บทที่ 1 วัตถุประสงค์และบทบาทหน้าที่ของลูกเสือไซเบอร์

1. ความหมายของลูกเสือโลก ลูกเสือไทยและลูกเสือไซเบอร์

1.1 ความหมายของลูกเสือโลก

ลอร์ด เบเดน โพเอลล์ ได้แต่งหนังสือคู่มือการฝึกอบรมลูกเสือขึ้นมาเล่มหนึ่ง มีชื่อว่า Scouting For Boys ซึ่งระบุว่า “ลูกเสือ” มาจากคำว่า “SCOUT” ซึ่งมีความหมายดังนี้ [1]

S	:	Sincerity	หมายถึง	ความจริงใจ มีน้ำใสใจจริงต่อกัน
C	:	Courtesy	หมายถึง	ความสุภาพอ่อนโยน เป็นผู้มีมารยาทดี
O	:	Obedience	หมายถึง	การเชื่อฟัง อ่อนน้อมถ่อมตน อยู่ในโอวาท
U	:	Unity	หมายถึง	ความเป็นน้ำหนึ่งใจเดียวกัน รู้รักสามัคคี
T	:	Thrifty	หมายถึง	ความมัธยัสถ์ ใช้ทรัพยากรอย่างประหยัด

1.2 ความหมายของลูกเสือไทย

พระราชบัญญัติลูกเสือ พ.ศ. 2551 ระบุว่า “ลูกเสือ” หมายความว่า เด็กและเยาวชนทั้งชายและหญิงที่สมัครเข้าเป็นลูกเสือทั้งในสถานศึกษาและนอกสถานศึกษา ส่วนลูกเสือที่เป็นหญิงให้เรียกว่า “เนตรนารี”[2]

1.3 ความหมายของลูกเสือไซเบอร์

“ลูกเสือไซเบอร์” หมายความว่า ลูกเสือและบุคลากรทางการลูกเสือตามกฎหมายลูกเสือและบุคคลทั่วไปที่สมัครและผ่านการฝึกอบรมหลักสูตรลูกเสือไซเบอร์ ตามที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกำหนด [3]

2. ประวัติ ภูมิหลังและกิจการลูกเสือโลก ลูกเสือไทยและลูกเสือไซเบอร์

2.1 ประวัติ ภูมิหลังและกิจการลูกเสือโลก

บี-พี เกิดที่บ้านเลขที่ 6 ถนนแสตนโฮป แพดดิงตั้น ลอนดอน มีชื่อเต็มว่า โรเบิร์ต สตีเฟนสัน สมิทธ์ เบเดน-โพเอลล์ บิดาชื่อ สาธุคุณ เอ็ช.จี เบเดน-โพเอลล์ เป็นศาสตราจารย์ทางวิทยาศาสตร์มีชื่อเสียงของมหาวิทยาลัยอ๊อกซฟอร์ด เสียชีวิตในปีพ.ศ. 2430 (ค.ศ. 1860) มารดาของบี-พีเป็นภรรยาคนที่ 3 ชื่อเดิม คือ นางสาวเฮนเรียตต้า เกรซ สมิทธ์ เมื่อบิดาบี-พีเสียชีวิตในปี พ.ศ. 2403 (ค.ศ. 1860) เธอต้องเลี้ยงลูกทั้ง 7 คน ด้วยตนเอง ทั้งที่ฐานะทางการเงินไม่ค่อยดีนัก มารดาของบี-พีเปลี่ยนนามสกุลเป็น เบเดน-โพเอลล์ ในปี พ.ศ. 2412

บี-พี ได้รับทุนการศึกษาเข้าศึกษาที่โรงเรียนชาร์ตเตอร์เฮ้าส์ ซึ่งเป็นโรงเรียนประจำของเอกชนในกรุงลอนดอน เรียนอยู่ที่นี่ได้ 2 ปี โรงเรียนก็ย้ายลงไปอยู่ที่เมืองโกดาลมิ่ง เซอร์เร่ย์ ทางตอนใต้ของลอนดอน เป็นเมืองชนบทที่เงียบสงบถูกกับนิสัยของบี-พีเป็นอย่างยิ่ง คือ ได้ใช้ชีวิตแบบเป็นลูกเสือคนหนึ่ง ได้ศึกษาหาความรู้เกี่ยวกับสัตว์ ต้นไม้ ได้เล่นเรือ พักแรมในเต็นท์ และได้สร้างสรรค์สิ่งต่างๆ จากวัสดุที่มีอยู่ในธรรมชาติ

บี-พี สามารถสอบเข้าเป็นทหารบกในเหล่าทหารม้า ได้ที่ 2 และได้ที่ 4 ในเหล่าทหารราบนับเป็นความสำเร็จของบี-พีที่เกินจากความคาดหมาย เพราะตามปกติบี-พี เรียนหนังสือไม่ค่อยเก่ง และในสมัยนั้นการสอบเข้าเป็นทหารมีการแข่งขันค่อนข้างสูงจากลูกผู้ดีมีเงินทั้งหลาย

บี-พี เลือกเป็นทหารม้า ได้รับการบรรจุเป็นนายทหารสัญญาบัตรยศ “ร้อยตรี” ในกรมทหารอุสซ่าร์ที่ 13 ซึ่งขณะนั้นประจำอยู่ที่เมืองลัคเนา ประเทศอินเดีย บี-พีออกเดินทางไปอินเดีย เมื่อวันที่ 30 ตุลาคม พ.ศ. 2419 และในปีพ.ศ. 2421 บี-พีได้เลื่อนยศเป็น “ร้อยโท” นายร้อยโทบี-พีได้รับคำสั่งให้ประจำกรมทหารในอาฟกานิสถาน ซึ่งปฏิบัติราชการสงครามกับชนเผ่าพื้นเมืองอาฟกานิสถานอยู่ กรมทหารนี้มีนายพันเอกเบเกอร์ รัชเซลล์เป็นผู้บังคับบัญชา นายพันเอกท่านนี้มีแนวทางการฝึกทหารแนวเดียวกันกับท่านบี-พี คือ ไม่เคร่งครัดกับเรื่องระเบียบวินัยมากนัก แต่มุ่งเน้นที่จะให้ทหารมีความคิดริเริ่มและมีความมั่นใจในตนเอง

บี-พี รับหน้าที่เป็นผู้สอดแนมหาข่าวให้กับหน่วย ซึ่งท่านสามารถปฏิบัติงานได้ประสบผลสำเร็จอย่างดียิ่ง เมื่อสงครามสงบ ท่านย้ายกลับมาประจำกรมทหารอุสซ่าร์ที่ 13 อีกครั้งหนึ่งที่อินเดีย และช่วงนี้ท่านได้รู้จักกับมิสเตอร์ เดอร์บัวส์ แมคคลาเรน และในปีพ.ศ. 2427 (ค.ศ. 1884) บี-พีได้เลื่อนยศเป็น “ร้อยเอก” ท่านพิมพ์หนังสือเล่มแรกของท่าน คือ คู่มือการหาข่าวและการสอดแนม (Reconnaissance and Scouting)

รูปที่ 1-1 บี-พีใส่หมวกทรงสูง

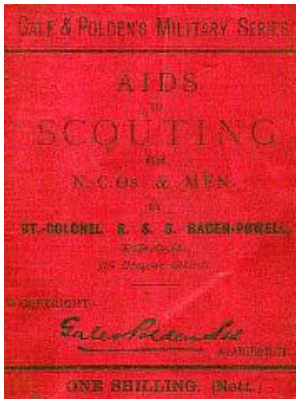
ท่านเริ่มใช้หมวกปีกกว้างในช่วงปี พ.ศ. 2427 (ค.ศ. 1884) และได้กลายเป็นสัญลักษณ์ส่วนตัว ของท่านและกลายเป็นหมวกลูกเสือ ต่อมา ท่านได้รับคำสั่งให้ไปเป็นนายทหารคนสนิทของลุงของท่าน คือ พลเอก เซอร์ เฮนรี สมิทธิ์ ซึ่งดำรงตำแหน่งเป็นผู้ว่าการอาณานิคมแหลมอาฟริกา พ.ศ. 2430 (ค.ศ. 1887)

ในปี พ.ศ. 2431 (ค.ศ. 1888) เกิดสงครามกับชนเผ่าซูลู ซึ่งมีดินูซูลูเป็นหัวหน้า บี-พีทำหน้าที่เป็นนายทหารการข่าวของกองกำลังที่ยกไปปราบกบฏซูลู ด้วยความสามารถด้านการสอดแนมหาข่าวของท่าน ทำให้ทหารอังกฤษรบชนะเผ่าซูลูได้โดยไม่ยากนัก บี-พีประทับใจในความมีระเบียบวินัยและความรู้ความสามารถของนักรบเผ่าซูลูมาก ท่านได้นำเอาธรรมเนียมประเพณี และเพลงปลุกใจของซูลูมาใช้ในกิจการลูกเสือ และเมื่อเสร็จสงคราม บี-พีได้เลื่อนยศเป็น “พันตรี”

บี-พี ได้รับคำสั่งให้ดำรงตำแหน่งเลขานุการฝ่ายการทหารของลุงของท่าน เซอร์ เฮนรี สมิทธ์ในปีพ.ศ. 2433 (ค.ศ. 1890) ซึ่งได้ย้ายไปเป็นผู้ว่าราชการเกาะมอลต้า (Governer of Malta) และในปีต่อมาก็ได้เลื่อนตำแหน่งเป็นนายทหารการข่าวประจำภาคพื้นเมดิเตอร์เรเนียน และท่านได้ปฏิบัติงานด้านการข่าวอีกหลายๆ พื้นที่ในยุโรปอีกด้วย

กรมทหารที่บี-พีสังกัดอยู่ได้รับคำสั่งให้ไปปราบกบฏเผ่าอาซานติ ในปี พ.ศ. 2438 (ค.ศ. 1895) ซึ่งมีกษัตริย์ชื่อ เปรมเป่ห์ หน้าที่ของบี-พี คือ คุมกองกำลังชาวพื้นเมืองสร้างทางจากฝั่งทะเล เพื่อเข้าไปที่เมืองที่มั่นของเผ่าอาซานติ คือ เมืองคุมแมสซี่ งานสร้างทางนี้ยากลำบากมาก ต้องถางป่า สร้างสะพานข้ามน้ำหลายแห่ง ต้องใช้ความเป็นผู้นำและความคิดริเริ่มในการแก้ปัญหาตลอดเวลา ซึ่งถูกกับนิสัยท่านอยู่แล้ว บี-พี ได้รับตำแหน่งเป็นเสนาธิการกองกำลังปราบกบฏมาทาเบลเล่ ในปี พ.ศ. 2440 (ค.ศ.1897) ด้วยความสามารถด้านการข่าวและการสอดแนม ทำให้กองกำลังทหารอังกฤษได้รับชัยชนะอย่างงดงาม

จากผลงานที่แล้วมาและผลงานในการรบครั้งนี้ บี-พีได้รับการยกย่องว่าเป็นผู้สอดแนมที่ยิ่งใหญ่ที่สุดในกองทัพบกอังกฤษ ได้รับเลื่อนยศเป็น “พันเอก” และเลื่อนตำแหน่งเป็น ผู้บัญชาการกรมแครกกูนการ์ดที่ 5 บี-พีรับผิดชอบการฝึกทหารในกรมของท่านโดยตรง ท่านจึงได้นำเอาวิธีการฝึกที่ท่านเคยได้ทดลองฝึกมาใช้ฝึกทหารของท่านมาก่อน คือ ท่านเชื่อว่าการเคร่งครัดกับการฝึกแถว ฝึกระเบียบวินัยเพียงอย่างเดียวไม่สามารถทำให้ทหารมีความคิดริเริ่ม มีความเชื่อมั่นในตนเองได้ ท่านเชื่อว่าหากทหารมีความสนุกสนานกับการฝึกแล้วจะได้ผลมากกว่า ท่านจึงแบ่งทหารออกเป็นกลุ่มเล็กๆ ฝึกวิชาการหาข่าวและสอดแนมตามที่ท่านมีประสบการณ์มาจากการรบ ผู้ใดผ่านการทดสอบก็จะได้ชื่อว่าเป็น ผู้สอดแนม (Scout) และจะได้รับเครื่องหมายเป็นรูปดอกลิลลี่ ซึ่งปกติใช้เป็นเครื่องแสดงทิศเหนือในแผนที่หรือในเข็มทิศ บี-พีได้บันทึกวิธีการฝึกทหารตามวิธีการของท่านนี้ไว้ในหนังสือ “คู่มือการสอดแนม” (Aids to Scouting) ซึ่งได้รับความนิยมจากเด็กและเยาวชนเป็นอย่างสูงในเวลาต่อมา และกลายมาเป็นต้นแบบของการฝึกอบรมลูกเสือของท่านนั้นเอง



รูปที่ 1-2 หนังสือคู่มือการสอดแนม

เดือนกรกฎาคม พ.ศ. 2442 บี-พีได้รับคำสั่งให้เดินทางไปประจำหน่วยทหารที่อาฟริกาใต้ เพราะขณะนั้นกองทัพอังกฤษกำลังเตรียมกำลังเพื่อทำสงครามกับพวกบัวร์ (Boer) ซึ่งเป็นชาวฮอลันดาที่อพยพไปตั้งถิ่นฐานอยู่ในอาฟริกาใต้ สงครามครั้งนี้รู้จักกันในนามว่า สงครามบัวร์ (Boer War) และสงครามนี้เองที่ทำให้บี-พี กลายเป็นวีรบุรุษระดับชาติ ชื่อของบี-พีเป็นที่รู้จักของคนอังกฤษทั่วๆ ไป รวมทั้งควีนวิคตอเรีย พระราชินีของอังกฤษขณะนั้น

สงครามบัวร์เกิดขึ้นระหว่างปี พ.ศ. 2442 – 2445 (ค.ศ. 1899 – 1902) เมื่อบี-พีเดินทางมาถึงอาฟริกาใต้ ท่านก็ได้รับคำสั่งให้ไปรักษาการเมืองมาฟเฟ็กกิ่ง (Mafeking) ซึ่งเป็นเมืองชายทะเลเล็กๆ อยู่ด้านมหาสมุทรแอตแลนติก แต่เมืองนี้เป็นศูนย์กลางทางการค้าและเป็นฐานส่งกำลังบำรุงขนาดใหญ่ของกองทัพอังกฤษในแถบนั้น ดังนั้นเมืองนี้จึงมีความสำคัญทางยุทธศาสตร์พอสมควร บี-พีจัดการป้องกันเมืองมาฟเฟ็กกิ่งอย่างเร่งรีบ ย้ายผู้หญิงและเด็กออกจากเมืองไปที่ๆ ปลอดภัย การเตรียมการยังไม่เรียบร้อยดี ทหารบัวร์

ประมาณ 9,000 คนก็เข้าล้อมเมืองมาฟเฟ็กกิ่งเอาไว้ เมื่อ 13 ตุลาคม พ.ศ. 2442 ในขณะที่บี-พีมีทหารป้องกันเมืองเพียง 1,250 คน และยังเป็นทหารที่มีอาวุธที่ค่อนข้างล้าสมัย และภายในเมืองยังมีประชาชนเหลืออยู่ประมาณ 9,000 คนด้วย เนื่องจากกำลังน้อยกว่าข้าศึกมาก บี-พีต้องใช้กลอุบายหลอกล่อข้าศึกด้วยวิธีการต่าง ๆ เพื่อให้ข้าศึกเข้าใจผิดว่าในเมืองมีทหารป้องกันอยู่จำนวนมาก เช่น การทำลวดหนามปลอมรอบๆ เมือง วางทุ่นระเบิดปลอม กลางคืนก็ให้คนถือไฟฉายที่มีอยู่เพียงดวงเดียววิ่งไปรอบๆ เมือง เพื่อให้พวกทหารบัวร์เข้าใจผิด ไม่กล้าโจมตีตอนกลางคืน บี-พีออกหาข่าวข้าศึกด้วยตนเอง จึงรู้ความเคลื่อนไหวของข้าศึกตลอดเวลา และท่านได้จัดการฝึกเด็กหนุ่มในเมืองให้ทำหน้าที่ต่างๆ เช่น ส่งหนังสือ ส่งไปรษณีย์ เป็นต้น โดยจัดให้เด็กหนุ่มเหล่านี้แต่งเครื่องแบบ มีผู้นำของตนเอง ตั้งชื่อเด็กกลุ่มนี้ว่า “กองนักเรียนทหารแห่งมาฟเฟ็กกิ่ง” เด็กเหล่านี้เอาจริงเอาจังกับหน้าที่ของเขามาก มีความกล้าหาญ ไม่กลัวตาย ความสำเร็จในครั้งนี้เป็นแรงบันดาลใจให้บี-พีจัดตั้งกองลูกเสือในโอกาสต่อมา

สำหรับประชาชนมาฟเฟ็กกิ่ง บี-พีก็ดูแลเป็นอย่างดี จัดให้มีการรวมตัวทำกิจกรรมต่างๆ เพื่อสร้างขวัญและกำลังใจ จัดให้มีการปันส่วนอาหาร เพื่อให้ทุกคนมีอาหารรับประทานอย่างทั่วถึงตลอดเวลาที่ถูกปิดล้อม บี-พีสามารถรักษาเมืองจากการปิดล้อมและโจมตีของพวกบัวร์ได้นานถึง 217 วัน จนกระทั่งกองกำลังทหารอังกฤษส่งมาช่วยเมื่อ 17 พฤษภาคม พ.ศ. 2443 ข่าวคราวการปิดล้อมเมืองมาฟเฟ็กกิ่งและความสามารถในการป้องกัน ความเป็นผู้นำของบี-พีเป็นที่สนใจของชาวอังกฤษโดยทั่วไป แม้แต่ควีนวิคตอเรีย ยังส่งพระราชสาส์นมาให้กำลังใจกับบี-พี เมื่อกองกำลังอังกฤษโจมตีพวกทหารบัวร์ที่ปิดล้อมเมืองอยู่ เมื่อ 17 พฤษภาคม พ.ศ. 2443 นั้น และข่าวนี้ไปถึงอังกฤษ ประชาชนอังกฤษมีการฉลองชัยชนะกันโดยทั่วไป รูปบี-พี ปรากฏอยู่ในหนังสือพิมพ์ทุกฉบับ บี-พีกลายเป็นวีรบุรุษอย่างเต็มภาคภูมิ ด้วยผลงานครั้งนี้ บี-พีจึงได้รับโปรดเกล้าฯ เป็น “พลตรี” ดำรงตำแหน่งผู้บังคับกรมตำรวจอาฟริกาใต้ (Inspector General of South African Constabulary) นับว่า บี-พีเป็นนายพลที่อายุน้อยที่สุดคนหนึ่งของกองทัพอังกฤษ

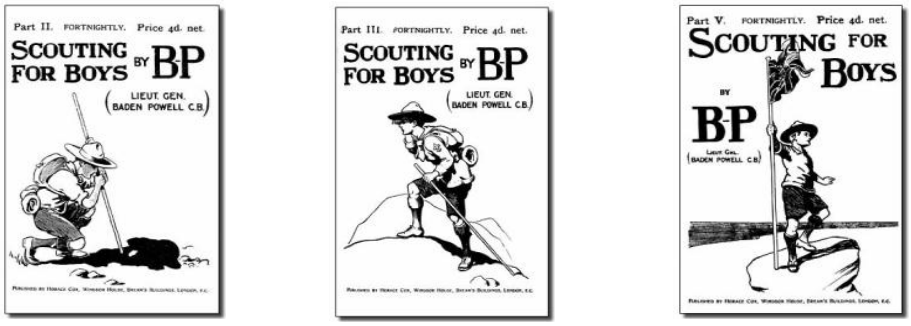
ในต้นปี พ.ศ. 2446 บี-พีก็ย้ายกลับมาประเทศอังกฤษ เพื่อดำรงตำแหน่ง “ผู้บังคับการกรมทหารม้า” ซึ่งท่านก็ประสบความสำเร็จเป็นอย่างสูงในการปรับปรุงพัฒนาวิธีการฝึกอบรมทหารม้าเสียใหม่ในช่วงหลังจากที่บี-พีกลายเป็นวีรบุรุษและเป็นที่รู้จักของคนทั่วประเทศ ปรากฏว่า หนังสือ “คู่มือการสอดแนม”(Aids to Scouting) ที่ท่านเขียนก่อนสงครามบัวร์ก็พลอยขายดีไปด้วย เป็นที่นิยมในหมู่เด็กและเยาวชนมาก และบางโรงเรียนก็นำไปเป็นคู่มือฝึกเด็กๆ ในโรงเรียน ผู้ที่ให้ความสนใจเป็นพิเศษ คือ เซอร์ วิลเลี่ยม สมิทธ์ ผู้ก่อตั้งองค์กรเด็กและเยาวชนที่มีชื่อเสียงในขณะนั้น คือ “สมาคมเด็กชาย” ท่านเซอร์ผู้นี้จึงชักชวนให้ บี-พีมาร่วมงานด้วย โดยตั้งให้เป็น “รองสภานายกกิตติมศักดิ์” ของสมาคมฯ และได้ขอให้บี-พีจัดทำแบบฝึกขึ้นมาใหม่เพื่อใช้ในการฝึกเด็กชายในทำนองเดียวกันกับการฝึกผู้สอดแนม ซึ่งบี-พีก็เห็นชอบด้วยและเตรียมการค้นคว้าเพิ่มเติมจากประสบการณ์ของท่านตั้งแต่บัดนั้น

บี-พี ได้เลื่อนยศเป็น “พลโท” ในตำแหน่ง “ผู้บัญชาการกองพลนอร์ธธัมเบรียน” ซึ่งเป็นส่วนหนึ่งของกำลังทหารรักษาดินแดน (Territorial Army) ซึ่งตั้งขึ้นใหม่ มีหน้าที่ฝึกทหารใหม่โดยตรง ซึ่งเป็นงานที่ บี-พีถนัดอยู่แล้ว ปีพ.ศ. 2450 (ค.ศ.1907) งานในตำแหน่งใหม่นี้ไม่หนักนัก บี-พีจึงมีเวลาว่างพอที่จะทำแบบฝึกเด็กตามที่ได้ตกลงกันเอาไว้ ก่อนที่จะทำแบบฝึกหรือคู่มือการฝึกขึ้นมา ท่านก็มีความรอบคอบที่จะทดลองฝึกเด็กจริง ๆ ดูก่อน ดังนั้นในประมาณต้นเดือนสิงหาคม พ.ศ. 2450 ท่านจึงได้รวบรวมเด็กชาย 20 คน ซึ่งมีภูมิหลังครอบครัวที่ต่างๆ กันไปอยู่ค่ายพักแรมที่เกาะบราวน์ซี (Brownsea Island) ซึ่งเป็นเกาะเล็กๆ ใกล้ๆ กับเมืองพูล (Poole) ทางตอนใต้ของอังกฤษ การเข้าค่ายใช้เวลาประมาณ 7 วัน

รูปที่ 1-3 บี-พี ในการพักแรมที่เกาะบราวน์ซี

บี-พี แบ่งเด็กออกเป็น 4 หมู่ๆ ละ 5 คน ตั้งเด็กที่อาวุโสในแต่ละหมู่เป็น “นายหมู่” (Patrol Leader) ทุกวันจะมีการฝึกอบรมกิจกรรมลูกเสือ สลับกับการเล่นเกม การเล่านิทาน จากประสบการณ์ของตัวท่านเอง ซึ่งเด็กๆจะให้ความสนใจมาก เพราะเด็กๆ รู้จักชื่อเสียง ความเก่งกล้าสามารถของท่านอยู่แล้ว ตอนกลางคืนก็มีการเล่นรอบกองไฟ ร้องเพลง และมีการจัดให้แต่ละหมู่ทำหน้าที่เป็นยามช่วงกลางคืน สลับเปลี่ยนกันไปทุกคืน หมู่ที่เป็นยามจะต้องไปตั้งแค้มป์นอกค่ายใหม่ ต้องทำอาหารกินเอง และผลัดกันเข้ายาม ในวันสุดท้ายบี-พีเชิญพ่อแม่เด็กและแขกผู้มีเกียรติจำนวนหนึ่งมาชมการแสดงต่างๆ ของเด็กที่ได้รับการฝึกอบรมมา การเข้าค่ายทดลองของบี-พี ในครั้งนี้ประสบความสำเร็จเป็นอย่างสูง ซึ่งท่านเชื่อว่าเหตุผลหลักของความสำเร็จ คือ การแบ่งเด็กออกเป็นหมู่ โดยเด็กในหมู่อยู่ด้วยกัน กินด้วยกัน เล่นด้วยกัน ทำงานด้วยกัน ตลอดจนมีหัวหน้าดูแลรับผิดชอบพวกเขากันเอง และการที่เด็กได้ใช้ชีวิตค่อนข้างอิสระกลางแจ้ง ในธรรมชาติก็เป็นสิ่งที่ถูกใจเด็กๆ มาก บี-พีก็ได้นำเครื่องหมายลูกเสือโลกมาใช้ประดับเครื่องแบบของเด็กๆ ในการเข้าค่ายครั้งแรกนี้ด้วย

ในต้นปี พ.ศ. 2451 บี-พีก็เขียนหนังสือ “การลูกเสือสำหรับเด็กชาย” โดยพิมพ์ออกขายทีละบท รวมทั้งสิ้นหกบท ได้รับการต้อนรับอย่างกว้างขวางทั่วประเทศ โดยเฉพาะพวกเด็กๆ



รูปที่ 1-4 หนังสือ Scouting for Boys ที่แต่งโดย บี-พี

ประมาณเดือนเมษายน พ.ศ. 2451 บี-พีออกหนังสือรายสัปดาห์ ชื่อ “Scout” ซึ่งขายดีมากอีกเช่นกัน หนังสือรายสัปดาห์ฉบับนี้มีส่วนช่วยเผยแพร่กิจการลูกเสือออกไปสู่มหาชนอย่างมาก การชุมนุมอย่างเป็นทางการของลูกเสือครั้งแรก ก็คือ งานชุมนุมลูกเสือที่คริสตัล พาเลซ ในเดือนกันยายน พ.ศ. 2452 มีลูกเสือมาร่วมชุมนุมกันประมาณ 11,000 คน กษัตริย์อังกฤษ คือ เอ็ดเวิดที่ 7 ได้ทรงมีพระราชโทรเลขมาแสดงความยินดีกับงานชุมนุมครั้งนี้ด้วย ทำความปลื้มใจให้กับบี-พี และเหล่าลูกเสือทั้งหลายเป็นอย่างมาก

ในปี พ.ศ. 2452 นี้ ทางหนังสือ Scout ได้จัดให้มีการฝึกเข้าค่ายทางทะเลขึ้นโดยจัดบนเรือฝึกชื่อเมอร์คิวรี่ อันถือว่าเป็นต้นกำเนิดของ “ลูกเสือสมุทร” ตั้งแต่บัดนั้น หลังจากงานชุมนุมลูกเสือที่คริสตัลพาเลซได้ไม่นาน บี-พีก็ได้รับโปรดเกล้าฯ เป็นเซอร์ โรเบิร์ต เบเดน – เพาเวลด์ โดยได้รับพระราชทานเครื่องราชฯ Knight Commander of the Royal Victorian Order (K.C.V.O) และ Knight Commander of the Order of the Bath (K.C.B) การฝึกอบรมลูกเสือของบี-พีมีทั้งผู้สนับสนุนและผู้ต่อต้าน เพราะในสมัยนั้นวิธีการฝึกอบรมลูกเสือเป็นสิ่งที่ใหม่มาก จะถือว่าเป็นการปฏิวัติการฝึกอบรมเด็กก็ว่าได้ ผู้ที่ต่อต้านเชื่อว่าวิธีการของบี-พีเป็นวิธีที่ใช้ฝึกทหารมากกว่าฝึกเด็ก แต่ความจริงบี-พีเน้นเสมอว่าการฝึกอบรมลูกเสือของท่านถึงแม้จะใช้วิธีการของทหารอยู่บ้าง แต่ท่านไม่ได้ต้องการให้เด็กเป็นทหารแต่อย่างใด ความมุ่งประสงค์ของการลูกเสือ คือ ต้องการให้เด็กเติบโตเป็นคนดี เป็นพลเมืองดีนั่นเอง

ประมาณเดือนพฤษภาคมปี พ.ศ. 2453 กิจการลูกเสือเติบโตอย่างรวดเร็ว และเริ่มกระจายไปในต่างประเทศหลายประเทศ บี-พีจำเป็นจะต้องเลือกระหว่างการที่จะรับราชการต่อไปหรือลาออก เพื่อมากำกับดูแลกิจการลูกเสือแต่เพียงอย่างเดียว บี-พีเลือกที่จะลาออกจากราชการนับว่าเป็นการตัดสินใจที่ยากสำหรับท่าน และนับเป็นการเสียสละของท่านเป็นอย่างยิ่งเพราะหากท่านรับราชการต่อไป ท่านอาจจะได้เป็นใหญ่ถึงระดับผู้บัญชาการทหารบกก็ได้ แต่มีการกล่าวกันว่ากษัตริย์อังกฤษขณะนั้นทรงสนับสนุนให้บี-พีลาออกจากราชการเพื่อมาดูแลกิจการลูกเสือ ซึ่งอาจจะเป็นไปได้ เมื่อมองย้อนกลับไปนับได้ว่า บี-พีตัดสินใจได้อย่างถูกต้อง เพราะกิจการลูกเสือทำให้ท่านอยู่ในความทรงจำของคนทั่วโลกอีกนานเท่านาน

ในระหว่างการชุมนุมลูกเสือที่คริสตัลพาเลซ ในปี พ.ศ. 2452 นั้น ปรากฏว่ามีลูกเสือหญิงแอบเข้ามามีส่วนร่วมชุมนุมด้วยจำนวนหนึ่ง เมื่อบี-พีตรวจพบท่านตกใจมากเพราะในสมัยนั้นเด็กผู้หญิงจะต้องอยู่กับเหย้าเฝ้าอยู่กับเรือน จะทำอะไรๆ แบบเด็กชายไม่ได้ แต่ลูกเสือหญิงเหล่านี้มีความตั้งใจแน่วแน่ที่จะเป็นลูกเสือให้ได้โดยไม่เกรงกลัวข้อทัดทานใดๆ จากพ่อแม่และสังคม บี-พีจึงตกลงใจให้มีลูกเสือหญิงได้ตามคำเรียกร้อง และได้ขอร้องให้น้องสาวคนเดียวของท่านชื่อ แอกเนส เป็นผู้ดูแลกิจการลูกเสือหญิง โดยในปี พ.ศ. 2453 แอกเนสได้จัดตั้ง “สมาคมเนตรนารี” ขึ้น มีสมาชิกเริ่มต้นกว่า 6,000 คน การจัดตั้งสมาคมเนตรนารีแยกต่างหากจากเด็กชายก็เพื่อให้เป็นที่ยอมรับของพ่อแม่และสังคมในสมัยนั้น ในปัจจุบันถึงแม้การทำกิจกรรมระหว่างเด็กหญิงและชายจะเป็นที่ยอมรับกันโดยทั่วไปแล้ว แต่องค์กรทั้งสองก็ยังคงแยกกันอยู่เหมือนเดิม

วันที่ 30 ตุลาคม พ.ศ. 2455 บี-พีแต่งงานกับนางสาวโอเลฟ เซนท์แคล โซมส์ ซึ่งอายุเพียง 23 ปี ซึ่งบี-พีรู้จักเป็นครั้งแรกในเรือโดยสารระหว่างเดินทางไปสหรัฐอเมริกาเมื่อตอนต้นปี ถึงแม้ทั้งสองคนจะอายุต่างกันถึงสามสิบกว่าปี ทั้งคู่ก็มีความสุขในชีวิตสมรสเป็นอย่างมาก เพราะมีรสนิยมในชีวิตที่คล้ายกัน เลดี้ บี-พีเป็นกำลังสำคัญของบี-พี ในงานพัฒนากิจการเนตรนารีและกิจการลูกเสือ ทั้งคู่มีบุตรด้วยกัน 3 คน

สงครามโลกครั้งที่ 1 ลูกเสือและเนตรนารีแสดงบทบาทช่วยเหลือสังคมได้จริงตามที่ บี-พี มุ่งหวังทุกประการ ถึงแม้อยู่ในภาวะสงครามสมาชิกลูกเสือเพิ่มขึ้นจากประมาณ 1.5 แสน ในปี พ.ศ. 2457 เป็นเกือบ 2.0 แสนคน ในปี พ.ศ. 2461

บี-พี ออกหนังสือ “คู่มือลูกเสือสำรอง” (The Wolf Cub’s Handbook) ลูกเสือสำรองถือกำเนิดเป็นทางการในปี พ.ศ. 2459 (ค.ศ. 1916) บี-พีพบว่ากิจกรรมสำหรับลูกเสือทั่วไปไม่ค่อยเหมาะสมกับเด็กโตหรือเด็กหนุ่ม ท่านจึงจัดทำกิจกรรมขึ้นมาใหม่ให้เหมาะสมกับวัยของเด็ก จึงนับว่า “ลูกเสือวิสามัญ” ถือกำเนิดขึ้นในปี พ.ศ. 2461 (ค.ศ. 1918) หนังสือคู่มือลูกเสือวิสามัญ ซึ่งบี-พีตั้งชื่อว่า “การเดินทางสู่ความสำเร็จ”

(Rovering to Success) ออกมา 4 ปี ให้หลัง คือ ปี พ.ศ. 2465 (ค.ศ. 1922)

เนื่องจากเลดี้ บี-พี มีความสนใจและเข้าร่วมในกิจกรรมลูกเสือและเนตรนารีเป็นประจำ บี-พี จึงสนับสนุนให้ท่านรับภาระดูแลสมาคมเนตรนารีแทนน้องสาวของบี-พี โดยรับตำแหน่ง “ประมุขเนตรนารี”แต่ในปี พ.ศ. 2473 (ค.ศ. 1930) ตำแหน่งเปลี่ยนชื่อเป็น “ประมุขเนตรนารีโลก และครองตำแหน่งนี้จนวันสุดท้ายของชีวิตท่าน ในปีพ.ศ. 2520 (ค.ศ. 1977)

มิสเตอร์ เดอร์บัวส์ แมคคลาเรน (Ms. De Bois Maclaren) มอบกิลเวลล์พาร์ค (Gilwell Park) ให้แก่คณะลูกเสืออังกฤษ เพื่อใช้ในกิจการลูกเสือ ในเดือนกันยายนปีเดียวกันนี้ ก็มีการฝึกอบรมลูกเสือหลักสูตรวูดแบดจ์ ในปี พ.ศ. 2462 (ค.ศ. 1919) บี-พี เชิญลูกเสือจากทั่วโลกมาชุมนุมที่อาคารโอลิมเปียในกรุงลอนดอน นับว่าเป็น “งานชุมนุมลูกเสือโลกครั้งแรก” ในช่วงปลายเดือนกรกฎาคม – 7 สิงหาคม พ.ศ. 2463 มีลูกเสือจากทั่วโลกราว 21 ประเทศ มาร่วมชุมนุมประมาณ 8,000 คน ในวันสุดท้ายของงานชุมนุมฯ ลูกเสือทุกคนที่ร่วมงาน ประกาศยกย่องให้บี-พีเป็น “ประมุขลูกเสือโลก” งานชุมนุมครั้งนี้เป็นครั้งแรกที่บี-พีตกลงใช้คำว่า “jamboree” สำหรับงานชุมนุมลูกเสือและเนตรนารี แม้จะมีผู้ไม่ค่อยเห็นด้วยอยู่บ้างเพราะเป็นคำมีความหมายเดิมไม่ค่อยดีนัก (แปลว่า งานเลี้ยงที่ส่งเสียงดังเอะอะ)

รูปที่ 1-5 งานชุมนุมลูกเสือโลกครั้งแรก

ในระหว่างงานนี้ได้มีการประชุมสมัชชาลูกเสือนานาชาติ เป็นครั้งแรกด้วย ซึ่งภายหลังเปลี่ยนชื่อเป็นการประชุมสมัชชาลูกเสือโลก ขณะเดียวกันก็มีการจัดตั้ง “สำนักงานลูกเสือนานาชาติ” ซึ่งภายหลังเปลี่ยนชื่อเป็น “สำนักงานลูกเสือโลก” ตั้งอยู่ที่กรุงเจนีวา ประเทศสวิตเซอร์แลนด์ นับได้ว่าในปีนี้กิจการลูกเสือกลายเป็นกิจการระดับโลกอย่างแท้จริง [4]

2.2 ประวัติ ภูมิหลังและกิจการลูกเสือไทย

พระบาทสมเด็จพระมงกุฎเกล้าเจ้าอยู่หัวทรงพระราชดำริตั้งกองเสือป่า วันที่ 16 เมษายน พ.ศ.2454 (ค.ศ. 1991) พระบาทสมเด็จพระมงกุฎเกล้าเจ้าอยู่หัวเสด็จประพาสหัวเมืองชายทะเลปักษ์ใต้ โดยเรือพระที่นั่งมหาจักรี และทรงเริ่มจดชื่อผู้สมัครเป็นเสือป่าแล้ว เรียกประชุมในเรือพระที่นั่ง ได้โปรดเกล้าฯ ให้สถาปนากองเสือป่าขึ้นโดยประกาศเป็นพระบรมราชโองการ เมื่อวันที่ 1 พฤษภาคม ร.ศ. 130 (ซึ่งตรงกับ พ.ศ. 2454, ค.ศ. 1911) นอกจากนี้ยังมีพระราชประสงค์ดังต่อไปนี้ [5]

1. ปลูกฝังความจงรักภักดีต่อพระมหากษัตริย์
2. ปลูกฝังความรักชาติบ้านเมือง และนับถือพุทธศาสนา

3. ปลูกฝังความสามัคคีในหมู่คณะ และไม่ทำลายซึ่งกันและกัน

ทั้งนี้ได้มีประกาศเป็นกระแสพระราชปรารภแจ้งอยู่ใน “จดหมายเหตุเสือป่า” เล่ม 1 ตอน 1 และเมื่อมีผู้มาสมัครเข้ามีจำนวนมากพอ ที่จะตั้งเป็นกองร้อยขึ้นได้กองหนึ่งแล้ว ควรจะให้กระทำประพาสสาบานตนเข้าประจำกอง จึงทรงพระกรุณาโปรดเกล้าฯ ให้เตรียมจัดตั้งการพิธีถือน้ำ ณ วัดพระศรีรัตนศาสดาราม

รูปที่ 1-6 พระบาทสมเด็จพระมงกุฎเกล้าเจ้าอยู่หัวทรงฉายพระรูปพร้อมพระบรมวงศานุวงศ์

รูปที่ 1-7 พระบาทสมเด็จพระมงกุฎเกล้าเจ้าอยู่หัว ทรงฉายพระรูปพร้อมสมาชิกเสือป่ารุ่นแรก

ถ่ายที่หน้าระเบียงอุโบสถวัดพระศรีรัตนศาสดาราม พ.ศ. 2454

กำหนดวันที่ 6 พฤษภาคม ร.ศ.130 (พ.ศ.2454, ค.ศ. 1991) โดยมีสมเด็จพระมหาสมณะเจ้ากรมพระยาวชิรญาณวโรรส [6] เป็นประธานเจริญพระพุทธมนต์พระบาทสมเด็จพระเจ้าอยู่หัวได้ทรงดำรงพระยศเป็นนายกองใหญ่ผู้บังคับการกองเสือป่า การกระทำสัตย์สาบานในพิธีการถือน้ำพิเศษเสือป่า เมื่อวันที่ 6 พฤษภาคม พ.ศ.2454 (ค.ศ. 1991) และสมาชิกเสือป่ารุ่นแรก ได้เข้าร่วมพิธีจำนวน 141 คน ภายหลังสถาปนากิจการเสือป่าได้ 2 เดือน พระบาทสมเด็จพระมงกุฎเกล้าเจ้าอยู่หัวทรงมีพระราชปรารภในการจัดตั้งกองลูกเสือ ซึ่งพระราชปรารภในการจัดตั้งกองลูกเสือ ได้ปรากฏอยู่ในคำปรารภของข้อบังคับลักษณะปกครองลูกเสือฉบับแรก ซึ่งประกาศใช้เมื่อวันที่ 1 กรกฎาคม ร.ศ.130 ดังนี้

พระบาทสมเด็จพระปรเมนทร์มหาวชิราวุธ พระมงกุฎเกล้าเจ้าอยู่หัว ผู้ทรงดำรงพระยศเป็นนายกองใหญ่ในกองเสือป่า ทรงพระราชดำริว่ากองเสือป่าได้ตั้งขึ้นเป็นหลักฐานแล้ว พอจะเป็นที่หวังได้ว่าจะเป็นผลดีตามพระราชประสงค์ แต่ผู้ที่จะเป็นเสือป่าต้องเป็นผู้ที่นับว่าเป็นผู้ใหญ่แล้ว ฝ่ายเด็กชายที่ยังอยู่ในปฐมวัยก็เป็นผู้ที่สมควรจะได้รับการฝึกฝนทั้งในส่วนร่างกายและในส่วนใจให้มีความรู้ในทางเสือป่า เพื่อว่าเมื่อเติบใหญ่ขึ้นแล้วจะได้รู้จักน่าที่ซึ่งผู้ชายไทยทุกคนควรจะประพฤติให้เป็นประโยชน์แก่ชาติบ้านเมือง อันเป็นที่เกิดเมืองนอนของตน และการฝึกฝนปลุกใจให้คิดถูกเช่นนี้ ต้องเริ่มฝึกฝนเสีย เมื่อยังเยาว์อยู่เปรียบเสมือนไม้ที่ยังอ่อนจะดัดไปเป็นรูปอย่างไรก็เป็นไปได้ง่ายและงดงาม แต่ถ้ารอไว้จนแก่เสียแล้ว เมื่อจะดัดก็ต้องเข้าไฟ และมักจะหักลงได้ในขณะที่ดัด ดังนี้ฉันใดสันดานคนก็ฉันนั้น จึงทรงพระกรุณาโปรดเกล้าฯ พระบรมราชานุญาติให้จัดตั้งกองลูกเสือขึ้นตามโรงเรียนและสถานที่อันสมควร

กิจการลูกเสือของประเทศไทยได้ถูกสถาปนาขึ้น มีมูลเหตุมาจากข้อบังคับลักษณะปกครองลูกเสือ ซึ่งพระบาทสมเด็จพระมงกุฎเกล้าเจ้าอยู่หัวได้ทรงพระกรุณาโปรดเกล้าฯ ให้ประกาศใช้ข้อบังคับลักษณะปกครองลูกเสือ เมื่อวันที่ 1 กรกฎาคม ร.ศ.130 โดยข้อบังคับลักษณะปกครองลูกเสือนี้แบ่งออกเป็น 10 หมวด บรรจุความรวม 62 ข้อด้วยกัน และมีความยาวถึง 42 หน้ากระดาษ ดังนี้

หมวด 1 นามและลักษณะใช้ข้อบังคับ
หมวด 2 การปกครองกลาง
หมวด 3 การปกครองประจำมณฑล
หมวด 4 การปกครองลูกเสือ
หมวด 5 ว่าด้วยลูกเสือ
หมวด 6 การรับลูกเสือและเลื่อนขั้น
หมวด 7 การจดและการถอนทะเบียน
หมวด 8 เครื่องแต่งตัว
หมวด 9 เครื่องประกอบเครื่องแต่งตัว
หมวด 10 การเคารพ

ตั้งสภากรรมการกลางและผู้ตรวจการใหญ่ ภายหลังที่ได้ประกาศใช้ข้อบังคับลักษณะปกครองลูกเสือแล้วนั้น เพื่อให้การได้ดำเนินไปดังพระราชประสงค์ที่ปรากฏอยู่ในข้อบังคับนั้น จึงได้ทรงพระกรุณาโปรดเกล้าฯ ให้ตั้งสภากรรมการกลางขึ้น โดยได้ทรงพระกรุณาเข้ารับตำแหน่งหน้าที่เป็นสภานายกแห่งสภากรรมการกลางด้วยพระองค์เอง และได้ทรงพระกรุณาโปรดเกล้าฯ ให้พระบรมวงศ์เธอ กรมพระดำรงราชานุภาพ และดำรงตำแหน่งเสนาบดีกระทรวงมหาดไทยเป็นผู้ตรวจการใหญ่และเป็นอุปนายกด้วย ตามข้อบังคับลักษณะปกครองลูกเสือนั้น กับทรงพระกรุณาโปรดเกล้า ฯ ให้พระยาบุรีนวราษฐ์เป็นเลขานุการ

ขณะนั้นกำลังดำรงตำแหน่งผู้รั้งตำแหน่งเสนาบดีกระทรวงธรรมการ เป็นกรรมการตำแหน่งผู้ตรวจการใหญ่และอุปนายกนี้ ต่อมาในปีพ.ศ. 2457 พระเจ้าบรมวงศ์เธอ กรมพระดำรงราชานุภาพได้กราบถวายบังคมลาพักราชการไป จึงได้ทรงพระกรุณาโปรดเกล้า ฯ ให้เจ้าพระยาพระเสด็จสุเรนทราธิบดี (ม.ร.ว. เปีย มาลากุล) เข้ารับตำแหน่งแทนสืบต่อมา จนถึงเวลาที่ป่วยหนักจึงได้ทรงพระกรุณาโปรดเกล้า ฯ ให้พระยาไพศาลศิลปศาสตร์ (รื่น ศยามานนท์) อธิบดีกรมศึกษาธิการเข้ารับตำแหน่งแทนต่อมา ตั้งแต่วันที่ 27 พฤษภาคม พ.ศ.2457 และได้ดำรงตำแหน่งนี้ตลอดมาจนสิ้นรัชสมัยพระบาทสมเด็จพระมงกุฎเกล้าเจ้าอยู่หัว

ตั้งสภากรรมการมณฑลกรุงเทพฯ หลังจากที่ทรงตั้งสภากรรมการกลาง และผู้ตรวจการใหญ่แล้ว เพื่อให้กองลูกเสือได้ตั้งขึ้นโดยเร็วในมณฑลกรุงเทพฯ อันเป็นมณฑลราชธานี เพื่อที่จะได้เป็นตัวอย่างแก่มณฑลอื่นๆ ต่อไป จึงได้ทรงพระกรุณาโปรดเกล้าฯ ให้มีสภากรรมการประจำมณฑลกรุงเทพฯ ขึ้นในอันดับต่อมา ทรงพระกรุณาโปรดเกล้าฯ ให้เจ้าพระยายมราช (ปั้น สุขุม) เสนาบดีกระทรวงนครบาลในขณะนั้นเป็นสภานายกกรรมการประจำมณฑลกรุงเทพฯ

รูปที่ 1-8 เสวกตรี นายลิขิตสารสนอง (ชัพน์ บุนนาค)

ลูกเสือไทยคนแรกของประเทศสยามในขณะนั้น คือ นายชัพน์ บุนนาค นักเรียนมหาดเล็กหลวง ซึ่งต่อมาได้รับพระราชทานบรรดาศักดิ์เป็น นายลิขิตสารสนอง

กองลูกเสือกองแรกของประเทศไทยได้ตั้งขึ้นที่โรงเรียนมหาดเล็กหลวง จึงได้นามว่า “กองลูกเสือกรุงเทพฯ ที่ 1” ปรากฏว่าได้ทรงเอาเป็นพระราชธุระในการอบรมสั่งสอน ตลอดจนการดำเนินงานทั่วๆ ไปของกองลูกเสือกองนี้โดยตรง ทั้งนี้เพื่อจะให้เป็นแบบอย่างสำหรับโรงเรียนอื่นๆ หรือสถานที่อื่นๆ ที่มีความประสงค์จะตั้งกองลูกเสือขึ้น ได้ยึดถือเป็นบรรทัดฐานในการดำเนินงานของตนต่อไป ในการนี้ได้ทรงพระกรุณาโปรดเกล้าฯ ให้จัดพิมพ์พระบรมราโชวาทที่พระราชทานแก่เสือป่า และพระราชนิพนธ์แบบสั่งสอนขึ้นเพื่อเจ้าหน้าที่จะได้นำไปอบรมสั่งสอนนักเรียนที่สมัครเป็นลูกเสือต่อไป

รูปที่ 1-9 ธงกองลูกเสือกรุงเทพ ที่ 1 วชิราวุธวิทยาลัย

ต่อมาเมื่อวันที่ 2 กันยายน พ.ศ.2454 (ค.ศ.1911) ได้พระราชทานพระราชวโรกาสให้กองลูกเสือโรงเรียนมหาดเล็กหลวงได้เข้าเฝ้าทูลละอองธุลีพระบาท ณ สโมสรเสือป่า ในโอกาสนั้นผู้กำกับได้ฝึกลูกเสือถวายตัว และได้การสอบซ้อมวิชาลูกเสือ ตามแบบที่ได้ทรงพระราชนิพนธ์ไว้สำหรับสั่งสอนเสือป่าและลูกเสือ ในโอกาสนี้เองพระราชกรุณาโปรดเกล้าฯ พระราชทานนามกองลูกเสือโรงเรียนมหาดเล็กหลวงซึ่งเป็นกองเริ่มแรกที่ได้จัดตั้งขึ้นนี้ว่า “กองลูกเสือหลวง” และวันที่ 3 กันยายนได้ตามเสด็จพระราชดำเนินประพาสพระราชวังสนามจันทร์ จังหวัดนครปฐม และได้พระราชทานในโอกาสคราวประกอบพิธีถือน้ำพิเศษของกองเสือป่ามณฑลนครชัยศรี โดยนายหมู่โทหลวงอภิรักษ์ราชฤทธิ์ อาจารย์โรงเรียนมหาดเล็กหลวง เป็นผู้รับพระราชทาน ต่อมาในวันที่ 16 กันยายนได้ทรงพระกรุณาโปรดเกล้าฯ พระราชทานธงรูปพระมนูแถลงสารให้เป็นธงประจำกองลูกเสือหลวงกองนี้

ทรงวางนโยบายให้มีการจัดตั้งกองลูกเสือในโรงเรียนต่างๆ โรงเรียนรุ่นแรกที่มีการจัดตั้งกองลูกเสือ คือ โรงเรียนมหาดเล็กหลวง โรงเรียนราชวิทยาลัย โรงเรียนสวนกุหลาบวิทยาลัย โรงเรียนเทพศิรินทร์ โรงเรียนปทุมคงคา มีจำนวนลูกเสือทั้งหมดใน 4 โรงเรียน (เว้นโรงเรียนราชวิทยาลัย) ในเดือนกันยายนพ.ศ.

2454 (ค.ศ.1911) รวม 346 คน ต่อมาได้มีการจัดตั้งกองลูกเสือเพิ่มขึ้นในโรงเรียนต่างๆ โดยลำดับตามสถิติเดือนกุมภาพันธ์ พ.ศ.2454 (ค.ศ.1911) มีกองลูกเสือ 65 กอง รวมจำนวนเจ้าหน้าที่ลูกเสือ และลูกเสือ 2,648 คน

ทรงรับกองลูกเสืออังกฤษ The 8th South-West London Troop ไว้ในพระบรมราชูปถัมภ์และให้เป็นกองลูกเสือในพระองค์แห่งพระเจ้าแผ่นดินกรุงสยาม (The King of Siam's Own) กับพระราชทานตราเครื่องหมายประจำกองเป็นรูปช้างเผือกยืนบนพื้นธงสีแดง ซึ่งเป็นรูปคล้ายธงช้างเดิม

ต่อมากองลูกเสือนี้ได้ขยายตัวเป็นกลุ่มและเปลี่ยนชื่อใหม่ตามชื่อของตำบลที่ตั้งกลุ่มเป็น The First Balham and Tooting Scout Group (The King of Siam's Own) โดยยังคงใช้ตราช้างเผือกยืนบนธงพื้นสีแดงเป็นตราประจำกลุ่มสืบมา และใช้อักษรย่อของกลุ่มว่า K.S.O ซึ่งย่อมาจากคำว่า the King of Siam's own

รูปที่ 1-10 ลูกเสือของกองลูกเสือในพระองค์แห่งพระเจ้าแผ่นดินกรุงสยาม

รูปที่ 1-11 สมาชิกรุ่นแรกของ K.S.O

ผู้ที่จะเข้าเป็นลูกเสือและเสือป่าในรัชสมัยพระบาทสมเด็จพระมงกุฎเกล้าเจ้าอยู่หัว ต้องศึกษาบทพระราชนิพนธ์ "ปลุกใจเสือป่า" ซึ่งได้ทรงเริ่มแสดงบรรยายครั้งแรก เมื่อวันที่ 26 พฤษภาคม ร.ศ.130 (พ.ศ. 2454, ค.ศ.1911) เป็นต้นมา เป็นบทความเรื่องยาวหลายตอนติดต่อกัน เป็นพระราชนิพนธ์ที่ปลุกใจให้ผู้อ่านสำนึกในหน้าที่แต่ละคน พึงมีต่อชาติเป็นอย่างดียิ่ง กระทรวงธรรมการในเวลานั้น ได้ออกประกาศให้บรรดาครูอาจารย์ตามสถานศึกษาต่างๆ ได้สนใจศึกษาบทพระราชนิพนธ์นี้เป็นกรณีพิเศษ และในเวลาต่อมาก็ได้พระราชทานบทพระราชนิพนธ์ปลุกใจ "เทศนาเสือป่า" โดยแทรกหลักธรรมลงไปด้วยอีกชิ้นหนึ่งแก่เสือป่าและลูกเสือ ซึ่งเป็นเรื่องยาวหลายตอนติดต่อกัน 17 กัณฑ์

นอกจากนี้ ยังทรงมีบทพระราชนิพนธ์อีกบทหนึ่ง คือ “แบบสั่งสอนเสือป่าและลูกเสือ” เป็นบทพระราชนิพนธ์อันเกี่ยวด้วยวิชาการของลูกเสือโดยตรง เป็นแบบเรียนที่เสือป่าและลูกเสือต้องศึกษาอย่างจริงจัง ประกอบด้วยบทต่างๆ ดังต่อไปนี้

บทที่ 1	การสืบข่าวและการเดินทาง
บทที่ 2	อาณัติสัญญาณ
บทที่ 3	การช่างและความรู้เบ็ดเตล็ด
บทที่ 4 - 5	การตั้งค่ายและที่พักแรม
บทที่ 6	ยามและด่าน
บทที่ 7	การพิจารณาสังเกตและจดจำ
บทที่ 8	การสะกดรอย
บทที่ 9	การสันนิษฐาน
บทที่ 10	การแฝงกายและเกลื่อนรอย
บทที่ 11	รายงานและแจ้งเหตุ
บทที่ 12	กำบัง
บทที่ 13	ตั้งรับ
บทที่ 14	ป้องกันตัว
บทที่ 15	จับผู้ร้าย
บทที่ 16	ช่วยชีวิตและกันภัย
บทที่ 17 - 18	ปัจจุบันพยาบาล

การสอบไล่วิชาลูกเสือครั้งแรกพระบาทสมเด็จพระมงกุฎเกล้าเจ้าอยู่หัวทรงเห็นว่า กองลูกเสือกรุงเทพฯ ที่ 1 (ลูกเสือหลวง) ได้รับการฝึกหัดจนมีความรู้ขั้นต้นพอจะเข้าประจำกองเป็นลูกเสือโท ตามข้อบังคับลักษณะปกครองลูกเสือได้แล้ว จึงทรงพระกรุณาโปรดเกล้าฯ ให้พระเจ้าบรมวงศ์เธอ กรมพระยาดำรงราชานุภาพ ซึ่งทรงดำรงตำแหน่งผู้ตรวจการใหญ่และอุปนายกสภากรรมการกลางโดยหน้าที่ เป็นประธานกรรมการสอบไล่วิชาลูกเสือโทของกองลูกเสือกรุงเทพฯ ที่ 1 (ลูกเสือหลวง) เป็นครั้งแรก ในการสอบไล่แม้จะได้มีเวลาฝึกหัดกันเพียงเล็กน้อย ยังปรากฏว่ามีลูกเสือที่สามารถสอบไล่ผ่าน ผ่านขึ้นไปเป็นลูกเสือโทกันเป็นจำนวนมาก

สำหรับการสอบไล่วิชาลูกเสือ ซึ่งโดยมากมีแต่วิชาลูกเสือโททั้งสิ้น ต่อมาได้ดำเนินเกือบไปถ้วนทั่วทุกมณฑลในระยะแรกๆ นั้น ปรากฏตามรายงานว่าหลายมณฑลลูกเสือมักสอบตกในวิชาว่ายน้ำ แต่ทั้งนี้มิใช่ความบกพร่องของผู้ฝึกหัด เป็นด้วยหาที่ฝึกหัดได้ยาก มณฑลเหล่านี้ ได้แก่ มณฑลนครราชสีมา มณฑลสุราษฎร์ และมณฑลภูเก็ต เป็นต้น ซึ่งในท้องที่ดังกล่าวนี้หาแหล่งน้ำอันปราศจากสัตว์ร้ายได้ยาก ต้องอาศัยฝึกหัดตามสระที่ขุดขึ้น กับยังมีบางมณฑลที่ราษฎรไม่เห็นความจำเป็นที่จะต้องว่ายน้ำเป็น มีมณฑลมหาราษฎร์ เป็นต้น จึงไม่พยายามฝึกหัดให้บุตรหลานว่ายน้ำกัน แม้จะได้รับคำแนะนำชี้แจงให้หัดไว้เพื่อว่าเมื่อต้องไปในที่ๆ อาจจะได้รับอันตรายทางน้ำก็ปรากฏว่าฝึกหัดไม่ได้อยู่เอง เพราะตัวเองก็ว่ายน้ำกันไม่ใคร่เป็นอยู่แล้ว นี่คือ ส่วนหนึ่งของข้อขัดข้องเกี่ยวกับการสอบวิชาลูกเสือในขณะนั้น

ส่วนวิชาลูกเสือเอกนั้น ปรากฏว่าลูกเสือชนบทได้เปรียบลูกเสือในกรุง ในทางหุงต้มอาหาร เพราะความจำเป็นในชีวิตประจำวันบังคับให้ต้องทำกันเกือบทุกคน รวมทั้งขึ้นต้นไม้ด้วย จึงทำให้เบาแรงผู้ฝึกหัดลงไปได้มาก ซึ่งในเรื่องเหล่านี้ลูกเสือในกรุงยังต้องอาศัยการฝึกหัดอบรมกันขึ้นใหม่เกือบทั้งสิ้น

พิธีเข้าประจำกองครั้งแรก เมื่อพระบาทสมเด็จพระมงกุฎเกล้าเจ้าอยู่หัว ได้ทรงทราบใต้ฝ่าละอองธุลีพระบาท ว่ามีลูกเสือที่สมควรเข้าประจำกองได้แล้ว จึงได้ทรงเป็นพระราชธุระฝึกหัด อบรม และกำกับลูกเสือในการที่จะทำพิธีเข้าประจำกองด้วยพระองค์เองโดยใกล้ชิด ทั้งนี้ก็ด้วยทรงมีพระราชประสงค์ที่จะให้เป็นแบบอย่างอันดี สำหรับกองลูกเสืออื่นๆ ที่จะประกอบพิธีเข้าประจำกองต่อไปในภายหน้าให้ยึดถือไว้เป็นแบบฉบับในการปฏิบัติต่อไป

วันที่ 3 สิงหาคม พ.ศ.2455 ทรงพระกรุณาโปรดเกล้าฯ ให้ลูกเสือหลวงที่สอบไล่ได้แล้วนั้นเข้ากระทำพิธีเข้าประจำกองต่อหน้าพระที่นั่ง ณ พระที่นั่งอภิเศกดุสิต ในโอกาสนั้นได้ทรงพระกรุณาโปรดเกล้าฯ ให้กองลูกเสือต่างๆ ที่มีอยู่ในกรุงเทพฯ ได้เข้าเฝ้าทูลละอองธุลีพระบาทอยู่ในที่นั้นด้วย เพื่อศึกษาพิธีเข้าประจำกองในครั้งนี้ เมื่อพิธีเข้าประจำกองครั้งแรกได้เสร็จสิ้นลงได้ทรงพระกรุณาโปรดเกล้าฯ พระราชทานพระบรมราโชวาทแก่ลูกเสือและเจ้าหน้าที่ลูกเสือ ซึ่งได้เฝ้าทูลละอองธุลีพระบาทอยู่ในที่นั้น

สำหรับตามหัวเมืองต่างๆ ในครั้งนี้ ในการกระทำพิธีรับลูกเสือเข้าประจำกองก็ได้ปรากฏว่าได้จัดทำกันเป็นอย่างดียิ่งข้าราชการฝ่ายการปกครองชั้นผู้ใหญ่นับตั้งแต่อุปราชและสมุหเทศาภิบาลลงมาได้ให้ความร่วมมือในการนี้เป็นอย่างดี โดยการมาเป็นประธานในพิธีให้และให้โอวาทปลุกใจลูกเสือล้วนเป็นที่จับใจยิ่ง

พระบาทสมเด็จพระมงกุฎเกล้าเจ้าอยู่หัวทรงขยายกิจการลูกเสือไปตามมณฑลต่างๆ โดยมีพระราชกระแสดำรัสสั่งพระเจ้าบรมวงศ์เธอ กรมพระดำรงราชานุภาพ เสนาบดีกระทรวงมหาดไทย แนะนำวิธีการฝึกหัดสั่งสอนลูกเสือขึ้น และได้ทรงพระกรุณาโปรดเกล้าฯ ให้สมุหเทศาภิบาลของแต่ละมณฑล เป็นสภานายกกรรมการจัดการลูกเสือประจำมณฑลที่ตนปกครองระหว่าง พ.ศ.2454 – 2455 (ค.ศ.1911-1912) ทรงจัดให้มาแสดงตำนานของชาติไทยกลางแจ้งปีละ 3 คืน คืนละ 3 เรื่อง เพื่อให้การศึกษาอบรมแก่เสือป่าที่สนามเสือป่า วิธีการเป็นของพระองค์เองซึ่งไม่เคยมีมาก่อนในประเทศสยาม ซึ่งทรงเรียกว่า “ตำนานเสือป่า” [7]

2.3 ประวัติ ภูมิหลังและกิจการลูกเสือไซเบอร์

ลูกเสือไซเบอร์ (Cyber Scout) เป็นคำที่ใช้เรียกแทนผู้ผ่านการฝึกอบรมในโครงการสร้างลูกเสือบนเครือข่ายอินเทอร์เน็ต ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เริ่มต้นจาก นายจุติ ไกรฤกษ์ อดีตรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้มีนโยบายให้มีการจัดอบรมความรู้ด้านเทคโนโลยีสารสนเทศและการสื่อสารให้กับกลุ่มลูกเสือจำนวน 200 คน ในวันที่ 1 กรกฎาคม พ.ศ. 2553 ณ สนามกีฬาไทย-ญี่ปุ่นดินแดงในปี พ.ศ. 2553 และเมื่อวันจันทร์ที่ 9 พฤษภาคม พ.ศ. 2554 ได้มีพิธีลงนามบันทึกข้อตกลงความร่วมมือระหว่าง กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกับกระทรวงศึกษาธิการ

2.3.1 ข้อปฏิบัติของลูกเสือไซเบอร์

1) ปฏิบัติตามกฎของลูกเสือ
2) ส่งเสริมการใช้ ICT อย่างสร้างสรรค์
3) สอดส่องการกระทำความผิดบนโลกไซเบอร์
4) ส่งเสริมให้ปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

2.3.2 สัญลักษณ์ของลูกเสือไซเบอร์

รูปที่ 1-12 สัญลักษณ์ของลูกเสือไซเบอร์

สัญลักษณ์ของลูกเสือไซเบอร์ จัดทำขึ้นเพื่อเป็นการสร้างตราสัญลักษณ์ของโครงการและเพื่อใช้ในประชาสัมพันธ์กิจกรรมต่างๆ โดยองค์ประกอบต่างๆของตราสัญลักษณ์มีความหมายดังนี้

1) ตราสัญลักษณ์ของคณะลูกเสือแห่งชาติที่มีสีเหลืองทอง หมายถึง ลูกเสือไทย
2) วงกลมโค้ง ที่มีลักษณะเป็น 3 สี ประกอบด้วย
    2.1) สีแดง หมายถึง ชาติไทยและไซเบอร์
    2.2) สีขาว หมายถึง ศาสนา
    2.3) สีน้ำเงิน หมายถึง พระมหากษัตริย์ผู้ทรงเป็นประมุขของประเทศ
3) เมาส์สีเหลือง หมายถึง กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
4) แว่นขยาย หมายถึง การสอดส่องและการดูแล
5) หมวก หมายถึง หมวกลูกเสือ

3. สาระสำคัญของการลูกเสือ คำปฏิญาณ และกฎของลูกเสือ

3.1 สาระสำคัญของการลูกเสือ

3.1.1 ขบวนการลูกเสือ

ขบวนการลูกเสือ คือ ขบวนการเยาวชนมีวัตถุประสงค์เพื่อการฝึกอบรมให้การศึกษาและพัฒนาเยาวชนให้เป็นพลเมืองดี โดยไม่คำนึงถึงเชื้อชาติ ศาสนา ทั้งนี้เป็นไปตามความมุ่งประสงค์ หลักการและวิธีการซึ่งผู้ให้กำเนิดลูกเสือโลกได้ให้ไว้ ขบวนการนี้เป็นขบวนการระดับโลก มีประเทศสมาชิก 150 ประเทศกอปรด้วย ผู้บังคับบัญชาลูกเสือและลูกเสือประมาณ 28,000,000 คน

3.1.2 องค์ประกอบสำคัญของการลูกเสือ

1) ลูกเสือ
2) ผู้บังคับบัญชาลูกเสือ
3) มีจุดมุ่งหมายหรืออุดมการณ์
4) กิจกรรม (โดยเฉพาะกิจกรรมกลางแจ้ง)
5) การบริหารงาน

3.1.3 จุดหมายหรืออุดมการณ์ของคณะลูกเสือแห่งชาติ

ตามมาตรา 7 แห่งพระราชบัญญัติลูกเสือ (ฉบับที่ 3) พ.ศ. 2528 ระบุว่า คณะลูกเสือแห่งชาติมีวัตถุประสงค์เพื่อพัฒนาลูกเสือทั้งทางกาย สติปัญญา จิตใจและศีลธรรมให้เป็นพลเมืองดี มีความรับผิดชอบ ช่วยสร้างสรรค์สังคมให้มีความเจริญก้าวหน้า เพื่อความสงบสุขและความมั่นคงของประเทศชาติ

3.1.4 หลักการสำคัญของลูกเสือ

1) มีศาสนา

2) มีความจงรักภักดีต่อประเทศชาติของตน

3) มีความศรัทธาในมิตรภาพและความเป็นพี่น้องของลูกเสือทั่วโลก

4) การบำเพ็ญประโยชน์ต่อผู้อื่น

5) การยอมรับและปฏิบัติตามคำปฏิญาณและกฎของลูกเสือ

6) การเข้าเป็นสมาชิกด้วยความสมัครใจ

7) มีความเป็นอิสระต่ออิทธิพลทางการเมือง

8) มีกำหนดการพิเศษสำหรับการฝึกอบรมโดยอาศัย

8.1) ระบบหมู่ ระบบกลุ่ม - การทดสอบเป็นขั้นๆ

8.2) เครื่องหมายวิชาพิเศษ – กิจกรรมกลางแจ้ง

3.1.5 วิธีการ

วิธีการที่จะบรรลุถึงจุดหมายหรืออุดมการณ์ของคณะลูกเสือแห่งชาติ คือ การจัดให้มีการฝึกอบรมที่ก้าวหน้า สนุกสนาน ดึงดูดใจ โดยอาศัยคำปฏิญาณและกฎของลูกเสือเป็นบรรทัดฐาน มีผู้ใหญ่เป็นผู้คอยให้คำแนะนำ นโยบายในการฝึกอบรมลูกเสือ ใช้หลักสำคัญ ดังต่อไปนี้

1) เครื่องแบบลูกเสือถือว่าเป็นเครื่องแบบที่มีเกียรติ เป็นเครื่องหมายแห่งความดี ดังนั้นลูกเสือจะต้องพิถีพิถันในการแต่งเครื่องแบบลูกเสือที่ถูกต้องและสะอาด เรียบร้อยอยู่เสมอกับทั้งจะต้องประพฤติดี ปฏิบัติตนให้สมกับที่ได้ชื่อว่าเป็นลูกเสือ เพื่อเป็นการรักษาชื่อเสียงของตนเองและคณะลูกเสือแห่งชาติ ส่วนเจ้าหน้าที่ทุกคนก็ควรแต่งเครื่องแบบลูกเสือในโอกาสอันควร และถือว่าเครื่องแบบลูกเสือเป็นเครื่องหมายแห่งความเสียสละในการที่ตนได้มีบทบาทในการฝึกอบรมเด็กให้เป็นพลเมืองดี

2) คำปฏิญาณและกฎของลูกเสือ ผู้กำกับพึงหมั่นฝึกอบรมให้เด็กเข้าใจ และปฏิบัติตามคำปฏิญาณและกฎของลูกเสืออยู่เสมอ โดยเฉพาะในเรื่องของความจงรักภักดีต่อชาติ ศาสนา พระมหากษัตริย์ ความเป็นพี่น้องของลูกเสือทั่วโลก และการกระทำความดีต่างๆ โดยเน้นให้เห็นว่า ผู้เป็นพลเมืองดีนั้นจะต้องเป็นผู้กระทำความดีและใช้ความดีนั้นให้เป็นประโยชน์ มิใช่เป็นคนดีโดยอยู่เฉยๆ ไม่ทำอะไรเลย

3) การบำเพ็ญประโยชน์ต่อผู้อื่นเรื่องนี้เป็นเรื่องที่ทำให้กิจการลูกเสือมีชื่อเสียง และเป็นที่รู้จักของบุคคลโดยทั่วไป รากฐานของคติพจน์ของลูกเสือทั้ง 4 ประเภทเกี่ยวข้องกับอุดมการณ์ของลูกเสือในการบำเพ็ญประโยชน์ต่อผู้อื่น

“ทำดีที่สุด” คือ การทำเพื่อคนอื่นหรือเพื่อส่วนรวม เป็นการกระทำที่ดีที่สุด

“จงเตรียมพร้อม” คือ พร้อมที่จะทำความดี พร้อมเพื่อจะสร้าง พร้อมเพื่อส่วนรวม

“มองไกล” คือ มองให้เห็นเหตุผล มองให้เห็นคนอื่น มองให้เห็นส่วนรวม มิใช่มองแต่ตัวเองหรือประโยชน์ของตัวเอง

“บริการ” คือ การให้ความช่วยเหลือแก่ผู้อื่น และแก่ส่วนรวม

นอกจากนี้ในคำปฏิญาณและกฎของลูกเสือก็ได้ระบุถึงการบำเพ็ญประโยชน์ต่อผู้อื่น โดยถือว่าสำคัญ แหล่งหรือโอกาสที่ลูกเสือจะบำเพ็ญประโยชน์นั้นควรเริ่มจากสิ่งที่ใกล้ตัวก่อน แล้วขยายให้กว้างขวางออกไปตามวัยและความสามารถของเด็ก

1) การฝึกอบรมที่ต่อเนื่องกันและก้าวหน้าสูงขึ้น

2) ระบบหมู่ ฝึกความรับผิดชอบ การเป็นผู้นำ ผู้ตาม

3) ระบบเครื่องหมายวิชาพิเศษมีมากมายหลายอย่าง ซึ่งลูกเสืออาจเลือกเรียนเรื่องที่ตนสนใจก็ได้ และเมื่อได้ผ่านการทดสอบแล้วก็จะได้รับเครื่องหมายซึ่งนำมาประดับกับเครื่องแบบ เป็นการเชิดชูเกียรติและแสดงสมรรถภาพของตนส่วนหนึ่ง

4) กิจกรรมโดยเฉพาะกิจกรรมกลางแจ้ง เช่น เดินทางไกล อยู่ค่ายพักแรม

5) การเล่น (เกมต่างๆ)

6) การร้องเพลงและการชุมนุมรอบกองไฟ

3.1.6 วิธีการของลูกเสือ

เป็นระบบวิธีการศึกษาด้วยตนเอง โดยมีรายละเอียด ดังนี้

1) คำปฏิญาณและกฎ ปัจจัยอันแรกของวิธีการลูกเสือ คือ “คำปฏิญาณและกฎ”ในคำปฏิญาณนั้น เยาวชนแต่ละคนผู้เป็นสมาชิกของขบวนการลูกเสือต่างให้คำมั่นส่วนตัวเขาด้วยจิตใจอันเป็นอิสรเสรี ที่จะปฏิบัติตามข้อบังคับที่กำหนดไว้ในคำปฏิญาณและกฎนั้น ทั้งเขายอมรับเอาไว้ต่อหน้ากลุ่มเพื่อนฝูงของเขา เขารับว่าจะปฏิบัติตามคำของข้อบังคับนั้นด้วยความบริสุทธิ์ใจ การที่เขายอมรับเช่นนี้มีผลในทางค่านิยมและธรรมจริยา และการยอมรับที่จะดำรงชีวิตอยู่ตามอุดมการณ์นั้นอย่างเต็มความสามารถ คำปฏิญาณและกฎจึงเป็นเครื่องมืออันสำคัญยิ่งในการพัฒนาเยาวชน

2) การเรียนรู้ด้วยการกระทำเป็นปัจจัยอันที่สองของวิธีการลูกเสือ วิธีนี้สืบเนื่องมาจากการศึกษาภาคปฏิบัติ (ACTIVE EDUCATION) วิธีการเรียนรู้ด้วยการกระทำนี้ได้กลายเป็นวิธีการสำคัญในการศึกษาแผนปัจจุบัน สำหรับท่านผู้ให้กำเนิดลูกเสือโลกนั้น ท่านได้กล่าวย้ำเสมอว่า “เด็กพร้อมที่จะทำมากกว่าที่จะฟัง” การเรียนรู้ด้วยการกระทำนั้นอาจมาในรูปการสังเกต การทดลอง การกระทำด้วยตนเอง กำหนดการใดที่ได้จัดทำขึ้นโดยไม่มีแนวทางที่จะให้เยาวชนได้เรียนรู้ด้วยการกระทำแล้ว กำหนดการนั้นมิอาจยอมรับได้ว่าเป็นกำหนดการของลูกเสือ (SCOUT PROGRAM)

3) การเป็นสมาชิกในกลุ่มเล็ก (ระบบหมู่) ปัจจัยที่สามของวิธีการลูกเสือเป็นที่ยอมรับกันแล้วว่า การเป็นสมาชิกในกลุ่มที่มีบุคคลเท่าเทียมกัน ความสัมพันธ์ คุ้นเคยกันย่อมเกิดขึ้นตั้งแต่

ระยะแรก ทุกคนในกลุ่มจะเข้าใจกันเอง มีความรู้จักซึ่งกันและกันอย่างดี ทั้งมีความรู้สึกเป็นอิสระเสรี การบังคับปกครองของสังคมก็เกิดขึ้นเอง ทุกคนปฏิบัติตามวัตถุประสงค์ของกลุ่ม สิ่งเหล่านี้เป็นบรรยากาศอันเหมาะสมสำหรับเยาวชนที่จะพัฒนาตนเองไปสู่การเป็นผู้ใหญ่ต่อไป การปฏิบัติงานในกลุ่มจะให้โอกาสเยาวชนได้เรียนรู้ ได้ค้นคว้าอย่างก้าวหน้ายอมรับความคิดเห็นของผู้อื่น มีความรับผิดชอบ เยาวชนได้ฝึกหัดปกครองตนเองอีก ด้วย ในขบวนการนี้บทบาทของผู้กำกับ คือ การแนะแนวให้คำปรึกษาเท่านั้น ไม่ควรใช้บทบาทควบคุม

4) กำหนดการที่ก้าวหน้าและเร่งเร้าใจ เป็นปัจจัยที่สี่เกี่ยวกับกำหนดการของลูกเสือควรจัดในแง่ของการค้นคว้า เพื่อส่งเสริมการพัฒนาเยาวชนตามขั้นตอนทีละน้อย มีความกลมกลืนกันไป เครื่องมืออันหนึ่งที่ก่อให้เกิดความก้าวหน้า คือ การทดสอบในระบบเครื่องหมายวิชาพิเศษ กำหนดการนั้นควรเป็นสิ่งที่เร่งเร้าใจ และเชิญชวน กำหนดการควรประกอบด้วย กิจกรรมหลายอย่างแตกต่างกัน รวมกันเข้าด้วยความสมดุล ได้สัดส่วน และกิจกรรมเหล่านั้นสนองความต้องการ

3.2 คำปฏิญาณและกฎของลูกเสือ

ปัจจัยอันแรกของวิธีการลูกเสือ คือ **“คำปฏิญาณและกฎ”** ในคำปฏิญาณนั้น เยาวชนแต่ละคนผู้เป็นสมาชิกของขบวนการลูกเสือ ต่างให้คำมั่นส่วนตัวเขาด้วยจิตใจอันเป็นอิสรเสรี ที่จะปฏิบัติตามข้อบังคับที่กำหนดไว้ในคำปฏิญาณและกฎนั้น ทั้งเขายอมรับเอาไว้ต่อหน้ากลุ่มเพื่อนฝูงของเขา เขารับว่าจะปฏิบัติตามคำของข้อบังคับนั้นด้วยความบริสุทธิ์ใจ การที่เขายอมรับเช่นนี้มีผลในทางค่านิยม และธรรมจริยา และยอมรับที่จะดำรงชีวิตอยู่ตามอุดมการณ์นั้นอย่างเต็มความสามารถ คำปฏิญาณและกฎจึงเป็นเครื่องมืออันสำคัญยิ่งในการพัฒนาเยาวชน

3.2.1 คำปฏิญาณของลูกเสือ

คำปฏิญาณ คือ คำมั่นสัญญาที่ลูกเสือได้ให้ไว้แก่ผู้บังคับบัญชาต่อหน้าแถวในพิธีเข้าประจำกอง หรือพิธีการของลูกเสือด้วยความจริงใจหรือสมัครใจ โดยมีเนื้อความ ดังนี้

ด้วยเกียรติของข้า ข้าสัญญาว่า

ข้อ 1 ข้าจะจงรักภักดีต่อชาติ ศาสนา พระมหากษัตริย์

ข้อ 2 ข้าจะช่วยเหลือผู้อื่นทุกเมื่อ

ข้อ 3 ข้าจะปฏิบัติตามกฎของลูกเสือ [8]

ความหมายของคำปฏิญาณ

ข้อ 1 ข้าจะจงรักภักดีต่อชาติ ศาสนา พระมหากษัตริย์

ความหมาย : ลูกเสือจะต้องมีความศรัทธา เชื่อมั่นในชาติ ศาสนา และพระมหากษัตริย์ของตน เคารพ เทิดทูนทั้ง 3 สถาบันด้วยความซื่อสัตย์

ข้อ 2 ข้าจะช่วยเหลือผู้อื่นทุกเมื่อ

ความหมาย : ลูกเสือจะต้องประพฤติปฏิบัติตนให้เป็นประโยชน์ต่อผู้อื่นในทุก

โอกาส ทุกสถานการณ์ เท่าที่จะทำได้ โดยเริ่มตั้งแต่ครอบครัว จนถึงสังคมภายนอก

ข้อ 3 ข้าจะปฏิบัติตามกฎของลูกเสือ

ความหมาย : ลูกเสือต้องปฏิบัติตนตามกฎ 10 ข้อของลูกเสือซึ่งเป็นหลักยึดเหนี่ยวให้ลูกเสือปฏิบัติแต่สิ่งดีงาม

3.2.2 กฎของลูกเสือ

กฎ คือ ข้อกำหนดสำหรับเป็นแนวทางให้ลูกเสือนำไปปฏิบัติในชีวิตประจำวันจนเกิดเป็นนิสัยประจำตัว โดยกฎของลูกเสือมี 10 ข้อ ดังนี้

ข้อ 1 ลูกเสือมีเกียรติเชื่อถือได้

ข้อ 2 ลูกเสือมีความจงรักภักดีต่อชาติ ศาสนา พระมหากษัตริย์ และซื่อตรงต่อผู้มีพระคุณ

ข้อ 3 ลูกเสือมีหน้าที่กระทำตนให้เป็นประโยชน์และช่วยเหลือผู้อื่น

ข้อ 4 ลูกเสือเป็นมิตรของคนทุกคนและเป็นพี่น้องกับลูกเสืออื่นทั่วโลก

ข้อ 5 ลูกเสือเป็นผู้สุภาพเรียบร้อย

ข้อ 6 ลูกเสือมีความเมตตากรุณาต่อสัตว์

ข้อ 7 ลูกเสือเชื่อฟังคำสั่งของบิดา มารดา และผู้บังคับบัญชาด้วยความเคารพ

ข้อ 8 ลูกเสือมีใจร่าเริง ไม่ย่อท้อต่อความยากลำบาก

ข้อ 9 ลูกเสือเป็นผู้มัธยัสถ์

ข้อ 10 ลูกเสือประพฤติชอบด้วยกาย วาจา ใจ [9]

ความหมายของกฎลูกเสือ

ข้อ 1 ลูกเสือมีเกียรติเชื่อถือได้

ความหมาย : ลูกเสือจะต้องยึดมั่นในความซื่อสัตย์ ปฏิบัติตามคำมั่นสัญญา กระทำตนให้เป็นที่เชื่อถือและไว้วางใจได้

ข้อ 2 ลูกเสือมีความจงรักภักดีต่อชาติ ศาสนา พระมหากษัตริย์ และซื่อตรงต่อผู้มีพระคุณ

ความหมาย : ลูกเสือจะปกป้องสถาบันชาติ ศาสนา พระมหากษัตริย์ และยึดมั่นในความซื่อสัตย์ กตัญญูต่อผู้มีพระคุณทุกท่าน

ข้อ 3 ลูกเสือมีหน้าที่กระทำตนให้เป็นประโยชน์และช่วยเหลือผู้อื่น

ความหมาย : ลูกเสือจะต้องพร้อมอยู่เสมอที่จะบำเพ็ญประโยชน์ และเป็นที่พึ่งแก่ผู้อื่นได้

ข้อ 4 ลูกเสือเป็นมิตรของคนทุกคน และเป็นพี่น้องกับลูกเสืออื่นทั่วโลก

ความหมาย : ลูกเสือจะต้องมีใจโอบอ้อมอารี มีความเอื้อเฟื้อเผื่อแผ่แก่ทุกคน

โดยไม่เลือกเชื้อชาติ ศาสนา และปฏิบัติต่อเขาเหมือนญาติพี่น้อง

ข้อ 5 ลูกเสือเป็นผู้สุภาพเรียบร้อย

ความหมาย : ลูกเสือจะต้องเป็นผู้มีกิริยาวาจาสุภาพ อ่อนโยน อ่อนน้อม มีความสัมมาคารวะต่อบุคคลทั่วไป

ข้อ 6 ลูกเสือมีความเมตตากรุณาต่อสัตว์

ความหมาย : ลูกเสือจะต้องมีใจเมตตากรุณา สงสารสัตว์ ไม่รังแกหรือทรมานสัตว์ หรือเมื่อพบสัตว์บาดเจ็บต้องให้การช่วยเหลือ

ข้อ 7 ลูกเสือ เชื่อฟังคำสั่งของบิดา มารดาและผู้บังคับบัญชาด้วยความเคารพ

ความหมาย : ลูกเสือจะต้องปฏิบัติตามคำสั่งสอน คำชี้แนะของบิดามารดา ครูอาจารย์ และผู้บังคับบัญชาด้วยความเต็มใจและเคารพ

ข้อ 8 ลูกเสือมีใจร่าเริง ไม่ย่อท้อต่อความยากลำบาก

ความหมาย : ลูกเสือจะต้องมีความร่าเริง ยิ้มแย้มแจ่มใสอยู่เสมอ ถึงแม้จะตกอยู่ในความยากลำบาก ก็จะไม่แสดงอาการย่อท้อให้เห็น

ข้อ 9 ลูกเสือเป็นผู้มัธยัสถ์

ความหมาย : ลูกเสือจะต้องรู้จักประหยัดทรัพย์ทั้งของตนเองและผู้อื่น ไม่สุรุ่ยสุร่าย

ข้อ 10 ลูกเสือประพฤติชอบด้วยกาย วาจา ใจ

ความหมาย : ลูกเสือจะต้องรู้จักสำรวม และระวังกาย วาจา ใจ ไม่ให้มีความอิจฉาริษยา มีความบริสุทธิ์ใจต่อทุกคน

4. ระบบหมู่และการฝึกอบรมนายหมู่ลูกเสือ

4.1 ระบบหมู่ลูกเสือ

ระบบหมู่ลูกเสือ คือระบบการทำงาน การปฏิบัติภารกิจของสมาชิกในหมู่-กอง-กลุ่ม เพื่อความก้าวหน้าของส่วนรวม ด้วยความเต็มใจและพอใจของสมาชิกทุกคนทางลูกเสือนั้น สมาชิกหลายคนรวมกันเป็นหมู่ หลายหมู่รวมกันเป็นกอง หลายกองรวมกันเป็นกลุ่ม ผู้กำกับกลุ่มจะรับผิดชอบดูแลลูกเสือทุกกอง ทุกกลุ่ม ทุกคน ผู้กำกับก็จะดูแลเพียงทุกหมู่ในกอง และลูกเสือทุกคนในกอง รวมทั้งนายหมู่ทุกคนด้วย ส่วนนายหมู่จะดูแลเพียงสมาชิกภายในหมู่ของตนเอง เป็นการกระจายอำนาจ และแบ่งหน้าที่กันรับผิดชอบตามระบอบประชาธิปไตยโดยหมู่ลูกเสือสำรองจะมี 4-5 คน หมู่ลูกเสือสามัญมี 6-8 คน หมู่ลูกเสือสามัญรุ่นใหญ่มี 4-8 คนและหมู่ลูกเสือวิสามัญจะมี 4-6 คน การที่กำหนดเช่นนี้ได้กำหนดตามวัยและคำนึงถึงพลังตามกลุ่มของช่วงวัยต่างๆ

4.2 การฝึกอบรมนายหมู่ลูกเสือ

เมื่อบุคคลจำนวนหนึ่งมารวมกันเพื่อประกอบกิจการอย่างหนึ่งอย่างใด บุคคลเหล่านั้นมีความต้องการใครคนหนึ่งมาเป็นหัวหน้าหรือผู้นำ เพื่อเขาเหล่านั้นจะได้ช่วยกันทำงานนั้นให้ลุล่วงไปสู่จุดแห่งความสำเร็จผลดังที่ตั้งใจไว้

ตามข้อบังคับลักษณะปกครอง ฯ ของคณะลูกเสือแห่งชาติ กองลูกเสือวิสามัญกองหนึ่งจะมีลูกเสือวิสามัญตั้งแต่ 20 คน ถึง 30 คน หรือ 10 คน ถึง 60 คน อย่างมาก มีผู้กำกับคนหนึ่ง รองผู้กำกับ 1-2 คน ในกองลูกเสือวิสามัญแต่ละกองจะแบ่งลูกเสือออกเป็นหมู่ ๆ ละ 4 ถึง 6 คน ในจำนวนนี้มีนายหมู่ 1 คน และรองนายหมู่ 1 คน รวมอยู่ด้วย

แต่ละหมู่เลือกใครคนหนึ่งจากสมาชิกของหมู่เป็นนายหมู่หรือหัวหน้า บุคคลที่เลือกขึ้นมาเป็นนายหมู่นั้น ควรเป็นบุคคลที่พร้อมจะรับผิดชอบในการบริหารธุรกิจของหมู่ ระยะเวลาการเป็นนายหมู่ช่วงหนึ่งไม่ควรเกิน 1 ปี เพื่อที่จะให้สมาชิกในหมู่ได้มีโอกาสเป็นนายหมู่เป็นจำนวนหลายคน เพื่อเป็นการฝึกหัดการเป็นผู้นำ แต่อย่างไรก็ตามหมู่อาจกำหนดเงื่อนไขเรื่องระยะเวลาเป็นอย่างอื่นก็ได้

ผู้ที่จะได้รับเลือกเป็นนายหมู่ ควรเป็นผู้ที่ได้ผ่านการฝึกอบรมหลักสูตรนายหมู่ลูกเสือวิสามัญมาแล้ว ความรับผิดชอบของนายหมู่ลูกเสือวิสามัญมีมาก แต่ความสุขใจที่จะเกิดขึ้นจากการได้ปฏิบัติภารกิจที่เพื่อน ๆ ไว้วางใจ และมอบหมายให้ทำนั้นมีมากมายเช่นกัน

4.2.1 ภารกิจของนายหมู่ลูกเสือ

1) นายหมู่เป็นผู้นำของหมู่ มีหน้าที่บริหารและรับผิดชอบธุรกิจต่าง ๆ ของหมู่ลูกเสือวิสามัญ และเป็นประธานในที่ประชุมหมู่

2) จัดและปฏิบัติพิธีการต่าง ๆ เกี่ยวกับหมู่

3) แบ่งงานและธุรการให้กับสมาชิกในหมู่โดยทั่วถึงกัน และระบุงานในแต่ละหน้าที่ให้ชัดแจ้ง

4) ดูแลให้เป็นที่แน่ชัดว่ามาตรฐานที่ได้กำหนดให้สมาชิกแต่ละคนทำนั้น สมาชิกได้ปฏิบัติตามนั้นจริง และงานที่แบ่งให้ทำได้รับผลสำเร็จดี

5) ทำทะเบียนสมาชิกของกลุ่ม แสดงความสำเร็จ และความก้าวหน้าในการเรียนการฝึกอบรมของสมาชิกแต่ละคน

6) เป็นผู้แทนหมู่ไปร่วมประชุมในกองลูกเสือวิสามัญ และในการประชุมอื่น

7) ส่งเสริมความสามัคคีของหมู่ ทำให้สมาชิกในหมู่อยู่และทำงานร่วมกันอย่างมีความสงบสุข และได้ผลดี

8) นายหมู่ไม่ควรหวังความสำเร็จอันดีเยี่ยมจากงานการที่มอบให้สมาชิกทำ แต่เวลาเดียวกันไม่ควรจะพอใจในผลงานที่ทำให้แล้วเสร็จอย่างเสียไม่ได้ แต่ทั้งนี้พึงงดเว้นการกล่าวตำหนิต่อหน้าผู้อื่น ควรพูดจากันสองต่อสอง [10]

5. บทบาทหน้าที่และพิธีการเข้าประจำหน่วยของลูกเสือไซเบอร์

5.1 บทบาทหน้าที่ของลูกเสือไซเบอร์

การสร้างลูกเสือไซเบอร์เป็นจุดเริ่มต้นของการสร้างความตระหนักในการใช้เทคโนโลยีสารสนเทศและการสื่อสารบนโลกออนไลน์อย่างรู้เท่าทันสร้างสรรค์ มีคุณธรรมและจริยธรรม เพื่อร่วมกันทำหน้าที่ดังต่อไปนี้

1) เฝ้าระวังข้อมูลข่าวสารที่เป็นภัยต่อสถาบันชาติ ศาสนา และ พระมหากษัตริย์

2) เป็นแบบอย่างในการส่งเสริมการใช้งานอินเทอร์เน็ตอย่างเหมาะสมแก่เครือข่ายทางสังคม

3) ขยายเครือข่ายอาสาสมัครลูกเสือไซเบอร์ที่มีจิตสำนึกด้านคุณธรรมด้านจริยธรรมในการใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ICT) อย่างสร้างสรรค์และสามารถป้องกันตนเองจากภัยในโลกออนไลน์

4) สร้างความตระหนักในการใช้ข้อมูลสารสนเทศให้เกิดความมั่นคง

5) สามารถถ่ายทอดองค์ความรู้ที่ได้สร้างความเข้มแข็งให้กับชุมชนและสังคม เพื่ออนาคตอย่างยั่งยืน

5.2 พิธีการเข้าประจำหน่วยของลูกเสือไซเบอร์

พิธีการเข้าประจำหน่วยของลูกเสือไซเบอร์ ปฏิบัติคล้ายคลึงกับพิธีเข้าประจำกองลูกเสือหรือที่เรียกว่าพิธีปฏิญาณตน โดยให้ปฏิบัติดังต่อไปนี้

พิธีสำรวจตัวเองก่อนเข้าประจำกองลูกเสือวิสามัญ

เมื่อเตรียมลูกเสือวิสามัญได้รับการฝึกอบรมเครื่องหมายลูกเสือโลกครบตามหลักสูตรแล้ว ให้ผู้กำกับลูกเสือวิสามัญในกองนั้นๆ ดำเนินการจัดให้เตรียมลูกเสือวิสามัญเหล่านั้นเข้าพิธีประจำกองตามลำดับขั้นตอนต่างๆ ดังนี้ คือ

1) จัดให้มีพิธีเข้าประจำกองในตอนกลางคืน ควรจะเริ่มตั้งแต่เวลา 19.30 น.เป็นต้นไป จนกว่าจะเสร็จพิธีเข้าประจำกองลูกเสือวิสามัญ

2) ผู้เข้ารับการฝึกอบรมซึ่งเปรียบเสมือนลูกเสือวิสามัญ แต่งเครื่องแบบครบเรียบร้อยเข้านั่งที่ที่จัดไว้ อันเป็นที่นั่งที่สบายพอสมควรและสงบเงียบ

3) ประธานในพิธีเข้าชี้แจงถึงวัตถุประสงค์ของการสำรวจตัวเอง ให้ทุกคนปฏิบัติด้วยศรัทธา สงบ จริงใจ และมีสมาธิที่แน่วแน่ ให้ถือว่าเป็นพิธีการ ไม่ใช่เรื่องทำเล่น ๆ หรือสนุกสนาน ทุกคนต้องสงบและสำรวมอย่างแท้จริง

4) หลังจากที่ประธานกล่าวถึงวัตถุประสงค์ในข้อ 3 แล้ว ประธานจะกล่าวปราศรัยถึงเกาะแก่งแห่งชีวิต ซึ่งจะเป็นตัวอุปสรรคขัดขวางมิให้การดำเนินชีวิตของคนเราดำเนินไปด้วยดี เกาะแก่งแห่งชีวิตดังกล่าว คือ อบายมุขต่าง ๆ ได้แก่ สุรา นารี ภาชี กีฬาบัตร ฯลฯ

5) กองลูกเสือวิสามัญได้เตรียมแผนการสำรวจตัวเองไว้ล่วงหน้าก่อนแล้ว โดยเขียนกฎลูกเสือ 10 ข้อ เพียงย่อๆ เช่น "มีเกียรติ" "ประพฤติชอบ" ลงบนก้อนหินที่มีขนาดโตหรือในกระดาษแผ่นโต สุดแต่กรณีเพื่อให้ผู้พบอ่านง่าย จำนวน 10 ก้อน ครบจำนวนกฎทั้ง 10 ข้อ แล้วนำก้อนหินหรือกระดาษตอกติดเสา ไปตั้งไว้ในป่า (หากมี) หรือรอบๆ สนาม โดยวางให้ห่างๆ กันตามลำดับกฎข้อ 1-10 ระยะทางที่วางให้วกวนพอสมควร (สิ่งต่างๆ ดังกล่าวในข้อนี้ต้องเตรียมไว้ก่อนล่วงหน้าในตอนเย็นของวันสำรวจตัวเอง) พร้อมทั้งกำหนดตัวบุคคลจำนวน 11 คน ไว้ประจำจุดทั้ง 10 จุด รวมทั้งผู้ที่จะกล่าวสรุปอีก 1 คน อยู่รวมกับกฎข้อที่

10 ทั้งนี้ผู้ประจำตามจุดทั้ง 10 ต้องมีไฟฉายติดตัวด้วย เพื่อไว้อ่านข้อความซึ่งอธิบายความหมายของกฎลูกเสือได้ และอย่าลืมว่าตามจุดต่างๆ ดังกล่าว ต้องมีตะเกียงจุดตั้งไว้เพื่อแสดงจุดที่ตั้งด้วย เพราะลูกเสือจะต้องเดินผ่านโดยมี ผู้กำกับนำทางไป เมื่อลูกเสือได้ฟังเรื่อง "อบายมุข" จบแล้ว

6) ผู้กำกับหรือรองผู้กำกับคนหนึ่ง จะเป็นผู้พากองลูกเสือออกเดินทางไปในระหว่างความมืด ซึ่งเปรียบเสมือนผ่านวิธีทางแห่งชีวิตลูกเสือ โดยเรียกแถวลูกเสือให้อยู่ในรูปแถวตอนหมู่ (ตอนลึก) เมื่อเรียบร้อยแล้วถือไฟฉายเดินนำลูกเสือไปช้าๆ ทุกคนอยู่ในภาวะสงบ ไม่พูด ไม่คุยสิ่งใดทั้งสิ้น และเดินตามผู้นำไป เมื่อถึงกฎข้อ 1 ให้ผู้นำแถวให้สัญญาณด้วยไฟฉายแก่ผู้ประจำฐาน ซึ่งซ่อนตัวอยู่ไม่ให้ลูกเสือเห็น อ่านข้อความของกฎข้อ 1 และคำสอนประกอบดัง ๆ และช้า ๆ ด้วยเสียงที่หนักแน่น ในท่ามกลางความมืดอันสงบเงียบนั้น เมื่อจบข้อความแล้วผู้นำแถวก็นำลูกเสือผ่านฐานต่อไปตามลำดับจนครบกฎข้อ 10 และแล้วตอนท้ายสุดจะมีผู้กล่าวสรุปกฎทั้ง 10 ข้อ อีกครั้งหนึ่ง

7) หลังจากการกล่าวสรุปแล้ว ผู้นำแถวจึงนำแถวไปสู่ลานกว้างอีกแห่งหนึ่ง ซึ่งมีโต๊ะหมู่บูชาตั้งอยู่พร้อมแล้ว ผู้นำแถวเชิญประธานจุดธูปเทียนบูชาพระรัตนตรัย ผู้นำแถวและลูกเสือยืนพนมมือเสร็จแล้ว ผู้นำแถวมอบเทียน - ไม้ขีดไฟ พร้อมทั้งคำสำรวจตัวเอง (ข้อบังคับฯ ข้อ 297) ให้ลูกเสือทุกคน ลูกเสือแต่ละคนเมื่อรับของดังกล่าวแล้ว ให้แยกกันไปหาที่นั่ง ที่จุดใดจุดหนึ่งในบริเวณนั้น ต่างคนต่างนั่งให้ห่างกัน เสมือนนั่งอยู่โดดเดี่ยวแล้วพิจารณาตัวเองตามข้อความทั้ง 21 ข้อ ในแผ่นกระดาษคำสำรวจตัวเองที่ได้รับแจกมา หากมีข้อใดที่ไม่อาจปฏิบัติได้หรือยากแก่การปฏิบัติ ให้พิจารณาสำรวจตัวเองในข้อนั้นนาน ๆ อีกครั้งหนึ่ง หากยังถือปฏิบัติไม่ได้เช่นเดิม ลูกเสือผู้นั้นมีสิทธิ์เดินออกไปจากลูกเสือบริเวณที่สำรวจตัวเองได้ และไม่มีสิทธิ์ที่จะเข้าร่วมพิธีประจำกองลูกเสือวิสามัญในวันนั้น จนกว่าลูกเสือผู้นั้นจะผ่านการสำรวจตัวเองทุกข้อ จึงจะเข้าพิธีประจำกองลูกเสือวิสามัญได้ในวันต่อไป

8) เมื่อผู้นำแถวเห็นว่าลูกเสือได้กระทำการสำรวจตัวเองเรียบร้อยแล้วให้นำลูกเสือเข้าสู่สถานที่ที่จะประกอบพิธีเข้าประจำกองลูกเสือวิสามัญ และติดแถบสามสีต่อไป สถานที่ที่จะประกอบพิธีเข้าประจำกองลูกเสือวิสามัญ ควรจะเป็นคูหาลูกเสือวิสามัญหรือพุทธศาสนา หรือโบสถ์ ซึ่งเป็นสถานที่สงบเงียบ ต่อจากนั้น กองลูกเสือวิสามัญทำพิธีเข้าประจำกอง ตามข้อบังคับคณะลูกเสือแห่งชาติ เมื่อลูกเสือได้ติดแถบสามสีเรียบร้อยแล้ว ผู้กำกับกล่าวให้โอวาท ลูกเสือเก่า (ถ้ามี) หรือผู้กำกับลูกเสือจับมือแสดงความยินดี เป็นอันเสร็จพิธี

พิธีเข้าประจำกองลูกเสือวิสามัญ ให้ปฏิบัติดังต่อไปนี้

นำเตรียมลูกเสือวิสามัญในเครื่องแบบมายืนอยู่ข้างหน้ากองลูกเสือวิสามัญ และอยู่ระหว่างพี่เลี้ยงสองคน มีโต๊ะพิธีซึ่งปูด้วยธงชาติ ผู้กำกับยืนด้านหนึ่งของโต๊ะพิธีหันหน้าเข้าหาลูกเสือที่จะเข้าประจำกองแล้วเรียกชื่อผู้ที่จะเข้าพิธี และถามดังนี้

ผู้กับกับเรียกชื่อผู้สมัคร	"เจ้ามาที่นี่เพื่อที่จะเข้าเป็นลูกเสือวิสามัญในคณะพี่น้องลูกเสือแห่งโลกอันยิ่งใหญ่หรือ"
ผู้สมัครใหม่	"ครับ / ค่ะ"
ผู้กับกับลูกเสือวิสามัญ	"ถึงแม้ว่าเจ้าจะมีข้อยุ่งยากมาบ้างแล้วในอดีต แต่บัดนี้ เจ้าก็ได้ตั้งใจที่จะทำให้ดีที่สุดเพื่อเป็นผู้มีเกียรติ มีสัจจะ มีความซื่อตรงในการงานทั้งปวง พร้อมที่จะปฏิบัติชอบด้วยกาย วาจา ใจ ใช่หรือไม่"
ผู้สมัครใหม่	"ใช่ครับ / ใช่ค่ะ"

ผู้กับกับลูกเสือวิสามัญ "เจ้าได้คิดรอบคอบดีแล้วหรือว่า เจ้าพร้อมที่จะเข้าเป็นลูกเสือวิสามัญ"

ผู้สมัครใหม่ "ข้าได้คิดรอบคอบดีแล้ว"

ผู้กับกับลูกเสือวิสามัญ "เจ้าเข้าใจหรือไม่ว่าคำว่า "บริการ" นั้นหมายความว่า ตลอดเวลาเจ้าจะต้องมีใจหนักแน่น ต่อผู้อื่นทุกคนและเจ้าจะทำดีที่สุดเพื่อช่วยเหลือผู้อื่น ถึงแม้ว่าการช่วยเหลือนั้นไม่สะดวก หรือไม่เป็นที่พอใจ หรือไม่เป็นที่ปลอดภัยแก่ตัวเองและเจ้าจะไม่หวังสิ่งตอบแทนใด ๆ ในการให้บริการนั้น"

ผู้สมัครใหม่ "ข้าเข้าใจดีแล้ว"

ผู้กำกับลูกเสือวิสามัญ ข้าขอให้เจ้า ล้างมือในอ่างน้ำ เพื่อเป็นการแสดงว่า เจ้าได้ชำระจิตใจให้ใสสะอาด ปราศจากข้อเศร้าหมองทั้งปวง อันเป็นเครื่องบัดทอน ความก้าวหน้าในชีวิตการเป็นลูกเสือวิสามัญของเจ้า เจ้าจะทำหรือไม่

ผู้สมัครใหม่ *ก้าวมาที่โต๊ะพิธี ล้างมือทั้งสอง ในอ่างน้ำ หยิบหินในอ่างน้ำ 1 ก้อน เก็บใส่กระเป๋าเสื้อ เช็ดมือที่ผ้า แล้วกลับไปยืนที่เดิม*

ผู้กับกับลูกเสือวิสามัญ "เจ้าเข้าใจดีหรือไม่ว่า การที่จะเป็นลูกเสือวิสามัญนั้น เจ้ากำลังจะร่วมอยู่ในคณะลูกเสือที่ต้องการจะช่วยเหลือเจ้า ให้สามารถปฏิบัติตามอุดมคติของเจ้า และเราขอให้เจ้าปฏิบัติตามข้อบังคับและคติพจน์ของเรา ในเรื่องการให้บริการแก่ผู้อื่น"

ผู้สมัครใหม่ "ข้าเข้าใจดีแล้ว"

ผู้กับกับลูกเสือวิสามัญ "ถ้าเช่นนั้น ข้อขอให้เจ้ากล่าวคำปฏิญาณของลูกเสือ และพึงเข้าใจได้ด้วยว่า เจ้าแปลความหมายของคำปฏิญาณนี้ ไม่ใช่อย่างเด็ก แต่จะแปลอย่างผู้ใหญ่"
ลูกเสือก้าวออกมาข้างหน้า เอามือซ้ายจับธง มือขวาแสดงรหัส
ลูกเสือในกองลูกเสือวิสามัญทุกคนแสดงรหัส

ผู้สมัครใหม่ "ด้วยเกียรติของข้า ข้าสัญญาว่า"
ข้อ 1 ข้าจะจงรักภักดีต่อชาติ ศาสนา พระมหากษัตริย์
ข้อ 2 ข้าจะช่วยเหลือผู้อื่นทุกเมื่อ
ข้อ 3 ข้าจะปฏิบัติตามกฎของลูกเสือ

ผู้กำกับลูกเสือวิสามัญ "ข้าฯ เชื่อเจ้าว่าด้วยเกียรติของเจ้า เจ้าจะปฏิบัติตามคำปฏิญาณที่เจ้าให้ไว้แล้ว"
ผู้กำกับลูกเสือวิสามัญ ติดแถบที่ไหล่แก่ลูกเสือวิสามัญ [11]

บรรณานุกรมประจำบทที่1

[1] สุชาติ กลศาสตร์เสนี, ประวัติลอร์ด โรเบิร์ต เบเดน-โพเอลล์, หน้า 1-14.

[2] พระราชบัญญัติลูกเสือ พ.ศ. 2551.

[3] ที่ประชุมเชิงปฏิบัติการเพื่อการจัดทำแผนยุทธศาสตร์และหลักสูตรในการดำเนินงานโครงการสร้างลูกเสือบนเครือข่ายอินเทอร์เน็ต (Cyber Scout) ประจำปีงบประมาณ 2556 ระหว่างวันที่ 2-5 เมษายน 2556 ณ โรงแรมรามาการ์เด้นส์ ถ.วิภาวดีรังสิต.

[4] สุชาติ กลศาสตร์เสนี, ประวัติลอร์ด โรเบิร์ต เบเดน-โพเอลล์, หน้า 1-14.

[5] วรรณภา พรหมถาวร และคณะ, 2552, ประวัติลูกเสือไทย พ.ศ. 2454-2552, โรงพิมพ์ลาดพร้าว, กรุงเทพฯ, หน้า 7-16.

[6] ราชกิจจานุเบกษา: 2453, หน้า 2562.

[7] วรรณภา พรหมถาวร และคณะ, 2552, ประวัติลูกเสือไทย พ.ศ. 2454-2552, โรงพิมพ์ลาดพร้าว, กรุงเทพฯ, หน้า 7-16.

[8] Thai Thip Group, 2548, คำปฏิญาณของลูกเสือสามัญ ลูกเสือสามัญรุ่นใหญ่ และลูกเสือวิสามัญ [Online], Available : http://www.thaiscouts.com/scout/rule.html [1 สิงหาคม 2556].

[9] Thai Thip Group, 2548, กฎของลูกเสือสามัญ ลูกเสือสามัญรุ่นใหญ่ และลูกเสือวิสามัญ [Online],Available : http://www.thaiscouts.com/scout/rule.html [1 สิงหาคม 2556].

[10] www.krutujao.com/word/039.botbaat%20visaman.doc [1 สิงหาคม 2556].

[11] http://school.obec.go.th/privatechon1/scoutweb/%BE%D4%B8%D5%E0%A2%E9%D2%BB%C3%D0%A8%D3%A1%CD%A7%C5%D9%A1%E0%CA%D7%CD%CA%D2%C1%D1%AD.doc [1 สิงหาคม 2556].

บทที่ 2 คุณธรรม จริยธรรมในการใช้เทคโนโลยีสารสนเทศและการสื่อสาร

2.1 คุณธรรม จริยธรรมในการใช้คอมพิวเตอร์

เทคโนโลยีสารสนเทศได้เข้ามามีส่วนเกี่ยวข้องกับมนุษย์ทุกคนไม่ทางตรงก็ทางอ้อม ผลกระทบของเทคโนโลยีสารสนเทศมีทั้งทางบวกและทางลบ ทางบวกทำให้มนุษย์มีความเป็นอยู่ดีช่วยส่งเสริมให้มีประสิทธิภาพในการทำงาน ทำให้เกิดการผลิตในอุตสาหกรรม ส่งเสริมให้เกิดกาค้นคว้าวิจัยสิ่งใหม่ ส่งเสริมสุขภาพและ ความเป็นอยู่ให้ดีขึ้น ทางลบทำให้เกิดอาชญากรรม ทำให้ความสัมพันธ์ของมนุษย์เสื่อมถอย ทำให้เกิดการเสี่ยงภัยทางด้านธุรกิจ ธุรกิจในปัจจุบันจำเป็นต้องพึ่งพาอาศัยเทคโนโลยีสารสนเทศมากขึ้น ข้อมูลข่าวสารของธุรกิจฝากไว้ในศูนย์ข้อมูล หากข้อมูลเกิดการสูญหาย ย่อมทำให้เกิดผลกระทบต่อธุรกิจโดยตรง คอมพิวเตอร์เป็นอุปกรณ์ที่ทำงานตามคำสั่ง การนำมาใช้ในทางใดจึงขึ้นอยู่กับผู้ใช้ จริยธรรมการใช้คอมพิวเตอร์จึงเป็นเรื่องสำคัญที่จะต้องปลูกฝังให้กับผู้ใช้คอมพิวเตอร์ เพื่อให้รู้จักการใช้งานที่เหมาะสม ในเรื่องการใช้เทคโนโลยีสารสนเทศก็จำเป็นต้องปลูกฝังเช่นเดียวกัน เพื่อให้ผู้ใช้นำไปใช้งานที่เป็นประโยชน์เชิงสร้างสรรค์หรือทางบวก

ปัจจุบันมีผู้ใช้งานอินเทอร์เน็ตเป็นจำนวนมาก และมีจำนวนเพิ่มขึ้นทุกวัน เครือข่ายอินเทอร์เน็ตเป็นระบบออนไลน์ที่สามารถแลกเปลี่ยนข้อมูลซึ่งกันและกันได้ ในเครือข่ายย่อมมีผู้ประพฤติไม่ดีปะปนอยู่ ซึ่งก่อให้เกิดปัญหาต่อส่วนรวมอยู่เสมอ แต่ละเครือข่ายจึงได้ออกกฎเกณฑ์การใช้งานภายในเครือข่าย เพื่อให้สมาชิกในเครือข่ายของตนยึดถือและปฏิบัติตาม กฎเกณฑ์เหล่านี้จะช่วยให้สมาชิกโดยส่วนรวมได้รับประโยชน์สูงสุด และป้องกันปัญหาที่เกิดจากผู้ใช้บางคนได้

ดังนั้นผู้ใช้อินเทอร์เน็ตทุกคนจะต้องเข้าใจกฎเกณฑ์ ข้อบังคับของเครือข่ายที่ตนเองเป็นสมาชิก จะต้องมีความรับผิดชอบต่อตนเองและผู้ร่วมใช้บริการคนอื่น และจะต้องรับผิดชอบต่อการกระทำของตนเองที่เข้าไปขอใช้บริการต่างๆ บนเครือข่ายคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ที่ผู้ใช้อินเทอร์เน็ตใช้บริการอยู่ มิได้เป็นเพียงเครือข่ายขององค์กรที่ผู้ใช้เป็นสมาชิกอยู่เท่านั้น แต่เป็นเครือข่ายคอมพิวเตอร์ที่เชื่อมโยงเครือข่ายต่างๆ จำนวนมากเข้าไว้ด้วยกัน มีข้อมูลข่าวสารวิ่งอยู่ระหว่างเครือข่ายมากมาย การส่งข่าวสารลงในเครือข่ายนั้นอาจทำให้ข่าวสารกระจายไปยังเครือข่ายอื่นๆ เช่น การส่งจดหมายอิเล็กทรอนิกส์ฉบับหนึ่ง อาจจะต้องเดินทางผ่านเครือข่ายหลายเครือข่ายจนกว่าจดหมายฉบับนั้นจะเดินทางถึงปลายทาง ผู้ใช้อินเทอร์เน็ตจะต้องให้ความสำคัญและตระหนักถึงปัญหา ปริมาณข้อมูลข่าวสารที่วิ่งอยู่บนเครือข่าย แม้ผู้ใช้งานอินเทอร์เน็ตจะได้รับสิทธิ์จากผู้บริหารเครือข่ายให้ใช้บริการต่างๆ บนเครือข่ายนั้นได้ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่เครือข่ายนั้นวางไว้ด้วย ไม่พึงละเมิดสิทธิ์หรือกระทำการใดๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่แต่ละเครือข่ายวางไว้และจะต้องปฏิบัติตาม คำแนะนำอย่างเคร่งครัด

การใช้งานอินเทอร์เน็ตอย่างสร้างสรรค์และเป็นประโยชน์ จะทำให้สังคมอินเทอร์เน็ตเป็นสังคมที่น่าใช้และเป็นประโยชน์ ต่อส่วนรวม ผู้ใช้จะต้องหลีกเลี่ยงกิจกรรมบางอย่างที่ไม่ควรปฏิบัติ เช่น การส่งกระจายข่าวลือจำนวนมากบนเครือข่าย การกระจายข่าวแบบส่งกระจายไปยังปลายทางจำนวนมาก การส่งจดหมายลูกโซ่เป็นต้น กิจกรรมเหล่านี้จะเป็นผลเสียต่อส่วนรวม และไม่เกิดประโยชน์ใดๆ ต่อสังคมอินเทอร์เน็ต [1]

2.2 จรรยามารยาทการใช้งานเครือข่ายสังคมออนไลน์

Netiquette เป็นคำที่มาจาก “Network Etiquette” หมายถึง จรรยามารยาทของการอยู่ร่วมกันในสังคมอินเทอร์เน็ต หรือ Cyberspace ซึ่งเป็นพื้นที่ที่เปิดโอกาสให้ผู้คนเข้ามาแลกเปลี่ยน สื่อสาร และทำกิจกรรมร่วมกัน ชุมชนใหญ่บ้างเล็กบ้างบนอินเทอร์เน็ตนั้นก็ไม่ต่างจากสังคมบนโลกแห่งความเป็นจริง ซึ่งจำเป็นต้องมีกฎกติกา (Codes of Conduct) เพื่อใช้เป็นกลไกสำหรับการกำกับดูแลพฤติกรรมและการปฏิสัมพันธ์ของสมาชิก

จรรยามารยาทการใช้อินเทอร์เน็ต (Netiquette) คือ กิริยาอาการที่พึงประพฤติปฏิบัติในการอยู่ร่วมกันอย่างสันติในสังคม กล่าวอีกนัยหนึ่ง คือ มารยาทอินเทอร์เน็ต คือ วิธีประพฤติตนที่เหมาะสมเมื่อใช้อินเทอร์เน็ต Netiquette มีดังต่อไปนี้

1. อย่าลืมว่าเรากำลังติดต่อกับคนที่มีตัวตนอยู่จริง ก่อนส่งอีเมลล์หรือโพสต์ข้อความอะไรบนอินเทอร์เน็ต ต้องถามตัวเองก่อนว่า ถ้าเจอกันต่อหน้าคุณจะพูดแบบนี้กับเขาหรือไม่ ถ้าคำตอบคือไม่ก็จงแก้ไขข้อความนั้นแล้วอ่านใหม่อีกครั้ง ทำแบบนี้ซ้ำๆ จนรู้สึกว่าไม่ลำบากใจที่จะพูดแบบนี้กับใครแล้วจึงค่อยส่ง

2. การสื่อสารออนไลน์ให้ยึดมาตรฐานความประพฤติเดียวกับการสื่อสารในชีวิตจริง คนส่วนใหญ่มักจะเคารพกฎหมายเพราะกลัวโดนจับ แต่ในโลกอินเทอร์เน็ตโอกาสถูกจับมีน้อย ก็จะปฏิบัติต่อกันโดยมีมาตรฐานทางศีลธรรมต่ำกว่าในโลกแห่งความเป็นจริง ถ้าอยากทำอะไรผิดกฎหมายใน Cyberspace สิ่งที่คุณกำลังจะทำนั้นก็น่าจะผิดด้วย

3. รู้ว่าคุณอยู่ที่ไหนใน Cyberspace การกระทำอะไรก็ตามอาจเป็นเรื่องยอมรับได้ในที่แห่งหนึ่ง แต่ถ้าเป็นที่แห่งอื่นๆ อาจจะไม่ใช่ ลองใช้เวลาสักพักสังเกตการณ์ก่อนว่า ที่นั่นเขาคุยอะไรกัน ปฏิบัติต่อกันอย่างไร หรือเข้าไปอ่านข้อความเก่าๆ จากนั้นค่อยเข้าไปมีส่วนร่วมกับเขา

4. เคารพเวลาและการใช้ Bandwidth ปัจจุบันดูเหมือนคนจะมีเวลาน้อยลงกว่าที่เคยเป็นมามากนัก เมื่อคุณส่งอีเมลล์หรือโพสต์ข้อความลงอินเทอร์เน็ต รู้ไว้ว่าคุณกำลังให้คนอื่นเสียเวลามาอ่าน ดังนั้นเป็นความรับผิดชอบที่คุณควรแน่ใจก่อนส่งว่า ข้อความหรืออีเมลล์นั้นไม่ทำให้ผู้รับเสียเวลา

5. สำหรับกระดานสนทนา ผู้ที่เข้ามาอ่านกระดานแบบนี้ส่วนใหญ่นั่งอยู่หน้าจอคอมพิวเตอร์นานเกินไป ไม่มีใครชอบถ้าต้องเสียเวลาทำทั้งหมดนั้นแล้ว พบว่าไม่เห็นจะคุ้มค่ากับเวลาที่เสียไป หากจะส่งข้อมูลอะไรไปให้ใคร ลองถามตัวเองดูก่อนว่าเขาจำเป็นจะต้องรู้เรื่องในอีเมลล์นั้นหรือไม่ ถ้าไม่ก็อย่าส่ง ถ้าอาจจะอยากรู้ก็ทบทวนก่อนส่ง

6. ทำให้ตัวเองดูดีเวลาออนไลน์ โลกอินเทอร์เน็ตก็เหมือนโลกแห่งความเป็นจริง คนที่สื่อสารกันในนั้นอยากให้คนอื่นชอบ แต่คุณไม่ต้องถูกตัดสินด้วย สีผิว, สีตา, สีผม น้ำหนัก, อายุ หรือการแต่งตัวของคุณ คุณจะถูกตัดสินผ่านคุณภาพของสิ่งที่คุณเขียน ดังนั้นการสะกดคำให้ถูกและเขียนให้ตรงตามหลักไวยากรณ์จึงเป็นเรื่องสำคัญ ควรรู้ว่าตัวเองกำลังพูดอะไรอยู่ และพูดอย่างมีเหตุมีผล

7. แบ่งปันความรู้ของผู้เชี่ยวชาญ จุดแข็งของ Cyberspace คือ มีผู้เชี่ยวชาญมากมายที่อ่านคำถามบนอินเทอร์เน็ต และถึงแม้ว่าจะมีส่วนน้อยมากในจำนวนนั้นที่ตอบคำถาม ความรู้โดยรวมของโลกก็เพิ่มขึ้นอยู่ดี แม้ว่ามารยาทการใช้อินเทอร์เน็ตจะมีข้อห้ามยาวเหยียด คุณก็มีความรู้ที่เป็นประโยชน์กับคนอื่น อย่ากลัวที่จะแบ่งปันในสิ่งที่คุณรู้

8 ช่วยกันควบคุมสงครามการใส่อารมณ์ เวลาที่ต้องการแสดงความคิดเห็นอย่างรุนแรง ควรรู้จักยับยั้งชั่งใจ หรือพยายามควบคุมอารมณ์ให้มาก

9. เคารพความเป็นส่วนตัวของผู้อื่น คุณไม่ควรไปเปิดอ่านอีเมลล์ของคนอื่น การไม่เคารพความเป็นส่วนตัวของผู้อื่นเป็นมารยาทการใช้อินเทอร์เน็ตที่ไม่ดี

10. อย่าใช้อำนาจในทางไม่สร้างสรรค์ การรู้มากกว่าคนอื่นหรือมีอำนาจมากกว่าไม่ได้แปลว่า คุณมีสิทธิที่จะเอาเปรียบคนอื่นได้ เช่น ผู้ดูแลระบบไม่ควรอ่านอีเมลล์ส่วนตัวของคนอื่น

11. ให้อภัยในความผิดพลาดของผู้อื่น ทุกคนเคยเป็นมือใหม่มาก่อน บางคนจึงทำผิดพลาดในแง่มารยาทการใช้อินเทอร์เน็ต จงใจเย็นเข้าไว้ ถ้าคุณตัดสินใจจะบอกคนที่ทำผิดมารยาทการใช้อินเทอร์เน็ต ก็จงบอกอย่างสุภาพและเป็นส่วนตัวดีกว่าไปป่าวประกาศให้คนอื่นรับรู้ด้วย จงให้โอกาสในความไม่รู้ของคนอื่น การประณามว่าผู้อื่นไม่มีมารยาทตรงๆ ก็มักจะเป็นตัวอย่างของมารยาทที่ไม่ดีเช่นกัน [2]

2.3 บัญญัติ 10 ประการในการใช้อินเทอร์เน็ต และเครือข่ายทางสังคม

บัญญัติ 10 ประการ เป็นจรรยาบรรณที่ผู้ใช้อินเทอร์เน็ตยึดถือไว้เสมือนเป็นแม่บทของการปฏิบัติ ผู้ใช้พึงระลึกและเตือนความจำเสมอ มีดังนี้

1) ต้องไม่ใช้คอมพิวเตอร์ทำร้าย หรือละเมิดผู้อื่น
2) ต้องไม่รบกวนการทำงานของผู้อื่น
3) ต้องไม่สอดแนม แก้ไข หรือเปิดดูแฟ้มข้อมูลของผู้อื่น
4) ต้องไม่ใช้คอมพิวเตอร์เพื่อการโจรกรรมข้อมูลข่าวสาร
5) ต้องไม่ใช้คอมพิวเตอร์สร้างหลักฐานที่เป็นเท็จ
6) ต้องไม่คัดลอกโปรแกรมของผู้อื่นที่มีลิขสิทธิ์
7) ต้องไม่ละเมิดการใช้ทรัพยากรคอมพิวเตอร์โดยที่ตนเองไม่มีสิทธิ์
8) ต้องไม่นำเอาผลงานของผู้อื่นมาเป็นของตน
9) ต้องคำนึงถึงสิ่งที่จะเกิดขึ้นกับสังคมอันติดตามมาจากการกระทำของท่าน
10) ต้องใช้คอมพิวเตอร์โดยเคารพกฎระเบียบ กติกา และมีมารยาท

จรรยาบรรณเป็นสิ่งที่ทำให้สังคมอินเทอร์เน็ตเป็นระเบียบ ความรับผิดชอบต่อสังคมเป็นเรื่องที่จะต้องปลูกฝังกฎเกณฑ์ ของแต่ละ เครือข่าย จะต้องมีการวางระเบียบ เพื่อให้การดำเนินงานเป็นไปอย่างมีระบบ และเอื้อประโยชน์ซึ่งกันและกัน บางเครือข่ายมีบทลงโทษที่ชัดเจน เช่น การปฏิบัติผิดกฎเกณฑ์ของเครือข่าย จะต้องตัดสิทธิ์การเป็นผู้ใช้ของเครือข่าย

ในอนาคตจะมีการใช้เครือข่ายคอมพิวเตอร์เป็นจำนวนมาก จรรยาบรรณจึงเป็นสิ่งที่ช่วยให้สังคมอินเทอร์เน็ต สงบสุข หากมีการละเมิดอย่างรุนแรง กฎหมายจะเข้ามามีบทบาทต่อไป (โครงการเครือข่ายคอมพิวเตอร์เพื่อโรงเรียนไทย : http://www.school.net.th/)

2.4 การกระตุ้นให้เกิดคุณธรรม จริยธรรมในการใช้เทคโนโลยีสารสนเทศและการสื่อสาร

เทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology:ICT) ถือเป็นหัวใจสำคัญในการผลักดันประเทศเข้าสู่สังคมโลกาภิวัตน์ ซึ่งมีพื้นฐานแห่งการระดมสมอง ภูมิปัญญาและการเรียนรู้อย่างไม่หยุดนิ่ง การที่เทคโนโลยีสารสนเทศ เทคโนโลยีคอมพิวเตอร์และเทคโนโลยีโทรคมนาคมในปัจจุบันมีการพัฒนาอย่างต่อเนื่องจนทำให้เกิด สภาพที่เรียกว่าพื้นที่ไซเบอร์ (Cyberspace) และโลกเสมือนจริง (Virtual World) นั้น มีผลทั้งในด้านดีและด้านเสีย ในด้านดีคือ เทคโนโลยีช่วยให้สังคมมีความเจริญก้าวหน้าอย่างรวดเร็ว การทำงานต่างๆมีความสะดวกและรวดเร็ว มีความถูกต้องแม่นยำมากขึ้น เป็นเครื่องมือในการศึกษาหาความรู้เพิ่มเติม เพราะเทคโนโลยีสารสนเทศนั้นได้ย่อโลกเราให้แคบลง ทุกสิ่งทุกอย่างเราสามารถค้นคว้าได้ภายในเวลาไม่กี่นาที ในด้านการทำงานนั้นมันเป็นตัวช่วยที่ดีเลยทีเดียว เพราะมันช่วยให้เราประหยัดเวลาในการทำงาน มันเป็นสื่อกลางในการติดต่อสื่อสารทำให้เราไม่ต้องเสียเวลาในการเดินทางไปติดต่อธุรกิจ

นอกจากนี้มันยังมีประโยชน์อีกมากมายแต่ในด้านดีนั้นมันก็ยังมีด้านเสียประกอบอยู่ด้วยเพราะสภาพสังคมในปัจจุบันที่มีความเปลี่ยนแปลงอย่างรวดเร็ว จะเห็นว่ามีปัญหาต่างๆมากมายที่เกิดตามมาจากการใช้งานอินเทอร์เน็ต เช่น คนในสังคมได้รับผลกระทบจากอัตราการจ้างงาน เมื่อมีการนำเอาระบบสารสนเทศมาใช้การจ้างงานจึงลดลง ทำให้คนขาดรายได้ และตกงาน เกิดอาชญากรรมคอมพิวเตอร์ เช่น การโจรกรรมผ่านระบบออนไลน์ เว็บไซด์ลามก การล่อลวงทางเพศในโลกออนไลน์ นอกจากนี้ยังมีอันตรายทางอ้อมจากเว็บไซต์อันตราย เช่น เกมส์ออนไลน์ที่อาจนำไปสู่การใช้ความรุนแรงในหมู่เด็กๆ และการไม่รับผิดชอบต่อความผิดที่เกิดขึ้น เพราะยากในการสืบสวน สอบสวน เนื่องจากโลกไซเบอร์นั้นมันมีอยู่ทั่วทุกที่ ยากต่อการควบคุมให้อยู่ในกฎระเบียบ อีกทั้งมันยังส่งผลกระทบด้านภาษา เราพบว่ามีการใช้ภาษาที่สั้นกะทัดรัด เป็นคำที่ใช้เฉพาะกลุ่ม มีการใช้คำแผลง อาจส่งผลต่อการนำไปใช้ในชีวิตจริงๆพฤติกรรมของกลุ่มบุคคลที่ทำการสร้างข่าวสารเท็จก่อให้เกิดความวุ่นวายกับเว็บไซต์ การฉ้อโกง การล่อลวงทางเพศ อาชญากรรมทางธุรกิจ โดยผู้กระทำผิดนั้นล้วนแล้วแต่ดำเนินการผ่านเทคโนโลยีสารสนเทศ เพราะมันยากต่อการติดตามของเจ้าหน้าที่รักษาความเรียบร้อยบนพื้นที่ออนไลน์

ดังนั้นคุณธรรมและจริยธรรมในการทำกิจกรรมต่างๆ บนพื้นที่ไซเบอร์ คือ มาตรการหนึ่งที่จะเป็นปัจจัยในการป้องกันและแก้ไขปัญหาดังกล่าว และเพื่อที่จะให้เกิดการพัฒนาอย่างเหมาะสมและยั่งยืนต่อไปได้

แนวทางในการกระตุ้นให้เกิดคุณธรรม จริยธรรมในการใช้เทคโนโลยีสารสนเทศและการสื่อสาร

1. มาตรการทางการบริหาร หน่วยงานของรัฐ ต้องปฏิบัติหน้าที่อย่างจริงจัง รวมทั้งต้องมีบุคลากรที่เหมาะสม และเพียงพอต่อการปฏิบัติงาน และในขณะนี้ทางภาครัฐได้มีการดำเนินนโยบายขยายการใช้อินเทอร์เน็ตไปสู่ สังคมระดับรากหญ้า หากไม่มีการระมัดระวังและเตรียมการที่ดีก็อาจเป็นการเผยแพร่วัฒนธรรมและ กิจกรรมที่ไม่เหมาะสมบนอินเทอร์เน็ตไปสู่รากหญ้าและเยาวชนในชนบท แต่หากมีการเตรียมการที่ดี ตำบลอาจใช้อินเทอร์เน็ตเป็นสื่อในการกระจายความเจริญทางเทคโนโลยีและกระจาย องค์ความรู้ใหม่ ๆไปสู่สังคมได้ ดังนั้นหน่วยงานดังกล่าวจะต้องมีการวางมาตรการที่เด็ดขาดในการควบคุมดูแลพื้นที่ไซเบอร์ มีนโยบายที่ชัดเจน มีประสิทธิภาพ

2. มาตรการทางกฎหมายหน่วยงานที่ทำหน้าที่ใน การบังคับใช้กฎหมายต้องมีบุคลากรอย่างเพียงพอ เช่น สำนักงานตำรวจแห่งชาติ นอกจากกำหนดให้การกระทำอันมิชอบทั้งหลายบนอินเทอร์เน็ต เป็นความผิดที่ไม่ต่างจากการกระทำในโลกจริงแล้วยังพยายามแก้ไขเพิ่มเติม กฎหมาย เพิ่มอำนาจการสืบสวนสอบสวน เพื่อแสวงหาพยานหลักฐานให้กับเจ้าพนักงานของรัฐรวมทั้งกำหนดให้ผู้ให้บริการ อินเทอร์เน็ตที่เกี่ยวพันกับข้อมูลการใช้อินเทอร์เน็ตทั้งหลายมีหน้าที่ตาม กฎหมายต้องจัดเก็บส่งมอบหรือให้ความร่วมมือกับเจ้าพนักงานเพื่อช่วยกันนำตัว ผู้กระทำความผิดมาลงโทษ

3. มาตรการทางการ ควบคุมจรรยาบรรณ จะต้องมีเครือข่าย ที่มีการดูแล ผู้ประกอบอาชีพและทำกิจกรรมบนพื้นที่ไซเบอร์ ที่สามารถทำหน้าที่ได้อย่างต่อเนื่องและจริงจัง ควรมีการป้องกันการชี้นำความคิดที่ผิดให้แก่คนในสังคม การที่ต้องมีการกระตุ้นให้เกิดสมาคมและเครือข่ายเพื่อดูแลกันเอง เพราะการเก็บข้อมูลหรือแสดงข้อมูล เพื่อแสดงตัวตน และความน่าเชื่อถือในขอบเขตเรื่องธุรกิจ และพาณิชย์อิเล็กทรอนิกส์ ก็เพื่อให้สามารถยืนยันตัวตนของผู้ใช้อินเทอร์เน็ตได้อย่างชัดเจนยิ่งขึ้น และองค์กร เครือ ข่าย สมาคม ของผู้ใช้อินเทอร์เน็ตยังสามารถช่วยเหลือคนในวงการอินเตอร์เน็ต ช่วยคนทำเว็บไซต์ ใช้สายสัมพันธ์ในการให้คำปรึกษาและแก้ไขปัญหาที่เกิดขึ้น

4. มาตรการทางสังคม ต้องยกระดับและพัฒนาสถาบันพื้นฐาน เช่น สถาบันครอบครัวสถาบันศาสนา สถาบันทางสังคม และสถาบันทางธุรกิจให้มีความรู้ ความสามารถด้านไอทีเพียงพอที่จะดูแลบุคคลในสถาบันของตน โดยที่ผู้นำองค์กรทางธุรกิจและสังคมต้องมีความรู้ทาง ไอทีเป็นอย่างดี

5. มาตรการทางการศึกษา ควรพัฒนาการศึกษาระบบสารสนเทศและความรู้ไอทีให้กว้างขวาง รวมทั้งจัดทำหลักสูตรออนไลน์ ให้ครอบคลุมทุกสาขาวิชา ทั้งในและนอกระบบการศึกษา

6. มาตรการทาง คุณธรรมและจริยธรรม ได้แก่ การจัดระบบการให้การศึกษาแก่ผู้ใช้เทคโนโลยีเหล่านี้ทางด้านคุณธรรมและ จริยธรรม เพื่อให้เขาเหล่านั้นเข้าไปชักนำโลกเสมือนจริงและการทำกิจกรรมบนพื้นที่ไซเบอร์ไปในทางที่ถูกที่ควร

ดังนั้นการแก้ปัญหาที่ดีที่สุด การส่งเสริมให้ประชาชนมีคุณธรรม จริยธรรมในการใช้เทคโนโลยี คือการดำเนินการเอาผิดกับผู้ที่กระทำผิดอย่างจริงจัง มีผู้ควบคุมดูและระบบใหญ่และระบบย่อยทั้งหมด เพื่อไม่ให้เกิดการกระทำผิดขึ้น นอกจากนี้ต้องมีการส่งเสริมให้คนมีคุณภาพเข้ามาใช้อินเทอร์เน็ต และต้องสร้างเว็บไซต์ที่มีคุณภาพให้เกิดขึ้นมากๆ รณรงค์ให้ผู้บริหารฯ อาจารย์ นักวิชาการ หรือแม้กะทั่งนักเรียน นิสิต นักศึกษา ทำการเขียนบทความลง website webblog เหล่านี้ จะเป็นการส่งเสริมผลักดันให้มีเว็บไซต์คุณภาพ ที่สำคัญคือสถานศึกษาต้องปลูกฝังจิตสำนึกของนักเรียนในสถาบันของตนเองให้มีความรู้ ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารอย่างถูกต้อง[3]

บรรณานุกรมประจำบทที่ 2

[1] http://home.kku.ac.th/regis/student/Unnamed%20Site%201/Untitled-6.htm

[2] Arlene H. Rinaldi “The Net User Guidelines and Netiquette” Academic/Instititional Support Services, Florida Atlantic University, 1993

[3] http://pirun.kps.ku.ac.th/~b5127172/link7.html

บทที่ 3 คอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์สำหรับลูกเสือไซเบอร์

3.1 คอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์สำหรับลูกเสือไซเบอร์

3.1.1 นิยามของคอมพิวเตอร์

เครื่องอิเล็กทรอนิกส์แบบอัตโนมัติ ทำหน้าที่เหมือนสมองกล ใช้สำหรับแก้ปัญหาต่างๆ ที่ยากและซับซ้อนโดยวิธีทางคณิตศาสตร์ คอมพิวเตอร์จึงเป็นเครื่องจักรอิเล็กทรอนิกส์ที่ถูกสร้างขึ้นเพื่อใช้ทำงานแทนมนุษย์ ในด้านการคิดคำนวณและสามารถจำข้อมูล ทั้งตัวเลขและตัวอักษรได้เพื่อการเรียกใช้งานในครั้งต่อไป นอกจากนี้ยังสามารถจัดการกับสัญลักษณ์ได้ด้วยความเร็วสูง โดยปฏิบัติตามขั้นตอนของโปรแกรม คอมพิวเตอร์ยังมีความสามารถในด้านต่างๆ อีกมาก อาทิเช่น การเปรียบเทียบทางตรรกศาสตร์ การรับส่งข้อมูล การจัดเก็บข้อมูลในตัวเครื่องและสามารถประมวลผลจากข้อมูลต่างๆ ได้ [1]

3.1.2 การรู้คอมพิวเตอร์ (Computer Literacy)

คนส่วนใหญ่เชื่อว่าความรู้ในวิธีการใช้คอมพิวเตอร์ โดยเฉพาะอย่างยิ่ง คือ คอมพิวเตอร์ส่วนบุคคลที่ถือเป็นทักษะพื้นฐานที่จำเป็น เพื่อการประสบความสำเร็จในการทำธุรกิจได้อย่างมีประสิทธิภาพ ทักษะในการใช้คอมพิวเตอร์จึงเป็นสิ่งที่จำเป็น

1) การรู้สารสนเทศ (Information Literacy)

การรู้สารสนเทศ (Information literacy) หมายถึง รู้วิธีการสืบค้น การวิเคราะห์และการนำข้อมูลมาใช้ เป็นความสามารถในการรวบรวมข้อมูลจากหลายแหล่ง การเลือกเฉพาะวัตถุดิบที่เกี่ยวข้อง และจัดระเบียบเพื่อช่วยในการตัดสินใจ หรือการดำเนินการเฉพาะด้าน

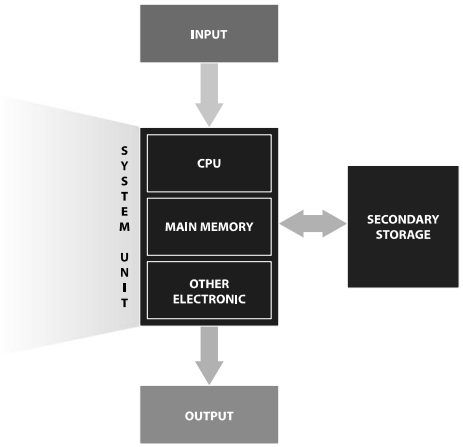
2) คอมพิวเตอร์ทำงานอย่างไร

สำหรับคอมพิวเตอร์ที่จะดำเนินการในวงจรการประมวลผลข้อมูล จะต้องมีรายละเอียดของชุดคำสั่งที่จะต้องบอกว่ามันควรทำอย่างไร ชุดคำสั่งที่ว่านี้เราเรียกว่า โปรแกรมคอมพิวเตอร์ หรือซอฟต์แวร์ ก่อนจะมีการประมวลผลในวงจรประมวลผลข้อมูล โปรแกรมคอมพิวเตอร์จะทำการดึงข้อมูลเข้าสู่ระบบหน่วยความจำ และโปรแกรมคอมพิวเตอร์ถึงจะทำการประมวลผลเพื่อให้ได้ผลลัพธ์ หลังจากเสร็จแล้ว จึงจะทำการประมวลผลข้อมูลอื่นๆ ต่อไป

3) วงจรการประมวลผลข้อมูล (Information Process Cycle)

เป็นพื้นฐานในการทำความเข้าใจและวิธีที่คอมพิวเตอร์ประมวลข้อมูลให้เป็นสารสนเทศ ในวงจรการประมวลผลข้อมูล ประกอบไปด้วย 4 หน่วยคือ หน่วยรับข้อมูล หน่วยประมวลผล หน่วยแสดงผล และหน่วยจัดเก็บข้อมูล

ในสามหน่วยแรก หน่วยรับข้อมูล หน่วยประมวลผล หน่วยแสดงผล จะทำหน้าที่ในการแปลงข้อมูลเป็นสารสนเทศ ส่วนที่สี่จะเป็นส่วนจัดเก็บข้อมูลลงบนสื่อจัดเก็บอิเล็กทรอนิกส์ [1]



รูปที่ 3 - 1 องค์ประกอบของระบบคอมพิวเตอร์ (System Unit)

3.1.3 องค์ประกอบของระบบคอมพิวเตอร์

ข้อมูลจะถูกประมวลผลโดยอุปกรณ์เฉพาะที่มักจะเรียกว่า คอมพิวเตอร์ฮาร์ดแวร์ อุปกรณ์เหล่านี้ ประกอบด้วย

1) ฮาร์ดแวร์ (Computer Hardware) คือ ลักษณะทางกายภาพของเครื่องคอมพิวเตอร์ ซึ่งหมายถึง ตัวเครื่องคอมพิวเตอร์และอุปกรณ์รอบข้าง (peripheral) ที่เกี่ยวข้อง เช่น ฮาร์ดดิสก์ เครื่องพิมพ์ เป็นต้น

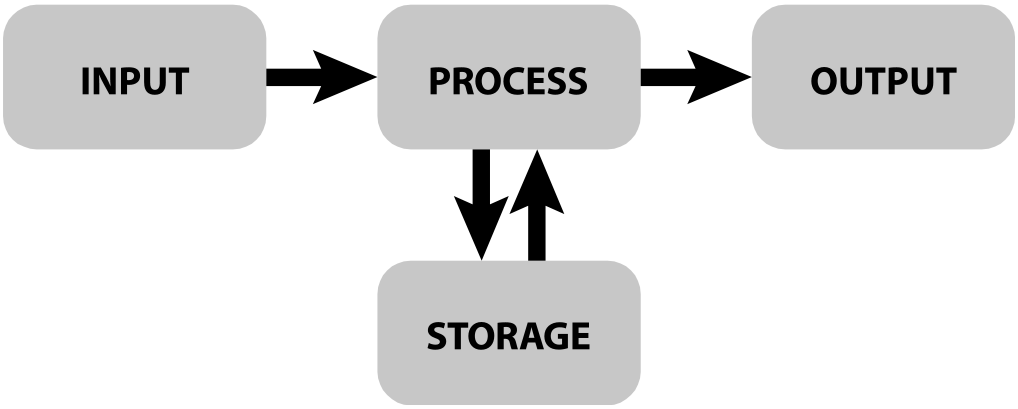
2) สถาปัตยกรรมของระบบคอมพิวเตอร์

2.1) หน่วยรับข้อมูล (Input Device) เครื่องคอมพิวเตอร์จะทำการรับข้อมูลจากหน่วยรับข้อมูล (Input Unit) เช่น แป้นพิมพ์ (keyboard) หรือ เมาส์ (mouse) เป็นต้น

2.2) หน่วยระบบ (System Unit) จะประกอบไปด้วย หน่วยประมวลผลกลาง หน่วยความจำหลัก และอุปกรณ์อิเล็กทรอนิกส์อื่น

2.3) หน่วยแสดงผล (Output Device) เครื่องคอมพิวเตอร์จะให้ผลลัพธ์จากการประมวลผลออกมายังหน่วยแสดงผลลัพธ์ (Output Unit) เช่น เครื่องพิมพ์ หรือจอภาพ

2.4) หน่วยเก็บข้อมูล (Secondary Storage Device) เครื่องคอมพิวเตอร์จะทำการเก็บผลลัพธ์จากการประมวลผลไว้ในหน่วยเก็บข้อมูล เพื่อให้สามารถนำมาใช้ใหม่ได้ในอนาคต [2]



รูปที่ 3 - 2 องค์ประกอบของวงจรการประมวลผลข้อมูล

3) ซอฟต์แวร์ (Computer Software) คอมพิวเตอร์ฮาร์ดแวร์ที่ประกอบออกมาจากโรงงานจะยังไม่สามารถทำงานใดๆ ได้เนื่องจาก ต้องมี ซอฟต์แวร์ (Software) ซึ่งเป็นชุดคำสั่งหรือโปรแกรมที่สั่งให้ฮาร์ดแวร์ทำงานต่างๆ ตามต้องการ โดยชุดคำสั่งหรือโปรแกรมนั้นจะเขียนขึ้นมาจากภาษาคอมพิวเตอร์ (Programming Language) ภาษาใดภาษาหนึ่ง และมีโปรแกรมเมอร์ (Programmer) หรือนักเขียนโปรแกรมเป็นผู้ใช้ภาษาคอมพิวเตอร์เหล่านั้นเขียนซอฟต์แวร์ต่างๆ ขึ้นมา ซอฟต์แวร์ แบ่งออกเป็น 2 ประเภท คือ

3.1) ซอฟต์แวร์ระบบ (System Software) โดยส่วนมากแล้วจะติดตั้งมากับเครื่องคอมพิวเตอร์เนื่องจากซอฟต์แวร์ระบบเป็นส่วนควบคุมการทำงานต่างๆ ของคอมพิวเตอร์ เพื่อให้สามารถเริ่มต้นการทำงานอื่นๆ ที่ผู้ใช้ต้องการได้ต่อไป โดยมีหน้าที่หลัก คือ ใช้ในการจัดการหน่วยรับเข้าและหน่วยส่งออก ใช้ในการจัดการจองพื้นที่บนหน่วยความจำ (RAM) และเป็นตัวเชื่อมต่อระหว่างผู้ใช้กับคอมพิวเตอร์ ซึ่งซอฟต์แวร์ระบบประกอบไปด้วย

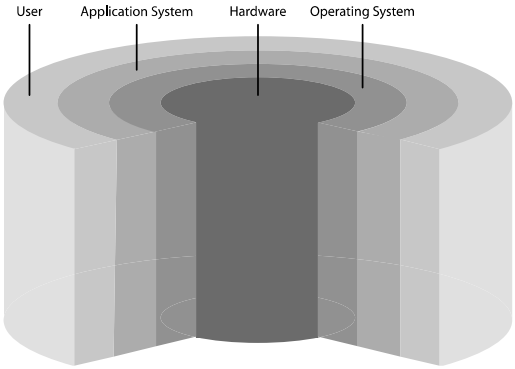
3.1.1) Programming Language เป็นภาษาที่สามารถใช้ควบคุมกำหนดการทำงานของคอมพิวเตอร์ (Flow Control) ภาษาโปรแกรมก็เหมือนภาษามนุษย์จะต้องใช้วากยสัมพันธ์ (Syntax) และความหมาย (Semantic) เพื่อกำหนดโครงสร้างและตีความหมายตามลำดับ ในแต่ละภาษาจะมีโครงสร้างของภาษา รูปแบบไวยากรณ์ และคำศัพท์ที่ไม่เหมือนกัน แต่หลักการของภาษาจะเหมือนกัน เช่น ตัวแปรชนิดต่างๆ การควบคุมการทำงาน ฟังก์ชัน เช่น ภาษา Pascal, C, VB, Java เป็นต้น

3.1.2) ยูทิลิตี้โปรแกรม (System Utility Program) ยูทิลิตี้โปรแกรม คือ ซอฟต์แวร์เสริมช่วยให้เครื่องทำงานมีประสิทธิภาพมากขึ้น เช่น ช่วยในการตรวจสอบฮาร์ดดิสก์ ช่วยในการจัดเก็บข้อมูล ช่วยในการสำเนาข้อมูล ค้นหาไวรัส เป็นต้น

3.2) ซอฟต์แวร์ประยุกต์ (Application Software) เป็นซอฟต์แวร์ที่เน้นในการช่วยการทำงานต่างๆ ให้กับผู้ใช้ ซึ่งแตกต่างกันไปตามความต้องการของผู้ใช้แต่ละคน ซึ่งซอฟต์แวร์ประยุกต์ก็ประกอบไปด้วย

3.2.1) ซอฟต์แวร์ใช้งานเฉพาะ (Special purpose software) เป็นซอฟต์แวร์ที่พัฒนาขึ้นมาเพื่อใช้งานเฉพาะด้าน ซึ่งต้องศึกษารูปแบบการทำงานขององค์กรหรือความต้องการของธุรกิจนั้นๆ ไม่สามารถนำไปใช้งานทั่วไปได้ ตัวอย่างเช่น ระบบการลงทะเบียนของนักเรียน เป็นต้น

3.2.2) ซอฟต์แวร์สำเร็จรูป (General purpose software) เป็นซอฟต์แวร์ที่สามารถนำมาประยุกต์ใช้ได้กับงานทั่วๆ ไปในองค์กร ซอฟต์แวร์สำเร็จรูปมีการวางจำหน่ายทั่วไปในท้องตลาด ตัวอย่างเช่น ไมโครซอฟท์ ออฟฟิศ (Microsoft Office)



รูปที่ 3 - 3 แนวคิดระดับชั้นของระบบ (System Layer Concept)

4) บุคลากร (People ware)

หมายถึง เจ้าหน้าที่ที่ทำงานอยู่ในหน่วยงานที่ใช้เครื่องคอมพิวเตอร์ ซึ่งมีหน้าที่และมีความรับผิดชอบแตกต่างกัน ขึ้นอยู่กับความรู้ การฝึกอบรม และประสบการณ์ในการทำงาน สำหรับบุคลากรในหน่วยงานจะแบ่งออกได้ ดังนี้

- ผู้ใช้งาน (User) หมายถึง ผู้ใช้โดยทั่วๆ ไปอาจเป็นผู้ใช้ตามบ้านหรือผู้ใช้ในสำนักงานก็ได้ ยูสเซอร์ไม่จำเป็นต้องมีความรู้ทางด้านคอมพิวเตอร์มากนัก มักจะใช้งานได้เฉพาะโปรแกรมที่จำเป็นต้องใช้งานอยู่เสมอเท่านั้น

- วิศวกรคอมพิวเตอร์ (Computer Engineer) หมายถึง ผู้ที่จะต้องมีความรู้ทางด้านการบำรุงรักษาอุปกรณ์ต่างๆ ของเครื่องคอมพิวเตอร์ และสามารถแก้ไข ให้คอมพิวเตอร์ทำงานได้ตลอดเวลา ดังนั้นวิศวกรคอมพิวเตอร์จะต้องเป็นผู้ที่มีความรู้และเชี่ยวชาญทางด้านเทคนิคและทางด้านอุปกรณ์ของคอมพิวเตอร์ดีพอสมควร

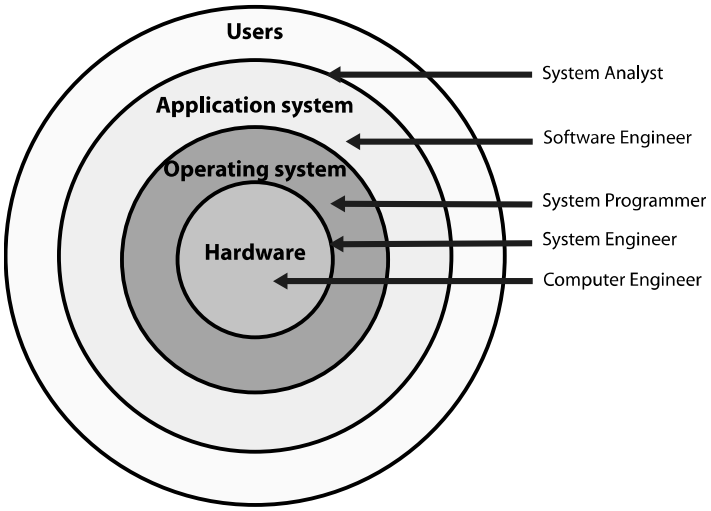
- วิศวกรระบบ (System Engineer) เป็นผู้ที่จะต้องมีความรู้ทางด้านการบำรุงรักษาระบบต่างๆ รวมไปถึงการวิเคราะห์ ออกแบบ พัฒนา และทดสอบ ทั้งในด้าน ฮาร์ดแวร์ และซอฟต์แวร์เป็นอย่างดี อีกทั้งยังสามารถตอบโจทย์ความต้องการต่างๆ ขององค์กร เพื่อนำไปวางแผนพัฒนาระบบโดยรวม

- นักเขียนโปรแกรม (System Programmer) หมายถึง ผู้ที่ทำหน้าที่ในการเขียนคำสั่งโดยใช้ภาษาคอมพิวเตอร์ เพื่อให้เครื่องทำงานตามขั้นตอนที่ต้องการและที่สำคัญคือ นักเขียนโปรแกรมจะต้องเข้าใจและมีความรู้ในหลักการต่างๆ ของการเขียนโปรแกรมเป็นอย่างดี สามารถแก้ไขข้อบกพร่องของโปรแกรมได้

- วิศวกรซอฟต์แวร์ (Software Engineer) หมายถึง ผู้ที่ทำหน้าที่ในการวิเคราะห์ออกแบบ พัฒนาและทดสอบซอฟต์แวร์เพื่อใช้เป็นแผนในการสั่งให้นักเขียนโปรแกรมสามารถนำไปพัฒนาได้อย่างถูกต้อง

- นักวิเคราะห์และออกแบบระบบ (System Analyst) หมายถึง ผู้ที่จะทำหน้าที่ในการวิเคราะห์ระบบงาน ตลอดจนดูแลและรับผิดชอบระบบงานต่างๆ โดยเริ่มตั้งแต่การวิเคราะห์และออกแบบระบบงานระบบข้อมูล ตลอดจนประสานงานระหว่างผู้ใช้เครื่องกับหน่วยงานคอมพิวเตอร์ นักวิเคราะห์ระบบจะต้องเป็นผู้มีความรู้ความสามารถเกี่ยวกับระบบงานและระบบโปรแกรมเป็นอย่างดี มีความรู้กว้างขวางในด้านต่างๆ โดยเฉพาะอย่างยิ่งด้านธุรกิจ

นอกจากนี้ยังมีบุคลากรอื่นๆ ที่เกี่ยวข้องกับคอมพิวเตอร์อีกมาก เช่น พนักงานควบคุมเครื่อง ผู้ดูระบบ พนักงานเตรียมข้อมูล ผู้จัดการฐานข้อมูล ฯลฯ



รูปที่ 3 - 4 โครงสร้างของพีเพิลแวร์ (People ware)

3.1.4 ประเภทของคอมพิวเตอร์

คอมพิวเตอร์ในปัจจุบันสามารถแบ่งเป็นประเภทต่างๆ ได้ 4 ชนิด โดยพิจารณาจากความสามารถในการเก็บข้อมูล และ ความเร็วในการประมวลผลเป็นหลัก ดังต่อไปนี้ [3]

1) ซูเปอร์คอมพิวเตอร์ (Super Computer) หมายถึง เครื่องคอมพิวเตอร์ที่ใช้ในการประมวลผลข้อมูล มีความสามารถในการประมวลผลสูงที่สุด โดยจะทำการสร้างขึ้นเป็นการเฉพาะเพื่องานด้านวิทยาศาสตร์ที่ต้องการการประมวลผลซับซ้อน และต้องการความเร็วสูง เช่น งานวิจัยขีปนาวุธ งานโครงการอวกาศสหรัฐ (NASA) งานสื่อสารดาวเทียม หรืองานพยากรณ์อากาศ เป็นต้น

2) เมนเฟรม (Mainframe Computer) หมายถึง เครื่องคอมพิวเตอร์ที่มีประสิทธิภาพรองจากซูเปอร์คอมพิวเตอร์ สามารถรองรับการทำงานจากผู้ใช้ได้จำนวนมากในเวลาเดียวกัน ประมวลผลด้วยความเร็วสูง มีหน่วยความจำหลักขนาดใหญ่ ตลอดจนสามารถจัดเก็บข้อมูลได้เป็นจำนวนมาก คอมพิวเตอร์เมนเฟรม นิยมใช้กับองค์การขนาดใหญ่ที่มีการเข้าถึงข้อมูลของผู้ใช้จำนวนมากในเวลาเดียวกัน เช่น คอมพิวเตอร์ของธนาคารที่เชื่อมต่อไปยังตู้ ATM และสาขาของธนาคารทั่วประเทศ เป็นต้น

3) มินิคอมพิวเตอร์ (Mini Computer) หมายถึง เครื่องคอมพิวเตอร์ขนาดเล็ก มีสมรรถนะน้อยกว่าเครื่องเมนเฟรม คือทำงานได้ช้า และควบคุมอุปกรณ์รอบข้างได้น้อยกว่าเครื่องเมนเฟรม แต่ทำงานร่วมกับอุปกรณ์ประกอบรอบข้างที่มีความเร็วสูงได้ มินิคอมพิวเตอร์สามารถอ่านเขียนข้อมูลได้อย่างรวดเร็ว และจะทำการบันทึกข้อมูลลงบนฮาร์ดดิสก์ (Hard disk)

4) ไมโครคอมพิวเตอร์ (Micro Computer)

หมายถึง เครื่องประมวลผลข้อมูลขนาดเล็ก มีส่วนของหน่วยความจำและความเร็วในการประมวลผลน้อยที่สุด สามารถใช้งานได้คนเดียว จึงมักถูกเรียกว่า คอมพิวเตอร์ส่วนบุคคล (Personal Computer : PC) ปัจจุบันไมโครคอมพิวเตอร์มีประสิทธิภาพสูงกว่าในสมัยก่อน อาจเท่ากับหรือมากกว่าเครื่องเมนเฟรมในยุคก่อน นอกจากนั้นยังราคาถูกลงจึงเป็นที่นิยมใช้กันอย่างแพร่หลาย

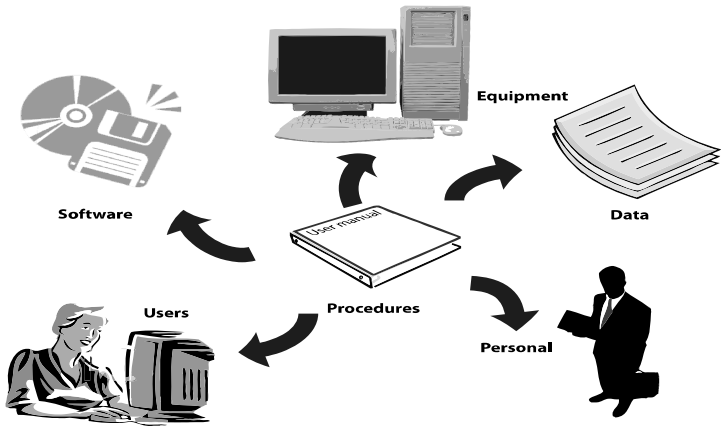
เมื่อได้ทำการศึกษา เรียนรู้และทำความเข้าใจใน ความหมาย หลักการทำงานของคอมพิวเตอร์ องค์ประกอบของระบบคอมพิวเตอร์ และประเภทของคอมพิวเตอร์แล้ว ก่อนที่จะนำมาประยุกต์ใช้งานนั้น ยังต้องมีองค์ความรู้และทักษะในการคิดวิเคราะห์เพื่อตัดสินใจในเรื่องของการใช้คอมพิวเตอร์ และการใช้สารสนเทศให้เกิดประโยชน์สูงสุดในชีวิตประจำวันอีกด้วย

3.1.5 องค์ประกอบของ Information System

การได้รับข้อมูลที่เป็นประโยชน์และทันท่วงทีจากการประมวลผลคอมพิวเตอร์ต้องมีมากกว่าอุปกรณ์และซอฟต์แวร์ ยังมีองค์ประกอบอื่นที่สำคัญเพื่อให้ประสบความสำเร็จในการประมวลผลข้อมูล คือ การอบรมระบบสารสนเทศ การให้ความรู้แก่ผู้ใช้งาน และเอกสารกระบวนการต่าง ๆ

กระบวนการทำงานหรือโพรซีเยอร์ หมายถึง ขั้นตอนที่ผู้ใช้จะต้องทำตาม เพื่อให้ได้งานเฉพาะอย่างจากคอมพิวเตอร์ ซึ่งผู้ใช้คอมพิวเตอร์ทุกคนต้องรู้การทำงานพื้นฐานของเครื่องคอมพิวเตอร์เพื่อที่จะสามารถใช้งานได้อย่างถูกต้อง [4]

การใช้คอมพิวเตอร์ปฏิบัติงานในส่วนต่างๆ นั้นมักจะมีขั้นตอนที่สลับซับซ้อน และเกี่ยวข้องกับช่วงเวลาต่างๆ ในการปฏิบัติงานด้วย จึงต้องมีคู่มือการปฏิบัติงานที่ชัดเจน เช่น คู่มือสำหรับผู้ควบคุมเครื่อง (Operation Manual) คู่มือสำหรับผู้ใช้ (User Manual) เป็นต้น



รูปที่ 3 - 5 โครงสร้างกระบวนการทำงาน (Procedure)

3.1.6 การติดต่อสื่อสารและระบบเครือข่ายคอมพิวเตอร์

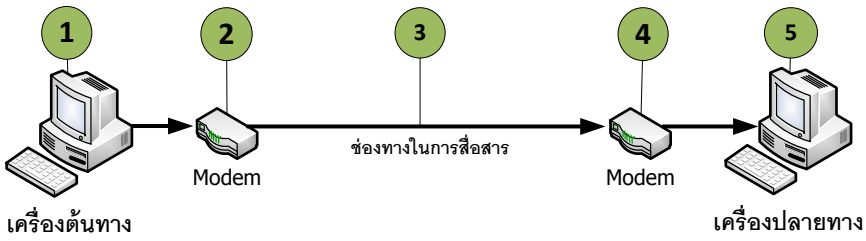
การติดต่อสื่อสารเป็นการพูดคุยหรือส่งข่าวกันของมนุษย์ โดยส่วนใหญ่เป็นการสื่อสารในระยะใกล้ ต่อมาเมื่อเทคโนโลยีก้าวหน้ามากขึ้นมีการพัฒนาอุปการณ์อิเล็กทรอนิกส์สำหรับใช้ในการสื่อสาร ทำให้สามารถสื่อสารได้ในระยะไกลและสะดวกรวดเร็วมากยิ่งขึ้น สำหรับการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์หลายเครื่องในเวลาเดียวกันนั้นเรียกว่าระบบเครือข่าย (network)

1) รูปแบบระบบการสื่อสารข้อมูล (Communications System Model)

การสื่อสารข้อมูล (Data Communications) หมายถึง กระบวนการถ่ายโอนหรือแลกเปลี่ยนข้อมูลกันระหว่างผู้ส่งและผู้รับโดยผ่านช่องทางสื่อสาร เช่น อุปกรณ์อิเล็กทรอนิกส์ หรือคอมพิวเตอร์เป็นตัวกลางในการส่งข้อมูล เพื่อให้ผู้ส่ง และผู้รับเกิดความเข้าใจซึ่งกันและกัน โดยการส่งข้อมูลนั้นจะแปลงข้อมูลเป็นสัญญาณ หรือรหัสเสียก่อนแล้วจึงส่งไปยังผู้รับและเมื่อถึงผู้รับก็จะต้องมีการแปลงสัญญาณนั้นกลับมาให้อยู่ในรูปแบบที่มนุษย์สามารถเข้าใจได้

ระบบการสื่อสารข้อมูลจะมีองค์ประกอบขั้นพื้นฐานดังนี้

- เครื่องคอมพิวเตอร์ต้นทาง
- อุปกรณ์สื่อสารที่ใช้ในการส่งข้อมูล
- ช่องทางในการติดต่อสื่อสารที่ใช้ในการส่งข้อมูล
- อุปกรณ์สื่อสารที่ใช้ในการรับข้อมูล
- เครื่องคอมพิวเตอร์ปลายทาง



รูปที่ 3 - 6 รูปแบบพื้นฐานระบบการสื่อสารข้อมูล

2) สื่อกลางในการสื่อสารข้อมูล (Communications channel)

การสื่อสารทุกชนิดต้องอาศัยสื่อกลางในการส่งผ่านข้อมูลเพื่อนำข้อมูลไปยังจุดหมายปลายทาง สื่อกลางในการสื่อสารมีความสำคัญเพราะเป็นปัจจัยหนึ่งที่กำหนดประสิทธิภาพในการสื่อสาร

สื่อกลางที่ใช้ในการสื่อสารแบ่งเป็น 2 ชนิด คือ

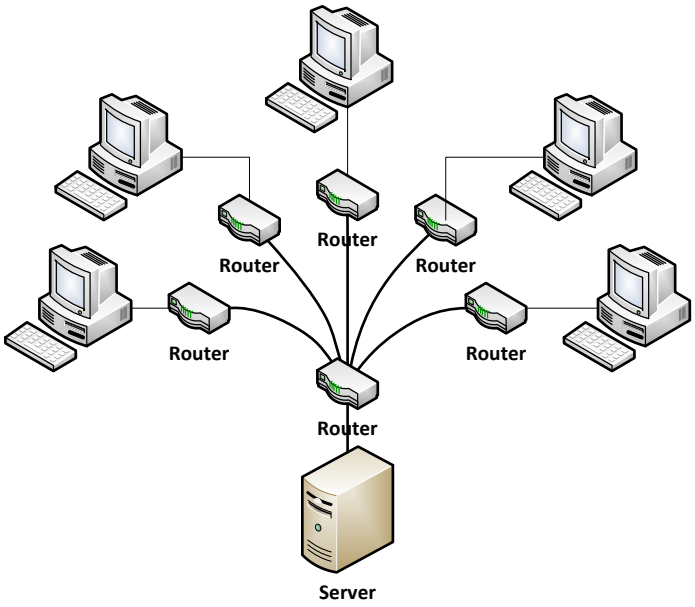
- สื่อกลางแบบใช้สาย เช่น สายแลนแบบไม่ป้องกันสัญญาณรบกวน (UTP) สายแลนแบบป้องกันสัญญาณรบกวน (STP) และ สายไฟเบอร์ออฟติก (fiber – optic cable) เป็นต้น

- สื่อกลางแบบไร้สาย เช่น อินฟราเรด (Infrared : IR) ไมโครเวฟ (microwave) คลื่นวิทยุ (radio- wave) และดาวเทียมสื่อสาร (communications satellite) เป็นต้น

3) รูปแบบการเชื่อมต่อเครือข่าย (Line Configuration)

การสร้างเส้นทางการสื่อสารเพื่อส่งข้อมูลจากอุปกรณ์หนึ่งไปยังอุปกรณ์หนึ่ง แบ่งออกเป็น 2 รูปแบบ

- รูปแบบการเชื่อมต่อเครือข่ายแบบจุดต่อจุด (point- to-point) เป็นรูปแบบการเชื่อมต่อแบบพื้นฐาน โดยจะทำการต่ออุปกรณ์รับหรือส่ง 2 ชุด และใช้สายสื่อสารเพียงสายเดียว
- การเชื่อมต่อแบบหลายจุด (Multi Point) เป็นรูปแบบการเชื่อมต่อโดยการใช้สายสื่อสารเพียงสายเดียวแต่ทำการเชื่อมต่อกับหลายๆ จุด โดยจะมีที่พักเก็บข้อมูลชั่วคราวก่อนทำการส่ง และทำการรับข้อมูลมาเก็บเรื่อยๆ จนเต็มแล้วจึงทำการส่งข้อมูลทันทีหรือเมื่อมีคำสั่ง



รูปภาพที่ 3 - 7 การเชื่อมต่อแบบหลายจุด (Multi Point)

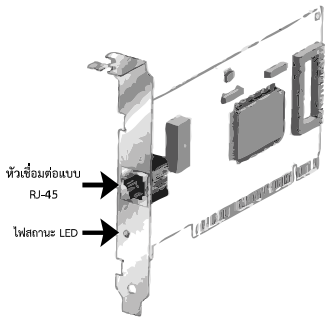
3.1.7 อุปกรณ์การสื่อสาร (Communications Equipment)

อุปกรณ์การสื่อสาร ทำหน้าที่รับส่งข้อมูล โดยมีการส่งผ่านทางสื่อกลางดังที่กล่าวมาแล้วข้างต้น สัญญาณที่ส่งออกไปอาจอยู่ในรูปแบบดิจิทัล หรือแบบอนาล็อก ขึ้นอยู่กับอุปกรณ์สื่อกลางที่ใช้ในการเชื่อมต่อ

อุปกรณ์การสื่อสารประเภทต่างๆ ที่ใช้กันอยู่ในปัจจุบัน มีดังต่อไปนี้

1) อุปกรณ์ในการเชื่อมต่อเครือข่าย (Network Interface Card – NIC)

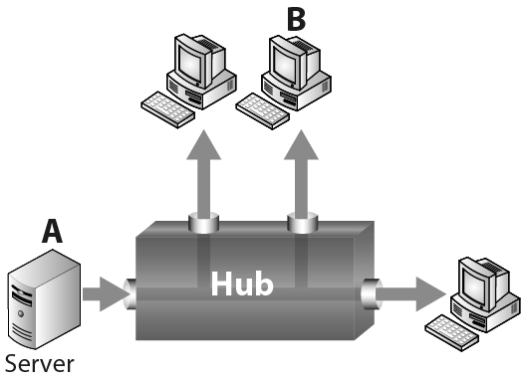
อุปกรณ์ในการเชื่อมต่อเครือข่าย หรือชื่อเรียกอีกอย่างหนึ่งว่า การ์ดแลน (LAN card) เป็นอุปกรณ์ที่เชื่อมระหว่างคอมพิวเตอร์กับสายตัวนำสัญญาณ ทำให้คอมพิวเตอร์สามารถรับและส่งข้อมูลกับระบบเครือข่ายได้



รูปที่ 3 - 8 การ์ดแลน (LAN card)

2) HUB

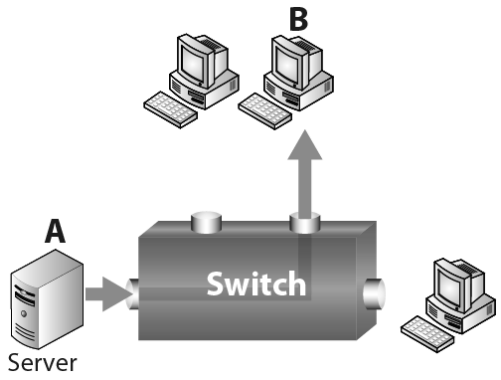
เป็นอุปกรณ์รวมสัญญาณที่มาจากอุปกรณ์รับส่งหรือเครื่องคอมพิวเตอร์หลายเครื่องเข้าด้วยกันข้อมูลที่รับส่งผ่านฮับจะกระจายไปยังทุกสถานีที่ต่ออยู่บนฮับนั้น ดังนั้นทุกสถานีจะรับสัญญาณข้อมูลที่กระจายมาได้ทั้งหมด แต่จะเลือกคัดลอกเฉพาะข้อมูลที่ส่งมาถึงตนเท่านั้น เช่น เครื่อง A ส่งข้อมูลผ่านฮับที่กระจายไปยังทุกเครื่อง แต่เครื่อง B เท่านั้นที่ทำการคัดลอกข้อมูลของตน



รูปภาพที่ 3 - 5 รูปแบบการทำงานของฮับ

3) สวิตช์ (Switch)

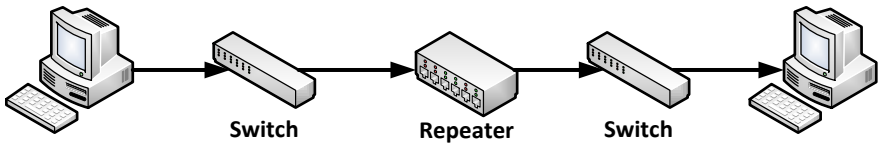
เป็นอุปกรณ์รวมสัญญาณที่มาจากอุปกรณ์รับส่งหรือคอมพิวเตอร์หลายเครื่องเช่นเดียวกับฮับ ข้อแตกต่างคือ การรับส่งข้อมูลของสวิตช์ จะไม่กระจายไปยังทุกจุดเหมือนฮับ เพราะสวิตช์จะรับกลุ่มข้อมูลมาตรวจสอบก่อนว่าเป็นของคอมพิวเตอร์หรืออุปกรณ์ใด แล้วจึงนำข้อมูลนั้นส่งต่อไปยังคอมพิวเตอร์หรืออุปกรณ์เป้าหมายให้อย่างอัตโนมัติ เช่น เครื่อง A ส่งข้อมูลผ่านสวิตช์ ไปยังเครื่อง B เท่านั้น โดยเครื่องอื่นไม่สามารถรับข้อมูลได้



รูปภาพที่ 3 - 6 รูปแบบการทำงานของสวิตช์

4) รีพีตเตอร์ (Repeater)

เป็นอุปกรณ์ที่ทวนและขยายสัญญาณ เพื่อส่งต่อไปยังอุปกรณ์อื่น ให้ได้ระยะทางที่ยาวไกลขึ้น

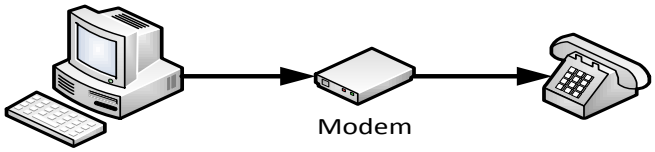


รูปที่ 3 - 7 รูปแบบการทำงานของรีพีตเตอร์ (Repeater)

5) โมเด็ม (Modem)

เป็นอุปกรณ์ที่แปลงสัญญาณดิจิทัลเป็นสัญญาณแอนะล็อกและแปลงสัญญาณแอนะล็อกเป็นดิจิทัลเพื่อให้ข้อมูลส่งผ่านทางสายโทรศัพท์ได้ โมเด็มมีหลายประเภทแบ่งตามลักษณะการใช้งานดังนี้

- โมเด็มแบบหมุนโทรศัพท์ (Dial-up modem) เป็นโมเด็มที่ใช้ต่อเข้ากับผู้ให้บริการอินเทอร์เน็ตผ่านทางสายโทรศัพท์ การเชื่อมต่อใช้วิธีการหมุนโทรศัพท์ ติดต่อไปยังผู้ให้บริการอินเทอร์เน็ตความเร็วในการส่งผ่านข้อมูลต่ำ ประมาณ 56 kbps ระบบการเชื่อมต่ออินเทอร์เน็ตผ่านโมเด็มแบบหมุนโทรศัพท์



รูปที่ 3 - 8 รูปแบบการทำงานของโมเด็มแบบหมุนโทรศัพท์ (Dial-up modem)

- ดิจิทัลโมเด็ม (Digital modem) เป็นโมเด็มที่ใช้รับและส่งข้อมูลผ่านสายเชื่อมสัญญาณแบบดิจิทัล การเชื่อมต่อโมเด็มแบบนี้ไม่จำเป็นต้องหมุนโทรศัพท์ไปที่ผู้ให้บริการอินเทอร์เน็ต เนื่องจากโมเด็มจะทำการเชื่อมต่ออัตโนมัติ สามารถส่งข้อมูลด้วยความเร็วสูงตั้งแต่ 128 kbps ขึ้นไป โดยทั่วไปจะเป็นโมเด็มที่ติดตั้งภายนอก (external modem)

6) จุดเชื่อมต่อแบบไร้สาย (Wireless access point)

จุดเชื่อมต่อแบบไร้สาย หรือ ไวร์เลสแลน ทำหน้าที่คล้ายกับฮับของเครือข่ายแบบใช้สายเพื่อใช้สำหรับติดต่อสื่อสารระหว่างอุปกรณ์แบบไร้สาย ซึ่งข้อมูลจะถูกส่งผ่านทางคลื่นวิทยุความถี่สูง

7) ซอฟต์แวร์ที่ใช้ในการติดต่อสื่อสาร (Communications Software)

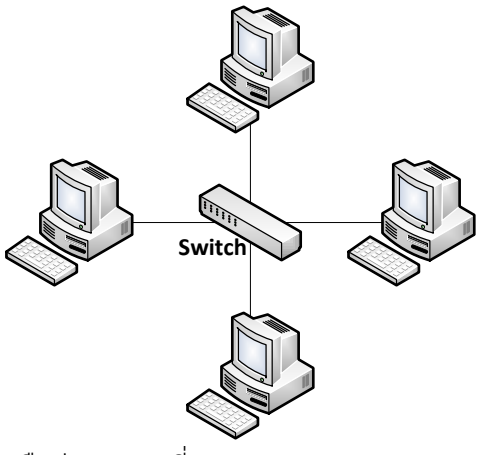
เป็นซอฟต์แวร์ที่ใช้ในการติดต่อสื่อสารกับคอมพิวเตอร์เครื่องอื่นในระบบเครือข่าย เพื่อใช้ในการส่งข้อมูลในลักษณะต่างๆ เช่น การรับส่งไปรษณีย์อิเล็กทรอนิกส์ การโอนย้ายแฟ้มข้อมูล การแลกเปลี่ยนข้อมูลข่าวสาร การประชุม พูดคุย และสนทนาออนไลน์ หรือการค้นหาข้อมูลต่างๆ

3.1.8 เครือข่ายคอมพิวเตอร์ (Communications Networks)

เครือข่ายคอมพิวเตอร์ เป็นการเชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่อพ่วงเข้าด้วยกันเพื่อให้สามารถใช้ข้อมูลทรัพยากรร่วมกันองค์กร เครือข่ายคอมพิวเตอร์สามารถแบ่งออกเป็นประเภทตามพื้นที่ที่ครอบคลุมการใช้งานของเครือข่าย ดังนี้

1) เครือข่ายเฉพาะที่ หรือแลน (Local Area Network: LAN)

เป็นเครือข่ายที่ใช้ในการเชื่อมโยงคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่อยู่ในพื้นที่เดียวกันหรือใกล้เคียงกัน เช่น ภายในบ้าน ภายในสำนักงาน และภายในอาคาร เป็นต้น [5]

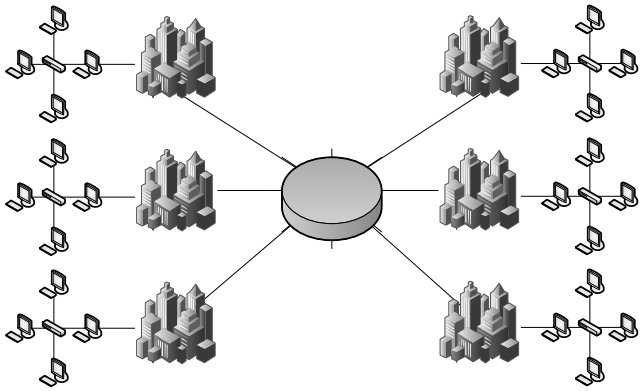


รูปที่ 3 - 13 เครือข่ายเฉพาะที่ (Local Area Network: LAN)

2) เครือข่ายนครหลวง หรือแมน (Metropolitan Area Network: MAN)

เป็นเครือข่ายที่ใช้เชื่อมโยงแลนที่อยู่ห่างไกลออกไป เช่น การเชื่อมต่อเครือข่ายระหว่างสำนักงานที่อาจอยู่คนละอาคารและมีระยะทางไกลกัน การเชื่อมต่อเครือข่ายชนิดนี้อาจใช้สายไฟเบอร์

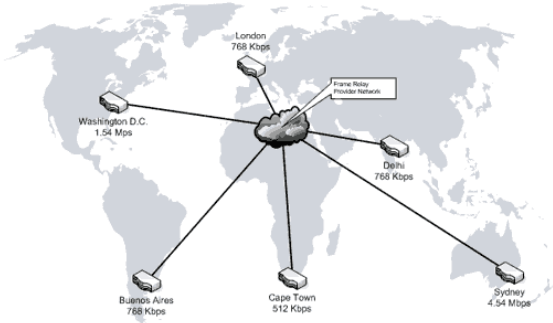
ออฟติก หรือบางครั้งอาจใช้คลื่นไมโครเวฟในเชื่อมต่อ เครือข่ายแบบนี้ใช้ในสถานศึกษามีชื่อเรียกอีกอย่างหนึ่งว่าเครือข่ายแคมปัส (Campus Area Network: CAN)



รูปที่ 3 - 9 เครือข่ายนครหลวง หรือแมน (Metropolitan Area Network: MAN)

3) เครือข่ายวงกว้าง หรือแวน (Wide Area Network: WAN)

เป็นเครือข่ายที่ใช้ในการเชื่อมโยงกับเครือข่ายอื่นที่อยู่ไกลกันมาก เช่น เครือข่ายระหว่างประเทศ



รูปที่ 3 - 10 เครือข่ายวงกว้าง หรือแวน (Wide Area Network: WAN)

4) เครือข่ายอินทราเน็ต (intranet)

เป็นระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรที่ใช้เทคโนโลยีอินเทอร์เน็ตในการใช้งานอินทราเน็ตจะต้องใช้โปรโตคอล IP เหมือนกับอินเทอร์เน็ต สามารถมีเว็บไซต์และใช้เว็บเบราว์เซอร์ได้เช่นกัน รวมถึงอีเมล ถ้าเราเชื่อมต่ออินทราเน็ตของเรากับอินเทอร์เน็ต เราก็สามารถใช้ได้ทั้งอินเทอร์เน็ตและอินทราเน็ตไปพร้อม ๆ กัน แต่ในการใช้งานนั้นจะแตกต่างกันด้านความเร็ว ในการโหลดไฟล์ใหญ่ๆ จากเว็บไซต์ในอินทราเน็ตจะรวดเร็วกว่าการโหลดจากอินเทอร์เน็ตมาก ดังนั้นประโยชน์ที่จะได้รับจากอินทราเน็ตสำหรับองค์กรหนึ่ง คือ สามารถใช้ความสามารถต่างๆ ที่มีอยู่ในอินเทอร์เน็ตได้อย่างเต็มประสิทธิภาพ [15]

5) เครือข่ายอินเทอร์เน็ต (Internet)

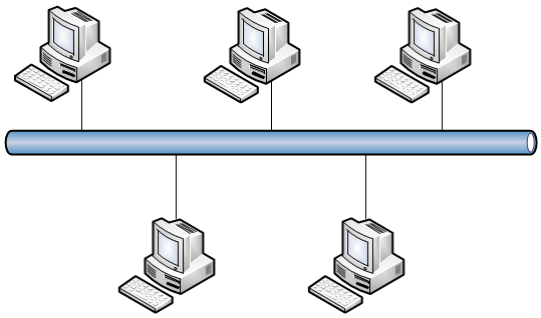
เป็นเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่มีการเชื่อมต่อระหว่างเครือข่ายหลาย ๆ เครือข่ายทั่วโลก โดยใช้ภาษาที่ใช้สื่อสารกันระหว่างคอมพิวเตอร์ที่เรียกว่า โปรโตคอล (Protocol) ผู้ใช้เครือข่ายนี้สามารถสื่อสารถึงกันได้ในหลายๆ ทาง อาทิเช่น อีเมล เว็บบอร์ด และสามารถสืบค้นข้อมูลและข่าวสารต่างๆ รวมทั้งคัดลอกแฟ้มข้อมูลและโปรแกรมมาใช้ได้

3.1.9 โครงสร้างการเชื่อมต่อเครือข่าย (Network Configurations)

โครงสร้างการเชื่อมต่อเครือข่ายคอมพิวเตอร์หรืออุปกรณ์รับส่งข้อมูลที่ประกอบกันเป็นเครือข่ายที่มีการเชื่อมโยงถึงกันในรูปแบบต่างๆ ตามลักษณะทางกายภาพที่เรียกว่ารูปร่างเครือข่าย (network topology) โดยทั่วไปรูปร่างเครือข่ายสามารถแบ่งออกตามลักษณะของการเชื่อมต่อได้ 3 รูปแบบคือ

1) เครือข่ายแบบบัส (Bus topology)

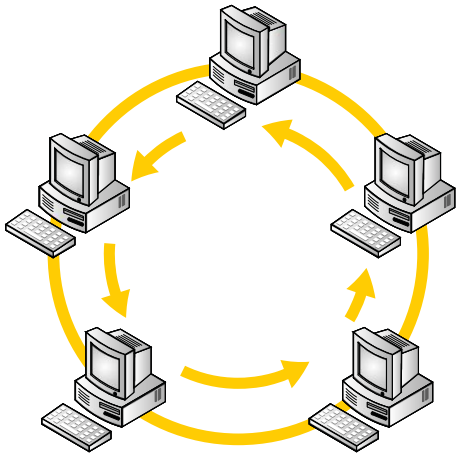
เป็นรูปแบบที่มีโครงสร้างไม่ยุ่งยาก สถานีทุกสถานีในเครือข่ายจะเชื่อมต่อเข้ากับสายสื่อสารหลักเพียงสายเดียว การจัดส่งวิธีนี้ต้องกำหนดวิธีการที่จะไม่ให้ทุกสถานีส่งข้อมูลพร้อมกันเพราะจะทำให้เกิดการชนกัน (collision) ของข้อมูล เครือข่ายแบบบัส ไม่ได้รับความนิยมในปัจจุบัน เนื่องจากความเสียหายที่เกิดขึ้นกับบัสเพียงจุดเดียวก็จะส่งผลให้ทุกอุปกรณ์ไม่สามารถสื่อสารถึงกันได้



รูปที่ 3 - 16 รูปแบบการเชื่อมต่อแบบบัส (Bus topology)

2) เครือข่ายแบบวงแหวน (Ring topology)

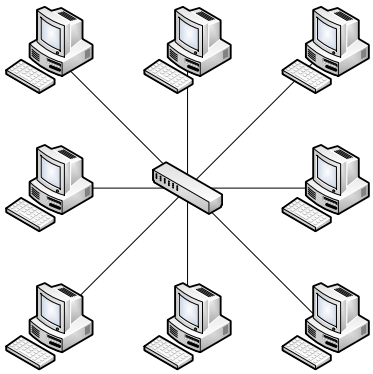
เป็นการเชื่อมแต่ละสถานีเข้าด้วยกันแบบวงแหวน สัญญาณข้อมูลจะถูกส่งไปในทิศทางเดียวกันจนถึงผู้รับ ซึ่งระบบเครือข่ายแบบวงแหวนนี้ สามารถรองรับจำนวนสถานีได้เป็นจำนวนมาก แต่ข้อเสีย คือ สถานีจะต้องรอจนถึงรอบของตนเอง ก่อนที่จะสามารถส่งข้อมูลได้



รูปที่ 3 - 17 รูปแบบการเชื่อมต่อแบบวงแหวน (Ring topology)

3) เครือข่ายแบบดาว (Star topology)

เป็นการเชื่อมต่อสถานีในเครือข่าย โดยทุกสถานีจะต่อเข้ากับจุดเชื่อมต่อ เช่น สวิตช์ (Switch) ซึ่งทำหน้าที่เป็นศูนย์กลางของการเชื่อมต่อระหว่างสถานีต่างๆ ข้อดีของการเชื่อมต่อแบบดาว คือ ถ้าสถานีใดชำรุด จะไม่กระทบกับการเชื่อมต่อของสถานีอื่น ดังนั้นจึงเป็นที่นิยมใช้กันในปัจจุบัน



รูปที่ 3 - 11 รูปแบบการเชื่อมต่อแบบวงแหวน (Ring topology)

3.1.10 การเชื่อมต่อทางเครือข่าย (Connecting Networks)

อุปกรณ์การเชื่อมต่อทางเครือข่าย ที่ใช้กันอยู่ในปัจจุบัน มีดังต่อไปนี้

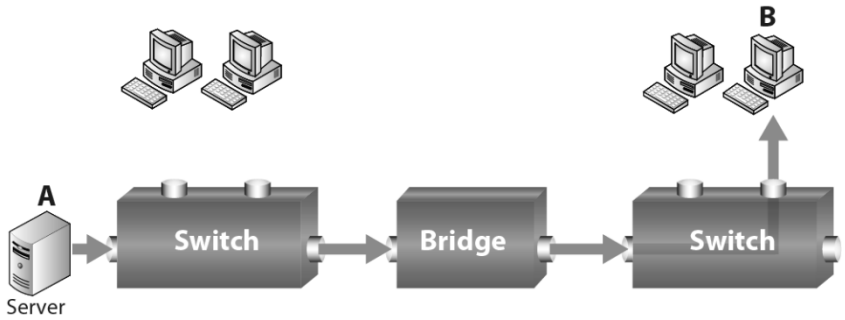
1) เกตเวย์ (Gateway)

เป็นอุปกรณ์ที่ทำให้เครือข่ายคอมพิวเตอร์ 2 เครือข่ายหรือมากกว่า ที่มีลักษณะไม่เหมือนกันสามารถติดต่อกันได้เหมือนเป็นเครือข่ายเดียวกัน เปรียบเสมือนเป็นประตูทางผ่านในการสื่อสารข้อมูลระหว่างคอมพิวเตอร์ต่างชนิดกัน เช่น ระหว่างเครื่องไมโครคอมพิวเตอร์ทั่ว ๆ ไปกับเครื่องมินิคอมพิวเตอร์ หรือเมนเฟรม ซึ่งเป็นเครื่องคอมพิวเตอร์ขนาดใหญ่ เป็นต้น อุปกรณ์ที่ทำหน้าที่เป็น Gateway นั้นอาจจะใช้คอมพิวเตอร์เครื่องใดเครื่องหนึ่งทำหน้าที่ก็ได้

รูปที่ 3 - 12 รูปแบบการทำงานของเกตเวย์ (Gateway)

2) บริดจ์ (Bridge)

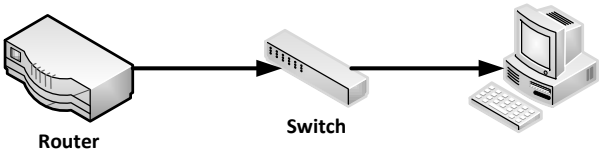
เป็นอุปกรณ์ที่ใช้ในการเชื่อมต่อเครือข่ายสองเครือข่ายเข้าด้วยกัน ซึ่งดูแล้วคล้ายกับเป็นสะพานเชื่อมสองฟากฝั่งเข้าด้วยกัน ด้วยเหตุนี้จึงเรียกอุปกรณ์นี้ว่า “บริดจ์”



รูปที่ 3 - 13 รูปแบบการทำงานของบริดจ์ (Bridge)

3) เร้าท์เตอร์ (Router)

เร้าท์เตอร์ หรือ อุปกรณ์จัดเส้นทาง เป็นอุปกรณ์ที่ใช้งานในการเชื่อมโยงเครือข่ายหลายเครือข่ายเข้าด้วยกัน



รูปที่ 3 - 21 รูปแบบการทำงานของเร้าท์เตอร์ (Router)

3.2 อินเทอร์เน็ตเบื้องต้น

3.2.1 นิยามของอินเทอร์เน็ต

อินเทอร์เน็ต (Internet) นั้นย่อมาจากคำว่า “International Network” หรือ “Inter Connection Network” ซึ่งหมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายคอมพิวเตอร์ทั่ว

โลกเข้าไว้ด้วยกัน เพื่อให้เกิดการสื่อสาร และการแลกเปลี่ยนข้อมูลร่วมกัน โดยสามารถส่งข้อมูลได้ในหลายๆ รูปแบบไม่ว่าจะเป็น ข้อความ ภาพ หรือแม้กระทั่งเสียง อาศัยตัวเชื่อมเครือข่ายภายใต้มาตรฐานการเชื่อมโยงเดียวกัน นั่นก็คือ TCP/ IP Protocol ซึ่งเป็นข้อกำหนดวิธีการติดต่อสื่อสารระหว่างคอมพิวเตอร์ในระบบเครือข่าย ในโปรโตคอลนี้จะช่วยให้คอมพิวเตอร์ที่มีฮาร์ดแวร์ที่แตกต่างกันสามารถติดต่อถึงกันได้ [6]

3.2.2 หลักการทำงานของอินเทอร์เน็ต (Internet System Concept)

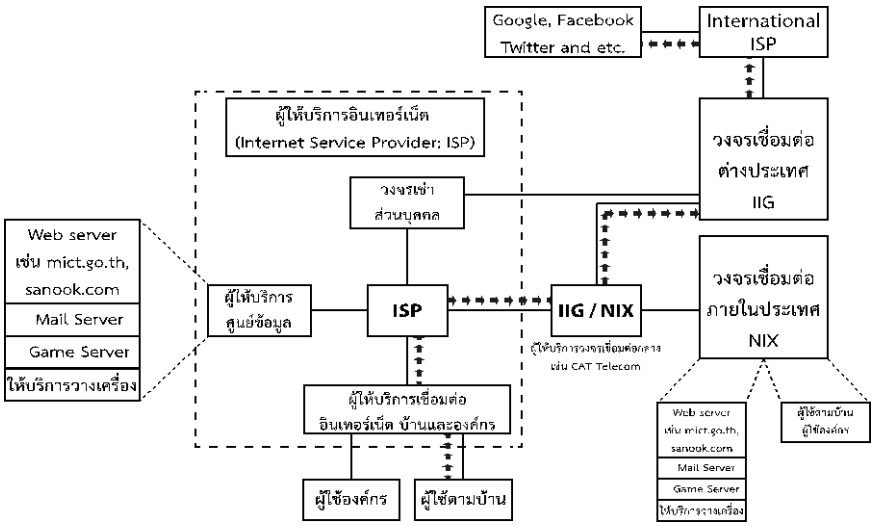
หลักการทำงานของอินเทอร์เน็ต เมื่อใช้งานอินเทอร์เน็ตภายในประเทศไทย จะมีองค์ประกอบใหญ่ๆ อยู่ 2 ส่วนด้วยกัน คือ

1) ผู้ให้บริการอินเทอร์เน็ต (ISP)

จะมีการให้บริการเชื่อมต่อเข้าสู่อินเทอร์เน็ต ให้บริการเช่าพื้นที่ในการเชื่อมต่อเครื่องแม่ข่าย (Server) เข้าสู่โครงข่ายความเร็วสูง

2) ผู้ให้บริการวงจรเชื่อมต่อกลาง (Internet backbone)

เป็นส่วนที่สำคัญที่สุดของอินเทอร์เน็ต ซึ่งทำหน้าที่เป็นกระดูกสันหลัง หรือแกนหลัก (Backbone) ของระบบ ที่ใช้เป็นช่องทางการสื่อสารระหว่างโหนด (Node) ต่างๆ ทั่วโลก

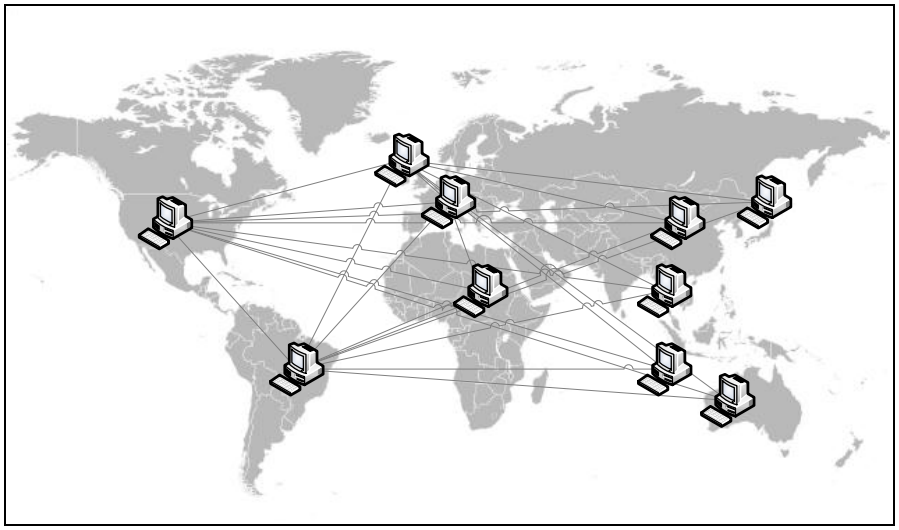


รูปที่ 3 - 14 แสดงภาพรวมหลักการเชื่อมต่ออินเทอร์เน็ตในและต่างประเทศ

3.2.3 เวิล์ดไวด์เว็บ (World Wide Web : www)

เวิล์ดไวด์เว็บ หรือเรียกกันสั้นๆ ว่า “เว็บ” คือรูปแบบหนึ่งของระบบการเชื่อมโยงเครือข่ายข่าวสาร ใช้ในการค้นหาข้อมูลข่าวสาร ซึ่งในอินเทอร์เน็ตนั้นข้อมูลจะอยู่ในรูปแบบของสื่อผสม หรือ มัลติมีเดีย

(Multimedia) ที่มีทั้งตัวอักษร รูปภาพ เสียง หรือภาพเคลื่อนไหว



รูปที่ 3 - 23 แสดงภาพการเชื่อมต่อเป็นเครือข่ายอินเทอร์เน็ต

3.2.4 URL

URL ย่อมาจากคำว่า Uniform Resource Locator คือ ที่อยู่ของข้อมูลต่างๆ ใน อินเทอร์เน็ต เช่น ที่อยู่ของไฟล์หรือเว็บไซต์บนอินเทอร์เน็ต

รูปแบบของ URL จะประกอบด้วย

- ชื่อโปรโตคอลที่ใช้ (http ซึ่งย่อมาจาก HyperText Transfer Protocol)
- ชื่อเครื่องคอมพิวเตอร์ และชื่อเครือข่ายย่อย
- ประเภทของเว็บไซต์
- ไดเร็คทอรี่
- ชื่อไฟล์และนามสกุล

3.2.5 เว็บไซต์ Web Site

เว็บไซต์ พัฒนามาจากเอกสารอิเล็กทรอนิกส์ ที่ใช้รูปแบบการเชื่อมโยงแบบไฮเปอร์ลิงก์หรือไฮเปอร์มีเดีย (Hyperlink/Hypermedia) ถ้าเปรียบเว็บไซต์เป็นหนังสือ เว็บไซต์ จะมีองค์ประกอบดังนี้

1) โฮมเพจ (Home Page) คือหน้าแรกของเว็บไซต์ จะทำหน้าที่คล้ายหน้าปกหนังสือ คำนำ คำชี้แจงและสารบัญ ดังนั้นในหน้าโฮมเพจจึงประกอบด้วยชื่อเว็บไซต์ สัญลักษณ์ คำแนะนำเว็บไซต์และการเชื่อมโยงไปยังหน้าอื่นๆ ในเว็บไซต์นั้นๆ [7]

2) เว็บเพจ (Web Page) คือหน้าของเว็บที่บรรจุเนื้อหาต่างๆ เหมือนเนื้อหาของหนังสือ แต่ออกแบบเป็นลักษณะของเอกสารอิเล็กทรอนิกส์ที่สามารถเชื่อมโยงไปยังหน้าเอกสารต่างๆ ที่ต้องการ โดยใช้รูปแบบการเชื่อมโยงแบบไฮเปอร์ลิงก์หรือไฮเปอร์มีเดีย (Hyperlink/Hypermedia) [7]

3) เว็บไซต์ (Web site) คือการรวมเอาหน้าเว็บเพจหลายๆ หน้าไว้ด้วยกัน โดยมีโฮมเพจเป็นหน้าปก [10]

3.2.6 Hypertext Link

การเชื่อมโยงหลายมิติ หรือ ไฮเปอร์ลิงก์ (hyperlink) นิยมเรียกโดยย่อว่า ลิงก์ (link) คือ คำหรือวลีต่าง ๆ ที่ปรากฏอยู่ในเอกสารข้อความ ใช้สำหรับเปิดเอกสารอื่นที่เชื่อมโยงด้วยวิธีการคลิกลงบนคำหรือวลีนั้น โดยเฉพาะกับเว็บเพจซึ่งจะทำงานบนเว็บเบราว์เซอร์ ข้อความที่เป็นลิงก์มักจะปรากฏเป็นสีหรือรูปแบบที่โดดเด่นกว่าข้อความรอบข้าง ผู้ใช้งานอินเทอร์เน็ตสามารถคลิกบนลิงก์เพื่อเปลี่ยนหน้าไปยังเว็บเพจที่กำหนดไว้ แทนที่จะพิมพ์ในแถบที่อยู่ของเว็บเบราว์เซอร์โดยตรง

3.2.7 Hypertext Markup Language

เอชทีเอ็มแอล (HTML ย่อมาจาก Hypertext Markup Language) เป็นภาษามาร์กอัปหลักในปัจจุบันที่ใช้ในการสร้างเว็บเพจ หรือข้อมูลอื่นที่เรียกดูผ่านทางเว็บเบราว์เซอร์ ซึ่งตัวโค้ดจะแสดงโครงสร้างของข้อมูล ในการแสดง หัวข้อ ลิงก์ ย่อหน้า รายการ รวมถึงการสร้างแบบฟอร์ม เชื่อมโยงภาพหรือวิดีโอด้วย โครงสร้างของโค้ดเอชทีเอ็มแอลจะอยู่ในลักษณะภายในวงเล็บสามเหลี่ยม [8]

3.2.8 เลขที่อยู่ไอพี (IP Address)

เลขที่อยู่ไอพี คือหมายเลขที่ใช้ในระบบเครือข่าย ใช้โปรโตคอลอินเทอร์เน็ตคล้ายกับหมายเลขโทรศัพท์ ไอพีแอดเดรสมีไว้เพื่อให้ผู้ส่งให้ผู้ส่งรู้ว่าเครื่องของผู้รับคือใคร และผู้รับสามารถรู้ได้ว่าผู้ส่งคือใครเช่นกัน ที่เครื่องคอมพิวเตอร์ เครื่องเร้าท์เตอร์ จะมีหมายเลขเฉพาะตัว โดยใช้เลยฐานสอง จำนวน 32 บิต การเขียนจะเขียนเป็น 4 ชุด แต่ละชุดจะใช้เลขฐานสองจำนวน 8 บิต ซึ่งโดยทั่วไปแล้วผู้คนส่วนใหญ่จะคุ้นเคยกับระบบเลขฐานสิบ จึงมักแสดงผลโดยการใช้เลขฐานสิบ จำนวน 4 ชุด ซึ่งแสดงถึงหมายเลขเฉพาะของเครื่องนั้น [9]

3.2.9 โปรโตคอล (Protocol)

โปรโตคอล (Protocol) คือระเบียบวิธีที่กำหนดขึ้นสำหรับการสื่อสารข้อมูล โดยสามารถส่งผ่านข้อมูลไปยังปลายทางได้อย่างถูกต้อง ซึ่งตัวโปรโตคอลที่นิยมใช้ในปัจจุบันคือ TCP/IP นอกจากนี้ยังมีการออกแบบโปรโตคอลตัวอื่นๆ ขึ้นมาใช้งานอีก เช่น โปรโตคอล IPX/SPX,โปรโตคอล NetBEUI และโปรโตคอล Apple Talk เป็นต้น

3.2.10 HTTP

เอชทีทีพี (HyperText Transfer Protocol : HTTP) คือ โปรโตคอลในระดับชั้นโปรแกรมประยุกต์เพื่อการแจกจ่ายและการทำงานร่วมกันกับสารสนเทศของสื่อผสม ใช้สำหรับการรับทรัพยากรที่เชื่อมโยงกับภายนอก ซึ่งนำไปสู่การจัดตั้งเวิลด์ไวด์เว็บ

การพัฒนาเอชทีทีพีเป็นการทำงานร่วมกันของเวิลด์ไวด์เว็บคอนซอร์เทียม (W3C) และคณะทำงานเฉพาะกิจด้านวิศวกรรมอินเทอร์เน็ต(IETF) ซึ่งมีผลงานเด่นในการเผยแพร่เอกสารขอความเห็น (RFC) หลายชุด เอกสารที่สำคัญที่สุด คือ RFC 2616(เดือนมิถุนายน พ.ศ. 2542) ได้กำหนด HTTP/1.1 ซึ่งเป็นรุ่นที่ใช้กันอย่างกว้างขวางในปัจจุบัน [10]

เอชทีทีพีเป็นมาตรฐานในการร้องขอและการตอบรับระหว่างเครื่องลูกข่ายกับเครื่องแม่ข่าย ซึ่งเครื่องลูกข่ายคือผู้ใช้ปลายทาง (end-user) และเครื่องแม่ข่ายคือเว็บไซต์ เครื่องลูกข่ายจะสร้างการร้องขอเอชทีทีพีผ่านทางเว็บเบราว์เซอร์ เว็บครอว์เลอร์ หรือเครื่องมืออื่น ๆ ที่จัดว่าเป็น ตัวแทนผู้ใช้ (user agent) ส่วนเครื่องแม่ข่ายที่ตอบรับ ซึ่งเก็บบันทึกหรือสร้างทรัพยากร (resource) อย่างเช่นไฟล์เอชทีเอ็มแอลหรือรูปภาพ จะเรียกว่า เครื่องให้บริการต้นทาง (origin server) ในระหว่างตัวแทนผู้ใช้กับเครื่องให้บริการต้นทางอาจมีสื่อกลางหลายชนิด อาทิพร็อกซีเกตเวย์และทุนเนล เอชทีทีพีไม่ได้จำกัดว่าจะต้องใช้ชุดเกณฑ์วิธีอินเทอร์เน็ต (TCP/IP) เท่านั้น แม้ว่าจะเป็นการใช้งานที่นิยมมากที่สุดบนอินเทอร์เน็ตก็ตาม โดยแท้จริงแล้วเอชทีทีพีสามารถนำไปใช้ได้บนโปรโตคอลอินเทอร์เน็ตอื่น ๆ หรือบนเครือข่ายอื่นได้

ปกติเครื่องลูกข่ายเอชทีทีพีจะเป็นผู้เริ่มสร้างการร้องขอก่อน โดยเปิดการเชื่อมต่อด้วยเกณฑ์วิธีควบคุมการขนส่งข้อมูล (TCP) ไปยังพอร์ตเฉพาะของเครื่องแม่ข่าย (พอร์ต 80 เป็นค่าปริยาย) เครื่องแม่ข่ายเอชทีทีพีที่เปิดรอรับอยู่ที่พอร์ตนั้น จะเปิดรอให้เครื่องลูกข่ายส่งข้อความร้องขอเข้ามา เมื่อได้รับการร้องขอแล้ว เครื่องแม่ข่ายจะตอบรับด้วยข้อความสถานะอันหนึ่ง ตัวอย่างเช่น “HTTP/1.1 200 OK” ตามด้วยเนื้อหาของมันเองส่งไปด้วย เนื้อหานั้นอาจเป็นแฟ้มข้อมูลที่ร้องขอ ข้อความแสดงข้อผิดพลาด หรือข้อมูลอย่างอื่นเป็นต้น

3.2.11 ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider : ISP)

ISP คือ หน่วยงานที่ให้บริการเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก ผู้ที่ต้องการใช้งานอินเทอร์เน็ตจะต้องสมัครเข้าเป็นสมาชิกของ ISP ก่อน ซึ่งต้องเสียค่าใช้จ่ายต่างๆ อัตราค่าบริการจะขึ้นอยู่กับ ISP แต่ละราย ISP ในประเทศไทยที่นิยมใช้กันมาก เช่น CAT Telecom 3BB TRUE CS Loxinfo เป็นต้น

3.2.12 Uniform Resource Locator : URL

URL ย่อมาจากคำว่า Uniform Resource Locator คือ ที่อยู่ของข้อมูลต่างๆ ในอินเทอร์เน็ต เช่น ที่อยู่ของไฟล์หรือเว็บไซต์บนอินเทอร์เน็ต [11]

รูปแบบของ URL จะประกอบด้วย

- ชื่อโปรโตคอลที่ใช้ (http ซึ่งย่อมาจาก HyperText Transfer Protocol)
- ชื่อเครื่องคอมพิวเตอร์ และชื่อเครือข่ายย่อย
- ประเภทของเว็บไซต์
- ไดเร็คทอรี่
- ชื่อไฟล์และนามสกุล

3.2.13 Domain Name

ชื่อโดเมน หรือ โดเมนเนม (domain name) หมายถึง ชื่อที่ใช้ระบุลงในคอมพิวเตอร์ (เช่นเป็นส่วนหนึ่งของที่อยู่เว็บไซต์ หรืออีเมลแอดเดรส) เพื่อไปค้นหาในระบบ โดเมนเนมซีสเทม เพื่อระบุถึง ไอพีแอดเดรส ของชื่อนั้นๆ เป็นชื่อที่ผู้จดทะเบียนระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตน บางครั้งเราอาจจะใช้ "ที่อยู่เว็บไซต์" แทนก็ได้

- Domain Name System : DNS

เนื่องจากเลขที่อยู่ไอพีอยู่ในรูปของชุดตัวเลขซึ่งยากต่อการจดจำและอ้างอิงระหว่างการใช้งาน ดังนั้นจึงกำหนดให้มีระบบชื่อโดเมน (Domain Name System : DNS) ซึ่งแปลงเลขที่อยู่ไอพีให้เป็นชื่อโดเมนที่อยู่ในรูปของชื่อย่อภาษาอังกฤษหลายส่วน คั่นด้วยเครื่องหมายจุด ผู้ใช้สามารถจดทะเบียนชื่อโดเมนสำหรับคอมพิวเตอร์ของตนผ่านผู้ให้บริการจดทะเบียนชื่อโดเมนที่ได้รับอนุญาต ซึ่งจะทำการค้นหาหมายเลขดังกล่าว ในฐานข้อมูลแล้วแจ้งให้ Host ดังกล่าวทราบ ระบบ DNS แบ่งออกได้เป็น 3 ส่วน คือ

- Name Resolvers

คือเครื่อง Client ที่ต้องการสอบถามเลขที่อยู่ไอพี เรียกว่า Resolver ซึ่งซอฟต์แวร์ที่ทำหน้าที่เป็น Resolvers นั้นจะถูกสร้างมากับแอพพลิเคชันหรือเป็น Library ที่มีอยู่ใน Client [12]

- Domain Name Space

เป็นฐานข้อมูลของ DNS ซึ่งมีโครงสร้างเป็น Tree หรือเป็นลำดับชั้น แต่ละโหนดคือโดเมนโดยสามารถมีโดเมนย่อย (Sub Domain) ซึ่งจะใช้จุดในการแบ่งแยก [12]

- Name Servers

เป็นคอมพิวเตอร์ที่รันโปรแกรมจัดการฐานข้อมูลบางส่วนของ DNS โดย Name Server จะตอบรับการร้องขอทันที โดยการหาข้อมูลตัวเอง หรือส่งต่อการร้องขอไปยัง Name Server อื่น ซึ่งถ้า Name Server มีข้อมูลของส่วนโดเมนแสดงว่า Server นั้นเป็นเจ้าของโดเมนเรียกว่า Authoritative แต่ถ้าไม่มีเรียกว่า Non-Authoritative [12]

3.2.14 วิธีการจดทะเบียนโดเมนเนมในประเทศไทย

การจดทะเบียนชื่อโดเมน แบ่งออกเป็น 2 ประเภท คือ

1) การจดทะเบียนโดเมนต่างประเทศ

- .com ใช้ทำเว็บไซต์ของบริษัท ห้างร้านโดยทั่วไป รวมทั้งเว็บไซต์ส่วนตัว
- .net ใช้ทำเว็บบนไซต์เกี่ยวกับระบบเน็ตเวิร์คของคอมพิวเตอร์ หรือเว็บไซต์บริการอินเทอร์เน็ต
- .org ใช้ทำเว็บไซต์ของส่วนราชการ

2) การจดทะเบียนโดเมนภายในประเทศ

- .co.th ใช้ทำเว็บไซต์ของบริษัท ห้างร้านโดยทั่วไป
- .or.th ใช้ทำเว็บไซต์ของส่วนราชการ และชื่อโดเมนต้องเป็นชื่อขององค์กร หรือตัว ย่อของชื่อองค์กรนั้นๆ ต้องใช้สำเนาเอกสารทางราชการ เป็นหลักฐานการจด ทะเบียน
- .ac.th ใช้ทำเว็บไซต์ของสถานศึกษาต่างๆ ชื่อของโดเมนที่จดทะเบียน

ต้องเป็นชื่อของสถานศึกษานั้นๆ หรือชื่อย่อของชื่อสถานศึกษา ใช้สำเนาเอกสารการขออนุญาตก่อตั้งสถานศึกษาเป็นหลักฐานการจดทะเบียน

- .go.thใช้ทำเว็บไซต์ส่วนของราชการ โดยปกติจะเป็นองค์กรขนาดใหญ่

- .in.th ใช้ทำเว็บไซต์ของบุคคลธรรมดาโดยทั่วไป ชื่อโดเมนจะใช้ชื่ออะไรก็ได้ แต่ต้องอยู่ภายใต้นโยบายชื่อโดเมน ของ THNIC การจดโดเมนนี้ ใช้สำเนาบัตรประชาชน หรือสำเนาใบขับขี่เป็นหลักฐานการจดทะเบียน โดยสามารถศึกษารายละเอียดเพิ่มเติมได้ที่ www.thnic.co.th

- หลักที่ใช้ในการตั้งชื่อโดเมน

1) ความยาวของชื่อ Domain ตั้งได้ไม่เกิน 63 ตัวอักษร

2) สามารถใช้ตัวอักษรภาษาอังกฤษผสมกับตัวเลข หรือเครื่องหมายขีด (-) ได้

3) ตัวอักษรภาษาอังกฤษ ใช้ตัวเล็กหรือตัวใหญ่ก็ได้

4) ห้ามใช้เครื่องหมายขีด (-) นำหน้าชื่อ domain

5) ห้ามเว้นวรรคในชื่อโดเมน

3.3 การใช้ประโยชน์จากระบบเครือข่ายคอมพิวเตอร์และระบบอินเทอร์เน็ต

3.3.1 การใช้ประโยชน์จากระบบเครือข่ายคอมพิวเตอร์

ระบบเครือข่ายคอมพิวเตอร์หนึ่งเครือข่ายจะมีการทำงานรวมกันเป็นกลุ่ม ที่เรียกว่า กลุ่มงาน (workgroup) แต่เมื่อเชื่อมโยงหลายๆ กลุ่มงานเข้าด้วยกัน ก็จะเป็นเครือข่ายขององค์กร และถ้าเชื่อมโยงระหว่างองค์กรผ่านเครือข่ายแวน ก็จะได้เครือข่ายขนาดใหญ่ขึ้น การประยุกต์ใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างกว้างขวาง และสามารถใช้ประโยชน์ได้มากมาย ทั้งนี้เพราะระบบเครือข่ายคอมพิวเตอร์ ทำให้เกิดการเชื่อมโยงอุปกรณ์ต่างๆ เข้าด้วยกัน และสื่อสารข้อมูลระหว่างกันได้ โดยการใช้ประโยชน์จากระบบเครือข่ายคอมพิวเตอร์ มีดังนี้

1) การแลกเปลี่ยนข้อมูล

โดยผู้ใช้ในเครือข่ายสามารถที่จะดึงข้อมูลจากส่วนกลาง หรือข้อมูลจากผู้ใช้คนอื่นมาใช้ได้อย่างรวดเร็วและง่ายดาย เหมือนกับการดึงข้อมูลมาใช้จากเครื่องของตนเอง และนอกจากดึงไฟล์ข้อมูลมาใช้แล้ว ยังสามารถคัดลอกไฟล์ไปให้ผู้อื่นได้อีกด้วย

2) การใช้ทรัพยากรร่วมกัน

อุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อกับเครือข่ายนั้น ถือว่าเป็นทรัพยากรส่วนกลางที่ผู้ใช้ในเครือข่ายทุกคน สามารถใช้ได้โดยการสั่งงานจากเครื่องคอมพิวเตอร์ของ ตัวเองผ่านเครือข่ายไปยังอุปกรณ์นั้น เช่น มีเครื่องพิมพ์ส่วนกลางในเครือข่าย เป็นต้น ซึ่งทำให้ประหยัดค่าใช้จ่ายได้ด้วย

3) การใช้โปรแกรมร่วมกัน

ผู้ใช้ในเครือข่ายสามารถที่จะรันโปรแกรมจาก เครื่องคอมพิวเตอร์ส่วนกลาง เช่น โปรแกรม Word, Excel, Power Point ได้ โดยไม่จำเป็นจะต้องจัดซื้อโปรแกรม สำหรับคอมพิวเตอร์ทุกเครื่อง เป็นการประหยัดงบประมาณในการจัดซื้อ และยังประหยัดเนื้อที่ในหน่วยความจำด้วย

4) การทำงานประสานกันเป็นอย่างดี

ก่อนที่เครือข่ายจะเป็นที่นิยม องค์กรส่วนใหญ่จะใช้คอมพิวเตอร์ขนาดใหญ่ เช่น เมนเฟรม หรือมินิคอมพิวเตอร์ ในการจัดการงาน และข้อมูลทุกอย่างในองค์กร แต่ปัจจุบันองค์กรสามารถกระจายงานต่าง ๆ ให้กับหลาย ๆ เครื่อง แล้วทำงานประสานกัน เช่น การใช้เครือข่ายในการจัดการระบบงานขาย โดยให้เครื่องหนึ่งทำหน้าที่จัดการการเกี่ยวกับใบสั่งซื้อ อีกเครื่องหนึ่งจัดการกับระบบสินค้าคงคลัง

5) ติดต่อสื่อสารสะดวก รวดเร็ว

เครือข่ายนับว่าเป็นเครื่องมือที่ใช้ในการติดต่อสื่อสาร ได้เป็นอย่างดี ผู้ใช้สามารถแลกเปลี่ยนข้อมูล กับเพื่อนร่วมงานที่อยู่คนละที่ ได้อย่างสะดวก และรวดเร็ว

6) เรียกใช้ข้อมูลได้ทุกที่ ทุกเวลา

เครือข่ายในปัจจุบันมักจะมีการติดตั้งคอมพิวเตอร์ เครื่องหนึ่งเป็นเซิร์ฟเวอร์ เพื่อให้ผู้ใช้สามารถเข้าใช้เครือข่ายจากระยะไกล เช่น จากที่บ้าน โดยใช้ติดตั้งโมเด็มเพื่อใช้หมุนโทรศัพท์เชื่อมต่อ เข้ากับเครื่องเซิร์ฟเวอร์ คอมพิวเตอร์เครื่องนั้นก็จะเป็นส่วนหนึ่งของเครือข่าย[3]

3.3.2 การใช้ประโยชน์จากระบบเครือข่ายอินเทอร์เน็ต

อินเทอร์เน็ต (Internet) เป็นเครือข่ายคอมพิวเตอร์รูปแบบหนึ่ง ที่มีผู้ใช้งานหลายสิบล้านคนกระจายไปทั่วโลก และมีรูปแบบการใช้ประโยชน์แตกต่างกันไปตามความต้องการของผู้ใช้ อาทิ

1) **การสืบค้นหาข้อมูลบนอินเทอร์เน็ต (Search Engine)**

Search Engine คือโปรแกรมที่ช่วยในการสืบค้นหาข้อมูล โดยเฉพาะข้อมูลบนอินเทอร์เน็ต โดยครอบคลุมทั้งข้อความ รูปภาพ ภาพเคลื่อนไหว เพลง ซอฟต์แวร์ แผนที่ ข้อมูลบุคคล กลุ่มข่าว และอื่น ๆ ซึ่งแตกต่างกันไปแล้วแต่โปรแกรมหรือผู้ให้บริการแต่ละราย ระบบค้นหาข้อมูลส่วนใหญ่จะค้นหาข้อมูลจากคำสำคัญ (คีย์เวิร์ด) ที่ผู้ใช้ป้อนเข้าไป จากนั้นจะแสดงรายการผลลัพธ์ที่คิดว่าผู้ใช้น่าจะต้องการขึ้นมา ในปัจจุบัน ระบบค้นหาข้อมูลบางตัว เช่น กูเกิล (Google) จะบันทึกประวัติการค้นหาและการเลือกผลลัพธ์ของผู้ใช้ไว้ด้วย และจะนำประวัติที่บันทึกไว้นั้นมาช่วยกรองผลลัพธ์ในการค้นหาครั้งต่อๆ ไป

2) การติดต่อสื่อสาร

2.1) อีเมล (E-Mail)

อีเมล เป็นการส่งข้อความในรูปแบบของจดหมายอิเล็กทรอนิกส์จากคอมพิวเตอร์เครื่องหนึ่งไปยังคอมพิวเตอร์อีกเครื่องหนึ่ง โดยการส่งข้อความดังกล่าวนั้น จะถูกส่งผ่านโปรแกรม

คอมพิวเตอร์ไปยังเมลเซิร์ฟเวอร์ (Mail Server) ผ่านทางอินเทอร์เน็ต จากนั้นข้อมูลจะถูกนำไปเก็บไว้ในเมลล์บ็อกซ์ของผู้รับ

2.2) เครือข่ายสังคมออนไลน์ (Social Network)

Social Network คือ แพลตฟอร์ม (สภาวะแวดล้อมในการทำงานร่วมกัน) หรือเว็บไซต์ที่มุ่งเน้นไปในการสร้างและสะท้อนให้เห็นถึงเครือข่าย หรือความสัมพันธ์ทางสังคม ในกลุ่มคนที่มีความสนใจ หรือมีกิจกรรมร่วมกัน บริการเครือข่ายทางสังคม จะมีองค์ประกอบหลักที่ใช้เป็นตัวแทนของผู้ใช้งาน เช่น ข้อมูลส่วนตัว ความสัมพันธ์เชื่อมโยงระหว่างแต่ละบุคคล และบริการเสริมต่างๆ ที่มีความหลากหลาย บริการเครือข่ายทางสังคมเกือบทั้งหมด จะให้บริการผ่านหน้าเว็บ และให้มีการตอบโต้กันระหว่างผู้ใช้งานผ่านทางอินเทอร์เน็ต

<u>ตัวอย่างเครือข่ายทางสังคมออนไลน์</u>

เฟซบุ๊ก (Facebook) เป็นบริการเครือข่ายสังคมและเว็บไซต์ เปิดใช้งานเมื่อ 4 กุมภาพันธ์ พ.ศ. 2547 ก่อตั้งขึ้นโดย มาร์ก ซักเคอร์เบิร์ก ร่วมกับเพื่อนร่วมห้องในวิทยาลัย จากข้อมูลเดือนมีนาคม ค.ศ. 2012 เฟซบุ๊กมีผู้ใช้ประจำ 901 ล้านบัญชี ผู้ใช้สามารถสร้างข้อมูลส่วนตัว เพิ่มรายชื่อผู้ใช้อื่นในฐานะเพื่อนและแลกเปลี่ยนข้อความ รวมถึงได้รับแจ้งโดยทันทีเมื่อพวกเขาปรับปรุงข้อมูลส่วนตัว นอกจากนั้นผู้ใช้ยังสามารถร่วมกลุ่มความสนใจส่วนตัว จัดระบบตาม สถานที่ทำงาน โรงเรียน มหาวิทยาลัย หรือ อื่น ๆ

อินสตาแกรม (Instagram) เป็นโปรแกรมแบ่งปันรูปภาพ โดยถูกคิดค้นและพัฒนาขึ้นมาในเดือน ตุลาคม พ.ศ. 2553 โดยผู้ใช้งานสามารถถ่ายรูปและตกแต่งรูปภาพได้ตามใจต้องการ และแบ่งปันผ่าน โซเชียลเน็ตเวิร์ก โดยการตกแต่งรูปนั้นจะเน้นในแนวย้อนยุค หรือ กล้องโพลารอยด์

ทวิตเตอร์ (Twitter) เป็นบริการเครือข่ายสังคมออนไลน์จำพวกไมโครบล็อก โดยผู้ใช้สามารถส่งข้อความยาวไม่เกิน 140 ตัวอักษร ว่าตัวเองกำลังทำอะไรอยู่ หรือ ทวีต (tweet - เสียงนกร้อง) ทวิตเตอร์ก่อตั้งขึ้นโดย แจ็ก คอร์ซีย์ ,บิซ สโตน และ อีวาน วิลเลียมส์ เจ้าของบริษัท Obvious Corp ที่ซานฟรานซิสโก สหรัฐอเมริกา เมื่อเดือนมีนาคม พ.ศ. 2549

กูเกิลพลัส (Google+) เป็นบริการเครือข่ายสังคมออนไลน์ให้บริการโดยกูเกิล โดยเปิดให้ใช้งานครั้งแรกเมื่อวันที่ 28 มิถุนายน พ.ศ. 2554 ผู้ที่จะเข้ามาทดลองใช้ต้องได้รับเชิญจากบุคคลที่ใช้อยู่เท่านั้น ภายหลังในวันที่ 20 กันยายน พ.ศ. 2554 จึงเปิดให้ผู้ใช้ทั่วไปได้ใช้งาน

โซเชียลแคม (Socialcam) เป็นโปรแกรมวิดีโอมือถือทางสังคมสำหรับไอโฟน และ แอนดรอยด์ ช่วยให้ผู้ใช้งานสามารถจับภาพและแบ่งปันวิดีโอออนไลน์บนมือถือรวมทั้งผ่านทางเฟซบุ๊ก ทวิตเตอร์ และเครือข่ายทางสังคมอื่นๆ

ยูทูบ (YouTube) เป็นเว็บไซต์ที่ให้ผู้ใช้งานสามารถอัปโหลดและแลกเปลี่ยนคลิปวีดีโอผ่านทางเว็บไซต์ ก่อตั้งเมื่อ 15 กุมภาพันธ์ พ.ศ. 2548 โดย แชด เฮอร์ลีย์, สตีฟ เชง และ ยาวีด คาริม อดีตพนักงานบริษัทเพย์พอล (paypal) และมีสำนักงานอยู่ที่ ซานบรูโนในมลรัฐแคลิฟอร์เนีย ปัจจุบันยูทูบเป็นส่วนหนึ่งของกูเกิล

ไลน์ (Line) เป็นบริการเครือข่ายสังคมออนไลน์ที่พัฒนาจากโปรแกรมสนทนาสำหรับอุปกรณ์พกพา ไลน์สามารถใช้การติดต่อแบบเสียงได้เหมือนการโทรศัพท์ทั่วไป ผ่านโปรแกรม

โดยไม่ต้องเสียค่าบริการกับผู้ให้บริการโทรศัพท์ ในส่วนของการส่งข้อความยังมีรูปภาพประกอบที่น่ารักเป็นที่ชื่นชอบของวัยรุ่นอีกด้วย

3.4 การรักษาความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย

ระบบเครือข่ายไร้สายและระบบอินเทอร์เน็ตได้กลายมาเป็นวิธีการสื่อสารหลักสำหรับผู้คนสมัยใหม่ แต่การรักษาความปลอดภัยในระบบนี้ยังไม่ได้รับการพัฒนาให้ดีพอ ทั้ง ๆ ที่การรักษาความปลอดภัยข้อมูลและข่าวสารส่วนบุคคลในระบบเครือข่ายสมัยใหม่ควรจะเป็นเรื่องที่ต้องให้ความสำคัญเป็นอย่างยิ่ง คณะวิจัยกลุ่มหนึ่งในมหาวิทยาลัย Carnegie-Mellon ประเทศสหรัฐอเมริกาได้จัดตั้งทีมสำหรับให้ความช่วยเหลือผู้ใช้ระบบคอมพิวเตอร์ชื่อ CERT (Computer Emergency Response Team) ขึ้นในปี พ.ศ 2532 ซึ่งจะให้ความช่วยเหลือพร้อมทั้งรวบรวมข้อมูลทางสถิติของเหตุการณ์ที่เกี่ยวข้องทางด้านความปลอดภัยที่เกิดขึ้นในระบบอินเทอร์เน็ต ในปีดังกล่าวมีเหตุการณ์เกิดขึ้นเพียง 132 ครั้งเท่านั้น แต่ในปี พ.ศ. 2542 เกิดขึ้นมากถึง 9,859 ครั้ง และเพียงสิ้นเดือนเมษายนปี พ.ศ. 2543 ได้มีเหตุการณ์เกิดขึ้นแล้วถึง 4,266 ครั้ง รวมตั้งแต่ปี พ.ศ. 2531 ถึง 2543 มีเหตุการณ์เกี่ยวข้องกับการรักษาความปลอดภัยที่ทีม CERT รวบรวมไว้มากกว่า 30,000 ครั้ง เหตุการณ์ที่เกิดขึ้นส่วนใหญ่เป็นผลงานของพวกแฮกเกอร์ (Hackers) ซึ่งเป็นกลุ่มเป็นบุคคลที่เขียนโปรแกรมขึ้นมาเพื่อบุกรุกเข้าไปในระบบเครือข่ายที่ตนเองไม่ได้รับอนุญาตให้เข้าไปใช้บริการ ระบบคอมพิวเตอร์ของหน่วยงานราชการ มหาวิทยาลัย และองค์กรเอกชนมักจะตกเป็นเป้าหมายของแฮกเกอร์ แต่ในช่วงหลายปีที่ผ่านมานี้ ปรากฏว่าคนทั่วไปก็กลายเป็นเป้าหมายของแฮกเกอร์เช่นกัน

การปกป้องข้อมูลบนระบบเครือข่ายมีความยุ่งยากมากซึ่งมักจะเป็นอยู่กับชนิดของสื่อที่ใช้ สถานที่ตั้งเทอร์มินอล และระดับการให้บริการแก่ผู้ใช้ บางครั้งอาจใช้การป้องกันทางฮาร์ดแวร์บางครั้งใช้ซอฟแวร์ แต่ส่วนใหญ่ต้องใช้ทั้งซอฟต์แวร์และฮาร์ดแวร์

ระบบการรักษาความปลอดภัยแบ่งออกเป็นหลายระดับ เรียกว่า ระดับการรักษาความปลอดภัย (Security levels) ผู้ที่ทำหน้าที่ในการรักษาความปลอดภัยโดยปกติจะมีเพียงคนเดียวคือ ผู้จัดการระบบเครือข่าย (Network Administrator) จะต้องได้รับอนุญาตให้เข้าไปใช้ข้อมูลและโปรแกรมทั้งหมดที่มีอยู่ในระบบเครือข่ายได้ ในขณะที่ผู้ใช้แต่ละคนจะได้รับอนุญาตให้ใช้ข้อมูล โปรแกรม เทอร์มินอล และอุปกรณ์ต่าง ๆ ได้เท่าที่จำเป็นตามระดับการรักษาความปลอดภัย ผู้ใช้ที่อยู่ในระดับการรักษาความปลอดภัยขั้นต่ำสุดจะได้รับอนุญาตให้ใช้บริการต่าง ๆ น้อยที่สุดซึ่งเป็นมาตรการการรักษาความปลอดภัยที่เข้มงวดมากและเหมาะที่จะนำมาใช้ในระบบเครือข่ายเพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาต เข้ามาปั่นป่วนการทำงานหรือนำไวรัสคอมพิวเตอร์เข้ามาเผยแพร่ในระบบ

การรักษาความปลอดภัยที่จำเป็นสำหรับระบบเครือข่ายทุกแบบ การรักษาความปลอดภัยทางกายภาพและการใช้ซอฟต์แวร์ รวมทั้งการรักษาความปลอดภัยเมื่อใช้งานระบบอินเทอร์เน็ตและบนระบบเครือข่ายไร้สาย

1) การรักษาความปลอดภัยทางกายภาพ

ระบบคอมพิวเตอร์ยุคแรก ๆ นำวิธีการรักษาความปลอดภัยทางกายภาพ (Physical

Security) มาใช้งานอย่างได้ผลด้วยการติดตั้งเครื่องเมนเฟรมคอมพิวเตอร์และเครื่องเทอร์มินอลทั้งหมดไว้ในห้องที่มีรั้วรอบขอบชิด เมื่อไม่ต้องการให้ใช้งานก็ปิดห้องและใส่กุญแจอย่างแน่นหนา เฉพาะผู้ที่มีลูกกุญแจเท่านั้นจึงจะสามารถเข้าห้องนี้ได้ ต่อมาเมื่อมีการเชื่อมต่อเครื่องเทอร์มินอลจากสถานที่อื่นให้สามารถใช้งานเครื่องเมนเฟรมได้ทำให้การรักษาความปลอดภัยยุ่งยากขึ้น และการที่ข้อมูลจะต้องถูกส่งผ่านสายสื่อสารไปยังสถานที่ห่างไกลทำให้มีความเสี่ยงจากการถูกขโมยสัญญาณ (Tapping) เพิ่มขึ้น ในปัจจุบัน การใช้เครื่องพีซีโน้ตบุ๊กและอุปกรณ์มือถือที่เชื่อมต่อเข้ากับระบบเครือข่ายทำให้การรักษาความปลอดภัยยิ่งทวีความสำคัญมากขึ้นกว่าแต่ก่อนมาก

1.1) มาตรการควบคุมการการเข้ามาใช้ระบบเครือข่ายทางกายภาพ

การนำเครื่องคอมพิวเตอร์และอุปกรณ์เก็บไว้ในห้องที่ปิดมิดชิดและใส่กุญแจเป็นวิธีการรักษาความปลอดภัยทางกายภาพชนิดหนึ่ง วิธีการอื่นได้แก่การใช้เครื่องอ่านลายนิ้วมือแทนการใช้กุญแจ บางแห่งมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อควบคุม การเข้า-ออกพื้นที่ที่ต้องการรักษาความปลอดภัย หรือการใช้อุปกรณ์ตรวจจับการเคลื่อนไหวในพื้นที่และช่วงเวลาที่ไม่ต้องการให้ใช้งาน

การเลือกใช้สื่อสำหรับการถ่ายทอดข้อมูลมีผลต่อการรักษาความปลอดภัยทางกายภาพ เช่น การถ่ายทอดข้อมูลโดยใช้วิธีแพร่กระจายคลื่นมีความปลอดภัยน้อยกว่าการถ่ายทอดข้อมูลผ่านสื่อประเภทสายสื่อสาร (สายใยแก้วนำแสงเป็นสื่อที่มีความปลอดภัยสูงที่สุดในปัจจุบัน) คนทั่วไปที่อยู่ภายในเขตรัศมีการแพร่กระจายคลื่นจะสามารถรับฟังสัญญาณได้และอาจนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต ในกรณีที่การส่งข้อมูลด้วยคลื่นวิทยุเป็นหนทางเลือกเพียงวิธีเดียวที่มีอยู่ ข้อมูลจะต้องถูกเข้ารหัส (Encryption) ก่อนที่จะส่งออกไป การเข้ารหัสคือการเปลี่ยนแปลงรูปแบบข้อมูลซึ่งจะกล่าวถึงในลำดับต่อไป

องค์กรที่ยอมให้ผู้ใช้เข้าระบบผ่านทางระบบเครือข่ายโทรศัพท์ก็จะมีปัญหาในเรื่องความปลอดภัยแม้ว่าจะเป็นสื่อประเภทสายสื่อสารก็ตาม การขโมยสัญญาณโดยตรงด้วยการแทปสาย (Tapping) คือการพ่วงสายสัญญาณแบบเดียวกับการพ่วงสายโทรศัพท์สามารถทำได้ง่ายเนื่องจากระบบเครือข่ายโทรศัพท์อยู่ภายนอกการควบคุมขององค์กร โปรแกรมบางอย่างถูกออกแบบมาสำหรับการขโมยข้อมูลผ่านระบบเครือข่ายโทรศัพท์โดยเฉพาะ ระบบเครือข่ายองค์กรหลายแห่งจะติดตั้งโมเด็มไว้คอยรับสัญญาณการเชื่อมต่อจากผู้ใช้ภายนอกโปรแกรมที่จะขโมยข้อมูลก็จะใช้โมเด็มติดต่อเข้ามา และพยายามเจาะเข้าไปในระบบด้วยวิธีการต่าง ๆ

1.2) อุปกรณ์รักษาความปลอดภัยระบบเครือข่ายและข้อมูล

องค์กรที่ใช้ระบบเครือข่ายในการถ่ายทอดข้อมูลจะต้องหาวิธีป้องกันการนำข้อมูลไปใช้หรือการเปลี่ยนแปลงข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต ไม่ว่าการถ่ายทอดข้อมูลจะใช้สื่อประเภทใดก็ตามข้อมูลก็อาจถูกขโมยไปใช้ได้เสมอ เช่น สายโทรศัพท์อาจถูกเทปสายตรงจุดไหนก็ได้ หรือการใช้คลื่นวิทยุในรูปแบบต่าง ๆ ก็อาจถูกขโมยสัญญาณไปใช้ได้ตลอดเวลา

วิธีการรักษาความปลอดภัยอย่างหนึ่งเรียกว่า อุปกรณ์โทรกลับ (Call Back Unit) ซึ่งมีความสามารถในการป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้งานระบบแม้ว่าผู้นั้นจะมีชื่อผู้ใช้และรหัสผ่านที่ถูกต้องก็ตาม อุปกรณ์นี้จะให้ผู้ใช้โทรเข้ามาโดยใช้โมเด็มตามปกติ แต่ว่าผู้ใช้จะโทรเข้ามาเพื่อป้อนรหัสการใช้

งานเท่านั้น แล้วก็จะต้องวางโทรศัพท์ อุปกรณ์โทรกลับจะนำรหัสการใช้งานไปตรวจสอบควบคู่กับหมายเลขโทรศัพท์ที่ผู้ใช้โทรเข้ามา ถ้ารหัสการใช้งานถูกต้องและ (ขึ้นอยู่กับระดับการรักษาความปลอดภัย) หมายเลขโทรศัพท์นั้นเป็นหมายเลขที่กำหนดให้ใช้ล่วงหน้า อุปกรณ์โทรกลับจึงจะโทรกลับไปหาผู้ใช้และอนุญาตให้ใช้งานได้ตามปกติ มิฉะนั้นก็จะไม่ตอบกลับไป แม้ว่าผู้นั้นจะพยายามโทรกลับมาอีกกี่ครั้งก็ตามถ้ารหัสการใช้งานไม่ถูกต้องก็จะไม่ได้รับอนุญาตให้ใช้ระบบอยู่ดี

อุปกรณ์โทรกลับก็เหมือนกับอุปกรณ์แบบอื่น ๆ คือต้องมีจุดอ่อน แม้ว่าอุปกรณ์นี้จะไม่ได้เพิ่มปริมาณงานเข้ามาในระบบเครือข่ายแต่การโทรกลับทำให้องค์กรกลายเป็นผู้ที่จะต้องจ่ายค่าบริการโทรศัพท์ โดยเฉพาะถ้าเป็นโทรศัพท์ทางไกลก็จะยิ่งเพิ่มค่าใช้จ่ายสูงขึ้นปัญหานี้อาจแก้ไขโดยให้ทางองค์กรเก็บค่าบริการโทรศัพท์จากผู้ใช้ ปัญหาที่สองคือผู้ใช้จะต้องโทรมาจากสถานที่ที่มีหมายเลขโทรศัพท์แบบถาวร เช่น ตามสถานที่ทำงานหรือบ้านพักเพราะระบบนี้จะโทรกลับไปยังหมายเลขโทรศัพท์ที่ได้รับการกำหนดไว้ล่วงหน้าเท่านั้น ผู้ใช้ที่ต้องเดินทางอยู่เสมอ เช่น บุคลากรฝ่ายขาย จะไม่มีหมายเลขโทรศัพท์ที่แน่นอน (แต่เป็นกลุ่มบุคลากรที่เป็นเป้าหมายในการโจมตีจากผู้บุกรุกมากที่สุด) จึงไม่อาจนำระบบนี้มาใช้งานได้อย่างไรก็ตาม การนำโทรศัพท์มือถือมาใช้ก็สามารถแก้ปัญหานี้ได้ แต่อัตราค่าบริการโทรศัพท์มือถือมักจะแพงกว่าโทรศัพท์ปกติ

2) ซอฟต์แวร์รักษาความปลอดภัย

หลังจากการติดต้องการรักษาความปลอดภัยทางกายภาพไปแล้ว ขั้นต่อไปคือการติดตั้งซอฟต์แวร์รักษาความปลอดภัย (Software Security) เพื่อการรักษาป้องกันข้อมูล หัวข้อนี้กล่าวถึงวิธีการที่นำมาใช้ทั่วไปคือ การใช้ชื่อผู้ใช้ รหัสผ่าน และการเข้ารหัสข้อมูล รวมทั้งการคุกคามจากไวรัสคอมพิวเตอร์และวอร์ม

2.1) ชื่อผู้ใช้และรหัสผ่าน

การรักษาความปลอดภัยด้วยซอฟต์แวร์แบบที่นิยมใช้มากที่สุดคือการกำหนดชื่อผู้ใช้สำหรับระบบคอมพิวเตอร์ (user name) และกำหนดรหัสผ่าน (password) ให้แก่ผู้ใช้ทุกคนผู้ใช้แต่ละคนควรรักษาชื่อผู้ใช้โดยเฉพาะอย่างยิ่งรหัสไว้เป็นความลับอย่างที่สุด โดยปกติรหัสผ่านควรมีความยาวไม่น้อยกว่า 8 ตัวอักษรและเลือกใช้ตัวอักษรและสัญลักษณ์ที่ยากแก่การเดา การนำชื่อคู่สมรส ลูก สัตว์เลี้ยงมาใช้ถือว่าเป็นรหัสผ่านที่ไม่ดีเพราะสามารถเดาได้ง่ายโดยคนใกล้ชิด ในระบบที่มีความลับมาก ควรเปลี่ยนรหัสผ่านอยู่เสมอ

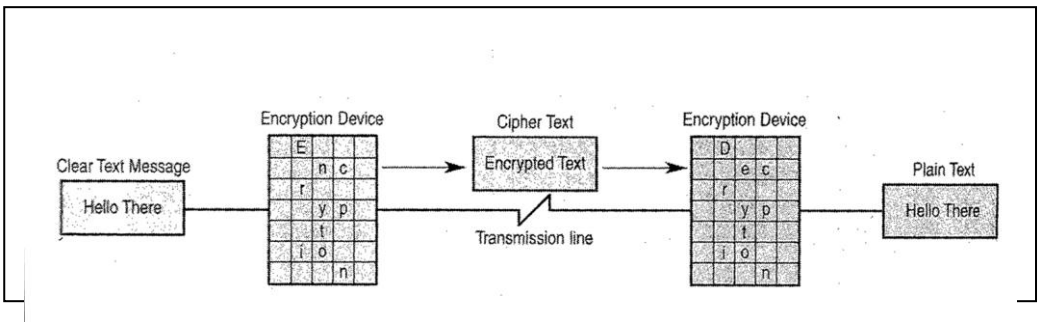
ซอฟต์แวร์ระบบเครือข่ายสามารถนำมาใช้ในการตรวจสอบการใช้งานของชื่อผู้ใช้และรหัสผ่าน รายงานจะมีข้อมูลเกี่ยวกับการใช้งานระบบของชื่อผู้ใช้แต่ละชื่อ และอาจมีข้อมูลรายละเอียดการใช้งานต่าง ๆ เช่น ใช้งานจากเทอร์มินอลเครื่องใด ความพยายามในการใช้ชื่อผู้ใช้แต่ใช้รหัสผ่านไม่ถูกต้องหลาย ๆ ครั้งเป็นจุดที่ซอฟต์แวร์ต้องตรวจพบ เพราะอาจเป็นความพยายามเข้ามาบุกรุกระบบจากบุคคลภายนอกก็ได้

การกำหนดชื่อผู้ใช้และรหัสผ่านสามารถนำมาใช้สำหรับโปรแกรมประยุกต์แต่ละโปรแกรมได้ หมายความว่า ผู้ใช้แต่ละคนเมื่อสามารถเข้ามาสู่ระบบได้แล้ว ยังไม่สามารถใช้โปรแกรมบางอย่างได้ เช่น ระบบจัดการฐานข้อมูล ซึ่งจะกำหนดชื่อผู้ใช้และรหัสผ่านขึ้นอีกชุดหนึ่งที่แตกต่างออกไป ทำให้ผู้ใช้แต่ละคน

มีสิทธิในการใช้ซอฟต์แวร์ในระบบแตกต่างออกไปคล้ายกับการซื้อบัตรผ่านประตูเข้าไปในสวนสนุก ภายในสวนสนุกจะมีเครื่องเล่นมากมายที่บางส่วนก็ให้เล่นได้ฟรี และบางส่วนก็ต้องซื้อบัตรเพิ่มเพื่อเล่นเครื่องเล่นนั้นต่างหาก การซื้อบัตรผ่านประตูก็เปรียบได้กับการใช้ชื่อผู้ใช้และรหัสผ่านเพื่อเข้าสู่ระบบ จากนั้นบางโปรแกรมก็สามารถใช้งานได้ในทันที ในขณะที่โปรแกรมบางอย่างจะต้องซื้อบัตรเพิ่ม คือจะต้องมีชื่อผู้ใช้และรหัสผ่านอีกชุดหนึ่งต่างหาก วิธีการนี้ทำให้การใช้งานระบบมีความยุ่งยากซับซ้อนมาก คือจะต้องจดจำชื่อผู้ใช้และรหัสผ่านหลายชุด แต่ก็เพิ่มระดับความปลอดภัยให้สูงมากขึ้นด้วย ระบบบางระบบบังคับให้ผู้ใช้ต้องเปลี่ยนรหัสผ่านเป็นประจำ

2.2) การเข้ารหัสข้อมูล

วิธีการทำให้ข้อมูลปลอดภัยที่ดีวิธีหนึ่งคือ การเข้ารหัสข้อมูล (Encryption) ซึ่งหมายถึงการเปลี่ยนข้อมูลจากรูปแบบปกติไปเป็นรูปแบบอื่นที่ทำให้ดูเหมือนว่าไม่มีความหมายใด ๆ สำหรับผู้ที่ไม่ทราบวิธีการแก้ไขหรือไม่มีอุปกรณ์ที่เหมาะสม ดังแสดงในรูป 9.1 ข้อมูลพิเศษชุดหนึ่ง เรียกว่า กุญแจเข้ารหัส (Encryption key) หรืออุปกรณ์เข้ารหัส (Encryption device) ถูกนำมาใช้ในการเปลี่ยนข้อมูลธรรมดา (Clear text or Plain text) ไปเป็นรูปแบบที่แตกต่างไปจากปกติ เรียกว่า ข้อมูลที่เข้ารหัส (Encrypted text or Cipher text) ซึ่งจะถูกส่งเข้าสู่ระบบเครือข่าย ถ้าข้อมูลนี้ถูกขโมยไปใช้ ผู้ที่นำข้อมูลไปจะไม่สามารถอ่านข้อมูลเหล่านี้ได้โดยไม่มีกุญแจถอดรหัสหรืออุปกรณ์ถอดรหัส เฉพาะผู้รับข้อมูลตัวจริงเท่านั้นที่จะทราบวิธีการแปลงข้อมูลเข้ารหัสกลับไปเป็นข้อมูลปกติ



รูปที่ 3-24 กระบวนการเข้าและถอดรหัสข้อมูล

วิธีการเข้ารหัสข้อมูลมีหลักการทำงานเช่นเดียวกันกับการเข้ารหัสสัญญาณโทรทัศน์ที่ส่งมาทางสายเคเบิลหรือส่งออกอากาศของบริษัทยูบีซีทางบริษัทฯ จะนำสัญญาณที่จะส่งมาเข้ารหัสเสียก่อน จากนั้นจึงจะแพร่สัญญาณภาพออกไป โดยปกติคนทั่วไปแม้ว่าจะมีเครื่องรับสัญญาณหรือสามารถเชื่อมต่อเข้ากับสายเคเบิลได้ก็ตามจะได้รับสัญญาณที่เข้ารหัสไว้ ทำให้ไม่สามารถรับชมรายการโทรทัศน์ได้ตามปกติ ในขณะที่ลูกค้าของบริษัทยูบีซีจะได้รับการติดตั้งอุปกรณ์ถอดรหัสสัญญาณที่ส่งมาทางอากาศหรือทางสายก็ตามให้กลับเป็นสัญญาณที่สามารถรับชมได้ตามปกติ

ข้อมูลที่มีความสำคัญที่จะต้องส่งผ่านระบบเครือข่ายจำเป็นจะต้องได้รับการเข้ารหัสก่อนที่จะส่งออกไปวิธีการเข้ารหัสมีอยู่หลายวิธีได้แก่ การเข้ารหัสโดยใช้กุญแจรหัสแบบสามาตรการเข้ารหัสโดยใช้กุญแจรหัสสาธารณะ และการเข้ารหัสแบบอีลิปติกเคอฟ

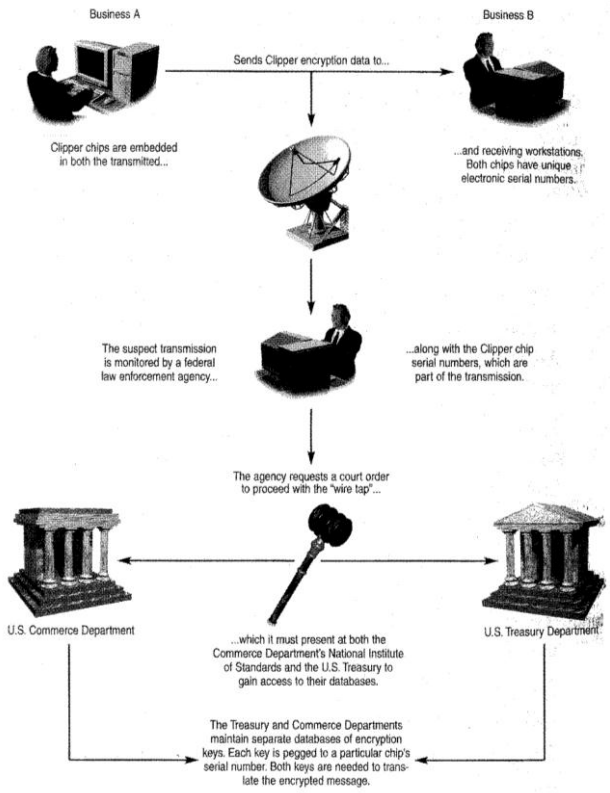
2.3) การเข้ารหัสแบบคีย์สมมาตร

การเข้ารหัสแบบคีย์สมมาตร (Symmetric Key Encryption) จะมีกุญแจรหัสเพียงตัวเดียว ผู้ส่งจะใช้กุญแจนี้สำหรับการเข้ารหัสและทางผู้รับก็จะต้องใช้รหัสตัวเดียวกันในการถอดรหัส การเข้ารหัสแบบคีย์สมมาตรที่เคยถูกนำไปใช้อย่างแพร่หลายในอดีต เรียกว่า การเข้ารหัสแบบดีอีเอส (Data Encryption Standard) ได้รับการพัฒนาขึ้นมาโดยองค์กรชื่อ National Institute of Standards and Technology ในประเทศสหรัฐอเมริกา วิธีการนี้จะแบ่งข้อมูลที่จะนำมาเข้ารหัสเป็นกลุ่ม กลุ่มละ 64 บิต โดยจะเลือกข้อมูลมาเพียง 56 บิต สำหรับการเข้ารหัส ผลที่เกิดขึ้นนั้นไม่เป็นที่น่าพอใจเนื่องจากมีประสิทธิภาพต่ำกว่าที่ต้องการนั่นคือสามารถใช้เครื่องคอมพิวเตอร์ประสิทธิภาพสูงมาถอดรหัสโดยไม่ต้องใช้กุญแจรหัสได้ภายใน 6 เดือน หรือน้อยกว่านี้ (ในการรักษาข้อมูลที่มีความลับมาก ระยะเวลาเพียง 6 เดือนถือว่าสั้นมาก) ผู้เชี่ยวชาญหลายคนคิดว่ากุญแจรหัสขนาด 56 บิต นั้นมีความยาวน้อยเกินไป อย่างไรก็ตาม วิธีการนี้จัดว่ามีความปลอดภัยเพียงพอสำหรับการนำมาใช้งานบางประเภท เช่น การเข้ารหัสหมายเลขบัตรเครดิตเพื่อส่งไปตรวจสอบในการชำระค่าสินค้าหรือบริการผ่านทางระบบอินเทอร์เน็ต แต่ไม่สามารถนำมาใช้ในการทำธุรกรรมโอนเงินข้ามบัญชีผ่านระบบอินเทอร์เน็ตได้ วิธีการนี้ได้รับการรับรองจากรัฐบาลประเทศสหรัฐอเมริกาให้เป็นวิธีการมาตรฐานสำหรับการเข้ารหัสข้อมูลที่ไม่จัดอยู่ในประเภทที่ต้องรักษาความลับ (Unclassified documents)

วิธีการดีอีเอสได้รับการพัฒนาต่อมาให้สามารถปกป้องเอกสารได้ดียิ่งขึ้น เรียกว่า ทรีดีอีเอส (Tripple DES; 3DES) ซึ่งนำวิธีการแบบดีอีเอสมาทำงานซ้อนกันสองชั้นโดยใช้กุญแจรหัสที่แตกต่างกัน และมีความยาวรวมกันเป็น 112 บิต ทำให้เพิ่มความปลอดภัยมากขึ้นในขณะที่ไม่ได้เพิ่มปริมาณข้อมูลเข้าสู่ระบบเครือข่ายมากนัก

การเข้ารหัสแบบใช้กุญแจสมมาตรอีกวิธีการหนึ่งเรียกว่า บโลฟิซซ์ (Blowfish) ได้รับการพัฒนาขึ้นมาตั้งแต่ พ.ศ. 2536 โดย Bruce Schneier ซึ่งใช้กุญแจรหัสที่มีความยาวตั้งแต่ 32 ถึง 448 บิต วิธีการนี้ไม่ได้มีการจดทะเบียนลิขสิทธิ์ไว้ ทุกคนจึงสามารถนำมาใช้งานได้โดยอิสระ และกลายเป็นหนทางเลือกที่นิยมนำมาใช้สำหรับผู้ที่ไม่ชอบใช้วิธีดีอีเอส

วิธีไอดีอีเอ (International Data Encryption Algorithm; IDEA) ใช้กุญแจรหัสยาว 128 บิตทำให้กลายเป็นวิธีการที่ให้ความปลอดภัยสูงมากวิธีหนึ่งซึ่งได้รับการพัฒนาขึ้นมาที่เมือง Zurich ประเทศสวิตเซอร์แลนด์ ปัจจุบันเป็นลิขสิทธิ์ของบริษัท Ascom-Tech ประเทศสหรัฐอเมริกา ซึ่งอนุญาตให้ใช้ได้ฟรีสำหรับงานที่ไม่เกี่ยวข้องกับทางธุรกิจ เช่น สถาบันการศึกษาต่าง ๆ



รูปที่ 3-25 การทำงานของคลิปเปอร์ชิป

อุปกรณ์แบบหนึ่งที่ได้รับการกำหนดให้เป็นมาตรฐานสำหรับการใช้งาน เรียกว่าคลิปเปอร์ชิป (Clipper Chip) ดังแสดงในรูป 9.2 เครื่องคอมพิวเตอร์ของทางผู้ส่งและของผู้รับจะต้องติดตั้งคลิปเปอร์ชิป ลักษณะเฉพาะของชิปตัวนี้คือ จะอนุญาตให้ผู้รับที่แท้จริงและหน่วยงานของรัฐบาลกลางสหรัฐสามารถถอดรหัสได้ ทำให้กลายเป็นข้อโต้แย้งเนื่องจากมีบริษัทเอกชนจำนวนมากที่ไม่ต้องการให้รัฐบาลกลางฯ เข้ามาตรวจดูข้อมูลของตนเองได้ตามใจชอบ ชิปตัวนี้ไม่ได้รับการพัฒนาขึ้นมาจนสมบูรณ์ แต่ก็เป็นตัวกระตุ้นให้เกิดการพิจารณาอย่างกว้างขวางเกี่ยวกับการเข้ารหัสข้อมูลโดยเฉพาะอย่างยิ่งเกี่ยวกับสิทธิการถอดรหัสข้อมูลโดยคนระดับต่าง ๆ

2.4) การเข้ารหัสโดยใช้กุญแจสาธารณะ

วิธีการเข้ารหัสข้อมูลอีกแบบหนึ่งเรียกว่า การเข้ารหัสโดยใช้กุญแจสาธารณะ (Public Key Encryption) หรือ การเข้ารหัสโดยใช้กุญแจแบบอสมมาตร (Asymmetric Crypto system) ซึ่งต้องใช้กุญแจรหัสสองตัว องค์กรส่วนใหญ่ที่เลือกใช้วิธีการนี้จะจัดตั้งระบบพีเคไอ (Public Key Infrastructure) ซึ่งประกอบ ด้วย โปรแกรมและขั้นตอนการทำงานที่เกี่ยวข้องกับการเข้ารหัสข้อมูล กุญแจรหัสตัวแรกเรียกว่า กุญแจสาธารณะ (Public key) ซึ่งจะแจกจ่ายให้แก่ผู้ที่เกี่ยวข้องกับการสื่อสารทุกคน กุญแจรหัสตัวที่สอง เรียกว่า กุญแจส่วนตัว (Private Key) ซึ่งจะมีอยู่ที่ผู้รับข่าวสารเท่านั้น ข้อมูลที่ถูกเข้ารหัสแล้วก็จะมีเพียงผู้รับเท่านั้นที่สามารถถอดรหัสได้ ผู้ส่งจะไม่สามารถอ่านข้อความที่เข้ารหัสโดยใช้กุญแจสาธารณะได้

วิธีการพีเคไอแบบที่ได้รับความนิยมมากที่สุดคือ การเข้ารหัสแบบอาร์เอสเอ (RSA) ที่ได้รับการพัฒนาขึ้นมาโดย Ron Rivest, Adi Shamir, และ Leonard Adleman โดยใช้กุญแจรหัสยาว 1024

บิตทำให้กลายเป็นวิธีการเข้ารหัสที่ถือว่าปลอดภัยมากที่สุดแบบหนึ่งวิธีการนี้นำแนวทางการทำงานของวิธีไอดีอีเอมาผสมกับการทำงานของโพรโตคอลพีจีพี (Pretty Good Privacy) ที่ใช้งานในการส่งที่ต้องการเข้ารหัสและใช้ปกป้องแฟ้มข้อมูลของผู้ใช้ พีจีพีได้รับการพัฒนาขึ้นมาโดย Phil Zimmerman ซึ่งได้รับการนำไปใช้งานอย่างกว้างขวางในระดับสากลสำหรับการเข้ารหัสและถอดรหัสแฟ้มข้อมูลและเป็นวิธีการเข้ารหัสที่มีความปลอดภัยมากอีกแบบหนึ่ง

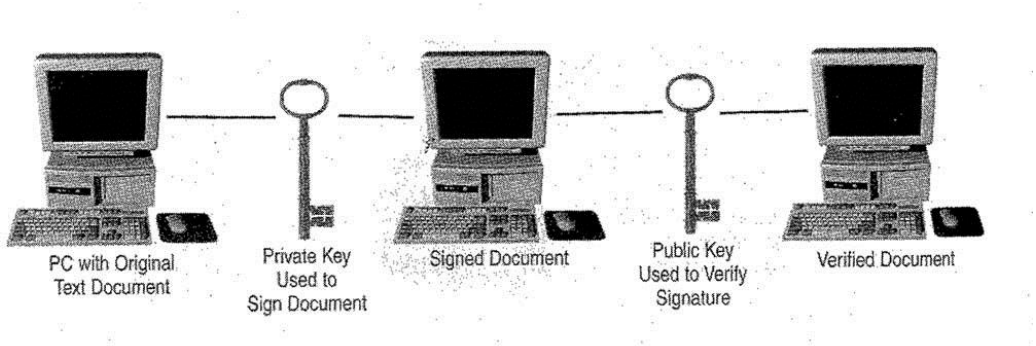
2.5) การเข้ารหัสโดยวิธีอีลิปติกเคอฟ

การเข้ารหัสแบบอีลิปติกเคอฟ (Elliptic Curve) เป็นวิธีการใหม่สำหรับการเข้ารหัสข้อมูลซึ่งมีวิธีการทำงานเหมือนวิธีอาร์เอสเอเกือบทุกอย่างยกเว้นการใช้วิธีการเรียกว่า Elliptical curve discrete logarithm สำหรับการสร้างกุญแจรหัสขึ้นมาใช้งาน ซึ่งมีวัตถุประสงค์ในการลดจำนวนบิตของกุญแจรหัสลงทำให้มีประสิทธิภาพสูงขึ้นในขณะที่ยังคงมีความปลอดภัยในระดับเดิม

3) ลายเซ็นดิจิตอล

การเข้ารหัสแบบใช้กุญแจสาธารณะใช้ลายเซ็นดิจตอล (Digital Signature) สำหรับการตรวจสอบความถูกต้องของแฟ้มข้อมูลที่ส่งมาทางระบบเครือข่ายในลักษณะที่ผู้ใช้สามารถแน่ใจได้ว่าข้อมูลที่ปรากฏในเอกสารนั้นไม่ได้ถูกแก้ไขโดยผู้อื่นใดนอกจากเจ้าของเอกสารนั้น วัตถุประสงค์ข้อที่สองคือ นำมาใช้ในการแสดงความเป็นเจ้าของเอกสาร โดยปกติเอกสารอิเล็กทรอนิกส์จะไม่สามารถบอกได้ว่าผู้ใดคือเจ้าของที่แท้จริง แต่การใส่ลายเซ็นดิจิตอลเข้าไปในเอกสารจะเป็นเครื่องมือในการพิสูจน์ความเป็นเจ้าของเอกสารนั้น เนื่องจากลายเซ็นดิจิตอลไม่สามารถปลอมแปลงได้หรือปลอมแปลงได้ยากมากนั่นเอง

กระบวนการทำงานสำหรับลายเซ็นดิจิตอลแสดงในรูป 3-26 แทนที่จะใช้วิธีการเข้ารหัสข้อมูลผู้ส่งจะใช้กุญแจส่วนตัวในการเข้ารหัสข้อมูลแสดงตนเองเช่นชื่อและนามสกุลของผู้ส่งแล้วจึงส่งเอกสารไปยังผู้รับซึ่งก็จะใช้กุญแจสาธารณะในการดูว่าเอกสารนั้นส่งมาจากผู้ใด



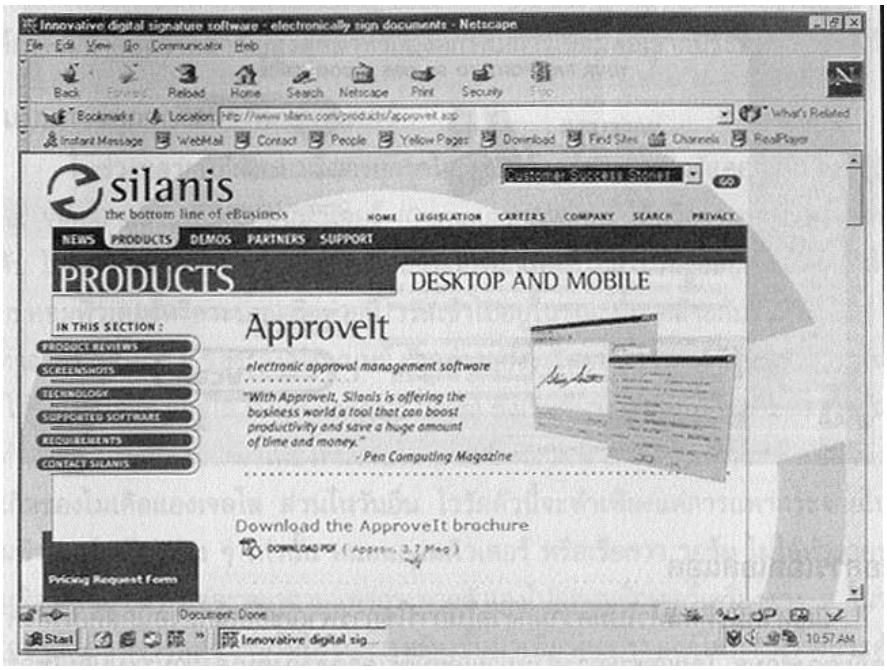
รูป 3-26 การใช้ลายเซ็นดิจิตอล

ลายเซ็นดิจิตอลอีกรูปแบบหนึ่งที่นิยมนำมาใช้งานอย่างกว้างขวางคือ อี-ซิกเนเซอร์ (e-Signature) ซึ่งเป็นลายเซ็นจริงของเจ้าของเอกสารที่ถูกนำมาผสมเข้าเป็นชิ้นเดียวกันกับเอกสาร เสมือนหนึ่งเอกสารที่พิมพ์บนกระดาษที่จะต้องมีลายเซ็นกำกับเพื่อใช้เป็นหลักฐานทางกฎหมาย การใช้อี-ซิกเนเซอร์จึงมีกฎหมายเรียกว่า Electronic Signatures in Global and National Commerce Act (e-sign) ออกมาบังคับใช้ใน

ประเทศสหรัฐอเมริกาใน พ.ศ. 2543 มีสาระสำคัญคือ

- ลายเซ็นจะต้องมีลักษณะเฉพาะตัวสำหรับผู้ใช้แต่ละคน
- ลายเซ็นจะต้องสามารถถูกตรวจสอบความเป็นเจ้าของให้
- ลายเซ็นจะต้องอยู่ในความควบคุมของเจ้าของลายเซ็นเท่านั้น
- ลายเซ็นจะต้องติดอยู่กับเอกสารอย่างถาวรโดยที่จะต้องมีความผูกมัดกับข้อมูลที่ปรากฏในเอกสารนั้น
- ลายเซ็นจะต้องถูกนำมาใช้โดยเจ้าของลายเซ็นด้วยความตั้งใจในลักษณะเดียวกับการเซ็นเอกสารด้วยมือ

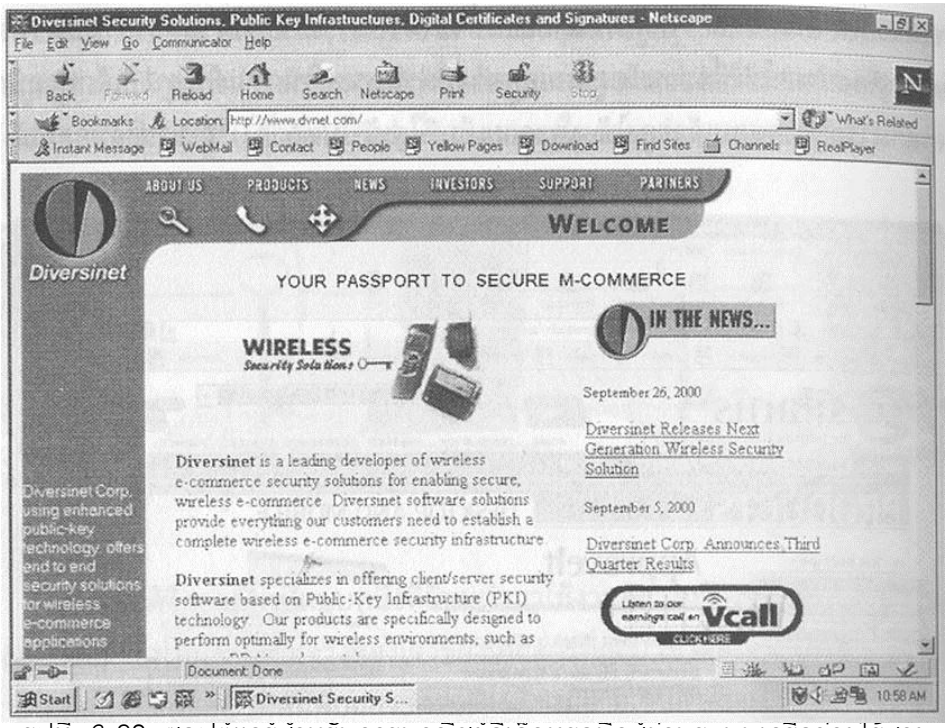
ลายเซ็นดิจิตอลมีความสำคัญต่อการอยู่รอดของการทำธุรกิจผ่านระบบการพาณิชย์อิเล็กทรอนิกส์ บริษัทหลายแห่งได้พัฒนาซอฟต์แวร์ที่สามารถสร้างรูปแบบทางอิเล็กทรอนิกส์ของลายเซ็นผู้ใช้และผสานลายเซ็นนั้นเข้ากับเอกสารเพื่อให้เป็นลายเซ็นที่ถูกต้องตามกฎหมายได้ ตัวอย่างเช่น บริษัท Silanis ได้พัฒนาซอฟต์แวร์สำหรับอี-ซิกเนเชอร์ขึ้นมา ดังแสดงในรูป 3-27 ขั้นตอนแรกของการทำอี-ซิกเนเชอร์ คือการสร้างแฟ้มลายเซ็น (Signature file) ซึ่งบรรจุข้อมูลภาพคอมพิวเตอร์ของรูปลายเซ็นผู้ใช้ ข้อมูลสำหรับการตรวจสอบเจ้าของลายเซ็นและกุญแจรหัสทั้งกุญแจสาธารณะและกุญแจส่วนตัวที่ใช้สำหรับการเซ็นกำกับเอกสารด้วยวิธีการทางอิเล็กทรอนิกส์ ตัวแฟ้มลายเซ็นนี้จะได้รับการปกป้องด้วยการกำหนดรหัสผ่านพิเศษที่จะต้องนำมาใช้เพื่ออ่านข้อมูล เอกสารที่ผ่านกระบวนการเซ็นทางอิเล็กทรอนิกส์ไปแล้วจะสามารถตรวจสอบเจ้าของได้ และลายเซ็นที่ใส่เข้าไปแล้วก็ไม่สามารถลบออกได้



รูปที่ 3-27 ขั้นตอนแรกของการทำอี-ซิกเนเชอร์

ปัญหาประการหนึ่งเกี่ยวกับวิธีการนี้คือการปลอมลายเซ็นที่แม้ว่าจะยังไม่เกิดขึ้นแต่ก็อาจจะเกิดขึ้นได้ในอนาคต การแก้ปัญหาลายเซ็นปลอมทำได้ด้วย การรับรองทางดิจิตอล (digital certificate; certs) ซึ่งนำข้อมูลแสดงตนเองหลายรูปแบบมาใช้ในการยืนยันความเป็นเจ้าของกุญแจสาธารณะที่จะนำมาใช้ในการเซ็นชื่อนั้น มาตรฐานที่นำมาใช้ในการรับรองทางดิจิตอล เรียกว่า มาตรฐานโอซีเอสพี (Online Certificate Status Protocol) ซึ่งเป็นวิธีการตรวจสอบที่ง่ายและรวดเร็วในการตรวจรับรองลายเซ็นดิจิตอล ถ้าลายเซ็นดิจิตอลเปรียบได้กับการเซ็นชื่อแล้วการรับรองทางดิจิตอลก็คือกระบวนการตรวจสอบว่าคนที่เซ็นชื่อนั้นคือเจ้าของลายเซ็นที่แท้จริงนั่นเอง

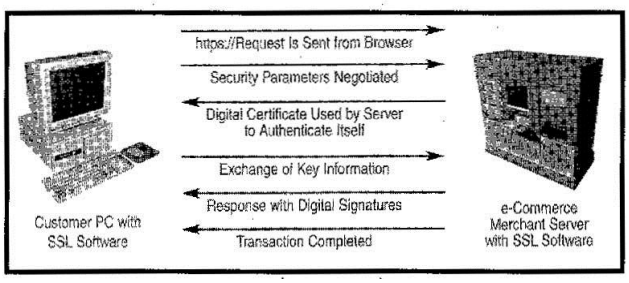
ระบบเครือข่ายไร้สายส่งข้อมูลออกไปทางอากาศซึ่งมีความเสี่ยงต่อการถูกขโมยสัญญาณได้ง่าย การทำให้เกิดความปลอดภัยข้อมูลจึงเป็นสิ่งที่สำคัญที่สุด การเข้ารหัสข้อมูลลายเซ็นดิจิตอล และการรับรองทางดิจิตอลจึงถูกนำมาใช้อย่างกว้างขวางเพื่อให้มั่นใจได้ว่าข้อมูลที่ส่งออกไปในอากาศนั้นมีความปลอดภัยเพียงพอ เช่น บริษัท Diversinet Corp ได้พัฒนาซอฟต์แวร์สำหรับการพาณิชย์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับระบบเครือข่ายไร้สายดังแสดงในรูป 3-28



รูปที่ 3-28 ซอฟต์แวร์สำหรับการพาณิชย์อิเล็กทรอนิกส์ผ่านระบบเครือข่ายไร้สาย

3.4) ชั้นสื่อสารเอสเอสแอล

ปัญหาหนึ่งที่คนทั่วไปมีความกังวลในการใช้การพาณิชย์อิเล็กทรอนิกส์คือเรื่องความปลอดภัยของข้อมูล โดยเฉพาะการส่งหมายเลขบัตรเครดิตของตนเองผ่านระบบอินเทอร์เน็ตชั้นสื่อสารเอสเอสแอล (Secure Socket Layer) จึงได้รับการพัฒนาขึ้นมาเพื่อแก้ปัญหานี้โดยตรงเมื่อผู้ใช้กรอกข้อมูลเกี่ยวกับการซื้อสินค้าหรือบริการเรียบร้อยและพร้อมที่จะส่งข้อมูลหมายเลขบัตรเครดิต บราวเซอร์ของผู้ใช้จะถูกสลับไปอีกหน้าจอหนึ่งซึ่งจะสังเกตได้ว่าที่อยู่ URL นั้นจะเปลี่ยนไปเป็นคำที่ลงท้ายด้วย “s” ซึ่งเป็นจุดสังเกตุได้ว่าขณะนี้เครื่องของผู้ใช้กำลังทำงานในชั้นสื่อสารเอสเอสแอล



รูปที่ 3-29 การทำงานในชั้นสื่อสารเอสเอสแอล

ซอฟต์แวร์สำหรับชั้นสื่อสารเอสเอสแอลจะต้องถูกติดตั้งทั้งที่เครื่องผู้ใช้และเครื่องผู้ให้บริการ รูปที่ 3-29แสดงขั้นตอนการแลกเปลี่ยนข้อมูลที่เกิดขึ้นในชั้นสื่อสารเอสเอสแอล ทางฝั่งผู้ใช้จะส่งความต้องการทำรายการลับไปยังเครื่องผู้ให้บริการ ซอฟต์แวร์จากทั้งสองฝั่งจะแลกเปลี่ยนข้อมูลเกี่ยวกับกุญแจรหัสสาธารณะระหว่างกัน ท้ายที่สุดข้อมูลหมายเลขบัตรเครดิตของผู้ใช้จะถูกเข้ารหัสเพื่อส่งไปยังเครื่องผู้ให้บริการได้โดยอัตโนมัติทำให้การส่งข้อมูลลับผ่านระบบอินเทอร์เน็ตมีความปลอดภัยมากขึ้น

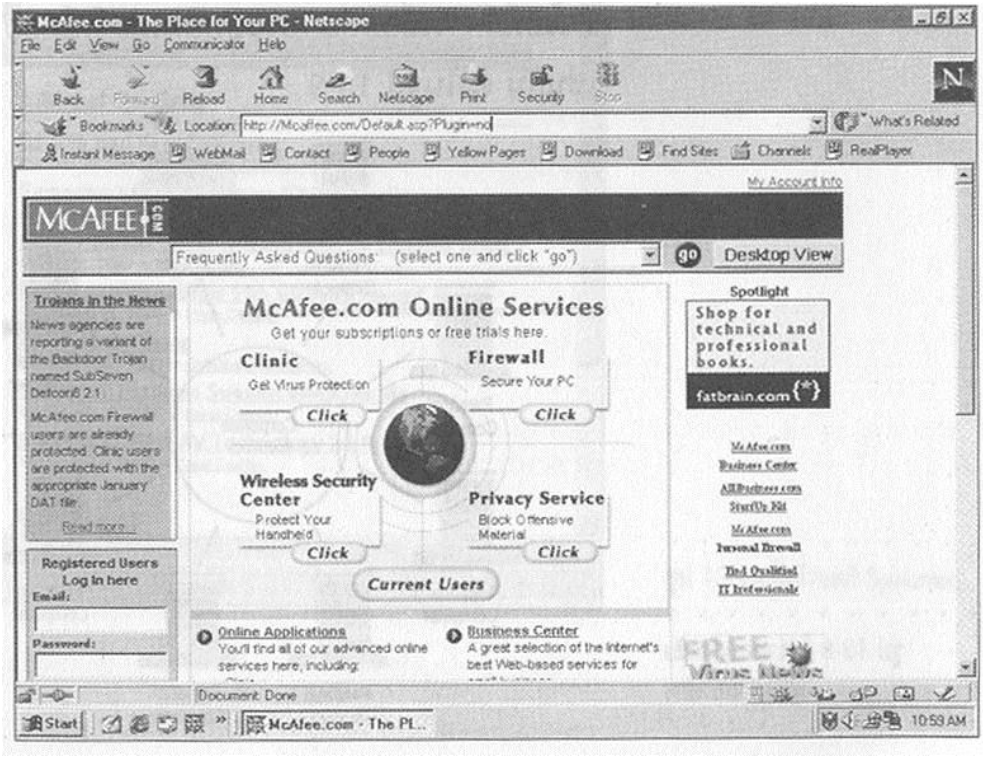
4) ในการพิจารณาเกี่ยวกับความปลอดภัย

ผู้บริหารระบบเครือข่ายและผู้ใช้ระบบอินเทอร์เน็ตเป็นประจำมีความต้องการอย่างหนึ่งเหมือนกันคือการป้องกันไม่ให้ผู้อื่นบุกรุกเข้ามาในเครื่องคอมพิวเตอร์ของตนเอง การพัฒนาซอฟต์แวร์เพื่อการป้องกันไม่ให้เกิดการบุกรุกเข้ามาในเว็บไซต์หรือบุกรุกเข้ามาในระบบเครือข่ายองค์กรจึงมีลำดับความสำคัญสูงสุดสำหรับองค์กรที่มีการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ต

4.1) รูปแบบการบุกรุกระบบคอมพิวเตอร์

ในช่วงหลายปีที่ผ่านมานี้ การบุกรุกโดยซอฟต์แวร์ประเภทไวรัสคอมพิวเตอร์ (Computer Virus) และ หนอนคอมพิวเตอร์ (Computer Worm) ได้ทวีความรุนแรงมากขึ้นเป็นลำดับ ไวรัสคอมพิวเตอร์ หรือเรียกสั้น ๆ ว่า ไวรัส เป็นโปรแกรมที่ถูกออกแบบมาให้ทำลายระบบคอมพิวเตอร์หรือระบบเครือข่ายที่ไวรัสเข้าไปอยู่ในขณะนั้น คล้ายกับไวรัสจริง ๆ ที่เข้ามาทำลายระบบต่าง ๆ ของร่างกายมนุษย์ ตัวอย่างของไวรัสคอมพิวเตอร์ที่รู้จักกันทั่วไปในอดีต คือ ไวรัสไมเคิลแองเจลโล (Michelangelo Virus) ซึ่งเริ่มต้นระบาดในปี พ.ศ. 2538 ไวรัสตัวนี้จะทำลายระบบคอมพิวเตอร์เพียงหนึ่งวันในแต่ละปี คือวันที่ 5 เดือนมีนาคม ซึ่งเป็นวันคล้ายวันเกิดของไมเคิลแองเจลโล ส่วนในวันอื่น ไวรัสตัวนี้จะทำเพียงแค่การแพร่กระจายไปตามคอมพิวเตอร์เครื่องต่าง ๆ เท่านั้น หนอนคอมพิวเตอร์ หรือเรียกว่า วอร์ม ไม่ได้ทำลายระบบคอมพิวเตอร์โดยตรงแต่จะพยายามแพร่กระจายตัวเองไปสู่คอมพิวเตอร์เครื่องต่าง ๆ ในระบบเครือข่าย อันที่จริงแล้ว วอร์มได้รับการสร้างขึ้นมาเพื่อวัตถุประสงค์ในทางสร้างสรรค์ คือ เป็นวิธีการส่งข่าวสารไปยังผู้ใช้ทั้งหมดในระบบเครือข่ายโดยอัตโนมัติ แต่ผู้สร้างวอร์มช่วงหลังได้ออกแบบให้วอร์มกลายเป็นเพชฌฆาต ตัวอย่างวอร์มที่มีชื่อเสียงในด้านลบคือ วอร์มอินเทอร์เน็ต (Internet Worm) ซึ่งจะแพร่กระจายด้วยการสร้างสำเนาตัวเองส่งไปยังผู้ใช้ในระบบเครือข่ายอินเทอร์เน็ตไปเรื่อย ๆ อัตราการสร้างสำเนาตัวเองของวอร์มนี้สูงมากจนทำให้เกิดสถานะการณ์เรียกว่า combinatorial explosion คือ อัตรา

การเติบโตจะเป็นทวีคูณซึ่งทำให้บางส่วนของระบบอินเทอร์เน็ต ในปี พ.ศ. 2541 เป็นอัมพาตไปชั่วระยะเวลาหนึ่งโปรแกรมต่อต้านไวรัสเช่น McAfee ดังแสดงในรูป 3-30 สามารถนำมาใช้ตรวจหาและทำลายไวรัสและวอร์มได้เป็นอย่างดี



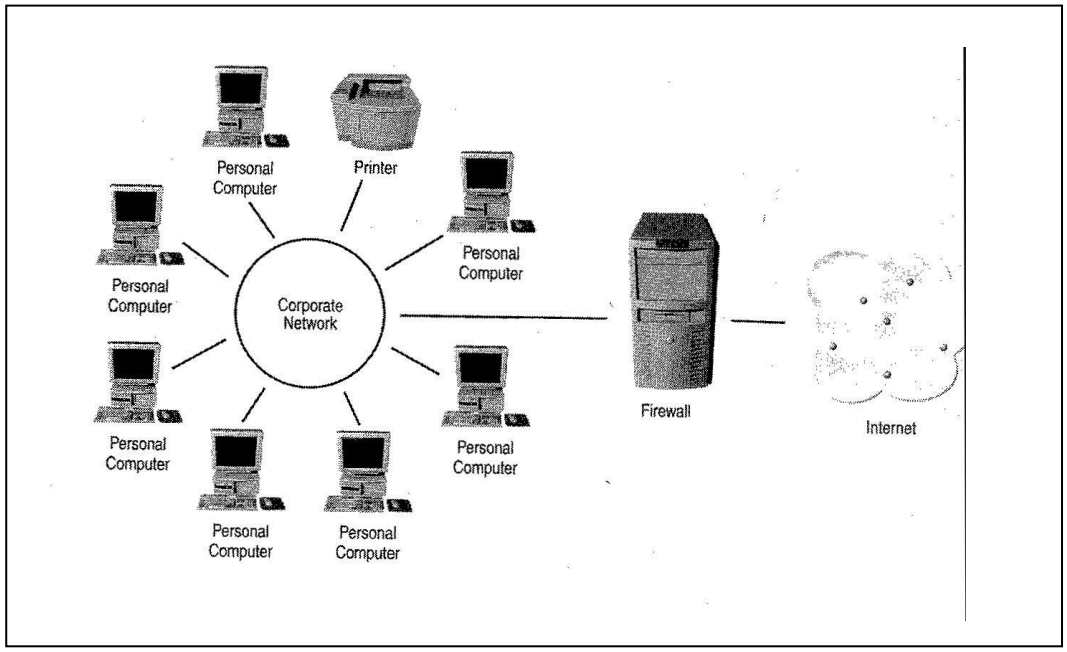
รูปที่ 3 – 30 เว็บไซต์ของโปรแกรมต่อต้านไวรัส

นับตั้งแต่ไวรัสได้ทำการแนะนำตนเองให้ชาวโลกได้รู้จักผ่านระบบอินเทอร์เน็ตทำให้เกิดเป็นเสมือนแรงกระตุ้นให้มีการพัฒนาไวรัสตัวใหม่ออกมาอย่างต่อเนื่อง ในปี พ.ศ.2543 บริษัทผู้ผลิต McAfee ได้ประกาศว่ามีไวรัสอยู่ในโลกนี้มากกว่า 53,000 ชนิด เนื่องจากไวรัสตัวใหม่ได้ถือกำเนิดขึ้นมาตลอดเวลา ผู้ใช้จำเป็นจะต้องทำการปรับปรุงข้อมูลเกี่ยวกับไวรัสอยู่อย่างสม่ำเสมอผ่านทางบริษัทผู้ผลิตโปรแกรมต่อต้านไวรัสนั้น ๆ เรียกว่าเป็นการ Update Virus Patterns ซึ่งจะเป็นข้อมูลให้โปรแกรมต่อต้านไวรัสรู้จักวิธีการทำงานของไวรัสตัวใหม่ ๆ เพื่อที่จะได้สามารถตรวจจับ ทำลาย และแก้ไขแฟ้มข้อมูลที่ติดไวรัสนั้นให้กลับคืนสู่สภาพเดิม

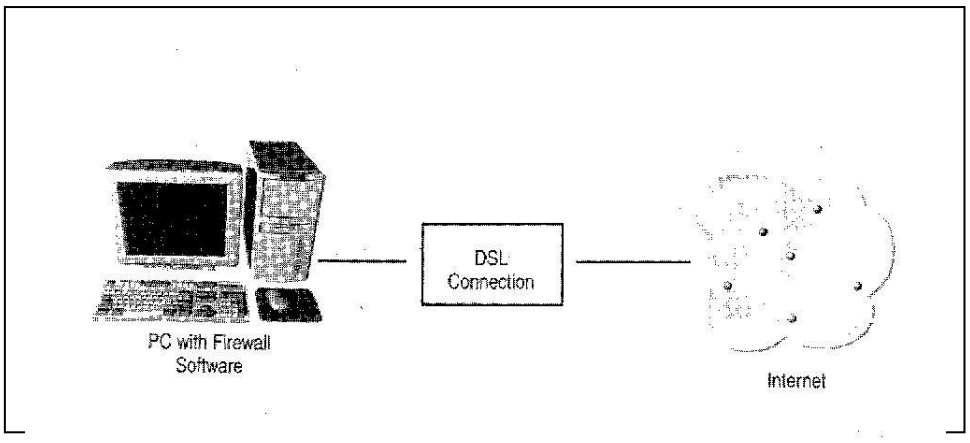
วิธีการทำงานของไวรัสอีกแบบหนึ่งเรียกว่า เป็นการทำดีโอเอส (Denial of Service DoS) ซึ่งไม่ใช่การทำลายระบบคอมพิวเตอร์โดยตรงแบบเดียวกับวอร์ม คือจะทำการเพิ่มปริมาณงานที่ดูเหมือนกับงานปกติจากผู้ใช้ทั่วไปแต่ว่ามีปริมาณงานสูงมากให้แก่เซิร์ฟเวอร์อย่างต่อเนื่อง จนกระทั่งเซิร์ฟเวอร์เครื่องนั้นไม่สามารถจะให้บริการแก่ผู้ใช้จริง ๆ ได้อีกต่อไปและอาจจะทำให้เกิดผลข้างเคียงเช่นทำให้อุปกรณ์บางส่วนของเซิร์ฟเวอร์ถูกใช้งานหนักจนเสียหายอย่างถาวร เว็บไซต์ที่มีชื่อเสียงอย่าง ยาฮู (Yahoo) ก็เคยโดนโจมตีจากไวรัสประเภทนี้จนต้องปิดบริการไปเป็นระยะเวลาสั้น ๆ มาแล้ว

4.2) โปรแกรมไฟร์วอลล์

ซอฟต์แวร์ที่มีขีดความสามารถในการต่อต้านไวรัสอีกชนิดหนึ่งเรียกว่า ไฟร์วอลล์ (Firewall) ซึ่งจะตรวจสอบข้อมูลทุกชนิดจากภายนอกที่จะเข้ามาสู่ระบบเครือข่ายขององค์กรและจะปล่อยให้ข้อมูลนั้นเข้าสู่เครือข่ายองค์กรได้ก็ต่อเมื่อเป็นข้อมูลที่ได้รับการอนุญาตไว้ล่วงหน้ามิฉะนั้นก็จะไม่ยอมให้หลุดรอดเข้ามาได้เลย ในอดีต ไฟร์วอลล์ได้รับการออกแบบมาให้ทำงานกับระบบเครือข่ายองค์กรเท่านั้น ดังแสดงในรูปที่ 3-31 แต่ในปัจจุบันผู้ใช้ตามบ้านหรือผู้ใช้ทั่วไปที่มีการเชื่อมต่อกับระบบอินเทอร์เน็ตอย่างสม่ำเสมอก็สามารถนำไฟร์วอลล์ไปใช้งานได้ เช่นกัน ดังในรูปที่ 3-32

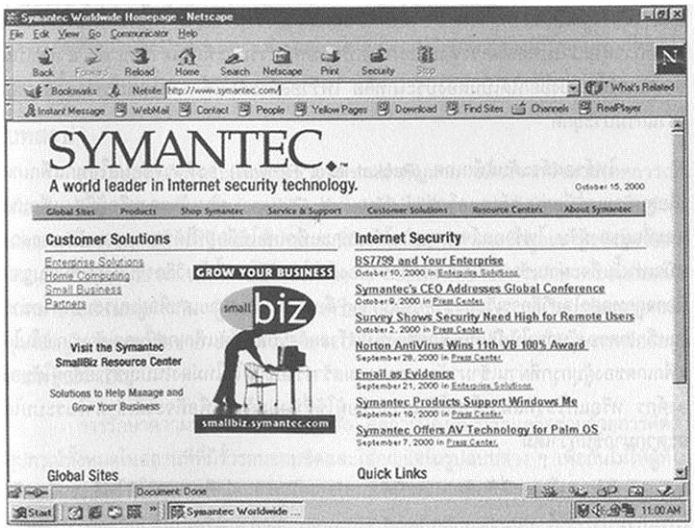


รูปที่ 3-31 ไฟร์วอลล์สำหรับเครือข่ายองค์กร

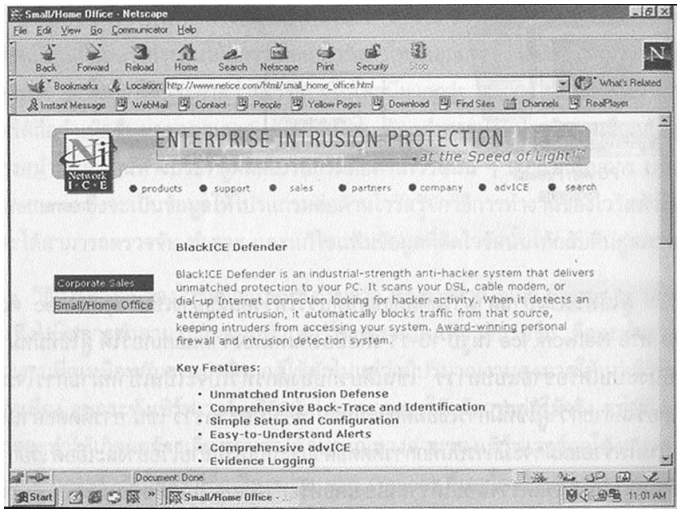


รูปที่ 3-32 ไฟร์วอลล์สำหรับผู้ใช้ตามบ้าน

ผู้ใช้พีซีตามบ้านสามารถติดตั้งซอฟต์แวร์ไฟร์วอลล์อย่างเช่น Symantec ดังในรูปที่ 3-33 หรือ Network Ice ในรูปที่ 3-34 เพื่อป้องกันตนเองจากแฮกเกอร์ได้ ผู้ใช้ที่มีหมายเลขที่อยู่บนระบบเครือข่ายแบบถาวร เช่นเดียวกับองค์กรทั่วไปจะเป็นเป้าหมายการโจมตีจากแฮกเกอร์ได้ง่ายกว่าผู้ใช้ที่มีการเชื่อมต่อระบบอินเทอร์เน็ตชั่วคราว เช่น การติดต่อผ่านโมเด็มโปรแกรมไฟร์วอลล์มักจะมีการบันทึกการติดต่อผ่านระบบเครือข่ายไว้อย่างละเอียด เรียกว่า log file ทำให้ผู้ใช้สามารถตรวจสอบได้ว่าตนเองเคยหรือกำลังตกเป็นเหยื่อของแฮกเกอร์หรือไม่



รูปที่ 3-33 ไฟร์วอลล์ Symantec



รูปที่ 3-34 ไฟร์วอลล์ Network Ice

ระบบเครือข่ายองค์กรได้รับการปกป้องโดยไฟร์วอลล์มานานหลายปีก่อนผู้ใช้ตามบ้าน เนื่องจากเป็นเป้าหมายของการโจมตีจากแฮกเกอร์จำนวนมาก ไฟร์วอลล์ระดับองค์กรได้รับการพัฒนาไปพอสมควรทั้งประเภทที่เป็นซอฟต์แวร์และที่เป็นฮาร์ดแวร์ ส่วนที่เป็นซอฟต์แวร์นั้นแบ่งออกได้เป็นสองประเภทคือ ไฟร์วอลล์ระดับแพ็กเกต และไฟร์วอลล์ระดับโปรแกรมประยุกต์

ไฟร์วอลล์ระดับแพ็กเกต (Packet-level Firewall) จะตรวจข้อมูลในทุกแพ็กเกตเพื่อดูหมายเลขที่อยู่บนระบบเครือข่าย (Network Address) ของเจ้าของหรือผู้ที่ส่งแพ็กเกตและที่อยู่ของผู้รับ ไฟร์วอลล์จะอนุญาตให้เฉพาะแพ็กเกตใช้ที่อยู่ที่ได้รับอนุญาตเป็นการล่วงหน้าเท่านั้นที่จะผ่านเข้ามาในระบบเครือข่ายองค์กรได้ วิธีการนี้เป็นวิธีการป้องกันขั้นพื้นฐานที่อาจถูกหลอกโดยวิธีการเรียกว่า IP Spoofing คือการแก้ไขหมายเลขที่อยู่บนระบบเครือข่ายในแพ็กเกตของผู้บุกรุกให้เป็นที่อยู่ที่ถูกต้องซึ่งไฟร์วอลล์จะปล่อยให้แพ็กเกตนี้หลุดเข้ามาภายในได้แพ็กเกตของผู้บุกรุกที่ผ่านเข้ามามักจะพยายามสร้างรายชื่อผู้ใช้ใหม่ลงในบัญชีรายชื่อผู้ใช้ขององค์กร หรือแก้ไขรหัสผ่านใหม่ให้แก่รายชื่อผู้ใช้ที่มีอยู่แล้ว เพื่อที่จะได้เข้ามาในระบบได้สะดวกมากขึ้นกว่าเดิม

วิธีการทำงานที่ซับซ้อนและมีความปลอดภัยมากกว่าคือ การใช้ไฟร์วอลล์ระดับโปรแกรมประยุกต์ (Application-level Firewall) ซึ่งทำหน้าที่เป็นตัวกลางการเชื่อมต่อระหว่างระบบอินเทอร์เน็ตและระบบเครือข่ายองค์กร ผู้ใช้ที่ติดต่อมาจากภายนอกองค์กรผ่านระบบอินเทอร์เน็ตจะถูกบังคับให้ลงทะเบียนการใช้งาน (log-in) เข้าที่ไฟร์วอลล์โดยตรงก่อนที่จะสามารถเข้ามาใช้ระบบเครือข่ายองค์กรได้ รายชื่อผู้ใช้รวมทั้งรหัสผ่านจะถูกเก็บรักษาและบริหารโดยไฟล์วอลล์ซึ่งจะมีรายละเอียดต่าง ๆ เช่น รายชื่อโปรแกรมประยุกต์ที่ได้รับอนุญาตให้ใช้เก็บไว้ด้วย ดังนั้นแม้จะผู้ใช้ที่เป็นพนักงานจริง ๆ ขององค์กรก็จะสามารถใช้งานได้เฉพาะโปรแกรมที่ได้รับอนุญาตเท่านั้น ไฟร์วอลล์นี้ยังมีความสามารถในด้านอื่นอีก เช่น การป้องกันไม่ให้ผู้ใช้จากภายนอกส่งสำเนาโปรแกรมซึ่งอาจเป็นไวรัสเข้ามาในระบบเครือข่ายองค์กรด้วย

ไฟร์วอลล์ระดับโปรแกรมประยุกต์ได้รับการพัฒนาไปเป็น โปรแกรมพร็อกซี่ (Proxy Server) เมื่อผู้ใช้ภายในะรบบเครือข่ายองค์กรติดต่อขอข้อมูลจากเว็บไซต์ในระบบอินเทอร์เน็ตโปรแกรมพร็อกซี่จะเปลี่ยนที่อยู่ของผู้ใช้ไปเป็นที่อยู่สำรองซึ่งเป็นที่อยู่ของเครื่องพร็อกซี่เองดังนั้นข้อมูลความต้องการจากผู้ใช้คนใดก็ตามที่ส่งออกไปยังเว็บไซต์ภายนอกจะใช้ที่อยู่เดียวกันทั้งหมด ข้อมูลที่ตอบกลับมาจึงถูกส่งมาที่เครื่องพร็อกซี่เพียงเครื่องเดียวทำให้เครื่องพร็อกซี่สามารถตรวจสอบข้อมูลที่ส่งออกไปและส่งกลับเข้ามาได้และสามารถเลือกวิธีการตอบสนองได้หลายแบบ เช่น เครื่องพร็อกซี่จะเก็บข้อมูลจากเว็บไซต์ต่าง ๆ เอาไว้ในระยะเวลาพอสมควร ถ้าผู้ใช้คนเดิมหรือผู้ใช้คนใหม่ร้องขอมูลชุดเดิม เครื่องพร็อกซี่ก็จะส่งสำเนาที่เก็บไว้ไปให้แทน ซึ่งจะช่วยลดปริมาณข้อมูลที่จะส่งออกไปและส่งกลับเข้ามาได้ หรือการปฏิเสธไม่ให้ผู้ใช้เข้าไปดูหรือรับข้อมูลจากเว็บไซต์บางแห่งก็ได้ ในกรณีที่เป็นข้อมูลปกติเครื่องพร็อกซี่ซึ่งจะเก็บที่อยู่ที่แท้จริงของแต่ละแพ็กเกตเอาไว้ ก็จะเปลี่ยนที่อยู่ของผู้รับกลับเป็นที่อยู่เดิมและส่งข้อมูลนั้นไปให้

ความปลอดภัยในระบบเครือข่ายมีความสำคัญมาก เนื่องจากจำนวนเหตุการณ์ที่เกี่ยวข้องกับการบุกรุกเข้ามาในระบบเครือข่ายโดยผู้ไม่ได้รับอนุญาตได้เพิ่มสูงขึ้นมาเป็นลำดับแฮกเกอร์คือบุคคลกลุ่มหนึ่งที่พัฒนาโปรแกรมที่มีเจตนาในการทำลายข้อมูลและระบบเครือข่ายและแพร่กระจายโปรแกรมเหล่านั้นไปยังที่ต่าง ๆ ระบบเครือข่ายมีการรักษาความปลอดภัยในหลายระดับแตกต่างกัน ผู้จัดการระบบเครือข่ายมีสิทธิในการจัดการบริหารข้อมูลทุกชนิดทุกที่ที่อยู่ในระบบเครือข่าย ส่วนผู้ใช้ทั่วไปจะได้รับการกำหนดสิทธิใน

การใช้บริการหรือข้อมูลตามความจำเป็น

การรักษาความปลอดภัยทางกายภาพ คือการป้องกันระบบเครือข่ายด้วยการติดตั้งอุปกรณ์ทั้งหมดในสถานที่ที่มีรั้วรอบขอบชิดและใส่กุญแจในรูปแบบต่าง ๆ เพื่อกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าไปใช้บริการและข้อมูลในระบบเครือข่าย การตรวจลายนิ้วมือ การใช้กล้องโทรทัศน์วงจรปิด และเครื่องตรวจจับการเคลื่อนไหวเป็นตัวอย่างอุปกรณ์นำมาใช้ในการป้องกันทางกายภาพ ชนิดของสื่อที่ใช้ถ่ายทอดข้อมูลก็มีส่วนช่วยรักษาความปลอดภัยได้ในระดับที่แตกต่างกัน สื่อประเภทคลื่นวิทยุมีความปลอดภัยในการใช้งานน้อยที่สุด ในขณะที่สายใยแก้วนำแสงเป็นสื่อที่มีความปลอดภัยสูงสุด อุปกรณ์โทรกลับนำมาใช้เพิ่มความปลอดภัยในการให้บริการผู้ใช้ที่ใช้โมเด็มเป็นสื่อในการติดต่อเข้าสู่ระบบเครือข่าย

การรักษาความปลอดภัยด้วยซอฟต์แวร์มีความสำคัญมากในการพาณิชย์อิเล็กทรอนิกส์ชื่อผู้ใช้และรหัสผ่านเป็นวิธีการป้องกันแบบที่ง่ายและสะดวกที่สุดที่สามารถให้ความปลอดภัยได้ถ้าผู้ใช้เก็บรักษาชื่อผู้ใช้และรหัสผ่านไว้เป็นความลับ การเข้ารหัสข้อมูลคือการเปลี่ยนแปลงรูปแบบข้อมูลปกติให้ไปอยู่ในรูปแบบข้อมูลที่ไม่ทราบความหมาย แล้วจึงส่งข้อมูลนั้นเข้าสู่ระบบเครือข่าย แม้ว่าผู้ที่ไม่ได้รับอนุญาตให้ใช้ข้อมูลนั้นจะสามารถขโมยข้อมูลไปได้แต่ก็จะไม่ทราบความหมายของข้อมูลนั้น การเข้ารหัสโดยการใช้กุญแจสมมาตรจะมีกุญแจรหัสเพียงชุดเดียวที่ผู้ส่งข้อมูลใช้ในการเข้ารหัสและผู้รับข้อมูลจะต้องใช้กุญแจรหัสเดิมในการแปลงข้อมูลรหัสกลับมาเป้นข้อมูลปกติตัวอย่างวิธีการเข้ารหัสแบบนี้ได้แก่ ดีอีเอส ทรีดีอีเอส บโลฟิซซ์ไอดีอีเอ และคลิปเปอร์ชิป เป็นต้น การเข้ารหัสโดยใช้กุญแจสาธารณะจะมีกุญแจรหัสสองตัวคือกุญแจสาธารณะและกุญแจส่วนตัว ผู้ส่งใช้กุญแจสาธารณะสำหรับเข้าสำหรับเข้ารหัสข้อมูล ส่วนผู้รับจะต้องใช้กุญแจส่วนตัวในการถอดรหัสนั้น อาร์เอสเอเป็นวิธีการหนึ่งที่ใช้การทำงานแบบนี้

ลายเซ็นดิจิตอลถูกนำมาผสานเข้าไปในแฟ้มข้อมูลเพื่อใช้ในการพิสูจน์ความเป็นเจ้าของแฟ้มข้อมูลนั้น อี-ซิกเนเซอร์คือกระบวนการเซ็นชื่อด้วยลายเซ็นดิจิตอลลงในแฟ้มข้อมูลอิเล็กทรอนิกส์ การรับรองแบบดิจิตอลใช้ข้อมูลหลายรูปแบบในการพิสูจน์ว่าผู้ที่ส่งแฟ้มข้อมูลมานั้นคือบุคคลที่เป็นเจ้าของจริง ซอฟต์แวร์ในชั้นสื่อสารเอสเอสแอลทำงาร่วมกับโปรแกรมบราวเซอร์เพื่อรักษาความปลอดภัยในการส่งข้อมูลที่มีความสำคัญมาให้กับผู้ใช้ระบบอินเทอร์เน็ต

ไรรัสคอมพิวเตอร์คือโปรแกรมที่ออกแบบมาเพื่อการสร้างความเสียหายให้กับคอมพิวเตอร์ ส่วนวอร์มเป็นโปรแกรมที่ไม่ได้สร้างความเสียหายโดยตรงแต่จะทำการสร้างสำเนาของตัวเองขึ้นมาเป็นจำนวนมาก โปรแกรมทั้งสองชนิดนี้ถูกนำเข้ามาเผยแพร่หรือระบาดในระบบอินเทอร์เน็ตและระบบคอมพิวเตอร์ทั่วโลกมานานหลายปีแล้ว ซึ่งก็ได้สร้างความเสียหายขึ้นมากมาย โปรแกรมประเภทดีโอเอสก็เป็นอีกวิธีหนึ่งที่แฮกเกอร์ใช้ในการรบกวนการทำงานของระบบคอมพิวเตอร์จนไม่สามารถให้บริการได้ตามปกติ

ไฟร์วอลล์เป็นซอฟต์แวร์ที่ทำหน้าที่ปกป้องคอมพิวเตอร์และระบบเครือข่ายจากการบุกรุกโดยแฮกเกอร์และผู้ที่ไม่ได้รับอนุญาต ผู้ใช้ตามบ้านสามารถติดตั้งโปรแกรมประเภทนี้เพื่อป้องกันการบุกรุกผ่านโมเด็มหรือบริการอินเทอร์เน็ตผ่านสายเคเบิลชนิดต่าง ๆ ได้ ระบบเครือข่ายองค์กรใช้ไฟร์วอลล์ระดับแพ็กเกตในการตรวจสอบข้อมูลแต่ละแพ็กเกตที่ถูกส่งเข้ามาภายในระบบ หรือใช้ไฟร์วอลล์ระดับโปรแกรมประยุกต์แต่ละโปรแกรมการดัดแปลงไฟร์วอลล์ไปเป็นพร็อกซี่ก็เพื่อสร้างหมายเลขที่อยู่บนระบบเครือข่ายปลอมให้กับทุกแพ็กเกต เมื่อได้รับตอบกลับมาแล้วพร็อกซี่ก็สามารถตรวจสอบข้อมูลในทุกแพ็กเกตและส่งต่อไปให้ผู้ใช้เฉพาะส่วนที่อนุญาตเท่านั้น [13]

3.5 หลักการใช้งานอินเทอร์เน็ตอย่างปลอดภัย

ในปัจจุบันมีผู้ใช้บริการ บนระบบเครือข่ายอินเทอร์เน็ต ได้เพิ่มมากขึ้นเรื่อยๆทั่วโลก เพราะเป็นช่องทางที่สามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูลกันได้อย่างรวดเร็ว รวมถึงธุรกิจและพาณิชย์ในด้านต่างๆ ช่วยในเรื่องการลดระยะเวลาและต้นทุนในการติดต่อสื่อสาร แต่อย่างไรก็ตามผู้ใช้โดยทั่วไป ยังไม่เห็นความสำคัญ ของการใช้งานอินเทอร์เน็ตที่ปลอดภัยเท่าที่ควร เนื่องจากยังขาดความรู้ในการใช้งานและวิธีป้องกัน หรืออาจคิดว่าคงไม่มีปัญหาอะไรมาก ในการใช้งาน แต่เมื่อเกิดปัญหาขึ้นกับตัวเองแล้ว ก็ทำให้ตนเองเดือดร้อน เราสามารถป้องกันปัญหาเหล่านี้ได้ ดังนี้

1) ไม่เปิดเผยข้อมูลส่วนตัว ไม่บอกชื่อนามสกุลจริง ที่อยู่ เบอร์โทรศัพท์ โดยเฉพาะเบอร์โทรศัพท์บ้าน เพราะผู้ร้ายสามารถใช้หมายเลขโทรศัพท์บ้านเพื่อโทรสอบถามที่อยู่ของเจ้าของบ้านได้จากบริการ 1133 ซึ่งเป็นบริการมาตรฐาน โจรผู้ร้ายและพวกจิตวิปริตอาจมาดักทำร้ายคุณได้ เวลาแชทก็ให้ใช้ชื่อเล่นหรือชื่อสมมุติแทน

2) ไม่ส่งหลักฐานส่วนตัวของตนเองและคนในครอบครัวให้ผู้อื่น เช่น สำเนาบัตรประชาชน เอกสารต่างๆ รวมถึงรหัสบัตรต่างๆ เช่น เอทีเอ็ม บัตรเครดิต ฯลฯ ให้กับผู้อื่น แม้แต่เพื่อน เพราะเพื่อนเองก็อาจถูกหลอกให้มาถามจากเราอีกต่อหนึ่ง

3) ไม่ควรโอนเงินให้ใครอย่างเด็ดขาด นอกจากจะเป็นญาติสนิทที่เชื่อใจได้จริงๆ

4) ไม่ออกไปพบเพื่อนที่รู้จักทางอินเทอร์เน็ต เว้นเสียแต่ว่าได้รับอนุญาตจากพ่อแม่ผู้ปกครอง และควรมีผู้ใหญ่หรือเพื่อนไปด้วยหลายๆ คน เพื่อป้องกันการลักพาตัว หรือการกระทำมิดีมิร้ายต่างๆ

5) ระมัดระวังการซื้อสินค้าทางอินเทอร์เน็ต รวมถึงคำโฆษณาชวนเชื่ออื่นๆ เด็กต้องปรึกษาพ่อแม่ผู้ปกครอง โดยต้องใช้วิจารณญาณ พิจารณาความน่าเชื่อถือของผู้ขาย เช่นดูประวัติ ดูการให้คอมเมนท์ Comment จากผู้ซื้อรายก่อนๆ ที่เข้ามาเขียนไว้ พิจารณาวิธีการจ่ายเงิน ฯลฯ และต้องไม่บอกรหัสบัตรเครดิตและเลขท้าย3หลักที่อยู่ด้านหลังบัตรให้แก่ผู้ขาย หรือใครๆ โดยเด็ดขาด เพราะเป็นรหัสสำหรับการซื้อสินค้าออนไลน์ผ่านบัตรเครดิต คุณอาจถูกยักยอกเงินจากบัตรเครดิตจนเต็มวงเงินที่คุณมี แล้วมารู้ตัวอีกทีก็มีหนี้บานมหาศาล นอกจากนี้คุณผู้ปกครองก็ไม่ควรวางกระเป๋าเงินที่ใส่บัตรเครดิต บัตรเอทีเอ็ม ฯลฯ ให้เด็กหยิบง่ายๆ เพราะคำโฆษณาล่อหลอกทางเน็ต อาจทำให้เด็กอยากซื้อสินค้าที่ไม่เหมาะสมบางอย่าง แล้วอาจมาเปิดดูรหัสบัตร เพื่อไปซื้อสินค้าออนไลน์ได้

6) สอนให้เด็กบอกพ่อแม่ผู้ปกครองหรือคุณครู ถ้าถูกกลั่นแกล้งทางอินเทอร์เน็ต (Internet Bullying) เช่น ได้รับอีเมล์หยาบคาย การข่มขู่จากเพื่อน การส่งต่ออีเมลข้อความใส่ร้ายป้ายสีรุนแรง หรือถูกนำรูปถ่ายไปตัดต่อเข้ากับภาพโป๊แล้วส่งไปให้เพื่อนทุกคนดู ถูกแอบถ่ายขณะทำภารกิจส่วนตัว เป็นต้น ให้เด็กบอกพ่อแม่ ถ้าเป็นการกลั่นแกล้งในหมู่เพื่อน พ่อแม่ควรแจ้งคุณครูหรือทางโรงเรียนและผู้ปกครองของเด็กคู่กรณีให้รับทราบพฤติกรรมการกลั่นแกล้งของเพื่อนนักเรียน เพราะการกลั่นแกล้งด้วยความรู้เท่าไม่ถึง การณ์แบบนี้ อาจทำให้เด็กที่ถูกแกล้งเสียสุขภาพจิต ไม่อยากไปโรงเรียน และมีปัญหาการเรียนได้ ซึ่งพ่อแม่เองก็ควรจะสังเกตอาการลูกๆ ด้วยว่าซึมเศร้าผิดปกติหรือเปล่า และควรพูดคุยกันอย่างเปิดเผย ส่วนการกลั่นแกล้ง แบล็คเมล์ในกรณีรุนแรงควรแจ้งตำรวจเพื่อเอาโทษกับผู้กระทำผิด

7) ไม่เผลอบันทึกยูสเซอร์เนมและพาสเวิร์ดขณะใช้เครื่องคอมพิวเตอร์สาธารณะ การใช้คอมพิวเตอร์ที่โรงเรียน ที่อินเทอร์เน็ตคาเฟ่ ที่บ้านคนอื่นต้องระวังเวลาใส่ชื่อยูสเซอร์เนมและพาสเวิร์ดในการล็อคอิน เข้าไปในเว็บไซท์ หรือเปิดใช้โปรแกรมต่างๆ เช่น เปิดเช็คอีเมลล์ เปิดใช้โปรแกรมสนทนาMSN เปิดดูข้อมูลทางการเงินส่วนตัวผ่านเว็บไซท์ธนาคารที่ให้บริการออนไลน์ โดยเฉพาะอย่างยิ่ง การล็อคอินเข้าไปยังเว็บ

ไซท์ เพื่อชำระค่าใช้จ่ายต่างๆ ผ่านทางอินเทอร์เน็ต จะต้องไม่เผลอไป ติ๊กถูกที่หน้ากล่องข้อความที่มีความหมายประมาณว่า “ให้บันทึก ชื่อผู้ใช้และพาสเวิร์ดของคุณบนเครื่องคอมพิวเตอร์นี้” อย่างเด็ดขาด เพราะผู้ที่มาใช้เครื่องต่อจากคุณ สามารถล็อคอินเข้าไป จากชื่อของคุณที่ถูกบันทึกไว้ แล้วสวมรอยเป็นคุณ หรือแม้แต่โอนเงินในบัญชีของคุณจ่ายค่าสินค้าและบริการต่างๆ ที่เขาต้องการ ผลก็คือคุณอาจหมดตัวและล้มละลายได้

8) การใช้โปรแกรมสนทนาอย่างปลอดภัย ถ้าเจอเพื่อนทางเน็ตที่พูดจาข่มขู่ หยาบคาย ชวนคุยเรื่องเซ็กซ์ พยายามชวนออกไปข้างนอก ให้เลิกคุย และควรบอกพ่อแม่ด้วย รวมทั้งสกัดกั้น Block ชื่อของเพื่อนคนนั้นๆ ไม่ให้เข้ามาคุยกับเรา/ลูกของเรา หรือไม่ให้ส่งอีเมล์มาหาเราได้อีก นอกจากนี้คุณยังสามารถตั้งค่าการใช้งานโปรแกรมสนทนาให้เป็นแบบ Private ได้ เช่น ในโปรแกรมสนทนายอดนิยมอย่าง MSN Messenger สามารถตั้งค่าให้เพื่อนใหม่ที่อยากจะเข้ามาคุยกับคุณ ต้องขออนุญาตก่อน เมื่อคุณตอบตกลง เขาจึงส่งข้อความมาคุยโต้ตอบกับคุณได้ ซึ่งถ้าไม่ได้ตั้งค่าเอาไว้ ใครๆ ก็สามารถส่งข้อความมาถึงคุณได้ ซึ่งถ้าผู้ใช้เป็นเด็ก อาจได้รับข้อความถามขนาดอวัยวะ ข้อความชวนไปมีเซ็กส์พร้อมบรรยายสรรพคุณต่างๆ ข้อความเสนอขายเซ็กส์ทอย ฯลฯโผล่ขึ้นมาได้ ซึ่งคงไม่ดีแน่ ดังนั้นการตั้งค่า Privacy จึงเป็นการ สกรีนผู้ใช้ และป้องกันไม่ให้คุณหรือเด็ก ได้รับข้อความลามก ข้อความเชิญชวนแปลกๆ จากผู้ใช้ที่เราไม่รู้จักและไม่อยากจะคุยด้วย นอกจากนี้ ไม่ควรใส่ข้อมูลส่วนตัว เช่น ชื่อนามสกุลจริง ที่อยู่ เบอร์โทรศัพท์ในข้อมูลส่วนตัวผู้ใช้ ถ้าเคยใส่ไว้ ให้ลบออกให้หมด ถึงแม้ว่าคุณจะใช้โปรแกรมสนทนาอื่นๆ เช่น ICQ หรือแชทรูมตามเว็บไซท์วัยรุ่นอื่นๆ ก็ขอให้ยึดหลักปฏิบัติเดียวกันนี้ เพื่อความปลอดภัย

9) ระวังการใช้กล้องเว็บแคม ขณะที่เราใช้โปรแกรมสนทนา เช่น MSN เราสามารถใช้กล้องเว็บแคมเพื่อให้คู่สนทนาเห็นภาพวีดีโอสดของเราได้ ถ้าเขาเองก็มีกล้องเว็บแคมเช่นกัน เราก็จะเห็นหน้าของเขาด้วย ยิ่งถ้ามีไมโครโฟนเสียบต่อกับคอม ก็จะสามารถพูดคุยออนไลน์แบบเห็นภาพและเสียงได้เลย ประหยัดและใช้ดีกว่าโทรศัพท์โดยเฉพาะเวลาคุยกับคนที่อยู่ต่างประเทศ แต่ผู้ใช้จะต้องใช้อินเทอร์เน็ตความเร็วสูงเท่านั้น จึงจะส่งผ่านภาพ และเสียงได้ทัน ที่น่าเป็นห่วงก็คือ การใช้แชทกับเพื่อนใหม่ ที่เพิ่งรู้จักกันทางอินเทอร์เน็ต เขาสามารถบันทึกภาพของเราขณะพูดคุยกับเขา เพื่อเอาไปใช้ในทางไม่ดีๆ ได้ เช่น เอาไปตัดต่อแล้วขาย นอกจากนี้ ถ้าผู้ใช้เป็นเด็ก อาจถูกมิจฉาชีพออนไลน์ พยายามขอให้เด็กเปิดเว็บแคม เพื่อจะได้เห็นภาพ/เสียง ของเด็กชัดๆ หลอกให้เด็กเอากล้องเว็บแคม หันไปยังทิศต่างๆ ของบ้าน เพื่อเก็บข้อมูลรายละเอียดบ้าน เตรียมการลักพาตัว หรือ โจรกรรมได้ ดังนั้น การติดตั้งอุปกรณ์เสริม อย่างกล้อง และไมค์ นี้ผู้ปกครองควรพิจารณาให้ดี ว่าสมควรหรือไม่ เด็กโตพอที่จะระมัดระวังป้องกันตัว และไม่หลงเชื่อพวกล่อลวงออนไลน์แล้วหรือยัง

นอกจากนี้การติดกล้องเว็บแคมที่ต่อติดอยู่กับเครื่องคอมตลอดเวลา เพราะระหว่างที่คุณไม่ได้อยู่หน้าเครื่องคอมฯ แต่ต่ออินเทอร์เน็ตทิ้งไว้ นักแคร็กมืออาชีพ พวกมิจฉาชีพไฮเทค สามารถล็อคเข้ามาในเครื่องของคุณ และสั่งเปิดกล้องเว็บแคมของคุณ เพื่อแอบบันทึกภาพบ้านของคุณ ประตู หน้าต่าง ทางเข้าออก เพื่อเตรียมการโจรกรรม หรือแอบถ่ายอิริยาบถของคุณตอนที่ไม่รู้ตัว แล้วเอาไปขายเป็นวีซีดีประเภทแอบถ่ายทั้งหลาย เรื่องแบบนี้ เกิดขึ้นจริงในต่างประเทศ อาจเกิดขึ้นแล้วในประเทศไทย แต่คงยังไม่รู้ตัวกัน ดังนั้นให้ถอดกล้องเว็บแคมออกทุกครั้งที่ไม่ใช้คอมพิวเตอร์ และถ้าไม่มีความจำเป็น ก็ไม่ต้องต่ออินเทอร์เน็ตทิ้งเอาไว้ถึงจะใช้บรอดแบรนด์(ไฮสปีด)อินเทอร์เน็ตก็ตาม

10) ไม่ควรบันทึกภาพวิดีโอ หรือเสียงที่ไม่เหมาะสมบนคอมพิวเตอร์ หรือบนมือถือ เพราะภาพ เสียง หรือวีดีโอนั้นๆ อาจรั่วไหลได้ เช่นจากการแคร็กข้อมูลหรือถูกดาวน์โหลดผ่านโปรแกรม เพียร์

ทู เพียร์ (P2P) และถึงแม้ว่าคุณจะลบไฟล์นั้นออกไปจากเครื่องแล้ว ส่วนใดส่วนหนึ่งของไฟล์ยังตกค้างอยู่ แล้วอาจถูกกู้กลับขึ้นมาได้ โดยช่างคอม ช่างมือถือ

11) จัดการกับ Junk Mail จังค์ เมล หรือ อีเมลขยะ ปกติ การใช้อีเมลจะมีกล่องจดหมายส่วนตัว หรือ Inbox กับ กล่องจดหมายขยะ Junk mail box หรือ Bulk Mail เพื่อแยกแยะประเภทของอีเมล เราจึงต้องทำความเข้าใจ และเรียนรู้ที่จะคัดกรองจดหมายอิเล็กทรอนิกส์ด้วยตัวเอง เพื่อกันไม่ให้มาปะปนกับจดหมายดีๆ ซึ่งเราอาจเผลอไปเปิดอ่าน แล้วถูกสปายแวร์ แอดแวร์เกาะติดอยู่บนเครื่อง หรือแม้แต่ถูกไวรัสคอมพิวเตอร์เล่นงาน

เวลาที่คุณใช้อีเมล ถ้าใครที่เป็นเพื่อนหรือคนรู้จัก ให้คุณ เซฟ (Save) หรือ บันทึกอีเมลของเพื่อนคุณเอาไว้ในสมุดจดที่อยู่(Address Book) ซึ่งจะมีอยู่แล้วใน Inbox หรือกล่องจดหมายอิเล็กทรอนิกส์ส่วนตัวของคุณ

เวลาที่คุณพบอีเมลที่มาจากคนไม่รู้จัก อีเมลที่มีหัวข้อส่อไปในทางลามก หรือพยายามขายสินค้า ให้คุณไปคลิกเลือกที่หน้าอีเมลนั้น แล้วเลือก Block หรือสกัดกั้น เขาก็จะส่งอีเมลมาหาเราไม่ได้อีก แต่เนื่องจากอีเมลขยะมีจำนวนมากมาจากหลายที่หลากหลายชื่อผู้ส่งจนบางครั้งเว็บไซต์ที่ให้บริการอีเมล ของเราเองก็สกัดกั้นไม่ไหว เราก็ต้องค่อยๆ เลือกทีละอันแล้ว คลิกแจ้งว่าอีเมลนี้เป็นอีเมลขยะ (Report as junk mail) ในครั้งต่อไป อีเมล์นั้นก็จะตกไปอยู่ใน Junk Mail Box แทน

บางครั้งอีเมลจากเพื่อนใหม่ที่เป็นเพื่อนของเราจริงๆ ส่งมาหาเราแต่เรายังไม่เคยบันทึกชื่ออีเมลของเขาไว้ในaddress book มาก่อน อีเมลของเพื่อนคนนั้นก็จะตกไปอยู่ในกล่องจดหมายขยะปะปนกับขยะจริงๆ เราจึงต้องหมั่นเข้าไปตรวจดูกล่องจดหมายขยะ เพื่อเลือกอีกครั้งว่ามีจดหมายดีๆ หลงเข้าไปอยู่บ้างหรือไม่ ถ้ามี ก็แค่บันทึกชื่ออีเมลของเพื่อนคนนั้นไว้ในสมุดจดที่อยู่ เพื่อที่คราวต่อไปเมื่อเพื่อนส่งอีเมลมาหาก็จะตรงเข้ากล่องจดหมายหลักแทนที่จะเข้ากล่องจดหมายขยะ

ปกติถ้าคุณเป็นคนที่ใช้อีเมล ควรหมั่นเข้าไปเช็คเมล์เรื่อยๆเพราะบางครั้งอีเมลขยะก็อาจจะทำให้พื้นที่รับจดหมายของคุณเต็ม ทำให้พลาดโอกาสรับข่าวสารดีๆ หรือข้อมูลสำคัญจากเพื่อนๆ
คุณควรมีอีเมลไว้ใช้อย่างน้อย 3 อีเมล์แอคเค้าท์ อันแรกอาจเป็นอีเมลงาน เอาไว้ติดต่อธุรกิจเท่านั้น ซึ่งไม่ควรให้อีเมลนี้กับคนทั่วไป อันที่สองคืออีเมลไว้ใช้ติดต่อกับเพื่อนๆ และอันที่ 3 ใช้เวลาไปกรอกข้อมูลสมัครสมาชิกร่วมรายการชิงโชคต่างๆ เพื่อกันพวกสแปมเมล ไวรัสเมล แอดแวร์ สปายแวร์ ออกจากอีเมลหลักที่ใช้เป็นประจำให้มากที่สุด

12) จัดการกับแอดแวร์ สปายแวร์จัดการกับสปายแวร์แอดแวร์ที่ลักลอบเข้ามาสอดส่องพฤติกรรมการใช้เน็ตของคุณ ด้วยการซื้อโปรแกรมหรือไปดาวน์โหลดฟรีโปรแกรมมาดักจับและขจัดเจ้าแอดแวร์ สปายแวร์ออกไปจากเครื่องของคุณ ซึ่งสามารถดาวน์โหลดโปรแกรมฟรีได้ที่ www.lavasoftusa.com/software/adaware/ www.safernetworking.org แต่แค่มีโปรแกรมไว้ในเครื่องยังไม่พอ คุณต้องหมั่นอัพเดทโปรแกรมออนไลน์และสแกนเครื่องของคุณบ่อยๆด้วย เพื่อให้เครื่องของคุณปลอดสปาย ข้อมูลของคุณก็ปลอดภัย

* โปรแกรมล้าง แอดแวร์ และ สปายแวร์ จะใช้โปรแกรมตัวเดียวกัน ซึ่งบางครั้งเขาอาจตั้งชื่อโดยใช้แค่เพียงว่า โปรแกรมล้าง แอดแวร์ แต่อันที่จริง มันลบทิ้งทั้ง แอดแวร์ และสปายแวร์พร้อมๆ กัน เพราะเจ้าสองตัวนี้ มันคล้ายๆ กัน

13) จัดการกับไวรัสคอมพิวเตอร์ คอมพิวเตอร์ทุกเครื่องจำเป็นต้องมีโปรแกรมสแกนดักจับและฆ่าไวรัส ซึ่งอันนี้ควรจะดำเนินการทันทีเมื่อซื้อเครื่องคอม เนื่องจากไวรัสพัฒนาเร็วมาก มีไวรัสพันธุ์ใหม่เกิดขึ้นทุกวัน แม้จะติดตั้งโปรแกรมฆ่าไวรัสไว้แล้ว ถ้าไม่ทำการอัพเดทโปรแกรมทางอินเทอร์เน็ต เวลาที่มีไวรัส

ตัวใหม่ๆ แอบเข้ามากับอินเทอร์เน็ต เครื่องคุณก็อาจจะโดนทำลายได้ โปรแกรมตรวจจับไวรัสที่นิยมได้แก่ Norton Antivirus นอร์ตันแอนไทไวรัส, McAfee VirusScan แมคอะฟี่ ไวรัสสแกน, Kaspersky Anti-Virus Personal แคสเปอร์สกาย แอนไทไวรัส เพอเซินนอล, Trend PC-Cillin เทรนด์ พีซี ซิลลิน ฯลฯ ซึ่งคุณสามารถไปซื้อแผ่นโปรแกรม หรือ จะดาวน์โหลดฟรีโปรแกรม (AVG Virus Scan Free Edition) มาใช้ก็ได้ ที่ http://free.grisoft.com/freeweb.php/doc/2/ นอกจากโปรแกรมเหล่านี้จะช่วยดักจับไวรัสแล้ว ยังมีโปรแกรมเสริมที่เรียกว่า Firewall เช่น McAfree Personal Firewall Plus, Norton Personal Firewall หรือแม้แต่ในตัว WindowsXP Service Pack2 ขึ้นไป ก็จะมีโปรแกรมไฟร์วอล มาให้ด้วยซึ่ง ไฟร์วอลนี้ทำหน้าที่เหมือนตำรวจจราจรออนไลน์ คอยหยุดตรวจและดักจับสิ่งแปลกปลอมที่จะเข้ามารุกรานเครื่องคุณซึ่งจะช่วยป้องกันการถูกคนนอกเข้ามาแคร็กเอาข้อมูลจากเครื่องของคุณได้ นอกจากนี้ยังช่วยสกัดกั้นสิ่งแปลกปลอมที่อาจจะออกจากเครื่องของคุณ เช่นกรณีคอมของคุณติดไวรัส เป็นต้น โดยไฟร์วอลนี้ จะคอยตั้งคำถามคุณเสมอเวลาคุณเปิดเว็บไหน หรือใช้โปรแกรมอะไร เพื่อรอฟังคำอนุญาตของคุณ แล้วจดบันทึกเอาไว้ว่า เว็บลักษณะนี้ โปรแกรมประเภทนี้คุณอนุญาตหรือไม่อนุญาตให้ใช้ นอกจากจะช่วยกันพวกไวรัส สแปม สปายแล้ว ยังเป็นการสกรีนและป้องกันการเปิดเข้าไปในเว็บไม่เหมาะสมได้ทางหนึ่ง สำหรับโปรแกรมไฟร์วอลนี้ ยังเป็นที่ถกเถียงกันอยู่ว่า จำเป็นต้องใช้จริงหรือ สามารถช่วยกันเด็กจากเว็บไม่เหมาะ สมได้จริงหรือ คุณจะใช้หรือไม่คงต้องตัดสินใจกันเอาเอง แต่สำหรับโปรแกรมดักจับไวรัสคอมฯ เป็นสิ่งจำเป็นสำหรับคอมพิวเตอร์ทุกเครื่องแน่นอน

14) ใช้ Adult Content Filter ในโปรแกรม P2P สำหรับผู้ชื่นชอบการดาวน์โหลดผ่านโปรแกรมแชร์ข้อมูล P2P ให้ระวังข้อมูลสำคัญ ไฟล์ภาพ วีดีโอส่วนตัว หรืออะไรที่ไม่ต้องการจะเปิดเผยสู่สาธารณะชน ควรบันทึกลงซีดี ดีวีดี หรือเทปไว้ อย่าเก็บไว้บนเครื่องคอมพิวเตอร์ เพราะคุณอาจถูกเจาะเอาข้อมูลเหล่านี้ไปได้ สำหรับครอบครัวที่จำเป็นต้องใช้โปรแกรมดาวน์โหลด แต่ก็ไม่อยากให้เด็กในบ้านเปิดใช้แล้วดาวน์โหลดเจอแต่ภาพ วีดีโอโป๊ สามารถตั้งค่ากรอง เนื้อหาไม่เหมาะสมจากการสืบค้นได้ ยกตัวอย่างโปรแกรม Kazaa กาซ่า จะมีฟังก์ชั่น สกรีนเนื้อหาไม่เหมาะสมออกจากการสืบค้นได้ ซึ่งเรียกว่า Family Filter แฟมิลี่ ฟิลเตอร์ หรือการกรองเนื้อหาไม่เหมาะสมสำหรับครอบครัว ซึ่งเข้าไปตั้งค่าได้ใน Kazaa Media Destop Options กาซ่า มีเดีย เดสท็อป อ็อปชั่นส์

15) เซิร์ชข้อมูลอย่างปลอดภัย ด้วย Google ปัจจุบันการเซิร์ชหรือสืบค้นข้อมูลผ่าน Search Engine เซิร์ชเอ็นจิ้น อย่าง Google.com เป็นเสมือนหนึ่งในกิจวัฏของผู้ใช้อินเทอร์เน็ตไปแล้ว แต่เนื่องจากผลจากการสืบค้นนั้นมีหลากหลายมาก และถ้าเด็กใช้ ก็อาจเผลอเปิดไปเจอเว็บไซท์สำหรับผู้ใหญ่ ที่อาจแอบแฝงตัวด้วยการใช้ชื่อธรรมดาๆ หรือชื่อน่ารักๆ ชื่อตัวการ์ตูนต่างๆได้ แต่เราป้องกันได้ ด้วยการตั้งค่า Google Preferences เพื่อให้ กูเกิ้ล กรองเนื้อหา และภาพไม่เหมาะสมสำหรับเด็กออกไปจากผลการสืบค้น ซึ่งมีขั้นตอนง่ายๆ ดังนี้

- เข้าไปที่หน้า Google Preferences
- แล้วลงไปตั้งค่าที่หัวข้อ Safe Search Filtering
- เลือกระดับความเข้มงวดในการคัดกรองภาพและเนื้อหาที่ไม่เหมาะสมสำหรับเด็กได้ตามความต้องการ
- แล้วคลิก “เซฟ” (Save preferences) เพื่อบันทึกการตั้งค่า

16) กรองเว็บไม่เหมาะสมด้วย Content Advisor ในอินเทอร์เน็ต เอ็กซ์พลอเรอ ในโปรแกรมเว็บ บราวเซอร์ อย่าง อินเทอร์เน็ต เอ็กซ์พลอเรอ ก็มีการตั้งค่า คอนเทนท์ แอดไวเซอร์ หรือฟังก์ชั่นการกรองเนื้อหาที่ไม่เหมาะสมสำหรับเด็ก ซึ่งจะทำให้เด็กไม่สามารถเปิดเข้าไปในเว็บไซท์ที่มีภาพและเนื้อหา

โป๊ เปลือย ภาษาหยาบคาย รุนแรงได้ และยังมีการตั้งพาสเวิร์ด หรือรหัส สำหรับผู้ปกครอง เพื่อกันเด็กเข้าไปแก้ไขการตั้งค่าของคุณ ซึ่งคุณสามารถเข้าไปปลดล็อกได้ทุกเมื่อ ถ้าคุณจำเป็นต้องเข้าเว็บไซท์บางเว็บไซต์

17) POP-UP Blocker การจัดการกับกล่องข้อความ ป๊อป-อัพ ที่เปิดตัวอัตโนมัติทันทีที่เราเปิดเว็บไซท์บางเว็บไซท์ ซึ่งบ่อยครั้งจะเป็นข้อความ ขายสินค้าสำหรับผู้ใหญ่ต่างๆและมักจะมีพวกสปายแวร์กระโดด เข้ามาซ่อนอยู่ในคอมของเราอีกด้วย การป้องกัน ป๊อป-อัพ เปิดตัวอัตโนมัติทำได้ง่ายนิดเดียว สำหรับผู้ใช้อินเทอร์เน็ต เอ็กซ์พลอเรอ เข้าไปที่ Tools เลือก Pop-up Blocker เพียงเท่านี้ ก็จะไม่มีป๊อป-อัพ โผล่ขึ้นมากวนใจคุณอีก

18) ปลาวาฬ บราวเซอร์ (Plawan Browser)

ทางเลือกใหม่ในการท่องเว็บ อย่างปลอดภัย สำหรับคนไทย ใช้งานง่ายด้วยเมนูภาษาไทย พร้อมดิกชันนารีในตัว ติดขัดศัพท์คำไหนคลิกแปลได้ทันที แถมยังมีระบบรักษาความปลอดภัยเป็นเยี่ยม ช่วยกรองเว็บที่มีภาพ ภาษา และเนื้อหาไม่เหมาะสม เข้าไปอ่านรายละเอียดเพิ่มเติม และดาวน์โหลดมาใช้ (ฟรี) ที่ www.plawan.com

19) ปลาวาฬ ทูลบาร์ (Plawan Toolbar) สำหรับผู้ใช้ ที่ยังคงติดใจ เว็บบราวเซอร์ เดิมๆ อย่าง Internet Explorer แต่ต้องการความปลอดภัย สามารถดาวน์โหลดเฉพาะ Plawan toolbar เป็นอุปกรณ์เสริม ซึ่งสามารถติดตั้ง และใช้ควบคู่ไปกับ Internet Explorer ได้ โดยปลาวาฬ ทูลบาร์นี้มีหน้าที่อำนวยความสะดวกในการ แจ้งชื่อเว็บไซต์ที่ไม่เหมาะสม และแนะนำเว็บไซต์ที่ดีๆ เหมาะสำหรับเยาวชน โปรแกรมสามารถติดตั้งได้บนคอมพิวเตอร์ทั่วไป ที่ใช้ระบบ ปฏิบัติการ Windows98 และ WindowsXP เข้าไปอ่านรายละเอียดเพิ่มเติมและดาวน์โหลดมาใช้(ฟรี)ที่ www.plawan.com

นอกจากนี้ทางกระทรวงไอซีที ยังได้ออกโปรแกรมตัวใหม่ Housekeeper เฮ้าส์คีปเปอร์ เพื่อช่วยบล็อกเว็บไม่เหมาะสม ช่วยจำกัดเวลาการใช้อินเทอร์เน็ตใช้คอม โดยผู้ปกครองเป็นคนตั้งค่าเอง ซึ่งสามารถดาวน์โหลดได้ที่ www.icthousekeeper.com

บรรณานุกรมประจำบทที่ 3

[1] http://www.com5dow.com/ทิป-ความรู้ทั่วไป/2063-ส่วนประกอบของคอมพิวเตอร์-และหลักการทำงานของคอมพิวเตอร์.html (สืบค้นเมื่อ 20 สิงหาคม 2556).

[2] Waggoner, Shelly Cashman, 1996, Using Computers a Gateway to Information, Boyd & Fraser Pub Co.

[3] http:// www.pirun.ku.ac.th/~b4904281/page3.html (สืบค้นเมื่อ 20 สิงหาคม 2556).

[4] http://www.lks.ac.th/kuanjit/it002_1.htm (สืบค้นเมื่อ 20 สิงหาคม 2556).

[5] http://www.krusunanta.net/content/เครือข่ายคอมพิวเตอร์ (สืบค้นเมื่อ 21 สิงหาคม 2556).

[6] http://www.thaigoodview.com/node/90636 (สืบค้นเมื่อ 21 สิงหาคม 2556).

[7] http://www.kmcenter.rid.go.th/kcitc/2011/index.php?option=com_content&view=article&id=326:2011-08-29-09-18-07&catid=60:2011-08-29-08-47-05&Itemid=31 (สืบค้นเมื่อ 21 สิงหาคม 2556).

[8] http://www.th.wikipedia.org/wiki/เอชทีเอ็มแอล (สืบค้นเมื่อ 20 สิงหาคม 2556).

[9] http://www.th.wikipedia.org/wiki/เลขที่อยู่ไอพี (สืบค้นเมื่อ 20 สิงหาคม 2556).

[10] http://www.th.wikipedia.org/wiki/เอชทีทีพี (สืบค้นเมื่อ 20 สิงหาคม 2556).

[11] http://www.thaigoodview.com/node/90636 (สืบค้นเมื่อ 20 สิงหาคม 2556).

[12] http://www.dpu.ac.th/compcntre/page.php?id=2362 (สืบค้นเมื่อ 20 สิงหาคม 2556).

[13] เชลลี, การี บี, การสื่อสารข้อมูลระดับพื้นฐาน, กรุงเทพฯ : ทอมสัน, 2544.

[14] http://safenet.wetpaint.com (สืบค้นเมื่อวันที่ 1 สิงหาคม 2556)

บทที่ 4 ภัยคุกคามจากการใช้งานทางอินเทอร์เน็ต

ภัยคุกคามทางอินเทอร์เน็ตถือได้ว่าเป็นภัยอันตรายต่อสังคมในปัจจุบันเป็นอย่างมาก เพราะนอกจากภัยนี้จะเป็นการรบกวนการทำงานของผู้ที่ใช้งานคอมพิวเตอร์และอินเทอร์เน็ตแล้ว ยังส่งผลเสียต่อข้อมูลสำคัญๆ ที่มีอยู่ ชนิดของภัยคุกคามที่เกิดขึ้นบนอินเทอร์เน็ต จำแนกได้ดังนี้

1. มัลแวร์ (Malware) คือความไม่ปกติทางโปรแกรมที่สูญเสียความลับทางข้อมูล (Confidentiality) ข้อมูลถูกเปลี่ยนแปลง (Integrity) สูญเสียเสถียรภาพของระบบปฏิบัติการ (Availability) ซึ่งมัลแวร์แบ่งออกได้เป็นหลายประเภท ดังนี้

1.1 ไวรัสคอมพิวเตอร์ (Computer Virus) คือ รหัสหรือโปรแกรมที่สามารถทำสำเนาตัวเองและแพร่กระจายสู่เครื่องอื่นได้ โดยเจ้าของเครื่องนั้นๆ ไม่รู้ตัว ถือว่าเป็นสิ่งไม่พึงประสงค์ซึ่งฝังตัวเองในโปรแกรมหรือไฟล์ แล้วแพร่กระจายจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นๆ ผ่านทางสื่อต่างๆ สิ่งสำคัญคือไวรัสไม่สามารถแพร่กระจายได้หากขาดคนกระทำ เช่น แบ่งปันไฟล์ที่ติดไวรัสหรือส่งอีเมล์ที่ติดไวรัสเป็นต้น

1.2 หนอนคอมพิวเตอร์ (Computer Worm) เรียกสั้นๆ ว่า เวิร์ม เป็นหน่วยย่อยลงมาจากไวรัส มีคุณสมบัติต่างๆ เหมือนไวรัสแต่ต่างกันที่เวิร์มไม่ต้องอาศัยผู้ใช้งาน แต่จะอาศัยไฟล์หรือคุณสมบัติในการส่งต่อข้อมูลในคอมพิวเตอร์เพื่อกระจายตัวเอง บางทีเวิร์มสามารถติดตั้ง Backdoor ที่เริ่มติดเวิร์มและสร้างสำเนาตัวเองได้ ซึ่งผู้สร้างเวิร์มนั้นสามารถสั่งการได้จากระยะไกล ที่เรียกว่า Botnet โดยมีเป้าหมายเพื่อโจมตีคอมพิวเตอร์และเครือข่าย ส่งที่อันตรายอย่างยิ่งของเวิร์มคือ สามารถจำลองตัวเองในคอมพิวเตอร์เครื่องหนึ่งแล้วแพร่กระจายตัวเองออกไปได้จำนวนมาก ตัวอย่างเช่น สามารถดักจับ username และ password และใช้ข้อมูลนี้เพื่อบุกรุกบัญชีผู้ใช้นั้น ทำสำเนาตัวเองแล้วส่งต่อไปยังทุกรายชื่อที่มีอยู่ในลิสต์อีเมล และเมื่อสำเนาตัวเองเป็นจำนวนมากจะทำให้การส่งข้อมูลผ่านเครือข่ายช้าลง เป็นเหตุให้ Web Server และเครื่องคอมพิวเตอร์หยุดทำงาน

1.3 ม้าโทรจัน (Trojan Horse) คือ โปรแกรมชนิดหนึ่งที่ดูเหมือนมีประโยชน์ แต่แท้ที่จริงก่อให้เกิดความเสียหายเมื่อรันโปรแกรม หรือติดตั้งบนคอมพิวเตอร์ ผู้ที่ได้รับไฟล์โทรจันมักถูกหลอกลวงให้เปิดไฟล์ดังกล่าว โดยหลงคิดว่าเป็นซอฟต์แวร์ถูกกฎหมาย หรือไฟล์จากแหล่งที่ถูกต้องตามกฎหมาย เมื่อไฟล์ถูกเปิดอาจส่งผลลัพธ์หลายรูปแบบ เช่น สร้างความรำคาญด้วยการเปลี่ยนหน้าจอ สร้างไอคอนที่ไม่จำเป็น จนถึงขั้นลบไฟล์และทำลายข้อมูล โทรจันต่างจากไวรัสและเวิร์มคือโทรจันไม่สามารถสร้างสำเนาโดยแพร่กระจายสู่ไฟล์อื่น และไม่สามารถจำลองตัวเองได้

1.4 Backdoor แปลเป็นไทยก็คือประตูหลัง ที่เปิดทิ้งไว้ให้บุคคลอื่นเดินเข้านอกออกในบ้านได้โดยง่าย ซึ่งเป็นช่องทางลัดที่เกิดจากช่องโหว่ของระบบ ทำให้ผู้ไม่มีสิทธิเข้าถึงระบบหรือเครื่องคอมพิวเตอร์เพื่อทำการใดๆ

1.5 สปายแวร์ (Spyware) คือ มัลแวร์ชนิดหนึ่งที่ติดตั้งบนเครื่องคอมพิวเตอร์แล้วทำให้ล่วงรู้ข้อมูลของผู้ใช้งานได้โดยเจ้าของเครื่องไม่รู้ตัว สามารถเฝ้าดูการใช้งานและรวบรวมข้อมูลส่วนตัวของผู้ใช้ได้ เช่น นิสัยการท่องอินเทอร์เน็ต และเว็บไซต์ที่เข้าชม ทั้งยังสามารถเปลี่ยนค่าที่ตั้งไว้ของคอมพิวเตอร์ ส่งผลให้ความเร็วในการเชื่อมต่ออินเทอร์เน็ตช้าลง เป็นต้น สายแวร์ที่มีชื่อคุ้นเคยกันดีคือโปรแกรม Keylogger ซึ่งตกเป็นข่าวหน้าหนึ่งของหนังสือพิมพ์ เมื่อผู้ใช้ดาวน์โหลดไฟล์จากอินเทอร์เน็ตที่แฝงโปรแกรมนี้ จะทำให้โปรแกรมเข้าฝังตัวในคอมพิวเตอร์ส่วนตัว เมื่อผู้ใช้คอมพิวเตอร์ทำธุรกรรมการเงินทางอินเทอร์เน็ต ข้อมูล username และ password ของบัญชีผู้ใช้จึงถูกส่งตรงถึงมิจฉาชีพ และลักลอบโอนเงินออกมาโดยเจ้าของตัวจริงไม่รู้ตัว เป็นต้น

2. การโจมตีแบบ DoS/DDos คือการพยายามโจมตีเพื่อทำให้เครื่องคอมพิวเตอร์ปลายทางหยุดทำงาน หรือสูญเสียเสถียรภาพ หากเครื่องต้นทาง(ผู้โจมตี) มีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากผู้โจมตีมีมากและกระทำพร้อมๆ กัน จะเรียกกว่าการโจมตีแบบ Distributed Denial of Service (DDoS) ซึ่งในปัจจุบันการโจมตีส่วนใหญ่มักเป็นการโจมตีแบบ DDoS

3. BOTNET หรือ “Robot network” คือเครือข่ายหุ่นรบที่ถือเป็นสะพานเชื่อมภัยคุกคามทางเครือข่ายคอมพิวเตอร์ ด้วยมัลแวร์ทั้งหลายที่กล่าวในตอนต้นต้องการนำทางเพื่อต่อยอดความเสียหายและทำให้ยากแต่การควบคุมมากขึ้น

4. ข้อมูลขยะ (Spam) คือ ภัยคุกคามส่วนใหญ่ที่เกิดจากอีเมลหรือเรียกว่า อีเมลขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับได้ ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ anti-spam หรือใช้บริการคัดกรองอีเมลของเว็บไซต์ที่ให้บริการอีเมล หลายคนอาจจะสงสัยว่า spammer รู้อีเมลเราได้อย่างไร คำตอบคือได้จากเว็บไซต์ ห้องสนทนา ลิสต์รายชื่อลูกค้า รวมทั้งไวรัสชนิดต่างๆ ที่เป็นแหล่งรวบรวมอีเมลและถูกส่งต่อกันไปเป็นทอดๆ ซึ่งหากจำเป็นต้องเผยแพร่อีเมลทางอินเทอร์เน็ตโดยป้องกันการถูกค้นเจอจาก Botnet สามารถทำได้โดยเปลี่ยนวิธีการสะกดโดยเปลี่ยนจาก “@” เป็น “at” แทน

5. Phishing เป็นคำพ้องเสียงกับ “fishing” หรือการตกปลาเพื่อให้เหยื่อมาติดเบ็ด คือ กลลวงชนิดหนึ่งในโลกไซเบอร์ด้วยการส่งข้อมูลผ่านอีเมลหรือเมสเซนเจอร์ หลอกให้เหยื่อหลงเชื่อว่าเป็นสถาบันการเงินหรือองค์กรน่าเชื่อถือ แล้วทำลิงค์ล่อให้เหยื่อคลิก เพื่อหวังจะได้ข้อมูลสำคัญ เช่น username/password, เลขที่บัญชีธนาคาร, เลขที่บัตรเครดิต เป็นต้น แต่ลิงค์ดังกล่าวถูกนำไปสู่หน้าเว็บเลียนแบบ หากเหยื่อเผลอกรอกข้อมูลส่วนตัวลงไป มิจฉาชีพสามารถนำข้อมูลไปหาประโยชน์ในทางมิชอบได้

6. Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งบนเครือข่ายในองค์กร (LAN) เป็นวิธีการหนึ่งที่นักโจมตีระบบนิยมใช้ดักข้อมูลเพื่อแกะรหัสผ่านบนเครือข่ายไร้สาย (Wirdless LAN) และดักข้อมูล User/Password ของผู้อื่นที่ไม่ได้ผ่านการเข้ารหัส [1]

4.1 วิธีสังเกตภัยคุกคามจากอินเทอร์เน็ต

ปัจจุบันการขยายตัวของเครือข่ายออนไลน์เป็นไปอย่างรวดเร็วและเติบโตอย่างกว้างขวางจนเรียกได้ว่ากลายเป็นศูนย์รวมสินค้าขนาดมหึมา สำหรับกลุ่มนักล่าออนไลน์ที่มุ่งจะล่วงละเมิดทางเพศต่อเยาว ชน เว็บไซต์ประเภทต่างๆ ไม่ว่าจะเป็นไดอารี่ออนไลน์ เว็บหาเพื่อนร่วมโรงเรียนหรือต่างโรงเรียน เว็บหาคู่ ที่เรียก ว่าชุมชนออนไลน์ หรือการเล่นแชทไลน์ 1900 กลายเป็นสื่อร้ายที่ผู้กระทำผิดคิดมิชอบต่อเยาวชน ผู้อ่อนด้อยต่อโลก เข้าไปค้นหาข้อมูลแล้วกระทำการล่อลวง เยาวชนของเราให้กลายเป็นเหยื่อชั้นดีอย่างง่ายดาย ตามข่าวเศร้าที่ได้พบ เห็นจากสื่อต่างๆ ทั้ง TV และ หนังสือพิมพ์ เหตุเพราะเยาวชนของเราหลงไปติดกับดัก โพสต์ข้อมูลส่วนตัว วิธีการติดต่อผ่าน mail และโปรแกรมรูปแบบต่างๆ

4.1.1 แนวทางการรับมือกับภัยออนไลน์

1) เมื่อตัวเราเอง หรือบุคคลใกล้ชิด ใช้เวลาเล่น Net มากเกินจำเป็น โดยเฉพาะช่วงเย็นถึงดึก และมักมีพิรุธปิดหน้าจอหรือเปลี่ยนหน้าจอทันทีที่ท่านเดินผ่าน

2) เมื่อพบว่าได้มีการ down load ภาพลามกไว้ใน computer ซึ่งได้รับจากนักล่าออนไลน์ส่งมากระตุ้นเร้าความรู้สึก และสร้างความคุ้นเคยทางเพศให้ผู้รับภาพ

3) เมื่อพบว่าตัวเอง หรือบุคคลใกล้ชิด ได้รับโทรศัพท์ จากบุคคลที่ไม่เคยรู้จักมาก่อนหรือมีการใช้โทรศัพท์ทางไกลไปยังหมายเลขที่ไม่รู้จัก

4) เมื่อมีพัสดุ ของขวัญ จดหมายลึกลับมาให้ตัวเรา หรือบุคคลใกล้ชิดของท่าน

5) เมื่อตัวเรา หรือบุคคลใกล้ชิด มีอาการห่างเหินกับกิจกรรมของสมาชิกในครอบครัวแยกตัวจากกลุ่ม หรือเก็บตัวอยู่คนเดียว [2]

4.1.2 วิธีป้องกันภัยคุกคามทางอินเทอร์เน็ต

1) การตั้งสติก่อนเปิดเครื่อง ต้องรู้ตัวก่อนเสมอว่าเราอยู่ที่ไหน ที่นั่นปลอดภัยเพียงใด

2) ก่อน login เข้าใช้งานคอมพิวเตอร์ต้องมั่นใจว่าไม่มีใครแอบดูรหัสผ่านของเรา

3) เมื่อไม่ได้อยู่หน้าจอคอมพิวเตอร์ ควรล็อกหน้าจอให้อยู่ในสถานะที่ต้องใส่ค่า login

4) ตระหนักอยู่เสมอว่าข้อมูลความลับและความเป็นส่วนตัวอาจถูกเปิดเผยได้เสมอในโลกออนไลน์

5) การกำหนด password ที่ยากแก่การคาดเดา ควรมีความยาวไม่ต่ำกว่า 8 ตัวอักษร และใช้อักขระพิเศษไม่ตรงกับความหมายในพจนานุกรม เพื่อให้เดาได้ยากมากขึ้นและการใช้งานอินเทอร์เน็ตทั่วไป เช่นการ Login ระบบ e-mail, ระบบสนทนาออนไลน์ (chat), ระบบเว็บไซต์ที่เป็นสมาชิกอยู่ ทางที่ดีควรใช้ password ที่ต่างกันบ้างพอให้จำได้

6) การสังเกตขณะเปิดเครื่องว่ามีโปรแกรมไม่พึงประสงค์ถูกเรียกใช้ขึ้นมาพร้อมๆ กับการเปิด

เครื่องหรือไม่ ถ้าสังเกตไม่ทันให้สังเกตระยะเวลาบูธเครื่อง หากนานผิดปกติอาจเป็นไปได้ว่าเครื่องคอมพิวเตอร์ติดปัญหาจากไวรัส หรือภัยคุกคามรูปแบบต่างๆ ได้

7) การหมั่นตรวจสอบและอัพเดท OS หรือซอฟต์แวร์ที่ใช้ให้เป็นปัจจุบัน โดยเฉพาะโปรแกรมป้องกันภัยในเครื่องคอมพิวเตอร์ เช่น โปรแกรมป้องกันไวรัส, โปรแกรมไฟร์วอลล์ และควรใช้ระบบปฏิบัติการและซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย นอกจากนี้ควรอัพเดทอินเทอร์เน็ตเบราเซอร์ให้ทันสมัยอยู่เสมอ

8) ไม่ลงซอฟต์แวร์มากเกินความจำเป็น

<u>ซอฟต์แวร์ที่จำเป็นต้องลงในเครื่องคอมพิวเตอร์</u> ได้แก่

- อินเทอร์เน็ตเบราเซอร์ เพื่อให้เปิดเว็บไซต์ต่างๆ
- อีเมลเพื่อใช้รับส่งข้อมูลและติดต่อสื่อสาร
- โปรแกรมสำหรับงานด้านเอกสาร, โปรแกรมตกแต่งภาพ เสียง วีดีโอ
- โปรแกรมป้องกันไวรัสคอมพิวเตอร์และโปรแกรมไฟร์วอลล์

<u>ซอฟต์แวร์ที่ไม่ควรมีบนเครื่องคอมพิวเตอร์ที่ใช้งาน</u> ได้แก่

- ซอฟต์แวร์ที่ใช้ในการ Crack โปรแกรม
- ซอฟต์แวร์สำเร็จรูปที่ใช้ในการโจมตีระบบ, เจาะระบบ (Hacking Tools)
- โปรแกรมที่เกี่ยวกับการสแกนข้อมูล การดักรับข้อมูล (Sniffer) และอื่นๆ ที่อยู่ในรูปซอฟต์แวร์สำเร็จรูปที่ไม่เป็นที่รู้จัก
- ซอฟต์แวร์ที่ใช้หลบหลีกการป้องกัน เช่น โปรแกรมซ่อน IP Address

9) ไม่ควรเข้าเว็บไซต์เสี่ยงภัยเว็บไซต์ประเภทนี้ ได้แก่

- เว็บไซต์ลามก อนาจาร
- เว็บไซต์การพนัน
- เว็บไซต์ที่มีหัวเรื่อง “Free” แม้กระทั่ง Free Wi-Fi
- เว็บไซต์ที่ให้ดาวน์โหลดโปรแกรมที่มีการแนบไฟล์พร้อมทำงานในเครื่องคอมพิวเตอร์
- เว็บไซต์ที่แจก Serial Number เพื่อใช้ Crack โปรแกรม
- เว็บไซต์ที่ให้ดาวน์โหลดเครื่องมือในการเจาะระบบ

10) สังเกตความปลอดภัยของเว็บไซต์ที่ให้บริการธุรกรรมออนไลน์ เว็บไซต์ E-Commerce ที่ปลอดภัยควรมีการทำ HTTPS มีใบรับรองทางอิเล็กทรอนิกส์ และมีมาตรฐานรองรับ

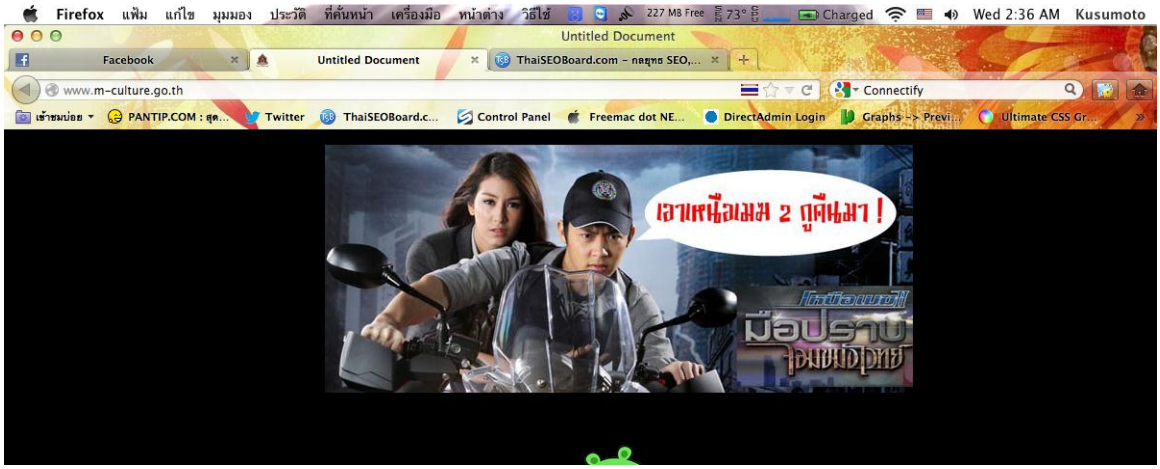
11) ไม่เปิดเผยข้อมูลส่วนตัวลงบนเว็บ Social Network ชื่อที่ใช้ควรเป็นชื่อเล่นหรือฉายาที่กลุ่มเพื่อนรู้จัก และไม่ควรเปิดเผยข้อมูลดังต่อไปนี้ เลขที่บัตรประชาชน เบอร์โทรศัพท์ หมายเลขบัตรเครดิต หมายเลขหนังสือเดินทาง ข้อมูลทางการแพทย์ ประวัติการทำงาน

12) ศึกษาถึงข้อกฎหมายเกี่ยวกับการใช้สื่ออินเทอร์เน็ต ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยมีหลักการง่ายๆ ที่จะช่วยให้สังคมออนไลน์สงบสุข คือให้คำนึงถึงใจเขาใจเรา

13) ไม่หลงเชื่อโดยง่าย อย่าเชื่อในสิ่งที่เห็น และงมงายกับข้อมูลบนอินเทอร์เน็ต ควรหมั่นศึกษาหาความรู้จากเทคโนโลยีอินเทอร์เน็ต และศึกษาข้อมูลให้รอบด้าน ก่อนปักใจเชื่อในสิ่งที่ได้รับรู้

4.2 กรณีศึกษาเกี่ยวกับภัยคุกคามจากการใช้งานทางอินเทอร์เน็ต

แฮกเว็บกระทรวงวัฒนธรรม



รูปที่ 3-35 ตัวอย่างเว็บไซต์ที่ถูกแอกระบบข้อมูล

เว็บไซต์ของกระทรวงวัฒนธรรม (www.m-culture.go.th) ถูกแฮกระบบข้อมูล มีการนำลิงค์เว็บไซต์พนันบอลมาโพสต์ไว้ มีแฮกเกอร์ ใช้ชื่อว่า THE BAD PIGGIES TEAM โดยโพสต์ภาพละครเหนือเมฆ 2 โดยมีข้อความระบุว่า “เอาเหนือเมฆ 2 กูคืนมา”

จากการระงับการถ่ายทอดละครหลังข่าวทางโทรทัศน์ เข้าใจว่าอาจเป็นการแสดงให้เห็นถึง การจำกัดสิทธิในการแสดงออกทางความคิด และส่งผลให้เกิดกลุ่มบุคคลที่ไม่พึงพอใจกับการกระทำนี้ ถึงแม้ว่าการแฮกเข้าเว็บของกระทรวงวัฒนธรรม กระทำเพื่อเรียกร้องสิทธิเสรีภาพในการแสดงออกทางความคิด แต่ก็ก่อให้เกิดความเสียหายต่อข้อมูล และชื่อเสียงของกระทรวงวัฒนธรรม ที่เป็นหน่วยงานระดับประเทศนั้น เป็นการกระทำที่ผิด ไม่สมควรที่จะกระทำ เพราะยังมีวิธีการแสดงความคิดในแบบอื่นๆอีกหลายวิธี โดยที่จะไม่ก่อให้เกิดความเสียหายในด้านอื่นๆ และการกระทำนี้จะส่งผลในทางเสียหายอื่นๆอีกมาก เช่น การถูกมองว่าเป็นหน่วยงานระดับประเทศแต่มีการป้องกันระบบสารสนเทศที่ไม่มีความปลอดภัย ข้อมูลใดๆที่สำคัญหรือเป็นความลับก็มีความเสี่ยง และไม่ปลอดภัยมาก ขาดความน่าเชื่อถือ เป็นต้น อีกทั้งการกระทำในลักษณะนี้ยังเป็นการกระทำผิดกฎหมายเกี่ยวกับคอมพิวเตอร์ ในการก่อความเสียหายให้กับเว็บไซต์ โดยการเข้าระบบที่ผู้อื่นมีการป้องกันและก่อความเสียหายทางข้อมูล ซึ่งการแสดงออกทางความคิดอาจไม่ผิดในแง่จริยธรรม แต่การคุกคามระบบที่มีการป้องกันก็ไม่ใช้การกระทำที่มีความประสงค์ที่ดีแน่นอน

สาเหตุของปัญหาเกิดจากความไม่พอใจในเรื่องส่วนบุคคล ที่เกิดจากการระงับการถ่ายทอดละครหลังข่าวทางโทรทัศน์ ของกลุ่มบุคคลที่ไม่ประสงค์ดี

ผู้มีส่วนรับผิดชอบ ได้แก่ เจ้าหน้าที่ผู้ดูแลเว็บไซต์ของกระทรวงวัฒนธรรม, กลุ่มบุคคลที่ทำการแฮกเว็บไซต์ให้เกิดความเสียหาย, ผู้บริการด้านสารสนเทศ และผู้บริหารระดับสูงของกระทรวงวัฒนธรรม

วิธีการแก้ปัญหา ได้แก่ เพิ่มนโยบาย มาตรการต่างๆให้ระบบสารสนเทศมีความแข็งแรง เช่น การกำหนดระยะเวลาในการเปลี่ยนพาสเวิร์ดของการเข้าถึงข้อมูลสำคัญ หาข้อบกพร่อง ช่องโหว่จากความเสียหายครั้งนี้และพัฒนาระบบเพื่ออุดช่องโหว่ และป้องกันเว็บไซต์ เช่น การนำระบบสมาชิก เพื่อทำการยืนยันบุคคล

มีการตรวจสอบ และเก็บข้อมูลการเข้าถึง เพื่อสังเกตกลุ่มบุคคลที่เข้าข่ายเสี่ยง หรือมีพฤติกรรมที่น่าสงสัยในการเข้าเว็บไซต์ [3]

บรรณนานุกรมประจำบทที่ 4

[1] http://www.nattapon.com/2011/12/%E0%B8%A0%E0%B8%B1%E0%B8%A2%E0%B8%84%E0%B8%B8%E0%B8%81%E0%B8%84%E0%B8%B2%E0%B8%A1%E0%B8%97%E0%B8%B2%E0%B8%87%E0%B8%AD%E0%B8%B4%E0%B8%99%E0%B9%80%E0%B8%97%E0%B8%AD%E0%B8%A3%E0%B9%8C%E0%B9%80%E0%B8%99/ (สืบค้นเมื่อวันที่ 23 สิงหาคม 2556)

[2] http://www.dkt.ac.th/kruya/50webm6/unit1/internet/page7.htm (สืบค้นเมื่อวันที่ 23 สิงหาคม 2556)

[3] http://news.mthai.com/general-news/213055.html (สืบค้นเมื่อวันที่ 23 สิงหาคม 2556)

บทที่ 5 เครือข่ายสังคมออนไลน์

5.1 โครงสร้างของเครือข่ายสังคมออนไลน์

Social Network คือ แพลตฟอร์ม (สภาวะแวดล้อมในการทำงานร่วมกัน) หรือเว็บไซต์ที่มุ่งเน้นไปในการสร้างและสะท้อนให้เห็นถึงเครือข่าย หรือความสัมพันธ์ทางสังคม ในกลุ่มคนที่มีความสนใจ หรือมีกิจกรรมร่วมกัน บริการเครือข่ายทางสังคม จะมีองค์ประกอบหลักที่ใช้เป็นตัวแทนของผู้ใช้งาน เช่น ข้อมูลส่วนตัว ความสัมพันธ์เชื่อมโยงระหว่างแต่ละบุคคล และบริการเสริมต่างๆ ที่มีความหลากหลาย บริการเครือข่ายทางสังคมเกือบทั้งหมด จะให้บริการผ่านหน้าเว็บ และให้มีการตอบโต้กันระหว่างผู้ใช้งานผ่านทางอินเทอร์เน็ต[1]

ปัจจุบันมีเว็บไซต์ประเภท Social Network เกิดขึ้นจำนวนมาก ทั้งที่มีเป้าหมายเชิงพาณิชย์ และไม่แสวงหากำไร ที่กำลังได้รับความนิยมอยู่ทั่วทุกมุมโลก อาทิ

1) Facebook

Mark Zuckerberg ก่อตั้ง Facebook เว็บชุมชนออนไลน์ (Social Networking Site) ที่กำลังได้รับความนิยมสุดขีดในขณะนี้ เมื่อ 3 ปีก่อน ขณะยังเรียนอยู่ที่ Harvard ก่อนจะลาออกกลางคัน เจริญรอยตาม Bill Gates แห่ง Microsoft เพื่อเป็น CEO ของเว็บชุมชนออนไลน์ที่เขาก่อตั้งขึ้น ด้วยวัยเพียง 22 ปีเท่านั้น ภายในเวลาเพียง 3 ปี เว็บที่เริ่มต้นจากการเป็นเว็บชุมชนออนไลน์สำหรับนักศึกษามหาวิทยาลัย กลายเป็นเว็บที่มีผู้ใช้ที่ลงทะเบียน 19 ล้านคน ซึ่งรวมถึงข้าราชการในหน่วยงานรัฐบาล และพนักงานบริษัทที่ติดอันดับ Fortune 500 มากกว่าครึ่งหนึ่งของผู้ใช้ เข้าเว็บนี้เป็นประจำทุกวัน และขณะนี้กลายเป็นเว็บที่มีผู้เข้าชมมากเป็นอันดับ 6 ในสหรัฐ 1% ของเวลาทั้งหมดที่ใช้บน Internet ถูกใช้ในเว็บ Facebook นอกจากนี้ยังได้รับการจัดอันดับเป็นเว็บที่ผู้ใช้ Upload รูปขึ้นไปเก็บไว้มากเป็นอันดับหนึ่งของสหรัฐฯ โดยมีจำนวนรูปที่ถูก Upload ขึ้นไปบนเว็บ 6 ล้านรูปต่อวัน

2) Twitter

ทวิตเตอร์ (Twitter) เป็นบริการเครือข่ายสังคมออนไลน์จำพวกไมโครบล็อก โดยผู้ใช้สามารถส่งข้อความยาวไม่เกิน 140 ตัวอักษร ว่าตัวเองกำลังทำอะไรอยู่ หรือ ทำการทวีต (tweet - ส่งเสียงนกร้อง) ทวิตเตอร์ก่อตั้งโดยบริษัท Obvious Corp เมื่อเดือนมีนาคม ค.ศ. 2006 ที่ซานฟรานซิสโก สหรัฐอเมริกา ข้อความอัปเดตที่ส่งเข้าไปยังทวิตเตอร์จะแสดงอยู่บนเว็บเพจของผู้ใช้คนนั้นบนเว็บไซต์ และผู้ใช้คนอื่นสามารถเลือกรับข้อความเหล่านี้ทางเว็บไซต์ทวิตเตอร์,อีเมล,เอสเอ็มเอส,เมสเซนเจอร์หรือผ่านโปรแกรมเฉพาะอย่าง Twitterific Twhirl ปัจจุบันทวิตเตอร์มีหมายเลขโทรศัพท์สำหรับส่งเอสเอ็มเอสในสามประเทศ คือ สหรัฐอเมริกา แคนาดา และสหราชอาณาจักร ปัจจุบันประเทศไทยเองก็มีบริการลักษณะนี้เช่นกัน นั่นคือ Noknok และ Kapook OnAir เว็บไซต์แห่งหนึ่งถึงกับรวบรวมบริการแบบเดียวกับทวิตเตอร์ได้ถึง 111 แห่ง ตัวระบบซอฟต์แวร์ของทวิตเตอร์เดิมทีนั้นพัฒนาด้วย Ruby on Rails จนเมื่อราวสิ้นปี ปี 2008 จึงได้เปลี่ยนมาใช้ภาษา Scala บนแพลตฟอร์มจาวา จนกระทั่งปี 2009 ทวิตเตอร์ได้รับความนิยมสูงขึ้นอย่างมาก จนนิตยสารไทม์ ฉบับวันที่ 15 ปี 2009 ได้นำเอาทวิตเตอร์ขึ้นปก และเป็นเรื่องเด่นประจำฉบับ ภายในนิตยสาร

บทบรรณาธิการกล่าวถึงการเปลี่ยนแปลงการนำเสนอข่าวที่มีที่มาจากเทคโนโลยีใหม่อย่างทวิตเตอร์ โดยทวิตเตอร์เป็นเว็บไซต์ที่ก่อตั้งขึ้นโดย แจ็ก คอร์ซีย์ บิซ สโตน และอีวาน วิลเลียมส์ เมื่อเดือนมีนาคม ปี 2006

3) My Space

My Space คือ เว็บบล็อกที่ทาง msn ให้ผู้ที่ใช้ msn ได้เข้าไปใช้บริการกัน ก็มีคำถามต่ออีกว่า เจ้า web blog คืออะไร สำหรับ เจ้า Web Blog คล้ายกับไดอารี่ โดยบล็อกจะมีความหลากหลายมากกว่า เพราะในบล็อก ผู้ที่เป็นเจ้าของเนื้อที่นั้นจะเป็นผู้ที่ดูแลเนื้อหาว่าจะให้เป็นแนวไหน หรือว่าจะเป็นเนื้อเรื่องอะไร

4) Instagram

Instagram เป็นโปรแกรมแบ่งปันรูปภาพ โดยถูกคิดค้นและพัฒนาขึ้นมาในเดือน ตุลาคม พ.ศ. 2553 โดยผู้ใช้งานสามารถถ่ายรูปและตกแต่งรูปภาพได้ตามใจต้องการ และแบ่งปันผ่าน โซเชียลเน็ตเวิร์ก โดยการตกแต่งรูปนั้นจะเน้นในแนวย้อนยุค หรือ กล้องโพลารอยด์

5) Google+

Google+ เป็นบริการเครือข่ายสังคมออนไลน์ให้บริการโดยกูเกิล โดยเปิดให้ใช้งานครั้งแรก เมื่อวันที่ 28 มิถุนายน พ.ศ. 2554 ผู้ที่จะเข้ามาทดลองใช้ต้องได้รับเชิญจากบุคคลที่ใช้อยู่เท่านั้น ภายหลังในวันที่ 20 กันยายน พ.ศ. 2554 จึงเปิดให้ผู้ใช้ทั่วไปได้ใช้งาน

6) Socialcam

Socialcam เปิดตัว 7 มีนาคม 2554 Socialcam เป็นโปรแกรมวิดีโอมือถือทางสังคม สำหรับ ไอโฟน และ แอนดรอยด์ ช่วยให้ผู้ใช้งานสามารถจับภาพและแบ่งปันวิดีโอออนไลน์บนมือถือรวมทั้งผ่านทาง เฟซบุ๊ก ทวิตเตอร์ และเครือข่ายทางสังคมอื่นๆ

7) YouTube

YouTube เป็นเว็บไซต์ที่ให้ผู้ใช้งานสามารถอัปโหลดและแลกเปลี่ยนคลิปวีดีโอผ่านทางเว็บไซต์ ก่อตั้งเมื่อ 15 กุมภาพันธ์ พ.ศ. 2548 โดย แชด เฮอร์ลีย์, สตีฟ เชง และ ยาวีด คาริม อดีตพนักงานบริษัทเพย์พอล (paypal) และมีสำนักงานอยู่ที่ ซานบรูโนในมลรัฐแคลิฟอร์เนีย ปัจจุบันยูทูบเป็นส่วนหนึ่งของกูเกิล

8) Line

Line เปิดตัววันที่ 23 มิถุนายน 2554 เป็นบริการเครือข่ายสังคมออนไลน์ที่พัฒนาจากโปรแกรมสนทนาสำหรับอุปกรณ์พกพา ไลน์สามารถใช้การติดต่อแบบเสียงได้เหมือนการโทรศัพท์ทั่วไป ผ่านโปรแกรมโดยไม่ต้องเสียค่าบริการกับผู้ให้บริการโทรศัพท์ ในส่วนของการส่งข้อความยังมีรูปภาพประกอบที่น่ารักเป็นที่ชื่นชอบของวัยรุ่นอีกด้วย

บริการเครือข่ายสังคม (Social Network Service) เป็นรูปแบบเว็บไซต์ ในการสร้างเครือข่ายสำหรับ

ผู้ใช้งานในอินเทอร์เน็ต เขียนและอธิบายความสนใจ และกิจการที่ได้ทำและเชื่อมโยงกับความสนใจและกิจกรรมของผู้อื่น ในบริการเครือข่ายสังคมมักจะประกอบไปด้วยการแชท ส่งข้อความ ส่งอีเมล วีดีโอ เพลง อัพโหลดรูป บล็อก ซึ่งสามารถจำแนกได้เป็น 7 กลุ่มดังนี้

1) Publish การเผยแพร่ข้อมูล เอกสาร หรือบทความ

2) Share การแบ่งปันข้อมูล รูปภาพหรือความรู้

3) Discuss สังคมในการระดมความคิด

4) Commerce เครือข่ายสังคมที่เกี่ยวกับธุรกิจ

5) Location การแบ่งปันสถานที่ที่น่าสนใจ

6) Network เครือข่ายเพื่อน ธุรกิจ งาน

7) Game เครือข่ายเกมส์

5.2 วิธีการป้องกันภัยบนเครือข่ายสังคมออนไลน์

อินเทอร์เน็ตเปรียบเสมือนดาบสองคมอาจทำให้เกิดประโยชน์ หรืออาจเป็นเครื่องมือในการสร้างความเสียหายได้ เช่น การโจรกรรมและภัยอันตรายต่างๆ แม้จะไม่สามารถสร้างความเสียหายโดยตรงทางกายได้ แต่ก็สามารถสร้างความเสียหายทางทรัพย์สิน ชื่อเสียงได้ไม่น้อย รูปแบบของภัยมักมีรูปแบบใหม่อยู่เสมอ แต่หากมีสิ่งที่ป้องกันไม่ว่าจะด้วยเทคโนโลยีและนโยบายการป้องกันส่วนตัว ก็สามารถชะลอการถูกอาชญากรบนโลกไซเบอร์โจมตีเราได้ โดยมีสิ่งที่ควรปฏิบัติโดยง่าย [2] ดังนี้

5.2.1 วิธีการใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารให้ถูกต้อง

บางครั้งความเสียหายที่เกิดขึ้นจากการใช้อุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารไม่ถูกต้อง เช่น เครื่องคอมพิวเตอร์ อุปกรณ์พกพา เป็นต้น ปัญหาส่วนใหญ่มักจะเกิดจากความประมาทของผู้ใช้งาน เช่น เข้าเว็บไซต์ที่เกี่ยวข้องกับธุรกรรมอิเล็กทรอนิกส์ หรือเปิดอีเมลลค้างไว้ในสถานที่ทำงานหรือสถานที่สาธารณะโดยไม่ได้ออกจากระบบ (Log Out) ส่งผลให้เกิดความเสียหายได้ ผู้ใช้งานจึงควรตระหนักและหาวิธีป้องกันปัญหาดังกล่าว เช่น ไม่ความเปิดเครื่องหรืออุปกรณ์ที่มีข้อมูลสำคัญทิ้งไว้โดยไม่อยู่ที่หน้าจอ ไม่เผลอบันทึก username และ password ขณะใช้เครื่องคอมพิวเตอร์สาธารณะ หลังจากเข้าอีเมลลแล้วไม่ควรลืมออกจากระบบ

5.2.2 การตั้งรหัสผ่าน

รหัสผ่านเปรียบเสมือนกุญแจบ้าน รหัสผ่านอาจจะประกอบไปด้วยตัวอักษร อักขระ ไปจนถึงตัวเลข ถ้าตั้งรหัสผ่านเป็นวลี หรือคำที่สามารถคาดเดาได้ ถ้ากระบวนการตั้งรหัสผ่านนั้นไม่ดีพอ ซึ่งเรียกว่ารหัสผ่านที่ไม่เข้มแข็ง อาจทำให้มีผู้ไม่ประสงค์ดีหรือแฮคเกอร์สามารถล่วงรู้และนำไปใช้ประโยชน์ในทางมิชอบได้ ดังนั้นสถาบันทางด้านความมั่นคงปลอดภัยไปจนถึงผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัย จึงมีการให้คำแนะนำการตั้งรหัสผ่านให้ยากต่อการคาดเดาได้

รหัสผ่านที่ปลอดภัย มีลักษณะโดยการผสมผสาน ดังต่อไปนี้ (โดยต้องมีการผสมกันอย่างน้อยสามในห้าข้อ)

- อักขระตัวเล็ก
- อักขระตัวใหญ่
- ตัวเลข
- วรรคตอน
- อักษรพิเศษ เช่น [ ] { } # % ^ * + = _ \ | ~ < > $. , ? ! - / : ; ( ) ฿ & @
- ต้องมีอย่างน้อย 8 ถึง 15 ตัวอักษร โดยที่มีตัวอักขระผสมกัน

5.2.3 การติดตั้งโปรแกรมป้องกันไวรัส (Anti-Virus Software)

ซอฟต์แวร์ป้องกันไวรัส (Anti-Virus Software) ของแต่ละผู้ผลิตจะโฆษณาถึงข้อดีของผลิตภัณฑ์ตัวเอง ผู้ผลิตบางรายสามารถกำจัดได้ทั้งไวรัสและสปายแวร์ พร้อมทั้งมีไฟร์วอล (Firewall) ในตัวโปรแกรม ผู้ผลิตบางรายอาจอ้างถึงความสามารถในการออกซิกเนเจอร์ (Signature) เพื่อกำจัดไวรัสใหม่ๆ ผู้ผลิตบางรายอาจมีให้ใช้งานฟรี หรือเป็นโอเพนซอร์ซ (Open-Source) ผู้ผลิตบางรายอาจมีราคาสูงแต่มีคุณสมบัติมากมาย ไม่ว่าจะเป็นของผู้ผลิตใดก็ตาม สิ่งที่สำคัญที่สุดในการใช้งาน คือ การอัพเดตซิกเนเจอร์อยู่เสมอและทำการสแกนไวรัสบ่อยๆ ซึ่งเป็นสิ่งที่หลายๆ คนละเลย จึงเป็นสาเหตุหลักที่ทำให้ยังคงมีไวรัสแพร่ระบาดเป็นประจำ

การเปรียบเทียบประสิทธิภาพในด้านต่างๆ ไม่ว่าจะเป็นด้านประสิทธิภาพ การให้ความช่วยเหลือเมื่อเกิดปัญหา การอัพเกรดและอัพเดตซิกเนเจอร์ เป็นต้น ซึ่งเป็นข้อมูลที่ช่วยในการตัดสินใจที่จะเลือกซอฟต์แวร์ป้องกันไวรัสได้ [11] ในการเปรียบเทียบนั้นจะมีเกณฑ์การให้คะแนนด้านความง่ายต่อการใช้งาน ประสิทธิภาพ ความเร็วในการอัพเดต ความง่ายในการติดตั้ง การช่วยเหลือการใช้งาน และคุณสมบัติเสริมอื่นๆ สามารถดูข้อมูลเพิ่มเติมได้ที่ http://anti-virus-software-review.toptenreviews.com/

5.2.4 การป้องกันการหลอกลวงทางโทรศัพท์

การหลอกลวงทางโทรศัพท์หรือแก๊งคอลเซ็นเตอร์เพื่อให้เหยื่อหลงเชื่อ คนร้ายส่วนใหญ่เป็นชาวจีนแผ่นดินใหญ่และไต้หวัน [10] ภายหลังพบชาวยุโรป [2] ออสเตรเลีย และหมู่ประเทศเพื่อนบ้านมากขึ้น ส่วนคนไทยหรือคนชาติอื่นที่เข้าร่วมขบวนการ เป็นเพียงพนักงานรับโทรศัพท์กับผู้เปิดบัญชีรับเงินที่ได้จากการล่อลวงเท่านั้น การตั้งคอลเซ็นเตอร์มี 2 รูปแบบ คือ ศูนย์ในประเทศไทยและศูนย์นอกประเทศไทย

นอกจากนั้นยังได้จำแนกกลุ่มแก๊ง “คอลเซ็นเตอร์” ออกเป็น 2 กลุ่มใหญ่ๆ ดังนี้ คือ แก๊งคืนเงินภาษี และแก๊งหนี้บัตรเครดิต

วิธีการป้องกันการหลอกลวงทางโทรศัพท์ มีดังนี้ [1]

1) ตรวจสอบหมายเลขที่โทรมาว่าเป็นหมายเลขของทางธนาคารที่ใช้บริการจริงหรือไม่

2) หากเป็นหมายเลขลักษณะ +56459876 ให้ต้องสงสัยไว้ก่อน

3) หากเป็นหมายเลข “ไม่โชว์เบอร์” ให้แจ้งต้นสายว่าจะติดต่อกลับไปที่ธนาคารเอง

4) ห้ามบอกรายละเอียดใดๆ ทั้งสิ้น ให้พยายามเป็นผู้ถามและฟังน้ำเสียง ส่วนมากคนร้ายเมื่อถูกถามถึงรายละเอียดหรือที่ตั้งธนาคาร ทุกรายเริ่มลังเล

5) หากยังสงสัยให้รีบวางหู

6) ข้อสำคัญที่สุด หากดำเนินการไปแล้วให้รีบแจ้งเจ้าหน้าที่ตำรวจให้เร็วที่สุด เพื่อออกให้อายัตเงินบัญชีของเรากับทางธนาคาร

5.3 กรณีศึกษาของเครือข่ายสังคมออนไลน์

ในสื่อสังคมออนไลน์อย่างเครือข่ายสังคมออนไลน์ (Social Network) จัดเป็นบริการออนไลน์ซึ่งอยู่บนพื้นฐานของการสร้างความสัมพันธ์ระหว่างบุคคลอันสะท้อนถึงความสนใจที่คล้ายคลึงกันหรือมีความเกี่ยวข้องกันในสังคม ไม่ว่าจะเป็นเฟซบุ๊ค (Facebook) มายสเปซ (MySpace) ทวิตเตอร์ (Twitter) หรือเว็บไซต์เครือข่ายสังคมออนไลน์อื่นๆต่างก็มีลักษณะเด่นที่เหมือนกันในการเปิดให้สมาชิกสร้างแฟ้มประวัติส่วนตัวเป็นเสมือนอีกตัวตนหนึ่งบนโลกออนไลน์เพื่อใช้ปฏิสัมพันธ์กับสมาชิกคนอื่นๆผ่านบริการช่องทางการสื่อสารที่หลากหลายบนเว็บไซต์ ทำให้ช่วง 5 ปีที่ผ่านมาจำนวนสมาชิกของเครือข่ายสังคมออนไลน์ต่างๆเพิ่มจำนวนขึ้นอย่างมหาศาล เครือข่ายสังคมออนไลน์ที่ใหญ่ที่สุดอย่างเฟซบุ๊คมีรายชื่อสมาชิกรวมทั้งโลกกว่า 500 ล้านรายชื่อ และมีสถิติรวมการใช้งานจากสมาชิกทุกคนเป็นเวลา 7 แสนล้านนาทีต่อเดือน (สถิติจากเฟซบุ๊ค 2011) ในขณะที่เทคโนโลยีการสื่อสารได้รับการพัฒนาอย่างก้าวล้ำ สื่อสังคมออนไลน์กลับส่งอิทธิพลลบต่อชีวิตประจำวันและความสัมพันธ์ของคนในสังคมอย่างชัดเจนมากยิ่งขึ้นจนกลายเป็นประเด็นทางสังคม ที่ทั้งสื่อบทกฎหมาย และประชาชนเองจะต้องให้ความสำคัญในการป้องกันและแก้ไขปัญหาเหล่านี้

1) การคุกคามผ่านสื่อออนไลน์ (Cyber Bullying) คือการคุกคามหรือรังแกกันผ่านเทคโนโลยีสารสนเทศ ทั้งอีเมลข่มขู่หรือแบล็คเมล การส่งข้อความทางโทรศัพท์ การข่มขู่ทางโทรศัพท์ โปรแกรมออนไลน์ และชัดเจนที่สุดคือการคุกคามผ่านสื่อสังคมออนไลน์ แม้ว่าการคุกคามกันบนโลกออนไลน์จะไม่ใช่การทำร้ายร่างกายหรือมีใครได้รับบาดเจ็บ แต่เป็นการทำร้ายทางอารมณ์ความรู้สึกซึ่งสามารถสร้างบาดแผลที่รุนแรงมากในทางจิตวิทยาอันจะส่งผลให้เกิดอาการหวาดระแวง ซึมเศร้า หดหู่ ไปจนถึงการฆ่าตัวตายในที่สุด

สำหรับในสื่อสังคมออนไลน์แล้ว การคุกคามในรูปแบบนี้กลายเป็นปัญหาที่นับวันจะทวีความรุนแรงมากขึ้นเรื่อยๆตามจำนวนของเยาวชนที่เข้ามาเป็นสมาชิกของเครือข่ายสังคมออนไลน์ที่เพิ่มมากขึ้น เพราะเครือข่ายสังคมออนไลน์กลายเป็นเครื่องมือให้มือมืดใช้พูดว่าคนอื่นอย่างที่ไม่สามารถทำได้ต่อหน้าจริงๆ ในสภาวะนิรนามโดยมีสื่อออนไลน์เป็นดังกำแพงกั้นระหว่างผู้กระทำและผู้ถูกกระทำ อย่างไรก็ตามข้อความว่าร้ายหรือข่มขู่ก็สามารถสร้างผลเสียให้กับคนที่ถูกคุกคามอย่างสาหัส การคุกคามผ่านออนไลน์จะเพิ่มจำนวนแซงการคุกคามเชิงกายภาพได้อย่างง่ายดายเพราะทำได้ง่ายทุกที่ ทุกเวลา

ตัวอย่างเช่นในปี 2009 เด็กหญิงชาวออสเตรเลียวัย 14 ปีก่อเหตุฆ่าตัวตายหลังจากถูกรังแกผ่านสื่อสังคมออนไลน์ แม่ของเด็กหญิงให้สัมภาษณ์กับสำนักข่าวเอบีซี (ABC News) ว่าถ้าลูกสาวของเธอไม่เข้าไปเห็นข้อความในคอมพิวเตอร์วันนั้นก็คงจะไม่ฆ่าตัวตาย[3]

และกรณีตัวอย่างอันเป็นที่รู้จักดีของการคุกคามผ่านโลกออนไลน์จนเป็นเหตุให้เกิดการฆ่าตัวตายของเมแกน ไมเยอร์ (Megan Meier) ซึ่งถูกล้อเลียนและว่าร้ายอย่างต่อเนื่องจากเครือข่ายสังคมออนไลน์จนเธอตัดสินใจจบชีวิตตัวเอง “เมแกนซึ่งมีอายุเพียง 13 ปีเริ่มได้รับข้อความว่าร้ายต่างๆนานจากเด็กผู้ชายที่เธอเพิ่งจะคบหาด้วยบนเครือข่ายออนไลน์ผ่านเว็บไซต์มายสเปซ โดยข้อความสุดท้ายที่ส่งถึงเธอเขียนว่าโลกคงจะดีกว่านี้ถ้าไม่มีผู้หญิงอย่างเธอ ทำให้เมแกนที่คิดว่าตนเองถูกปฏิเสธจากคนรักตัดสินใจฆ่าตัวตายในบ้านของเธอเอง” และที่แย่ไปกว่านั้นคือความจริงที่ว่าแฟนของเมแกนนั้นเป็นเพียงตัวละครสมมติที่ถูกสร้างขึ้นโดยแม่ของเพื่อนเก่าของเมแกนเอง ทั้ง 2 กรณีศึกษานี้แสดงให้เห็นถึงความรุนแรงของการคุกคามบนโลกออนไลน์ซึ่งสามารถพบได้ทุกที่ในโลกที่เครือข่ายสังคมออนไลน์เข้าถึง อัตราการฆ่าตัวตายของวัยรุ่นทั่วโลกไม่เคยสูงเท่านี้ก่อนที่จะเกิดสื่อสังคมออนไลน์ [4]

การตั้งกรุ๊ปบนเฟซบุ๊คก็สามารถใช้ในการคุกคามผู้อื่นได้ ดังที่เรามักจะเห็นปรากฏการณ์ล่าแม่มดเกิดขึ้นแล้วแม้กระทั่งในสังคมไทยเอง ทั้งในกรณีของสาวซีวิค มาร์คเอเอฟ หรือเด็กหญิงก้านธูป เพราะคนส่วนใหญ่มักลืมคิดไปว่าแม้คำพูดสั้นๆก็ถือเป็นการคุกคามกันได้ เช่นเมื่อปีที่แล้วในออสเตรเลียมีข่าวการโจมตีกันผ่านการแสดงความคิดเห็นระหว่างผู้ปกครองบนกรุ๊ปงานประกวดภาพเด็กแรกเกิดในเฟซบุ๊ค หลายความคิดเห็นต่อภาพของเด็กทารกเขียนว่าร้ายเด็กที่ยังไม่รู้เรื่องรู้ราวอะไรเลย

และนี่ก็เป็นอีกตัวอย่างของการคุกคามผ่านสื่อออนไลน์อันเป็นข้อเสียหนึ่งที่ยังไม่มีบทกฎหมายที่ชัดเจนมารองรับปัญหานี้โดยตรง[5]

2) การโจรกรรมเอกลักษณ์บุคคล (Identity Theft) ได้กลายเป็นปัญหาใหญ่ทั้งในสังคมไทยและประเทศอื่นๆทั่วโลก และยังเป็นอีกสาเหตุของการเติบโตอันรวดเร็วของจำนวนสมาชิกที่เพิ่มขึ้นบนเครือข่ายสังคมออนไลน์ มีรายงานจากกรมสถิติออสเตรเลียเมื่อปี 2008 ว่ามีประชาชนตั้งแต่อายุ 12 ปีขึ้นไปตกเป็นเหยื่อของการโจรกรรมเอกลักษณ์บุคคลหรือข้อมูลส่วนตัวอื่นๆรวมกว่า 806,000 คน เช่นเดียวกับที่สื่อมวลชนไทยรายงานข่าวการโจรกรรมเอกลักษณ์บุคคลที่เพิ่มขึ้นใน 5 ปีที่ผ่านมาอย่างต่อเนื่อง ซึ่งมีทั้งในกรณีของการแอบอ้างต้มตุ๋นเพื่อขูดรีดทรัพย์สิน ไปจนถึงการล่อลวงไปมีสัมพันธ์เชิงชู้สาว เป็นต้น

เฟซบุ๊คและทวิตเตอร์ก็เป็นเว็บเครือข่ายสังคมออนไลน์ที่เอื้ออำนวยให้เกิดการโจรกรรมเอกลักษณ์หรือข้อมูลส่วนบุคคลได้อย่างง่ายดายด้วยเครื่องมือ “แก้ไขข้อมูลส่วนตัว” (Edit your profile) ซึ่งจะแสดงทั้งชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ ความสนใจส่วนตัว อีเมลล์ รายชื่อเพื่อนสนิท หรือแม้กระทั่งข้อมูลส่วนตัวมากๆอย่างสถานะความสัมพันธ์กับคนรัก ซึ่งยิ่งข้อมูลเหล่านี้ที่แสดงอยู่บนเว็บไซต์เครือข่ายสังคมออนไลน์มากเท่าไหร่ก็จะยิ่งช่วยให้ผู้ร้ายสามารถลอกเลียนเอกลักษณ์และอัตลักษณ์ของเราเพื่อไปแอบอ้างในการก่ออาชญากรรมได้ง่ายขึ้น

อีกปัจจัยหนึ่งที่เอื้ออำนวยให้เกิดการโจรกรรมเอกลักษณ์บุคคลคือเครื่องมือ “การตั้งค่าความเป็นส่วนตัว” (Privacy Setting) ซึ่งมีให้ผู้ที่เป็นสมาชิกของเครือข่ายเปลี่ยนค่าการแสดงผลไม่ให้ผู้อื่นเห็นข้อมูลหรือข้อความบางอย่างที่เป็นเรื่องส่วนตัวหรือเราไม่ประสงค์จะให้คนอื่นรับรู้ แต่ปัญหาอยู่ที่ค่าความเป็นส่วนตัว

นี้จะไม่กลายเป็นค่าถาวร ดังนั้นผู้ที่ใช้งานเครือข่ายสังคมออนไลน์ที่ไม่ได้ระมัดระวังการตั้งค่าตัวนี้อาจเผลอส่งข้อความส่วนตัวหรือข้อความลับไปให้ทั้งคนรัก ครอบครัว เพื่อนสนิท เพื่อนไม่สนิท เพื่อนร่วมงาน และสาธารณชนทั่วทุกมุมโลก เช่นเมื่อเดือนตุลาคมที่ผ่านมา นายเอริค เบสชง รัฐมนตรีว่าการกระทรวงอุตสาหกรรมของฝรั่งเศสตกเป็นข่าวอื้อฉาวหลังจากที่ได้ทวิตข้อความส่วนตัวถึงภรรยาผ่านเว็บไซต์ทวิตเตอร์แต่เกิดความผิดพลาด เพราะข้อความที่ส่งไปกลายเป็นข้อความที่ส่งไปสู่สาธารณะหลังจากลืมตั้งค่าความเป็นส่วนตัว[6]

นอกจากนี้เครือข่ายสังคมออนไลน์ยังสนับสนุนให้สมาชิกแบ่งปันข้อมูลส่วนตัวของตนมากจนเกินความปลอดภัย จนทำให้ผู้ไม่หวังดีนำข้อมูลเหล่านั้นย้อนมาสร้างภัยให้กับเจ้าของข้อมูลได้ ยกตัวอย่างโฟร์สแควร์ (FourSquare) ซึ่งเป็นเครือข่ายสังคมที่ให้สมาชิกได้ “เช็คอิน” (Check-In) ตามสถานที่ต่างๆที่ตัวเองเดินทางไปถึงเพื่อสะสมแต้มและโล่รางวัล หรือใช้เช็คอินเพื่อรับส่วนลดจากร้านค้าต่างๆตามกลยุทธ์ทางการตลาด แต่การเช็คอินนั้นก็ทำให้ผู้อื่นรู้ว่าเรากำลังทำอะไรที่ไหนอยู่บ้าง เหล่าหัวขโมยก็จะอาศัยข้อมูลจากสื่อออนไลน์ตรงนี้ในการดูต้นทางในการขึ้นบ้านเพื่อไปลักขโมยทรัพย์สินมีค่าได้อย่างสะดวกทันทีที่รู้ว่าเจ้าของบ้านไม่อยู่ ดังนั้นเราจึงไม่ควรใส่ข้อมูลส่วนตัวที่มากจนเกินไปของเราลงบนเครือข่ายออนไลน์

3) เครือข่ายสังคมออนไลน์สร้างปัญหาทางความสัมพันธ์ของคนในสังคม ทำให้คนห่างไกลกันมากขึ้น เพราะวิธีการสื่อสารกับคนรู้จักและคนแปลกหน้าบนอินเทอร์เน็ตทำให้ความรู้สึกของคนเปลี่ยนไป ผลกระทบทางลบอีกอย่างหนึ่งของเครือข่ายสังคมออนไลน์คือความสัมพันธ์ของคนในสังคม แม้มันจะช่วยสร้างสัมพันธภาพให้เรากับคนที่ไม่สนิทให้รู้จักกันแน่นแฟ้นได้ง่ายขึ้น แต่คนเรามักจะมองไม่เห็นว่าเครือข่ายสังคมออนไลน์นั้นก็ทำให้เราห่างไกลจากคนที่เราสนิทด้วยมากขึ้น ด้วยความเป็น “เครือข่ายสังคม” จึงทำให้สมาชิกส่วนใหญ่คิดว่าเพียงแค่เป็นสมาชิกในเครือข่ายก็เท่ากับเป็นการเข้าสังคมแล้ว

หน้าต่างแสดง “สถานะล่าสุด” (News Feed) ทั้งบนเฟซบุ๊คและทวิตเตอร์ทำให้เรารู้ว่าญาติสนิทมิตรสหายของเราว่าเป็นอย่างไรกันบ้างโดยอัตโนมัติ ดังนั้นคนเราจะถามไถ่สารทุกข์สุขดิบกันทำไมในเมื่อเราสามารถเช็คสถานะ พร้อมรูปถ่ายที่บอกเล่ารายละเอียดของชีวิตเพื่อนผองเอาไว้แล้วอย่างครบถ้วน เมื่อก่อนเราอาจจะต้องโทรศัพท์หาหรือนัดทานข้าวเพื่อแลกเปลี่ยนเรื่องราวกันกับเพื่อนๆ แต่นั่นก็ไม่ใช่กิจกรรมที่จำเป็นอีกต่อไปแล้วในโลกปัจจุบันที่เรามีเครือข่ายสังคมออนไลน์ที่คอยเชื่อมสัมพันธ์ของเรากับคนสนิทไว้ไม่ให้หลุดหายจากกัน สิ่งที่เกิดขึ้นนี้ยิ่งทำให้คนเรามีปฏิสัมพันธ์กันแค่เพียงผิวเผิน เมื่อคนเราพบกันจึงมักปล่อยให้เวลาผ่านไปเรื่อยๆเพราะคิดว่าตัวเองได้พบปะกับคนเหล่านี้บนเครือข่ายออนไลน์มาก่อนแล้ว

มีผลสำรวจในกลุ่มนักศึกษาอเมริกันเกี่ยวกับความสัมพันธ์กับคนรอบข้างผ่านเครือข่ายสังคมออนไลน์พบว่า 1 ใน 7 เกิดความรู้สึกโดดเดี่ยวห่างไกลผู้คนมากขึ้นเมื่อใช้เครือข่ายสังคมออนไลน์ ผู้ตอบแบบสำรวจจำนวนมากได้เห็นข้อความแสดงสถานะของคนใกล้ชิดที่เข้าข่ายซึมเศร้าหรือระบายปัญหาในใจออกมา แต่มีคนเพียงนิดเดียวที่จะโทรหาหรือไปเยี่ยมคนใกล้ชิดของตนเป็นการส่วนตัวเมื่อเห็นข้อความเหล่านี้ ซึ่งถือเป็นผลข้างเคียงด้านลบของสื่อสังคมออนไลน์แม้จะไม่ได้เป็นปัญหาตามกฎหมายก็ตาม[7]

4) สื่อสังคมออนไลน์มีผลกระทบทางลบต่อการทำงานทั้งของนายจ้าง ลูกจ้าง และแม้กระทั่งว่าที่พนักงานในอนาคต เพราะสื่อที่เป็นเครือข่ายสังคมออนไลน์จะคอยรบกวนการทำงาน สมาธิของพนักงาน ทำให้ประสิทธิภาพในการทำงานลดลง เพิ่มมูลค่าต้นทุนของบริษัท และยังเป็นอันตรายต่อชื่อเสียงอีกทั้งความน่าเชื่อถือของบริษัท เพียงแค่พนักงานบางคนลืมตั้งค่าความเป็นส่วนตัวในทะเบียน

เครือข่ายสังคมออนไลน์ก็อาจต้องลงเอยด้วยการถูกไล่ออกจากบริษัทเพราะไปแสดงข้อความที่ไม่เหมาะสมไว้ก็เป็นได้ ยิ่งไปกว่านั้นเครือข่ายสังคมออนไลน์ก็อาจเป็นภัยแก่คนที่กำลังหางานทำ เพราะทั้งเฟซบุ๊คและมายสเปซต่างก็เป็นแหล่งข้อมูลชั้นเยี่ยมของหลายบริษัทต่างๆในการสอดส่องพฤติกรรมของผู้สมัครงานเพื่อใช้คัดกรองพนักงาน แฟ้มประวัติบนเฟซบุ๊คจำนวนมากแสดงข้อมูลหลายๆสิ่งที่คนหางานไม่อยากให้เจ้านายในอนาคตของตัวเองรับรู้ เว็บไซต์หางานชื่อดังอย่าง Careerbuilder.com ระบุว่ากว่า 45% ของนายจ้างใช้เครือข่ายสังคมออนไลน์ในการคัดเลือกพนักงาน

อย่างไรก็ตามสิ่งที่พลเมืองในสังคมสามารถทำได้ในการป้องกันภัยที่มาจากสื่อสังคมออนไลน์ก็คือการรู้เท่าทันสื่อ (Media Literacy) โดยต้องเข้าใจสภาพของสังคมสื่อออนไลน์ว่ามันก็เป็นสังคมอีกรูปแบบหนึ่งซึ่งมีทั้งพื้นที่ส่วนตัวและพื้นที่สาธารณะ เรียนรู้ธรรมชาติของการสื่อสารและการมีปฏิสัมพันธ์บนโลกออนไลน์กับชีวิตจริงว่ามีความแตกต่างกันอย่างไร และมีความระมัดระวัง รอบคอบในการจะแสดงความคิดเห็นข้อมูลส่วนตัว หรือภาพถ่ายต่างๆลงสู่เครือข่ายออนไลน์

และเช่นเดียวกับปัญหาอื่นๆที่เกิดขึ้นในสังคมภายนอก สาเหตุของปัญหาที่แท้จริงของสื่อออนไลน์นั้นอยู่ที่คนในสังคมขาดจริยธรรมและศีลธรรม ทั้งปัญหาการโจรกรรมทรัพย์สินในโลกแห่งความเป็นจริงหรือการโจรกรรมข้อมูลและเอกลักษณ์ส่วนตัวบนออนไลน์ การรังแกหรือคุกคามกันที่โรงเรียนหรือในเครือข่ายสังคมออนไลน์ เหล่านี้ล้วนแล้วเป็นเพราะคนไม่คำนึงถึงศีลธรรมอันดีงามในสังคม (Codes of Ethics)

หากสมาชิกในสังคมทั้งทางกายภาพและสังคมออนไลน์รู้หน้าที่ของตัวเอง มีความรับผิดชอบไม่ประมาท และคำนึงผลกระทบที่จะเกิดขึ้นจากการกระทำของตน ปัญหาของสังคมไม่ว่าจะเป็นสังคมใดก็ตามก็คงจะลดลง

บรรณานุกรมประจำบทที่ 5

[1] http://www.nattapon.com/2011/12/social-network/ (สืบค้นเมื่อวันที่ 11 สิงหาคม 2556).

[2] http://www.tistr.or.th/tistrblog/?p=567 (สืบค้นเมื่อวันที่ 11 สิงหาคม 2556).

[3] http://www.abc.net.au/news/2009-07-23/teens-death-highlights-cyber-bullying-trend/1363362 (สืบค้นเมื่อวันที่ 11 สิงหาคม 2556).

[4] http://topics.nytimes.com/topics/reference/timestopics/people/m/megan_meier/index.html 2011 (สืบค้นเมื่อวันที่ 11 สิงหาคม 2556).

[5] http://au.sports.yahoo.com/football/w-league/news/article/-/8946214/cute-baby-competition-turns-ugly/ (สืบค้นเมื่อวันที่ 11 สิงหาคม 2556).

[6] http://www.matichon.co.th/news_detail.php?newsid=1319088974&grpid=01&catid=01 (สืบค้นเมื่อวันที่ 11 สิงหาคม 2556).

[7] http://www.katonda.com/news/08/2010/1996 (สืบค้นเมื่อวันที่ 11 สิงหาคม 2556).

บทที่ 6 การกระทำความผิดทางคอมพิวเตอร์

การกระทำความผิดทางคอมพิวเตอร์ คือ การกระทำการที่ถือว่าเป็นความผิดตามกฎหมายและเป็นการกระทำผ่านหรือโดยอาศัยคอมพิวเตอร์ในการกระทำความผิด ซึ่งมีวัตถุประสงค์มุ่งต่อระบบคอมพิวเตอร์ ข้อมูลของคอมพิวเตอร์ หรือบุคคล

6.1 ประเภทการกระทำความผิดทางคอมพิวเตอร์

เมื่อพูดถึงภัยบนโลกอินเทอร์เน็ตที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศ “ไวรัสคอมพิวเตอร์” มีบทบาทตั้งแต่ยุคแรกเริ่มของคอมพิวเตอร์จนถึงปัจจุบัน เป็นที่คุ้นเคยของคนทุกเพศทุกวัยไม่ว่าจะเป็นผู้ที่เชี่ยวชาญ หรือบุคคลทั่วไป ไวรัสคอมพิวเตอร์เป็นเพียงส่วนหนึ่งของภัยคุกคามทางคอมพิวเตอร์จัดอยู่ในกลุ่ม มัลแวร์ (Malware หรือ Malicious Code Software) ซึ่งสามารถจำแนกได้ 2 ประเภท คือ การกระทำต่อระบบคอมพิวเตอร์ และ การใช้คอมพิวเตอร์ในการกระทำความผิด ดังนี้ [1]

6.1.1 การกระทำต่อระบบคอมพิวเตอร์

1) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 1

สปายแวร์ (Spyware), สนิฟเฟอร์ (Sniffer) มีผลกระทบต่อความมั่นคงปลอดภัย และความเสียหายคือ การสอดแนมข้อมูลส่วนตัว การแอบดักฟัง packet

2) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 2

การใช้ชุดคำสั่งในทางมิชอบ (Malicious Code) เช่น Viruses, Worms, Trojan Horses มีผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ การตั้งเวลาให้โปรแกรมทำลายข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์, การทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม หรือหยุดทำงาน (Denial of Service) [1]

3) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 3

การทำสแปม (Spamming) ปกปิด/ปลอมแปลงแหล่งที่มา ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ รบกวนการใช้ระบบคอมพิวเตอร์ตามปกติ อาจถึงขั้นทำให้เป็น Zombie [1]

4) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 4

BOT หรือ Botnet ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ ผลกระทบต่อความมั่นคงปลอดภัยของประเทศ หรือทางเศรษฐกิจ, ความปลอดภัยสาธารณะ, การบริการสาธารณะ อาจเกิดสงครามข้อมูลข่าวสาร (Information Warfare) [1]

5) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 5

Hacking Tools, Spam Tools ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหายคือ สอดแนมข้อมูลส่วนตัว, การแอบดักฟัง packet, การทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม หรือหยุดทำงาน (Denial of Service) [1]

6.1.2 การใช้คอมพิวเตอร์ในการกระทำความผิด

6) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 6

การใช้ชุดคำสั่งในทางมิชอบ (Malicious Code) เช่น Viruses, Worms, Trojan Horses, Phishing, ยุยง, หลอกลวง, ภาพลามก ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ การตั้งเวลาให้โปรแกรมทำลายข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์, การทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม หรือหยุดทำงาน (Denial of Service) หรือทำให้เกิดความวุ่นวายต่อเศรษฐกิจ ความมั่นคงของประเทศ

7) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 7

การสนับสนุน ส่งเสริม การใช้ชุดคำสั่งในทางมิชอบ (Malicious Code) เช่น Viruses, Worms, Trojan Horses, Phishing, ยุยง, หลอกลวง, ภาพลามก ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ เกิดความเสียหายต่อผู้อื่น

8) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 8

การตัดต่อภาพ ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ ผู้ถูกกระทำถูกดูหมิ่น ถูกเกลียดชัง หรืออับอาย

6.2 ชนิดภัยคุกคามที่เกิดขึ้นบนอินเทอร์เน็ต

เมื่อพูดถึงภัยบนโลกอินเทอร์เน็ตที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศ “ไวรัสคอมพิวเตอร์” มีบทบาทตั้งแต่ยุคแรกเริ่มของคอมพิวเตอร์จนถึงปัจจุบัน เป็นที่คุ้นเคยของคนทุกเพศทุกวัยไม่ว่าจะเป็นผู้ที่เชี่ยวชาญ หรือบุคคลทั่วไป ไวรัสคอมพิวเตอร์เป็นเพียงส่วนหนึ่งของภัยคุกคามทางคอมพิวเตอร์จัดอยู่ในกลุ่ม มัลแวร์ (Malware หรือ Malicious Code Software) ซึ่งสามารถจำแนกออกไปได้อีกหลากหลายรูปแบบ [2]

1) ชนิดภัยคุกคามรูปแบบมัลแวร์ (Malware)

การที่จะบอกได้ว่าข้อมูลนั้นมีความปลอดภัยหรือไม่จะต้องทำการวิเคราะห์คุณสมบัติทั้ง 3 ด้าน คือ ความลับ ความถูกต้อง และความพร้อมใช้งานว่ามีอยู่ครบหรือไม่ ถ้าขาดคุณสมบัติด้านใดด้านหนึ่งไปแสดงว่าข้อมูลนั้นไม่มีความปลอดภัย ดังนั้น การรักษาความปลอดภัยข้อมูลจึงเป็นการปกป้องรักษาคุณสมบัติทั้ง 3 ด้าน ดังต่อไปนี้

- ความลับ (Confidentiality) หมายถึง การทำให้ข้อมูลสามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- ความถูกต้อง (Integrity) หมายถึง การรักษาความคงสภาพของข้อมูลจากแหล่งที่มา หรือไม่ได้ถูกแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต
- ความพร้อมใช้งาน (Availability) หมายถึง การทำให้ผู้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้เมื่อต้องการ

มัลแวร์ คือ ความไม่ปกติทางโปรแกรม ที่สูญเสีย CIA อย่างใดอย่างหนึ่ง หรือทั้งหมดจนเกิดเป็นไวรัส เวิร์ม โทรจัน สปายแวร์ แบ็คดอร์ และ รู๊ทคิต

- การสูญเสีย C (Confidentiality) คือ สูญเสียความลับทางข้อมูล
- การสูญเสีย I (Integrity) คือ สูญเสียความไม่เปลี่ยนแปลงของข้อมูล นั่นคือ ข้อมูลถูกเปลี่ยนแปลงแก้ไข โดยเฉพาะส่วนสำคัญที่เกี่ยวโยงกับระบบภายในระบบปฏิบัติการ
- การสูญเสีย A (Availability) คือ สูญเสียเสถียรภาพของระบบปฏิบัติการ

2) ไวรัสคอมพิวเตอร์ (Computer Virus)

คือ รหัสหรือโปรแกรมที่สามารถทำสำเนาตัวเองและแพร่กระจายสู่เครื่องอื่นได้ โดยเจ้าของเครื่องนั้นๆ ไม่รู้ตัว (หากไม่ติดตั้งโปรแกรมป้องกันไวรัส หรือโปรแกรมดังกล่าวไม่รู้จักไวรัสชนิดนั้นๆ) ถือเป็นสิ่งไม่พึงประสงค์ซึ่งฝังตัวเองในโปรแกรมหรือไฟล์ [1] แล้วแพร่กระจายจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นๆ ผ่านสื่อรูปแบบต่างๆ เช่น CD, DVD, Multimedia Card, USB Drive หรือผ่านทางเครือข่าย เช่น อินเทอร์เน็ตระบบ LAN หรืออีเมล เป็นต้น ไวรัสอาจอาศัยอยู่ในเครื่องคอมพิวเตอร์ แต่ไม่แสดงความผิดปกติให้พบ หากผู้ใช้ไม่เรียกใช้โปรแกรมดังกล่าว สิ่งสำคัญคือไวรัสไม่อาจแพร่กระจายได้หากขาดคนกระทำ เช่น แบ่งปันไฟล์ที่ติดไวรัส หรือส่งอีเมลโดยแนบไฟล์ที่ติดไวรัส เป็นต้น ไวรัสคอมพิวเตอร์มีความรุนแรงหลายระดับ ตั้งแต่สร้างความรำคาญให้ผู้ใช้งาน จนถึงทำลายฮาร์ดแวร์ ซอฟต์แวร์ หรือไฟล์ข้อมูล ทำให้ผู้ใช้งานคอมพิวเตอร์จำเป็นต้องติดตั้งโปรแกรมป้องกันไวรัส จนกลายเป็นโปรแกรมสำคัญสำหรับคอมพิวเตอร์ทุกเครื่อง

3) หนอนคอมพิวเตอร์ (Computer Worm)

เรียกสั้นๆ ว่า “เวิร์ม” เป็นหน่วยย่อยลงมาจากไวรัส สามารถทำสำเนาตัวเองและแพร่กระจายผ่านเครือข่ายหรืออินเทอร์เน็ตสู่คอมพิวเตอร์หรือเครือข่ายอื่นได้ เวิร์มต่างจากไวรัสตรงที่ไม่ต้องอาศัยผู้ใช้งาน แต่จะอาศัยไฟล์หรือคุณสมบัติในการส่งต่อข้อมูลในคอมพิวเตอร์เพื่อกระจายตัวเอง [1] โดยสแกนเครือข่ายเพื่อหาระบบที่มีช่องโหว่ โจมตีช่องโหว่และบุกรุกเข้าระบบเหล่านั้นโดยอัตโนมัติ เวิร์มบางชนิดสามารถติดตั้ง Backdoor ในเครื่องคอมพิวเตอร์ที่ติดเวิร์ม และสร้างสำเนาตัวเองได้ โดยผู้สร้างเวิร์มชนิดนั้นสามารถสั่งการได้จากระยะไกล เรียกว่า Botnet มีเป้าหมายเพื่อโจมตีสร้างความเสียหายให้กับคอมพิวเตอร์และเครือข่าย หรือเพียงแค่ต้องการโฆษณาสินค้าหรือบริการ เวิร์มถึงจะเป็นหน่วยย่อยของไวรัส แต่ก็มีความรุนแรงกว่าไวรัสมาก สิ่งที่อันตรายอย่างยิ่งของเวิร์ม คือ สามารถจำลองตัวเองในคอมพิวเตอร์เครื่องหนึ่ง แล้วแพร่กระจายสำเนาของตัวเองออกไปได้จำนวนมาก ตัวอย่างเช่น สามารถดักจับ username และ password และใช้ข้อมูลนี้เพื่อบุกรุกบัญชีผู้ใช้นั้นทำสำเนาตัวเองแล้วส่งต่อไปยังทุกรายชื่อที่มีอยู่ในลิสต์อีเมล จากนั้นทำสำเนาต่อ แล้วส่งไปยังบัญชีรายชื่อของผู้รับอีเมลนั้นทุกคน ท้ายที่สุดส่งผลให้การรับส่งข้อมูลผ่านเครือข่าย (Network Bandwidth) ทำได้ช้าลง เป็นเหตุให้ Web Server, Network Server และเครื่องคอมพิวเตอร์หยุดทำงาน

4) BOTNET หรือ “Robot Network”

คือ เครือข่ายหุ่นรบที่ถือเป็นสะพานเชื่อมภัยคุกคามทางเครือข่ายคอมพิวเตอร์ด้วยมัลแวร์ทั้งหลายที่กล่าวในตอนต้น มัลแวร์ต้องการตัวนำทางเพื่อต่อยอดความเสียหายและทำให้ยากแก่การควบคุม ตัวนำทางที่ว่านี้ก็คือ Botnet ซึ่งก่อให้เกิดภัยคุกคามที่ไม่สามารถเกิดขึ้นได้เองโดยลำพัง เช่น Spam DoS/DDoS และ Phishing เป็นต้น ภัยคุกคามดังกล่าวจะมีคนควบคุมอยู่เบื้องหลัง เมื่อเครื่องของผู้

รู้เท่าไม่ถึงการณ์ติดมัลแวร์จะกลายเป็นผู้แพร่กระจาย Botnet ซึ่งจะถูกควบคุมจากระยะไกล ผู้ควบคุมอาจเป็น แฮคเกอร์ หรือกระทำการอิสระโดยอัตโนมัติตามที่ตั้งโปรแกรมไว้ แหล่งควบคุม Botnet ส่วนใหญ่อยู่ใน IRC (Internet Relay Chat) ห้องสนทนายุคแรกเริ่ม ด้วยเหตุผลหลัก 2 ประการ คือ

1.Protocol ในการติดต่อ IRC เป็นแบบ UDP (User Datagram Protocol) ซึ่งมีความเร็ว และ ไม่ต้องการความถูกต้องในการสื่อสารมากนัก ทำให้เครื่องที่ติด Botnet ไม่รู้ตัวว่าได้เชื่อมต่อ Server IRC ที่อยู่ห่างไกลออกไป
2.IRC เป็นแหล่งที่แฮคเกอร์ส่วนใหญ่ในอดีตใช้แลกเปลี่ยนเทคนิค รวมทั้งเรื่องราวต่างๆ เป็นแหล่งที่ยากต่อการควบคุมและค้นหาตัวตนที่แท้จริง

5) สปายแวร์ (Spyware)

คือ มัลแวร์ชนิดหนึ่งที่ติดตั้งบนเครื่องคอมพิวเตอร์ ทำให้ล่วงรู้ข้อมูลของผู้ใช้งานได้โดยเจ้าของเครื่องไม่รู้ตัว สปายแวร์จะทำการเฝ้าดูการใช้งานและรวบรวมข้อมูลส่วนตัวของผู้ใช้งาน อีกทั้งยังสามารถเปลี่ยนค่าที่ตั้งไว้ของคอมพิวเตอร์ ส่งผลให้ความเร็วในการเชื่อมต่ออินเทอร์เน็ตช้าลง หรือหน้าโฮมเพจเปลี่ยนแปลง เป็นต้น สปายแวร์ที่มีชื่อคุ้นเคยกันดีคือโปรแกรม Keylogger เมื่อผู้ใช้ดาวน์โหลดไฟล์จากอินเทอร์เน็ตที่แฝงโปรแกรม Keylogger ทำให้โปรแกรมเข้ามาฝังตัวในคอมพิวเตอร์ส่วนตัว เมื่อผู้ใช้ได้ใช้เครื่องคอมพิวเตอร์ทำธุรกรรมการเงินในเว็บไซต์ E-Banking ข้อมูล username และ password ของบัญชีผู้ใช้จะถูกส่งตรงถึงมิจฉาชีพ และทำการสวมรอยเป็นเจ้าของบัญชี เพื่อลักลอบโอนเงินออกมาจากบัญชีโดยที่เจ้าของนั้นไม่รู้ตัว

6) ม้าโทรจัน (Trojan Horse)

คือ โปรแกรมชนิดหนึ่งที่ดูเหมือนจะมีประโยชน์ แต่แท้จริงแล้วก่อให้เกิดความเสียหายเมื่อติดตั้งโปรแกรมลงบนคอมพิวเตอร์ ผู้ที่ได้รับไฟล์โทรจันมักถูกหลอกให้เปิดไฟล์ดังกล่าว โดยคิดว่าเป็นซอฟต์แวร์ หรือไฟล์จากแหล่งที่ถูกต้องตามกฎหมาย เมื่อไฟล์ถูกเปิดอาจเกิดผลลัพธ์หลากหลายรูปแบบ ตั้งแต่สร้างความรำคาญ เช่น เปลี่ยนหน้า Desktop หรือสร้างไอคอนที่ไม่จำเป็นบนหน้า Desktop จนถึงขั้นสร้างความเสียหายรุนแรง ด้วยการลบไฟล์และทำลายข้อมูลในคอมพิวเตอร์ โทรจันบางชนิดอาจฝัง Backdoor ไว้ในเครื่องคอมพิวเตอร์ เป็นเหตุให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงเครื่องคอมพิวเตอร์นั้นแล้วทำการล้วงข้อมูลส่วนตัว และข้อมูลที่เป็นความลับ สร้างความเสียหายได้ สิ่งหนึ่งที่โทรจันแตกต่างจากไวรัสและเวิร์มคือ โทรจันไม่สามารถสร้างสำเนาโดยแพร่กระจายสู่ไฟล์อื่น และไม่สามารถจำลองตัวเองได้

7) ประตูหลัง (Backdoor)

คือ ช่องทางลับที่เกิดจากช่องโหว่ของระบบ ทำให้ผู้ไม่ประสงค์ดีเข้าถึงระบบหรือเครื่องคอมพิวเตอร์ เพื่อใช้ทรัพยากรในเครื่องนั้นกระทำการใดๆ ได้ โดยทั่วไป Backdoor อาจเกิดจากความตั้งใจของผู้ดูแลระบบ เพื่อสร้างช่องทางลัดเข้าสู่ระบบเองก็เป็นได้ แต่เมื่อไปผสมผสานกับภัยคุกคามอื่น เช่น โทรจัน ทำให้ระบบเกิดช่องโหว่ ผู้ไม่ประสงค์ดีสามารถเข้าถึงและสร้างความเสียหายได้

8) ชนิดภัยคุกคามรูปแบบการโจมตีแบบขัดขวางหรือก่อกวนระบบ (DoS/DDoS)

คือ การพยายามโจมตีเพื่อทำให้เครื่องคอมพิวเตอร์ปลายทางหยุดทำงาน หรือสูญเสียเสถียรภาพ หากเครื่องต้นทาง (ผู้โจมตี) มีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากผู้โจมตีมีมากและกระทำพร้อมๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่าการโจมตีแบบ Distributed Denial of Service (DDoS) ด้วยเทคโนโลยีที่ก้าวล้ำในปัจจุบัน ซึ่งมีภัยคุกคามมากมาย และแพร่กระจายอย่างรวดเร็ว ทำให้การโจมตีส่วนใหญ่ในโลกออนไลน์ มักเป็นการโจมตีแบบ DDoS

9) ชนิดภัยคุกคามรูปแบบข้อมูลขยะ (Spam)

ส่วนใหญ่เกิดจากอีเมลหรือเรียกว่า อีเมลขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับโดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ anti spam หรือหากใช้ฟรีอีเมล เช่น hotmail yahoo ก็จะมีโปรแกรมคัดกรองอีเมลขยะในระดับหนึ่ง

10) ชนิดภัยคุกคามรูปแบบการหลอกลวงข้อมูล (Phishing)

เป็นคำพ้องเสียงกับ “fishing” หรือการตกปลาเพื่อให้เหยื่อมาติดเบ็ด คือ กลลวงชนิดหนึ่งในโลกไซเบอร์ด้วยการส่งข้อความผ่านอีเมลล์หรือเมสเซนเจอร์ หลอกให้เหยื่อเชื่อว่าเป็นสถาบันการเงินหรือองค์กรน่าเชื่อถือ เชิญชวนด้วยกลวิธีต่างๆ เช่น คุณได้รับรางวัล แล้วทำลิงค์หลอกให้เหยื่อคลิก เพื่อหวังจะได้ข้อมูลสำคัญ เช่น username / password เลขที่บัญชีธนาคาร เลขที่บัตรเครดิต เป็นต้น แต่ลิงค์ดังกล่าวจะนำไปสู่หน้าเว็บไซต์เลียนแบบ หากเหยื่อกรอกข้อมูลส่วนตัวลงไปมิจฉาชีพสามารถนำไปหาประโยชน์ในทางมิชอบได้ [1]

11) ชนิดภัยคุกคามรูปแบบการดักข้อมูล (Sniffing)

การดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งบนเครือข่ายในองค์กร (Local Area Network: LAN) เป็นวิธีการหนึ่งที่นักโจมตีระบบนิยมใช้ดักข้อมูล เพื่อแกะรหัสผ่านบนเครือข่ายไร้สาย (Wireless LAN) และดักข้อมูล Username / Password ของผู้อื่นที่ไม่ได้ผ่านการเข้ารหัส

6.3 แนวโน้มการกระทำความผิดทางคอมพิวเตอร์

แนวโน้มการกระทำความผิดทางคอมพิวเตอร์ในปี 2556 จะเกิดขึ้นกับอุปกรณ์พกพาเป็นส่วนมาก เนื่องจากมีผู้ใช้จำนวนมากที่หันไปใช้อุปกรณ์พกพาและคลาวด์ อาชญากรก็ปรับตัวตามไปโจมตีผู้ใช้งานเหล่านั้นเช่นกัน เราคาดการณ์ว่าแพลตฟอร์มอุปกรณ์พกพาต่างๆ และคลาวด์เซอร์วิซ จะเป็นเป้าหมายหลักที่มีแนวโน้มในการถูกโจมตีและการถูกละเมิดในปี 2556 นี่คือสิ่งที่จะเกิดมากขึ้นเป็นสองเท่าของมัลแวร์บนโทรศัพท์มือถือจากปี 2553-2554 เช่นเดียวกับการเพิ่มขึ้นอย่างรวดเร็วของมัลแวร์ของ Android ในปี 2555

นอกจากนี้ อุปกรณ์พกพาที่ไม่มีการจัดการเป็นอย่างดีและมีการเชื่อมต่อการใช้งานเข้า-ออกจากระบบเครือข่ายองค์กรและรับข้อมูลอย่างต่อเนื่อง มีแนวโน้มว่าภายหลังข้อมูลเหล่านั้นจะถูกเก็บไว้ในคลาวด์อื่นๆ โดยมีความเสี่ยงเพิ่มขึ้นจากการรั่วไหลและการโจมตีเป้าหมายของอุปกรณ์พกพา ขณะที่ผู้ใช้เพิ่มการใช้แอพพลิเคชั่นลงในโทรศัพท์มือถือก็รับเอามัลแวร์เข้ามาด้วย

จากการชำระเงินผ่านโทรศัพท์มือถือที่เพิ่มขึ้น เราอาจจะเห็นคนร้ายที่ใช้มัลแวร์ในการโจรกรรมข้อมูล

การชำระเงินจากผู้คนที่อยู่ในโลกการซื้อขายสินค้าออนไลน์ บางระบบการชำระเงินที่ใช้อย่างแพร่หลายกับผู้ไม่เคยมีประสบการณ์ด้านเทคนิค อาจมีช่องโหว่ที่ปล่อยให้ข้อมูลถูกโจรกรรมไปได้

ในขณะเดียวกัน เราคาดการณ์การเติบโตของแอดแวร์ในมือถือหรือ "ภัยร้ายทางโทรศัพท์มือถือ"ที่จะสร้างความรำคาญและรบกวนผู้ใช้และอาจจะเปิดเผยรายละเอียดสถานที่, ที่อยู่ติดต่อ และระบุอุปกรณ์ที่ใช้ให้อาชญากรไซเบอร์เห็น แมดแวร์ จะย่องเข้าไปในอุปกรณ์ของผู้ใช้เมื่อพวกเขาดาวน์โหลดแอพพลิเคชั่น - มักจะเป็นการส่งป๊อปอัพขึ้นแจ้งเตือนไปที่แถบการแจ้งเตือนบนไอคอน การเปลี่ยนแปลงการตั้งค่าเบราว์เซอร์ และรวบรวมข้อมูลส่วนบุคคล

วิธีการสร้างกระแสเงินสดในเครือข่ายสังคมนำมาซึ่งภัยคุกคามรูปแบบใหม่ การเพิ่มขึ้นของรูปแบบการสร้างกระแสเงินสดผ่านทางแพลตฟอร์มของโซเชี่ยลมีเดียจะทำอาชญกรรมในโลกไซเบอร์ใช้เป็นช่องทางในการโจมตีเหยื่อได้

ในฐานะผู้บริโภค เราใช้โซเชียลมีเดียกันอย่างไว้วางใจมากขึ้น เริ่มตั้งแต่การแชร์ข้อมูลส่วนบุคคล ใช้ซื้อเกมส์ ซื้อของขวัญให้เพื่อน เครือข่ายเหล่านี้เป็นจุดเริ่มต้นในการใช้แพลตฟอร์มเป็นสื่อกลางในการซื้อขายโดยอนุญาตให้สมาชิกซื้อของขวัญและส่งให้เพื่อนฝูง ซึ่งแพลตฟอร์มเหล่านั้นก็เป็นช่องทางใหม่ที่อาชกรในโลกไซเบอร์ใช้โจมตีเหยื่อได้ ซึ่งไซแมนเทคได้คาดการณ์ไว้ว่า การขโมยข้อมูลที่เหยื่อใช้ในการซื้อของในโลกโซเชียลเน็ตเวิร์ก หรือล่อลวงให้บอกข้อมูลการชำระเงิน ข้อมูลส่วนตัว โดยปลอมแปลงเครือข่ายสังคมออนไลน์หรือโซเชียลเน็ตเวิร์กจะเพิ่มมากขึ้น ซึ่งยังรวมถึงการสร้างของขวัญปลอม หรือส่งข้อความทางอีเมลเพื่อขอที่อยู่บ้านและข้อมูลส่วนตัวอื่นๆ อีกด้วย

<u>ตัวอย่างเช่น</u>

1) บัตรของขวัญจากสตาร์บัค ที่อาชญากรที่เรียกว่า scammers เสแสร้งว่าเป็นเจ้าของบัตรกำนัลของสตาร์บัคและหลอกให้เหยื่อให้ข้อมูลส่วนตัว อาทิ อีเมล ที่อยู่ และที่อยู่ในการจัดส่งบัตรกำนัลไปให้พร้อมกับมูลค่าในบัตรที่นำไปแลกสินค้าได้ อาชญากรประเภทนี้ยังใช้วิธีการใหม่ๆ ที่จะบ่ายเบี่ยงการตรวจจับ เช่น หลอกให้เหยื่อคิดว่ากำลังสนทนากับเจ้าหน้าที่หรือพนักงานของสตาร์บัคซึ่งเป็นแบรนด์ที่เหยื่อรายนั้นชื่นชอบ

2) โปรแกรมเรียกค่าไถ่ (Ransomeware) คือ สแกร์แวร์ รูปแบบใหม่

3) โปรแกรมเรียกค่าไถ่ หรือ แรนซัมแวร์ (Ransomware) เป็นอีกหนึ่งรูปแบบของภัยที่ต้องจับตามอง เพราะมีแนวโน้มเพิ่มขึ้นเรื่อยๆ โดยเป็นการอาศัยขั้นตอนวิธีการชำระเงินเพื่อขโมยข้อมูลจากเหยื่อเป้าหมาย

แรมซัมแวร์ (Ransomware) เป็นรูปแบบหนึ่งของโปรแกรมประสงค์ร้าย (malicious software) ซึ่งจะทำลายการทำงานของระบบคอมพิวเตอร์ทำให้ไม่สามารถเข้าอินเตอร์เน็ตได้และเรียกค่าไถ่เป็นข้อมูลส่วนตัวเพื่อให้สามารถกู้คืนระบบให้กลับสู่สภาวะปกติ แรนซัมแวร์ที่พบเมื่อเร็วๆ นี้ จะใช้วิธีขึ้นภาพบนหน้าจอและข้อความเตือนในลักษณะที่มาจากตำรวจว่าต้องจ่ายค่าปรับเพราะเข้าเว็บผิดกฎหมาย มัลแวร์ประเภทนี้จะใช้บริการการระบุสถานที่ตั้งของเครื่องคอมพิวเตอร์ที่กำลังเปิดใช้งานอยู่ หลังจากทำการล็อคหน้าจอให้เข้าใช้งานอินเทอร์เน็ตไม่ได้ ก็จะส่งข้อความขู่ในภาษากฎหมายที่ใช้อยู่ทั่วไปในประเทศนั้นๆ

แรมซัมแวร์ เป็นการหลอกลวงที่เหนือชั้นกว่าการพยายามหลอกเหยื่อ เพราะมันจะพยายามบังคับให้เหยื่อต้องยอมจำนน อาชญากรประเภทนี้ เลียนแบบวิธีการจับตัวประกันไปเรียกค่าไถ่ แต่ทำในโลกไซเบอร์คือ อาศัยหน้าจอเว็บไซต์ที่ผู้ใช้กำลังทำการชำระเงินทางออนไลน์[3]

6.4 กรณีศึกษาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์

6.4.1 กรณีศึกษาที่ 1

เมื่อวันที่ 16 ม.ค. 2556 ผู้สื่อข่าวได้รับการร้องเรียนจากประชาชนว่าขณะนี้มีภาพเด็กนักเรียนแต่งกายไม่เหมาะสมถูกนำมาเผยแพร่ผ่านทางอินเตอร์เน็ตในโลกโซเชียลเน็ตเวิร์ค และเว็บไซต์เฟซบุ๊ค โดยมีการส่งเผยแพร่ต่อกันมาเป็นจำนวนมาก รายละเอียดของภาพเป็นภาพเด็กสวมใส่ชุดนักเรียนหญิง 7 คน ส่วนใหญ่มีการถอดเสื้อผ้าออกเหลือเพียงยกทรงนั่งบ้างยืนบ้างโชว์หน้าอก ส่วนอีกคนสวมใส่เสื้อชุดนักเรียนคอซองแต่นั่งถ่างขาโชว์กางเกงในสีแดง และยังมีบางคนใส่เสื้อสายเดี่ยวและมีการแสดงท่าทางกอดรัดกัน โดยทั้งหมดได้ถ่ายภาพด้วยสีหน้ายิ้มแย้มแจ่มใสไม่ละอายในสิ่งที่ทำ

ผู้สื่อข่าวได้ตรวจสอบภาพดังกล่าว พบว่า มีต้นตอการส่งภาพมาจากบุคคลที่ใช้ชื่อว่า Beer nirvana มีผู้มาแสดงความคิดเห็นแสดงความชื่นชอบภาพดังกล่าวอย่างรวดเร็ว ในระยะเวลา 10 นาที มีผู้กดชื่นชอบเพิ่มขึ้นนับพันๆราย รวมทั้งมีการนำภาพดังกล่าวไปเผยแพร่แบ่งปันต่อๆกันเป็นจำนวนมาก.....[4]

<u>การกระทำความผิดตาม พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550</u>

จากข่าวข้างต้นเป็นการโพสต์รูปที่ไม่เหมาะสมลง Internet ในระบบ Social network ที่เข้าถึงได้ง่าย ซึ่งการโพสต์รูปเป็นรูปที่มีลักษณะโป๊เปลือย เป็นรูปเด็กนักเรียนหญิงม.ต้น 7 คน โพสต์ท่ายั่วยวน นุ่งน้อยห่มน้อย ถือว่าเป็นการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ใน มาตราต่อไปนี้

1) มาตรา 14 (4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

2) มาตรา 14 (5) ผู้ใดเผยแพร่และส่งต่อซึ่งข้อมูลลามก ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ

อีกทั้งยังผิดประมวลกฎหมายอาญาฐานหมิ่นประมาท มาตรา 326 และ 328 โดยต้องโทษจำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 2 แสนบาท

6.4.2 กรณีศึกษาที่ 2

กองปราบบุก จู่โจมค้น-จับ "เว็บประชาไท" หมิ่นสถาบัน

(6 มี.ค.) เมื่อเวลา 14.00 น.พล.ต.ต.วรศักดิ์ นพสิทธิพร รอง ผบช.ก.พ.ต.อ.สาธิต ต ชยภพ รอง ผบก.ป.พร้อมกำลังเจ้าหน้าที่ตำรวจกองปราบปรามนำหมายค้น ศาลอาญา เลขที่ 183/2552 ลงวันที่ 5 มี.ค. 2551 เข้าตรวจค้นภายในสำนักงานเว็บไซต์ประชาไท เลขที่ 409 ชั้น 1 อาคาร มอส.ซอยประชาราษฎร์ บำเพ็ญ 5 แขวงและเขตห้วยขวาง หลังจากทางเจ้าหน้าที่ตำรวจได้รับการร้องเรียนจากทางกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที) ว่า เว็บไซต์หนังสือพิมพ์ประชาไทออนไลน์ (www.prachatai.com) มีการโพสต์ข้อความลักษณะหมิ่นเบื้องสูง ในช่วงตั้งแต่วันที่ 15 ต.ค.-3 พ.ย.2551 ต่อเนื่องกัน เหตุเกิดในพื้นที่เขตพระราชวัง เขตปทุมวัน และ เขตห้วยขวาง

ทั้งนี้ จากหลักฐานที่ทางกระทรวงไอซีที มอบให้กับทางเจ้าหน้าที่พบข้อความภายในเว็บไซต์ดังกล่าวที่เข้าข่ายหมิ่นเบื้องสูงมากกว่า 40 ข้อความ จึงได้รวบรวมพยานหลักฐานเพื่อขอหมายค้น และหมายจับ นางสาวจีรนุช เปรมชัยพร อายุ 42 ปี ผู้อำนวยการเว็บไซต์ประชาไท อยู่บ้านเลขที่ 48/282 ซอยรามคำแหง 104 แขวงและเขตสะพานสูง ซึ่งทางศาลอาญาได้อนุมัติหมายจับผู้ต้องหา เลขที่551/2552 ลงวันที่ 3 มี.ค. 2551 ในข้อหากระทำผิด พ.ร.บ.คอมพิวเตอร์ พ.ศ.2550 มาตรา 14(1)(3)(5) เป็นผู้ให้บริการจงใจสนับสนุนหรือยินยอมให้มีการกระทำผิด นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมด หรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่จะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน, นำเข้าสู่ระบบคอมพิวเตอร์ ข้อมูลอันเป็นเท็จโดยประการที่จะเกิดความเสียหายต่อความมั่นคงประเทศ และเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพ์ตาม (1)(3)(5) และผิด พ.ร.บ.คอมพ์ มาตรา 15

จากการตรวจค้นภายในสำนักงานเว็บไซต์ดังกล่าว เจ้าหน้าที่ได้ทำการยึดคอมพิวเตอร์โน้ตบุ๊กของนางสาวจีรนุช มาทำการตรวจสอบ พร้อมกับเชิญตัว นางสาวจีรนุช ผอ.เว็บไซต์ประชาไท มาสอบปากคำที่กองปราบปราม โดยผู้ต้องหาได้ให้การปฏิเสธตลอดข้อกล่าวหา โดยอ้างว่าข้อความดังกล่าวที่อยู่ในเว็บไซต์ประชาไท เป็นข้อความของผู้ที่เข้ามาอ่านข่าวสารในเว็บ และเขียนไว้ในเว็บบอร์ดสาธารณะของเว็บไซต์ดังกล่าว ซึ่งภายหลังเจ้าหน้าที่ผู้ดูแลเว็บไซต์ตรวจพบก็ได้ลบข้อความที่มีเนื้อหาเชิงหมิ่นเบื้องสูงทิ้งหมดแล้ว

ผู้สื่อข่าวรายงานว่า สำหรับกรณีการตรวจค้นและจับกุม ผอ.เว็บไซต์หนังสือพิมพ์ประชาไทออนไลน์ ครั้งนี้ ทางเจ้าหน้าที่ตำรวจชุดจับกุมไม่สามารถเปิดเผยข้อมูลรายละเอียดเชิงลึกต่อสื่อมวลชนได้ เนื่องจากเป็นคดีสำคัญ

อย่างไรก็ตาม จากการสอบถาม นายชูวัส ฤกษ์ศิริสุข บรรณาธิการ ให้การในเบื้องต้น ว่า เข้าใจว่าประเด็นที่เจ้าหน้าที่ตำรวจจับกุมในครั้งนี้ น่าจะเกิดจากการที่มีผู้เข้ามาโพสต์ข้อความในเว็บบอร์ด ซึ่งมีข้อความเป็นจำนวนมาก อาจลบไม่ทันจึงเกิดปัญหาขึ้น

<u>การกระทำความผิดตาม พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550</u>

จากข่าวข้องต้น เป็นการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ในมาตรา 14 ระบุว่า ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ ได้แก่

14 (1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอม ไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

14 (3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

14 (5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1)(2)(3)(4)

มาตรา 15 ระบุว่า ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมา

และ ตามประมวลกฎหมายอาญา มาตรา 112 ซึ่งบัญญัติว่า “ผู้ใดหมิ่นประมาท ดูหมิ่น หรือแสดงความอาฆาตมาดร้ายพระมหากษัตริย์ พระราชินี รัชทายาท หรือผู้สำเร็จราชการแทนพระองค์ ต้องระวางโทษจำคุกตั้งแต่สามปี ถึงสิบห้าปี”

บรรณนานุกรมประจำบทที่ 6

[1] http://www.slideshare.net/tasawawan2k/04-rull-12767545 (สืบค้นเมื่อวันที่ 10 กรกฎาคม 2556).

[2] samtech-lms.net/Intranet_km/file_pdf/Threats.pdf (สืบค้นเมื่อวันที่ 10 กรกฎาคม 2556).

[3] http://www.ryt9.com/s/prg/1616696 (สืบค้นเมื่อวันที่ 10 กรกฎาคม 2556).

[4] http://www.komchadluek.net (สืบค้นเมื่อวันที่ 10 กรกฎาคม 2556).

[5] http://www.manager.co.th/Crime/ViewNews.aspx?NewsID=9520000025994 (สืบค้นเมื่อวันที่ 6 สิงหาคม 2556).

บทที่ 7 กฎหมายเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสาร และกฎหมายเกี่ยวกับโทรคมนาคม

7.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ ใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือ ทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

หรือสรุปเจตนารมณ์ได้ว่า “เพื่อกำหนดฐานความผิดและบทลงโทษ กำหนดอำนาจเจ้าหน้าที่ของพนักงานเจ้าหน้าที่ และกำหนดหน้าที่ของผู้ให้บริการ”

7.1.1 พนักงานเจ้าหน้าที่

เพื่อให้การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีความชัดเจนและเป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา 28 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารจึงได้กำหนดหลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ ดังต่อไปนี้ [1]

ข้อ (1) “พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 “รัฐมนตรี” หมายความว่า รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ (2) พนักงานเจ้าหน้าที่ ต้องมีคุณสมบัติ ดังต่อไปนี้

(1) มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์

(2) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรีทางวิศวกรรมศาสตร์ วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือรัฐประศาสนศาสตร์

(3) ผ่านการอบรมทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) สืบสวน สอบสวน และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics)

(4) มีคุณสมบัติอื่นอย่างหนึ่งอย่างใด ดังต่อไปนี้

ก. รับราชการหรือเคยรับราชการไม่น้อยกว่าสองปีในตำแหน่งเจ้าหน้าที่ตรวจพิสูจน์พยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์ หรือพยานหลักฐานอิเล็กทรอนิกส์

ข. สำเร็จการศึกษาตามข้อ 2 (2) ในระดับปริญญาตรี และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสี่ปี

ค. สำเร็จการศึกษาตามข้อ 2 (2) ในระดับปริญญาโท หรือสอบไล่ได้เป็นเนติบัณฑิตตามหลักสูตรของสำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสามปี

ง. สำเร็จการศึกษาตามข้อ 2 (2) ในระดับปริญญาเอก หรือมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงาน ตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสองปี

จ. เป็นบุคคลที่ทำงานเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ หรือมีประสบการณ์ในการดำเนินคดีเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ไม่น้อยกว่าสองปี

ข้อ (3) ในกรณีที่มีความจำเป็นเพื่อประโยชน์ของทางราชการในการสืบสวนและสอบสวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จำเป็นต้องมีบุคลากรซึ่งมีความรู้ ความชำนาญ หรือประสบการณ์สูง เพื่อดำเนินการสืบสวนและสอบสวนการกระทำผิดหรือคดีเช่นว่านั้น หรือเป็นบุคลากรในสาขาที่ขาดแคลน รัฐมนตรีอาจยกเว้นคุณสมบัติตามข้อ 2 ไม่ว่าทั้งหมด หรือบางส่วนสำหรับการบรรจุและแต่งตั้งบุคคลใดเป็นการเฉพาะก็ได้

ข้อ (4) การแต่งตั้งบุคคลหนึ่งบุคคลใดเป็นพนักงานเจ้าหน้าที่ ให้แต่งตั้งจากบุคคลซึ่งมีคุณสมบัติตามข้อ 2 หรือข้อ 3 โดยบุคคลดังกล่าวต้องผ่านการประเมินความรู้ความสามารถ หรือทดสอบตามหลักสูตรและหลักเกณฑ์ที่รัฐมนตรีประกาศกำหนด การแต่งตั้งบุคคลใดเป็นพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ดำรงตำแหน่ง

ข้อ (5) พนักงานเจ้าหน้าที่ต้องไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(1) เป็นบุคคลล้มละลาย บุคคลไร้ความสามารถ หรือบุคคลเสมือนไร้ความสามารถ

(2) เป็นสมาชิกสภาผู้แทนราษฎร สมาชิกวุฒิสภา ข้าราชการการเมือง สมาชิกสภาท้องถิ่น ผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งที่รับผิดชอบในการ

บริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่ในพรรคการเมือง

(3) เป็นผู้อยู่ระหว่างถูกสั่งให้พักราชการ หรือถูกสั่งให้ออกจากราชการไว้ก่อน

(4) ถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หน่วยงานของรัฐหรือรัฐวิสาหกิจ เพราะทำผิดวินัย หรือรัฐมนตรีให้ออกจากการเป็นพนักงานเจ้าหน้าที่ เพราะมีความประพฤติเสื่อมเสีย บกพร่อง หรือไม่สุจริตต่อหน้าที่ หรือหย่อนความสามารถ

(5) ได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่กระทำโดยประมาท หรือความผิดลหุโทษ

(6) ต้องคำพิพากษาหรือคำสั่งของศาลให้ทรัพย์สินตกเป็นของแผ่นดิน เพราะร่ำรวยผิดปกติหรือมีทรัพย์สินเพิ่มขึ้นผิดปกติ

ข้อ (6) พนักงานเจ้าหน้าที่พ้นจากตำแหน่งเมื่อ

(1) ตาย

(2) ลาออก

(3) ถูกจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก

(4) ขาดคุณสมบัติ หรือมีลักษณะต้องห้ามตามข้อ 5

(5) รัฐมนตรีให้ออก เพราะมีความประพฤติเสื่อมเสีย บกพร่อง หรือไม่สุจริตต่อหน้าที่ หรือหย่อนความสามารถ

(6) ครบวาระการดำรงตำแหน่ง [1]

7.1.2 สิ่งที่ต้องปฏิบัติตาม

พระราชบัญญัตินี้มีผลกับผู้ใช้คอมพิวเตอร์และอินเทอร์เน็ตทั่วไป เพราะหากกระทำความผิดจะด้วยตั้งใจหรือไม่ ก็อาจมีผลกระทบได้ในส่วนของผู้ให้บริการ ซึ่งรวมไปถึงหน่วยงานต่างๆ ที่เปิดบริการอินเทอร์เน็ตให้แก่ผู้อื่น หรือกลุ่มพนักงาน นักศึกษาในองค์กรก็ต้องมีภาระหน้าที่หลายอย่าง ในฐานะ “ผู้ให้บริการ”

ผู้ใช้คอมพิวเตอร์และอินเทอร์เน็ตควรจะทราบและระมัดระวังในสิ่งที่ผู้ใช้อินเทอร์เน็ตไม่ควรทำ 9 ประการ

1. อย่าบอก password ของท่านแก่ผู้อื่น
2. อย่าให้ผู้อื่นยืมใช้เครื่องคอมพิวเตอร์ หรือโทรศัพท์เคลื่อนที่เพื่อเข้าอินเทอร์เน็ต
3. อย่าติดตั้งระบบเครือข่ายไร้สายในบ้านหรือที่ทำงาน โดยไม่ใช้มาตรการการตรวจสอบ

ผู้ใช้งานและการเข้ารหัสลับ

4. อย่าเข้าสู่ระบบด้วย user ID และ password ที่ไม่ใช่ของตนเอง
5. อย่านำ user ID และ password ของผู้อื่นไปใช้งานหรือเผยแพร่
6. อย่าส่งต่อซึ่งภาพ ข้อความ หรือภาพเคลื่อนไหวที่ผิดกฎหมาย
7. อย่ากด “remember me” หรือ “remember password” ที่เครื่องคอมพิวเตอร์สาธารณะ และอย่า log-in เพื่อทำธุรกรรมทางการเงินที่เครื่องสาธารณะ ถ้าหากไม่มีความเชี่ยวชาญทาง computer security
8. อย่าใช้ WiFi (Wireless LAN) ที่เปิดให้ใช้ฟรี โดยปราศจากการเข้ารหัสลับข้อมูล
9. อย่าทำผิดตามมาตรา 14 ถึง มาตรา16 ไม่ว่าโดยบังเอิญ หรือโดยรู้เท่าไม่ถึงการณ์

7.1.3 ลักษณะการกระทำความผิด

มาตรการกระทำความผิดตามกฎหมาย	**บทลงโทษ**	**ประเภทภัยคุกคาม/ตัวอย่างการกระทำความผิด**
1. การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นที่มีมาตรการป้องกันโดยมิชอบ (มาตรา 5)	จำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 10,000 บาท หรือทั้งจำทั้งปรับ	Hack ระบบ
2. การล่วงรู้และเปิดเผยวิธีการเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันของผู้อื่นโดยมิชอบ (มาตรา 6)	จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท หรือทั้งจำทั้งปรับ	การบอกรหัสผ่าน หรือวิธีการเข้าสู่ระบบคอมพิวเตอร์ของผู้อื่นให้บุคคลที่สามทราบ
3. การเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นที่มีมาตรการป้องกันโดยมิชอบ (มาตรา 7)	จำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 40,000 บาท หรือทั้งจำทั้งปรับ	การปลดล็อกไฟล์ข้อมูลที่เข้ารหัสไว้
4. ดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 8)	จำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ	การ sniff

มาตรการกระทำความผิดตามกฎหมาย	บทลงโทษ	ประเภทภัยคุกคาม/ตัวอย่างการกระทำความผิด
5. รบกวนข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (ทำลาย แก้ไข เปลี่ยนแปลงข้อมูล (มาตรา 9)	จำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ	ซ่อนไฟล์ ลบข้อมูล แก้ไข นำข้อมูลของผู้อื่นไปเข้ารหัส
6. การรบกวน (ขัดขวาง ระงับ) การทำงานของระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา 10)	จำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ	การทำ Denial of Service
7. สแปมเมล (เป็นการส่งโดยปกปิดแหล่งที่มาของการส่งอีเมล) (มาตรา 11)	ปรับไม่เกิน 100,000 บาท	อีเมลเชิญชวนทำธุรกิจ ขายสินค้า
8.ทำการรบกวนข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของผู้อื่นและมีผลให้เกิดความเสียหายกับประชาชน หรือความมั่นคงของประเทศ (มาตรา 12)	จำคุกตั้งแต่ 3-15 ปี ปรับไม่เกิน 200,000 บาท หรือทั้งจำทั้งปรับ แต่ถ้าทำให้มีการเสียชีวิตต้องจำคุกตั้งแต่ 10-20 ปี	รบกวนระบบคอมพิวเตอร์ที่ควบคุมจราจร หรือการบิน
9. จำหน่าย หรือเผยแพร่ชุดคำสั่งที่ใช้ในการกระทำผิด (ตั้งแต่ข้อ 1-7)	จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท	แจกโปรแกรมที่ใช้ในการแฮคระบบ
10. ลงข้อมูลคอมพิวเตอร์ปลอมหรือเท็จ และทำให้ผู้อื่นหรือประชาชนเสียหาย (มาตรา 14(1))	จำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ	ลงข้อมูลขายสินค้าโดยไม่มีสินค้าจริง เพื่อให้ผู้ซื้อโอนเงินมาให้ เป็นต้น
11. ลงข้อมูลคอมพิวเตอร์เท็จที่น่าจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ หรือสร้างความตื่นตระหนก (มาตรา 14(2))	เหมือนข้อ 10	เขียนกระทู้ว่าจะมีแผ่นดินไหวหรือน้ำท่วมใหญ่ในกรุงเทพฯ
12. ลงข้อมูลคอมพิวเตอร์ที่ถือเป็นความผิดตามกฎหมายอาญา ใน	เหมือนข้อ 10	ส่งอีเมล หรือเขียนกระทู้ข่มขู่ที่จะวางระเบิดสถานที่ราชการ

มาตรการกระทำความผิดตามกฎหมาย	บทลงโทษ	ประเภทภัยคุกคาม/ตัวอย่างการกระทำความผิด
ส่วนความมั่นคงแห่งราชอาณาจักร หรือการก่อการร้าย (มาตรา 14(3))		
13. ลงข้อมูลคอมพิวเตอร์ที่ลามก (มาตรา 14(4))	เหมือนข้อ 10	ลงภาพ หรือวิดีโอลามกอนาจาร
14. การเผยแพร่ หรือส่งต่อข้อมูลตามข้อ 10 - 13 (มาตรา 14(5))	เหมือนข้อ 10	การส่งต่อข้อความ ข่าวลือ หรือภาพลามกไปทางอีเมล
15. ผู้ให้บริการให้การสนับสนุนหรือยินยอมให้มีการทำผิดตามข้อ 10 - 14 (มาตรา 15)	เหมือนข้อ 10	
16. การตัดต่อภาพของผู้อื่น ทำให้ผู้ถูกตัดต่อภาพเสียหาย (มาตรา 16)	จำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ	

ตารางที่ 7.1.3 แสดงลักษณะการกระทำความผิด มาตรการกระทำความผิดตามกฎหมาย

7.1.4 ลักษณะการกระทำความผิดในมุมมองด้านเทคนิค

ในลักษณะการกระทำความผิด จะสามารถแบ่งให้สอดคล้องกับหมวดหมู่ฐานความผิดได้เช่นกัน

1) การกระทำต่อระบบคอมพิวเตอร์

1.1) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 1

สปายแวร์ (Spyware), สนิฟเฟอร์ (Sniffer) มีผลกระทบต่อความมั่นคงปลอดภัยและความเสียหายคือ การสอดแนมข้อมูลส่วนตัว การแอบดักฟัง packet [35] ซึ่งจะเทียบได้กับฐานความผิดมาตรา 5 เข้าถึงระบบคอมพิวเตอร์, มาตรา 6 เปิดเผยมาตรการป้องกันระบบ, มาตรา 7 เข้าถึงข้อมูลคอมพิวเตอร์ และมาตรา 8 ดักรับข้อมูลคอมพิวเตอร์

1.2) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 2

การใช้ชุดคำสั่งในทางมิชอบ (Malicious Code) เช่น Viruses, Worms, Trojan Horses มีผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ การตั้งเวลาให้โปรแกรมทำลายข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์, การทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม หรือหยุดทำงาน (Denial of Service) ซึ่งจะเทียบได้กับฐานความผิด มาตรา 9 แก้ไข/เปลี่ยนแปลงข้อมูลคอมพิวเตอร์,

มาตรา 10 รบกวน/ขัดขวางระบบคอมพิวเตอร์

1.3) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 3

การทำสแปม (Spamming) ปกปิด/ปลอมแปลงแหล่งที่มา ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ รบกวนการใช้ระบบคอมพิวเตอร์ตามปกติ อาจถึงขั้นทำให้เป็น Zombie ซึ่งจะเทียบได้กับฐานความผิด มาตรา 11 สแปมเมล

1.4 กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 4

BOT หรือ Botnet ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ ผลกระทบต่อความมั่นคงปลอดภัยของประเทศ หรือทางเศรษฐกิจ, ความปลอดภัยสาธารณะ, การบริการสาธารณะ อาจเกิดสงครามข้อมูลข่าวสาร (Information Warfare) [35] ซึ่งจะเทียบได้กับฐานความผิด มาตรา 12 เหตุฉกรรจ์ อันเกิดจากการกระทำข้างต้น (1) แก่ประชาชน (2) ความมั่นคง

1.5 กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 5

Hacking Tools, Spam Tools ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ สอดแนมข้อมูลส่วนตัว, การแอบดักฟัง packet, การทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม หรือหยุดทำงาน (Denial of Service) อันเป็นผลจากการเผยแพร่เครื่องมือดังกล่าว ซึ่งจะเทียบได้กับฐานความผิด มาตรา 13 การจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์

2) การใช้คอมพิวเตอร์ในการกระทำความผิด

2.1 กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 6

การใช้ชุดคำสั่งในทางมิชอบ (Malicious Code) เช่น Viruses, Worms, Trojan Horses, Phishing, ยุยง, หลอกลวง, ภาพลามก ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ การตั้งเวลาให้โปรแกรมทำลายข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์, การทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม หรือหยุดทำงาน (Denial of Service) หรือทำให้เกิดความวุ่นวายต่อเศรษฐกิจ ความมั่นคงของประเทศ ซึ่งจะเทียบได้กับฐานความผิด มาตรา 14 การนำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ปลอม/ เท็จ /ภัยต่อความมั่นคง/ ลามก /หรือการส่งต่อข้อมูล (forward) นั้น

2.2 กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 7

การสนับสนุน ส่งเสริม การใช้ชุดคำสั่งในทางมิชอบ (Malicious Code) เช่น Viruses, Worms, Trojan Horses, Phishing, ยุยง, หลอกลวง, ภาพลามก ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ เกิดความเสียหายต่อผู้อื่น ซึ่งจะเทียบได้กับฐานความผิด มาตรา 15 ความรับผิดฐานสนับสนุนการกระทำความผิดของผู้ให้บริการ จงใจสนับสนุนและยินยอม

2.3 กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 8

การตัดต่อภาพ ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ ผู้ถูกกระทำถูกดูหมิ่น ถูกเกลียดชัง หรืออับอาย ซึ่งจะเทียบได้กับฐานความผิด มาตรา 16 การตัดต่อภาพ เป็นเหตุให้ถูกดูหมิ่น ถูกเกลียดชัง หรืออับอาย

7.1.4 ขั้นตอนการดำเนินคดีและการจับกุม

ระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิด ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ประกาศ ณ วันที่ 30 พฤศจิกายน พ.ศ. 2550

อาศัยอำนาจตามมาตรา 29 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นายกรัฐมนตรีและรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารออกระเบียบไว้ ดังต่อไปนี้

ข้อ (1) ระเบียบนี้เรียกว่า “ระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิด ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550”

ข้อ (2) ระเบียบนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ (3) ในระเบียบนี้

“พนักงานเจ้าหน้าที่” หมายความถึง ผู้ซึ่งรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

“พนักงานสอบสวน” หมายความถึง เจ้าพนักงานซึ่งกฎหมายให้มีอำนาจและหน้าที่ทำการสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา

“การปฏิบัติหน้าที่ร่วมกัน” หมายความว่า การที่พนักงานเจ้าหน้าที่และหรือพนักงานสอบสวนได้ให้ความเห็นหรือคำแนะนำ และหรือตรวจสอบพยานหลักฐานตั้งแต่ชั้นเริ่มการสอบสวนในคดี โดยให้เริ่มดำเนินการนับแต่โอกาสแรกเท่าที่จะพึงกระทำได้

“การสอบสวนร่วมกัน” หมายความว่า การสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ข้อ (4) ให้พนักงานเจ้าหน้าที่ หรือพนักงานสอบสวนเป็นผู้รับคำร้องทุกข์หรือคำกล่าวโทษในกรณีที่มีการกระทำความผิดเกิดขึ้น หรืออ้าง หรือเชื่อว่าได้เกิดขึ้นภายในเขตอำนาจของตน หรือผู้ต้องหามีที่อยู่ หรือถูกจับภายในเขตอำนาจของตน และเป็นความผิดที่บัญญัติไว้ในหมวด 1 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ข้อ (5) ในกรณีที่พนักงานสอบสวนได้รับคำร้องทุกข์ หรือคำกล่าวโทษตามข้อ 4 แล้วให้พนักงานสอบสวนประสานงานกับพนักงานเจ้าหน้าที่ เพื่อประโยชน์ในการแสวงหาพยานหลักฐานประกอบการกระทำความผิด

ข้อ (6) ในการจับ ควบคุม และค้น เมื่อพนักงานเจ้าหน้าที่ประสานมายังพนักงานสอบสวนผู้รับผิดชอบแล้ว ให้พนักงานสอบสวนผู้รับผิดชอบดำเนินการตามอำนาจหน้าที่ต่อไป

ข้อ (7) ให้พนักงานเจ้าหน้าที่ผู้รับผิดชอบดำเนินการแสวงหาพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดตามที่บัญญัติไว้ในหมวด 1 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยให้มีการปฏิบัติหน้าที่ร่วมกันและการสอบสวนร่วมกัน และมีหน้าที่ส่งมอบพยานหลักฐานที่รวบรวมได้ทั้งหมดให้กับพนักงานสอบสวนผู้รับผิดชอบจนกว่าการสอบสวนในคดีนั้นจะเสร็จสิ้น

ข้อ (8) เมื่อพนักงานสอบสวนผู้รับผิดชอบในการสอบสวน เห็นว่าการสอบสวนเสร็จสิ้นแล้ว ให้พนักงานสอบสวนเป็นผู้ทำความเห็นในรายงานความเห็นทางคดี ลงลายมือชื่อและส่งสำนวนการสอบสวนไปยังพนักงานอัยการในท้องที่ที่มีเขตอำนาจ เพื่อพิจารณาสั่งการต่อไป

ข้อ (9) บรรดาการใดที่พนักงานเจ้าหน้าที่และหรือพนักงานสอบสวนได้ดำเนินการไปแล้วตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ก่อนระเบียบนี้มีผลใช้บังคับให้ใช้ระเบียบนี้บังคับ [11]

3.1.10 เมื่อพบการกระทำความผิดสามารถร้องเรียนได้ที่

- สำนักงานคณะกรรมการคุ้มครองผู้บริโภค
- ศูนย์จัดการข้อร้องเรียนด้านพาณิชย์อิเล็กทรอนิกส์ กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์
- สำนักงานคณะกรรมการอาหารและยา กระทรวงสาธารณสุข
- มูลนิธิเพื่อผู้บริโภค

หากต้องการดำเนินคดีอาญา สามารถร้องเรียนได้ที่

- กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)
- สำนักคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ (ดีเอสไอ)
- สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

7.2 พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ.2544 และที่แก้ไขเพิ่มเติม

พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ภูมิพลอดุลยเดช ป.ภ.ร. ให้ไว้ ณ วันที่ 2 ธันวาคม พ.ศ. 2544 เป็นปีที่ 56 ในรัชกาลปัจจุบัน

มาตรา 1 พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544"

มาตรา 2 พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา 3 ในพระราชบัญญัตินี้ให้ใช้บังคับแก่ธุรกรรมในทางแพ่งและพาณิชย์ที่ดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์ เว้นแต่ธุรกรรมที่มีพระราชกฤษฎีกากำหนดมิให้นำพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับ

ความในวรรคหนึ่งไม่มีผลกระทบกระเทือนถึงกฎหมายหรือกฎใดที่กำหนดขึ้นเพื่อคุ้มครองผู้บริโภค พระราชบัญญัตินี้ให้ใช้บังคับแก่ธุรกรรมในการดำเนินงานของรัฐตามที่กำหนดใน หมวด 4 มาตรา 4 ในพระราชบัญญัตินี้

"ธุรกรรม" หมายความว่า การกระทำใด ๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ หรือในการดำเนินงานของรัฐตามที่กำหนด ใน หมวด 4

"อิเล็กทรอนิกส์" หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่านั้น

"ธุรกรรมทางอิเล็กทรอนิกส์" หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมด หรือแต่บางส่วน

"ข้อความ" หมายความว่า เรื่องราว หรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ

"ข้อมูลอิเล็กทรอนิกส์" หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

"ลายมือชื่ออิเล็กทรอนิกส์" หมายความว่า อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์

"ระบบข้อมูล" หมายความว่า กระบวนการประมวลผลด้วยเครื่องมืออิเล็กทรอนิกส์ สำหรับสร้าง ส่ง รับ เก็บรักษา หรือประมวล ผลข้อมูลอิเล็กทรอนิกส์

"การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์" หมายความว่า การส่งหรือรับข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่อง คอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า

"ผู้ส่งข้อมูล" หมายความว่า บุคคลซึ่งเป็นผู้ส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ก่อนจะมีการเก็บรักษาข้อมูลเพื่อส่งไปตามวิธีการ ที่ผู้นั้นกำหนด โดยบุคคลนั้นอาจจะส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง หรือมีการส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนบุคคลนั้นก็ได้ ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

"ผู้รับข้อมูล" หมายความว่า บุคคลซึ่งผู้ส่งข้อมูลประสงค์จะส่งข้อมูลอิเล็กทรอนิกส์ให้ และได้รับข้อมูลอิเล็กทรอนิกส์นั้น ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

"บุคคลที่เป็นสื่อกลาง" หมายความว่า บุคคลซึ่งกระทำการในนามผู้อื่นในการส่ง รับ หรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์อันใด อันหนึ่งโดยเฉพาะ รวมถึงให้บริการอื่นที่เกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้น

"ใบรับรอง" หมายความว่า ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใด ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูล สำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์

"เจ้าของลายมือชื่อ" หมายความว่า ผู้ซึ่งถือข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ และสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ในนามตนเองหรือแทนบุคคลอื่น

"คู่กรณีที่เกี่ยวข้อง" หมายความว่า ผู้ซึ่งอาจกระทำการใด ๆ โดยขึ้นอยู่กับใบรับรองหรือ ลายมือชื่ออิเล็กทรอนิกส์

"หน่วยงานของรัฐ" หมายความว่า กระทรวง ทบวง กรม ส่วนราชการที่เรียกชื่ออย่างอื่น และมีฐานะเป็นกรมราชการส่วนภูมิ ภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจที่ตั้งขึ้นโดยพระราชบัญญัติหรือพระราชกฤษฎีกา และให้หมายความรวมถึงนิติบุคคล คณะบุคคล หรือบุคคล ซึ่งมีอำนาจ หน้าที่ดำเนินงานของรัฐไม่ว่าในกรณีใด ๆ

"คณะกรรมการ" หมายความว่า คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา 5 บทบัญญัติ **มาตรา 13** ถึง **มาตรา 24** และบทบัญญัติ **มาตรา 26** ถึง **มาตรา 31** จะตกลงกันเป็นอย่างอื่นก็ได้

มาตรา 6 ให้นายกรัฐมนตรีรักษาการตามพระราชบัญญัตินี้

1 ธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 7 ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใด เพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูป ของข้อมูลอิเล็กทรอนิกส์

มาตรา 8 ภายใต้บังคับบทบัญญัติแห่ง **มาตรา 9** ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือ มีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อ ความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว

มาตรา 9 ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

(1) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ

(2) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้าง หรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

มาตรา 10 ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสาร ต้นฉบับตามกฎหมายแล้ว

(1) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้อง ของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และ

(2) สามารถแสดงข้อความนั้นในภายหลังได้

ความถูกต้องของข้อความตาม (1) ให้พิจารณาถึงความครบถ้วนและไม่มีการเปลี่ยนแปลงใดของข้อความ เว้นแต่การรับรอง หรือบันทึกเพิ่มเติม หรือการเปลี่ยนแปลงใด ๆ ที่อาจจะเกิดขึ้นได้ตามปกติในการติดต่อสื่อสาร การเก็บรักษา หรือการแสดงข้อความซึ่งไม่มีผลต่อความถูกต้องของข้อความนั้น

ในการวินิจฉัยความน่าเชื่อถือของวิธีการรักษาความถูกต้องของข้อความตาม (1) ให้พิเคราะห์ถึงพฤติการณ์ที่เกี่ยวข้องทั้งปวง รวมทั้งวัตถุประสงค์ของการสร้างข้อความนั้น

มาตรา 11 ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน ในกระบวนการพิจารณาตามกฎหมายเพียงเพราะ เหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือ วิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะ หรือวิธีการรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะหรือวิธีการ ที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง

มาตรา 12 ภายใต้บังคับบทบัญญัติ มาตรา 10 ในกรณีที่กฎหมายกำหนดให้เก็บรักษาเอกสารหรือข้อความใด ถ้าได้เก็บรักษา ในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการเก็บรักษาเอกสารหรือข้อความตามที่กฎหมายต้องการแล้ว

(1) ข้อมูลอิเล็กทรอนิกส์นั้นสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง

(2) ได้เก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นให้อยู่ในรูปแบบที่เป็นอยู่ในขณะที่สร้าง ส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์นั้น หรือ อยู่ในรูปแบบที่สามารถแสดงข้อความที่สร้าง ส่ง หรือได้รับให้ปรากฏอย่างถูกต้องได้ และ

(3) ได้เก็บรักษาข้อความส่วนที่ระบุถึงแหล่งกำเนิด ต้นทาง และปลายทางของข้อมูลอิเล็กทรอนิกส์ ตลอดจนวันและเวลาที่ส่งหรือ ได้รับข้อความดังกล่าว ถ้ามี

ความในวรรคหนึ่ง มิให้ใช้บังคับกับข้อความที่ใช้เพียงเพื่อวัตถุประสงค์ในการส่งหรือรับข้อมูลอิเล็กทรอนิกส์

หน่วยงานของรัฐที่รับผิดชอบในการเก็บรักษาเอกสารหรือข้อความใด อาจกำหนดหลักเกณฑ์ รายละเอียดเพิ่มเติมเกี่ยวกับการ เก็บรักษาเอกสารหรือข้อความนั้นได้ เท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติในมาตรานี้

มาตรา 13 คำเสนอหรือคำสนองในการทำสัญญา อาจทำเป็นข้อมูลอิเล็กทรอนิกส์ก็ได้ และห้ามมิให้ปฏิเสธการมีผลทางกฎหมายของสัญญาเพียงเพราะเหตุที่สัญญานั้นได้ทำคำเสนอหรือคำสนองเป็นข้อมูลอิเล็กทรอนิกส์

มาตรา 14 ในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล การแสดงเจตนาหรือคำบอกกล่าวอาจทำเป็นข้อมูลอิเล็กทรอนิกส์

มาตรา 15 บุคคลใดเป็นผู้ส่งข้อมูลไม่ว่าจะเป็นการส่งโดยวิธีใด ให้ถือว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้นั้นในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล ให้ถือว่าเป็นข้อมูลอิเล็กทรอนิกส์ของผู้ส่งข้อมูล หากข้อมูลอิเล็กทรอนิกส์นั้นได้ส่งโดย

(1) บุคคลผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูลเกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้น หรือ

(2) ระบบข้อมูลที่ผู้ส่งข้อมูลหรือบุคคลผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูลได้กำหนด ไว้ล่วงหน้าให้สามารถทำงานได้โดยอัตโนมัติ

มาตรา 16 ผู้รับข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูลและชอบที่จะดำเนินการไป ตามข้อมูลอิเล็กทรอนิกส์นั้นได้ ถ้า

(1) ผู้รับข้อมูลได้ตรวจสอบโดยสมควรตามวิธีการที่ได้ตกลงกับผู้ส่งข้อมูล ว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูล หรือ

(2) ข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นเกิดจากการกระทำของบุคคลซึ่ง ใช้วิธีการที่ผู้ส่งข้อมูลใช้ในการแสดงว่าข้อมูล อิเล็กทรอนิกส์นั้นเป็นของผู้ส่งข้อมูล ซึ่งบุคคลนั้นได้ล่วงรู้โดยอาศัยความสัมพันธ์ระหว่างบุคคลนั้นกับผู้ส่งข้อมูล หรือผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูล ความในวรรคหนึ่งมิให้ใช้บังคับ ถ้า

(1) ในขณะนั้นผู้รับข้อมูลได้รับแจ้งจากผู้ส่งข้อมูลว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นมิใช่ของผู้ส่งข้อมูล และในขณะเดียวกันผู้รับข้อมูลมีเวลาพอสมควรที่จะตรวจสอบข้อเท็จจริงตามที่ได้รับแจ้งนั้น หรือ

(2) กรณีตามวรรคหนึ่ง (2) เมื่อผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์นั้นไม่ใช่ของผู้ส่งข้อมูล หากผู้รับข้อมูล ได้ใช้ความระมัดระวังตามสมควร หรือดำเนินการตามวิธีการที่ได้ตกลงกันไว้ก่อนแล้ว

มาตรา 17 ในกรณีตาม มาตรา 15 หรือ มาตรา 16 วรรคหนึ่ง ในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล ผู้รับข้อมูล ผู้รับข้อมูลมีสิทธิถือว่าข้อมูลอิเล็กทรอนิกส์ที่รับนั้นถูกต้องตามเจตนาของผู้ส่งข้อมูล และสามารถดำเนินการไปตามข้อมูลอิเล็กทรอนิกส์นั้นได้ เว้นแต่ผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับนั้นมีข้อผิดพลาดอันเกิดจากการส่ง หากผู้รับข้อมูลได้ใช้ความระมัดระวังตามสมควรหรือดำเนินการ ตามวิธีการที่ได้ตกลงกันไว้ก่อนแล้ว

มาตรา 18 ผู้รับข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับแต่ละชุดเป็นข้อมูลที่แยกจากกันและสามารถดำเนินการไป ตามข้อมูลอิเล็กทรอนิกส์แต่ละชุดนั้นได้ เว้นแต่ข้อมูลอิเล็กทรอนิกส์ชุดนั้นจะซ้ำกับข้อมูลอิเล็กทรอนิกส์อีกชุดหนึ่ง และผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอ นิกส์นั้นเป็นข้อมูลอิเล็กทรอนิกส์ซ้ำ หากผู้รับข้อมูลได้ใช้ความระมัดระวังตามสมควรหรือดำเนินการตามวิธีการที่ได้ตกลงกันไว้ก่อนแล้ว

มาตรา 19 ในกรณีที่ต้องมีการตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์ ไม่ว่าผู้ส่งข้อมูลได้ร้องขอ หรือตกลงกับผู้รับข้อมูล ไว้ก่อนหรือขณะที่ส่งข้อมูลอิเล็กทรอนิกส์ หรือปรากฏในข้อมูลอิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) ในกรณีที่ผู้ส่งข้อมูลมิได้ตกลงให้ตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์ในรูปแบบหรือวิธีการใดโดยเฉพาะ การตอบ แจ้งการรับอาจทำได้ด้วยการติดต่อสื่อสารจากผู้รับข้อมูล ไม่ว่าโดยระบบข้อมูลที่ทำงานโดยอัตโนมัติหรือโดยวิธีอื่นใด หรือด้วยการกระทำใดๆ ของผู้รับข้อมูลซึ่งเพียงพอจะแสดงต่อผู้ส่งข้อมูลว่าผู้รับข้อมูลได้รับข้อมูลอิเล็กทรอนิกส์นั้นแล้ว

(2) ในกรณีที่ผู้ส่งข้อมูลกำหนดเงื่อนไขว่าจะถือว่ามีการส่งข้อมูลอิเล็กทรอนิกส์ต่อเมื่อ ได้รับการตอบแจ้งการรับจากผู้รับข้อมูล ให้ถือว่ายังไม่มีการส่งข้อมูลอิเล็กทรอนิกส์จนกว่าผู้ส่งข้อมูลจะได้รับการตอบแจ้งการรับแล้ว

(3) ในกรณีที่ผู้ส่งข้อมูลมิได้กำหนดเงื่อนไขตามความใน (2) และผู้ส่งข้อมูลมิได้รับการตอบแจ้งการรับนั้นภายในเวลาที่กำหนด หรือตกลงกัน หรือภายในระยะเวลาอันสมควรในกรณีที่มิได้กำหนดหรือตกลงเวลาไว้

(4) ผู้ส่งข้อมูลอาจส่งคำบอกกล่าวไปยังผู้รับข้อมูลว่าตนยังมิได้รับการตอบแจ้งการรับ และกำหนดระยะเวลาอันสมควรให้ผู้รับ ข้อมูลตอบแจ้งการรับ และ

(5) หากผู้ส่งข้อมูลมิได้รับการตอบแจ้งการรับภายในระยะเวลาตาม (ก) เมื่อผู้ส่งข้อมูลบอกกล่าวแก่ผู้รับข้อมูลแล้ว ผู้ส่งข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมิได้มีการส่งเลย หรือผู้ส่งข้อมูลอาจใช้สิทธิอื่นใดที่ผู้ส่งข้อมูลมีอยู่ได้

มาตรา 20 ในกรณีที่ผู้ส่งข้อมูลได้รับการตอบแจ้งการรับจากผู้รับข้อมูล ให้สันนิษฐานว่า ผู้รับข้อมูลได้รับข้อมูลอิเล็กทรอนิกส์ ที่เกี่ยวข้องแล้ว แต่ข้อสันนิษฐานดังกล่าวมิได้ถือว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นถูกต้องตรงกันกับข้อมูลอิเล็กทรอนิกส์ผู้ส่งข้อมูลได้ส่งมา

มาตรา 21 ในกรณีที่ปรากฏในการตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์นั้นเองว่า ข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับเป็นไปตามข้อกำหนดทางเทคนิคที่ผู้ส่งข้อมูลและผู้รับข้อมูลได้ตกลง หรือระบุไว้ในมาตรฐานซึ่ง ใช้บังคับอยู่ ให้สันนิษฐานว่าข้อมูลอิเล็กทรอนิกส์ที่ส่งไปนั้น ได้เป็นไปตามข้อกำหนดทางเทคนิคทั้งหมดแล้ว

มาตรา 22 การส่งข้อมูลอิเล็กทรอนิกส์ให้ถือว่าได้มีการส่งเมื่อข้อมูลอิเล็กทรอนิกส์นั้น ได้เข้าสู่ระบบข้อมูลที่อยู่นอกเหนือการควบคุมของผู้ส่งข้อมูล

มาตรา 23 การรับข้อมูลอิเล็กทรอนิกส์ให้ถือว่ามีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลของผู้รับข้อมูล หากผู้รับข้อมูลได้กำหนดระบบข้อมูลที่ประสงค์จะใช้ในการรับข้อมูลอิเล็กทรอนิกส์ไว้โดยเฉพาะ ให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลที่ผู้รับข้อมูลได้กำหนดไว้นั้น แต่ถ้าข้อมูลอิเล็กทรอนิกส์ดังกล่าวได้ส่งไปยังระบบข้อมูลอื่นของผู้รับข้อมูล ซึ่งมิใช่ระบบข้อมูลที่ผู้รับข้อมูลกำหนดไว้ ให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ได้เรียกข้อมูลอิเล็กทรอนิกส์จากระบบข้อมูลนั้น ความในมาตรานี้ให้ใช้บังคับแม้ระบบข้อมูลของผู้รับข้อมูลตั้งอยู่ในสถานที่อีกแห่งหนึ่งต่างหากจากสถานที่ที่ถือว่าผู้รับข้อมูล ได้รับข้อมูลอิเล็กทรอนิกส์ตาม มาตรา 24

มาตรา 24 การส่งหรือการรับข้อมูลอิเล็กทรอนิกส์ ให้ถือว่าได้ส่ง ณ ที่ทำการงานของผู้ส่งข้อมูล หรือได้รับ ณ ที่ทำการงาน ของผู้รับข้อมูล แล้วแต่กรณี

ในกรณีที่ผู้ส่งข้อมูลหรือผู้รับข้อมูลมีที่ทำการงานหลายแห่ง ให้ถือเอาที่ทำการงานที่เกี่ยวข้องมากที่สุดกับธุรกรรมนั้นเป็นที่ทำการงาน เพื่อประโยชน์ตามวรรคหนึ่ง แต่ถ้าไม่สามารถกำหนดได้ว่าธุรกรรมนั้นเกี่ยวข้องกับที่ทำการงานแห่งใดมากที่สุด ให้ถือเอาสำนักงานใหญ่เป็นสถานที่ที่ได้รับหรือส่ง ข้อมูลอิเล็กทรอนิกส์นั้น

ในกรณีที่ไม่ปรากฏที่ทำการงานของผู้ส่งข้อมูลหรือผู้รับข้อมูล ให้ถือเอาถิ่นที่อยู่ปกติเป็นสถานที่ที่ส่งหรือได้รับข้อมูลอิเล็กทรอนิกส์

ความในมาตรานี้มิให้ใช้บังคับกับการส่ง และการรับข้อมูลอิเล็กทรอนิกส์โดยวิธีการทางโทรเลข และโทรพิมพ์ หรือวิธีการสื่อสาร อื่นตามที่กำหนดในพระราชกฤษฎีกา

มาตรา 25 ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกา ให้สันนิษฐานว่าเป็น วิธีการที่เชื่อถือได้

:: หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์

มาตรา 26 ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

(1) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อ โดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

(2) ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของลายมือชื่อ โดยไม่มีการควบคุมของบุคคลอื่น

(3) การเปลี่ยนแปลงใด ๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้ และ

(4) ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่ออิเล็กทรอนิกส์เป็นไปเพื่อรับรองความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลายมือชื่ออิเล็กทรอนิกส์

บทบัญญัติในวรรคหนึ่ง ไม่เป็นการจำกัดว่าไม่มีวิธีการอื่นใดที่แสดงได้ว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ หรือการแสดงพยานหลักฐานใดเกี่ยวกับความไม่น่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์

มาตรา 27 ในกรณีมีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ เพื่อสร้างลายมือชื่ออิเล็กทรอนิกส์ที่จะมีผลตาม กฎหมายเจ้าของลายมือชื่อต้องดำเนินการดังต่อไปนี้

(1) ใช้ความระมัดระวังตามสมควรเพื่อมิให้มีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ โดยไม่ได้รับอนุญาต

(2) แจ้งให้บุคคลที่คาดหมายได้โดยมีเหตุอันควรเชื่อว่าจะกระทำการใดโดยขึ้นอยู่กับลายมือชื่ออิเล็กทรอนิกส์ หรือให้บริการเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ ทราบโดยมิชักช้า เมื่อ

(3) เจ้าของลายมือชื่อรู้หรือควรได้รู้ว่าข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้น สูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผย โดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(4) เจ้าของลายมือชื่อรู้จากสภาพการณ์ที่ปรากฏว่ากรณีมีความเสี่ยงมากพอที่ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ สูญ หาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(5) ในกรณีมีการออกใบรับรองสนับสนุนการใช้ลายมือชื่ออิเล็กทรอนิกส์ จะต้องใช้ความระมัดระวังตามสมควรให้แน่ใจในความถูกต้อง และสมบูรณ์ของการแสดงสาระสำคัญทั้งหมด ซึ่งกระทำโดยเจ้าของลายมือชื่อ เกี่ยวกับใบรับรองนั้นตลอดอายุใบรับรอง หรือตามที่มีการกำหนดในใบรับรอง

มาตรา 28 ในกรณีมีการให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ ให้มีผลทางกฎหมายเสมือนหนึ่ง ลงลายมือชื่อ ผู้ให้บริการออกใบรับรองต้องดำเนินการ ดังต่อไปนี้

(1) ปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ตนได้แสดงไว้

(2) ใช้ความระมัดระวังตามสมควรให้แน่ใจในความถูกต้อง และความสมบูรณ์ของการแสดงสาระสำคัญทั้งหมดที่ตนได้กระทำเกี่ยวกับใบรับรองนั้นตลอดอายุใบรับรอง หรือตามที่มีการกำหนดในใบรับรอง

(3) จัดให้มีวิธีการในการเข้าถึงโดยสมควร ให้คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบข้อเท็จจริงในการแสดงสาระสำคัญทั้งหมดจาก ใบรับรองได้ ในเรื่องดังต่อไปนี้

(1) การระบุผู้ให้บริการออกใบรับรอง

(2) เจ้าของลายมือชื่อซึ่งระบุในใบรับรองได้ควบคุมข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ในขณะมีการออกใบรับรอง

(3) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์มีผลใช้ได้ในขณะหรือก่อนที่มีการออกใบรับรอง

(4) จัดให้มีวิธีการเข้าถึงโดยสมควร ให้คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบกรณีดังต่อไปนี้จากใบรับรองหรือจากวิธีอื่น

(1) วิธีการที่ใช้ในการระบุตัวเจ้าของลายมือชื่อ

(2) ข้อจำกัดเกี่ยวกับวัตถุประสงค์และคุณค่าที่มีการนำข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์หรือใบรับรอง

(3) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์มีผลสมบูรณ์ใช้ได้ และไม่สูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผย โดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(4) ข้อจำกัดเกี่ยวกับขอบเขตความรับผิดที่ผู้ให้บริการออกใบรับรองได้ระบุไว้

(5) การมีวิธีการให้เจ้าของลายมือชื่อส่งคำบอกกล่าวเมื่อมีเหตุตาม มาตรา 27 (2)

(6) การมีบริการเกี่ยวกับการเพิกถอนใบรับรองที่ทันการ

(5) ในกรณีที่มีบริการตาม (4) (จ) บริการนั้นต้องมีวิธีการที่ให้เจ้าของลายมือชื่อสามารถแจ้งได้ตามหลักเกณฑ์ที่กำหนด ตาม มาตรา 27 (2) และในกรณีที่มีบริการตาม (4) (ฉ) บริการนั้นต้องสามารถเพิกถอนใบรับรองได้ทันการ

(6) ให้ระบบ วิธีการ และบุคลากรที่เชื่อถือได้ในการให้บริการ

มาตรา 29 ในการพิจารณาความเชื่อถือได้ของระบบ วิธีการ และบุคลากรตาม มาตรา 28 (6) ให้คำนึงถึงกรณีดังต่อไปนี้

(1) สถานภาพทางการเงิน บุคลากร และสินทรัพย์ที่มีอยู่

(2) คุณภาพของระบบฮาร์ดแวร์และซอฟต์แวร์

(3) วิธีการออกใบรับรอง การขอใบรับรอง และการเก็บรักษาข้อมูลการให้บริการนั้น

(4) การจัดให้มีข้อมูลข่าวสารเกี่ยวกับเจ้าของลายมือชื่อ ที่ระบุในใบรับรองและผู้ที่อาจคาดหมายได้ว่าจะเป็นคู่กรณีที่เกี่ยวข้อง

(5) ความสม่ำเสมอและขอบเขตในการตรวจสอบโดยผู้ตรวจสอบอิสระ

(6) องค์กรที่ให้การรับรองหรือให้บริการออกใบรับรองเกี่ยวกับการปฏิบัติหรือการมีอยู่ของสิ่งที่กล่าวมาใน (1) ถึง (5)

(7) กรณีใด ๆ ที่คณะกรรมการประกาศกำหนด

มาตรา 30 คู่กรณีที่เกี่ยวข้องต้องดำเนินการ ดังต่อไปนี้

(1) ดำเนินการตามสมควรในการตรวจสอบความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์

(2) ในกรณีลายมือชื่ออิเล็กทรอนิกส์มีใบรับรอง ต้องมีการดำเนินการตามสมควร ดังนี้

(3) ตรวจสอบความสมบูรณ์ของใบรับรอง การพักใช้ หรือการเพิกถอนใบรับรอง และ

(4) ปฏิบัติตามข้อจำกัดใด ๆ ที่เกี่ยวกับใบรับรอง

มาตรา 31 ใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ให้ถือว่ามีผลทางกฎหมายโดยไม่ต้องคำนึงถึง

(1) สถานที่ออกใบรับรองหรือสถานที่สร้าง หรือใช้ลายมือชื่ออิเล็กทรอนิกส์ หรือ

(2) สถานที่ทำการงานของผู้ออกใบรับรอง หรือเจ้าของลายมือชื่ออิเล็กทรอนิกส์

ใบรับรองที่ออกในต่างประเทศให้มีผลตามกฎหมายในประเทศ เช่นเดียวกับใบรับรองที่ออกในประเทศ หากการออกใบรับรองดังกล่าวได้ใช้ระบบที่เชื่อถือได้ไม่น้อยกว่าระบบที่เชื่อถือได้ตามพระราชบัญญัตินี้ ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างหรือใช้ในต่างประเทศให้ถือว่ามีผลตามกฎหมายในประเทศ เช่นเดียวกับลายมือชื่ออิเล็กทรอนิกส์ที่ สร้างหรือใช้ในประเทศ หากการสร้างหรือใช้ลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวได้ใช้ระบบที่เชื่อถือได้ไม่น้อยกว่าระบบที่เชื่อถือได้ตามพระราชบัญญัตินี้

ในการพิจารณาว่าใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ใดมีความเชื่อถือได้ตามวรรคสอง หรือวรรคสาม ให้คำนึงถึงมาตร ฐานระหว่างประเทศและปัจจัยอื่น ๆ ที่เกี่ยวข้องประกอบด้วย

:: หมวด 3 ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 32 บุคคลย่อมมีสิทธิประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ แต่ในกรณีที่จำเป็นเพื่อรักษาความมั่น คงทางการเงินและการพาณิชย์ หรือเพื่อประโยชน์ในการเสริมสร้างความเชื่อถือและยอมรับในระบบลายมือชื่ออิเล็กทรอนิกส์ หรือเพื่อป้องกันความเสียหายต่อสาธารณชนให้มีการตราพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทาง อิเล็กทรอนิกส์ใดเป็นกิจการที่ต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาตก่อนก็ได้

ในการกำหนดให้กรณีใดต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาตตามวรรคหนึ่ง ให้กำหนดโดยพิจารณาจากความเหมาะสมในการป้องกันความเสียหายตามระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นจากการ ประกอบธุรกิจนั้น

ในการนี้ จะกำหนดให้หน่วยงานของรัฐแห่งหนึ่งแห่งใดเป็นผู้รับผิดชอบในการควบคุมดูแลในพระราชกฤษฎีกาดังกล่าวก็ได้

ก่อนเสนอให้ตราพระราชกฤษฎีกาตามวรรคหนึ่ง ต้องจัดให้มีการรับฟังความคิดเห็นของประชาชนตามความเหมาะสม และนำ ข้อมูลที่ได้รับมาประกอบการพิจารณา

มาตรา 33 ในกรณีที่มีพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ใดเป็นกิจการ ที่ต้องแจ้งให้ทราบ หรือต้องขึ้นทะเบียน ให้ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวต้องแจ้ง หรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาก่อนเริ่ม เพื่อเป็นหลักฐานการแจ้งหรือการขึ้นทะเบียนในวันที่ได้รับแจ้งหรือรับขึ้นทะเบียน และให้ผู้แจ้งหรือผู้ขึ้นทะเบียนประกอบธุรกิจนั้น ได้ตั้ง แต่วันที่ได้รับแจ้งหรือรับขึ้นทะเบียน แต่ถ้าพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาตรวจพบในภายหลังว่า การแจ้งหรือขึ้นทะเบียนไม่ถูกต้อง หรือไม่ครบถ้วน ให้มีอำนาจสั่งผู้แจ้ง หรือผู้ขึ้นทะเบียนแก้ไขให้ถูกต้องหรือครบถ้วนภายในเจ็ดวันนับแต่วันที่ได้รับคำสั่งดังกล่าว

ในการประกอบธุรกิจ ผู้แจ้งหรือผู้ขึ้นทะเบียนตามวรรคหนึ่งต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกาและตาม ที่คณะกรรมการประกาศกำหนด

ถ้าผู้แจ้งหรือผู้ขึ้นทะเบียนตามวรรคหนึ่งไม่แก้ไขการแจ้งหรือขึ้นทะเบียนให้ถูกต้อง หรือครบถ้วนตามวรรคสอง หรือฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์การประกอบธุรกิจตามวรรคสาม ให้คณะกรรมการพิจารณามีคำสั่งลงโทษปรับทางปกครอง ไม่เกินหนึ่งล้านบาท โดยคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด และในกรณีที่เห็นสมควรคณะกรรมการอาจมีคำสั่งให้ผู้นั้นดำเนินการใด ๆ เพื่อแก้ไข ให้ถูกต้องหรือเหมาะสมได้

หลักเกณฑ์ในการพิจารณาลงโทษปรับทางปกครองให้เป็นไปตามที่คณะกรรมการกำหนดและ ถ้าผู้ถูกลงโทษปรับทางปกครอง ไม่ยอมชำระค่าปรับทางปกครอง ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม และในกรณี ไม่มีเจ้าหน้าที่ดำเนินการบังคับตามคำสั่ง ให้คณะกรรมการมีอำนาจฟ้องคดีต่อศาลปกครองเพื่อบังคับชำระค่าปรับ ในการนี้ถ้าศาลปกครองเห็นว่าคำสั่งให้ชำระค่าปรับนั้นชอบด้วยกฎหมายก็ให้ศาลปกครองมีอำนาจพิจารณาพิพากษาและบังคับให้มีการยึด หรืออายัดทรัพย์สินขายทอดตลาดเพื่อชำระค่าปรับได้

ในกรณีผู้กระทำผิดตามวรรคสี่ไม่ดำเนินการแก้ไขตามคำสั่งของคณะกรรมการหรือกระทำความผิดซ้ำอีก ให้คณะกรรมการมีอำนาจออกคำสั่งห้ามมิให้ผู้นั้นประกอบธุรกิจตามที่ได้แจ้งหรือขึ้นทะเบียนอีกต่อไป

มาตรา 34 ในกรณีที่มีพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์กรณีใดเป็น กิจการที่ต้องได้รับใบอนุญาต ให้ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวยื่นคำขอรับใบอนุญาตต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกา

คุณสมบัติของผู้ขอรับใบอนุญาต หลักเกณฑ์และวิธีการขออนุญาต การออกใบอนุญาต การต่ออายุใบอนุญาต การคืนใบ อนุญาต และการสั่งพักใช้หรือเพิกถอนใบอนุญาต ให้เป็นไปตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกา

ในการประกอบธุรกิจ ผู้ได้รับใบอนุญาตตามวรรคหนึ่ง ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกา ประกาศที่ คณะกรรมการกำหนดหรือเงื่อนไขในใบอนุญาต

ในกรณีที่ผู้ได้รับใบอนุญาตฝ่าฝืนหรือปฏิบัติไม่ถูกต้องตามหลักเกณฑ์การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ตามวรรคสาม ให้คณะกรรมการพิจารณาคำสั่งลงโทษปรับทางปกครองไม่เกินสองล้านบาท โดยคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด และในกรณีที่เห็นสมควรคณะกรรมการอาจมีคำสั่งให้ผู้นั้นดำเนินการใด ๆ เพื่อแก้ไขให้ถูกต้องหรือเหมาะสมได้ ทั้งนี้ ให้นำความใน มาตรา 33 วรรคห้า มาใช้บังคับโดยอนุโลม

ถ้าผู้กระทำความผิดตามวรรคสี่ไม่ดำเนินการแก้ไขตามคำสั่งของคณะกรรมการหรือกระทำความผิดซ้ำอีก ให้คณะกรรมการ มีอำนาจออกคำสั่งเพิกถอนใบอนุญาต

:: หมวด 4 ธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 35 คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใด ๆ ตาม กฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับ และให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่ กฎหมายในเรื่องนั้นกำหนด ทั้งนี้ ในพระราชกฤษฎีกาอาจกำหนดให้บุคคลที่เกี่ยวข้องต้องกระทำหรืองดเว้นกระทำการใด ๆ หรือให้หน่วยงานของรัฐออกระเบียบเพื่อ กำหนดรายละเอียดในบางกรณีด้วยก็ได้

ในการออกพระราชกฤษฎีกาตามวรรคหนึ่ง พระราชกฤษฎีกาดังกล่าวอาจกำหนดให้ผู้ประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทาง อิเล็กทรอนิกส์ต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาต แล้วแต่กรณี ก่อนประกอบกิจการก็ได้ ในกรณีนี้ ให้นำบทบัญญัติใน หมวด 3 และบทกำหนดโทษที่เกี่ยวข้อง มาใช้บังคับโดยอนุโลม

:: หมวด 5 คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 36 ให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วยรัฐมนตรีว่าการกระทรวงวิทยาศาสตร์ เทคโนโลยีและ สิ่งแวดล้อมเป็นประธานกรรมการ และกรรมการซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้ทรงคุณวุฒิ ที่ได้รับการสรรหาอีกจำนวนสิบสองคน โดยในจำนวนนี้เป็นผู้ทรงคุณวุฒิ ในด้านดังต่อไปนี้ด้านละสองคน

(1) การเงิน

(2) การพาณิชย์อิเล็กทรอนิกส์

(3) นิติศาสตร์

(4) วิทยาการคอมพิวเตอร์

(5) วิทยาศาสตร์หรือวิศวกรรมศาสตร์

(6) สังคมศาสตร์

ทั้งนี้ ผู้ทรงคุณวุฒิคนหนึ่งของแต่ละด้านต้องมาจากภาคเอกชน และให้ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และ คอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติเป็นกรรมการและเลขานุการ

หลักเกณฑ์และวิธีการสรรหาและการเสนอชื่อบุคคลที่เห็นสมควรต่อคณะรัฐมนตรีเพื่อพิจารณาแต่งตั้งเป็นคณะกรรมการ ตามวรรคหนึ่ง ให้เป็นไปตามระเบียบที่รัฐมนตรีประกาศกำหนด ให้เลขานุการแต่งตั้งผู้ช่วยเลขานุการอีกไม่เกินสองคน

มาตรา 37 ให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ มีอำนาจหน้าที่ดังต่อไปนี้

(1) เสนอแนะต่อคณะรัฐมนตรีเพื่อวางนโยบายการส่งเสริมและพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ตลอดจนการแก้ไขปัญหา และอุปสรรคที่เกี่ยวข้อง

(2) ติดตามดูแลการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

(3) เสนอแนะหรือให้คำปรึกษาต่อรัฐมนตรีเพื่อการตราพระราชกฤษฎีกาตามพระราชบัญญัตินี้

(4) ออกระเบียบหรือประกาศเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ เพื่อให้เป็นไปตามพระราชบัญญัตินี้ หรือตามพระราช กฤษฎีกาที่ออกตามพระราชบัญญัตินี้

(5) ปฏิบัติการอื่นใดเพื่อให้เป็นไปตามพระราชบัญญัตินี้ หรือกฎหมายอื่น ในการปฏิบัติตามพระราชบัญญัตินี้ให้คณะกรรมการเป็นเจ้าพนักงาน ตามประมวลกฎหมายอาญา

มาตรา 38 กรรมการผู้ทรงคุณวุฒิมีวาระการดำรงตำแหน่งสามปี กรรมการซึ่งพ้นจากตำแหน่งอาจได้รับแต่งตั้งอีกได้ แต่ไม่เกินสองวาระติดต่อกัน

มาตรา 39 นอกจากการพ้นจากตำแหน่งตามวาระตาม มาตรา 38 กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่ง เมื่อ

(1) ตาย

(2) ลาออก

(3) คณะรัฐมนตรีให้ออกเพราะมีความประพฤติเสื่อมเสีย บกพร่อง หรือไม่สุจริตต่อหน้าที่ หรือหย่อนความสามารถ

(4) เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(5) ได้รับโทษจำคุกโดยต้องคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือ ความผิดลหุโทษ

มาตรา 40 ในกรณีที่กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งตาม มาตรา 39 ให้ถือว่าคณะกรรมการประกอบด้วยกรรมการ เท่าที่เหลืออยู่ และให้ดำเนินการแต่งตั้งกรรมการใหม่แทนภายในหกสิบวันนับแต่วันที่กรรมการพ้นจากตำแหน่ง ให้กรรมการซึ่งได้รับแต่งตั้งแทนอยู่ในตำแหน่งเท่ากับวาระที่เหลืออยู่ของผู้ซึ่งต นแทน

มาตรา 41 การประชุมคณะกรรมการต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่ง ของจำนวนกรรมการทั้งหมดจึงเป็นองค์ประชุม ถ้าประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้คณะกรรมการเลือกกรรมการคนหนึ่งทำหน้าที่ประธาน ในที่ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากันให้ ประธานออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

มาตรา 42 คณะกรรมการมีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณาหรือปฏิบัติการอย่างหนึ่งอย่างใด แทนคณะกรรมการก็ได้ ให้นำความใน มาตรา 41 มาใช้บังคับแก่การประชุมคณะอนุกรรมการโดยอนุโลม

มาตรา 43 ให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยี แห่งชาติ ทำหน้าที่เป็นหน่วยงานธุรกรรมของคณะกรรมการ

:: หมวด 6 บทกำหนดโทษ

มาตรา 44 ผู้ใดประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ โดยไม่แจ้งหรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ ตามที่กำหนดในพระราชกฤษฎีกาตาม มาตรา 33 วรรคหนึ่ง หรือโดยฝ่าฝืนคำสั่งห้ามการประกอบธุรกิจของคณะกรรมการตาม มาตรา 33 วรรคหก ต้องระวางโทษจำคุกไม่เกิน หนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาทหรือทั้งจำทั้งปรับ

มาตรา 45 ผู้ใดประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่ได้รับใบอนุญาต ตามมาตรา 34 ต้องระวาง โทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสองแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 46 บรรดาความผิดตามพระราชบัญญัตินี้ที่กระทำโดยนิติบุคคล ผู้จัดการหรือผู้แทนนิติบุคคล หรือผู้ซึ่งมีส่วนร่วมในการดำเนินงานของนิติบุคคลต้องรับผิดในความผิดนั้นด้วย เว้นแต่พิสูจน์ได้ว่า ตนมิได้รู้เห็นหรือมีส่วนร่วมในการกระทำความผิดนั้น

*หมายเหตุ : เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่การทำธุรกรรมในปัจจุบันมีแนวโน้มที่จะปรับเปลี่ยนวิธีการในการติดต่อสื่อสารที่อาศัยการพัฒนาการเทคโนโลยีทางอิเล็กทรอนิกส์ซึ่งมีความสะดวก รวดเร็วและมีประสิทธิภาพ แต่เนื่องจากการทำธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวมีความแตกต่างจากวิธีการทำธุรกรรมซึ่งมีกฎหมายรองรับอยู่ในปัจจุบัน เป็นอย่างมาก อันส่งผลให้ต้องมีการรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ ให้เสมอกับการทำเป็นหนังสือ หรือหลักฐานเป็น หนังสือ การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการส่งเสริมการทำธุรกรรม ทางอิเล็กทรอนิกส์ให้น่าเชื่อถือและมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิม ควรกำหนดให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ทำหน้าที่วางนโยบายกำหนดหลักเกณฑ์เพื่อส่งเสริมการทำธุรกรรมทาง อิเล็กทรอนิกส์ ติดตามดูแลการประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งมีหน้าที่ในการส่งเสริมการพัฒนาการทางเทคโนโลยี เพื่อติดตามความก้าวหน้าของเทคโนโลยี ซึ่งมีการเปลี่ยนแปลงและพัฒนาศักยภาพตลอดเวลาให้มีมาตรฐานน่าเชื่อถือ ตลอดจนเสนอแนะแนวทางแก้ไขปัญหาและอุปสรรค ที่เกี่ยวข้อง อันจะเป็นการส่งเสริมการให้ธุรกรรมทางอิเล็กทรอนิกส์ทั้งภายในประเทศและระหว่างประเทศ ด้วยการมีกฎหมายรองรับในลักษณะ ที่เป็นเอกรูป และสอดคล้องกับมาตรฐานที่นานาประเทศยอมรับ จึงจำเป็นต้องตราพระราชบัญญัตินี้

7.3 กฎหมายอื่น ๆ ที่เกี่ยวข้อง

นอกจากหัวข้อต่าง ๆ ที่กล่าวมา ยังมีบทกฎหมายอื่น ๆ ที่เกี่ยวข้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ดังนี้

7.3.1 ความผิดซึ่งหน้า

ประมวลกฎหมายวิธีพิจารณาความอาญา

- มาตรา 80

การกระทำผิดซึ่งหน้า ที่เรียกว่า ความผิดซึ่งหน้านั้น ได้แก่ ความผิดซึ่งกำลังกระทำ หรือพบในอาการใดซึ่งแทบจะไม่มีความสงสัยเลยว่าเขาได้กระทำความผิดมาแล้วสดๆ

อย่างไรก็ดี ความผิดทางอาญาดั่งระบุไว้ในบัญชีท้ายประมวลกฎหมายนี้ ให้ถือว่าความผิดนั้นเป็นความผิดซึ่งหน้า ในกรณี ดังนี้

(1) เมื่อบุคคลหนึ่งถูกไล่จับดั่งผู้กระทำ โดยมีเสียงร้องเอะอะ

(2) เมื่อพบบุคคลหนึ่งแทบจะทันทีทันใดหลังจากการกระทำผิดในถิ่นแถวใกล้เคียงกับที่เกิดเหตุนั้น และมีส่งของที่ได้มาจากการกระทำผิด หรือมีเครื่องมือ อาวุธ หรือวัตถุอย่างอื่นอันสันนิษฐานได้ว่าได้ใช้ในการกระทำผิด หรือมีร่องรอยพิรุธเห็นประจักษ์ที่เสื้อผ้าหรือเนื้อตัวของผู้นั้น [2]

7.3.2 แก้ตัวว่าไม่รู้กฎหมาย

ประมวลกฎหมายอาญา

- มาตรา 64

บุคคลจะแก้ตัวว่าไม่รู้กฎหมาย เพื่อให้พ้นจากความรับผิดในทางอาญาไม่ได้ แต่ถ้าศาลเห็นว่าตามสภาพและพฤติการณ์ ผู้กระทำความผิดอาจจะไม่รู้ว่ากฎหมายบัญญัติว่าการกระทำนั้นเป็นความผิด ศาลอาจอนุญาตให้แสดงพยานหลักฐานต่อศาล และถ้าศาลเชื่อว่าผู้กระทำไม่รู้ว่ากฎหมายบัญญัติไว้เช่นนั้น ศาลจะลงโทษน้อยกว่าที่กฎหมายกำหนดไว้สำหรับความผิดนั้นเพียงใดก็ได้ [3]

7.3.3 หมิ่นประมาท

การหมิ่นประมาทบุคคลธรรมดา

ประมวลกฎหมายอาญา

- มาตรา 326

หมิ่นประมาท ผู้ใดใส่ความผู้อื่นต่อบุคคลที่สาม โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นหรือถูกเกลียดชัง ผู้นั้นกระทำความผิดฐานหมิ่นประมาท ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ [4]

ประมวลกฎหมายอาญา

- มาตรา 328

หมิ่นประมาทโดยการโฆษณา ถ้าความผิดฐานหมิ่นประมาทได้กระทำโดยการโฆษณา ด้วยเอกสาร ภาพวาด ภาพระบายสี ภาพยนตร์ ภาพ หรือตัวอักษรที่ทำให้ปรากฏ ไม่ว่าด้วยวิธีใดๆ แผ่นเสียง หรือสิ่งบันทึกเสียง บันทึกภาพ หรือบันทึกอักษร กระทำโดยการกระจายเสียง หรือการกระจายภาพ หรือโดยการป่าวประกาศด้วยวิธีอื่น ผู้กระทำต้องระวางโทษจำคุกไม่เกินสองปี และปรับไม่เกินสองแสนบาท

ประมวลกฎหมายอาญา มาตรา 393

- หมิ่นซึ่งหน้า

- การหมิ่นประมาทเจ้าหน้าที่รัฐ

ประมวลกฎหมายอาญา มาตรา 136

- การหมิ่นประมาทเจ้าพนักงาน

ประมวลกฎหมายอาญา มาตรา 198

- การหมิ่นประมาทศาล

- การหมิ่นประมาทบุคคลสำคัญระดับชาติ

ประมวลกฎหมายอาญา มาตรา 112

หมิ่นพระบรมเดชานุภาพ ผู้ใดหมิ่นประมาท ดูหมิ่น หรือแสดงความอาฆาตมาดร้ายพระมหากษัตริย์ พระราชินี รัชทายาท หรือผู้สำเร็จราชการแทนพระองค์ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี

ประมวลกฎหมายอาญา มาตรา 133

ผู้ใดใช้กำลังประทุษร้าย หรือขู่เข็ญว่าจะใช้กำลังประทุษร้ายเพื่อ

(1) ล้มล้างหรือเปลี่ยนแปลงรัฐธรรมนูญ

(2) ล้มล้างอำนาจนิติบัญญัติ อำนาจบริหาร หรืออำนาจตุลาการแห่งรัฐธรรมนูญ หรือให้ใช้อำนาจดังกล่าวแล้วไม่ได้ หรือ

(3) แบ่งแยกราชอาณาจักรหรือยึดอำนาจปกครองในส่วนหนึ่งส่วนใดแห่งราชอาณาจักร

ผู้นั้นกระทำความผิดฐานเป็นกบฏ ต้องระวางโทษประหารชีวิต หรือจำคุกตลอดชีวิต

- การหมิ่นประมาทบุคคลสำคัญของรัฐต่างชาติ

7.3.4 ลามก อนาจาร

ประมวลกฎหมายอาญา มาตรา 287 ผู้ใด

(1) เพื่อความประสงค์แห่งการค้า หรือโดยการค้าเพื่อการแจกจ่าย หรือเพื่อการแสดงอวดแก่ประชาชน ทำการผลิต มีไว้ นำเข้า หรือยังให้นำเข้าในราชอาณาจักร ส่งออก หรือยังให้ส่งออกไปนอกราชอาณาจักร พาไปหรือยังให้พาไป หรือทำให้แพร่หลายโดยประการใดๆ ซึ่งเอกสาร ภาพเขียน ภาพพิมพ์ ภาพระบายสี สิ่งพิมพ์ รูปภาพ ภาพโฆษณา เครื่องหมาย รูปถ่าย ภาพยนตร์ แถบบันทึกเสียง แถบบันทึกภาพ หรือสิ่งอื่นใดอันลามก

(2) ประกอบการค้า หรือมีส่วน หรือเข้าเกี่ยวข้องในการค้าเกี่ยวกับวัตถุ หรือสิ่งของลามกดังกล่าวแล้ว จ่ายแจก หรือแสดงอวดแก่ประชาชน หรือให้เช่าวัตถุหรือสิ่งของเช่นว่านั้น

(3) เพื่อจะช่วยการทำให้แพร่หลาย หรือการค้าวัตถุหรือสิ่งของลามกดังกล่าวแล้ว โฆษณา หรือไขข่าวโดยประการใดๆ ว่ามีบุคคลกระทำการอันเป็นความผิดตามมาตรานี้ หรือโฆษณา หรือไขข่าวว่าวัตถุ หรือสิ่งของลามกดังกล่าวแล้ว จะหาได้จากบุคคลใด หรือโดยวิธีใด

ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ

หมายเหตุ

1. คำว่า “การทำให้แพร่หลาย” หมายถึง การทำให้แพร่ออกไปสู่สาธารณะ ทำให้บุคคลอื่นสามารถเข้าถึงข้อมูล เป็นที่รู้รับทราบกันทั่วไปได้ ถึงแม้การแพร่หลายนั้นจะเป็นการเผยแพร่กันแค่ภายในกลุ่มปิด เช่น การนำภาพลามกไว้ในเว็บไซต์ที่เปิดรับเฉพาะสมาชิกเท่านั้นถือว่าเป็นการแพร่หลายเช่นกัน (เทียบเคียงจาก คำพิพากษาฎีกาที่ 3213/2526 น. 2533 การมีวิดีโอเทปภาพลามกไว้ให้เช่น หรือแลกเปลี่ยนกับสมาชิกเป็นความผิดฐานค้าวัตถุลามกตามมาตรา 287 ประมวลกฎหมายอาญา)

2. คำว่า “ลามก” ยังเป็นคำที่มีการถกเถียงกันอยู่ในวงกว้าง โดยยังไม่สามารถระบุได้ชัด เนื่องจากทัศนะและอัตวิสัยของบุคคลนั้นแตกต่างกัน โดยมีหลายปัจจัยที่เป็นตัวกำหนดทัศนะของผู้มอง เช่น อายุ เพศ ประสบการณ์ หรือบรรทัดฐานของสังคม ตามจารีตประเพณีในสังคมหนึ่งในช่วงเวลาหนึ่ง อย่างไรก็ตาม มีคำพิพากษาฎีกาได้วางบรรทัดฐานไว้ว่าสิ่งใดอาจถือได้ว่ามีลักษณะอันลามก ฎีกาที่ 978/2492 ฎ.675 สิ่งอันลามก คือ น่าอับอายในทางเพศต่อตา น่าอุจาดบัดสี ตรงกันข้ามกับสิ่งที่เป็นศิลปะอันแสดงถึงความงามและฝีมือของศิลปิน ศิลปะหรือลามกพิจารณาตามความรู้สึกของวิญญูชนผู้มิใช่เคร่งต่อจารีตประเพณีโดยไม่ยอมเปลี่ยนแปลงไปตามสมัยของโลก รูปหญิงเปลือยกาย เห็นเด่นชัดเฉพาะกันน ส่วนโยนีถูกระบายให้ลบเลือนเห็นเพียงฐาน แสดงสุขภาพ อนามัยของการอาบแดด สอนวิธีเขียนส่วนสัดความงามของร่างกาย ไม่น่าเกลียด

ประมวลกฎหมายแพ่งและพาณิชย์

- มาตรา 423

ผู้ใดกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนต่อความจริง เป็นที่เสียหายแก่ชื่อเสียงหรือเกียรติคุณของบุคคลอื่นก็ดี หรือเป็นที่เสียหายแก่ทางทำมาหาได้ หรือทางเจริญของเขาโดยประการอื่นก็ดี ท่านว่าผู้นั้นจะต้องใช้ค่าสินไหมทดแทนให้แก่เขาเพื่อความเสียหายอย่างใด ๆ อันเกิดแต่การนั้น แม้ทั้งเมื่อตนมิได้รู้ว่าข้อความนั้นไม่จริง แต่หากควรจะรู้ได้

ผู้ใดส่งข่าวสารอันตนมิได้รู้ว่าเป็นความไม่จริง หากว่าตนเองหรือผู้รับข่าวสารนั้นมีทางได้เสียโดยชอบในการนั้นด้วยแล้ว ท่านว่าเพียงที่ส่งข่าวสารเช่นนั้นหาทำให้ผู้นั้นต้องรับผิดใช้ค่าสินไหมทดแทนไม่

หมวด 2 ความผิดฐานเปิดเผยความลับ

- มาตรา 322

ผู้ใดเปิดผนึกหรือเอาจดหมาย โทรเลขหรือเอกสารใด ๆ ซึ่งปิดผนึกของผู้อื่นไปเพื่อล่วงรู้ข้อความก็ดี เพื่อนำข้อความในจดหมาย โทรเลข หรือเอกสารเช่นว่านั้นออกเปิดเผยก็ดี ถ้าการกระทำนั้นน่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ

- มาตรา 323

ผู้ใดล่วงรู้หรือได้มาซึ่งความลับของผู้อื่น โดยเหตุที่เป็นเจ้าพนักงานผู้มีหน้าที่ โดยเหตุที่ประกอบอาชีพเป็นแพทย์ เภสัชกร คนจำหน่ายยา นางผดุงครรภ์ ผู้พยาบาล นักบวช หมอความ ทนายความหรือผู้สอบบัญชี หรือโดยเหตุที่เป็นผู้ช่วยในการประกอบอาชีพนั้น แล้วเปิดเผยความลับนั้นในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ ผู้รับการศึกษาอบรมในอาชีพดังกล่าวในวรรคแรกเปิดเผยความลับของผู้อื่นอันตนได้ล่วงรู้ หรือได้มาในการศึกษาอบรมนั้น ในประการที่น่าจะเกิดความเสียหายแต่ผู้หนึ่งผู้ใดต้องระวางโทษเช่นเดียวกัน

- มาตรา 324

ผู้ใดโดยเหตุที่ตนมีตำแหน่งหน้าที่ วิชาชีพ หรืออาชีพอันเป็นที่ไว้วางใจ ล่วงรู้ หรือได้มาซึ่งความลับของผู้อื่นเกี่ยวกับอุตสาหกรรม การค้นพบ หรือการนิมิตในวิทยาศาสตร์ เปิดเผยหรือใช้ความลับนั้นเพื่อประโยชน์ตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ

- มาตรา 325 ความผิดในหมวดนี้เป็นความผิดอันยอมความได้

พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551

- มาตรา 4

ในพระราชบัญญัตินี้ “แสวงหาประโยชน์โดยมิชอบ” หมายความว่า การแสวงหาประโยชน์จากการค้าประเวณีการผลิต หรือเผยแพร่วัตถุหรือสื่อลามก การแสวงหาประโยชน์ทางเพศในรูปแบบอื่น การเอาคนลงเป็นทาส การนำคนมาขอทาน การบังคับใช้แรงงานหรือบริการ การบังคับตัดอวัยวะเพื่อการค้า หรือการอื่นใดที่คล้ายคลึงกันอันเป็นการขูดรีดบุคคลไม่ว่าบุคคลนั้นจะยินยอมหรือไม่ก็ตาม

- มาตรา 30

ในกรณีที่มีเหตุอันควรเชื่อได้ว่าเอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์หรือสื่อสารสนเทศอื่นใดถูกใช้ หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานค้ามนุษย์ พนักงานเจ้าหน้าที่ซึ่งได้รับอนุมัติเป็นหนังสือจากผู้บัญชาการตำรวจแห่งชาติ อธิบดีกรมสอบสวนคดีพิเศษหรือผู้ว่าราชการจังหวัด แล้วแต่กรณีจะยื่นคำขอฝ่ายเดียวต่อศาลอาญาหรือศาลจังหวัดที่มีเขตอำนาจ เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ได้มาซึ่งเอกสารหรือข้อมูลข่าวสารดังกล่าวก็ได้ ทั้งนี้ตามหลักเกณฑ์และวิธีการที่กำหนดในข้อบังคับประธานศาลฎีกา

การอนุญาตตามวรรคหนึ่ง ให้ศาลพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็น ดังต่อไปนี้

(1) มีเหตุอันควรเชื่อว่ามีการกระทำความผิด หรือจะมีการกระทำความผิดฐานค้ามนุษย์

(2) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดฐานค้ามนุษย์จากการเข้าถึงข้อมูลข่าวสารดังกล่าว

(3) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสม หรือมีประสิทธิภาพมากกว่าได้

การอนุญาตตามวรรคหนึ่ง ให้ศาลสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวันโดยจะกำหนดเงื่อนไขใดๆ ก็ได้ และให้ผู้เกี่ยวข้องกับเอกสารหรือข้อมูลข่าวสารตามคำสั่งดังกล่าวให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายหลังที่มีคำสั่งอนุญาตหากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุ หรือพฤติการณ์เปลี่ยนแปลงไปให้ศาลมีอำนาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

ในการดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่มีอำนาจร้องขอให้บุคคลใดช่วยเหลือในการปฏิบัติหน้าที่ได้ เมื่อพนักงานเจ้าหน้าที่ได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้พนักงานเจ้าหน้าที่บันทึกรายละเอียดผลการดำเนินการนั้น และให้ส่งบันทึกนั้นไปยังศาลที่มีคำสั่งโดยเร็ว

บรรดาเอกสารหรือข้อมูลข่าวสารที่ได้มาตามวรรคหนึ่ง ให้เก็บรักษาและใช้ประโยชน์ในการสืบสวนและใช้เป็นพยานหลักฐานในการดำเนินคดีความผิดฐานค้ามนุษย์เท่านั้น ทั้งนี้ตามระเบียบที่รัฐมนตรีกำหนด

- มาตรา 56

ผู้ใดกระทำการหรือจัดให้มีการกระทำการดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

(1) บันทึกภาพ แพร่ภาพ พิมพ์รูป บันทึกเสียง แพร่เสียงหรือสิ่งอื่นที่สามารถแสดงว่าบุคคลใดเป็นผู้เสียหายจากการกระทำความผิดฐานค้ามนุษย์ ทั้งนี้ไม่ว่าขั้นตอนใด ๆ

(2) โฆษณาหรือเผยแพร่ข้อความ ซึ่งปรากฏในทางสอบสวนของพนักงานสอบสวนหรือในทางพิจารณาคดีของศาลที่ทำให้บุคคลอื่นรู้จักชื่อตัว ชื่อสกุลของผู้เสียหายจากการกระทำความผิดฐานค้ามนุษย์หรือบุคคลในครอบครัวผู้เสียหายนั้น ทั้งนี้ไม่ว่าโดยสื่อสารสนเทศประเภทใด

(3) โฆษณาหรือเผยแพร่ข้อความ ภาพ หรือเสียง ไม่ว่าโดยสื่อสารสนเทศประเภทใด เปิดเผยประวัติ สถานที่อยู่ สถานที่ทำงาน หรือสถานศึกษาของบุคคลซึ่งเป็นผู้เสียหายจากการกระทำความผิดฐานค้ามนุษย์

ความในวรรคหนึ่งมิให้ใช้บังคับแก่การกระทำที่ผู้กระทำจำต้องกระทำ เพื่อประโยชน์ของทางราชการในการคุ้มครอง หรือช่วยเหลือผู้เสียหาย หรือผู้เสียหายยินยอมโดยบริสุทธิ์ใจ

พระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546

- มาตรา 4

“ทารุณกรรม” หมายความว่า การกระทำหรือละเว้นการกระทำด้วยประการใดๆ จนเป็นเหตุให้เด็กเสื่อมเสียเสรีภาพ หรือเกิดอันตรายแก่ร่างกายหรือจิตใจ การกระทำผิดทางเพศต่อเด็กการใช้เด็กให้กระทำหรือประพฤติในลักษณะที่น่าจะเป็นอันตรายแก่ร่างกาย หรือจิตใจหรือขัดต่อกฎหมายหรือศีลธรรมอันดี ทั้งนี้ไม่ว่าเด็กจะยินยอมหรือไม่ก็ตาม

- มาตรา 26

ภายใต้บังคับบทบัญญัติแห่งกฎหมายอื่น ไม่ว่าเด็กจะยินยอมหรือไม่ ห้ามมิให้ผู้ใดกระทำการดังต่อไปนี้

(1) กระทำหรือละเว้นการกระทำอันเป็นการทารุณกรรมต่อร่างกายหรือจิตใจของเด็ก

(2) จงใจหรือละเลยไม่ให้สิ่งจำเป็นแก่การดำรงชีวิต หรือการรักษาพยาบาลแก่เด็กที่อยู่ในความดูแลของตนจนน่าจะเกิดอันตรายแก่ร่างกายหรือจิตใจของเด็ก

(3) บังคับ ขู่เข็ญ ชักจูง ส่งเสริม หรือยินยอมให้เด็กประพฤติตนไม่สมควรหรือน่าจะทำให้เด็กมีความประพฤติเสี่ยงต่อการกระทำผิด

(4) โฆษณาทางสื่อมวลชนหรือเผยแพร่ด้วยประการใด เพื่อรับเด็กหรือยกเด็กให้แก่บุคคลอื่นที่มิใช่ญาติของเด็ก เว้นแต่เป็นการกระทำของทางราชการหรือได้รับอนุญาตจากทางราชการแล้ว

(5) บังคับ ขู่เข็ญ ชักจูง ส่งเสริม ยินยอม หรือกระทำด้วยประการใดให้เด็กไปเป็นขอทาน เด็กเร่ร่อน หรือใช้เด็กเป็นเครื่องมือในการขอทานหรือการกระทำผิด หรือกระทำด้วยประการใดอันเป็นการแสวงหาประโยชน์โดยมิชอบจากเด็ก

(6) ใช้จ้าง หรือวานเด็กให้ทำงาน หรือกระทำการอันอาจเป็นอันตรายแก่ร่างกายหรือจิตใจมีผลกระทบต่อการเจริญเติบโต หรือขัดขวางต่อพัฒนาการของเด็ก

(7) บังคับ ขู่เข็ญ ใช้ชักจูง ยุยง ส่งเสริม หรือยินยอมให้เด็กเล่นกีฬาหรือให้กระทำการใด เพื่อแสวงหาประโยชน์ทางการค้าอันมีลักษณะเป็นการขัดขวางต่อการเจริญเติบโตหรือพัฒนาการของเด็กหรือมีลักษณะเป็นการทารุณกรรมต่อเด็ก

(8) ใช้หรือยินยอมให้เด็กเล่นการพนันไม่ว่าชนิดใด หรือเข้าไปในสถานที่เล่นการพนัน สถานค้าประเวณี หรือสถานที่ที่ห้ามมิให้เด็กเข้า

(9) บังคับ ขู่เข็ญ ใช้ชักจูง ยุยง ส่งเสริม หรือยินยอมให้เด็กแสดงหรือกระทำการอันมีลักษณะลามกอนาจาร ไม่ว่าจะเป็นไปเพื่อให้ได้มาซึ่งค่าตอบแทนหรือเพื่อการใด

(10) จำหน่าย แลกเปลี่ยน หรือให้สุราหรือบุหรี่แก่เด็ก เว้นแต่การปฏิบัติทางการแพทย์ ถ้าการกระทำความผิดตามวรรคหนึ่งมีโทษตามกฎหมายอื่นที่หนักกว่าก็ให้ลงโทษตามกฎหมายนั้น

- มาตรา 27

ห้ามมิให้ผู้ใดโฆษณา หรือเผยแพร่ทางสื่อมวลชน หรือสื่อสารสนเทศประเภทใด ซึ่งข้อมูลเกี่ยวกับตัวเด็กหรือผู้ปกครอง โดยเจตนาที่จะทำให้เกิดความเสียหายแก่จิตใจ ชื่อเสียง เกียรติคุณ หรือสิทธิประโยชน์อื่นใดของเด็ก หรือเพื่อแสวงหาประโยชน์สำหรับตนเองหรือผู้อื่นโดยมิชอบ

- มาตรา 50

ห้ามมิให้ผู้ปกครองสวัสดิภาพ หรือผู้คุ้มครองสวัสดิภาพเด็ก เปิดเผยชื่อตัว ชื่อสกุลภาพหรือข้อมูลใดๆ เกี่ยวกับตัวเด็กและผู้ปกครอง

ในลักษณะที่น่าจะเกิดความเสียหายแก่ชื่อเสียง เกียรติคุณหรือสิทธิประโยชน์อย่างใดอย่างหนึ่งของเด็กหรือผู้ปกครอง บทบัญญัติในวรรคหนึ่งให้ใช้บังคับแก่พนักงานเจ้าหน้าที่ นักสังคมสงเคราะห์ นักจิตวิทยาและผู้มีหน้าที่คุ้มครองสวัสดิภาพเด็กตามมาตรา 24 ซึ่งได้ล่วงรู้ข้อมูลดังกล่าว เนื่องในการปฏิบัติหน้าที่ของตนด้วยโดยอนุโลม

ห้ามมิให้ผู้ใดโฆษณา หรือเผยแพร่ทางสื่อมวลชน หรือสื่อสารสนเทศประเภทใดซึ่งข้อมูลที่เปิดเผย โดยฝ่าฝืนบทบัญญัติในวรรคหนึ่งหรือวรรคสอง

7.3.5 การก่อการร้าย

ตามประมวลกฎหมายอาญามาตรา 135/1: ผู้ใดกระทำการอันเป็นความผิดอาญา ดังต่อไปนี้

(1) ใช้กำลังประทุษร้าย หรือกระทำการใดอันก่อให้เกิดอันตรายต่อชีวิต หรืออันตรายอย่างร้ายแรงต่อร่างกาย หรือเสรีภาพของบุคคลใดๆ

(2) กระทำการใดอันก่อให้เกิดความเสียหายอย่างร้ายแรงแก่ระบบการขนส่งสาธารณะ ระบบโทรคมนาคม หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

(3) กระทำการใดอันก่อให้เกิดความเสียหายแก่ทรัพย์สินของรัฐหนึ่งรัฐใด หรือของบุคคลใด หรือต่อสิ่งแวดล้อม อันก่อให้เกิดหรือน่าจะก่อให้เกิดความเสียหายทางเศรษฐกิจอย่างสำคัญ

ถ้าการกระทำนั้นได้กระทำโดยมีความมุ่งหมายเพื่อขู่เข็ญหรือบังคับรัฐบาลไทย รัฐบาลต่างประเทศ หรือองค์การระหว่างประเทศ ให้กระทำหรือไม่กระทำการใดอันจะก่อให้เกิดความเสียหายอย่างร้ายแรง หรือเพื่อสร้างความปั่นป่วนโดยให้เกิดความหวาดกลัวในหมู่ประชาชน ผู้นั้นกระทำความผิดฐานก่อการร้าย ต้องระวางโทษประหารชีวิต จำคุกตลอดชีวิต หรือจำคุกตั้งแต่สามปีถึงยี่สิบปี และปรับตั้งแต่หกหมื่นบาทถึงหนึ่งล้านบาท

การกระทำในการเดินขบวน ชุมนุม ประท้วง โต้แย้ง หรือเคลื่อนไหวเพื่อเรียกร้องให้รัฐช่วยเหลือหรือให้ได้รับความเป็นธรรมอันเป็นการใช้เสรีภาพตามรัฐธรรมนูญ ไม่เป็นการกระทำความผิดฐานก่อการร้าย

- มาตรา 135/2

(1) ผู้ใดขู่เข็ญว่าจะกระทำการก่อการร้าย โดยมีพฤติการณ์อันควรเชื่อได้ว่าบุคคลนั้นจะกระทำการตามที่ขู่เข็ญจริง หรือ

(2) ผู้ใดสะสมกำลังพลหรืออาวุธ จัดหา หรือรวบรวมทรัพย์สิน ให้หรือรับการฝึกการก่อการร้าย ตระเตรียมการอื่นใด หรือสมคบกัน เพื่อก่อการร้าย หรือกระทำความผิดใดๆ อันเป็นส่วนของแผนการเพื่อก่อการร้าย หรือยุยงประชาชนให้เข้ามีส่วนในการก่อการร้าย หรือรู้ว่ามีผู้จะก่อการร้ายแล้วกระทำการใดอันเป็นการช่วยปกปิดไว้

ผู้นั้นต้องระวางโทษจำคุกตั้งแต่สองปีถึงสิบปี และปรับตั้งแต่สี่หมื่นบาทถึงสองแสนบาท

- มาตรา 135/3

ผู้ใดเป็นผู้สนับสนุนในการกระทำความผิดตามมาตรา 135/1 หรือมาตรา 135/2 ต้องระวางโทษเช่นเดียวกับตัวการในความผิดนั้นๆ

- มาตรา 135/4

ผู้ใดเป็นสมาชิกของคณะบุคคลซึ่งมีมติของ หรือประกาศภายใต้คณะมนตรีความมั่นคงแห่งสหประชาชาติกำหนดให้เป็นคณะบุคคลที่มีการกระทำอันเป็นการก่อการร้าย และรัฐบาลไทยได้ประกาศให้ความรับรองมติหรือประกาศดังกล่าวด้วยแล้ว ผู้นั้นต้องระวางโทษจำคุกไม่เกินเจ็ดปี และปรับไม่เกินหนึ่งแสนสี่หมื่นบาท

7.3.6 ความผิดเกี่ยวกับข้อมูลส่วนบุคคล

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

- มาตรา 14

ข้อมูลข่าวสารของราชการที่อาจก่อให้เกิดความเสียหายต่อสถาบันพระมหากษัตริย์จะเปิดเผยมิได้

- มาตรา 15

ข้อมูลข่าวสารของราชการที่มีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้ หน่วยงานของรัฐ หรือเจ้าหน้าที่ของรัฐอาจมีคำสั่งมิให้เปิดเผยก็ได้ โดยคำนึงถึงการปฏิบัติหน้าที่ตามกฎหมายของหน่วยงานของรัฐ ประโยชน์สาธารณะ และประโยชน์ของเอกชนที่เกี่ยวข้องประกอบกัน

(1) การเปิดเผยจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศ หรือความมั่นคงในทางเศรษฐกิจหรือการคลังของประเทศ

(2) การเปิดเผยจะทำให้การบังคับใช้กฎหมายเสื่อมประสิทธิภาพ หรือไม่อาจสำเร็จตามวัตถุประสงค์ได้ ไม่ว่าจะเกี่ยวกับการฟ้องคดี การป้องกัน การปราบปราม การทดสอบ การตรวจสอบ หรือการรู้แหล่งที่มาของข้อมูลข่าวสารหรือไม่ก็ตาม

(3) ความเห็นหรือคำแนะนำภายในหน่วยงานของรัฐในการดำเนินการเรื่องหนึ่งเรื่องใด แต่ทั้งนี้ไม่รวมถึงรายงานทางวิชาการ รายงานข้อเท็จจริง หรือข้อมูลข่าวสารที่นำมาใช้ในการทำความเห็นหรือคำแนะนำภายในดังกล่าว

(4) การเปิดเผยจะก่อให้เกิดอันตรายต่อชีวิต หรือความปลอดภัยของบุคคลหนึ่งบุคคลใด

(5) รายงานการแพทย์หรือข้อมูลข่าวสารส่วนบุคคล ซึ่งการเปิดเผยจะเป็นการรุก

ล้ำสิทธิส่วนบุคคลโดยไม่สมควร

(6) ข้อมูลข่าวสารของราชการที่มีกฎหมายคุ้มครองมิให้เปิดเผย หรือข้อมูลข่าวสารที่มีผู้ให้มาโดยไม่ประสงค์ ให้ทางราชการนำไปเปิดเผยต่อผู้อื่น

(7) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

คำสั่งมิให้เปิดเผยข้อมูลข่าวสารของราชการจะกำหนดเงื่อนไขอย่างใดก็ได้ แต่ต้องระบุไว้ด้วยว่าที่เปิดเผยไม่ได้เพราะเป็นข้อมูลข่าวสารประเภทใดและเพราะเหตุใด และให้ถือว่าการมีคำสั่งเปิดเผยข้อมูลข่าวสารของราชการเป็นดุลพินิจ โดยเฉพาะของเจ้าหน้าที่ของรัฐตามลำดับสายการบังคับบัญชา แต่ผู้ขออาจอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารได้ตามที่กำหนดในพระราชบัญญัตินี้ [4]

- มาตรา 24

หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่น หรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่เป็นการเปิดเผย ดังต่อไปนี้

(1) ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตน เพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

(2) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

(3) ต่อหน่วยงานของรัฐที่ทำงานด้านการวางแผน หรือการสถิติหรือสำมะโนต่างๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

(4) เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัย โดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด

(5) ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา 26 วรรคหนึ่ง เพื่อการตรวจดูคุณค่าในการเก็บรักษา

(6) ต่อเจ้าหน้าที่ของรัฐเพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม

(7) เป็นการให้ซึ่งจำเป็นเพื่อการป้องกัน หรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

(8) ต่อศาลและเจ้าหน้าที่ของรัฐ หรือหน่วยงานของรัฐ หรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว

(9) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา การเปิดเผยข้อมูลข่าวสารส่วนบุคคล

ตามวรรคหนึ่ง (3) (4) (5) (6) (7) (8) และ (9) ให้มีการจัดทำบัญชีแสดงการเปิดเผยกำกับไว้กับข้อมูลข่าวสารนั้น ตามหลักเกณฑ์และวิธีการที่กำหนดในกฎกระทรวง

3.2.7 การละเมิดสิทธิส่วนบุคคล

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550

- มาตรา 4

ศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาคของบุคคลย่อมได้รับความคุ้มครอง

พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519

- มาตรา 14 จัตวา

ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดเกี่ยวกับยาเสพติด เจ้าพนักงานซึ่งได้รับอนุมัติจากเลขาธิการเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญา เพื่อมีคำสั่งอนุญาตให้เจ้าพนักงานได้มาซึ่งข้อมูลข่าวสารดังกล่าวได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญา พิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคล หรือสิทธิอื่นใด ประกอบกับเหตุผลและความจำเป็น ดังต่อไปนี้

(1) มีเหตุอันควรเชื่อว่ามีการกระทำความผิด หรือจะมีการกระทำความผิดเกี่ยวกับยาเสพติด

(2) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดเกี่ยวกับยาเสพติดจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

(3) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวันโดยกำหนดเงื่อนไขใดๆ ก็ได้ และให้ผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งดังกล่าว จะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

เมื่อเจ้าพนักงานได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้รายงานการดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบ

บรรดาข้อมูลข่าวสารที่ได้มาตามวรรคหนึ่ง ให้เก็บรักษาและใช้ประโยชน์ในการสืบสวนและใช้เป็นพยานหลักฐานในการดำเนินคดีเท่านั้น ทั้งนี้ตามระเบียบที่คณะกรรมการกำหนด [5]

- ส่วนที่ 3 สิทธิและเสรีภาพส่วนบุคคล

- มาตรา 35 สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง

การกล่าวหรือไขข่าวแพร่หลาย ซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ตามที่กฎหมายบัญญัติ [6]

- มาตรา 36 บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางที่ชอบด้วยกฎหมาย

การตรวจ การกัก หรือการเปิดเผยสิ่งสื่อสารที่บุคคลมีติดต่อถึงกัน รวมทั้งการกระทำด้วยประการอื่นใด เพื่อให้ล่วงรู้ถึงข้อความในสิ่งสื่อสารทั้งหลายที่บุคคลมีติดต่อถึงกันจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย เฉพาะเพื่อรักษาความมั่นคงของรัฐ หรือเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน [6]

- ส่วนที่ 7 เสรีภาพในการแสดงความคิดเห็นของบุคคลและสื่อมวลชน

- มาตรา 45 บุคคลย่อมมีเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อความหมายโดยวิธีอื่น

การจำกัดเสรีภาพตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย เฉพาะเพื่อรักษาความมั่นคงของรัฐ เพื่อคุ้มครองสิทธิ เสรีภาพ เกียรติยศ ชื่อเสียง สิทธิในครอบครัว หรือความเป็นอยู่ส่วนตัวของบุคคลอื่น เพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือเพื่อป้องกัน หรือระงับความเสื่อมทรามทางจิตใจ หรือสุขภาพของประชาชน

การสั่งปิดกิจการหนังสือพิมพ์หรือสื่อมวลชนอื่น เพื่อลิดรอนเสรีภาพตามมาตรานี้จะกระทำมิได้

การห้ามหนังสือพิมพ์หรือสื่อมวลชนอื่นเสนอข่าวสาร หรือแสดงความคิดเห็นทั้งหมดหรือบางส่วน หรือการแทรกแซงด้วยวิธีการใดๆ เพื่อลิดรอนเสรีภาพตามมาตรานี้จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายซึ่งได้ตราขึ้นตามวรรคสอง

การให้นำข่าวหรือบทความไปให้เจ้าหน้าที่ตรวจก่อนนำไปโฆษณาในหนังสือพิมพ์ หรือสื่อมวลชนอื่นจะกระทำมิได้ เว้นแต่จะกระทำในระหว่างเวลาที่ประเทศอยู่ในภาวะสงคราม แต่ทั้งนี้จะต้องกระทำโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายซึ่งได้ตราขึ้นตามวรรคสอง

เจ้าของกิจการหนังสือพิมพ์หรือสื่อมวลชนอื่นต้องเป็นบุคคลสัญชาติไทย

การให้เงินหรือทรัพย์สินอื่น เพื่ออุดหนุนกิจการหนังสือพิมพ์หรือสื่อมวลชนอื่นของเอกชนและรัฐจะกระทำมิได้

- มาตรา 46 พนักงานหรือลูกจ้างของเอกชนที่ประกอบกิจการหนังสือพิมพ์

วิทยุกระจายเสียง วิทยุโทรทัศน์ หรือสื่อมวลชนอื่น ย่อมมีเสรีภาพในการเสนอข่าวและแสดงความคิดเห็น

ภายใต้ข้อจำกัดตามรัฐธรรมนูญ โดยไม่ตกอยู่ภายใต้อาณัติของหน่วยราชการ หน่วยงานของรัฐ รัฐวิสาหกิจ หรือเจ้าของกิจการนั้น แต่ต้องไม่ขัดต่อจริยธรรมแห่งการประกอบวิชาชีพ และมีสิทธิจัดตั้งองค์กรเพื่อปกป้องสิทธิ เสรีภาพและความเป็นธรรม รวมทั้งมีกลไกควบคุมกันเองขององค์กรวิชาชีพ

ข้าราชการ พนักงาน หรือลูกจ้างของหน่วยราชการ หน่วยงานของรัฐ หรือรัฐวิสาหกิจในกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ หรือสื่อมวลชนอื่น ย่อมมีเสรีภาพเช่นเดียวกับพนักงานหรือลูกจ้างของเอกชนตามวรรคหนึ่ง

การกระทำใดๆ ไม่ว่าโดยทางตรงหรือทางอ้อมของผู้ดำรงตำแหน่งทางการเมือง เจ้าหน้าที่ของรัฐ หรือเจ้าของกิจการ อันเป็นการขัดขวางหรือแทรกแซงการเสนอข่าว หรือแสดงความคิดเห็นในประเด็นสาธารณะของบุคคลตามวรรคหนึ่งหรือวรรคสอง ให้ถือว่าเป็นการจงใจใช้อำนาจหน้าที่โดยมิชอบและไม่มีผลใช้บังคับ เว้นแต่เป็นการกระทำเพื่อให้เป็นไปตามกฎหมายหรือจริยธรรมแห่งการประกอบวิชาชีพ

7.3.7 ความผิดเกี่ยวกับยาเสพติด

พระราชบัญญัติยาเสพติดให้โทษ พ.ศ. 2522

- มาตรา 4 ในพระราชบัญญัตินี้

“ยาเสพติดให้โทษ” หมายความว่า สารเคมีหรือวัตถุชนิดใดๆ ซึ่งเมื่อเสพเข้าสู่ร่างกายไม่ว่าจะโดยรับประทาน ดม สูบ ฉีด หรือด้วยประการใดๆ แล้วทำให้เกิดผลต่อร่างกายและจิตใจในลักษณะสำคัญ เช่น ต้องเพิ่มขนาดการเสพขึ้นเป็นลำดับ มีอาการถอนยาเมื่อขาดยา มีความต้องการเสพทั้งทางร่างกายและจิตใจอย่างรุนแรงตลอดเวลา และสุขภาพโดยทั่วไปจะทรุดโทรมลง กับให้รวมตลอดถึงพืชหรือส่วนของพืชที่เป็นหรือให้ผลผลิตเป็นยาเสพติดให้โทษ หรืออาจใช้ผลิตเป็นยาเสพติดให้โทษและสารเคมีที่ใช้ในการผลิตยาเสพติดให้โทษด้วย ทั้งนี้ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา แต่ไม่หมายความถึง ยาสามัญประจำบ้านบางตำรับตามกฎหมายว่าด้วยยาที่มียาเสพติดให้โทษผสมอยู่

“ผลิต” หมายความว่า เพาะ ปลูก ทำ ผสม ปรุง แปรสภาพ เปลี่ยนรูป สังเคราะห์ทางวิทยาศาสตร์ และให้หมายความรวมตลอดถึงการแบ่งบรรจุ หรือรวมบรรจุด้วย

“จำหน่าย” หมายความว่า ขาย จ่าย แจก แลกเปลี่ยน ให้

“นำเข้า” หมายความว่า นำหรือสั่งเข้ามาในราชอาณาจักร

“ส่งออก” หมายความว่า นำหรือส่งออกนอกราชอาณาจักร

“เสพ” หมายความว่า การรับยาเสพติดให้โทษเข้าสู่ร่างกายไม่ว่าด้วยวิธีใด

“ติดยาเสพติดให้โทษ” หมายความว่า เสพเป็นประจำติดต่อกันและตกอยู่ในสภาพที่จำเป็นต้องพึ่งยาเสพติดให้โทษนั้น โดยสามารถตรวจพบสภาพเช่นว่านั้นได้ตามหลักวิชาการ

“หน่วยการใช้” หมายความว่า เม็ด ซอง ขวด หรือหน่วยอย่างอื่นที่ทำขึ้น ซึ่งโดยปกติสำหรับการใช้เสพหนึ่งครั้ง

“การบำบัดรักษา” หมายความว่า การบำบัดรักษาผู้ติดยาเสพติดให้โทษ ซึ่งรวมตลอดถึงการฟื้นฟูสมรรถภาพและการติดตามผลหลังการบำบัดรักษาด้วย

“สถานพยาบาล” หมายความว่า โรงพยาบาล สถานพยาบาล สถานพักฟื้น หรือสถานที่อื่นใดเฉพาะที่รัฐมนตรีประกาศในราชกิจจานุเบกษาให้เป็นสถานที่ทำการบำบัดรักษาผู้ติดยาเสพติดให้โทษ

“เภสัชกร” หมายความว่า ผู้ประกอบวิชาชีพเภสัชกรรมตามกฎหมายว่าด้วยวิชาชีพเภสัชกรรม

“ตำรับยา” หมายความว่า สูตรของสิ่งปรุงไม่ว่าจะมีรูปลักษณะใดที่มียาเสพติดให้โทษรวมอยู่ด้วย ทั้งนี้รวมทั้งยาเสพติดให้โทษที่มีลักษณะเป็นวัตถุสำเร็จรูปทางเภสัชกรรม ซึ่งพร้อมที่จะนำไปใช้แก่คนหรือสัตว์ได้

“ข้อความ” หมายความรวมถึง การกระทำให้ปรากฏด้วยตัวอักษร ภาพ ภาพยนตร์ แสง เสียง เครื่องหมายหรือการกระทำอย่างใดๆ ที่ทำให้บุคคลทั่วไปสามารถเข้าใจความหมายได้

“โฆษณา” หมายความรวมถึง กระทำการไม่ว่าด้วยวิธีใดๆ ให้ประชาชนเห็นหรือทราบข้อความเพื่อประโยชน์ในทางการค้า แต่ไม่หมายความรวมถึง เอกสารทางวิชาการหรือตำราที่เกี่ยวกับการเรียนการสอน

“ผู้รับอนุญาต” หมายความว่า ผู้ได้รับใบอนุญาตตามพระราชบัญญัตินี้

“ผู้อนุญาต” หมายความว่า เลขาธิการคณะกรรมการอาหารและยา หรือผู้ซึ่งได้รับมอบหมายจากเลขาธิการคณะกรรมการอาหารและยา

“คณะกรรมการ” หมายความว่า คณะกรรมการควบคุมยาเสพติดให้โทษตามพระราชบัญญัตินี้

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“เลขาธิการ” หมายความว่า เลขาธิการคณะกรรมการอาหารและยา

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

7.3.8 ทรัพย์สินทางปัญญา

ทรัพย์สินทางปัญญา หมายถึง สิทธิทางกฎหมายที่ให้เจ้าของสิทธิ หรือ “ผู้ทรงสิทธิ” มีอยู่เหนือสิ่งที่เกิดจากความคิดสร้างสรรค์ทางปัญญาของมนุษย์ โดยอาจแบ่งทรัพย์สินทางปัญญาออกได้ 2 ประเภทหลัก คือ [7]

- ทรัพย์สินทางอุตสาหกรรมและ
- ลิขสิทธิ์

สำหรับทรัพย์สินทางอุตสาหกรรมยังแบ่งออกได้อีก 5 ประเภท ได้แก่

- สิทธิบัตร
- เครื่องหมายการค้า
- แบบผังภูมิของวงจรรวม
- ความลับทางการค้า
- สิ่งบ่งชี้ทางภูมิศาสตร์

ประเทศไทยมีกฎหมายให้ความคุ้มครองทรัพย์สินทางปัญญาหลายฉบับ เช่น พระราชบัญญัติสิทธิบัตร พ.ศ. 2522 ซึ่งแก้ไขเพิ่มเติมมาแล้วสองครั้งโดยพระราชบัญญัติสิทธิบัตร (ฉบับที่ 2) พ.ศ. 2535 และพระราชบัญญัติสิทธิบัตร (ฉบับที่ 3) พ.ศ. 2542 พระราชบัญญัติเครื่องหมายการค้า พ.ศ. 2534 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติเครื่องหมายการค้า (ฉบับที่ 2) พ.ศ. 2537 พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 พระราชบัญญัติคุ้มครองแบบผังภูมิของวงจรรวม พ.ศ. 2543 เป็นต้น

ปัญหาการการละเมิดลิขสิทธิ์ในประเทศไทย

การละเมิดลิขสิทธิ์ถือเป็นปัญหาที่สำคัญอีกปัญหาหนึ่ง สินค้าละเมิดลิขสิทธิ์สามารถพบเห็นได้โดยทั่วไป ไม่ว่าจะเป็นซีดีเพลง วีซีดี และดีวีดีภาพยนตร์ ทั้งภาพยนตร์ไทยและต่างประเทศ เอกสารรายงานวิชาการ รวมไปถึงซอฟต์แวร์ เกม และโปรแกรมประยุกต์ต่างๆ ซึ่งสามารถพบเห็น และหาซื้อสินค้าละเมิดลิขสิทธิ์ได้โดยง่าย

ประเทศไทยอยู่ในอันดับต้นๆ ของประเทศที่มีปัญหาเรื่องการละเมิดลิขสิทธิ์ โดยในปีพ.ศ. 2550 นั้น ประเทศไทยมีการละเมิดลิขสิทธิ์สูงสุดเป็นอันดับ 4 ในเอเชียแปซิฟิก ส่งผลเสียต่อชื่อเสียงและอุตสาหกรรมต่างๆ ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ

7.3.9 ความผิดเกี่ยวกับการก่อการร้ายและต่อสถาบันพระมหากษัตริย์

พระราชบัญญัติการประกอบกิจการกระจายเสียงและกิจการโทรทัศน์ พ.ศ. 2551

- มาตรา 37

ห้ามมิให้ออกอากาศรายการที่มีเนื้อหาสาระที่ก่อให้เกิดการล้มล้างการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข หรือที่มีผลกระทบต่อความมั่นคงของรัฐ ความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน หรือมีการกระทำซึ่งเข้าลักษณะลามกอนาจาร หรือมีผลกระทบต่อการให้เกิดความเสื่อมทรามทางจิตใจ หรือสุขภาพของประชาชนอย่างร้ายแรง

ผู้รับใบอนุญาตมีหน้าที่ตรวจสอบ และให้ระงับการออกอากาศรายการที่มีลักษณะตามวรรคหนึ่ง หากผู้รับใบอนุญาตไม่ดำเนินการให้กรรมการซึ่งคณะกรรมการมอบหมายมีอำนาจสั่งด้วยวาจา หรือเป็นหนังสือให้ระงับการออกอากาศรายการนั้นได้ทันที และให้คณะกรรมการสอบสวนข้อเท็จจริงกรณีดังกล่าวโดยพลัน

ในกรณีที่คณะกรรมการสอบสวนแล้วเห็นว่าการกระทำดังกล่าวเกิดจากการละเลยของผู้รับใบอนุญาตจริง ให้คณะกรรมการมีอำนาจสั่งให้ผู้รับใบอนุญาตดำเนินการแก้ไขตามที่สมควร หรืออาจพักใช้หรือเพิกถอนใบอนุญาตก็ได้

7.3.10 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- มาตรา 14

ผู้ใดกระทำความผิดที่ระบุไว้ ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมด หรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4)

- มาตรา 15

ผู้ให้บริการผู้ใดจงใจสนับสนุน หรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

- มาตรา 16

ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูล คอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ ถ้าการกระทำตามวรรคหนึ่งเป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้ ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย [8]

7.4 กรณีศึกษาการบังคับใช้กฎหมาย

การบังคับใช้กฎหมายกับมือปราบโซเชียลเน็ตเวิร์ก

พ.ต.อ.นิเวศน์ อาภาวศิน ผู้กำกับการกลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร กล่าวถึงประเด็นปัญหาเรื่องการบังคับใช้ พ.ร.บ.คอมพิวเตอร์ฯ กับกรณีต่างๆ ที่เกิดขึ้นในระบบอินเทอร์เน็ต หรือเครือข่ายสังคมออนไลน์ประเภทต่างๆ ที่กำลังมีการถกเถียง วิพากษ์วิจารณ์กันอยู่

หากมีการปฏิบัติตาม หรือบังคับใช้กฎหมายฉบับดังกล่าวอย่างถูกต้องและจริงจังแล้ว ก็จะไม่เกิดประเด็นปัญหาอย่างทุกวันนี้ เนื่องจากกฎหมายฉบับนี้มีรายละเอียดครอบคลุมทั้งการป้องกันและปราบปรามอยู่แล้ว แต่การปฏิบัติของผู้ที่เกี่ยวข้องมุ่งเน้นไปที่การปราบปรามมากกว่า ทั้งที่หลักการแก้ไขปัญหาที่เกิดขึ้นซึ่งได้ผลที่ดีสุดคือการปฏิบัติตามหลักการของกฎหมายด้านการป้องกัน

นอกจากนี้ไม่ว่าจะเกิดคดีลักษณะใด สิ่งสำคัญที่สุด คือ การระบุตัวตนของผู้กระทำความผิดให้ได้เสียก่อน หากมีการร้องเรียนในเรื่องการกระทำผิดข้อหาต่างๆ ในระบบคอมพิวเตอร์เข้ามายังเจ้าหน้าที่ แต่เจ้าหน้าที่ไม่สามารถระบุตัวตนผู้กระทำความผิดได้ ก็ไม่มีประโยชน์ การที่เจ้าหน้าที่จะสามารถระบุตัวผู้ต้องสงสัยหรือระบุตัวตนของผู้นำข้อมูลเข้าสู่ระบบคอมพิวเตอร์ได้นั้น ต้องมีการจัดเก็บข้อมูลการใช้บริการอย่างถูกต้อง เป็นระบบ และมีประสิทธิภาพ

แต่ทุกวันนี้ทั้งเจ้าหน้าที่ภาครัฐและเอกชนที่รับผิดชอบได้บังคับใช้หรือปฏิบัติตามกฎหมายที่ระบุไว้หรือไม่ ผู้ให้บริการทั้งระบบคอมพิวเตอร์และโทรศัพท์เคลื่อนที่มีการจัดเก็บข้อมูลตามที่กฎหมายกำหนดหรือไม่ เจ้าหน้าที่ที่เกี่ยวข้องเข้าใจเจตนารมณ์ของกฎหมายและสามารถนำมาบังคับใช้อย่างมีประสิทธิภาพหรือไม่ การจัดเก็บข้อมูลตามกฎกระทรวงอาจเก็บมากเกินความจำเป็น และเป็นภาระแก่ผู้ให้บริการมากจนเกินไป ทั้งที่สาระสำคัญตาม พ.ร.บ.คอมพิวเตอร์ มาตรา 26 วรรคสอง ระบุว่า ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการ แต่ทุกวันนี้ผู้ให้บริการเก็บข้อมูลตามหลักเกณฑ์ของกฎกระทรวงเป็นหลัก โดยไม่ได้คำนึงถึงตัวพระราชบัญญัติ ซึ่งระบุไว้อย่างชัดเจนว่า เก็บเท่าที่จำเป็น แต่ต้องระบุตัวตนของผู้ใช้บริการให้ได้

หากผู้ให้บริการจัดเก็บข้อมูลโดยคัดเฉพาะผู้นำข้อมูลเข้าสู่ระบบคอมพิวเตอร์ และมีเจ้าหน้าที่ตรวจสอบข้อมูลเหล่านี้อย่างจริงจังแล้ว ก็เชื่อว่าปัญหาการกระทำผิดในระบบคอมพิวเตอร์จะดีขึ้น เพราะปัญหาทุกวันนี้เกิดจากผู้นำข้อมูลเข้าสู่ระบบคอมพิวเตอร์ หากเรามีการจัดเก็บข้อมูลเหล่านี้ดีอยู่แล้วก็จะทำให้การบังคับใช้กฎหมายทำได้อย่างมีประสิทธิภาพและประสิทธิผล

การรับเรื่องร้องเรียนเว็บไซต์ที่ผิดกฎหมาย แล้วใช้วิธีปิดกั้นนั้น เป็นมาตรการชั่วคราวเท่านั้น ไม่ใช่วิธีการแก้ปัญหา ซึ่งในระยะยาวจะมีผลกระทบต่อการให้บริการที่ล่าช้า ผู้ให้บริการส่วนใหญ่จึงไม่ค่อยเห็นด้วย และสุดท้ายก็ไม่สามารถจับกุมผู้กระทำผิดมาดำเนินคดีได้

อย่างไรก็ตาม พ.ต.อ.นิเวศน์ กล่าวว่า ในการบังคับใช้กฎหมายเพื่อเข้าถึงเนื้อหาข้อมูลในระบบคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่นั้น จะต้องขออนุมัติหมายจากศาล ในส่วนการตรวจสอบข้อมูลทั่วไปซึ่งไม่ใช่เนื้อหาการติดต่อสื่อสาร พนักงานสอบสวนสามารถใช้อำนาจตามประมวลกฎหมายวิธีพิจารณาความ

อาญา ออกหมายเรียกเพื่อขอข้อมูลจากผู้ที่เกี่ยวข้องได้ เช่น เรียกผู้ให้บริการมาสอบปากคำเพื่อให้ข้อมูล หรือส่งข้อมูลให้ แต่หากต้องลงลึกถึงเนื้อหาก็ต้องขอหมายศาล ซึ่งประเด็นเหล่านี้มีกำหนดไว้ในกฎหมายอยู่แล้ว

ทั้งนี้ กรณีของสื่อสังคมออนไลน์หรือแอพพลิเคชั่นแชทชื่อดังต่างๆ นั้น อยู่ที่ผู้ใช้จะเลือกใช้เป็นส่วนตัวหรือสาธารณะ ซึ่งผู้ใช้สามารถกำหนดได้ ถ้าไม่มีการแชร์ออกไปก็คงไม่มีปัญหา [9]

บรรณานุกรมประจำบทที่ 7

[1] 2550, “หลักเกณฑ์เกี่ยวกับคุณสมบัติพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐”, ราชกิจจานุเบกษา, เล่มที่ 124, ตอนพิเศษ 102 ง, 23 สิงหาคม 2550, หน้า 9-11.

[2] http://www.kodmhai.com/m2/m2-3/m3-77-90.html (สืบค้นเมื่อวันที่ 24 มิถุนายน 2556).

[3] thaiconsulatechicago.org/ebook/law/criminalcode1.pdf (สืบค้นเมื่อวันที่ 24 มิถุนายน 2556).

[4] 2540, “พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.๒๕๔๐”, ราชกิจจานุเบกษา, เล่มที่ 114, ตอนที่ 46 ก, 10 กันยายน 2540, หน้า 6.

[5] พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ.๒๕๑๙, หน้า 7-8

[6] 2550, “รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.๒๕๕๐”, ราชกิจจานุเบกษา, เล่มที่ 124, ตอนที่ 47 ก, 24 สิงหาคม 2550, หน้า 9-10.

[7] http://www.th.wikipedia.org/wiki/ทรัพย์สินทางปัญญา (สืบค้นเมื่อวันที่ 24 มิถุนายน 2556).

[8] 2550, “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐”, ราชกิจจานุเบกษา, เล่มที่ 124, ตอนที่ 27 ก, 18 มิถุนายน 2550, หน้า 7.

[9] http://www.komchadluek.net/detail/20130815 (สืบค้นเมื่อวันที่ 15 สิงหาคม 2556).

บทที่ 8 การใช้เทคโนโลยีสารสนเทศและการสื่อสารอย่างสร้างสรรค์

ปัจจุบันเทคโนโลยีสารสนเทศเพื่อการสื่อสารมีความก้าวหน้าไปอย่างรวดเร็ว ถูกนำมาใช้แลกเปลี่ยนข้อมูลอย่างกว้างขวาง และเป็นเครื่องมือที่มีประสิทธิภาพ หากนำไปใช้ในเชิงสร้างสรรค์ ซึ่งมีแนวทางและหลักการในการใช้ ดังนี้

<u>หลักการและแนวปฏิบัติทั่วไป</u>

1) ผู้ใช้งานสังคมออนไลน์ สามารถ เผยแพร่ ประชาสัมพันธ์ข้อมูลที่เป็นประโยชน์ได้ แต่ต้องแยกแยะให้ชัดเจนว่า ข้อความใดเป็น “ข่าวประชาสัมพันธ์” “ความคิดเห็น” “ความคิดเห็นส่วนบุคคล” “การแลกเปลี่ยนข่าวสารส่วนตัว” “การเผยแพร่ข่าวสารเรื่องงาน” หรืออื่นๆ และความคิดเห็นดังกล่าวควรคำนึงถึงประโยชน์สาธารณะด้วย
2) การเผยแพร่ประชาสัมพันธ์ที่ประชาสัมพันธ์ในนามของหน่วยงาน ผู้เผยแพร่ต้องแสดงตำแหน่งหน้าที่ สังกัด ให้ชัดเจน เพื่อความน่าเชื่อถือ และเพื่อให้ผู้ที่ติดตามสามารถใช้ดุลพินิจในการติดตามได้
3) ระมัดระวังการใช้ถ้อยคำและภาษา ที่อาจเป็นการดูหมิ่น หรือ หมิ่นประมาทบุคคลอื่น และควรใช้ภาษาให้ถูกต้อง สุภาพ สร้างสรรค์
4) งดเว้นการโต้ตอบ ด้วยความรุนแรง กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง การละเว้นไม่โต้ตอบจะทำให้ความขัดแย้งไม่บานปลายจนหาที่สิ้นสุดไม่ได้
5) งดเว้นการใช้สื่อสังคมวิพากษ์ วิจารณ์ ตลอดจนแสดงความเห็นที่อาจส่งผลกระทบได้
6) ใช้รูปแสดงตัวตนที่แท้จริง และงดเว้นการนำรูปบุคคลอื่น รูปบุคคลสาธารณะ มาแสดงว่าเป็นรูปของตนเอง เว้นแต่เป็นสื่อสังคมในนามตัวแทนบุคคลอื่น
7) องค์กร หรือ แผนกงานที่สังกัด อาจใช้รูปสัญลักษณ์ เครื่องหมายแสดงสังกัดได้ แต่ต้องคำนึงถึงความเหมาะสมในการใช้งาน
8) ระมัดระวังข้อความที่ส่งผลกระทบต่อเด็ก สตรี หรือ การละเมิดสิทธิมนุษยชน
9) การใช้สื่อสังคมที่แสดงสังกัด หรือหน่วยงาน ควรแจ้งให้ผู้บังคับบัญชาทราบก่อนทุกครั้ง

<u>หลักการส่งต่อข้อมูล</u>

1) ควรส่งข้อมูลข่าวสารเฉพาะบุคคลที่รู้จัก แสดงตัวตน ตำแหน่ง หน้าที่การงาน สถานะที่ชัดเจนเท่านั้น
2) ละเว้นการส่งข้อมูลที่เป็นข่าวลือ ข่าวไม่ปรากฏที่มา หรือเป็นเพียงการคาดเดา
3) งดเว้นการส่งต่อข้อความเกี่ยวข้องกับสถาบันทุกกรณี ยกเว้น ข้อความนั้นๆ เป็นข้อความที่เผยแพร่จากหน่วยงานที่เกี่ยวข้อง และมีแหล่งที่มา เพื่อประโยชน์ต่อสาธารณะ
4) พึงระลึกเสมอว่า การส่งต่อข้อความที่เป็นเท็จ หรือ ข้อความที่เจ้าของประสงค์กระจายข่าวสร้างความสับสน วุ่นวายในบ้านเมือง เท่ากับตกเป็นเครื่องมือของบุคคลเหล่านั้น
5) ควรงดเว้นการส่งต่อข้อความเรื่องบุคคลเสียชีวิต เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้ว
6) การส่งต่อข้อความเชิญชวนไปร่วมชุมนุม หรือ กระทำกิจกรรมทางสังคมใดๆ ต้องตรวจสอบข้อเท็จจริงให้แน่ชัดเสียก่อน

หลักความรับผิดชอบ

1) ควรแสดงความรับผิดชอบ ด้วยการขอโทษ แสดงความเสียใจทันที เมื่อรู้ว่า มีการเผยแพร่ข้อมูลที่ผิดพลาดหรือกระทบต่อบุคคลอื่น
2) กรณีการส่งต่อข้อความข่าวลือ หรือ ข่าวเท็จ ต้องแก้ไขข้อความนั้นโดยทันที หากสามารถตรวจสอบข้อเท็จจริงได้ พึงแสดงข้อเท็จจริงให้เป็นที่ประจักษ์

8.1 การใช้และการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารอย่างสร้างสรรค์

8.1.1 การประยุกต์ใช้เทคโนโลยีสารสนเทศในสำนักงาน

1) งานจัดเตรียมเอกสาร เช่น การใช้เครื่องประมวลผลคำหรือเครื่องประมวลผลเนื้อหาเป็นเครื่องมือในการจัดเตรียมอุปกรณ์ ประกอบการใช้เทคโนโลยีนี้ ได้แก่ เครื่องคอมพิวเตอร์ โมเด็มและช่องทางการสื่อสาร
2) งานกระจายเอกสาร เช่น ระบบเครือข่ายคอมพิวเตอร์ เทเลเท็กซ์ โทรสาร ระบบการประชุมทางไกล เป็นต้น
3) งานจัดเก็บและค้นคืนเอกสาร สามารถปฏิบัติได้ทั้งระบบออนไลน์และระบบออฟไลน์ ผ่านระบบเครือข่ายคอมพิวเตอร์ หรือผ่านเครือข่าย โทรคมนาคมรูปแบบอื่นๆ เช่น ระบบงานฐานข้อมูล เป็นต้น
4) งานจัดเตรียมสารสนเทศในลักษณะภาพ เทคโนโลยีสารสนเทศที่สามารถดำเนินงานดังกล่าวนี้ได้ ได้แก่ เครื่องคอมพิวเตอร์ สร้างภาพ (Computer Graphic Devices) เครื่อง Scanner โทรทัศน์ และ วีดีทัศน์ เป็นต้น
5) งานสื่อสารสนเทศด้วยเสียง เช่น การใช้โทรศัพท์ การประชุมทางโทรศัพท์ การบันทึกข้อมูลเสียงโดยใช้ Sound Blaster เป็นต้น
6) งานสื่อสารสนเทศด้วยภาพและเสียง เช่น ระบบมัลติมีเดีย ระบบการประชุมทางไกลด้วยภาพและเสียง เป็นต้น

8.1.2 การประยุกต์ใช้เทคโนโลยีสารสนเทศในงานอุตสาหกรรม

1) อุตสาหกรรมการผลิตภัณฑ์ ได้ใช้คอมพิวเตอร์ออกแบบ รถยนต์ ปฏิบัติการผลิต เช่น การพ่นสี การเชื่อมอุปกรณ์ต่างๆ เข้าด้วยกัน ฯลฯ
2) อุตสาหกรรมการพิมพ์ เช่นระบบการพิมพ์อิเล็กทรอนิกส์ (Electronic Publishing) ในการจัดเตรียมต้นฉบับบรรณาธิกร ตีพิมพ์ จัดเก็บ และจัดจำหน่าย และสามารถพิมพ์ข้อมูลจากระบบไปรษณีย์อิเล็กทรอนิกส์ (E-mail) วีดีโอเท็กซ์ วัสดุย่อส่วนและเทเลเท็กซ์ได้รวมทั้งการพิมพ์ภาพโดยใช้เทอร์มินัลเสนอภาพ (Visual Display)
3) การประยุกต์ใช้เทคโนโลยีสารสนเทศในงานการเงินและการพาณิชย์ สถาบันการเงิน เช่น ธนาคาร ได้ใช้เทคโนโลยีสารสนเทศในรูปแบบของ ATM เพื่ออำนวยความสะดวกในการฝาก ถอน โอนเงิน ในส่วนของงานประจำของธนาคารต่างนำคอมพิวเตอร์ระบบออนไลน์และออฟไลน์เข้ามาช่วยปฏิบัติงาน ทำให้การเชื่อมโยงข้อมูลธนาคารเป็นไปอย่างสะดวกรวดเร็ว ทุกสาขาสามารถเชื่อมโยงกับสาขาอื่นหรือสำนักงานใหญ่ และสามารถเชื่อมโยงกับธนาคารอื่นได้

4) การประยุกต์ใช้เทคโนโลยีสารสนเทศในงานการบริการการสื่อสาร ได้แก่ การบริการโทรศัพท์ โทรศัพท์เคลื่อนที่ วิทยุ โทรทัศน์ เคเบิลทีวี การค้นคืนสารสนเทศระบบออนไลน์ ดาวเทียม และโครงข่ายบริการสื่อสารร่วมระบบดิจิตอล (ISDN) เป็นต้น

8.1.3 การประยุกต์ใช้เทคโนโลยีสารสนเทศกับงานด้านการฝึกอบรมและการศึกษา

1) การใช้คอมพิวเตอร์ช่วยสอน (Computer Assisted Instruction : CAI) เช่น การนำเอาคำอธิบายบทเรียนมาบรรจุไว้ในคอมพิวเตอร์ แล้วนำบทเรียนนั้นมาแสดงแก่ผู้เรียน
2) การศึกษาทางไกล เช่น การใช้วิทยุ โทรทัศน์ ออกอากาศให้ ผู้เรียนศึกษาเอง จนไปถึงการใช้ระบบแพร่ภาพผ่านดาวเทียม (Direct To Home : DTH) หรือการประยุกต์ใช้ระบบประชุมทางไกล (Video Teleconference)
3) เครือข่ายการศึกษา เช่น บริการ ส่งจดหมายอิเล็กทรอนิกส์ (Electronics Mail : E-mail) การเผยแพร่และค้นหาข้อมูลในระบบเวิลด์ไวด์เว็ป
4) การใช้งานในห้องสมุด เช่น การค้นหาหนังสือ การจัดหนังสือ
5) การใช้ในห้องปฏิบัติการ เช่น การจำลองแบบ การออกแบบวงจรไฟฟ้า การควบคุมการทดลอง
6) การใช้ในงานประจำและงานบริหาร เช่น การจัดทำทะเบียนประวัตินักเรียนนักศึกษา การเลือกเรียน การลงทะเบียนเรียน การแนะแนวอาชีพ และการศึกษาต่อ ข้อมูลผู้ปกครองหรือข้อมูลของครู
7) การประยุกต์ใช้เทคโนโลยีสารสนเทศที่บ้าน เช่น ใช้คอมพิวเตอร์ในแสวงหาความรู้ ใช้สื่อสารทาง Internet ใช้พิมพ์งานและจัดเก็บข้อมูลที่สำคัญ [1]

8.2 การแลกเปลี่ยนเรียนรู้ในสังคมออนไลน์

เป็นการเรียนรู้ด้วยตัวเองผ่านเครือข่ายคอมพิวเตอร์อินเทอร์เน็ต (Internet) หรืออินทราเน็ต (Intranet) ผู้เรียนจะได้เรียนตามความสามารถและความสนใจของตน โดยเนื้อหาของบทเรียนจะถูกส่งไปยังผู้เรียนผ่านเว็บเบราว์เซอร์(Web Browser) โดยผู้เรียน ผู้สอน และเพื่อนร่วมชั้นเรียนทุกคน สามารถติดต่อปรึกษา แลกเปลี่ยนความคิดเห็นระหว่างกันได้เช่นเดียวกับการเรียนในชั้นเรียนปกติ โดยอาศัยเครื่องมือการติดต่อสื่อสารที่ทันสมัยสำหรับทุกคนที่สามารถเรียนรู้ได้ทุกเวลา และทุกสถานที่ (Learn for all : anyone, anywhere and anytime) ซึ่งการให้บริการการเรียนแบบออนไลน์ มีองค์ประกอบที่สำคัญ 4 ส่วน แต่ละส่วนได้รับการออกแบบเป็นอย่างดี เมื่อนำมาประกอบเข้าด้วยกัน แล้วระบบทั้งหมดจะต้องทำงานประสานกันได้อย่างลงตัว ดังนี้

1) เนื้อหาของบทเรียน ประกอบด้วย ข้อความ รูปภาพ เสียง วิดีโอและมัลติมีเดียอื่นๆ

2) ระบบบริหารการเรียน ทำหน้าที่เป็นศูนย์กลาง กำหนดลำดับของเนื้อหาในบทเรียน เราเรียกระบบนี้ว่า ระบบบริหารการเรียน (E-Learning Management System : LMS) ดังนั้น ระบบบริหารการเรียนจึงเป็นส่วนที่เอื้ออำนวยให้ผู้เรียนได้ศึกษาเรียนรู้ได้ด้วยตนเองจนจบหลักสูตร

3) การติดต่อสื่อสาร นำรูปแบบการติดต่อสื่อสารแบบ 2 ทาง มาใช้ประกอบในการเรียน โดย

เครื่องมือที่ใช้ในการติดต่อสื่อสารอาจแบ่งได้เป็น 2 ประเภทคือ ประเภท Real-time ได้แก่ Chat (message, voice), White board/Text slide, Real-time Annotations, Interactive poll, Conferencing และอื่นๆ ส่วนอีกแบบคือ ประเภท Non real-time ได้แก่ Web-board, E-mail

4) บทเรียนคอมพิวเตอร์ช่วยสอน (Computer Assisted Instruction - CAI)

บทเรียนคอมพิวเตอร์ช่วยสอนจะเสนอสารสนเทศที่ได้ผ่านกระบวนการสร้าง และพิจารณามาเป็นอย่างดี โดยมีเนื้อหาวิชาหรือสารสนเทศ แบบฝึกหัด การทดสอบ และการให้ข้อมูลป้อนกลับให้ผู้เรียนได้ตอบสนองต่อบทเรียนได้ตามระดับความสามารถของตนเอง เนื้อหาวิชาที่นำเสนอจะอยู่ในรูปมัลติมีเดีย ซึ่งประกอบด้วย อักษร รูปภาพ เสียง และหรือ ทั้งภาพและเสียง โดยมีจุดมุ่งหมายนำผู้เรียนไปสู่การเรียนรู้อย่างมีประสิทธิภาพ ซึ่งอาศัยการสอนที่มีการวางโปรแกรมไว้ล่วงหน้า เป็นการให้ผู้เรียนมีโอกาสเรียนรู้ได้ด้วยตนเอง และมีผลย้อนกลับทันทีและเรียนรู้ไปทีละขั้นตอนอย่างเหมาะสม ตามความต้องการและความสามารถของตน

5) วีดิทัศน์ตามอัธยาศัย (Video on Demand - VOD)

การจัดการฐานข้อมูลต้องอาศัยโปรแกรมที่ทำหน้าที่ ในการกำหนดลักษณะข้อมูลที่จะเก็บไว้ในฐานข้อมูล อำนวยความสะดวกในการบันทึกข้อมูลลงในฐานข้อมูล กำหนดผู้ที่ได้รับอนุญาตให้ใช้ฐานข้อมูลได้ พร้อมกับกำหนดด้วยว่าให้ใช้ได้แบบใด เช่น ให้อ่านข้อมูลได้อย่างเดียวหรือให้แก้ไขข้อมูลได้ด้วย นอกจากนั้นยังอำนวยความสะดวกในการค้นหาข้อมูล การแก้ไขปรับปรุงข้อมูล ตลอดจนการจัดทำข้อมูลสำรองด้วย โดยอาศัยโปรแกรมที่เรียกว่า ระบบการจัดการฐานข้อมูล(Database Management System: DBMS) ซึ่งโปรแกรมที่ได้รับความนิยมในการจัดการฐานข้อมูล ได้แก่ Microsoft Access, Oracle, Informix, dBase, FoxPro, และ Paradox เป็นต้น

6) หนังสืออิเล็กทรอนิกส์ (E-books)

หนังสืออิเล็กทรอนิกส์ที่สามารถอ่านได้ทางอินเทอร์เน็ต สำหรับเครื่องมือที่จำเป็นต้องมีในการอ่านหนังสือประเภทนี้ก็คือ ฮาร์ดแวร์ประเภทเครื่องคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์พกพาอื่นๆ พร้อมทั้งติดตั้งระบบปฏิบัติการหรือซอฟต์แวร์ที่ใช้อ่านข้อความต่างๆ ตัวอย่างเช่น ออแกไนเซอร์แบบพกพา พีดีเอ เป็นต้น ส่วนการดึงข้อมูล E-books ซึ่งจะอยู่บนเว็บไซต์ที่ให้บริการทางด้านนี้มาอ่าน ก็จะใช้วิธีการดาวน์โหลดผ่านทางอินเทอร์เน็ตเป็นส่วนใหญ่

ลักษณะไฟล์ของ E-books หากนักเขียนหรือสำนักพิมพ์ต้องการสร้าง E-books จะสามารถเลือกได้สี่รูปแบบ คือ Hyper Text Markup Language (HTML), Portable Document Format (PDF), Peanut Markup Language (PML) และ Extensive Markup Language (XML)

7) ห้องสมุดอิเล็กทรอนิกส์ (E-library)

บริการงานห้องสมุดระบบอัตโนมัติ เช่น

1) ระบบที่สามารถให้บริการและตรวจสอบได้

2) ระบบบริการยืม - คืน ทรัพยากรด้วยแถบรหัสบาร์โค้ด

3) ระบบบริการสืบค้นข้อมูลทรัพยากร

4) ระบบตรวจเช็คสถิติการใช้บริการห้องสมุด

5) ระบบตรวจเช็คสถิติการยืม - คืนทรัพยากร

6) การสำรวจทรัพยากรประจำปี

7) การพิมพ์บาร์โค้ดทรัพยากรและสมาชิก[2]

8.3 กรณีศึกษาเกี่ยวกับการใช้เทคโนโลยีสารสนเทศอย่างสร้างสรรค์

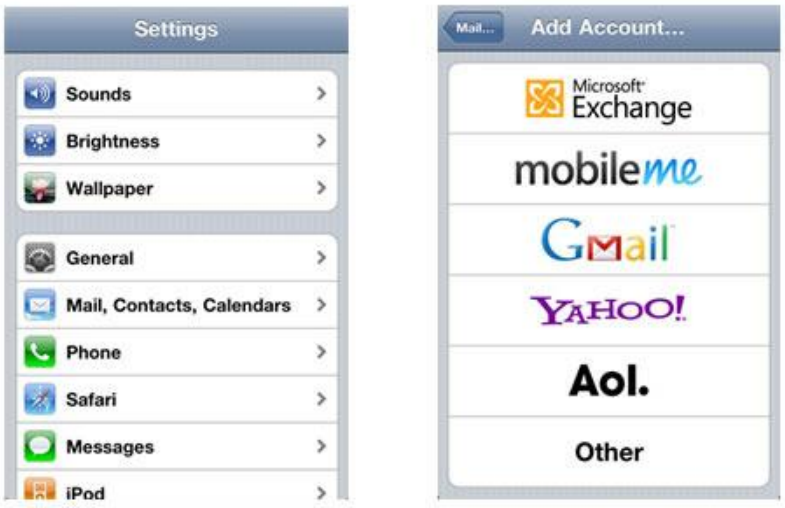
ปัจจุบันด้วยเทคโนโลยีที่ทันสมัยประกอบกับ โทรศัพท์มือถือแบบสมาร์ทโฟนในปัจจุบันติดตั้ง GPS Receiver มาแทบจะทุกเครื่องแล้ว ทำให้เมื่อโทรศัพท์มือถือหายหรือถูกขโมยไป ก็สามารถตามหาได้ไม่ยาก อย่างเช่นกรณี ที่สิงคโปร์เมื่อชายวัย 18 ปีได้ขโมย iPhone จากเหยื่อผู้เคราะห์ร้าย แต่ด้วยบริการ Find My iPhone ก็ทำให้ตำรวจสามารถตามรอยคนร้ายและจับกุมได้ภายใน 48 ชั่วโมง ส่วนในประเทศไทย ก็มีกรณีที่ iPad ของชายผู้หนึ่งหายไป และสามารถตามจนเจอได้ด้วยบริการ Find my iPhone นี้เช่นกัน และก็ได้กลับคืนมาในที่สุด เราจึงขอแนะนำบริการดีๆฟรีๆใกล้ตัว ที่จะช่วยให้ตามหาอุปกรณ์มือถือที่หายไปได้ 2 บริการด้วยกัน ครอบคลุมทั้งผู้ใช้ iPhone, iPad, iPod Touch, Blackberry, Android และ Windowsmobile ซึ่งหวังว่าจะเป็นประโยชน์ต่อท่านผู้อ่านที่เป็นเจ้าของอุปกรณ์เหล่านี้

1) Find my iPhone จาก Apple

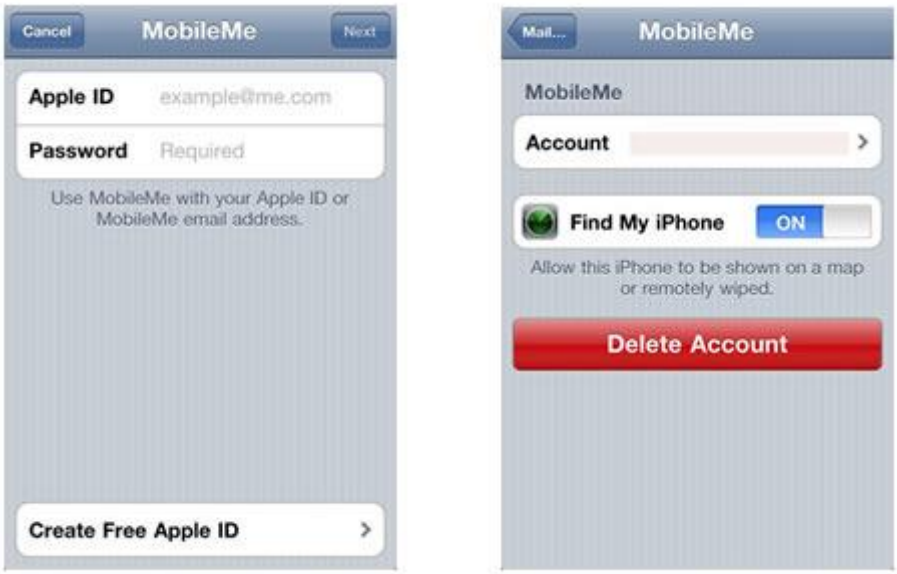
ก่อนหน้านี้ ผู้ที่จะสามารถใช้บริการนี้ได้ต้องเป็นสมาชิก Mobile Me ซึ่งเสียเงินเสียก่อน แต่ปัจจุบันนี้ ทาง Apple เปิดให้ใช้ได้แบบฟรีๆกันแล้วสำหรับอุปกรณ์ iPhone, iPad, iPod ที่ใช้ระบบปฏิบัติการ iOS 4.2 ขึ้นไป (แต่สำหรับ version ที่ต่ำกว่านี้ก็สามารถใช้ผ่านบริการ Mobile Me แบบเสียเงินได้อยู่ บริการนี้นอกจากจะช่วยให้เราสามารถหาว่าเครื่องเราอยู่ที่ไหนในตอนนี้แล้ว ยังสามารถสั่งให้ส่งข้อความให้ขึ้นที่หน้าจอของอุปกรณ์ที่เราตามหา, สั่งให้เครื่องส่งเสียงดังขึ้น แม้จะอยู่ใน Silent Mode ก็ตาม, สั่งให้เครื่อง Lock และตั้ง Password ไว้ หรือกรณีที่เราคิดว่าคงไม่ได้อุปกรณ์นั้นๆคืนแล้ว ก็ป้องกันข้อมูลสำคัญรั่วไหลด้วยการสั่งลบข้อมูลทั้งหมดไปเลยก็ได้

<u>วิธีการติดตั้ง</u>

เข้าไปที่ Settings > Mail, Contacts, Calendars >เลือก Mobile Me >ใส่ Apple ID ของเรา (ซึ่งก็คือ ID เดียวกันกับที่เราใช้ใน iTune และ Appstore) ซึ่งถ้าหากยังไม่มี Apple ID ก็สามารถกดสร้าง Free Account ได้ > และสั่งเปิด “Find My iPhone” on



รูปที่ 8-1 วิธีการติดตั้ง Find my iPhone



รูปที่ 8-2 วิธีการติดตั้ง Find my iPhone 2

เพียงเท่านี้ เมื่อ iPhone, iPod Touch 4th Gen หรือ iPad ที่เปิดใช้บริการ Find My iPhone ได้หายไป ก็สามรถตามหาได้ด้วยวิธีง่ายดังนี้ (แต่ถ้าหากอุปกรณ์ที่เราตามหา ไม่ได้สั่งให้ “Find My iPhone” เป็น “on” เอาไว้ก็ไม่สามารถที่จะระบุตำแหน่งของอุปกรณ์นั้นๆได้เมื่อหายไป หรือถ้าหากสั่งปิดการ push หรือปิดเครื่องไปแล้ว ก็ตามหาไม่ได้เช่นกัน)

2) โปรแกรม Lookout

Lookout เป็นโปรแกรมด้าน backup ข้อมูลต่าง รองรับทั้ง Blackberry android และ windowsmobile และต้องรองรับการต่อ GPS ด้วย (ยกเว้น windowsphone7) โปรแกรมนี้รองรับการ backup ข้อมูล , การสแกนพวกไวรัสมัลแวร์บนมือถือ และ ตามหามือถือคุณด้วย GPS ผ่านทางหน้าเว็บไซต์

ได้ เวลาเราเผลอลืมมือถือไว้ หรือโทรศัพท์มือถือหาย ก็เปิดคอมพิวเตอร์หรือโทรศัพท์มือถือหรือ tablet เครื่องอื่น แล้วเข้าเว็บไซต์ www.mylookout.com ทำการ login เข้าสู่ระบบ ด้วยอีเมลที่คุณได้สมัครไว้ ซึ่งก็จะคล้ายกันกับการใช้บริการตามหา iPhone, iPad, iPod Touch ใน Mobile Me จาก Apple

บรรณานุกรมประจำบทที่ 8

[1] http://www.hpk.ac.th/hpk3/grouplearning/tecnology/songkrant/ict/technology3.htm (สืบค้นเมื่อวันที่ 15 กรกฎาคม 2556)

[2] http://www.pbj.ac.th/IT11/C8.htm (สืบค้นเมื่อวันที่ 15 กรกฎาคม 2556)**.**

บทที่ 9 ระบบการสื่อสารและการแจ้งภัยออนไลน์ของลูกเสือไซเบอร์

9.1 ระบบข้อมูลสมาชิก

ท่านที่สนใจเข้าร่วมเป็นสมาชิกลูกเสือไซเบอร์ สามารถเข้าสมัครสมาชิกได้ที่ www.cyberscout.in.th

การใช้งานเว็บไซต์ Cyber Scout ในส่วนของการสมัครสมาชิกสามารถเข้าได้ที่ปุ่มสมาชิก หรือเข้าได้ที่ www.cyberscout.in.th ดังรูป

รูปที่ 9-1 หน้าแรกของเว็บไซต์

ขั้นตอนการสมัครสมาชิก

หน้าสมัครสมาชิกมีอยู่ 2 ประเภท คือ

- สมาชิกแกนนำ Cyber Scout
- สมาชิกอาสาสมัคร Cyber Scout

โดยมีรายละเอียดการสมัครสมาชิก ดังต่อไปนี้

- การสมัครสมาชิกแกนนำ Cyber Scout

ขั้นตอนที่ 1 ให้แกนนำเลือกเมนู **“สมัครสมาชิก”** ดังรูป

รูปที่ 9-2 หน้าจอสำหรับสมัครสมาชิก

ขั้นตอนที่ 2 ให้คลิกเลือกที่ **“สมาชิกแกนนำ Cyber Scout (สำหรับ ครู/อาจารย์)”** ดังรูป

รูปที่ 9-3 หน้าจอสำหรับสมัครสมาชิกแกนนำ Cyber Scout

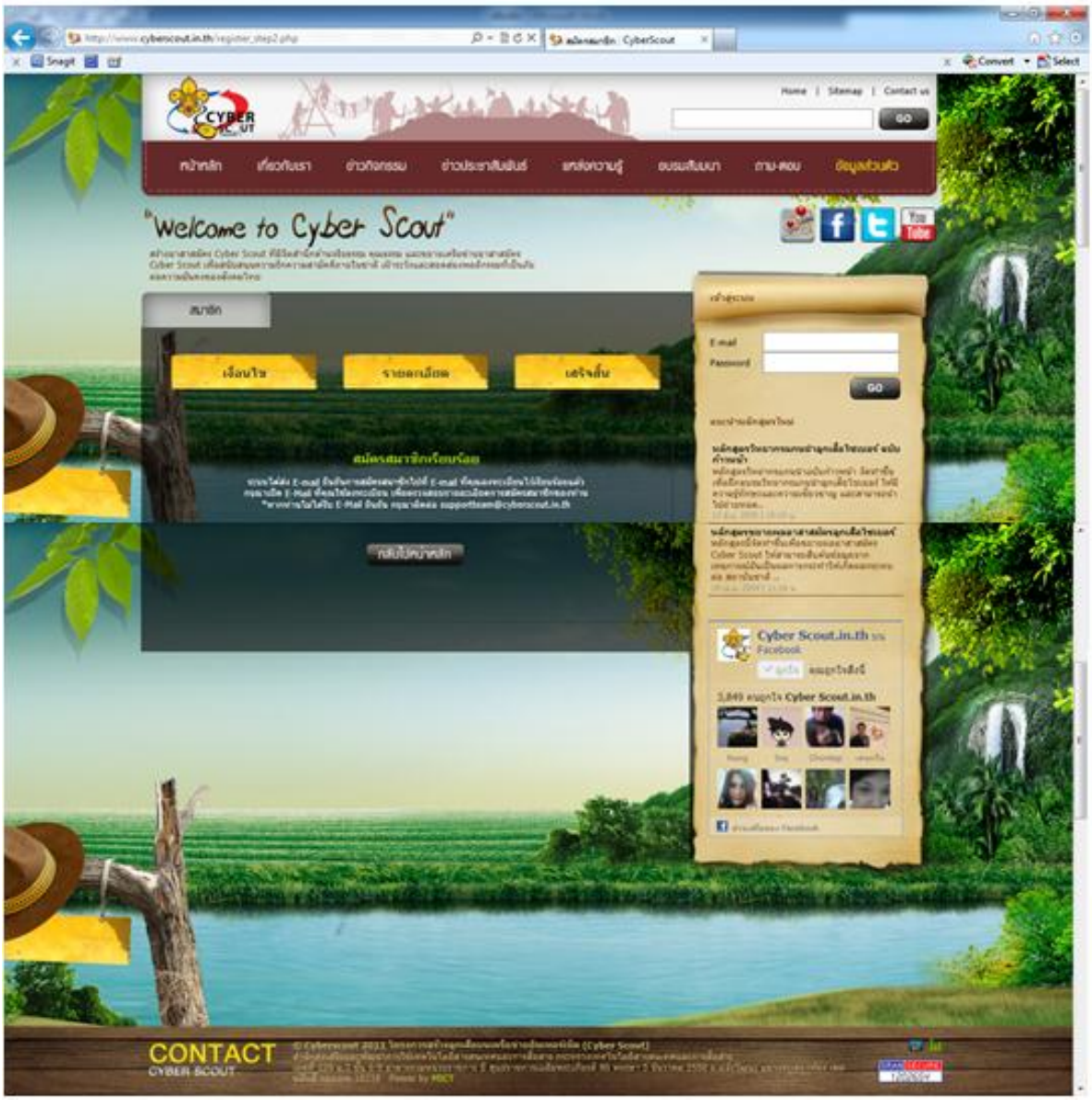
ขั้นตอนที่ 3 เว็บไซต์จะแสดงเงื่อนไขสำหรับการสมัครสมาชิกแกนนำ Cyber Scout หากสมาชิกแกนนำยอมรับเงื่อนไขของโครงการฯ ได้ให้กดปุ่ม **“ตกลง”**เพื่อเข้าสู่หน้ารายละเอียดการสมัครดังรูป

รูปที่ 9-4 หน้าจอเงื่อนไขการสมัครสมาชิกแกนนำ Cyber Scout

ขั้นตอนที่ 4 เมื่อเข้าสู่หน้ารายละเอียดการสมัครจะมีหน้าตาแสดงผล กรอกข้อมูลให้ครบถ้วนแล้วคลิกที่ **“ตกลง”** ดังรูป

รูปที่ 9-5 หน้าจอแสดงรายละเอียดสำหรับการสมัครสมาชิกแกนนำ Cyber Scout

เมื่อทำการสมัครแกนนำ Cyber Scout เรียบร้อยแล้ว ผู้สมัครจะไม่สามารถเข้าสู่ระบบได้จนกว่าผู้ดูแลระบบจะทำการตรวจสอบข้อมูลเสร็จ ผู้สมัครจะได้รับรหัสผ่านจาก Cyber Scout ทางอีเมลของผู้สมัคร มีหน้าจอดังรูป



รูปที่ 9-6 หน้าจอรายละเอียดสำหรับการสมัครสมาชิกแกนนำ Cyber Scout เสร็จสิ้น

- การสมัครสมาชิกอาสาสมัคร Cyber Scout

ขั้นตอนที่ 1 ให้อาสาสมัครเลือกเมนู **“สมัครสมาชิก”** ดังรูป

รูปที่ 9-7 หน้าจอสำหรับสมัครสมาชิก

ขั้นตอนที่ 2 ให้คลิกเลือกที่ **“สมาชิกอาสาสมัคร Cyber Scout (สำหรับ นักเรียน/บุคคลที่สนใจ)** ดังรูป

รูปที่ 9-8 หน้าจอสำหรับสมัครสมาชิกอาสาสมัคร Cyber Scout

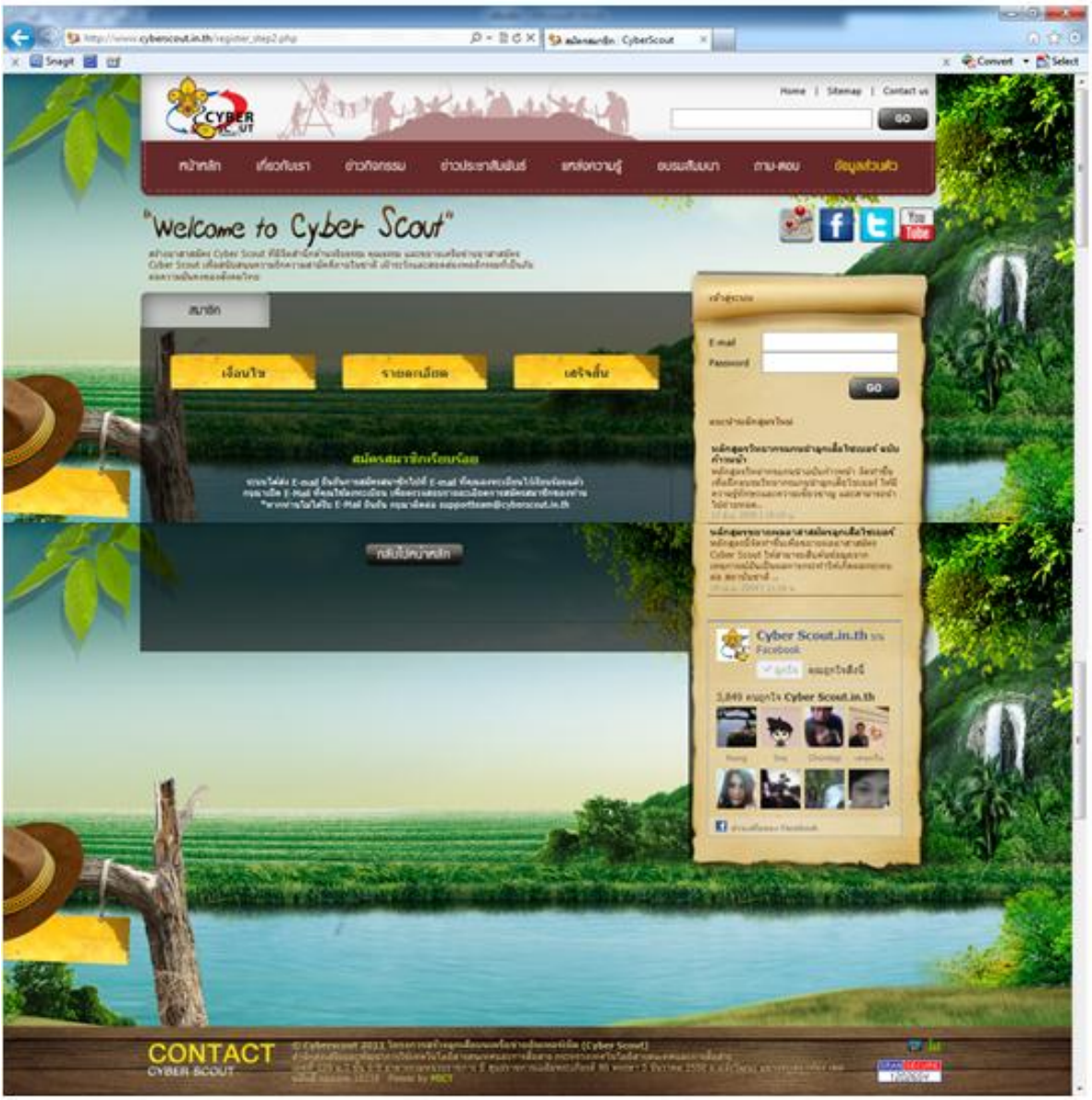
ขั้นตอนที่ 3 เว็บไซต์จะแสดงเงื่อนไขสำหรับการสมัครสมาชิกอาสาสมัคร Cyber Scout ให้กดปุ่ม **“ตกลง”** เพื่อเข้าสู่หน้ารายละเอียดการสมัคร ดังรูป

รูปที่ 9-9 หน้าจอเงื่อนไขการสมัครสมาชิกอาสาสมัคร Cyber Scout

ขั้นตอนที่ 4 เมื่อเข้าสู่หน้ารายละเอียดการสมัครจะมีหน้าตาแสดงผล กรอกข้อมูลให้ครบถ้วนแล้วคลิกที่ **“ตกลง”** ดังรูป

รูปที่ 9-10 หน้าจอแสดงรายละเอียดสำหรับการสมัครสมาชิก Cyber Scout

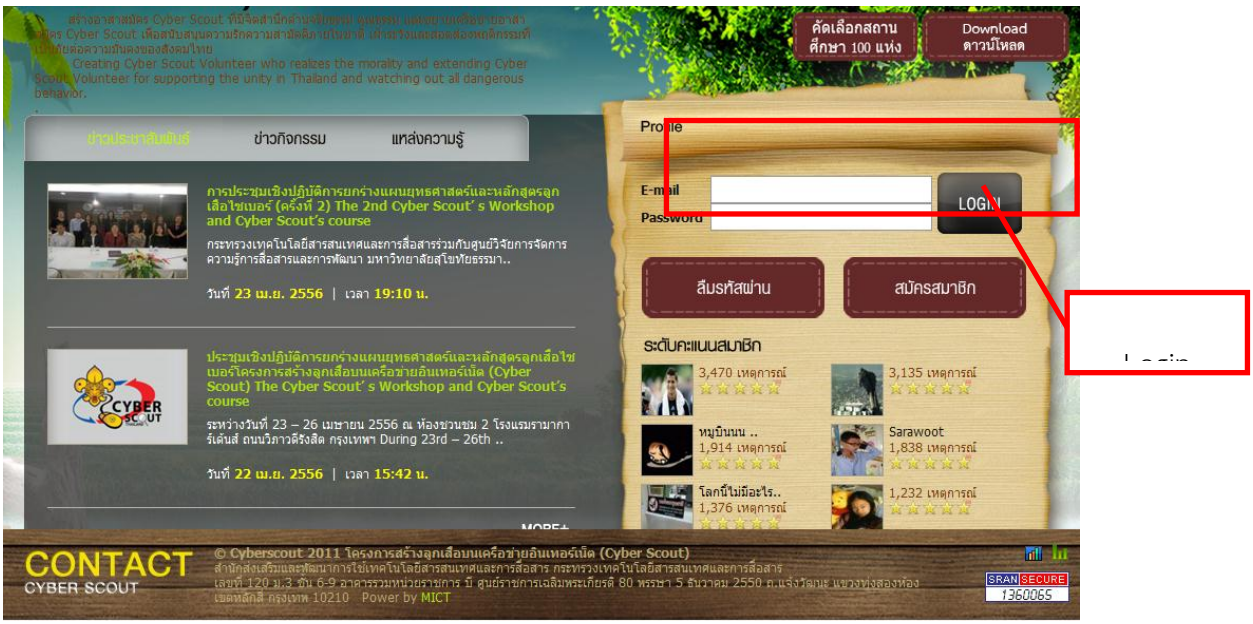
เมื่อทำการสมัครอาสาสมัคร Cyber Scout เรียบร้อยแล้ว ผู้สมัครจะไม่สามารถเข้าสู่ระบบได้ จนกว่าผู้ดูแลระบบจะทำการตรวจสอบข้อมูลเสร็จ ผู้สมัครจะได้รับรหัสผ่านจาก Cyber Scout ทางอีเมลล ของผู้สมัคร มีหน้าจอดังรูป



รูปที่ 9-11 หน้าจอรายละเอียดสำหรับการสมัครสมาชิก Cyber Scout เสร็จสิ้น

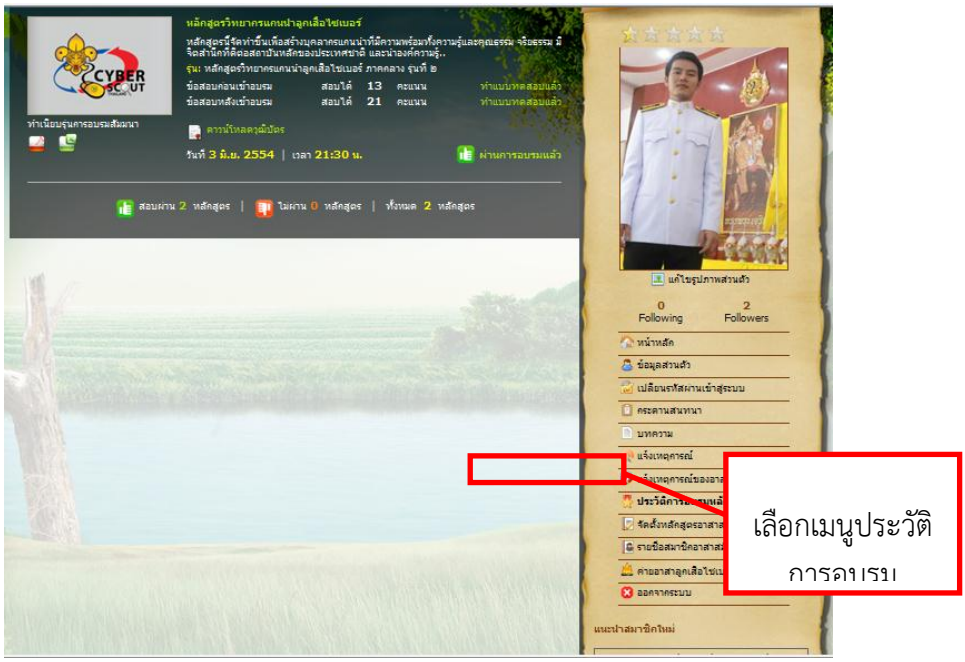
9.2 ระบบหลักสูตรและการฝึกอบรม

ขั้นตอนที่ 1 Log in เข้าสู่ระบบ



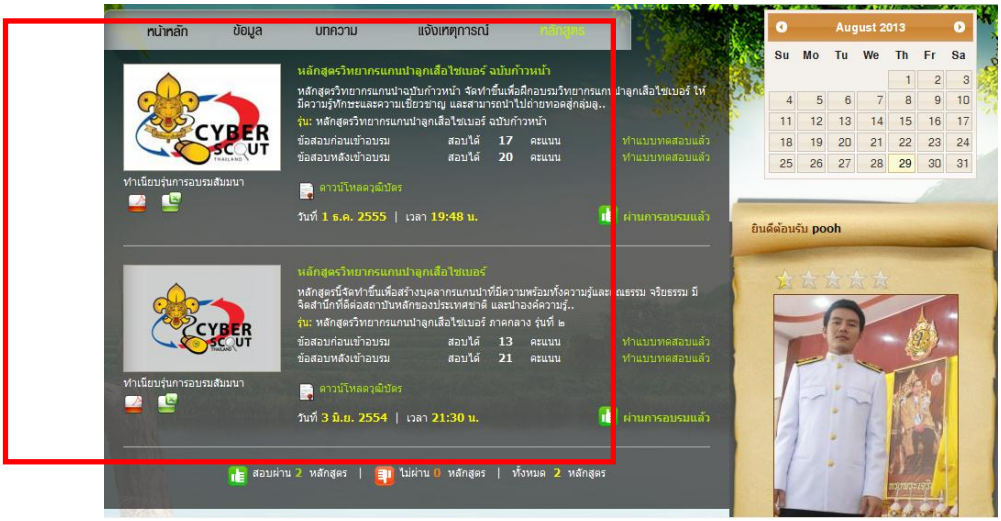
รูปที่ 9-11 หน้าจอการเข้าระบบสมาชิก

ขั้นตอนที่ 2 เมื่อเข้าสู่ระบบเรียบร้อยแล้ว ให้เลือกเมนู “ประวัติการอบรมหลักสูตร”



รูปที่ 9-12 ภาพเมนูประวัติการอบรมหลักสูตร

เมื่อเลือกเมนูประวัติการอบรมหลักสูตรแล้วจะพบหน้าต่างดังภาพ หน้าต่างนี้แสดงถึงข้อมูลหลักสูตรและการฝึกอบรมที่กระทำอยู่ ณ ปัจจุบันและที่ผ่านมาแล้ว



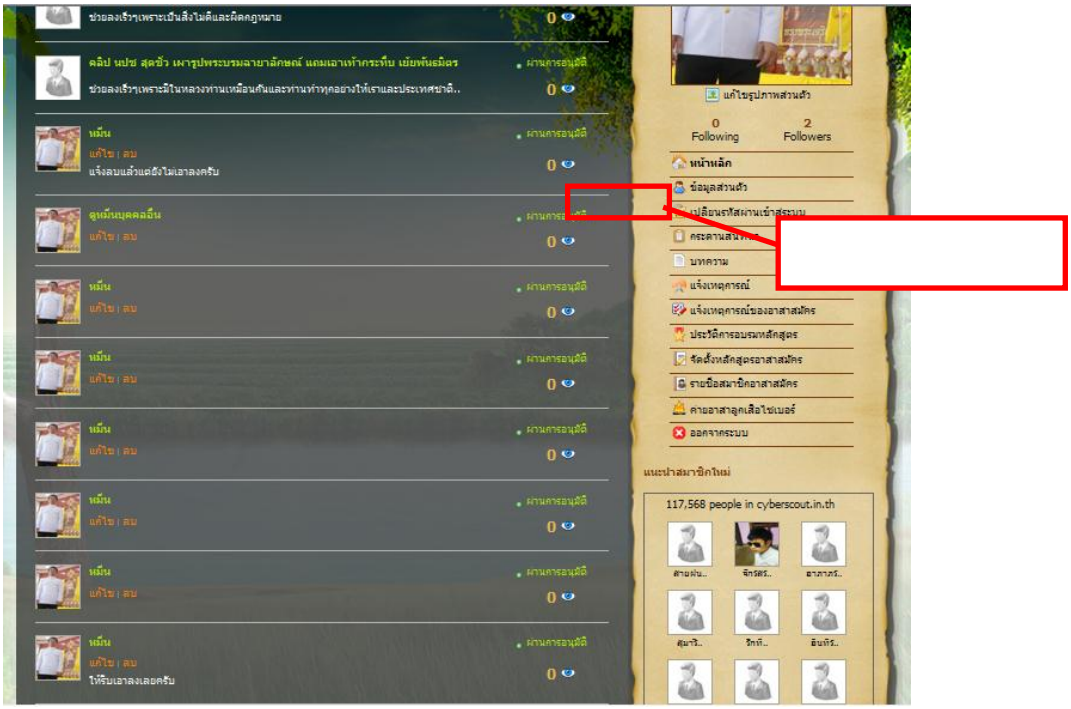
รูปที่ 9-13 หน้าจอการอบรมหลักสูตร

เมื่อเลือกหลักสูตรที่ต้องการพิจารณาแล้วจะปรากฏหน้าจอรายละเอียดของหลักสูตรนั้น ดังภาพ

รูปที่ 9-14 หน้าจอรายละเอียดหลักสูตรการอบรม

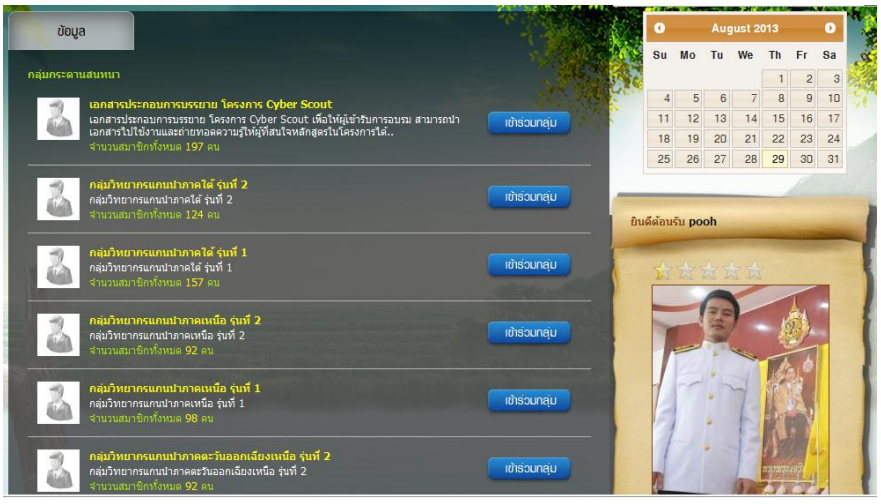
9.3ระบบการแลกเปลี่ยนเรียนรู้

เมื่อเข้าระบบสมาชิกแล้ว เลือกเมนู “กระดานสนทนา”



รูปที่ 9-15 หน้าจอการเลือกเมนูกระดานสนทนา

เมื่อเลือกเมนูกระดานสนทนาแล้วจะปรากฏหน้าข้อมูลห้องแลกเปลี่ยนเรียนรู้ทั้งหมดดังภาพ



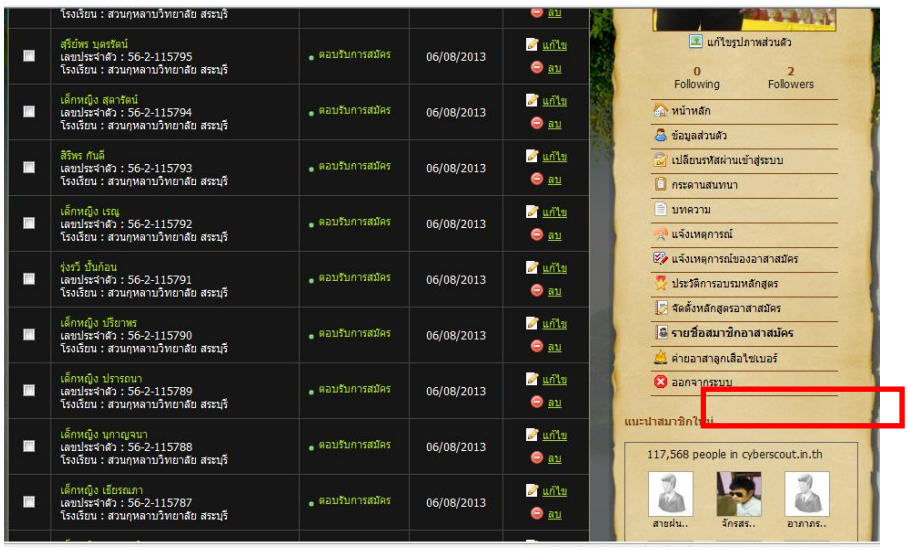
รูปที่ 9-16 หน้าจอหัวข้อกระดานสนทนา

เมื่อเลือกหัวข้อที่ต้องการแล้วจะปรากฏหน้าจอห้องสนทนาดังภาพ

รูปที่ 9-17 กระดานสนทนาแลกเปลี่ยนเรียนรู้

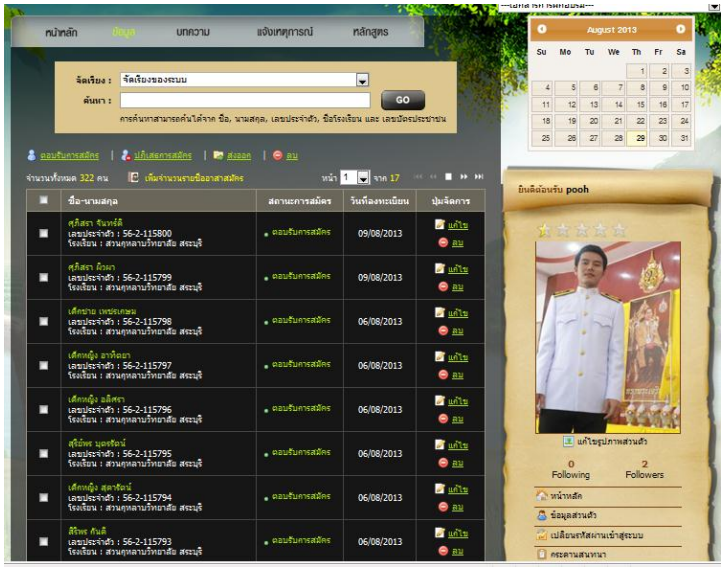
9.4 ระบบติดตามการขยายเครือข่ายอาสาสมัคร

เมื่อ Login เข้าสู่ระบบสมาชิกแล้ว ให้เลือกเมนู “รายชื่อสมาชิกอาสาสมัคร” เพื่อทำการขยายเครือข่ายอาสาสมัคร”



รูปที่ 9-18 หน้าจอเมนูรายชื่อสมาชิกอาสาสมัคร

เมื่อทำการเลือกเมนูรายชื่อสมาชิกอาสาสมัครแล้ว จะปรากฏหน้าจอข้อมูลการขยายผลสมาชิกอาสาสมัคร และสามารถเพิ่ม ตอบรับการสมัคร ปฏิเสธการสมัคร นำข้อมูลออกมาเป็นรายงานได้ในหน้าจอนี้



รูปที่ 9-19 หน้าจอข้อมูลการขยายผลเครือข่ายอาสาสมัคร

9.5 ระบบการแจ้งภัยออนไลน์

ขั้นตอนการแจ้งเหตุการณ์สำหรับสมาชิกแกนนำ Cyber Scout และสมาชิกอาสาสมัคร Cyber Scout

ขั้นตอนที่ 1 กรอก E-Mail และ Password โครงการ Cyber Scout แล้วคลิกที่ปุ่ม “LOGIN” ดังรูป

รูปที่ 9-20 หน้าจอกรอกข้อมูล E-Mail และ Password

หลังจากที่เข้าสู่ระบบสมาชิก ใช้ระบบแจ้งเหตุการณ์เพื่อรายงานเหตุการณ์ ดังนี้

ขั้นตอนที่ 2 คลิกที่ **“แจ้งเหตุการณ์”** เพื่อเข้าสู่เมนูเหตุการณ์ และคลิกที่ **“แจ้งเหตุการณ์ใหม่”** ดังรูป

รูปที่ 9-21 หน้าจอการเข้าสู่การแจ้งเหตุการณ์ใหม่

การแจ้งเหตุการณ์ใหม่ ให้กรอกข้อมูลที่จำเป็น ซึ่งประกอบด้วย

- **หมวดหมู่** คือ หมวดหมู่ที่ผู้ดูแลระบบตั้งขึ้นเพื่อบางประเภทของเหตุการณ์ที่มีการแจ้งเข้ามา
- **หัวข้อ** คือ ชื่อเหตุการณ์ที่แจ้งเข้ามา
- **ลิงก์** คือ ลิงก์ของเว็บไซต์ที่มีการแจ้งว่าไม่เหมาะสม หากข้อมูลซ้ำจะมีการแจ้งเตือน
- **ข้อความ** คือ คำบรรยายเกี่ยวกับลิงก์หรือเว็บไซต์ที่ไม่เหมาะสม
- **รูปภาพ** คือ ภาพจากเว็บไซต์ที่ไม่เหมาะสม
- **วิดีโอ** คือ วิดีโอจากเว็บไซต์ที่ไม่เหมาะสม

ขั้นตอนที่ 3 เมื่อกรอกข้อมูลครบถ้วนแล้ว ให้คลิกที่ **“ตกลง”** ดังรูป

รูปที่ 9-22 หน้าจอรายละเอียดการกรอกข้อมูลเพื่อแจ้งเหตุการณ์

หลังจากที่มีการแจ้งเหตุการณ์เพื่อรายงานเหตุการณ์ที่ไม่เหมาะสม สมาชิกสามารถเข้าดูรายละเอียดของเว็บไซต์ที่แจ้งเหตุการณ์ได้ ดังรูป

รูปที่ 9-23 หน้าจอรวมเหตุการณ์ที่แจ้งทั้งหมด

บทที่ 10 การพัฒนาหน่วยลูกเสือไซเบอร์ประจำสถานศึกษา

หน่วยลูกเสือไซเบอร์ประจำสถานศึกษา คือ สถานศึกษาที่ได้รับการคัดเลือกจากกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นหน่วยเฝ้าระวัง ทำหน้าที่สอดส่องดูแล เพื่อให้สังคม รู้สึกปลอดภัยว่ามีคนทำหน้าที่ช่วยระวังภัย และทำหน้าที่กระจายความรู้ความเข้าใจเกี่ยวกับภัยบนอินเตอร์เน็ตอย่างรอบด้าน ทั้งนี้ หน่วยลูกเสือไซเบอร์ประจำสถานศึกษายังทำหน้าที่สร้างอาสาสมัคร Cyber Scout ที่มีจิตสำนึกด้านจริยธรรมและคุณธรรมในการใช้ ICT เพื่อการเรียนรู้ ICT อย่างสร้างสรรค์ สามารถป้องกันตนเองจากภัย บนโลกไซเบอร์และสร้างความปลอดภัยในการใช้งานบนโลกออนไลน์

10.1 การวางแผนการพัฒนาหน่วยลูกเสือไซเบอร์ประจำสถานศึกษา

การวางแผนการพัฒนาหน่วยลูกเสือไซเบอร์ประจำสถานศึกษา ภายหลังจากการได้รับการจัดตั้งจากกระทรวงเทคโนโลยีสารสนเทศละการสื่อสาร คือประเด็นที่สถานศึกษาจำเป็นต้องให้ความสำคัญเป็นลำดับต้นๆ เพื่อเป็นแนวทางในการดำเนินงานให้เป็นไปตามวัตถุระสงค์และเป้าหมายที่ตั้งไว้ โดยจะต้องระบุระยะเวลาและขั้นตอนการดำเนินงานที่แน่นอน ชัดเจน ดังตัวอย่างตารางต่อไปนี้

ลำดับ	กิจกรรม	ขั้นตอน	ระยะเวลาการดำเนินงาน				
			1	2	3	4	5

ตารางที่ 10.1 ตัวอย่างตารางการวางแผนการพัฒนาหน่วยลูกเสือไซเบอร์ประจำสถานศึกษา

10.2 การทำโครงการและโครงงานลูกเสือไซเบอร์ประจำสถานศึกษา

โครงการ หมายถึง การวางแผนล่วงหน้าที่จัดทำขึ้นอย่างมีระบบ ประกอบด้วยกิจกรรมย่อยหลายกิจกรรมที่ต้องใช้ทรัพยากรในการดำเนินงาน และคาดหวังที่จะได้ผลตอบแทนอย่างคุ้มค่า แต่ละโครงการมีเป้าหมายเพื่อการผลิตหรือการให้บริการเพื่อเพิ่มพูนสมรรถภาพของแผนงาน การเขียนโครงการจึงเป็นส่วนสำคัญส่วนหนึ่งของการวางแผนที่จะทำให้องค์กรบรรลุผลสำเร็จตามเป้าหมาย [1]

10.2.1 ลักษณะของโครงการที่ดี

1) สามารถแก้ปัญหาขององค์กรหรือหน่วยงานนั้น ๆ ได้
2) มีรายละเอียด วัตถุประสงค์เป้าหมายต่าง ๆ ชัดเจน สามารถดำเนินงานได้
3) รายละเอียดของโครงการต่อเนื่องสอดคล้องสัมพันธ์กัน
4) ตอบสนองความต้องการของกลุ่มชน สังคมและประเทศชาติ
5) ปฏิบัติแล้วสอดคล้องกับแผนงานหลักขององค์กร
6) กำหนดขึ้นอย่างมีข้อมูลความจริงและเป็นข้อมูลที่ได้รับการวิเคราะห์อย่างรอบคอบ
7) ได้รับการสนับสนุนจากผู้บริหารทุกด้าน โดยเฉพาะด้านทรัพยากรที่จำเป็น
8) มีระยะเวลาในการดำเนินงานแน่นอน ระบุวันเวลาเริ่มต้นและสิ้นสุด

9) สามารถติดตามประเมินผลได้

10.2.2 ขั้นตอนการเขียนโครงการ

1) วิเคราะห์ปัญหาหรือความต้องการ ดำเนินการโดย

- ศึกษาสภาพแวดล้อมเพื่อค้นหาปัญหา
- กำหนดสภาพแห่งการหมดปัญหา
- กำหนดแนวทางแก้ไข

2) เขียนโครงการ โดยมีเทคนิค ดังนี้

2.1) ก่อนลงมือ ต้องตั้งคำถามและตอบคำถาม 6 W 1H

W1 = WHO หมายถึง คำถาม “ใครเป็นผู้ดำเนินโครงการ”

W2 = WHAT หมายถึง คำถาม “จะทำอะไรบ้าง”

W3 = WHEN หมายถึง คำถาม “จะทำเมื่อไหร่”

W4 = WHERE หมายถึง คำถาม “จะดำเนินโครงการที่ไหน”

W5 = WHY หมายถึง คำถามที่เกี่ยวกับ “จะทำโครงการนี้ไปทำไม”

W6 = TO WHOM หมายถึง คำถาม “ใครเป็นผู้ได้รับประโยชน์”

H1 = HOW หมายถึง คำถาม “จะดำเนินโครงการอย่างไร”

2.2) ศึกษาเกณฑ์การคัดเลือกโครงการ

2.3) ลงมือเขียนโครงการ โดยใช้ภาษาเขียนที่กระชับ สื่อความหมายได้ชัดเจน

10.2.2 รูปแบบการเขียนโครงการ

การเขียนโครงการจะประกอบด้วย

1) ชื่อโครงการ เป็นการระบุเพื่อให้ทราบถึงแนวทางปฏิบัติและการคาดหวังผลตอบแทนที่สืบเนื่องจากการปฏิบัติโครงการตลอดจนทิศทางของการดำเนินโครงการนั้น

2) หลักการและเหตุผล เป็นการระบุถึงสภาพปัญหาและความจำเป็นในการจัดทำโครงการขึ้นมาเพื่อแก้ไขปัญหาดังกล่าว

3) วัตถุประสงค์โครงการ เป็นการแสดงให้เห็นถึงสิ่งหรือผลงานที่เป็นจุดหมายปลายทางที่ต้องการจะให้เกิดขึ้นจาการปฏิบัติงานนั้น การกำหนดวัตถุประสงค์ที่ดีจะเป็นการช่วยให้การกำหนดขั้นตอน

สำหรับปฏิบัติเป็นอย่างรัดกุม การกำหนดวัตถุประสงค์ที่ดีควรประกอบด้วยองค์ประกอบที่เรียกว่า “SMART”

S = Sensible (เป็นไปได้) วัตถุประสงค์ที่ดีต้องมีความเป็นไปได้

M = Measurable (วัดได้) วัตถุประสงค์ที่ดีจะต้องสามารถวัดและประเมินผลได้

A = Attainable (ระบุสิ่งที่ต้องการ) วัตถุประสงค์ที่ดีจะต้องระบุสิ่งที่ต้องการดำเนินงานอย่างชัดเจนและเฉพาะเจาะจงมากที่สุด

R = Reasonable (เป็นเหตุเป็นผล) วัตถุประสงค์ที่ดีต้องมีความเป็นเหตุเป็นผลในการปฏิบัติงาน

T = Time (เวลา) วัตถุประสงค์ที่ดีต้องมีขอบเขตของเวลาที่แน่นอนในการปฏิบัติงาน

4) **กลุ่มเป้าหมาย** ระบุกลุ่มเป้าหมายและจำนวนให้ชัดเจน ใครคือผู้ที่จะได้รับผลดีจากโครงการนี้ จำนวนผู้ที่ได้รับผลดีจากโครงการนี้

5) สถานที่ดำเนินการ ระบุสถานที่ดำเนินการโครงการ ระบุพื้นที่ โดยระบุหมู่บ้าน ตำบล อำเภอ จังหวัด

6) **ระยะเวลาดำเนินการโครงการ** เป็นการกำหนดช่วงเวลาการปฏิบัติโครงการตั้งแต่ระยะเริ่มต้นปฏิบัติโครงการจนถึงการสิ้นสุดโครงการนั้น

7) **วิธีดำเนินการ** ควรแสดงถึงกิจกรรมและกระบวนการปฏิบัติงานที่สอดรับกับวัตถุประสงค์ แสดงรายละเอียดกิจกรรมเพียงพอ และมีกำหนดระยะเวลาของแต่ละกิจกรรมที่สมเหตุสมผล และควรมีกิจกรรมต่อเนื่อง หากเป็นโครงการที่มีการฝึกอบรม ดูงาน จะต้องมีกิจกรรมต่อเนื่องที่จะส่งผลต่อการคุ้มครอง การส่งเสริม และการสนับสนุนผู้สูงอายุ และมีกำหนดการการฝึกอบรม หัวข้อที่จะฝึกอบรม

การเขียนวิธีดำเนินการ ให้แจกแจงดังนี้

- ขั้นเตรียมการ
- ขั้นดำเนินงาน
- กิจกรรมที่จะดำเนินงานตามโครงการ

8) งบประมาณ งบประมาณหรือค่าใช้จ่ายของโครงการนับเป็นทรัพยากรที่สำคัญต่อการปฏิบัติโครงการ โดยทั่วไปมีองค์ประกอบ ดังนี้

- ยอดรวมค่าใช้จ่ายทั้งโครงการ
- ค่าใช้จ่ายของแต่ละกิจกรรมหรือแต่ละช่วงเวลาพร้อมทั้งรายละเอียดค่าใช้จ่าย

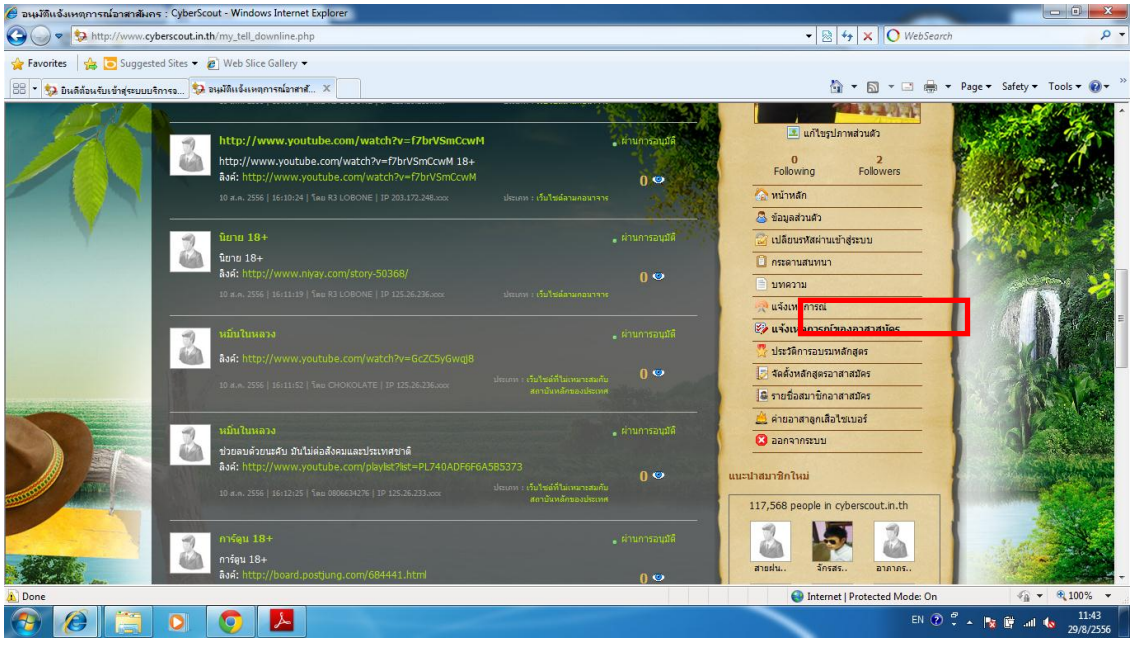
9) การประเมินโครงการ เป็นกระบวนการในการเก็บรวบรวมและวิเคราะห์ข้อมูลของการดำเนินโครงการและพิจารณาบ่งชี้ให้ทราบถึงจุดเด่นหรือจุดด้อยของโครงการนั้น

10) ผลที่คาดว่าจะได้รับ เป็นผลที่เกิดขึ้นจากการที่โครงการบรรลุวัตถุประสงค์ ผลที่เกิดขึ้นจากการปฏิบัติโครงการ สามารถแสดงให้เห็นผลที่เป็นประโยชน์ทางตรง ทางอ้อม

10.3 การติดตามผลการดำเนินงานลูกเสือไซเบอร์บนเว็บไซต์ www.cyberscout.in.th

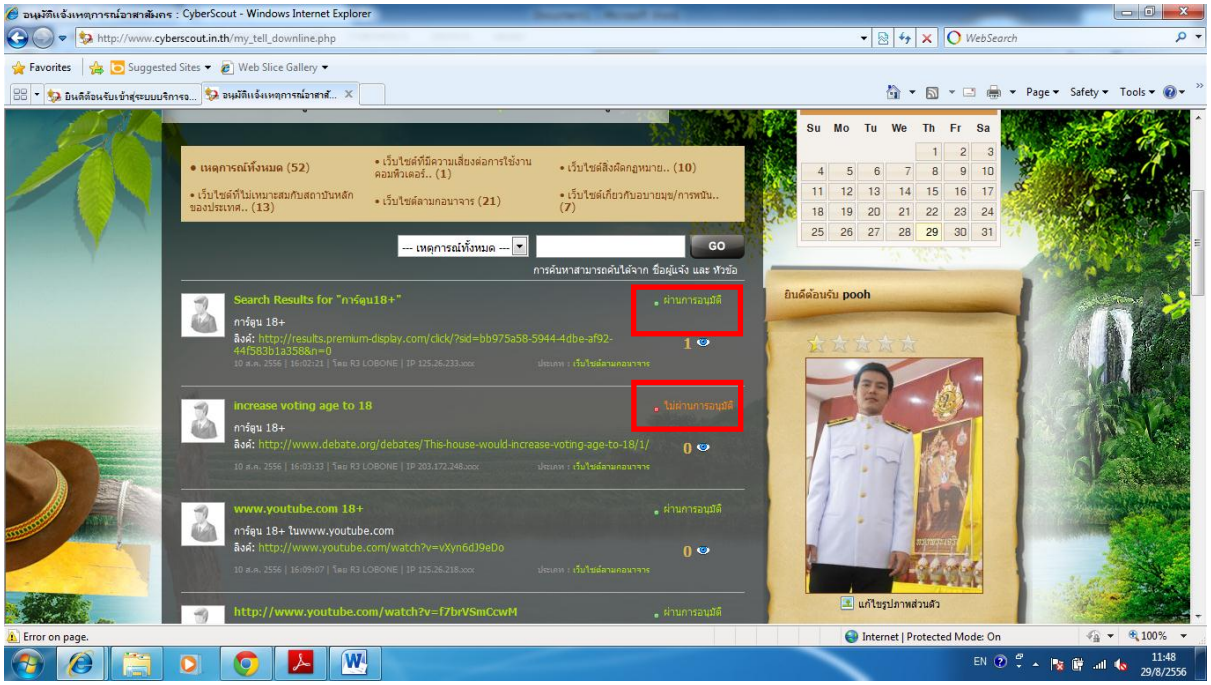
การติดตามผลการดำเนินงานลูกเสือไซเบอร์ สามารถติดตามผ่านระบบใน www.cyberscout.in.th โดยมีขั้นตอนการติดตามผล ดังนี้

เมื่อLogin เข้าสู่หน้าสมาชิกเรียบร้อยแล้ว จะปรากฏเมนูให้เลือกเมนู “แจ้งเหตุการณ์ของอาสาสมัคร” เพื่อเข้าไปพิจารณาเหตุการณ์ต่างๆ ที่อาสาสมัครลูกเสือไซเบอร์แจ้งมา เพื่อเป็นการคัดกรองการแจ้งนั้นๆ ก่อน ดังภาพ



รูปที่ 10-1 หน้าจอแสดงเมนูแจ้งเหตุการณ์ของอาสาสมัคร

เมื่อเลือกเมนูแจ้งเหตุการณ์ของอาสาสมัครแล้ว จะปรากฏหน้าจอดังภาพ โดยแกนนำลูกเสือไซเบอร์สามารถพิจารณาคัดกรองการแจ้งเหตุการณ์ต่างๆ ของอาสาสมัครก่อนที่จะโพสต์เข้าระบบหลัก โดยถ้าพิจารณาแล้วว่าสามารถโพสต์ขึ้นได้ให้เลือกผ่านการอนุมัติ แต่ถ้าหัวข้อไหนพิจารณาแล้วว่าไม่เหมาะสมหรือเป็นเท็จให้เลือกไม่ผ่านการอนุมัติ ดังรูป



รูปที่ 10-2 แสดงหน้าจอการพิจารณาการแจ้งเหตุการณ์ของอาสาสมัครลูกเสือไซเบอร์

บรรณนานุกรมประจำบทที่ 10

[1] www.prachinburi.m-society.go.th/work/download23.doc (สืบค้นเมื่อวันที่ 24 สิงหาคม 2556).