บทที่ 11
การรักษาความปลอดภัยระบบสารสนเทศและจรรยาบรรณเบื้องต้น

1. วัตถุประสงค์ของบท

เมื่อได้ศึกษาเนื้อหาของบทนี้แล้ว ผู้ศึกษาควรสามารถเข้าใจถึง

1. ประเภทของบุคคลที่เกี่ยวข้องกับความเสี่ยงของระบบสารสนเทศ
2. ประเภทของความเสี่ยงของระบบสารสนเทศ
3. การรักษาความปลอดภัยของระบบสารสนเทศ
4. จรรยาบรรณที่เกี่ยวข้องกับระบบสารสนเทศ

2. บทนำ

เป็นที่ทราบกันดีแล้วว่าปัจจุบันธุรกิจต่างๆ ไม่ว่าจะเป็นกิจการขนาดเล็ก กลาง หรือใหญ่ จะนำระบบสารสนเทศมาใช้งานอย่างกว้างขวาง ซึ่งการใช้งานระบบสารสนเทศนั้นมิได้จำกัดภายในหน่วยงานของกิจการเท่านั้นแต่ยังมีการเชื่อมโยงระบบสารสนเทศเป็นเครือข่าย เพื่อสื่อสารข้อมูลและสารสนเทศทั้งภายในและภายนอกกิจการ การนำระบบสารสนเทศมาใช้งานก่อให้เกิดภัยในรูปแบบใหม่ซึ่งมีความแตกต่างจากภัยในรูปแบบเดิมโดยเฉพาะกับระบบเครือข่ายคอมพิวเตอร์ จากการสำรวจถึงความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ของกิจการต่างๆ โดยบริษัท RDI Computer จำกัด พบว่า 46% ของกิจการที่สำรวจเคยมีประสบการณ์จากการถูกคุกคามความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ 57% ของกิจการที่สำรวจมีความเห็นว่าความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์มีความสำคัญ ในขณะที่ 80% ของกิจการที่สำรวจทั้งหมดยังมิได้ติดตั้งระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ (Aldridge, 1997) ในบทนี้จะกล่าวถึงความเสี่ยงและการรักษาความปลอดภัยระบบสารสนเทศเบื้องต้น รวมถึงจรรยาบรรณที่เกี่ยวข้องกับระบบสารสนเทศ

3. ความเสี่ยงและการรักษาความปลอดภัยระบบสารสนเทศ

ความเสี่ยงของระบบสารสนเทศ (Information system risk) หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่ก่อให้เกิดการสูญเสียหรือทำลายฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) ข้อมูล สารสนเทศ หรือความสามารถในการประมวลผลข้อมูลของระบบ ความเสี่ยงที่เกิดกับระบบสารสนเทศมีทั้งที่กระทำโดยตั้งใจและไม่ตั้งใจ การทำอันตรายกับระบบสารสนเทศโดยตั้งใจมักเป็นการกระทำที่ผิดกฎหมายซึ่งถือเป็นอาชญากรรมทางคอมพิวเตอร์ (Computer crime) ถ้าอาชญากรรมนั้นเป็นการกระทำที่ขัดต่อกฎหมายออนไลน์หรืออินเทอร์เน็ตจะเรียกว่า Cybercrime ซึ่งเป็นอาชญากรรมที่ติดอันดับหนึ่งในสามของอาชญากรรมที่เป็นภัยสูงที่สุดที่ FBI ต้องทำคดี ปัจจุบันประเทศไทยได้ออกพระราชบัญญัติว่าด้วยการ

กระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และบังคับใช้แล้ว โดยกฎหมายดังกล่าวจะกล่าวถึงความผิดเกี่ยวกับคอมพิวเตอร์และบทลงโทษ เช่น การดักฟังข้อมูลทางคอมพิวเตอร์ระหว่างการจัดส่ง การทำลาย แก้ไข และเปลี่ยนแปลง ซึ่งข้อมูลทางคอมพิวเตอร์ของผู้อื่น เป็นต้น อย่างไรก็ตามในการศึกษาการรักษาความปลอดภัยระบบสารสนเทศควรทำความเข้าใจเกี่ยวกับสิ่งต่าง ๆ ดังนี้

3.1 ประเภทของบุคคลที่เกี่ยวข้องกับความเสี่ยงของระบบสารสนเทศ

ประเภทของบุคคลที่ก่อให้เกิดความเสี่ยงกับระบบสารสนเทศประกอบด้วย แฮกเกอร์ (Hacker) แครกเกอร์ (Cracker) ผู้ก่อให้เกิดภัยมือใหม่ (Script Kiddies) ผู้สอดแนม (Spies) เจ้าหน้าที่ขององค์กร (Employees) และผู้ก่อการร้ายทางคอมพิวเตอร์ (Cyberterrorist) ดังนี้

3.1.1 แฮกเกอร์ สามารถให้ความหมายทั้งแบบแคบและกว้าง ในความหมายแบบกว้างนั้น แฮกเกอร์คือบุคคลใดก็ตามที่พยายามเจาะเข้าไปในระบบสารสนเทศอย่างผิดกฎหมาย สำหรับความหมายแบบแคบ แฮกเกอร์คือบุคคลที่ใช้ทักษะหรือความสามารถที่สูงทางคอมพิวเตอร์เพื่อเจาะเข้าไปในระบบสารสนเทศของผู้อื่น แม้ว่าการกระทำดังกล่าวจะเป็นการกระทำที่ผิดกฎหมาย แต่แฮกเกอร์เชื่อว่าการกระทำดังกล่าวยอมรับได้ เพราะมีวัตถุประสงค์ในการแสดงให้เจ้าของระบบสารสนเทศทราบช่องโหว่ของการรักษาความปลอดภัยของระบบสารสนเทศ และปรับปรุงระบบรักษาความปลอดภัยของตนต่อไป แม้ว่าการแอบเข้าไปในระบบสารสนเทศของผู้อื่นจะเป็นการกระทำที่ผิดกฎหมายก็ตาม แต่แฮกเกอร์เชื่อว่าการกระทำดังกล่าวยอมรับได้ตราบใดที่ตนไม่ได้ขโมย ทำลายทรัพย์สิน หรือเปิดเผยความลับของกิจการ โดยแฮกเกอร์พวกนี้เชื่อว่าเป็นหน้าที่ของตนในการค้นหาช่องโหว่ของการักษาความปลอดภัยเพื่อแก้ไขช่องโหว่นั้นและมักจะเรียกตนเองว่า แฮกเกอร์ที่มีจรรยาบรรณ (Ethical hackers)

3.1.2 แครกเกอร์ คือบุคคลที่ทำอันตรายต่อการรักษาความปลอดภัยของระบบสารสนเทศโดยมีวัตถุประสงค์ร้าย โดยแครกเกอร์จะเป็นผู้ที่มีความรู้ทางคอมพิวเตอร์อย่างมากเช่นเดียวกับแฮกเกอร์ ต่างกันที่แครกเกอร์จะทำลายข้อมูลและทำให้ระบบสารสนเทศและเครือข่ายของกิจการมีปัญหาอย่างมาก

3.1.3 ผู้ก่อให้เกิดภัยมือใหม่ เป็นบุคคลที่มีเป้าหมายเช่นเดียวกับแครกเกอร์คือทำลายระบบสารสนเทศหรือเครือข่ายที่ตนเองสามารถเจาะเข้าไปได้ ความแตกต่างอยู่ที่ผู้ก่อให้เกิดภัยมือใหม่มักไม่มีทักษะทางด้านคอมพิวเตอร์มากนัก ส่วนมากจะทำการดาวน์โหลดซอฟต์แวร์ที่ช่วยในการเจาะระบบจากเว็บไซต์ (ซึ่งส่วนมากเป็นซอฟต์แวร์ที่ไม่ต้องจ่ายเงินซื้อ) ต่อจากนั้นจะใช้ซอฟต์แวร์ดังกล่าวเพื่อเจาะระบบสารสนเทศต่อไป แม้ว่าผู้ก่อให้เกิดภัยมือใหม่จะมีทักษะทางคอมพิวเตอร์น้อยก็ตามแต่ก็เป็นบุคคลที่อาจก่อให้เกิดภัยกับกิจการอย่างใหญ่หลวง เนื่องจากบุคคลพวกนี้มักเป็นคนที่มีอายุน้อยซึ่งมีเวลาอย่างไม่จำกัดที่จะใช้ในการเจาะระบบ นอกจากนี้บุคคลพวกนี้จะสนุกสนานกับการเจาะระบบให้มากที่สุดเท่าที่จะมากได้ จากการที่ไม่ค่อยมีความรู้ทางด้านเทคนิคคอมพิวเตอร์ ผู้ก่อให้เกิดภัยมือใหม่จะไม่เข้าใจเทคนิคของซอฟต์แวร์ที่นำมาใช้ทำให้ไม่กำหนดเป้าหมายในการเจาะระบบซึ่งส่งผลให้เกิดปัญหาอย่างมากได้

3.1.4 ผู้สอดแนม เป็นบุคคลที่ถูกจ้างเพื่อเจาะระบบสารสนเทศและขโมยข้อมูล ผู้สอดแนมมักเป็นคนที่มีทักษะทางคอมพิวเตอร์สูง โดยมีเป้าหมายของระบบที่ต้องการเจาะอย่างชัดเจน ไม่กระทำอย่างไร้จุดหมายของผู้ก่อให้เกิดภัยมือใหม่

3.1.5 เจ้าหน้าที่ขององค์กร เป็นภัยคุกคามที่มีจำนวนมากขึ้น โดยเจ้าหน้าที่จะเจาะเข้าไปในระบบสารสนเทศของกิจการของตนโดยมีเหตุผลเพื่อแสดงให้เห็นว่าระบบรักษาความปลอดภัยขององค์กรมีจุดอ่อน หรือเจ้าหน้าที่คิดว่าตนเองไม่ได้รับการยอมรับจึงต้องการแสดงให้เห็นว่าตนมีความสามารถ และต้องการเงินเช่นเดียวกับผู้สอดแนม

3.1.6 ผู้ก่อการร้ายทางคอมพิวเตอร์ เป็นบุคคลที่ถูกกล่าวถึงอย่างมากในประเทศต่างๆ ผู้ก่อการร้ายจะใช้ทุกสิ่งทุกอย่าง ไม่ว่าจะเป็นเครื่องบิน รถไฟ รถยนต์ หรือแม้แต่ชีวิตตนเองเพื่อทำอันตรายประชาชนผู้บริสุทธิ ทำให้เกิดความตื่นตระหนกกับประชาชนทั่วไป ประเทศต่างๆ เกรงว่าผู้ก่อการร้ายทางคอมพิวเตอร์จะใช้ความเชื่อของตนเองในการปรับเปลี่ยนข้อมูลสารสนเทศ หรือการทำให้ระบบสารสนเทศปฏิเสธการให้บริการกับผู้ใช้ที่มีสิทธิในการใช้ระบบอย่างถูกต้อง หรือเจาะเข้าไปในระบบเพื่อทำให้ข้อมูลเสียหายอย่างมาก ผู้ก่อการร้ายทางคอมพิวเตอร์เป็นนักเจาะระบบที่น่ากลัวมากที่สุดในจำนวนนักเจาะระบบทั้งหมดเนื่องจากเป็นผู้ที่มีทักษะทางคอมพิวเตอร์ที่สูงมาก นอกจากนี้ยังเป็นการยากที่จะทำนายว่าการโจมตีจะเกิดเวลาไหนและที่ใด เนื่องจากผู้ก่อการร้ายทางคอมพิวเตอร์จะหลบซ่อนตัวเป็นเวลานานและโจมตีเครือข่ายในรูปแบบใหม่อย่างฉับพลันและรวดเร็ว

3.2 ประเภทของความเสี่ยงของระบบสารสนเทศ

ประเภทของความเสี่ยงของระบบสารสนเทศ ประกอบด้วย การโจมตีระบบเครือข่าย การเข้าถึงระบบโดยไม่ได้รับอนุญาต การขโมย และความล้มเหลวของระบบสารสนเทศ

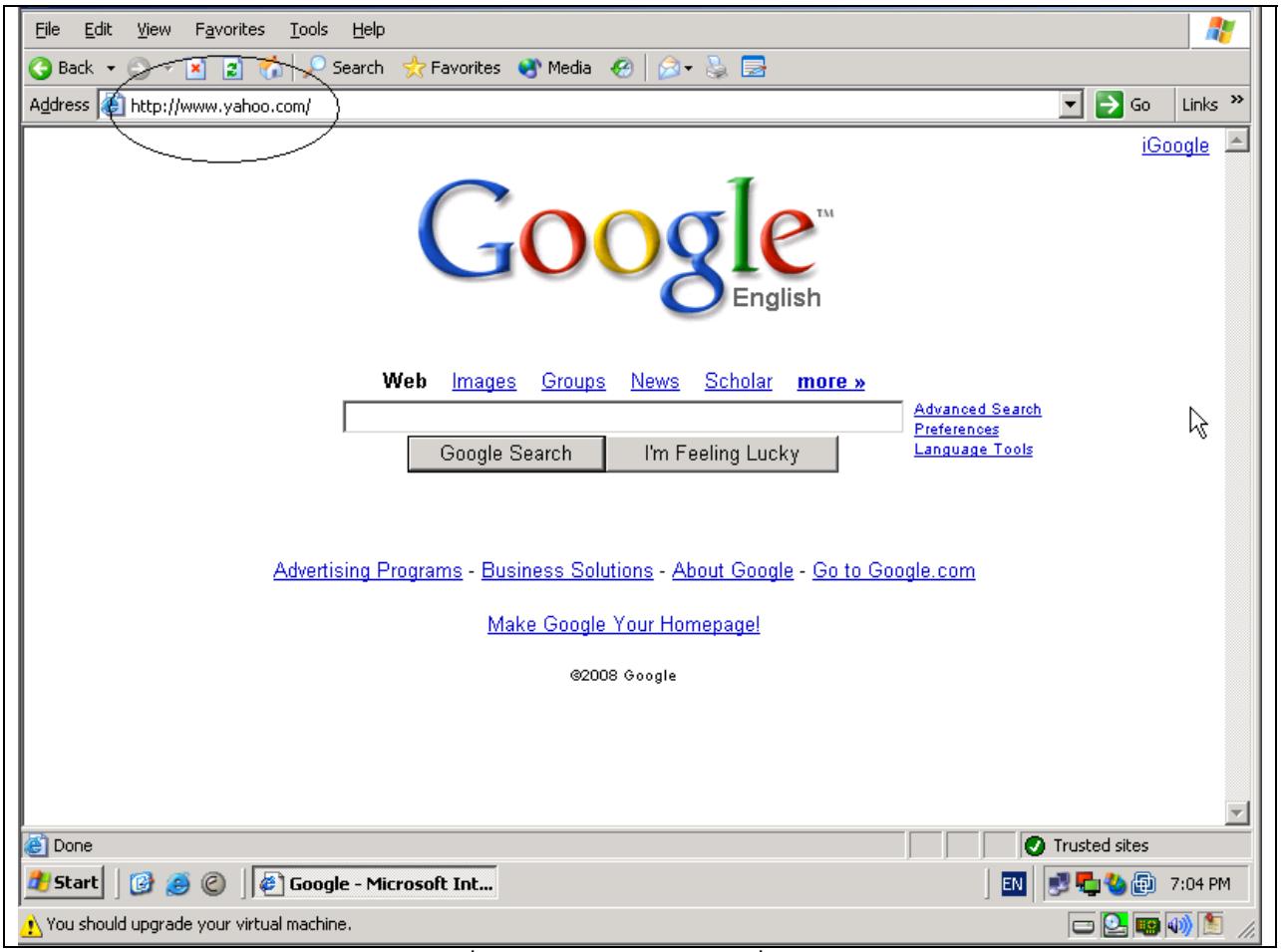
3.2.1 การโจมตีระบบเครือข่าย (Network attack)

การโจมตีระบบเครือข่ายสามารถแบ่งออกเป็น 4 ประเภทคือ การโจมตีขั้นพื้นฐาน (Basic Attacks) การโจมตีด้านคุณลักษณะ (Identity Attacks) การปฏิเสธการให้บริการ (Denial of Service หรือ DoS) และการโจมตีด้วยมัลแวร์ (Malware)

(1) การโจมตีขั้นพื้นฐาน เป็นการโจมตีระบบเครือข่ายคอมพิวเตอร์ที่ผู้โจมตีไม่ต้องมีความรู้ทางด้านเทคนิคคอมพิวเตอร์มากนัก ส่วนมากจะใช้หลักการเดาและความฉลาดแกมโกง ตัวอย่างการโจมตีขั้นพื้นฐาน เช่น กลลวงทางสังคม (Social Engineering) เป็นวิธีการง่ายๆ ที่ใช้โจมตีระบบซึ่งไม่ต้องใช้ความรู้ทางด้านเทคโนโลยี ทำโดยการหลอกลวงผู้ที่เกี่ยวข้องกับระบบคอมพิวเตอร์เพื่อสอบถามข้อมูลเบื้องต้นของผู้เข้าระบบ เช่น เจ้าหน้าที่ของหน่วยงานให้ความช่วยเหลือ (Help Desk) ถูกหลอกให้หลงเชื่อและเปิดเผยข้อมูลที่จำเป็นต่อการเข้าถึงระบบหรือรหัสผ่านของผู้ใช้งาน เป็นต้น อนึ่งวิธีการกลลวงทางสังคม

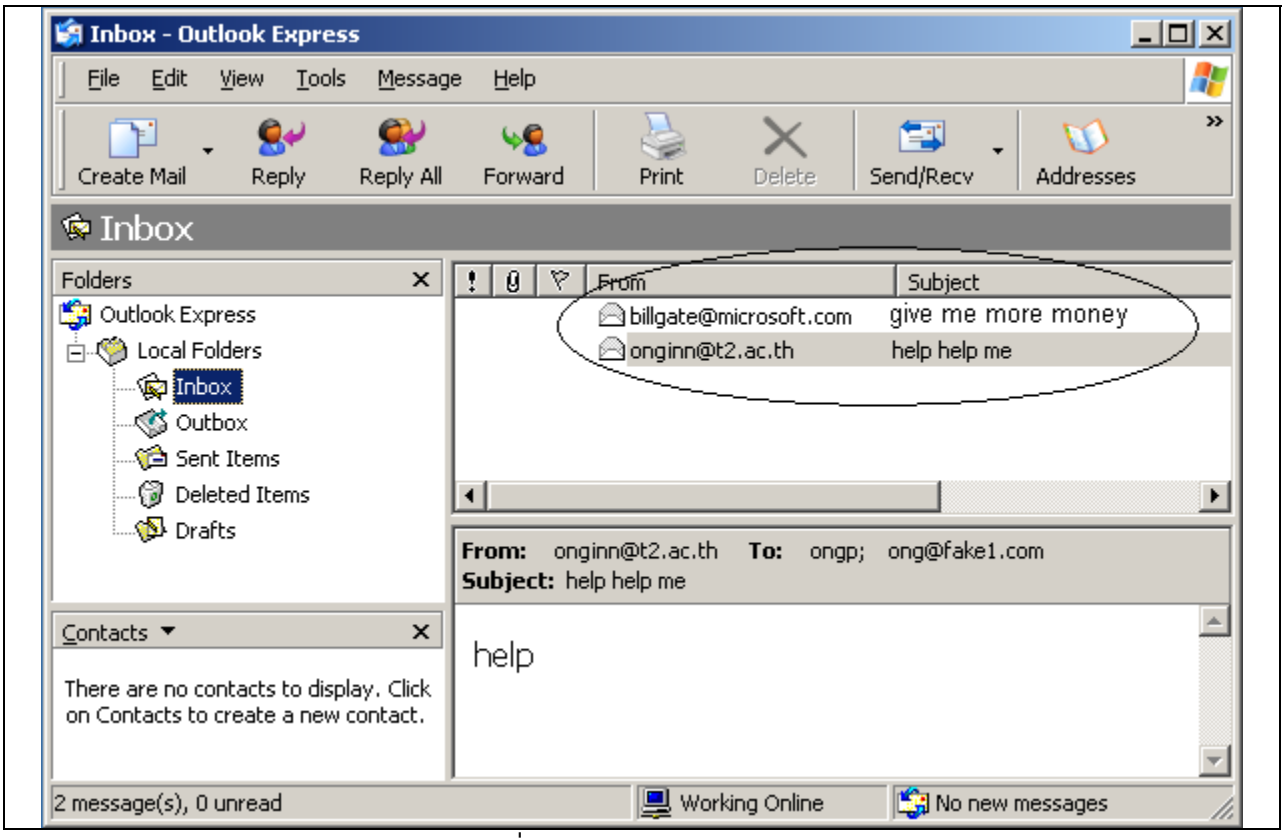
ยังหมายรวมถึงการค้นหาคู่มือคอมพิวเตอร์ รายงานที่พิมพ์จากคอมพิวเตอร์ หรือรายละเอียดรหัสผ่านที่ถูกนำไปทิ้งที่ถังขยะ ซึ่งเรียกวิธีการนี้ว่า Dumpster Diving

(2) การโจมตีด้านคุณลักษณะ เป็นการโจมตีระบบเครือข่ายคอมพิวเตอร์ที่ผู้โจมตีพยายามลักลอบดักจับข้อมูลซึ่งเป็นลักษณะเฉพาะของผู้ใช้ระหว่างการส่งผ่านข้อมูลในระบบเครือข่าย ตัวอย่างการโจมตีด้านคุณลักษณะ เช่น การโจมตีแบบปล้น TCP/IP (Transmission Control Protocol/Internet Protocol (TCP/IP) hijacking attacks) เป็นการโจมตีในลักษณะของการปลอมตัวหรือสปูฟฟิง (Spoofing) กล่าวคือทำให้อีกฝ่ายหนึ่งเข้าใจว่าตนเป็นอีกบุคคลหนึ่ง ประเภทของการปลอมตัวที่นิยมนำมาโจมตีกัน เช่น DNS Spoofing เป็นต้น วิธีการดังกล่าวเป็นวิธีที่เมื่อผู้ใช้ป้อน URL ของเว็บที่ต้องการเข้าถึง เช่น Yahoo เป็นต้น แทนที่เครื่องคอมพิวเตอร์จะเข้าไปที่เว็บนั้นแต่กลับไปเข้าที่เว็บอื่นที่ผู้เจาะระบบกำหนดไว้ (ซึ่งส่วนมากจะเป็นเว็บปลอม) ดังแสดงในภาพที่ 1



ภาพที่ 1 การเข้า Web page ที่ถูก spoof

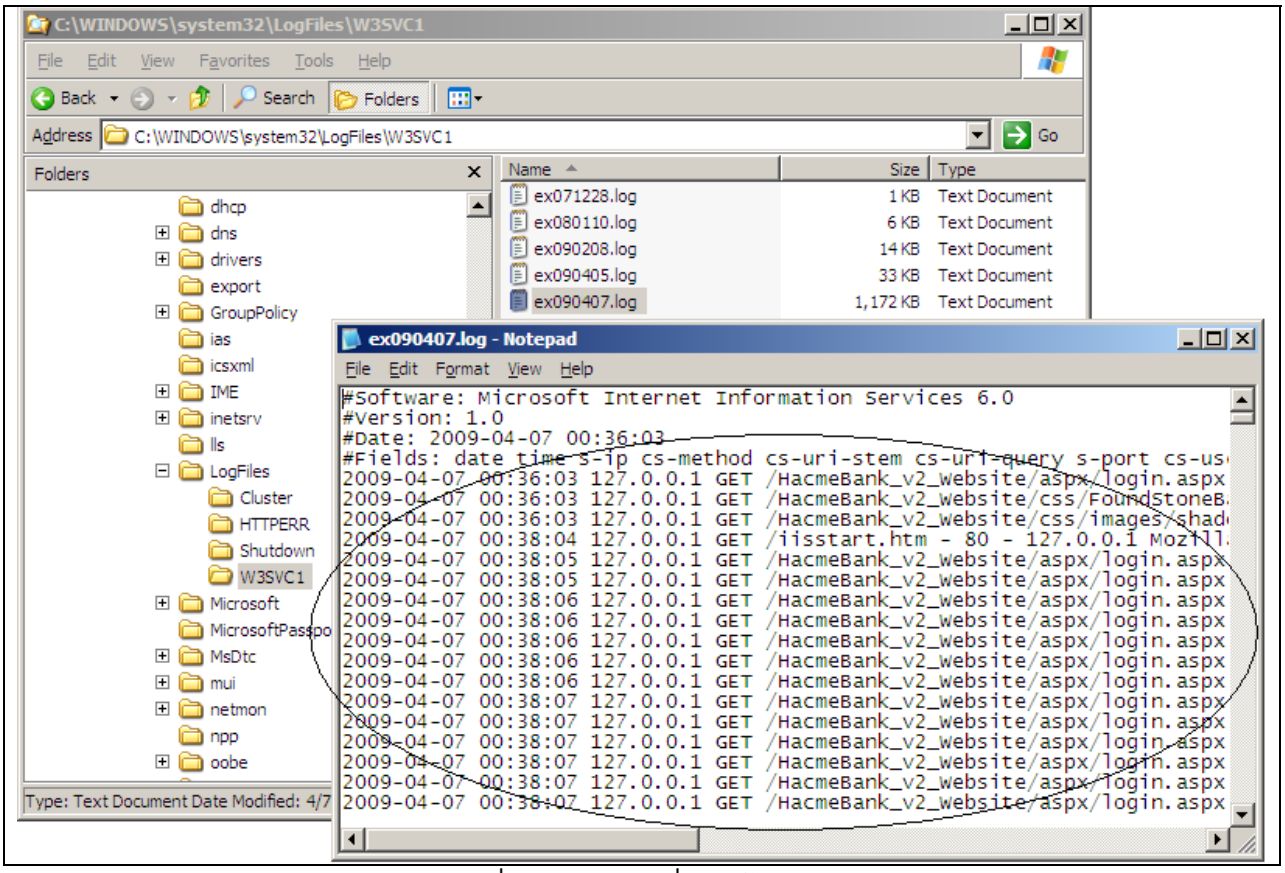
อีกตัวอย่างของการทำ Spoofing หรือการปลอมตัวที่พบเห็นบ่อยคือ การทำ e-mail spoofing ซึ่งเป็นการปลอมหรือเปลี่ยนแปลงชื่อผู้ส่งอีเมลหรือองค์ประกอบส่วนหัวของอีเมลเพื่อให้ดูเหมือนว่าอีเมลส่งมาจากเจ้าของอีเมลจริง ภาพที่ 2 แสดงตัวอย่างของอีเมลปลอมที่จัดส่งมาจาก billgate@microsoft.com



ภาพที่ 2 ตัวอย่างของอีเมลปลอม

(3) การปฏิเสธการให้บริการ เป็นการโจมตีระบบเครือข่ายคอมพิวเตอร์โดยพยายามทำให้เครื่องเซิร์ฟเวอร์ (Server) หยุดให้บริการ ซึ่งทำโดยการใช้ทรัพยากรของเซิร์ฟเวอร์จนหมด ในการโจมตีนั้นสามารถใช้เครื่องคอมพิวเตอร์เครื่องเดียวเพื่อร้องขอบริการจากเครื่องเซิร์ฟเวอร์เป็นจำนวนมาก หรือทำการติดตั้งโปรแกรมที่เครื่องคอมพิวเตอร์เครื่องอื่นๆ แล้วส่งคำสั่งให้เครื่องเหล่านั้นไปขอบริการจากเครื่องเซิร์ฟเวอร์ซึ่งเรียกว่า การโจมตีแบบ Distributed denial-of-service (DDoS) ส่วนเครื่องที่ถูกบังคับให้ส่งคำร้องขอนี้ว่าถูกเรียกว่า Zombie โดยเครื่องที่เป็น Zombie ไม่เพียงแต่ส่งคำร้องขอเป็นจำนวนมากเท่านั้นยังทำให้การค้นหาว่าเครื่องใดก่อให้เกิด DDos เป็นไปได้ยากเช่นกัน ปัจจุบันการโจมตีในลักษณะการปฏิเสธ

การให้บริการจะทำในลักษณะของ DDoS มากกว่า ภาพที่ 3 แสดงให้เห็นถึงกลุ่มข้อมูลจำนวนมากที่ถูกส่งมายังเว็บ HacmeBank ด้วยโปรแกรม DoSHTTP (HTTP Flood Denial of Service)



ภาพที่ 3 กลุ่มข้อมูลที่จัดส่งไปยังเว็บ

นอกเหนือจาก DDoS ดังกล่าวข้างต้นแล้ว เครื่องคอมพิวเตอร์ยังอาจถูก Hijacking กล่าวคือเครื่องคอมพิวเตอร์หรือกลุ่มเครื่องคอมพิวเตอร์ถูกติดตั้งโปรแกรมขนาดเล็กที่เรียกว่า bot โดยไม่รู้ตัวเหมือนการติดโปรแกรมไวรัส ซึ่งโปรแกรม bot นี้อาจมีแหล่งที่มาจากการเข้า Chat rooms และการแลกเปลี่ยนแฟ้มข้อมูลผ่านทางระบบเครือข่ายคอมพิวเตอร์ การนำโปรแกรม bot เข้าไปใส่ในเครื่องคอมพิวเตอร์เครื่องต่างๆ เพื่อสร้างเป็น botnet และเรียกกลุ่มเครื่องคอมพิวเตอร์นั้นว่า zombie army โดยวัตถุประสงค์หลักของ botnet คือการทำ Spam โดยโปรแกรม bot จะสั่งให้เครื่องคอมพิวเตอร์ที่ถูก Hijacking ปฏิบัติงานซ้ำๆ ในการส่งอีเมลเป็นจำนวนมาก (Spam via e-mail) หรือการส่งไวรัสและโปรแกรมมัลแวร์ ไปโจมตีระบบเครือข่ายอื่นๆ บนอินเทอร์เน็ต เครื่องคอมพิวเตอร์ที่ถูก Hijacking จะทำให้การเชื่อมต่อทางอินเทอร์เน็ตช้ามาก

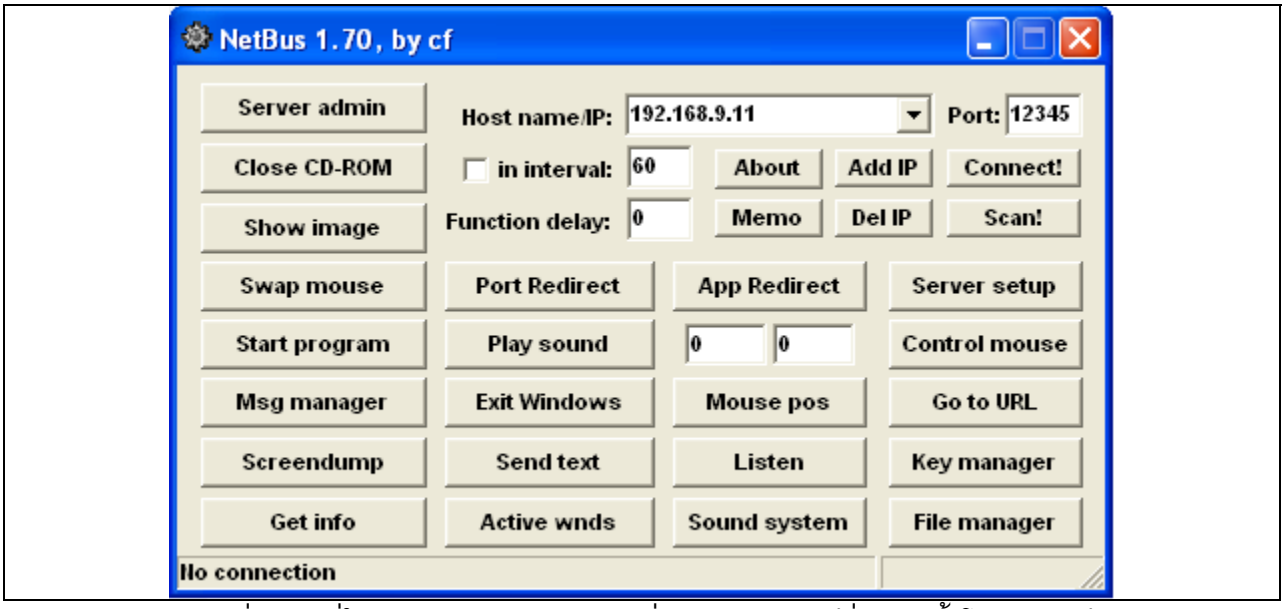
(4) การโจมตีด้วยมัลแวร์ บางครั้งเรียกว่าโปรแกรมมุ่งร้าย หมายถึงโปรแกรมทางคอมพิวเตอร์ที่ถูกออกแบบมาเพื่อสร้างความเสียหายให้กับเครื่องคอมพิวเตอร์ ในที่นี้จะแบ่งโปรแกรมมุ่งร้ายเป็น 2 ประเภทคือ โปรแกรมมุ่งร้ายที่โจมตีการปฏิบัติงานของคอมพิวเตอร์ (Computer's operations) ประกอบด้วย ไวรัส (Viruses) เวิร์ม (Worms) โทรจันฮอร์ส (Trojan horse) และลอจิกบอมบ์ (Logic bombs) และโปรแกรมมุ่งร้ายที่โจมตีความเป็นส่วนตัวของสารสนเทศ (Information privacy) ที่มีชื่อเรียกทั่วไปว่า สปายแวร์ (Spyware) ซึ่งเป็นโปรแกรมที่ละเมิดความปลอดภัยของบุคคล โดยสปายเวร์มีลักษณะที่ก่อให้เกิดอันตรายมากกว่าไวรัสและเวิร์ม เนื่องจากสปายเวร์มีเป้าหมายในการลักลอบขโมยข้อมูลส่วนบุคคลของผู้ใช้คอมพิวเตอร์ ต่อจากนั้นจะนำข้อมูลดังกล่าวไปซื้อสินค้า กู้เงิน และอื่นๆ ทำให้สปายเวร์ถูกออกแบบมาให้ยากต่อการตรวจจับและการทำลายทิ้ง เครื่องมือของสปายเวร์ประกอบด้วย แอดแวร์ (Adware) พิชชิง (Phishing) คีลอกเกอะ (Keyloggers) การเปลี่ยนการปรับแต่งระบบ (Configuration Changers) การต่อหมายเลข (Dialers) และ แบ็คดอร์ (Backdoors) ต่อไปจะกล่าวถึงมัลแวร์ข้างต้น

- **ไวรัส** หมายถึงโปรแกรมที่ติดตัวเองไปกับเอกสารหรือโปรแกรมและจะทำการประมวลผลเมื่อเอกสารหรือโปรแกรมนั้นถูกเปิด ไวรัสจะก่อให้เกิดปัญหาได้มากมายกับเครื่องคอมพิวเตอร์ เช่น ล้างข้อมูลออกจากที่จัดเก็บ ขยายขนาดของโปรแกรมเพื่อให้ใช้พื้นที่ของเครื่องคอมพิวเตอร์เป็นจำนวนมาก หรืออนุญาตให้ผู้โจมตีสามารถเข้าถึงเครื่องคอมพิวเตอร์ในระยะไกลได้ เป็นต้น

การติดไวรัสอาจอยู่ในรูปของ Virus hoax ซึ่งอยู่ในรูปของการส่งข้อความทางอีเมล ซึ่งไม่มีไวรัส เวิร์ม หรือโทรจันฮอร์ส แต่เป็นการส่งจดหมายลูกโซ่ (Chain letter) โดยอีเมลจะขอให้ผู้รับส่งสำเนาของข้อความในอีเมลนั้นไปยังคนอื่นๆ ให้มากที่สุดเท่าที่จะมากได้

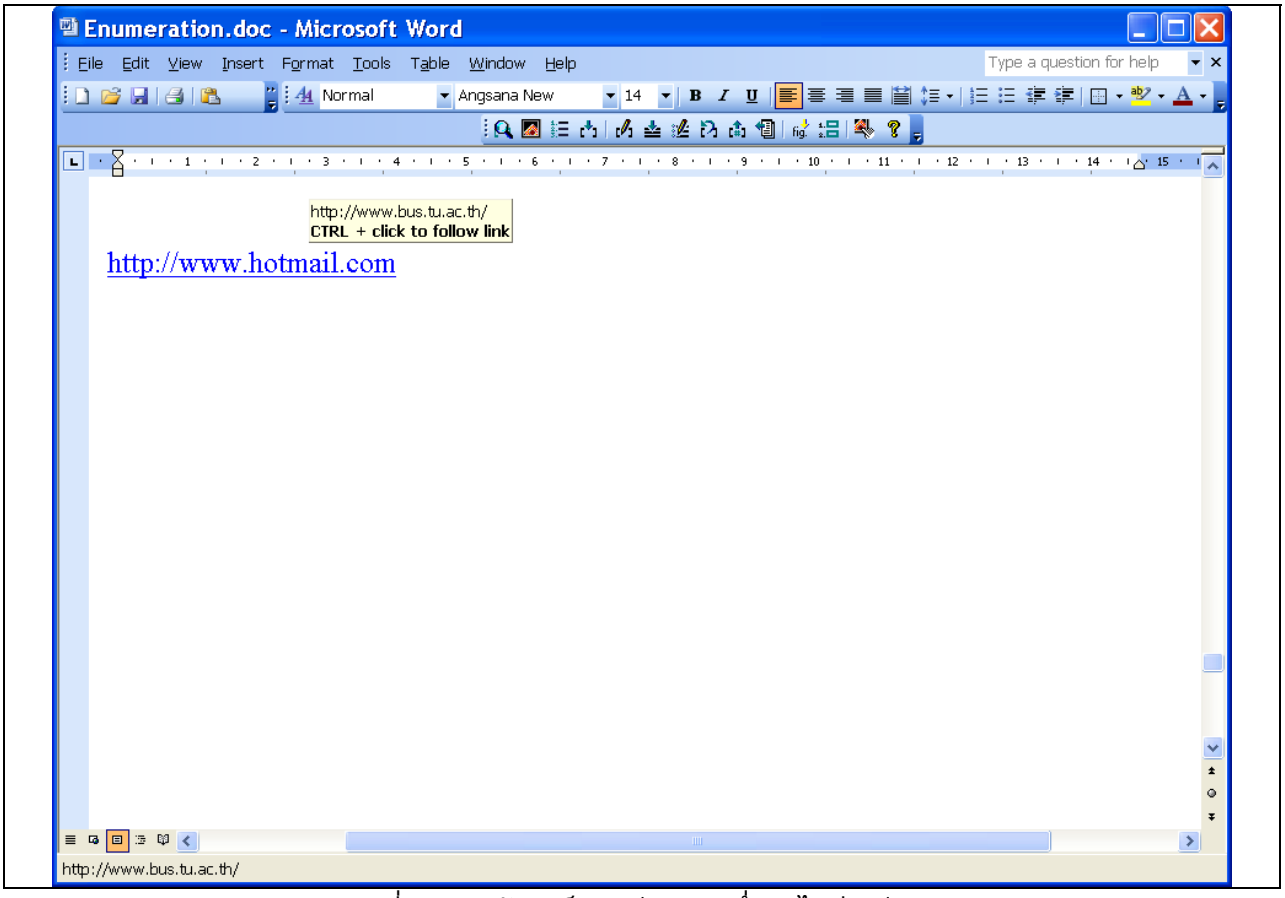
- **เวิร์ม** เป็นโปรแกรมมุ่งร้ายเช่นเดียวกับไวรัส แต่มีความแตกต่างกัน 2 ประการคือ ประการแรก ไวรัสเป็นโปรแกรมที่ติดตัวเองไปกับเอกสารทางคอมพิวเตอร์ ในขณะที่เวิร์มสามารถที่จะไปยังที่ต่างๆ ได้ด้วยตัวเอง ประการที่สอง ไวรัสต้องอาศัยผู้ใช้งานสั่งให้ประมวลผลโปรแกรม แต่เวิร์ม สามารถประมวลผลได้ด้วยตนเอง ส่งผลให้เวิร์มทำการเพิ่มขนาดตัวเองจนกระทั่งเต็มพื้นที่จัดเก็บข้อมูล

- **โทรจันฮอร์ส** คือโปรแกรมที่ทำลายระบบคอมพิวเตอร์โดยแฝงมากับโปรแกรมอื่นๆ เช่น เกม เป็นต้น ซึ่งเมื่อติดตั้งโปรแกรมที่มีโทรจันฮอร์สแฝงมาด้วยก็จะทำลายระบบคอมพิวเตอร์ เช่น ลบไฟล์ต่างๆ เป็นต้น ภาพที่ 4 แสดงปุ่มที่เครื่องคอมพิวเตอร์ระยะไกล (Remote computer) สามารถส่งคำสั่งเพื่อควบคุมการทำงานของเครื่องคอมพิวเตอร์ที่ถูกติดตั้งโปรแกรมโทรจันฮอร์สที่ชื่อว่า NetBus เช่น การควบคุม Mouse (Control mouse) ของเครื่องคอมพิวเตอร์ที่มีหมายเลข IP 192.168.9.11 เป็นต้น



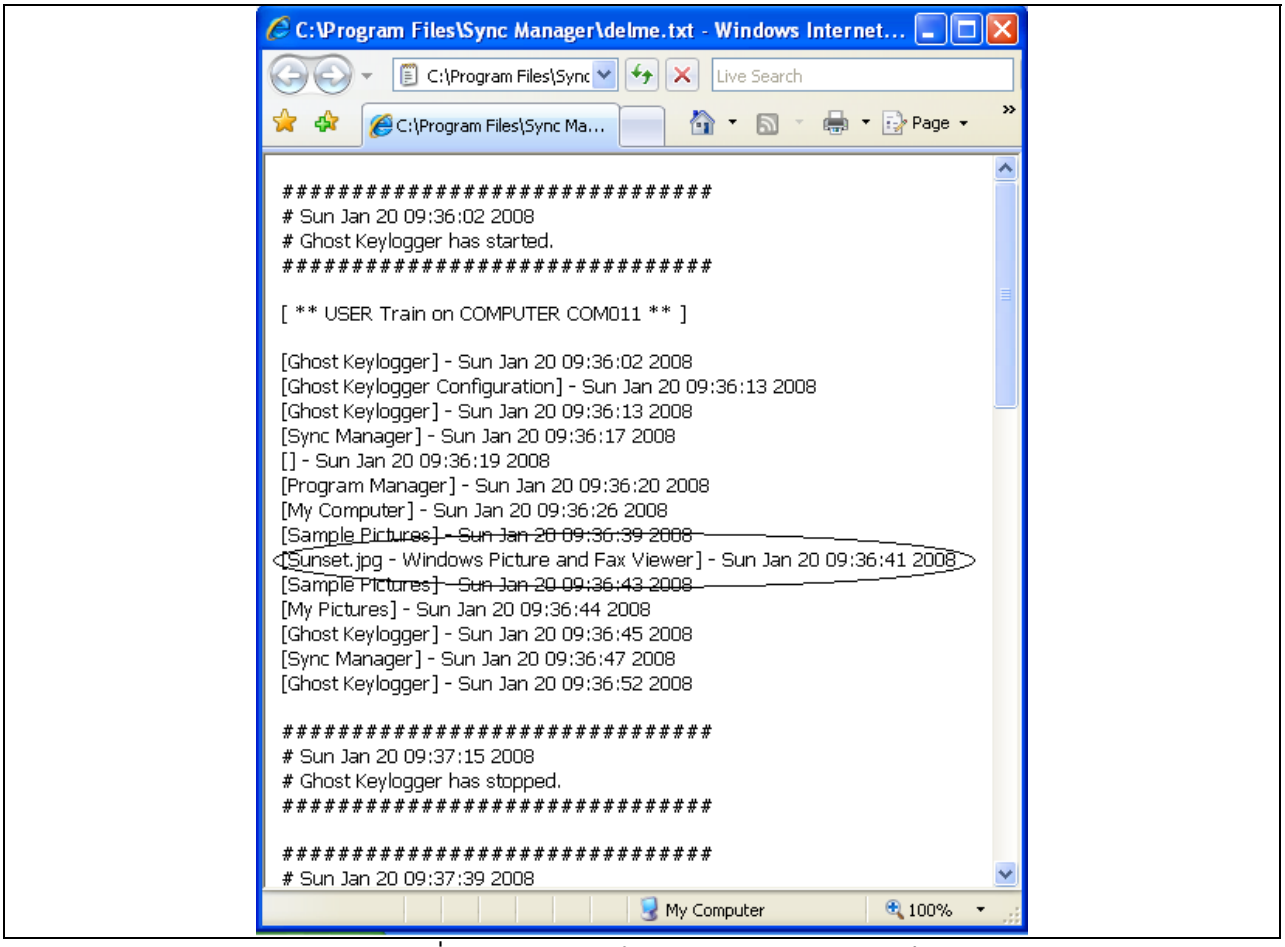
ภาพที่ 4 ปุ่มที่ใช้บังคับการทำงานของเครื่องคอมพิวเตอร์ที่ถูกติดตั้งโทรจันฮอร์ส

- **ลอจิกบอมบ์** เป็นโปรแกรมที่แฝงตัวในโปรแกรมคอมพิวเตอร์ แต่จะยังไม่ทำงานจนกว่าเงื่อนไขที่กำหนดเกิดขึ้น
- **แบ็คดอร์** เป็นวิธีการเข้าถึงโปรแกรมหรือระบบคอมพิวเตอร์โดยไม่ได้รับอนุมัติ โดยวิธีการดังกล่าวทำให้การเข้าถึงระบบไม่ต้องผ่านขั้นตอนการป้อนรหัสประจำตัวและรหัสผ่าน เมื่อผู้บุกรุกสามารถเข้าสู่ระบบแล้วมักจะทำกิจกรรมต่างๆ ต่อระบบ เช่น เปิดโปรแกรม จัดส่งแฟ้มข้อมูล รวมถึงการทำสำเนา เปลี่ยนชื่อ ลบแฟ้มข้อมูล และทำให้คอมพิวเตอร์ไม่สามารถทำงานตามปกติได้ เป็นต้น
- **แอดแวร์** คือโปรแกรมที่จะแสดงข้อความโฆษณาที่เว็บเพจโดยที่ผู้ใช้งานมิได้คาดหวังหรือไม่ต้องการ การแสดงโฆษณาดังกล่าวจะทำให้ผู้ใช้งานเกิดความรำคาญและทำให้ประสิทธิภาพการทำงานต่ำได้
- **พิชชิง** คือการส่งอีเมลไปให้ผู้ใช้ เมื่อผู้ใช้เข้าไปในเว็บไซต์ที่แสดงในอีเมลก็จะแสดงเว็บเพจ ปลอมซึ่งมีการจัดทำหน้าเว็บเพจให้เหมือนของจริง ถ้าผู้ใช้ป้อนรหัสผ่านหรือเลขที่บัตรเครดิตเข้าไปในเว็บเพจดังกล่าว ข้อมูลก็จะถูกขโมยและนำไปใช้ต่อไป ภาพที่ 5 แสดงให้เห็นว่าข้อความในอีเมลที่ส่งให้ผู้ใช้แสดงลิงค์ไปที่เว็บ www.hotmail.com แต่เมื่อผู้ใช้คลิกลิงค์นั้นจะไปที่ www.bus.tu.ac.th แทน นอกจากนี้ยังมีวิธีการ **พาร์มมิง (Pharming)** ที่มีเป้าหมายเพื่อต้องการข้อมูลส่วนตัวและข้อมูลทางการเงินของผู้ใช้คอมพิวเตอร์เช่นเดียวกับฟิชชิง แตกต่างกันที่แทนที่จะขอให้ผู้ใช้เข้าเยี่ยมชมเว็บไซต์ปลอมดังเช่นพิชชิง วิธีการนี้จะเชื่อมโยงผู้ใช้ไปยังเว็บไซต์ปลอมอัตโนมัติเมื่อผู้ใช้ป้อนที่อยู่เว็บในเว็บเบราว์เซอร์ ด้วยวิธีการของ DNS Spoofing (ดังแสดงในภาพที่ 1)



ภาพที่ 5 การเข้าลิงค์ของเว็บเพจหนึ่งแต่ไปอีกเว็บเพจ

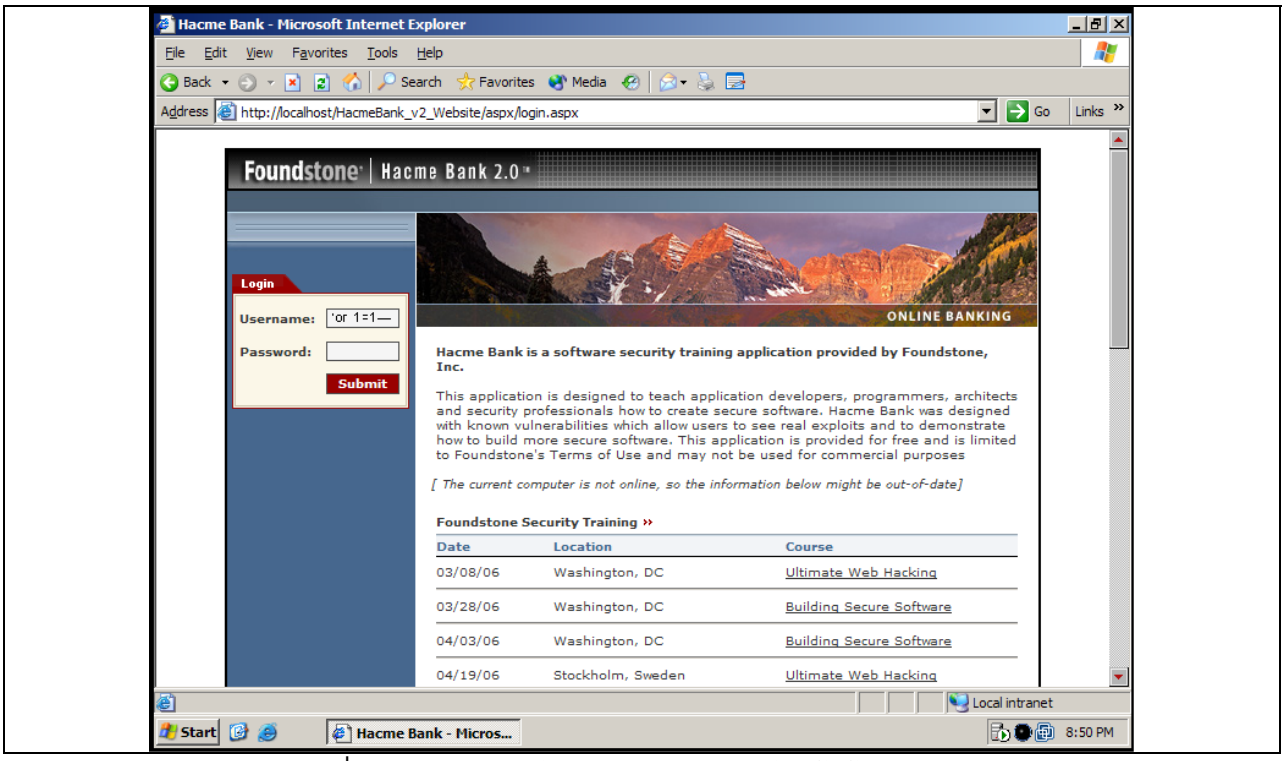
- **คีลอกเกอะ**อาจเป็นอุปกรณ์คอมพิวเตอร์หรือโปรแกรมขนาดเล็กที่บันทึกการกดแป้นพิมพ์เพื่อป้อนตัวอักขระและจัดเก็บในแฟ้มข้อมูล ต่อจากนั้นจะจัดส่งแฟ้มดังกล่าวไปยังผู้มุ่งร้ายซึ่งจะหาข้อมูลการกดแป้นพิมพ์ที่เกี่ยวกับรหัสประจำตัวและรหัสผ่าน เลขที่บัตรเครดิต และข้อมูลส่วนบุคคล ภาพที่ 6 แสดงรายงานที่บันทึกข้อมูลการเรียกแฟ้มรูปภาพ Sunset.jpg ของเครื่องคอมพิวเตอร์ที่ถูกแอบติดตั้งโปรแกรมคีลอกเกอะ



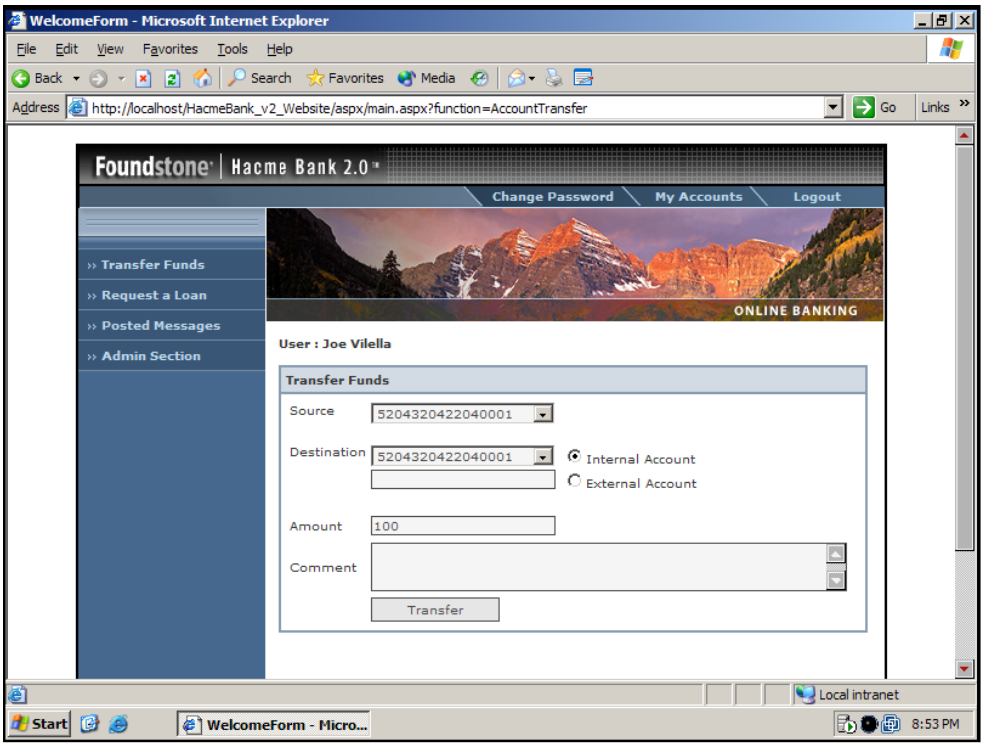
ภาพที่ 6 รายงานบันทึกข้อมูลการกดแป้นพิมพ์

นอกเหนือจากการโจมตีระบบเครือข่ายด้วยวิธีดังกล่าวข้างต้นแล้วยังมีการโจมตีด้วย การเดารหัสผ่าน (Password Guessing) การขโมยทรัพย์สินทางกายภาพ (Physical Theft) การนำคอมพิวเตอร์เก่ามาใช้ใหม่อย่างไม่เหมาะสม (Recycled Computers) การโจมตีแบบผ่านบุคคลที่สาม (Man-in-the-middle) และการตอบกลับ (Replay) การเปลี่ยนการปรับแต่งระบบ และการต่อหมายเลข ซึ่งจะไม่กล่าวถึงรายละเอียดในที่นี้ ผู้สนใจสามารถศึกษาในรายละเอียดจากวิชาที่เกี่ยวข้อง

3.2.2 การเข้าถึงระบบโดยไม่ได้รับอนุญาต (Unauthorized access) หมายถึงการใช้คอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์โดยไม่มีสิทธิ ซึ่งส่วนมากจะเป็นการใช้คอมพิวเตอร์หรือข้อมูลในเครื่องคอมพิวเตอร์เพื่อทำกิจกรรมบางอย่างที่ผิดกฎระเบียบของกิจการหรือการกระทำที่ผิดกฎหมาย เช่น พนักงานใช้เครื่องคอมพิวเตอร์ของกิจการทำงานส่วนตัว หรือการเข้าระบบคอมพิวเตอร์ของทางธนาคารเพื่อโอนเงินของผู้อื่นเข้าบัญชีตนเอง เป็นต้น ภาพที่ 7 แสดงตัวอย่างของการใช้วิธีที่เรียกว่า SQL injection เพื่อเข้าถึงระบบโอนเงินของทางธนาคารและโอนเงินของผู้อื่นเข้าบัญชีของตนโดยไม่ได้รับอนุญาต จากภาพจะเห็นว่าเมื่อป้อนรหัสผ่านเป็น ‘or 1=1— จะสามารถเข้าสู่ระบบคอมพิวเตอร์ของธนาคารเพื่อทำธุรกรรมต่างๆ ได้โดยไม่จำเป็นต้องเป็นผู้ที่มีสิทธิเท่านั้น อีกวิธีหนึ่งที่สามารถเข้าสู่ระบบโดยไม่ได้รับอนุญาตซึ่งเป็นวิธีที่มีการนำมาใช้อย่างกว้างขวาง คือการเดารหัสผ่านซึ่งสามารถทำโดยการใช้โปรแกรมช่วยเดารหัสผ่านหรือวิธีกลลวงทางสังคมดังกล่าวมาแล้วข้างต้น



ภาพที่ 7 การเข้าระบบโอนเงินของธนาคารโดยไม่ได้รับอนุญาต



ภาพที่ 7 การเข้าระบบโอนเงินของธนาคารโดยไม่ได้รับอนุญาต (ต่อ)

3.2.3 การขโมย (Theft) คือการนำทรัพย์สินด้านระบบสารสนเทศของกิจการออกไปโดยไม่มีสิทธิ ซึ่งการนำทรัพย์สินออกไปนั้นอาจอยู่ในรูปของการขโมยหรือการทำลายทรัพย์สิน (Vandalism) โดยทรัพย์สินในที่นี้ประกอบด้วย ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) และสารสนเทศ (Information)

การขโมยฮาร์ดแวร์ทำโดยการลักเครื่องคอมพิวเตอร์โดยตรง ส่วนการทำลายฮาร์ดแวร์มักอยู่รูปของการตัดสายเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์เพื่อไม่สามารถเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ได้ ส่วนการขโมยซอฟต์แวร์อาจอยู่ในรูปของการขโมยสื่อจัดเก็บซอฟต์แวร์ การลบโปรแกรมโดยตั้งใจ และการทำสำเนาโปรแกรมอย่างผิดกฎหมาย เช่น ซื้อซอฟต์แวร์สำหรับผู้ใช้คนเดียว (Single-user license agreement) แต่จัดทำสำเนา ให้ยืม ให้เช่า หรือทำการกระจายซอฟต์แวร์ดังกล่าวให้กับคนอื่น เป็นต้น การกระทำดังกล่าวเป็นการละเมิดลิขสิทธิ์ (Violation of copyright law) นอกจากนี้การขโมยซอฟต์แวร์ยังรวมถึงการนำซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ (Software piracy) ไปใช้งาน ในบางกรณีซอฟต์แวร์เหล่านั้นเป็นที่กระจายไวรัสได้เช่นกัน ท้ายที่สุดการขโมยสารสนเทศ มักอยู่ในรูปของการขโมยข้อมูลที่เป็นความลับส่วนบุคคล ผลเสียหายที่เกิดจากข้อมูลถูกขโมยนั้นเทียบเท่ากับการที่ฮาร์ดแวร์และซอฟต์แวร์ถูกขโมย กล่าวคือข้อมูลที่ถูกขโมยอาจถูกนำไปขายให้กับคู่แข่งหรือเลขที่บัตรเครดิตที่ถูกขโมยถูกนำไปซื้อสินค้าและบริการตามที่ต่างๆ

3.2.4 ความล้มเหลวของระบบสารสนเทศ (System failure) เป็นภัยที่ก่อให้เกิดผลกระทบอย่างกว้างขวางต่อฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล หรือสารสนเทศ สาเหตุสำคัญที่ทำให้ระบบล้มเหลว ประกอบด้วย ภัยธรรมชาติ (Natural disasters) เช่น ไฟไหม้ น้ำท่วม พายุ ปัญหาด้านกำลังไฟฟ้า และข้อผิดพลาดของการทำงานของโปรแกรม เป็นต้น การเปลี่ยนแปลงของไฟฟ้า (Electrical disturbances) ประกอบด้วย เสียง (Noise) แรงดันไฟฟ้าต่ำ (Undervoltages) และ แรงดันไฟฟ้าสูง (overvoltages)

เสียง คือสัญญาณที่ไม่ต้องการซึ่งส่วนมากจะแทรกมากับแรงดันไฟฟ้าที่ถูกส่งเข้าเครื่องคอมพิวเตอร์ เสียงนี้อาจเกิดจากอุปกรณ์ภายนอกเครื่องคอมพิวเตอร์เช่น หลอดไฟ วิทยุ และโทรทัศน์ หรือจากองค์ประกอบภายในเครื่องคอมพิวเตอร์เอง อย่างไรก็ตามเสียงไม่ก่อให้เกิดความเสี่ยงกับฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล เนื่องจากตัวจ่ายกระแสไฟ (Computer power supplies) สามารถกรองเสียงออกแรงดันไฟฟ้าได้

แรงดันไฟฟ้าต่ำ เกิดขึ้นเมื่อกระแสไฟตก กล่าวคือแรงดันไฟฟ้าต่ำกว่า 240 โวลต์ (สำหรับประเทศไทย ส่วนประเทศสหรัฐอเมริกาแรงดันไฟฟ้าปกติจะอยู่ที่ 120 โวลต์) โดยแรงดันไฟฟ้าอาจต่ำเป็นเวลานาน (Brownout) หรือไม่มีกระแสไฟเลย (Blackout) ก็ได้ ผลของกระแสไฟตกจะส่งผลให้ข้อมูลหายได้แต่ไม่ทำให้อุปกรณ์คอมพิวเตอร์เสียหาย

แรงดันไฟฟ้าสูง เกิดขึ้นเมื่อกระแสไฟมีกำลังสูงกว่าปกติ (สูงกว่า 240 โวลต์ สำหรับประเทศไทย) โดยฟ้าผ่าเป็นสาเหตุประการหนึ่งที่ทำให้เกิดแรงดันไฟฟ้าสูงได้ ผลของแรงดันไฟฟ้าสูงจะทำให้ฮาร์ดแวร์ถูกทำลายอย่างถาวร

3.3 การรักษาความปลอดภัยของระบบสารสนเทศ

ในส่วนนี้จะกล่าวถึงการรักษาความปลอดภัยเพื่อป้องกันการโจมตีระบบเครือข่าย การเข้าถึงระบบโดยไม่ได้รับอนุญาต การขโมย และความล้มเหลวของระบบสารสนเทศ

3.3.1 การรักษาความปลอดภัยการโจมตีระบบเครือข่าย การรักษาความปลอดภัยการโจมตีระบบเครือข่ายคอมพิวเตอร์สามารถทำได้ดังนี้

- ติดตั้งโปรแกรมป้องกันไวรัสและปรับปรุง Virus signature หรือ Virus definition ให้ทันสมัยอยู่เสมอ โดย Virus signature คือรูปแบบเฉพาะของโปรแกรมไวรัสที่รู้จัก การติดตั้งโปรแกรมป้องกันไวรัสในเครื่องคอมพิวเตอร์นอกจากป้องกันเครื่องคอมพิวเตอร์จากโปรแกรมมัลแวร์ต่างๆ นอกจากนี้ยังช่วยป้องกันเครื่องคอมพิวเตอร์จากการโจมตีการปฏิเสธการให้บริการด้วยเช่นกัน
- ติดตั้งไฟร์วอลล์ (Firewall) โดยไฟร์วอลล์เป็นการผสมผสานระหว่างอุปกรณ์คอมพิวเตอร์และโปรแกรมที่ติดตั้งระหว่างระบบคอมพิวเตอร์ของธุรกิจกับอินเทอร์เน็ต วัตถุประสงค์หลักของการติดตั้งไฟร์วอลล์ เพื่อควบคุมไม่ให้บุคคลภายนอกที่ไม่ได้รับอนุญาตเข้ามาในระบบเครือข่ายของธุรกิจได้ (ถ้าเปรียบเทียบระบบคอมพิวเตอร์เป็นบ้าน ไฟร์วอลล์เปรียบเสมือนกำแพงบ้านที่ป้องกันคนบุกรุก

เข้ามาในบ้านโดยไม่ได้รับอนุญาต) นอกจากนี้ไฟร์วอลล์ยังมีหน้าที่ในการป้องกันการส่งข้อมูลที่ไม่ได้รับอนุมัติจากภายในหน่วยธุรกิจออกไปสู่อินเทอร์เน็ตด้วย ปกติกิจการขนาดใหญ่มักกำหนดให้กำหนดให้การสื่อสารข้อมูลระหว่างกันให้กระทำผ่านเครื่อง Proxy server ซึ่งเป็นเครื่องเซิร์ฟเวอร์ภายนอกระบบเครื่องข่ายคอมพิวเตอร์ของกิจการซึ่งทำหน้าที่ควบคุมการสื่อสารข้อมูลทั้งเข้าและออกจากระบบเครือข่ายของกิจการ โดยเทคนิคที่เครื่องนำมาควบคุมการสื่อสารข้อมูลอาจเป็นการตรวจสอบ Domain name หรือ IP address ของการสื่อสารข้อมูลระหว่างกันว่ามาจากแหล่งที่ถูกต้อง หรือจะต้องมีลายเซ็นต์อิเล็กทรอนิกส์กำกับการสื่อสารข้อมูล (Digital signatures) โดยทั่วไปแล้วเครื่อง Proxy server มักเป็นองค์ประกอบหนึ่งของไฟร์วอลล์ สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลสามารถที่จะติดตั้ง Personal firewall ที่มากับระบบปฏิบัติการ Windows Vista หรือ Windows XP หรืออาจซื้อโปรแกรมไฟร์วอลล์โดยเฉพาะซึ่งราคาไม่สูงมาก สำหรับสำนักงานขนาดเล็กมักจะติดตั้ง Hardware firewall เช่น อุปกรณ์จัดเส้นทาง (Routers) หรืออุปกรณ์อื่นๆ ที่มีไฟร์วอลล์ เป็นต้น ร่วมกับ Personal firewall

- ติดตั้งซอฟต์แวร์ตรวจจับการบุกรุก (Intrusion detection software) กิจการขนาดใหญ่ส่วนมากจะติดตั้งซอฟต์แวร์ตรวจจับการบุกรุกเพิ่มเติมจากไฟร์วอลล์เพื่อให้ซอฟต์แวร์ตรวจดูว่ามีการบุกรุกเข้ามาในระบบเครือข่ายของกิจการโดยทำการวิเคราะห์การจราจรในเครือข่าย (Network traffic) ประเมินช่องโหว่ของระบบ (Vulnerabilities) ระบุการเข้าถึงระบบโดยไม่ได้รับอนุญาต และแจ้งให้ผู้ดูแลระบบเครือข่ายทราบถึงพฤติกรรมที่สงสัยว่าอาจมีการทำลายระบบ การติดตั้งซอฟต์แวร์ดังกล่าวจำเป็นต้องอาศัยผู้เชี่ยวชาญเนื่องจากเป็นซอฟต์แวร์ที่มีความซับซ้อนอย่างมากและมีราคาค่อนข้างแพง อย่างไรก็ตามเมื่อนำซอฟต์แวร์ดังกล่าวมาใช้งานร่วมกับไฟร์วอลล์จะทำให้เพิ่มการปกป้องข้อมูลที่สำคัญๆ ของกิจการได้เป็นอย่างดี

- ติดตั้ง Honeypot หรือคอมพิวเตอร์ที่มีช่องโหว่เพื่อล่อให้ผู้บุกรุกเข้ามาในระบบนั้น เพื่อศึกษาวิธีการเข้าสู่ระบบของผู้บุกรุก โดย Honeypot จะเป็นระบบที่ติดตั้งให้เหมือนระบบจริงแต่แยกออกมาจากระบบที่กิจการใช้งานอยู่ กิจการ Web hosting ขนาดใหญ่ เช่น Yahoo และ AT&T มักติดตั้งระบบ Honeypot ดังกล่าว

3.3.2 การควบคุมการเข้าถึงระบบโดยไม่ได้รับอนุญาต การควบคุมการเข้าถึงระบบโดยไม่ได้รับอนุญาตสามารถทำด้วยการติดตั้งไฟร์วอลล์และซอฟแวร์ตรวจจับการบุกรุกดังกล่าวมาแล้วข้างต้น นอกจากนี้ยังสามารถใช้วิธีการพิสูจน์ตัวจริง (Authentication) ดังจะกล่าวต่อไป

ปัจจุบันระบบต่างๆ ควบคุมการเข้าถึงระบบโดยใช้กระบวนการสองขั้น (Two-phase process) ประกอบด้วย การระบุตัวตน (Identification) และการพิสูจน์ตัวจริง (Authentication) โดยการระบุตัวตนเพื่อทำให้มั่นใจว่าบุคคลนั้นเป็นผู้ใช้ที่เป็นคนๆ นั้นจริงๆ ส่วนการพิสูจน์ตัวจริงเพื่อให้มั่นใจว่าบุคคลนั้นเป็นบุคคลที่ตนกล่าวอ้างจริง วิธีการสำหรับการระบุตัวตนทำโดยการใช้ชื่อผู้ใช้ (User name) ส่วนวิธีการพิสูจน์ตัวจริงทำได้ทำได้หลายวิธีแต่ที่นิยมใช้คือ รหัสผ่าน(Password) วิธีนี้เป็นการใช้ข้อมูลที่ทราบเฉพาะ

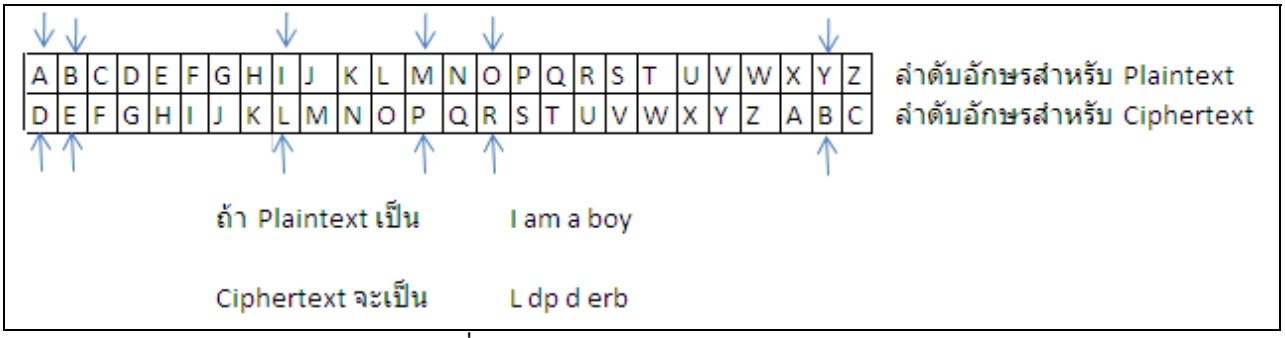
บุคคลที่เป็นเจ้าของ (What you know) นอกจากนี้ยังอาจใช้บัตรผ่านที่มีลักษณะเป็นบัตรประจำตัว (What you have) เช่น บัตร ATM เป็นต้น อย่างไรก็ตามบัตรนี้มักใช้ร่วมกับรหัสระบุตัวตน (Personal identification number หรือ PIN) เพื่อเพิ่มการควบคุมให้มากขึ้น และท้ายที่สุดสามารถใช้ลักษณะทางกายภาพของบุคคล (What you are) เช่น ม่านตา เป็นต้น

3.3.3 การควบคุมการขโมย การรักษาความปลอดภัยจากการที่ฮาร์ดแวร์ ซอฟต์แวร์ และสารสนเทศถูกขโมยหรือถูกทำลาย สามารถทำโดยการควบคุมการเข้าถึงทางกายภาพ (Physical access control) เช่น การปิดห้องและหน้าต่าง เป็นต้น กิจการบางแห่งมีการใส่กุญแจที่เครื่องคอมพิวเตอร์ หรือนำสื่อต่างๆ มาจัดเก็บในตู้เซฟที่ต้องใช้รหัสในการเปิด นอกจากนี้กิจการบางแห่งนำระบบ Real time location system (RTLS) มาใช้เพื่อระบุสถานที่ที่มีความเสี่ยงสูงโดยนำ RFID tags ติดที่อุปกรณ์คอมพิวเตอร์เพื่อใช้ในการติดตามอุปกรณ์นั้นๆ ปัจจุบันมีการออกแบบเครื่องคอมพิวเตอร์ให้สามารถควบคุมการเปิดเครื่องและการเข้าใช้งานเครื่องด้วยการใช้ลักษณะทางกายภาพของบุคคล เช่น ลายนิ้วมือ เป็นต้น

ส่วนการรักษาความปลอดภัยของซอฟต์แวร์ทำโดยเก็บรักษาแผ่นซอฟต์แวร์ในสถานที่มีการรักษาความปลอดภัย ผู้ใช้ทุกคนต้องทำการสำเนาแฟ้มข้อมูลของตนเป็นประจำ ในกรณีที่มีโปรแกรมเมอร์ลาออกหรือถูกให้ออก ต้องควบคุมและติดตามโปรแกรมเมอร์ทันที (Escort) เนื่องจากถ้าโปรแกรมเมอร์มีเวลาก็อาจจะทำอันตรายต่อแฟ้มข้อมูลและระบบเครือข่ายคอมพิวเตอร์ได้ ในกรณีของการป้องกันการใช้ซอฟต์แวร์ที่ไม่ถูกลิขสิทธินั้น ผู้ผลิตซอฟต์แวร์ส่วนมากจะกำหนดให้ผู้ซื้อลงทะเบียนและออก License agreement ซึ่งปัจจุบันกระทำทางออนไลน์

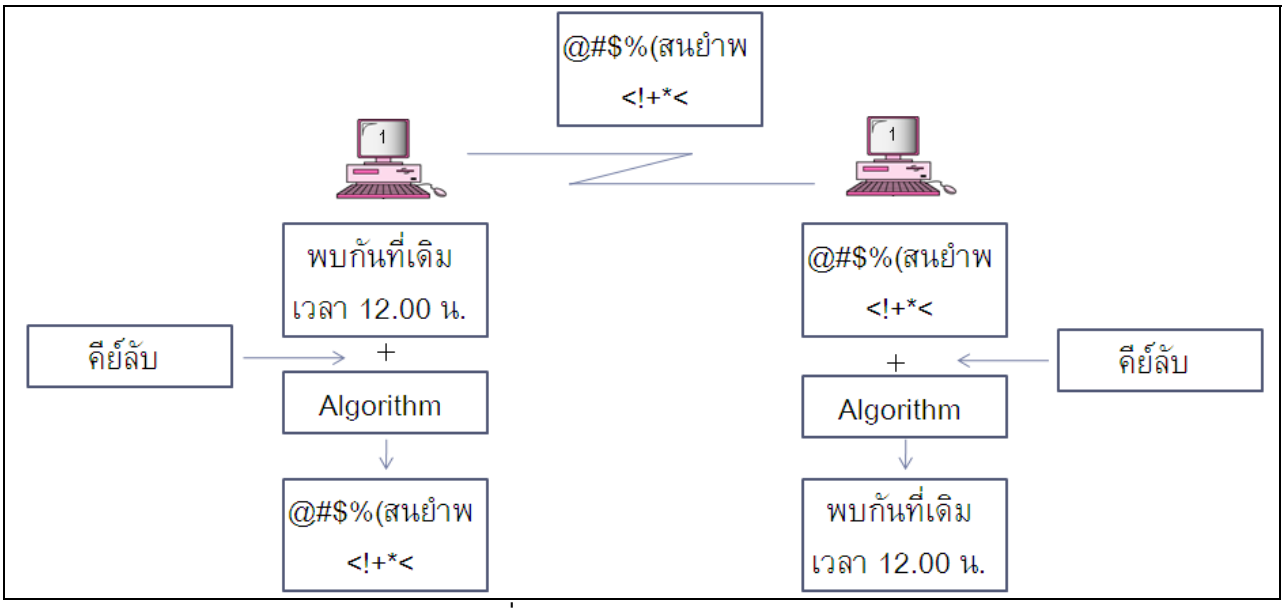
ในด้านการรักษาความปลอดภัยของสารสนเทศ วิธีที่นำมาใช้กันอย่างกว้างขวางคือ การเข้ารหัส (Encryption) ใบรับรองอิเล็กทรอนิกส์ (Digital certificates) Secure Sockets Layer, Secure HTTP, VPN ดังนี้

- การเข้ารหัส คือกระบวนการในการแปลงหรือเข้ารหัสข้อมูลที่อยู่ในรูปที่คนทั่วไปสามารถอ่านได้ (Plaintext) ให้อยู่ในรูปที่เฉพาะผู้ที่เกี่ยวข้องเท่านั้นสามารถอ่านข้อมูลได้ (Ciphertext) ทั้งนี้เพื่อป้องกันคนที่ไม่เกี่ยวข้องแอบอ่านข้อมูลที่ต้องการส่งได้ กระบวนการเข้ารหัสข้อมูลจะประกอบด้วยองค์ประกอบ 2 ส่วนด้วยกันคือ ขั้นตอนการแปลงรหัสหรืออัลกอริธึม (Algorithm) และคีย์ลับ(Encryption key หรือ Secret key) โดยขั้นตอนในการแปลงรหัสจะเป็นสูตรคำนวณหรือวิธีการแปลงข้อมูล ซึ่งอาจเป็น Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Rivest Shamir Adleman (RSA), Diffie-Hellman, และ Elliptic Curve Cryptography ในอดีตวิธีการแปลงข้อมูลอาจใช้วิธีการสลับตำแหน่งข้อมูลดังแสดงในภาพที่ 8 จะเห็นได้ว่าถ้า Plaintext ที่ต้องการส่งเป็นข้อความว่า I am a boy ถ้าผู้รับและผู้ส่งใช้วิธีการแปลงข้อมูลโดยสลับตำแหน่งของตัวอักษรที่อยู่ในแนวเดียวกัน ข้อความที่เป็น Ciphertext เพื่อจัดส่งจะเป็น L dp d erb



ภาพที่ 8 วิธีการเข้ารหัสแบบสลับตำแหน่ง

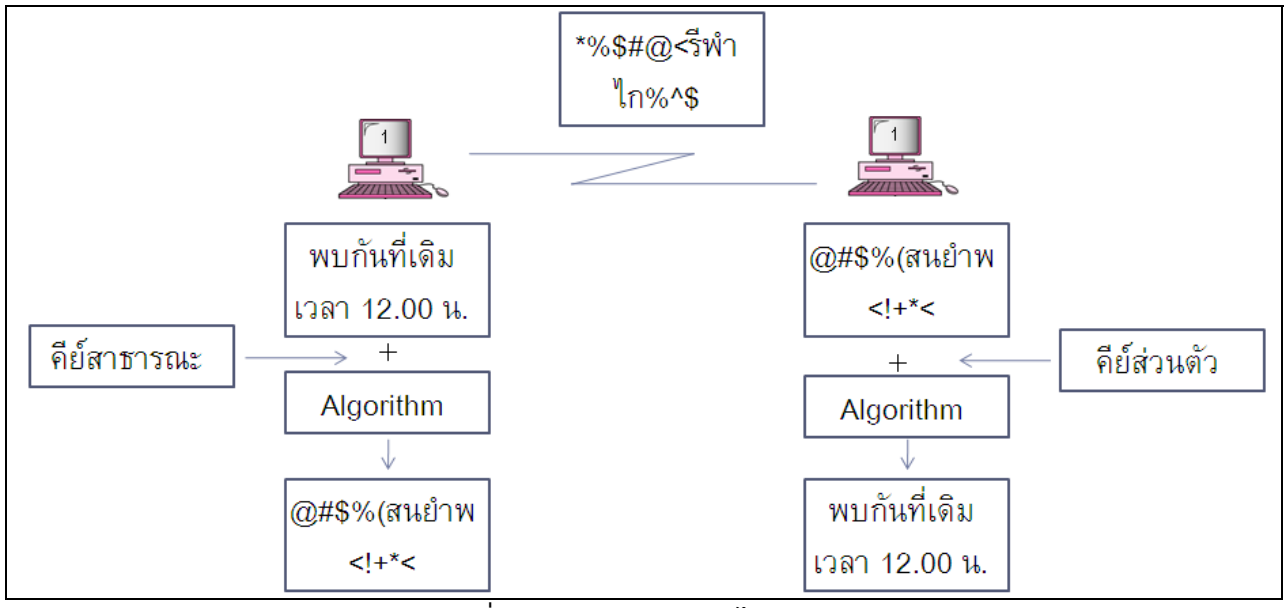
จะเห็นได้ว่าถ้ากำหนดการเข้ารหัสด้วยวิธีการเข้ารหัสอย่างเดียวจะไม่ปลอดภัย เนื่องจากบุคคลอื่นที่ไม่เกี่ยวข้องอาจทราบวิธีการเข้ารหัสได้ โดยเฉพาะอย่างยิ่งโปรแกรมเมอร์ที่เป็นผู้เขียนโปรแกรมการเข้ารหัส ดังนั้นจึงต้องกำหนดคีย์ลับ (Secret key) เข้าร่วมกับวิธีการเข้ารหัสดังแสดงในภาพที่ 9 อนึ่งคีย์ลับจะเป็นคีย์ที่เฉพาะผู้รับและผู้ส่งข้อมูลระหว่างกันเท่านั้นที่จะทราบคีย์นี้และผู้ติดต่อกันต้องจัดเก็บคีย์ดังกล่าวไว้เป็นความลับ จะเห็นว่าในภาพที่ 9 ผู้ส่งและผู้รับข้อมูลจะใช้คีย์ลับตัวเดียวกันสำหรับเข้าและถอดรหัสข้อมูล การเข้ารหัสแบบนี้ว่า การเข้ารหัสแบบสมมาตร (Symmetric Encryption)



ภาพที่ 9 การเข้ารหัสแบบสมมาตร

เนื่องจากปัญหาที่สำคัญของการเข้ารหัสแบบสมมาตรคือการเก็บรักษาคีย์ที่ใช้ในการเข้ารหัสและถอดรหัสซึ่งเป็นคีย์ตัวเดียวกันให้เป็นความลับ นอกจากนี้ผู้ส่งและผู้รับจะมั่นใจได้อย่างไรว่าคีย์ที่แลกเปลี่ยนกันนั้นไม่ถูกเปิดเผยให้ผู้ใดทราบ ในกรณีที่ทำการติดต่อกับคนจำนวนมากอาจทำให้คีย์ที่ใช้ไม่

เป็นความลับ การแก้ปัญหาทำโดยกำหนดคีย์ที่แตกต่างสำหรับคนที่ติดต่อด้วยด้วยการเข้ารหัสแบบไม่สมมาตร (Asymmetric Encryption) ดังภาพที่ 10



ภาพที่ 10 การเข้ารหัสแบบไม่สมมาตร

โดยการเข้ารหัสแบบสมมาตรจะกำหนดให้มีการใช้คีย์สองคีย์ที่แตกต่างกัน ซึ่งคีย์แรกเรียกว่า คีย์ส่วนตัว (Private Key) ส่วนคีย์ที่สองเรียกว่า คีย์สาธารณะ (Public Key) ซึ่งถ้าข้อมูลถูกเข้ารหัสด้วยคีย์ส่วนตัวจะต้องถอดรหัสด้วยคีย์สาธารณะที่คู่กัน หรือในกรณีที่เข้ารหัสด้วยคีย์สาธารณะก็ต้องถอดรหัสด้วยคีย์ส่วนตัวที่คู่กันเช่นกัน การใช้คีย์สองคีย์ดังกล่าวช่วยแก้ปัญหาการจัดการคีย์ที่เกิดขึ้นกับการเข้ารหัสแบบสมมาตร กล่าวคือสามารถกระจายคีย์สาธารณะไปยังคนต่างๆ ที่ต้องการติดต่อด้วยโดยเก็บคีย์ส่วนตัวเอาไว้โดยไม่เปิดเผยให้ผู้อื่นทราบ อย่างไรก็ตามการเข้ารหัสแบบไม่สมมาตรก็มีปัญหาด้านการจัดส่งคีย์สาธารณะ กล่าวคือผู้รับที่ได้รับข้อมูลพร้อมกับคีย์สาธารณะของผู้ส่งจะทราบได้อย่างไรว่าคีย์สาธารณะเป็นของผู้ส่งจริงๆ ซึ่งวิธีการจัดการสามารถทำโดยการใช้ใบรับรองอิเล็กทรอนิกส์ ซึ่งเป็นเอกสารที่ให้ข้อมูลที่เกี่ยวข้องกับคีย์สาธารณะ เช่น คีย์สาธารณะ รายละเอียดเจ้าของคีย์สาธารณะ และข้อมูลอื่นๆ ที่รับรองโดยบุคคลที่สามที่ได้รับความเชื่อถือ (Trusted Third Party) เป็นต้น เมื่อผู้ส่งจัดส่งข้อมูลไปให้ผู้รับพร้อมด้วยใบรับรองอิเล็กทรอนิกส์ ผู้รับก็จะมั่นใจได้ว่าคีย์สาธารณะที่ได้รับเป็นของผู้ส่งจริง อย่างไรก็ตามผู้จัดส่งไม่จำเป็นที่จะต้องจัดส่งใบรับรองอิเล็กทรอนิกส์ไปให้ผู้รับพร้อมกับข้อมูลทุกครั้ง โดยผู้จัดส่งสามารถนำใบรับรองอิเล็กทรอนิกส์ไปไว้ในไดเร็กทรอรี่อิเล็กทรอนิกส์สาธารณะ (Public Electronic Directory) โดยผู้รับข้อมูลสามารถดึงใบรับรองอิเล็กทรอนิกส์จากไดเร็กทรอรีดังกล่าวได้ ปกติจะให้บุคคลที่สามที่ได้รับความ

เชื่อถือหรือเรียกว่า ผู้ออกใบรับรอง (Certification Authority หรือ CA) เช่น เวอริไซน์ (Verisign) เป็นต้น เป็นผู้ออกใบรับรองอิเล็กทรอนิกส์

- Secure sockets layer (SSL) เป็นการเข้ารหัสข้อมูลทั้งหมดที่จัดส่งระหว่างเครื่องไคลเอ็นต์ (Client) และ Internet server โดย SSL จะกำหนดให้เครื่องไคลเอ็นต์ต้องมีใบรับรองอิเล็กทรอนิกส์ เมื่อเครื่องเซิร์ฟเวอร์ได้รับใบรับรองอิเล็กทรอนิกส์แล้วจะทำให้โปรแกรม Web browser สื่อสารกับเครื่องไคลเอ็นต์อย่างปลอดภัย โดยเว็บเพจที่ใช้ SSL จะขึ้นต้นด้วย https แทนที่จะเป็น http
- Secure HTTP (S-HTTP) จะอนุญาตให้ผู้ใช้เลือกการเข้ารหัสข้อมูลที่สื่อสารกันระหว่างเครื่องไคลเอ็นต์และเครื่องเซิร์ฟเวอร์ ในกรณีที่ใช้ S-HTTP เครื่องไคลเอ็นต์และเครื่องเซิร์ฟเวอร์ต้องมีใบรับรองอิเล็กทรอนิกส์ โดย S-HTTP จะใช้งานยากกว่า SSL แต่จะมีความปลอดภัยมากกว่า โปรแกรมประยุกต์ที่ต้องการพิสูจน์ตัวจริงของเครื่องไคลเอ็นต์ เช่น ระบบธนาคารออนไลน์จะใช้ S-HTTP
- VPN ผู้ใช้เครื่อง Mobile ส่วนมากจะเข้าถึงระบบเครือข่ายคอมพิวเตอร์ของกิจการผ่านทาง Virtual private network (VPN) ซึ่งจะทำให้การเชื่อมต่อมีความปลอดภัยสูงเหมือนผู้ใช้มีสายส่วนตัว (Private line) โดย VPN จะช่วยให้มั่นใจว่าข้อมูลที่ส่งระหว่างกันนั้นปลอดภัยการดักฟังจากผู้ที่ไม่ได้รับอนุญาตด้วยการเข้ารหัสข้อมูลที่ส่งจากคอมพิวเตอร์ส่วนบุคคล, Tablet PC, smart Phone, PDA, หรืออุปกรณ์ Mobile อื่นๆ

3.3.4 การควบคุมความล้มเหลวของระบบสารสนเทศ การป้องกันแรงดันไฟฟ้านั้นกิจการสามารถทำโดยการใช้ Surge protector หรือ Surge suppressor ซึ่งเป็นอุปกรณ์ที่ช่วยลดเสียงและทำให้กระแสไฟไหลอย่างสม่ำเสมอ นอกจากนี้ยังช่วยป้องกันแรงดันไฟฟ้าสูงไม่ให้เข้าไปในเครื่องคอมพิวเตอร์

ในกรณีที่ไฟฟ้าดับกิจการสามารถเชื่อมต่อเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบเข้ากับเครื่อง Uninterruptible power supply (UPS) เพื่อทำหน้าที่ในการแจกจ่ายไฟฟ้าให้อุปกรณ์ต่างๆ เพื่อให้ผู้ปฏิบัติงานสามารถปิดอุปกรณ์เหล่านั้นได้อย่างสมบูรณ์ พึงระลึกไว้เสมอว่า UPS ไม่ใช่เครื่องปั่นไฟแต่เป็นเครื่องจ่ายกระแสไฟฟ้าในช่วงเวลาที่จำกัด (เช่น 3 ชั่วโมง เป็นต้น) ในกรณีที่ไฟฟ้าดับเท่านั้น เพื่อมิให้เกิดปัญหาในกรณีที่ซอฟต์แวร์ปิดอย่างไม่สมบูรณ์เท่านั้น

กรณีที่ระบบสารสนเทศถูกทำลายจนไม่สามารถให้บริการได้ เช่น ไฟไหม้ โคลนถล่ม เป็นต้น การควบคุมที่กิจการมักนำมาใช้คือการจัดทำแผนการทำให้กลับคืนสู่สภาพเดิมจากภัยพิบัติ (Disaster Recovery – DR) คือ การที่องค์กรสามารถกลับมาดำเนินงานตามปกติได้ภายหลังจากประสบกับภัยพิบัติ อนึ่งจะเห็นได้ว่าองค์กรบางแห่งใช้คำว่า Business continuity planning (BCP) ในความหมายเดียวกับ Disaster Recovery โดยคำทั้งสองนี้มีความหมายใกล้เคียงกันแต่ไม่เหมือนกันทีเดียว กล่าวคือ Business continuity มีเป้าหมายให้องค์กรสามารถดำเนินธุรกิจต่อไป แต่ Disaster Recovery เป็นส่วนหนึ่งของ BCP อย่างไรก็ตามในบทนี้จะไม่กล่าวถึงรายละเอียดเกี่ยวกับการจัดทำแผนดังกล่าว

การสำรองข้อมูล (Data Backup) เป็นสิ่งที่ต้องคำนึงถึงเป็นลำดับแรกในการควบคุมความล้มเหลวของระบบสารสนเทศ การสำรองข้อมูลคือ การสำเนาแฟ้มข้อมูล โปรแกรม หรือดิสก์ เพื่อให้สามารถเรียกคืนข้อมูลและโปรแกรม (Restore) ระบบสารสนเทศกลับคืนมาสู่สภาพเดิมสภาพเดิมเมื่อเกิดปัญหาได้ สิ่งที่ต้องตัดสินใจเกี่ยวกับการสำรองข้อมูลประกอบด้วย

1. เลือกสื่อบันทึก (Media) ที่จะทำการสำรองข้อมูล เช่น CD DVD หรือ Portable Harddisk เป็นต้น สิ่งที่ต้องพิจารณาคือสื่อบันทึกนั้นต้องมีความจุที่เพียงพอที่จะจัดสำรองข้อมูลได้ทั้งหมด นอกจากนี้ควรเลือกสื่อบันทึกที่เหมาะสมกับการทำ Recovery ด้วย
2. ระยะเวลาที่ต้องสำรองข้อมูล รวมถึงการสำรองข้อมูลด้วยมือหรืออัตโนมัติ ในการกำหนดตารางเวลาสำรองข้อมูลควรกำหนดว่าจะต้องปิดเครื่องเซิร์ฟเวอร์หรือไม่ ถ้าต้องปิดเครื่องควรกำหนดวันให้เหมาะสมกล่าวคือไม่ควรเป็นวันระหว่างสัปดาห์ แต่ถ้าไม่ต้องปิดเครื่องควรกำหนดช่วงเวลาที่มีการใช้งานเครื่องเซิร์ฟเวอร์น้อย อนึ่งพึงระมัดระวังด้วยว่าบางแฟ้มข้อมูลจะไม่สามารถสำรองได้ถ้ามีการเปิดแฟ้มนั้นเพื่อประมวลอยู่
3. ความถี่ในการสำรองข้อมูล ขึ้นอยู่กับระยะเวลาสูงสุดที่ระบบจะไม่สามารถให้บริการได้โดยไม่ส่งผลต่อการดำเนินงานปกติขององค์กร
4. สถานที่จัดเก็บสื่อบันทึกที่สำรองข้อมูล ซึ่งสามารถจัดเก็บ On Site หรือ Offsite ซึ่งแต่ละประเภทมีข้อดีและข้อเสียแตกต่างกันออกไป

การรักษาความปลอดภัยของแลนไร้สาย (Wireless LAN) เนื่องจากปัจจุบันการใช้บริหารแลนไร้สายเพิ่มจำนวนมากขึ้นในที่นี้จะกล่าวถึงการรักษาความปลอดภัยของแลนไร้สายเบื้องต้นเท่านั้น

- ควบคุมการเชื่อมโยงเข้าสู่แลนไร้สายด้วย Service Set Identifier (SSID) ปกติเครื่องคอมพิวเตอร์ไร้สายที่ต้องการเชื่อมโยงเข้าเครือข่ายจะต้องกำหนด SSID ให้เป็นชื่อเดียวกับ SSID ของแอ็กเซสพอยน์ (Access Point) ที่บริการในพื้นที่นั้น ในการค้นหา SSID ทำโดยการให้เครื่องคอมพิวเตอร์ไร้สายตรวจจับ SSID ที่แอ็กเซสพอยน์แพร่กระจายออกมา (Broadcast) ซึ่งจะทำให้สามารถใช้เครื่องคอมพิวเตอร์เชื่อมโยงเข้าเครือข่ายได้ (กรณีที่ไม่มีระบบความปลอดภัยอื่นๆ รองรับดังจะกล่าวต่อไป) หากไม่ต้องการให้บุคคลภายนอกที่มีเครื่องคอมพิวเตอร์ไร้สายเชื่อมต่อเข้าเครือข่ายได้ กิจการสามารถควบคุมการเชื่อมโยงเบื้องต้นได้ด้วยการให้แอ็กเซสพอยน์หยุดการแพร่กระจาย SSID อย่างไรก็ตามวิธีการควบคุมนี้ควรใช้ควบคู่กับวิธีการอื่นๆ ด้วย

เพื่อให้การลักลอบเชื่อมโยงสู่เครือข่ายทำได้ยากขึ้น โดยแอ็กเซสพอยน์จะทำหน้าที่เป็นศูนย์กลางเชื่อมโยงเครื่องคอมพิวเตอร์ไร้สายเข้าด้วยกัน

- กลั่นกรองผู้ใช้งานด้วยการกรองหมายเลขการ์ดเน็ตเวิร์ก (MAC Addressing Filtering) โดยหมายเลขการ์ดเน็ตเวิร์ก (MAC Address) เป็นชุดตัวเลขที่ใช้อ้างอิงแลนการ์ดไร้สาย (Wirless LAN Card) ซึ่งเป็นเลขประจำตัวที่ไม่ซ้ำกัน กิจการสามารถกำหนดว่าจะให้เครื่องคอมพิวเตอร์ไร้สายเครื่องไหนเชื่อมโยงเครือข่าย โดยป้อนหมายเลขการ์ดเน็ตเวิร์กของเครื่องนั้นเข้าไปในแอ็กเซสพอยน์ ในกรณีที่เครื่องคอมพิวเตอร์ที่เชื่อมโยงเข้าเครือข่ายไร้สายมีหมายเลขการ์ดเน็ตเวิร์กไม่ตรงกับที่เก็บไว้ในแอ็กเซสพอยน์ก็จะไม่สามารถเชื่อมโยงเข้าสู่เครือข่ายได้ อย่างไรก็ตามวิธีการนี้เหมาะกับเครือข่ายที่มีขนาดเล็ก เนื่องจากฐานข้อมูลที่จัดเก็บหมายเลขการ์ดเน็ตเวิร์กบนแอ็กเซสพอยน์มีจำนวนจำกัด
- การเข้ารหัสและถอดรหัสด้วยวิธีการ Wired Equivalency Privacy (WEP) เนื่องจากข้อมูลที่สื่อสารระหว่างกันของเครื่องคอมพิวเตอร์บนแลนไร้สายมักอยู่ในรูปของข้อมูลที่ไม่มีการเข้ารหัส ทำให้ผู้ที่ต้องการโจมตีระบบสามารถดักจับข้อมูลที่แพร่กระจายออกมาได้ ดังนั้น มาตรฐาน IEEE802.11 จึงได้กำหนดให้สามารถใช้ WEP เพื่อสร้างความปลอดภัยให้กับข้อมูลที่สื่อสารได้โดยการเข้ารหัสและถอดรหัสแบบ RC4 ในการใช้งาน WEP ผู้ใช้ต้องกำหนดค่าคีย์ ที่มีขนาด 64 บิตหรือ 128 บิต บนแอ็กเซสพอยน์ซึ่งสนับสนุนมาตรฐาน IEEE802.11 เมื่อกำหนด WEP แล้วจะทำให้ข้อมูลที่ส่งออกมาเป็นข้อมูลที่ถูกเข้ารหัส ดังนั้นผู้ที่ต้องการเชื่อมโยงเข้าเครือข่ายต้องทราบคีย์เพื่อให้สามารถเชื่อมโยงเข้าเครือข่ายได้ อนึ่งวิธีการดังกล่าวเป็นวิธีการป้องกันแบบเก่าที่มีโปรแกรมที่สามารถถอดรหัสได้ ดังนั้นกิจการที่ต้องการความปลอดภัยในระดับสูงควรใช้วิธีการอื่นประกอบด้วย
- จำกัดขอบเขตพื้นที่ให้บริการด้วยการควบคุมกำลังส่งของแอ็กเซสพอยน์ เนื่องจากการสื่อสารบนเครือข่ายแลนไร้สายจะอาศัยการแพร่กระจายคลื่นหรือสัญญาณ ดังนั้นกำลังส่งคลื่นจึงเป็นตัวแปรที่กำหนดขอบเขตพื้นที่ให้บริการ อนึ่งอุปกรณ์เครือข่ายแลนไร้สายที่มีกำลังส่งสูงจะสามารถแพร่กระจายคลื่นหรือสัญญาณได้ไกล ในขณะที่เครื่องที่มีกำลังส่งต่ำจะแพร่กระจายสัญญาณน้อย ดังนั้นการรักษาความปลอดภัยสามารถทำโดยจำกัดขอบเขตพื้นที่ให้บริการด้วยการควบคุมกำลังส่งของแอ็กเซสพอยน์

นอกเหนือจากการรักษาความปลอดภัยดังกล่าวข้างต้นแล้วยังสามารถใช้การพิสูจน์สิทธิเข้าใช้งานแลนไร้สายด้วย Radius Server การสร้าง Virtual Private Network (VPN) บนแลนไร้สายและการ

ป้องกันด้วยวิธี Wi-Fi Protected Access (WPA) แต่จะไม่กล่าวในที่นี้ผู้สนใจสามารถศึกษารายละเอียดในวิชาอื่นๆ ที่เกี่ยวข้อง

4. จรรยาบรรณ

จากการที่เทคโนโลยีด้านคอมพิวเตอร์มีความสามารถอย่างมากมายส่งผลให้อาจมีผู้นำเทคโนโลยีดังกล่าวไปใช้เทคโนโลยีคอมพิวเตอร์ทั้งในทางที่ดีและไม่ดี โดยมาตรฐานที่กำหนดว่าการกระทำใดเป็นสิ่งที่ดีหรือไม่ดีก็คือ จรรยาบรรณ (Ethics)

จรรยาบรรณทางคอมพิวเตอร์ คือหลักปฏิบัติที่แสดงให้เห็นถึงความรู้สึกผิดชอบเกี่ยวกับการใช้ระบบสารสนเทศ ซึ่งประกอบด้วยการใช้คอมพิวเตอร์และเครือข่ายโดยไม่ได้รับอนุญาต การขโมยซอฟต์แวร์ (การละเมิดลิขสิทธิ์) ความถูกต้องของสารสนเทศ สิทธิ์ต่อทรัพย์สินทางปัญญา (Intellectual property rights) หลักปฏิบัติ (Code of conduct) และความเป็นส่วนตัวของสารสนเทศ (Information privacy) ในที่นี้จะไม่กล่าวถึงการใช้คอมพิวเตอร์และเครือข่ายโดยไม่ได้รับอนุญาตและการขโมยซอฟต์แวร์ เนื่องจากกล่าวมาแล้วข้างต้นโดยจะกล่าวเฉพาะส่วนที่เหลือเท่านั้น

จากการที่ผู้ใช้สามารถเข้าถึงสารสนเทศของที่ต่างๆ ผ่านทางอินเทอร์เน็ต โดยผู้ใช้ไม่ได้เป็นผู้จัดสร้างและบำรุงรักษาสารสนเทศเหล่านั้น ดังนั้นผู้ใช้ควรตระหนักว่าสารสนเทศจากเว็บหนึ่งๆ อาจไม่ถูกต้องได้และประเมินคุณค่าของสารสนเทศนั้นก่อนจะเชื่อถือองค์ประกอบของสารสนเทศ นอกจากนี้ผู้ใช้ควรตระหนักว่ากิจการที่ให้สารสนเทศผ่านทางเว็บอาจไม่ใช่ผู้จัดสร้างสารสนเทศนั้นก็ได้ ปัจจุบันองค์กรและบุคคลต่างๆ ตั้งคำถามเกี่ยวกับจรรยาบรรณของการใช้คอมพิวเตอร์ในการเปลี่ยนแปลงผลลัพธ์โดยเฉพาะตกแต่งรูปภาพซึ่งสามารถทำได้ง่ายมากด้วยซอฟต์แวร์ตกแต่งรูปภาพ อย่างไรก็ตามคนบางกลุ่มคิดว่าการตกแต่งรูปภาพแม้เพียงเล็กน้อยเท่านั้นสามารถก่อให้เกิดความเข้าใจที่คลาดเคลื่อนได้ แต่บางกลุ่มคิดว่าการตกแต่งรูปภาพยอมรับได้ตราบใดที่องค์ประกอบและความหมายที่สำคัญๆ ของรูปภาพไม่เปลี่ยแปลง

ส่วนทรัพย์สินทางปัญญาคือ งานที่มีลักษณะเป็นหนึ่งเดียว (Unique) และเป็นต้นฉบับ (Origin) เช่น ความคิด สิ่งประดิษฐ์ ศิลปะ งานเขียน กระบวนการ ชื่อบริษัทและสินค้า และตราสัญญลักษณ์ เป็นต้น ดังนั้นสิทธิ์ต่อทรัพย์สินทางปัญญา หมายถึงสิทธิ์ของผู้คิดค้นสิ่งต่างๆ เหล่านั้นที่จะได้รับสิทธิจากชิ้นงานของตน จากการที่ทรัพย์สินทางปัญญาในปัจจุบันส่วนมากจะอยู่ในรูปของดิจิตัลทำให้มีข้อถกเถียงเกี่ยวกับจรรยาบรรณด้านนี้ เนื่องจากลิขสิทธิ์ (Copyright) ให้สิทธิแก่เจ้าของในการสำเนา ตีพิมพ์ และขายทรัพย์สินนั้น ปัญหาที่กระทำกันอย่างกว้างขวางเกี่ยวกับลิขสิทธิ์คือการละเมิดลิขสิทธิ์ด้วยการสำเนาซอฟต์แวร์ ภาพยนต์และเพลง เนื่องจากกฎหมายทางลิขสิทธิ์มักกำหนดว่าถ้าการใช้งานซอฟต์แวร์เป็น Fair use จะอนุญาตให้สามารถใช้งานทางการศึกษาได้ส่งผลให้มีคำถามอย่างกว้างขวางเกี่ยวกับลิขสิทธิ์ดังนี้

- บุคคลสามารถ Download ส่วนประกอบของเว็บไซต์ ต่อจากนั้นปรับปรุง แล้วนำไปแสดงบนเว็บในนามของตนเองได้หรือไม่

- เจ้าหน้าที่ของมหาวิทยาลัยสามารถพิมพ์เอกสารบนเว็บและกระจายให้นักศึกษาเพื่อใช้สำหรับการเรียนการสอนได้หรือไม่
- บุคคลสามารถสแกนรูปภาพหรือหนังสือ ต่อจากนั้นนำไปลงในเว็บซึ่งอนุญาตให้คน Download ได้หรือไม่
- บุคคลสามารถสามารถนำเพลงใส่ในเว็บได้หรือไม่
- นักศึกษาสามารถนำข้อสอบหรือโครงการต่างๆ ที่อาจารย์กำหนดในชั้นเรียนเข้าไปใส่ในเว็บเพื่อให้นักศึกษาคนอื่นๆ ลอกโครงการนั้นแล้วส่งอาจารย์ว่าเป็นงานของตนได้หรือไม่

หลักปฏิบัติ คือสิ่งที่เขียนเป็นลายลักษณ์อักษรเพื่อเป็นแนวทางในการตัดสินใจว่าการกระทำใดที่เกี่ยวข้องกับคอมพิวเตอร์เป็นสิ่งที่มีหรือไม่มีจรรยาบรรณ หลักปฏิบัติมีดังนี้

- ต้องไม่ใช้คอมพิวเตอร์ในการทำอันตรายบุคคลอื่น
- ต้องไม่รบกวนการทำงานทางคอมพิวเตอร์ของคนอื่น
- ต้องไม่เข้าไปยุ่งเกี่ยวกับแฟ้มข้อมูลของคนอื่น
- ต้องไม่ใช้คอมพิวเตอร์ในการขโมย
- ต้องไม่ใช้คอมพิวเตอร์เพื่อให้หลักฐานที่เป็นเท็จ
- ต้องไม่สำเนาหรือใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์
- ต้องไม่ใช้ทรัพยากรทางคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต
- ต้องไม่ใช้ทรัพสินทางปัญญาของผู้อื่นเหมือนเป็นของตน
- ต้องคำนึงถึงผลกระทบทางสังคมของโปรแกรมที่ออกแบบ
- ต้องใช้คอมพิวเตอร์ในทางที่แสดงให้เห็นถึงความเคารพในมนุษย์แต่ละคน

ความเป็นส่วนตัวของสารสนเทศ คือสิทธิของแต่ละบุคคลหรือกิจการที่จะปฏิเสธหรือจำกัดการจัดเก็บข้อมูลและการใช้สารสนเทศของตน ในอดีตความเป็นส่วนตัวของสารสนเทศสามารถกระทำได้โดยง่าย เนื่องจากหน่วยงานที่เป็นผู้จัดเก็บข้อมูลจะจัดเก็บข้อมูลแยกต่างหากจากกัน ปัจจุบันการรักษาความเป็นส่วนตัวของข้อมูลกระทำได้ลำบาก เนื่องจากเครื่องคอมพิวเตอร์ต่างๆ สามารถเชื่อมโยงกันได้อย่างทั่วถึง วิธีการที่นำมาใช้ควบคุมความเป็นส่วนตัวของข้อมูลคือ การควบคุมการเข้าถึงข้อมูลดังกล่าว แต่คำถามที่ตามมาคือ จะมั่นใจได้อย่างไรว่าบุคคลหรือกิจการที่มีข้อมูลส่วนตัวของคนอื่นๆ จะไม่ใช้ข้อมูลนั้นถ้าไม่ได้ขออนุญาตเจ้าของข้อมูลก่อน วิธีการที่จะรักษาความเป็นส่วนตัวของข้อมูลของท่านทำได้ดังนี้

- ให้เฉพาะข้อมูลที่จำเป็นเท่านั้นในการกรอกข้อมูลใบลงทะเบียน ใบรับประกัน และอื่นๆ
- ไม่พิมพ์เบอร์โทรศัพท์ เลขที่บัตรประชาชน บนเช็ค ล่วงหน้า (Preprint)
- แจ้งองค์การโทรศัพท์ไม่ให้พิมพ์หมายเลขโทรศัพท์ของท่านลงใบสมุดโทรศัพท์

- ถ้าหมายเลขโทรศัพท์ของท่านอยู่ในพื้นที่ๆ สามารถแสดงหมายเลขโทรศัพท์ที่เครื่องของผู้รับได้ ให้ท่านระงับการแสดงหมายเลขโทรศัพท์ที่เครื่องของผู้รับด้วย
- ไม่ควรเขียนหมายเลขโทรศัพท์ของท่านบนในบิลของบัตรเครดิต
- ซื้อสินค้าด้วยเงินสด แทนที่จะเป็นบัตรเครดิต
- ถ้าร้านค้าสอบถามข้อมูลส่วนตัวของท่าน ให้หาเหตุผลว่าทำไมจึงถามคำถามนั้นก่อนที่จะตัดสินใจว่าจะให้หรือไม่ให้ข้อมูล
- กรอกข้อมูลส่วนตัวของท่านบนเว็บเฉพาะส่วนที่ต้องกรอกเท่านั้น
- ติดตั้งตัวจัดการ Cookie เพื่อกลั่นกรอง Cookie
- ลบ History file ภายหลังจากเลิกใช้โปรแกรมเบาวร์เซอร์
- ยกเลิกการเปิดบริการแบ่งปันข้อมูล (File sharing) หรือเครื่องพิมพ์ก่อนการเชื่อมต่ออินเทอร์เน็ต
- ติดตั้งไฟร์วอลล์ส่วนบุคคล
- ติดตั้งโปรแกรม Anti-spam
- ไม่ตอบ e-mail ที่เป็น spam ไม่ว่าจะด้วยเหตุผลใดก็ตาม

อนึ่ง Cookie คือ Text file ขนาดเล็กที่เครื่อง Web server นำมาติดตั้งที่เครื่องคอมพิวเตอร์ (ฮาร์ดดิสก์) ของผู้เรียกเว็บไซต์นั้นๆ โดย Cookie จะมีข้อมูลเกี่ยวกับผู้ใช้ ประกอบด้วย ชื่อหรือเว็บไซต์ที่ชอบเข้า เมื่อผู้ใช้ติดต่อกับเว็บไซต์ โปรแกรมเบาวร์เซอร์จะจัดส่งข้อมูลใน Cookie ไปยังเว็บไซต์ อนึ่งเว็บไซต์จะใช้ Cookies เพื่อ

- ติดตามความชอบของผู้ใช้ โดยดูจากเว็บไซต์และจำนวนครั้งที่ผู้ใช้เข้าเป็นประจำ
- จัดเก็บรหัสผ่านของผู้ใช้ ทำให้ผู้ใช้ไม่ต้องป้อนรหัสผ่านทุกครั้งที่เข้าไปที่เว็บไซต์นั้น
- ติดตามและจัดเก็บรายการสินค้าที่ผู้ซื้อนำไปใส่ใน Shopping cart ซึ่งเป็นการซื้อสินค้าผ่านทางเว็บขายสินค้าออนไลน์ โดยรายการเหล่านั้นจะถูกจัดเก็บใน Session cookie ทำให้ลูกค้าสามารถกลับมาเลือกรายการสินค้าเพิ่มเติมจากครั้งก่อนหรือทำรายการซื้อให้สำเร็จอีกวัน
- โฆษณาสินค้า โดยดูจากความสนใจและพฤติกรรมของผู้ใช้ที่จัดเก็บใน Cookie

เนื่องจากเว็บไซต์บางแห่งจะขายข้อมูลใน Cookie ให้กับบริษัทโฆษณา ซึ่งการกระทำดังกล่าวถือว่าเป็นการกระทำที่ผิดจรรยาบรรณ ถ้าท่านไม่ต้องการให้ข้อมูลของท่านกระจายไปยังที่ต่างๆ จะต้องจำกัดการให้สารสนเทศของท่านในเว็บไซต์ อย่างไรก็ตามการการปิดบริการ Cookie ของเครื่องคอมพิวเตอร์อาจทำให้ท่านไม่สามารถเข้าเว็บไซต์บางเว็บได้ ซึ่งท่านสามารถแก้ไขได้ด้วยการซื้อซอฟต์แวร์ที่เลือกปิด Cookies บางอันเท่านั้น

ปัจจุบันประเทศต่างได้ออกกฎหมายเกี่ยวกับความเป็นส่วนตัวของสารสนเทศ เช่น Privacy Act และ Family Educational Rights and Privacy Act เป็นต้น โดยกฎหมายนี้ส่วนใหญ่จะกล่าวถึง

- จำนวนของสารสนเทศที่จัดเก็บจะต้องจัดเก็บเท่าที่จำเป็นเพื่อการดำเนินงานของธุรกิจหรือรัฐบาลเท่านั้น
- จำกัดการเข้าถึงข้อมูลที่รวบรวมนั้น โดยให้พนักงานที่เกี่ยวข้องและจำเป็นต้องใช้ข้อมูลเพื่อการปฏิบัติงานสามารถใช้ข้อมูลนั้นได้เท่านั้น
- แจ้งให้ผู้ที่ถูกจัดเก็บข้อมูลทราบว่ากำลังจัดเก็บข้อมูลอยู่ เพื่อให้บุคคลนั้นมีโอกาสในการพิจารณาความถูกต้องของข้อมูล

5. บทสรุป

จากการที่ระบบสารสนเทศมีการพัฒนาและปรับเปลี่ยนรูปแบบการดำเนินงานที่แตกต่างไปจากเดิมทำให้ต้องกำหนดให้มีการรักษาความปลอดภัยของระบบสารสนเทศที่แตกต่างไปจากเดิมตั้งแต่การรักษาความปลอดภัยการโจมตีระบบเครือข่าย การควบคุมการเข้าถึงระบบโดยไม่ได้รับอนุญาต การควบคุมการขโมยและการควบคุมความล้มเหลวของระบบสารสนเทศ นอกจากนี้สิ่งที่มีความสำคัญอย่างมากเช่นกันคือจรรยาบรรณที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

6. บรรณานุกรม

Ciampa, M. (2005). Security+ Guide to Network Security Fundamentals, Second Edition, Thomson Course Technology, a division of Thomson Learning, Inc, Canada.

Shelly, C. V. (2009). Discovering Computers 2009 : A Gateway to Information, Web Enhanced, Thomson Learning.

Oz Effy (2006), Management Information Systems (Fifth Edition), Thomson Course Technology.