บทที่ 6
จริยธรรมและความปลอดภัย

ในปัจจุบันเราอาจพบเห็นข่าวเกี่ยวกับปัญหาอาชญากรรมประเภทต่างๆ ตามหน้าหนังสือพิมพ์หรือในสื่อโทรทัศน์ทั่วไป สิ่งหนึ่งที่ทำให้เกิดปัญหาต่างๆเหล่านี้ขึ้นก็คือ การขาดจริยธรรมและจิตสำนึกที่ดีนั่นเอง เหตุผลด้านหนึ่งคือผู้คนยุคใหม่โดยเฉพาะอย่างยิ่งในยุคของสังคมสารสนเทศ (information society) ที่มีการนำเอาเทคโนโลยีสารสนเทศมาใช้ในชีวิตประจำวันกันอย่างมากมายนั้น ยังขาดสามัญสำนึกพื้นฐานที่ดี มีการนำเอาเทคโนโลยีสารสนเทศมาใช้ในทางที่ผิด ก่อให้เกิดความเสื่อมเสียกับผู้อื่น การใส่ร้ายป้ายสีกันบน อินเทอร์เน็ต หรือการสักลอบโจรกรรมข้อมูลของผู้อื่น แล้วนำไปใช้เพื่อเป็นประโยชน์แก่ตนเองที่มีพบเห็นอยู่เป็นประจำ เหตุผลอีกด้านหนึ่งคือ ยิ่งเทคโนโลยีเจริญมากขึ้นเพียงใด คนในสังคมยุคสารสนเทศก็ยิ่งหนีหรือห่างไกลกับคำสอนทางศาสนามากยิ่งขึ้น

ในยุคสมัยเดิม ผู้คนมักพึ่งพาและอาศัยหลักธรรมคำสอนทางศาสนาเข้ามาช่วยขัดเกลาจิตใจและสร้างสามัญสำนึกที่ดี แต่ในปัจจุบันอาจพบเห็นกลุ่มคนเหล่านี้ลดน้อยลงไปมาก โดยเฉพาะในกลุ่มคนที่เป็นวัยรุ่นหรือหนุ่มสาวยุคใหม่ ซึ่งเป็นวัยที่เกี่ยวข้องกับการนำเอาเทคโนโลยีสารสนเทศมาใช้มากที่สุด อาจหนีห่างกิจกรรมการขัดเกลาจิตใจมากยิ่งขึ้น คำสั่งสอนทางศาสนาหรือข้อควรปฏิบัติที่ดีจึงถูกมองข้ามอยู่เสมอ ส่งผลให้การนำเทคโนโลยีสารสนเทศมาใช้กับสังคมมีปัญหาขึ้นมาได้ เนื่องจากการขาดความมีจริยธรรมที่ดีนั่นเอง

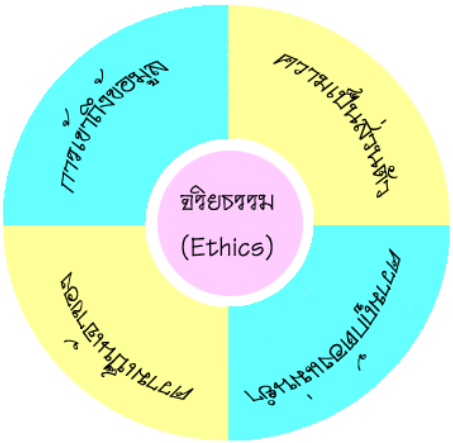
ความหมายของจริยธรรม

- จริยธรรม (ethics) หมายถึง แบบแผนความประพฤติหรือความมีสามัญสำนึกต่อสังคมในทางที่ดี โดยไม่มีกฎเกณฑ์ตายตัว ขึ้นอยู่กับกลุ่มสังคมหรือการยอมรับในสังคมนั้นๆ เป็นหลัก โดยส่วนใหญ่จริยธรรมจะเกี่ยวข้องกับการคิดและตัดสินใจได้ว่าสิ่งไหน ควร-ไม่ควร ดี-ไม่ดี ถูก-ผิด เช่น นายอมรลอกข้อสอบปลายภาคของนางสาวสมศรี การลอกข้อสอบดังกล่าวของนายอมรไม่ใช่เป็นสิ่งที่ผิดกฎหมายแต่เป็นสิ่งที่คนในสังคมการศึกษาถือว่าเป็นสิ่งที่ไม่ควรกระทำ ถือได้ว่านายอมรขาดจริยธรรมทางด้านการศึกษาที่ดีนั่นเอง
- จริยธรรมกับกฎระเบียบ คนที่ “มีจริยธรรม” อาจหมายถึง คนที่ในกลุ่มสังคมยอมรับว่ามีสามัญสำนึกที่ดี มีความประพฤติปฏิบัติดีและไม่ก่อให้เกิดผลเสียหายต่อสังคมโดยรวม ตรงกันข้ามกับคนที่ “ขาดจริยธรรม” อาจกล่าวได้ว่าเป็นคนที่กลุ่มในสังคมไม่ยอมรับ เนื่องจากมีรูปแบบการประพฤติหรือปฏิบัติตนที่ไม่มีประโยชน์ต่อสังคมโดยรวม หรืออาจส่งผลที่ไม่ดีต่อสังคม การควบคุมให้คนมีจริยธรรมที่ดีนั้นอาจใช้ข้อบังคับกฎหรือระเบียบของสังคมมาเป็นส่วนสนับสนุน เพื่อชี้ชัดลงไปว่า ถูกหรือผิด เช่น สถาบันการศึกษาออกกฎระเบียบและลงโทษนักศึกษาที่ลอกข้อสอบ โดยปรับให้ตกทุกรายวิชาที่ลงทะเบียนในภาคการศึกษานั้นๆ กรณีที่นายอมรลอกข้อสอบของเพื่อน นอกจาก “ขาดจริยธรรม” แล้วยังถือว่า “ทำผิดกฎระเบียบ” ของสถาบันอีกด้วย

จริยธรรมกับสังคมยุคสารสนเทศ

จากที่ได้เกริ่นไว้ตั้งแต่ต้น จะเห็นได้ว่าคนในสังคมยุคสารสนเทศ “ขาดจริยธรรม” กันมากขึ้น ซึ่งก่อให้เกิดปัญหาต่างๆ ต่อสังคมโดยรวมมาก นอกจากการ “ขาดจริยธรรม” แล้วในสังคมอาจพบเห็นกลุ่มคนที่ “ทำผิดกฎระเบียบ” ที่สังคมบัญญัติไว้ร่วมกันอีกด้วย โดยเฉพาะการทำผิดต่อกฎหมายของสังคมและประเทศชาติ ซึ่งเป็นภัยที่ส่งผลเสียอย่างร้ายแรง

โดยทั่วไปเมื่อพูดถึงจริยธรรมที่เกี่ยวข้องกับสังคมยุคสารสนเทศ จะพูดถึงประเด็นหรือกรอบแนวคิดทางด้านจริยธรรมที่ตั้งอยู่บนพื้นฐาน 4 ประเด็นด้วยกันคือ


จริยธรรม
(Ethics)

รูป กรอบแนวคิดทางด้านจริยธรรมที่เกี่ยวข้องกับสังคมยุคสารสนเทศ

1. ความเป็นส่วนตัว (Information Privacy)

หมายถึง สิทธิส่วนตัวของบุคคล หน่วยงาน หรือองค์กรที่จะคงไว้ซึ่งสารสนเทศ ที่มีอยู่นั้น เพื่อตัดสินว่าสารสนเทศดังกล่าวสามารถเปิดเผยหรือยินยอมให้ผู้อื่นนำไปใช้ประโยชน์ต่อหรือเผยแพร่ได้หรือไม่ หากมีการนำไปใช้จะมีการขัดการกับสิทธิดังกล่าวอย่างไร ซึ่งเป็นสิ่งที่เจ้าของสิทธิควรที่จะได้รับรู้ และด้วยเหตุที่สังคมยุคสารสนเทศมีการเจริญเติบโตอย่างต่อเนื่อง อีกทั้งข้อมูลมีการเผยแพร่และเชื่อมโยงกันอย่างมากมาย การควบคุมไม่ให้มีการละเมิดสิทธิความเป็นส่วนตัวกันนั้นอาจทำได้ค่อนข้างยาก โดยเฉพาะในยุคของ อินเทอร์เน็ตที่เพื่องฟูและคนทั่วไปสามารถเข้าถึงข้อมูลได้โดยง่าย เราอาจพบเห็นการละเมิดความเป็นส่วนตัวโดยทั่วไป เช่น มีการใช้โปรแกรมติดตามและสำรวจพฤติกรรมของผู้ที่ใช้งานบนเว็บไซท์และแอบเอาข้อมูลส่วนตัวของผู้ใช้งานนั้นไปใช้เพื่อผลประโยชน์อื่น มีการนำฐานข้อมูลส่วนตัวรวมถึงอีเมล์ของสมาชิกผู้ใช้งานบนเครือข่ายส่งให้กับบริษัทผู้รับทำโฆษณาออนไลน์ เพื่อวิเคราะห์หากลุ่มลูกค้ากลุ่มเป้าหมายว่าผู้ใช้งานใดเหมาะกับกลุ่มสินค้าที่จะโฆษณาประเภทไหนมากที่สุด จากนั้นก็ยัดส่งโฆษณาไปให้ผ่านอีเมล์เพื่อนำเสนอขายสินค้า เป็นต้น การกระทำดังกล่าวผู้ใช้งานไม่มีทางทราบเลยว่าข้อมูลของตนนั้นได้ถูกนำไปใช้กับแหล่งข้อมูลที่ไหน บ้าง มีข้อมูลส่วนใดที่ถูกนำไปใช้ ใครเป็นผู้ นำไปใช้ และจะก่อให้เกิดความไม่เป็นส่วนตัวตามมาอย่างไร

การที่อุปกรณ์ทางเทคโนโลยีสารสนเทศมีความก้าวหน้ามากขึ้น บริษัทหรือ นายจ้างอาจมีการใช้ระบบตรวจสอบและติดตามพฤติกรรมของลูกจ้างเพื่อพัฒนาประสิทธิภาพและการทำงานโดย รวม เช่น นำระบบกล้องวิดีโอวงจรปิดมาตรวจสอบและติดตามดูพฤติกรรมการทำงานของลูกจ้าง รวมถึงการใช้โปรแกรมตรวจสอบพฤติกรรมการทำงานของพนักงานบางประเภท ซึ่งผู้บริหารหรือหัวหน้างานสามารถเรียกดูข้อมูลได้ตลอดเวลา ประเด็นนี้ถึงแม้นายจ้างจะไม่ได้ทำผิดกฎหมายแต่อย่างใด เนื่องจากเป็นการตรวจสอบการทำงานของพนักงานโดยปกติ แต่ก็ถือว่าเป็นการกระทำที่ผิดจริยธรรม เนื่องจากพฤติกรรมของพนักงานถูกแอบดูอยู่ตลอดเวลา จึงทำให้พนักงานไม่มีความเป็นส่วนตัวนั่นเอง

ความเป็นส่วนตัวนี้ อาจหลีกเลี่ยงการละเมิดสิทธิดังกล่าวได้ เช่น ในกรณีของบางบริษัทที่ต้องการเข้าถึงข้อมูลส่วนตัวของลูกค้า อาจมีการประกาศแจ้งหรือสอบถามลูกค้าก่อนที่จะเข้าใช้บริการว่าจะยอมรับที่จะให้นำข้อมูลส่วนตัวนี้ไปเผยแพร่หรือนำไปให้กับบริษัทอื่นเพื่อใช้งานอย่างใดอย่างหนึ่งหรือไม่ จะพบเห็นได้จากผู้ให้บริการข้อมูลบนอินเทอร์เน็ตทั้งหลายที่ให้ใช้งานฟรีๆ เพื่อแลกกับการยอมได้ค่าโฆษณาที่ผู้ให้บริการขายนั้นจะได้มา เช่น บริการฟรีอีเมล์ บริการพื้นที่เก็บข้อมูล บริการใช้งานโปรแกรมฟรี เป็นต้น ซึ่งผู้ที่ประสงค์จะเข้าใช้งานจำเป็นจะต้องกรอกและให้รายละเอียดข้อมูลส่วนตัวเสียก่อน จากนั้นจึงจะสามารถเป็นสมาชิกโดยสมบูรณ์และใช้งานได้ในที่สุด เป็นต้น

2. ความถูกต้องแม่นยำ (Information Accuracy)

ความถูกต้องแม่นยำของข้อมูลข่าวสารเป็นประเด็นที่มีการพูดถึงมากเช่นเดียวกัน ข้อมูลและสารสนเทศที่ถูกนำเสนอ เผยแพร่ มีการเข้าถึงและใช้งานได้ง่ายในยุคของสังคมสารสนเทศนั้น อาจมีบางประเด็นที่ไม่ตรงกับความเป็นจริง มีความคลาดเคลื่อนอยู่มาก ตลอดจนความน่าเชื่อถือมีค่อนข้างน้อย การนำข้อมูลและสารสนเทศไปใช้งาน อาจก่อให้เกิดผลเสียหายได้ในกรณีที่ผู้ใช้งานขาดการวิเคราะห์ รวมถึงการตรวจสอบแหล่งที่มาของข้อมูลที่ดีพอ อคติยธรรมสำหรับผู้ที่ทำหน้าที่เผยแพร่หรือนำเสนอข้อมูลต่างๆ เหล่านี้ ยิ่งควรตระหนักว่า การนำเสนอข้อมูลสารสนเทศนั้น ควรเป็นข้อมูลที่มีการกลั่นกรองและตรวจสอบความถูกต้อง ข้อมูลมีความแม่นยำและสามารถนำไปใช้ประโยชน์ได้โดยไม่ส่งผลกระทบใดๆ กับผู้ใช้งาน

เราอาจพบเห็นแ หล่งข่าว +ทางอินเทอร์เน็ต หนังสือพิมพ์ หรือรายการโทรทัศน์ที่นำเสนอข้อมูลข่าวสาร โดยเนื้อหาที่นำเสนออาจมีทั้งข้อมูลจริง ข้อมูลที่สร้างขึ้นเอง หรือข่าวสารที่ไม่ได้มีการกลั่นกรอง เมื่อผู้ใช้งานอ่าน หรือนำไปตีความ และเข้าใจว่าข่าวสารนั้นเป็นเรื่องจริง อาจทำ ให้เกิดความผิดพลาดต่อสังคมโดยรวมและส่งผลกระทบต่อบุคคลที่เกี่ยวข้องได้ ดังนั้นการรับข้อมูลข่าวสารมาใช้จึงควรมีการตรวจสอบ ตีความและวิเคราะห์พิจารณาให้ดีเสียก่อน ผู้ใช้งานสารสนเทศจึงควรเลือกรับข้อมูลข่าวสารจากแหล่งที่มีความน่าเชื่อถือได้ และสามารถตรวจสอบแหล่งที่มาได้โดยง่าย

อคติยธรรมในประเด็นของความถูกต้องแม่นยำ อาจเกิดขึ้นจากการขาดความรอบคอบของผู้ที่เสนอและเผยแพร่ข้อมูล การขาดการดูแลเอาใจใส่กับข้อมูลอย่างดีพอ ไม่มีการปรับปรุงข้อมูลต่างๆ ให้เป็นปัจจุบัน รวมถึงมีการบันทึกและประมวลผลข้อมูลที่ผิดพลาด เมื่อนำข้อมูลข่าวสารที่ผิดพลาดนั้น ไปใช้ประกอบการตัดสินใจก็อาจทำให้เกิดผลเสียได้ ประเด็นนี้เมื่อเกิดขึ้นแล้วผู้ที่มีหน้าที่เกี่ยวข้องต้องแสดงออกถึงการมี “อคติยธรรมที่ดี” ด้วยการรับผิดชอบต่อสิ่งผิดพลาดที่เกิดขึ้น รวมถึงปรับปรุง แก้ไขรายการต่างๆ ให้มีความถูกต้อง และเพื่อสามารถนำไปใช้ประโยชน์ได้ ก่อให้เกิดผลเสียหายน้อยที่สุด

3. ความเป็นเจ้าของ (Information Property)

สังคมยุคสารสนเทศที่มีการเผยแพร่และนำเสนอข้อมูลได้อย่างง่ายดาย มีเครื่องมือและอุปกรณ์ที่ทันสมัยสนับสนุนวิธีการจัดสร้างและเผยแพร่ที่ง่ายขึ้น ก่อให้เกิ ดการลอกเลียนแบบ ทำซ้ำหรือล่วงละเมิดทางลิขสิทธิ์ (copyright) อันเป็นสิทธิ์โดยชอบในการแสดงความเป็นเจ้าของชิ้นงานนั้นๆ ของบุคคลหรือบริษัทผู้ทำการผลิต การละเมิดดังกล่าวอาจทำได้โดยที่เจ้าของผลงานได้รับผลกระทบทั้งโดยตรงและโดยอ้อม (ผลกระทบโดยตรงเช่น ยอดจำหน่ายสิ นค้านั้นลดลง เนื่องจากมีคนหันไปซื้อของที่ทำซ้ำมากขึ้น ทำให้รายได้ลดลง ส่วนผลโดยอ้อมเช่น ก่อให้เกิดภาพลักษณ์เสียหายแก่บริษัท เนื่องจากมีการดัดแปลง ต่อเติมข้อมูลและนำไปใช้ในทางที่ผิดและผู้ใช้เข้าใจว่าเป็นสิ่งที่บริษัทได้กระทำขึ้น เป็นต้น) ตัวอย่างของการขาดอคติยธรรมประเด็นนี้ ได้แก่ การทำซ้ำหรือผลิตซีดีเพลง ซีดีภาพยนตร์รวมถึงซีดีโปรแกรมละเมิดลิขสิทธิ์ออกมาจำหน่ายในตลาดมืดอย่างมากมาย โดยเฉพาะอุปกรณ์สนับสนุนในการบันทึกข้อมูลซ้ำได้นั้น มีการผลิตขึ้นมาอย่างมากและมีแนวโน้มที่ถูกลง เช่น CD-Writer, DVD-Writer ทำให้ผู้ใช้ตามบ้านก็สามารถเบันทึกข้อมูลซ้ำและนำไปใช้งานต่อได้อย่างง่ายดาย กรณีของข้อมูลบนเว็บไซต์ที่เผยแพร่ไปยังผู้ใช้งานทั่วไปก็เช่นเดียวกัน ข้อมูลบางอย่างอาจถูกสักลอบและขโมยเผยแพร่ได้ ผู้ให้บริการบางรายจึงต้องนี้แจงข้อตกลงเบื้องต้นเกี่ยวกับการประกาศความเป็นเจ้าของลิขสิทธิ์ต่างๆ ไว้ภายในเว็บไซท์แห่งนั้นด้วย

คนส่วนใหญ่มักมองว่าการ “ขโมย” สินค้าที่ขับต้องใช้และเป็นรูปธรรม เช่น ทีวี วิทยุ โทรทัศน์ เป็นการกระทำที่ผิดและไม่ควรกระทำเป็นอย่างยิ่ง แต่ถ้าเป็นการทำซ้ำข้อมูลสื่ออิเล็กทอลดังที่ยกตัวอย่างไปนั้น อาจไม่รู้สึกผิดแต่อย่างใด เพราะเป็นสินค้าที่จำต้องใช้ได้ มองไม่เห็นและรู้สึก เป็นนามธรรมมากกว่า ประเด็นนี้ผู้ใช้ควรเปลี่ยนแนวความคิดเสียใหม่ และพึงระลึกอยู่เสมอว่าการกระทำดังกล่าวเสมือนเป็นการ “ขโมย” สินค้าของผู้อื่นเช่นเดียวกันซึ่งนอกจากผิดอคติยธรรมอันดีงามแล้วยังถือว่าได้เป็นการกระทำที่ผิดกฎหมายด้วย

อย่างไรก็ดี ปัจจุบันบริษัทผู้ผลิตอาจมีแนวทางป้องกันการ ทำซ้ำข้อมูลหรือเอาข้อมูลนั้นไปใช้ต่อโดยใช้เทคโนโลยีการป้องกันแบบต่างๆ เช่น มีการใช้ serial number ซึ่งเป็นรหัสที่ได้จากการซื้อโปรแกรมที่ขายโดยผู้ผลิตและตัวแทนจำหน่ าย เพื่อเอาไว้ตรวจสอบการใช้โปรแกรมของผู้ที่เอาไปใช้ว่ามีสิทธิ์ที่ถูกต้องหรือไม่ หรือมีการใช้

เทคนิคของการเข้ารหัสสำหรับป้องกันการทำซ้ำหรือคัดลอกซีดีต้นฉบับ รวมถึงการให้ลูกค้าที่นำโปรแกรมไปใช้ต้องทำการลงทะเบียนการใช้งานไปยังบริษัทผู้ผลิตเพื่อตรวจสอบการใช้งานด้วย

4. การเข้าถึงข้อมูล (Information Accessibility)

ข้อมูลที่มีเผยแพร่และแลกเปลี่ยนกันอย่างแพร่หลายนั้น อาจจะมีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้ต่างระดับกัน โดยผู้ทำหน้าที่ดูแลระบบ (system administration) จะเป็นผู้กำหนดสิทธิ์ในการเข้าถึงข้ อมูลว่าใครควรใช้งานระดับใด และใช้ในระดับใดได้บ้าง ซึ่งบางหน่วยงานอาจกำหนดสิทธิ์ให้ใช้ได้เฉพาะกับพนักงานบางคน หรือบางแผนกที่จะเข้าถึงข้อมูลได้เท่านั้น หากเป็นพนักงานคนอื่นๆ ก็ไม่สามารถใช้ได้ บางแห่งอาจจะกำหนดให้บุคคลภายนอกให้ใช้ได้ตามความเหมาะสม หรือไม่สามารถเข้าใช้งานได้เลย ข้อมูลเกี่ยวกับเอกสารเผยแพร่ต่างๆ ข้อมูลการค้นคว้า หรือใช้อ้างอิงซึ่งมีการเก็บไว้เป็นฐานข้อมูล อาจกำหนดสิทธิ์ให้เข้าใช้งานได้เฉพาะสมาชิกที่ลงทะเบียนแล้วเท่านั้น บุคคลอื่นที่ไม่ได้เป็นสมาชิกอาจจะเข้าไปใช้บริการต่างๆ นั้นไม่ได้ เป็นต้น

เหตุที่ต้องมีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลเช่นนี้ ก็เพราะในความเป็นอิสระขององค์กรไม่สามารถเราบาบได้ว่าใครบ้างที่ "ประสงค์ดี" และใครบ้างที่ "ไม่ประสงค์ดี" ต่อองค์กร เนื่องจากในปัจจุบันสารสนเทศมีการแลกเปลี่ยนและเผยแพร่ผ่านระบบเครือข่ายมากยิ่งขึ้น ข้อมูลต่ างๆ และการเข้าถึงข้อมูลจึงกระจายมากขึ้นตามไปด้วย ข้อมูลบางอย่างที่มีความสำคัญอาจรั่วไหล หรือถูกเผยแพร่ได้โดยที่หน่วยงานนั้นๆ ไม่อาจทราบได้ ดังนั้นการกำหนดสิทธิ์เพื่อให้เข้าถึงข้อมูลได้เฉพาะบุคคลที่เกี่ยวข้องจึงสามารถป้องกันปัญหานี้ได้ในระดับหนึ่ง

อย่างไรก็ดี ถึงแม้จะมีการกำหนดสิทธิ์ดังกล่าวแล้วก็ตาม เราอาจพบเห็น "ผู้ไม่ประสงค์ดี " นี้ในสังคมยุคสารสนเทศนี้อยู่เสมอ โดยลักลอบเข้ามาใช้ข้อมูลที่ไม่ได้รับอนุญาตเพื่อนำไปใช้เพื่อประโยชน์บางอย่าง หรือเข้าก่อกวนระบบในองค์กรให้เกิดความเสียหาย เช่น ทำให้ข้อมูลถูกลบทิ้งจากฐานข้อมูล มีการเปลี่ยนแปลงแก้ไขรายการบางประการ รวมถึงการปลอมแปลงและทำความเสียหายต่อบริษัทผู้เป็นเจ้าของข้อมูล Information accessibility อาจรวมถึงการที่ข้อมูลนั้นสามารถให้บริการและเข้าถึงได้หลากหลายวิธี โดยเฉพาะอย่างยิ่งข้อมูลที่อยู่บนเว็บไซท์ อาจจำเป็นต้องออกแบบเพื่อสนับสนุนการเข้าถึงข้อมูลดังกล่าวด้วย เช่น ภาพถ่ายหรือรูปภาพที่ปรากฏบนเว็บไซท์ ควรมีคำอธิบายภาพ (Attribute alt) เพื่อสื่อความหมายไว้ด้วยว่า เป็นภาพอะไรหรือมีข้อมูลที่เกี่ยวข้องกับภาพนั้นอย่างไรบ้าง ในกรณีที่ภาพนั้นไม่ปรากฏหรืออาจ เป็นการสร้าง link หรือส่วนเชื่อโยงที่ต้องมีความหมายในตัวเพื่อบอกให้ผู้ใช้ทราบด้วยว่า หากคลิกแล้วจะไปยังหน้าใด

จากประเด็นที่กล่าวข้างต้น ผู้ใช้สารสนเทศจึงควรมีจริยธรรมที่ดีในเรื่องของการเข้าถึงข้อมูล ไ ม่ควรลักลอบเข้าไปใช้ข้อมูลของผู้ใดโดยไม่ได้รับอนุญาต ไม่พยายามก่อกวนหรือเข้าไปใช้งานข้อมูลที่อาจส่งผลเสียหายใดๆ รวมถึงการปกป้องไม่ให้สิทธิ์การเข้าถึงข้อมูลของตนเองตกไปอยู่ในมือของ "ผู้ไม่ประสงค์ดี " ควรเก็บรักษาสิทธิ์การเข้าถึงข้อมูลนั้นไว้กับตนเองอย่างปล อดภัย เช่น รหัสผ่าน ATM ของธนาคารที่เราเปิดบัญชีหรือ ข้อมูลเกี่ยวกับหมายเลขบัตรเครดิตสำหรับซื้อสินค้าไม่ควรบอกกล่าวกับใครถึงแม้จะเป็นเพื่อน หรือญาติสนิทก็ตาม เพราะอาจทำให้สิทธิ์นั้นรั่วไหลและอาจส่งผลร้ายแรงขึ้นมาได้

อาชญากรรมคอมพิวเตอร์ (Computer Crime)

การลักลอบนำเอาข้อมูลไปใช้โดยไม่ได้รับอนุญาต รวมถึง การสร้างความเสียหายต่อบุคคลและสังคมสารสนเทศโดย "ผู้ไม่ประสงค์ดี " ที่กระจายอยู่ทั่วทุกมุมโลกนี้ ทำให้เกิดปัญหาที่เรียกว่า *อาชญากรรมคอมพิวเตอร์ (computer crime)* ขึ้น ซึ่งเป็นปัญหาที่ก่อให้เกิดความเสียหายเป็นอย่างมาก สิ่งเหล่านี้เกิดขึ้นจากการขาด "จริยธรรมที่ดี" ดังที่กล่าวไว้แต่ต้นนั่นเอง

อาชญากรรมคอมพิวเตอร์ไม่ใช่เรื่องใหม่ในสังคมสารสนเทศ เราอาจเคยพบปัญหาเกี่ยวกับการกำเนิดของไวรัสคอมพิวเตอร์ซึ่งเป็นโปรแกรมที่สร้างความเสียหายให้กับระบบมาแล้วในยุคก่อนๆ ซึ่งผลเสียหายนั้นมีตั้งแต่ไม่รุนแรง เพียงแค่สร้างความรำคาญในการใช้งานไปจนถึงทำให้คอมพิวเตอร์ขององค์กรล่มทั้งระบบ นับเป็นมูลค่าความเสียหายมากมายมหาศาลทีเดียว

ปัจจุบันการก่ออาชญากรรมคอมพิวเตอร์ไม่ได้มีแค่การโจมตีหรือแพร่กระจายไวรัสอีกต่อไป ยิ่งรูปแบบของการดำเนินงานทางด้านธุรกิจที่มีการแข่งขันกันสูงอย่างในปัจจุบัน อาจพบเห็นอาชญากรรมคอมพิวเตอร์ที่สร้างความร้ายแรงมากกว่าเดิม มีการบุกรุกและเจาะระบบเพื่อแอบเข้าไปแก้ไขข้อมูลทางการเงินของธนาคาร การเข้าไปขโมยข้อมูลความลับของบริษัทคู่แข่ง รวมถึงการก่อกวนเพื่อให้ระบบคอมพิวเตอร์เป้าหมายเสียหายและไม่สามารถทำงานได้ สิ่งเหล่านี้เกิดขึ้นเพราะการแพร่กระจายของการใช้งานเทคโนโลยีที่เกี่ยวข้องกับอินเทอร์เน็ตที่ไม่หยุดยั้งนี่เอง

การก่ออาชญากรรมทางคอมพิวเตอร์ นอกจากเป็นการกระทำที่ “ขาดจริยธรรม” ที่ดีแล้ว ยังถือว่าเป็นการกระทำที่ผิดกฎหมายเช่นเดียวกัน หลายประเทศมีการออกกฎหมายของตัวเกี่ยวกับการก่ออาชญากรรมคอมพิวเตอร์ขึ้นแล้ว แต่อาจแตกต่างกันไปในประเด็นของเนื้อหาที่กระทำผิด ทั้งนี้ขึ้นอยู่กับวัฒนธรรม สภาพแวดล้อมและระดับความร้ายแรงของการก่ออาชญากรรมที่กระทำขึ้นด้วย สำหรับประเทศไทยได้เล็งเห็นถึงความสำคัญเกี่ยวกับอาชญากรรมคอมพิวเตอร์ เช่นเดียวกับนานาประเทศ และได้ออกร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ซึ่งผ่านคณะรัฐมนตรีแล้วเมื่อวันที่ 23 กันยายน 2546 ใช้เป็นกฎหมายที่กำหนดฐานความผิดเกี่ยวกับการกระทำต่อระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ (รายละเอียดเพิ่มเติมที่ www.ictlaw.thaigov.net/cc/index.html) รูปแบบของการก่ออาชญากรรมทางคอมพิวเตอร์ที่พบเห็นทั่วไป ยกตัวอย่างได้ดังนี้

การสักลอบเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access and Use)

ข้อมูลหรือสารสนเทศในปัจจุบันถือว่าเป็นสิ่งที่มีความสำคัญยิ่ง โดยเฉพาะข้อมูลเกี่ยวกับการดำเนินธุรกิจ ข้อมูลส่วนบุคคลรวมถึงข้อมูลความลับขององค์กร อาจมีผู้ไม่ประสงค์ดีเข้ามาสักลอบอ่านข้อมูลและนำไปใช้ในทางที่เสียหายได้ กลุ่มบุคคลเหล่านี้จะสักลอบเข้ามาใช้เครื่องคอมพิวเตอร์เป้าหมายเสมือนเป็นเครื่องของตนเอง โดยที่เป้าหมายมิอาจรู้ตัวได้ การสักลอบเข้าถึงข้อมูลโดยไม่อนุญาตมีทั้งที่เจตนาแค่เข้าไปดูข้อมูลอย่างเดียวและตั้งใจก่อให้เกิดความเสียหายต่างๆกับข้อมูลด้วย

ตัวอย่างของการสักลอบเข้าถึงข้อมูลที่พบเห็นบ่อยที่สุดในปัจจุบัน เช่น การสักลอบเข้าไปเปลี่ยน ยนแปลงแก้ไขข้อมูลเว็บเพจหน้าแรกขององค์กรต่างๆ ซึ่งเกิดจากความไม่พอใจในเหตุการณ์บางอย่าง การต่อต้านสงคราม การแบ่งกลุ่มชนนั้น หรือทำเพื่อให้องค์กรนั้นได้รับความเสียหาย หรือเพียงแค่สร้างชื่อเสียงให้ตนเอง การกระทำดังกล่าวเป็นสิ่งที่เกิดขึ้นและพบเห็นบ่อยมาก บนเครือข่ายอินเทอร์เน็ต บางรายมักจะทิ้งร่องรอยเพื่อบ่งบอกให้ทราบว่าพวกเขาได้เข้ามายังระบบเว็บเซิร์ฟเวอร์ขององค์กรนั้นๆ แล้ว โดยพิมพ์ข้อความรวมถึงนำภาพลามกอนาจารติดตั้งไว้แทนหน้าเว็บเพจอันเดิม (หาข้อมูลเพิ่มเติมได้ที่ www.zone-h.org) กลุ่มคนที่สักลอบการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต สามารถแบ่งออกได้เป็น 3 กลุ่มด้วยกันคือ

1. แฮกเกอร์ (Hacker)

เป็นกลุ่มคนที่มีความรู้ ความสามารถทางด้านคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เป็นอย่างดี มักอาศัยช่องโหว่ของเทคโนโลยีสักลอบดูข้อมูลของผู้อื่นที่ไม่ได้รับอนุญาต บางครั้งทำเพื่อต้องการทดสอบความรู้ของตนเอง มักเป็นคนที่ชอบเสาะแสวงหาความรู้ใหม่ๆ อยู่เสมอ และมีความอยากรู้ อยากเห็น หรือต้องการศึกษาเพื่อทดลองขีดความสามารถของตนเองเกินกว่าผู้ใช้งานปกติธรรมดาที่ใช้งานเพียงเพื่อจำเป็นเท่านั้น โดยเจตนาแล้วไม่ได้มุ่งร้ายต่อข้อมูลแต่อย่างใด แฮกเกอร์บางคนอาจเข้าไปหาจุดบกพร่องต่างๆ ของระบบเครือข่ายแล้วแจ้งกับผู้ดูแลระบบว่า ระบบเครือข่ายนั้นบกพร่องและควรแก้ไขข้อมูลส่วนไหนอีกบ้าง ด้วยเจตนาที่ไม่ได้มีความประสงค์ร้ายต่อข้อมูลนี้ บางครั้งจึงมักนิยมเรียกว่า เป็นพวก *กลุ่มคนหมวกขาว* หรือ white hat โดยปกติแล้วมักไม่ยอมเปิดเผยตัวให้คนอื่นทราบแต่อย่างใด แต่หากเราเข้าไปยังกลุ่มพบปะแลกเปลี่ยนความคิดเห็นทั่วไปบนอินเทอร์เน็ตแล้วขอความช่วยเหลืออาจจะพบเห็นค่อนข้างบ่อย

2. แครกเกอร์ (Cracker)

เป็นกลุ่มคนที่ มีความรู้ความสามารถเช่นเดียวกันกับกลุ่มแฮกเกอร์ แต่มีเจตนาที่แตกต่างกันอย่างสิ้นเชิง มักเรียกกันว่าเป็น *กลุ่มคนหมวกดำ* หรือ *black hat* ซึ่งจะมีพฤติกรรมที่ตรงกันข้ามกับกลุ่มหมวกขาว เพราะจะสร้างความเสียหายที่รุนแรงกว่า

โดยปกติแครกเกอร์จะมุ่งทำลายระบบหรือสักลอบเข้าไปแก้ไข เปลี่ยนแปลงหรือทำลายข้อมูลในระบบนั้นทิ้ง การกระทำของแครกเกอร์มีเจตนาให้เกิดความเสียหายของมูลค่ามากกว่าแฮกเกอร์ ส่วนใหญ่เป็นกลุ่มคนที่มีความชำนาญทางด้านคอมพิวเตอร์ ระบบเครือข่าย หรือหากเขียนโปรแกรมคอมพิวเตอร์มากเป็นพิเศษ ซึ่งถือได้ว่าเป็นกลุ่มบุคคลที่มีความร้ายแรงมากในยุคปัจจุบัน

3. สคริปต์คิดดี้ (Script Kiddy)

แปลตามศัพท์ว่า พวกเด็กที่นอบเล่นสคริปต์ บุคคลกลุ่มนี้ปัจจุบันเริ่มมีจำนวนมากขึ้นอย่างรวดเร็ว เนื่องจากในสังคมของอินเทอร์เน็ตมักมีแหล่งพบปะแลกเปลี่ยนโปรแกรมหรือสคริปต์ (scripts) ที่มีคนเขียนและนำออกมาเผยแพร่ให้ทดลองใช้กันอย่างมากมายทั่วโลก คนกลุ่มนี้มักเป็นเด็กวัยอยากรู้อยากเห็น หรือนักศึกษาจบใหม่ที่ไม่จำเป็นต้องมีความรู้เกี่ยวกับการเจาะระบบมากนัก เพียงแค่อาศัยโปรแกรมหรือเครื่องมือบางอย่างที่หามาได้จากแหล่งต่างๆ บนอินเทอร์เน็ต และทำตามข้อมูลการใช้งาน ก็สามารถเข้าไปก่อกวนระบบคอมพิวเตอร์ผู้อื่นให้เกิดความเสียหายได้แล้ว เช่น การลอบอ่านอีเมล์ การขโมยรหัสผ่านของผู้อื่น การใช้โปรแกรมก่อกวนอย่างง่าย เป็นต้น

การขโมยและทำลายอุปกรณ์ (Hardware Theft and Vandalism)

อุปกรณ์คอมพิวเตอร์เป็นอีกสิ่งหนึ่งที่เสี่ยงต่อการสักลอบขโมยไปใช้งานเช่นเดียวกับการสักลอบโจรกรรมข้อมูล โดยเฉพาะอย่างยิ่งกับอุปกรณ์ขนาดเล็ก เครื่องคอมพิวเตอร์แบบโน๊ตบุ๊คหรืออุปกรณ์ประเภทโทรศัพท์มือถือ ซึ่งมักเกิดจากการไม่รอบคอบและวางอุปกรณ์ไว้ในที่มีความเสี่ยงต่อการโจรกรรม เช่น วางไว้บนโต๊ะทำงานโดยไม่มีใครอยู่ในห้อง หรือไม่มีระบบกุญแจป้องกันที่ดีพอ อาจทำให้ผู้ไม่ประสงค์ดีเข้ามาโจรกรรมได้ บางครั้งอาจเกิดจากบุคคลภายนอกหรือภายในองค์กรก็ได้ โดยเฉพาะกลุ่มคนประเภทหลังที่เคยทำงานอยู่หรือเคยเกี่ยวข้องกับองค์กรนั้นมาก่อน อาจเกิดความไม่พอใจและมีการทำลายอุปกรณ์ต่างๆ เพื่อองค์กรได้รับความเสียหายด้วย

ในสถาบันศึกษาบางแห่ง อาจพบเห็นการโจรกรรมเกี่ยวกับอุปกรณ์ภายในคอมพิวเตอร์ เช่น ฮาร์ดดิสก์ หรือ RAM ได้ ผู้ไม่ประสงค์ดีในคราบนักศึกษาอาจสวมรอยเข้าไปใช้บริการของศูนย์คอมพิวเตอร์ แล้วทำการแกะหรือถอดเอาอุปกรณ์ที่ต้องการไปโดยง่ายหรือกรณีของตู้ ATM ของธนาคารพาณิชย์ที่กระจายอยู่ทั่วประเทศที่มีเงินอยู่ในตู้จำนวนมากในแต่ละวัน อาจเป็นเป้าหมายของผู้ไม่ประสงค์ดี โดยอาจจับแกะ ทุบทิ้งหรือทำลาย เพื่อสักลอบโจรกรรมเอาธนบัตรที่เก็บอยู่ในตู้ไปได้ โดยเฉพาะอย่างยิ่งกับตู้ที่มีการติดตั้งไว้ในบริเวณที่ปลอดคน สิ่งเหล่านี้มีทางแก้และป้องกันที่ทำได้ง่ายที่สุดคือการสร้างระบบการรักษาความปลอดภัยที่ดีพอ มีการติดตั้งอุปกรณ์เพื่อช่วยป้องกันและรักษาความปลอดภัย มีการตรวจการเข้าออกของบุคคลที่มาติดต่ออย่างเป็น ระบบ รวมถึงวางมาตรการใช้งานอุปกรณ์อย่างเข้มงวด ซึ่งอาจช่วยป้องกันปัญหาต่างๆ เหล่านี้ได้

การขโมยโปรแกรมคอมพิวเตอร์ (Software Theft)

เป็นการก่ออาชญากรรมทางคอมพิวเตอร์ที่กระทำเพื่อขโมยเอาข้อมูลของโปรแกรมรวมถึงศัตลอกข้อมูลโปรแกรมโดยผิดกฎหมาย โดยเฉพาะการทำซ้ำหรือการละเมิดลิขสิทธิ์ข้อมูล ซึ่งอาจพบเห็นได้โดยทั่วไป การกระทำดังกล่าวถูกเปรียบเทียบว่าเหมือนกับการกระทำของโจรสลัดที่พยายามขโมยเอาทรัพย์สินอันมีค่าของผู้ที่อยู่บนเรือและหายตัวไปอย่างง่ายดายกลางน่านน้ำทะเล การละเมิดสิทธิ์โปรแกรมโดยๆ ก็เหมือนกับการปล้น นทรัพย์สินอันมีค่าของผู้อื่นเช่นเดียวกัน และยากที่จะจับตัวได้เนื่องจากสามารถทำซ้ำได้ง่ายมาก บางครั้งสามารถทำได้เพียงไม่กี่วินาทีส่งผลให้บริษัทผู้ผลิตโปรแกรมได้รับความเสียหายตามมา เนื่องจากมีการสักลอบทำซ้ำข้อมูลโปรแกรมและนำออกวาง

จำหน่ายแทนที่โปรแกรมต้น ฉบับจริง อีกทั้งยังมีราคาที่ถูกกว่ามาก ผู้ใช้งานทั่วไปใช้โปรแกรมที่มีการทำซ้ำเหล่านั้นแทน

บริษัทผู้ผลิตบางราย อาจกำหนดให้ผู้ใช้งานที่ซื้อโปรแกรมไปใช้สามารถใช้ได้จำนวนจำกัด ไม่สามารถนำไปทำซ้ำหรือใช้กับเครื่องคอมพิวเตอร์เครื่องอื่นๆได้ โดยอาจมีการจำกัดปริมาณการใช้งานต่อเครื่อง หากผู้ใช้งานนำไปใช้เกินกว่าที่กำหนดก็ถือว่าเป็นการละเมิดลิขสิทธิ์เช่นเดียวกัน การนี้อาจพบเห็นได้กับการกำหนดสิทธิ์ควบคุมการใช้งานในร้านอินเทอร์เน็ตคาเฟ่หรือตามบริษัทที่มีคอมพิวเตอร์เชื่อมต่อกันเป็นจำนวนมาก เป็นต้น

การใช้งานในโปรแกรม ที่ผลิตจากบริษัทขนาดใหญ่ได้รับความนิยมจาก ผู้ใช้มาก ซึ่งมีการผลิตและจำหน่ายออกไปในหลายๆ ประเทศ สร้างรายได้อย่างมหาศาลกับบริษัทผู้ผลิตโปรแกรมขนาดใหญ่เหล่านี้ จึงทำให้การละเมิดลิขสิทธิ์มากขึ้นด้วยเช่นกัน ด้วยเหตุนี้บริษัทผู้ผลิตโปรแกรมและบริษัทคอมพิวเตอร์ที่เกี่ยวข้อง จึงได้รวมตัวกันก่อตั้งองค์กรที่เรียกว่า BSA (Business Software Alliance) ขึ้นมาเพื่อควบคุมและดูแลเรื่องการละเมิดลิขสิทธิ์ รวมถึงการทำความเข้าใจกับ ผู้บริโภคให้ตระหนักถึง (รายละเอียดเพิ่มเติมที่ www.bsa.org) ซึ่งประกอบด้วยพันธมิตรที่เกี่ยวข้องจำนวน 23 รายด้วยกันและกระจายอยู่ใน 60 ประเทศทั่วโลก ซึ่งส่งผลกระทำให้ระดับการละเมิดลิขสิทธิ์โปรแกรมลดน้อยลงไปบ้าง

กลุ่มพันธมิตรธุรกิจซอฟแวร์หรือกลุ่ม BSA

การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย (Malicious Code)

รูปแบบ อาชญากรรมทางคอมพิวเตอร์ที่พบมากในปัจจุบันและสร้างความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์เป็นอย่างมาก คือ กลุ่มโปรแกรมประสงค์ร้าย (malicious code) ซึ่งเป็นโปรแกรมที่มุ่งเน้นการก่อกวนและทำลายระบบข้อมูลคอมพิวเตอร์ ซึ่งพอจะยกตัวอย่างของกลุ่มโปรแกรมต่างๆ ได้ดังนี้

ไวรัสคอมพิวเตอร์ (Computer Virus)

ไวรัสคอมพิวเตอร์ จัดเป็นรูปแบบโปรแกรมชนิดหนึ่งที่พัฒนาขึ้นโดยนักพัฒนาโปรแกรมที่มีความชำนาญเฉพาะด้าน มุ่งทำให้เกิดผลเสียหายต่อข้อมูลทางคอมพิวเตอร์ หลักการทำงานจะอาศัยคำสั่งที่เขียนมาไว้ในตัวโปรแกรม เพื่อกระจายไปยังเ คอมพิวเตอร์เป้าหมาย อาจแพร่กระจายผ่านการทำสำเนาข้อมูลด้วยสื่อบันทึกข้อมูลสำรองจากคอมพิวเตอร์เครื่องหนึ่งไปอีกเครื่องหนึ่ง หรือมีการแลกเปลี่ยนข้อมูลกันระหว่างเครื่องคอมพิวเตอร์ โดยอาศัยคนกระทำการอย่างใดอย่างหนึ่งกับพาหะที่โปรแกรมไวรัสนั้นแฝงตัวอยู่เพื่อแพร่กระจาย เช่น รันโปรแกรมอ่านอีเมล์ เปิดเว็บเพจ หรือเปิดไฟล์ที่แนบมากับอีเมล์ ฯลฯ เป็นต้น

เมื่อไวรัสคอมพิวเตอร์แพร่กระจายจะส่งผลให้ไฟล์และคอมพิวเตอร์เป้าหมายนั้นติดโปรแกรมไวรัสและได้รับความเสียหายตามไปด้วยโดยเจ้าของเครื่องแ ทบไม่รู้ตัวเลย การแฝงตัวมากับพาหะ เช่น อีเมล์หรือโปรแกรมโดยที่เจ้าของไม่ทันระวังตัวนี้เอง จึงเป็นเหตุผลให้เรียกโปรแกรมกลุ่มนี้ว่าเป็น “ไวรัสคอมพิวเตอร์ ” เช่นเดียวกับการที่มนุษย์ได้รับไวรัสเชื้อโรคที่ส่งระบบการทำงานของร่างกายผิดพลาดนั่นเอง

เวิร์มหรือหนอนอินเทอร์เน็ต (Worm)

เวิร์มหรือมักเรียกอีกชื่อหนึ่งว่า หนอนอินเทอร์เน็ต เป็นกลุ่มโปรแกรมประสงค์ร้ายอีกประเภทหนึ่งที่เกิดขึ้นมากในปัจจุบัน เหตุที่มีการเรียก ชื่อเหมือนกับสัตว์ประเภทหนอนนี้ เพราะเป็นโปรแกรมที่มีความรุนแรงกว่าไวรัสคอมพิวเตอร์แบบเดิมมาก สามารถเจาะไชไปยังเครื่อง คอมพิวเตอร์ต่างๆ ได้เอง เกิดขึ้นมาในยุคของอินเทอร์เน็ตที่เฟื่องฟู ซึ่งจะคอยทำลายระบบทรัพยากรทางคอมพิวเตอร์ให้มีประสิทธิภาพที่ลดลงและไม่อาจทำงานต่อไปได้ เปรียบเสมือนกับหนอนที่แอบกัดกินผลไม้อยู่ภายใน จนทำให้ไม่สามารถรับประทานผลไม้นั้นได้

เวิร์มเป็นโปรแกรมที่คล้ายกับไวรัสคอมพิวเตอร์แต่ถูกสร้างขึ้นเพื่อมุ่งเน้นการกระจายที่แพร่หลายและรุนแรงมากกว่าไวรัสแบบเดิม อาศัยเครือข่ายคอมพิวเตอร์เพื่อการแพร่กระจาย โดยเฉพาะอย่างยิ่งในเครือข่ายอินเทอร์เน็ต ซึ่งมีปริมาณผู้ใช้มหาศาล การแพร่กระจายของเวิร์มจึงมากขึ้นไปด้วย การทำงานจะมีการตรวจสอบเพื่อหาเครื่องเป้าหมายที่เชื่อมต่อกับอินเทอร์เน็ตเสียก่อน จากนั้นจะวิ่งเจาะเข้าไปเองได้ การติดเวิร์มนี้จะเป็นไปได้อย่างรุนแรงและรวดเร็วมากเพราะลักษณะที่เด่นของเวิร์มคือ จะสามารถสำเนาซ้ำตัวมันเองได้อย่างมหาศาลภายในเวลาเพียงไม่กี่นาที ผลของการติดเวิร์มจะทำให้ทรัพยากรระบบเครื่องคอมพิวเตอร์มีน้อยลง เกิดทำงานผิดพลาดและอาจส่งผลเสียหายอย่างร้ายแรงได้ เช่น ฮาร์ดดิสก์มีข้อมูลเต็ม เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ สั่งพิมพ์งานไม่ได้ หน้าจอดับไปเอง หรือตัวคอมพิวเตอร์ปิดลงไปเองโดยไม่มีเหตุผล

ม้าโทรจัน (Trojan horses)

เป็นรูปแบบของโปรแกรมประสงค์ร้ายอีกชนิดหนึ่ง แตกต่างจากไวรัสและหนอนอินเตอร์เน็ต ปกติจะทำงานโดยอาศัยการฝังตัวอยู่ในระบบคอมพิวเตอร์เครื่องนั้น และจะไม่มีการแพร่กระจายตัวแต่อย่างใด โปรแกรมจะถูกตั้งเวลาการทำงานหรือควบคุมการทำงา นระยะไกลจากผู้ไม่ประสงค์ดี เพื่อให้เข้ามาทำงานยังเครื่องคอมพิวเตอร์เป้าหมายได้ ชื่อของ “ม้าโทรจัน” มาจากเรื่องเล่าของชาวกรีกที่ว่าด้วยการบุกยึดเมืองทรอยในสมัยก่อน จะบุกยึดเมืองยังไงก็ไม่สำเร็จ จึงออกอุบายทำทีเป็นถอยทัพ และนำทหารส่วนหนึ่งไปแอบซ่อนอยู่ในม้าไม้และทิ้งไว้หน้าเมืองเพื่อเป็นสัญลักษณ์ของการยอมแพ้ ชาวเมืองหลงกลจึงลากม้าไม้ผ่านเข้าประตูเมืองไป พอตกกลางคืนทหารที่แอบซ่อนตัวอยู่จึงเปิดท้องม้าไม้ออกมาและเปิดประตูให้กับเพื่อนทหารฝ่ายเดียวกันมาโจมตียึดเมืองทรอยได้สำเร็จ โปรแกรมแบบม้าโทรจันก็อาศัย ลักษณะการทำงานโดยกลยุทธ์แบบดังกล่าว นั่นคือจะแอบเข้าไปอยู่ในเครื่องคอมพิวเตอร์เป้าหมายโดยที่ไม่ให้รู้ตัว เช่น แสร้งทำเป็นโปรแกรมยูทิลิตี้ให้ใช้งานแต่แท้ที่จริงแล้วก็คือโปรแกรมอันตรายที่มีผู้ไม่ประสงค์ดีสักลอบเข้ามาติดตั้งไว้แล้วนั้นเอง เมื่อถึงเวลาหรือต้องการควบคุมเพื่อเป้าประสงค์ร้ายบางอย่างก็จะทำงานได้ทันที เช่น เปิดปิดไดรว์ CD-ROM เปลี่ยนแปลง ลบ แก้ไขข้อมูล หรือควบคุมคีย์บอร์ดและดูภาพการทำงานที่หน้าจอของเครื่องเป้าหมายได้ เป็นต้น

แนวทางการป้องกันและแก้ปัญหาที่จะถูกโจมตีด้วยวิธีการเหล่านี้ เราจึงควรติดตามรับข่าวสารใหม่ ๆ เกี่ยวกับโปรแกรมประสงค์ร้ายอยู่อย่างสม่ำเสมอ ซึ่งจะทำให้ทราบถึงรูปแบบการแพร่กระจายของโปรแกรมวิธีการกำจัดและลบข้อมูล รวมถึงหลักการแก้ปัญหาเบื้องต้นได้เป็นอย่างดี ซึ่งมีหน่วยงานที่น่วยเหลือและให้ข้อมูลได้เป็นอย่างดี สำหรับประเทศไทยสามารถหาข้อมูลได้ที่เว็บไซท์ของศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย หรือศูนย์ ThaiCERT (Thai Computer Emergency Response Team) ได้ที่ www.thaicert.nectec.or.th หรือ สามารถติดตามข่าวสารได้ จากศูนย์ประสานงานการรักษาความปลอดภัยของต่างประเทศหรือศูนย์ CERT/CC (Computer Emergency Response Team Coordination Center) ได้เช่นเดียวกันที่ www.cert.org

การก่อกวนระบบด้วยสปายแวร์ (Spyware)

การเข้าใช้งานอินเตอร์เน็ตโดยเปิ ดดูบางเว็บไซท์ที่ไม่เหมาะสมหรือเลือกติดต่อเพื่อดาวน์โหลดเอาข้อมูลฟรีต่าง ๆ ทั้งหลายโดยไม่ทันระมัดระวัง อาจทำให้ถูกก่อกวนด้วยโปรแกรมประเภทสะกดรอยข้อมูลหรือที่นิยมเรียกกันว่า สปายแวร์ (spyware) ได้

สปายแวร์เป็นกลุ่มของโปรแกรมที่ถูกเขียนขึ้นมาใช้งานบนอินเ ตอร์เน็ตเป็นหลัก โดยอาจไม่ก่อระทำการร้ายแรงต่อคอมพิวเตอร์เป้าหมายเท่ากับโปรแกรมประสงค์ร้ายอย่างที่ยกตัวอย่างไว้แต่ต้น เพียงบางครั้งอาจสร้าง

ความรำคาญให้กับผู้ใช้เมื่อเชื่อมต่อเข้ากับอินเตอร์เน็ต สปายแวร์บางตัวอาจฝังแถมด้วยการแทรกโฆษณาทั้งหลายที่เราไม่ต้องการให้เห็นอยู่บนหน้าบราวเซอร์ที่ใช้สำหรับท่องเว็บอยู่ตลอดเวลา บางโปรแกรมอาจเข้าไปเปลี่ยนหน้าแรกของบราวเซอร์ที่ตั้งไว้แล้วให้เป็นโฆษณาของเว็บอื่น ๆ ที่เราไม่ต้องการด้วย ซึ่งบางครั้งอาจทำให้หงุดหงิดใจเนื่องจากไม่สามารถทำการเปลี่ยนค่าต่าง ๆ เหล่านั้นกลับคืนมาได้อีก

โดยปกติแล้วโปรแกรมประเภทสปายแวร์นี้มักจะแฝงตัวอยู่กับเว็บไซท์ไม่พึงประสงค์บางประเภท รวมถึงโปรแกรมที่แจกฟรีทั้งหลาย ซึ่งผู้เขียนโปรแกรมบางรายก็จะฝังสปายแวร์นี้มาด้วย บางโปรแกรมที่ร้ายกว่านั้นยังสามารถควบคุมการเชื่อมต่ออินเตอร์เน็ตได้ด้วย เช่น หยุดการติดต่อ (disconnect) และเริ่มเชื่อมต่อใหม่ (connect) โดยหมุนโมเด็มไปยังเลขหมายปลายทางในต่างประเทศตามที่โปรแกรมระบุไว้เองโดยอัตโนมัติ ซึ่งอาจทำให้ผู้ใช้งานได้รับแจ้งยอดค่าใช้จ่ายโทรศัพท์แพงมากขึ้นตามไปด้วยนั่นเอง

การก่อกวนระบบด้วยสแปมเมล์ (Spam Mail)

สแปมเมล์ คือ รูปแบบของจดหมายอิเล็กทรอนิกส์ที่เราไม่ต้องการ เป็นภัยคุกคามอีกประเภทหนึ่งที่มักพบเห็นในปัจจุบัน วิธีการก่อกวนจะอาศัยการส่งอีเมล์แบบหว่านแห และส่งต่อให้กับผู้รับจำนวนมากที่ถึงแม้จะไม่รู้จักกันมาก่อนก็ตามให้ได้รับข้อมูลข่าวสารประเภทเชิญชวนให้ซื้อสินค้า หรือเสนอให้ใช้บริการของเว็บไซท์นั้น

ตามปกติ สแปมเมล์อาจถูกส่งโดยแฮกเกอร์ที่ได้รับจากการว่าจ้างมาจากบริษัทผู้ที่ต้องการสร้างโฆษณาแบบเหวี่ยงแหนี้ หรืออาจเกิดจากการถูกสะกดรอยตามด้วยการใช้โปรแกรมประเภทสปายแวร์ดังที่กล่าวไว้ข้างต้นซึ่งจะเก็บฐานข้อมูลการใช้งานต่าง ๆ บนอินเตอร์เน็ตที่ผู้ใช้งานได้เชื่อมต่อไว้ จากนั้นก็จะส่งโฆษณามาให้ตามความสนใจที่ได้จากข้อมูลในโปรแกรมสปายแวร์บางโปรแกรมดังกล่าวนั่นเอง

การก่อกวนด้วยวิธีนี้ นอกจากจะก่อให้เกิดความน่ารำคาญใจกับผู้ใช้แล้ว ข้อมูลพื้นที่สำหรับเก็บอีเมล์ ของผู้ใช้รายนั้นบนเครื่องแม่ข่ายที่ให้บริการที่เรียกว่า mail server อาจไม่พอมีที่เหลือสำหรับรับจดหมายฉบับอื่นอีกได้ เป็นผลให้ผู้ใช้รายนั้นอาจพลาดกับการรับข้อมูลข่าวสารสำคัญ ๆ บางฉบับจากเพื่อนหรือคนที่ต้องการส่งมายังบัญชีอีเมล์นั้นได้ เนื่องจากพื้นที่เก็บข้อมูลนั้นเต็มไปแล้วนั่นเอง

การหลอกลวงเหยื่อเพื่อล้วงเอาข้อมูลส่วนตัว (Phishing)

การใช้งานบนเครือข่ายอินเตอร์เน็ต โดยเฉพาะอย่างยิ่งกับการทำธุรกรรมที่จำเป็นต้องใส่ข้อมูลส่วนตัวบ้อนเข้าไปก่อนเรียกขอใช้บริการ เช่น รายละเอียดหมายเลขบัตรเครดิต ชื่อผู้ใช้หรือรหัสผ่านในการใช้งานบนเว็บไซท์ของผู้ให้บริการตัวจริง เช่น เว็บไซท์ประมูลสินค้าออนไลน์ เว็บไซท์สำหรับทำธุรกรรมการเงิน อาจถูกหลอกลวงจากผู้ไม่ประสงค์ดีด้วยการส่งอีเมล์หลอกไปยังสมาชิก เพื่อขอข้อมูลบางอย่างที่จำเป็น โดยใช้คำกล่าวอ้างต่าง ๆ เขียนขึ้นมาเองให้เหยื่อตายใจและหลงเชื่อในที่สุด

วิธีการจะอาศัยกลลวงโดยใช้ URL (uniform resource locator หรือตำแหน่งที่ตั้งของไฟล์บนอินเตอร์เน็ต) ปลอม เพื่อหลอกล่อเหยื่อให้ตายใจเสมือนกับว่าเป็นของผู้ให้บริการตัวจริง แต่แท้ที่จริงแล้ว กลับเป็น URL ของผู้ไม่ประสงค์ดีที่ทำขึ้น มาเลียนแบบนั่นเอง (จะเหมือนกับเอาของเว็บไซท์ตัวจริงแทบทุกประการ) เมื่อผู้ใช้ขาดความรอบคอบและเผลอคลิกไปยังข้อมูลที่แอ้งไว้และป้อนข้อมูลส่วนตัว เช่นหมายเลขบัตรเครดิต ข้อมูลดังกล่าวจะถูกเก็บไว้และเอาไปใช้ในทางที่อาจทำให้เกิดความเสียหายต่อสมาชิกผู้นั้นได้ ก็ กล่าวได้อีกอย่างหนึ่งว่าเป็นวิธีการแบบอ่อยเหยื่อออนไลน์เหมือนกับกิจกรรมของการตกปลานั่นเอง

การรักษาความปลอดภัยระบบคอมพิวเตอร์

การใช้งานคอมพิวเตอร์และการเข้าถึงข้อมูลบนเครือข่าย มีความเสี่ยงต่อการถูกบุกรุก ถูกโจมตี รวมถึงการล้วงเอาข้อมูลโดยไม่ได้รู้ บอนุญาตด้วยรูปแบบและวิธีการแตกต่างกันไป บางวิธีอาจมีผลเสียหายต่อระบบเพียงเล็กน้อย แต่บางวิธีการนำมาซึ่งความเสียหายอย่างร้ายแรง จนบางครั้งระบบคอมพิวเตอร์ไม่สามารถทำงานได้ต่อไป ส่งผลถึงความเสียหายทางธุรกิจต่าง ๆ ได้ การเตรียมรักษาความปลอดภัยจากการใช้งานจึงเป็นวิธีการที่ดีที่สุดที่จะไม่ให้เกิดเหตุการณ์เหล่านี้ได้ ตัวอย่างของการรักษาความปลอดภัยเบื้องต้นที่นิยมใช้กันในปัจจุบัน พอจะยกตัวอย่างได้ดังนี้

การติดตั้งโปรแกรมป้องกันไวรัส (Antivirus Program)

การแพร่กระจายตัวของไวรัส หนอนอินเตอร์เน็ต และโปรแกรมประสงค์ร้ายอื่น ๆ เป็นไปอย่างรวดเร็ว บางครั้งผู้ใช้เครื่องคอมพิวเตอร์แทบจะไม่รู้เลยว่าเครื่องของตนติดกับดักโปรแกรมประสงค์ร้ายเหล่านั้นแล้วหรือไม่ การใช้เครื่องมือเพื่อคอยตรวจสอบและเฝ้าติดตามการฆมาเยือนของโปรแกรมเหล่านี้จึงเป็นหนทางที่ดีที่สุด ซึ่งที่นิยมกันมากคือการใช้โปรแกรมป้องกันไวรัส (Antivirus Program) ซึ่งเปรียบเสมือนกับยามรักษาความปลอดภัยที่มาเฝ้าดูแลหน้าบ้าน หากโครงที่แปลกปลอมหรือต้องสงสัยก็จะสามารถเข้ามาได้ยกเว้นว่าจะได้รับอนุญาตเสียก่อนเท่านั้น

โปรแกรมป้องกันไวรัสจะทำหน้าที่คอยตรวจสอบและติดตามการบุกรุกของ โปรแกรมอันตรายประเภทไวรัส หนอนอินเตอร์เน็ต และม้าโทรจัน ตลอดจนโปรแกรมประสงค์ร้ายในรูปแบบอื่น ๆ โดยที่จะแจ้งเตือนให้เจ้าของเครื่องทราบได้ว่า ขณะนี้มีโปรแกรมประสงค์ร้ายใดแปลกปลอมเข้ามาและจะให้กำจัดหรือลบทิ้งออกไปเลยหรือไม่

การใช้งานโปรแกรมป้องกันไวรัสที่ถูก ต้อง จำเป็นต้องทำให้ตัวโปรแกรมได้รู้จักไวรัสสายพันธุ์ใหม่ และหาทางกำจัดให้ได้อยู่อย่างสม่ำเสมอ ซึ่งบริษัทผู้ผลิตโปรแกรมมักจะเปิดเว็บไซท์ให้ลูกค้าที่ซื้อโปรแกรมเข้าไปอัพเดทข้อมูล ใหม่ ๆ อยู่เสมอ ซึ่งเป็นกิจกรรมที่จำเป็นอย่างยิ่งสำหรับผู้ใช้คอมพิวเตอร์ทั่ วไป เนื่องจากการแพร่กระจายของไวรัสสายพันธุ์ใหม่เกิดขึ้นแทบทุกวัน หากโปรแกรมป้องกันไวรัสไม่รู้จักตัวไวรัสหรือโปรแกรมประสงค์เหล่านี้ที่จะต้องป้องกันและรักษา ไม่ว่าจะเป็นข้อมูลหรือไฟล์ต่าง ๆ ที่มีความสำคัญก็จะไม่สามารถทำได้ เปรียบเหมือนกับยามรักษาความปลอดภัยหน้าบ้านที่ไม่ได้รักษาความปลอดภัยเต็มที่ ขาดความรอบคอบ รวมถึงไม่รู้จักหน้าตาของสมาชิกในบ้าน และยอมปล่อยให้คนแปลกหน้าเข้ามาทำการปล้นบ้านเอาทรัพย์สินมีค่าออกไปได้ในที่สุด

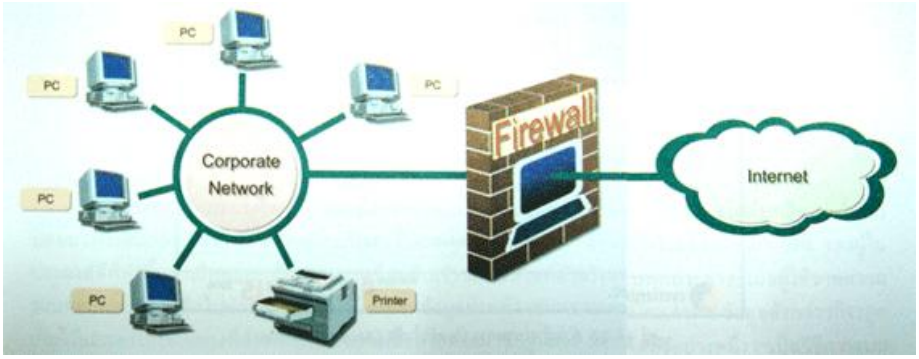
ตัวอย่างโปรแกรมป้องกันไวรัส (Antivirus Program)

โปรแกรมป้องกันไวรัสบางโปรแกรม อาจไม่สามารถลบหรือกำจัดโปรแกรมประเภทสปายแวร์ได้ ผู้ใช้จำเป็นต้องเลือกหาตัวกำจัดโดยเฉพาะ เพื่อไม่ให้โปรแกรมดังกล่าวแฝงหรือติดตั้งอยู่ในเครื่อง

การใช้ระบบไฟร์วอลล์ (Firewall System)

การบุกรุกและถูกโจมตีจากผู้ไม่ประสงค์ดีที่ไม่สามารถทราบว่ามาจากแหล่งใด หรือเวลาใดบ้างที่จะบุกรุกและเจาะระบบเข้ามา อาจป้องกันได้ด้วยการติดตั้งระบบที่เรียกว่า ไฟร์วอลล์ (Firewall) ซึ่งเป็นระบบรักษาความปลอดภัยที่ประกอบด้วยฮาร์ดแวร์หรือซอฟต์แวร์ก็ได้ องค์กรธุรกิจทั่วไปมักจะติดตั้งระบบนี้ไว้เพื่อทำหน้าที่คอยตักจับ ป้องกันและตรวจสอบการบุกรุก (intrusion) รวมถึงการเข้าถึงที่ไม่ได้รับอนุญาตจากผู้ไม่ประสงค์ดีภายนอก

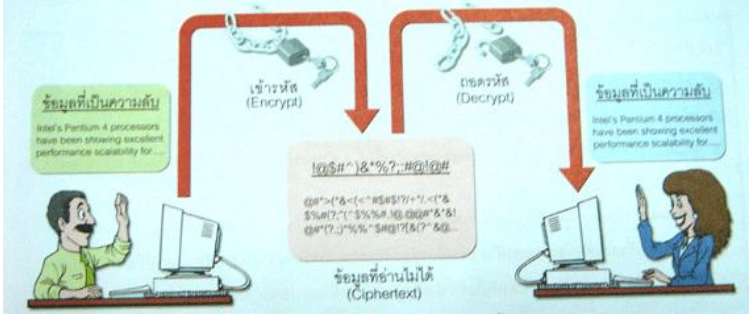
อย่างไรก็ตาม หลังจากมีการติดตั้งระบบดังกล่าวไว้เป็นอย่างดีแล้ว แต่ก็ไม่อาจมั่นใจได้ 100 % ว่าการถูกบุกรุกจากผู้ไม่ประสงค์ดีจากภายนอกจะทำไม่ได้ เลย เพราะระบบไฟร์วอลล์เป็นเสมือนเครื่องมือเพื่อช่วยป้องกันภัยดังกล่าวได้ในระดับหนึ่งเท่านั้น แต่สิ่งที่สำคัญมากที่สุดในการป้องกันได้ดีกว่าก็คือ “คน” นั่นเอง พนักงานซึ่งเป็นคนภายในของบริษัทจึงจำเป็นที่จะต้องปฏิบัติตาม กฎระเบียบหรือเงื่อนไขนโยบายการใช้งานด้านคอมพิวเตอร์ขององค์กรที่วางไว้อย่างเคร่งครัด รวมถึงการช่วยกันตรวจสอบและดูแลข้อมูลที่เข้ามาอย่างผิดปกติก็จะช่วยในการป้องกันการบุกรุกทำได้ดียิ่งขึ้นกว่าเดิม



การเข้ารหัสข้อมูล (Encryption)

เราอาจเคยได้ยินข่าวคราวเกี่ยวกับการลักลอบนำข้อมูลบัตรเครดิตไปใช้ ยับจ่ายซื้อของบนอินเตอร์เน็ต การแอบโอนการรมและแก้ไขเปลี่ยนแปลงข้อมูลรายการค้าเพื่อประโยชน์บางอย่างของผู้ไม่ประสงค์ดี หรือการใช้รหัสผ่านของผู้อื่นเข้าไปทำรายการเสมือนเป็นเจ้าของตัวจริง สิ่งเหล่านี้ล้วนเป็นข้อมูลที่มีความสำคัญทั้งสิ้น และอาจถูกลักลอบไปใช้ได้อยู่เสมอโดยที่บางครั้งก็ไม่สามารถตรวจสอบและจับกุมได้ แนวทางที่จะป้องกันเบื้องต้นที่นิยมทำกันมากคือ อาศัยเทคนิคที่เรียกว่า การเข้ารหัสข้อมูล (encryption)

การเข้ารหัสข้อมูล เป็นการรมวิธีการรักษาความปลอดภัยของข้อมูลโดยอาศัยสมการทางคณิตศาสตร์ที่ซับซ้อนทำการเปลี่ยนแปลง ข้อมูลที่อ่านได้ปกติ (plaintext) ให้ไปอยู่ในรูปแบบของ ข้อมูลที่ไม่สามารถอ่านได้ (ciphertext) กระบวนการดังกล่าวทำให้ข้อมูลมีความปลอดภัยมากยิ่งขึ้น ผู้ไม่ประสงค์ดีที่แอบเอาข้อมูลไปใช้จะไม่สามารถอ่านข้อมูลสำคัญนั้นได้ เพราะมีการรหัส (encryption) ไว้แล้ว ซึ่งในการอ่านข้อมูลนั้นจำเป็นต้องถอดรหัสข้อมูล (decryption) ออกมาก่อนจึงจะนำข้อมูลนั้นไปใช้ประโยชน์ได้ โดยในการถอดรหัสนี้ผู้รับจะต้องมีกุญแจ (หรือ Key) สำหรับไขอ่านข้อมูลที่ได้รับอนุญาตแล้วนั่นเอง



เทคนิคการเข้าและถอดรหัสของข้อมูล

การสำรองข้อมูล (Back Up)

การทำงานของระบบคอมพิวเตอร์ เมื่อใช้ไปในช่วงเวลาหนึ่งอาจเกิดปัญหาในการทำงานได้ ซึ่งอาจเกิดจากหลายสาเหตุ เช่น ถูกโจมตีด้วยไวรัสคอมพิวเตอร์หรือหนอนอินเตอร์เน็ตเข้ามาก่อกวนจนทำให้ข้อมูลที่มีอยู่นั้นเสียหายอย่างร้ายแรง พนักงานขาดการดูแลรักษาความปลอดภัยที่ดีพอ ฮาร์ดดิสก์หรืออุปกรณ์บางอย่างเสียหายสิ่งต่างเหล่านี้ไม่อาจคาดล่วงหน้าได้ว่าจะเกิดเมื่อใด และหากเกิดขึ้นแล้วจะส่งผลร้ายแรงต่อข้อมูลที่มีอยู่ในระบบมากน้อยแค่ไหน วิธีการที่ดีที่สุดเพื่อรับมือกับเหตุการณ์ที่อาจเกิดขึ้นซึ่งจำเป็นต้องอาศัยการสำรองข้ อมูล (back up) ไว้ด้วยทุกครั้ง เพราะข้อมูลเมื่อสูญเสียแล้วโอกาสที่จะกู้คืนกลับมาได้นั้นจะยากเต็มที

ความหมายของการสำรวจข้อมูล คือ การทำสำข้อมูล ไฟล์ หรือโปรแกรมที่เก็บข้อมูลเพื่อให้สามารถนำเอากลับมาใช้อีกได้ วิธีการสำรองข้อมูลอาจสำรองทั้งระบบหรือแค่บางส่ วนเท่านั้นก็ได้ ซึ่งสามารถเลือกใช้โปรแกรมยูทิลิตี้บางประเภทเพื่อเก็บลงสื่อบันทึกข้อมูลสำรอง เช่น ฮาร์ดดิสก์หรือ CD-COM ทั้งนี้ขึ้นอยู่กับว่าข้อมูลมีความสำคัญหรือถูกแก้ไขเปลี่ยนแปลงมากน้อยเพียงใด และต้องการระยะเวลาในการสำรองข้อมูลบ่อยมากน้อยแค่ไหน ซึ่งโดยปกติหากข้อมูลมีความสำคัญมากหรือเปลี่ยนแปลงตลอดเวลาก็อาจจำเป็นต้องสำรองข้อมูลทุกวัน หรือทุกสัปดาห์ แต่หากข้อมูลนั้นมีความสำคัญน้อยอาจสำรองเพียงแค่ทุกเดือนก็พอ

สภาพแวดล้อมและแนวโน้มของเทคโนโลยีสารสนเทศในอนาคต

พัฒนาการของเทคโนโลยีสารสนเทศ

หากกล่าวถึงคำว่า “เทคโนโลยีสารสนเทศ ” แล้ว จะมีความหมายครอบคลุมกว้างกว่าคำว่า “ระบบคอมพิวเตอร์” เพราะจะพูดรวมถึงระบบการเชื่อมโยงสารสนเทศด้วยเครื่องมือสื่อสารและโทรคมนาคมเข้าไปด้วย ซึ่งแทบจะเรียกได้ว่า มีแนวโน้มของการพัฒนาที่ไม่หยุดยั้ง ช่วยให้การติดต่อและแลกเปลี่ยนสารสนเท ศทำได้อย่างไร้ขีดจำกัดของพรมแดน มีการเชื่อมโยงกันอย่างทั่วถึงมากยิ่งขึ้น ระบบคอมพิวเตอร์ซึ่งเป็นส่วนหนึ่งของเทคโนโลยีสารสนเทศ ก็มีแนวโน้มในการพัฒนาให้สอดคล้องกับเทคโนโลยีสื่อสารที่เปลี่ยนไปด้วย โดยมีการออกแบบและพัฒนาอุปกรณ์คอมพิวเตอร์ให้มีขนาดเล็กและมีประสิทธิภาพในการประมวลผลมากยิ่งขึ้น

ในเอกสารการวิจัยของสำนักงานคณะกรรมการการศึกษาแห่งชาติ ได้กล่าวถึงคุณสมบัติของเทคโนโลยีสารสนเทศ ที่ทำให้เกิดการแพร่กระจายของการใช้อุปกรณ์เทคโนโลยีสารสนเทศอย่างแพร่หลายในปัจจุบัน ซึ่งประกอบด้วยคุณสมบัติต่าง ๆ ดังนี้

- การรวม ตัวกันของเทคโนโลยี (Convergence) เทคโนโลยีสารสนเทศ เป็นการรวมตัวกันของเทคโนโลยีทางด้านคอมพิวเตอร์ การสื่อสาร รวมถึงระบบเทคโนโลยีอื่น ๆ เช่น การกระจายเสียง (broadcasting) เข้าไว้ด้วยกัน ทำให้สามารถรับและส่งสัญญาณ โดยเฉพาะข้อมูลที่อยู่ในรูปของสื่อแบบผสม (multimedia) ที่ประกอบด้วยภาพ เสียง และข้อความต่าง ๆ ได้อย่างรวดเร็ว สมบูรณ์และสามารถส่งได้ในปริมาณมาก การเผยแพร่ข้อมูลต่าง ๆ ทำได้อย่างทั่วถึงกันมากขึ้น โดยเฉพาะการเผยแพร่ข้อมูลในยุคไร้พรมแดน
- ต้นทุนที่ถูกลง (Cost reduction) เทคโนโลยีสารสนเทศมีคุณสมบัติที่ทำ ให้ราคา และการเป็นเจ้าของอุปกรณ์เทคโนโลยีสารสนเทศถูกลงเป็นอย่างมาก ทั้งในส่วนของอัตราค่าบริการสื่อสารโทรคมนาคม เช่น ค่าโทรศัพท์ ค่าบริการอินเทอร์เน็ต ค่าเช่าสัญญาณเคเบิ้ลข่าย รวมถึงราคาของเครื่องคอมพิวเตอร์ที่มีแนวโน้มถูกลงเรื่อย ๆ สิ่งต่าง ๆ เหล่านี้ดำเ นินการเป็นไปตามกลไกราคาของตลาดนั่นเอง ซึ่งเมื่อมีผู้บริโภคมากขึ้นราคาก็ย่อมมีแนวโน้มที่จะถูกลง
- การพัฒนาอุปกรณ์ที่เล็กลง (Miniaturization) อุปกรณ์เทคโนโลยีสารสนเทศหลากหลายประเภท รวมทั้งเครื่องคอมพิวเตอร์และโทรศัพท์ได้รับการพัฒนาให้มีขนาดเล็กลงกว่าเดิมมาก ด้วยวิวัฒนาการของไมโครชิพทำให้สะดวกต่อการใช้งานมากยิ่งขึ้น
- การพกพาและการเคลื่อนที่ (Portability / Mobility) เทคโนโลยีสารสนเทศทำให้การต่อเชื่อมเครือข่ายคอมพิวเตอร์เป็นไปได้ง่ายมากยิ่งขึ้น อาทิเช่น คอมพิวเตอร์แบบโน๊ตบุ๊คที่มีโมเด็มและโทรศัพท์ใช้สายในระบบดิจิตอล สามารถต่อเข้ากับเครือข่ายอินเทอร์เน็ตนอกสถานที่ทำงานได้อย่างง่ายดาย

- การประมวลผลที่ดีขึ้น (Processing Power) เทคโนโลยีสารสนเทศมีแนวโน้มของการประมวลผลที่ดีขึ้นโดยอาศัยพัฒนาการของผู้ผลิตหน่วยประมวลผลกลาง หรือซีพียูที่ทำงานเร็วขึ้นกว่าเดิม รวมถึงการสร้างโปรแกรมเพื่อตอบสนองการทำงานของผู้ใช้ ที่มีประสิทธิภาพดียิ่งขึ้น
- การใช้งานที่ง่าย (User Friendliness) การพัฒนาโปรแกรมในปัจจุบัน มีการออกแบบส่วนประสานงานกับผู้ใช้เพื่อช่วยเหลือและสนับสนุนการทำงานให้ง่ายและดียิ่งขึ้น โดยเฉพาะอย่างยิ่งกับคนที่ไม่คุ้นเคยเรื่องเทคโนโลยีมากนัก หรือที่เรียกว่า User-friendly นั่นเอง ทำให้ไม่ต้องกลัวว่าจะใช้งานได้ยากเหมือนกับแต่ก่อน เพียงแค่ศึกษาการใช้โปรแกรมเพียงเล็กน้อยก็สามารถทำได้แล้วโดยมากจะมีการนำรูปแบบของ GUI มาใช้มากยิ่งขึ้น เช่น แบบเมนูเลือกรายการ หรือกดคลิกผ่านเมาส์บนหน้าจอ เป็นต้น ซึ่งช่วยให้การแพร่กระจายของการใช้เทคโนโลยีสารสนเทศเป็นไปได้อย่างรวดเร็วมากยิ่งขึ้น
- การเปลี่ยนจากอะตอมเป็นบิต (Bits versus Atoms) ทิศทางของความนิยมและการกระจายของการใช้เทคโนโลยีสารสนเทศอย่างรวดเร็ว ผ่านการใช้งานโดยเครือข่ายอินเทอร์เน็ตนี้ นับได้ว่าเป็นตัวอย่างที่ชัดเจนของการหักเหจากกิจกรรมที่ใช้ "อะตอม" เช่น การส่งเอกสารที่เป็นกระดาษ ไปสู่การใช้ "บิต" (binary digit : BIT) มากยิ่งขึ้น ซึ่งในปัจจุบันจะเห็นว่าหลายองค์กรปรับเปลี่ยนการใช้งานที่มุ่งเน้นสู่สำนักงานแบบไร้กระดาษ (paperless office) กันบ้างแล้ว
- เวลาและภูมิศาสตร์ (Time & Distance) วิวัฒนาการของเทคโนโลยีสารสนเทศทำให้มนุษย์สามารถเอาชนะเงื่อนไขด้าน "เวลา" และ "ภูมิศาสตร์" ได้เป็นอย่างมาก เช่น การประชุมทางไกล (teleconference) สำหรับบางองค์กรที่มีขนาดใหญ่และมีสาขาอยู่ทั่วประเทศ ซึ่งหากต้องจัดการประชุมโดยให้ผู้บริหารทุกสาขาเดินทางมายังสำนักงานใหญ่พร้อมกัน อาจจะทำได้ไม่สะดวกหรือจัดเวลาไม่ตรงกัน การประชุมแบบทางไกลสามารถเข้ามาช่วยแก้ปัญหานี้ได้ หรือการใช้จานรับสัญญาณดาวเทียมเพื่อถ่ายทอดสัญญาณรายการเพื่อการศึกษาให้กับโรงเรียนชนบทที่ห่างไกล (tele-education) โดยที่นักเรียนไม่จำเป็นต้องเข้ามาแสวงหาความรู้ในเมืองใหญ่ ก็สามารถได้แหล่งความรู้ที่เหมือน ๆ กัน เป็นการลดปัญหาในเรื่องภูมิศาสตร์ลงไปได้ด้วยเช่นกัน

เทคโนโลยีสารสนเทศน่ารู้

เทคโนโลยีที่ใช้กันอยู่ในปัจจุบันปรับเปลี่ยนและเติบโตอย่างรวดเร็วมาก เครือข่ายการสื่อสารต่าง ๆ มีการพัฒนาให้เชื่อมต่อที่เร็วขึ้น การปฏิสัมพันธ์ระหว่างผู้ใช้และระบบทำได้ง่ายกว่าเดิมมาก ดังจะเห็นได้จากการนำเอาประโยชน์ของเทคโนโลยีต่าง ๆ เหล่านั้นมาใช้กันอย่างมากมาย ทั้งในเรื่องของธุรกิจ และการใช้ชีวิตประจำวันซึ่งอาจยกตัวอย่างได้ดังนี้

- SMS (Short Message Service) เทคโนโลยีบริการเสริมที่มีในระบบโทรศัพท์มือถือ (และโทรศัพท์บ้านของผู้ให้บริการบางราย) ได้รับความนิยมอย่างมาก จัดอยู่ในบริการที่เรียกว่า non voice โดยอนุญาตให้ผู้ใช้ส่งข้อความเข้าไปหาสมาชิกในเครือข่ายได้ ผู้ให้บริการอาจคิดค่าธรรมเนียมการใช้งานแตกต่างกันไป ในการส่งข้อความแต่ละครั้ง นอกจากนั้นยังมีการประยุกต์เอาไปใช้ในเชิงธุรกิจด้วย เช่น การโหวต หรือร่วมแสดงความคิดเห็นในรายการโทรทัศน์ การตอบคำถามผ่านคอลัมน์ในนิตยสาร การตอบปัญหาชิงรางวัล เป็นต้น
- MMS (Multimedia Massage Service) เป็นบริการเสริมที่คล้ายกับ SMS หากแต่สามารถจัดส่งข้อมูลที่เป็นแบบสื่อผสม หรือ multimedia ได้ดีกว่า เช่น การส่งภาพถ่าย ภาพเคลื่อนไหว หรือเสียงเพลง เป็นต้น ผู้ให้บริการในระบบโทรศัพท์มือถือบางค่ายมักจะมีระบบเสริมเช่นนี้รองรับไว้แล้ว ทั้งนี้อัตราค่าใช้บริการก็อาจแตกต่างกันด้วย

บทบาทของภาครัฐที่มีต่อเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Policy)

นโยบายเทคโนโลยีสารสนเทศของประเทศไทย

ในปี พ.ศ. 2535 รัฐบาลได้จัดตั้งคณะกรรมการการเทคโนโลยีสารสนเทศแห่งชาติ หรือ กทสช . (National Information Technology Committee : NITC) ขึ้น ด้วยเล็งเห็นว่าสังคมต้องมีการเตรียมการเพื่อรองรับการพัฒนาเศรษฐกิจและสังคมในยุคข่าวสารข้อมูล จึงมีการตั้งหน่วยงานเพื่อรองรับงานทางด้านนโยบายขึ้น โดยมอบหมายให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ หรือเนคเทคทำหน้าที่เป็นสำนักงานเลขานุการ เพื่อกลั่นกรองนโยบายและมาตรการที่จะมีผลต่อการพัฒนาเทคโนโลยีสารสนเทศให้เอื้ออำนวยต่อการพัฒนาประเทศ

หน้าที่หลักของคณะกรรมการฯดังกล่าว จะต้องมีการเสนอแนะนโยบายและแผนพัฒนา เทคโนโลยีสารสนเทศต่อคณะรัฐมนตรี ทั้งในเรื่องของการพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศ การสร้างบรรยากาศให้มีการนำเทคโนโลยีสารสนเทศเข้ามาใช้ในการดำเนินงานต่าง ๆ การพัฒนาโครงสร้างพื้นฐานด้านโทรคมนาคม การปรับปรุง กฎหมาย จะเบียบข้อบังคับให้สอดคล้องกับการดำเนินธุรกิจสมัยใหม่ โดยสื่ออิเล็กทรอนิกส์ การส่งเสริมการผลิต การบริการ การวิจัย และการพัฒนาให้มีเทคโนโลยีด้านสารสนเทศขึ้นในประเทศไทย นอกจากนี้ยังมีหน้าที่ที่สำคัญอีกประการหนึ่ง คือ เสนอมาตรการแก้ไขปัญหาและอุปสรรคที่เกิดขึ้นในการพัฒนาเทคโนโลยีสารสนเทศของประเทศต่อคณะรัฐมนตรี

นโยบายเทคโนโลยีสารสนเทศแห่งชาติฉบับแรก หรือ IT 2000 ได้มีการประกาศใช้เมื่อปี พ.ศ. 2539 โดยมีสาระสำคัญที่เป็นเสาหลักในการพัฒนา 3 ประการ คือ

- พัฒนาโครงสร้างพื้นฐานสารสนเทศแห่งชาติ (National Information Infrastructure)
- พัฒนาทรัพยากรมนุษย์ (Human Resource Development)
- พัฒนาระบบสารสนเทศและปรับปรุงบทบาทภาครัฐเพื่อบริการที่ดีขึ้น รวมทั้งการสร้างฐานของอุตสาหกรรมสารสนเทศที่แข็งแกร่ง (IT for good governance)

อย่างไรก็ตาม เมื่อการเปลี่ยนแปลงของสังคมในระดับนานาประเทศเป็นไปอย่างรวดเร็ว อีกทั้งยังมุ่งเน้นการพัฒนาประเทศ ไปสู่เศรษฐกิจและสังคมแห่งภูมิปัญญาและการเรียนรู้ (Knowledge-based Economy / Society : KBE/KBS) คณะกรรมการฯ ได้ตระหนักถึงความสำคัญที่จะต้องมีนโยบายเทคโนโลยีสารสนเทศที่สอดรับกับการเปลี่ยนแปลงทั้งในและต่างประเทศดังกล่าว จึงได้จัดทำกรอบนโยบายเทคโนโลยีสารสนเทศของประเทศไทยในระยะที่สอง หรือ IT 2010 ขึ้น ซึ่งครอบคลุมเป็นเวลา 10 ปี (พ.ศ.2544-2553) โดยให้ความสำคัญกับบทบาทของเทคโนโลยีสารสนเทศในฐานะเป็นเครื่องมือขับเคลื่อนการพัฒนาประเทศ ทั้งด้านเศรษฐกิจและสังคม ซึ่งจะเน้นการประยุกต์ใช้ในสาขาหลักที่เป็นเป้าหมายของการพัฒนา โดยคำนึงถึงความสมดุลระหว่างภาคเศรษฐกิจและภาคสังคม ซึ่งกรอบ นโยบายดังกล่าว (IT 2010) ได้รับความเห็นชอบจากคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติในวันที่ 3 ตุลาคม พ.ศ.2544 และจากคณะรัฐมนตรีในวันที่ 19 มีนาคม พ.ศ.2545

กรอบนโยบายเทคโนโลยีสารสนเทศของประเทศไทยระยะที่สอง หรือ IT 2010 นี้ ตั้งอยู่บนพื้นฐานของการสร้างสังคม แห่งภูมิปัญญาและการเรียนรู้ของประเทศไทย ที่จะครอบคลุมช่วงเวลาถึง 10 ปี ทั้งนี้เพื่อให้เศรษฐกิจมีความเข้มแข็งและยั่งยืน สามารถแข่งขันได้ในเวทีสากล ในขณะเดียวกันเพื่อให้ประชาชนในสังคมมีคุณภาพชีวิตที่ดี มีความเหลื่อมล้ำน้อยที่สุด ซึ่งมีองค์ประกอบที่สำคัญ 3 ประการ คือ

- ลงทุนในการเสริมสร้างทรัพยากรมนุษย์ที่มีความรู้เป็นพื้นฐานสำคัญ (Build Human Capital)
- ส่งเสริมให้มีนวัตกรรมในระบบเศรษฐกิจและสังคม (Promote Innovation)
- ลงทุนในโครงสร้างพื้นฐานสารสนเทศและส่งเสริมอุตสาหกรรมสารสนเทศ (Strengthen Information Infrastructure & Industry)

สรุปท้ายบท

จริยธรรมเป็นแบบแผนความประพฤติหรือความมีสามัญสำนึกต่อสังคมในทางที่ดี เมื่อกล่าวถึงจริยธรรมที่เกี่ยวข้องกับสังคมยุคสารสนเทศ จะเกี่ยวข้องกับกรอบแนวคิดที่ตั้งอยู่บนพื้นฐาน 4 ประการคือ ความเป็นส่วนตัว ความถูกต้องแม่นยำ ความเป็นเจ้าของ และการเข้าถึงข้อมูล

อาชญากรรมคอมพิวเตอร์เป็นอีกการณีหนึ่งที่พบเห็นได้ โดยนอกจากจะเป็นการกระทำที่ “ขาดจริยธรรม” แล้ว ยังถือว่าผิดกฎหมายด้วย การก่ออาชญากรรมทางคอมพิวเตอร์มีหลายรูปแบบ เช่น การลักลอบเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การขโมยและทำลายอุปกรณ์ การขโมยโปรแกรมคอมพิวเตอร์ การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย เป็นต้น วิธีป้องกันและรักษาความปลอดภัยระบบคอมพิวเตอร์อาจทำหลายแบบ เช่น การติดตั้งโปรแกรมป้องกันไวรัส การใช้ระบบไฟร์วอลล์ การเข้ารหัสข้อมูล และการสำรองข้อมูล

เทคโนโลยีสารสนเทศสามารถนำไปประยุกต์ใช้ในการพัฒนาประเทศได้หลายด้าน เช่น เศรษฐกิจ สังคม การศึกษา สาธารณสุข สิ่งแวดล้อม ฯลฯ สำหรับประเทศไทยเองได้เล็งเห็นถึงความสำคัญ โดยได้วางกรอบนโยบายเทคโนโลยีสารสนเทศ หรือ IT 2010 ขึ้นโดยตั้งอยู่บนพื้นฐานของ “การสร้างสังคมแห่งภูมิปัญญาและการเรียนรู้”