บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบัน เทคโนโลยีสารสนเทศเข้ามามีบทบาทในชีวิตประจำวันของคนเรามากยิ่งขึ้นกว่าแต่ก่อน ผู้ใช้อินเทอร์เน็ต และเครือข่ายสังคมออนไลน์ ไม่ว่าจะเป็นเฟซบุ๊ค ไลน์ ทวิตเตอร์ ยูทูบ อินสตาแกรม เป็นต้น ได้เพิ่มจำนวนมากขึ้นอย่างก้าวกระโดด เนื่องจากมีอุปกรณ์ที่ผู้ใช้สามารถเข้าถึงอินเทอร์เน็ตได้หลากหลายชนิด ทั้งโน้ตบุ๊คคอมพิวเตอร์ สมาร์ทโฟน แท็บเล็ต สามารถเข้าถึงได้ทุกที่ทุกเวลา ประกอบกับกับนโยบายของรัฐบาลไทยมุ่งเน้นแนวทางการพัฒนาประเทศไปสู่ ประเทศไทย 4.0 (Thailand 4.0) ด้วยการขับเคลื่อนเศรษฐกิจด้วยนวัตกรรม นั่นก็คือการนำเอาเทคโนโลยีสารสนเทศเข้ามาช่วยในการสร้างนวัตกรรมใหม่ๆ ซึ่งจะเป็นการช่วยยกระดับรายได้ของประชากรในประเทศไทยจากประเทศที่มีรายได้ปานกลางไปสู่ประเทศที่มีรายได้สูง ในขณะเดียวกันก็ต้องเผชิญกับความท้าทายต่างๆ อย่างมากมาย โดยเฉพาะเรื่องเกี่ยวกับการละเมิดจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ เนื่องจากสิ่งแวดล้อมทางคอมพิวเตอร์มีความซับซ้อนมากขึ้น ผู้ใช้มีความคาดหวังสูงขึ้น จำนวนของผู้ใช้งานด้านคอมพิวเตอร์ได้เพิ่มขยายขึ้นอย่างต่อเนื่อง ระบบการทำงานและระบบคอมพิวเตอร์มีการเปลี่ยนแปลง มีการเชื่อมต่อเครือข่ายเพิ่มมากขึ้นเป็นลำดับ องค์กรและพนักงานเป็นจำนวนมากหันมาใช้คอมพิวเตอร์แบบกลุ่มเมฆ (Cloud Computing) ในการทำงานและใช้งานในการจัดเก็บข้อมูล การให้บริการผ่านอินเทอร์เน็ต รวมถึงซอฟต์แวร์ยังมีช่องโหว่ มีผู้ใช้บางคนใช้งานคอมพิวเตอร์อย่างขาดคุณธรรมและจริยธรรม ได้แก่ (1). การใช้งานคอมพิวเตอร์อย่างขาดความรับผิดชอบ (2).การละเมิดความเป็นส่วนตัวของผู้อื่น (3). การขโมยอัตลักษณ์ (4). การเจาะระบบ การทำลายข้อมูล การล้วงความลับส่วนบุคคลและองค์กร (5). การโจมตีด้วยไวรัสประเภทต่างๆ (6). การละเมิดลิขสิทธิ์ (7). การส่งอีเมลที่ไม่ได้รับเชิญ รบกวนสร้างความรำคาญให้กับผู้อื่น (8).การใช้ Facebook Like ถ่ายทอดสดในเรื่องที่ไม่เหมาะสม เช่น การเปลื้องผ้าโชว์สัดส่วนลามก อนาจาร การฆาตกรรมผู้อื่น และฆ่าตัวตายตาม (9). การก่ออาชญากรรมคอมพิวเตอร์ในลักษณะต่างๆ เช่น การปลอมแปลง การหลอกหลวงทางอินเทอร์เน็ตทำให้ผู้ใช้คอมพิวเตอร์ทั่วไปเกิดความรู้สึกไม่ปลอดภัย

นอกจากนี้ การสื่อสารและการแลกเปลี่ยนสารสนเทศเป็นไปอย่างรวดเร็วกว้างขวาง ไม่ว่าจะเป็นการแลกเปลี่ยนข้อมูลส่วนตัวหรือองค์กร ดังนั้น องค์กรต่างๆ จึงต้องให้ความสำคัญเกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศด้วย เช่น ความลับทางธุรกิจ ข้อมูลส่วนตัวของลูกค้า ข้อมูลด้านการศึกษาและข้อมูลของพนักงาน เป็นต้น ควรได้รับการดูแลปกป้องเป็นอย่างดี และระบบขององค์กรจะต้องสามารถป้องกันการกระทำที่มุ่งร้ายของผู้ไม่หวังดี หรือการกระทำที่ขัดขวางการทำงานของคอมพิวเตอร์ ตัวอย่างเช่น เรื่องราวเกี่ยวกับจริยธรรมและความปลอดภัยของเทคโนโลยีสารสนเทศ

มีปริมาณเพิ่มมากขึ้น ตามที่ได้มีการดำเนินการศึกษาเกณฑ์การเปรียบเทียบบริษัทในสหรัฐอเมริกา โดยสถาบันโพนิมอน เมื่อเดือนกรกฎาคม ค.ศ. 2010 พบว่าการโจมตีทางไซเบอร์ได้กลายเป็นเหตุการณ์ที่เกิดขึ้นร่วมกัน แต่ละบริษัท รวม 45 บริษัท จากรายงานการศึกษายังพบอีกว่า บริษัทเหล่านั้น ได้ตกเป็นเหยื่อการโจมตีอย่างน้อย 1 ครั้งต่อสัปดาห์ แสดงให้เห็นถึงการเพิ่มขึ้นของเหตุการณ์ด้านความปลอดภัยของคอมพิวเตอร์ ที่มีการสำรวจองค์กรมากถึง 443 องค์กรในสหรัฐ ที่ส่งคืนตอบแบบสอบถาม ในปี ค.ศ. 2009 สำหรับในประเทศไทย มีรายงานจากหนังสือพิมพ์ **"ประชาชาติธุรกิจ"** (ฉบับออนไลน์) วันที่ 19 มิถุนายน พ.ศ.2558 พบว่า สถิติข้อมูลภัยคุกคามไซเบอร์ที่รวบรวมโดย ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต (ThaiCERT) พบว่า ปี พ.ศ.2557 ที่ผ่านมา มีการแจ้งเหตุภัยคุกคาม จำนวน 4,008 กรณี และ 3 อันดับแรก ได้แก่ การโจมตีด้วยโปรแกรมไม่พึงประสงค์ (Malicious Code) 40.1% (1,735 กรณี) การหลอกลวงออนไลน์ (Fraud) เพื่อการได้มาซึ่งข้อมูลหรือทรัพย์สินของผู้อื่น 26.4% (1,010 กรณี) และการบุกรุก/เจาะระบบคอมพิวเตอร์จนสามารถดึงข้อมูลได้สำเร็จ (Intrusion) 19.8% (711 กรณี) ขณะที่ 5 เดือนแรกของปี พ.ศ.2558 มีการแจ้งแล้ว 1,797 กรณี อันดับแรกเป็นการโจมตีด้วยมัลแวร์ 644 กรณี การหลอกลวงออนไลน์ 503 กรณี ความพยายามบุกรุกเข้าระบบ 324 กรณี และเจาะระบบได้สำเร็จ 323 กรณี

ด้วยสาเหตุดังกล่าว ผู้วิจัยจึงต้องการศึกษาวิเคราะห์ถึงปัจจัยที่มีผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ที่มีผลกระทบต่อวิถีชีวิตความเป็นอยู่ของคนในสังคมอุดมศึกษา ในเขตกรุงเทพมหานคร และปริมณฑล

แนวคิด หลักการ ทฤษฎีทางคุณธรรมจริยธรรม

แนวคิด หลักการ ทฤษฎี รวมทั้งหลักคำสอนทางศาสนาต่างๆ มีอยู่มากมาย ผู้บริหารควรศึกษาน้อมนำมาพิจารณาเป็นแนวทางปฏิบัติตนและการดำเนินงาน หลักคำสอนที่จะนำมาพอเป็นตัวอย่างต่อไปนี้มีทั้งจากคำสอนทางศาสนา หลักปรัชญา แนวคิดของนักปราชญ์ทั้งในอดีตกาล และแนวใหม่ ทั้งของประเทศทางตะวันตก และประเทศตะวันออก ที่มีปรากฏในเว็บไซต์ www.baanjomyut.com มีรายละเอียดดังต่อไปนี้ คือ:

ตามหลักของจริยศาสตร์นั้น พระพุทธเจ้าทรงสอนพุทธจริยศาสตร์อันเป็นหลักคำสอนทางพระพุทธศาสนาได้ทรงบัญญัติไว้ เพื่อเป็นมาตรฐานความประพฤติของมนุษย์ โดยแบ่งออกเป็น 3 ระดับ ได้แก่

1. พุทธจริยศาสตร์ระดับต้น บัญญัติไว้เพื่อความสงบเรียบร้อยของสังคม หลักธรรม คือ ศีล 5 ธรรม 5 ทิศ 6 เป็นต้น

2. พุทธจริยศาสตร์ระดับกลาง บัญญัติไว้เพื่อให้ทุกคนประพฤติปฏิบัติอบรมขัดเกลาตนเองให้มีคุณธรรมสูงขึ้น หลักธรรม คือ ศีล 5 กุศลกรรมบถ 10

3. พุทธจริยศาสตร์ระดับสูง เป็นจริยศาสตร์เพื่อพัฒนาตนเป็นอริยบุคคล หลักธรรม คือ มรรค 8 ส่วนหัวใจสำคัญของพุทธจริยศาสตร์ หรือหัวใจสำคัญของพระพุทธศาสนาก็คือ

1. ไม่ทำชั่วทั้งปวง
2. ทำกุศลคือความดีให้พรั่งพร้อม
3. ทำจิตของตนให้ผ่องแผ้ว

พระราชวรมุนี : ประยุทธ์ ปยุตโต (2562:2). พระนักปราชญ์ทางพระพุทธศาสนาได้กล่าวถึงความหมายของจริยธรรมเอาไว้ว่า จริยธรรมในความหมายอย่างกว้าง หมายถึง **การดำเนินชีวิตความเป็นอยู่ การคลองชีวิตการใช้ชีวิตการเคลื่อนไหวของชีวิตทุกด้านทุกระดับ ทั้งทางกาย ทางวาจา ทางใจ การปฏิบัติกรรมฐานเจริญสมาธิ บำเพ็ญสมถะ เจริญวิปัสสนา**

จากนิยามข้างต้น แม้ว่าจริยธรรมไม่สามารถแยกเด็ดขาดจากศีลธรรม แต่คำว่าจริยธรรม จะมีความหมายกว้างกว่าศีลธรรม เพราะศีลธรรมเป็นหลักคำสอนทางศาสนาที่ว่าด้วยความประพฤติปฏิบัติชอบ ส่วนจริยธรรม หมายถึง หลักแห่งความประพฤติปฏิบัติชอบ ซึ่งมีรากฐานอยู่บนหลักคำสอนของศาสนา ปรัชญาและขนบธรรมเนียมประเพณี เป็นแนวทางประพฤติปฏิบัติตนเพื่อการบรรลุถึงสภาพชีวิตอันทรงคุณค่าที่พึงประสงค์ ทั้งนี้ เหตุที่จริยธรรมมักอิงอยู่กับศาสนา เนื่องจากคำสอนทางศาสนามีส่วนสร้างระบบจริยธรรมให้สังคม แต่ไม่ได้หมายความว่าจริยธรรมอิงอยู่กับหลักคำสอนทางศาสนาเพียงอย่างเดียว แท้ที่จริงจริยธรรมยังหยั่งรากอยู่บนวัฒนธรรมขนบธรรมเนียมประเพณี และโดยนัยนี้ บางท่านเรียกหลักแห่งความประพฤติอันเนื่องมาจากคำสอนทางศาสนาว่า ศีลธรรม และเรียกหลักแห่งความประพฤติอันพัฒนามาจากแหล่งอื่นว่าจริยธรรม นอกจากนี้จริยธรรมยังมิใช่กฎหมาย เนื่องจากกฎหมายเป็นสิ่งบังคับให้คนทำตาม และมีบทลงโทษสำหรับผู้ฝ่าฝืน สาเหตุที่คนเคารพเชื่อฟังกฎหมายเพราะกลัวถูกลงโทษ ขณะที่จริยธรรมไม่มีบทลงโทษ ดังนั้น คนมีจริยธรรมเพราะมีแรงจูงใจ อย่างไรก็ตาม กฎหมายก็มีส่วนเกี่ยวข้องกับจริยธรรมในฐานะเป็นแรงหนุนจากภายนอกเพื่อให้คนมีจริยธรรม

ส่วนคำว่า จริยศาสตร์ มาจากภาษาสันสกฤต 2 คำ คือ จริย หมายถึงความประพฤติ กับ ศาสตร์ หมายถึงความรู้ ถ้าจะแปลความตามตัวอักษร จริยศาสตร์ หมายถึงความรู้เกี่ยวกับความประพฤติ จริยศาสตร์ในภาษาอังกฤษ คือ Ethicsซึ่งมาจากคำภาษากรีกว่า Ethos มีความหมายว่า Customllคือ ขนบธรรมเนียม หรือ ธรรมเนียมปฏิบัติ และคำว่า Ethics มีความหมายว่า ศาสตร์แห่งศีลธรรม (Science of Morals) ทั้งนี้ ตามพจนานุกรมราชบัณฑิตยสถาน พ.ศ. 2525 ได้ให้ความหมายจริยศาสตร์ว่า เป็นปรัชญาสาขาหนึ่งว่าด้วยความประพฤติ และการครองชีวิต ว่าอะไรดี อะไรชั่ว อะไรถูก อะไรผิด หรืออะไรควร อะไรไม่ควร

ดังนั้น จริยศาสตร์จึงหมายถึง ความรู้ หลักการ หรือทฤษฎีที่ใช้เหตุผลแยกความดีออกจากความชั่ว เป็นสาขาหนึ่งของปรัชญา และเป็นศาสตร์ที่เป็นบรรทัดฐานของความประพฤติของมนุษย์ ทำให้จริยศาสตร์มีความเด่นชัดแตกต่างไปจากศาสตร์ที่มีรูปแบบอื่น ๆ อาทิ คณิตศาสตร์ ตรรกศาสตร์ และวิทยาศาสตร์เชิงผัสสะต่างๆ (Empirical Sciences) เช่น เคมี และฟิสิกส์

นอกจากนี้ ยังมีคำที่มีความหมายใกล้เคียงกับคำว่าจริยธรรม ซึ่งบางกรณีอาจก่อให้เกิดความสับสน มีการนำไปใช้ในความหมายที่แตกต่างกัน และไม่ตรงกับความหมายที่แท้จริง อาทิคำว่า จรรยา คุณธรรม ศีลธรรม จรรยาบรรณ มโนธรรม มารยาท ธรรมาภิบาล กล่าวคือ

“จรรยา” (Etiquette) หมายถึง ความประพฤติ กิริยาที่ควรประพฤติในหมู่คณะ เช่น จรรยาครู จรรยาตำรวจ ฯลฯ

“คุณธรรม” (Virtue) คือ คุณ + ธรรมะ เป็นคุณงามความดีที่เป็นธรรมชาติ ก่อให้เกิดประโยชน์ต่อตนเองและสังคม คุณธรรมจึงเป็นจริยธรรมที่แยกเป็นรายละเอียดแต่ละประเภท หากประพฤติปฏิบัติอย่างสม่ำเสมอก็จะเป็นสภาพคุณงามความดีทางความประพฤติและจิตใจของ ผู้นั้น คุณธรรมจึงเป็นจริยธรรมที่ฝึกฝนจนเป็นนิสัย เช่น ซื่อสัตย์ ขยัน อดทน เสียสละ รับผิดชอบ

“จรรยาบรรณ” (Code of Conduct) หมายถึง ประมวลความประพฤติที่ผู้ประกอบอาชีพการงานแต่ละอย่างกำหนดขึ้น เพื่อรักษาและส่งเสริมเกียรติคุณ ชื่อเสียง และฐานะของสมาชิก

“มโนธรรม” (Conscience)หมายถึง ความรู้สึกผิดชอบชั่วดี ความรู้สึกว่าอะไรควรทำ อะไรไม่ควรทำ เชื่อกันว่า มนุษย์ทุกคนมีมโนธรรม เนื่องจากบางขณะเราจะเกิดความรู้สึกขัดแย้งในใจระหว่างความรู้สึกว่าต้องการทำสิ่งหนึ่ง และรู้ว่าควรทำอีกสิ่งหนึ่ง

“มารยาท” (Manner) หมายถึง กิริยา วาจา ที่สังคมกำหนดไว้เป็นที่ยอมรับในกลุ่มแต่ละท้องถิ่นซึ่งมีแตกต่างกันไป

“ธรรมาภิบาล” (Good Governance) หมายถึง การจัดการปกครอง การบริหารกิจการบ้านเมือง การควบคุมดูแลกิจการ การกำกับดูแลที่ดี อันเป็นเรื่องที่เกี่ยวข้องกับกระบวนการ (Process) และระบบ (System)เซึ่งองค์การหรือสังคมได้มีการปฏิบัติหรือดำเนินการ (Operate) ปกครองด้วยคุณความดี ซื่อตรงต่อกัน มั่นคงในสัญญาที่มีต่อกัน ซึ่งจะครอบคลุมประเด็นเรื่องการมีส่วนร่วมของประชาชน นิติธรรม ความโปร่งใส การตอบสนอง การแสวงหาฉันทามติ ความถูกต้อง ความเสมอภาค ยุติธรรม เที่ยงธรรม ประสิทธิผลและประสิทธิภาพ ภาระรับผิดชอบ

นอกจากนี้ ยังคำที่มีความเกี่ยวข้องกับคำว่า จริยธรรม อีกหนึ่งคำ คือ คำว่า ทศพิธราชธรรม (Virtues of the King) ซึ่งหมายถึงจริยวัตร 10 ประการที่พระเจ้าแผ่นดินทรงประพฤติเป็นหลักธรรมประจำพระองค์ หรือเป็นคุณธรรมประจำตนของผู้ปกครองบ้านเมือง ให้มีความเป็นไปโดยธรรมและยังประโยชน์สุขให้เกิดแก่ประชาชน ถือได้ว่าเป็นหลักจริยธรรมอีกอันหนึ่งสำหรับนักการเมือง ที่ต้องนำไปปฏิบัติในหน้าที่ทางการงานการปกครอง คุณธรรมทั้ง 10 ประการ สามารถแจกแจงได้ ดังนี้

ทาน คือ การให้ การเสียสละ การให้น้ำใจ

ศีล คือ ความประพฤติที่ดีงาม ทั้ง กาย วาจา ใจ ให้ปราศจากโทษ

บริจาค คือ การเสียสละความสุขส่วนตน เพื่อความสุขส่วนรวม

ความซื่อตรง คือ ความซื่อตรงในฐานะที่เป็นผู้ปกครอง ดำรงอยู่ในสัตย์สุจริต

ความอ่อนโยน คือ การมีอัธยาศัยอ่อนโยน เคารพในเหตุผลที่ควร มีสัมมาคารวะต่อ ผู้อาวุโส

ความเพียร คือ ความอุตสาหะในการปฏิบัติงาน โดยปราศจากความเกียจคร้าน

ไม่โกรธ คือ ไม่มุ่งร้ายผู้อื่น แม้จะลงโทษผู้ทำผิดก็ทำตามเหตุผล

ความไม่เบียดเบียน คือ การไม่ก่อทุกข์หรือเบียดเบียนผู้อื่น

ความอดทน คือ การรักษาอาการ กาย วาจา ใจให้เรียบร้อย การอดทนต่อสิ่งทั้งปวง

ความยุติธรรม คือ ความหนักแน่น ถือความถูกต้อง เที่ยงธรรมเป็นหลัก

จากที่กล่าวมาข้างต้นคำว่าจริยธรรม คุณธรรม ศีลธรรม จรรยาบรรณ ล้วนมีเป้าหมายเพื่อการควบคุมตนเอง และส่งผลต่อพฤติกรรมของบุคคลนั้น ส่วนคำว่าธรรมาภิบาลใช้เพื่อเป็นกลไกควบคุมโครงสร้าง ระบบ และกระบวนการส่งผลต่อการปฏิบัติงานของหน่วยงานหรือองค์กร กล่าวโดยสรุปจริยธรรมคือ สิ่งที่มีอยู่แล้วในตัวมนุษย์ โดยธรรมชาติ ซึ่งจะต้องพัฒนาขึ้นโดยอาศัยกฎเกณฑ์ความประพฤติที่มนุษย์ควรประพฤติที่ได้จากหลักการทางศีลธรรม หลักปรัชญา วัฒนธรรม กฎหมายหรือจารีตประเพณี เพื่อประโยชน์สุขแก่ตนเองและสังคม นอกจากนี้ จริยธรรมยังใช้เป็นแนวทางประกอบการติดสินใจเลือกความประพฤติ การกระทำที่ถูกต้องเหมาะสมในแต่ละสถานการณ์ เป็นศีลธรรมที่ใช้เฉพาะกลุ่ม

ม.ร.ว.คึกฤทธิ์ ปราโมช (2562:1). อดีตนายกรัฐมนตรีและนักคิดนักเขียนท่านหนึ่งได้กล่าวถึงความหมายของจริยธรรมเอาไว้ว่า **“จริยธรรมของสังคมไทยขึ้นอยู่กับระบบศีลธรรมของ**

พุทธศาสนาว่า กำหนดหลักในการปฏิบัติในชีวิตประจำไว้อย่างไร หลักจริยธรรมก็จะกำหนดให้ปฏิบัติตามนั้น"

ทั้งนี้ จริยธรรมมาจากคำว่า จริย กับ ธรรมะ จริย หมายถึง ความประพฤติ กิริยาที่ควรประพฤติ ธรรมะหมายถึง คุณความดี คำสั่งสอนในศาสนา หลักประพฤติปฏิบัติในศาสนา ความจริง ความยุติธรรม ความถูกต้อง กฎเกณฑ์ กฎหมาย สิ่งของทั้งหลาย เมื่อพิจารณาตามรูปคำจากพจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2535 ให้คำนิยามว่า "จริยธรรม" คือ ธรรมที่เป็น ข้อประพฤติปฏิบัติ ศีลธรรม กฎศีลธรรม

แสง จันทร์งาม (2562:1) นักปราชญ์ทางพระพุทธศาสนาอีกท่านหนึ่ง ได้กล่าวถึงจริยธรรมเอาไว้ว่า จริยธรรมกับค่านิยมมีความหมายแตกต่างกันเฉพาะในทางทฤษฎี แต่ในทางปฏิบัติยากที่จะชี้ให้เห็นความแตกต่างกันอย่างชัดเจน กล่าวคือ

จริยธรรม หมายถึง คุณสมบัติทางความประพฤติ ที่สังคมมุ่งหวังให้คนในสังคมนั้นประพฤติมีความถูกต้องในความประพฤติ มีเสรีภาพภายในขอบเขตของมโนธรรม (Conscience) เป็นหน้าที่ที่สมาชิกในสังคมพึงประพฤติปฏิบัติต่อตนเอง ต่อผู้อื่น และต่อสังคม ทั้งนี้เพื่อก่อให้เกิดความเจริญรุ่งเรืองขึ้นในสังคม การที่จะปฏิบัติให้เป็นไปเช่นนั้นได้ ผู้ปฏิบัติจะต้องรู้ว่าสิ่งใดถูกสิ่งใดผิด

ค่านิยม หมายถึง ความโน้มเอียง หรือแนวทางที่คนจะประพฤติตนไปในแนวทางใดแนวทางหนึ่งที่ตัวเองได้พิจารณาไตร่ตรองแล้วว่า เป็นสิ่งที่ดีสำหรับตนหรือสังคมยอมรับนับถือและปฏิบัติตามแนวคิดนั้น ๆ อย่างสม่ำเสมอ อย่างน้อยก็ช่วงระยะเวลาหนึ่ง ค่านิยมมีความหมายถึงแนวคิดเกี่ยวกับความดีงามในความประพฤติ โดยผ่านการพิจารณาอย่างรอบคอบถึงผลที่จะเกิดขึ้นจากความประพฤตินั้น ๆ ถ้าหากเป็นเพียงเจตคติ (Attitude) ความเชื่อ (Belief) ยังไม่อาจเรียกได้ว่าเป็นค่านิยมจนกว่าจะได้พิจารณาถึงผลที่จะตามมาจากความประพฤติหรือการกระทำนั้นๆ อย่างรอบคอบและมีการปฏิบัติตามอย่างสม่ำเสมอ

นอกจากนี้ ยังเห็นว่าโครงสร้างของแนวคิดด้านจริยธรรม จะประกอบด้วยคุณธรรมหลายประการ ซึ่งส่วนมากมาจากคำสอนทางศาสนา ดังนี้

1. ความรับผิดชอบ (Accountability) คือ ความมุ่งมั่นที่จะปฏิบัติหน้าที่ด้วยความผูกพันด้วยความพากเพียร และความละเอียดรอบคอบ ยอมรับผลการกระทำในการปฏิบัติหน้าที่ เพื่อให้บรรลุผลสำเร็จตามความมุ่งหมาย ทั้งพยายามที่จะปฏิบัติหน้าที่ ให้ดียิ่งขึ้น

2. ความซื่อสัตย์ (Honesty) คือ การประพฤติอย่างเหมาะสม และตรงต่อความเป็นจริง ประพฤติ ปฏิบัติ อย่างตรงไปตรงมา ทั้งกาย วาจา ใจ ต่อตนเองและผู้อื่น

3. ความมีเหตุผล (Rationality) คือ ความสามารถในการใช้ปัญญา ในการประพฤติปฏิบัติรู้จักไตร่ตรอง พิสูจน์ให้ประจักษ์ ไม่หลงงมงาย มีความยับยั้งชั่งใจ โดยไม่ผูกพันกับอารมณ์และความยึดมั่นของตนเอง ที่มีอยู่เดิมซึ่งอาจผิดได้

4. ความกตัญญูกตเวที (Gratitude) คือ ความรู้สำนึกในอุปการคุณหรือบุญคุณที่ผู้อื่นมีต่อเรา

5. ความมีระเบียบวินัย (Disciplined) คือ การควบคุมความประพฤติปฏิบัติให้ถูกต้องและเหมาะสมกับจรรยามารยาท ข้อบังคับ ข้อตกลง กฎหมาย และศีลธรรม

6. ความเสียสละ (Sacrifice) คือ การละความเห็นแก่ตัว การให้ปันแก่บุคคลที่ควรให้ด้วยกำลังกาย กำลังสติปัญญา รวมทั้งการรู้จักสลัดทิ้งอารมณ์ร้ายในตนเอง

7. การประหยัด (Thrifty) คือ การใช้สิ่งของพอเหมาะพอควรให้ได้ประโยชน์มากที่สุด ไม่ให้มี

ส่วนเกินมากนัก รวมทั้งการรู้จักระมัดระวัง รู้จักยับยั้งความต้องการให้อยู่ในกรอบและขอบเขตที่พอเหมาะ

8. ความอุตสาหะ (Diligence) คือ ความพยายามอย่างเข้มแข็ง เพื่อให้เกิดความสำเร็จในงาน

9. ความสามัคคี (Harmony) คือ ความเป็นน้ำหนึ่งใจเดียวกัน มีความพร้อมเพรียงร่วมมือกันกระทำกิจการให้สำเร็จลุล่วงด้วยดี โดยเห็นแก่ประโยชน์ส่วนรวมมากกว่าส่วนตัว

10. ความเมตตาและกรุณา (Loving Kindness and Compassion) คือ ความรักใคร่ปรารถนาจะให้ผู้อื่นมีสุข กรุณา หมายถึง ความสงสาร คิดจะช่วยให้ผู้อื่นพ้นทุกข์

11. ความยุติธรรม (Justice) คือ การปฏิบัติด้วยความเที่ยงตรง สอดคล้องกับความเป็นจริงและเหตุผล ไม่มีความลำเอียง

ความสำคัญของคุณธรรมจริยธรรม

คุณธรรมจริยธรรมนับว่าเป็นพื้นฐานที่สำคัญของคนทุกคนและทุกวิชาชีพ หากบุคคลใดหรือวิชาชีพใดไม่มีคุณธรรมจริยธรรมเป็นหลักยึดเบื้องต้นแล้วก็ยากที่จะก้าวไปสู่ความสำเร็จแห่งตนและแห่งวิชาชีพนั้นๆ ที่ยิ่งกว่านั้นก็คือการขาดคุณธรรมจริยธรรมทั้งในส่วนบุคคลและในวิชาชีพ อาจมีผลร้ายต่อตนเอง สังคมและวงการวิชาชีพในอนาคตได้อีกด้วย ดังจะพบเห็นได้จากการเกิดวิกฤติศรัทธาในวิชาชีพหลายแขนงในปัจจุบัน ทั้งวงการวิชาชีพครู แพทย์ ตำรวจ ทหาร นักการเมืองการปกครอง ฯลฯ จึงมีคำกล่าวว่าเราไม่สามารถสร้างครูดีบนพื้นฐานของคนไม่ดี และไม่สามารถสร้างแพทย์ ตำรวจ ทหารและนักการเมืองที่ดี ถ้าบุคคลเหล่านั้นมีพื้นฐานทางนิสัยและความประพฤติที่ไม่ดี ดังพระบรมราโชวาทพระบาทสมเด็จพระเจ้าอยู่หัวภูมิพลอดุลยเดชฯ ในพระราชพิธีบวงสรวงสมเด็จพระมหากษัตริ-ยาธิราช ณ ท้องสนามหลวง เมื่อวันจันทร์ที่ 5 เมษายน พ. ศ.2525 ไว้ ดังนี้

“.....การจะทำงานให้สัมฤทธิ์ผลที่พึงปรารถนา คือให้เป็นประโยชน์และเป็นธรรมด้วยนั้น จะอาศัยความรู้แต่เพียงอย่างเดียวมิได้ จำเป็นต้องอาศัยความสุจริต ความบริสุทธิ์ใจ และความถูกต้องเป็นธรรม ประกอบด้วย เพราะเหตุว่าความรู้นั้น เสมือนเครื่องยนต์ที่ทำให้ยวดยานเคลื่อนที่ไปได้ประการเดียว ส่วนคุณธรรมดังกล่าวแล้ว เป็นเสมือนหนึ่งพวงมาลัยหรือหางเสือ ซึ่งเป็นปัจจัยที่นำทางให้ยวดยานดำเนินไปถูกทางด้วยความสวัสดี คือ ปลอดภัย บรรลุจุดประสงค์..”

จริยธรรมจึงเป็นสิ่งสำคัญในสังคม ที่จะนำความสุขสงบและความและความเจริญก้าวหน้ามาสู่สังคมนั้นๆ เพราะเมื่อคนในสังคมมีจริยธรรม จิตใจก็ย่อมสูงส่ง มีความสะอาด และสว่างในจิตใจ จะทำการงานใดก็ไม่ก่อให้เกิดความเดือดร้อน ไมก่อให้เกิดทุกข์แก่ตนเองและผู้อื่น เป็นบุคคลมีคุณค่ามีประโยชน์ และสร้างสรรค์คุณงามความดี อันเป็นประโยชน์ต่อบ้านเมืองต่อไป

วศิน อินทสระ (2562 : 6-9) นักปราชญ์ทางพระพุทธศาสนาได้กล่าวถึงความสำคัญและประโยชน์ของจริยธรรมดังจะกล่าวโดยย่อดังนี้

1.จริยธรรมเป็นรากฐานอันสำคัญแห่งความเจริญรุ่งเรือง ความมั่นคงและความสงบสุขของปัจเจกชน สังคมและประเทศชาติอย่างยิ่ง รัฐควรส่งเสริมประชาชนให้มีจริยธรรมเป็นอันดับแรกเพื่อให้เป็นแกนกลางของการพัฒนาด้านอื่นๆ ทั้งเศรษฐกิจ การศึกษา การเมืองการปกครอง ฯลฯ การพัฒนาที่ขาดจริยธรรมเป็นหลักยึดย่อมเกิดผลร้ายมากกว่าดี เพราะผู้มีความรู้แต่ขาดคุณธรรมย่อมก่อให้เกิดความเสื่อมเสียได้มากกว่าผู้ด้อยความรู้ โดยท่านกล่าวว่า “ผู้มีความรู้แต่ไม่รู้วิธีที่จะประพฤติตน ย่อมก่อให้เกิดความเสื่อมเสียได้มากกว่าผู้มีความรู้น้อย ถ้าเปรียบความรู้เหมือนดิน จริยธรรมย่อมเป็นเหมือนน้ำ ดินที่ไม่มีน้ำยึดเหนี่ยวเกาะกุมย่อมเป็นฝุ่นละอองให้ความรำคาญ

มากกว่าให้ประโยชน์ คนที่มีความรู้แต่ไม่มีจริยธรรมจึงมักเป็นคนที่ก่อความรำคาญหรือเดือดร้อนให้แก่ผู้อื่นอยู่เนืองๆ”

2. การพัฒนาบ้านเมือง ต้องพัฒนาจิตใจคนก่อน หรืออย่างน้อยก็ให้พร้อมๆไปกับการพัฒนาเศรษฐกิจ สังคม การศึกษาวิชาการอื่นๆ เพราะการพัฒนาที่ไม่มีจริยธรรมเป็นแกนนำนั้นจะสูญเปล่าและเกิดผลเสียเป็นอันมากทำให้บุคคลลุ่มหลงในวัตถุและอบายมุข การที่เศรษฐกิจต้องเสื่อมโทรม ประชาชนทุกข์ยาก เพราะคนในสังคมละเลยจริยธรรม กอบโกยทรัพย์สินเป็นประโยชน์ส่วนตัวมากเกินไปขาดความเมตตาปราณี แล้งน้ำใจในการดำเนินชีวิตซึ่งกันและกัน

3. จริยธรรม มิได้หมายถึง การถือศีล กินเพล เข้าวัดฟังธรรม จำศีลภาวนา โดยไม่ช่วยเหลือทำประโยชน์ให้แก่สังคม แต่จริยธรรมหมายถึงความประพฤติ การกระทำและความคิดที่ถูกต้องเหมาะสมการทำหน้าที่ของตนอย่างถูกต้องสมบูรณ์ เว้นสิ่งควรเว้น ทำสิ่งควรทำ ด้วยความฉลาดรอบคอบ รู้เหตุรู้ผลถูกต้องตามกาลเทศะและบุคคล ดังนั้นจะเห็นว่าจริยธรรมจึงจำเป็นและมีคุณค่าสำหรับทุกคนในทุกวิชาชีพทุกสังคม สังคมจะอยู่รอดด้วยจริยธรรม

4. การทุจริต คดโกง การเบียดเบียนกันในรูปแบบต่างๆอันเป็นเหตุให้สังคมเสื่อมโทรม มีสาเหตุมาจากการขาดจริยธรรมของคนในสังคม ทรัพยากรธรรมชาติในโลกนี้น่าจะพอเลี้ยงชาวโลกไปได้อีกนาน ถ้าชาวโลกช่วยกันละทิ้งความละโมบโลภมาก แล้วมามีชีวิตอยู่อย่างเรียบง่าย ช่วยกันสร้างสรรค์สังคม ยึดเอาจริยธรรมเป็นทางดำเนินชีวิต ไม่ใช่ยึดเอาลาภยศความมีหน้ามีตาในสังคมเป็นจุดหมาย ถ้าสิ่งนั้นจะเกิดขึ้นก็ถือเป็นเพียงผลพลอยได้และนำมาใช้เป็นเครื่องมือในการประพฤติธรรม เช่น อาศัยลาภผลเป็นเครื่องมือในการบำเพ็ญสาธารณประโยชน์อาศัยยศและความมีหน้ามีเกียรติในสังคมเป็นเครื่องมือในการจูงใจคนผู้เคารพนับถือเข้าหาธรรม

5. จริยธรรมสอนให้เราเลิกดูหมิ่นกดขี่คนจน ให้เอาใจใส่ดูแลเอื้ออาทรต่อผู้สูงอายุ ซึ่งเป็นบุพการีของชาติ สอนให้เราถ่อมตัวเพื่อเข้าหากันได้ดีกับคนทั้งหลาย และไม่วางโตโอหังอวดดีหรือก้าวร้าวผู้อื่น สอนให้เราลดทิฏฐิมานะลงให้มากๆเพื่อจะได้มองเห็นสิ่งต่างๆตามความจริง ไม่หลงสำคัญตัวว่ารู้ดีกว่า มีความสามารถกว่าใคร ผู้นำที่มีจริยธรรมสูงย่อมเป็นที่เคารพกราบไหว้ของทั้งหลายได้อย่างสนิทใจ เราควรเลือกผู้นำที่สามารถนำความสงบสุขทางใจมาสู่มวลชนได้ด้วย เพื่อสันติสุขจะเกิดขึ้นทั้งภายในและภายนอก ความแข็งแกร่งทางกำลังกายกำลังทรัพย์และอาวุธนั้น ถ้าปราศจากความแข็งแกร่งทางจริยธรรมเสียแล้ว บุคคลหรือประเทศชาติจะมั่นคงอยู่ได้ไม่นาน สังคมที่เจริญมั่นคงต้องมีจริยธรรมเป็นเครื่องรับรอบหรือเป็นแกนกลาง เหมือนถนนที่มั่นคงหรือตึกที่แข็งแรงเขาใช้คอนกรีตเสริมเหล็กแม้เหล็กจะไม่ปรากฏออกมาให้เห็นภายนอก แต่มีความสำคัญอยู่ภายในนายช่างย่อมรู้ดี ทำนองเดียวกันกับบัณฑิตย่อมมองเห็นอย่างแจ่มแจ้งว่าจริยธรรมมีความสำคัญในสังคมเพียงใด

โสคราตีส (2560: 1) กล่าวถึงคุณธรรมว่า คุณธรรมคือความรู้ การแสวงหาความรู้เกี่ยวกับศีลธรรม จริยธรรม คือการแสวงหาคุณธรรม เพราะคุณธรรมคือความรู้ที่แท้จริง ถ้าบุคคลรู้และเข้าใจถึงธรรมชาติของความดีจริงๆ แล้ว เขาจะไม่พลาดจากการประกอบความดีละเว้นความชั่ว คุณธรรมที่ทำให้คนเป็นมนุษย์มี 5 ประการ คือ

1. ปัญญา หรือความรู้ หมายถึง รู้ว่าอะไรดี อะไรไม่ดี

2. การปฏิบัติหน้าที่ทางศาสนา คือ การทำความดี การเคารพยกย่องสิ่งที่ควรเคารพ เช่น พระผู้เป็นเจ้า พระธรรม การปฏิบัติตามคำสอนของศาสนา

3. ความกล้าหาญ คือกล้าในสิ่งควรกล้าและกลัวในสิ่งควรกลัว

4. การควบคุมตนเอง คือ การใช้ปัญญาควบคุมอารมณ์ ความรู้สึก

5. ยุติธรรม คือการปฏิบัติต่อผู้อื่น และต่อตนเองอย่างเหมาะสม ไม่เบียดเบียนตนเองและผู้อื่น

เพลโต (2560:1) กล่าวว่า คุณธรรม คือ การปฏิบัติที่ดีตามหน้าที่ของวิญญาณ และคุณธรรมไม่สารถเกิดขึ้นได้โดยบังเอิญ เพราะมนุษย์จะต้องรู้ว่าเขากำลังทำอะไร เพื่ออะไร และทำอย่างไร คุณธรรมจึงเกิดขึ้นจากความรู้ ไม่ใช่ความรู้ทฤษฎี แต่เป็นความรู้ที่มาจากการปฏิบัติจริง คุณธรรมตามแนวคิดของเพลโต มี 4 ประการ คือ

1. ปัญญาหรือความรู้ คือการหยั่งรู้ว่าอะไรถูก อะไรผิด อะไรดี อะไรไม่ดี อะไรควรประพฤติหรือไม่ควรประพฤติ

2. ประมาณ คือ การรู้จักควบคุมตัวเองให้อยู่ในขอบเขตของจุดมุ่งหมายชีวิต มีความรับผิดชอบ รู้จักบทบาทหน้าที่ของตนเอง

3. กล้าหาญ คือ กล้าเสี่ยงต่อความยากลำบาก อันตราย เพื่ออุดมการณ์ของตนเอง หรือด้วยความมั่นใจว่าได้กระทำดีที่สุดแล้ว

4. ยุติธรรม คือการให้แก่ทุกคนอย่างเหมาะสม เช่น การให้แก่ตนเอง ครอบครัว มิตรสหาย ผู้บังคับบัญชา ผู้ใต้บังคับบัญชา อย่างมีเหตุผลอันควร

อริสโตเติล (2560:1) ได้นำคุณธรรมของเพลโต มาอธิบายว่าคุณธรรม ได้แก่ การเดินสายกลางระหว่างความไม่พอดีกับความพอดี หรือคุณธรรมคือความพอดีพองาม ไม่เอียงสุดไปทางด้านใดด้านหนึ่ง เช่น ความกล้าหาญจะอยู่ระหว่างความบ้าบิ่นกับความขลาด ความสุภาพอยู่ระหว่างความขี้อายกับความไร้ยางอาย และความเอื้อเฟื้ออยู่ระหว่างความฟุ่มเฟือยกับความตระหนี่ คุณธรรมจึงแบ่งออกเป็น 2 ประเภทคือ

1. คุณธรรมทางสติปัญญา เป็นเรื่องของความรู้ทั้งภาคทฤษฎีและภาคปฏิบัติ เป็นส่วนหนึ่งของวิญญาณที่มีเหตุผล และหน้าที่ของวิญญาณคือการรู้และค้นหาความจริงนั่นเอง

2. คุณธรรมทางศีลธรรม เป็นส่วนหนึ่งของวิญญาณ อยู่ในรูปคำสอน ละมุ่งเพื่อความดีงาม คนมีคุณธรรมก็คือคนที่มีความพอดี ทำด้วยเจตนาดี มีเหตุผล เห็นแก่ส่วนรวม อริสโตเติลเสนอคุณธรรมพิเศษไว้ 4 ประการ คือ มิตรภาพ ประมาณ กล้าหาญ และยุติธรรม

ดังนั้น จะเห็นได้ว่า แนวคิด หลักการ ทฤษฎีทางคุณธรรมจริยธรรมนั้น มีความสอดคล้องสัมพันธ์กัน ไม่ว่าจะเป็นหลักคำสอนในทางพระพุทธศาสนา และหลักปรัชญาทั้งประเทศทางตะวันออก และตะวันตก ในส่วนที่ว่าสัมพันธ์กับหลักของคำสอนในทางพระพุทธศานา ซึ่งจัดเป็นหลักพุทธจริยศาสตร์ระดับต้น ที่พระพุทธเจ้าได้ทรงบัญญัติไว้ เพื่อความสงบเรียบร้อยของคนในสังคม เช่น หลักของศีล 5 ข้อที่ 2 ที่ว่า อทินนาทานา เวรมณี หมายถึง การเว้นจากการลักทรัพย์ หรือทรัพย์ที่เจ้าของเขาไม่ได้ให้สอดคล้องกับความหมายในการไม่ละเมิดจริยธรรมทางด้านเทคโนโลยีสารสนเทศ ได้แก่ การไม่ลักทรัพย์ที่เป็นฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล การเจาะระบบเพื่อล้วงความลับทางการค้าต่างๆ รวมถึงทรัพย์สินทางปัญญาอื่นๆ

แนวคิด หลักการ ทฤษฎีเรื่องความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ

การี่ บี. เชอร์รี่ : Gary B. Shelly (2006:556) ได้แสดงทรรศนะเกี่ยวกับเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศด้วยระบบที่เรียกว่า ไบโอเมตทริกซ์เทคโนโลยี (Biometrics Technologies) คือ เทคโนโลยีที่สำหรับยืนยันตัวบุคคล โดยผสมผสานเทคโนโลยี

ทางด้านชีวภาพ และทางการแพทย์เข้าด้วยกัน หรือแนวคิดการนำเอาเทคโนโลยีด้านชีวภาพทางการแพทย์ และเทคโนโลยีด้านคอมพิวเตอร์มาบูรณาการเข้าด้วยกัน เพื่อใช้กำหนดหรือระบุคุณลักษณะเฉพาะส่วนบุคคลทั้งด้านกายภาพ และพฤติกรรม ได้แก่ ลายพิมพ์นิ้วมือ ฝ่ามือ ม่านตา ใบหน้า เสียงพูด ลายเซ็น ดีเอ็นเอ เป็นต้น ซึ่งการพิสูจน์คุณลักษณะเฉพาะส่วนบุคคลด้วยวิธีการเช่นนี้ เป็นวิธีการที่แม่นยำและได้รับความน่าเชื่อถือมากที่สุด เนื่องจากมนุษย์ที่เกิดมาทุกคน ย่อมมีลักษณะเฉพาะเหล่านี้ไม่เหมือนกัน แม้กระทั่งพี่น้องฝาแฝดที่เกิดไล่เลี่ยกันเพียงไม่กี่นาที เคยมีผลสรุปทางวิทยาศาสตร์กล่าวว่า มนุษยชาติจำนวน 600 ล้านคน เมื่อผ่านมาเป็นระยะเวลา 300 ปี จะมีโอกาสที่ลายนิ้วมือซ้ำกันเพียง 1 คู่เท่านั้น ในส่วนของทารกเมื่ออยู่ในครรภ์มารดาเป็นเวลา 7 เดือนก็มีลายนิ้วมือเป็นของตัวเอง ครั้นเมื่อเจริญเติบโตขึ้นมาเป็นผู้ใหญ่ เส้นลายมือเหล่านั้นไม่ได้เปลี่ยนแปลงเลย เมื่อพบอุบัติเหตุกับลายนิ้วมือ ลายมือ ร่างกายก็จะทำการซ่อมแซมส่วนที่สึกหรอได้ดังเดิม เพราะฉะนั้นธรรมชาติของลายมือจึงเป็นเอกลักษณ์ของแต่ละบุคคล (www.hitop.co.th) ลักษณะการทำงานของเทคโนโลยี Biometrics นั้น จะมีการแปลคุณลักษณะเฉพาะส่วนบุคคลผ่านเข้าไปทางอุปกรณ์นำเข้าข้อมูล (Input) และแปลงเป็นรหัสดิจิตอล เพื่อทำการเปรียบเทียบกับรหัสดิจิตอลที่ถูกจัดเก็บไว้ในคอมพิวเตอร์ ถ้ารหัสดิจิตอลในคอมพิวเตอร์นั้นไม่สัมพันธ์กับ (Match) รหัสคุณลักษณะส่วนบุคคล คอมพิวเตอร์นั้นก็จะปฏิเสธการเข้าถึงข้อมูลนั้นทันที Biometrics เทคโนโลยีที่ได้รับความนิยมอย่างแพร่หลายในปัจจุบันมีหลายประเภท คือ :

- เครื่องสแกนลายพิมพ์นิ้วมือ (Fingerprint Scanner) ซึ่งราคาปัจจุบันประมาณ 1 ดอลล่าร์สหรัฐ โดยสามารถนำเอาเทคโนโลยีนี้ไปใช้ภายในบ้าน หรือในธุรกิจขนาดเล็ก บางบริษัทซื้อเครื่องคอมพิวเตอร์ชนิดที่มีเครื่องพิมพ์ลายนิ้วมือติดกับแป้นพิมพ์มาด้วย เพื่อให้พนักงานพิมพ์ลายนิ้วมือแทนการเข้าชื่อผู้ใช้ (User Name) และรหัสผ่าน (Password) ก่อนเข้าใช้งานคอมพิวเตอร์, โน้ตบุ๊คคอมพิวเตอร์ หรือแม้กระทั่งการเข้าสู่เว็บไซต์ ตามร้านขายของชำ และร้านขายปลีก ในปัจจุบันมีการนำเอาเครื่องสแกนลายพิมพ์นิ้วมือเข้าไปใช้กันเป็นจำนวนมาก โดยเฉพาะเกี่ยวกับเรื่องการชำระเงิน ไม่ว่าลูกค้าจะอยู่ที่ไหน ลูกค้าสามารถผ่านการพิมพ์ลายนิ้วมือลงบนเครื่องพิมพ์ลายนิ้วมือ เสร็จแล้วก็จะมีการเชื่อมโยงไปในเรื่องทฤษฎีการเลือกชำระเงินว่าผู้ใช้เลือกใช้รูปแบบไหน ซึ่งระบบจะมีการตรวจสอบบัญชีของลูกค้า รวมทั้งสินเชื่อบัตรเครดิตของลูกค้าได้ด้วย

ภาพประกอบ 1.1 การสแกนลายพิมพ์นิ้วมือเพื่อตรวจสอบเอกลักษณ์ส่วนบุคคลของนักท่องเที่ยว (Gary B. Shelly, 2007:568)

- ระบบเครื่องจดจำใบหน้า (A Face Recognition Systems) โดยระบบจะดึงรูปภาพของใบหน้า และทำการเปรียบเทียบกับรูปภาพจริงของผู้ใช้ที่ถูกต้องตามกฎหมาย ระบบการจดจำใบหน้านี้ถูกพัฒนาขึ้นมาใช้เพื่อรักษาความปลอดภัยของผู้ที่เดินเข้าออกในห้องทำงาน, การดำเนินการกับผู้กระทำผิดทางกฎหมาย, การตรวจตรารักษาความปลอดภัย และใช้จดจำใบหน้าของบุคคลที่ผ่านเข้าออกตามสนามบินเพื่อป้องกันความปลอดภัย เครื่องโน้ตบุ๊คคอมพิวเตอร์บางชนิดใช้เทคโนโลยีนี้ เพื่อรักษาความปลอดภัยของคอมพิวเตอร์ เครื่องคอมพิวเตอร์จะไม่สามารถทำงานได้หากผู้ใช้คนนั้นไม่มีสิทธิ์โดยชอบด้วยกฎหมาย เทคโนโลยีนี้มีความชาญฉลาดมาก มันสามารถที่จะจดจำคนได้ทั้งคนที่สวมแว่นตา และไม่ได้สวมแว่นตา คนที่ไปทำศัลยกรรมตกแต่งใบหน้า หรือคนที่สวมใส่เครื่องประดับ และแม้กระทั่งคนที่ปรับเปลี่ยนทรงผมใหม่ หรือใส่วิกผมปลอมก็ตาม

ภาพประกอบ 1.2 การจดจำใบหน้า, สแกนม่านตา และการพิมพ์ลายเส้นบนฝ่ามือเพื่อทำบัตรประจำตัวที่ได้รับการอนุญาตให้พักอยู่อาศัย (Gary B. Shelly, 2007:568)

- เครื่องพิมพ์ลายเส้นบนฝ่ามือ (A Hand Geometry) อุปกรณ์ชนิดนี้ จะทำการวัดสัณฐานและขนาดของเส้นลายมือบนฝ่ามือของแต่ละบุคคล ซึ่งจะมีลายเส้นที่แตกต่างกันไป ราคาของเครื่องสแกนพิมพ์ลายฝ่ามือนี้ ราคาประมาณ 1,000 ดอลล่าร์สหรัฐ บางองค์กร หรือบางมหาวิทยาลัย ใช้อุปกรณ์ชนิดนี้ เพื่อลงเวลาการเข้าทำงานของพนักงาน ซึ่งเป็นเสมือนระบบการรักษาความปลอดภัยไปในตัว ใช้ตรวจสอบนักศึกษาที่เข้าไปใช้ห้องสันทนาการ หรือแม้กระทั่งในสถานที่รับเลี้ยงเด็ก และโรงพยาบาล ก็ใช้เทคโนโลยีนี้ สำหรับตรวจสอบผู้ปกครองที่มารับเด็กและบุตรของตน (http://nwes.bbc.co.uk)
- ระบบการพิสูจน์หรือจดจำเสียง (A Voice Verification System) ระบบนี้จะทำการเปรียบเทียบเสียงพูดสดจริงกับรูปแบบของเสียงที่ถูดจัดเก็บเอาไว้ว่าตรงกันหรือไม่ บางองค์กรใช้เทคโนโลยีนี้ลงเวลาการเข้าทำงาน และมีอีกหลายบริษัทใช้เทคโนโลยีนี้ ในการเข้าถึงแฟ้มข้อมูลและเครือข่ายคอมพิวเตอร์ที่เสี่ยงต่อความเสียหายได้ง่าย หรือแฟ้มข้อมูลที่เป็นความลับขององค์กร สถาบันการเงินบางแห่งใช้เพื่อรักษาความปลอดภัยเกี่ยวกับการประมวลรายการทางธุรกิจของธนาคารผ่านโทรศัพท์ (Telephone Banking)

- ระบบการตรวจพิสูจน์ลายเซ็น (A Signature Verification System) เทคโนโลยีนี้.ใช้การจดจำรูปร่างเส้นสายลายเซ็นซึ่งเซ็นโดยใช้ปากกาพิเศษหรือปากกาสำหรับรับข้อมูลเข้าสู่คอมพิวเตอร์ (Tablet) โดยจะวัดจากแรงกด และอารมณ์ในการเซ็น (Gary B. Shelly : 2008 : 263)
- ระบบการจดจำม่านตา (Iris Recognition System) เป็นระบบรักษาความปลอดภัยที่มีประสิทธิภาพสูงมาก โดยจะมีกล้องสำหรับถ่ายรูปม่านตาของคน และอ่านจดจำบันทึกเปรียบเทียบรูปแบบของม่านตาที่ถูกจัดเก็บไว้ในคอมพิวเตอร์เช่นเดียวกับการพิมพ์ลายนิ้วมือ ระบบการจดจำม่านตามีราคาแพงมาก ส่วนใหญ่มักใช้ในการรักษาความปลอดภัยในหน่วยงานของรัฐบาล ในกองทัพ รวมถึงสถาบันทางด้านการเงิน ในมลรัฐเท็กซัสมีการใช้เทคโนโลยีนี้ ในการทำบัตร ATM ให้กับลูกค้า และสามารถเบิกถอนเงินสดได้อย่างรวดเร็ว

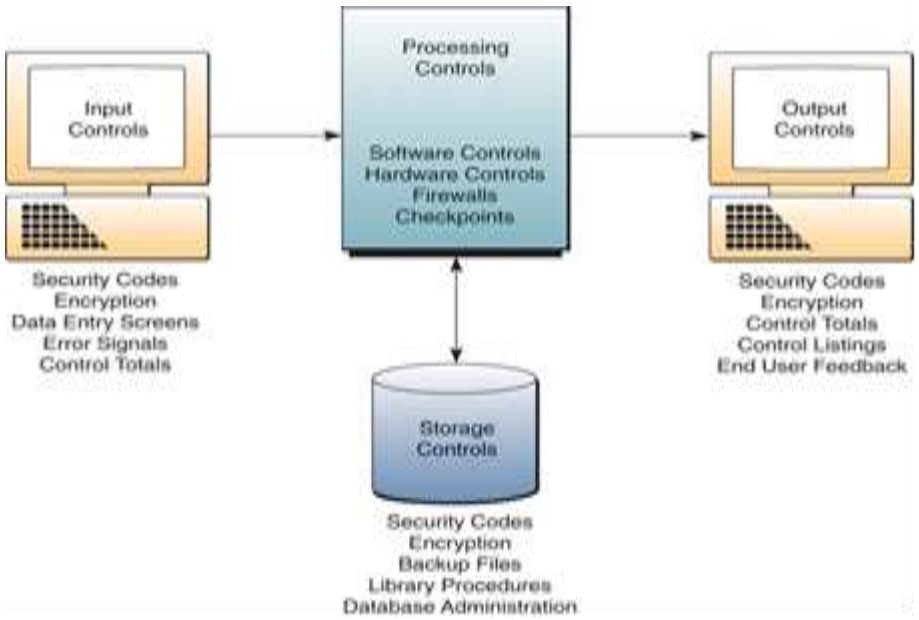
ดังนั้นจะเห็นได้ว่า Biometrics เทคโนโลยี มีประโยชน์มาก สามารถใช้งานได้ง่าย เป็นที่ยอมรับของผู้ใช้ และมีอัตราเสี่ยงต่อการติดเชื้อต่ำ เนื่องจากไม่ต้องนำอวัยวะที่ไวต่อการติดเชื้อ เช่น ดวงตา ไปสัมผัสกับอุปกรณ์ที่ใช้ในการอ่านข้อมูล นอกจากนั้น ยังเป็นการเพิ่มความปลอดภัยให้กับองค์กรและประเทศชาติได้ หากมีบุคคลผู้ต้องสงสัยเข้ามาโดยมีจุดประสงค์ร้ายหรือก่อการร้าย (www.matcom.co.th) ในปัจจุบันมีการนำเอา Biometric เทคโนโลยีนี้มาใช้กันอย่างแพร่หลาย เพราะถือว่าเป็นระบบการรักษาความปลอดภัยที่มีประสิทธิภาพสูงมาก เช่น การจัดเก็บฐานข้อมูลของเหล่าอาชญากร การตรวจสอบคนเข้าเมือง การตรวจจับผู้ร้ายข้ามแดนและยังมีธนาคารอีกเป็นจำนวนมากใช้เทคโนโลยีเหล่านี้ เพื่อป้องกันปัญหาอาชญากรรมต่างๆ ที่อาจจะเกิดขึ้นได้จากการระบุตัวบุคคลผิดพลาด

- การควบคุมความล้มเหลวของ คอมพิวเตอร์ (Computer Failure Controls) เมื่อคอมพิวเตอร์เกิดความล้มเหลว ย่อมทำให้เสียใจ สาเหตุอาจมาจากสิ่งเหล่านี้ คือกระแสไฟแรง ต่ำ กระชาก, ไวรัสคอมพิวเตอร์, ปัญหาเรื่องการสื่อสารเครือข่ายทางไกล เป็นต้น ดังนั้น ต้องมีระบบป้องกันความปลอดภัยที่ดี
- ระบบทนทานต่อข้อผิดพร่อง (Fault Tolerant Systems) หลายบริษัทที่เคยใช้เครื่องคอมพิวเตอร์ ล้วนเจอะเจอกับปัญหาต่างๆ ที่เกิดข้อบกพร่องขึ้นจากการทำงานของเครื่องคอมพิวเตอร์ ไม่ว่าจะเป็นการประมวลผลข้อมูลที่ซ้ำซ้อน, อุปกรณ์รอบข้างคอมพิวเตอร์มีปัญหา, หรือองค์ประกอบการทำงานของซอฟต์แวร์ และฮาร์ดแวร์ไม่สมบูรณ์ ทำให้เกิดความหงุดหงิด หรือความเสียหายบางอย่าง ซึ่งก็ต้องจำทนรับสภาพกับเหตุการณ์ที่เกิดขึ้น ซึ่งไม่รู้ว่าจะเกิดขึ้นตอนไหน และเมื่อไหร่ ขึ้นอยู่กับช่วงเวลาของการใช้งาน
- การกู้คืนข้อมูลที่เสียหาย (Disaster Recovery) ในปัจจุบันภัยคุกคามที่เกิดขึ้นมีมากมาย ทั้งที่มาจากธรรมชาติ คือ แผ่นดินไหว, น้ำท่วม, โคลนถล่ม, ลมพายุ, ภูเขาไฟระเบิด หรือความเสียหายที่เกิดจากฝีมือมนุษย์ คือ ไฟไหม้, การทำลายข้อมูลขององค์กรโดยรู้เท่าไม่ถึงการณ์ หรือแม้ปัญหาเรื่องสุขภาพ สิ่งเหล่านี้ล้วนเป็นอันตรายต่อการทำธุรกิจพาณิชย์อิเล็กทรอนิกส์, การขายส่ง-ขายปลีก สายการบิน และธนาคาร ดังนั้น องค์กรหรือบริษัทต้องมีการพัฒนาคู่มือการกู้คืนข้อมูลที่เสียหายจากภัยเหล่านี้ เรียกว่า การวางแผนการกู้คืนข้อมูลที่เสียหาย (Disaster Recovery Plan) เพื่อป้องกันความเสียหายที่จะเกิดขึ้น

แนวคิด หลักการ ทฤษฎีระบบการควบคุมและตรวจสอบ (System Controls and Audits)

การจัดการควบคุมความปลอดภัยที่จะกล่าวถึงสุดท้าย ซึ่งเป็นเรื่องจำเป็นต้องมี ทั้งนี้เพื่อดูแลระบบสารสนเทศให้มีความปลอดภัย และสามารถใช้งานในองค์กรได้ต่อไป ซึ่งเรื่องที่จะกล่าวถึงนี้ 2 เรื่อง คือ การควบคุมระบบสารสนเทศ และการตรวจสอบความปลอดภัยด้านเทคโนโลยีสารสนเทศ

- การควบคุมระบบสารสนเทศ (Information System Controls) การควบคุมระบบสารสนเทศเกี่ยวข้องกับทฤษฎีความพยายามที่จะทำให้ข้อมูลสารสนเทศมีความถูกต้อง ไม่มีข้อผิดพลาด หรือการป้องกันทรัพย์สินทางปัญญา การควบคุมระบบสารสนเทศ จำเป็นต้องพัฒนาระบบขึ้นมา นั่นคือ (1) การป้อนข้อมูล (Data Entry), (2) ทฤษฎีเทคนิคการประมวลผล (Processing Techniques), (3) ทฤษฎีการจัดเก็บข้อมูล (Storage Methods) และ (4) การแสดงผลลัพธ์ของสารสนเทศ (Information Output) นอกจากนี้ การควบคุมระบบสารสนเทศ ต้องมีการออกแบบการติดตามและการดูแลคุณภาพ และความปลอดภัยของการนำเข้าข้อมูล, การประมวลผล, การแสดงผลลัพธ์ และการจัดเก็บสารสนเทศด้วย



ภาพประกอบ 1.3 การควบคุมความปลอดภัยของระบบสารสนเทศ
(James A.O'Brien : 2008 : 527)

- การตรวจสอบความปลอดภัยของเทคโนโลยีสารสนเทศ (Auditing IT Security) การตรวจสอบโดยปกติแล้วจะมีทั้งการตรวจสอบภายในโดยพนักงานและผู้บริหาร และมีการตรวจสอบภายนอก ซึ่งส่วนใหญ่จะเป็นผู้ทรงวุฒิจากภายนอก เช่น ระบบการตรวจสอบด้านบัญชี สำหรับในทางธุรกิจต้องมีการตรวจสอบความซื่อสัตย์ในการทำงานที่เรียกว่า ตามรอยตรวจสอบ (Audit Trail) ซึ่งจะตรวจสอบเกี่ยวกับเรื่องเอกสาร หรือคู่มือการปฏิบัติงาน ในส่วนของเทคโนโลยีสารสนเทศ หรือระบบคอมพิวเตอร์ทั้งหมด จะมีการตรวจสอบโดยใช้ซอฟท์แวร์เข้ามาตรวจสอบที่เรียกว่า ตรวจสอบการประมวลผลข้อมูลอิเล็กทรอนิกส์ (Electronic Data Processing : EDP) ซึ่งก็จะทำให้ข้อมูลและเทคโนโลยีสารสนเทศมีความผิดพลาดน้อยลง

แนวคิดเกี่ยวกับการจัดการเทคโนโลยีสารสนเทศ

การนำเทคโนโลยีสารสนเทศมาใช้ จำเป็นต้องอาศัยงบประมาณค่าใช้จ่ายด้านวัสดุอุปกรณ์สูง ไม่ว่าจะเป็นระบบคอมพิวเตอร์ ซอฟต์แวร์ และระบบเครือข่าย ต้องมีผู้เชี่ยวชาญพร้อมผู้ปฏิบัติงานที่มีความสามารถ รวมทั้งการวางแผนการพัฒนาระบบและการนำวัสดุอุปกรณ์ไปใช้อย่างรอบคอบรัดกุม จึงจะบรรลุผลตามเป้าหมาย แม้เทคโนโลยีสารสนเทศจะมีประโยชน์ แต่การนำมาใช้ให้เกิดประสิทธิภาพและประสิทธิผลสูงสุดไม่ใช่เรื่องง่าย เพราะเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงอยู่ตลอดเวลา เช่น ซอฟต์แวร์บางตัว กว่าจะเรียนรู้วิธีใช้ประโยชน์ได้ครบถ้วน อาจมีซอฟต์แวร์รุ่นใหม่ออกจำหน่ายอีกแล้ว การจัดการเทคโนโลยีสารสนเทศจึงต้องมีวิธีการที่เหมาะสม มิฉะนั้นอาจเกิดปัญหากับหน่วยงานได้

การจัดการเทคโนโลยีสารสนเทศ ลัดดา โกรส (2553:1) สามารถจำแนกเป็นกลยุทธ์การจัดการที่สำคัญ 3 ด้าน คือ กลยุทธ์ระบบสารสนเทศ กลยุทธ์เทคโนโลยีสารสนเทศ และกลยุทธ์ระบบการจัดการสารสนเทศ ซึ่งกลยุทธ์ทั้ง 3 นี้ ต้องสัมพันธ์และสอดคล้องกับนโยบายกลยุทธ์ วัตถุประสงค์ แผนงานขององค์การรวมทั้งวิธีการดำเนินงาน กล่าวคือ ต้องการจัดทำระบบสารสนเทศอะไร ใครเป็นผู้ใช้ระบบ ใช้ในงานลักษณะใด ใช้เทคโนโลยีสารสนเทศอะไรในการสร้างระบบจึงจะบรรลุผลสำเร็จ ตามวัตถุประสงค์ และมีระบบการจัดการอะไรในการจัดสรรทรัพยากรควบคุมการใช้ให้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

1. กลยุทธ์ระบบสารสนเทศ คือ การกำหนดระบบสารสนเทศที่ต้องการว่า ต้องการสร้างระบบสารสนเทศอะไร (What) และเพราะอะไร (Why) เช่น เป็นระบบสารสนเทศทั้งองค์การ หรือเป็นระบบระดับฝ่ายงานในองค์การ ลักษณะและรูปแบบของสารสนเทศที่ต้องการคืออะไร ซึ่งความต้องการสารสนเทศต้องสอดคล้องกับแผนกลยุทธ์ขององค์การ ซึ่งเป็นแผนงานองค์การที่กำหนดว่าหน่วยงานควรมีระบบสารสนเทศอะไรบ้างในช่วง 3 ถึง 5 ปีข้างหน้า รวมทั้งแผนปฏิบัติการประจำปีเพื่อให้สนองเป้าหมายดังกล่าว ระบบเหล่านี้มีโครงสร้างข้อมูล ฐานข้อมูลอะไร และมีความสัมพันธ์กันอย่างไร การกำหนดความต้องการระบบสารสนเทศว่า องค์การต้องการระบบใด อาจใช้การวิเคราะห์ระบบสารสนเทศของทั้งองค์การ จำแนกตามหน้าที่การทำงาน กระบวนการทำงาน และข้อมูลที่ต้องใช้ หรืออาจใช้การวิเคราะห์เชิงกลยุทธ์ โดยใช้วิธีวิเคราะห์ปัจจัยแห่งความสำเร็จ

โดยทั่วไประบบสารสนเทศในองค์การจำแนกได้หลายประเภท ได้แก่ ระบบสารสนเทศตามระดับการจัดการในองค์การ ระบบสารสนเทศตามหน้าที่งาน และระบบสารสนเทศสนับสนุนการทำงานขององค์การ ซึ่งบางระบบอาจเป็นสามารถจำแนกได้มากกว่าหนึ่งประเภท และระบบสารสนเทศใดๆ ก็อาจนำไปใช้เป็นระบบสารสนเทศเชิงกลยุทธ์ก็ได้ขึ้นอยู่กับกลยุทธ์ขององค์การในขณะนั้น เช่น ระบบสารสนเทศบริหารลูกค้าสัมพันธ์ ใช้เป็นกลยุทธ์เพื่อรักษาลูกค้าเดิม และหาลูกค้าใหม่ ระบบสารสนเทศการบัญชีเป็นระบบงานของฝ่ายบัญชี แต่อาจนำผลหรือสารสนเทศที่ได้ไปใช้ในระบบสนับสนุนการตัดสินใจ เป็นต้น

2. กลยุทธ์เทคโนโลยีสารสนเทศ คือ การนำเทคโนโลยีสารสนเทศไปใช้ เพื่อจัดทำหรือพัฒนาระบบสารสนเทศ โดยพิจารณาว่า ระบบสารสนเทศที่ต้องการนั้นมีกิจกรรมหรือกระบวนการทำงานใด ที่ต้องใช้เทคโนโลยี ใช้อุปกรณ์ เทคนิคอะไร จะทำได้อย่างไร (How) เป็นต้นว่า ต้องการเครื่องคอมพิวเตอร์แบบใด จำนวนเท่าไร ซอฟต์แวร์อะไร อุปกรณ์สำหรับใช้บันทึก จัดเก็บข้อมูล และ

แสดงผลลัพธ์ ระบบจัดการฐานข้อมูล และฐานข้อมูลที่เกี่ยวข้อง รวมถึงการสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์ต่าง ๆ เพื่อนำไปใช้ในงานแต่ละงานที่เกี่ยวข้อง

3. กลยุทธ์ระบบการจัดการสารสนเทศ คือ การบริหารจัดการเพื่อให้การจัดทำระบบสารสนเทศสำเร็จตามวัตถุประสงค์และเป้าหมายที่ตั้งไว้ โดยพิจารณาว่า จะสามารถทำได้อย่างไรและทำอย่างไรจึงเกิดประสิทธิภาพ ดังนั้นกลยุทธ์ระบบการจัดการสารสนเทศจึงเกี่ยวข้องกับประเด็นการจัดการ 3 ประการ คือ 1) ประเด็นปัญหาของการพัฒนาระบบสารสนเทศและ การทำแผนการใช้เทคโนโลยีสารสนเทศ 2) ประเด็นการจัดการทรัพยากรในการจัดการระบบสารสนเทศ ซึ่งได้แก่ การจัดองค์การเทคโนโลยีสารสนเทศ การจัดการทรัพยากรบุคคล ทรัพยากรการเงิน และ 3) ประเด็นการควบคุมความมั่นคงปลอดภัยของระบบสารสนเทศ ลัดดา โกรส (2553)

ยุทธศาสตร์การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

เพื่อให้วิสัยทัศน์และเป้าหมายในการพัฒนาเศรษฐกิจและสังคมด้วยเทคโนโลยีดิจิทัลบรรลุผล แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมจึงได้กำหนด กรอบยุทธศาสตร์การพัฒนา 6 ด้านคือ

ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ จะมุ่งพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูง ที่ประชาชนทุกคนสามารถเข้าถึงและใช้ประโยชน์ได้แบบทุกที่ ทุกเวลา โดยกำหนดให้เทคโนโลยีที่ใช้มีความเร็วพอเพียงกับความต้องการและให้มีราคาค่าบริการที่ไม่เป็นอุปสรรคในการเข้าถึงบริการของประชาชนอีกต่อไป นอกจากนี้ ในระยะยาว โครงสร้างพื้นฐานอินเทอร์เน็ตความเร็วสูง จะกลายเป็นสาธารณูปโภคขั้นพื้นฐาน เช่นเดียวกับถนนไฟฟ้า น้ำประปา ที่สามารถรองรับการเชื่อมต่อของ ทุกคน และทุกสรรพสิ่ง โดยยุทธศาสตร์นี้ประกอบด้วยแผนงานเพื่อขับเคลื่อนยุทธศาสตร์ 4 ด้าน คือ

1. พัฒนาโครงสร้างพื้นฐานอินเทอร์เน็ตความเร็วสูงให้ครอบคลุมทั่วประเทศ มีความทันสมัย มีเสถียรภาพตอบสนองความต้องการใช้งานของทุกภาคส่วนในราคาที่เหมาะสมและเป็นธรรม

2.ผลักดันให้ประเทศไทยเป็นหนึ่งในศูนย์กลางการเชื่อมต่อและแลกเปลี่ยนข้อมูลของอาเซียน โดยเป็นเส้นทางผ่านการจราจรของข้อมูลในภูมิภาค และเป็นที่ตั้งของผู้ประกอบการเนื้อหารายใหญ่ของโลก

3. จัดให้มีนโยบายและแผนบริหารจัดการโครงสร้างพื้นฐาน คลื่นความถี่ และการหลอมรวมของเทคโนโลยีในอนาคต เพื่อให้เกิดการใช้ทรัพยากรของประเทศอย่างมีประสิทธิภาพสูงสุด

4.ปรับรัฐวิสาหกิจโทรคมนาคมให้เหมาะสมกับสถานการณ์และความก้าวหน้าของอุตสาหกรรมดิจิทัลเพื่อให้เท่าทันการเปลี่ยนแปลงในอนาคต

ยุทธศาสตร์ที่ 2 ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล

จะกระตุ้นเศรษฐกิจของประเทศโดยผลักดันให้ภาคธุรกิจไทยใช้เทคโนโลยีดิจิทัลในการลดต้นทุนการผลิตสินค้าและบริการ เพิ่มประสิทธิภาพในการ ดำเนินธุรกิจ ตลอดจนพัฒนาไปสู่การแข่งขันเชิงธุรกิจรูปแบบใหม่ในระยะยาว นอกจากนี้ ยุทธศาสตร์ยังมุ่งเน้นการสร้างระบบนิเวศสำหรับธุรกิจดิจิทัล เพื่อเสริมความสามารถในการแข่งขันของภาคธุรกิจไทยที่จะส่งผลต่อการขยาย

ฐานเศรษฐกิจและอัตราการจ้างงานของไทยอย่างยั่งยืนในอนาคต โดยยุทธศาสตร์นี้ประกอบด้วยแผนงานเพื่อขับเคลื่อนยุทธศาสตร์ 4 ด้าน คือ

1. เพิ่มขีดความสามารถในการแข่งขันของภาคธุรกิจตลอดห่วงโซ่คุณค่า โดยผลักดันธุรกิจให้เข้าสู่ระบบการค้าดิจิทัลสู่สากล และให้เกิดการใช้เทคโนโลยีและข้อมูลเพื่อปฏิรูปการผลิตสินค้าและบริการ

2. เร่งสร้างธุรกิจเทคโนโลยีดิจิทัล (Digital Technology Startup) ให้เป็นฟันเฟืองสำคัญในการขับเคลื่อนเศรษฐกิจดิจิทัล

3. พัฒนาอุตสาหกรรมเทคโนโลยีดิจิทัลของไทยให้มีความเข้มแข็งและสามารถแข่งขันเชิงนวัตกรรมได้ในอนาคต โดยเฉพาะอย่างยิ่งอุตสาหกรรมที่ไทยมีศักยภาพและเป็นอุตสาหกรรมแห่งอนาคต

4. เพิ่มโอกาสทางอาชีพเกษตรและการค้าขายสินค้าของชุมชนผ่านเทคโนโลยีดิจิทัล โดยดำเนินการร่วมกันระหว่างหน่วยงานจากทั้งภาครัฐ ภาคเอกชนและภาคประชาชน

ยุทธศาสตร์ที่ 3 สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล

จะมุ่งสร้างประเทศไทยที่ประชาชนทุกกลุ่มโดยเฉพาะอย่างยิ่งกลุ่มเกษตรกร ผู้ที่อยู่ในชุมชนห่างไกล ผู้สูงอายุ ผู้ด้อยโอกาส และคนพิการ สามารถ เข้าถึงและใช้ประโยชน์จากบริการต่าง ๆ ของรัฐผ่านเทคโนโลยีดิจิทัล มีข้อมูล องค์ความรู้ ทั้งระดับประเทศและระดับท้องถิ่น ในรูปแบบดิจิทัลที่ประชาชนสามารถเข้าถึงและนำไปใช้ประโยชน์ได้โดยง่ายและสะดวก และมีประชาชนที่รู้เท่าทันข้อมูลข่าวสาร และมีทักษะในการใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างมีความรับผิดชอบต่อสังคม โดยยุทธศาสตร์นี้ประกอบด้วยแผนงานเพื่อขับเคลื่อนยุทธศาสตร์ 5 ด้าน คือ

1. สร้างโอกาสและความเท่าเทียมในการเข้าถึงและใช้ประโยชน์จากเทคโนโลยีดิจิทัลสำหรับประชาชนโดยเฉพาะอย่างยิ่งกลุ่มผู้สูงอายุกลุ่มผู้พิการ กลุ่มผู้ที่อยู่อาศัยในพื้นที่ห่างไกล

2. พัฒนาศักยภาพของประชาชนในการใช้เทคโนโลยีดิจิทัลให้เกิดประโยชน์และสร้างสรรค์ รวมถึงความสามารถในการคิดวิเคราะห์ และแยกแยะข้อมูลข่าวสารในสังคมดิจิทัลที่เปิดกว้างและเสรี

3. สร้างสื่อ คลังสื่อและแหล่งเรียนรู้ดิจิทัลเพื่อการเรียนรู้ตลอดชีวิตที่ประชาชนเข้าถึงได้อย่างสะดวก ผ่านทั้งระบบโทรคมนาคม ระบบแพร่ภาพกระจายเสียง และสื่อหลอมรวม

4. เพิ่มโอกาสการได้รับการศึกษาที่มีมาตรฐานของนักเรียนและประชาชน แบบทุกวัย ทุกที่ทุกเวลาด้วยเทคโนโลยีดิจิทัล

5. เพิ่มโอกาสการได้รับบริการทางการแพทย์และสุขภาพที่ทันสมัยทั่วถึง และเท่าเทียม สู่สังคมสูงวัย ด้วยเทคโนโลยีดิจิทัล

ยุทธศาสตร์ที่ 4 ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล

จะมุ่งใช้เทคโนโลยีดิจิทัลในการปรับปรุงประสิทธิภาพการบริหารจัดการของหน่วยงานรัฐทั้งส่วนกลางและส่วนภูมิภาค ให้เกิดบริการภาครัฐในรูปแบบดิจิทัลที่ประชาชนสามารถเข้าถึงบริการได้โดยไม่มีข้อจำกัดทางกายภาพ พื้นที่ และภาษานำไปสู่การหลอมรวมการทำงานของภาครัฐเสมือนเป็นองค์กรเดียว นอกจากนี้ รัฐบาลดิจิทัลในอนาคตจะเปิดโอกาสให้ประชาชนมีส่วนร่วมในการกำหนดแนวทางการพัฒนาสังคมและเศรษฐกิจ การบริหารบ้านเมือง และเสนอความคิดเห็นต่อการดำเนินงานของภาครัฐ โดยยุทธศาสตร์นี้ประกอบด้วยแผนงานเพื่อขับเคลื่อนยุทธศาสตร์ 4 ด้าน คือ

1. จัดให้มีบริการอัจฉริยะที่ขับเคลื่อนโดยความต้องการของประชาชนหรือผู้ใช้บริการ โดยเฉพาะอย่างยิ่งบริการที่อำนวยความสะดวกต่อประชาชนนักธุรกิจ และนักท่องเที่ยว

2. ปรับเปลี่ยนการทำงานของภาครัฐด้วยเทคโนโลยีดิจิทัล ให้มีประสิทธิภาพ และธรรมาภิบาลโดยเน้นบูรณาการการลงทุนในทรัพยากรการเชื่อมโยงข้อมูล และการทำงานของหน่วยงานรัฐเข้าด้วยกัน

3. สนับสนุนให้มีการเปิดเผยข้อมูลที่เป็นประโยชน์ตามมาตรฐาน open data และส่งเสริมให้เกิดการมีส่วนร่วมของประชาชนและภาคธุรกิจในกระบวนการทำงานของรัฐ

4. พัฒนาแพลตฟอร์มบริการพื้นฐานภาครัฐ (government service platform) เพื่อรองรับการพัฒนาต่อยอดแอปพลิเคชั่นหรือบริการรูปแบบใหม่

ยุทธศาสตร์ที่ 5 พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล

จะให้ความสำคัญกับการพัฒนากำลังคนวัยทำงานทุกสาขาอาชีพ ทั้งบุคลากรภาครัฐ และภาคเอกชน ให้มีความสามารถในการสร้างสรรค์และใช้เทคโนโลยีดิจิทัลอย่างชาญฉลาดในการประกอบอาชีพ และการพัฒนาบุคลากรในสาขาเทคโนโลยีดิจิทัลโดยตรง ให้มีความรู้ ความสามารถและความ เชี่ยวชาญเฉพาะด้าน ในระดับมาตรฐานสากลเพื่อนำไปสู่การสร้างและจ้างงานที่มีคุณค่าสูงในยุคเศรษฐกิจและสังคมที่ใช้เทคโนโลยีดิจิทัลเป็นปัจจัย หลักในการขับเคลื่อน โดยยุทธศาสตร์นี้ประกอบด้วยแผนงานเพื่อขับเคลื่อนยุทธศาสตร์ 3 ด้าน คือ

1. พัฒนาทักษะด้านเทคโนโลยีดิจิทัลให้แก่บุคลากรในตลาดแรงงาน ที่รวมถึงบุคลากรภาครัฐ ภาคเอกชน บุคลากรทุกสาขาอาชีพ และบุคลากรทุกช่วงวัย

2. ส่งเสริมการพัฒนาทักษะ ความเชี่ยวชาญเทคโนโลยีเฉพาะด้าน ให้กับบุคลากรในสายวิชาชีพด้านเทคโนโลยีดิจิทัล ที่ปฏิบัติงานในภาครัฐและเอกชน เพื่อรองรับความต้องการในอนาคต

3. พัฒนาผู้บริหารเทคโนโลยีสารสนเทศให้สามารถวางแผนการนำเทคโนโลยีดิจิทัลไปพัฒนาภารกิจ ตลอดจนสามารถสร้างคุณค่าจากข้อมูลขององค์กร

ยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

จะมุ่งเน้นการมีกฎหมาย กฎระเบียบ กติกาและมาตรฐานที่มีประสิทธิภาพ ทันสมัย และสอดคล้องกับหลักเกณฑ์สากล เพื่ออำนวยความสะดวก ลดอุปสรรคเพิ่มประสิทธิภาพในการประกอบกิจกรรมและทำธุรกรรมออนไลน์ต่างๆ รวมถึงสร้างความมั่นคงปลอดภัย และความเชื่อมั่น ตลอดจนคุ้มครองสิทธิ์ให้แก่ผู้ใช้งานเทคโนโลยีดิจิทัลในทุกภาคส่วนเพื่อรองรับการเติบโตของเทคโนโลยีดิจิทัลและการใช้งานที่เพิ่มขึ้นในอนาคต โดยยุทธศาสตร์นี้ประกอบด้วยแผนงานเพื่อขับเคลื่อนยุทธศาสตร์ 3 ด้าน คือ

1. กำหนดมาตรฐาน กฎ ระเบียบ และกติกาด้านดิจิทัลให้มีความทันสมัยและมีประสิทธิภาพ โดยเฉพาะอย่างยิ่งเพื่ออำนวยความสะดวกด้านการค้าและการใช้ประโยชน์ในภาคเศรษฐกิจและสังคม

2. ปรับปรุงกฎหมายที่เกี่ยวข้องกับเศรษฐกิจและสังคมดิจิทัลให้มีความทันสมัย สอดคล้องต่อพลวัตของเทคโนโลยีดิจิทัลและบริบทของสังคม

3. สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัลและการทำธุรกรรมออนไลน์ ด้วยการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศและการสื่อสารการคุ้มครองข้อมูลส่วนบุคคล การคุ้มครองผู้บริโภค

กลไกการขับเคลื่อนยุทธศาสตร์การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

การพัฒนาเศรษฐกิจและสังคมดิจิทัลในครั้งนี้จะต้องดำเนินการผ่านกลไกการขับเคลื่อนยุทธศาสตร์อย่างครบวงจรและเต็มรูปแบบเพื่อวางรากฐาน เศรษฐกิจและสังคมไทยให้พร้อมเข้าสู่ยุคดิจิทัล โดยมีประเด็น ใน 4 ด้าน ดังต่อไปนี้

1.การขับเคลื่อนที่เป็นรูปธรรมในระยะเร่งด่วนโดยจัดให้มีกิจกรรมและโครงการระยะเร่งด่วนที่สุด (1 ปี 6 เดือน) ที่มุ่งเน้นการลงทุนด้านโครงสร้างพื้นฐานดิจิทัลและสร้างรากฐานการพัฒนาดิจิทัลใน 6 ด้านตามยุทธศาสตร์การพัฒนาดิจิทัลฯ ตั้งแต่ การพัฒนาความพร้อมด้านโครงสร้างพื้นฐาน การเร่งพัฒนาระบบเศรษฐกิจดิจิทัล การพัฒนาเข้าสู่สังคมดิจิทัล การปฏิรูปการดำเนินการภาครัฐ การพัฒนาทุนมนุษย์ ไปจนถึงการวางรากฐานด้านกฎ กติกามาตรฐานด้านดิจิทัล

2. การเปลี่ยนแปลงโครงสร้างเชิงสถาบันโดยจะต้องมีการปรับปรุงรูปแบบและวิธีการทำงานของภาครัฐ บูรณาการการทำงานในลักษณะข้ามกระทรวงเพิ่มประสิทธิภาพของระบบราชการ ลดบทบาทภาครัฐกระจายและมอบอำนาจการปฏิบัติราชการ นอกจากนี้กลไกข้อนี้จะรวมถึงการจัดให้มีหน่วยงานกลาง เพื่อทำหน้าที่กำหนดนโยบาย ประสาน และขับเคลื่อนให้การพัฒนาดิจิทัลของประเทศ เป็นไปอย่างมีเอกภาพ และประสิทธิภาพ ประสิทธิผลสูงสุด

3. การบูรณาการงาน งบประมาณ และทรัพยากรในการดำเนินงาน โดยจะต้องบูรณาการการทำงานร่วมกันหรือเชื่อมโยงงานและข้อมูลในลักษณะที่เป็นองค์รวม กำหนดเจ้าภาพรับผิดชอบแต่ละภารกิจ ปรับปรุงกฎระเบียบ และระบบงบประมาณให้เอื้ออำนวยต่อการทำงานร่วมกันของส่วนราชการ มีระบบประสานงานระหว่างส่วนราชการในการให้บริการประชาชน นอกจากนี้ กลไกข้อนี้จะรวมถึงการจัดตั้งกองทุนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ให้เป็นกลไกทางเลือกในการสนับสนุนทางการเงินกับโครงการด้านการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม นอกเหนือจากการสนับสนุนด้วยงบประมาณรายจ่ายประจำปีของภาครัฐ

4. กลไกติดตามความก้าวหน้าของนโยบายแผนงาน โดยจะต้องมีการติดตาม ตรวจสอบ และประเมินผลความเป็นไปได้อย่างต่อเนื่องเป็นระยะเมื่อพบปัญหาและอุปสรรคในการนำนโยบายสู่การปฏิบัติ ต้องจัดให้มีกลไกช่วยเหลือแก้ปัญหาหรือจัดสรรทรัพยากรเพิ่มเติมตามความจำเป็นและเหมาะสมอย่างเพียงพอและทันท่วงที และนำผลที่ได้จากการติดตามมาทบทวนเพื่อปรับปรุงให้สามารถดำเนินการได้อย่างเป็นรูปธรรม นอกจากนี้ จะต้องเปิดโอกาสให้ทุกภาคส่วนมีส่วนร่วมตั้งแต่กระบวนการปรึกษาหารือ การเปิดรับฟังความเห็นของประชาชนไปจนถึงการตรวจสอบ ติดตามความคืบหน้าการดำเนินงาน เพื่อนำไปสู่การบริหารจัดการภาครัฐที่มุ่งเน้นความโปร่งใสและผลสัมฤทธิ์ของการปฏิบัติงานเป็นหลัก (วิกิซอร์ซ: https://th.wikisource.org)

ผลกระทบของเทคโนโลยีสารสนเทศ

เทคโนโลยีสารสนเทศมีบทบาทในชีวิตประจำวันของมนุษย์มากขึ้น ขณะเดียวกันเครื่องคอมพิวเตอร์ก็มีราคาถูกลง ดังนั้นการประยุกต์ใช้เทคโนโลยีสารสนเทศกับงานต่าง ๆ จึงเป็นไปอย่างกว้างขวาง ซึ่งการประยุกต์ใช้เทคโนโลยีนั้นมีผลกระทบต่อการดำรงชีวิตของมนุษย์ทั้งด้านบวกและด้านลบ ในบทความของปรานอม หยวกทอง ได้เขียนถึงผลกระทบของเทคโนโลยีสารสนเทศ ดังนี้

1. ผลกระทบทางบวกของเทคโนโลยีสารสนเทศ เทคโนโลยีสารสนเทศมีผลกระทบทางบวกต่อการดำรงชีวิตของมนุษย์ ดังนี้

1) ด้านคุณภาพชีวิต เทคโนโลยีสารสนเทศทำให้ได้รับความสะดวกสบายขึ้น ได้แก่

-มนุษย์ใช้เทคโนโลยีคอมพิวเตอร์และโปรแกรมออฟฟิศช่วยให้เกิดความรวดเร็วและเพิ่มประสิทธิภาพในการทำงาน

-มนุษย์ใช้ระบบโทรคมนาคมในการสื่อสารที่รวดเร็ว เช่น การใช้โทรศัพท์เคลื่อนที่ติดต่อสื่อสารในขณะเดินทางไปยังที่ต่าง ๆ มนุษย์ใช้หุ่นยนต์ช่วยในอุตสาหกรรมการผลิตที่ต้องเสี่ยงกับอันตราย หรือในงานที่ต้องการความแม่นยำและความรวดเร็วในการผลิต เช่น หุ่นยนต์สำหรับงานสำรวจ หุ่นยนต์ที่ใช้งานในอวกาศ เป็นต้น

- มนุษย์นำเอาเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในด้านการแพทย์ให้มีความเจริญก้าวหน้าขึ้นมาก เช่น เครื่องมือตรวจคลื่นหัวใจที่ทันสมัย มีเครื่องเอกซเรย์ภาคตัดขวางที่สามารถตรวจดูอวัยวะต่าง ๆ ของร่างกายได้อย่างละเอียด เครื่องมือช่วยในการผ่าตัดที่ทำให้คนไข้ปลอดภัยมากยิ่งขึ้น รวมทั้งการผลิตยา และวัคซีนสมัยใหม่ที่ใช้เทคโนโลยีขั้นสูงเข้าช่วยด้วย

ภาพประกอบ 1.4 เครื่อง Computed Tomography Scanner : CT Scan เป็นเครื่องเอกซเรย์ที่ใช้คอมพิวเตอร์คำนวณและสร้างภาพออกมา (ที่มา: www.thewaltoncentre.nhs.uk)

2) ด้านสังคม เทคโนโลยีสารสนเทศมีผลกระทบทางด้านบวกต่อสังคม ดังนี้

-เทคโนโลยีสารสนเทศทำให้เกิดการเปลี่ยนแปลงจากสังคมอุตสาหกรรมมาเป็นสังคมสารสนเทศ กล่าวคือเป็นสังคมที่ใช้สารสนเทศในการตัดสินใจและการกระจายข้อมูลข่าวสารไปได้ทั่วทุกหนแห่งแม้แต่ถิ่นทุรกันดาร ซึ่งจะก่อให้เกิดความเสมอภาคเท่าเทียมกันในสังคม

-เทคโนโลยีสารสนเทศทำให้เกิดชุมชนเสมือน ซึ่งเป็นกลุ่มคนที่มีความสนใจเรื่องเดียวกัน สามารถแลกเปลี่ยนความคิดเห็น ความรู้ซึ่งกันและกันได้ และความรู้เหล่านี้จะถูกบันทึกไว้ในระบบคอมพิวเตอร์และสามารถเรียกใช้ได้ตามต้องการ

ภาพประกอบ 1.5 จานดาวเทียมสำหรับการศึกษาทางไกล
(ที่มา: http://www.chaoprayanews.com)

3) ด้านการเรียนการสอน เทคโนโลยีสารสนเทศทำให้เกิดประสิทธิภาพการเรียนรู้

- การสร้างโปรแกรมจำลองสถานการณ์ต่าง ๆ ทำให้นักเรียนเข้าใจเนื้อหาของบทเรียนได้อย่างชัดเจน เช่น การจำลองสภาวะสิ่งแวดล้อม การจำลองระบบมลภาวะ การจำลองการไหลของของเหลว หรือแม้แต่การนำเอาคอมพิวเตอร์มาจำลองให้ผู้เรียนได้อยู่ในสภาพที่เสมือนจริง เช่น จำลองการเดินเรือ จำลองการขับเครื่องบิน จำลองการขับรถยนต์ เป็นต้น ซึ่งลดความผิดพลาดจากความเสียหายและความเสี่ยงจากการได้รับอันตรายของผู้เรียนลงได้

ภาพประกอบ 1.6 โปรแกรมจำลองการบินเสมือนจริง
(ที่มา: http://sro33671.blogspot.com)

- เทคโนโลยีสารสนเทศทำให้เกิดการเรียนรู้ตลอดชีวิต (Lifelong learning) ได้อย่างมีประสิทธิภาพ กล่าวคือ การเปลี่ยนแปลงของสังคม การเมือง เศรษฐกิจโลก รวมทั้งเทคโนโลยีที่รวดเร็ว ทำให้มนุษย์ต้องขวนขวายพัฒนาตนเอง และปรับตนเองให้ก้าวทันความเปลี่ยนแปลงต่าง ๆ โดยการเรียนรู้ด้วยตนเองจากแหล่งความรู้ต่าง ๆ ทั่วโลก

ภาพประกอบ 1.7 ตารางการเรียนทางไกลผ่านดาวเทียมในถิ่นทุรกันดาร
(ที่มา: http://www.thailibrary.in.th)

2. ผลกระทบทางลบของเทคโนโลยีสารสนเทศ

เทคโนโลยีสารสนเทศมีผลกระทบทางลบต่อการดำรงชีวิตของมนุษย์ ดังนี้

1) คุณภาพชีวิต เทคโนโลยีสารสนเทศก่อให้เกิดผลกระทบด้านคุณภาพชีวิต ซึ่งส่วนใหญ่มักเกิดผลกระทบต่อสุขภาพกายและสุขภาพจิต ดังนี้

- โรคอันเกิดจากการใช้งานเครื่องคอมพิวเตอร์เป็นเวลานาน ได้แก่ อาการบาดเจ็บของกล้ามเนื้อบริเวณข้อมือเนื่องจากจับเมาส์ หรือใช้แป้นพิมพ์เป็นเวลานาน อาการปวดคอ ไหล่ และหลัง การเกิดปัญหาด้านสายตาเนื่องจากเพ่งมองที่หน้าจอคอมพิวเตอร์เป็นเวลานานติดต่อกัน เป็นต้น

ภาพประกอบ 1.8 ตัวอย่างท่านั่งโต๊ะทำงานคอมพิวเตอร์ที่ถูกต้อง
(ที่มา: http://www.safetechthailand.net)

ภาพประกอบ 1.9 ตัวอย่างท่านั่งโต๊ะทำงานคอมพิวเตอร์ที่ไม่ถูกต้อง
(ที่มา: http://www.safetechthailand.net)

- โรคทนรอไม่ได้ (Hurry Sickness) เกิดกับผู้ที่ใช้งานอินเทอร์เน็ต ซึ่งทำให้ผู้ใช้เป็นคนขี้เบื่อ หงุดหงิดง่าย ใจร้อน เครียดง่าย ความอดทนลดลง ทนรอเครื่องดาวน์โหลดนาน ๆ ไม่ได้ จะกระวนกระวาย ซึ่งจะเป็นพฤติกรรมติดตัวไปใช้ในการดำเนินกิจกรรมในชีวิตประจำวันด้วย หากมีอาการมาก ๆ อาจจะเข้าข่ายโรคประสาทได้

ภาพประกอบ 1.10 โรคทนรอไม่ได้ (ที่มา: https://sites.google.com/site/kroonom)

- มนุษย์เกิดความเครียดจากการเลือกใช้ข้อมูลและสารสนเทศที่มีอยู่อย่างมากมายรวมถึงความเครียดจากความวิตกกังวลว่าจะมีการนำคอมพิวเตอร์มาทดแทนแรงงานของคน

ภาพประกอบ 1.11 โรคเครียด (ที่มา: https://sites.google.com/site/kroonom)

2) ด้านสังคม เทคโนโลยีสารสนเทศมีผลกระทบทางด้านลบต่อสังคม ดังนี้

- การขาดทักษะทางสังคม เนื่องจากอินเทอร์เน็ตทำให้เกิดการสื่อสารพันได้โดยไม่ต้องพบเจอกัน ซึ่งพบว่าปัจจุบันคนในสังคมจะนิยมใช้บริการเครือข่ายสังคม หรือที่เรียกว่า social network มากขึ้น เช่น เว็บไซต์ Hi5 และเว็บไซต์ Facebook ทำให้ความสัมพันธ์ระหว่าบุคคลในสังคมน้อยลง ทักษะทางสังคมต่าง ๆ ที่ใช้ในการปฏิสัมพันธ์และการสื่อสารระหว่างกัน ได้แก่ ทักษะการพูด การฟัง การทำงานร่วมกัน รวมทั้งความสามารถในการเข้าใจถึงสถานการณ์ที่หลากหลาย กฎกติกาต่าง ๆ ในสังคม และการคิดคำนึงถึงคนรอบข้างอย่างเข้าอกเข้าใจ ซึ่งทักษะทางสังคมเป็นสิ่งที่สำคัญและจำเป็นสำหรับทุกเพศทุกวัย ดังนั้นการขาดทักษะทางสังคมจะทำให้คนขาดการทำความเข้าใจผู้อื่น ไม่มีการทำงานร่วมกัน จนกระทั่งอาจก่อให้เกิดความขัดแย้งกันในสังคมขึ้นได้

ภาพประกอบ 1.12 สื่อที่ทำให้เกิดความขัดแย้งทางความคิดบนโลกไซเบอร์
(ที่มา: https://sites.google.com/site/kroonom)

- การเกิดอาชญากรรมคอมพิวเตอร์มากขึ้นและรุนแรงขึ้น เทคโนโลยีสารสนเทศเป็นเครื่องมือหนึ่งในการก่ออาชญากรรมได้ง่าย ผู้ไม่หวังดีอาจใช้เทคโนโลยีสารสนเทศในทางที่ผิด เช่น

การขโมยข้อมูลของบริษัทและนำไปเปิดเผยกับบริษัทคู่แข่ง การเจาะระบบของธนาคารและเปลี่ยนแปลงข้อมูลเงินในบัญชีธนาคารให้สูงขึ้น การล่อลวงผู้ที่เล่นอินเทอร์เน็ตและก่อคดีล่วงละเมิดทางเพศ การเผยแพร่ข้อมูลที่ไม่ชอบด้วยกฎหมายในแง่มุมต่าง ๆ ทั้งภาพลามกอนาจ การพนันออนไลน์ การจำหน่ายของผิดกฎหมาย หรือเผยแพร่ข้อมูลที่มีเนื้อหาแอบแฝงแนวคิด ก้าวร้าว รุนแรง การส่งไวรัสเข้าไปทำลายข้อมูลของผู้อื่น เป็นต้น

ภาพประกอบ 1.13 ก่อให้เกิดปัญหาอาชญากรรมคอมพิวเตอร์
(ที่มา: http://www.aseanthai.net)

3) ด้านการเรียนการสอน ผลกระทบในทางลบกับการเรียนการสอนจะเกิดขึ้นหากผู้สอน ใช้เทคโนโลยีสารสนเทศในการจัดการเรียนการสอนทั้งหมด และปล่อยให้ผู้เรียนศึกษาและเรียนรู้ด้วยตนเอง ผู้เรียนที่มีประสบการณ์น้อยอาจตีความได้ไม่ถูกต้อง รวมถึงการใช้อินเทอร์เน็ตในทางที่ผิด ดังนั้น ผู้สอนจำเป็นอย่างยิ่งที่จะต้องเรียนรู้การประยุกต์ใช้เทคโนโลยีสารสนเทศกับการเรียนการสอน รวมทั้งให้คำแนะนำ อบรมสั่งสอนด้านคุณธรรม จริยธรรมควบคู่ไปกับการใช้เครือข่ายอินเทอร์เน็ต

ภาพประกอบ 1.14 ปัญหาเด็กติดเกมคอมพิวเตอร์ที่มาของอาชญากรรม
(ที่มา: https://sites.google.com/site/kroonom)

1.2 วัตถุประสงค์ของการวิจัย

การวิจัยนี้เป็นการวิจัยองค์ความรู้เพื่อให้ทราบถึงปัจจัยที่มีผลกระทบต่อจริยธรรมทางและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 โดยมีวัตถุประสงค์ดังนี้

1. เพื่อศึกษาการละเมิดจริยธรรมและภัยคุกคามความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: ของสถาบันอุดมศึกษาในเขตกรุงเทพมหานครและปริมณฑล
2. เพื่อกำหนดประเภทของการละเมิดจริยธรรม และภัยคุกคามทางด้านเทคโนโลยีสารสนเทศ
3. เพื่อหาแนวทางป้องกันและการแก้ไขปัญหาเกี่ยวกับการละเมิดจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ

1.3 คำถามการวิจัย

คำถามวิจัยได้กำหนดขึ้นตามวัตถุประสงค์ของการวิจัย สามารถจำแนกออกเป็นได้ 3 ข้อ ดังต่อไปนี้ คือ :

1. อะไรคือปัจจัย-ปัญหาการละเมิดจริยธรรม และภัยคุกคามความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศในปัจจุบัน
2. ประเภทของการละเมิดจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศมีกี่ประเภท อะไรบ้าง
3. แนวทางในการแก้ปัญหาการละเมิดจริยธรรม และความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ สามารถทำได้อย่างไรบ้าง

1.4 สมมุติฐานการวิจัย

1. ในปัจจุบันปัญหาการละเมิดจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ มีความรุนแรงมาก
2. ประเภทของการการละเมิดจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศมี 7 ประเภท ได้แก่ (1) การใช้งานคอมพิวเตอร์อย่างขาดความรับผิดชอบ (2) การละเมิดความเป็นส่วนตัวของผู้อื่น (3) การขโมยอัตลักษณ์ (4) การเจาะระบบ (5) การใช้ไวรัสโจมตี (6) การละเมิดลิขสิทธิ์ (7) การส่งอีเมลที่ไม่ได้รับเชิญ (Spamming) รบกวนสร้างความรำคาญให้กับผู้อื่น
3. ปัจจัยที่มีผลกระทบต่อจริยธรรมทั่วไป และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ได้แก่ (1) ความรู้เกี่ยวกับคอมพิวเตอร์ (2) ความรู้เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ และกฎหมายที่เกี่ยวข้องอื่นๆ (3) ปัจจัยทางสังคม (4) ปัจจัยทางด้านเศรษฐกิจ (5) ปัจจัยทางด้านพฤติกรรมการใช้คอมพิวเตอร์

1.5 ขอบเขตของการวิจัย

งานวิจัยเรื่อง **“ปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: กรณีศึกษาสถาบันอุดมศึกษาในเขตกรุงเทพมหานคร และปริมณฑล”** มีเนื้อหาครอบคลุมถึงเรื่องคุณธรรมจริยธรรมในการใช้เทคโนโลยีสารสนเทศทั้งในประเทศและต่างประเทศ ซึ่งสมาคมผู้เป็นมืออาชีพทางเทคโนโลยีสารสนเทศ (Association of Information Technology Professional : AITP) ได้ร่วมกันกำหนดกฎเกณฑ์ทางด้านจริยธรรมทางเทคโนโลยีสารสนเทศขึ้น ได้แก่ (1) ต้องมีความซื่อสัตย์สุจริต (2) เพิ่มสมรรถนะความเป็นมืออาชีพของตนเอง (3) ตั้งเกณฑ์การทำงานไว้ให้สูง (4) มีความรับผิดชอบในการทำงาน และ (5) รักษาสุขภาพ, รักษาความเป็นส่วนตัว และ ดูแลสวัสดิการสาธารณะชนทั่วไปและยังต้องพยายามหลีกเลี่ยงจากปัญหาอาชญากรรมคอมพิวเตอร์ และเพิ่มการพัฒนาระบบความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศให้มากขึ้น ผู้วิจัยได้เลือกกลุ่มประชากรตัวอย่างคือกลุ่มของสถาบันอุดมศึกษาในเขตกรุงเทพมหานครและปริมณฑล เนื่องจากผู้วิจัยต้องการศึกษาถึงปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศทั้งในช่วงของกรอบระยะเวลาที่นักศึกษาได้ใช้ชีวิตการศึกษาในรั้วมหาวิทยาลัย มีตั้งแต่ 1-4 ปี และบุคลากรที่ทำงานอยู่ประจำทุกวันอาจได้พบเจอกับการละเมิดจริยธรรมบ้างในบางกรณี

1.6 นิยามศัพท์

1.6.1 จริยธรรม (Ethics) คือ ชุดของความเชื่อเกี่ยวกับพฤติกรรมที่ถูกต้อง และไม่ถูกต้องของคนในสังคม จริยธรรมความประพฤตินั้นจะต้องสอดคล้องกับมาตรฐานที่ได้รับการยอมรับทุกพฤติกรรมเหล่านั้นจะต้องได้รับการยอมรับในระดับสากล

1.6.2 จริยธรรมทางธุรกิจ (Ethics in Business) คือ การทำธุรกิจอย่างมีจริยธรรม หมายถึง เป็นผู้ประกอบการไม่ว่าจะเป็นผู้ผลิตจำหน่ายหรือบริการด้วยจริยวัตรที่ดีงาม มีคุณธรรม มีความ ซื่อตรง ยุติธรรม

1.6.3 จริยธรรมทางด้านเทคโนโลยีสารสนเทศ (Ethics in Information Technology) คือ การใช้เทคโนโลยีสารสนเทศอย่างมีจริยธรรม เช่น การไม่ละเมิดความเป็นส่วนตัวของผู้อื่น การไม่ละเมิดลิขสิทธิ์ซอฟต์แวร์ ไม่เข้าถึงเครื่องคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต เป็นต้น

1.6.4 ศีลธรรม (Morals) เป็นความเชื่อของคนเกี่ยวกับความถูกต้อง หรือไม่ถูกต้อง หรืออีกนัยหนึ่ง ตามความหมายของวิกิพีเดีย ศีลธรรม (อังกฤษ: Morality) หมายถึงความประพฤติที่ดีที่ชอบทั้งศีลและธรรมศีลธรรม ในคำวัดหมายถึง เบญจศีล และ เบญจธรรม คือศีล 5 และธรรม 5 ซึ่งเป็นกฎเกณฑ์ของสังคมระดับต้นสำหรับให้สมาชิกสังคมประพฤติปฏิบัติเพื่อให้เกิดความสงบสุข ไม่สะดุ้งกลัว ไม่หวาดระแวงภัย เป็นหลักประกันสังคมที่สำคัญ สังคมที่สงบสุข ไว้วางใจกันได้ เอื้อเฟื้อเผื่อแผ่ต่อกัน ไม่เบียดเบียน ไม่ทะเลาะ ไม่กดขี่ข่มเหง ไม่เอารัดเอาเปรียบกัน เป็นต้น

1.6.5 ความเป็นส่วนตัว (Privacy) คือ “สิทธิ์อันชอบธรรมที่จะอยู่คนเดียวโดยลำพัง ซึ่งครอบคลุมไปถึงเรื่องความถูกต้องทั้งหมด และ เป็นความถูกต้องที่มีมูลค่า และคำนึงถึงอิสระของประชาชน” หรือ “สิทธิ์อันชอบธรรมที่จะอยู่คนเดียวโดยลำพัง โดยปราศจากการรบกวนจากบุคคลอื่น หรือองค์กรอื่น”

1.6.6 อาชญากรรมคอมพิวเตอร์ (Computer Crime) คือ การใช้คอมพิวเตอร์, เครือข่าย และอินเทอร์เน็ตกระทำผิดทางด้านอาชญากรรม เช่น การเจาะระบบ การโจมตีด้วยไวรัส และการหลอกลวงทางอินเทอร์เน็ต เป็นต้น

1.6.7 การขโมยอัตลักษณ์ (Identity Theft) หรือลักษณะเฉพาะตน อัตลักษณ์ หรือลักษณะเฉพาะตัว ได้แก่ข้อมูลที่ใช้ระบุตัวตน ใช้ในการติดต่อสื่อสาร หรือใช้ค้นหาบุคคล หรือเป็นข้อมูลที่ใช้ร่วมกับข้อมูลอื่นเพื่อระบุตัวบุคคล ตัวอย่างต่อไปนี้ คือ สิ่งที่ระบุว่าเป็นอัตลักษณ์ คือ ชื่อเต็ม นามสกุลของมารดาก่อนแต่งงาน ที่อยู่ วัน เดือน ปีเกิด สถานที่เกิด ข้อมูลพันธุกรรม หมายเลขบัตรประจำตัวประชาชน หมายเลขบัตรประกันสังคม หมายเลขใบอนุญาตขับขี่ หมายเลขทะเบียนยานพาหนะ หมายเลขหนังสือเดินทาง หมายเลขบัตรเครดิต ใบหน้า ม่านตา ลายพิมพ์นิ้วมือ ลายมือ ลายเซ็น เป็นต้น

1.6.8 ความมั่นคงปลอดภัย (Security) คือ การทำให้รอดพ้นจากอันตรายหรืออยู่ในสถานะที่มีความปลอดภัยไร้ความกังวลและไร้ความกลัว และได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือโดยบังเอิญ

1.6.9 ประเทศไทย 4.0 (Thailand 4.0) คือการเปลี่ยนแปลงโครงสร้างเศรษฐกิจ หรือ “เศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม” โดยมีเป้าหมายมุ่งไปสู่ความคุ้มค่าทางเศรษฐกิจ (Value-Based Economy)

1.6.10 ความรู้ด้านเทคโนโลยีสารสนเทศ (Information Technology Knowledge) หมายถึง มีความรู้เรื่องฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) บุคคล (People) ข้อมูล (Data) และเครือข่ายคอมพิวเตอร์ (Network) รวมไปถึงกิจกรรมของระบบสารสนเทศ คือ การนำเข้าข้อมูล (Input) การประมวลผล (Process) และการนำออกข้อมูล หรือแสดงผลลัพธ์ (Output)

1.6.11 ความรู้เกี่ยวกับพระราชบัญญัติ (ACT.) คือ มีความรู้เกี่ยวเกี่ยวกับพระราชบัญญัติต่าง ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม พ.ศ. 2560 พระราชบัญว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ.2544 พระราชบัญญัติลิขสิทธิ์ พ.ศ.2537 พระราชบัญญัติให้ใช้ประมวลกฎหมายอาญา พ.ศ.2499 พระราชบัญญัติการพนัน พ.ศ.2475 พระราชบัญญัติคุ้มครองเด็ก พ.ศ.2546 พระราชบัญญัติสิทธิบัตร พ.ศ.2522 แก้ไขเพิ่มเติม พ.ศ.2542 พระราชบัญัติเครื่องหมายการค้า พ.ศ.2534 แก้ไขเพิ่มเติม พ.ศ.2543 พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ.2560

1.6.12 ปัจจัยทางด้านสังคม (Social Factors) หมายถึง ปัจจัยที่ส่งผลกระทบทั้งในด้านบวกและด้านลบ ได้แก่ การที่ประเทศไทยก้าวเข้าสู่สังคมผู้สูงอายุ ก่อให้เกิดแอพพลิชันที่เข้ามาดูแลผู้สูงอายุมากมาย รวมถึงแอพลิเคชันเรื่องของการดูแลสุขภาพกายและสุขภาพใจ, กระแสการเปลี่ยนแปลงของโลกก่อให้เกิดการเปลี่ยนแปลงของสภาพแวดล้อม ภูมิอากาศ และปรากฏการณ์ต่างๆ ที่ก่อให้เกิดความเสียหาย, สังคมโลกาภิวัฒน์ ทำให้เกิดการสื่อสารไร้พรมแดน มีความเปลี่ยนแปลงอย่างรวดเร็วทั้งด้านความเป็นอยู่ ด้านกฎหมายระหว่างประเทศ รวมถึงด้านสังคม และการเมือง, สื่อสังคมออนไลน์ มีประโยชน์ในทางบวก คือ ช่วยให้มีความสะดวกรวดเร็วในการติดต่อสื่อสาร การทำธุรกิจ ในทางลบก่อให้เกิดความวุ่นวายในสังคม เช่น การละเมิดความเป็นส่วนตัว การปลอมแปลงเฟซบุ๊ค การโพสต์ภาพลามกอนาจาร การพนันออนไลน์

1.6.13 ปัจจัยด้านเศรษฐกิจ (Economy Factor) หมายถึง ปัจจัยที่มีผลกระทบต่อเศรษฐกิจทั้งในด้านบวกและด้านลบ ในด้านบวก คือ เทคโนโลยีสารสนเทศและอินเทอร์เน็ตช่วยสร้างการเติบโต

ทางเศรษฐกิจทำให้ GDP ของประเทศสูงขึ้น, เทคโนโลยีสารสนเทศก่อให้เกิดนวัตกรรม, เทคโนโลยีสารสนเทศช่วยอำนวยความสะดวกรวดเร็วในการติดต่อสื่อสารไม่ว่าจะเป็นการส่งไปรษณีย์อิเล็กทรอนิกส์ การประชุมผ่านจอภาพวิดีโอ การขายสินค้าออนไลน์ การประชาสัมพันธ์ การสรรหาบุคลากร การฝึกอบรมการเปิดตลาดใหม่ และการทำงานรวมถึงการตัดสินใจของผู้บริหาร, เทคโนโลยีสารสนเทศ ช่วยอำนวยความสะดวกเรื่องการผลิตสินค้า และการบริการได้รวดเร็วมากขึ้น ในทางลบเทคโนโลยีสารสนเทศ เข้ามาทำลายล้างระบบเดิม (Disruptive) เช่น Fintech ทำให้สาขาของธนาคารปิดตัวลงเป็นจำนวนมาก ลดการจ้างพนักงานลง หรือการผลิตชิ้นส่วนอุปกรณ์คอมพิวเตอร์บางอย่างก่อให้เกิดมลพิษต่อสิ่งแวดล้อม

1.6.14 ปัจจัยด้านพฤติกรรม (behavior Factor) หมายถึง พฤติกรรมการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศ มีทั้งในด้านบวก และด้านลบ ในด้านบวก ไดแก่ เทคโนโลยีสารสนเทศคอมพิวเตอร์ และอินเทอร์เน็ตทำให้การติดต่อสื่อสารสะดวกรวดเร็ว ไม่ว่าจะเป็นการติดต่อสื่อสารกับเพื่อน ครอบครัว การแสวงหาความรู้ การติดตามข่าวสาร การซื้อขายสินค้าและการบริการ และการสร้างความบันเทิง ในด้านลบ การใช้เทคโนโลยีสารสนเทศไปในทางที่ไม่ถูกต้อง เช่น การเล่นการพนันออนไลน์ หรือการเล่มเกมออนไลน์นานเกินไป ทำให้เสียงาน นอกจากนั้น การใช้คอมพิวเตอร์เป็นเวลานานอาจทำให้เกิดอาการปวดหัว น้ำตาไหล ปวดหลัง หรือบางครั้งการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์อาจทำให้เกิดความหลงไหล เมื่อไม่ได้ใช้เครื่องคอมพิวเตอร์อาจทำให้เกิดอารมณ์เสีย มีความกระวนกระวาย

1.6.15 การหลอกลวงทางอินเทอร์เน็ต หรือ ฟิชชิง (Phishing) ฟิชชิง คือ เป็นการใช้อีเมลตลบตะแลง โดยพยายามให้ผู้รับทำการเปิดเผยข้อมูลส่วนบุคคลออกมา เช่น รหัสผ่านหรือหมายเลขบัตรเครดิต, ชื่อและชื่อผู้ใช้ที่อยู่และหมายเลขโทรศัพท์,รหัสผ่านหรือ PIN, หมายเลขบัญชีธนาคาร, บัตรเดบิต/บัตรเอทีเอ็ม, รหัสการตรวจสอบความถูกต้องของการ์ด (CVC) หรือค่าการตรวจสอบการ์ด (CVV) หมายเลขประกันสังคม (SSN) เป็นต้น ซึ่งเป็นเสมือนการใช้เหยื่อเกี่ยวเบ็ดเพื่อล่อปลาให้มาติดเบ็ด หรือการปลอมแปลงอีเมลจากเหล่าแฮกเกอร์ โดยจะทำให้เหมือนว่า ถูกส่งมาจากจากเว็บไซต์ที่ทำธุรกรรมด้านค้าขายทางอินเทอร์เน็ต เว็บไซต์ทำการประมูลซื้อขายทางออนไลน์ ธนาคาร และแหล่งสินเชื่อบัตรเครดิต เช่น Citibank eBay และ PayPal ลักษณะการหลอกหลวงได้แก่ ส่งอีเมล์ไปตามเหล่าสมาชิกหรือลูกค้าเหล่านั้น รวมถึงการส่งข้อความมาทาง Messenger เป็นลิงค์ให้เข้าไปยังเว็บหลอกที่ถูกสร้างขึ้นมาเหมือนกับเว็บของจริง เพื่อให้เหยื่อกรอกข้อมูลส่วนตัว เช่น User Name} Password หมายเลขบัตรเครดิตต่างๆ ที่นี้เมื่อเหยื่อกรอกข้อมูลลงไปแล้ว พวกแฮกเกอร์ก็จะนำข้อมูลเหล่านั้นไปใช้หาผลประโยชน์ต่ออีกที ทำให้ความเสียหายตกอยู่กับเจ้าของข้อมูลเหล่านั้น ซึ่งพฤติกรรมเหล่านี้ก็คล้ายกับการอ่อยเหยื่อตกปลา โดยหวังให้ปลามาฮุบเหยื่อไปกิน การหลอกลวงทางอินเทอร์เน็ต เป็นการหลอกล่อผู้ใช้อินเทอร์เน็ตเพื่อขโมยสารสนเทศส่วนบุคคล เช่น หมายเลขบัตรเครดิต, หมายเลขบัตรประกันสังคม หรือสารสนเทศที่อ่อนไหวอื่นๆ ซึ่งก่อให้เกิดการขโมยอัตลักษณ์ บุคคลผู้สร้างเล่ห์อุบายจะส่งข้อความไปทางอีเมล์ว่า เป็นเหมือนพวกเขาดำเนินธุรกิจถูกต้องตามกฎหมาย เช่น ธนาคารออนไลน์ สภาพของอีเมลนั้นผู้รับต้องการปรับให้ทันสมัย หรือให้ยืนยันว่าเขาหรือเธอต้องการปรับสารสนเทศทางบัญชีให้ทันสมัย เมื่อผู้รับคลิกลิงค์จัดการ, เขา หรือเธอก็จะเข้าสู่เว็บไซต์ เว็บไซต์นั้นดูคล้ายจะถูกต้องตามกฎหมาย แต่จริงๆ แล้วคือการหลอกลวงคัดลอกด้วยเล่ห์อุบายที่ถูกสร้างขึ้น ประการหนึ่งเมื่อผู้รับอีเมลยืนยันสารสนเทศของเขาหรือเธอ ผู้สร้างเล่ห์อุบายนี้ก็จะทำการจับเอาสารสนเทศเหล่านั้น และสามารถที่จะเริ่มใช้งานมันได้

1.6.16 ขยะไปรษณีย์อิเล็กทรอนิกส์หรือ สแปม (Spam) คือ ชื่อเรียกของการส่งข้อความที่ผู้รับไม่ได้ร้องขอ หรือไม่ได้รับเชิญของบุคคลเป็นจำนวนมาก ผ่านทางระบบอิเล็กทรอนิกส์ เป็นการส่งอีเมลในทางที่ผิด โดยส่วนมากจะทำให้เกิดความไม่พอใจต่อผู้รับข้อความ สแปมที่พบเห็นได้บ่อยได้แก่ การส่งสแปมผ่านทางอีเมล ในการโฆษณาชวนเชื่อ หรือโฆษณาขายของ โดยการส่งอีเมลประเภทหนึ่งที่เราไม่ต้องการ ซึ่งจะมาจากทั่วโลก โดยที่เราไม่รู้เลยว่า ผู้ที่ส่งมาให้นั้นเป็นใคร จุดประสงค์คือ ผู้ส่งส่วนใหญ่ต้องการที่จะโฆษณา สินค้าหรือบริการต่าง ๆ ของบริษัทของตนเอง ซึ่งเป็นประเภทหนึ่งของเมลขยะซึ่งนอกจากจะทำให้ผู้รับรำคาญใจและเสียเวลาในการกำจัดข้อความเหล่านี้แล้ว ผู้ที่นิยมใช้สแปมในการส่งข้อความเป็นเพราะมีต้นทุนต่ำ เป็นทฤษฎีหนึ่งในการทำการตลาด หรือบางครั้งเกิดมาจากงานหรือเว็บไซต์ลามก เราสามารถพบเห็นสแปมได้โดยทั่วไป บางครั้งสแปมส่งไปเพื่อให้ตอบแบบสอบเกี่ยวกับสินค้าและผลิตภัณฑ์ บางครั้งสแปมก็ถูกนำไปใช้โดยบริษัทที่ถูกต้องตามกฎหมายจำนวนมาก สแปมยังทำให้ประสิทธิภาพการขนส่งข้อมูลบนอินเทอร์เน็ตลดลงด้วย สแปมในรูปแบบอื่นนอกจาก อีเมลสแปม ได้แก่ เมสเซนเจอร์สแปม นิวส์กรุ๊ปสแปม บล็อกสแปม และเอสเอ็มเอสสแปม การส่งสแปมเริ่มแพร่หลายเนื่องจากค่าใช้จ่ายในการส่งข้อความผ่านทางระบบอิเล็กทรอนิกส์ มีค่าใช้จ่ายน้อยมากเมื่อเทียบการการส่งข้อความชักชวนทางอื่น เช่นทางจดหมาย หรือการโฆษณาทางสื่อต่างๆ ทำให้ผู้ส่งประหยัดค่าใช้จ่ายในการส่งข้อความเชิญชวน และในขณะเดียวกันกฎหมายเกี่ยวกับระบบอิเล็กทรอนิกส์ที่เกี่ยวข้องกับสแปมยังไม่ครอบคลุม จนกระทั่งเริ่มมีใช้ครั้งแรกปี พ.ศ. 2546 (ค.ศ. 2003) ในประเทศสหรัฐอเมริกา หลายบริษัทได้ส่งออกขยะไปรษณีย์อิเล็กทรอนิกส์-สิ่งที่ไม่เป็นที่ต้องการ หรือไปรณีย์อิเล็กทรอนิกส์ที่โยนทิ้งแล้ว ค้นหาที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ของคุณหรือไม่ก็ค้นหาดูจากรายการซื้อสินค้า หรือซอฟต์แวร์ที่มองหาที่อยู่ไปรษณีย์อิเล็กทรอนิกส์บนอินเทอร์เน็ต (ข้อความรีบด่วนที่ไม่ได้เชิญซึ่งเป็นรูปแบบของขยะไปรษณีย์อิเล็กทรอนิกส์ ถูกเรียกว่า สปิม (spim) ถ้าคุณเคยใช้ที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ซื้อของหลายอย่างบนระบบออนไลน์, เปิดบัญชีออนไลน์, เข้าร่วมในเว็บเครือข่ายสังคมออนไลน์ เช่น เฟซบุ๊ก ในที่สุดที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ของคุณจะปรากฏอยู่บนหนึ่งในรายการที่จะได้รับขยะไปรษณีย์อิเล็กทรอนิกส์

1.6.17 สารสนเทศความเป็นส่วนตัว (Information Privacy) นิยามความเป็นส่วนตัว คือ “สิทธิ์อันชอบธรรมที่จะอยู่คนเดียว- ซึ่งครอบคลุมไปถึงเรื่องความถูกต้องทั้งหมด และ เป็นความถูกต้องที่ถูกเพิ่มให้มูลค่าโดยความเป็นอิสระของประชาชน” หรืออีกความหมายหนึ่งตามวิกิพีเดีย คือ สิทธิในความเป็นส่วนตัวหรือ สิทธิส่วนบุคคล หมายถึงสิทธิของบุคคลที่ประกอบไปด้วยสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว ในเรื่องดังกล่าวน่าจะจัดอยู่ในเรื่องของความเป็นอยู่ส่วนตัวซึ่งหมายความว่า สถานะที่บุคคลจะรอดพ้นจากการสังเกต การรู้เห็น การสืบความลับ การรบกวนต่างๆ และความมีสันโดษ ไม่ติดต่อสัมพันธ์กับสังคม โดยทั้งนี้ ขอบเขตที่บุคคลควรได้รับการคุ้มครองและการเคารพในสิทธิส่วนบุคคลก็คือการดำรงชีวิตอย่างเป็นอิสระ มีการพัฒนาบุคลิกลักษณะตามที่ต้องการ สิทธิที่จะแสวงหาความสุขในชีวิตตามวิถีทางที่อาจเป็นไปได้และเป็นความพอใจตราบเท่าที่ไม่ขัดต่อกฎหมาย ไม่ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน และไม่เป็นการล่วงละเมิดสิทธิเสรีภาพของผู้อื่น ซึ่งสิทธิในความเป็นส่วนตัวหรือสิทธิส่วนบุคคล นี้เป็นสิทธิขั้นพื้นฐาน มีบัญญัติไว้ใน รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 35 ความว่า สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ ส่วนตัว ย่อมได้รับความคุ้มครอง การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่

ส่วนตัว จะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูล ส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติเป็นต้น สำหรับสารสนเทศความเป็นส่วนตัวนั้นเป็นการรวมหลายอย่างเข้าด้วยกัน ประกอบด้วย :

(1). ความเป็นส่วนตัวเรื่องการสื่อสาร (Communications privacy) ได้แก่ ความสามารถในการสื่อสารกับคนอื่น โดยปราศจากการติดตามโดยบุคคล หรือองค์กรอื่น และ ข้อมูลความเป็นส่วนตัว (Data privacy) ได้แก่ ความสามารถในการจำกัดการเข้าถึงข้อมูลส่วนบุคคลของคนๆ หนึ่งโดยปัจเจกชน และองค์กรนั้น จะต้องมีคำสั่งในการปฏิบัติในแต่ละระดับที่แน่นอน เพื่อควบคุมข้อมูลเหล่านั้น รวมถึงการนำไปใช้ประโยชน์ด้วย

1.6.18 ทรัพย์สินทางปัญญา (Intellectual Property) หมายถึง “ความเป็นเจ้าของ” หรืองานที่ถูกสร้างสรรค์ขึ้นโดยบุคคล หรือกลุ่มบุคคล เช่น งานศิลปะ หนังสือ ฟิล์ม สูตร สิ่งประดิษฐ์ เพลง และกระบวนการซึ่งมีความแตกต่าง ทรัพย์สินทางปัญญานั้นเป็นสิ่งที่ถูกปกป้องคุ้มครอง รวมถึงงานที่มีการจดลิขสิทธิ์ สิทธิบัตร และกฎหมายที่มีการคุ้มครองเกี่ยวกับความลับในการแลกเปลี่ยน สินค้าวิกิพีเดีย สารานุกรมเสรี ได้ให้ความของทรัพย์ทางปัญญาเอาไว้ว่า ทรัพย์สินทางปัญญา หมายถึง สิทธิทางกฎหมายที่ให้เจ้าของสิทธิ หรือ "ผู้ทรงสิทธิ" มีอยู่เหนือสิ่งที่เกิดจากความคิดสร้างสรรค์ทางปัญญาของมนุษย์ โดยอาจแบ่งทรัพย์สินทางปัญญาออกได้ 2 ประเภทหลัก คือ (1)ทรัพย์สินทางอุตสาหกรรมและ (2)ลิขสิทธิ์ สำหรับทรัพย์สินทางอุตสาหกรรมยังแบ่งออกได้อีก 5 ประเภท ได้แก่ (1)สิทธิบัตร (2) อนุสิทธิบัตร (3) เครื่องหมายการค้า (4) ความลับทางการค้า และ (5)สิ่งบ่งชี้ทางภูมิศาสตร์ (6)แบบผังภูมิของวงจรรวม (7)คุ้มครองพันธุ์พืช (8)ภูมิปัญญาท้องถิ่น

1.6.19 ลิขสิทธิ์ (Copyrights) คือ การให้สิทธิ์กับผู้สร้างสรรค์งานต้นฉบับขึ้นมาอย่างถูกต้องตามกฎหมายแต่เพียงผู้เดียว ในการเผยแพร่, แสดง, กระทำ, ผลิตงานใหม่, ตระเตรียมงานหรือสิ่งที่พัฒนามาจากสิ่งอื่นซึ่งตั้งอยู่บนพื้นฐานของเรื่องงาน ผู้เขียน มีสิทธิ์แต่เพียงผู้เดียวในการยินยอมมอบให้กับผู้อื่น ผลงานที่ได้ชื่อว่า เป็นงานมีลิขสิทธิ์ ได้แก่ : (1) งานสถาปัตยกรรม (Architecture), (2) งานศิลปะ (Art), (3) งานโสตทัศน์ (Audiovisual works) (4) การเต้น (Choreography), (5) บทละคร (Drama), (6) ภาพพิมพ์ (Graphics), (7) การประพันธ์ (Literature) (8) ภาพเคลื่อนไหว (Motion pictures), (9) เพลง (Music), (10) ละครใบ้ (Pantomimes), (11) รูปภาพ (Pictures), (12) งานแกะสลัก (Sculptures), (13) การบันทึกเสียง (Sound recordings), (14) งานทางสติปัญญาอื่นๆ (Other intellectual works)

1.6.20 สิทธิบัตร (Patents) คือ การให้สิทธิ์อย่างถูกต้องกับทรัพย์สินทางปัญญาของผู้ประดิษฐ์ เรื่องนี้ถูกประกาศโดยสำนักงานสิทธิบัตร และสำนักงานเครื่องหมายการค้าของสหรัฐอเมริกา (U.S. Patent and Trademark Office: USPTO) อนุญาตให้ผู้ที่เป็นเจ้าของแต่เพียงผู้เดียว ที่สามารถเผยแพร่ต่อสาธารณะ ได้แก่ การทำ, การใช้, การขาย เพื่อปกป้องงานประดิษฐ์ของผู้ประดิษฐ์ อนุญาตให้ดำเนินการได้ตามกฎหมายแก่บุคคลผู้ที่ฝ่าฝืน สามารถป้องกันงานประดิษฐ์ของตนเองได้อย่างอิสระทั้งการสร้าง และการทำสำเนา ส่วนประเภทของสิทธิบัตร มีอยู่ 3 ประเภท คือ

(1). สิทธิบัตรการประดิษฐ์ หมายถึง การคิดค้นเกี่ยวกับ กลไก โครงสร้าง ส่วนประกอบ ของสิ่งของเครื่องใช้ เช่น กลไกของกล้องถ่ายรูป, กลไกของเครื่องยนต์, ยารักษาโรค เป็นต้น หรือการคิดค้นกรรมวิธีในการผลิตสิ่งของ เช่น วิธีการในการผลิตสินค้า, วิธีการในการเก็บรักษาพืชผักผลไม้ไม่ให้เน่าเสียเร็วเกินไป เป็นต้น

(2). สิทธิบัตรการออกแบบผลิตภัณฑ์ หมายถึง การออกแบบรูปร่าง ลวดลาย หรือสีสัน ที่มองเห็นได้จากภายนอก เช่น การออกแบบแก้วน้ำให้มีรูปร่างเหมือนรองเท้า เป็นต้น (3). อนุสิทธิบัตร (Petty patent) เป็นการให้ความคุ้มครองสิ่งประดิษฐ์คิดค้น เช่นเดียวกับสิทธิบัตรการประดิษฐ์ แต่แตกต่างกันตรงที่การประดิษฐ์ที่จะขอรับอนุสิทธิบัตร เป็นการประดิษฐ์ที่มีเป็นการปรับปรุงเพียงเล็กน้อย และมีประโยชน์ใช้สอยมากขึ้นมาก

1.6.21 เครือข่ายสังคมออนไลน์ (Social Networking) คือ การสร้างชุมชนออนไลน์ของผู้ใช้อินเทอร์เน็ต ซึ่งทำให้สามารถขจัดอุปสรรคในเรื่องของเวลา, ระยะทางไกล, และความแตกต่างทางด้านวัฒนธรรม อนุญาตให้ประชาชนสามารถมีปฏิสัมพันธ์ออนไลน์กับบุคคลอื่นได้ โดยการแบ่งปันความคิดเห็น, เชาว์ปัญญา, สารสนเทศ, เรื่องราวที่สนใจ และประสบการณ์ชีวิต สมาชิกอาจจะใช้เว็บไซต์ทำการปฏิสัมพันธ์กับเพื่อน, สมาชิกในครอบครัว, และเพื่อนร่วมงานที่พวกเขารู้จัก สมาชิก อาจจะปรารถนาในการสร้างบุคลิกภาพส่วนบุคคลใหม่ และสร้างความสัมพันธ์กับคนที่เป็นมืออาชีพเป็นการรวมกลุ่มคนผู้ที่สนใจเรื่องเดียวกันอย่างไม่มีขอบเขต

ภาพประกอบ 1.15 เครือข่ายสังคมออนไลน์ซึ่งได้รับความนิยมมาก 15 อันดับ
(ที่มา: http://www.bloggermentor.com)

1.6.22 อันธพาล (Cyberbullying) คือ การข่มขู่, การรบกวน, การทำให้รู้สึกอัปยศ, หรือจดหมายขู่ของใครคนหนึ่ง โดยเห็นว่าไม่สำคัญ หรือกลุ่มของบุคคลบนอินเทอร์เน็ต หรือขู่ทางโทรศัพท์อันธพาล อาจกลายเป็นเรื่องที่เข้มข้นรุนแรงได้, หรืออาจทำให้เด็กคิดฆ่าตัวตายได้

1.6.23 การเฝ้าติดตามทางอินเทอร์เน็ต (Cyberstalking) หมายถึงพฤติกรรมคุกคามหรือพฤติกรรมที่ไม่พึงประสงค์โดยใช้ความล้ำหน้าของการใช้อินเทอร์เน็ตและการสื่อสารอิเล็กทรอนิกส์ออนไลน์เป็นเครื่องมือ การกลั่นแกล้งทางอินเทอร์เน็ตของผู้ใหญ่ พอจะขยายใจความได้คือ: ความไม่เหมาะสมในการใช้สายโทรศัพท์มากจนเกินไป, ส่งจดหมายคุกคามหรือเกี่ยวกับเรื่องลามกอนาจาร, การละเมิด, การกระทำในเรื่องที่ป่าเถื่อนที่สังคมยอมรับไม่ได้, การคุกคามทางกายภาพ, การทำร้าย

ร่างกาย เป็นต้น ในสหรัฐอเมริกามีรัฐมากว่า 30 รัฐที่มีกฎหมายห้ามเกี่ยวกับเรื่องเหล่านี้ แต่กฎหมายก็มีช่องว่างขนาดใหญ่ระหว่างของรัฐบาลกลางและรัฐต่างๆ

1.6.24 การเผชิญหน้ากับนักล่าทางเพศ (Encounters with sexual predators) ในเว็บไซต์เครือข่ายสังคมบางเว็บไซต์จะวิพากษ์วิจารณ์และไม่ปกป้องผู้เยาว์จากการไล่ล่าทางเพศ เว็บไซต์ MySpace ถูกไม่อนุญาต ให้เผยแพร่การกระทำผิดทางเพศ ซึ่งมีผู้ที่ลงทะเบียนในเว็บไซต์จำนวนมากว่า 90,000 คน ที่มีการกระทำผิดทางเพศในเว็บไซต์ของมายสเปซ (MySpace)

1.6.25 การสร้างรหัสลับ (Encryption) เกี่ยวข้องกับทฤษฎีของคณิตศาสตร์ ในการถ่ายโอนข้อมูลดิจิทัลถึงกัน และมีการแปลงรหัส มีการถอดรหัส เพื่อสร้างความความปลอดภัยให้เกิดขึ้นในระบบ เพื่อป้องไม่ให้ผู้อื่นสามารถล่วงรู้ได้ ซอฟต์แวร์ที่ใช้ในการสร้างรหัสลับที่นิยมกันอย่างแพร่หลายมีอยู่ 2 ชนิด คือ RSA ซึ่งพัฒนาโดย RSA Data Security และอีกชนิดหนึ่ง คือ PGP (Pretty good privacy) เป็นซอฟต์แวร์ใช้งานบนอินเทอร์เน็ต

บทที่ 2

วรรณกรรมที่เกี่ยวข้อง

2.1 ความรู้พื้นฐานเกี่ยวกับเรื่องที่วิจัย

การวิจัย (Research) ตามความหมายของพจนานุกรมฉบับราชบัณฑิตยสถาน คือ การสะสม การรวบรวม. (ป. ส.).น. การค้นคว้าเพื่อหาข้อมูลอย่างถี่ถ้วนตามหลักวิชา เช่น วิจัยเรื่องปัญหาการจราจรในกรุงเทพมหานคร. ก. ค้นคว้าเพื่อหาข้อมูลอย่างถี่ถ้วนตามหลักวิชา เช่น เขากำลังวิจัยเรื่องมลพิษทางอากาศอยู่.ว. ที่ค้นคว้าเพื่อหาข้อมูลอย่างถี่ถ้วนตามหลักวิชา เช่น งานวิจัย.(อ. research).

การวิจัยทางวิทยาศาสตร์ อาศัยการประยุกต์ระเบียบวิธีทางวิทยาศาสตร์ที่ได้แรงผลักดันจากความอยากรู้อยากเห็น การวิจัยเป็นตัวสร้างข้อมูลข่าวสารเชิงวิทยาศาสตร์และทฤษฎีที่มนุษย์นำมาใช้ในการอธิบายธรรมชาติและคุณสมบัติของสรรพสิ่งต่าง ๆ รอบตัวเรา การวิจัยช่วยให้การประยุกต์ทฤษฎีต่าง ๆ มีความเป็นไปได้ในเชิงปฏิบัติ การวิจัยทางวิทยาศาสตร์ได้รับเงินสนับสนุนจากหน่วยงานของรัฐ องค์การการกุศล กลุ่มเอกชนซึ่งรวมถึงบริษัทต่าง ๆ งานวิจัยทางวิทยาศาสตร์จำแนกได้เป็นประเภทตามสาขาวิทยาการและวิชาเฉพาะทาง คำว่าการวิจัยยังใช้หมายถึงการเก็บรวบรวมข้อมูลข่าวสารที่เกี่ยวกับวิชาการบางสาขาอีกด้วย

วัตถุประสงค์หลักของการวิจัยขั้นพื้นฐานคือการสร้างความก้าวหน้าในความรู้และความเข้าใจเชิงทฤษฎีของสิ่งที่เชื่อมโยงระหว่างตัวแปรต่าง ๆ ด้วยการบุกเบิกที่เกิดจากการผลักดันของความอยากรู้อยากเห็น, ความสนใจ และการรู้เองของตัวผู้วิจัยเอง เป็นการดำเนินการที่ยังไม่มีการคำนึงถึงการนำไปใช้ประโยชน์ไว้ล่วงหน้าแม้ว่าในระหว่างการวิจัยจะมีการส่อว่าอาจนำผลไปประยุกต์เชิงปฏิบัติได้ก็ตาม คำว่า **“พื้นฐาน”** เป็นการบ่งชี้ว่าการวิจัยขั้นพื้นฐานเป็นการวางรากฐานให้เกิดการก้าวไปข้างหน้าด้วยการสร้างทฤษฎีที่บางครั้งอาจนำไปประยุกต์ในเชิงปฏิบัติได้ เนื่องจากการที่ไม่อาจประกันได้ว่าการวิจัยจะมีประโยชน์เชิงปฏิบัติได้ในระยะสั้นได้นี้เองที่ทำให้นักวิจัยขั้นพื้นฐานหาแหล่งเงินทุนสนับสนุนได้ยากกว่าการวิจัยแบบอื่น

อีกนัยหนึ่ง (**Best and Kahn, 2561:17)** ได้ให้ความหมายของวิจัยไว้ดังนี้ **การวิจัย** หมายถึง การวิเคราะห์ที่มีระบบ ระเบียบ และจุดมุ่งหมายที่ชัดเจน อันจะนำไปสู่การพัฒนาเป็นข้อสรุปที่เป็นนัยทั่วไป หรือได้มาซึ่งหลักเกณฑ์หรือทฤษฎีอันสามารถนำไปใช้ในการพยากรณ์ได้และมีคุณลักษณะต่าง ๆ ดังต่อไปนี้

1. การวิจัยจะต้องนำไปสู่การแก้ปัญหาเพื่อบรรลุเป้าหมายสุดท้าย (Ultimate Goal) กล่าวคือการค้นพบความสัมพันธ์เชิงเหตุและผลระหว่างตัวแปร (Variable) ต่าง ๆ

2. การวิจัยควรเน้นการพัฒนาข้อสรุปที่เป็นนัยทั่วไป (Generalization) หลักการ (Principle) หรือทฤษฎี (Theory) ซึ่งจะเป็นประโยชน์ในการพยากรณ์สิ่งที่จะเกิดขึ้นในอนาคต

3. การวิจัยต้องอยู่บนพื้นฐานของประสบการณ์ที่สามารถสังเกตได้ (Observable

Experience) หรือหลักฐานเชิงประจักษ์ (Empirical Evidence) ซึ่งในหลายกรณีจะเห็นว่ามีคำถามที่น่าสนใจหลายประการที่ไม่สามารถนำไปสู่กระบวนการทำวิจัยได้ เพราะไม่สามารถสังเกตได้

4. การวิจัยต้องมีการสังเกตที่ถูกต้อง (Accurate Observation) และพรรณาความได้นักวิจัยอาจเลือกวิธีการวัดและเครื่องมือทางด้านปริมาณ หากมีความเหมาะสมในการหาคำตอบได้ นักวิจัยก็จะต้องใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) หรือวิธีการที่ไม่ใช่เชิงปริมาณ (Non Qualitative Method) แทน

5. การวิจัยเกี่ยวข้องกับการเก็บข้อมูลใหม่ ซึ่งเป็นข้อมูลปฐมภูมิหรือข้อมูลที่ใช้เป็นครั้งแรกหรือมิฉะนั้นก็จะเป็นการใช้ข้อมูลที่มีอยู่แล้วสำหรับวัตถุประสงค์ใหม่ ในทางตรงข้ามการจัดการใหม่ (Reorganizing) หรือการนำเอาผลงานของผู้ทำวิจัยไว้แล้วมาศึกษาใหม่ (Restating) ไม่ถือว่าเป็นการทำวิจัย เพราะการศึกษาดังกล่าวไม่ได้ทำให้เกิดความรู้ใหม่ขึ้นมา

6. การวิจัยมีวิธีการหรือแบบการวิจัย (Research Procedure or Research Design) ซึ่งนำไปสู่การวิเคราะห์ที่เข้มแข็งและถือได้ว่าเป็นการวิจัย

7. การทำวิจัยต้องการความรู้ ความชำนาญ หรือความเชี่ยวชาญ (Expertise) ดังนั้นผู้ทำวิจัยจะต้องรู้และเข้าใจปัญหา (Problem) ที่จะทำพร้อมกับต้องรู้ด้วยว่าคนอื่นได้ทำวิจัยอะไรไว้บ้างและอย่างไรผู้ทำวิจัยจะต้องรู้ถ้อยคำที่ใช้ (Terminology) แนวคิด (Concept) และทักษะด้านเทคนิค (Technical Skill) เพื่อที่จะเข้าใจและวิเคราะห์ข้อมูลที่เก็บรวบรวมมาได้อย่างถูกต้อง

8. การวิจัยต้องมีวัตถุประสงค์และเหตุผลถูกต้องตามหลักตรรกวิทยา ดังนั้น ผู้ที่จะทำการวิจัยจึงควรใช้เครื่องทดสอบทุกอันที่เป็นไปได้เพื่อทำให้วิธี การศึกษา (Procedure) ที่ใช้ข้อมูลที่เก็บรวบรวมมา หรือแม้แต่ข้อสรุปของงานวิจัยที่ค้นพบมีเหตุผลและนักวิจัยต้องพยายามขจัดอคติส่วนตัว (Bias) หรือไม่ใช้อารมณ์ในการวิเคราะห์หากแต่ใช้เหตุผลและความรู้ทางวิชาการในการทำวิจัย

9. งานวิจัยที่จะทำจะต้องเกี่ยวข้องกับคำถามที่ต้องการคำตอบของปัญหาที่ยังแก้ไม่ได้

10. การทำวิจัยเป็นกิจกรรมที่ต้องใช้ความอดทน นักวิจัยควรคาดการณ์ไว้ก่อนถึงความผิดหวังหรือความหมดกำลังใจ หากถึงตอนที่จะหาคำตอบสำหรับคำถามที่ตั้งขึ้นได้อย่างยากลำบาก

11. การทำวิจัยจะต้องมีการบันทึกและรายงานอย่างระมัดระวัง โดยจะต้องให้คำนิยาม (Definition) คำศัพท์สำคัญ (Key Word) และจะต้องตระหนักถึงข้อจำกัด (Limitation) ต่างๆ ด้วย วิธีการศึกษาจะต้องกล่าวโดยละเอียดนอกจากนี้การอ้างอิง (Reference) ก็ต้องกระทำอย่างระมัดระวังผลการวิจัยจะต้องมีการบันทึกไว้อย่างชัดเจนและจะต้องเสนอข้อสรุป (Conclusion) ด้วยความระมัดระวัง

12. การทำวิจัยบางครั้งต้องการกำลังใจหรือการสนับสนุน ไม่ว่างานวิจัยนั้นจะมีผลเกื้อกูลหรือขัดทางต่อกลุ่มคนใดก็ตาม

ประเภทการวิจัย

การแบ่งประเภทของการวิจัย มีหลากหลายแบบขึ้นอยู่กับเกณฑ์ที่จะใช้ในการแบ่ง ต่อไปนี้ขอกล่าวถึงประเภทของการวิจัยที่ใช้เกณฑ์ต่าง ๆกันดังนี้

แบ่งตามจุดมุ่งหมายของการวิจัย แบ่งออกเป็น 3 ประเภท

1. การวิจัยเชิงพยากรณ์ (Predictive Research) เป็นการวิจัยเพื่อนำผลไปใช้ทำนายสิ่งที่จะเกิดในอนาคตซึ่งอาจพยากรณ์ได้ไม่ถูกต้องเสมอไป เพราะอาจมีสาเหตุอื่นทำให้เกิดคลาดเคลื่อนได้

2. การวิจัยเชิงวินิจฉัย (Diagnostic Research) เป็นการวิจัยเพื่อศึกษาสาเหตุของปัญหาต่าง ๆที่เกิดขึ้นกับบุคคล กลุ่มชน หรือชุมชน เพื่อให้เข้าใจถึงสาเหตุของปัญหารู้ถึงพฤติกรรม จะได้ให้ความช่วยเหลือและแก้ไขต่อไปการวิจัยประเภทนี้ นักสังคมสงเคราะห์นิยมใช้กันมาก

3. การวิจัยเชิงอรรถาธิบาย (Explanatory Research) เป็นการวิจัยเพื่อศึกษาเหตุการณ์ที่เกิดขึ้นแล้วว่าเกิดขึ้นอย่างไร มีสาเหตุมาจากอะไรและทำไมจึงเป็นเช่นนั้นในเชิงเหตุและผล

นอกจากนี้ **ยังมีวิจัยอีก 2 ประเภท** คือ **การวิจัยเชิงปริมาณและการวิจัยเชิงคุณภาพ** ดังมีรายละเอียดดังนี้ คือ

1. การวิจัยเชิงปริมาณ (Quantitative Research) เป็นการวิจัยที่มุ่งหาข้อเท็จจริงและข้อสรุปเชิงปริมาณ เน้นการใช้ข้อมูลที่เป็นตัวเลขเป็นหลักฐานยืนยันความถูกต้องของข้อค้นพบ และสรุปต่างๆ มีการใช้เครื่องมือที่มีความเป็นปรนัยในการเก็บรวบรวมข้อมูลเช่น แบบสอบถาม แบบทดสอบ การสังเกต การสัมภาษณ์ การทดลอง เป็นต้น

2. การวิจัยเชิงคุณภาพ (Qualitative Research) เป็นการวิจัยที่นักวิจัยจะต้องลงไปศึกษาสังเกต และกลุ่มบุคคลที่ต้องการศึกษาโดยละเอียดทุกด้านในลักษณะเจาะลึก ใช้วิธีการสังเกตแบบมีส่วนร่วม และการสัมภาษณ์แบบไม่เป็นทางการเป็นหลักในการเก็บรวบรวมข้อมูลการวิเคราะห์ข้อมูลจะใช้การวิเคราะห์เชิงเหตุผลไม่ได้มุ่งเก็บเป็นตัวเลขมาทำการวิเคราะห์ คำว่า คุณภาพในการวิจัย หมายถึง ข้อมูลที่ไม่เป็นตัวเลขหรือหมวดหมู่และมีรหัสเลขที่จะไปวิเคราะห์กันในทางสถิติ แต่เป็นข้อมูลที่ได้จากคำถามปลายเปิดหรือ จากการบันทึกสังเกตของผู้วิจัยหรือจากคำให้สัมภาษณ์ของกลุ่มผู้ให้ข้อมูลหลัก เป็นข้อมูลที่ไม่ได้วัดออกมาเป็นตัวเลข

ข้อแตกต่างระหว่างการวิจัยเชิงเชิงคุณภาพและการวิจัยปริมาณ

การวิจัยเชิงปริมาณและการวิจัยเชิงคุณภาพมีที่มาแตกต่างกัน กล่าวคือ การวิจัยเชิงคุณภาพมีพื้นฐานปรัชญาแบบธรรมชาตินิยม (Naturalism) ในขณะที่การวิจัยเชิงปริมาณมีพื้นฐานแบบปรัชญาแบบปฏิฐานนิยม (Positivism) ดังนั้น การค้นหาความจริงด้วยวิธีวิจัยเชิงคุณภาพจะเน้นปรากฏการณ์ที่เกิดขึ้นตามสภาพการณ์ที่เป็นธรรมชาติ ซึ่งบางครั้งเรียกว่า แนวคิดแบบปรากฏการณ์นิยม (Phenomenalism) แล้วอาศัยวิธีการพรรณนาเป็นสำคัญ ในขณะที่การค้นหาความจริงด้วยวิธีการวิจัยเชิงปริมาณต้องอาศัยกระบวนการหรือวิธีการทางวิทยาศาสตร์ที่อยู่บนรากฐานของข้อมูลเชิงประจักษ์ และขั้นตอนที่มีระเบียบแบบแผน คำว่า ปริมาณในทางวิจัย หมายถึง ข้อมูลเป็นตัวเลขสามารถนำไปใช้ในทางสถิติได้ มีระดับการวัดเป็นกลุ่ม เป็นช่วง และเป็นอัตราส่วน ในทางสถิติของการวิจัย . สุชาต ประสิทธิ์รัฐสินธุ์ (2550 : 292-293)

สำหรับการวิจัยเชิงคุณภาพและเชิงปริมาณนี้มีการเปรียบเทียบได้ดังที่ มนัส สุวรรณ (2544 : 16) ความว่า (1). การวิจัยเชิงคุณภาพมีพื้นฐานมาจากแนวคิดแบบธรรมชาตินิยม แต่ในเชิงปริมาณมาจากปฏิฐานนิยม (2). เชิงคุณภาพมุ่งเน้นปรากฏการณ์ที่เกิดขึ้นอย่างลึกซึ้ง แต่เชิงปริมาณมุ่งหาความจริงที่คนทั่วไปยอมรับ (common reality) (3).เชิงคุณภาพเป็นการวิจัยเน้นการพรรณนา /

อธิบาย (Descriptive approach) แต่เชิงปริมาณเน้นการวิเคราะห์ ทดลอง (Analytical and Experimental) ต้องอาศัยวิธีการทางสถิติเข้าช่วย (4) . เชิงคุณภาพให้ความสำคัญกับกระบวนการได้มาซึ่งความจริงแบบองค์รวม (Wholistic view) แต่เชิงปริมาณให้ความสำคัญต่อผลที่จะได้รับมากกว่ากระบวนการ (5). เชิงคุณภาพใช้วิธีวิเคราะห์แบบอุปมาน แต่เชิงปริมาณใช้แบบอนุมานด้วยการทดสอบคำตอบที่คาดคิดไว้ล่วงหน้า (Hypothesis) (6). เชิงคุณภาพมุ่งแสวงหาความรู้เพื่อสร้างเป็นทฤษฎี (Theory building) แต่เชิงปริมาณเริ่มต้นศึกษาวิจัยด้วยทฤษฎี (Hypothesis testing) (7). เชิงคุณภาพสิ้นสุดการวิจัยด้วยทฤษฎี (Ends with theory) แต่เชิงปริมาณกับเริ่มต้นด้วยทฤษฎี (Begins with theory) (8).เชิงคุณภาพส่วนใหญ่เป็นการวิจัยในสาขาวิชามนุษยศาสตร์และสังคมศาสตร์ แต่เชิงปริมาณนั้นส่วนใหญ่เป็นการวิจัยในสาขาวิชาวิทยาศาสตร์

แบ่งตามประโยชน์ของการวิจัย แบ่งออกเป็น 2 ประเภท ดังนี้

1. การวิจัยพื้นฐาน (Basic Research) หรือการวิจัยบริสุทธิ์ (Pure Research) หรือการวิจัยเชิงทฤษฎี (Theoretical Research) เป็นการวิจัยที่เสาะแสวงหาความรู้ใหม่ เพื่อสร้างเป็นทฤษฎีเพิ่มพูนความรู้ต่าง ๆ ที่มีความลึกซึ้งและสลับซับซ้อน ได้แก่ การวิจัยทางวิทยาศาสตร์และคณิตศาสตร์

2. การวิจัยประยุกต์ (Applied Research) หรือการวิจัยเชิงปฏิบัติ (Applied Research) หรือการวิจัยเชิงปฏิบัติ (Action Research) หรือการวิจัยเพื่อหาแนวทางปฏิบัติ (Operational Research) เป็นการวิจัยที่มุ่งเสาะแสวงหาความรู้และประยุกต์ใช้ความรู้ให้เป็นประโยชน์ในทางปฏิบัติหรือนำผลวิจัยไปแก้ไขปัญหาโดยตรงการวิจัยประเภทนี้อาจนำผลการวิจัยพื้นฐานมาวิจัยต่อแล้วทดลองใช้ เช่น การวิจัยเกี่ยวกับอาหาร ยารักษาโรค การเกษตร และการเรียนการสอน ดังนั้นเราจึงไม่สามารถที่จะแยกการวิจัยพื้นฐานและวิจัยประยุกต์ออกจากกันได้ โดยเด็ดขาด

นิภา ศรีไพโรจน์ (2561:2) การวิจัยจะมีประโยชน์อย่างแท้จริงหรือไม่ย่อมขึ้นอยู่กับความรับผิดชอบของนักวิจัย ตลอดจนความร่วมมือของผู้ให้ข้อมูลด้วย โดยทั่วไปแล้วอาจกล่าวได้ว่า การวิจัยมีประโยชน์ดังต่อไปนี้ (1) การวิจัยช่วยให้เกิดวิทยาการใหม่ ๆ เพิ่มพูนมากยิ่งขึ้นทั้งทางด้านทฤษฎีและปฏิบัติ (2) การวิจัยสามารถใช้แก้ปัญหาได้อย่างมีประสิทธิภาพ ถูกต้องและยุติธรรม (3) การวิจัยจะช่วยให้เข้าใจปรากฏการณ์และพฤติกรรมต่าง ๆ ได้ดีขึ้น และสามารถใช้ทำนายปรากฏการณ์และพฤติกรรมต่าง ๆ ได้อย่างถูกต้อง และมีประสิทธิภาพมากกว่าการคาดคะเนแบบสามัญสำนึก (4) การวิจัยสามารถช่วยในด้านการกำหนดนโยบาย การวางแผนงาน การตัดสินปัญหาหรือการวินิจฉัยสั่งการของผู้บริหารให้เป็นได้อย่างถูกต้องและรวดเร็ว (5). การวิจัยสามารถตอบคำถามที่ยังคลุมเครือให้กระจ่างชัดยิ่งขึ้น (6) การวิจัยจะช่วยกระตุ้นความสนใจของนักวิชาการ ให้มีการใช้ผลการวิจัยและทำงานค้นคว้าวิจัยต่อไป (7) การวิจัยจะทำให้ทราบข้อเท็จจริงต่าง ๆ ซึ่งนำมาใช้เป็นประโยชน์เพื่อการปรับปรุงหรือพัฒนาบุคคลและหน่วยงานต่าง ๆ ให้เจริญก้าวหน้าดียิ่งขึ้น (8) การวิจัยทำให้มีผลงานวิจัยเพิ่มมากขึ้น ซึ่งจะช่วยเสริมให้ทราบข้อเท็จจริงได้กว้างขวางและแจ่มชัดยิ่งขึ้น (9) การวิจัยจะช่วยกระตุ้นบุคคลให้มีเหตุผล รู้จักคิด และค้นคว้าหาความรู้อยู่เสมอ (10) การวิจัยช่วยให้มีเครื่องมือและเทคโนโลยีใหม่ ๆ ที่ทันสมัยเกิดขึ้นอยู่ตลอดเวลา ซึ่งอำนวยความสะดวกสบายให้แก่มนุษย์เป็นอย่างมาก (http://mcpswis.mcp.ac.th)

แบ่งตามวิธีการเก็บรวบรวมข้อมูล แบ่งออกเป็น 7 ประเภท ดังนี้

1. การวิจัยจากเอกสาร (Documentary Research) เป็นการวิจัยที่ผู้วิจัยทำการเก็บรวบรวมข้อมูลจากเอกสาร รายงาน จดหมายเหตุ ศิลาจารึก แล้วเสนอผลในเชิงวิเคราะห์ ส่วนใหญ่เอกสารที่ผู้วิจัยเก็บรวบรวมนี้จะอยู่ในห้องสมุด ดังนั้นจึงอาจเรียกการวิจัยประเภทนี้อีกอย่างหนึ่งว่า การวิจัยจากห้องสมุด (Library Research)

2. การวิจัยจากการสังเกต (Observation Research) เป็นการวิจัยที่ผู้วิจัยทำการเก็บรวบรวมข้อมูลด้วยวิธีการสังเกต การวิจัยประเภทนี้นิยมใช้มากทางด้านมานุษยวิทยา ซึ่งส่วนใหญ่เป็นการสังเกตุพฤติกรรมของบุคคลในสังคมในแง่ของสถานภาพ (Status) และบทบาท (Role)

3. การวิจัยแบบสำมะโน (Census Research) เป็นการวิจัยที่ผู้วิจัยทำการเก็บรวบรวมข้อมูลจากทุกๆหน่วยของประชาการ

4. การวิจัยแบบสำรวจจากตัวอย่าง (Sample Survey Research) เป็นการวิจัยที่ผู้วิจัยทำการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง

5. การศึกษาเฉพาะกรณี (Case Study) การศึกษาเฉพาะกรณีเป็นการวิจัยที่นักสังคมสงเคราะห์นิยมใช้มาก ที่เรียกว่าการศึกษาเฉพาะกรณีก็เพราะเป็นการศึกษาเรื่องที่สนใจในขอบเขตจำกัดหรือแคบ ๆ และใช้จำนวนตัวอย่างไม่มากนัก แต่จะศึกษาอย่างลึกซึ้งในเรื่องนั้น ๆ เพื่อให้ได้มาซึ่งข้อเท็จจริงที่จะทำให้ทราบว่าบุคคลนั้นหรือกลุ่มบุคคลนั้นมีความบกพร่องในเรื่องใด เนื่องมาจากสาเหตุใดเพื่อจะได้หาทางแก้ไขหรือช่วยเหลือต่อไป

6. การศึกษาแบบต่อเนื่อง (Panel Study) เป็นการศึกษาที่มีการเก็บข้อมูลเป็นระยะๆ เพื่อดูการเปลี่ยนแปลงตามกาลเวลาของกลุ่มตัวอย่าง ซึ่งการศึกษาแบบต่อเนื่องนี้จะช่วยให้เข้าใจและทราบถึงลักษณะการเปลี่ยนแปลงได้เป็นอย่างดี

7. การวิจัยเชิงทดลอง (Experimental Research) เป็นการวิจัยที่ผู้วิจัยเก็บข้อมูลมาจากการทดลองซึ่งเป็นผลมาจากการกระทำ (Treatment) โดยมีการควบคุมตัวแปรต่าง ๆ ให้เป็นไปตามวัตถุประสงค์ที่กำหนดไว้

แบ่งตามลักษณะการวิเคราะห์ข้อมูล แบ่งออกเป็น 2 ประเภท ดังนี้

1. การวิจัยเชิงคุณภาพ (Qualitative Research) เป็นการวิจัยที่นำเอาข้อมูลทางด้านคุณภาพเป็นข้อมูลที่ไม่เป็นตัวเลขแต่จะเป็นข้อความบรรยายลักษณะสภาพเหตุการณ์ของสิ่งต่าง ๆ ที่เกี่ยวข้องและการเสนอผลการวิจัยก็จะออกมาในรูปของข้อความที่ไม่มีตัวเลขทางสถิติสนับสนุน เช่นเดียวกัน การวิจัยประเภทนี้จึงมุ่งบรรยายหรืออธิบายเหตุการณ์ต่างๆโดยอาศัยความคิดวิเคราะห์เพื่อประเมินผลหรือสรุปผลนั่นเอง

2. การวิจัยเชิงปริมาณ (Quantitative Research) เป็นการวิจัยที่นำเอาข้อมูลเชิงปริมาณมาวิเคราะห์กล่าวคือใช้ตัวเลขประกอบการวิเคราะห์ สรุปผล และการเสนอผลการวิจัยก็ออกมาเป็นตัวเลขเช่นเดียวกัน ดังนั้น การวิจัยประเภทนี้จึงมุ่งที่จะอธิบายเหตุการณ์ต่าง ๆ โดยอาศัยตัวเลขยืนยันแสดงปริมาณมากน้อยแทนที่จะใช้ข้อความบรรยายให้เหตุผล

อนึ่งการวิจัยที่ดีนั้นไม่ควรใช้แบบใดแบบหนึ่งโดยเฉพาะ เพราะจะทำให้ผลที่ได้ไม่แจ่มชัดเท่าที่ควร ดังนั้นในการปฏิบัติมักจะประยุกต์การวิจัยทั้ง 2 ประเภทนี้เข้าด้วยกันเพื่อให้ผลการิวจัยมีทั้งเหตุและผลและมีตัวเลขสนับสนุนอันจะทำให้ผลการวิจัยน่าเชื่อถือมากยิ่งขึ้น

แบ่งตามลักษณะวิชาหรือศาสตร์ แบ่งออกเป็น 2 ประเภท ดังนี้

1. การวิจัยทางวิทยาศาสตร์ (Scientific Research) เป็นการวิจัยเกี่ยวกับปรากฏการณ์ธรรมชาติของสิ่งมีชีวิตและไม่มีชีวิต ทั้งที่มองเห็นและมองไม่เห็นการวิจัยประเภทนี้ได้กระทำกันมานานแล้ว และก่อให้เกิดประโยชน์ต่อมวลมนุษย์อย่างมากมายเช่น การค้นพบยา รักษาโรค การค้นพบสิ่งประดิษฐ์ใหม่ๆ เป็นต้น นอกจากนี้การวิจัยทางวิทยาศาสตร์ยังสามารถใช้แก้ปัญหาที่เกิดจากธรรมชาติได้อีกด้วย เนื่องจากการวิจัยทางวิทยาศาสตร์มีเครื่องมือและอุปกรณ์ที่เที่ยงตรงและมีกฎเกณฑ์แน่นอน ตลอดจนสามารถควบคุมการทดลองได้เพราะทำการทดลองในห้องปฏิบัติการ จึงทำให้ผลการวิจัยทางด้านวิทยาศาสตร์ได้รับความเชื่อถือมาก

2. วิจัยทางสังคมศาสตร์ (Social Research) เป็นการวิจัยที่เกี่ยวกับสภาพแวดล้อม สังคม วัฒนธรรมและพฤติกรรมของมนุษย์ เช่น การวิจัยด้านปรัชญา สังคมวิทยาศาสตร์ เศรษฐศาสตร์ เป็นต้น การวิจัยทางสังคมศาสตร์นี้แตกต่างกับการวิจัยทางวิทยาศาสตร์มาก เนื่องจากสังคมศาสตร์เป็นวิชาที่ว่าด้วยสังคม สิ่งแวดล้อม และพฤติกรรมของมนุษย์ ซึ่งวัดไม่ได้โดยตรงและควบคุมได้ยาก แต่มนุษย์ก็ได้พยายามวัดโดยใช้เครื่องมือวัดทางอ้อม เช่น ใช้แบบทดสอบ แบบสอบถาม แบบวัดเจตคติ ฯลฯ และได้นำเอาวิธีการทางวิทยาศาสตร์มาช่วยในกาวิจัยทำให้ผลการวิจัยเป็นที่น่าเชื่อถือมากยิ่งขึ้น แม้ว่าการวิจัยทางสังคมศาสตร์จะมีข้อจำกัดอยู่หลายประการก็ตาม แต่การวิจัยทางด้านนี้ก็สามารถศึกษาพฤติกรรมของมนุษย์ได้มากพอสมควร

แบ่งตามระเบียบวิธีวิจัย แบ่งออกเป็น 3 ประเภท ดังนี้

1. การวิจัยเชิงประวัติศาสตร์ (Historical Research) เป็นการวิจัยเพื่อค้นหาข้อเท็จจริงของเหตุการณ์ที่ผ่านมาแล้วในอดีต โดยมีจุดมุ่งหมายที่จะบันทึกอดีตอย่างมีระบบ และมีความเป็นปรนัยจากการรวบรวมประเมินผล ตรวจสอบ และวิเคราะห์เหตุการณ์เพื่อค้นหาข้อเท็จจริงในอันที่จะนำมาสรุปอย่างมีเหตุผล การวิจัยประเภทนี้ต้องอ้างอิงเอกสารและวัตถุโบราณที่มีเหลืออยู่ ซึ่งโดยส่วนใหญ่แล้วมักไม่ใช้สถิติ สรุปได้ว่าการวิจัยประเภทนี้มุ่งที่จะบอกว่า “เป็นอะไรในอดีต” (What was)

2. การวิจัยเชิงบรรยายหรือพรรณนา (Descriptive Research) เป็นการวิจัยเพื่อค้นหาข้อเท็จจริงในสภาพการณ์หรือภาวการณ์ของสิ่งที่เป็นอยู่ในปัจจุบันว่าเป็นอย่างไร การวิจัยประเภทนี้มักจะทำการสำรวจหรือหาความสัมพันธ์ต่าง ๆ เกี่ยวกับเรื่องของความเชื่อ ความคิดเห็น และเจตคติ จึงกล่าวได้ว่าเป็นการวิจัยที่มุ่งจะบอกว่า เป็นอะไรในปัจจุบัน (What is) นั่นเองเช่น การวิจัยเรื่อง “เจตคติของครูน้อยที่มีต่อผู้บริหารการศึกษา”

3. การวิจัยเชิงทดลอง (Experimental Research) เป็นการวิจัยเพื่อค้นหาความสัมพันธ์เชิงเหตุและผลของปรากฏการณ์ต่าง ๆ การวิจัยประเภทนี้ต้องมีการควบคุมตัวแปรต้น เพื่อสังเกตตัวแปรตามที่เปลี่ยนแปลงไปเพื่อจะได้ทราบว่าอะไรเป็นสาเหตุที่ทำให้เกิดผล ดังนั้นตัวแปรในการวิจัยจึงต้องมีทั้งกลุ่มควบคุมและกลุ่มทดลอง สรุปได้ว่า การวิจัยประเภทนี้มุ่งที่จะบอกว่า “อะไรอาจจะเกิดขึ้น” (What may be) (https://www.gotoknow.org/posts/625137)

2.2 ทฤษฎีที่รองรับเรื่องที่วิจัย

สังคมสารสนเทศ (The Information Society) คลังศัพท์ไทย ได้ให้นิยามคำว่า สังคมสารสนเทศเอาไว้ว่า คือสังคมที่มีการนำข้อมูลสารสนเทศในรูปแบบต่างๆ มาช่วยดำเนินกิจกรรมทั้งเพื่อประโยชน์ส่วนตนและประโยชน์ส่วนรวม สังคมสารสนเทศเริ่มมีความเด่นชัดในสังคมโลกเมื่อ ปี ค.ศ. 1996-1998 ที่ทั่วโลกต่างยอมรับร่วมกันว่า สารสนเทศจะเป็นสิ่งที่เป็นพื้นฐานสู่การขับเคลื่อนต่าง ๆ ของโลก สังคมอุตสาหกรรม เศรษฐกิจ และวัฒนธรรม ต่างถูกขับเคลื่อนด้วยข้อมูลข่าวสาร ทำให้มีการกำหนดร่วมกันว่า ยุคปัจจุบันคือยุคของสังคมสารสนเทศ หรือยุคของสังคมข้อมูลข่าวสาร ในทศวรรษที่ผ่านมา เทคโนโลยีสารสนเทศซึ่งรวมทั้งเทคโนโลยีคอมพิวเตอร์ และเทคโนโลยีการสื่อสาร (ICT: Information and Communication Technology) อีกทั้งยังรวมถึงเทคโนโลยีนำสมัยอื่น ๆ เช่น เทคโนโลยีชีวภาพและพันธุวิศวกรรมศาสตร์ ได้ก่อให้เกิดผลกระทบเกี่ยวกับกิจกรรมต่าง ๆ ของสังคม รวมทั้งกิจกรรมทางเศรษฐกิจอย่างกว้างขวาง ก่อให้เกิดความเจริญเติบโตทางเศรษฐกิจบนพื้นฐานของ "เศรษฐกิจแห่งภูมิปัญญาและการเรียนรู้" (knowledge-Based Economy) กอปรกับการเติบโตของระบบการสื่อสารที่ทันสมัย ทำให้เกิดภาวะการณ์การเปลี่ยนแปลงอย่างก้าวกระโดดในด้านเศรษฐกิจอย่างรวดเร็ว เกิดเป็นระบบ เศรษฐกิจใหม่ (New Economy) ที่แตกต่างไปจากระบบเศรษฐกิจในรูปแบบเดิมที่เน้นการใช้แรงงานและทุนเป็นหลัก ระบบเศรษฐกิจใหม่ดังกล่าวนับว่าเป็นผลผลิตที่เกิดจากการใช้ประโยชน์จากปัจจัยการผลิตประเภท "สารสนเทศ" (Information) และ "ความรู้" (Knowledge)ในระดับสูงอย่างไม่เคยเป็นมาก่อน การเจริญเติบโตของเทคโนโลยีสารสนเทศและการสื่อสารก่อให้เกิดกระบวนการผลิตที่มีประสิทธิภาพ (Productivity) มีความเปลี่ยนแปลงและผันแปรอย่างรวดเร็ว (High Volatility) มีนวัตกรรมใหม่ ๆ (Innovation) เกิดขึ้นตลอดเวลาทั้งในส่วนของโครงสร้างองค์กรและในระบบธุรกิจทุกระดับ เทคโนโลยีสารสนเทศและการสื่อสารทำให้เกิดปฏิสัมพันธ์ใกล้ชิดและรวดเร็วระหว่างหน่วยต่าง ๆ ของประชาสังคม (Civil Society) ไม่ว่าจะเป็นภาครัฐ ภาคเอกชน และองค์กรพัฒนาเอกชน สภาวการณ์ของเทคโนโลยีสารสนเทศในปัจจุบัน ทำให้ สารสนเทศ และ ความรู้ มีบทบาทสูงมากโดยเฉพาะในระบบเศรษฐกิจ และในส่วนของการช่วยเสริมสร้างความมั่งคั่งและงานอาชีพต่าง ๆ ให้กับสังคมทุกระดับ (Wealth & Employment Creation) สภาวการณ์ดังกล่าวทำให้เกิดกระแสการใช้ "เทคโนโลยีสารสนเทศการสื่อสารและความรู้" เป็นกลไกสำคัญในการขับเคลื่อนกิจกรรมต่าง ๆ ในสังคมท่ามกลางกระแสโลกาภิวัตน์ โดยมีความหวังร่วมกันว่า เทคโนโลยีสารสนเทศและการสื่อสารดังกล่าว จะสามารถช่วยให้สังคมพัฒนาอย่างเท่าเทียมกัน และสามารถส่งผลต่อการพัฒนาคุณภาพชีวิตของประชาชนในสังคมดีขึ้นกว่าเดิม

กองบรรณาธิการ (2560:24-27) ได้รายงานใน Section Security Report วารสาร CIO World & Business เรื่อง “โจรไซเบอร์อาศัยช่องโหว่ DDoS และ POS ฉกเงินร้านค้า” จากรายงานของแคสเปอร์สกี้ แลป เรื่อง IT Security Economics Report พบว่า บริษัทมากกว่า 77% ได้รับความเสียหายจากการโจมตีทางไซเบอร์ในช่วง 12 เดือนที่ผ่านมา ขณะที่การโจมตี DDoS และช่องโหว่ของระบบขายหน้าร้าน (POS system) มีการระบาดเพิ่มขึ้น 16% ซึ่งจากตัวเลขนี้ยังชี้ให้เห็นว่าโจรไซเบอร์มีการวางแผนการโจมตีเพิ่มขึ้นในช่วงเทศกาลคริสต์มาสและปีใหม่ที่ผู้คนจะออกมาจับจ่ายใช้สอยหนาแน่นมากกว่าปกติ

ในปี 2017 นี้ มีการรายงานการรุกล้ำระบบความปลอดภัยไซเบอร์ระดับสูงในระบบการจ่ายเงินของแบรนด์ใหญ่ๆ มากมาย ได้แก่ Chipotle, Hyatt Hotels และจากรายงานล่าสุดของแคสเปอร์สกี้ แลป เรื่อง DDoS Intelligence Report ก็พบการโจมตี Botnet DDoS ที่เพิ่มจำนวนมากขึ้นและแพร่ระบาดในช่วงไตรมาสที่ 3 ของปีนี้ ซึ่งมีเป้าหมายการโจมตีประเทศต่างๆ ทั่วโลกจำนวนมากถึง 98 ประเทศ (เปรียบเทียบกับไตรมาสที่ 2 มี 82 ประเทศ)

ชนินทร์ นาทะพันธ์ (2555:29) ได้รายงานในงานวิจัยเรื่อง “การศึกษาดัชนีความสุขมวลรวมในประเทศไทยทางด้านเทคโนโลยีสารสนเทศ” ผลวิจัยพบว่า ปัจจัยความสุขในประเทศไทยครอบคลุมทุกปัจจัยของปัจจัยความสุขสากล แต่มีบางปัจจัยที่ไม่มีในการวัดความสุขสากลซึ่งอาจเป็นปัจจัยที่กำหนดขึ้นเพื่อให้เข้ากับวัฒนธรรม หรือเหตุการณ์ในประเทศที่เกิดขึ้น ผู้เชี่ยวชาญมีความเห็นว่า เทคโนโลยีสารสนเทศที่มีผลกระทบต่อความสุขมากที่สุด คือ การมีบริการเทคโนโลยีสารสนเทศที่มีผลต่อด้านเศรษฐกิจ (ร้อยละ 80.00 ของจำนวนผู้เชี่ยวชาญ) รองลงมาคือ ความสามารถในการเข้ารับบริการของประชาชน (ร้อยละ 79.02) ของจำนวนผู้เชี่ยวชาญ) และมีการบริการเทคโนโลยีสารสนเทศที่มีผลต่อธรรมาภิบาล (ร้อยละ 74.63 ของผู้เชี่ยวชาญ) โดยรวม เทคโนโลยีสารสนเทศมีผลกระทบต่อความสุขจริง ในระดับกลาง (ค่าเฉลี่ย 3.29) แสดงให้เห็นว่า ในปัจจุบัน เทคโนโลยีสารสนเทศมีบทบาทในการดำเนินชีวิตประจำวัน และควรพิจารณาใช้เป็นปัจจัยหนึ่งในการวัดความสุขของประชากรได้

พงศ์สุข หิรัญพฤกษ์ (2560:2) ปัจจุบันมีเทคโนโลยี และ Applications ใหม่ๆ เกิดขึ้นเป็นจำนวนมาก เรียกกันว่าเป็นสิ่งก่อให้เกิด Disruptive คือ การทำลายล้างระบบเดิมที่เคยเป็นมา เช่น การจองตั๋วเครื่องบิน, การจองห้องพักโรงแรม เป็นต้น ในประเทศไทยเรามีแผนเหมือนกันที่จะรองรับในเรื่องนี้ นั่นคือ Thailand 4.0 ทุกคนเคยได้ยินคำว่า **Thailand 4.0** เรื่องนี้เป็นเรื่องของความตั้งใจที่ดีมากของรัฐบาลชุดนี้ ซึ่งก็คือ การนำเอา Innovation มาใช้นั่นเอง ก่อนหน้าเราอาจเคยได้ยินคำว่า Creative Economy, Digital Economy พอเปลี่ยนรัฐบาลทีหนึ่งเราก็จะได้ยินแคมเปญใหม่ๆ เกิดขึ้นเรื่อยๆ แต่คำๆ นี้คือ Thailand 4.0 น่าสนใจมาก คนที่พูดเป็นคนแรกคือนายกรัฐมนตรี เป็นผู้ประกาศขึ้นมา และเบื้องหลังกระทรวงการคลัง คือ ดร.สมคิด จาตุศรีพิทักษ์ ก็คิดให้ทะลุมากขึ้น แต่ก่อนจะมาถึง Thailand 4.0 นั้นก็ต้องมาดูวิวัฒนาการกันก่อน Thailand 4.0 เริ่มมีมาตั้งแต่ **Thailand 1.0 คือยุคเกษตรกรรม** เน้นการผลิต การขายพืชพันธุ์ทางการเกษตร เช่น ขายข้าว ขายพืชผัก พืชไร่ สุกร เป็ด ไก่ เป็นต้น เราคงเคยได้ยินเพลงที่เปิดทางทีวีช่อง 7 สี ที่มีข้อความว่า กสิกรแข็งขันคือกระดูกสันหลังของชาติ ไทยจะเรืองอำนาจ เพราะเราเป็นชาติกสิกรรม แต่จริงๆ แล้ว เราจะเรืองอำนาจได้ไหมครับ เห็นมีแต่ธนาคารกสิกรไทยเท่านั้นที่เรืองอำนาจจากการเก็บดอกเบี้ย เพราะประชาชนที่เป็นชนชั้นกสิกรรมไม่สามารถจะสร้างแต้มต่อทางด้านเศรษฐกิจได้ ต่อมาเข้าสู่**ยุค Thailand 2.0 ยุคอุตสาหกรรมเบา** เน้นการผลิตสินค้าที่มีน้ำหนักเบา เป็นอุตสาหกรรมที่ไม่ต้องใช้ทุนมากนัก เช่น การผลิตเครื่องนุ่งห่ม รองเท้า กระเป๋า เครื่องดื่ม เครื่องเขียน การทำอาหารกระป๋อง การผลิตยา และเครื่องเวชภัณฑ์ การผลิตอลูมิเนียม เครื่องวิทยุ โทรทัศน์ การผลิตเครื่องเด็กเล่น รวมถึงการผลิตแป้งชนิดต่างๆ ในยุคนี้เป็นยุคที่นายกรัฐมนตรีของไทย คือ พลเอกชาติชาย ชุณหวรรณ ที่บอกว่าประเทศไทยจะเป็นนิค (New Industry Country) ประเทศอุตสาหกรรมใหม่ จนกระทั่งคุณแอ๊ด คาราบาวแต่งเพลง เมดอินไทยแลนด์ ต่อมาเศรษฐกิจพัฒนาเข้ามาสู่**ยุค Thailand 3.0 เน้นอุตสาหกรรมหนักและการส่งออก** เช่น ผลิต และส่งออกขายเหล็กกล้า เช่น รถยนต์ กลั่นน้ำมัน ก๊าซธรรมชาติ ปูนซีเมนต์ เป็นต้น และมีคำหนึ่งที่บอกว่า เราจะเป็น ดีทร้อยด์

แห่งเอเชีย คือ การผลิตรถยนต์ส่งออกไปขายยังต่างประเทศ รวมไปถึงการผลิตฮาร์ดดิสก์ ซึ่งเราก็ตื่นเต้นที่มีแบรนด์ต่างชาติใหม่ๆ ที่เข้ามา และแรงงานไทยก็ได้เข้าไปทำงานในอุตสาหกรรมเหล่านั้น ตั้งแต่ฐานล่างสุดคือแรงงานไปถึงตำแหน่งผู้บริหาร แต่มันก็ไม่ใช่แบรนด์ของเรา สุดท้ายคือ**ยุค Thailand 4.0** เป็นวิสัยทัศน์เชิงนโยบายโมเดลพัฒนาเศรษฐกิจของรัฐบาลที่ยึดหลัก **"มั่นคง มั่งคั่ง และยั่งยืน"** เพื่อรับมือกับการเปลี่ยนแปลงของโลกที่มีการเปลี่ยนแปลงอย่างรวดเร็ว ทำให้ประเทศไทยจำเป็นต้องมี Innovation หรือนวัตกรรม จึงจะสามารถแข่งขันกับประเทศอื่นได้ ส่วนที่เรียกว่า 4.0 เพราะไปสอดคล้องกับประเทศเยอรมันนี ที่เป็นศูนย์กลางของประเทศยุโรปที่เขาเข้าสู่อุตสาหกรรม 4.0 แล้ว ตั้งชื่อว่า Industry 4.0 หรืออาจจะเรียกว่า Machine Learning หมายถึงการสอนให้เครื่องจักรสามารถเรียนรู้ได้ด้วยตนเอง และคิดแทน และคิดต่อได้ด้วย ซึ่งมันก็ต้องมีคุณสมบัติหลายๆ อย่าง เราจะเห็นรูปภาพ Infographic ที่มีอุปกรณ์แต่ละชนิดมีการเชื่อมต่อกัน หรือ Connection กันนั้นนั่นเองคือ การส่งข้อมูลถึงกัน เมื่อก่อนการผลิตสินค้าออกมาเป็นจำนวนมาก ไม่ทราบว่าเหลืออีกเท่าไร ค้างอยู่ในสต็อกอีกเท่าไร แต่ยุคใหม่นี้สามารถจะทำให้ทราบได้ว่าเหลือสินค้าอีกเท่าไร และถึงเวลาจะผลิตพืชพันธุ์ทางการเกษตรเพิ่มได้หรือยัง เพราะการเกษตรเหล่านั้นมีการเชื่อมต่ออุปกรณ์ด้วย Internet of Things (IoT) รวมไปถึงสามารถจับความเร็วแรงลม น้ำ ฝนจะตกหรือไม่ ทางด้านการเกษตรจะผลิตทันหรือเปล่า และนำข้อมูลเหล่านั้นมาทำการประมวลผลว่า จะเปิดไลน์การผลิตเมื่อไร เป็นอย่างไร สมควรจะผลิตพืชผลได้หรือยัง นอกจากนี้ ยังมีการพัฒนา Application ใหม่ๆ ขึ้นมา รวมถึงการนำ Application เหล่านั้นมาใช้กับระบบธนาคาร คุณธนาเธียรอัจฉริยะ (โจ้) รักษาการ Chief Marketing Officer ธนาคารไทยพาณิชย์ ได้รวมกลุ่มของธนาคารพยามยามที่พัฒนาสิ่งใหม่ๆ ขึ้นมา เพราะใกลุ่มของธนาคารมีโอกาสเสี่ยงที่จะสูญพันธุ์มากที่สุด และพนักงานธนาคารก็กลัวตกงานกันมากที่สุด ตัวอย่างที่เห็นได้ชัดเจนของ Application ใหม่ที่เข้ามา คือ พร้อมเพย์ (PromptPay) คือ การชำระเงินโดยไม่ต้องเสียค่าธรรมเนียม และมาตรฐานใหม่อีกอย่างหนึ่งที่เกิดขึ้น คือ การชำระเงินผ่าน QR Code ด้วยการสแกนชำระเงินระหว่างธนาคาร ซึ่งไม่ต้องเสียค่าธรรมเนียม

ศุกรีย์ ศรีสารคาม (2557:2) ได้รายงานในวิจัยเรื่อง "ปัจจัยที่มีผลต่อคุณธรรม จริยธรรมในการใช้อินเทอร์เน็ต" ผลการวิจัยพบว่า ผู้ตอบแบบสอบถามส่วนใหญ่ เป็นเพศหญิง มีอายุต่ำกว่าหรือเท่ากับ 13 ปี ศึกษาอยู่ชั้นมัธยมศึกษาปีที่ 2 การใช้อินเทอร์เน็ตส่วนใหญ่ใช้ช่วงเวลาหลังเลิกเรียนในวันจันทร์-ศุกร์ และวันเสาร์-อาทิตย์ ใช้อินเทอร์เน็ตในช่วงเวลา ตั้งแต่ 18.01-24.00 น. โดยใช้โทรศัพท์มือถือเป็นอุปกรณ์ในการใช้อินเทอร์เน็ต ส่วนใหญ่ใช้ที่บ้าน ศึกษาการใช้อินเทอร์เน็ตด้วยตนเอง พอมีความรู้บ้างเกี่ยวกับกฎหมายในการใช้อินเทอร์เน็ต ใช้ระบบเครือข่ายอินเทอร์เน็ตเพื่อความบันเทิง เพื่อค้นหาข้อมูลภายในประเทศและจากต่างประเทศ

ผลการทดสอบสมมติฐานพบว่า เพศ อายุ และระดับชั้นการศึกษา มีผลต่อคุณธรรม จริยธรรมในการใช้อินเทอร์เน็ตในภาพรวม และช่วงเวลา สถานที่ในการใช้อินเทอร์เน็ต การใช้ระบบเครือข่ายอินเทอร์เน็ตมีผลต่อคุณธรรม จริยธรรมในการใช้อินเทอร์เน็ตในภาพรวม

สาวตรี สุขศรี และคณะ (2555: 261-262) ได้เสนอไว้ในงานวิจัยเรื่อง **"ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น"** ความว่า สำหรับอาชญากรรมคอมพิวเตอร์ กับการเผยแพร่เนื้อหาผิดกฎหมายในสื่อออนไลน์นั้น ในประเทศสหพันธรัฐเยอรมนีนั้น ถือว่าเป็นประเทศต้นๆ ในทวีปยุโรปที่ให้ความสำคัญกับปัญหาการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์และ

อินเทอร์เน็ต การถกเถียงในวงวิชาการเพื่อแสวงหามาตรการทางกฎหมายรวมทั้งมาตรการอื่นๆ ที่เหมาะสมเพื่อป้องกันและปราบปรามการกระทำผิดเหล่านี้เกิดขึ้นตั้งแต่ก่อนปี 1986 ทั้งนี้ เนื่องจากอัตราการกระทำความผิดในลักษณะดังกล่าวเพิ่มขึ้นอย่างต่อเนื่องไม่ว่าจะเป็น การฉ้อโกงทางคอมพิวเตอร์ (Computerbetrug) การปลอมแปลงข้อมูลคอมพิวเตอร์ (Datenveranderung) การเจาะรบบคอมพิวเตอร์ การจารกรรมข้อมูลส่วนบุคคลหรือข้อมูลทางการค้า (Computerspionage) การพนันผิดกฎหมายออนไลน์ รวมไปถึงการเผยแพร่ภาพลามกอนาจารเด็กและเยาวชน (Kinderpornographie) เคยมีรายงานสำรวจการกระทำความผิดเหล่านี้ในยุคต้นๆ ในเยอรมันนี พบว่า ประมาณร้อยละ 1 ของเว็บไซต์ที่ให้บริการอยู่ในประเทศทั้งหมดเป็นเว็บไซต์ที่มีเนื้อหาผิดกฎหมาย ปัญหาต่างๆ ที่เกิดขึ้น ส่งผลให้หน่วยงานผู้รับผิดชอบเร่งหาแนวทางในการป้องกันและปราบปรามที่มีประสิทธิภาพไม่ว่าจะเป็นการจัดตั้งหน่วยงานพิเศษเพื่อรับผิดชอบการกระทำความผิดด้านนี้เป็นการเฉพาะ ซึ่งในบางกรณีก็จำเป็นต้องกำหนด หรือใช้มาตรการบางประการที่ส่งผลกระทบทั้งต่อผู้ให้บริการและผู้ใช้บริการอินเทอร์เน็ตด้วย

แม้อนุสัญญาว่าด้วยอาชญากรรมไซเบอร์ (Convention on Cybercrime) ซึ่งออกโดยคณะมนตรียุโรป (Europarat) จะมีผลตั้งแต่วันที่ 1 กรกฎคม 2004 ภายหลังมีประเทศลงนามให้สัตยาบันครบ 5 ประเทศ ตามเงื่อนไขที่กำหนด แต่ประเทศเยอรมนีซึ่งลงนามในอนุสัญญาฉบับดังกล่าวตั้งแต่วันที่ 23 พฤศจิกายน 2001 กลับให้สัตยาบันและยังผลให้ประเทศมีหน้าที่ต้องบัญญัติหรือปรับปรุงกฎหมายให้สอดคล้องกับอนุสัญญาฉบับนี้เมื่อวันที่ 9 มีนาคม 2009 สาเหตุที่เยอรมนีให้สัตยาบันรวมทั้งอนุวัติการตามอนุสัญญา (วันที่ 1 กรกฎาคม 2009) ค่อนข้างล่าช้า เยอรมนีให้เหตุผลว่าข้อกำหนด และหลักเกณฑ์หลายข้อในอนุสัญญาดังกล่าวไม่สอดคล้องกับนโยบาย และมาตรการที่ประเทศเยอรมนีใช้บังคับอยู่แล้ว จึงต้องใช้เวลาในการศึกษาวิจัย และพิจารณาว่าจะสามารถปรับเปลี่ยนข้อกฎหมายภายในได้มากน้อยเพียงใด อย่างไรก็ตาม หากกล่าวถึงประวัติการบัญญัติรวมทั้งการแก้ไขปรับปรุงกฎหมายเพื่อรองรับปัญหาการกระทำความผิดในรูปแบบใหม่เหล่านี้ ต้องนับว่า ประเทศเยอรมนีตื่นตัวและดำเนินการมาเป็นระยะเวลานานแล้ว ตั้งแต่ปี 1986 ซึ่งมีการปฏิรูปกฎหมายหลายฉบับเพื่อป้องกันและปราบปรามอาชญากรรมทางเศรษฐกิจ (2.WiKG) เยอรมนีเพิ่มเติมฐานความผิดหลักๆ ที่เกี่ยวกับคอมพิวเตอร์ไว้ในประมวลกฎหมายอาญาร่วมกับฐานความผิดดั้งเดิมในหมวดเดียวกัน ในขณะที่ฐานความผิดเฉพาะอื่นๆ อาทิ ความผิดเกี่ยวกับการละเมิดทรัพย์สินทางปัญญาบนอินเทอร์เน็ต ข้อกำหนดเกี่ยวกับภาระหน้าที่รวมทั้งความรับผิดชอบของผู้ให้บริการอินเทอรืเน็ตประเภทต่างๆ จะถูกบัญญัติแยกไว้ในกฎหมายเฉพาะ สำหรับปัญหาในทางแพ่งและพาณิชย์ก็มีกฎหมายในเรื่องนั้นต่างหากเช่นกัน โดยฌพาะอย่างยิ่ง เพื่อรองรับปฏิบัติการและธุรกรรมรูปแบบใหม่ๆ

อมรรัตน์ วงศ์โสภา (2561:2) ได้รายงานวิจัยเรื่อง “พฤติกรรมการใช้และผลกระทบของสื่อสังคมออนไลน์ประเภทเฟซบุ๊คต่อการดำเนินชีวิตของนักศึกษา กรณีศึกษามหาวิทยาลัยราชภัฏเลย” ผลการวิจัยพบว่าพฤติกรรมการใช้งานเฟซบุ๊คของนักศึกษา ใช้งานสื่อสังคมออนไลน์มากกว่า 1 ประเภท เกือบทั้งหมดใช้งานสื่อสังคมออนไลน์ประเภทเฟซบุ๊ค รู้จักเฟซบุ๊คจากเพื่อนแนะนำ และมีจำนวนเพื่อนในเฟซบุ๊ค 501 คนขึ้นไป ใช้เฟซบุ๊ค 3-4 ปี มีจำนวนบัญชีเฟซบุ๊ค 1 บัญชี และส่วนใหญ่ใช้งานอินเทอร์เน็ตจากหอพักโดยเชื่อมต่อเฟซบุ๊คผ่านโน้ตบุ๊ค เน็ตบุ๊ค และไอแพด ใช้งานเฟซบุ๊คทุกวัน เฉลี่ย 1-3 ครั้ง/วัน แต่ละครั้งใช้เวลามากกว่า 4 ชั่วโมง ช่วงเวลาที่ใช้เฟซบุ๊ค ในวันจันทร์-ศุกร์

เวลา 19:01 – 24:00 น. และวันเสาร์-อาทิตย์ และวันหยุดนักขัตฤกษ์ เวลา 13.01 – 19:00 น. วัตถุประสงค์หลักที่ใช้เฟซบุ๊คใช้เพื่อผ่อนคลาย และติดต่อสื่อสาร

ผลกระทบจากการใช้สื่อสังคมออนไลน์ประเภทเฟซบุ๊คต่อนักศึกษาเรียงตามลำดับคือ ด้านสุขภาพ ด้านการดำเนินชีวิตประจำวันและด้านการศึกษาตามลำดับ โดยผลกระทบด้านสุขภาพพบว่า มีอาการปวดตา ปวดศรีษะ เมื่อยมือ ปวดไหล่ เวลาเล่นนาน ๆ ผลกระทบด้านการดำเนินชีวิตประจำวัน พบว่านักศึกษาเลือกใช้งานเฟซบุ๊คมากกว่าทำกิจกรรมอื่นในช่วงเวลาว่าง ทำให้ทำกิจกรรมอื่นน้อยลง มีโลกส่วนตัวสูง คุยกับคนในครอบครัวน้อยลง คนรอบข้างรู้สึกหงุดหงิด หวาดระแวง และเกิดการทะเลาะกัน เนื่องจากความคิดเห็นไม่ตรงกัน และผลกระทบด้านการศึกษา พบว่านักศึกษาทำการบ้านและงานที่รับมอบหมายต่างๆ เสร็จช้า เนื่องจากใช้เวลาส่วนใหญ่อยู่กับการใช้งานเฟซบุ๊ค ผลกระทบที่ตามมาพบว่านักศึกษาไม่ส่งงาน ส่งงานช้า ขาดสมาธิในการเรียน เกรดตกในบางรายวิชา ขาดสมาธิในการทำงานและการอ่านหนังสือสอบ ขาดเรียน ใช้ภาษาไม่ถูกต้องใช้คำแสลงในยุคสมัยใหม่ และสะกดคำไม่ถูกต้องตามหลักภาษา

พิชญาณี ภู่ตระกูล (2561:2) ได้ทำรายงานวิจัยเรื่อง “การเปิดเผยตนเองในเครือข่ายสังคมออนไลน์: แนวทางการศึกษา ปัจจัยที่มีอิทธิพล และผลกระทบ” การวิจัยพบว่า การเปิดเผยตนเองไม่ได้ส่งผลกระทบ ด้านลบต่อผู้ใช้เพียงด้านเดียว แต่ยังสร้างผลกระทบด้านบวกได้เช่นเดียวกัน กล่าวคือ การเปิดเผยตนเอง มีความสัมพันธ์กับการได้รับทุนทางสังคม (Social Capital) ที่ส่งเสริมให้บุคคลมีเครือข่ายทางสังคม (Social Network) โดยเครือข่ายสังคมออนไลน์เป็นพื้นที่ให้บุคคลสามารถสร้างทุนทางสังคมด้วยการเชื่อมโยง กระชับ และ รักษาความสัมพันธ์กับผู้ใช้คนอื่นในเครือข่ายสังคมออนไลน์ รวมทั้ง การเปิดเผยตนเองยังทำให้บุคคลได้รับการสนับสนุนทางสังคม (Social Support) คือ ได้รับความช่วยเหลือด้านข้อมูล คำแนะนำ สิ่งของต่างๆ จากผู้ใช้คนอื่น ในเครือข่ายสังคมออนไลน์ และการได้รับการสนับสนุนทางด้านอารมณ์ทำให้ได้รับรู้ถึงความรักใคร่ผูกพัน รู้สึกว่า มีคนรักและสนใจ และการเป็นส่วนหนึ่งของสังคม นอกจากนี้ผลจากการวิจัยยังสามารถยืนยันได้ว่า การได้รับทุน ทางสังคม และการได้รับการสนับสนุนทางสังคมในเครือข่ายสังคมออนไลน์ส่งผลให้ผู้ใช้มีคุณภาพชีวิตและมีสุขภาวะ ทางจิตที่ดีขึ้น (Ellison et al., 2007; กฤษณพร ประสิทธิ์วิเศษ, 2557; Leung & Lee, 2005)

โพสต์ทูเดย์ (2560: B1) หนังสือพิมพ์โพสต์ทูเดย์ Section ธุรกิจการตลาด ได้รายงานเกี่ยวกับ“แนวโน้มภัยไซเบอร์ปี 61” โมเดลธุรกิจหลักของอาชญากรไซเบอร์ พบว่า ในปี 2556 ซอฟต์แวร์เรียกค่าไถ่ CryptoLocker เข้ารหัสไฟล์เลือกระบบและเรียกร้องเงิน 300 ดอลลาร์, ปี 2557 ซอฟต์แวร์เรียกค่าไถ่ BitCrypt เข้ารหัสไฟล์และเรียกร้องเงินเป็นบิดคอยน์, ปี 2558 ซอฟต์แวร์เรียกค่าไถ่เติบโตขึ้น และยังเข้ารหัสเรียกร้องเงิน, ปี 2559 จำนวนซอฟต์แวร์เรียกค่าไถ่ตระกูลใหม่เพิ่มขึ้น 752% เริ่มมีการใช้ซอฟต์แวรีเรียกค่าไถ่ในฐานะบริการ (Ransomware-as-s-Service-RaaS), ปี 2560 การแพร่ระบาดของซอฟต์แวร์เรียกค่าไถ่ที่ไม่เคยเกิดขึ้นมาก่อนผ่านทาง WannaCry และ Petya, ปี 2561 ซอฟต์แวรีเรียกค่าไถ่ และการกรรโชกทางดิจิทัลจะกลายเป็นแหล่งหาเงินของอาชญากรคอมพิวเตอร์ (ที่มา: บริษัท เทรนด์ ไมโคร, 2560)

2.2.1 **การจัดการเทคโนโลยีสารสนเทศ (Managing Information Technology)** แรงกดดันในการทำธุรกิจในปัจจุบัน คือเรื่องของเทคโนโลยีสารสนเทศ เนื่องจากลูกค้าและร้านค้าต่างๆ ล้วนต้องเทคโนโลยีสารสนเทศเข้ามาช่วยในการทำงาน ดังนั้น นับจากนี้ไป เทคโนโลยีสารสนเทศ จะกลายมาเป็นองค์ประกอบหลักสำคัญในการทำธุรกิจ ซึ่งต้องมีการปรับเปลี่ยนการบริหารจัดการใหม่

เพื่อให้ทันกับสถานการณ์ ไม่ว่าจะเป็นอินเตอร์เน็ต อินทราเน็ต เอ็กทราเน็ต หรือเครือข่ายผู้รับ/ผู้ให้บริการ(Client/Server networks) ดังนั้น เทคโนโลยีสารสนเทศเป็นตัวทำให้เกิดการเปลี่ยนแปลงในการพัฒนาการโฆษณาสินค้า การบริหารตัดสินใจ ปรับเปลี่ยนโครงสร้างขององค์กร และมาช่วยเรื่องกิจกรรมการทำงานในองค์กรที่มีอยู่ทั่วโลก

บิล เกต (Bill Gates) ประธานผู้บริหารของบริษัทไมโครซอฟต์ (Microsoft Corporation) ซึ่งเป็นบริษัทผู้ผลิตซอฟต์แวร์รายใหญ่ของโลก บริษัทของเขามีการบริหารในลักษณะกลุ่มบุคคลผู้มีประสบการณ์ บริษัทของเขาได้รับผลกระทบอย่างมากจากการที่ปัจจุบันมีหลายบริษัทหันมาใช้เทคโนโลยีสารสนเทศไม่ว่าจะเป็นการทำธุรกิจอิเล็กทรอนิกส์ (e-Business) และการทำพาณิชย์อิเล็กทรอนิกส์ (E-Commerce) มีการใช้กลยุทธ์การส่งแฟ้มข้อมูลถึงกันด้วยระบบอิเล็กทรอนิกส์ทั้งหมด ทำให้องค์กรของเขาต้องปรับเปลี่ยนกลยุทธ์มากมาย แม้กระทั่งการลดจำนวนพนักงานให้มีจำนวนน้อยลง เป็นต้น

การจัดการด้านเทคโนโลยีสารสนเทศจะช่วยสนับสนุนกระบวนการทำงานของบริษัทและองค์กร เพราะฉะนั้น จึงเป็นความท้าทายอย่างมากสำหรับผู้บริหาร และผู้ทำธุรกิจมืออาชีพในปัจจุบัน สำหรับแนวทางในการจัดการเทคโนโลยีสารสนเทศนั้นมีหลักการใหญ่ 3 ประการ คือ การจัดการร่วมกันพัฒนาและการพัฒนาธุรกิจ/กลยุทธ์เทคโนโลยีสารสนเทศ (Managing the joint implementation of business/IT strategies) ในขั้นตอนนี้ หัวหน้าผู้สำนักงานฝ่ายบริหาร (Chief Executive Officer : CEO) และหัวหน้าสำนักงานสารสนเทศ (Chief Information Officer : CIO) จะเป็นผู้ร้องขอเสนอให้มีการพัฒนาทางธุรกิจ เพื่อให้ผู้บริหารและผู้ที่เป็นมืออาชีพทางธุรกิจใช้เทคโนโลยีสารสนเทศสนับสนุนกลยุทธ์ทางธุรกิจของบริษัทก่อนเป็นอันดับแรก นอกจากนั้นจะมีการปรับนำเอากระบวนการวางแผนทางเทคโนโลยีสารสนเทศทางธุรกิจ มาประยุกต์ใช้งานร่วมกับกลยุทธ์เป้าหมายทางธุรกิจ สำหรับกระบวนการนั้นมีการรวมไปถึงการประเมินผลลักษณะของธุรกิจที่เหมาะสมที่จะลงทุนพัฒนา และมีการพัฒนาข้อเสนอของแต่ละธุรกิจ แต่ละโครงการของเทคโนโลยีสารสนเทศขึ้นมาตามโอกาสอันควร

การจัดการพัฒนาและการพัฒนาประยุกต์ใช้ธุรกิจ/เทคโนโลยีสารสนเทศใหม่ และเทคโนโลยี (Managing the development and implementation of new business/IT applications and technology) ในขั้นตอนนี้เป็นความรับผิดชอบพื้นฐานเบื้องต้นของหัวหน้าสำนักงานสารสนเทศและหัวหน้าสำนักงานเทคโนโลยี (Chief Technology Officer : CTO) การจัดการเทคโนโลยีสารสนเทศในพื้นที่นี้ เกี่ยวข้องกับการจัดการกระบวนการการพัฒนาระบบสารสนเทศ และแนวทางการพัฒนาทางด้านธุรกิจ และมีความรับผิดชอบในการทำวิจัยการใช้กลยุทธ์ทางธุรกิจสำหรับระบบเทคโนโลยีสารสนเทศใหม่ๆ

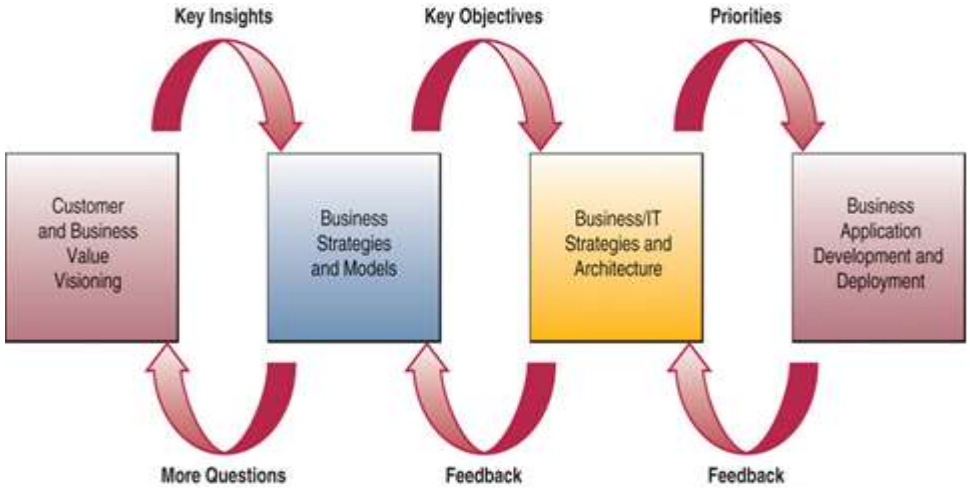
ภาพประกอบ 2.1 องค์ประกอบในการจัดการเทคโนโลยีสารสนเทศ (James A.O'Brien : 2008 : 541)

การจัดการเทคโนโลยีสารสนเทศในองค์กรและโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ (Managing the IT organization and the IT infrastructure) หัวหน้าสำนักงานสารสนเทศ และผู้บริหารด้านเทคโนโลยีสารสนเทศต้องแบ่งปันความรับผิดชอบสำหรับจัดการเทคโนโลยีสารสนเทศให้เหมาะสมกับผู้เป็นมืออาชีพทางธุรกิจ ซึ่งเป็นผู้ที่รวบรวมกลุ่มคนทำงานโครงการต่างๆ และโครงการในหน่วยย่อยขององค์กร นั่นก็คือหัวหน้าสำนักงานสารสนเทศ และผู้บริหารด้านเทคโนโลยีสารสนเทศต้องรับผิดชอบเกี่ยวกับการจัดการโครงสร้างพื้นฐานด้านฮาร์ดแวร์, ซอฟต์แวร์, ฐานข้อมูล, เครือข่ายการสื่อสารโทรคมนาคม, และทรัพยากรเทคโนโลยีสารสนเทศ ซึ่งต้องมีการจัดหา, ปฏิบัติการ, ติดตาม และดูแลรักษาด้วย

2.2.2 การวางแผนธุรกิจและเทคโนโลยีสารสนเทศ (Business/IT Planning) กระบวนการวางแผนธุรกิจและเทคโนโลยีสารสนเทศนี้ มีเป้าหมายเน้นไปที่การเพิ่มมูลค่าให้กับธุรกิจและลูกค้า กระบวนการวางแผนนี้จะนำไปสู่การพัฒนากลยุทธ์ และตัวแบบการประยุกต์ใช้ธุรกิจแนวใหม่, กระบวนการ, ผลิตภัณฑ์ และการบริการ ดังนั้น องค์กรต้องมีการพัฒนากลยุทธ์เทคโนโลยีสารสนเทศ และสถาปัตยกรรมเทคโนโลยีสารสนเทศ เพื่อสนับสนุนการสร้างและการพัฒนาการวางแผนการประยุกต์ใช้ในธุรกิจใหม่ของพวกเขา

เพราะฉะนั้น หัวหน้าสำนักงานผู้บริหาร และหัวหน้าสำนักงานสารสนเทศของบริษัทต้องจัดการพัฒนาองค์ประกอบที่สมบูรณ์ทางธุรกิจและกลยุทธ์เทคโนโลยีสารสนเทศร่วมกันเพื่อเป็นวิสัยทัศน์สร้างมูลค่าเพิ่มให้กับธุรกิจและลูกค้า เนื่องจากเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงไปรวดเร็วมาก และองค์ประกอบที่สำคัญและกลยุทธ์ทางธุรกิจที่จำเป็นต้องทำก่อนเป็นอันดับแรกคือกระบวนการวางแผนธุรกิจและเทคโนโลยีสารสนเทศ ซึ่งมีอยู่ 3 ประการหลัก คือ
การพัฒนากลยุทธ์ (Strategy Development) การพัฒนากลยุทธ์ทางธุรกิจนั้น จะช่วยสนับสนุนวิสัยทัศน์ทางธุรกิจขององค์กร ตัวอย่างเช่น การใช้เทคโนโลยีสารสนเทศสร้างระบบธุรกิจอิเล็กทรอนิกส์ขึ้นมา โดยเน้นไปที่การสร้างมูลค่าเพิ่มให้กับธุรกิจ และลูกค้า
การจัดการทรัพยากร (Resource Management) กลยุทธ์การวางแผนพัฒนาสำหรับใช้จัดการเรื่องการทำงาน และจัดการเทคโนโลยีสารสนเทศในองค์กรนั้น รวมไปถึงการจัดการระบบสารสนเทศส่วนบุคคล, ฮาร์ดแวร์, ซอฟต์แวร์, ข้อมูล และทรัพยากรของเครือข่ายคอมพิวเตอร์

สถาปัตยกรรมเทคโนโลยี (Technology Architecture) ได้แก่การสร้างตัวเลือกของกลยุทธ์ว่ารูปแบบของสถาปัตยกรรมเทคโนโลยีแบบไหน มีความเหมาะสมที่จะนำมาช่วยสนับสนุนธุรกิจ และด้านเทคโนโลยีสารสนเทศขององค์กร



ภาพประกอบ 2.2 กระบวนการวางแผนธุรกิจและเทคโนโลยีสารสนเทศ (James A.O'Brien : 2006 : 479)

สถาปัตยกรรมของเทคโนโลยีสารสนเทศ (Information Technology Architecture)

สถาปัตยกรรมของเทคโนโลยีสารสนเทศนี้ ก็ถูกสร้างขึ้นมาโดยกระบวนการวางแผนกลยุทธ์ทางธุรกิจและเทคโนโลยีสารสนเทศ ซึ่งได้แก่ แนวความคิดในการออกแบบ หรือการจัดทำพิมพ์เขียว และรวมทั้งองค์ประกอบหลักต่อไปนี้ คือ รูปแบบแนวราบพื้นฐานของเทคโนโลยี (Technology Platform) ซึ่งได้แก่ อินเทอร์เน็ต, อินทราเน็ต เอ็กทราเน็ตและเครือข่ายประเภทอื่น, ระบบคอมพิวเตอร์, ซอฟต์แวร์ระบบ, ซอฟต์แวร์แบบรวมประยุกต์ใช้งานภายในองค์กรเพื่อจัดการด้านการทำงานของคอมพิวเตอร์ และเพื่อเป็นโครงสร้างทางการสื่อสาร หรือเรียกอีกอย่างหนึ่งว่ารูปแบบแนวราบพื้นฐาน (Platform) ส่วนระบบการสนับสนุนนั้น รวมไปถึงกลยุทธ์การใช้เทคโนโลยีสารสนเทศสำหรับธุรกิจอิเล็กทรอนิกส์, พาณิชย์อิเล็กทรอนิกส์, หรือการประยุกต์ใช้เทคโนโลยีสารสนเทศในธุรกิจอื่นๆ ทรัพยากรข้อมูล (Data Resources) มีฐานข้อมูลชนิดพิเศษและฐานข้อมูลเพื่อปฏิบัติการหลายประเภท รวมทั้งข้อมูลโกดังสินค้า, ฐานข้อมูลบนอินทราเน็ต อินเตอร์เน็ต ที่ถูกจัดเก็บเอาไว้เพื่อนำมาช่วยสนับสนุนการตัดสินใจในธุรกิจ

สถาปัตยกรรมการประยุกต์ใช้ (Application Architecture) การประยุกต์เทคโนโลยีสารสนเทศในธุรกิจนั้น ได้ถูกออกแบบมาอย่างรวม หรือ ระบบการประยุกต์ใช้กระเป๋าเอกสารในองค์กร (Portfolio) ซึ่งมีส่วนช่วยสนับสนุนธุรกิจ เช่นเดียวกับกระบวนการของระบบการใช้งานไขว้หรือสลับข้ามหน้าที่กัน (Cross-Functional) ในธุรกิจ ตัวอย่างเช่น สถาปัตยกรรมการประยุกต์ใช้อาจจะช่วยสนับสนุนการพัฒนาและดูแลเกี่ยวกับการประยุกต์ใช้ห่วงโซ่อุปทาน, การวางแผนทรัพยากรในองค์กร และการจัดการความสัมพันธ์ระหว่างลูกค้า

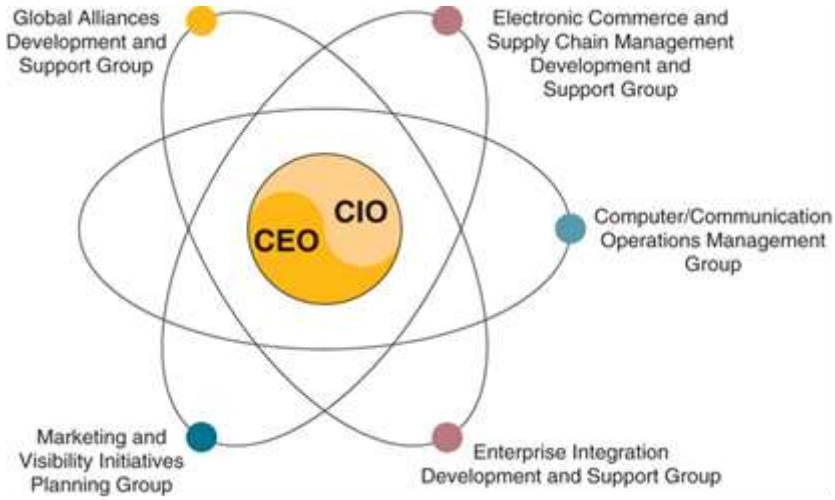
เทคโนโลยีสารสนเทศในองค์กร (IT Organization) โครงสร้างหน้าที่ของระบบสารสนเทศในองค์กรนั้น และการเผยแพร่สารสนเทศนั้น ได้ถูกออกแบบมารวมกับกลยุทธ์การเปลี่ยนแปลงธุรกิจ ซึ่งรูปแบบของเทคโนโลยีสารสนเทศในองค์กรจะขึ้นอยู่กับปรัชญาในการบริหารจัดการและกลยุทธ์

ธุรกิจ/เทคโนโลยีสารสนเทศ ซึ่งได้ถูกจัดเป็นสูตรสำเร็จ ในระหว่างที่มีการจัดทำเรื่องกระบวนการกลยุทธ์การวางแผน

2.2.3 หน้าที่การจัดการของระบบสารสนเทศ (Managing the IS Function) ตั้งแต่ปี ค.ศ.1980 และมาถึง ปี 1990 แผนกและองค์กรต่างๆ หันมาใช้คอมพิวเตอร์ส่วนบุคคลและซอฟต์แวร์, ระบบเครือข่ายผู้รับ/ผู้ให้บริการ (Client/Server Networks) และหลังจากนั้นมาอีก 2-3 ปี เมื่ออินเตอร์เน็ตได้รับความนิยมมาก ก็ทำให้องค์กรต่างๆ มีการเชื่อมต่ออินเตอร์เน็ต และอินทราเน็ตกันมากมาย โดยไม่ได้ใส่หน้าที่ทางธุรกิจของพวกเขาลงไป ดังนั้น จึงมีการดูแลเอาใจใส่เครื่องคอมพิวเตอร์ส่วนบุคคลบนเครือข่ายคอมพิวเตอร์กันมากขึ้น และจนกระทั่งมีความต้องการจะเปลี่ยนมาเป็นการประมวลผลแบบรวมศูนย์ (Centralization)

การรวบรวมเทคโนโลยีสารสนเทศ (Organizing IT) การบริหารของระบบธุรกิจเท่าที่ผ่านมามีการใช้เทคโนโลยีสารสนเทศการประมวลผลแบบรวมศูนย์และการประมวลผลแบบกระจายศูนย์เพื่อมาช่วยจัดการรวบรวมการทำงานของเทคโนโลยีสารสนเทศให้เหมาะสมกับงานในแต่ละรูปแบบ ซึ่งระบบทั้ง 2 อย่างนี้ สามารถสนับสนุนด้านระบบสารสนเทศ, การดำเนินการ และการตัดสินใจ ซึ่งมีการใช้คอมพิวเตอร์ภายในองค์กรนั่นเอง ตัวอย่างเช่น ระบบการประมวลผลแบบรวมศูนย์ (Centralization) จะอำนวยความสะดวกในเรื่องของการเชื่อมต่อส่วนหรือแผนกทั้งหมดขององค์กรโดยเครือข่ายการสื่อสารโทรคมนาคม ซึ่งสามารถที่จะอนุญาตให้ผู้บริหารระดับสูงเป็นผู้สิทธิ์ในการตัดสินใจเป็นหลัก หรือรวบอำนาจในการตัดสินใจนั่นเอง ส่วนเครื่องคอมพิวเตอร์อาจใช้เมนเฟรมคอมพิวเตอร์เป็นหลัก นั่นหมายถึงการประมวลผลทั้งหมดต้องขึ้นอยู่กับเครื่องคอมพิวเตอร์ศูนย์กลาย เช่น ธนาคารสำนักงานใหญ่ ระบบรวมศูนย์จะช่วยจัดการทรัพยากรเทคโนโลยีสารสนเทศในองค์กร ซึ่งเป็นกลยุทธ์บริการให้กับธุรกิจย่อย, ธุรกิจอิเล็กทรอนิกส์ และพาณิชย์อิเล็กทรอนิกส์ ส่วนแนวโน้มต่อไปก็จะมีการใช้มินิคอมพิวเตอร์และไมโครคอมพิวเตอร์เชื่อมโยงกัน ทำให้การติดต่อสื่อสารรวดเร็วและขนาดขององค์กรเล็กลง (Downsizing)

ส่วนการประมวลผลแบบกระจายศูนย์ (Decentralization) การดำเนินการ หรือการปฏิบัติการจะมีการกระจายอำนาจในการประมวลผลไปยังเครื่องคอมพิวเตอร์สาขา (Branch Office) หมายถึงเครื่องศูนย์กลางจะเป็นเมนเฟรมคอมพิวเตอร์ และมีการเชื่อมโยงไปยังสาขาด้วยเครื่องมินิคอมพิวเตอร์ ซึ่งสามารถประมวลผลได้ด้วยตัวเองเป็นอิสระ เช่น สาขาของธนาคาร ในปัจจุบันมีการพัฒนาระบบรวมศูนย์ และกระจายศูนย์เข้าด้วยกันเพื่อจัดการเกี่ยวกับการทำธุรกิจเป็นกลุ่ม หรือกลุ่มย่อย บางบริษัทก็มีการจ้างให้บริษัทภายนอกมารับจัดทำให้ (Outsource) ทำหน้าที่จัดการให้ทุกอย่างตั้งแต่การพัฒนาซอฟต์แวร์จนถึงการบำรุงรักษา



ภาพประกอบ 2.3 องค์ประกอบขององค์กรเทคโนโลยีสารสนเทศ (James A.O'Brien : 2008 : 542)

การพัฒนาจัดการประยุกต์ใช้ (Managing Application Development) เกี่ยวข้องกับการจัดทำกิจกรรมต่างๆ เช่น การวิเคราะห์ และออกแบบระบบ, การจัดทำต้นแบบ, การประยุกต์ใช้การเขียนโปรแกรม, การจัดการโครงการ, การรับประกันคุณภาพงาน, และการดูแลรักษาระบบเพื่อพัฒนางานตามโครงการของเทคโนโลยีสารสนเทศ และทางธุรกิจ ในส่วนการพัฒนาการจัดการประยุกต์ใช้นี้ สิ่งที่ต้องการในกิจกรรมการทำงาน คือ กลุ่มของนักวิเคราะห์ระบบ, กลุ่มคนผู้พัฒนาซอฟต์แวร์, หรือกลุ่มคนผู้เป็นมืออาชีพทางระบบสารสนเทศ เพื่อมาช่วยกันทำงานพัฒนาโครงการในด้านธุรกิจ ดังนั้นการจัดการโครงการจึงเป็นเรื่องหลักเพื่อรับผิดชอบการจัดการทางด้านเทคโนโลยีสารสนเทศตามงบประมาณในองค์กร และในส่วนของกลุ่มผู้ออกแบบต้องมีการประชุมร่วมกัน นอกจากนี้ ยังต้องมีศูนย์กลางการพัฒนา (Development Centers) เพื่อเป็นศูนย์รวมของกลุ่มนักพัฒนาซอฟต์แวร์

การจัดการระบบสารสนเทศเพื่อการปฏิบัติการ (Managing IS Operations) เกี่ยวข้องกับการใช้ฮาร์ดแวร์, ซอฟต์แวร์, เครือข่ายคอมพิวเตอร์, ทรัพยากรส่วนบุคคลในองค์กร หรือในหน่วยของศูนย์ข้อมูลธุรกิจ หรือศูนย์คอมพิวเตอร์ (Data Centers or Computer Centers) ขององค์กร ในส่วนของกิจกรรมการปฏิบัติการนั้น ต้องมีการจัดการเรื่องระบบปฏิบัติการของเครื่องคอมพิวเตอร์, การจัดการเครือข่ายคอมพิวเตอร์, การควบคุมการผลิต, และการสนับสนุนการผลิต ระบบการจัดการสารสนเทศเพื่อการปฏิบัติการนี้ ส่วนใหญ่ใช้ชุดของซอฟท์แวร์สำหรับจัดการด้านการทำงานของระบบคอมพิวเตอร์ มีระบบติดตามการทำงาน (System performance monitors) เพื่อช่วยติดตามการประมวลผลทำงานของคอมพิวเตอร์

การจัดการทรัพยากรมนุษย์ด้วยเทคโนโลยีสารสนเทศ (Human Resource Management of IT) ซึ่งได้แก่ การรับสมัครงาน, การฝึกอบรม, การฝึกอบรมพนักงานใหม่ เพื่อให้ได้คุณภาพสูงสุด. และเกี่ยวข้องกับการจัดการสารสนเทศ ได้แก่ การบริหารจัดการในองค์กร, การจัดการด้านเทคนิคและด้านบุคคล และที่สำคัญมากที่สุด คือ การรับสมัครคนเข้ามาทำงาน รวมไปถึงกระบวนการพัฒนา, การจัดรวบรวมขีดความสามารถของบุคคลที่มีอยู่เพื่อจัดเก็บเอาไว้ในฐานข้อมูลขององค์กร

หัวหน้าสำนักงานสารสนเทศและผู้บริหารเทคโนโลยีสารสนเทศ (The CIO and Other

ITExecutives)หัวหน้าสำนักงานสารสนเทศที่ทำงานอยู่ทั่วโลกจะมีการใช้เทคโนโลยีสารสนเทศในบริษัท และมีการนำพวกเขาให้เข้าร่วมสู้เป้าหมายทางธุรกิจ ดังนั้น ธรรมเนียมของการบริการด้วยระบบคอมพิวเตอร์, การบริการด้วยเทคโนโลยีอินเตอร์เน็ต, การบริการด้วยการสื่อสารโทรคมนาคม และการบริการด้วยการสนับสนุนด้วยเทคโนโลยีต่างๆ เป็นความรับผิดชอบของผู้บริหาร ดังนั้น หัวหน้าสำนักงานสารสนเทศไม่ได้ทำงานบริการสารสนเทศวันต่อวันอย่างเดียว แต่ยังทำหน้าที่ในการวางแผนกลยุทธ์ในธุรกิจ และกลยุทธ์ด้านเทคโนโลยีสารสนเทศด้วย สำหรับ CIO ยังทำงานร่วมกับ CEO และผู้บริหารระดับสูงในธุรกิจ เพื่อพัฒนากลยุทธ์การใช้สารสนเทศในระบบธุรกิจอิเล็กทรอนิกส์ ทั้งนี้เพื่อให้บริษัทสามารถแข่งในตลาดโลกได้

การจัดการเทคโนโลยี (Technology Management) ปรัชญาของการจัดการทรัพยากรสารสนเทศนั้น รวมไปถึงกระบวนการของเทคโนโลยีทั้งหมดไม่ว่าจะเป็นการจัดเก็บ การขนส่งข้อมูล และการจัดการสารสนเทศในองค์กร ในส่วนของเทคโนโลยีนั้นรวมทั้งอินเตอร์เน็ต อินทราเน็ต พาณิชย์อิเล็กทรอนิกส์ และระบบการทำงานร่วมกันซึ่งก็คือกระบวนการประมวลผลสารสนเทศนั่นเอง การจัดการทรัพยากรสารสนเทศนั้น เป็นความรับผิดชอบของหัวหน้าสำนักงานสารสนเทศ (Chief Information Officer : CIO) สำหรับในส่วนของการจัดการนั้นยังมีอีกหลายส่วน ดังจะกล่าวต่อไป คือ (1) การจัดการเครือข่ายคอมพิวเตอร์ (Network Management) ระบบที่องค์กรต่างๆ ใช้กันอยู่ในปัจจุบัน ไม่ว่าจะเป็น อินเตอร์เน็ต อินทราเน็ต เอ็กทราเน็ต และเครือข่ายผู้รับ/ผู้ให้บริการ ล้วนแล้วแต่เป็นการจัดการโดยการจัดการเครือข่ายคอมพิวเตอร์ (Network Management) ทั้งนั้น การจัดการเครือข่ายคอมพิวเตอร์นี้ จำเป็นต้องมีทรัพยากรฮาร์ดแวร์ ซอฟท์แวร์ ส่วนผู้บริหารเครือข่ายนั้น รับผิดชอบในการประเมินผล และการบริการด้านอินเตอร์ อินทราเน็ต เว็บบราวเซอร์ ตลอดจนการติดต่อเชื่อมโยงสื่อสารเกี่ยวกับฮาร์ดแวร์ ซอฟท์แวร์ ถ้าเป็นผู้บริหารเกี่ยวกับธุรกิจ จะทำหน้าที่ในการปรับปรุงการออกแบบ คุณภาพของการดำเนินการ การบริการ และดูแลระบบความปลอดภัยของเครือข่ายการสื่อสารโทรคมนาคมขององค์กร และ (2) ความก้าวหน้าในการจัดการเทคโนโลยี (Advanced Technology Management : ATGs) เป็นการจัดการโดยการใช้อินเตอร์เน็ต อินทราเน็ต เอ็กทราเน็ต และเครือข่ายผู้รับ/ผู้ให้บริการ บางบริษัทมีการสร้างกลุ่มย่อยขึ้นมา เพื่อกำหนด, แนะนำ และติดตามการนำเอาเทคโนโลยีสารสนเทศใหม่ๆ มาใช้ในองค์กร โดยเฉพาะระบบที่สามารถที่จะชำระเงินได้เร็วและได้หมด กลุ่มย่อยที่ว่านี้ อาจเรียกว่า การจัดการเทคโนโลยี (Technology Management), หน่วยประสานงานด้านเทคโนโลยี (Emerging Technology), หรือกลุ่มความก้าวหน้าทางเทคโนโลยี (Advance Technology Group) หน้าที่ของบุคคลกลุ่มนี้ ยังมีหน้าที่รายงานผลการทำงานต่อหัวหน้าสำนักงานสารสนเทศอีกทีหนึ่งด้วย

การจัดการด้านบริการให้กับผู้ใช้งาน (Managing User Service) ผู้รับผิดชอบในฝ่ายนี้ ต้องทำหน้าที่ในการจัดการทรัพยากรและการบริการสารสนเทศให้กับผู้ใช้อย่างมีประสิทธิภาพภายในธุรกิจ อาจจะใช้เครื่องคอมพิวเตอร์ส่วนบุคคลสถานีงาน (PC Workstations) หรือหน่วยงานของตนเอง ซึ่งอาจจะมีการทำงานเป็นกลุ่ม นอกจากนี้ ยังรวมไปถึง การพัฒนาโครงการใหม่ๆ ขึ้นมา, การจัดการด้านฮาร์ดแวร์ ซอฟท์แวร์ ทรัพยากรข้อมูล หน่วยงานของตนเอง และระบบหนึ่งซึ่งเป็นที่นิยมมากสำหรับการจัดการบริการให้กับผู้ใช้งาน คือระบบผู้รับ/ผู้ให้บริการ (Client/Server Systems) หรือศูนย์บริการสารสนเทศ (Information Center)

2.2.4 ความล้มเหลวในการจัดการเทคโนโลยีสารสนเทศ (Failures in IT Management)

มีบางองค์กรนำเอาระบบสารสนเทศไปใช้แล้วประสบผลผลสำเร็จมีให้เห็นอยู่มากมาย เช่น ธนาคาร มหาวิทยาลัย เป็นต้น แต่ที่ไม่ประสบผลสำเร็จตามเป้าหมายก็มีบ้างเหมือนกัน เนื่องจากอาจมีข้อผิดพลาดเกิดขึ้นเป็นเพราะสารสนเทศที่ยังมีข้อผิพลาด, เพราะเทคโนโลยีเกิดการติดขัด เช่น เครื่องคอมพิวเตอร์เสีย หรือระบบออนไลน์มีปัญหา เป็นต้น ทำให้การทำงานหยุดชะงัก ดังนั้น ความล้มเหลวของการนำเอาเทคโนโลยีสารนเทศไปใช้ก่อให้เกิดผลเสีย 3 ด้าน คือ

ด้านประสิทธิภาพ (Effectively)

ด้านประสิทธิผล (Efficiently)

เศรษฐกิจ (Economically)

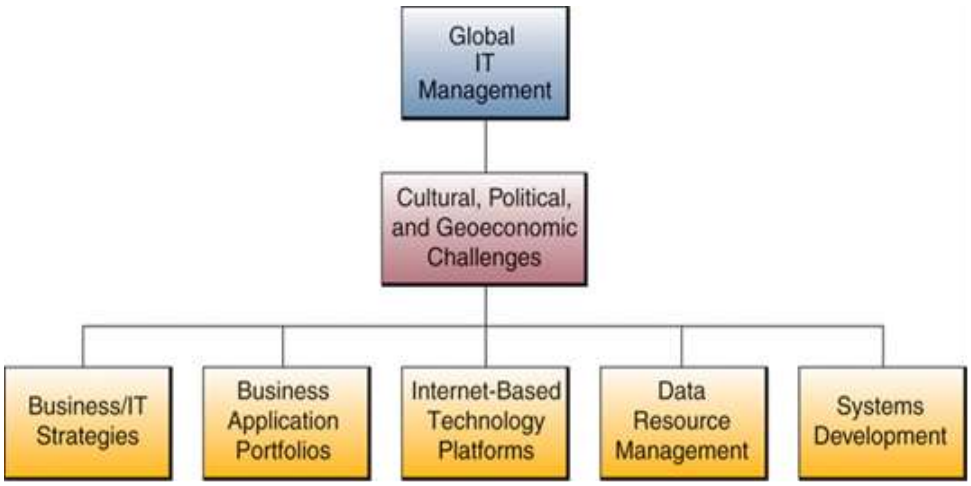
ตัวอย่างเช่น Empire Blue Cross/Blue Shield เป็นบริษัท ประกันสุขภาพ เคยเกิดปัญหาคอมพิวเตอร์ทำงานติดขัด เนื่องจากเครื่องคอมพิวเตอร์เก่าล้าสมัย ใช้งานมาแล้วกว่า 25 ปี เป็นต้น การเกี่ยวข้องกับการจัดการและการปกครอง (Management Involvement and Governance) ผู้บริหารบางคนในหน่วยงานการปกครองไม่ชำนาญการใช้ IT ทำให้ผลงานออกมาล่าช้า ดังนั้น ผู้บริหารต้องมีความสัมพันธ์กัน คือ ต้องรู้การจัดการที่ดีและต้องมีความรู้เรื่อง IT ของในหน่วยงานปกครองของตนเอง ในส่วนของการจัดการเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการปกครองนั้น มีรายละเอียดดังนี้

ผู้บริหารในฐานะเป็นกรรมการเทคโนโลยีสารสนเทศ (Executive IT Committee) ซึ่งในที่นี้ คือ หัวหน้าสำนักงานสารสนเทศ (Chief Information Officer : CIO) ต้องทำหน้าที่ในการวางแผน การประสานงานในการพัฒนาโครงการของการพัฒนาระบบสารสนเทศหลักๆ ขององค์กร คณะกรรมการเทคโนโลยีสารสนเทศ (IT Steering Committee) เป็นคณะกรรมการบริหารงานในระบบธุรกิจ ซึ่งมีหลายตำแหน่ง ไม่ว่าจะเป็นผู้จัดการด้านปฏิบัติการ, ผู้จัดการด้านบุคคล ไปจนถึงผู้จัดการสารสนเทศ ซึ่งมีหน้าที่ในการสร้างโครงการระบบสารสนเทศใหม่ๆ ขึ้นมา นอกจากนั้น ยังทำหน้าที่ในการนำเอางานมาทบทวนทำใหม่ หรือปรับเปลี่ยนตามความเหมาะสม

2.2.5 มิติระหว่างประเทศ (The International Dimension) ในการทำธุรกิจระหว่างประเทศ เป็นการใช้การเชื่อมต่อระหว่างประเทศ (Internetworked) ทำให้ระบบเศรษฐกิจและการตลาดสามารถเชื่อมโยงกันอย่างไร้พรมแดน จะเห็นได้ว่าปัจจุบันหลายประเภทมีการเชื่อมโยงถึงกันหมดทั่วโลกได้แก่เรื่อง เศรษฐกิจ, การตลาด, บัญชี, การเงิน, การผลิต, ทรัพยากรมนุษย์ และระบบสารสนเทศอื่นๆ ถ้าใครก็ตามคิดจะทำธุรกิจขึ้นมาสักอย่างหนึ่งไม่ว่าจะเป็นขนาดเล็กหรือขนาดใหญ่ ย่อมได้รับผลกระทบในเรื่องเหล่านี้หมดถ้าไม่มีการปรับตัว และต้องมีการพัฒนาระบบธุรกิจให้เป็นการเชื่อมโยงถึงกันระหว่างประเทศหมด นั่นคือสามารถที่จะเชื่อมโยงกับคนหรือลูกค้า แหล่งผลิตภัณฑ์ และการบริการจากบ้านหรือบริษัทของตนเอง

2.2.6 การจัดการไอทีไร้พรมแดน (Global IT Management) การจัดการเทคโนโลยีสารสนเทศไร้พรมแดนเกี่ยวข้องกับ วัฒนธรรม, นโยบาย, และความท้าทายเศรษฐกิจภูมิภาค (Geoeconomics Challenges) เนื่องจากเป็นการทำธุรกิจในลักษณะระหว่างประเทศ และยังเกี่ยวพันธ์ย่อยลงมาถึงการพัฒนากลยุทธ์เทคโนโลยีสารสนเทศมาใช้ในธุรกิจ (Business/IT Strategies),

และผู้บริหารต้องนำเอากิจกรรมต่างๆ ขององค์กรมาช่วยในการสนับการวางแผนการทำงานที่เรียกว่า การประยุกต์ใช้กระเป๋าเอกสารหรือแฟ้มสะสมงาน (Application Portfolios), มีการนำเอาฮาร์ดแวร์ ซอฟต์แวร์ เทคโนโลยีเครือข่ายคอมพิวเตอร์มาสนับสนุนด้วยที่เรียกว่า การประยุกต์ใช้เทคโนโลยีแบบแนวราบ (Technology Platforms), ในส่วนของการจัดการข้อมูลนั้น ฐานข้อมูลนับว่ามีส่วนสำคัญในการสนับสนุนการจัดการข้อมูล (Data Management), และสุดท้ายเป็นการพัฒนาระบบ (Systems Development) ขึ้นมา เพื่อพัฒนาโครงการใหม่ๆ ขึ้นมาสนับสนุนและผลิตระบบสารสนเทศเพื่อการกระจายข้อมูลไปอย่างไร้พรมแดน



ภาพประกอบ 2.4 มิติการจัดการเทคโนโลยีสารสนเทศไร้พรมแดน (James A.O'Brien : 2008 : 554)

ความสำคัญของการจัดการไอที (The important of IT management)

แรงกดดันทั่วโลกทำให้เกิดสิ่งใหม่ ๆ ในธุรกิจ เกิดรูปแบบการค้าขายบน Web ที่เรียกว่า E-Commerce มีจัดการองค์ความรู้ (Knowledge Management) นำความรู้จากประสบการณ์ในอดีตกลับมาใช้ใหม่ โดยอาศัย IT (Information Technology) มีเทคนิคในการสกัดข้อมูล (Data Mining) กองโตที่อยู่ในฐานข้อมูล เพื่อให้เห็นถึงข้อมูลที่ซ่อนเร้นอยู่ และเป็นข้อมูลที่เราไม่เคยรู้มาก่อน (Unknow) มีการจัดการความสัมพันธ์กับลูกค้า (Cutomer Relationship Management :CRM) ให้ความสำคัญกับลูกค้ามากกว่าในอดีต เพื่อเป็นการชักจูงลูกค้าและต้องการความจงรักภักดีจากลูกค้า ตลอดจนใช้ระบบวางแผนการใช้ทรัพยากร (Enterprise Resource Planing :ERP) เช่น นำไปใช้กับโรงงานผลิตในการจัดทำระบบจัดซื้อ วางบิล หรือจัดการกับระดับสินค้าคงเหลือที่เหมาะสม

จะเห็นได้ว่าสิ่งที่กล่าวมานี้ ล้วนแล้วแต่เป็นเรื่องที่องค์กรธุรกิจไม่ควรมองข้าม และต้องให้ความสำคัญเป็นอย่างยิ่งต่อการจัดการ IT เพื่อความอยู่รอดของธุรกิจ และเพื่อสร้างระบบสารสนเทศเพื่อนำมาซึ่งความได้เปรียบในการแข่งขัน

ในโลกปัจจุบันที่เต็มไปด้วยระบบข่าวสาร (Information System: IS) จำนวนมหาศาล จึงเป็นสิ่งที่เลี่ยงไม่ได้ที่องค์กรจะต้องนำเทคโนโลยี (Technology) เข้ามาเพื่อช่วยจัดการกับข่าวสาร ซึ่งถ้าเรานำ 2 สิ่งมารวมกัน จะเรียกว่า "เทคโนโลยีข่าวสาร" หรือ "เทคโนโลยีสารสนเทศ (Information Technology:IT)" นั่นเอง ซึ่งความหมายของ IS จะมุ่งเน้นในเรื่องของการบริหาร

จัดการข่าวสารในองค์กร โดยอาจจะใช้เทคโนโลยีมาช่วยหรือไม่ก็ได้ โดย IS จะมีความหมายในเชิงกว้าง ส่วนความหมายของ IT เป็นเรื่องของการนำเทคโนโลยีมาใช้เป็นเครื่องมือในการทำงานร่วมกับข่าวสารในองค์กร ซึ่ง IT จะมีความหมายในเชิงแคบ ในบางครั้ง IS กับ IT สามารถใช้แทนกันได้ ดังนั้นก่อนที่องค์กรจะเริ่มให้ความสำคัญกับการจัดการ IT ผู้บริหารขององค์กรจะต้องเข้าใจความหมายของ IT ให้ถ่องแท้เสียก่อน โดยแยกตัว I ออกจาก ตัว T ก็จะพบได้ว่า I ตัวแรกคือข่าวสาร (Information) ส่วน T ตัวหลังคือเทคโนโลยี (Technology) และต้องตระหนักเสมอว่าเราจะนำ T เข้ามาใช้เป็นเครื่องมือเพื่อสนับสนุน (support) I มิได้หมายความว่าจะปรับ I ทั้งหมดขององค์กรให้ขึ้นอยู่กับ T ที่จะนำเข้ามาใช้

หากธุรกิจทุกองค์กรสามารถปรับตัวให้เข้ากับยุคเทคโนโลยีข่าวสารได้ องค์กรนั้นก็จะสามารถอยู่รอดในธุรกิจ ซึ่งถ้าเรามองย้อนไปในอดีตในธุรกิจประเภทสื่อจัดเก็บข้อมูลในคอมพิวเตอร์ เช่น แผ่น Disk ขนาด 5” จุข้อมูลได้น้อย และไม่เหมาะสมกับราคา ในปัจจุบันสื่อชนิดนี้ได้เลิกผลิตไปนานแล้วและหากเราต้องการเปิดอ่านข้อมูลที่เคยเก็บเอาไว้ในแผ่น Disk ขนาด 5” นี้ ก็จะไม่มีสื่อที่จะเปิดอ่านได้ เนื่องจากผู้ผลิตได้เลิกผลิตและได้ปรับตัวไปตามวิวัฒนาการของเทคโนโลยี หรือแม้แต่ปัจจุบันแผ่น Disk ขนาด 3.5” ก็จะถูกแทนที่ด้วย Thumb Drive ม้วนวีดีโอจะถูกแทนที่ด้วยแผ่น VCD และแผ่น VCD จะถูกแทนที่ด้วยแผ่น DVD เป็นต้น

ดังนั้นจึงสรุปได้ว่า ผู้บริหารจำเป็นต้องให้ความสำคัญในการจัดการ IT พยายามมองถึงระบบข่าวสารในอดีตและลำดับเหตุการณ์มาถึงปัจจุบัน เพื่อให้เห็นวิวัฒนาการและการเปลี่ยนแปลง และอย่าลืมว่าจะต้องมองอนาคตด้วย เพราะปัจจุบันในวันนี้จะกลายเป็นอดีตในวันข้างหน้า และอนาคตก็จะกลายมาเป็นปัจจุบัน หากเราจัดการ IT ให้สอดคล้องกับระบบงานปัจจุบันและรองรับการขยายตัวในอนาคตได้ดี ก็จะส่งผลดีต่อองค์กร

อย่างไรก็ดีมีหลายองค์กรที่สามารถเปลี่ยนวิกฤตให้กลายเป็นโอกาส เปลี่ยนเหตุการณ์ร้ายให้กลายเป็นดี เนื่องจากองค์กรเหล่านั้นให้ความสำคัญกับการจัดการ IT ตัวอย่างเช่น ธุรกิจร้านถ่ายรูป มีการปรับเปลี่ยนกระบวนการทำงานโดยการนำ IT เข้ามาใช้ ซึ่งขอเปรียบเทียบให้เห็นความแตกต่างระหว่างธุรกิจในรูปแบบเดิมกับรูปแบบใหม่ดังนี้ (Efraim Turban, Ephraim Mclean and James Wetherbe,2002:6)

ตารางที่ 2.1 เปรียบเทียบธุรกิจรูปแบบเดิมและรูปแบบใหม่

ธุรกิจรูปแบบเดิม (Old Economy)	ธุรกิจรูปแบบใหม่ (New Economy)
-ซื้อฟิล์มที่ร้านและใช้กล้อง Manual เพื่อถ่ายภาพ	-ใช้กล้องถ่ายรูปดิจิตอล และใช้ Flat Memory ซึ่งเก็บภาพได้มากกว่าฟิล์ม
-เมื่อถ่ายภาพยังไม่หมดม้วน อาจต้องรอเป็นสัปดาห์หรือเป็นเดือน จึงจะส่งไปอัดภาพและล้างภาพ	-สามารถส่งล้างได้ทุกเมื่อตามต้องการ ในเวลาเพียงไม่กี่ชั่วโมง
-ไม่สามารถส่งภาพให้กับเพื่อนหรือครอบครัวอย่างทันทีทันใด	- ส่งภาพได้ทันทีในรูปแบบของ File โดยผ่านทาง E-mail หรือเครือข่ายการสื่อสาร
-กล้อง Manual มีฟังก์ชั่นในการทำงานน้อย	-กล้องดิจิตอล ทำงานได้หลากหลายฟังก์ชั่น เช่นถ่ายวีดีโอ

สามารถถ่ายภาพนิ่งได้อย่างเดียว	บันทึกเสียง ถ่ายภาพนิ่งและภาพเคลื่อนไหว นอกจากนี้ยังสามารถใช้ Software ในการตกแต่ง File ภาพ หรือนำ File วีดีโอ ไปสร้างเป็น Movie โดยกำหนด Sine ตามต้องการ
-ไม่สามารถเชื่อมต่อกับอุปกรณ์การสื่อสาร (Communication) ได้	เชื่อมต่อกับอุปกรณ์ Wireless เช่น palm หรือ Cell Phone เพื่อความสามารถในการถ่ายโอน File ได้ในเวลาอันรวดเร็ว

จากตัวอย่างในตารางจะพบว่า ถ้าเจ้าของร้านถ่ายรูปเห็นความสำคัญของผลกระทบที่เกิดจาก IT และยอมรับที่จะนำ IT เข้ามาใช้งาน มีวิธีการจัดการ IT ที่เหมาะสมกับรูปแบบการทำงานของร้าน ก็สามารถเปลี่ยนผลกระทบนั้นให้กลับกลายเป็นเหตุการณ์ที่ดีขึ้น เพราะสังเกตเห็นได้ว่าผู้คนมีการถ่ายภาพมากขึ้นเนื่องจาก Flat Memory ในกล้องดิจิตอลไม่จำกัดจำนวนภาพที่ 36 ภาพเหมือนกล้อง Manual ในอดีต อีกทั้งทางร้านถ่ายรูปยังมีบริการที่รวดเร็วขึ้น โดยการนำ IT เข้ามาสนับสนุนการทำงาน มีบริการตกแต่งภาพตามความต้องการของผู้ใช้บริการ

นอกจากผู้บริหารองค์กรจะนำ IT เข้ามาสนับสนุนการทำงานแล้ว ยังควรมองถึงรูปแบบธุระกิจใหม่ ๆ (Business Models) ซึ่งเป็นรูปแบบทางด้านการค้า ที่สามารถเพิ่มคุณค่าทางธุรกิจให้กับองค์กร โดยทำงานบนพื้นฐาน IT ซึ่งมีหลากหลายรูปแบบ ดังนี้ (Efraim Turban, Ephraim Mclean and James Wetherbe : 2002)

Name-Your-Own-Price : เป็นรูปแบบที่ยอมให้ลูกค้าทราบราคาสินค้าก่อนซื้อสินค้าและบริการหรือให้ลูกค้าบอกราคาที่ต้องการจ่าย เช่น การประกาศซื้อรถ ซึ่งผู้ขายจะเข้ามาตอบกลับ

Dynamic Brokering : เป็นรูปแบบที่ยอมให้ลูกค้าสามารถกำหนดความต้องการด้านผลิตภัณฑ์และบริการได้ โดยลูกค้าจะประกาศบน Web และให้ผู้ที่ต้องการขายมาเสนอราคา

Reverse Auctions : การประมูล เป็นวิธีการที่รวดเร็วโดยผู้ขายกำหนดราคาเริ่มต้นของผลิตภัณฑ์ และให้ผู้ซื้อร่วมเคาะราคาการประมูลผ่านทาง Web คนไหนเสนอราคาเป็นที่พอใจก็ขายให้กับคนนั้น

Affiliate marketing : การเข้าร่วมซื้อขายในตลาด มีการจัดหมวดหมู่ของการค้า มีคู่ค้าทางการตลาดทั้งภาคเอกชน รัฐวิสาหกิจ เป็นการหาพรรคพวกทางการตลาด มี Banner โฆษณาชื่อบริษัท Group Purchasing : เป็นการร่วมกันซื้อเป็นกลุ่ม สามารถซื้อสินค้าได้ในราคาถูก เมื่อซื้อในปริมาณมากจะมีส่วนลดสินค้าE-marketplaces and Exchanges: การตลาดบน Web และการแลกเปลี่ยน จะประกอบได้ด้วยกลุ่มสินค้าที่มีความแตกต่างและหลากหลาย

รูปแบบธุรกิจที่กล่าวมาในข้างต้นนี้ มีพื้นฐานการทำงานโดยอาศัยเทคโนโลยีและการสื่อสารผ่านเครือข่าย เมื่อองค์กรมีการลงทุนด้าน IT แล้ว ก็ควรที่จะใช้ความสามารถของ IT นั้นให้เต็มประสิทธิภาพ โดยพิจาณาถึงรูปแบบธุรกิจ (Business Models) ใหม่ ๆ ว่ามีรูปแบบใดที่องค์กรสามารถนำมาปรับใช้ประโยชน์ เพื่อเพิ่มคุณค่าในทางธุรกิจได้

อย่างไรก็ดีการที่ IT มีผลกระทบต่อการดำเนินงานด้านธุรกิจอย่างมากในประเทศไทย อาจมีสาเหตุจากหลายปัจจัย เช่น ผลกระทบของตลาดโลกโดยการย้ายถิ่นฐานการลงทุนของต่างชาติเข้ามาลงทุนในประเทศ เช่น ธุรกิจค้าปลีกของบริษัท TESCO LOTUS ของอังกฤษเมื่อขยายฐานการลงทุนเข้ามาในไทย ก็มีการนำ IT เข้ามาใช้กับธุรกิจของตน เพื่อประสิทธิภาพในการจัดการข่าวสาร

และการบริการลูกค้า ซึ่งส่งผลกระทบต่อธุรกิจคู่แข่งด้วย องค์กรอื่นก็จะต้องมีการปรับกลยุทธ์ของตนเอง เพื่อเพิ่มขีดความสามารถในการแข่งขัน ซึ่งแนวคิดของกลยุทธ์ที่ธุรกิจไทยนำมาใช้ส่วนใหญ่จะเป็นการนำเข้าแนวคิดหรือกลยุทธ์ของต่างชาติ โดยขอยกตัวอย่างบุคคล 3 ท่านที่จัดเป็นกูรู (ปรมจารย์) ซึ่งแนวคิดของ 3 ท่านนี้มีอิทธิพลต่อเศรษฐกิจไทยและการศึกษา ดังนี้ (www.businessthai.co.th)

1. ศ.ดร.ไมเคิล อี ฟอร์เตอร์: แห่งฮาร์วาร์ด เจ้าตำรับความคิด “การเพิ่มขีดความสามารถเชิงการแข่งขัน “ โดยผลงานที่สร้างชื่อเสียงแก่ Porter มากที่สุดได้แก่หนังสือเรื่อง Competitive Strategy ในหนังสือเล่มนี้ได้เสนอ Model “พลังทั้ง 5” หรือ FIVE Force อธิบายถึงการวางตำแหน่งบริษัทในอุตสาหกรรม แล้วใช้พลังทั้ง 5 เป็นแรงกดดันเพื่อสร้างกลยุทธ์ในการตอบสนองทางธุรกิจ 3 กลยุทธ์หลัก ได้แก่ 1) COST LEADERSHIP คือ การเป็นผู้นำด้านราคา เช่น การขายสินค้าในราคาที่ต่ำกว่าคู่แข่ง 2) DIFFERENTATION คือ ความแตกต่างด้านผลิตภัณฑ์และบริการสร้างความเป็นหนึ่งในคุณภาพที่เหนือกว่าคู่แข่ง 3) FOCUS คือ เอาข้อดีด้านราคาและคุณภาพมารวมกัน เช่น ขายสินค้าในราคาที่ต่ำกว่าแต่คุณภาพไม่ได้ลดลงแต่อย่างใด

2. จอห์น ซี แม็กซ์- เวลล์: เจ้าของหนังสือ “The 21 Irrefutable Laws of Leadership” หรือ “21 กฎเหล็กแห่งการเป็นผู้นำ” เป็นหนังสือที่ทรงพลังอย่างยิ่ง มีเนื้อหาชัดเจนแจ่มแจ้ง ชนิดว่าถ้าหากใครต้องการจะเป็นผู้นำที่ยิ่งใหญ่ต้องไม่พลาดที่จะอ่านหนังสือเล่มนี้

3.ซี.เค.ปราฮาลาด: เจ้าของแนวคิดใหม่ที่ได้รับความนิยมอย่างสูง เจ้าของหนังสือ “Competing for The Future” เป็นเจ้าของแนวคิดที่ตรงกันข้ามกับ Porter อย่างสิ้นเชิง เพราะเขาเสนอการเปลี่ยนกฎเกณฑ์การแข่งขันเสียใหม่ พร้อม ๆ กับการสร้างตลาดใหม่ และเคยโจมตีทฤษฎีของ Porter ว่าใช้ไม่ได้ผลในปัจจุบัน

จากการศึกษาเรื่องความสำคัญในการจัดการ IT สามารถสรุปได้ว่า แนวคิดของกูรู (GURU) ต่างชาติ ทั้ง 3 ท่านนี้ มีอิทธิพลอย่างมากในการดำเนินธุรกิจของไทย อีกทั้งการศึกษาของไทยก็ยังเป็นการศึกษาแบบนำเข้า (Import) ทั้งนำเข้าอาจารย์ และตำรา ดังนั้นผู้บริหารขององค์กร ควรใช้ดุลย์พินิจในการปรับใช้กลยุทธ์ร่วมกับ IT ไม่ให้ขัดต่อหลักกฎหมาย สังคมและจริยธรรมของไทยด้วย นอกจากผู้บริหารองค์กรจะนำ IT เข้ามาสนับสนุนการทำงานแล้ว ยังควรมองถึงรูปแบบธุระกิจใหม่ ๆ (Business Models) ซึ่งเป็นรูปแบบทางด้านการค้า ที่สามารถเพิ่มคุณค่าทางธุรกิจให้กับองค์กร โดยทำงานบนพื้นฐาน IT ซึ่งมีหลากหลายรูปแบบ ดังนี้ (Efraim Turban, Ephraim Mclean and James Wetherbe : 2002)

Name-Your-Own-Price : เป็นรูปแบบที่ยอมให้ลูกค้าทราบราคาสินค้าก่อนซื้อสินค้าและบริการหรือให้ลูกค้าบอกราคาที่ต้องการจ่าย เช่น การประกาศซื้อรถ ซึ่งผู้ขายจะเข้ามาตอบกลับ
Dynamic Brokering : เป็นรูปแบบที่ยอมให้ลูกค้าสามารถกำหนดความต้องการด้านผลิตภัณฑ์และบริการได้ โดยลูกค้าจะประกาศบน Web และให้ผู้ที่ต้องการขายมาเสนอราคา

Reverse Auctions : การประมูล เป็นวิธีการที่รวดเร็วโดยผู้ขายกำหนดราคาเริ่มต้นของผลิตภัณฑ์ และให้ผู้ซื้อร่วมเคาะราคาการประมูลผ่านทาง Web คนไหนเสนอราคาเป็นที่พอใจก็ขายให้กับคนนั้น

Affiliate marketing : การเข้าร่วมซื้อขายในตลาด มีการจัดหมวดหมู่ของการค้า มีคู่ค้าทางการตลาดทั้งภาคเอกชน รัฐวิสาหกิจ เป็นการหาพรรคพวกทางการตลาด มี Banner โฆษณาชื่อบริษัท

Group Purchasing : เป็นการร่วมกันซื้อเป็นกลุ่ม สามารถซื้อสินค้าได้ในราคาถูก เมื่อซื้อในปริมาณมากจะมีส่วนลดสินค้า E-marketplaces and Exchanges: การตลาดบน Web และการแลกเปลี่ยน จะประกอบได้ด้วยกลุ่มสินค้าที่มีความแตกต่างและหลากหลาย

รูปแบบธุรกิจที่กล่าวมาในข้างต้นนี้ มีพื้นฐานการทำงานโดยอาศัยเทคโนโลยีและการสื่อสารผ่านเครือข่าย เมื่อองค์กรมีการลงทุนด้าน IT แล้ว ก็ควรที่จะใช้ความสามารถของ IT นั้นให้เต็มประสิทธิภาพ โดยพิจาณาถึงรูปแบบธุรกิจ (Business Models) ใหม่ ๆ ว่ามีรูปแบบใดที่องค์กรสามารถนำมาปรับใช้ประโยชน์ เพื่อเพิ่มคุณค่าในทางธุรกิจได้

อย่างไรก็ดีการที่ IT มีผลกระทบต่อการดำเนินงานด้านธุรกิจอย่างมากในประเทศไทย อาจมีสาเหตุจากหลายปัจจัย เช่น ผลกระทบของตลาดโลกโดยการย้ายถิ่นฐานการลงทุนของต่างชาติเข้ามาลงทุนในประเทศ เช่น ธุรกิจค้าปลีกของบริษัท TESCO LOTUS ของอังกฤษเมื่อขยายฐานการลงทุนเข้ามาในไทย ก็มีการนำ IT เข้ามาใช้กับธุรกิจของตน เพื่อประสิทธิภาพในการจัดการข่าวสารและการบริการลูกค้า ซึ่งส่งผลกระทบต่อธุรกิจคู่แข่งด้วย องค์กรอื่นก็จะต้องมีการปรับกลยุทธ์ของตนเอง เพื่อเพิ่มขีดความสามารถในการแข่งขัน ซึ่งแนวคิดของกลยุทธ์ที่ธุรกิจไทยนำมาใช้ส่วนใหญ่จะเป็นการนำเข้าแนวคิดหรือกลยุทธ์ของต่างชาติ โดยขอยกตัวอย่างบุคคล 3 ท่านที่จัดเป็นกูรู (ปรมาจารย์) ซึ่งแนวคิดของ 3 ท่านนี้มีอิทธิพลต่อเศรษฐกิจไทยและการศึกษา ดังนี้ (www.businessthai.co.th)

2.2.7 ประโยชน์ของการให้ความสำคัญในการจัดการ IT หากผู้บริหารขององค์กรมองเห็นความสำคัญของการจัดการ IT และสามารถปรับใช้ได้อย่างเหมาะสมกับแผนธุรกิจในระยะสั้นและระยะยาวขององค์กรแล้ว ก็จะนำมาซึ่งประโยชน์หลากหลายด้าน ดังตัวอย่างต่อไปนี้

บริษัท BMS (Bristol-Myers Squibb) ในอเมริกา เป็นผู้นำทางด้านการผลิตยา เวชภัณฑ์ ผลิตภัณฑ์อาหารเพื่อสุขภาพและความสวยความงาม จำหน่วยสินค้าให้กับบริษัท เช่น ร้านขายยา โรงพยาบาล และร้านค้าปลีก บริษัทมีคู่แข่งทางธุรกิจประเภทเดียวกันเป็นจำนวนมากทั้งบริษัทผู้ขายตรงขนาดเล็กและขนาดใหญ่ และยากมากที่บริษัทจะรักษาคู่ค้า (Partner) เอาไว้กับตนเอง ดังนั้นบริษัทจึงพยายามปรับตัว เพื่อให้สามารถอยู่รอดได้โดยการนำ IT เข้ามาใช้และพัฒนาโครงการ Web-Base ระบบ Supply Chain และระบบ E-procement รวมทั้งได้ปรับโครงสร้างองค์กรเสียใหม่ จากเหตุการณ์นี้ทำให้บริษัทได้รับประโยชน์ในการลดจำนวนเอกสารในการดำเนินงาน (paperless) ลดข้อผิดพลาดเรื่องข้อมูลข่าวสาร (Cut down on error) และสามารถขายตรงได้
ห้างสรรพสินค้า Wall Mart Department storeในอเมริกา ดำเนินธุรกิจค้าปลีกได้รับยกย่องว่ามีระบบบริหารจัดการ IT ยอดเยี่ยม เช่น สามารถตัดยอดสต๊อกสินค้า ณ. ขาย(Point of Sale :POS) ส่งตรงไปยังบริษัทคู่ค้าทันทีทันใด (Just- in-Time) ช่วยลดปัญหาการมีสินค้าคงเหลือ (Discount Store) ล้นคลัง

บริษัท Dell Computer ในอเมริกา ได้นำ IT มาใช้โดยปรับกระบวนการทางธุรกิจ (Business Process) มีการควบคุมการทำงานทั้งระบบ เช่น ระบบขาย ระบบผลิต ซึ่ง Dell จะใช้วิธีขายสิ้นค้าทาง Internet และจะส่งยอดคำสั่งซื้อ (Order) ของลูกค้าไปยังผู้ผลิต (Supplier) จึงทำให้ Dell มีสินค้าคงเหลือน้อยมากและได้สินค้าที่ทันสมัย

เห็นได้ว่าเมื่อองค์กรต่าง ๆ นำ IT มาใช้จะทำให้ได้รับประโยชน์ และมีต้นทุนในการดำเนินงานที่ต่ำลง ทั้งนี้ผู้บริหารต้องให้ความสำคัญถึงผลกระทบในการใช้ IT ที่มีกับองค์กรด้วย

เนื่องจากการนำ IT เข้ามาใช้นั้นไม่ได้หมายความว่าทุกองค์กรจะประสบความสำเร็จเสมอไป ยังมีองค์กรอีกจำนวนมากที่ล้มเหลวจากการนำ IT มาใช้ เนื่องจากผู้บริหารองค์กรหรือ CEO ส่วนใหญ่ขององค์กรถูกแต่งตั้งมากจากบุคคลที่สังกัดฝ่ายบริหารหรือการเงิน (แต่ในปัจจุบันบุคคลด้าน IT จะถูกแต่งตั้งมากขึ้นแต่ต้องเพิ่มทักษะทางด้านการบริหารด้วย) ซึ่งขาดทักษะและความรอบรู้ทางด้าน IT ทำให้ไม่สามารถบริหารจัดการกระบวนการปรับเปลี่ยนระบบ ขาดความสามารถในการปรับใช้ IT ให้สอดคล้องกับแผนกลยุทธ์ ขาดความรู้ทางด้านเทคนิควิธี ดังนั้นองค์กรต้องปรับวัฒนธรรมภายใน ให้กลายเป็นองค์กรแห่งการเรียนรู้ ผู้บริหารจะต้องมีความรู้ด้าน IT สามารถปรับใช้ IT กับการทำงานได้อย่างเหมาะสมและเป็นที่ยอมรับของพนักงานในองค์กร

2.2.8 เรื่องราวเกี่ยวกับความปลอดภัย : ส่วนใหญ่เกี่ยวกับ (IT Security Incidents: A Major Concern)

ในปัจจุบันการสื่อสารและการแลกเปลี่ยนสารสนเทศเป็นไปอย่างรวดเร็วกว้างขวาง ไม่ว่าจะเป็นการแลกเปลี่ยนส่วนตัวหรือการแลกเปลี่ยนระหว่างองค์กร ดังนั้น องค์กรต่างๆ จึงต้องให้ความสำคัญเกี่ยวกับความปลอดภัยของสารสนเทศ ความปลอดภัย ด้านเทคโนโลยีสารสนเทศที่ถูกนำมาใช้ในธุรกิจ เป็นสิ่งที่มีความสำคัญมากที่สุด ข้อมูลความลับทางธุรกิจ และข้อมูลส่วนตัวของลูกค้า และสารสนเทศของพนักงานจะต้องได้รับการปกป้อง และระบบขององค์กรจะต้องสามารถป้องกันการกระทำที่มุ่งร้ายของขโมย หรือการกระทำที่ขัดขวาง ถึงแม้ว่า ความจำเป็นในเรื่องของความปลอดภัยนั้นต้องมีการกระทำให้ชัดเจน มันมักจะต้องสมดุลกับความต้องการทางธุรกิจประเภทอื่น ๆ ผู้บริหารทางธุรกิจ คนเป็นมืออาชีพทางด้านเทคโนโลยีสารสนเทศ และผู้ใช้งานไอทีทั้งหมดต้องเผชิญกับการตัดสินใจทางด้านจริยธรรมที่เกี่ยวข้องกับความปลอดภัยทางเทคโนโลยีสารสนเทศ
จำนวนมาก ตัวอย่าง เช่นถ้า บริษัท ที่ตกเป็นเหยื่อของอาชญากรรมคอมพิวเตอร์ ก็ควรมีการติดตามการฟ้องร้องจากอาชญากรซึ่งอาจมีค่าใช้จ่ายจำนวนมาก ในการรักษารายละเอียดเกี่ยวกับประวัติส่วนตัวของลูกค้าที่มีการดูแลไม่ค่อยดี และเพื่อหลีกเลี่ยงการประชาสัมพันธ์เชิงลบ และควรมีการแจ้งให้กับลูกค้าซึ่งได้รับผลกระทบได้รับทราบ จากการถูกกระทำของอาชญากรที่กระทำต่อองค์กร ซึ่งต้องใช้เวลาบางส่วนในการกระทำอื่น ๆ ในลักษณะเช่นนี้หรือ?จะใช้เงิน และความพยายามเท่าใดในการป้องกันอาชญากรรมคอมพิวเตอร์?หาก บริษัท ได้ตระหนักว่า เมื่อมีการผลิตซอฟต์แวร์ที่มีข้อบกพร่องขึ้นมา ซึ่งทำให้มันมีโอกาสจะเป็นไปได้ว่า อาจถูกแฮกเกอร์โจมตีข้อมูลของลูกค้าและข้อมูลที่มีอยู่ในคอมพิวเตอร์ เมื่อเป็นเช่นนี้ การกระทำอะไรที่บริษัทควรจะทำต่อไป? คำแนะนำอะไรคือสิ่งที่ควรทำ ในการป้องกันรักษาความปลอดภัยของคอมพิวเตอร์ อันจะส่งผลให้ชีวิตของลูกค้าและพนักงาน มีความเป็นอยู่ที่ยากลำบากมากขึ้น ซึ่งผลลัพธ์ก็คือยอดขายที่หายไปและค่าใช้จ่ายที่เพิ่มขึ้น? เป็นที่น่าเสียที่สุด จำนวนตัวเลขของเหตุการณ์เรื่องราวเกี่ยวกับทางด้านความปลอดภัยของเทคโนโลยีสารสนเทศ มีปริมาณเพิ่มมากขึ้น ตามที่ได้มีการดำเนินการศึกษาเกณฑ์การเปรียบเทียบบริษัทในสหรัฐอเมริกา โดยสถาบันโพนิมอน เมื่อเดือนกรกฎาคม ค.ศ. 2010 การโจมตีทางไซเบอร์ได้กลายเป็น

เหตุการณ์ที่เกิดขึ้นร่วมกัน แต่ละ บริษัท รวม 45 บริษัท จากรายงานการศึกษาพบว่า บริษัทเหล่านั้นได้ตกเป็นเหยื่อการโจมตีอย่างน้อย 1 อย่างต่อสัปดาห์ ตารางที่ 3.1 แสดงให้เห็นถึงการเพิ่มขึ้นของเหตุการณ์ด้านความปลอดภัยของคอมพิวเตอร์ ที่มีการสำรวจองค์กรมากถึง 443 องค์กรในสหรัฐ ที่ส่งคืนตอบแบบสอบถาม ในปี ค.ศ. 2009 ซึ่งสอบถามเกี่ยวกับเรื่องอาชญากรรมคอมพิวเตอร์ และความปลอดภัยทางด้านคอมพิวเตอร์

ตารางที่ 2.2 เหตุการณ์ด้านความปลอดภัยที่พบมากที่สุด

Credit: "2009 Computer Security Institute Computer Crime & Security Survey", courtesy of the Computer Security Institute. (George W. Reynolds: 2012)

เหตุการณ์ด้านความปลอดภัยของคอมพิวเตอร์	**ค.ศ.2009**	**ค.ศ.2008**
ผู้ตอบแบบสอบถามที่มีประสบการณ์การติดเชื้อมัลแวร์	64.3%	50%
ผู้ตอบแบบสอบถามที่มีประสบการณ์การโจมตีการปฏิเสธการให้บริการ	29.2%	21%
ผู้ตอบแบบสอบถามที่มีประสบการณ์รหัสผ่าน การดมกลิ่น	17.3%	9%
ผู้ตอบแบบสอบถามที่มีประสบการณ์ทำให้เว็บไซต์เสียหาย	13.5%	6%
ผู้ตอบแบบสอบถามที่มีประสบการณ์การทำผิดกฎเกี่ยวข้อความโต้ตอบแบบทันที	7.6%	21%

2.2.9 ทำไมเรื่องราวเกี่ยวกับความปลอดภัยของคอมพิวเตอร์ จึงสามารถพบเห็นได้บ่อยๆ

เนื่องสภาวการณ์ปัจจุบัน สิ่งแวดล้อมทางคอมพิวเตอร์มีความซับซ้อนมากขึ้น ผู้ใช้มีความคาดหวังสูง จำนวนของผู้ใช้งานด้านคอมพิวเตอร์ได้เพิ่มขยายขึ้นอย่างต่อเนื่อง ระบบการทำงานและระบบคอมพิวเตอร์มีการเปลี่ยนแปลง และความเชื่อมั่นในซอฟต์แวร์ก็มีเพิ่มขึ้น ทั้งๆ ที่ก็พอรู้กันดีว่า มันย่อมมีช่องโหว่บ้าง จึงเป็นเรื่องที่ไม่น่าแปลกใจว่า ทำไมผลกระทบของเหตุการณ์เกี่ยวกับการรักษาความปลอดภัยทางด้านคอมพิวเตอร์จึงต้องมีเพิ่มขึ้นอย่างมาก เหตุการณ์การรักษาความปลอดภัยของคอมพิวเตอร์ทั่วโลกเริ่มมีและตระหนักกันมากขึ้นเป็นลำดับ ตาราง ที่ 3.2 แสดงให้เห็นถึงการจัดอันดับของหกประเทศที่มีกิจกรรมที่เป็นอันตรายมากที่สุดในปี ค.ศ. 2009 ซึ่งมีการวัดโดย บริษัท ไซเมนเทค (Symantec)

ตาราง ที่ 2.3 การจัดอันดับ 6 ประเทศที่มีกิจกรรมที่เป็นอันตรายมากที่สุด ในปี ค.ศ. 2009 (Source: George W. Reynolds: 2012)

ประเทศ	การจัดอันดับในปี 2009	การจัดอันดับในปี 2008
สหรัฐอเมริกา	1	1
จีน	2	2
บราซิล	3	3
เยอรมันนี	4	4
อินเดีย	5	5
อังกฤษ	6	6

ความซับซ้อนเพิ่มมากขึ้น ความไม่มั่นคงจึงเพิ่มขึ้นตามไปด้วย (Increasing Complexity Increases Vulnerability) สิ่งแวดล้อมทางคอมพิวเตอร์มีความซับซ้อนเกิดขึ้นอย่างมากมาย ได้แก่ เครือข่ายคอมพิวเตอร์ เครื่องคอมพิวเตอร์ การปฏิบัติการ ระบบ การประยุกต์ใช้ เว็บไซต์ สวิตช์ เราเตอร์ และ เกตเวย์ ที่เชื่อมต่อและผลักดันจากหลายร้อยล้านเส้นทางของรหัสการเขียนโปรแกรม สิ่งแวดล้อมของความซับซ้อนทางคอมพิวเตอร์นี้ ยังคงมีเพิ่มมากขึ้นอย่างต่อเนื่องทุกวัน จำนวนตัวเลขของเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อเข้ามายังมีการขยายเพิ่มมากขึ้นอย่างต่อเนื่องตัวอย่างเช่น การเชื่อมต่อจากอุปกรณ์ต่างๆ อย่างมากมาย ในขณะเดียวกันก็มีการละเมิดความปลอดภัยทางด้านคอมพิวเตอร์อย่างต่อเนื่องด้วยเช่นกัน นอกจากนี้ องค์กรและพนักงานเป็นจำนวนมากหันมาใช้คอมพิวเตอร์แบบกลุ่มเมฆ (Cloud computing) ในการทำงานและใช้ในการจัดเก็บข้อมูลการให้บริการผ่านอินเทอร์เน็ต และซอฟต์แวร์เสมือนจริงก็เช่นเดียวกัน ซอฟต์แวร์เสมือนจริงเป็นซอฟต์แวร์ที่เลียนแบบการทำงานของคอมพิวเตอร์ฮาร์ดแวร์โดยสามารถปฏิบัติการได้หลายระบบที่ทำงานอยู่บนคอมพิวเตอร์แม่ข่ายที่เดียว

ผู้ใช้คอมพิวเตอร์ มีความคาดหวังสูงมากขึ้น (Higher Computer User Expectations)

เนื่องจากปัจจุบันนี้ เวลาเป็นเงินเป็นทอง คอมพิวเตอร์มีความเร็วมากขึ้น ผู้ใช้สามารถแก้ปัญหาเองได้ ในอนาคตไม่ช้านี้ ผู้ใช้สามารถที่จะผลิตได้เอง ด้วยเหตุผลดังกล่าวนี้ คนทำงานคอมพิวเตอร์ที่แผนกช่วยเหลือ (Help desks) ตกอยู่ภายใต้แรงกดดันในการที่จะให้คำตอบจากผู้ใช้ที่ร้องขอข้อมูลเข้ามาอย่างรวดเร็ว จากภายใต้แรงกดดันที่ว่านี้ บางครั้ง พนักงานคอมพิวเตอร์ที่แผนกช่วยเหลือ มีการลืมตรวจสอบไอดีของผู้ใช้ (users' IDs) หรือ ลืมตรวจสอบการอนุญาต และผู้ใช้คอมพิวเตอร์บางคน ได้แบ่งปัน ไอดีการเข้าสู่ระบบ และรหัสผ่าน (login IDs and passwords)

การขยายตัว/การเปลี่ยนแปลงระบบ ซึ่งเท่ากับการมีความเสี่ยงใหม่ (Expanding and Changing Systems Introduce New Risks)

ธุรกิจได้เคลื่อนย้ายจากยุคของการใช้เครื่องคอมพิวเตอร์ทำงานเครื่องเดียว ซึ่งมีการการเก็บข้อมูลที่สำคัญไว้ในคอมพิวเตอร์เมนเฟรมแยกไว้ในห้องจัดเก็บ จนต่อมาได้เข้าสู่ยุคที่คอมพิวเตอร์ส่วนบุคคลที่เชื่อมต่อกับเครือข่ายคอมพิวเตอร์อื่นๆ ที่มีจำนวนนับล้านๆ เครื่องที่มีความสามารถในการใช้ข้อมูลร่วมกัน ที่เรียกว่าเป็นยุคของเครือข่าย (Network era) และคอมพิวเตอร์ที่เชื่อมต่อกันทั้งหมดเหล่านั้น สามารถแบ่งปันสารสนเทศร่วมกันได้ เมื่อกล่าวถึงเรื่องของเทคโนโลยีสารสนเทศ ซึ่งในปัจจุบัน เราสามารถพบเห็นได้โดยทั่วไป ทุกคนต่างยอมรับโดยดุษฎีว่า เทคโนโลยีสารสนเทศถือว่าเป็นเครื่องมืออันทรงพลังอย่างหนึ่ง ซึ่งมีส่วนช่วยผลักดันทำให้องค์กรประสบความสำเร็จตามเป้าหมายที่ได้วางเอาไว้ และด้วยความเจริญก้าวหน้าของเทคโนโลยีสารสนเทศนี่เอง ทำให้มีความยากเพิ่มขึ้นในการที่จะทำให้การเปลี่ยนแปลงเทคโนโลยีนำมาปรับให้เข้ากันได้

เมื่อคุณจะใช้คอมพิวเตอร์และอินเทอร์เน็ต คุณจะต้องมีวิธีการป้องกันการเล่นอินเทอร์เน็ตของคุณก่อน เมื่อคุณใช้จุดเชื่อมโยงสาธารณะ (public hotspot) ในการเล่นอินเทอร์เน็ต เนื่องจากกิจกรรมการเล่นอินเทอร์เน็ตของคุณนั้น มีคนสอดแนม (snooping) ที่อยากรู้อยากเห็นความเคลื่อนไหวของคุณ เว็บไซต์ hotspotshield.com เป็นเว็บไซต์ที่บริการซอฟต์แวร์ที่เป็นประโยชน์ (software utility) เพื่อให้แน่ใจว่า ข้อมูลของคุณทั้งหมดที่ถูกส่งไปบนอินเทอร์เน็ตตลอดจนถึงเครือข่ายเสมือนจริงส่วนบุคคล (virtual private network : VPN) วีพีเอ็น คือ เส้นทางความปลอดภัยของอินเทอร์เน็ต มีบริษัทใหญ่ๆ จำนวนมาก ใช้ในการป้องกันข้อมูลที่ไวสัมผัส การใช้วีพีเอ็นเป็นเกราะป้องกันข้อมูล (shields your data)จากบุคคลผู้ต้องการอยากรู้อยากเห็น เช่น สารสนเทศที่คุณกรอกแบบฟอร์ม, ข้อมูลบัตรเครดิต, การส่งข้อความรีบด่วน และกิจกรรมของเว็บบราวซิ่ง ดังนั้นปัจจุบันจึงมีการติดตั้งเกราะป้องกันที่จุดเชื่อมโยง และเพิ่มระดับการป้องกันข้อมูลของคุณ

2.2.10 การรักษาความปลอดภัยข้อมูลของคุณ สื่อที่เป็นเรื่องราวสมบูรณ์เกี่ยวกับโปรแกรมความมุ่งร้ายที่สร้างความเสียหายให้กับคอมพิวเตอร์, เรื่องราวเกี่ยวกับการกระทำความผิด

ด้วยการกำหนดอัตลักษณ์ของประชาชนทางระบบออนไลน์ และการโจมตีเว็บไซต์ของบริษัท ซึ่งนำมาสู่ปัญหาหลักของบริษัทก็ยังคงมีอยู่จริง ตัวอย่างเหล่านี้เรียกว่า อาชญากรรมไซเบอร์ (cybercrime) ซึ่งก็คือ การถูกระบุด้วยการกระทำผิดกฎหมายบนพื้นฐานในการใช้คอมพิวเตอร์ การที่อาชญากรรมไซเบอร์ที่ยังคงมีอยู่นั้น หมายความว่า ผู้ใช้คอมพิวเตอร์จะต้องระมัดระวังเอาไว้ก่อนในการป้องกันความปลอดภัยของตัวเอง

ใครคืออาชญากรรมคอมพิวเตอร์กระทำผิดเกี่ยวกับกฎหมาย? การกระทำผิดกฎหมายไซเบอร์ (Cybercriminal) คือ บุคคลผู้ใช้คอมพิวเตอร์, เครือข่าย และอินเทอร์เน็ตกระทำผิดทางด้านอาชญากรรม ใครก็ตามเป็นคนที่มีความรู้ซึ่งมีคอมพิวเตอร์อยู่ในมือของเขา หรือของหล่อนสามารถจะเป็นผู้กระทำความผิดเกี่ยวกับกฎหมายไซเบอร์ได้ทั้งนั้น

2.2.11 ประเภทของความประพฤติเกี่ยวกับอาชญากรรมไซเบอร์บนอินเทอร์เน็ตมีอะไรบ้าง?

ศูนย์รับการร้องเรียนความไม่พอใจเกี่ยวกับอาชญากรรมทางอินเทอร์เน็ต (Internet Crime Complaint Center : IC3) เป็นหน่วยงานที่เป็นหุ้นส่วนระหว่างสำนักงานสหพันธรัฐการสืบสวน (Federal Bureau of Investigation : FBI) และศูนย์อาชญากรรมแห่งชาติไวท์คอลาร์ (National White Collar Crime Center : NW3C) ในปี ค.ศ. 2009 ล่าสุด ซึ่งมีข้อมูลที่ไม่เหมาะสมเป็นจำนวนมาก IC3 ได้ดำเนินการเรื่องที่ได้รับการร้องเรียนเกี่ยวกับอาชญากรรมทางอินเทอร์เน็ตมีมากกว่า 336,000 ครั้ง ซึ่งเพิ่มขึ้น 22 เปอร์เซ็นต์จากปี ค.ศ. 2008 เรื่องที่ได้รับการร้องเรียนเป็นจำนวนมากเป็นเรื่องเกี่ยวกับการโกง เช่น การโกงการประมูล, การไม่ส่งสินค้าตามใบสั่งซื้อ, บัตรเครดิต และบัตรหักบัญชี และเล่ห์อุบายเกี่ยวกับเรื่องค่าธรรมเนียม การร้องเรียนที่ไม่ได้เกี่ยวข้องกับการโกงแต่เป็นเรื่องอันตราย เช่น การบุกรุกทางคอมพิวเตอร์, ไปรษณีย์อิเล็กทรอนิกส์ที่ไม่ได้รับเชิญ, และเรื่องเร้าทางกามารมณ์ ที่พบเห็นเป็นจำนวนมาก คือ การโกงเกี่ยวกับบัตรเครดิตอันเป็นการกระทำที่ผิดกฎหมาย เมื่อหมายเลขบัตรเครดิตถูกขโมยโดยเล่ห์กลการกระทำผิดของใครบางคน ที่มีการเผยข้อมูลสารสนเทศให้รู้ โดยมีการใช้โปรแกรมคอมพิวเตอร์ขโมยข้อมูลบัตรเครดิต

จากการรายงานข่าวทั้งหมด เกี่ยวกับอาชญากรรมไซเบอร์ มีสิ่งอื่นๆ อีกที่ประชาชนไม่ได้ระมัดระวัง? (With all the news coverage about cybercrimes, aren't people being more cautious?) โชคไม่ดี, ที่พวกเขาไม่ได้ระมัดระวัง ถึงแม้ว่า ประชาชนส่วนใหญ่จะระมัดระวังเกี่ยวกับขยะไปรษณีย์อิเล็กทรอนิกส์, ปัจจุบันจากการสำรวจโดยกลุ่มคนที่ทำงานเกี่ยวกับการป้องกันการกระทำผิดทางด้านข้อความ (Messaging Anti-Abuse Working Group : MAAWG) พบว่า ครึ่งหนึ่งของผู้ใช้ไปรษณีย์อิเล็กทรอนิกส์ในอเมริกาเหนือ และยุโรป มีขยะไปรษณีย์อิเล็กทรอนิกส์ MAAWG ได้ค้นพบว่า 46 เปอร์เซ็นของประชาชนผู้ที่เปิดอ่านขยะไปรษณีย์อิเล็กทรอนิกส์อย่างตั้งใจ การที่จะออกจากข้อความที่ไร้สาระเหล่านั้นคือการยกเลิกการเป็นสมาชิกการเว็บไซต์ที่เชื่อมโยง เพื่อไม่ต้องการได้รับไปรษณีย์อิเล็กทรอนิกส์ที่ไม่ต้องการอีก (อันจะนำมาซึ่งขยะไปรษณีย์อิเล็กทรอนิกส์)

การที่ประชาชนได้รับขยะไปรษณีย์อิเล็กทรอนิกส์ ก็เพราะว่าพวกเขามีความสนใจในบรรดาสินค้าทั้งหลาย ที่ชัดเจนก็คือส่วนใหญ่มักเป็นข้อมูลที่มาจากฝ่ายตรงข้ามหรือศัตรู

2.2.12 ความมั่นใจในซอฟต์แวร์ทางการค้ามีเพิ่มมากขึ้น ซึ่งเป็นที่รู้กันดีว่า มันยังมีความไม่มั่นคงแฝงอยู่ (Increased reliance on commercial software with known vulnerabilities) ซึ่งความไม่มั่นคงนั้นมีสาเหตุมาจากหลายประการ คือ:

การเอารัดเอาเปรียบหาประโยชน์ใส่ตัว (Exploit) เช่น การโจมตีระบบสารสนเทศการหาประโยชน์จากความอ่อนแอไม่มั่นคงของระบบ, มีการกำหนดออกแบบระบบที่แย่มาก หรือการทำให้เกิดผลต่อการนำไปปฏิบัติ

การติดตั้ง (Patch) มีการกำหนดการขจัดปัญหา, ผู้ใช้สามารถได้รับการสนองตอบและการไม่ติดตั้ง, ความล่าช้าในการเปิดเผยออกมาถึงการใช้งานของผู้ใช้ในการฝ่าฝืนความปลอดภัยของระบบคอมพิวเตอร์

การโจมตีด้วยซีโร่เดย์ (Zero-day attack) คือการโจมตีที่ใช้ประโยชน์จากช่องโหว่ที่ไม่รู้จักก่อนหน้านี้ในโปรแกรมคอมพิวเตอร์ ที่มีความหมายว่าการโจมตีที่เกิดขึ้นบน **"วันศูนย์"** ของการรับรู้ของความเสี่ยง เป็นลักษณะของการกำหนดวันโจมตีที่แน่นอน แต่ความหมายทางคอมพิวเตอร์ ไวรัสมัลแวร์ก็จะกระจายออกมา เหมือนกับการวางระเบิดเวลาเอาไว้ที่เลขศูนย์ เมื่อเวลาเดินไปถึงเลขศูนย์ระเบิดเวลาก็ทำงาน หรือกล่าวอีกนัยหนึ่ง คือ นักพัฒนาระบบที่เป็นพวกแฮกเกอร์ ได้พัฒนาระบบขึ้นมาโดยอาศัยช่องโหว่ของโปรแกรมคอมพิวเตอร์ และมีการใช้ซอฟต์แวร์มัลแวร์ (Malware) ย่อมาจากคำว่า Malicious Software ซึ่งหมายถึงโปรแกรมประสงค์ร้ายต่างๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล มัลแวร์ แบ่งออกได้หลากหลายประเภท อาทิเช่น ไวรัส (Virus) เวิร์ม (Worm) หรือหนอนอินเทอร์เน็ต ม้าโทรจัน (Trojan Horse) การแอบดักจับข้อมูล (Spyware) คีย์ ล๊อกเกอร์ (Key Logger) บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน ตลอดจนโปรแกรมประเภทขโมยข้อมูล (Cookie) และการฝัง Malicious Mobile Code (MMC) ผ่านทางช่องโหว่ของโปรแกรม Internet Explorer (IE Vulnerability) ที่เกิดขึ้น โดยโปรแกรมจะทำการควบคุมการทำงานโปรแกรม Internet Explorer ให้เป็นไปตามความต้องการของผู้ที่ไม่หวังดี เช่น การแสดงโฆษณาในลักษณะของการ Pop-Up หน้าต่างโฆษณาออกมาเป็นระยะ ซึ่งเราเรียกโปรแกรมประเภทนี้ว่า แอ็ดแวร์ (Adware) ซึ่งภัยเหล่านี้ในปัจจุบันได้เพิ่มขึ้นอย่างรวดเร็ว ซึ่งอาจจะเกิดผลกระทบแก่ผู้ใช้งานได้ ถ้ารับโปรแกรมเหล่านี้เข้ามาในเครื่องคอมพิวเตอร์ นอกจากนั้นโปรแกรมประเภทนี้ ยังมีอีกหลายชนิดเช่น Toolbar, BHO, Hijacker, Downloader, Phishing, Exploit malware รวมไปถึง Zero-day attack, Zombie

network เป็นต้น ดังนั้น บริษัทในสหรัฐอเมริกาได้พึ่งพาอาศัยซอฟต์แวร์ในการทำธุรกิจ ด้วยเป็นที่รู้กันดีว่ามันมีช่องโหว่ที่คนรู้จักอยู่

2.2.13 ประเภทของการหาประโยชน์อย่างไม่ถูกต้อง (Types of Exploits) ปัจจุบันมีจำนวนประเภทการโจมตีทางคอมพิวเตอร์หลายประเภท มีการสร้างแนวทางใหม่ๆ เพื่อการโจมตีอยู่ตลอดเวลา ซึ่งในส่วนนี้จะได้กล่าวถึงประเภทของการโจมตีบางอย่าง ซึ่งรวมถึง ไวรัส หนอน ม้าโทรจัน การปฏิเสธการให้บริการแบ่งปัน (Distributed denial of service) การโจมตีแบบพิเศษที่สามารถซ่อนตัวอยู่ในโปรแกรมหลัก (Root) ในระบบที่ติดไวรัส ซึ่งผู้ดูแลไม่สามารถเห็นได้ จึงไม่สามารถตรวจจับได้ (Rootkit) อีเมลขยะ การหลอกลวงทางอินเทอร์เน็ต เป็นต้น ในปัจจุบันผู้โจมตีได้มุ่งเป้าหมายการโจมตีมาที่คอมพิวเตอร์ และสมาร์ทโฟนมากขึ้น เช่น โทรศัพท์ iPhone ของบริษัทแอปเปิล, แบลคเบอร์รี และเนื่องจากจำนวนตัวเลขของคอมพิวเตอร์ และโทรศัพท์สมาร์ทโฟนที่ใช้ระบบปฏิบัติการ Andriod ของกูเกิลเพิ่มมากขึ้นเรื่อยๆ และจำนวนเหล่านั้น พวกเขาได้บรรจุข้อมูลส่วนบุคคลลงไปมาก ได้แก่ หมายเลขบัตรเครดิต หมายเลขบัญชีธนาคาร พวกเขาสามารถใช้อินเทอร์เน็ตเว็บไซต์ และทำการประมวลผลรายการทางธุรกิจต่างๆ ได้ จึงทำให้ตกเป็นเป้าหมายในการโจมตีของพวกมิจฉาชีพทั้งหลาย สำหรับประเภทของการโจมตีนั้น มีรายละเอียดดังต่อไปนี้ คือ:

ไวรัส (Viruses) ไวรัสคอมพิวเตอร์ได้กลายเป็นคำที่ครอบคลุมสำหรับรหัสที่เป็นอันตรายหลายประเภท ในทางเทคนิค ไวรัสคอมพิวเตอร์เป็นส่วนเล็กๆ ของรหัสการเขียนโปรแกรม โดยปกติแล้วมันจะถูกปลอมแปลงให้ไปเป็นอย่างอื่น เป็นสาเหตุทางคอมพิวเตอร์ที่ไม่มีใครอยากคาดหวังจะให้เกิดขึ้น และเป็นพฤติกรรมที่ไม่เป็นที่ต้องการ ไวรัสคอมพิวเตอร์ที่มักพบเห็นบ่อย มักเกิดมาจากการแนบไฟล์ ดังนั้น เมื่อไฟล์ติดเชื้อถูกเปิดขึ้น ไวรัสคอมพิวเตอร์ก็จะทำงาน เมื่อไวรัสคอมพิวเตอร์เข้าไปอยู่ในหน่วยความจำของคอมพิวเตอร์ เมื่อไฟล์หรือแฟ้มข้อมูลที่ถูกเปิดขึ้นมาก็จะติดเชื้อ, มีการเปลี่ยนแปลง, และมีการสร้างการแพร่กระจายออกไป ไวรัสคอมพิวเตอร์เป็นซอฟต์แวร์ที่มุ่งร้าย และเป็นสาเหตุให้เครื่องคอมพิวเตอร์ทำงานไม่เป็นไปตามที่คาดหวัง ตัวอย่างเช่น ไวรัสอาจจะถูกเขียนขึ้นมาเพื่อให้แสดงข้อความบางอย่างที่หน้าจอของคอมพิวเตอร์, อาจจะลบ หรือแก้ไขเอกสารบางอย่าง หรือทำให้มีการเปลี่ยนรูปของฮาร์ดไดรฟ์

ความจริงไวรัสคอมพิวเตอร์ไม่แพร่กระจายด้วยตัวของมันเองจากคอมพิวเตอร์เครื่องหนึ่งไปยังคอมพิวเตอร์อีกเครื่องหนึ่งได้ ไวรัสคอมพิวเตอร์จะแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่นก็ต่อเมื่อมีผู้ใช้คอมพิวเตอร์เปิดไปรษณีย์อิเล็กทรอนิกส์ที่ติดเชื้อมา, การดาวน์โหลดโปรแกรมที่ติดเชื้อ หรือการเข้าไปเยี่ยมชมเว็บไซต์ อีกความหมายหนึ่งก็คือ ไวรัสคอมพิวเตอร์จะแพร่กระจายโดยการกระทำให้ติดเชื้อโดยผู้ใช้ มาโครไวรัสได้กลายเป็นเรื่องธรรมดาที่พบเห็นโดยทั่วไปและง่ายมากที่จะสามารถถูกสร้างขึ้นจากไวรัส ผู้แนบไฟล์ใช้ภาษามาโครในการประยุกต์ใช้ เช่นภาษา Visual Basic หรือ VBScript ในการสร้างโปรแกรมให้เอกสารและแบบฟอร์มสำเร็จรูปให้ติดเชื้อ มาโครไวรัส

สามารถที่จะแทรกคำ, หมายเลข หรือวลี ซึ่งไม่เป็นที่ต้องการในเอกสาร หรือเปลี่ยนแปลงการทำงานของคำสั่ง หลังจากมาโครไวรัสติดเชื้อในการประยุกต์ใช้งานของผู้ใช้ มันสามารถฝังตัวของมันเองในเอกสารทั้งหมดที่จะถูกสร้างขึ้นในอนาคต เมื่อมีการนำเอาไปประยุกต์ใช้งาน

ไวรัสบางชนิดซ่อนตัวอยู่บนเว็บไซต์จากสิ่งที่เขียนขึ้น สคริปหรือสิ่งที่เขียนขึ้นคือ ลำดับของคำสั่ง-อย่างที่เกิดขึ้นตามจริง, โปรแกรมขนาดเล็ก ซึ่งถูกบริการโดยปราศจากความรู้ของคุณ สคริปได้ถูกนำไปใช้ปฏิบัติในแนวทางที่เป็นประโยชน์ หน้าที่การทำงานของมันถูกต้องตามกฎหมายบนเว็บ เช่น การเก็บรวบรวมชื่อ และสารสนเทศที่อยู่จากลูกค้า อย่างไรก็ตาม บางสคริปมีความมุ่งร้าย ตัวอย่างเช่น คุณได้รับไปรษณีย์อิเล็กทรอนิกส์ที่กระตุ้นคุณให้เข้าไปเยี่ยมชมเว็บไซต์เต็มของโปรแกรมและสารสนเทศ เมื่อคุณคลิกลิงค์ที่แสดงวิดีโอบนเว็บไซต์เพื่อบอกทางไปยังเว็บ, สคริปก็จะทำงานทำให้คอมพิวเตอร์ของคุณติดเชื้อไวรัสโดยการปราศจากความรู้ของคุณ

ไวรัสคำสั่งที่ผู้ใช้เขียนขึ้นเองหรือมาโครไวรัส คือ ไวรัสที่แนบมากับตัวของมันเองที่เอกสาร (เช่น แฟ้มข้อมูลของ word และ excel) ที่ใช้มาโคร มาโครคือลำดับของคำสั่งสั้นๆ ซึ่งโดยปกติแล้วมันจะทำงานภารกิจที่เกิดขึ้นซ้ำๆ ได้โดยอัตโนมัติ อย่างไรก็ตามภาษาของมาโครปัจจุบันก็ยังเป็นเรื่องที่ซับซ้อน ซึ่งไวรัสสามารถที่จะเขียนด้วยตัวของมันเอง เมลิสสาไวรัส (Melissa virus) กลายเป็นไวรัสมาโครตัวแรกที่เป็นสาเหตุให้เกิดปัญหาทั่วโลกในปัจจุบัน

เมลิสสาไวรัสเป็นไวรัสที่ใช้งานได้จริงตัวแรกจากตัวอย่างของไวรัสไปรษณีย์อิเล็กทรอนิกส์ E-mail Viruses ใช้หนังสือที่อยู่ในระบบไปรษณีย์อิเล็กทรอนิกส์ของเหยื่อในการเผยแพร่ไวรัส การเปิดเอกสารที่ติดเชื้อทุกๆ ครั้ง ไวรัสก็จะถูกกระตุ้น และทำให้คอมพิวเตอร์ของเหยื่อที่มีเอกสารในโปรแกรมเวิร์ดติดเชื้อ การกระตุ้นครั้งหนึ่ง มาลิสสาไวรัสจะส่งตัวของมันเอง ไปยังหนังสือที่อยู่ของประชาชนทำให้ติดเชื้อบนคอมพิวเตอร์ของ 50 คนแรก ด้วยการช่วยเหลือตัวเองนี้ ทำให้มาลิสสาไวรัสกลายเป็นไวรัสเวอร์ชั่นที่แพร่กระจายไปอย่างกว้างขวางที่สุด

ไวรัสการเข้ารหัสลับ (Encryption Viruses) เมื่อไวรัสการเข้ารหัสลับติดเชื้อบนคอมพิวเตอร์ของคุณ มันจะรันโปรแกรมในการค้นหาประเภทของแฟ้มข้อมูลทั่วไป (เช่น แฟ้มข้อมูลในโปรแกรมไมโครซอฟท์เวิร์ด และเอ็กเซล) และทำการบีบอัดแฟ้มข้อมูลเหล่านั้น ด้วยการปรับใช้การเข้ารหัสที่ซับซ้อนส่งผลให้แฟ้มข้อมูลของคุณใช้การไม่ได้ และหลังจากนั้น คุณจะได้รับข้อความซึ่งถามคุณในการส่งเงินเข้าบัญชี ถ้าคุณต้องการรับโปรแกรมการถอดรหัสที่แฟ้มข้อมูลของคุณ ด้วยข้อบกพร่องของไวรัสประเภทนี้ ที่ถูกเก็บเอาไว้มันก็จะแพร่กระจายไปทั่ว ซึ่งสำนักงานผู้บังคับใช้กฎหมายสามารถที่จะติดตามร่องรอยการชำระเงินเข้าบัญชี และอาจเป็นไปได้ว่า คุณอาจจะถูกจับในฐานะเป็นผู้กระทำความผิดได้ แม้ในขณะนี้ เราได้พบเห็นไวรัสชนิดนี้ตลอดเวลา

การจำแนกประเภทของไวรัส (Virus Classifications) ไวรัสสามารถถูกจำแนกออกได้ตามทฤษฎีด้วยการหลีกเลี่ยงป้องกันด้วยซอฟต์แวร์ต่อต้านป้องกันไวรัส:

- ไวรัสมีพหุสัณฐาน (polymorphic virus) มันจะเปลี่ยนรหัสด้วยตัวของมันเอง (หรือเขียนรหัสด้วยตัวของมันCเองตามกำหนดเวลา) เพื่อหลีกเลี่ยงการป้องกัน แฟ้มข้อมูลที่ติดเชื้อไวรัสมีพหุสัณฐานมากที่สุดโดยปกติแล้วจะเป็นแฟ้มข้อมูล (แฟ้มข้อมูล.EXE เป็นตัวอย่าง)
- ไวรัสหลายฝ่าย (multipartite virus) ได้ถูกออกแบบมาให้ติดเชื้อกับแฟ้มข้อมูลหลายประเภทที่พยายามหลอกลวงด้วยซอฟต์แวร์ป้องกันไวรัส ที่มันกำลังมองหาอยู่
- ไวรัสพฤติการณ์ลับ (Stealth viruses) การลบรหัสชั่วคราวของเขาจากแฟ้มข้อมูลที่มันอาศัยอยู่ หรือซ่อนตัวอยู่ในขณะที่หน่วยความจำของคอมพิวเตอร์กำลังทำงานอยู่ ด้วยความช่วยเหลือให้มันหลีกเลี่ยงจากการป้องกัน แม้ว่ามีเพียงฮาร์ดไดร์ฟที่ถูกค้นหาอยู่สำหรับไวรัสด้วยความโชคดี ที่ซอฟต์แวร์ป้องกันไวรัสปัจจุบันสามารถตรวจสอบหน่วยความจำในฮาร์ดไดร์ฟได้เป็นอย่างดี

จากตัวอย่างของการสร้างของผู้เขียนโปรแกรมไวรัสที่ให้ไว้แล้วนี้ เพื่อให้เกิดความแน่ใจ คุณจะสามารถดูประเภทของไวรัสอื่นๆ ที่ปรากฏออกมาในอนาคต ในหมวดต่อไป เราจะได้อภิปรายการขัดขวางการติดเชื้อไวรัส

ไวรัสภาคของการปลุกเครื่องคืออะไร? (What are boot-sector viruses?) ไวรัสภาคของการปลุกเครื่องจะทำซ้ำหรือทำสำเนาใหม่ตัวของมันเองไปยังระเบียนการปลุกเครื่องของตัวควบคุมฮาร์ดไดร์ฟ ไวรัสภาคของการปลุกเครื่องคือโปรแกรมที่ใช้บริหารซึ่งเมื่อไหร่ก็ตามที่เริ่มมีการปลุกเครื่อง เพื่อให้แน่ใจว่า ไวรัสจะถูกถ่ายเทข้อมูลไปยังหน่วยความจำในทันที แม้ว่าก่อนหน้านั้นจะมีการถ่ายเทโปรแกรมป้องกันไวรัสไว้แล้วก็ตาม ไวรัสภาคของการปลุกเครื่องจะถูกส่งไปยังช่องเสียบแฟลซไดร์ฟซึ่งอยู่ทางด้านซ้ายมือ เมื่อคอมพิวเตอร์เริ่มปลุกเครื่องด้วยการเชื่อมต่อกับแฟลซไดร์ฟ คอมพิวเตอร์ก็จะพยายามปฏิบัติการระเบียนการปลุกตัวควบคุมจากแฟลซไดร์ฟ ซึ่งโดยปกติแล้ว มันจะเป็นตัวกระตุ้นไวรัสให้ติดเชื้อไปยังฮาร์ดไดร์ฟ

ลูกระเบิดของความมีเหตุผลคืออะไร? (What is a logic bombs?) ลูกระเบิดของความมีเหตุผล คือ ไวรัสที่ถูกกระตุ้น เมื่อได้พบกับเงื่อนไขบางอย่างของความมีเหตุผลบางอย่าง เช่น การเปิดแฟ้มข้อมูล หรือการเริ่มต้นโปรแกรมบางอย่างที่เป็นตัวเลขเวลา ส่วนลูกระเบิดเวลา คือ ไวรัสที่ถูกกระตุ้นโดยเวลาที่ผ่านไป หรือบนวันที่ซึ่งแน่นอน ตัวอย่างเช่น ไวรัสไมเคิลแองจีโล (Michelangelo virus) เป็นไวรัสลูกระเบิดเวลาที่ดังมาก มันถูกตั้งเวลากระตุ้นทุกๆ ปีในวันที่ 6 เดือนมีนาคม ซึ่งเป็นวันเกิดของไมเคิลแองจีโล แบล็คเวิร์มไวรัส (BlackWorm virus) (ไม่เช่นนั้นก็รู้จักกันอีกในนาม Kama Sutra, Mywife หรือ CME-24) เป็นลูกระเบิดเวลาอีกชนิดหนึ่งที่แพร่กระจายผ่านไปกับการแนบไฟล์

ไปรษณีย์อิเล็กทรอนิกส์ การเปิดไฟล์ที่แนบมาทำให้คอมพิวเตอร์ติดเชื้อไวรัส และทุกวันที่ 3 ของทุกๆ เดือน และไวรัสมันจะทำการค้นหาอย่างหนัก และลบประเภทของแฟ้มข้อมูลบางอย่าง (เช่น แฟ้มข้อมูลบริหารงาน หรือ .EXE) ของวินโดว์บนคอมพิวเตอร์ ผลกระทบของลูกระบิดของความมีเหตุผล และลูกระเบิดเวลาจะแสดงเป็นแถวข้อความที่น่ารำคาญบนจอเพื่อทำการแก้ไขให้ตรงกับเจตนาของฮาร์ดไดร์ฟ ซึ่งเป็นสาเหตุให้ข้อมูลสูญเสียโดยสมบูรณ์

2.2.14 การป้องกันคอมพิวเตอร์ : ซอฟต์แวร์ป้องกันไวรัส และซอฟต์แวร์ปรับให้ทันสมัย (Computer Safeguard: Antivirus Software and Software Updates) ซอฟต์แวร์บางชนิดปรากฏขึ้นเพียงแต่สร้างความรำคาญให้เพียงเล็กน้อยเท่านั้น เช่น การสุ่มด้วยการส่งภาพกราฟิกของรถพยาบาลข้ามไปที่ปุ่มหน้าจอ กรณีอย่างนี้เรียกว่า ไวรัสสภากาชาด (Red Cross virus) ไวรัสอื่นๆ บางชนิด มีลักษณะทำให้คอมพิวเตอร์ และเครือข่ายทำงานช้าลง หรือทำลายแฟ้มข้อมูลสำคัญ หรือทำลายเนื้อหาที่อยู่ในฮาร์ดไดร์ฟ วิธีการป้องกันไวรัสที่ดีที่สุดคือการติดตั้งซอฟต์แวร์ป้องกันไวรัส บริษัท Symantec, Kaspersky, AVG และ McAfee เป็นบริษัทที่เสนอขายซอฟต์แวร์ป้องกันไวรัสที่มีอัตราสูง การป้องกันไว้รัสรวมถึงชุดที่ครอบคลุมความปลอดภัยบนอินเทอร์เน็ตด้วย เช่น Norton Internet Security, Kaspersky Internet Security หรือ McAfee Total Protection ซึ่งเป็นชุดซอฟต์แวร์จะช่วยป้องกันคุณจากภัยคุกคามจากไวรัสคอมพิวเตอร์ได้เป็นอย่างดี

ซอฟต์แวร์ป้องกันไวรัส (Antivirus Software) ทำอย่างไร ฉันจะสามารถให้ซอฟต์แวร์ป้องกันไวรัสดำเนินงานได้บ่อยครั้ง? แม้ว่าซอฟต์แวร์ป้องกันไวรัสจะถูกออกแบบมาเพื่อป้องกันกิจกรรมที่ไม่น่าไว้ใจบนเครื่องคอมพิวเตอร์ของคุณตลอดเวลา คุณจะต้องตรวจสอบการดำเนินงานซอฟต์แวร์ป้องกันไวรัสในระบบของคุณอย่างแข่งขันอย่างน้อยอาทิตย์ละครั้ง ด้วยการกระทำดังนี้แฟ้มข้อมูลที่อยู่บนคอมพิวเตอร์ของคุณทั้งหมดจะถูกตรวจสอบการที่ไม่ได้ทำการป้องกันไวรัสเอาไว้ ซึ่งในการตรวจสอบดังกล่าวนี้มันจะต้องใช้เวลา คุณจะต้องปรับแต่งการดำเนินงานของซอฟต์แวร์ให้เป็นอัตโนมัติ เมื่อคุณไม่ได้ใช้ระบบของคุณ ยกตัวอย่าง เมื่อคืนที่ผ่านมา ทางเลือก ถ้าคุณสงสัยว่ามันจะมีปัญหา คุณสามารถดำเนินการตรวจสอบ และให้มันดำเนินงานได้ทันทีคุณว่าจะลบทิ้ง หรือซ่อมแซมแฟ้มข้อมูลที่ติดเชื้อนั้น หากโชคไม่ดี ที่ซอฟต์แวร์ป้องกันไวรัสนั้น ไม่สามารถซ่อมแซมแฟ้มข้อมูลที่ติดเชื้อได้นั้น ในการทำให้มันสามารถใช้การได้อีกครั้งหนึ่ง คุณต้องเก็บสำเนาสำรองข้อมูลที่วิกฤตินั้นเอาไว้ และคุณสามารถเรียกคืนกลับมาใหม่ได้ เพื่อป้องกันแฟ้มข้อมูลเสียหายหรือใช้การไม่ได้

ซอฟต์แวร์ป้องกันไวรัสส่วนใหญ่ จะพยายามขัดขวางการติดเชื้อ ด้วยการฉีดวัคซีนไปที่แฟ้มข้อมูลที่สำคัญของคุณ **การฉีดวัคซีน (inoculation)** คือการที่ซอฟต์แวร์ป้องกันไวรัสบันทึกคุณสมบัติที่สำคัญเกี่ยวกับแฟ้มข้อมูลบนคอมพิวเตอร์ของคุณ (เช่น ขนาดของแฟ้มข้อมูล และวันที่

สร้าง) และทำการเก็บสถิติเหล่านี้เอาไว้ในที่ซึ่งปลอดภัยบนฮาร์ดไดร์ฟของคุณ เมื่อมีการตรวจสอบไวรัส ซอฟต์แวร์ป้องกันไวรัสจะทำการเปรียบเทียบแฟ้มข้อมูลที่ถูกบันทึกคุณสมบัติที่ผ่านมาเอาไว้เพื่อช่วยป้องกันความพยายามของโปรแกรมไวรัสที่เข้ามาแก้ไขแฟ้มข้อมูลของคุณ

ซอฟต์แวร์ป้องกันไวรัสสามารถหยุดยั้งไวรัสได้เสมอหรือ? ซอฟต์แวร์ป้องกันไวรัสจะตรวจจับไวรัสอย่างมีประสิทธิผลเฉพาะไวรัสที่มันรู้จักเท่านั้น โชคไม่ดี ไวรัสใหม่ๆ ถูกเขียนมาตลอดเวลา การสู้รบกับไวรัสที่ไม่รู้จักเป็นเรื่องไม่ง่าย ซอฟต์แวร์ป้องกันไวรัสยุคใหม่ จะค้นหาไวรัสที่น่าสงสัย คล้ายกับที่มีลักษณะกิจกรรมที่มีสัญลักษณ์ไวรัสเท่านั้น อย่างไรก็ตาม ผู้เขียนไวรัสจะรู้ว่าซอฟต์แวร์ป้องกันไวรัสทำงานอย่างไร พวกเขาจึงทำการวัดพิเศษการปลอมแปลงรหัสไวรัสของเขาและซ่อนไวรัสที่ได้รับผลกระทบจนกระทั่งไวรัสนั้นได้แพร่กระจายไปอย่างรวดเร็ว และกระจายออกไป ดังนั้น คอมพิวเตอร์ของคุณสามารถถูกโจมตีโดยไวรัส ดังนั้น ซอฟต์แวร์ป้องกันไวรัสจะไม่สามารถจดจำได้ ในการลดความเสี่ยงเหล่านี้ คุณต้องทำการปรับซอฟต์แวร์ป้องกันไวรัสของคุณให้ทันสมัยอยู่เสมอ

ทำอย่างไร ฉันจึงสามารถแน่ใจได้ว่าซอฟต์แวร์ป้องกันไวรัสของฉันมีการปรับให้ทันสมัยอยู่เสมอ? ซอฟต์แวร์ป้องกันไวรัสส่วนใหญ่มีลักษณะปรับให้ทันสมัยอย่างอัตโนมัติ ด้วยการดาวน์โหลดการปรับให้ทันสมัยสำหรับแฟ้มข้อมูลที่มีสัญลักษณ์ของไวรัสทุกๆ ครั้งที่คุณเข้าถึงระบบออนไลน์

ฉันจะต้องทำอย่างไร ถ้าฉันคิดว่าคอมพิวเตอร์ของฉันติดเชื้อไวรัส? การปลุกเครื่องคอมพิวเตอร์ของคุณด้วยการใช้แผ่นดิสก์ติดตั้งซอฟต์แวร์ป้องกันไวรัส (ข้อสังเกต: ถ้าคุณดาวน์โหลดซอฟต์แวร์ป้องกันไวรัสของคุณจากอินเทอร์เน็ต มันเป็นความคิดที่ดีมากในการที่จะทำสำเนาซอฟต์แวร์ป้องกันไวรัสนั้นเก็บไว้ในแผ่นดีวีดี ในกรณีที่คุณมีปัญหาในอนาคต) ด้วยวิธีนี้ จะช่วยป้องกันโปรแกรมไวรัสทั้งหมดจากการโหลดมา และจะอนุญาตให้คุณดำเนินงานซอฟต์แวร์ป้องกันไวรัสได้โดยตรงที่แผ่นดิสก์ของคุณ ถ้าซอฟต์แวร์นั้นได้ตรวจสอบไวรัสแล้ว, คุณอาจต้องการค้นหามันต่อไปเพื่อที่จะระบุมัน ไม่ว่าซอฟต์แวร์ป้องกันไวรัสของคุณจะสามารถขจัดไวรัสออกไปได้อย่างสมบูรณ์หรือไม่ เว็บไซต์ซอฟต์แวร์ป้องกันไวรัสส่วนใหญ่ เช่น **Symantec.com** จะบรรจุไปด้วยสารสนเทศเกี่ยวกับไวรัสที่สำคัญเอาไว้ และจัดการแต่ละขั้นตอนของเงื่อนไขเพื่อลบไวรัสออกไป

โปรแกรมการส่งข้อความรีบด่วนปลอดภัยจากการโจมตีของไวรัสหรือ? การโจมตีด้วยไวรัส และอื่นๆ จากการมุ่งร้ายเจาะระบบสามารถทำผิดได้ผ่านโปรแกรมการส่งข้อความรีบด่วน เช่น Google Talk, Skype, Facebook Chat และ iChat ถึงแม้ว่าคุณจะมีการติดตั้งซอฟต์แวร์การป้องกันไวรัส คนอื่นก็ยังสามารถติดต่อคุณได้ด้วยวัตถุประสงค์เล่ห์กลเพื่อให้คุณเปิดเผยข้อมูลสารสนเทศที่อ่อนไหวให้รู้ ดังนั้น คุณต้องพยายามที่จะซ่อนกิจกรรมการส่งข้อความรีบด่วนของคุณ

จากทุกๆ คนยกเว้นคนที่คุณรู้จัก ในการเก็บการประชุมข้อความรีบด่วนของคุณให้ปลอดภัย คุณต้องระมัดระวังเอาไว้ก่อนด้วยการปฏิบัติตามขั้นตอนต่อไปนี้ :

อนุญาตการติดต่อให้เฉพาะผู้ใช้ที่อยู่ในรายการเป็นเพื่อนสนิทของคุณ (Allow contact only from users on your Buddy or Friends List) การขัดขวางอย่างนี้ จะทำให้คุณปลอดจากความรำคาญจากกลุ่มที่คนที่คุณไม่รู้จัก ในเฟซบุ๊กนั้น คุณจะต้องจำกัดสารสนเทศในโปรไฟล์ของคุณในการให้เปิดดูได้เฉพาะผู้ที่เป็นเพื่อนของคุณเท่านั้น และยอมรับการเป็นเพื่อนจากคนที่คุณรู้จักและเชื่อถือได้ในการจัดหน้าจอสำหรับโปรแกรมการส่งข้อความรีบด่วน (ดูรูปที่ 9.6) ที่เลือกอนุญาตให้เฉพาะผู้ใช้ในรายการเพื่อนสนิทของฉันเท่านั้น และแท้จริงแล้ว อย่าใส่ชื่อคนที่คุณไม่รู้จักและไม่น่าเชื่อถือลงไปในรายการเพื่อนสนิทของคุณ

ไม่รับข้อมูลที่ส่งต่อโดยอัตโนมัติมาอย่างเด็ดขาด (Never automatically accept Transfers of data) แม้ว่าการส่งแฟ้มวิดีโอรีบด่วน และข้อความรีบด่วนจะมีศักยภาพที่มีประโยชน์มากในการแลกเปลี่ยนแฟ้มข้อมูลกันผ่านการส่งข้อความรีบด่วน (ดูรูปที่ 9.6) แต่มันก็เป็นแนวทางการส่งแฟ้มข้อมูลที่มุ่งร้ายอย่างหนึ่ง ซึ่งอาจจะทำให้คอมพิวเตอร์ของคุณติดเชื้อไวรัสได้ การับข้อมูลที่ถูกส่งต่อโดยอัตโนมัติไม่ได้เป็นแนวความคิดที่ดีเลย

หลีกเลี่ยงโปรแกรมการส่งข้อความรีบด่วนบนคอมพิวเตอร์สาธารณะ (Avoid using instant messaging program on public computer) ถ้าคุณใช้คอมพิวเตอร์ที่มีการแบ่งปัน เช่น เครื่องคอมพิวเตอร์เครื่องหนึ่งในห้องปฏิบัติการคอมพิวเตอร์ของโรงเรียน ต้องแน่ใจว่า คุณไม่ได้เลือกลักษณะที่มีการจำรหัสผ่านของคุณ หรือติดต่อคุณอัตโนมัติ คนใช้คนต่อไปผู้ที่เข้าใช้คอมพิวเตอร์อาจจะสามารถติดต่อการบริการส่งข้อความรีบด่วนกับหน้าจอชื่อของคุณ (หรือหน้าบัญชีเฟซบุ๊กของคุณ) และอาจปลอมแปลงเป็นคุณได้

หนอน (Worms) เวิร์มหรือหนอน ไม่เหมือนกับไวรัสคอมพิวเตอร์ ซึ่งต้องอาศัยผู้ใช้ในการแพร่กระจายของไฟล์ที่ติดเชื้อไปยังผู้ใช้คนอื่นๆ เวิร์มหรือหนอนเป็นโปรแกรมที่เป็นอันตราย ซึ่งอาศัยอยู่ในหน่วยความจำของคอมพิวเตอร์ที่ทำงานอยู่ และทำการทำซ้ำด้วยตัวของมันเอง เวิร์มจะแตกต่างจากไวรัสคอมพิวเตอร์ นั่นก็คือเวิร์มสามารถแพร่พันธุ์หรือแพร่กระจายไป โดยปราศจากการแทรกแซงของมนุษย์, มีการส่งสำเนาด้วยตัวของมันเองไปยังคอมพิวเตอร์เครื่องอื่นโดยทางไปรษณีย์อิเล็กทรอนิกส์ หรือการสนทนาผ่านทางอินเทอร์เน็ต เวิร์มจะแตกต่างจากไวรัสเล็กน้อย นั่นคือ เวิร์มจะพยายามเดินทางไประหว่างระบบตลอดจนการเชื่อมต่อเครือข่าย ด้วยการกระจายไปทำให้ระบบติดเชื้อ แฟ้มของข้อมูลแม่ข่ายที่ติดเชื้อ และรอจนกระทั่งแฟ้มข้อมูลนั้นถูกบริหารบนเครื่อง

คอมพิวเตอร์เครื่องอื่นจึงทำการทำซ้ำหรือทำสำเนาใหม่ อย่างไรก็ตามเวิร์มจะทำงานด้วยตัวเอง เกี่ยวกับแฟ้มข้อมูลบริหารของแม่ข่าย และมีการกระจายไปอีกมากมายด้วยตัวของมันเอง เมื่อเวิร์มคอนฟิคเกอร์ (Conficker) ได้แตกกระจายแพร่ออก มันทำให้คอมพิวเตอร์ส่วนบุคคลติดเชื้ออย่างรวดเร็วประมาณ 9 ถึง 15 ล้านเครื่อง เวิร์มได้แพร่กระจายไปท่ามกลางความอ่อนแอของรหัสโปรแกรมวินโดว์ และการประนีประนอมของคอมพิวเตอร์ โดยทำให้การบริการของซอฟต์แวร์บางอย่างไร้ความสามารถ และซอฟต์แวร์อื่นที่เป็นประโยช์ (เช่น การปรับปรุงวินโดว์) ด้วยความโชคดี , มันเป็นการง่ายที่จะป้องกันคอมพิวเตอร์ของคุณจากเวิร์มให้มากที่สุด

การติดตั้งซอฟต์แวร์ป้องกันไวรัส (antivirus software) ซึ่งเป็นซอฟต์แวร์ที่ถูกออกแบบมาเป็นพิเศษในการตรวจสอบไวรัส และป้องกันคอมพิวเตอร์ของคุณ และแฟ้มข้อมูลจากอันตราย ซึ่งนับว่าเป็นการเริ่มต้นที่ดี คุณจะต้องสมัครในส่วนของ (เรื่องการปรับข้อมูลให้มีความทันสมัยจากบริษัทผู้ผลิตซอฟต์แวร์ เช่น วินโดว์ ซึ่งจะช่วยซ่อมแซมปัญหาความปลอดภัยที่มันรู้จัก) คอมพิวเตอร์ของคุณ เมื่อไหร่ก็ตามที่มันมีปัญหาเกี่ยวกับเรื่องเหล่านี้ เราจะได้อภิปรายเกี่ยวกับการวัดการป้องกันภายหลังบทนี้

ผลกระทบในทางลบของการโจมตีด้วยเวิร์ม คือ ทำให้คอมพิวเตอร์ขององค์กรได้รับความเสีย เช่น ทำให้ข้อมูล และโปรแกรมเสียหาย ทำให้การเพิ่มผลผลิตสูญหาย ทำให้ต้องเพิ่มความพยายามของคนทำงานด้านไอทีมากขึ้น นั่นคือ ต้องมีการกู้คืนข้อมูลและโปรแกรมที่เสียหายไปกลับมาใหม่ รวมไปถึงคนทำงานด้านไอทีต้องฟื้นฟู ทำความสะอาดเครื่องคอมพิวเตอร์ใหม่ เสียค่าใช้จ่ายไปในการซ่อมแซมรหัสโปรแกรมที่เสียหายไป เวิร์มที่ชื่อว่า SirCam และ Melissa คาดว่าจะเกิน $1 พันล้านดอลล่าร์สหรัฐ เมื่อรวมทั้งเวิร์มที่ชื่อ Conflicker, Storm และ ILOVEYOU ยอดรวมมากกว่า $5 พันล้านดอลล่าร์สหรัฐ

ภาพประกอบ 2.5 *แสดงประวัติความเป็นมาของม้าโทรจัน (Source: www.911review.com)*

ม้าโทรจัน (Trojan Horses) เป็นรหัสโปรแกรมที่มุ่งร้าย ซึ่งซ่อนตัวอยู่ภายใน ดูเหมือนว่าเป็นโปรแกรมไม่เป็นอันตรายผู้ใช้หลงเล่ห์เหลี่ยม ในการติดตั้งม้าโทรจันและทำให้เกิดอันตราย ม้าโทร

จันเป็นโปรแกรมที่ถูกออกแบบมาเพื่อให้ผู้เจาะระบบ สามารถทำลายฮาร์ดไดร์ฟ, ทุจริตไฟล์, ควบคุมระบบคอมพิวเตอร์, เปิดการโจมตีคอมพิวเตอร์เครื่องอื่น, ขโมยรหัสผ่าน, รหัสบัตรประกันสังคม หรือเลขที่บัตรประชาชน หรือสืบผู้ใช้คนอื่นๆ เพื่อที่จะบันทึกการเคาะแป้นพิมพ์ และทำการส่งข้อมูลเหล่านั้นไปยังเซิร์ฟเวอร์ที่ปฏิบัติการโดยบุคคลที่สาม ม้าโทรจันอาจถูกปล่อยมาผ่านการแนบอีเมล, การดาวน์โหลด, จากเว็บไซต์, ข้อสัญญา ผ่านการเคลื่อนย้ายอุปกรณ์สื่อ, หรือการเชื่อมต่อผ่านอุปกรณ์เคลื่อนย้าย เช่น ซีดีฝดีวีดี หรือ ยูเอสบีแฟลซไดร์ฟ ส่วนอีกประเภทหนึ่งของม้าโทรจันคือระเบิด ตรรกศาสตร์ (Logic bomb) ทำงาน เมื่อถูกกระตุ้น โดยเหตุการณ์ที่กำหนดไว้แน่นอน เช่น ระเบิดตรรกะสามารถเรียกมาให้เกิดโดยการเปลี่ยนแปลง โดยเฉพาะอย่างยิ่งไฟล์ โดยการเคาะแป้นพิมพ์ตามลำดับ หรือตามชนิดของวัน และเวลา

โดยปกติแล้วผู้เจาะระบบใช้คอมพิวเตอร์ส่วนบุคคลเป็นพื้นที่สำหรับการก่อกวน กระทำความผิดด้วยการโจมตีทางคอมพิวเตอร์อย่างแพร่หลาย ตัวอย่างเช่น ผู้เจาะระบบต้องการที่จะควบคุมคอมพิวเตอร์หลายๆ เครื่องในเวลาเดียวกัน พอเสร็จแล้ว ผู้เจาะระบบก็จะใช้ม้าโทรจันติดตั้งโปรแกรมอื่นๆ ลงบนคอมพิวเตอร์ **ม้าโทรจัน** คือ โปรแกรมที่แสดงตัวบางอย่างที่เป็นประโยชน์ และเป็นที่น่าต้องการ (อย่างเกม หรือผู้ช่วยให้หน้าจอปลอดภัย) แต่ในขณะที่มันทำงานบางอย่างเป็นการมุ่งร้ายต่อสิ่งแวดล้อมโดยปราศจากความรู้ของคุณ คำศัพท์ว่า *Trojan horse* เป็นแรงขับมาจากตำนานของกรีก และกล่าวถึงม้าไม้ที่ชาวกรีกที่ใช้แอบพาเข้าไปในเมืองทรอย และชนะสงคราม ดังนั้น โปรแกรมคอมพิวเตอร์ก็จะบรรจุด้วยสิ่งที่ซ่อนอยู่ (และโดยปกติแล้วเป็นสิ่งที่เลวร้ายมาก) “ประหลาดใจ” จึงใช้อ้างอิงเรียกชื่อว่า ม้าโทรจันม้าโทรจันทำให้อะไรเสียหาย? บ่อยครั้ง ที่กิจกรรมมุ่งร้ายทำผิดโดยม้าโทรจันโปรแกรม คือ การติดตั้งโปรแกรม วิถีทางที่ผิดกฎหมาย (backdoor program) ด้วยวิธีนี้ โปรแกรมจะอนุญาตให้ผู้เจาะระบบเข้าควบคุมคอมพิวเตอร์ทั้งหมดของคุณอย่างสมบูรณ์โดปราศจากความรู้ของคุณ การใช้โปรแกรมวิถีทางที่ผิดกฎหมายนี้ ผู้เจาะระบบสามารถเข้าถึง และลบแฟ้มข้อมูลที่อยู่บนคอมพิวเตอร์ของคุณทั้งหมด, การส่งไปรษณีย์อิเล็กทรอนิกส์, การดำเนินงานโปรแกรม, และทำอย่างอื่นๆ ทุกอย่างเหมือนกับคุณสามารถทำบนคอมพิวเตอร์ของคุณ วิธีการที่ผู้เจาะระบบเข้าควบคุมคอมพิวเตอร์นี้ถูกเรียกว่า **คนโง่หรือซอมบี้ (zombie)** ซอมบี้ถูกใช้ในการปฏิบัติการการโจมตีซึ่งปฏิเสธการให้บริการอยู่บ่อยครั้งบนคอมพิวเตอร์

โจมตีปฏิเสธการให้บริการ (Distributed Denial-of-Service (DDoS) Attacks) เป็นอีกโปรแกรมหนึ่งที่มุ่งร้าย คือ กระบวนการที่แฮ็กเกอร์สามารถที่เข้าไปควบคุมผ่านอินเทอร์เน็ต โดยที่พวกเขามีเป้าหมายต้องการที่จะให้ข้อมูลและข้อมูลขนาดเล็กท่วมท้นเว็บไซต์ การปฏิเสธการให้บริการแบ่งปันไม่ได้เกี่ยวข้องกับการแทรกซึมเป้าหมายของระบบ แต่มันเป็นการเข้าไปแทนที่ ทำให้ระบบเป้าหมายไม่ว่างในการตอบสนองต่อกระแสของการร้องขออัตโนมัติที่ผู้ใช้ถูกต้องตามกฎหมายร้องขอเข้ามา ผู้ใช้จึงไม่สามารถเข้าถึงข้อมูลในอินเทอร์เน็ตได้ การกระทำลักษณะนี้ มันจะ

ก่อกวนจัดการหมายเลขโทรศัพท์ที่ซ้ำแล้วซ้ำอีกเพื่อให้สายอื่น ๆ ทั้งหมดที่ได้ยินสัญญาณไม่ว่าง ผู้ใช้จึงไม่สามารถได้รับการให้บริการได้ กระบวนการที่เครื่องคอมพิวเตอร์ถูกเข้าทำการควบคุมเรียกว่าซอมบี้ หรือคนโง่ ส่วนบอทเน็ต (Botnet)เป็นกลุ่มที่มีขนาดใหญ่มากของเครื่องคอมพิวเตอร์ดังกล่าวมีบ่อยครั้งที่มีการใช้บอทเน็ตในการกระจายอีเมลขยะ และรหัสที่มุ่งร้าย ความสามารถในการประมวลผลเมื่อรวมกันเป็นกลุ่มใหญ่ของบอทเน็ตแล้ว มันเกินกว่าที่ซูเปอร์คอมพิวเตอร์ที่มีประสิทธิภาพมากที่สุดในโลกจะมีขีดความสามารถที่จะรองรับได้ โดยความเป็นจริงแล้วมันไม่ได้ไม่เกี่ยวข้องกับการหยุดการทำงานของเครื่องคอมพิวเตอร์เป้าหมาย แต่เครื่องคอมพิวเตอร์เป้าหมายจะมีสัญญาณไม่ว่างในการตอบสนองต่อกระแสของการร้องขอโดยอัตโนมัติ จึงทำให้ผู้ใช้ถูกต้องตามกฎหมายไม่สามารถเข้าถึงเครื่องคอมพิวเตอร์เป้าหมายได้ดังกล่าว

การโจมตีปฏิเสธการให้บริการคืออะไร? (What are denial-of-service attacks?) ในการโจมตีปฏิเสธการให้บริการ denial-of-service (DoS) attack คือ การที่ผู้ใช้ถูกต้องตามกฎหมายถูกปฏิเสธการเข้าถึงระบบคอมพิวเตอร์ เพราะว่าผู้เจาะระบบกระทำการร้องขอไปยังระบบคอมพิวเตอร์อย่างซ้ำๆ ผ่านไปยังคอมพิวเตอร์ของเขาหรือหล่อนผ่านซอมบี้ และคอมพิวเตอร์สามารถจัดการเฉพาะหมายเลขที่แน่นอนที่มีการร้องขอสารสนเทศในหนึ่งครั้ง เมื่อมันกระจายออกไปด้วยการร้องขอในการโจมตีปฏิเสธการให้บริการ คอมพิวเตอร์มันจะปิดลง และไม่ยอมรับคำถามจำนวนมากที่ร้องขอสารสนเทศเข้ามา แม้ว่าการร้องขอนั้นจะมาจากผู้ใช้ที่ถูกต้องตามกฎหมาย ดังนั้น คอมพิวเตอร์มันจะยุ่งมากจากการตอบสนองจากการปลอมร้องขอสารสนเทศเข้ามา ดังนั้นผู้ใช้ที่ถูกต้องตามกฎหมายนั้นจึงไม่สามารถเข้าถึงคอมพิวเตอร์ได้

การโจมตีปฏิเสธการให้บริการไม่สามารถถูกติดตามร่องรอยโดยคอมพิวเตอร์ที่ปฏิบัติการหรือ? การปฏิบัติการโจมตีด้วยปฏิเสธการให้บริการบนระบบคอมพิวเตอร์จากคอมพิวเตอร์เครื่องเดียวมันง่ายที่จะติดตามร่องรอย ดังนั้น ผู้เจาะระบบที่ฉลาดจะใช้การโจมตีปฏิเสธการให้บริการด้วยการปฏิบัติการโจมตีด้วย DoS จากซอมบี้หลายโปรแกรม (บางครั้งเป็นจำนวนพันซอมบี้) ในเวลาเดียวกัน รูปที่ 9.9 อธิบายถึงการทำงานของการโจมตีด้วย DoS ทำงานอย่างไร ผู้เจาะระบบสร้างหลายซอมบี้ และมีประสานงานกัน ดังนั้น เขาจึงเริ่มส่งคำร้องขอปลอมไปที่คอมพิวเตอร์เหมือนกันในเวลาเดียวกัน ผู้บริหารระบบซึ่งเป็นคอมพิวเตอร์เหยื่อ เขาได้มีการประสานงานที่แตกต่างกันใหญ่มากเพื่อที่จะหยุดจากการถูกโจมตี เพราะว่ามันมาจากคอมพิวเตอร์หลายๆ เครื่อง บ่อยครั้งการโจมตีได้ถูกประสานงานกันโดยอัตโนมัติโดยบ็อตเน็ต บ็อตเน็ต **(botnet)** คือ กลุ่มของโปรแกรมซอฟต์แวร์ที่ใหญ่มาก (ถูกเรียกว่า robots หรือ bots) ซึ่งจะมีการดำเนินงานโดยอัตโนมัติบนคอมพิวเตอร์ซอมบี้ บางบ็อตเน็ตเป็นที่รู้จักกันในการทอดข้ามคอมพิวเตอร์ 1.5 ล้านเครื่อง

การโจมตีด้วย DDoS เป็นปัญหาที่สาหัสมาก ในเดือนเมษายน ค.ศ. 2009 เว็บไซต์ของสหพันธรัฐนานาชาติแห่งโรงงานอุตสาหกรรมเครื่องเล่นจานเสียง (International Federation of the Phonographic Industry : IFPI) และ สมาคมผู้ให้สัญญาณรูปภาพเคลื่อนที่แห่งอเมริกา

(Motion Picture Association of America : MPAA)ถูกเป็นเป้าหมายโจมตี ในการคัดค้านการถูกพิพากษาลงโทษของอ่าวการละเมิดลิขสิทธิ์ของเขาเอง (ซึ่งเป็นเว็บไซต์แบ่งปันแฟ้มข้อมูลซึ่งมีชื่อไม่น่าเชื่อถือ) ในการปรับความช่วยเหลือในฐานะละเมิดลิขสิทธิ์ ในเดือนสิงหาคม ค.ศ.2009 เว็บเครือข่ายสังคมออนไลน์ รวมถึงทวิตเตอร์ และเฟซบุ๊ก ถูกเป็นเป้าหมายโจมตีด้วย DDoS โดยเฉพาะเป้าหมายที่ชัดเจนคือผู้เขียนบล็อก ผู้ใช้ที่มีประสบการณ์การใช้ทวิตเตอร์ และเฟซบุ๊ก ใช้เวลาในการเข้าถึงเว็บไซต์เป็นชั่วโมงในระหว่างการถูกโจมตี เพราะว่าเว็บไซต์จำนวนมากมีรายได้จากผู้ใช้โดยตรง (เช่น ผ่านการสมัครเป็นสมาชิกเกมออนไลน์) หรือโดยอ้อม (เช่น เมื่อมีการคลิกที่เว็บที่มีการโฆษณา) การโจมตีด้วย DDoS สามารถทำให้เว็บไซต์สถาบันด้านการเงินไม่มีความสุขจากการได้รับผลกระทบจากการโจมตีลักษณะนี้

รูทคิด (Rootkits) เป็นชุดของโปรแกรมชนิดหนึ่ง ที่มีความลึกลับและเป็นอันตรายออกแบบมาเพื่อซ่อนตัว หรือดำรงอยู่ในกระบวนการทำงานของคอมพิวเตอร์ สามารถช่วยให้ผู้ใช้หรือผู้โจมตีได้รับสิทธิพิเศษในการเข้าถึงเครื่องคอมพิวเตอร์ของผู้อื่นในระดับผู้ดูแล โดยปราศจากความยินยอมหรือความรู้ของผู้ใช้ปลายทาง คำว่า " ชุด " หมายถึง องค์ประกอบของซอฟต์แวร์ที่ใช้เป็นเครื่องมือในการโจมตี ส่วนคำว่า " rootkit " มีความหมาย เชิงลบ ผ่านการเชื่อมโยงกับมัลแวร์ ผู้โจมตีที่ใช้โปรแกรมรูทคิทนั้นสามารถได้รับการควบคุมอย่างเต็มรูปแบบของระบบและยังปิดบังสถานะของรูทคิทไว้ได้อีกด้วย รูทคิทเป็นโปรแกรมที่สามารถติดตั้งได้โดยอัตโนมัติ หรือสามารถโจมตีติดตั้งได้ทันที โดยอาศัยช่องโหว่จากรหัสผ่าน ปัญหาพื้นฐานที่เกิดขึ้น ก็คือ ระบบปฏิบัติการที่ทำงานอยู่ในปัจจุบัน ไม่สามารถที่จะทำให้เกิดความเชื่อมั่นว่า สามารถตรวจสอบและให้ผลการตรวจสอบรูทคิทที่ถูกต้องได้ เพราะการตรวจสอบรูทคิทถือว่าเป็นเรื่องยาก เนื่องจากรูทคิทสามารถที่จะล้มล้างซอฟต์แวร์ที่ทำหน้าที่ตรวจสอบ การแก้ปัญหาของรูทคิท ก็คือ การติดตั้งระบบปฏิบัติการใหม่และต้องเปลี่ยนฮาร์ดแวร์ หรือ อุปกรณ์พิเศษอื่นๆ ที่จำเป็น

ขยะไปรษณีย์อิเล็กทรอนิกส์หรือ สแปม (Spam) คือ ชื่อเรียกของการส่งข้อความที่ผู้รับไม่ได้ร้องขอ หรือไม่ได้รับเชิญของบุคคลเป็นจำนวนมาก ผ่านทางระบบอิเล็กทรอนิกส์ เป็นการส่งอีเมลในทางที่ผิด โดยส่วนมากจะทำให้เกิดความไม่พอใจต่อผู้รับข้อความ สแปมที่พบเห็นได้บ่อยได้แก่ การส่งสแปมผ่านทางอีเมล ในการโฆษณาชวนเชื่อ หรือโฆษณาขายของ โดยการส่งอีเมลประเภทหนึ่งที่เราไม่ต้องการ ซึ่งจะมาจากทั่วโลก โดยที่เราไม่รู้เลยว่า ผู้ที่ส่งมาให้นั้นเป็นใคร จุดประสงค์คือ ผู้ส่งส่วนใหญ่ต้องการที่จะโฆษณา สินค้าหรือบริการต่าง ๆ ของบริษัทของตนเอง ซึ่งเป็นประเภทหนึ่งของเมลขยะซึ่งนอกจากจะทำให้ผู้รับรำคาญใจและเสียเวลาในการกำจัดข้อความเหล่านี้แล้ว ผู้ที่นิยมใช้สแปมในการส่งข้อความเป็นเพราะมีต้นทุนต่ำ เป็นทฤษฎีหนึ่งในการทำการตลาด หรือบางครั้งเกิดมาจากงานหรือเว็บไซต์ลามก เราสามารถพบเห็นสแปมได้โดยทั่วไป บางครั้งสแปมส่งไปเพื่อให้ตอบแบบสอบเกี่ยวกับสินค้าและผลิตภัณฑ์ บางครั้งสแปมก็ถูกนำไปใช้โดยบริษัทที่ถูกต้องตามกฎหมายจำนวน

มาก สแปมยังทำให้ประสิทธิภาพการขนส่งข้อมูลบนอินเทอร์เน็ตลดลงด้วย สแปมในรูปแบบอื่นนอกจาก อีเมลสแปม ได้แก่ เมสเซนเจอร์สแปม นิวส์กรุ๊ปสแปม บล็อกสแปม และเอสเอ็มเอสสแปม การส่งสแปมเริ่มแพร่หลายเนื่องจากค่าใช้จ่ายในการส่งข้อความผ่านทางระบบอิเล็กทรอนิกส์ มีค่าใช้จ่ายน้อยมากเมื่อเทียบการการส่งข้อความชักชวนทางอื่น เช่นทางจดหมาย หรือการโฆษณาทางสื่อต่างๆ ทำให้ผู้ส่งประหยัดค่าใช้จ่ายในการส่งข้อความเชิญชวน และในขณะเดียวกันกฎหมายเกี่ยวกับระบบอิเล็กทรอนิกส์ที่เกี่ยวข้องกับสแปมยังไม่ครอบคลุม จนกระทั่งเริ่มมีใช้ครั้งแรกปี พ.ศ. 2546 (ค.ศ. 2003) ในประเทศสหรัฐอเมริกาหลายบริษัทได้ส่งออกขยะไปรษณีย์อิเล็กทรอนิกส์-สิ่งที่ไม่เป็นที่ต้องการ หรือไปรณีย์อิเล็กทรอนิกส์ที่โยนทิ้งแล้ว ค้นหาที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ของคุณหรือไม่ก็ค้นหาดูจากรายการซื้อสินค้า หรือซอฟต์แวร์ที่มองหาที่อยู่ไปรษณีย์อิเล็กทรอนิกส์บนอินเทอร์เน็ต (ข้อความรีบด่วนที่ไม่ได้เชิญซึ่งเป็นรูปแบบของขยะไปรษณีย์อิเล็กทรอนิกส์ ถูกเรียกว่าสปิม (spim) ถ้าคุณเคยใช้ที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ซื้อของหลายอย่างบนระบบออนไลน์, เปิดบัญชีออนไลน์, เข้าร่วมในเว็บเครือข่ายสังคมออนไลน์ เช่น เฟซบุ๊ก ในที่สุดที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ของคุณจะปรากฏอยู่บนหนึ่งในรายการที่จะได้รับขยะไปรษณีย์อิเล็กทรอนิกส์แนวทางหนึ่งในกาหลีกเลี่ยงขยะไปรษณีย์อิเล็กทรอนิกส์ในบัญชีพื้นฐานของคุณคือ การสร้างที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ฟรีของเว็บไซต์ ซึ่งคุณใช้ในตอนกรอกแบบฟอร์ม หรือซื้อรายการสินค้าบนเว็บไซต์ มีเว็บที่ให้บริการที่อยู่อีเมล 2 เว็บ คือ Windows Live Mail และ Yahoo! อนุญาตให้คุณติดตั้งบัญชีไปรษณีย์อิเล็กทรอนิกส์ฟรี ถ้าเว็บไซต์ฟรีอีเมลเหล่านั้นเต็มไปด้วยขยะไปรษณีย์อิเล็กทรอนิกส์ คุณสามารถที่จะยกเลิกบัญชีที่ไม่มีความสะดวกเล็กน้อยเหล่านั้น ถ้ามันมีความสะดวกที่จะยกเลิกคุณก็ควรจะยกเลิกที่อยู่ไปรษณีย์อิเล็กทรอนิกส์นั้น

อีกแนวทางหนึ่งในการหลีกเลี่ยงขยะไปรษณีย์อิเล็กทรอนิกส์คือ เครื่องกรอง เครื่องกรองขยะไปรษณีย์อิเล็กทรอนิกส์คือข้อเสนอหนึ่งที่คุณสามารถจะเลือกได้ในบัญชีที่อยู่อีเมลของคุณซึ่งคุณรู้หรือถูกสงสัยว่าข้อความขยะไปรษณีย์อิเล็กทรอนิกส์ซึ่งอยู่ในที่เก็บแฟ้มเอกสารนอกจากกล่องไปรษณีย์ของคุณ เว็บ 2 เว็บไซต์ที่มีข้อเสนอเครื่องกรอง คือ Office Live Mail และ Yahoo! แฟ้มข้อมูลที่ถูกรับรู้จะเป็นสแปมที่ถูกแยกออกจากกลุ่มในลักษณะที่เก็บเอกสารพิเศษ (ที่ถูกเรียกบ่อยๆ ว่า Spam หรือ Junk Mail) โปรแกรม Microsoft Outlook ก็มีข้อเสนอเครื่องกรองด้วยเหมือนกัน โปรแกรมที่หลายบริษัทผลิตรวมกัน จะมีการจัดการควบคุมบางอย่างเกี่ยวกับ สแปม รวมทั้งเว็บ SPAMfighter และ Cactus Spam Filter ทั้ง 2 เว็บนี้ สามารถถูกบรรจุอยู่ใน download.com

เครื่องกรองขยะไปรษณีย์อิเล็กทรอนิกส์ทำงานอย่างไร? เครื่องกรอง สแปม และซอฟต์แวร์การกรอง สามารถที่จะจับขยะไปรษณีย์อิเล็กทรอนิกส์ได้ถึง 95 เปอร์เซ็นต์ โดยตรวจสอบหัวข้อเรื่องอีเมลที่เข้ามา และที่อยู่ของผู้ส่งที่เกี่ยวข้องกับฐานข้อมูลเหตุการณ์ที่รู้ว่าเป็นสแปม เครื่องกรองสแปมก็เหมือนกัน มันก็จะตรวจสอบอีเมลของคุณสำหรับรูปแบบของสแปมที่ถูกใช้งานอยู่บ่อยๆ

และคำสำคัญ (เช่น คำว่า ฟรี และเกินกว่า 21) อีเมลนั้นก็จะกำหนดการกรองสแปมไม่ให้เข้าไปสู่กล่องไปรษณีย์ของคุณ แทนที่แหล่งเก็บเอกสารนั้นจะรับเอาสแปมไว้ เครื่องกรองสแปม ไม่ได้สมบูรณ์ทีเดียว คุณจะต้องตรวจสอบแหล่งเก็บเอกสารสแปมก่อนที่จะลบเนื้อหามันทิ้ง เพราะว่าอีเมลที่ถูกต้องตามกฎหมายอาจจะถูกลบทิ้งไปด้วยความผิดพลาด โปรแกรมส่วนใหญ่จะจัดการให้คุณด้วยเครื่องมือในการจำแนกกำหนดอีเมลที่เต็มไปด้วยสแปมใหม่อีกครั้ง

ทำอย่างไรอื่นอีกที่ฉันจะขัดขวางขยะไปรษณีย์อิเล็กทรอนิกส์? (How else can I prevent spam?) ยังมีแนวทางอื่นๆ เพิ่มเติมที่คุณสามารถขัดขวางสแปม :ก่อนการลงทะเบียนที่เว็บไซต์ อ่านมันเกี่ยวกับนโยบายความเป็นส่วนตัวเพื่อที่จะได้รู้ จะใช้ที่อยู่อีเมลของคุณอย่างไร อย่าอนุญาตให้เว็บไซต์นำที่อยู่อีเมลของคุณผ่านไปให้บุคคลที่ 3 อย่าตอบกลับสแปมในการที่จะลบคุณออกจากรายการสแปม ในการตอบกลับ อันจะเป็นการยืนยันว่า ที่อยู่อีเมลของคุณทำงานอยู่ แทนที่จะหยุดยั้งสแปม คุณอาจได้รับสแปมมากขึ้น

การสมัครสมาชิกการบริการส่งต่ออีเมล เช่น **emaillias.com** หรือ **sneakemail.com** การบริการนี้จะคัดกรองข้อความในไปรษณีย์อิเล็กทรอนิกส์ของคุณ การส่งต่อเพียงข้อความเหล่านี้คุณต้องกำหนดที่จะตกลงว่าจะรับ

ภาพประกอบ 2.6 *แสดงถึง แคปท์ชา (CAPTCHA) ซึ่งเป็นการทดสอบเข้าสู่ระบบคอมพิวเตอร์ (ที่มา: www.zdnet.com, 2019)*

ปัจจุบันได้มีการพัฒนา แคปท์ชา (CAPTCHA) คือการทดสอบเพื่อเข้าสู่ระบบคอมพิวเตอร์แบบโต้ตอบชนิดหนึ่ง เพื่อทดสอบว่าผู้ใช้งานเป็นมนุษย์จริงหรือไม่ (ว่าไม่ใช่บอตหรือโปรแกรมอัตโนมัติ) คำว่า CAPTCHA ย่อมาจาก "Completely Automated Public Turing test to tell Computers and Humans Apart" (การทดสอบของทัวริงสาธารณะแบบอัตโนมัติเพื่อแยกแยะว่าเป็นคอมพิวเตอร์กับมนุษย์อย่างสมบูรณ์) เป็นเครื่องหมายการค้าของมหาวิทยาลัยคาร์เนกีเมลลอน

สหรัฐอเมริกา คิดค้นขึ้นในปี ค.ศ. 2000 โดย ลูอิส วอน อาห์น (Luis von Ahn) แมนูล บลัม (Manuel Blum) นิโคลัส เจ. ฮอปเปอร์ (Nicholas J. Hopper) และ จอห์น แลงฟอร์ด (John Langford) (สามคนแรกมาจากมหาวิทยาลัย ส่วนคนสุดท้ายมาจากไอบีเอ็ม) ระบบ CAPTCHA เกี่ยวข้องกับคอมพิวเตอร์เครื่องหนึ่งซึ่งเป็นเครื่องแม่ข่าย จะถามผู้ใช้งานด้วยการทดสอบอย่างหนึ่งที่สร้างขึ้นมา และผู้ใช้จำเป็นต้องตอบให้ถูกต้องเพื่อให้สามารถเข้าสู่ระบบได้ แต่คอมพิวเตอร์เองนั้นไม่สามารถแก้ปัญหาที่ตัวมันเองสร้างขึ้นได้

สามารถตรวจได้แค่ว่าถูกหรือผิดตามที่ระบุไว้ตอนต้นเท่านั้น ระบบ CAPTCHA โดยทั่วไปจะให้ผู้ใช้ตอบคำถามด้วยการกดแป้นตัวอักษรตามที่ปรากฏในรูปภาพที่บิดเบี้ยว บางครั้งอาจมีการเพิ่มจุด แถบสี หรือเส้นหงิกงอลงในรูปภาพนั้น เพื่อวัตถุประสงค์ในการหลีกเลี่ยงการตรวจจับของโปรแกรมประเภทโอซีอาร์ ซึ่งอาจแก้ปัญหาที่ทดสอบได้โดยอัตโนมัติบางครั้งมีการอธิบายระบบ CAPTCHA ว่าเป็นการทดสอบของทัวริงแบบย้อนกลับ เพราะเป็นการทดสอบจากคอมพิวเตอร์ที่ส่งไปยังมนุษย์ ซึ่งในทางตรงข้าม การทดสอบของทัวริงเป็นการทดสอบจากมนุษย์ที่ส่งไปยังคอมพิวเตอร์หรือเครื่องจักรทัวริง CAPTCHA อาจใช้ในการตอบกลับฟอรั่มหรือเว็บบอร์ดสาธารณะทั่วไปตามอินเทอร์เน็ต ทั้งนี้เพื่อป้องกันบอตหรือโปรแกรมอัตโนมัติทำการส่งข้อความไม่พึงประสงค์ เช่น สแปม หรือโฆษณา กรรมวิธีนี้เป็นการทดสอบการบอกต่อไปยังคอมพิวเตอร์ และ โดยอัตโนมัติสมบูรณ์ โดยที่ไม่ได้มีเจตนา (Computers and Humans Apart : CAPTCHA) เป็นการทดสอบซอฟต์แวร์โดยทั่วไปว่า มนุษย์สามารถส่งผ่าน แต่โปรแกรมคอมพิวเตอร์ไม่สามารถส่งผ่าน

ภาพประกอบ 2.7 *แสดงถึงวิธีการใช้โปรแกรมเหยื่อล่อปลาให้เข้ามาติดเบ็ด*

(ที่มา: www.wit279.wordpress.com, 2019)

โปรแกรม CAPTCHA: ช่วยเก็บรักษาเว็บไซต์ให้ปลอดภัยจากการโกง โปรแกรมอัตโนมัติที่ถูกเรียกว่า bots (or Web robots) ถูกใช้ให้ทำงานง่ายๆ บนอินเทอร์เน็ต โปรแกรมการค้นหาข้อมูลใช้บอทเป็นเทคนิคที่ถูกเรียกว่า แมงมุม (spidering) ในการค้นหา และดรรชนีของเว็บเพจ, โชคไม่ดี, บอทสามารถถูกใช้เพื่อมุ่งร้าย หรือวัตถุประสงค์ในทางที่ผิดกฎหมาย เพราะว่า บอทเหล่านี้สามารถทำงานการคำนวณบางอย่างที่เร็วมากกว่ามนุษย์ ตัวอย่างเช่น บอทสามารถใช้ในการสั่งซื้อตั๋ว

จากเว็บไซต์ และพยายามที่จะซื้อช่วงตึกให้ใหญ่มากขึ้นของความต้องการที่สูงของตั๋วเข้าชมดนตรี หรือการทำซ้ำเพื่อเข้าไปแข่งขันในความพยายามที่จะเพิ่มโอกาสของการชนะพนัน หรือรางวัล ที่พบบ่อยๆ บอทถูกใช้ประกาศขยะไปรษณีย์อิเล็กทรอนิกส์ในภาคของการแสดงความคิดเห็นของบล็อก โชคดีที่ผู้เป็นเจ้าของเว็บไซต์สามารถใช้ซอฟต์แวร์ทำการแปรแถวที่รู้จักกันในนามโปรแกรม CAPTCHA ในการป้องกันกิจกรรมของบอท

CAPTCHA (Completely Automate Public Turing Test to Tell Computers and Humans Apart) เป็นโปรแกรมทั่วไปที่ทำให้ข้อความผิดรูป และต้องการให้มีการพิมพ์ลงไปในกล่องข้อความ เพราะว่าบอทยังคงไม่สามารถถูกเขียนโปรแกรมให้การอ่านข้อความที่ผิดรูป ซึ่งประชาชนส่วนใหญ่มักนิยมใช้ โปรแกรม CAPTCHA ถูกใช้ในการตรวจสอบว่า มนุษย์ทำงานอะไร และอะไรที่เขาถูกทดสอบอยู่ โปรแกรมนี้จะช่วยผู้ที่เป็นเจ้าของเว็บไซต์ในการต่อต้านในการได้รับประเภทของเล่ห์อุบายอัตโนมัติ ถ้าคุณต้องการที่จะบูรณาการโปรแกรม CAPTCHA ที่เว็บไซต์ของคุณ (ในการป้องกันที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ของคุณ), ให้เข้าไปที่เว็บไซต์ recaptcha.net , ซึ่งมีข้อเสนอเครื่องมือ CAPTCHA ฟรี ในการที่จะช่วยปกป้องข้อมูลของคุณ

แพ็คเก็ตสนิฟเฟอร์คืออะไร? (What's a packet sniffer?) ข้อมูลที่เดินทางไปบนอินเทอร์เน็ตชิ้นเล็กๆ แต่ละชิ้นถูกเรียกว่า กลุ่มหรือหีบห่อ (packet) แพ็คเก็ตจะถูกกำหนดด้วย IP address ซึ่งเป็นส่วนที่ช่วยกำหนดคอมพิวเตอร์ซึ่งเป็นตัวที่ส่งข้อมูล แพ็คเก็ตหนึ่งจะเอื้อมไปที่ปลายทางของมัน พวกมันจะรวมตัวกันใหม่ให้มีข้อความติดอยู่ด้วยกัน **แพ็คเก็ตสนิฟเฟอร์** คือโปรแกรมคอมพิวเตอร์ที่ถูกแปรแถวโดยผู้เจาะระบบที่กำลังมองหา (หรือคนที่สูดจมูก) แต่ละแพ็คเก็ตที่มันเดินทางไปอยู่บนอินเทอร์เน็ต ไม่เพียงแต่คอมพิวเตอร์ที่มีที่อยู่เท่านั้น แต่ว่าทุกแพ็คเก็ต แพ็คเก็ตสนิฟเฟอร์บางชนิดถูกปรับแต่งโดยการดึงแพ็คเก็ตทั้งหมดในหน่วยความจำ เพราะเหตุว่ามันจะดึงเอาเฉพาะแพ็คเก็ตที่บรรจุด้วยเนื้อหาเฉพาะแต่ละชนิด (เช่น หมายเลขบัตรเครดิต) โดยเฉพาะ เครือข่ายไร้สายเสี่ยงจากการแสวงหาผลประโยชน์จากประเภทนี้ เพราะว่ามีประชาชนจำนวนมากที่เขาไม่ได้สร้างรหัสลับของข้อมูล เมื่อเขาทำการติดตั้งเครือข่ายไร้สายของเขา ผู้เจาะระบบอาจจะนั่งอยู่ที่ร้านกาแฟและเชื่อมต่อเครือข่ายไร้สายอยู่ และให้แพ็คเก็ตสนิฟเฟอร์ดำเนินงานดึงข้อมูลจากคนอื่น ผู้ซึ่งใช้เครือข่ายไร้สาย วิธีการทำเช่นนี้มันง่ายสำหรับผู้เจาะระบบในการดัก และอ่านสารสนเทศที่มีความอ่อนไหวซึ่งถูกส่งไปโดยปราศจากการสร้างรหัสลับ เช่น หมายเลขบัตรเครดิต หรือ เนื้อหาของไปรษณีย์อิเล็กทรอนิกส์

ผู้เจาะระบบทำอะไรกับสารสนเทศด้วย "สนิฟเฟอร์"? สิ่งหนึ่งที่ผู้เจาะระบบมีคือสารสนเทศบัตรเครดิตของคุณ เขาหรือหล่อนสามารถใช้มันซื้อสิ่งของที่ผิดกฎหมายหรือขายหมายเลขให้กับใครบางคนที่เขาต้องการ ถ้าผู้เจาะระบบขโมยหมายเลขการเข้าสู่ระบบ และรหัสผ่านบัญชีเพื่อรู้ว่าคุณมีสารสนเทศบัตรเครดิตถูกจัดเก็บไว้ในที่ไหน (เช่น ใน ebay หรือ amazon) เขาหรือหล่อนสามารถใช้ชื่อบัญชีของคุณซื้อรายการสินค้า และให้ทำการส่งสินค้าให้เขาหรือหล่อนแทนที่จะเป็นคุณ

ถ้าผู้เจาะระบบรวบรวมสารสนเทศบัตรเครดิตของคุณได้มากพอแล้ว เขาอาจสามารถกระทำความผิดด้วยการขโมยอัตลักษณ์

การหลอกลวงทางอินเทอร์เน็ต หรือ ฟิชชิง (Phishing) ฟิชชิง คือ เป็นการใช้อีเมลตลบตะแลง โดยพยายามให้ผู้รับทำการเปิดเผยข้อมูลส่วนบุคคลออกมา เช่น รหัสผ่านหรือหมายเลขบัตรเครดิต, ชื่อและชื่อผู้ใช้ที่อยู่และหมายเลขโทรศัพท์,รหัสผ่านหรือ PIN, หมายเลขบัญชีธนาคาร, บัตรเดบิต/บัตรเอทีเอ็ม, รหัสการตรวจสอบความถูกต้องของการ์ด (CVC) หรือค่าการตรวจสอบการ์ด (CVV) หมายเลขประกันสังคม (SSN) เป็นต้น ซึ่งเป็นเสมือนการใช้เหยื่อเกี่ยวเบ็ดเพื่อล่อปลาให้มาติดเบ็ด หรือการปลอมแปลงอีเมลจากเหล่าแฮกเกอร์ โดยจะทำให้เหมือนว่า ถูกส่งมาจากจากเว็บไซต์ที่ทำธุรกรรมด้านค้าขายทางอินเทอร์เน็ต เว็บไซต์ทำการประมูลซื้อขายทางออนไลน์ ธนาคาร และแหล่งสินเชื่อบัตรเครดิต เช่น Citibank eBay และ PayPal ลักษณะการหลอกหลวงได้แก่ ส่งอีเมล์ไปตามเหล่าสมาชิกหรือลูกค้าเหล่านั้น รวมถึงการส่งข้อความมาทาง Messenger เป็นลิงค์ให้เข้าไปยังเว็บหลอกที่ถูกสร้างขึ้นมาเหมือนกับเว็บของจริง เพื่อให้เหยื่อกรอกข้อมูลส่วนตัว เช่น User Name} Password หมายเลขบัตรเครดิตต่างๆ ที่นี้เมื่อเหยื่อกรอกข้อมูลลงไปแล้ว พวกแฮกเกอร์ก็จะนำข้อมูลเหล่านั้นไปใช้หาผลประโยชน์ต่ออีกที ทำให้ความเสียหายตกอยู่กับเจ้าของข้อมูลเหล่านั้น ซึ่งพฤติกรรมเหล่านี้ก็คล้ายกับการอ่อยเหยื่อตกปลา โดยหวังให้ปลามาฮุบเหยื่อไปกิน

การหลอกลวงทางอินเทอร์เน็ต (อ่านออกเสียงว่า “ฟิชชิง”) เป็นการหลอกล่อผู้ใช้อินเทอร์เน็ตเพื่อขโมยสารสนเทศส่วนบุคคล เช่น หมายเลขบัตรเครดิต, หมายเลขบัตรประกันสังคม หรือสารสนเทศที่อ่อนไหวอื่นๆ ซึ่งก่อให้เกิดการขโมยอัตลักษณ์ บุคคลผู้สร้างเล่ห์อุบายจะส่งข้อความไปทางอีเมล์ว่า เป็นเหมือนพวกเขาดำเนินธุรกิจถูกต้องตามกฎหมาย เช่น ธนาคารออนไลน์ สภาพของอีเมลนั้นผู้รับต้องการปรับให้ทันสมัย หรือให้ยืนยันว่าเขาหรือเธอต้องการปรับสารสนเทศทางบัญชีให้ทันสมัย เมื่อผู้รับคลิกลิงค์จัดการ, เขา หรือเธอก็จะเข้าสู่เว็บไซต์ เว็บไซต์นั้นดูคล้ายจะถูกต้องตามกฎหมาย แต่จริงๆ แล้วคือการหลอกลวงคัดลอกด้วยเล่ห์อุบายที่ถูกสร้างขึ้น ประการหนึ่งเมื่อผู้รับอีเมลยืนยันสารสนเทศของเขาหรือเธอ ผู้สร้างเล่ห์อุบายนี้ก็จะทำการจับเอาสารสนเทศเหล่านั้น และสามารถที่จะเริ่มใช้งานมันได้

มีประเภทของเล่ห์อุบายการหลอกลวงทางอินเทอร์เน็ตหรือ? การรักษานั้นมีเงื่อนงำมากกว่าการหลอกลวงทางอินเทอร์เน็ต การหลอกลวงทางอินเทอร์เน็ตต้องการการกระทำในเชิงบวกโดยบุคคลผู้ใช้เล่ห์อุบาย เช่น การเข้าไปสู่เว็บไซต์ อ้างถึงอีเมล และการพิมพ์สารสนเทศในบัญชีธนาคารของคุณ **ส่วนเล่ห์อุบายการปลอมแปลง (Pharming)** เป็นรหัสมุ่งร้ายที่ถูกปลูกอยู่ในคอมพิวเตอร์ของคุณ ซึ่งสามารถปรับเปลี่ยนความสามารถของบราวเซอร์ในการค้นหาที่อยู่ของเว็บ

ผู้ใช้จะถูกแนะนำด้วยในการปลอมเว็บไซต์ แม้ว่าเขาเข้าไปสู่ที่อยู่ที่ถูกต้องของเว็บไซต์จริง หรืออนุญาตให้ทำการคั่นหน้าเว็บ นั่นหมายถึงว่าเขาได้สร้างสำหรับเว็บไซต์ที่ผ่านมาแล้ว ดังนั้น มันจะเข้าไปแทนที่ในที่สุดที่เว็บไซต์ธนาคารของคุณ เมื่อคุณพิมพ์ข้อมูลลงไปในเว็บ ในที่สุดคุณก็จะถูกปลอมแปลงเว็บไซต์ ซึ่งเหมือนกับเว็บไซต์ธนาคารของคุณ แต่มันจะทำการติดตั้งอย่างรวดเร็ว เพื่อวัตถุประสงค์ในการรวบรวมข้อมูล

ทำอย่างไรฉันจะสามารถหลีกเลี่ยงสาเหตุโดยการหลอกลวงทางอินเทอร์เน็ต และเล่ห์อุบาย?คุณจะต้องไม่เคยตอบกลับโดยตรงทุกอีเมลที่ถามสารสนเทศส่วนบุคคลของคุณ คุณต้องไม่เคยคลิกลิงค์ในอีเมลเพื่อให้เข้าไปสู่เว็บไซต์ แทนที่จะพิมพ์ชื่อที่อยู่ของเว็บไซต์ในเว็บบราวเซอร์ ตรวจสอบบริษัทที่ถามสารสนเทศของคุณ และให้เพียงสารสนเทศ ถ้าคุณไว้วางใจได้ว่าถูกต้องการเหมือนกัน, คุณต้องไม่เคยให้สารสนเทศส่วนบุคคลผ่านอินเทอร์เน็ต ถ้าคุณไม่รู้จักว่าเว็บไซต์นั้นปลอดภัย มองหาแพสล็อกปิด, https, หรือตราสัญลักษณ์ที่ได้รับการรับรอง เช่น VeriSign ในการช่วยเรียกความมั่นใจของคุณว่าเว็บไซต์นั้นปลอดภัย เวอร์ชั่นล่าสุดของ Firefox, Chrome, และ Internet Explorer มีการสร้างกลั่นกรองการหลอกลวงทางอินเทอร์เน็ตด้วย ดังนั้น แต่ละครั้งที่คุณเข้าถึงเว็บไซต์ ที่กลั่นกรองการหลอกลวงทางอินเทอร์เน็ตจะตรวจสอบเว็บไซต์ว่าถูกต้องตามกฎหมายหรือไม่ และเตือนคุณในสิ่งที่เป็นไปได้ในการปลอมแปลงเว็บไซต์ ท้ายที่สุด ต้องแน่ใจว่า คุณมีการติดตั้งซอฟต์แวร์รักษาความปลอดภัยทางอินเทอร์เน็ต และมีการปรับให้ทันสมัยอยู่อย่างสม่ำเสมอ ส่วนใหญ่ชุดของความปลอดภัยบนอินเทอร์เน็ตสามารถป้องกัน และขัดขวางการโจมตีด้วยเล่ห์อุบายชุดของความปลอดภัยทางอินเทอร์เน็ตหลักๆ ตัวอย่างเช่น McAfee และ Norton เหล่านี้เป็นเครื่องมือข้อเสนอการป้องกันการหลอกลวงทางอินเทอร์เน็ต เมื่อคุณมีโปรแกรม Norton ที่แถบเครื่องมือจะแสดงที่บราวเซอร์ของคุณ คุณก็จะถูกแจ้งสม่ำเสมอเกี่ยวกับเว็บไซต์ที่ถูกต้องตามกฎหมายที่คุณเข้าไปเยี่ยมชมอีกอย่างหนึ่งในการป้องกันของคุณเอง คุณต้องไม่เคยใช้หมายเลขบัตรเครดิต เมื่อคุณซื้อสินค้าทางออนไลน์ ถึงแม้ว่า ดูเหมือนว่ามันจะเป็นไปไม่ได้ ผู้ให้บริการบัตรเครดิต เช่น Citibank จะมีข้อเสนอการบริการ เช่น “หมายเลขบัญชีโดยแท้จริง” สำหรับลูกค้าของเขา ก่อนที่คุณจะซื้อสินค้าทางออนไลน์, คุณเข้าไปเยี่ยมเว็บไซต์ออนไลน์ ที่ไหนที่คุณถูกมอบหมายซึ่งหมายเลขบัญชีใหม่เสมือนจริงในแต่ละครั้งที่คุณเข้าไปเยี่ยมชม หมายเลขนี้มันเหมือนหมายเลขบัตรเครดิตโดยปกติ และ มันก็จะวุ่นวายไปที่หมายเลขบัตรเครดิตที่แท้จริงของคุณ อย่างไรก็ตาม หมายเลขบัญชีเสมือนจริงสามารถถูกใช้เพียงครั้งเดียว นั่นหมายความว่า หมายเลขนั้นเป็นของโจร มันไม่ดีในการขโมย พวกเขาไม่สามารถใช้บัญชีเสมือนจริง เพราะว่าคุณได้ใช้มันเรียบร้อยแล้ว

ประเภทของการหลอกลวงทางอินเทอร์เน็ต

- แบบสร้างลิงค์หลอกไปยังเว็บไซต์ที่สร้างขึ้นมาเพื่อให้เหยื่อหลงกรอกข้อมูล

- แบบรูปภาพแล้วทำลิงค์ไปยังเว็บไซต์ เพื่อหลบหลีกโปรแกรมที่ช่วยกรอกข้อมูลที่เป็น Phishing
- แบบเว็บไซต์ที่สร้างขึ้นมา เพื่อให้เหยื่อหลงไปสมัครสมาชิกแล้วกรอกข้อมูลต่างๆ ลงไป เพื่อสมัครแล้วถึงจะเข้าเว็บไซต์นั้นได้
- แบบโทรศัพท์หาเหยื่อ ลักษณะแบบนี้จะแอบอ้างมาว่า ในช่วงเวลานี้เหยื่ออาจจะไม่สามารถเข้าไปยังเว็บที่ตัวเองต้องทำธุรกรรมต่างๆ ได้ แต่ถ้าหากต้องการใช้งานนั้นก็เพียงแต่บอกกับเจ้าหน้าที่ที่โทรศัพท์มาหา แล้วให้รายละเอียดเกี่ยวกับข้อมูลของตนไป ก็จะใช้งานได้ตามปกติ
- เป็นการมองหาอีเมลของผู้ใช้ที่ถูกต้องตามกฎหมาย แล้วทำการปลอมแปลงเว็บไซต์
- หอก-ตะลบตะแลง (Spear-phishing) เป็นการตลบตะแลงอีเมลของพนักงานในองค์กร
- การหลอกลวง (Smishing) เป็นการหลอกลวงผ่านข้อความตัวหนังสือ
- การอวตาล (Vishing) เป็นการหลอกลวงผ่านไปรษณีย์เสียง

การป้องกันโดนการหลอกลวงทางอินเทอร์เน็ต

- ใช้โปรแกรมกรองข้อมูลจากในบราวเซอร์ เวอร์ชั่นใหม่ๆ ของ IE และ Mozilla Firefox
- สังเกตว่า เว็บนั้นมีสัญลักษณ์ของการป้องกันและรักษาความปลอดภัยของข้อมูลหรือไม่
- คอยติดตามข่าวคราวของเรื่องการโดน Phishing (พิษณุ ปุระศิริ : 2552) 15/12/2013)

ตัวอย่าง กรณีศึกษาของการหลอกลวงทางอินเทอร์เน็ต

สำนักข่าว The Guardian รายงานว่านักวิเคราะห์ออกมาประกาศเตือนภัยยูสเซอร์ ถึงวิวัฒนาการของกระบวนการฟิชชิ่ง (Phishing) เทคนิคล่าสุดที่พบในการสำรวจตัวอย่างการโจรกรรมข้อมูลแบบฟิชชิ่ง คือการอาศัยโปรแกรมม้าโทรจัน (Trojan horse) เป็นเครื่องมือในการส่งตรงหน้าเว็บไซต์ปลอมของธนาคาร ให้ปรากฏบนหน้าจอของยูสเซอร์ ฟิชชิ่งเป็นพฤติกรรมการหลอกลวงผ่านทางเครือข่ายอินเตอร์เน็ตเพื่อล้วงข้อมูลส่วนตัว ที่ผ่านมาวิธีการฟิชชิ่งจะเริ่มต้นจากการสุ่มส่งอีเมล์ไปยังสมาชิกของผู้ให้บริการอินเตอร์เน็ต (ไอเอสพี) หรือบริษัทการเงินที่น่าเชื่อถือ เนื้อหาในอีเมล์ที่ส่งไปมักจะขอให้ผู้เป็นสมาชิกติดต่อกลับ เช่นการโกหกว่าขณะนี้มีการเบิกเงินเกินจำนวน ทำให้ยูสเซอร์ต้องรีบเข้าไปตรวจสอบ ซึ่งกระบวนการตรวจสอบย่อมจะต้องใช้รหัสผ่าน หรือข้อมูลลับเฉพาะอื่นๆ โดยจะมีเว็บเพจที่ต้องการให้ติดต่อกลับระบุไว้ในตอนท้ายของอีเมล์ สุดยอดของกลลวงฟิชชิ่งคือการลวงโดยใช้ URL เดียวกันกับเว็บไซต์แท้ของบริษัทชื่อดังที่คนส่วนใหญ่รู้จัก ทำให้ยูสเซอร์หลงเชื่อคลิกเข้าไปที่เว็บเพจดังกล่าว โดยจะเชื่อมต่อไปยังเว็บไซต์ที่ถูกเลียนแบบให้มีรูปลักษณ์หน้าตาคล้ายคลึง

กับเว็บไซต์แท้บริษัทนั้นมากในหน้าเว็บไซต์ปลอม จะมีข้อความให้ยูสเซอร์กรอกรายละเอียดข้อมูลลับต่างๆ ไม่ว่าจะเป็นรหัสผ่านหรือหมายเลขบัตรเครดิต กลลวงฟิชชิ่งนี้สร้างความเสียหายให้กับสถาบันการเงินทั่วโลกหลายล้านปอนด์ต่อปี (www. http://hitech.sanook.com) 21/01/2019)

มัลแวร์คืออะไร? (What is Malware?) มัลแวร์ คือซอฟต์แวร์ที่มีเจตนามุ่งร้าย (ดังนั้น จึงมีคำนำหน้าว่า มัล) ซอฟต์แวร์มัลแวร์พื้นฐานมี 3 รูปแบบ คือ แอดแวร์, สปายแวร์ และไวรัส (ซึ่งได้อภิปรายไปเรียบร้อยแล้ว) แอดแวร์ และสปายแวร์ มีการทำลายไม่เป็นรูปธรรมเหมือนกับไวรัสและเวิร์ม (หนอน) ซึ่งสามารถทำลายข้อมูล เป็นที่รู้จักกันในกลุ่ม เกรแวร์ (Grayware) ส่วนใหญ่เป็นเครื่องมือ, การสร้างความรำคาญ หรือเป็นโปรแกรมที่สร้างความไม่พอใจ ซึ่งถูกดาวน์โหลดไปที่คอมพิวเตอร์ของคุณ เมื่อคุณติดตั้ง หรือใช้เนื้อหาออนไลน์ เช่น โปรแกรม Freeware หรือฟรีแวร์ (โปรแกรมที่มีการจดลิขสิทธ์ แต่อนุญาตให้คัดลอกได้โดยไม่คิดเงิน), เกม หรือสิ่งที่เป็นประโยชน์อื่นๆ

แอดแวร์คืออะไร? (What is Adware?) แอดแวร์คือซอฟต์แวร์ที่แสดงการโฆษณาของผู้สนับสนุนในหมวดของหน้าต่างเว็บบราวเซอร์ของคุณ หรืออันเป็นกล่องโฆษณาที่เป็นป๊อปอัพ แต่มันถูกพิจารณาว่าถูกต้องตามกฎหมาย (ถึงแม้ว่า บางครั้งมันจะสร้างความรำคาญ) อันเป็นวิธีการสร้างรายได้ทั่วไปสำหรับผู้พัฒนาระบบนี้ขึ้นมา ผู้ซึ่งไม่ได้มีค่าปรับสำหรับซอฟต์แวร์ และสารสนเทศของเขา หน้าต่างป๊อปอัพ (กล่องเล็กๆ ที่เปิดอัตโนมัติบนหน้าจอของคุณ) มีการอ้างอิงถึงประกาศหรือโฆษณาบนอินเทอร์เน็ต เพราะว่า มันจะปรากฏ และแสดงการโฆษณา หรือการส่งเสริมสารสนเทศอื่นๆ เมื่อคุณติดตั้งโปรแกรมฟรีแวร์ หรือเข้าถึงเว็บแน่นอน ณ จุดนี้หน้าต่างของป๊อปอัพจะเป็นแบบธรรมดา ซึ่งทำให้มันไม่น่าเชื่อถือ ทำให้โมโห และน่ารำคาญอย่างไรก็ตาม, บางหน้าต่างป๊อปอัพ, มันถูกต้องตามกฎหมาย และเพิ่มหน้าที่การประดิษฐ์คิดค้นขึ้นที่หน้าเว็บไซต์ ตัวอย่างเช่น ยอดบัญชีเงินคงเหลือของคุณอาจจะมีหน้าต่างป๊อปอัพเกิดขึ้นที่เว็บไซต์ธนาคารของคุณ โชคดี เพราะว่าเว็บบราวเซอร์อย่างไฟร์ฟอกซ์ , ซาฟารี, และอินเทอร์เน็ตเอ็กพลอเรอร์มีการสร้างป๊อปอัพกีดขวางที่เว็บบราวเซอร์ของเขา ความรำคาญของป๊อปอัพที่เกิดขึ้นก็จะช่วยลดความรำคาญได้อย่างมาก คุณสามารถเข้าถึงการติดตั้งป๊อปอัพผู้กีดขวางในบราวเซอร์ของคุณ และเพิ่มเว็บไซต์ ซึ่งคุณจะอนุญาตป๊อปอัพ เมื่อป๊อปอัพถูกกีดขวาง บราวเซอร์จะไม่แถบแสดงสารสนเทศที่อยู่ด้านบนของหน้าต่างบราวเซอร์ หรือแจ้งการเล่นเสียงไปที่คุณ ถ้าคุณรู้สึกว่า ป๊อปอัพนั้นมันถูกต้องตามกฎหมาย คุณสามารถปิดการรับมันได้

สปายแวร์คืออะไร? (What is Spyware?) สปายแวร์ คือโปรแกรมที่ไม่พึงประสงค์ที่อาศัยมาด้วย โดยปกติแล้วจะมาจากการดาวน์โหลดซอฟต์แวร์อื่นๆ ที่คุณต้องการติดตั้งจากอินเทอร์เน็ต มันจะดำเนินงานอยู่บนฉากหลังในระบบของคุณ ถ้าคุณไม่มีความรู้ สปายแวร์จะส่งสารสนเทศ

เกี่ยวกับคุณ เช่น นิสัยการเล่นอินเทอร์เน็ตของคุณ ไปจนถึงการเป็นเจ้าของซอฟต์แวร์ ดังนั้น สารสนเทศเหล่านั้นสามารถถูกใช้เพื่อเป็นวัตถุประสงค์ทางการตลาด มีโปรแกรมสปายแวร์จำนวนมากใช้คุกกี้ติดตาม (แฟ้มข้อมูลข้อความขนาดเล็กที่ถูกจัดเก็บอยู่บนคอมพิวเตอร์ของคุณ) ในการรวบรวมสารสนเทศ ในทางตรงกันข้ามอื่นๆ มันจะถูกปลอมแปลงให้เป็นโปรแกรมที่มีลักษณะดี ซึ่งแท้ที่จริงแล้วมันเป็นโปรแกรมที่มุ่งร้าย (เช่น ม้าโทรจัน) มีโปรแกรมสปายแวร์อีกชนิดหนึ่งซึ่งเป็นที่รู้จักกันในชื่อ **Keystroke Logger** ซึ่งจะติดตามการเคาะแป้นพิมพ์ซึ่งมีเจตนาที่จะขโมยรหัสผ่าน, รหัสการเข้าสู่ระบบ หรือสารสนเทศเกี่ยวกับหมายเลขบัตรเครดิต

เราสามารถขัดขวางสปายแวร์ได้หรือ? (Can I prevent Spyware?) มีชุดความปลอดภัยของอินเทอร์เน็ตจำนวนมาก รวมทั้งซอฟต์แวร์ป้องกันสปายแวร์ อย่างไรก็ตาม คุณสามารถได้รับซอฟต์แวร์เคลื่อนย้ายสปายแวร์ที่บนคอมพิวเตอร์เครื่องเดียว และรันมันบนคอมพิวเตอร์ของคุณเพื่อลบสปายแวร์ซึ่งไม่เป็นที่ต้องการ เพราะว่า มีสปายแวร์จำนวนมากที่ผันแปรได้, ซอฟต์แวร์ความปลอดภัยบนอินเทอร์เน็ตของคุณอาจจะไม่สามารถป้องกันสปายแวร์ทั้งหมดได้ ที่มันพยายามจะติดตั้งตัวของมันเองลงบนคอมพิวเตอร์ของคุณ ถ้าจะเป็นความคิดที่ดี คุณต้องควรติดตั้งซอฟต์แวร์ป้องกันสปายแวร์หนึ่ง หรือสองโปรแกรมบนเครื่องคอมพิวเตอร์เครื่องเดียวของคุณ เพราะว่า สปายแวร์ใหม่ๆ ได้ถูกสร้างขึ้นตลอดเวลา คุณจะต้องปรับให้ทันสมัย และรันการดำเนินงานของมันซึ่งเป็นซอฟต์แวร์เคลื่อนย้ายสปายแวร์อยู่อย่างสม่ำเสมอ บนโปรแกรมวินโดว์ก็มีโปรแกรมนี้ติดมาด้วยเหมือนกันเรียกว่า Windows Defender ซึ่งสามารถตรวจสอบระบบของคุณเพื่อหาสปายแวร์ และศักยภาพซอฟต์แวร์อื่นๆ ที่ไม่พึงประสงค์ โปรแกรม Malwarebytes AntiMalware, Ad-Aware, และ Spybot-Search & Destroy (โปรแกรมเหล่านี้สามารถดาวน์โหลดได้ที่ download.com) และเป็นโปรแกรมที่ง่ายต่อการติดตั้ง และปรับให้ทันสมัย รูปที่ 9.24 แสดงตัวอย่าง การทำงานของโปรแกรม Ad-Aware และ Spybot มันสามารถป้องกันโปรแกรมที่ไม่พึงประสงค์ และอนุญาตให้คุณลบซอฟต์แวร์ซึ่งทำให้ขุ่นเคืองได้บ่อยๆ

2.2.15 ประเภทของผู้ก่อการหรือผู้กระทำความผิด (Types of Perpetrators)

ประเภทของบุคคลกระทำความผิดมีอยู่หลายประเภทด้วยกัน ซึ่งอาจรวมถึง บุคคลผู้แสวงหาความหาท้าทายตื่นเต้น, ผู้กระทำผิดทางกฎหมายโดยทั่วไป ที่พยายามมองหาการได้รับผลประโยชน์ทางด้านการเงิน, ผู้สอดแนมในโรงงานอุตสาหกรรมเพื่อที่จะได้รับประโยชน์ทางการแข่งขัน, ผู้ก่อการร้ายที่กำลังมองหาสาเหตุที่จะทำลาย จะเห็นได้ว่า บุคคลผู้กระทำความผิดนั้นมีวัตถุประสงค์ที่แตกต่างกันออกไป เพื่อที่จะใช้ความพยายามของตนในการเข้าถึงซึ่งทรัพยากรต่างๆ อันจะเห็นได้ว่าบุคคลเหล่านี้ เป็นผู้สมัครใจที่จะกระทำความผิด โดยใช้ความเสี่ยงในระดับที่แตกต่างกันออกไป ทั้งนี้เพื่อ

ยินดีที่จะให้บรรลุวัตถุประสงค์ตามที่ตนเองได้ตั้งเอาไว้ สำหรับประเภทของบุคคลที่กระทำความผิดหรือเป็นผู้ก่อการนั้น โดยทั่วไปที่พบเห็นได้ชัดเจน ได้แก่บุคคลเหล่านี้ คือ:

ผู้เจาะระบบ และ พวกบ้าคลั่ง (Hackers and Crackers)

ผู้เจาะระบบ หรือแฮกเกอร์ (Hackers) แฮกเกอร์ คือ บุคคลที่มีความสนใจใคร่รู้ลึกลงไปในความลับและความซับซ้อนของการทำงานของคอมพิวเตอร์ โดยเฉพาะระบบปฏิบัติการและซอฟต์แวร์ต่างๆ และส่วนใหญ่จะเป็นโปรแกรมเมอร์มีฝีมือดีด้วย จึงอาจกล่าวได้ว่า คนประเภทนี้ เป็นผู้มีความลึกซึ้งในเรื่องระบบปฏิบัติการและการเขียนโปรแกรม พวกเขารู้ช่องโหว่ต่างๆ และรู้ไปถึงต้นเหตุของช่องโหว่เหล่านั้นในระบบ แฮกเกอร์คือผู้ที่หาความรู้อยู่ตลอดเวลา และยินดีถ่ายทอดความรู้ที่มีอยู่อย่างไม่หวงและไม่มีเจตนาทำความเสียหายให้กับข้อมูลและระบบแม้แต่นิดเดียว แฮกเกอร์บางคนเกิดมาจากการทดสอบระบบ ด้วยความอยากรู้อยากเห็น หรือทดสอบสติปัญญาความรู้ความสามารถของตนเอง บางคนฉลาดอัจฉริยะ บางคนมีพรสวรรค์ และมีความสามารถพิเศษ บางคนอาจขาดความสามารถ ที่เรียกว่า “โห่” หรือเป็น “งานเขียนแบบเด็กๆ” แฮกเกอร์ ผู้ใช้ความรู้ความสามารถไปในทางที่ผิด ได้ชื่อว่าเป็นผู้ก่อการเบื้องต้นในการสร้างความเสียหายให้แก่บุคคลอื่น หรือองค์กรอื่น รวมไปถึงอาจสร้างความเสียหายให้กับระบบเศรษฐกิจด้วย แม้ว่าจะมีการประสานงานที่ยิ่งใหญ่มากของผู้ที่มีความคิดเห็นไม่ตรงกัน เช่น เกี่ยวกับเรื่องอะไรที่ผู้เจาะระบบได้กระทำลงไป (โดยเฉพาะระหว่างผู้เจาะระบบด้วยกันเอง) ผู้เจาะระบบ คือ ชื่อของบุคคลผู้ถูกนิยามเรียกชื่อธรรมดาทั่วไป ผู้ซึ่งกระทำการละเมิดสิ่งมิชอบด้วยกฎหมายต่อระบบคอมพิวเตอร์ส่วนบุคคลหรือไม่ก็เครือข่ายคอมพิวเตอร์

ผู้เจาะระบบมีประเภทที่แตกต่างกันหรือ? ผู้เจาะระบบบางคนทำให้เกิดความไม่พอใจโดยถูกตราหน้าว่าเป็นผู้กระทำผิด ดังนั้น ความพยายามนั้นได้ถูกแยกแยะออกเป็นประเภทของผู้เจาะระบบ ผู้เจาะระบบผู้ซึ่งกระทำผิดในระบบขณะนี้ นับว่าเป็นความท้าทายอย่างยิ่ง (และผู้ที่ไม่ได้ปรารถนาที่จะขโมย หรือทำให้เกิดความหายนะต่อระบบ) อาจจะกล่าวถึงเขาและหล่อนว่า **ผู้เจาะระบบหมวกสีขาว (White-Hat Hacker)** บุคคลเหล่านี้จะชักชวนพวกเขาเองที่เชี่ยวชาญผู้ซึ่งมีความต้องการที่จะทำงานบริการเพื่อสังคม โดยให้ความช่วยเหลือบริษัทที่ไม่ได้มีการป้องกันความอ่อนของระบบของพวกเขาเอาไว้ ผู้เจาะระบบหมวกขาวมองไปที่กลุ่มผู้เจาะระบบ ผู้ซึ่งใช้ความรู้ของเขาทำลายสารสนเทศ หรือเพื่อได้รับประโยชน์จากสิ่งที่ไม่ถูกต้องตามกฎหมาย คำศัพท์ที่ใช้เรียกกลุ่มผู้เจาะระบบชั่วร้ายนี้คือ **ผู้เจาะระบบหมวกสีดำ (Black-Hat Hacker)** (คำศัพท์ที่ว่า หมวกสีขาวและหมวกสีดำ อ้างอิงมาจากภาพยนตร์เก่าของทางตะวันตกซึ่งพระเอกหรือวีระบุรุษจะสวมใส่หมวกสีขาว และพวกที่ทำผิดกฎหมายจะสวมใส่หมวกสีดำ) ความคิดเห็นเกี่ยวกับผู้เจาะระบบ กฎหมายในสหรัฐอเมริกา และหลายประเทศอื่นๆ พิจารณาว่า การเข้าถึงระบบของผู้อื่นที่ไม่ได้มอบอำนาจถือว่าเป็นอาชญากรรม

อะไรเกี่ยวกับผู้เจาะระบบที่เป็นวัยรุ่น บุคคลซึ่งถูกจับอยู่บ่อยๆ ผู้เจาะระบบมือสมัครเล่นเหล่านี้ถูกกล่าวถึงว่าเป็น **งานเขียนเด็ก (Script Kiddies)** งานเขียนเด็กไม่ได้สร้างโปรแกรม เขาใช้การเจาะระบบคอมพิวเตอร์ แทนที่ พวกเขาใช้เครื่องมือที่ถูกสร้างโดยผู้เจาะระบบที่ชำนาญ แต่เนื่องจากเป็นผู้ซึ่งกำลังเริ่มต้นจึงยังไม่มีความชำนาญในการทำลายข้อมูลให้เกิดความหายนะ เหมือนกับผู้เจาะระบบที่เป็นมืออาชีพโชคดี เนื่องจากผู้ใช้โปรแกรมเหล่านี้เป็นมือสมัครเล่น โดยปกติแล้ว พวกเขาจะไม่ซ่ำซองครอบคลุมเส้นทางอิเล็กทรอนิกส์ของพวกเขา ดังนั้น ด้วยความสัมพันธ์คล้ายกันนี้ มันเป็นการง่ายที่สำนักงานผู้บังคับใช้กฎหมายติดตามร่องรอย และความปลอดภัยของพวกเขาไม่มาก ถึงอย่างไรก็ตาม งานเขียนเด็ก สามารถเป็นสาเหตุขัดขวาง และทำความเสียหายให้กับคอมพิวเตอร์, เครือข่าย, และเว็บไซต์ได้

ทำไมพวกผู้เจาะระบบจึงมีความสนใจในการทำลายคอมพิวเตอร์ของฉันที่บ้าน? ผู้เจาะระบบบางคนเป็นพวกสอดรู้สอดเห็น พวกเขามีความสนุกท้าทายในการทำลายระบบ และกำลังมองหาสารสนเทศที่พวกเขาสามารถหาได้พบ มีผู้เจาะระบบคนอื่นๆ อีกเป็นผู้ทำงานอดิเรกในการค้นหาสารสนเทศเกี่ยวกับหัวข้อใดหัวข้อหนึ่งโดยเฉพาะไม่ว่าจะที่ไหนก็ตามที่เขาสามารถจะค้นพบ เพราะว่ามีประชาชนจำนวนมากเก็บรักษาสารสนเทศที่เขาเป็นเจ้าของกรรมสิทธิ์เอาไว้ที่คอมพิวเตอร์ที่บ้านของเขา ผู้เจาะระบบเชี่ยวชาญในการจารกรรมในโรงงานอุตสาหกรรม และอาจทำลายข้อมูลคอมพิวเตอร์ซึ่งอยู่ที่บ้านด้วยก็ได้ สำหรับผู้เจาะระบบคนอื่นๆ การเจาะระบบก็คืออุปกรณ์การจับเวลาเลี่ยง

ผู้เจาะระบบขโมยอะไร ถ้าคุณปฏิบัติการประมวลผลรายการทางธุรกิจบนระบบออนไลน์ เช่น ธนาคาร หรือซื้อสินค้า และบริการ ซึ่งโดยปกติแล้วคุณจะใช้บัตรเครดิต (หรือบัตรการหักบัญชี) บัตรเครดิต และสารสนเทศเกี่ยวบัญชีธนาคารที่มีอยู่ในฮาร์ดไดร์ฟของคุณ อาจถูกตรวจจับโดยผู้เจาะระบบ มีหลายเว็บไซต์ต้องการให้คุณกรอกรหัสเข้าสู่ระบบ (Login ID) และรหัสผ่านในการเข้าสู่ระบบ แม้ว่าข้อมูลนี้ไม่ได้ถูกจัดเก็บไว้ในคอมพิวเตอร์ของคุณ ผู้เจาะระบบอาจจะเข้ายึดจับมันได้ เมื่อคุณออนไลน์โดยใช้กลุ่มของคนที่สูดจมูกดม (packet sniffer) หรือกุญแจล็อก หรือ Keylogger (อันเป็นโปรแกรมที่ทำการเข้ายึดจับจากการเคาะแป้นพิมพ์บนคอมพิวเตอร์ทั้งหมด)

แพ็คเก็ตสนิฟเฟอร์คืออะไร? (What's a Packet Sniffer?) ข้อมูลที่เดินทางไปบนอินเทอร์เน็ตชิ้นเล็กๆ แต่ละชิ้นถูกเรียกว่า กลุ่มหรือหีบห่อ (packet) แพ็คเก็ตจะถูกกำหนดด้วย IP Address ซึ่งเป็นส่วนที่ช่วยกำหนดคอมพิวเตอร์ซึ่งเป็นตัวที่ส่งข้อมูล แพ็คเก็ตหนึ่งจะเอื้อมไปที่ปลายทางของมัน พวกมันจะรวมตัวกันใหม่ให้มีข้อความติดอยู่ด้วยกัน **แพ็คเก็ตสนิฟเฟอร์** คือโปรแกรมคอมพิวเตอร์ที่ถูกแปรแถวโดยผู้เจาะระบบที่กำลังมองหา (หรือคนที่สูดจมูก) แต่ละแพ็คเก็ตที่มันเดินทางไปอยู่บนอินเทอร์เน็ต ไม่เพียงแต่คอมพิวเตอร์ที่มีที่อยู่เท่านั้น แต่ว่าทุกแพ็คเก็ต แพ็คเก็ตสนิฟเฟอร์บางชนิดถูกปรับแต่งโดยการดึงแพ็คเก็ตทั้งหมดในหน่วยความจำ เพราะเหตุว่ามันจะดึงเอาเฉพาะแพ็คเก็ตที่บรรจุด้วยเนื้อหาเฉพาะแต่ละชนิด (เช่น หมายเลขบัตรเครดิต) โดยเฉพาะ

เครือข่ายไร้สายเสี่ยงจากการแสวงหาผลประโยชน์จากประเภทนี้ เพราะว่ามีประชาชนจำนวนมากที่เขาไม่ได้สร้างรหัสลับของข้อมูล เมื่อเขาทำการติดตั้งเครือข่ายไร้สายของเขา (เนื้อหานี้ครอบคลุมอยู่ในบทที่ 7) ผู้เจาะระบบอาจจะนั่งอยู่ที่ร้านกาแฟและเชื่อมต่อเครือข่ายไร้สายอยู่ และให้แพ็คเก็ตสนิฟเฟอร์ดำเนินงานดึงข้อมูลจากคนอื่น ผู้ซึ่งใช้เครือข่ายไร้สาย วิธีการทำเช่นนี้มันง่ายสำหรับผู้เจาะระบบในการดัก และอ่านสารสนเทศที่มีความอ่อนไหวซึ่งถูกส่งไปโดยปราศจากการสร้างรหัสลับ เช่น หมายเลขบัตรเครดิต หรือ เนื้อหาของไปรษณีย์อิเล็กทรอนิกส์

ผู้เจาะระบบทำอะไรกับสารสนเทศด้วย "สนิฟเฟอร์"? สิ่งหนึ่งที่ผู้เจาะระบบมีคือสารสนเทศบัตรเครดิตของคุณ เขาหรือหล่อนสามารถใช้มันซื้อสิ่งของที่ผิดกฎหมายหรือขายหมายเลขให้กับใครบางคนที่เขาต้องการ ถ้าผู้เจาะระบบขโมยหมายเลขการเข้าสู่ระบบ และรหัสผ่านบัญชีเพื่อรู้ว่าคุณมีสารสนเทศบัตรเครดิตถูกจัดเก็บไว้ในที่ไหน (เช่น ใน Ebay หรือ Amazon) เขาหรือหล่อนสามารถใช้ชื่อบัญชีของคุณซื้อรายการสินค้า และให้ทำการส่งสินค้าให้เขาหรือหล่อนแทนที่จะเป็นคุณ ถ้าผู้เจาะระบบรวบรวมสารสนเทศบัตรเครดิตของคุณได้มากพอแล้ว เขาอาจสามารถกระทำความผิดด้วยการขโมยอัตลักษณ์ **การขโมยอัตลักษณ์ (Identity Theft)** คือ การแสดงลักษณะพิเศษโดยบางคนด้วยการใช้สารสนเทศส่วนบุคคลเกี่ยวกับคุณ (เช่น ชื่อของคุณ, ที่อยู่ หรือหมายเลขบัตรประกันสังคม) ทึกทักเอาอัตลักษณ์ของคุณไปเพื่อวัตถุประสงค์ในการฉ้อโกง

ถึงแม้ว่า เรื่องที่ได้ยินนี้เป็นเรื่องที่น่ากลัว คุณสามารถป้องกันตัวของคุณอย่างง่ายจากแพ็คเก็ตสนิฟเฟอร์ ด้วยการติดตั้งซอฟต์แวร์ด่านกันบุกรุก (ซึ่งเราจะได้อภิปรายในภายหลังบทนี้) และการใช้การสร้างรหัสลับข้อมูลบนเครือข่ายไร้สาย

พวกบ้าคลั่ง หรือแคร็กเคอร์ (Crackers) แคร็กเกอร์ คือ บุคคลที่บุกเข้าไปในระบบของผู้อื่น โดยไม่ได้รับอนุญาต โดยมีจุดประสงค์ร้ายแอบแฝงอยู่ ไม่ว่าจะเป็นการขโมยข้อมูล การทำลายข้อมูล การทำให้ผู้อื่นใช้ระบบไม่ได้ และการสร้างปัญหาอื่นๆ ให้เกิดขึ้นในระบบ ซึ่งผลลัพธ์ที่ออกมาล้วนแล้วแต่สร้างความเดือดร้อนให้กับผู้ที่เกี่ยวข้อง **วิญญู กิ่งหิรัญวัฒนา (2545)** วัตถุประสงค์หลักของ Cracker คือ ต้องการทำลายระบบคอมพิวเตอร์หรือระบบสารสนเทศ การกระทำของ Cracker นั้นเรียกว่า Cracking คือ การบุกรุกเข้าไปในระบบคอมพิวเตอร์ของผู้ใช้ใดๆ โดยใช้วิธีเจาะรหัสผ่านเริ่มต้นจากการคัดลอกไฟล์ SAM (Security Account Manager) ซึ่งเป็นไฟล์ที่ใช้เก็บรหัสผ่านผู้ใช้ โดยจะทำการถอดรหัสด้วยอัลกอริทึม จนกว่าจะได้รหัสผ่านที่ถูกต้อง Cracker ที่มีความบ้าคลั่งนั้นที่มีสาเหตุมาจากการเจาะระบบเป็นกิจกรรมของการกระทำความผิดอย่างชัดเจน ตัวอย่างของพวกบ้าคลั่ง เช่น พวกคลั่งลัทธิ

คนภายในมุ่งร้าย (Malicious Insiders) ส่วนใหญ่เป็นเรื่องความปลอดภัยเกี่ยวกับบริษัทโดยเฉพาะปัญหาเรื่องการโกง ซึ่งในปัจจุบันมีข่าวเกี่ยวกับเรื่องเหล่านี้มากขึ้นทุกขณะ และเป็นความเสี่ยงขององค์กรต่างๆ ที่จะต้องพบเจอกับปัญหาเหล่านี้ ปัญหาเรื่องการโกงมีอยู่หลายประการ ได้แก่

การยักยอก การฉ้อโกง การขโมยทรัพย์สินขององค์กร การโกงเกี่ยวกับการเชื่อมต่อกระบวนการเรื่องการประมูล การโกงใบกำกับสินค้า และการชำระเงิน การโกงคอมพิวเตอร์ การโกงบัตรเครดิตสินเชื่อด้วยพฤติกรรมการโกงการโกงภายในองค์กรเหล่านี้ ทำให้องค์กรเกิดความอ่อนแอ โดยเฉพาะอย่างยิ่งความอ่อนแอของคู่มือการทำงานภายในองค์กรเอง การโกงภายในองค์กรอาจเกิดจากการสมรู้ร่วมคิดของพนักงานภายใน ซึ่งอาจมีสาเหตุมาจากรการทำงานร่วมกันระหว่างพนักงานภายในของบริษัทกับบุคคลภายนอก ส่วนความหมายของคนภายในองค์กรอาจไม่ได้หมายถึงพนักงานของบริษัท แต่อาจเป็นที่ปรึกษา หรือผู้รับเหมาก็ได้ เรื่องเหล่านี้มันเป็นการยากมากในการป้องกัน หรือหยุดไม่ให้กระทำ เช่น ในบางครั้งมีการมอบหมายอำนาจให้บุคคลสามารถเข้าถึงข้อมูลได้ทุกระบบ แต่พวกเขาอาจนำอำนาจนั้นไปใช้ในทางที่ผิด ดังนั้นความพลั้งเผลอของคนภายใน มีศักยภาพที่อาจก่อให้เกิดความเสียหายกับบริษัทได้อย่างมากทีเดียว ตัวอย่างที่เห็นได้ชัดเจนเกี่ยวกับ คนภายในบริษัทมุ่งร้าย ก็คือ พนักงานบริษัทเขียนรหัสโปรแกรมคอมพิวเตอร์ เพื่อนำเงินจ่ายเข้าบัญชีของตนเอง โดยไม่มีการบันทึกกิจกรรม ตัวอย่างมีธนาคารของอเมริกาเคยโดนมาแล้ว

การสอดแนมในโรงงานอุตสาหกรรม (Industrial Spies) หมายถึงการกระทำโดยผิดกฎหมาย เพื่อให้ได้ความลับในการแลกเปลี่ยนสินค้าจากคู่แข่งขัน เป็นลักษณะการสอดแนมหรือขโมยความลับทางการค้าไปให้กับคู่แข่งขันทางธุรกิจ ปัจจุบันได้มีการได้มีการออกกฎหมายเรื่องจารกรรมทางเศรษฐกิจในปี ค.ศ.1996 เพื่อป้องกันการสอดแนมความลับในการแลกเปลี่ยนสินค้า ในขณะเดียวกันก็มีบางคนบางกลุ่มได้ใช้ความฉลาดเกี่ยวกับการให้ได้ข้อมูลความลับเกี่ยวกับการแข่งขัน มันเป็นการใช้ความสามารถพิเศษอย่างถูกกฎหมาย หรือการอาศัยช่องโหว่ทางกฎหมายมาช่วยเพื่อให้ได้ข้อมูลความลับเหล่านั้น เช่นความพยายามเก็บรวบรวมสารสนเทศที่มีความไม่เหมาะสมนำไปเผยแพร่ในที่สาธารณะ ดังนั้น การสอดแนมหรือการจารกรรมในโรงงานอุตสาหกรรม จึงหมายถึง การใช้งานอย่างไม่ถูกต้องตามกฎหมาย เพื่อให้ได้รับสารสนเทศอย่างไม่เหมาะสมและนำไปเปิดเผยในที่สาธารณะ

คนที่เลี้ยงชีพในทางที่ผิดด้านไซเบอร์ (Cybercriminals) หรืออาชญากรไซเบอร์ ได้แก่บุคลผู้กระทำความผิดโดยอาศัยเทคโนโลยีสารสนเทศเป็นเครื่องมือในการแสวงหาผลประโยชน์ที่ด้านการเงินเป็นหลัก เช่น การเจาะระบบคอมพิวเตอร์ของธนาคารเพื่อขโมยเงินในบัญชีลูกค้ามาเป็นของตนเอง หรือการเจาะระบบเข้าไปขโมยข้อมูลในระบบคอมพิวเตอร์ของบริษัท อาชญากรไซเบอร์มีความหมายรวมถึง รูปแบบการโกงทางคอมพิวเตอร์ทั้งหมด ได้แก่ การขโมย การขายซ้ำหมายเลขบัตรเครดิต การขโมยลักษณ์ส่วนบุคคล และการขโมยหมายเลขโทรศัพท์ นอกจากนั้นอาจจะมีวิธีการที่ทำให้คอมพิวเตอร์ประมวลผลผิดพลาด ซึ่งจะส่งผลกระทบและสร้างความเสียหายให้บริษัทเป็นอย่างมาก และขาดความเชื่อถือจากลูกค้า ส่วนวิธีการป้องกันและลดการโกงบัตรเครดิตออนไลน์นั้น

สามารถทำได้โดย (1) การใช้เทคโนโลยีสร้างรหัสลับ, (2) ตรวจสอบที่อยู่ที่ยื่นเสนอเข้ามาทางออนไลน์ ซึ่งดูขัดแย้งกับธนาคาร , (3). ต้องมีร้องขอให้มีการตรวจสอบมูลค่าบัตร และ (4) ใช้ซอฟต์แวร์ประมวลผลความเสี่ยงในเรื่องแต้มคะแนน
ในขณะเดียวกันต้องพยายามศึกษาเรียนรู้เกี่ยวกับบัตรประเภทต่างๆ เช่น บัตรสมาร์ทการ์ด
ซึ่งประกอบไปด้วย : (1) บรรจุไปด้วยซิฟหน่วยความจำ (2) มีการปรับปรุงเปลี่ยนรหัสอยู่เสมอ (3) บัตรสมาร์ทการ์ดนิยมใช้กันมากในยุโรป และ (4). ยังไม่มีแพร่หลายในสหรัฐอเมริกา

นักเจาะระบบ และผู้ก่อการร้ายไซเบอร์ (Hacktivists and Cyberterrorists) เป็นลักษณะการก่อการร้ายบนโลกไซเบอร์ หรือผ่านระบบเครือข่ายอินเทอร์เน็ต ส่วนใหญ่เป็นการเจาะระบบเพื่อให้บรรลุเป้าหมายทางการเมืองหรือสังคม เช่น การเจาะระบบขององค์กรนาโต้ ด้วยการส่งอีเมลที่มุ่งร้ายไปยังคอมพิวเตอร์เครือข่ายขององค์กรนาโต้ โดยกลุ่มผู้ก่อการร้ายที่ไม่เห็นด้วยกับการทิ้งระเบิดของนาโต้ นอกจากนี้ ยังรวมไปถึงการโจมตีเพื่อขู่เข็ญ หรือบีบบังคับรัฐบาล เพื่อวัตถุประสงค์ทางการเมืองและสังคม หรืออีกตัวหนึ่ง เมื่อปี ค.ศ.2010 ที่ผู้ก่อการร้ายใช้ชื่อว่า “นิรนาม” ใช้ DDoS โจมตี บริษัท มาสเตอร์การ์ด เพพาล ซิติ้แบงค์ และวีซ่า โดยเจ้าของเว็บไซต์ วิกิลีกส์ (**WikiLeaks**) นักเจาะระบบ และผู้ก่อการร้ายทางไซเบอร์นี้ ส่วนใหญ่มองหาแนวทางที่ต้องการจะได้รับสารสนเทศที่สำคัญ โดยใช้เทคนิคการทำลายหรือทำให้ระบบการให้บริการเกิดความยุ่งเหยิง

กฎหมายของรัฐบาลกลางอัยการเพื่อโจมตีคอมพิวเตอร์ (Federal Laws for Prosecuting Computer Attacks) กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในสหรัฐอเมริกา ถูกนำมาใช้เป็นครั้งแรกในปี ค.ศ.1950 ซึ่งก่อนหน้านี้ ยังไม่มีกฎหมายออกมาบังคับใช้อย่างจริงเกี่ยวกับด้านนี้ ต่อมาเมื่อเหตุการณ์ที่อาชญากรไซเบอร์กลุ่มหนึ่งเข้ามาจี้ขโมยเงินที่ธนาคารไป จึงมีการตรากฎหมายนี้ขึ้น

2.2.16 การนำคอมพิวเตอร์ที่น่าเชื่อถือไปใช้ประโยชน์ (Implementing Trustworthy Computing) ลักษณะของคอมพิวเตอร์ที่น่าเชื่อถือ ต้องประกอบด้วย (1). การถ่ายโอนข้อมูลมีความปลอดภัย มีความเป็นส่วนตัว และคอมพิวเตอร์มีความน่าเชื่อถือ (2) อยู่บนพื้นฐานของการดำเนินธุรกิจ (3) ทุกระบบหรือเครือข่ายมีความปลอดภัย นั่นคือมีการผสมผสานกันระหว่างเทคโนโลยี นโยบาย และพนักงาน และต้องต้องสามารถทำกิจกรรมได้อย่างกว้างขวางเพื่อให้บรรลุความสำเร็จที่ดี (3) ระบบจะต้องมีการติดตามและป้องกันผู้บุกรุก (4) มีการวางแผนการตอบสนองอย่างชัดเจน คือ มีการแจ้งเตือน มีหลักฐานการป้องกัน มีกิจกรรมการเข้าไปดูแลเรื่องการบำรุงรักษา มีการควบคุมเอาไว้ มีการกำจัดและทำลาย และมีการกู้คืนข้อมูลที่เสียหาย

2.2.17 การประเมินค่าความเสี่ยง (Risk Assessment) ความเสี่ยง (Risk) หมายถึง ความเป็นไปได้ของเหตุการณ์ที่อาจจะเกิดขึ้นที่ส่งผลกระทบในทางลบต่อการบรรลุวัตถุประสงค์ (COSO : Committee of Sponsoring Organization of the Tread way Commission) การประเมินความเสี่ยง (Risk Assessment) หมายถึง การจำแนกและพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่ โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact)

- โอกาสที่จะเกิด (Likelihood) เป็นการพิจารณาความเป็นไปได้ที่จะเกิดเหตุการณ์ความเสี่ยงในช่วงเวลาหนึ่ง หรือจะเรียกว่า ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงก็ได้
- ผลกระทบ (Impact) ระดับความรุนแรงของผลเสียหายที่เกิดขึ้น จากความเสี่ยงและ มีผลกระทบต่อองค์กรซึ่งอาจเป็นได้ทั้งในด้านบวกและด้านลบ โดยสามารถแบ่งเป็นผลกระทบทางด้านการเงินและผลกระทบที่ไม่ใช่ทางการเงิน (ส่วนงานบริหารความเสี่ยง สำนักแผนยทธศาสตร์ กรกฎาคม : 2553)

กระบวนการของการประเมินความเสี่ยงด้านความปลอดภัยที่เกี่ยวข้องกับหลายอย่างด้วยกันคือ ประเมินคอมพิวเตอร์และเครือข่ายขององค์กรจากภัยคุกคามทั้งภายในและภายนอกองค์กร ในลำดับต่อมาต้อง มีการกำหนดการลงทุว่าโครงการไหนที่มีรายได้ดีที่สุดและมีภัยคุกคามมากที่สุด และ เน้นไปที่การใช้ความพยามยามให้เกิดความปลอดกับพื้นที่ซึ่งมีโอกาสจ่ายเงินได้หมดมากที่สุด

กระบวนการประเมินค่าความเสี่ยง 8 ขั้นตอน

1.ระบุสินทรัพย์ที่มีความกังวลมากที่สุด
2.ระบุเหตุการณ์ความสูญเสียซึ่งอาจเกิดขึ้น
3.ประเมินโอกาสของแต่ละภัยคุกคามที่อาจเกิดขึ้น
4.ตรวจสอบผลกระทบของแต่ละภัยคุกคาม
5.กำหนดวิธีการคุกคามแต่ละแห่งซึ่งอาจจะทำให้ลดลง
6.ประเมินความเป็นไปได้ของตัวเลือกการบรรเทาเบาบางลง
7.ดำเนินการวิเคราะห์ต้นทุนผลประโยชน์
8.ตัดสินใจที่จะดำเนินการวัดการนำไปใช้ประโยชน์

2.2.18 นโยบายการสร้างความปลอดภัย (Establishing a Security Policy)

การกำหนดด้านความปลอดภัยนั้น ต้องคำนึงถึง ความต้องการด้านความปลอดภัยขององค์กร การควบคุม และการให้การสนับสนุนที่ตรงกับความต้องการ มีการอธิบายหรือวาดภาพความรับผิดชอบให้เห็นชัดเจน และมีความคาดหวังของพฤติกรรมนั้นๆ ว่าจะทำให้ประสบความสำเร็จได้ตามพฤติกรรมที่ต้องการ มีการจัดทำโครงร่างขึ้นมาว่า อะไรบ้างที่ต้องการอยากจะทำ และจะทำมันได้อย่างไร เรื่องของนโยบายต้องการจัดทำให้เป็นระบบอัตโนมัติ ซึ่งจะเป็นเสมือนกระจกเงาที่ส่องให้เห็นถึงนโยบายที่มีการเขียนหรือวางแผนเอาไว้แล้วอย่างชัดเจน หากเป็นนโยบายเกี่ยวกับการ

แลกเปลี่ยน ต้องง่ายต่อการใช้งาน พร้อมทั้งมีการเพิ่มเรื่องความปลอดภัยที่ดี โดยเฉพาะความปลอดภัยทางด้านคอมพิวเตอร์ เช่น การแนบไฟล์อีเมล การใช้อุปกรณ์ไร้สาย หรือแม้กระทั่งเครือข่ายส่วนบุคคลเสมือนจริงที่มีการใช้วิธีถ่ายทอดการสื่อสารผ่านทางอินเทอร์เน็ต และในขณะเดียวกันต้องคอยดูแลเรื่องความเป็นส่วนตัว ตลอดจนความปลอดภัยในลักษณะอื่นๆ ด้วย

การให้การศึกษาแก่พนักงาน, ผู้รับเหมา, และคนทำงานล่วงเวลา สำหรับปัญหาด้านความปลอดภัยของบริษัทนั้น ทางบริษัทเองต้องตระหนักด้วยการสร้างและส่งเสริมสนับสนุนให้ผู้ใช้งานเกิดความระมัดระวังเกี่ยวกับเรื่องนโยบายด้านความปลอดภัย คนทำงานซึ่งเป็นพนักงานและผู้รับเหมาจะต้องศึกษาเรียนรู้เกี่ยวกับความสำคัญของความปลอดภัย ดังนั้นพวกเขาจะต้องถูกกระตุ้นให้เข้าใจและปฏิบัติตามนโยบายของบริษัท ด้วยเหตุผลประการดังกล่าวนี้จะทำให้องค์กรสามารถบรรลุเป้าหมายได้ โดยการอภิปรายถกเถียงกันถึงกรณีของความปลอดภัยที่เกิดขึ้นอยู่ในปัจจุบันอันส่งผลกระทบต่อองค์กร ผู้ใช้งานจะต้องมีความเข้าใจ เนื่องจากพวกเขาเป็นส่วนหนึ่งของความสำคัญเกี่ยวกับระบบความปลอดภัย และพวกเขาจะต้องมีส่วนในเรื่องของความรับผิดชอบอย่างแน่นอน ตัวอย่างเช่น ผู้ใช้จะต้องช่วยป้องกันระบบสารสนเทศและข้อมูลขององค์กร ด้วยการปฏิบัติตามระเบียบต่อไปนี้ คือ:

- การป้องกันรหัสผ่านไว้ให้ดี
- ต้องไม่แบ่งปันรหัสผ่าน
- ต้องมีการประยุกต์ใช้ในเรื่องการควบคุมการเข้าถึงข้อมูลอย่างเข้มงวด
- มีการจัดทำกิจกรรมรายงานประจำปีเอาไว้ทั้งหมด
- มีการป้องกันอุปกรณ์ในการจัดเก็บข้อมูลและเครื่องคอมพิวเตอร์ที่เคลื่อนย้ายได้เอาไว้อย่างดี

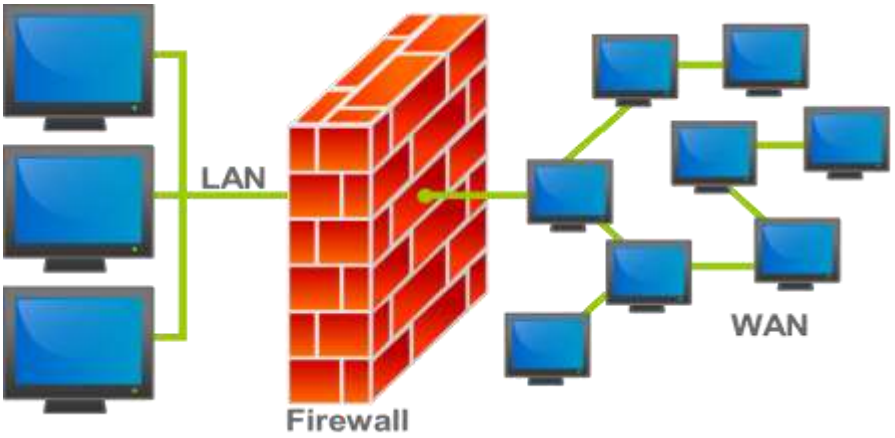
การป้องกัน (Prevention)

โดยทั่วไปแล้ว มักจะพบว่าไม่มีองค์ใดที่สามารถมีระบบป้องการการโจมตีได้อย่างสมบูรณ์ เรื่องที่สำคัญคือ อุปกรณ์เครื่องใช้ต้องมีการจัดวางและวิธีแก้ปัญหาระบบความปลอดภัยเอาไว้เป็นชั้นๆ ด้วยการที่ทำให้ระบบคอมพิวเตอร์มีความยุ่งยากต่อการถูกโจมตีจากผู้บุกรุก จนกระทั่งทำให้ผู้บุกรุกละทิ้งที่จะเข้ามาโจมตี สำหรับวิธีแก้ปัญหาเกี่ยวกับการป้องกันต่างๆ เหล่านี้ สามารถทำได้โดย:

(1). การติดตั้งโปรแกรมไฟร์วอลล์ขององค์กร นั่นคือ มีการกำหนดข้อจำกัดในการเข้าถึงเครือข่าย

(2). มีระบบป้องกันการบุกรุก คือ มีการสกัดกั้นไวรัส การป้องกันการทำให้ผิดรูปหรือผิดส่วน และมีการป้องกันภัยคุกคาม

(3). มีการติดตั้งโปรแกรมตรวจสอบและทำลายไวรัส คือ การการตรวจจับอยู่เป็นลำดับในทุกไบต์ หรือมีการลงนามความร่วมมือ หรือซื้อโปรแกรมไวรัสที่สามารถอัพเดทออนไลน์ได้ เช่น ในประเทศสหรัฐอเมริกา มีกลุ่มหน่วยงานกลางที่รับหน้าที่บริการแบบฉุกเฉินมาทำงานให้



ภาพประกอบ 2.8 *แสดงวิธีการทำงานของโปรแกรมไฟร์วอลล์*
(ที่มา: www.wikipedia.org, 2019)

(4). การปกป้องต่อสู้จากการโจมตี โดยผู้มุ่งร้ายภายใน เมื่อกล่าวกันโดยปกติแล้ว พนักงานของบริษัทจะต้องมีชื่อบัญชีผู้ใช้งานคอมพิวเตอร์ และยังสามารถใช้งานได้อยู่อย่างเป็นปกติ แม้ลาออกจากงานไปแล้ว ดังนั้น ชื่อบัญชีผู้ใช้ของพนักงานที่ลาออกไปแล้ว เป็นชื่อบัญชีที่มีความเสี่ยง ดังนั้นเพื่อต้องการลดความเสี่ยงของภัยคุกคามในการถูกโจมตี พนักงานไอทีต้องทำการลบชื่อบัญชี รหัสการเข้าสู่ระบบ รวมถึงรหัสผ่านของพนักงานที่ลาออไปแล้วออกจากระบบของแผนกที่พนักงานคนนั้นทำงานอยู่อย่างทันท่วงที รวมถึงผู้รับเหมาต่างๆ ด้วย นอกจากนั้น ในการกำหนดบทบาทของพนักงานก็ต้องมีความระมัดระวังอย่างเป็นพิเศษ และควรมีการแยกความสำคัญของความรับผิดชอบในการกำหนดและมอบหมายบทบาทให้กับพนักงาน ไม่ว่าจะเป็นเรื่องการกำหนดให้ชื่อบัญชีผู้ใช้งานควรมีขีดจำกัด

(5) การแก้ต่างหรือกล่าวแย้งต่อต้านคนที่เลี้ยงชีพในทางที่ผิด ในอเมริกา มีหน่วยงานที่ดูแลเรื่องความปลอดภัย และมันก็เป็นส่วนหนึ่งที่ถูกกำหนดไว้ในการกำกับดูแลความปลอดภัยทางด้านอินเทอร์เน็ตหรือไซเบอร์ ซึ่งก็เป็นเสมือนแหล่งรวบรวมข้อมูลทรัพยากรทางด้านนี้ คือ มีหน้าที่ในการสร้างและดูแลรักษาเกี่ยวกับระบบตอบสนองความปลอดภัยทางด้านอินเทอร์เน็ตของประเทศชาติ และทำหน้าที่ในการพัฒนาโปรแกรมขึ้นมาจัดการดูแลเกี่ยวกับความเสี่ยงทางอินเทอร์เน็ต เพื่อป้องกัน

โครงสร้างพื้นฐานที่วิกฤติ รวมถึงดูแลเรื่องการเงินการธนาคาร เรื่องน้ำ เรื่องการทำงานของรัฐบาล และการบริการแบบฉุกเฉิน

(6).มีการกำหนดระยะเวลาในการตรวจสอบทางด้านเทคโนโลยีสารสนเทศ นั่นคือ มีการประเมินผลนโยบาย หรือไม่ก็การปฏิบัติตามกฎของพนักงาน ควรมีการทบทวนการเข้าถึงข้อมูลในระบบ และมีลำดับของผู้ที่มีสิทธิ์ มีการทดสอบระบบการปกป้อง มีชุดเครื่องมือสำหรับป้องกันสารสนเทศ ที่มีความเหมาะสมจากสถาบันที่รักษาความปลอดภัยทางคอมพิวเตอร์

การตรวจตรา (Detection) ในการตรวจตรานั้น สิ่งที่ต้องทำคือ (1) มีระบบตรวจตรา มีการตรวจจับผู้ที่กระทำการบุกรุก (2) มีระบบป้องกันผู้บุกรุก ได้แก่ มีการติดตามระบบและทรัพยากร เครือข่าย และการจัดทำกิจกรรม (3) มีการกำหนดสิทธิ์ให้มีผู้รับผิดชอบงานอย่างเหมาะสม ถ้าเป็นไปได้ต้องมีระบบป้องกันการบุกรุกจากบุคคลที่อยู่ภายนอกองค์กร มีการตรวจตราดูแลการใช้คอมพิวเตอร์ในทางที่ผิดภายในองค์กร มีการสร้างฐานความรู้เรื่องความปลอดในองค์กร และมีการรณรงค์สร้างพฤติกรรมที่มีความเหมาะสมให้เกิดขึ้น

การตอบสนอง (Response) ควรมีการจัดทำแนวทางตามขั้นตอนต่อไปนี้ คือ (1) การวางแผนการตอบสนอง มีการพัฒนาเรื่องความก้าวหน้าที่ดีหลายๆ อย่าง มีการอนุมัติโดย หน่วยงานทางด้านกฎหมาย และมีลำดับของการจัดการแบบผู้มีประสบการณ์ (2) มีเป้าหมายพื้นฐาน ได้แก่ มีการควบคุมการกู้คืน และทำให้เกิดความเสียหายน้อยที่สุด มีการติดตามจับผู้ที่ทำการบุกรุก (3) การวางแผนการการตอบสนองอย่าคิดเพียงแค่ 56% เท่านั้น ควรหวังให้สูงไปกว่านั้นด้วย (4) มีการกำหนดการแจ้งเตือนว่า ใครที่จะทำการแจ้งเตือน และใครที่ไม่ต้องการแจ้งเตือน (5) มีบุคคลผู้เชี่ยวชาญด้านความปลอดคอยให้คำแนะนำในการเผยแพร่สารสนเทศประเภทต่างๆ และควรเป็นผู้ที่มีความสามารถในการประณีประนอมในสภาสาธารณะได้ (6) มีรายละเอียดของเอกสารเหตุการณ์ความปลอดภัยต่างๆ รวมถึง สถานการณ์ของระบบทั้งหมด ชนิดของการกระทำ และการสนทนาแลกเปลี่ยนกับบุคคลภายนอกองค์กร (7) มีการทบทวน คือ มีการกำหนดการตัดสินใจว่าอะไรบ้างที่จะเกิดขึ้น มีการประเมินผลการตอบสนองขององค์กร (8) มีความระมัดระวังในการนำเอาผู้ก่อการออกมา กระทำด้วยความเที่ยงธรรม (9) มั่นคอยพิจารณาสิ่งที่มีแนวโน้มว่าจะเกิดผลในทางลบ (10) ควรมีการนำคำพิพากษาที่เคยมีมาก่อนนำมาเป็นแบบอย่างในการพิจารณา การให้ผู้คนจำนวนมากใช้ชื่อบัญชีขององค์กรนั้น ถือว่าเป็นจุดอ่อนขององค์ ดังนั้น ต้องระมัดระวังเป็นพิเศษ

2.2.19 กระบวนการกฎหมายทางคอมพิวเตอร์ (Computer Forensics)

องค์ประกอบทางกฎหมายนั้น มีหลายอย่างหลายประการ รวมถึงวิทยาการคอมพิวเตอร์ด้วย ต้องมีการกำหนด การรวบรวม การทดสอบ และมีการจัดรวบรวมข้อมูลเอาไว้ให้เป็นหมวดหมู่ ตลอดจนเรื่องของความซื่อสัตย์นั้น เป็นสิ่งจำเป็นที่ต้องรณรงค์ให้คงมีอยู่ต่อไป กระบวนการกฎหมาย

ทางคอมพิวเตอร์นั้น ต้องมีการสืบสวนอย่างกว้างขวาง รวมทั้งมีการฝึกอบรม และมีความรู้ทางกฎหมาย เพื่อที่จะนำเอามาประยุกต์ใช้ในกานำผู้กระทำผิดมาลงโทษได้อย่างเหมาะสม

กรณีศึกษา

กรณีศึกษาเกี่ยวกับ อาชญากรรมคอมพิวเตอร์ และ การใช้กฎหมายการกระทำผิดเกี่ยวกับคอมพิวเตอร์ในกระบวนการยุติธรรมของประเทศเกาหลีใต้

by A.Pinya Hom-anek,
GCFW, CISSP, CISA, (ISC)2 Asian Advisory Board
President, ACIS Professional Center

ปัญหาอาชญากรรมคอมพิวเตอร์ทั่วโลก ในช่วงปี พ.ศ. 2547-2548 มีอัตราเพิ่มสูงขึ้น ยกตัวอย่าง จำนวนคดีด้านอาชญากรรมในประเทศเกาหลีใต้มีจำนวนทั้งหมด 77,099 คดี ในปี 2547 และเพิ่มเป็น 88,731 คดี ในปี 2548 ทางประเทศเกาหลีใต้ ได้ออกกฎหมายการการกระทำผิดเกี่ยวกับคอมพิวเตอร์ตั้งแต่ปี พ.ศ. 2539 และมีการปรับปรุงอย่างต่อเนื่องให้ทันยุคทันสมัยกับเทคโนโลยี ใหม่ ๆ ของแฮกเกอร์ ในปัจจุบันมีเทคนิคการโจมตีใหม่ ๆ เช่น Phishing attack หรือ Pharming attack ทางฝ่ายกฎหมายก็มีความจำเป็นต้องปรับปรุงร่างกฎหมาย ให้สามารถนำมาใช้กับเทคนิคใหม่ ๆ ดังกล่าว เนื่องจาก ทางเกาหลีใต้มีการฝึกอบรมพัฒนาความรู้ให้กับเจ้าหน้าที่อย่างสม่ำเสมอ ทำให้สามารถปิดคดีอาชญากรรมคอมพิวเตอร์ได้กว่า 99 เปอร์เซ็นต์ โดยอ้างอิงกระบวนการพิสูจน์หลักฐานที่มีแนวทางเหมือนประเทศญี่ปุ่น, อิตาลี และ ฝรั่งเศส ทำให้เกิดความผิดพลาดน้อยมากในการพิสูจน์หลักฐาน ยกตัวอย่าง กฎหมายของเกาหลีอนุญาต ให้เก็บหลักฐานที่กระทำผิดเกี่ยวกับคอมพิวเตอร์ไว้ได้นานสูงสุดถึง 15 ปี (ตามคำสั่งศาล) และสามารถยึดหลักฐานไว้จนกว่าจะพิจารณาคดีเสร็จสิ้น เช่น ยึดเครื่องคอมพิวเตอร์โน้ตบุ๊กไว้ในการควบคุมของฝ่ายยุติธรรม เป็นต้น สำหรับกฎหมายของประเทศไทย ในประเด็นนี้ มีความแตกต่างจากของประเทศเกาหลีใต้ ซึ่งผมเห็นควรที่จะมีการปรับปรุงในสอดคล้องกับสากลขณะที่กฎหมายการกระทำผิด เกี่ยวกับคอมพิวเตอร์ยังอยู่ในช่วงพิจารณาเวลานี้โครงสร้างของหน่วยงานทางกระบวนการยุติธรรมของเกาหลีใต้นั้น มีสองหน่วยงาน ที่มีศูนย์พิสูจน์หลักฐานทางดิจิตอล (Digital Forensic Center) คือ สำนักงานอัยการสูงสุด (Supreme Prosecutor’s Office) และ กรมตำรวจแห่งชาติฝ่ายปราบปรามอาชญากรรมคอมพิวเตอร์ (National Korean Cyber Police) โดยกรมตำรวจเป็นหน่วยงานที่ควบคุมโดยสำนักงานอัยการสูงสุดอีกทีหนึ่ง ผมได้มีโอกาสเข้าเยี่ยมชม ศูนย์ ปฏิบัติการพิสูจน์หลักฐานทางคอมพิวเตอร์ของทั้งสองหน่วยงาน นับว่าทันสมัยมาก สามารถพิสูจน์หลักฐานจาก ฮารด์ดิสก์ (Hard disk) ของคอมพิวเตอร์ทุกรุ่นตลอดจนหน่วยความจำในโทรศัพท์มือถือ มีโปรแกรมที่ใช้ใน

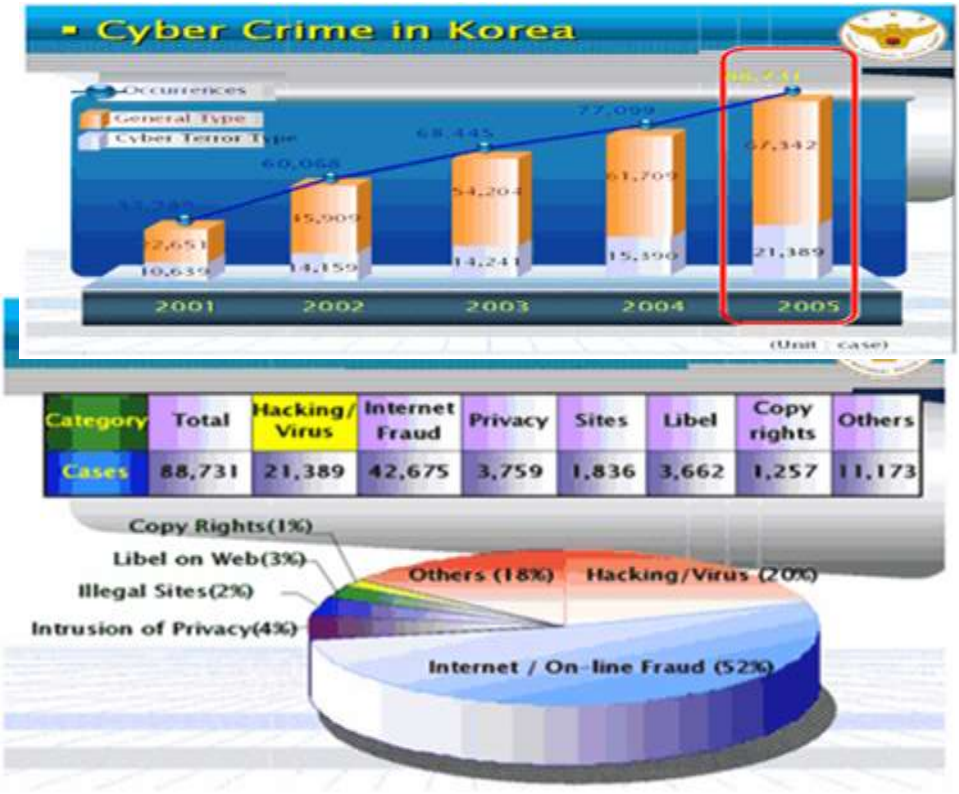
การพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensic Software) ทั้งแบบ Commercial และ Open Source Software เพื่อที่จะสามารถนำผลลัพธ์มาตรวจสอบซึ่งกันและกัน ตลอดจนมีการใช้เครื่องคอมพิวเตอร์ที่ออกแบบมาทางด้านการพิสูจน์หลักฐานทางดิจิตอลโดยเฉพาะ ที่เราเรียก ว่า FRED (Forensic Recovery of Evidence Device) ทีมผู้เชี่ยวชาญของทั้งสองหน่วยงานมีหลายสิบคนที่เชี่ยวชาญทั้งด้าน Computer Forensic ซึ่งเป็นการพิสูจน์หลักฐานในหน่วยความจำหรืออุปกรณ์เก็บข้อมูลที่เครื่องคอมพิวเตอร์ และ ด้าน Internet Forensic เกี่ยวกับการสืบสวนหาพยานหลักฐานทางระบบอินเทอร์เน็ต เช่น การตามหาแหล่งที่มาของแฮกเกอร์ หรือ การตามแกะรอยอิเล็กทรอนิกส์เมล์เป็นต้น

กฎหมายกระทำเกี่ยวกับคอมพิวเตอร์ของประเทศไทยนั้นมีความจำเป็นอย่างยิ่งยวดในการเร่งพิจารณาเพื่อที่จะสามารถนำมาใช้ในการแก้ปัญหาอาชญากรรมคอมพิวเตอร์ที่มีกรณีศึกษาเกิดขึ้นแล้วหลายกรณีในช่วงปีที่ผ่านมา ทางฝ่ายยุติธรรมจำเป็นต้องนำกฎหมายเดิมมาปรับใช้ซึ่งใช้ได้ในบางกรณีเท่านั้น ขณะเดียวกับประเทศไทยมีความจำเป็นต้องเร่งฝึกอบรมผู้เกี่ยวกับทั้งหมดเกี่ยวกับกระบวนการยุติธรรมไม่ว่าจะเป็น ตำรวจของสำนักงานตำรวจแห่งชาติ, เจ้าหน้าที่พิสูจน์หลักฐานของสถาบันนิติวิทยาศาสตร์,เจ้าหน้าที่ฝ่ายสืบสวนของกรมสวบสวนคดีพิเศษตลอดจนผู้พิพากษา และอัยการ ให้เกิดความรู้ความเข้าใจเตรียมพร้อมกับกฎหมายการกระทำผิดเกี่ยวกับคอมพิวเตอร์ที่กำลังจะถูกนำมาบังคับใช้ในอนาคตอันใกล้

ในปัจจุบัน เจ้าหน้าที่ของกรมสอบสวนคดีพิเศษ หรือ “DSI” นั้นได้รับการฝึกอบรมความรู้ทางด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์ทั้งจากผู้เชี่ยวชาญทั้งจากในประเทศและต่างประเทศ และ มีศูนย์พิสูจน์หลักฐานทางด้านคอมพิวเตอร์ที่มีอุปกรณ์พิสูจน์หลักฐานตลอดจนโปรแกรมเฉพาะทางที่เป็นเครื่องมือให้ทีมสอบสวนทำงานได้ง่ายขึ้น แสดงให้เห็นถึงความพร้อมในการปฏิบัติงานด้าน “Computer Forensic” ซึ่งหลายหน่วยงานควรนำไปเป็นต้นแบบ จะเห็นได้ว่าหน่วยงานภาครัฐของประเทศเกาหลี ได้มีความตื่นตัวการฝึกอบรมด้านเทคโนโลยีการพิสูจน์หลักฐานคอมพิวเตอร์อย่างมาก รวมทั้งหน่วยงานระดับโลกอย่าง UNODC (United Nation Office on Drugs and Crime) ยังให้การสนับสนุน เรื่องการฝึกอบรมด้านนี้แก่ประเทศในโลกที่สาม เช่นกัน ทางประเทศไทยของเราก็ควรจัดสัมมนาเป็นฟอรัมในลักษณะ ความร่วมมือระหว่างหน่วยงานของภาครัฐ เป็นการจัดสัมมนาที่มีความเกี่ยวข้องกับกฎหมายและกระบวนการยุติธรรมโดยเน้นไปที่การพัฒนาความรู้บุคลากรให้มีความเข้าใจถึงเทคโนโลยีสมัยใหม่ ของเหล่าอาชญากรคอมพิวเตอร์ ตลอดจนการจัดตั้งคณะกรรมการผู้เชี่ยวชาญพิจารณาร่างกฎหมายการกระทำผิดเกี่ยวกับคอมพิวเตอร์เพื่อให้ความเห็นทางวิชาการที่เหมาะสม กับเทคโนโลยีดังกล่าว โดยมีวัตถุประสงค์หลักให้กฎหมายสามารถถูกนำมาใช้โดยผู้พิทักษ์กฎหมายอย่างได้ผลในทางปฏิบัติ สามารถนำตัวผู้กระทำผิดมาลงโทษได้โดยปราศจากข้อโต้แย้งทางด้านเทคนิค ดังที่ประเทศเกาหลีใต้และประเทศในเอเชียประสบความสำเร็จมาแล้วและยังมีการพัฒนาแก้ไขกฎหมายอย่างต่อเนื่อง ดังนั้นประเด็นเรื่องกฎหมายที่เหมาะสมและความรู้ทางด้านการ

พิสูจน์หลักฐานทางดิจิตอล (Digital Forensic) ของผู้พิทักษ์กฎหมายที่เพียงพอเป็นประเด็นสำคัญในระดับประเทศที่ทุกคนไม่ควรจะมองข้ามและการให้ความสำคัญกับเรื่องนี้อย่างจริงจัง

จากบทสรุปในงานประชุมผู้เชี่ยวชาญด้านอาชญากรรมคอมพิวเตอร์เมื่อวันที่ 27 – 30 มิถุนายน 2549 ที่กรุงโซล ประเทศเกาหลีใต้ ซึ่งจัดโดย KICJP (Korean Institute of Criminal Justice Policy) และ UNODC (United Nation Office on Drugs and Crime) ที่ผมได้มีโอกาสเข้าร่วมประชุมนั้น ได้เน้นถึงความสำคัญของการฝึกอบรมถ่ายทอดความรู้ด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์ หรือ “Computer Forensic” ให้กับผู้รักษากฎหมายไม่ว่าจะเป็น ตำรวจ อัยการ และผู้พิพากษา เพื่อให้มีความรู้ความเข้าใจสามารถในการพิจารณาคดี ที่เกี่ยวข้องกับ การกระทำผิดเกี่ยวกับคอมพิวเตอร์ ในยุคสมัยที่อาชญากรรมคอมพิวเตอร์มีแนวโน้มเพิ่มขึ้นเป็นทวีคูณ (แหล่งที่มา: http://www.acisonline.net)



ภาพประกอบ 2.9 สถิติอาชญากรรมคอมพิวเตอร์ในประเทศเกหลีใต้

(ที่มา: : หนังสือ eBusinessWeek และ (http://www.acisonline.net, 2019)

2.3 ผลการวิจัยที่เกี่ยวข้อง

การวิจัยองค์ความรู้เรื่อง **“ปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: กรณีศึกษา สถาบันอุดมศึกษาในเขตกรุงเทพมหานครและปริมณฑล”** เพื่อใช้เป็นแนวทางในการป้องกันการละเมิดจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศนั้น มีกรอบแนวคิดและทฤษฎีที่เกี่ยวข้องมากมาย ได้แก่หลักคำสอนของพระพุทธเจ้าเรื่องพุทธจริยศาสตร์ ได้แก่ (1).ระดับต้น
(2). ระดับกลาง และ (3). ระดับสูง และอริสโตเติล (Aristotle) รวมถึงกฎเกณฑ์ทางด้านจริยธรรมทางเทคโนโลยีสารสนเทศ โดยสมาคมผู้เป็นมืออาชีพทางเทคโนโลยีสารสนเทศ ได้ร่วมกันกำหนดขึ้น รวมถึงงานวิจัยอื่นๆ ที่นำมาอ้างอิงเพื่อใช้เป็นแนวทางในการศึกษา ดังนี้

ชาญวิทย์ พรนภดล (2561:21) หนังสือพิมพ์ประชาชาติธุรกิจ Section ไอซีที ได้รายงานเกี่ยวกับวิจัยเรื่อง **“เปิดวิจัย Cyberbullying เยาวชนไทยกับความเสี่ยงยุค 4.0”** ของภาควิชาจิตเวชศาสตร์ คณะแพทยศาสตร์ ศิริราชพยาบาล ระบุว่า การกลั่นแกล้งบนโลกไซเบอร์ หรือ Cyberbullying หมายถึง การกลั่นแกล้งโดยใช้สื่อดิจิทัล เช่น คอมพิวเตอร์ สมาร์ทโฟน แท็บเลต โพสต์ ส่ง หรือแชร์ข้อความ รูปภาพ หรือคลิปวิดีโอที่มีเนื้อหาด้านลบของผู้อื่นสู่โลกออนไลน์ เพื่อล้อเลียนให้ผู้ถูกกลั่นแกล้งอับอายหรือเสื่อมเสียชื่อเสียง

ผลการศึกษาเรื่อง **“การกลั่นแกล้งบนโลกไซเบอร์ในนักเรียนระดับมัธยมศึกษาตอนต้น”** ซึ่งได้ดำเนินการภายใต้ความร่วมมือกับอีก 13 มหาวิทยาลัยทั่วโลก อาทิ ฟินแลนด์, ลิทัวเนีย, รัสเซีย, อิสราเอล, จีน, ญี่ปุ่น, สิงคโปร์, เวียดนาม, อินเดีย, อินโดนีเซีย, ไอซ์แลนด์, นอร์เวย์, กรีซ โดยเป็นการสำรวจในช่วงระหว่างมกราคม-ธันวาคม 2560 สำหรับในประเทศไทย ได้สำรวจกลุ่มนักเรียนมัธยมต้น อายุระหว่าง 12-16 ปี จำนวน 3,667 คน จาก 8 โรงเรียนในกรุงเทพมหานคร พบว่า กลุ่มตัวอย่างใช้งานโซเชียลมีเดีย 4.8 ชั่วโมงต่อวัน ใช้งาน YouTube มากที่สุด 82.79% Line 82.17% เฟซบุ๊ค 74.48% ในจำนวนนี้ 55.9% รับคนไม่รู้จักเป็นเพื่อน ข้อมูลที่น่าสนใจและตกใจคือ 56.5% ใช้รูปจริงโชว์เป็นรูปโปรไฟล์ในการใช้งานโซเชียลมีเดีย 55.9% มีคนอื่นที่ไม่รู้จักมาก่อนเป็นเพื่อนในโซเชียลมีเดีย 46.9% เคยแชตกับคนแปลกหน้า 6.4% เคยนัดพบกับคนแปลกหน้า และ 65% เคยให้เพื่อนยืมใช้สมาร์ทโฟน ขณะที่ยัง login อยู่ บนโซเชียลมีเดีย 28% เคยลืม logout หลังเลิกใช้คอมพิวเตอร์สาธารณะ

ขณะที่การใช้งานโซเชียลมีเดียมีถึง 48% ที่มีผู้อื่นรู้รหัสผ่านเข้าบัญชีใช้งาน ซึ่ง 32.5% คือเพื่อน อีก 26.3% คือพ่อแม่ และ 80% รู้วิธีการตั้งค่าความเป็นส่วนตัวในการใช้งาน แต่มีเพียง 39% เท่านั้นที่ตั้งไว้ตลอดเวลา กว่า 30% เคยแกล้ง-ถูกแกล้ง โดย 37.8% เคยถูกกลั่นแกล้ง และ 34.6% เคยแกล้งผู้อื่น ซึ่งเมื่อแยกตามเพศแล้ว เพศหญิงจะเคยแกล้งผู้อื่น 37% เคยถูกแกล้ง 40.8% ขณะที่เพศชาย 32% เคยแกล้งผู้อื่น และ 34.7% จะเคยถูกแกล้ง ทั้งยังมีถึง 39.1% ที่เคยแชร์หรือกลไลก์เวลาเห็นข้อความ รูปภาพ หรือคลิปของเพื่อนที่กำลังถูกแกล้งบนโลกไซเบอร์ (bystander)

ส่วนผลกระทบที่เกิดขึ้น หลังถูก Cyberbullying พบว่า มี 2.2% ที่จะไปโรงเรียน 6.6% ครอบครัวไม่เข้าใจตำหนิ ซ้ำเติม 8.3% เพื่อนเข้าใจผิดเลิกคบ 9% นอนไม่หลับ 18.6 ต้องการแก้แค้น 23.1% เศร้า เครียด วิตกกังวล และ 32.1% รู้สึกโกรธ **ยิ่งเสพติดออนไลน์ยิ่งเสี่ยงสูง** กลุ่มที่กลั่นแกล้งผู้อื่นยังมีพฤติกรรมเกเร สมาธิสั้น มีปัญหาด้านอารมณ์และจิตใจ ขณะที่พฤติกรรมติดสื่อสังคมออนไลน์ยังมีความสัมพันธ์กับการเป็นผู้กลั่นแกล้ง ผู้ถูกแกล้ง ผู้ที่ร่วมกดไลก์กดแชร์ (bystander)

“คนที่ติดสังคมออนไลน์มากมีแนวโน้มจะเป็นผู้กลั่นแกล้งผู้อื่นบนโลกไซเบอร์มากกว่าคนที่ไม่ติดออนไลน์ถึง 3.25 เท่า ในทางกลับกัน ผู้ที่ติดสังคมออนไลน์มากก็มีแนวโน้มจะเป็นผู้ถูกกลั่นแกล้งบนโลกไซเบอร์มากกว่าคนที่ไม่ติดถึง 2.13 เท่า ทั้งยังมีแนวโน้มที่จะเป็นผู้กดไลก์/แชร์ข้อความ รูปภาพ หรือคลิปที่กำลังถูกแกล้งบนโลกไซเบอร์มากกว่าคนที่ไม่ติดออนไลน์ 2.38 เท่า” **หยุดพฤติกรรมเสี่ยง** รศ.นพ.ชาญวิทย์ย้ำว่า การใช้งานอินเทอร์เน็ตอย่างปลอดภัยมีผลสัมพันธ์กับความเสี่ยงที่จะถูกกลั่นแกล้งบนโลกออนไลน์อย่างมาก การเปิดเผยข้อมูลส่วนตัวมากยิ่งเป็นความเสี่ยง ทั้งการรับคนอื่นที่ไม่รู้จักมาก่อนมาเป็นเพื่อน การแชตหรือการออกไปพบกับคนแปลกหน้า ใช้รูปจริงเป็นรูปโปร์ไฟล์ การไม่ตั้งค่าความเป็นส่วนตัวในการใช้งาน การปล่อยให้ผู้อื่นรู้รหัสเข้าใช้งาน รวมถึงการไม่ logout ออกเมื่อใช้งานเสร็จหรือให้ผู้อื่นยืมโทรศัพท์

“การแก้ไขปัญหาอย่างยั่งยืนจะต้องมองไปที่ต้นตอของปัญหา นั่นคือการสร้างวัฒนธรรมการใช้อินเทอร์เน็ตอย่างปลอดภัยและสร้างสรรค์ ซึ่งจำเป็นต้องอาศัยความร่วมมือระหว่างภาครัฐ เอกชน และประชาสังคม ในการร่วมกันแก้ปัญหาและปลูกฝังวัฒนธรรมนี้” **เด็กเปลี่ยนวิธีสร้างสัมพันธ์ “ลาร์ส นอร์ลิ่ง”** ประธานเจ้าหน้าที่บริหาร บมจ.โทเทิ่ล แอ็คเซ็ส คอมมูนิเคชั่น (ดีแทค) เปิดเผยว่า จากข้อมูลล่าสุดเกี่ยวกับการสำรวจความคิดเห็นของครัวเรือนในประเทศไทยเกี่ยวกับการใช้ไอซีที เมื่อปี 2560 โดยสำนักงานสถิติแห่งชาติ พบว่า การใช้อินเทอร์เน็ตของวัยรุ่นมีสูงถึง 80-90% โดยผู้ที่มีอายุ 19-25 ปี 95.6% ใช้อินเทอร์เน็ตผ่านทางสมาร์ทโฟน **“การเปลี่ยนแปลงข้อมูลดิจิทัลทำให้โลกเปลี่ยนไป เด็กๆ เปลี่ยนวิธีที่จะสร้างและรักษาความสัมพันธ์กับเพื่อนของตนเอง รวมถึงการใช้เวลาว่างด้วยการฟีดวิดีโอ วิดีโอโซเชียลมีเดียและเกมแบบ immersive อย่างต่อเนื่อง ซึ่งมีความเสี่ยงที่จะทำให้เกิดการกลั่นแกล้งบนอินเทอร์เน็ตและภาวะซึมเศร้าในที่สุด”**

ดีแทคจึงได้จัดทำโครงการ Safe Internet ตั้งแต่ปี พ.ศ.2557 ซึ่งที่ผ่านมาได้มีการจัดเวิร์กช็อปให้ความรู้กับนักเรียนกว่า 27,000 คนทั่วประเทศ รวมถึงเปิดบริการห้องแชต “Child Chat Line” เพื่อให้คำปรึกษากับเด็กๆ ที่มีปัญหาถูกกลั่นแกล้ง โดยตั้งแต่ มิ.ย.2560 มีผู้เข้ามาปรึกษาแล้ว 278 คน และมีผู้เข้าชมเว็บไซต์กว่า 40,000 ครั้ง เป็นสิ่งยืนยันถึงปัญหานี้ในกลุ่มเด็กและเยาวชน

ดีอีเปิดช่องปรึกษา “พิเชฐ ดุรงคเวโรจน์” รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอี) กล่าวว่า ผลกระทบจากการใช้อินเทอร์เน็ตในกลุ่มเด็กและเยาวชน เริ่มเห็นปัญหาได้ชัดขึ้น จึงได้บริการให้คำปรึกษาผ่าน “Stop Bullying Chat Line” ทั้งจะประสานกับกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลย (ปอท.) เพื่อให้เข้ามาให้คำปรึกษาเบื้องต้นทางเทคนิคสำหรับการส่งต่อกรณีที่มีการกลั่นแกล้งรังแกบนโลกออนไลน์ ในช่วงเวลา 16.00-22.00 น.ของทุกวัน รวมถึงจัดกิจกรรมอบรมการใช้อินเทอร์เน็ตอย่างปลอดภัยผ่านศูนย์ดิจิทัลชุมชนด้วย

ณมน จีรังสุวรรณ (2561:2) การวิเคราะห์ผลกระทบทางเทคโนโลยีสารสนเทศและการสื่อสารกับนักสื่อสารมวลชนอิเล็กทรอนิกส์

การวิจัยพบว่า 3. ปัจจัยที่ส่งผลกระทบต่อการปรับตัวของนักสื่อสารมวลชน อิเล็กทรอนิกส์ พบว่า ปัจจัยทางเทคโนโลยีสารสนเทศและการสื่อสารส่งผลให้ รูปแบบการใช้ชีวิตของผู้บริโภคข่าวสารเปลี่ยนไป ท าให้การอ่านหนังสือพิมพ์ฉบับ กระดาษลดน้อยลง ท าให้องค์กรสื่อสารมวลชนจ าเป็นต้องขยายรูปแบบการ น าเสนอไปบนสื่ออื่น เช่น อินเทอร์เน็ต บนเครือข่ายสังคมออนไลน์ สมาร์ทโฟน เพื่อหารายได้และท าก าไรให้กับองค์กร เป็นลักษณะการปรับเปลี่ยนบริบททาง นโยบายให้สอดคล้องกับเทคโนโลยีและสภาพแวดล้อม ปัจจัยทางเศรษฐกิจ ในด้านต้นทุนของกระดาษและ

ค่าแรงงานที่เพิ่ม สูงขึ้น เป็นแรงกดดันที่ท าให้สื่อต้องแสวงหารายได้จากช่องทางสื่อ Media Outlets ใหม่ๆจากทรัพยากรข่าวที่มีอยู่ เพราะในอนาคตองค์กรสื่อจะพึ่งพารายได้จากสื่อ สิ่งพิมพ์แบบดั้งเดิม อย่างหนังสือพิมพ์ได้น้อยลง ปัจจัยที่ส่งผลกระทบอีกปัจจัยหนึ่งคือ การมีส่วนร่วมของภาค ประชาชน ในบทบาทของการเป็น นักข่าวพลเมือง (Citizen Journalism) ที่ประชาชน ทั่วๆ ไปที่ไม่ได้ผ่านการ ฝึกฝนให้เป็นนักข่าวมืออาชีพ แต่สามารถใช้เครื่องมือ อุปกรณ์เทคโนโลยีอันทันสมัย รวมถึงการใช้ อินเทอร์เน็ตในการสร้างสรรค์ โต้แย้ง หรือตรวจสอบข้อมูลของสื่อด้วยตัวเอง

ณัฐนันท์ ศิริเจริญ (2558:52-53) รูปแบบการสื่อสารเพื่อการรู้เท่าทันสื่อและสารสนเทศจากสื่ออินเทอร์เน็ตของเยาวชนไทย

การวิจัยพบว่า รูปแบบการสื่อสารเพื่อการรู้เท่าทันสื่อและสารสนเทศ ที่มีประสิทธิภาพมีอยู่ 3 รูปแบบ คือ (1) รูปแบบการสื่อสารที่มุ่งเน้นเพื่อบอกสอนชี้แนะเรื่อง “การสื่อสารกับตนเอง หรือการสื่อสารภายในบุคคล” มาเป็นอันดับแรกที่สำคัญมาก เพราะโดยพื้นฐานแล้ว การชี้แนะบอก สอนให้เยาวชนรู้จักที่จะทำการสื่อสารภายในตนเองให้เป็นไปในทางที่ถูกต้องเหมาะสม ถือว่าเป็น ปัจจัยสำคัญมากที่สุดอันดับแรกของมนุษย์ทุกคนทุกเพศทุกวัย (2) การมุ่งเน้นนำเสนอเนื้อหา สอดแทรกในละครวัยรุ่น ซึ่งแอบแฝงด้วยความบันเทิงผสมกับความรู้เนื้อหาสาระด้านวิชาการที่ สะท้อนให้เห็นถึงลักษณะชีวิตความเป็นอยู่ ค่านิยม ขนบธรรมเนียมประเพณี และศิลปวัฒนธรรมใน ด้านต่างๆ ของสังคมนั้นๆ ได้เป็นอย่างดี (3) การมุ่งเน้นที่ใช้สื่ออินเทอร์เน็ตที่เป็นเว็บไซต์เฉพาะเรื่องที่ ถูกออกแบบมาอย่างเหมาะสม เพื่อให้เป็นที่ดึงดูดใจและทำให้น่าสนใจในสายตาของเยาวชน

ธีรินทร์ เกตุวิชิต (2557:74-75) การพัฒนาระบบแลกเปลี่ยนสารสนเทศทางการแพทย์ในระบบส่งต่อผู้ป่วย

ผลการวิจัยพบว่า ได้พัฒนาระบบการส่งต่อข้อมูลทางการแพทย์ในการส่งต่อผู้ป่วย ผ่านเว็บ เซอร์วิสเจสัน เพื่อการแลกเปลี่ยนข้อมูลทางการแพทย์ระหว่างระบบสารสนเทศ สามารถเชื่อมโยง ข้อมูลส่งต่อผู้ป่วย และมีความพึงพอใจของบุคลากรด้านสาธารณสุขที่เกี่ยวข้อง สามารถใช้งานได้ อย่างง่ายๆ ไม่ยุ่งยากซับซ้อน ลดการทำงานที่ซ้ำซ้อนลง

ประชาชาติธุรกิจ, 2561:3) หนังสือพิมพ์ประชาชาติธุรกิจ Section ไอซีที ได้รายงาน เกี่ยวกับวิจัยเรื่อง **“เปิดวิจัย Cyberbullying เยาวชนไทยกับความเสี่ยงยุค 4.0”** ความว่า เยาวชน ไทย 55.9% รับคนที่ไม่รู้จักเป็นเพื่อน กว่า 30% เคยแกล้ง-ถูกแกล้ง 39.1% เคยแชร์หรือกดไลก์เวลา เห็นข้อความ รูปภาพ หรือคลิปของเพื่อนที่กำลังถูกแกล้งบนโลกไซเบอร์ (Bystander)

ประจิต ลิ้มสายพรหม (2557:200-201) ตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและ วิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์ โดยใช้เทคนิคเหมืองข้อมูลและ โครงข่ายกราฟ

ผลการวิจัยพบว่า ตัวอย่างชุดข้อมูลประเทศไทย เดือนเมษายน 2556 พบความผิดปกติและ โอกาสถูกโจมตีสูงสุดด้วยการกระทำให้ระบบสื่อสารขัดข้องสูงถึง 16.10% รองลงมาเป็นความผิดปกติ ของ HTTP 12.85% และถูกเปิดเผยข้อมูลโดยผู้บุกรุกที่ใช้เส้นทางในการเข้าถึงข้อมูลข่าวสารผ่านมาง ระบบที่ตกเป็นเหยื่อ 12.30%

ประสงค์ ประณีตพลกรัง (2558:43) ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

สรุปว่า กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความมั่นคงปลอดภัยของข้อมูลข่าวสาร ทั้งในรูปแบบเชิงกายภาพและ อิเล็กทรอนิกส์ ความมั่นคงปลอดภัยของระบบ และเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และ

กระจายข้อมูล Cyber Security ยังรวมถึงการระวังป้องกันต่ออาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม อุบัติเหตุ และความผิดพลาดต่างๆ อีกด้วย

ธนกร มีหินกอง (2556:96) ตัวแบบการจัดหารการบุกรุกเชิงเวลาจริงแบบปรับตัวในการรักษาความมั่นคงปลอดภัยไซเบอร์บนพื้นฐานของสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ผลการวิจัยพบว่า ระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับสถาบันกรมพลศึกษาโดยรวมอยู่ในระดับปานกลางมีค่าเฉลี่ย 2.80 และทุกด้านมีระดับความพร้อมปานกลาง ด้านที่มีค่าเฉลี่ยสูงสุดคือด้านกายภาพสิ่งแวดล้อมมีค่าเฉลี่ย 3.00 ด้านที่มีค่าเฉลี่ยต่ำที่สุดคือด้านการจัดการเหตุการณ์ มีค่าเฉลี่ย 2.63 นอกนั้น มีค่าเฉลี่ยเรียงตามลำดับจากสูงไปหาต่ำคือ ด้านบุคลากรค่าเฉลี่ย 2.94 ด้านการจัดการทรัพย์สินค่าเฉลี่ย 2.93 ด้านนโยบายและโครงสร้างค่าเฉลี่ย 2.90 ด้านการบริหารจัดการค่าเฉลี่ย 2.88 ด้านการจัดกาพัฒนาบำรุงค่าเฉลี่ย 2.75 ด้านปฏิบัติตามข้อกำหนดค่าเฉลี่ย 2.72 ด้านการควบคุมการเข้าถึงสารสนเทศค่าเฉลี่ย 2.71 ด้านการบันทึกและจัดเก็บสารสนเทศค่าเฉลี่ย 2.69 ด้านการแลกเปลี่ยนข้อมูลค่าเฉลี่ย 2.69

ศักดิ์ เสกขุนทด (2560:7) งานวิจัยด้านธุรกรรมอิเล็กทนอนิกส์

สรุปว่า ผลกระทบต่อการทำงานในยุคดิจิทัล คือ **การทำงานแบบเดิม คือ** (1) จัดเก็บข้อมูลโดยเอกสาร (2) ปกปิด (3) เชิงรับและทำงานประจำวัน (4) ทำงานแบบแยกส่วน. **การทำงานแบบใหม่ คือ** (1) จัดเก็บข้อมูลในรูปแบบดิจิทัล (2) เปิดเผยความโปร่งใสและส่งเสริมการมีส่วนร่วม (3) เชิงรุก และสร้างสรรค์ (4) ทำงานแบบบูรณาการ

ผลการทดสอบสมมติฐานพบว่า ความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับสถาบันการพลศึกษา ไม่เป็นไปตามสมมติฐานที่ตั้งไว้ นั่นคือมีระดับความพร้อมฯ อยู่ในระดับปานกลาง มีค่าเฉลี่ยเท่ากับ 2.80

Dag Elgesem (2017:1) What is special about the ethical issues in online research?

สรุปว่า ในการวิเคราะห์ปัญหาทางจริยธรรมของการวิจัยทางออนไลน์ มีปัญหาหนึ่งเกี่ยวกับการวิจัยทางออนไลน์ ที่คล้ายคลึงกัน คือ รูปแบบการวิเคราะห์ความเป็นส่วนตัว การปกป้องความเป็นส่วนตัว และการป้องกันข้อมูล

Elizabeth A. Buchahan, Erin E. Hvizdak (2017:1) Online Survey Tools: Ethical and Methodological Concerns of Human Research Ethics Committees

สรุปว่า จากการสำรวจคณะกรรมการจรรยาบรรณด้านการวิจัยของมหาวิทยาลัยในประเทศสหรัฐอเมริกา (750 HRECs) จำนวน 750 คน เปิดเผยว่า การวิจัยทางอินเทอร์เน็ตที่เกี่ยวข้องกับการสำรวจออนไลน์หรือเว็บไซต์ (94% ของผู้ตอบแบบสอบถาม) แสดงให้เห็นถึงความแพร่หลายของงานวิจัยทางด้านวิชาการด้านนี้มีเพิ่มขึ้นมาก ผู้ตอบแบบสำรวจชี้ให้เห็นว่า ลักษณะทางอิเล็กทรอนิกส์และออนไลน์ของข้อมูลการสำรวจเหล่านี้ ส่วนใหญ่เป็นเรื่องท้าทายหลักการจริยธรรมในการวิจัยแบบดั้งเดิม เช่น ความยินยอมรับความเสี่ยง การละเมิดความเป็นส่วนตัว การเปิดเผยข้อมูล, การรักษาความลับ เป็นต้น

George W Reynolds (2012:22) จริยธรรมในด้านเทคโนโลยีสารสนเทศ (Ethics in Information Technology)

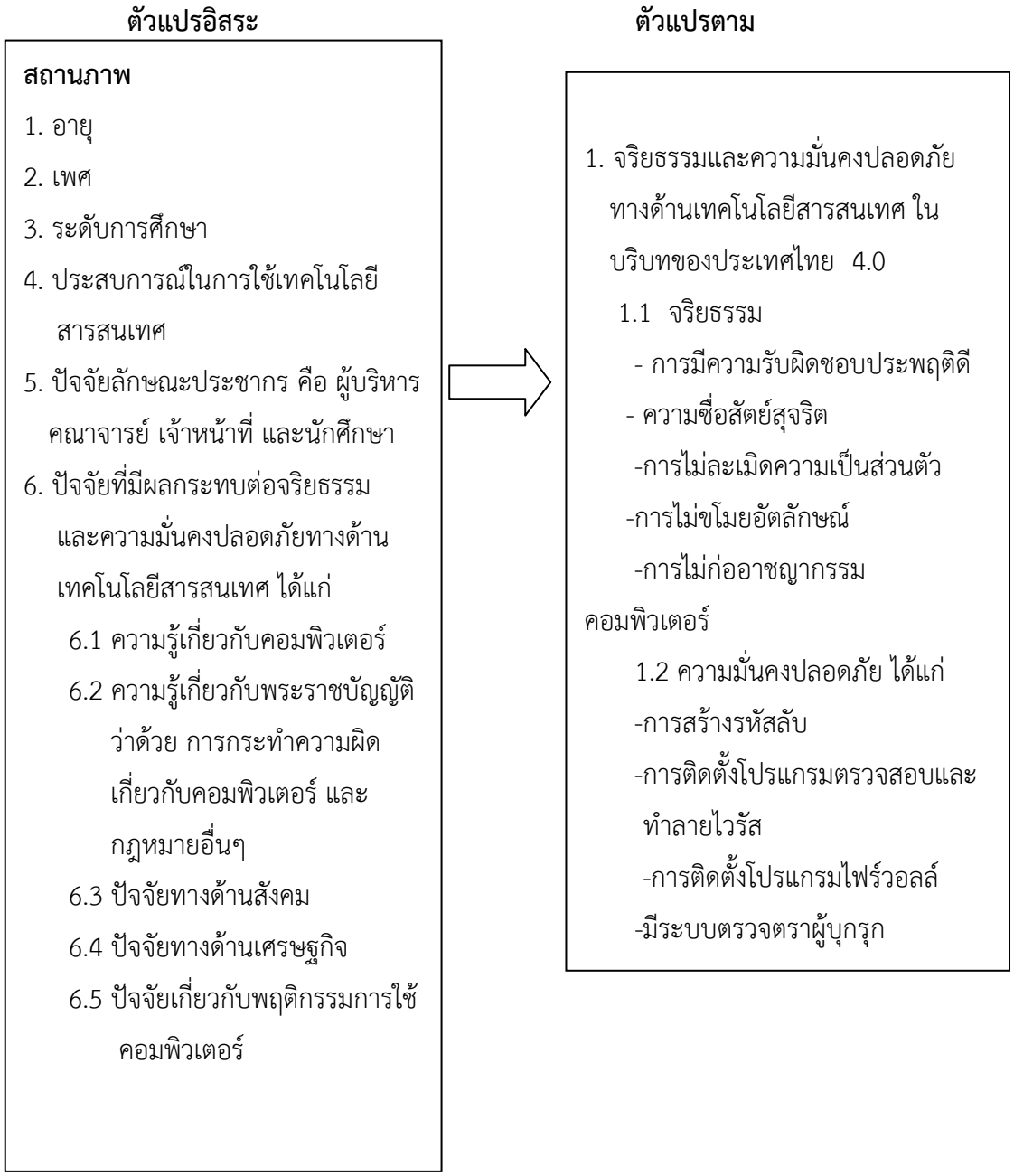
สรุปความว่า ด้วยปัจจุบันอินเทอร์เน็ตมีการเจริญเติบโตขึ้นอย่างรวดเร็ว ความสามารถในการดึง และการจัดเก็บข้อมูลส่วนบุคคลมีจำนวนมหาศาล ความไว้วางใจในระบบสารสนเทศก็มีมากขึ้นด้วย ในขณะเดียวกันในอีกมุมมองหนึ่ง ก็มีความเสี่ยงในการดำเนินชีวิตมากขึ้นด้วย นั่นก็คือ มีการใช้เทคโนโลยีสารสนเทศอย่างไม่มีจริยธรรม ขาดความรับผิดชอบของบางกลุ่ม บางคน เนื่องจากในปัจจุบันเทคโนโลยีสารสนเทศสามารถเข้าได้ง่ายจากอุปกรณ์คอมพิวเตอร์ลักษณะต่างๆ ไม่ว่าจะเป็นสมาร์ทโฟน แท็บเล็ต เป็นต้น มีวิธีการทำลายและการโจมตีผ่านเทคโนโลยีสารสนเทศ ซึ่งส่วนใหญ่แล้วจะเกี่ยวข้องกับละเมิดจริยธรรมในการใช้เทคโนโลยีสารสนเทศ ได้แก่ พนักงานมีการถูกตรวจสอบติดตามจากนายจ้าง, การดาวน์โหลดเพลง ซอฟต์แวร์ และภาพยนตร์ ที่ละเมิดกฎหมายลิขสิทธิ์,การส่งอีเมลที่ไม่ได้รับเชิญ เป็นจำนวนมากเพื่อใช้ในการโฆษณาสินค้าและสร้างความรำคาญให้กับผู้อื่น, การเจาะระบบเข้าสู่ฐานข้อมูลของสถาบันการเงินและบริษัทค้าปลีก เพื่อที่จะขโมยข้อมูลลูกค้า เป็นต้น

2.4 สรุป

สังคมสารสนเทศ (The Information Society) คลังศัพท์ไทย ได้ให้นิยามคำว่าสังคมสารสนเทศเอาไว้ว่า คือสังคมที่มีการนำข้อมูลสารสนเทศในรูปแบบต่างๆ มาช่วยดำเนินกิจกรรมทั้งเพื่อประโยชน์ส่วนตนและประโยชน์ส่วนรวม สารสนเทศจะเป็นสิ่งที่เป็นพื้นฐานสู่การขับเคลื่อนต่าง ๆ ของโลก สังคมอุตสาหกรรม เศรษฐกิจ และวัฒนธรรม ต่างถูกขับเคลื่อนด้วยข้อมูลข่าวสาร ทำให้มีการกำหนดร่วมกันว่า ยุคปัจจุบันคือยุคของสังคมสารสนเทศ หรือยุคของสังคมข้อมูลข่าวสาร ในทศวรรษที่ผ่านมา เทคโนโลยีสารสนเทศซึ่งรวมทั้งเทคโนโลยีคอมพิวเตอร์ และเทคโนโลยีการสื่อสาร (ICT: Information and Communication Technology) อีกทั้งยังรวมถึงเทคโนโลยีนำสมัยอื่น ๆ เช่น เทคโนโลยีชีวภาพและพันธุวิศวกรรมศาสตร์ ได้ก่อให้เกิดผลกระทบเกี่ยวกับกิจกรรมต่าง ๆ ของสังคม รวมทั้งกิจกรรมทางเศรษฐกิจอย่างกว้างขวาง ส่วนความหมายของ Thailand 4.0 คือ เป็นวิสัยทัศน์เชิงนโยบายโมเดลพัฒนาเศรษฐกิจของรัฐบาลที่ยึดหลัก **“มั่นคง มั่งคั่ง และยั่งยืน”** เพื่อรับมือกับการเปลี่ยนแปลงของโลกที่มีการเปลี่ยนแปลงอย่างรวดเร็ว ทำให้ประเทศไทยจำเป็นต้องมี Innovation หรือนวัตกรรม จึงจะสามารถแข่งขันกับประเทศอื่นได้

สำหรับกรอบแนวคิดและทฤษฎีของผู้วิจัยเองนั้น ใน**ตอนที่ 1** คือ ตัวแปรอิสระประกอบด้วย (1). (2). อายุ (3). เพศ (4). ระดับการศึกษา (5). ประสบการณ์ในการใช้เทคโนโลยีสารสนเทศ **ตอนที่ 2** ปัจจัย ประกอบด้วย (1).ปัจจัยลักษณะประชากร คือ ผู้บริหาร คณาจารย์ เจ้าหน้าที่ และนักศึกษา (2).ปัจจัยที่มีผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ได้แก่ ความรู้เกี่ยวกับคอมพิวเตอร์, ความรู้เกี่ยวกับพระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นๆ ปัจจัยทางด้านสังคม, ปัจจัยทางด้านเศรษฐกิจ, ปัจจัยเกี่ยวกับพฤติกรรมการใช้คอมพิวเตอร์

ส่วนตัวแปรตามประกอบด้วย (1). จริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 แยกย่อยออกมาเป็น จริยธรรม คือ การมีความรับผิดชอบประพฤติดี, ความซื่อสัตย์สุจริต, การไม่ละเมิดความเป็นส่วนตัว,การไม่ขโมยอัตลักษณ์, และการไม่ก่ออาชญากรรมคอมพิวเตอร์



จริยธรรมในการใช้อินเทอร์เน็ต มีผลการวิจัยพบว่า ส่วนใหญ่ใช้โทรศัพท์มือถือเป็นอุปกรณ์ในการเข้าถึงอินเทอร์เน็ต และใช้ที่บ้าน ศึกษาการใช้อินเทอร์เน็ตด้วยตนเอง พอมีความรู้บ้างเกี่ยวกับกฎหมายในการใช้อินเทอร์เน็ต ใช้ระบบเครือข่ายอินเทอร์เน็ตเพื่อความบันเทิง เพื่อค้นหาข้อมูลภายในประเทศและจากต่างประเทศ ผลการทดสอบสมมติฐานพบว่า เพศ อายุ และระดับชั้นการศึกษา มีผลต่อคุณธรรม จริยธรรมในการใช้อินเทอร์เน็ตในภาพรวม และช่วงเวลา สถานที่ในการใช้อินเทอร์เน็ต การใช้ระบบเครือข่ายอินเทอร์เน็ตมีผลต่อคุณธรรม จริยธรรมในการใช้อินเทอร์เน็ตในภาพรวม ส่วนกรณีของอาชญากรรมคอมพิวเตอร์ เหตุการณ์ที่เกิดขึ้นส่วนใหญ่เกี่ยวข้องกับการฉ้อโกงทางคอมพิวเตอร์,การปลอมแปลงข้อมูลคอมพิวเตอร์, การเจาะระบบคอมพิวเตอร์, การจารกรรมข้อมูล

ส่วนบุคคลหรือข้อมูลทางการค้า การพนันผิดกฎหมายออนไลน์ รวมไปถึงการเผยแพร่ภาพลามกอนาจารเด็กและเยาวชน เป็นต้น

ท้ายสุดเป็นเรื่องของผลกระทบจากการใช้สื่อสังคมออนไลน์ประเภทเฟซบุ๊คต่อนักศึกษาเรียง ตามลำดับคือ ด้านสุขภาพ ด้านการดำเนินชีวิตประจำวันและด้านการศึกษาตามลำดับ โดยผลกระทบด้านสุขภาพพบว่ามีอาการปวดตา ปวดศรีษะ เมื่อยมือ ปวดไหล่ เวลาเล่นนาน ๆ ผลกระทบด้านการดำเนินชีวิตประจำวัน พบว่านักศึกษาเลือกใช้งานเฟซบุ๊คมากกว่าทำกิจกรรมอื่นในช่วงเวลาว่าง ทำให้ทำกิจกรรมอื่นน้อยลง มีโลกส่วนตัวสูง คุยกับคนในครอบครัวน้อยลง คนรอบข้างรู้สึกหงุดหงิด หวาดระแวง และเกิดการทะเลาะกัน เนื่องจากความคิดเห็นไม่ตรงกัน และผลกระทบด้านการศึกษา พบว่านักศึกษาทำการบ้านและงานที่รับมอบหมายต่างๆ เสร็จช้า เนื่องจากใช้เวลาส่วนใหญ่อยู่กับการใช้งานเฟซบุ๊ค ผลกระทบที่ตามมาพบว่านักศึกษาไม่ส่งงาน ส่งงานช้า ขาดสมาธิในการเรียน เกรดตกในบางรายวิชา ขาดสมาธิในการทำงานและการอ่านหนังสือสอบ ขาดเรียน ใช้ภาษาไม่ถูกต้องใช้คำแสลงในยุคสมัยใหม่ และสะกดคำไม่ถูกต้องตามหลักภาษา

บทที่ 3

ระเบียบวิธีวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณ เพื่อศึกษาปัจจัยและปัญหาของผู้ใช้เทคโนโลยีสารสนเทศ ที่ได้รับผลกระทบจากการละเมิดจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ของสถาบันอุดมศึกษาในเขตกรุงเทพมหานคร และปริมณฑล โดยแยกประเด็นออกเป็น 5 เรื่องหลัก คือ (1). ศึกษาถึงปัญหาการละเมิดจริยธรรมและภัยคุกคามความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในเขตกรุงเทพมหานคร และปริมณฑล (2). ศึกษาถึงประเภทของการละเมิดจริยธรรม และภัยคุกคามทางด้านเทคโนโลยีสารสนเทศ (3). ศึกษาถึงจริยธรรมทางธุรกิจทั่วไป และสำหรับคนที่ทำงานทางด้านเทคโนโลยีสารสนเทศ (4). ศึกษาวิเคราะห์ถึงปัจจัยที่มีผลผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ และ (5).เพื่อศึกษาหาแนวทางป้องกันและการแก้ไขปัญหาเกี่ยวกับการละเมิดจริยธรรมและความปลอดภัยทางด้านเทคโนโลยีสารสนเทศโดยมีขั้นตอนการดำเนินงาน ได้เลือกกลุ่มประชากรตัวอย่าง 58 สถาบันตามที่มีการส่งรายงานข้อมูลมาที่สำนักงานคณะกรรมการอุดมศึกษา (สกอ.) งานวิจัยมีแบบแผนการวิจัย ดังนี้

3.1 แบบแผนทางการวิจัย

ดำเนินการสร้างแบบสอบถาม นำแบบสอบถามไปแจกตามสถาบันอุดมศึกษาในเขตกรุงเทพมหานคร และปริมณฑล ทั้งบุคลากรและนักศึกษาจาก 61 สถาบัน พร้อมเก็บรวบรวม นำเนื้อหารายละเอียดของแบบสอบถามเกี่ยวกับปัญหาการละเมิดจริยธรรมและภัยคุกคามควาปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในเขตกรุงเทพมหานคร และปริมณฑล, ประเภทของการละเมิดจริยธรรม และภัยคุกคามทางด้านเทคโนโลยีสารสนเทศ, กฎเกณฑ์จริยธรรมทางธุรกิจทั่วไป และสำหรับคนที่ทำงานทางด้านเทคโนโลยีสารสนเทศ, การวิเคราะห์ถึงปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศต่อสถาบันอุดมศึกษา รวมถึงสังคมและประเทศไทย, แนวทางป้องกันและการแก้ไขปัญหาเกี่ยวกับการละเมิดจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศเมื่อสิ้นสุดปี พ.ศ. 2561 แล้ว นำข้อมูลที่ได้มาทำการวิเคราะห์ด้วยสถิติเชิงพรรณา และสถิติเชิงอนุมาน สรุปผลและเขียนรายงานวิจัยในชั้นองค์ความรู้

3.2 ขั้นตอนการดำเนินงาน

ดำเนินการเขียน แบบเสนอโครงการวิจัยสำหรับบุคลากรภายใน (FM วจ.-01), ดำเนินการหาผู้ทรงคุณวุฒิมาเป็นที่ปรึกษาในการทำวิจัย จัดเตรียมรวบรวมเนื้อหารายละเอียดของ ปัจจัยที่มีผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศจากห้องสมุดและการศึกษาค้นคว้าจากสื่ออินเทอร์เน็ต สอบถามผู้มีประสบการณ์การทำวิจัย เข้ารับการฝึกอบรมในการ

ทำวิจัย ติดต่อสำนักวิจัยของมหาวิทยาลัย เพื่อนำรายละเอียดข้อมูลต่างๆ มาบูรณาการประกอบการศึกษา การตั้งคำถามวิจัย การเขียนเสนอโครงการวิจัย และการวิเคราะห์ถึงข้อดีข้อเสีย และสรุปผลการวิจัยและเขียนรายงาน

3.3 ประชากรและกลุ่มตัวอย่าง

ประชากร คือ ผู้บริหาร คณาจารย์ พนักงาน นักศึกษา จากสถาบันอุดมศึกษาในเขตกรุงเทพมหานคร และปริมณฑลรวม 61 สถาบัน โดยแบ่งกลุ่มมหาวิทยาลัยออกตามลักษณะของมหาวิทยาลัย ได้แก่ (1). มหาวิทยาลัยของรัฐบาล (จำกัดจำนวนรับ) (2). มหาวิทยาลัยราชภัฏ (3). มหาวิทยาลัยราชมงคล และ (4). มหาวิทยาลัยเอกชน บุคลากรทั้งสิ้น 38,591 คน และนักศึกษารวมทั้งสิ้น 696,796 คน ใช้การสุ่มตัวอย่างแบบหลายขั้นตอนโดย

ขั้นตอนที่ 1 จำแนกมหาวิทยาลัยออกเป็น 4 กลุ่ม ตามลักษณะของมหาวิทยาลัยได้แก่ มหาวิทยาลัยของรัฐบาล(จำกัดจำนวนรับ) มหาวิทยาลัยราชภัฏ มหาวิทยาลัยราชมงคล และ มหาวิทยาลัยเอกชน แล้วใช้วิธีการสุ่มตัวอย่างแบบชั้นภูมิกำหนดจำนวน 10 สถาบัน ดังตารางที่ 1

ตารางที่ 3.1. จำนวนมหาวิทยาลัยจำแนกตามกลุ่ม

มหาวิทยาลัย	จำนวนประชากร	จำนวนตัวอย่าง
1) มหาวิทยาลัยของรัฐบาล	12	2
2) มหาวิทยาลัยราชภัฏ	7	1
3) มหาวิทยาลัยราชมงคล	7	1
4) มหาวิทยาลัยเอกชน	35	6
รวม	60	10

ขั้นตอนที่ 2 สุ่มตัวอย่างมหาวิทยาลัยจากแต่ละกลุ่มโดยการสุ่มตัวอย่างอย่างง่ายด้วยวิธีจับฉลาก ได้มหาวิทยาลัยที่ใช้เป็นตัวอย่างดังตาราง 2

ขั้นตอนที่ 3 กำหนดขนาดตัวอย่างของจำนวนบุคลากรที่จะใช้ในการเก็บรวบรวมข้อมูลจากจำนวนประชากรใน 10 สถาบัน ด้วยวิธีการกำหนดขนาดของ ทอมสัน (Thompson, S.K.2002) ที่ระดับความเชื่อมั่น 99% ค่าความคลาดเคลื่อน (e) เท่ากับ 0.05 สัมประสิทธิ์ความผันแปรของประชากร (CV) เท่ากับ 0.5 ได้ขนาดตัวอย่างดังนี้

จำนวนตัวอย่างบุคลากร

$$n = \frac{1}{\frac{e^2}{Z^2(CV)^2} + \frac{1}{N}}$$

N แทน จำนวนประชาชนทั้งหมด

n แทน จำนวนตัวอย่าง

จำนวนตัวอย่างบุคลากร

$$n = \frac{1}{\frac{.05^2}{2.575^2(.5)^2} + \frac{1}{8,900}}$$

= 617 ตัวอย่าง

จำนวนตัวอย่างนักศึกษา

$$n = \frac{1}{\frac{.05^2}{2.575^2(.5)^2} + \frac{1}{172,312}}$$

= 661 ตัวอย่าง

ตารางที่ 3.2 จำนวนประชากรกลุ่มตัวอย่างของแต่ละมหาวิทยาลัย
(ที่มา : สำนักงานคณะกรรมการการอุมศึกษา (สกอ.)
(www.info.mua.go.th) ณ วันที่ 13 กรกฎาคม พ.ศ. 2560

สถาบัน	จำนวนบุคลากร		จำนวนนักศึกษา	
	ประชากร	ตัวอย่าง	ประชากร	ตัวอย่าง
1. มหาวิทยาลัยศรีนครินทรวิโรฒ	1,176	82	23,316	90
2. มหาวิทยาลัยธรรมศาสตร์	2,297	159	35,903	138
3. มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี	993	69	25,390	97
4. มหาวิทยาลัยราชภัฏจันทรเกษม	353	24	11,168	43
5. มหาวิทยาลัยเทคโนโลยีมหานตร	340	24	5,101	20
6. มหาวิทยาลัยกรุงเทพ	1,473	102	20,505	79
7. มหาวิทยาลัยศรีปทุม	712	49	21,146	81
8. มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ์	517	36	10,113	39
9. มหาวิทยาลัยอัสสัมชัญ	896	62	15,857	61
10. มหาวิทยาลัยราชพฤกษ์	143	10	3,813	15
รวม	8,900	617	148,996	661

ขั้นตอนที่ 4 สุ่มตัวอย่างแบบบังเอิญจากมหาวิทยาลัยทั้ง 10 แห่ง ตามจำนวนขนาดตัวอย่างที่ได้จากการคำนวณสัดส่วนในประชากรรวมเป็นจำนวนบุคลากร 617 ราย และ นักศึกษา 661 ราย รวมทั้งหมด 1,278 ราย ดังตารางที่ 2

ตัวแปรที่ศึกษา

ตัวแปรอิสระ ประกอบด้วย

1.1 ข้อมูลทั่วไป ได้แก่ อายุ เพศ ระดับการศึกษา สถานะของกลุ่มประชากรตัวอย่าง

1.2 ปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคงปลอดภัย

- ด้านเทคโนโลยีสารสนเทศ ได้แก่ (1) ความรู้เกี่ยวกับคอมพิวเตอร์ (2) ความรู้เกี่ยวกับพระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นๆ (3) ปัจจัยทางด้านสังคม (4) ปัจจัยทางด้านเศรษฐกิจ และ (5) ปัจจัยเกี่ยวกับพฤติกรรมการใช้คอมพิวเตอร์

ตัวแปรตาม คือ จริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยี
สารสนเทศ ในบริบทของประเทศไทย 4.0 รวมถึงจริยธรรมต่างๆ ได้แก่ (1) การไม่ละเมิดความเป็นส่วนตัว (2) การไม่เจาระบบ (3) การไม่ละเมิดทรัพย์สินทางปัญญา และไม่ละเมิดลิขสิทธิ์ซอฟต์แวร์ (4) ไม่ส่งอีเมลล สร้างความรำคาญให้กับผือื่น (5) การไม่ขโมยอัตลักษณ์ เป็นต้น

3.4 เครื่องมือการวิจัย

การศึกษาครั้งนี้แบ่งเครื่องมือในการวิจัยออกเป็น 3 ประเภทได้ดังนี้

1. ฮาร์ดแวร์ที่ใช้ในการวิจัย
   - 1.1 เครื่องคอมพิวเตอร์แบบตั้งโต๊ะหรือแบบพกพาที่มีซีพียูไม่ต่ำกว่า Core 2 Duo
   - 1.2 ฮาร์ดดิสก์ที่มีความจุไม่ต่ำกว่า 200 GB และหน่วยความจำไม่ต่ำกว่า 4GB and HP L1706 Intel Pentium D Inside
   - 1.3 เครื่องพิมพ์ HP Laser Jet Professional P1102 and Konica Print Multifunction
2. ซอฟต์แวร์ที่ใช้ในการทำวิจัย
   - 2.1 ระบบปฏิบัติการ Windows 7
   - 2.2 โปรแกรม MS-Office 2010
   - 2.3 โปรแกรม SPSS for Windows Version 17
3. แบบสอบถามการวิจัย

3.5 การรวบรวมข้อมูล

การเก็บและข้อมูลมีการดำเนินการดังนี้ ดังนี้
เก็บรวบรวมข้อมูลแบบสอบถาม ซึ่งส่งไปยังสถาบันอุดมศึกษา และมหาวิทยาลัยของรัฐและเอกชนต่างๆ ให้ได้ 70% ขึ้นไป ด้วยการตามเก็บแบบสอบถาม หากยังไม่ครบ ต้องนำไปแจกใหม่ให้ได้ครบตามจำนวนเก็บรวบรวมข้อมูลเกี่ยวกับปัจจัยที่มีผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้บริหาร คณาจารย์ เจ้าหน้าที่ และนักศึกษา เพื่อรวบรวมมาทำการประเมินลผล และวิเคราะห์หาบทสรุป

3.6 การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลในการวิจัยครั้งนี้วิเคราะห์ข้อมูลโดยใช้ คอมพิวเตอร์และโปรแกรมสำเร็จรูป สถิติที่ใช้ในการวิเคราะห์มีดังนี้

1. สถิติเชิงพรรณนา ได้แก่ จำนวน ร้อยละ ค่าเฉลี่ยเลขคณิต ($\overline{X}$) และส่วนเบี่ยงเบนมาตรฐาน (S.D.) ของแต้มเฉลี่ยที่ได้จากการทำแบบสอบถามเจตคติของผู้บริหาร คณาจารย์ เจ้าหน้าที่ นักศึกษา

2. สถิติเชิงอนุมาน การวิเคราะห์ถดถอยพหุคูณ (Multiple Regressions Analysis) ศึกษาปัจจัยที่มีผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ

บทที่ 4

ผลการวิเคราะห์ข้อมูล

การวิจัยเรื่อง **“ปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: กรณีศึกษา สถาบันอุดมศึกษาในเขตกรุงเทพมหานคร และปริมณฑล”** นำเสนอในรูปตารางประกอบความเรียงจำแนกเป็น ... ขั้นตอนตามลำดับดังนี้

4.1 ข้อมูลเกี่ยวกับสถานภาพทั่วไปของผู้บริหาร คณาจารย์ บุคลากร พนักงาน และนักศึกษา

ตารางที่ 4.1 : จำนวนร้อยละข้อมูลทั่วไปของตัวอย่างที่ใช้ในการศึกษา

ข้อมูลทั่วไป	จำนวน	ร้อยละ
เพศ		
ชาย	488	48.80
หญิง	445	44.50
ไม่ระบุเพศ	67	6.70
อายุ		
ต่ำกว่า 20 ปี	204	20.40
20 - 25 ปี	614	61.40
26 - 30 ปี	30	3.00
31 - 35 ปี	40	4.00
36 - 40 ปี	45	4.50
มากกว่า 40 ปี	67	6.70
ระดับการศึกษาสูงสุด		
ต่ำกว่าปริญญาตรี	191	19.10
ปริญญาตรี	688	68.80
ปริญญาโท	101	10.10
ปริญญาเอก	20	2.00
ประสบการณ์ในการใช้เทคโนโลยีสารสนเทศ		
มากที่สุด	**99**	9.90
มาก	347	34.70
ปานกลาง	338	33.80
น้อย	45	4.50
น้อยที่สุด	171	17.10

จากตารางที่ 4.1 พบว่ากลุ่มตัวอย่างที่ใช้ในการศึกษาเป็นเพศชายร้อยละ 48.80 เพศหญิงร้อยละ 44.50 และไม่ระบุเพศร้อยละ 6.70 ส่วนใหญ่มีอายุ 20 – 25 ปี คิดเป็นร้อยละ 61.40 รองลงมาเป็น

อายุต่ำกว่า 20 ปี คิดเป็นร้อยละ 20.40 กลุ่มตัวอย่างที่ใช้ในการศึกษาสาวนใหญ่จบการศึกษาสูงสุดระดับปริญญาตรีคิดเป็นร้อยละ 68.80 และต่ำกว่าปริญญาตรีคิดเป็นร้อยละ 19.10 กลุ่มตัวอย่างส่วนมากมีประสบการณ์ในการใช้เทคโนโลยีสารสนเทศ อยู่ในระดับมากและระดับปานกลาง คิดเป็นร้อยละ 34.70 และ 33.80 ตามลำดับ

4.2 ปัจจัยด้าน ด้านความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.) ด้านสังคม ด้านเศรษฐกิจและ ด้านพฤติกรรมการใช้คอมพิวเตอร์ และด้านสื่อสังคมออนไลน์ ในบริบทของประเทศไทย 4.0:

ในการศึกษาครั้งนี้จำแนกปัจจัยออกเป็น 5 ด้าน ได้แก่ ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.) ด้านสังคม ด้านเศรษฐกิจและ ด้านพฤติกรรมการใช้คอมพิวเตอร์ และสื่อสังคมออนไลน์ นำเสนอผลการวิเคราะห์ในรูปค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ทั้งในภาพรวม รายด้าน และรายข้อ ดังต่อไปนี้

ตารางที่ 4.2 : ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ภาพรวมปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0:

ด้าน	$\overline{X}$	S. D.	ความหมาย
1. ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ	3.72	.66	มาก
2. ความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.)	3.14	.91	ปานกลาง
3. ทางสังคม	3.96	.65	มาก
4. เศรษฐกิจ	3.85	.68	มาก
5. พฤติกรรมการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์	3.98	.70	มาก
รวม	3.72	.56	มาก

จากตารางที่ 4.2 พบว่าภาพรวมปัจจัยทั้ง 5 ด้าน มีค่าเฉลี่ยเท่ากับ 3.72 อยู่ในระดับมาก โดยด้านที่มีค่าเฉลี่ยสูงที่สุดใน 5 ด้านนี้ คือ ด้านพฤติกรรมการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์ มีค่าเฉลี่ยเท่ากับ 3.98 อยู่ในระดับมาก รองลงมาเป็นด้านสังคม มีค่าเฉลี่ยเท่ากับ 3.96 อยู่ในระดับมาก เช่นกัน ส่วนด้านที่มีค่าเฉลี่ยต่ำที่สุด คือ ด้านความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.) มีค่าเฉลี่ยเท่ากับ 3.14 อยู่ในระดับปานกลาง

ตารางที่ 4.3 : ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ

รายละเอียด	$\overline{X}$	S.D.	ความหมาย
1) ความรู้เรื่องเทคโนโลยีสารสนเทศ และคอมพิวเตอร์ของบุคลากรในองค์กร	3.69	.80	**มาก**
2) ความรู้เรื่องอุปกรณ์ฮาร์ดแวร์ เช่น หน่วยประมวลผลกลาง (CPU) หน่วยบันทึกข้อมูล ได้แก่ ฮาร์ดดิสก์	3.60	.87	**มาก**
3) ความรู้เรื่องซอฟต์แวร์ เช่น Windows, MS-Office	3.66	.86	**มาก**
4) ความรู้เรื่องเครือข่ายคอมพิวเตอร์ เช่น เครือข่ายท้องถิ่น หรือแลนด์ (LAN)ไวไฟ (WiFi)	3.56	.90	**มาก**
5) ความรู้เรื่องข้อมูล เช่น การจัดการข้อมูล และฐานข้อมูล (Database)	3.50	.90	**มาก**
6) ความรู้เรื่องของอินเทอร์เน็ต เช่น การสื่อสารผ่านเว็บไซต์ อีเมล การสนทนา การประชุมผ่านจอภาพวิดีโอ	3.84	.85	**มาก**
7) ความรู้เรื่องเว็บเครือข่ายสังคมออนไลน์ เช่น Facebook Line Twitter YouTube Instagram	3.99	.84	**มาก**
8) ความรู้เรื่องการจัดเก็บข้อมูล เช่น การสร้างโฟลเดอร์ (Folder) การจัดการแฟ้มข้อมูล (File) การสำรองข้อมูล (Backup)	3.86	.86	**มาก**
9) ความรู้เรื่องการพัฒนาระบบ เช่น ระบบการลงทะเบียนเรียน และแอพพลิเคชัน เช่น แอพลิเคชัน Line แอพพลิเคชันเรียกแท็กซี่ (Grab Taxi)	3.71	.90	**มาก**
10) ความรู้เรื่องการประยุกต์ใช้คอมพิวเตอร์ในธุรกิจ เช่น การใช้ช่องทางออนไลน์ในการขายสินค้า การจองห้องพักโรงแรม การจองตั๋วเครื่องบินออนไลน์	3.76	.87	**มาก**
รวม	3.72	.66	**มาก**

จากตารางที่ 4.3 พบว่าภาพรวมความรู้ความเข้าใจด้านเทคโนโลยี มีค่าเฉลี่ยเท่ากับ 3.72 อยู่ในระดับมาก โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คือ ความรู้เรื่องเว็บเครือข่ายสังคมออนไลน์ เช่น Facebook Line Twitter YouTube Instagram มีค่าเฉลี่ยเท่ากับ 3.99 อยู่ในระดับมากรองลงมาเป็นเรื่องความรู้เรื่องการจัดเก็บข้อมูล เช่น การสร้างโฟลเดอร์ (Folder) การจัดการแฟ้มข้อมูล (File) การสำรองข้อมูล (Backup) มีค่าเฉลี่ยเท่ากับ 3.86 อยู่ในระดับมาก เช่นกัน ส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือ ความรู้เรื่องข้อมูล เช่น การจัดการข้อมูล และฐานข้อมูล (Database) มีค่าเฉลี่ยเท่ากับ 3.50 อยู่ในระดับมาก

ตารางที่ 4.4 : ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.)

รายละเอียด	$\overline{X}$	S.D.	ความหมาย
11). พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ.2550	3.24	1.01	ปานกลาง
12). พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ.2550 แก้ไขเพิ่มเติม ปี พ.ศ.2560	3.22	1.04	ปานกลาง
13). พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ ปี พ.ศ.2544	3.11	1.03	ปานกลาง
14) พระราชบัญญัติ การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ปี พ.ศ.2560	3.15	1.05	ปานกลาง
15). พระราชบัญญัติลิขสิทธิ์ ปี พ.ศ.2537	3.14	1.02	ปานกลาง
16) พระราชบัญญัติให้ใช้ประมวลกฎหมายอาญา พ.ศ.2499	3.09	1.04	ปานกลาง
17) พระราชบัญญัติลิทธิบัตร ปี พ.ศ.2522 แก้ไขเพิ่มเติม พ.ศ. 2542	3.07	1.03	ปานกลาง
18) พระราชบัญญัติเครื่องหมายการค้า ปี พ.ศ.2534 แก้ไขเพิ่มเติม พ.ศ.2543	3.09	1.02	ปานกลาง
19) พระราชบัญญัติการพนัน ปี พ.ศ.2478	3.13	1.05	ปานกลาง
20) พระราชบัญญัติการคุ้มครองเด็ก ปี พ.ศ.2546	3.18	1.05	ปานกลาง
รวม	3.14	.91	ปานกลาง

จากตารางที่ 4.4 พบว่าภาพรวมความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.) มีค่าเฉลี่ยเท่ากับ 3.14 อยู่ในระดับปานกลาง โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ.2550 มีค่าเฉลี่ยเท่ากับ 3.24 อยู่ในระดับปานกลาง รองลงมาเป็นเรื่องพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ.2550 แก้ไขเพิ่มเติม ปี พ.ศ.2560 มีค่าเฉลี่ยเท่ากับ 3.22 อยู่ในระดับปานกลาง เช่นกัน ส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือ ความรู้เรื่องพระราชบัญญัติลิทธิบัตร ปี พ.ศ.2522 แก้ไขเพิ่มเติม พ.ศ. 2542 มีค่าเฉลี่ยเท่ากับ 3.07 อยู่ในระดับปานกลาง

ตารางที่ 4.5 : ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ปัจจัยด้านสังคม

รายละเอียด	$\overline{X}$	S.D.	ความหมาย
21) เกิดกลุ่มความสัมพันธ์ทางออนไลน์ เช่น ครอบครัว เพื่อน คนรู้จัก ตลอดจนอาจารย์ เพื่อนร่วมห้องเรียน	3.97	.88	มาก
22) เกิดการพบปะสนทนาออนไลน์ การใช้โทรศัพท์ผ่าน อินเทอร์เน็ต และ Facebook, Line, Instagram มากขึ้น	4.04	.85	มาก
23) รูปแบบการเรียนรู้เปลี่ยนแปลงไป การเรียนในห้องเรียนลดลง การเรียนทางออนไลน์เพิ่มมากขึ้น	3.84	.82	มาก
24) เกิดแอพลิเคชันใหม่เพิ่มมากขึ้น เช่น แอพลิเคชันเรียก รถแท็กซี่ (Grab Taxi), แอพลิเคชันเคลมประกัน (Claim Di)	3.92	.85	มาก
25) ด้านบันเทิงคนดูภาพยนตร์และโทรทัศน์ลดลง เพราะหันมาดูทางออนไลน์มากขึ้น เช่น YouTube	4.08	.86	มาก
26) สื่อสังคมออนไลน์มีผลกระทบต่อสังคมในด้านดี เช่น ทำให้การติดต่อสื่อสารสะดวกสบาย เป็นช่องทางการสร้างรายได้ และมีคุณภาพชีวิตดีขึ้น	4.00	.87	มาก
27) สื่อสังคมออนไลน์มีผลกระทบต่อสังคมในด้านลบ เช่น มีการหลอกลวงการปลอมเฟซบุ๊ค การละเมิดความเป็นส่วนตัว การโพสต์ภาพลามกอนาจาร การค้ายาเสพติด ตลอดจนการเล่นพนันออนไลน์	4.06	.85	มาก
28). สื่อสังคมออนไลน์มีผลกระทบต่อสังคมในด้านบวก เช่น ช่วยลดความเหลื่อมล้ำทางสังคม โน้ตบุ๊คคอมพิวเตอร์ และสมาร์ทโฟนมีราคาถูกลง	3.83	.86	มาก
29) สื่อสังคมออนไลน์มีผลกระทบต่อสังคมในด้านลบ เช่น การส่งไวรัส และสแปมลิงก์มัลแวร์	3.91	.85	มาก
รวม	3.96	.65	มาก

จากตารางที่ 4.5 พบว่าภาพรวมปัจจัยด้านสังคมมีค่าเฉลี่ยเท่ากับ 3.96 อยู่ในระดับมาก โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คือ เรื่องบันเทิงคนดูภาพยนตร์และโทรทัศน์ลดลง เพราะหันมาดูทางออนไลน์มากขึ้น เช่น YouTube มีค่าเฉลี่ยเท่ากับ 4.08 อยู่ในระดับมากรองลงมาเป็นเรื่องสื่อสังคมออนไลน์มีผลกระทบต่อสังคมในด้านลบ เช่น มีการหลอกลวงการปลอมเฟซบุ๊ค การละเมิดความเป็นส่วนตัว การโพสต์ภาพลามกอนาจารการค้ายาเสพติด ตลอดจนการเล่นพนันออนไลน์ มีค่าเฉลี่ยเท่ากับ 4.06 อยู่ในระดับมาก เช่นกัน ส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือ สื่อสังคมออนไลน์มีผลกระทบต่อสังคมในด้านบวก เช่น ช่วยลดความเหลื่อมล้ำทางสังคม โน้ตบุ๊คคอมพิวเตอร์ และสมาร์ทโฟนมีราคาถูกลง มีค่าเฉลี่ยเท่ากับ 3.83 อยู่ในระดับมาก

ตารางที่ 4.6 : ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ปัจจัยด้านเศรษฐกิจ

รายละเอียด	$\overline{X}$	S.D.	ความหมาย
30) การจ้างงานของภาคธุรกิจบางกลุ่มลดลง เช่น ธนาคาร ห้างสรรพสินค้า ร้านจำหน่ายสินค้า	3.78	.84	มาก
31) เกิดธุรกิจประเภทตัวแทนทางด้านการเงินในการจัดซื้อสินค้าทางออนไลน์	3.89	.83	มาก
32) เกิดธุรกิจบริการใหม่ๆ เช่น การรับส่งสินค้าพัสดุแบบรีบด่วน เช่น Kerry Express ฯลฯ	3.98	.88	มาก
33) การจ้างงานภาคบริการลดลง เพราะเกิดนวัตกรรมใหม่ๆ ขึ้นมาแทนที่ เช่น Fintech	3.79	.84	มาก
34) ระบบการค้าการลงทุนเปลี่ยนไป มีความสะดวกรวดเร็ว สามารถลงทุนได้ตลอด 24 ชั่วโมง	3.88	.84	มาก
35) ระบบการเงินสำหรับซื้อขายแลกเปลี่ยนมีการเปลี่ยนแปลงไป เกิดสกุลเงินใหม่ๆ เช่น Bitcoin	3.78	.88	มาก
36) มีการลดขั้นตอนแรงงานการผลิตในภาคการผลิตด้วยการใช้ระบบอัตโนมัติและการใช้หุ่นยนต์	3.79	.85	มาก
37) เทคโนโลยีสารสนเทศและการสื่อสาร เป็นตัวผลักดันที่ก่อให้เกิดการขยายตัวทางเศรษฐกิจ และมีการแข่งขันกันรุนแรงมากขึ้น เช่น ระบบพาณิชย์อิเล็กทรอนิกส์ (e-Commerce)	3.88	.85	มาก
รวม	3.85	.68	มาก

จากตารางที่ 4.6 พบว่าภาพรวมปัจจัยด้านเศรษฐกิจมีค่าเฉลี่ยเท่ากับ 3.85 อยู่ในระดับมาก โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คือ เกิดธุรกิจบริการใหม่ๆ เช่น การรับส่งสินค้าพัสดุแบบรีบด่วน เช่น Kerry Express ฯลฯ มีค่าเฉลี่ยเท่ากับ 3.98 อยู่ในระดับมากรองลงมาเป็นเรื่อง เกิดธุรกิจประเภทตัวแทนทางด้านการเงินในการจัดซื้อสินค้าทางออนไลน์มีค่าเฉลี่ยเท่ากับ 3.89 อยู่ในระดับมาก ส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือ การจ้างงานของภาคธุรกิจบางกลุ่มลดลง เช่น ธนาคาร ห้างสรรพสินค้า ร้าน จำหน่ายสินค้า มีค่าเฉลี่ยเท่ากับ 3.78 อยู่ในระดับมาก

ตารางที่ 4.7 : ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ปัจจัยด้านพฤติกรรมการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์

รายละเอียด	$\overline{X}$	S.D.	ความหมาย
38) พฤติกรรมการเรียนรู้ของเยาวชนเปลี่ยนแปลงไป โดยหันมาศึกษาเรียนรู้จากอินเทอร์เน็ตและสื่อสังคมออนไลน์ เช่น Google Facebook Line YouTube เป็นเวลานานมากขึ้น	4.12	.83	มาก
39) พฤติกรรมการซื้อขายสินค้าเปลี่ยนไป โดยผู้ซื้อ และผู้ขาย หันมาใช้บริการทางออนไลน์มากขึ้น	4.06	.80	มาก
40) การทำธุรกรรมทางการเงินระหว่างผู้ซื้อและผู้ขายเปลี่ยนไป โดยหันมาใช้ระบบการบริการโอนเงิน และรับเงินทางออนไลน์กันมากขึ้น เช่น การชำระเงินด้วยพร้อมเพย์ (Prompt Pay) และคิวอาร์โค้ต (Quick Response Code)	4.01	.89	มาก
41) พฤติกรรมการแสดงออกให้เป็นที่ยอมรับของสังคมเปลี่ยนไป โดยมีการหันมาใช้การกดไลค์ การแชร์ และการโหวตทางออนไลน์มากขึ้น	3.98	.87	มาก
42) พฤติกรรมทางสังคมเปลี่ยนจากการพูดคุยแบบเผชิญหน้าลดน้อยลง และหันมาใช้การสื่อสารบนแอพพลิเคชันบนสมาร์ทโฟน และการสื่อสารทางออนไลน์มากขึ้น เช่น Facebook, Line	3.95	.88	มาก
43) พฤติกรรมการสื่อสารทางด้านภาษาพูดเปลี่ยนไป มีการใช้ภาษาใหม่ๆ เกิดขึ้น และมีการสนทนาแบบมองเห็นหน้ากัน (Face to Face) รวมถึงอวัจนะภาษา หรือ ภาษากาย	3.89	.88	มาก
44) พฤติกรรมด้านบันเทิงเปลี่ยนไป คนดูภาพยนตร์ในโรงหนังลดลง โดยหันมาดูภาพยนตร์ และวิดีโอทางออนไลน์มาก และนานขึ้น เช่น YouTube, Netflix	3.95	.88	มาก
45) เกิดพฤติกรรมการใช้เทคโนโลยีอินเทอร์เน็ต และสื่อสังคมออนไลน์ทั้งในเวลาการทำงาน-ในช่วงเวลาเรียน และในช่วงเวลาอื่นๆ เช่น Facebook Line และ YouTube เป็นเวลานานมากขึ้น	4.01	.87	มาก
46) เกิดพฤติกรรมหลงไหลการติดเกม และการพนันออนไลน์เพิ่มมากขึ้น	3.88	.91	มาก
47) เกิดพฤติกรรมการเลียนแบบการแสดงออกและกิจกรรมของดารา หรือบุคคลที่ตนเองชื่นชอบ และอยากทำตาม ที่เรียกว่า เน็ตไอดอล (Net Idol)	3.92	.90	มาก
48) เกิดพฤติกรรมการโฆษณาสินค้าทางออนไลน์เพิ่มมากขึ้น เช่น บน Google Facebook Line เนื่องจากมีค่าใช้จ่ายที่ถูกกว่าการโฆษณาบนสื่อกระแสหลักอย่างหนังสือพิมพ์ และวิทยุ โทรทัศน์	4.00	.89	มาก
รวม	3.98	.70	มาก

จากตารางที่ 4.7 พบว่าภาพรวมปัจจัยด้านพฤติกรรมการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์ มีค่าเฉลี่ยเท่ากับ 3.98 อยู่ในระดับมาก โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คือ พฤติกรรมการเรียนรู้ของเยาวชนเปลี่ยนแปลงไป โดยหันมาศึกษาเรียนรู้จาก อินเทอร์เน็ตและสื่อสังคมออนไลน์ เช่น Google Facebook Line YouTube เป็นเวลานานมากขึ้น มีค่าเฉลี่ยเท่ากับ 4.12 อยู่ในระดับมาก รองลงมาเป็นเรื่อง พฤติกรรมการซื้อขายสินค้าเปลี่ยนไป โดยผู้ซื้อ และผู้ขาย หันมาใช้บริการทางออนไลน์มากขึ้น มีค่าเฉลี่ยเท่ากับ 4.06 อยู่ในระดับมาก ส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือ เกิดพฤติกรรมหลงใหลการติดเกม และการพนันออนไลน์เพิ่มมากขึ้น มีค่าเฉลี่ยเท่ากับ 3.78 อยู่ในระดับมา

ตอนที่ 4.3 จริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0

ตารางที่ 4.8 : ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน จริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศ ไทย 4.0

ด้าน	$\overline{X}$	S.D.	ความหมาย
จริยธรรม	3.93	.73	มาก
ความมั่นคงปลอดภัย	3.80	.70	มาก
รวม	3.86	.67	มาก

จากตารางที่ 4.8 พบว่าภาพรวมจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 มีค่าเฉลี่ยเท่ากับ 3.86 อยู่ในระดับมาก โดยด้านจริยธรรม มีค่าเฉลี่ยเท่ากับ 3.93 อยู่ในระดับมาก เช่นเดียวกับด้านความมั่นคงปลอดภัย มีเฉลี่ยเท่ากับ 3.80 อยู่ในระดับมากเช่นกัน

ตารางที่ 4.9 : ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ด้านจริยธรรมทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0

รายละเอียด	$\overline{X}$	S.D.	ความหมาย
49) มีปัญหาเรื่องการโกหกหลอกลวงทางอินเทอร์เน็ต และทางสื่อสังคมออนไลน์เพิ่มมากขึ้น	4.01	.85	มาก
50) ความมีวินัยเรียนรู้ในการทำงานลดลง	3.83	.82	มาก
51) การเข้าถึงภาพลามกอนาจาร ความรุนแรง และความน่ากลัวมีมากเพิ่มขึ้น	3.96	.87	มาก
52) มีการก่อปัญหาอาชญากรรมคอมพิวเตอร์ เช่น การขโมยข้อมูล และการปล่อยไวรัส การโจมตีประเภทต่างๆ	3.92	.86	มาก
53) มีการแสดงการทำลามกอนาจารออนไลน์เพิ่มมากขึ้น	3.93	.88	มาก
54) มีการละเมิดลิขสิทธิ์ภาพ ข้อมูล และซอฟต์แวร์ ด้วยความรู้เท่าไม่ถึงการณ์มากขึ้น	3.94	.87	มาก
55) มีการละเมิดความเป็นส่วนตัวเพิ่มมากขึ้น	3.93	.87	มาก
56) มีการส่งอีเมลโฆษณาที่ไม่ได้รับเชิญ (Spamming) จำนวนมากทั้งทางอีเมล และทางสื่อสังคมออนไลน์	3.91	.88	มาก
รวม	3.93	.73	มาก

จากตารางที่ 4.9 พบว่าภาพรวมจริยธรรมทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 มีค่าเฉลี่ยเท่ากับ 3.93 อยู่ในระดับมาก โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คือมีปัญหาเรื่องการโกหกหลอกลวงทางอินเทอร์เน็ต และทางสื่อสังคมออนไลน์เพิ่ม มากขึ้น มีค่าเฉลี่ยเท่ากับ 4.01 อยู่ในระดับมากรองลงมาเป็นเรื่องการเข้าถึงภาพลามกอนาจาร ความรุนแรง และความน่ากลัวมีมากเพิ่มขึ้นมีค่าเฉลี่ยเท่ากับ 3.96 อยู่ในระดับมากส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือความมีวินัยเรียนรู้ในการทำงานลดลงมีค่าเฉลี่ยเท่ากับ 3.83 อยู่ในระดับมาก

ตารางที่ 4.10 : ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ด้านความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศในบริบทของประเทศไทย 4.0

รายละเอียด	$\overline{X}$	S.D.	ความหมาย
1) รัฐ และองค์กร ต้องเพิ่มความเข้มงวดด้านนโยบาย ด้านความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศให้สูงขึ้น	3.84	.90	มาก
2) รัฐ และองค์กรต้องเพิ่มงบประมาณด้านความปลอดภัยมากขึ้น เช่น การติดตั้งโปรแกรมไฟร์วอลล์ และโปรแกรมการตรวจสอบ และป้องกันไวรัสคอมพิวเตอร์	3.79	.88	มาก
3) รัฐ และองค์กรต้องจ้างบุคลการด้านไอทีเพิ่มขึ้น	3.79	.88	มาก
4) เกิดอาชญากรรมทางด้านการเงินและธนาคารสูงขึ้น	3.79	.87	มาก
5) เกิดปัญหาทางด้านอาชญากรรมไซเบอร์ เช่น การเจาะระบบ ขโมยข้อมูล และทำลายข้อมูล	3.81	.86	มาก
6) มีการซื้อขายสินค้าและการดาวน์โหลดซอฟต์แวร์ที่มีลิขสิทธิ์	3.79	.86	มาก
7) มีการข่มขู่ กรรโชก ทางอีเมล์ และสื่อสังคมออนไลน์	3.78	.88	มาก
8) มีการนำความลับส่วนบุคคลและองค์กรไปเปิดเผยในทางที่ไม่เหมาะสม	3.82	.85	มาก
9) อินเทอร์เน็ตและสื่อสังคมออนไลน์ เป็นแหล่งการก่ออาชญากรรมทางคอมพิวเตอร์ เพราะสามารถใช้ได้ทุกที่ทุกเวลา	3.86	.89	มาก
10) มีการแก้ไขกฎหมาย และเพิ่มโทษมากขึ้น เช่น พ.ร.บ คอมพิวเตอร์ ปี 2550 แก้ไขเพิ่มเติม พ.ศ.2560	3.78	.88	มาก
11) มีการโจมตีด้วยไวรัสประเภทต่างๆ เพื่อให้ได้รหัสผ่าน แลการโจรกรรมข้อมูล	3.80	.88	มาก
รวม	3.80	.70	มาก

จากตารางที่ 4.10 พบว่าภาพรวมด้านความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 มีค่าเฉลี่ยเท่ากับ 3.80 อยู่ในระดับมาก โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้คืออินเทอร์เน็ตและสื่อสังคมออนไลน์ เป็นแหล่งการก่ออาชญากรรมทาง คอมพิวเตอร์ เพราะสามารถใช้ได้ทุกที่ทุกเวลามีค่าเฉลี่ยเท่ากับ 3.86 อยู่ในระดับมากรองลงมาเป็นเรื่องรัฐ และองค์กร ต้องเพิ่มความเข้มงวดด้านนโยบาย ด้านความมั่นคงปลอดภัย ทางด้านเทคโนโลยีสารสนเทศให้สูงขึ้น มีค่าเฉลี่ยเท่ากับ 3.84 อยู่ในระดับมากส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือมีการข่มขู่ กรรโชก ทางอีเมล์และสื่อสังคมออนไลน์ และ มีการแก้ไขกฎหมาย และเพิ่มโทษมากขึ้น เช่น พ.ร.บ คอมพิวเตอร์ ปี 2550 แก้ไขเพิ่มเติม พ.ศ.2560 มีค่าเฉลี่ยเท่ากับ 3.78 อยู่ในระดับมา

ตอนที่ 4.4 ความสัมพันธ์ระหว่าง ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ. สังคม เศรษฐกิจ และพฤติกรรม กับ จริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0

ตารางที่ 4.11 : ความสัมพันธ์ระหว่างปัจจัยกับจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศในบริบทของประเทศไทย 4.0

	ความรู้ความเข้าใจเรื่องเทคโน	ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ.	สังคม	เศรษฐกิจ	พฤติกรรมการใช้คอมพิวเตอร์ฯ	รวมปัจจัย	จริยธรรม	ความมั่นคงปลอดภัย
ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ	1.00							
ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ.	.555**	1.00						
สังคม	.601**	.275**	1.00					
เศรษฐกิจ	.557**	.297**	.709**	1.00				
พฤติกรรมการใช้คอมพิวเตอร์	.509**	.187**	.722**	.742**	1.00			
รวมปัจจัย	.828**	.654**	.815**	.813**	.789**	1.00		
จริยธรรม	.451**	.179**	.638**	.623**	.727**	.650**	1.00	
ความมั่นคงปลอดภัย	.497**	.250**	.591**	.628**	.708**	.671**	.770**	1.00
จริยธรรมและความมั่นคง	.507**	.233**	.649**	.665**	.760**	.702**	.922**	.957**

จากตารางที่ 4.11 พบว่า ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ. สังคม เศรษฐกิจ และพฤติกรรม มีความสัมพันธ์กับ ความมั่นคงปลอดภัยและจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ในทิศทางเดียวกัน ด้วยขนาดความสัมพันธ์เท่ากับ 0.507 0.233 0.649 0.665 และ 0.760 ตามลำดับ นอกจากนั้นยังพบว่าภาพรวมของทั้ง 5 ปัจจัยมีความสัมพันธ์ทางสถิติอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ด้วยขนาดความสัมพันธ์เท่ากับ 0.702 ในทิศทางเดียวกัน

ตอนที่ 4.5 อิทธิพลที่ปัจจัยด้าน ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ. สังคม เศรษฐกิจ และพฤติกรรม มีต่อ จริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0

ตารางที่ 4.12 : อิทธิพลที่ปัจจัยมีต่อความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศในบริบทของประเทศไทย 4.0

	Coefficients[a]				
	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
ค่าคงที่	.503	.091		5.509	.000
ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ	.084	.030	.082	2.818	.005
ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ.	.011	.018	.015	.623	.534
สังคม	.117	.033	.113	3.495	.000
เศรษฐกิจ	.140	.032	.142	4.387	.000
พฤติกรรมการใช้คอมพิวเตอร์	.504	.031	.529	16.228	.000
F	317.239**				
R	0.784				
R^2	0.615				
Std. Error of the Estimate	0.418				
Durbin-Watson	1.866				

จากตารางที่ 4.12 พบว่า ตัวแปรอิสระทั้ง 5 ได้แก่ ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ. สังคม เศรษฐกิจ และพฤติกรรม สามารถอธิบายความผันแปรของจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ได้อย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05 (F = 317.239) ตัวแปรอิสระทั้ง 5 มีความสัมพันธ์กับจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ร้อยละ 78.4 และสามารถอธิบายการเปลี่ยนแปลงของจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ได้ร้อยละ 61.5 เมื่อพิจารณาอิทธิพลพบว่าปัจจัยที่มีอิทธิพลต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 อย่างมีนัยสำคัญทางสถิติที่ระดับนัยสำคัญ 0.05 ได้แก่ ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ปัจจัยทางสังคม ปัจจัยเศรษฐกิจ และพฤติกรรม ด้วยขนาดอิทธิพลเท่ากับ 0.084 0.117 0.140 และ 0.504

บทที่ 5

สรุปการดำเนินงานวิจัย สรุปผลการวิจัย อภิปรายผล ข้อเสนอแนะเพื่อดำเนินการ ข้อเสนอแนะเพื่อการทำวิจัยครั้งต่อไป

5.1 สรุปผลการดำเนินงานวิจัย

ในการดำเนินงานวิจัยเรื่อง **“ปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: กรณีศึกษา สถาบันอุดมศึกษาในเขตกรุงเทพมหานคร และปริมณฑล”** โดยมีลำดับการดำเนินงานวิจัย ดังนี้ คือ: (1). เขียนแบบเสนอโครงการวิจัยสำหรับบุคลากรภายใน (FM วจ.-01), (2).การติดต่อหาผู้ทรงคุณวุฒิมาเป็นที่ปรึกษาในการทำวิจัย (3).จัดเตรียมรวบรวมเนื้อหารายละเอียดของปัจจัยที่มีผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศจากห้องสมุดและการศึกษาค้นคว้าข้อมูลเพิ่มเติมจากสื่อต่างๆ เช่น อินเทอร์เน็ต และสื่อสังคมออนไลน์ (4).สอบถามผู้มีประสบการณ์การทำวิจัย (5).เข้ารับการฝึกอบรมเพิ่มเติมในการทำวิจัย (6).ติดต่อสำนักวิจัยของมหาวิทยาลัยศรีปทุม เพื่อนำรายละเอียดข้อมูลต่างๆ มาบูรณาการประกอบการศึกษา การตั้งคำถามวิจัย การเขียนเสนอโครงการวิจัย และการวิเคราะห์ถึงข้อดีข้อเสีย และสรุปผลการวิจัยและเขียนรายงาน (6).การจัดทำแบบสอบถามวิจัย และเสนอให้ผู้ทรงคุณวุฒิทำการตรวจประเมิน (7). แจกแบบสอบถามวิจัยไปยังสถาบันการศึกษาในเขตกรุงเทพมหานครและปริมณฑล (8).เก็บแบบสอบถามที่ได้นำไปแจกไว้ตามสถาบันและมหาวิทยาลัย (9).นำข้อมูลที่ได้จาการตอบแบบสอบถามมาทำการสรุปผลวิเคราะห์ และอภิปรายผล

งานวิจัยนี้ เป็นการวิจัยเพื่อให้ทราบถึงปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ โดยมีประชากรกลุ่มตัวอย่าง คือ ผู้บริหาร คณาจารย์ พนักงาน นักศึกษา จากสถาบันอุดมศึกษาในเขตกรุงเทพมหานคร และปริมณฑลรวม 61 สถาบัน โดยแบ่งกลุ่มมหาวิทยาลัยออกตามลักษณะของมหาวิทยาลัย ได้แก่ (1). มหาวิทยาลัยของรัฐบาล (จำกัดจำนวนรับ) (2). มหาวิทยาลัยราชภัฏ (3). มหาวิทยาลัยราชมงคล และ (4). มหาวิทยาลัยเอกชน บุคลากรทั้งสิ้น 38,591 คน และนักศึกษารวมทั้งสิ้น 696,796 คน ใช้การสุ่มตัวอย่างแบบหลายขั้นตอนโดยการจำแนกมหาวิทยาลัยออกเป็น 4 กลุ่ม ตามลักษณะของมหาวิทยาลัยได้แก่ มหาวิทยาลัยของรัฐบาล (จำกัดจำนวนรับ) มหาวิทยาลัยราชภัฏ มหาวิทยาลัยราชมงคล และมหาวิทยาลัยเอกชน แล้วใช้วิธีการสุ่มตัวอย่างแบบชั้นภูมิกำหนดจำนวน 10 สถาบัน การจำแนกกลุ่มเหล่านี้ เพื่อวัดปัจจัยที่มีผลกระทบ คือ (1).เพื่อศึกษาการละเมิดจริยธรรมและภัยคุกคามความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: ของสถาบันอุดมศึกษาในเขตกรุงเทพฯ และปริมณฑล (2). เพื่อกำหนดประเภทของการละเมิดจริยธรรม และภัยคุกคามทางด้านเทคโนโลยีสารสนเทศ (3). เพื่อแสวงหาแนวทางป้องกันและการแก้ไขปัญหาเกี่ยวกับการละเมิดจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ และทำการแจกแบบสอบถามหรือแบบสำรวจ ตั้งเกณฑ์เป้าหมายเอาไว้จำนวน 1,000 ชุด และได้ทำการแจกไป 1,200 ชุด โดยตั้งเป้าในการจัดเก็บข้อมูลให้ได้ 70% ขึ้นไปและสามารถเก็บรวบรวมได้ทั้งหมดจำนวน 1,004 ชุด กรอบ

แนวคิดในการทำวิจัยครั้งนี้ ได้กำหนดขนาดตัวอย่างของจำนวนบุคลากรที่จะใช้ในการเก็บรวบรวมข้อมูลจากจำนวนประชากรใน 10 สถาบัน ด้วยการกำหนดขนาดของทอมสัน (Thompson, S.K.2002) ในส่วนของสถิติเชิงพรรณา ได้แก่จำนวนร้อยละ ค่าเฉลี่ยเลขคณิต ($\overline{X}$) และส่วนเบี่ยงเบนมาตรฐาน (S.D.) ของแต้มเฉลี่ยที่ได้จากการทำแบบสอบถามเจตคติของผู้บริหาร คณาจารย์ เจ้าหน้าที่ นักศึกษา และสถิติเชิงอนุมาน การวิเคราะห์ถดถอยพหุคูณ (Multiple Regressions Analysis) ศึกษาปัจจัยที่มีผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์ในการทำวิจัยครั้งนี้ เพื่อศึกษาการละเมิดจริยธรรมและภัยคุกคามความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: ของสถาบันอุดมศึกษาในเขตกรุงเทพฯ และปริมณฑล, เพื่อกำหนดประเภทของการละเมิดจริยธรรม และภัยคุกคามทางด้านเทคโนโลยีสารสนเทศ และเพื่อแสวงหาแนวทางป้องกันและการแก้ไขปัญหาเกี่ยวกับการละเมิดจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ

การศึกษาวิเคราะห์วิจัยนี้ เป็นลักษณะการวิจัยเชิงสำรวจ และสถิติเชิงอนุมาย มีการแบ่งแบบสอบถามออกเป็น 4 ตอน คือ **ตอนที่ 1** ข้อมูลเกี่ยวกับสถานภาพทั่วไปของผู้บริหาร คณาจารย์ บุคลากร พนักงาน และนักศึกษา **ตอนที่ 2** ปัจจัยที่มีผลกระทบด้านความรู้ทางเทคโนโลยีสารสนเทศ, พระราชบัญญัติ (พ.ร.บ.) ต่างๆ, ด้านสังคม, ด้านเศรษฐกิจ, ด้านพฤติกรรมการใช้คอมพิวเตอร์ และสื่อสังคมออนไลน์ โดยยึดระดับความรู้ความเข้าใจ และให้ผู้ตอบแบบสำรวจให้ระดับค่าคะแนน ตั้งแต่ 1 ถึง 5 **ตอนที่ 3** ปัจจัยที่มีผลกระทบด้านจริยธรรม และความมั่นคงปลอดภัย โดยยึดระดับความคิดเห็น และ**ตอนที่ 4** ความคิดเห็น และข้อเสนอแนะเกี่ยวกับปัจจัยที่มีผลกระทบต่อการละเมิดจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ

5.2 สรุปผลการวิจัย

จากการสำรวจกลุ่มประชากรตัวอย่างของงานวิจัยครั้งนี้ มีผู้ตอบแบบสำรวจระดับการศึกษาต่ำกว่าปริญญาตรี จนถึงระดับปริญญาเอก โดยพบว่า กลุ่มตัวอย่างที่ใช้ในการศึกษาเป็นเพศชายร้อยละ 48.80 เพศหญิงร้อยละ 44.50 จะเห็นได้ว่าจำนวนผู้ตอบแบบสอบถามเป็นเพศชายมากกว่าเพศหญิงและไม่ระบุเพศร้อยละ 6.70 ส่วนใหญ่มีอายุ 20 – 25 ปี ซึ่งเป็นเยาวชนคนรุ่นใหม่ คิดเป็นร้อยละ 61.40 รองลงมาเป็น อายุต่ำกว่า 20 ปี คิดเป็นร้อยละ 20.40 กลุ่มตัวอย่างที่ใช้ในการศึกษาส่วนใหญ่จบการศึกษาสูงสุดระดับปริญญาตรีคิดเป็นร้อยละ 68.80 และต่ำกว่าปริญญาตรีคิดเป็นร้อยละ 19.10 กลุ่มตัวอย่างส่วนมากมีประสบการณ์ในการใช้เทคโนโลยีสารสนเทศ อยู่ในระดับมากและระดับปานกลาง คิดเป็นร้อยละ 34.70 และ 33.80 ตามลำดับ

ต่อมาเมื่อกล่าวถึงภาพรวมในการศึกษาครั้งนี้จำแนกปัจจัยออกเป็น 5 ด้าน ได้แก่ ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.) ด้านสังคม ด้านเศรษฐกิจและ ด้านพฤติกรรมการใช้คอมพิวเตอร์ และสื่อสังคมออนไลน์ ขอนำเสนอผลการวิเคราะห์ในรูปค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ทั้งในภาพรวม รายด้าน และรายข้อ แสดงค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ภาพรวมปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคง

ปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: พบว่าภาพรวมปัจจัยทั้ง 5 ด้าน มีค่าเฉลี่ยเท่ากับ 3.72 อยู่ในระดับมาก โดยด้านที่มีค่าเฉลี่ยสูงที่สุดใน 5 ด้านนี้ คือ ด้านพฤติกรรมการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์ มีค่าเฉลี่ยเท่ากับ 3.98 อยู่ในระดับมาก ซึ่งแสดงให้เห็นว่า ผู้ตอบแบบสอบถามคนไทยส่วนใหญ่มีพฤติกรรมการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์กันมาก สอดคล้องกับ WP ได้รายงานในเว็บไซต์ www.brandbuffet.in.th ว่า ประเทศไทยมีประชากร 69.11 ล้านคน (53% อยู่ในเขตเมือง) แบ่งเป็นประชากรผู้หญิง 51.3% – ผู้ชาย 48.7% มีผู้ใช้งานอินเทอร์เน็ต 57 ล้านคน ผู้ใช้งาน Social Media มากถึง 51 ล้านคน ผู้ใช้งานโทรศัพท์มือถือสูงถึง 93.61 ล้านเลขหมาย มากกว่าจำนวนประชากรทั้งประเทศในจำนวนผู้ใช้งานอินเทอร์เน็ตทั้งหมด มีผู้ใช้ Social Media เป็นประจำผ่าน Smart Device 46 ล้านคน **“คนไทย”** ใช้เวลาเข้าอินเทอร์เน็ตต่อวันมากที่สุดในโลก – กรุงเทพฯ ยังคงครองแชมป์เมืองที่มีผู้ใช้ Facebook มากสุดในโลก แสดงให้เห็นชัดเจนว่าปัจจุบัน “ประเทศไทย” เป็นประเทศที่ใช้เวลาต่อวันอยู่กับอินเทอร์เน็ตมากที่สุดในโลก (รวมทุกอุปกรณ์) โดยเฉลี่ยอยู่ที่ 9 ชั่วโมง 38 นาทีต่อวัน และถ้าวัดเฉพาะการใช้งานอินเทอร์เน็ตบนสมาร์ทโฟน “ไทย” ยังคงเป็นประเทศที่ใช้เวลาท่องเน็ตต่อวันมากที่สุดในโลกเช่นกัน โดยเฉลี่ยอยู่ที่ 4 ชั่วโมง 56 นาที ส่วนรองลงมาเป็นด้านสังคม มีค่าเฉลี่ยเท่ากับ 3.96 อยู่ในระดับมากเช่นกัน ส่วนด้านที่มีค่าเฉลี่ยต่ำที่สุด คือ ด้านความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.) มีค่าเฉลี่ยเท่ากับ 3.14 อยู่ในระดับปานกลาง ซึ่งในประเด็นท้ายนี้จะเห็นว่า ประชากรกลุ่มตัวอย่าง มีการใช้สื่อสังคมออนไลน์กันอย่างมากมายกว้างขวาง เพราะค่าเฉลี่ยอยู่ในระดับมาก และนอกจากนี้ มีข้อสังเกตว่า ประชากรกลุ่มตัวอย่างยังไม่ค่อยมีความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ.คอมพิวเตอร์ และ พ.ร.บ. อื่นๆ มีค่าเฉลี่ยต่ำ ซึ่งมีความจำเป็นอย่างมากต่อการดำรงชีวิตในยุคดิจิทัล ด้วยข้อมูลวิจัยตรงนี้เอง จึงมีความจำเป็นที่สถาบันการศึกษาทั้งภาครัฐและเอกชน ควรรณรงค์ส่งเสริมและให้ความรู้แก่ประชาชนเกี่ยวกับพระราชบัญญัติต่างๆ โดยเฉพาะพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ.2550 และปรับปรุงปี พ.ศ.2560

สำหรับการสำรวจเกี่ยวกับความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศพบว่าภาพรวมความรู้ความเข้าใจด้านเทคโนโลยี มีค่าเฉลี่ยเท่ากับ 3.72 อยู่ในระดับมาก โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คือ ความรู้เรื่องเว็บเครือข่ายสังคมออนไลน์ เช่น Facebook Line Twitter YouTube Instagram มีค่าเฉลี่ยเท่ากับ 3.99 อยู่ในระดับมาก ตรงกับ Narongyod Mahittivanicha, The Flight 19 Agency ได้รายงานในเว็บ ETDA Thailand และเว็บ www.twfdigital.com ว่า คนไทยใช้ YouTube, Line, Facebook เป็น Top 3 Social/Chat platform โดยใช้ Youtube ใช้เปิดดูไฟล์วิดีโอต่างๆ มากที่สุด รองลงมาเป็นเรื่องความรู้เรื่องการจัดเก็บข้อมูล เช่น การสร้างโฟลเดอร์ (Folder) การจัดการแฟ้มข้อมูล (File) การสำรองข้อมูล (Backup) มีค่าเฉลี่ยเท่ากับ 3.86 อยู่ในระดับมาก เช่นกัน ส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือ ความรู้เรื่องข้อมูล เช่น การจัดการข้อมูลและฐานข้อมูล (Database) มีค่าเฉลี่ยเท่ากับ 3.50 อยู่ในระดับมาก แต่เมื่อเปรียบเทียบกับความรู้เรื่องอื่นๆ เกี่ยวกับเทคโนโลยีสารสนเทศ เช่น เรื่องฮาร์ดแวร์ ซอฟต์แวร์ เครือข่ายคอมพิวเตอร์ ความรู้เรื่องการจัดการข้อมูล และฐานข้อมูลยังต่ำกว่าด้านอื่นๆ

ในขั้นตอนต่อมาเป็นความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.) พบว่าภาพรวมความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.) มีค่าเฉลี่ยเท่ากับ 3.14 อยู่ในระดับปานกลาง โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ

คอมพิวเตอร์ ปี พ.ศ.2550 มีค่าเฉลี่ยเท่ากับ 3.24 อยู่ในระดับปานกลางรองลงมาเป็นเรื่องพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ.2550 แก้ไขเพิ่มเติม ปี พ.ศ. 2560 มีค่าเฉลี่ยเท่ากับ 3.22 อยู่ในระดับปานกลาง เช่นกัน ส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือ ความรู้เรื่องพระราชบัญญัติลิทธิบัตร ปี พ.ศ.2522 แก้ไขเพิ่มเติม พ.ศ. 2542 มีค่าเฉลี่ยเท่ากับ 3.07 อยู่ในระดับปานกลาง ในประเด็นนี้ จะเห็นว่า เมื่อกล่าวถึงพระราชบัญญัติทั้งหลาย นักศึกษาและประชาชนทั่วไป พอรู้เรื่องเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มากกว่าพระราชบัญญัติด้านอื่นๆ ซึ่งในที่นี้จะเห็นได้ว่า นักศึกษา และประชาชนทั่วไปมีความรู้เกี่ยวกับเรื่องสิทธิบัตรน้อยมาก ซึ่งควรจะมีการให้ความรู้ในด้านนี้ให้มากขึ้น เพราะจะช่วยส่งเสริมให้คนมีการจดสิทธิบัตรกันมากขึ้น ซึ่งจะตรงกับนโยบายของรัฐบาลที่ต้องการยกระดับรายได้ของประชากรไทยให้สูงขึ้นที่เรียกเรียกว่า นโยบายประเทศไทย 4.0 (Thailand 4.0)

ต่อมาเป็นค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ปัจจัยด้านสังคมพบว่า ภาพรวมปัจจัยด้านสังคมมีค่าเฉลี่ยเท่ากับ 3.96 อยู่ในระดับมาก โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คือ เรื่องบันเทิงคนดูภาพยนตร์และโทรทัศน์ลดลง เพราะหันมาดูทางออนไลน์มากขึ้น เช่น YouTube มีค่าเฉลี่ยเท่ากับ 4.08 อยู่ในระดับมากรองลงมาเป็นเรื่องสื่อสังคมออนไลน์มีผลกระทบต่อสังคมในด้านลบ เช่น มีการหลอกลวงการปลอมเฟซบุ๊ค การละเมิดความเป็นส่วนตัว การโพสต์ภาพลามกอนาจารการค้ายาเสพติด ตลอดจนการเล่นพนันออนไลน์ มีค่าเฉลี่ยเท่ากับ 4.06 อยู่ในระดับมาก เช่นกัน ส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือ สื่อสังคมออนไลน์มีผลกระทบต่อสังคมในด้านบวก เช่น ช่วยลดความเหลื่อมล้ำทางสังคม การมีโน้ตบุ๊ค คอมพิวเตอร์ และสมาร์ทโฟนมีราคาถูกลง มีค่าเฉลี่ยเท่ากับ 3.83 อยู่ในระดับมาก ในกรณีนี้ ชี้ให้เห็นว่า คนไทย มีนิสัยชอบเรื่องความบันเทิงสนุกสนาน โดยเบนความสนใจมาดูวิดีโอออนไลน์ผ่าน YouTube กันมากขึ้น ในขณะเดียวกันการชมภาพยนตร์และการบันเทิงทางโทรทัศน์ลดน้อยลง อันนี้ก็จะเป็นประโยชน์สำหรับภาคธุรกิจและเอกชน แม้กระทั่งหน่วยงานของรัฐบาลเอง ควรใช้ช่องทางการสื่อสารต่างๆ ไปยังคนไทยทั่วประเทศผ่านช่องทางสื่อสังคมออนไลน์อย่าง YouTube ให้มากขึ้น

สำหรับ ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ปัจจัยด้านเศรษฐกิจ พบว่า ภาพรวมปัจจัยด้านเศรษฐกิจมีค่าเฉลี่ยเท่ากับ 3.85 อยู่ในระดับมาก โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คือ เกิดธุรกิจบริการใหม่ๆ เช่น การรับส่งสินค้าพัสดุแบบรีบด่วน เช่น Kerry Express ฯลฯ มีค่าเฉลี่ยเท่ากับ 3.98 อยู่ในระดับมากรองลงมาเป็นเรื่อง เกิดธุรกิจประเภทตัวแทนทางด้านการเงินในการจัดซื้อสินค้าทางออนไลน์มีค่าเฉลี่ยเท่ากับ 3.89 อยู่ในระดับมาก ส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือ การจ้างงานของภาคธุรกิจบางกลุ่มลดลง เช่น ธนาคาร ห้างสรรพสินค้า ร้าน จำหน่ายสินค้า มีค่าเฉลี่ยเท่ากับ 3.78 อยู่ในระดับมาก ในประเด็นนี้ มองว่า ธุรกิจพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) มีการเจริญเติบโตอย่างมาก สังเกตได้จากธุรกิจด้านโลจิสติกส์ (logistic) อย่าง Kerry Express เติบโตรวดเร็วมาก

ส่วนค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ปัจจัยด้านพฤติกรรมการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์ พบว่าภาพรวมปัจจัยด้านพฤติกรรมการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์มีค่าเฉลี่ยเท่ากับ 3.98 อยู่ในระดับมาก โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คือ พฤติกรรมการเรียนรู้ของเยาวชนเปลี่ยนแปลงไป โดยหันมาศึกษาเรียนรู้จาก อินเทอร์เน็ตและสื่อสังคมออนไลน์มากขึ้น

เป็นลำดับ เช่น Google Facebook Line YouTube เป็นเวลานานมากขึ้น มีค่าเฉลี่ยเท่ากับ 4.12 อยู่ในระดับมาก รองลงมาเป็นเรื่อง พฤติกรรมการซื้อขายสินค้าเปลี่ยนไป โดยผู้ซื้อ และผู้ขาย หันมาใช้บริการทางออนไลน์มากขึ้น มีค่าเฉลี่ยเท่ากับ 4.06 อยู่ในระดับมาก ส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือ เกิดพฤติกรรมหลงใหลการติดเกม และการพนันออนไลน์เพิ่มมากขึ้น มีค่าเฉลี่ยเท่ากับ 3.78 อยู่ในระดับมากค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน จริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศ ไทย 4.0 พบว่า ภาพรวมจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 มีค่าเฉลี่ยเท่ากับ 3.86 อยู่ในระดับมาก โดยด้านจริยธรรม มีค่าเฉลี่ยเท่ากับ 3.93 อยู่ในระดับมาก เช่นเดียวกับด้านความมั่นคงปลอดภัย มีเฉลี่ยเท่ากับ 3.80 อยู่ในระดับมากเช่นกัน ในประเด็นนี้ เห็นว่า นักศึกษาและประชาชนทั่วไป ยังมีความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยน้อย ไม่ว่าจะเป็นการตั้งรหัสผ่าน การป้องกันความปลอดภัยต่างๆ ของข้อมูล เช่น การใช้ซอฟต์แวร์ป้องกันความปลอดภัยจากไวรัส และจากการโจมตีจากแฮกเกอร์ ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ด้านจริยธรรมทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 พบว่าภาพรวมจริยธรรมทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 มีค่าเฉลี่ยเท่ากับ 3.93 อยู่ในระดับมาก โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คือมีปัญหาเรื่องการโกหกหลอกลวงทางอินเทอร์เน็ต และทางสื่อสังคมออนไลน์เพิ่ม มากขึ้น มีค่าเฉลี่ยเท่ากับ 4.01 อยู่ในระดับมากรองลงมาเป็นเรื่องการเข้าถึงภาพลามกอนาจาร ความรุนแรง และความน่ากลัวมีมากเพิ่มขึ้นมีค่าเฉลี่ยเท่ากับ 3.96 อยู่ในระดับมากส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือความมีวินัยเรียนรู้ในการทำงานลดลงมีค่าเฉลี่ยเท่ากับ 3.83 อยู่ในระดับมาก ประเด็นนี้ ชี้ให้เห็นว่า ปัจจุบันภัยคุกคามทางอินเทอร์เน็ต และสื่อสังคมออนไลน์มีมากขึ้นตามลำดับ ค่าเฉลี่ยนี้ทำให้เป็นที่น่าสังเกตว่าคนรับรู้ข่าวสารการหลอกลวงทางอินเทอร์เน็ตและสื่อสังคมออนไลน์อย่างต่อเนื่องสม่ำเสมอ

ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ด้านความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 พบว่าภาพรวมด้านความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 มีค่าเฉลี่ยเท่ากับ 3.80 อยู่ในระดับมาก โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คืออินเทอร์เน็ตและสื่อสังคมออนไลน์ เป็นแหล่งการก่ออาชญากรรมทางคอมพิวเตอร์ เพราะสามารถใช้ได้ทุกที่ทุกเวลามีค่าเฉลี่ยเท่ากับ 3.86 อยู่ในระดับมากรองลงมาเป็นเรื่องรัฐ และองค์กร ต้องเพิ่มความเข้มงวดด้านนโยบาย ด้านความมั่นคงปลอดภัย ทางด้านเทคโนโลยีสารสนเทศให้สูงขึ้น มีค่าเฉลี่ยเท่ากับ 3.84 อยู่ในระดับมากส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือ มีการข่มขู่ กรรโชก ทางอีเมล์ และสื่อสังคมออนไลน์ และ มีการแก้ไขกฎหมาย และเพิ่มโทษมากขึ้น เช่น พ.ร.บ คอมพิวเตอร์ ปี 2550 แก้ไขเพิ่มเติม พ.ศ.2560 มีค่าเฉลี่ยเท่ากับ 3.78 อยู่ในระดับมาก ความสัมพันธ์ระหว่างความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ. สังคม เศรษฐกิจ และพฤติกรรม กับ จริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศในบริบทของประเทศไทย 4.0 พบว่า ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ. สังคม เศรษฐกิจ และพฤติกรรม มีความสัมพันธ์กับ ความมั่นคงปลอดภัยและ

จริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ในทิศทางเดียวกัน ด้วยขนาดความสัมพันธ์เท่ากับ 0.507 0.233 0.649 0.665 และ 0.760 ตามลำดับ นอกจากนั้นยังพบว่าภาพรวมของทั้ง 5 ปัจจัยมีความสัมพันธ์ทางสถิติอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ด้วยขนาดความสัมพันธ์เท่ากับ 0.702 ในทิศทางเดียวกัน

อิทธิพลที่ปัจจัยด้านความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ. สังคม เศรษฐกิจ และพฤติกรรม มีต่อ จริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 พบว่า ตัวแปรอิสระทั้ง 5 ได้แก่ ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ. สังคม เศรษฐกิจ และพฤติกรรม สามารถอธิบายความฝันแปรของจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ได้อย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05 (F = 317.239) ตัวแปรอิสระทั้ง 5 มีความสัมพันธ์กับจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ร้อยละ 78.4 และสามารถอธิบายการเปลี่ยนแปลงของจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ได้ร้อยละ 61.5 เมื่อพิจารณาอิทธิพลพบว่าปัจจัยที่มีอิทธิพลต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 อย่างมีนัยสำคัญทางสถิติที่ระดับนัยสำคัญ 0.05 ได้แก่ ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ปัจจัยทางสังคม ปัจจัยเศรษฐกิจ และพฤติกรรม ด้วยขนาดอิทธิพลเท่ากับ 0.084 0.117 0.140 และ 0.504

5.3 การอภิปรายผล

จากข้อมูลตารางเรื่อง อิทธิพลที่ปัจจัยมีต่อความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 พบว่า ตัวแปรอิสระทั้ง 5 ได้แก่ ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ. สังคม เศรษฐกิจ และพฤติกรรมการใช้คอมพิวเตอร์ สามารถอธิบายความผันแปรของจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ได้อย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05 (F = 317.239) ตัวแปรอิสระทั้ง 5 มีความสัมพันธ์กับจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ร้อยละ 78.4 และสามารถอธิบายการเปลี่ยนแปลงของจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ได้ร้อยละ 61.5 เมื่อพิจารณาอิทธิพลพบว่า ปัจจัยที่มีอิทธิพลต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 อย่างมีนัยสำคัญทางสถิติที่ระดับนัยสำคัญ 0.05 ได้แก่ ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ปัจจัยทางสังคม ปัจจัยเศรษฐกิจ และพฤติกรรม ด้วยขนาดอิทธิพลเท่ากับ 0.084 0.117 0.140 และ 0.504

วิเคราะห์ในประเด็นนี้ จะเห็นได้ว่า ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ. สังคม เศรษฐกิจ และพฤติกรรมการใช้คอมพิวเตอร์ มีค่าเฉลี่ยต่ำกว่า

0.05 แสดงว่า มีอิทธิพล สอดคล้องกับสมมุติฐานการวิจัยที่ตั้งเอาไว้ว่า ปัจจุบันปัญหาและการละเมิดจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศมีความรุนแรงมากขึ้น และสอดคล้องกับงานวิจัยของ สุพิชญา อาชวิรดา ที่สรุปผลการวิจัยประเด็นหนึ่งว่า ระดับการรักษาความมั่นคงปลอดภัย นอกจากจะขึ้นอยู่กับการรับรู้ถึงภัยคุกคาม และพฤติกรรมการใช้ระบบสารสนเทศในองค์กร ตามทฤษฎีพฤติกรรมตามแผนแล้ว ยังขึ้นอยู่กับปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ การฝึกอบรมและการให้ความรู้ และการตระหนักถึงความปลอดภัย ส่วนปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ ตามงานวิจัยเรื่องนี้ คือ ผู้บริหาร คณาจารย์ บุคลากร พนักงาน และนักศึกษา ยังมีความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศไม่มากนัก รวมถึงได้รับทราบพฤติกรรมการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์มีการละเมิดจริยธรรมทางเทคโนโลยีสารสนเทศของบุคคลทั่วไปในสังคม ซึ่งได้สร้างผลกระทบต่อสังคมและเศรษฐกิจของประเทศชาติโดยรวม

นอกจากนี้ เมื่อดูตามคำถามวิจัยในข้อที่ 1 ที่ถามว่า อะไรคือปัจจัย-ปัญหาการละเมิดจริยธรรม และภัยคุกคามความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศในปัจจุบัน สามารถตอบได้ว่า การขาดความรู้ความเข้าใจเกี่ยวเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.) ต่างๆ หรือคนไม่ได้ให้ความสำคัญเกี่ยวกับพระราชบัญญัติ โดยเฉพาะพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ รวมถึงพระราชบัญญัติลิขสิทธิ์ และสิทธิบัตรด้วย

ในประเด็นต่อมา คำถามวิจัยข้อที่ 2 และสมมุติฐานการวิจัย ข้อ 2 ประเภทของการละเมิดจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีทางด้านเทคโนโลยีสารสนเทศมีกี่ประเภทอะไรบ้าง ตอบได้ว่ามี 7 ประเภท ได้แก่ (1) การใช้งานคอมพิวเตอร์อย่างขาดความรับผิดชอบ รวมไปถึง การโพสต์ภาพลามกอนาจาร การสร้างความรุนแรงในลักษณะต่างๆ (2) การละเมิดความเป็นส่วนตัวของผู้อื่น (3) การขโมยอัตลักษณ์ การหลอกลวงทางอินเทอรีเน็ต (4) การเจาะระบบ (5) การใช้ไวรัสโจมตี (6) การละเมิดลิขสิทธิ์ (7) การส่งอีเมลที่ไม่ได้รับเชิญ (Spamming) รบกวนสร้างความรำคาญให้กับผู้อื่น และจากการวิจัยพบว่า ภาพรวมจริยธรรมทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 มีค่าเฉลี่ยเท่ากับ 3.93 อยู่ในระดับมาก โดยเรื่องที่มีค่าเฉลี่ยสูงที่สุดในด้านนี้ คือมีปัญหาเรื่องการโกหกหลอกลวงทางอินเทอร์เน็ต และทางสื่อสังคมออนไลน์เพิ่มมากขึ้น มีค่าเฉลี่ยเท่ากับ 4.01 อยู่ในระดับมากรองลงมาเป็นเรื่องการเข้าถึงภาพลามกอนาจาร ความรุนแรง และความน่ากลัวมีมากเพิ่มขึ้นมีค่าเฉลี่ยเท่ากับ 3.96 อยู่ในระดับมากส่วนเรื่องที่มีค่าเฉลี่ยต่ำที่สุด คือความมีวินัยเรียนรู้ในการทำงานลดลงมีค่าเฉลี่ยเท่ากับ 3.83 อยู่ในระดับมาก ในประเด็นนี้ จะเห็นได้ว่าปัจจุบันการโกหกหลอกลวงทางอินเทอร์เน็ต และทางสื่อสังคมออนไลน์เพิ่มมากขึ้นเป็นลำดับ สอดคล้องกับรายงานของ ฟอร์ติเน็ต ผู้นำระดับโลกด้านโซลูชั่นการรักษาความปลอดภัยแบบไซเบอร์แบบบูรณาการและแบบอัตโนมัติเผยถึงแนวโน้มภัยคุกคามในปี 2019 รวบรวมโดยทีมงานฟอร์ติเน็ต แล็บส์ (FortiGuard Labs) ซึ่งการคาดการณ์เหล่านี้แสดงให้เห็นถึงวิธีการและเทคนิคที่นักวิจัยคาดว่าจะเกิดขึ้นในอนาคตอันใกล้นี้ ที่อาชญกรไซเบอร์นิยมใช้ 1 ในนั้น คือ การใช้กลยุทธ์การหลอกลวงขั้นสูง: องค์กรควรรวมเทคนิคการหลอกลวงทั้งหลายเข้ากับกลยุทธ์ด้านความปลอดภัยขององค์กรเพื่อให้

ให้ได้เครือข่ายที่สร้างขึ้นจากข้อมูลที่เป็นเท็จ ซึ่งจะบังคับให้ผู้ประสงค์ร้ายตรวจสอบข้อมูลด้านภัยคุกคามอัจฉริยะ (Threat Intelligence) ของตนตลอดเวลา จะใช้เวลาและทรัพยากรในการตรวจหาข้อมูลที่ผิดพลาดไม่เป็นความจริง (False Positive) มากขึ้น และจะตรวจสอบว่า ทรัพยากรเครือข่ายที่ตนเห็นนั้นถูกต้องมีจริง

ในประเด็นสุดท้ายของสมมุติฐานการวิจัยในข้อ 3 ปัจจัยที่มีผลกระทบต่อจริยธรรมทั่วไปและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ได้แก่ (1) ความรู้เกี่ยวกับคอมพิวเตอร์ (2) ความรู้เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ และกฎหมายที่เกี่ยวข้องอื่นๆ (3) ปัจจัยทางสังคม (4) ปัจจัยทางด้านเศรษฐกิจ (5) ปัจจัยทางด้านพฤติกรรมการใช้คอมพิวเตอร์ จากการวิจัยพบว่า ปัจจัยด้าน ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ. สังคม เศรษฐกิจ และพฤติกรรม มีต่อ จริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 พบว่า ตัวแปรอิสระทั้ง 5 ได้แก่ ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ. สังคม เศรษฐกิจ และพฤติกรรม สามารถอธิบายความฝันแปรของจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ได้อย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05 (F = 317.239) ตัวแปรอิสระทั้ง 5 มีความสัมพันธ์กับจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ร้อยละ 78.4 และสามารถอธิบายการเปลี่ยนแปลงของจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 ได้ร้อยละ 61.5 เมื่อพิจารณาอิทธิพลพบว่าปัจจัยที่มีอิทธิพลต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0 อย่างมีนัยสำคัญทางสถิติที่ระดับนัยสำคัญ 0.05 ได้แก่ ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ปัจจัยทางสังคม ปัจจัยเศรษฐกิจ และพฤติกรรม ด้วยขนาดอิทธิพลเท่ากับ 0.084 0.117 0.140 และ 0.504 ประเด็นนี้สอดคล้องกับงานวิจัยเรื่อง เปิดวิจัย Cyberbullying เยาวชนไทยกับความเสี่ยงยุค 4.0
เกี่ยวกับพฤติกรรมเสี่ยง โดย รศ.นพ.ชาญวิทย์ย้ำว่า การใช้งานอินเทอร์เน็ตอย่างปลอดภัยมีผลสัมพันธ์กับความเสี่ยงที่จะถูกกลั่นแกล้งบนโลกออนไลน์อย่างมาก การเปิดเผยข้อมูลส่วนตัวมากยิ่งเป็นความเสี่ยง ทั้งการรับคนอื่นที่ไม่รู้จักมาเป็นเพื่อน การแชตหรือการออกไปพบคนแปลกหน้า ใช้รูปจริงเป็นรูปโปรไฟล์ การไม่ตั้งค่าความเป็นส่วนตัวในการใช้งาน การปล่อยให้ผู้อื่นรู้รหัสการใช้งาน รวมถึงไม่ Logout ออกจากระบบ เมื่อใช้งานเสร็จหรือให้ผู้อื่นยืมใช้โทรศัพท์ “การแก้ปัญหาอย่างยั่งยืนจะต้องมองไปถึงต้นตอของปัญหา นั่นคือการสร้างวัฒนธรรมการใช้อินเทอร์เน็ตอย่างปลอดภัยและสร้างสรรค์ ซึ่งจำเป็นต้องอาศัยความร่วมมือระหว่างภาครัฐเอกชน และประชาคม ในการร่วมกันแก้ปัญหาและปลูกฝังวัฒนธรรมนี้” ส่วนนายพิเชษฐ ดุรงคเวโรจน์ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอี) กล่าวว่า ผลกระทบจากการใช้อินเทอร์เน็ตในกลุ่มเด็กและเยาวชน เริ่มเห็นปัญหาได้ชัดขึ้น จึงได้บริการให้คำปรึกษาผ่าน “Stop Bullying Chat Line” ทั้งจะประสานกับกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) เพื่อให้เข้ามาให้คำปรึกษาเบื้องต้นทางเทคนิคสำหรับการส่งต่อกรณีที่มีการกลั่นแกล้งรังแกในโลกออนไลน์ ในช่วงเวลา 16.00-22.00 น. ของทุกวัน รวมถึงจัดกิจกรรมอบรมการใช้อินเทอรีเน็ตอย่างปลอดภัยผ่านศูนย์ดิจิทัลชุมชนด้วย

5.4 ข้อเสนอแนะเพื่อดำเนินการ

1. การดำเนินการวิจัยเรื่อง **“ปัจจัยที่มีผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: กรณีศึกษาสถาบันอุดมศึกษาในเขตกรุงเทพมหานคร และปริมณฑล”** ตามที่ได้ทำการสรุปผลแล้ว จะเห็นได้ว่า มีหลายประเด็นที่น่าสนใจ เช่น ผู้ตอบแบบสอบถามมีพฤติกรรมการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์ มีค่าเฉลี่ยเท่ากับ 3.98 อยู่ในระดับมาก แต่มีความรู้ความเข้าใจเกี่ยวพระราชบัญญัติ (พ.ร.บ.) มีค่าเฉลี่ยเท่ากับ 3.14 ในระดับปานกลาง ซึ่งข้อนี้ สถาบันการศึกษาต่างๆ ควรให้ความสำคัญและให้สนใจในการปรับปรุงหลักสูตร หรือเสนอแนะให้อาจารย์ผู้สอนเพิ่มความรู้ในส่วนที่เกี่ยวข้องกับพระราชบัญญัติใส่เข้าในชั่วโมงการสอน เช่น พระราชบัญญัติสิทธิบัตร ปี พ.ศ.2522 แก้ไขเพิ่มเติม พ.ศ.2542, พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, พระราชบัญญัติว่าด้วยธุรกรรรมอิเล็กทรอนิกส์ เป็นต้น

2.นอกจากนี้ ปัจจัยที่มีอิทธิพลต่อความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ จะเห็นได้ว่า ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ มีค่าเฉลี่ยต่ำกว่า 0.05 แสดงให้เห็นว่า พฤติกรรมการใช้คอมพิวเตอร์ และสื่อสังคมออนไลน์ มีผู้ใช้เป็นจำนวนมาก แต่ขาดความรู้ความเข้าใจที่ดี ซึ่งจะส่งผลกระทบต่อสังคม เช่น การละเมิดความเป็นส่วนตัว หรือโพสต์เรื่องที่ไม่เหมาะสมลงไป เช่น ภาพลามกอนาจาร, การค้ายาเสพติด, การสร้างความรุนแรงด้วยการทำร้ายร่างกายผู้อื่น, หรือแม้กระทั่งการใส่ข้อมูลเท็จลงไป โดยไม่รู้ว่า เป็นสิ่งที่ผิดกฎหมาย เป็นต้น

3. ในประเด็นต่อมา ขอเสนอแนะให้ข้อมูลเพิ่มเติมเรื่องความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ จะเห็นได้ว่า ผู้ตอบแบบสอบถามมีความรู้เรื่องเว็บเครือข่ายสังคมออนไลน์ เช่น Facebook, Line, Twitter, YouTube และ Instagram มีค่าเฉลี่ยเท่ากับ 3.99 อยู่ในระดับมาก แต่มีความรู้เรื่องข้อมูล เช่น การจัดการข้อมูล และฐานข้อมูล (Database) มีค่าเฉลี่ย 3.50 อยู่ในระดับมาก แต่ครั้นเปรียบเทียบกับด้านอื่นๆ เช่น ความรู้เรื่องอุปกรณ์ฮาร์ดแวร์ หน่วยประมวลผลกลาง หน่วยบันทึกข้อมูลได้แก่ ฮาร์ดดิสก์ และซอฟต์แวร์ เช่น Windows, MS-Office จะเห็นได้ว่า ต่ำกว่าเรื่องอื่นๆ ข้อนี้ ชี้ให้เห็นว่า สถาบันการศึกษาควรเพิ่มพูนความรู้ในเรื่องนี้ใส่เข้าไป

5.5 ข้อเสนอแนะเพื่อการทำวิจัยครั้งต่อไป

1. งานวิจัยนี้ เป็นการวิจัยเรื่อง **“ปัจจัยที่มีผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: กรณีศึกษาสถาบันอุดมศึกษาในเขตกรุงเทพมหานคร และปริมณฑล”** ดังนั้น จะเห็นได้ว่า ขอบเขตของการทำวิจัย จำกัดอยู่ภายในเขตกรุงเทพมหานคร และปริมณฑลเท่านั้น หากมีโอกาสทำในครั้งต่อไป อาจทำครอบคุมถึงภาคกลาง ภาคเหนือ ภาคตะวันออกเฉียงเหนือ ภาคตะวันออก และภาคใต้ หรืออาจทำครอบคุมทั้งประเทศก็เป็นได้ ซึ่งผลสรุปการวิจัยจะได้รับในอีกลักษณะหนึ่งที่แตกต่างกันออกไป

2. การวิจัยในครั้งนี้ ได้ทำการสุ่มตัวอย่างมหาวิทยาลัยจากแต่ละกลุ่มโดยการสุ่มตัวอย่างจาก

10 สถาบัน ด้วยวิธีการสุ่มอย่างง่ายคือวิธีจับฉลาก ซึ่งมหาวิทยาลัยในเขตกรุงเทพมหานคร และปริมณฑลมีจำนวนมากถึง 61 สถาบัน จึงไม่อาจสามารถเก็บข้อมูลได้หมดทุกสถาบัน

3. การทำวิจัยครั้งนี้ ยังไม่ได้เน้นไปที่การแสวงหาแนวทางในการแก้ไขปัญหาผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ หากมีโอกาสได้ทำครั้งต่อไป อาจจะได้ทำในส่วนนี้ ซึ่งจะทำให้งานวิจัยมีความสมบูรณ์มากขึ้น

4. ข้อสังเกตอีกอย่างหนึ่งในการเก็บข้อมูล คือ มีบางมหาวิทยาลัยให้ความร่วมมือในการตอบแบบสอบถามดีมาก แต่มีบางมหาวิทยาไม่ค่อยจะให้ความร่วมมือ และมีขั้นตอนยุ่งยากมาก หรือบางครั้งเขาอาจจคิดว่า มหาวิทยาลัยอื่นจะเข้าไปรู้ความลับของเขาและนำมาเปิดเผย ซึ่งตามความเป็นจริงแล้วในแบบสอบถามวิจัยนั้นก็ได้ระบุว่า ข้อมูลที่ได้รับมาจะนำมาใช้เพื่อเป็นประโยชน์ทางวิชาการเท่านั้น และจะไม่กระทบต่อตัวท่านแต่ประการใด

5. ในการศึกษาวิจัยครั้งนี้จำแนกปัจจัยออกเป็น 5 ด้าน ได้แก่ ความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ ความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.) ด้านสังคม ด้านเศรษฐกิจ และ ด้านพฤติกรรมการใช้คอมพิวเตอร์ และสื่อสังคมออนไลน์ ในการทำวิจัยครั้งต่อไป อาจเพิ่มปัจจัยในด้านอื่นๆ เข้ามา เช่น ด้านการเมือง เพราะปัจจุบันมีนักการเมืองจำนวนมาก ใช้สื่อสังคมออนไลน์เข้ามาช่วยในการหาเสียง และทำให้ได้รับชัยชนะ เช่น นายบารัค โอบามา ประธานาธิบดีสหรัฐอเมริกา เป็นต้น

บรรณานุกรม

บรรณานุกรม

กนกวรรณ ตาลเสี้ยน. 2560. “ความมั่นคงปลอดภัยของระบบสารสนเทศ” สืบค้น เมื่อวันที่ 29 พฤษภาคม 2560, จาก https://sites.google.com/site/kanokwant551/prawati- swn-taw

คึกฤทธิ์ ปราโมช, ม.ร.ว. 2562. “ความหมายของจริยธรรม”. สืบค้น เมื่อวันที่ 31 มีนาคม 2562, จาก www.baanjomyut.com

ชนินทร์ นาทะพันธ์. 2555. “การศึกษาดัชนีความสุขมวลรวมในประเทศไทย ทางด้านเทคโนโลยีสารสนเทศ” **วารสารศรีปทุมปริทัศน์ ฉบับวิทยาศาสตร์และเทคโนโลยี** ปีที่ 4, ฉบับที่ 1 :29.

ชาญวิทย์ พรนภดล, (2561). “เปิดวิจัย Cyberbullying เยาวชนไทยกับความเสี่ยงยุค 4.0” **หนังสือพิมพ์ประชาชาติธุรกิจ**: 21.

ณมน จีรังสุวรรณ. 2561. “การวิเคราะห์ผลกระทบทางเทคโนโลยีสารสนเทศและการสื่อสารกับนักสื่อสารมวลชนอิเล็กทรอนิกส์” สืบค้น เมื่อวันที่ 17 มกราคม 2561, จาก https://www.tci-thaijo.org/index.php/abc/article/view/.../44951

ณัฐนันท์ ศิริเจริญ. 2558. “รูปแบบการสื่อสารเพื่อการรู้เท่าทันสื่อและสารสนเทศจากสื่ออินเทอร์เน็ตของเยาวชนไทย.” **วารสารศรีปทุมปริทัศน์ ฉบับมนุษยศาสตร์และสังคมศาตร์** ปีที่ 15, ฉบับที่ 1 : 52-53.

ธนกร มีหินกอง. 2556. “ตัวแบบการจัดหารการบุกรุกเชิงเวลาจริงแบบปรับตัวในการรักษาความมั่นคงปลอดภัยไซเบอร์บนพื้นฐานของสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์” วิทยานิพนธ์ปริญญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ บัณฑิตวิทยาลัย มหาวิทยาลัยศรีปทุม.

ธีรินทร์ เกตุวิชิต. 2557. “การพัฒนาระบบแลกเปลี่ยนสารสนเทศทางการแพทย์ในระบบส่งต่อผู้ป่วย” **วารสารศรีปทุมปริทัศน์ ฉบับวิทยาศาสตร์และเทคโนโลยี** ปีที่ 6, ฉบับที่ 1: 74-75.

นิภา ศรีไพโรจน์. 2561. “ความรู้เบื้องต้นเกี่ยวกับการวิจัย” สืบค้น เมื่อวันที่ 15 มกราคม 2561, จาก http://mcpswis.mcp.ac.th.

ประจิต ลิ้มสายพรหม. 2557. “ตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์ โดยใช้เทคนิคเหมืองข้อมูลและโครงข่ายกราฟ” วิทยานิพนธ์ปริญญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ บัณฑิตวิทยาลัย มหาวิทยาลัยศรีปทุม.

ประชาชาติธุรกิจ. 2558. “อาชญากรไซเบอร์จ้องถล่มภาครัฐ สถิติ 5 เดือนแรกพุ่ง-แชร์ข้อมูลใน" โซเชียล"สุดเสี่ยง” สืบค้น เมื่อวันที่ 30 มิถุนายน 2560, จาก www.prachachat.net/news

ประสงค์ ประณีตพลกรัง. 2558. “ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)” เอกสารประกอบการบรรยาย บัณฑิตวิทยาลัย คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม. (มิถุนายน 2558): 43.

ปรานอม หยวกทอง. 2562. “ผลกระทบของเทคโนโลยีสารสนเทศ” สืบค้น เมื่อวันที่ 7 เมษายน 2562, จาก https://sites.google.com/site/kroonom/phlk-ra-thb-khxng-thekhnoloyi-sarsnthes

พงศ์สุข หิรัญพฤกษ์. 2560. “TREND IT 2018 Live สดทันที ที่มีเรื่องกับหนุ่ยแบไต๋” Teck Talk #9 คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม, วันที่ 8 พฤศจิกายน 2560.

พระราชวรมุนี (ประยุทธ์ ปยุตโต). 2562. “ความหมายของจริยธรรม”. สืบค้น เมื่อวันที่ 31 มีนาคม 2562, จาก www.baanjomyut.com

พิชญาณี ภู่ตระกูล. 2561. “การเปิดเผยตนเองในเครือข่ายสังคมออนไลน์: แนวทางการศึกษา ปัจจัยที่มีอิทธิพล และผลกระทบ” **วารสารพฤติกรรมศาสตร์เพื่อการพัฒนา** สืบค้น เมื่อวันที่ 15 มกราคม 2561, จาก http://bsris.swu.ac.th/jbsd/592/1.pdf

โพสต์ทูเดย์. 2560 : B/1.

เพลโต. 2560.“แนวคิด หลักการ ทฤษฎีทางคุณธรรมจริยธรรม” สืบค้น เมื่อวันที่ 13 กรกฎาคม 2560, จาก http://www.baanjomyut.com/library

ภาณุพงษ วงษ์รอด, บรรณาธิการ. 2560. “โจรไซเบอร์อาศัยช่องโหว่ DDoS และ POS ฉกเงินร้านค้า.” **วารสาร CIO World & Business** ISSUE 187, December 2017: 20.

แนวโน้มกลยุทธ์ของอาชญากรรมไซเบอร์ในปี 2019. 2562. Security Report, **วารสาร CIO World & Business** Issue 198, November 2018.

ราชกิจจานุเบกษา. 2562. “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) สืบค้น เมื่อวันที่ 22 เมษายน 2562, จาก http://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF

ราชบัณฑิตยสถาน, พจนานุกรม. 2562. “การวิจัย” สืบค้น. เมื่อวันที่ 3 กุมภาพันธ์ 2562, จาก https://dictionary.sanook.com/search/dict-th-th-royal-institute

ลัดดา โกรส. 2010. “แนวคิดเกี่ยวกับการจัดการเทคโนโลยีสารสนเทศ”. สืบค้น เมื่อวันที่ 11 มีนาคม 2010, จาก http://www.mua.go.th

วศิน อินทสระ. 2562. “ความหมายของคุณธรรมจริยธรรม” สืบค้น เมื่อวันที่ 31 มีนาคม 2562, จาก http://first66bobo.blogspot.com.

วิกิซอร์ซ, 2562 “แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม” สืบค้น เมื่อวันที่ 26 มีนาคม 2562, จาก https://th.wikisource.org/wiki

วีพี (WP).2562, สถิติผู้ใช้ดิจิทัลทั่วโลก “ไทย” เสพติดเน็ตมากสุดในโลก-“กรุงเทพ” เมืองผู้ใช้ Facebook สูงสุด, สืบค้น เมื่อวันที่ 20 มกราคม 2562, จาก www.brandbuffet.in.th

ศักดิ์ เสกขุนทด. 2560. “งานวิจัยด้านธุรกรรมอิเล็กทนอนิกส์” เอกสารประกอบการบรรยาย

บัณฑิตวิทยาลัย คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม. (มีนาคม 2560): 7.

ศุกรีย์ ศรีสารคาม. 2557. “ปัจจัยที่มีผลต่อคุณธรรม จริยธรรมในการใช้อินเทอร์เน็ต”. สืบค้น เมื่อวันที่ 21 มกราคม 2561, จาก www.repository.rmutt.ac.th/bitstream/.../RMUTT-106601.pdf?

สมชาย กรุสวนสมบัติ (ซูม). 2560. “ประเทศไทย 4.0 คืออะไร? จะไปสู่ฝันได้จริงหรือไม่?” สืบค้นเมื่อวันที่ 1 กรกฎาคม 2560, จาก https://www.thairath.co.th/content/617496

สาวตรี สุขศรี และคณะ. 2555. “ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น” โรงพิมพ์ภาพพิมพ์, 2555: 261-262.

แสง จันทร์งาม. 2562 “ความหมายของจริยธรรม”. สืบค้น เมื่อวันที่ 31 มีนาคม 2562, จาก www.baanjomyut.com

สุพล พรหมมาพันธุ์. 2555. “กลยุทธ์การใช้เทคโนโลยีสารสนเทศและการสื่อสาร สำหรับการแข่งขันของมหาวิทยาลัยเอกชน” การประชุมวิชาการระดับชาติ ประจำปี 2555 สมาคมสถาบันอุดมศึกษาเอกชนแห่งประเทศไทย (APHET CONFERENCE 2012).

สุพล พรหมมาพันธุ์. 2556**.“ระบบสารสนเทศเพื่อการจัดการธุรกิจ”** พิมพ์ครั้งที่ 4 ฉบับปรับปรุงใหม่โรงพิมพ์มหาวิทยาลัยศรีปทุม.

สุพล พรหมมาพันธุ์. 2561. “กฎหมายและจริยธรรมทางด้านเทคโนโลยีสารสนเทศ” เอกสารประกอบคำสอน มหาวิทยาลัยศรีปทุม.

สุพิชญา อาชวิรดา. 2559. “ปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร”, **วารสารระบบสารสนเทศด้านธุรกิจ** (JISB) ปีที่ 2 ฉบับที่ 2 : 78. สืบค้นเมื่อ 21 มกราคม 2562, จาก www.jisb.tbs.tu.ac.th/wp-content/uploads/2018/02/Jisb2559Vol2No2_5Supitchaya.pdf

โสคราติส. 2560. “แนวคิด หลักการ ทฤษฎีทางคุณธรรมจริยธรรม” สืบค้น เมื่อวันที่ 13 กรกฎาคม 2560,จาก http://www.baanjomyut.com/library

อมรรัตน์ วงศ์โสภา. 2561. “พฤติกรรมการใช้และผลกระทบของสื่อสังคมออนไลน์ประเภทเฟซบุ๊คต่อการดำเนินชีวิตของนักศึกษา กรณีศึกษามหาวิทยาลัยราชภัฏเลย” (ออนไลน์). เข้าถึงเมื่อ 15 มกราคม 2561, จาก https://www.tci-thaijo.org/index.php/researchjournal-lru

อริสโตเติล. 2560.“แนวคิด หลักการ ทฤษฎีทางคุณธรรมจริยธรรม” สืบค้น เมื่อวันที่ 13 กรกฎาคม 2560,จาก http://www.baanjomyut.com/library

อุทัย เอกสะพัง. 2562. “เปรียบเทียบการวิจัยเชิงคุณภาพและเชิงปริมาณ” สืบค้น เมื่อวันที่ 10 กุมภาพันธ์ 2562, จาก https://www.gotoknow.org/posts/491814

ไอซีที. 2561, “เปิดวิจัย Cyberbullying เยาวชนไทยกับความเสี่ยงยุค 4.0” **หนังสือพิมพ์ประชาชาติธุรกิจ** ฉบับวันจันทร์ที่ 23 – วันพุธที่ 25 เมษายน 2561: 21.

Best and Kahn. 2561. “”What is research?” Retrieved January 15, 2018, From https://www.gotoknow.org/posts/625137

Dag Elgesem. 2017 “What is special about the ethical issues in online research?” Retrieved July 2, 2017, From https://link.springer.com/article/10.1023%2FA%3A1021320510186?LI=true

Elizabeth A. Buchahan and Erin E. Hvizdak. 2017. “Online Survey Tools: Ethical and Methodological Concerns of Human Research Ethics Committees” Journal of Empirical Research on Human Research Ethics. Retrieved July 2, 2017, from http://journals.sagepub.com/doi/abs/10.1525/jer.2009.4.2.37

Gary B. Shelly. 2006. “Discovering Computers 2006: A Gateway to Information, Web Enhanced Introductory” Thomson Course Technology, 2006.

George W. Reynolds. 2012. “Ethics in Information Technology” 4th Edition, CENGAGE Learning. 2012: 22-23.

Jame A. O’Brien. 2008. “Management Information Systems” Eighth Edition, McGraw-Hill Irwin, 2008.

Narongyod Mahittivanicha. 2019, DIGITAL MARKETING CONSULTANCY. Retrieved January 20, 2019, from www.twfdigital.com.

Thanakrit k. 2019. “Quantitative Research and Qualitative Research”.Retrieved February 10, 2019, from https://rewsung.wordpress.com/tag

ภาคผนวก

ภาคผนวก ก
แบบสอบถามเพื่อการวิจัย
แบบสอบถามวิจัย

เรื่อง "ปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: กรณีศึกษา สถาบันอุดมศึกษาในเขตกรุงเทพมหานคร และปริมณฑล"

คำชี้แจง

แบบสอบถามนี้ สร้างขึ้น เพื่อเป็นเครื่องมือในการดำเนินการวิจัยเรื่อง **"ปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: กรณีศึกษา สถาบันอุดมศึกษาในเขตกรุงเทพมหานคร และปริมณฑล"** ซึ่งผลการศึกษาจะเป็นประโยชน์ต่อการนำไปปรับปรุงเกี่ยวกับการละเมิดจริยธรรมและความมั่นคงปลอดภัยของเทคโนโลยีสารเทศ อันจะเป็นประโยชน์ต่อบุคลากร นักศึกษา พนักงานของสถาบันอุดมศึกษา และประชาชนทั่วไปต่อไป

ผู้วิจัย จึงขอความร่วมมือจากท่าน ช่วยกรุณาเสียสละเวลาตอบแบบสอบถามด้วยตัวเองให้ตรงกับความเป็นจริงตามความคิดเห็นของท่านมากที่สุด ข้อมูลที่ได้รับจะนำมาใช้เพื่อเป็นประโยชน์ทางวิชาการเท่านั้น และจะไม่มีผลกระทบต่อตัวท่านแต่ประการใด ซึ่งการวิจัยครั้งนี้แบ่งแบบสอบถามออกเป็น 4 ตอน คือ

ตอนที่ 1 ข้อมูลเกี่ยวกับสภาพทั่วไปของผู้บริหาร คณาจารย์ บุคลากร พนักงาน และนักศึกษา

ตอนที่ 2 ปัจจัยที่มีผลกระทบด้านความรู้ทางเทคโนโลยีสารสนเทศ, พระราชบัญญัติ (พ.ร.บ.) ต่างๆ, ด้านสังคม, ด้านเศรษฐกิจ, ด้านพฤติกรรมการใช้คอมพิวเตอร์ และสื่อสังคมออนไลน์

ตอนที่ 3 ปัจจัยที่มีผลกระทบด้านจริยธรรม และความมั่นคงปลอดภัย

ตอนที่ 4 ความคิดเห็นและข้อเสนอแนะเกี่ยวกับปัจจัยที่มีผลกระทบต่อจริยธรรมและความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: กรณีศึกษา สถาบันอุดมศึกษาในเขตกรุงเทพมหานครและปริมณฑล

ตอนที่ 1 ข้อมูลเกี่ยวกับสถานภาพทั่วไปของผู้บริหาร คณาจารย์ บุคลากร พนักงาน และนักศึกษา

คำชี้แจง กรุณาขีดเครื่องหมาย ✓ ลงใช้ช่อง ○ หน้าข้อความตามความคิดเห็นของท่านที่ตรงกับความจริง

เพศ

ชาย ○ ไม่ต้องการระบุเพศ

หญิง

อายุ

○ ต่ำกว่า 20 ปี ○ อายุ 20 - 25 ปี ○ อายุ 26 -30 ปี

○ อายุ 31 -35 ปี ○ อายุ 36 – 40 ปี ○ อายุมากกว่า 40 ปี

ระดับการศึกษาสูงสุด

○ ต่ำกว่าปริญญาตรี ○ ปริญญาตรี ○ ปริญญาโท

○ ปริญญาเอก

ประสบการณ์ในการใช้เทคโนโลยีสารสนเทศ

○ มากที่สุด ○ มาก ○ ปานกลาง

○ น้อย ○ น้อยมาก

<u>ตอนที่ 2</u> ปัจจัยที่มีผลกระทบด้านความรู้ทางเทคโนโลยีสารสนเทศ, พระราชบัญญัติ (พ.ร.บ.) ต่างๆ, ด้านสังคม, ด้านเศรษฐกิจ, ด้านพฤติกรรมการใช้คอมพิวเตอร์ และสื่อสังคมออนไลน์

<u>คำชี้แจง</u> กรุณาขีดเครื่องหมาย ✓ ลงในช่องแสดงความคิดเห็นความรู้ความเข้าใจ และพฤติกรรมให้ตรงกับความคิดเห็น

ของท่านให้มากที่สุด ตามระดับความคิดเห็น จัดเป็น 5 ระดับ ดังนี้

1 หมายถึง เห็นด้วย/ความรู้ความเข้าใจ/มีพฤติกรรมเป็นจริง น้อยที่สุด

2 หมายถึง เห็นด้วย/ความรู้ความเข้าใจ/มีพฤติกรรมเป็นจริง น้อย

3 หมายถึง เห็นด้วย/ความรู้ความเข้าใจ/มีพฤติกรรมเป็นจริง ปานกลาง

4 หมายถึง เห็นด้วย/ความรู้ความเข้าใจ/มีพฤติกรรมเป็นจริง มาก

5 หมายถึง เห็นด้วย/ความรู้ความเข้าใจ/มีพฤติกรรมเป็นจริง มากที่สุด

ราบละเอียด	**ระดับความรู้ความเข้าใจ**				
	มากที่สุด 5	**มาก 4**	**ปานกลาง 3**	**น้อย 2**	**น้อยที่สุด 1**
1. การมีความรู้ความเข้าใจเรื่องเทคโนโลยีสารสนเทศ					
1) ความรู้เรื่องเทคโนโลยีสารสนเทศ และคอมพิวเตอร์ของบุคลากรในองค์กร					
2) ความรู้เรื่องอุปกรณ์ฮาร์ดแวร์ เช่น หน่วยประมวลผลกลาง (CPU), หน่วยบันทึกข้อมูล ได้แก่ ฮาร์ดดิสก์					
3) ความรู้เรื่องซอฟต์แวร์ เช่น Windows, MS-Office					
4) ความรู้เรื่องเครือข่ายคอมพิวเตอร์ เช่น เครือข่ายท้องถิ่น หรือแลนด์ (LAN), ไวไฟ (WiFi)					
5) ความรู้เรื่องข้อมูล เช่น การจัดการข้อมูล และฐานข้อมูล (Database)					
6) ความรู้เรื่องของอินเทอร์เน็ต เช่น การสื่อสารผ่านเว็บไซต์, อีเมล, การสนทนา, การประชุมผ่านจอภาพวิดีโอ					

7) ความรู้เรื่องเว็บเครือข่ายสังคมออนไลน์ เช่น Facebook, Line, Twitter, YouTube, Instagram					
8) ความรู้เรื่องการจัดเก็บข้อมูล เช่น การสร้างโฟลเดอร์ (Folder), การจัดการแฟ้มข้อมูล (File), การสำรองข้อมูล (Backup)					
9) ความรู้เรื่องการพัฒนาระบบ เช่น ระบบการลงทะเบียนเรียน และแอพพลิเคชัน เช่น แอพลิเคชัน Line, แอพลิอเคชันเรียกแท็กซี่ Grab Taxi					
10) ความรู้เรื่องการประยุกต์ใช้คอมพิวเตอร์ในธุรกิจ เช่น การใช้ช่องทางออนไลน์ในการขายสินค้า, การจองห้องพักโรงแรม, การจองตั๋วเครื่องบินออนไลน์					

รายละเอียด	**ระดับความรู้ความเข้าใจ**				
	มากที่สุด 5	**มาก 4**	**ปานกลาง 3**	**น้อย 2**	**น้อยที่สุด 1**
2. การมีความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติ (พ.ร.บ.) ต่างๆ ท่านมีความรู้ความเข้าใจเกี่ยวกับ พ.ร.บ. ต่อไปนี้					
11). พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ.2550					
12). พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ.2550 แก้ไขเพิ่มเติม ปี พ.ศ.2560					
13). พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ ปี พ.ศ.2544					
14) พระราชบัญญัติ การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ปี พ.ศ.2560					
15). พระราชบัญญัติลิขสิทธิ์ ปี พ.ศ.2537					
16) พระราชบัญญัติให้ใช้ประมวลกฎหมายอาญา พ.ศ.2499					
17) พระราชบัญญัติลิทธิบัตร ปี พ.ศ.2522 แก้ไขเพิ่มเติม พ.ศ. 2542					
18) พระราชบัญญัติเครื่องหมายการค้า ปี พ.ศ.2534 แก้ไขเพิ่มเติม พ.ศ.2543					
19) พระราชบัญญัติการพนัน ปี พ.ศ.2478					
20) พระราชบัญญัติการคุ้มครองเด็ก ปี พ.ศ.2546					

รายละเอียด	ระดับความรู้ความคิดเห็น				
	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1
3. ด้านสังคม					
21) เกิดกลุ่มความสัมพันธ์ทางออนไลน์ เช่น ครอบครัว เพื่อน คนรู้จัก ตลอดจนอาจารย์ เพื่อนร่วมห้องเรียน					
22) เกิดการพบปะสนทนาออนไลน์ การใช้โทรศัพท์ผ่าน อินเทอร์เน็ต และ Facebook, Line, Instagram มากขึ้น					
23) รูปแบบการเรียนรู้เปลี่ยนแปลงไป การเรียนในห้องเรียนลดลง การเรียนทางออนไลน์เพิ่มมากขึ้น					
24) เกิดแอพลิเคชันใหม่เพิ่มมากขึ้น เช่น แอพลิเคชันเรียก รถแท็กซี่ (Grab Taxi), แอพลิเคชันเคลมประกัน (Claim Di)					
25) ด้านบันเทิงคนดูภาพยนตร์และโทรทัศน์ลดลง เพราะหันมาดูทางออนไลน์มากขึ้น เช่น YouTube					
26) สื่อสังคมออนไลน์มีผลกระทบต่อสังคมในด้านดี เช่น ทำให้การติดต่อสื่อสารสะดวกสบาย เป็นช่องทางการสร้างรายได้ และมีคุณภาพชีวิตดีขึ้น					
27) สื่อสังคมออนไลน์มีผลกระทบต่อสังคมในด้านลบ เช่น มีการหลอกลวง การปลอมเฟซบุ๊ค การละเมิดความเป็นส่วนตัว การโพสต์ภาพลามกอนาจาร การค้ายาเสพติด ตลอดจนการเล่นพนันออนไลน์					
28). สื่อสังคมออนไลน์มีผลกระทบต่อสังคมในด้านบวก เช่น ช่วยลดความเหลื่อมล้ำทางสังคม โน้ตบุ๊คคอมพิวเตอร์ และสมาร์ทโฟนมีราคาถูกลง					
29) สื่อสังคมออนไลน์มีผลกระทบต่อสังคมในด้านลบ เช่น การส่งไวรัส และสแปมลิงก์มัลแวร์					

รายละเอียด	ระดับความรู้ความเข้าใจ				
	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1
4. ด้านเศรษฐกิจ					
30) การจ้างงานของภาคธุรกิจบางกลุ่มลดลง เช่น ธนาคาร ห้างสรรพสินค้า ร้านจำหน่ายสินค้า					
31) เกิดธุรกิจประเภทตัวแทนทางด้านการเงินในการจัดซื้อสินค้าทางออนไลน์					
32) เกิดธุรกิจบริการใหม่ๆ เช่น การรับส่งสินค้าพัสดุแบบรีบด่วน เช่น Kerry					

Express ฯลฯ					
33) การจ้างงานภาคบริการลดลง เพราะเกิดนวัตกรรมใหม่ๆ ขึ้นมาแทนที่ เช่น Fintech					
34) ระบบการค้าการลงทุนเปลี่ยนไป มีความสะดวกรวดเร็ว สามารถลงทุนได้ตลอด 24 ชั่วโมง					
35) ระบบการเงินสำหรับซื้อขายแลกเปลี่ยนมีการเปลี่ยนแปลงไป เกิดสกุลเงินใหม่ๆ เช่น Bitcoin					
36) มีการลดขั้นตอนแรงงานการผลิตในภาคการผลิตด้วยการใช้ระบบอัตโนมัติ และการใช้หุ่นยนต์					
37) เทคโนโลยีสารสนเทศและการสื่อสาร เป็นตัวผลักดันที่ก่อให้เกิดการขยายตัวทางเศรษฐกิจ และมีการแข่งขันกันรุนแรงมากขึ้น เช่น ระบบพาณิชย์อิเล็กทรอนิกส์ (e-Commerce)					

รายละเอียด	**ระดับพฤติกรรม**				
	มากที่สุด 5	**มาก 4**	**ปานกลาง 3**	**น้อย 2**	**น้อยที่สุด 1**
5. ด้านพฤติกรรมการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์					
38) พฤติกรรมการเรียนรู้ของเยาวชนเปลี่ยนแปลงไป โดยหันมาศึกษาเรียนรู้จากอินเทอร์เน็ตและสื่อสังคมออนไลน์ เช่น Google Facebook Line YouTube เป็นเวลานานมากขึ้น					
39) พฤติกรรมการซื้อขายสินค้าเปลี่ยนไป โดยผู้ซื้อ และผู้ขาย หันมาใช้บริการทางออนไลน์มากขึ้น					
40) การทำธุรกรรมทางการเงินระหว่างผู้ซื้อและผู้ขายเปลี่ยนไป โดยหันมาใช้ระบบการบริการโอนเงิน และรับเงินทางออนไลน์กันมากขึ้น เช่น การชำระเงินด้วยพร้อมเพย์ (Prompt Pay) และคิวอาร์โค้ต (Quick Response Code)					
41) พฤติกรรมการแสดงออกให้เป็นที่ยอมรับของสังคมเปลี่ยนไป โดยมีการหันมาใช้การกดไลค์ การแชร์ และการโหวตทางออนไลน์มากขึ้น					
42) พฤติกรรมทางสังคมเปลี่ยนจากการพูดคุยแบบเผชิญหน้าลดน้อยลง และหันมาใช้การสื่อสารบนแอพพลิเคชันบนสมาร์ทโฟน และการสื่อสารทางออนไลน์มากขึ้น เช่น Facebook, Line					
43) พฤติกรรมการสื่อสารทางด้านภาษาพูดเปลี่ยนไป มีการใช้ภาษาใหม่ๆ เกิดขึ้น และมีการสนทนาแบบมองเห็นหน้ากัน (Face to Face) รวมถึงอวัจนะภาษา หรือ ภาษากาย					

44) พฤติกรรมด้านบันเทิงเปลี่ยนไป คนดูภาพยนตร์ในโรงหนังลดลง โดยหันมาดูภาพยนตร์ และวิดีโอทางออนไลน์มาก และนานขึ้น เช่น YouTube, Netflix					
45) เกิดพฤติกรรมการใช้เทคโนโลยีอินเทอร์เน็ต และสื่อสังคมออนไลน์ทั้งในเวลาการทำงาน-ในช่วงเวลาเรียน และในช่วงเวลาอื่นๆ เช่น Facebook Line และ YouTube เป็นเวลานานมากขึ้น					
46) เกิดพฤติกรรมหลงไหลการติดเกม และการพนันออนไลน์เพิ่มมากขึ้น					
47) เกิดพฤติกรรมการเลียนแบบการแสดงออกและกิจกรรมของดารา หรือบุคคลที่ตนเองชื่นชอบ และอยากทำตาม ที่เรียกว่า เน็ตไอดอล (Net Idol)					
48) เกิดพฤติกรรมการโฆษณาสินค้าทางออนไลน์เพิ่มมากขึ้น เช่น บน Google Facebook Line เนื่องจากมีค่าใช้จ่ายที่ถูกกว่าการโฆษณาบนสื่อกระแสหลักอย่างหนังสือพิมพ์ และวิทยุ โทรทัศน์					

ตอนที่ 3 ปัจจัยที่มีผลกระทบด้านจริยธรรม และความมั่นคงปลอดภัย

รายละเอียด	**ระดับความคิดเห็น**				
	มากที่สุด 5	**มาก 4**	**ปานกลาง 3**	**น้อย 2**	**น้อยที่สุด 1**
6. ด้านจริยธรรม					
49) มีปัญหาเรื่องการโกหกหลอกลวงทางอินเทอร์เน็ต และทางสื่อสังคมออนไลน์เพิ่มมากขึ้น					
50) ความมีวินัยเรียนรู้ในการทำงานลดลง					
51) การเข้าถึงภาพลามกอนาจาร ความรุนแรง และความน่ากลัวมีมากเพิ่มขึ้น					
52) มีการก่อปัญหาอาชญากรรมคอมพิวเตอร์ เช่น การขโมยข้อมูล และการปล่อยไวรัส การโจมตีประเภทต่างๆ					
53) มีการแสดงการทำลามกอนาจารออนไลน์เพิ่มมากขึ้น					
54) มีการละเมิดลิขสิทธิ์ภาพ ข้อมูล และซอฟต์แวร์ ด้วยความรู้เท่าไม่ถึงการณ์มากขึ้น					
55) มีการละเมิดความเป็นส่วนตัวเพิ่มมากขึ้น					
56) มีการส่งอีเมลโฆษณาที่ไม่ได้รับเชิญ (Spamming) จำนวนมากทั้งทางอีเมล และทางสื่อสังคมออนไลน์					
รายละเอียด	**ระดับความคิดเห็น**				
	มากที่สุด 5	**มาก 4**	**ปานกลาง 3**	**น้อย 2**	**น้อยที่สุด 1**
7. ด้านความมั่นคงปลอดภัย					
57) รัฐ และองค์กร ต้องเพิ่มความเข้มงวดด้านนโยบาย ด้านความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศให้สูงขึ้น					
58) รัฐ และองค์กรต้องเพิ่มงบประมาณด้านความปลอดภัยมากขึ้น เช่น การติดตั้ง					

โปรแกรมไฟร์วอลล์ และโปรแกรมการตรวจสอบ และป้องกันไวรัสคอมพิวเตอร์					
59) รัฐ และองค์กรต้องจ้างบุคลการด้านไอทีเพิ่มขึ้น					
60) เกิดอาชญากรรมทางด้านการเงินและธนาคารสูงขึ้น					
61) เกิดปัญหาทางด้านอาชญากรรมไซเบอร์ เช่น การเจาะระบบ ขโมยข้อมูล และทำลายข้อมูล					
62) มีการซื้อขายสินค้าและการดาวน์โหลดซอฟต์แวร์ที่มีลิขสิทธิ์					
63) มีการข่มขู่ กรรโชก ทางอีเมล์ และสื่อสังคมมออนไลน์					
64) มีการนำความลับส่วนบุคคลและองค์กรไปเปิดเผยในทางที่ไม่เหมาะสม					
65) อินเทอร์เน็ตและสื่อสังคมออนไลน์ เป็นแหล่งการก่ออาชญากรรมทางคอมพิวเตอร์ เพราะสามาถใช้ได้ทุกที่ทุกเวลา					
66) มีการแก้ไขกฎหมาย และเพิ่มโทษมากขึ้น เช่น พ.ร.บคอมพิวเตอร์ ปี 2550 แก้ไขเพิ่มเติม พ.ศ.2560					
67) มีการโจมตีด้วยไวรัสประเภทต่างๆ เพื่อให้ได้รหัสผ่าน แลการโจรกรรมข้อมูล					

ตอนที่ 4 ความคิดเห็น และข้อเสนอแนะเกี่ยวกับปัจจัยที่มีผลกระทบต่อการละเมิดจริยธรรม และความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ

.....

.....

.....

.....

.....

.....

.....

.....

✪✪✪ ขอขอบคุณในความร่วมมือตอบแบบสอบถาม ✪✪✪

ภาคผนวก ข

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2)

พ.ศ.2560

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒)

พ.ศ. ๒๕๖๐

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร

ให้ไว้ ณ วันที่ ๒๓ มกราคม พ.ศ. ๒๕๖๐

เป็นปีที่ ๒ ในรัชกาลปัจจุบัน

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร มีพระราชโองการโปรดเกล้าฯ ให้ประกาศว่าโดยที่เป็นการสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้ยกเลิกความในมาตรา ๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจแต่งตั้งพนักงานเจ้าหน้าที่กับออกกฎกระทรวงและประกาศเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงและประกาศนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้”

มาตรา ๔ ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา ๑๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ต้องระวางโทษปรับไม่เกินสองแสนบาท

ให้รัฐมนตรีออกประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับและลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย"

มาตรา ๕ ให้ยกเลิกความในมาตรา ๑๒ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท"

มาตรา ๖ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๒/๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"มาตรา ๑๒/๑ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นเหตุให้เกิดอันตรายแก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท"

มาตรา ๗ ให้เพิ่มความต่อไปนี้เป็นวรรคสอง วรรคสาม วรรคสี่ และวรรคห้าของมาตรา ๑๓ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย ก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นนั้นด้วย

ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคหนึ่งหรือวรรคสองและตามวรรคสามหรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทงเดียว”

มาตรา ๘ ให้ยกเลิกความในมาตรา ๑๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑)(๒) (๓) หรือ (๔)

ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้”

มาตรา ๙ ให้ยกเลิกความในมาตรา ๑๕ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๑๕ ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์
ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้องรับโทษ”

มาตรา ๑๐ ให้ยกเลิกความในมาตรา ๑๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดามารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอายผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิดความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรสหรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย”

มาตรา ๑๑ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๖/๑ และมาตรา ๑๖/๒ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“มาตรา ๑๖/๑ ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่าจำเลยมีความผิด ศาลอาจสั่ง

(๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว

(๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ วิทยุกระจายเสียงวิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณาหรือเผยแพร่

(๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น

มาตรา ๑๖/๒ ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา ๑๖/๑ ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา ๑๔ หรือมาตรา ๑๖ แล้วแต่กรณี”

มาตรา ๑๒ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๗/๑ ในหมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“มาตรา ๑๗/๑ ความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๑๑ มาตรา ๑๓ วรรคหนึ่งมาตรา ๑๖/๒ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๗ ให้คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งมีอำนาจเปรียบเทียบได้

คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งตามวรรคหนึ่งให้มีจำนวนสามคนซึ่งคนหนึ่งต้องเป็นพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา

เมื่อคณะกรรมการเปรียบเทียบได้ทำการเปรียบเทียบกรณีใดและผู้ต้องหาได้ชำระเงินค่าปรับตามคำเปรียบเทียบภายในระยะเวลาที่คณะกรรมการเปรียบเทียบกำหนดแล้ว ให้ถือว่าคดีนั้นเป็นอันเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา

ในกรณีที่ผู้ต้องหาไม่ชำระเงินค่าปรับภายในระยะเวลาที่กำหนด ให้เริ่มนับอายุความในการฟ้องคดีใหม่นับตั้งแต่วันที่ครบกำหนดระยะเวลาดังกล่าว”

มาตรา ๑๓ ให้ยกเลิกความในมาตรา ๑๘ และมาตรา ๑๙ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอตามวรรคสองให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

เพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิดหรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น พนักงานสอบสวนอาจร้องขอให้พนักงานเจ้าหน้าที่ตามวรรคหนึ่งดำเนินการตามวรรคหนึ่งก็ได้ หรือหากปรากฏข้อเท็จจริงดังกล่าวต่อพนักงานเจ้าหน้าที่เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่รีบรวบรวมข้อเท็จจริงและหลักฐานแล้วแจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการต่อไป

ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (๑) (๒) และ (๓) ดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเจ็ดวันนับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงาน

เจ้าหน้าที่กำหนดซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาตจากพนักงานเจ้าหน้าที่ ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดระยะเวลาที่ต้องดำเนินการที่เหมาะสมกับประเภทของผู้ให้บริการก็ได้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘)ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๘ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้วพนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง”

มาตรา ๑๔ ให้ยกเลิกความในมาตรา ๒๐ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๒๐ ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ ดังต่อไปนี้ พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้

(๑) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามพระราชบัญญัตินี้

(๒) ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาค ๒ ลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา

(๓) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญาหรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนและเจ้าหน้าที่ตามกฎหมายนั้นหรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาได้ร้องขอ

ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน รัฐมนตรีโดยความเห็นชอบของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์จะมอบหมายให้พนักงานเจ้าหน้าที่ยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบซึ่งข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้ ทั้งนี้ ให้นำบทบัญญัติว่าด้วยคณะกรรมการที่มีอำนาจดำเนินการพิจารณาทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับกับการประชุมของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์โดยอนุโลม

ให้รัฐมนตรีแต่งตั้งคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ตามวรรคสองขึ้นคณะหนึ่งหรือหลายคณะ แต่ละคณะให้มีกรรมการจำนวนเก้าคนซึ่งสามในเก้าคนต้องมาจากผู้แทนภาคเอกชนด้านสิทธิมนุษยชน ด้านสื่อสารมวลชน ด้านเทคโนโลยีสารสนเทศ หรือด้านอื่นที่เกี่ยวข้อง และให้กรรมการได้รับค่าตอบแทนตามหลักเกณฑ์ที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

การดำเนินการของศาลตามวรรคหนึ่งและวรรคสอง ให้นำประมวลกฎหมายวิธีพิจารณาความอาญามาใช้บังคับโดยอนุโลม ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ตามวรรคหนึ่งหรือวรรคสอง พนักงานเจ้าหน้าที่จะทำการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นเองหรือจะสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นก็ได้ ทั้งนี้ ให้รัฐมนตรีประกาศกำหนดหลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ของพนักงานเจ้าหน้าที่หรือผู้ให้บริการให้เป็นไปในแนวทางเดียวกันโดยคำนึงถึงพัฒนาการทางเทคโนโลยีที่เปลี่ยนแปลงไป เว้นแต่ศาลจะมีคำสั่งเป็นอย่างอื่น

ในกรณีที่มีเหตุจำเป็นเร่งด่วน พนักงานเจ้าหน้าที่จะยื่นคำร้องตามวรรคหนึ่งไปก่อนที่จะได้รับความเห็นชอบจากรัฐมนตรี หรือพนักงานเจ้าหน้าที่โดยความเห็นชอบของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์จะยื่นคำร้องตามวรรคสองไปก่อนที่รัฐมนตรีจะมอบหมายก็ได้ แต่ทั้งนี้ต้องรายงานให้รัฐมนตรีทราบโดยเร็ว”

มาตรา ๑๕ ให้ยกเลิกความในวรรคสองของมาตรา ๒๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่ง หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง เว้นแต่เป็นชุดคำสั่งไม่พึงประสงค์ที่อาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ทั้งนี้รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดรายชื่อ ลักษณะ หรือรายละเอียดของชุดคำสั่งไม่พึงประสงค์ซึ่งอาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งไม่พึงประสงค์ก็ได้”

มาตรา ๑๖ ให้ยกเลิกความในมาตรา ๒๒ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๕ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่และพนักงานสอบสวนในกรณีตามมาตรา ๑๘ วรรคสองเปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นในกรณีตามมาตรา ๑๘ วรรคสองหรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบหรือกับพนักงานสอบสวนในส่วนที่เกี่ยวกับการปฏิบัติหน้าที่ตามมาตรา ๑๘ วรรคสอง โดยมิชอบหรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนในกรณีตามมาตรา ๑๘ วรรคสอง ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้หรือที่พนักงานสอบสวนได้มาตามมาตรา ๑๘ วรรคสอง ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วย

การสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น”

มาตรา ๑๗ ให้ยกเลิกความในวรรคหนึ่งของมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้”

มาตรา ๑๘ ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา ๒๘ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“ผู้ที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ อาจได้รับค่าตอบแทนพิเศษตามที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

ในการกำหนดให้ได้รับค่าตอบแทนพิเศษต้องคำนึงถึงภาระหน้าที่ ความรู้ความเชี่ยวชาญ ความขาดแคลนในการหาผู้มาปฏิบัติหน้าที่หรือมีการสูญเสียผู้ปฏิบัติงานออกจากระบบราชการเป็นจำนวนมากคุณภาพของงาน และการดำรงตนอยู่ในความยุติธรรมโดยเปรียบเทียบค่าตอบแทนของผู้ปฏิบัติงานอื่นในกระบวนการยุติธรรมด้วย”

มาตรา ๑๙ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๓๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“มาตรา ๓๑ ค่าใช้จ่ายในเรื่องดังต่อไปนี้ รวมทั้งวิธีการเบิกจ่ายให้เป็นไปตามระเบียบที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

(๑) การสืบสวน การแสวงหาข้อมูล และรวบรวมพยานหลักฐานในคดีความผิดตามพระราชบัญญัตินี้

(๒) การดำเนินการตามมาตรา ๑๘ วรรคหนึ่ง (๔) (๕) (๖) (๗) และ (๘) และมาตรา ๒๐

(๓) การดำเนินการอื่นใดอันจำเป็นแก่การป้องกันและปราบปรามการกระทำความผิดตามพระราชบัญญัตินี้”

มาตรา ๒๐ บรรดาระเบียบหรือประกาศที่ออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ที่ใช้บังคับอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ยังคงใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติแห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ จนกว่าจะมีระเบียบหรือประกาศที่ต้องออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ ใช้บังคับ

การดำเนินการออกระเบียบหรือประกาศตามวรรคหนึ่ง ให้ดำเนินการให้แล้วเสร็จภายในหกสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

มาตรา ๒๑ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้

ผู้รับสนองพระราชโองการ
พลเอก ประยุทธ์ จันทร์โอชา
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งมีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้นตามพัฒนาการทางเทคโนโลยีซึ่งเปลี่ยนแปลงอย่างรวดเร็วและโดยที่มีการจัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมซึ่งมีภารกิจในการกำหนดมาตรฐานและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของประเทศสมควรปรับปรุงบทบัญญัติในส่วนที่เกี่ยวกับผู้รักษาการตามกฎหมาย กำหนดฐานความผิดขึ้นใหม่ และแก้ไขเพิ่มเติมฐานความผิดเดิม รวมทั้งบทกำหนดโทษของความผิดดังกล่าว การปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ ตลอดจนกำหนดให้มีคณะกรรมการเปรียบเทียบซึ่งมีอำนาจเปรียบเทียบความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และแก้ไขเพิ่มเติมอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้เหมาะสมยิ่งขึ้น จึงจำเป็นต้องตราพระราชบัญญัตินี้__

ประวัติย่อผู้วิจัย

ชื่อ นายสุพล พรหมมาพันธุ์

วัน เดือน ปี เกิด วันที่ 6 พฤศจิกายน พ.ศ. 2505

สถานที่เกิด อำเภอเมือง จังหวัดเพชรบูรณ์

สถานที่อยู่ปัจจุบัน บ้านเลขที่ 36/3 หมู่ 3 หมู่บ้านวิมานแก้ววิว ตำบลบึงคำพร้อย อำเภอลำลูกกา จังหวัดปทุมธานี 12130

ตำแหน่งหน้าที่การงานปัจจุบัน อาจารย์ประจำ

สถานที่ทำงานปัจจุบัน สาขาวิชาคอมพิวเตอร์ธุรกิจ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

ประวัติการศึกษา

พ.ศ. 2530 ศน.บ. ปรัชญา จากมหาวิทยาลัยมหามกุฏราชวิทยาลัย กรุงเทพฯ

พ.ศ. 2535 M.S. Information Systems (IS), Strayer University Washington D.C. (U.S.A.)