียม วัฒนธรรมและประเพณีของประเทศนั้นๆ แต่สำหรับในยุคปัจจุบันที่มีเทคโนโลยีใหม่ๆ มากมาย โดยเฉพาะเทคโนโลยีสารสนเทศและระบบสารสนเทศ ซึ่งส่งผลกระทบต่อวิถีการดำเนินชีวิตของมนุษย์ให้เปลี่ยนแปลงไปจากเดิมอย่างเห็นได้ชัด สิ่งที่ตามมาคือ ปัญหาในประเด็นต่างๆที่เกิดจากการนำเทคโนโลยีและระบบสารเทศเหล่านี้เข้ามาใช้งาน ซึ่งมีความเกี่ยวข้องในทางจริยธรรมประเด็นต่างๆ ได้แก่ สิทธิส่วนบุคคล (Privacy) ความถูกต้อง (Accuracy) ความเป็นเจ้าของ (Property) และการเข้าถึง (Access)

8.6.3 สิทธิส่วนบุคคล (Privacy)

ระบบสารสนเทศอาจส่งผลกระทบต่อผู้ที่เกี่ยวข้อง 2 ด้านด้วยกัน คือ ด้านกายภาพ (Physical Privacy) และด้านสารสนเทศ (Information Privacy)

สิทธิส่วนบุคคลทางด้านกายภาพ (Physical Privacy) หมายถึง สิทธิในสถานที่ เวลาและสินทรัพย์ที่บุคคลพึงมี เพื่อหลีกเลี่ยงจากการถูกก้าวก่ายหรือถูกรบกวนจากบุคคลอื่น จากการพัฒนาความสามารถให้เพิ่มมากขึ้นอย่างต่อเนื่องของเทคโนโลยีสารสนเทศ ทำให้ผู้ใช้มีช่องทางที่จะรุกล้ำสิทธิส่วนบุคคลผู้อื่นได้สะดวกขึ้น เช่น การส่งจดหมายขยะ (Junk Mail) การส่งจดหมายเวียนหรือที่เรียกว่า “Spam Mail” เป็นต้น ดังนั้นผู้ใช้งานในระบบสารสนเทศต่างๆ จึงควรตระหนักถึงข้อนี้ด้วยเพื่อไม่ให้เป็นการรบกวนและรุกล้ำสิทธิส่วนบุคคลผู้อื่นจนเกินไปซึ่งนอกจากการส่งจดหมายอิเล็กทรอนิกส์แล้ว ยังมีการใช้อุปกรณ์ติดต่อสื่อสาร เช่น โทรศัพท์ เพื่อรวบกวนบุคคลอื่นอีกด้วย

สิทธิส่วนบุคคลทางด้านสารสนเทศ (Information Privacy) สิทธิส่วนบุคคลทางด้านสารสนเทศในที่นี้ คือ ข้อมูลทั่วไปเกี่ยวกับตัวบุคคล เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ หมายเลขบัตรเครดิต เลขที่บัญชี เป็นต้น ที่บุคคลอื่นจะไม่สามารถนำไปเปิดเผยได้หากไม่ได้รับอนุญาตปัจจุบันหน่วยงานราชการหรือเอกชนได้มีการจัดเก็บข้อมูลของประชาชนหรือลูกค้าบางส่วนไว้ในฐานข้อมูล เช่น หน่วยงานทะเบียนงานทะเบียนราษฎร์ หรือบริษัทให้สินเชื่อ บัตรเครดิต เป็นต้น ซึ่งข้อมูลที่หน่วยงานต่างๆ ได้รับสิทธิ์ในการจัดเก็บไว้นั้น หากมองโดยภาพรวมแล้ว จะทำให้ทราบถึงสถานะความเป็นอยู่ของลูกค้าหรือประชาชนได้ ถึงแม้ว่าระบบสารสนเทศจะทำให้การจัดเก็บข้อมูลในฐานข้อมูลมีความปลอดภัยเป็นอย่างดีแล้วก็ตาม แต่เทคโนโลยีสารสนเทศเองก็ทำให้ผู้ใช้บางคนที่อยู่ในหน่วยงานที่ประชาชนหรือลูกค้าให้ความไว้วางใจ ลักลอบเข้าไปใช้ข้อมูลเหล่านั้นในฐานข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้เพื่อนำไปเผยแพร่ในทางอื่นอันไม่สมควร จากการกระทำดังกล่าวทำให้ลูกค้าได้รับความเสียหายเป็นอย่างมาก และต้องการให้มีการคุ้มครองสิทธิส่วนบุคคลทางด้านสารสนเทศเหล่านี้ให้มากยิ่งขึ้น

8.6.4 ความถูกต้อง (Accuracy)

ความถูกต้องของข้อมูลและสารสนเทศที่จัดเก็บอยู่ในฐานข้อมูลของระบบสารสนเทศต่างๆ มีความสำคัญเป็นอย่างมาก ซึ่งนอกจากข้อมูลและสารสนเทศนั้นจะต้องมีความถูกต้องแล้ว ผู้ที่ได้รับอนุญาตให้นำเสนอสารสนเทศต่างๆ ยังจะต้องนำเสนอสารสนเทศนั้นโดยไม่ผิดเพี้ยนหรือไม่มีการบิดเบือนให้ผู้อ่านเกิดความเข้าใจผิดได้ ทั้งนี้ หากสารสนเทศเกี่ยวกับบุคคลที่จัดเก็บในฐานข้อมูลมีความผิดพลาดอาจก่อให้เกิดความเสียหายแก่บุคคลนั้นได้ เช่น ข้อมูลรายได้ประจำของลูกค้า จาก 20,000 บาท แต่จัดเก็บไว้ในฐานข้อมูล เป็น 2,000 บาท และเมื่อนำมาพิจารณาอนุมัติสินเชื่อ ก็จะทำให้ลูกค้าดังกล่าวไม่ได้รับการพิจารณาและเสียโอกาสไปในที่สุด หรือในกรณีข้อมูลยอดที่ต้องชำระค่าบริการโทรศัพท์เกิดความผิดพลาด และหากลูกค้าไม่ได้ตรวจสอบยอดค่าบริการดังกล่าว ก็จะทำให้ลูกค้าต้องชำระเงินค่าบริการมากกว่าความเป็นจริง ซึ่งไม่ยุติธรรมต่อลูกค้า เป็นต้น

8.6.5 กฎหมายทรัพย์สินทางปัญญา (Intellectual Property Rights)

ในระบบสารสนเทศและเทคโนโลยีสารสนเทศซอฟต์แวร์ที่ถูกพัฒนาขึ้นมาเพื่อการค้านั้นจำเป็นต้องได้รับความคุ้มครองในความเป็นเจ้าของผลิตภัณฑ์นั้นๆ ในฐานะที่เป็น “ทรัพย์สินทางปัญญา (Intellectual Property)” ของผู้ผลิต ทั้งนี้เนื่องจากในการผลิตต้องใช้เงินลงทุนและกำลังคนเป็นจำนวนมาก หากซอฟต์แวร์หรือแม้กระทั่งเครื่องหมายการค้าถูกลักลอบทำสำเนา ทำซ้ำ หรือปลอมแปลงเพื่อนำไปขายต่อ ย่อมก่อให้เกิดความเสียหายต่อเจ้าของผู้ทำการผลิตมากมายมหาศาล ทรัพย์สินทางปัญญาแบ่งเป็น 3 ประเภท ได้แก่

ลิขสิทธิ์ (Copyrights) ลิขสิทธิ์เป็นการให้สิทธิ์แก่ผู้ผลิตหรือผู้ประดิษฐ์แต่เพียงผู้เดียวที่จะสามารถทำการจำลอง คัดลอก โฆษณาหรือขายสิ่งที่สร้างหรือประดิษฐ์ขึ้น สำหรับการละเมิดลิขสิทธิ์โดยส่วนใหญ่แล้วจะเป็นการละเมิดลิขสิทธิ์ทางด้านซอฟต์แวร์ (Software Piracy) ซึ่งจะเป็นการ

คัดลอกหรือผลิตซอฟต์แวร์ซ้ำกับซอฟต์แวร์ที่ได้มีการจดลิขสิทธิ์ไว้แล้ว โดยการละเมิดลิขสิทธิ์ซอฟต์แวร์จะถือว่าเป็นการกระทำผิดกฎหมายตามพระราชบัญญัติ

เครื่องหมายทางการค้า (Trademark) เครื่องหมายทางการค้า คือ เครื่องหมายที่ใช้หรือจะใช้เป็นเครื่องหมายเกี่ยวข้องกับสินค้า เพื่อแสดงว่าสินค้าที่ใช้เครื่องหมายของเจ้าของเครื่องหมายการค้านั้น แตกต่างกับสินค้าที่ใช้เครื่องหมายการค้าของบุคคลอื่น

สิทธิบัตร (Patent) สิทธิบัตร หมายถึง สิทธิพิเศษที่กฎหมายบัญญัติให้เจ้าของสิทธิบัตรมีสิทธิแต่เพียงผู้เดียว ในการแสวงหาประโยชน์จากการประดิษฐ์หรือการออกแบบผลิตภัณฑ์ที่ได้รับสิทธิบัตรนั้น เช่น การผลิตและจำหน่าย เป็นต้น

กฎหมายทรัพย์สินทางปัญญา (Intellectual Property Rights) จะเป็นการอ้างถึงงานที่สร้างหรือผลิตโดยนักประดิษฐ์ ผู้ประพันธ์ และผู้สร้างสรรค์ ซึ่งกฎหมายทรัพย์สินทางปัญญาเป็นการคุ้มครองผลงานที่สร้างหรือผลิตขึ้นเพื่อป้องกันไม่ให้ผู้ใดทำการคัดลอก หรือทำซ้ำเพื่อการค้าโดยไม่ได้รับอนุญาต สำหรับปัญหาที่เกิดขึ้นในโลกของระบบสารสนเทศปัจจุบัน ก็คือ การละเมิดลิขสิทธิ์ซอฟต์แวร์ ไม่ว่าจะเป็นการคัดลอก ทำสำเนาและแก้ไข หรือแม้กระทั่งดาวน์โหลดซอฟต์แวร์เพื่อนำมาจำหน่ายโดยไม่ได้รับอนุญาต สำหรับประเทศไทยกำลังให้ความสำคัญ ปราบปราม และป้องกันปัญหานี้อย่างเร่งด่วน

ปัญหาในประเด็นทรัพย์สินทางปัญญาที่เกิดขึ้น มีความเกี่ยวข้องกับจรรยาบรรณในการใช้งานคอมพิวเตอร์ของผู้ใช้ที่พึงมี เพื่อไม่ก่อความเสียหายให้ผู้อื่น ดังรายละเอียดในหัวข้อต่อไป

8.6.6 จรรยาบรรณในการใช้งานคอมพิวเตอร์

จรรยาบรรณ หมายถึง ประมวลความประพฤติที่ผู้ประกอบอาชีพการงานแต่ละอย่างกำหนดขึ้นเพื่อรักษาและส่งเสริมเกียรติคุณชื่อเสียงและฐานะของสมาชิก เช่น จรรยาบรรณของแพทย์ จรรยาบรรณของครู-อาจารย์ หรือจรรยาบรรณของผู้สื่อข่าว เป็นต้น

ในวงการคอมพิวเตอร์ก็เช่นเดียวกัน ผู้ประกอบอาชีพที่เกี่ยวข้องกับคอมพิวเตอร์มีหลายอาชีพ แต่ละอาชีพก็จะต้องมีจรรยาบรรณเพื่อเป็นขอบเขตในการประพฤติตนของผู้ที่ประกอบอาชีพนั้น เช่น จรรยาบรรณของนักวิเคราะห์ระบบที่ควรจดจำไว้เสมอว่าไม่ควรเปิดเผยความลับของบริษัทที่ตนทำหน้าที่นักวิเคราะห์ระบบอยู่ หรือจรรยาบรรณของโปรแกรมเมอร์ก็เช่นเดียวกัน ไม่ควรเขียนโปรแกรมไวรัสแนบไปกับโปรแกรมที่กำลังพัฒนาให้กับบริษัท เป็นต้น สำหรับผู้ใช้งานคอมพิวเตอร์ทั่วไป ถึงแม้ว่าจะไม่ได้ประกอบอาชีพทางด้านคอมพิวเตอร์โดยตรงก็ตาม แต่การใช้คอมพิวเตอร์ไปในทางที่ผิดก็อาจก่อให้เกิดความเสียหายต่อผู้อื่นได้เช่นกัน ดังนั้น ผู้ใช้คอมพิวเตอร์จึงควรปฏิบัติตนตามจรรยาบรรณของผู้ใช้คอมพิวเตอร์ดังต่อไปนี้

จรรยาบรรณในการใช้คอมพิวเตอร์ มีดังนี้

1. จะต้องไม่ใช้คอมพิวเตอร์เพื่อก่ออาชญากรรมหรือละเมิดสิทธิของผู้อื่น
2. จะต้องไม่ใช้คอมพิวเตอร์รบกวนผู้อื่น
3. จะต้องไม่ทำการสอดแนม แก้ไข หรือเปิดดูไฟล์เอกสารของผู้อื่นก่อนได้รับอนุญาต
4. จะต้องไม่ใช้คอมพิวเตอร์ในการโจรกรรมข้อมูล ข่าวสาร
5. จะต้องไม่ใช้คอมพิวเตอร์สร้างหลักฐานเท็จ
6. จะต้องไม่ใช้คอมพิวเตอร์ในการคัดลอกโปรแกรมที่มีลิขสิทธิ์
7. จะต้องไม่ใช้คอมพิวเตอร์ในการละเมิดการใช้ทรัพยากรคอมพิวเตอร์โดยที่ตนเองไม่มีสิทธิ์
8. จะต้องไม่ใช้คอมพิวเตอร์เพื่อนำเอาผลงานของผู้อื่นมาเป็นของตนเอง
9. จะต้องคำนึงถึงสิ่งที่จะเกิดขึ้นกับสังคม ที่จะตามมาจากการกระทำนั้น
10. จะต้องใช้คอมพิวเตอร์ โดยเคารพกฎ ระเบียบ กติกา และมารยาท

สรุป

เทคโนโลยีสารสนเทศและระบบสารสนเทศมีความสำคัญต่อวิถีชีวิตในปัจจุบันเป็นอย่างมาก ดังนั้นจึงต้องมีระบบรักษาความปลอดภัยเพื่อสร้างความมั่นใจให้แก่ผู้ใช้ การสร้างความปลอดภัยในปัจจุบันมี 3 ลักษณะ คือ การรักษาความปลอดภัยคอมพิวเตอร์ในองค์กร บนเครือข่ายอินเตอร์เน็ต และข้อมูลส่วนบุคคล การรักษาความปลอดภัยทั้ง 3 ลักษณะนี้มีจุดประสงค์ที่เหมือนกันคือ ป้องกันการบุกรุก และป้องกันข้อมูลที่เก็บรักษาไว้ ซึ่งรูปแบบของการบุกรุกและก่อความเสียหายนั้นมีหลายรูปแบบ ไม่ว่าจะเป็นการใช้ไวรัสคอมพิวเตอร์ การเจาะระบบ หรือการโจรกรรมข้อมูล ซึ่งล้วนแล้วแต่สร้างความเสียหายแก่ผู้ใช้ระบบสารสนเทศได้

การพัฒนาระบบรักษาความปลอดภัยสำหรับคอมพิวเตอร์ มีการพัฒนาขึ้นควบคู่กับการพัฒนารูปแบบของการบุกรุก ซึ่งสร้างความเสียหายต่อคอมพิวเตอร์และระบบสารสนเทศอย่างมากมาย ดังนั้นบริษัทผู้ผลิตจึงได้คิดค้นวิธีการต่างๆ ในการป้องกันข้อมูล เช่น การใช้ User Name และ Password การพัฒนาอุปกรณ์ Biometric การสร้างรหัสลับ (Encryption) ไปจนถึงการพัฒนาซอฟต์แวร์สำหรับรักษาความปลอดภัยในคอมพิวเตอร์

ปัจจุบันในต่างประเทศได้มีกฎหมายที่เกี่ยวข้องกับการรักษาความปลอดภัย และการก่ออาชญากรรมคอมพิวเตอร์ประกาศใช้อย่างมากมาย รวมทั้งมีการจัดตั้งองค์กรเพื่อทำงานเกี่ยวกับการป้องกันและลงโทษอาชญากรคอมพิวเตอร์โดยมุ่งหวังที่จะแก้ปัญหาเกี่ยวกับอาชญากรรมคอมพิวเตอร์ซึ่งมีแนวโน้มที่รุนแรงขึ้น

ถึงแม้ว่าเทคโนโลยีสารสนเทศ จะช่วยให้ผู้ใช้มีความสะดวกสบายขึ้นมากก็ตาม แต่สิ่งเหล่านี้ก็เปรียบเทียบเสมือนดาบสองคมที่อาจให้ทั้งผลดีและผลเสีย แต่ก็ขึ้นอยู่กับจรรยาบรรณของผู้ใช้ว่าจะใช้เทคโนโลยีเหล่านี้ไปในทิศทางใด ดังนั้นเนื้อหาในส่วนสุดท้ายจึงกล่าวถึงจริยธรรมทางด้านคอมพิวเตอร์ (Computer Ethics) เนื่องจากประโยชน์ที่ได้รับอาจทำให้เป็นการรุกล้ำสิทธิส่วนบุคคลของผู้อื่นทั้งทางด้านกายภาพและสารสนเทศ โดยไม่มีเจตนาก็เป็นได้ นอกจากนี้ ประโยชน์ที่ได้รับจากเทคโนโลยีดังกล่าวอาจทำให้เกิดการละเมิดลิขสิทธิ์ที่ได้รับความคุ้มครองให้เป็นทรัพย์สินทางปัญญา โดยเฉพาะการละเมิดลิขสิทธิ์ซอฟต์แวร์ที่เป็นปัญหาใหญ่ในขณะนี้

แบบฝึกหัด

1. อธิบายแนวคิดเกี่ยวกับระบบรักษาความปลอดภัยในระบบคอมพิวเตอร์
2. ให้อธิบาย Hacker คืออะไร
3. ให้อธิบาย Cracker คืออะไร
4. ให้บอกระบบรักษาความปลอดภัยของคอมพิวเตอร์สามารถแบ่งออกได้กี่รูปแบบ อะไรบ้าง
5. อธิบายการรักษาความปลอดภัยในองค์กร
6. อธิบายการรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ต
7. อธิบายการรักษาความปลอดภัยของข้อมูลส่วนบุคคลแนวโน้มของระบบรักษาความปลอดภัยในอนาคต
8. ให้บอกจริยธรรมทางด้านคอมพิวเตอร์ มีอะไรบ้าง