แผนบริหารการสอนประจำบทที่ 6

วัตถุประสงค์เชิงพฤติกรรม

1. อธิบายจริยธรรมในการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศได้
2. อธิบายอาชญากรรมทางคอมพิวเตอร์ได้
3. อธิบายวิธีการป้องกันการเข้าถึงข้อมูลและคอมพิวเตอร์ได้
4. อธิบายความสำคัญของกฎหมายที่เกี่ยวข้องกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศได้

เนื้อหา

1. จริยธรรมทางคอมพิวเตอร์
2. อาชญากรรมทางคอมพิวเตอร์
3. วิธีการป้องกันการเข้าถึงข้อมูลและคอมพิวเตอร์
4. ข้อควรระวังในการเข้าไปยังโลกไซเบอร์หรือใช้งานอินเทอร์เน็ต
5. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
6. บทสรุป
7. แบบฝึกหัดท้ายบท

วิธีสอนและกิจกรรมการเรียนการสอนประจำบท

1. ศึกษาเอกสารประกอบการสอน
2. บรรยาย
3. แบ่งกลุ่มค้นคว้าและแสดงความคิดเห็น
4. นักศึกษาทำแบบฝึกหัดท้ายบท
5. ประเมินผลและเฉลยแบบฝึกหัดท้ายบท

สื่อการเรียนการสอน

1. เอกสารประกอบการสอน
2. สไลด์ประกอบการสอน
3. อินเทอร์เน็ต
4. แบบฝึกหัดท้ายบท

การวัดผลและประเมินผล

1. การตอบคำถามของนักศึกษา
2. ผลสรุปการทำกิจกรรมกลุ่ม
3. ทดสอบจากแบบฝึกหัดท้ายบท

บทที่ 6
จริยธรรมและความปลอดภัยของสารสนเทศ

ปัจจุบันเป็นยุคการสื่อสารที่ไร้พรมแดน คอมพิวเตอร์และเทคโนโลยีสารสนเทศเข้ามามีบทบาทต่อการดำรงชีวิตประจำวันของมนุษย์เรามากยิ่งขึ้น ช่วยลดขั้นตอนการทำงาน ช่วยเพิ่มคุณภาพชีวิตให้มนุษย์มีความสะดวกสบายมากขึ้น เราสามารถใช้คอมพิวเตอร์หรือใช้โทรศัพท์มือถือ ที่เชื่อมต่อระบบอินเทอร์เน็ตทำการติดต่อสื่อสารกัน สั่งซื้อสินค้า โอนเงิน ชำระค่าสินค้าและบริการได้ง่าย สะดวกรวดเร็ว เมื่อเทียบกับอดีตที่ผ่านมา ทุกวันนี้เทคโนโลยีคอมพิวเตอร์ เทคโนโลยีการสื่อสารข้อมูลมีการพัฒนาไปอย่างรวดเร็ว คอมพิวเตอร์ประมวลผลได้รวดเร็วขึ้น จัดเก็บข้อมูลได้มากขึ้น ใช้งานได้สะดวกขึ้น มีความรวดเร็วในการสื่อสารข้อมูล ดังนั้นข้อมูลต่าง ๆ จึงถูกเก็บไว้ในเครื่องคอมพิวเตอร์ ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์แม่ข่าย ข้อมูลและสารสนเทศสามารถถูกส่งจากที่หนึ่งไปจัดเก็บไว้อีกที่หนึ่งได้ง่ายยิ่งขึ้น

แม้ว่าเทคโนโลยีคอมพิวเตอร์และการสื่อสารข้อมูลจะมีประโยชน์มากเพียงไร หากพิจารณาอีกด้านหนึ่งแล้ว คอมพิวเตอร์ก็อาจจะเป็นภัยได้เช่นกัน หากผู้ใช้ไม่ระมัดระวังหรือนำไปใช้ในทางที่ไม่ถูกต้อง เราอาจจะเห็นข่าวเกี่ยวกับการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศในการก่ออาชญากรรมหรือละเมิดสิทธิของผู้อื่นมากขึ้นเรื่อย ๆ ดังนั้นในการใช้งานคอมพิวเตอร์ร่วมกันในสังคมในแต่ละประเทศจึงได้มีการกำหนดระเบียบ กฎเกณฑ์ รวมถึงกฎหมายที่ใช้เป็นแนวทางในการปฏิบัติเพื่อให้เกิดคุณธรรมและจริยธรรมในการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศ

6.1 จริยธรรมทางคอมพิวเตอร์

จริยธรรม (Ethics) หมายถึง แนวทางประพฤติปฏิบัติของคนในสังคมหนึ่ง ๆ ซึ่งเป็นมาตรฐานของสังคมนั้น ๆ ว่าเป็นคนประพฤติดีหรือชั่ว ถูกหรือผิด ควรทำหรือไม่ควรทำ เป็นหลักเกณฑ์ที่ประชาชนตกลงร่วมกันเพื่อใช้เป็นแนวทางในการประพฤติปฏิบัติร่วมกันในสังคม

จริยธรรมทางคอมพิวเตอร์ หมายถึง แนวทางการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศอย่างมีศีลธรรม มีความรู้สึกผิดชอบชั่วดี หรือใช้งานในสิ่งที่บุคคลในสังคมยอมรับ ไม่ทำให้เกิดความวุ่นวายในสังคม

การที่จะระบุว่าการกระทำสิ่งใดผิดจริยธรรมนั้นอาจกล่าวได้ไม่ชัดเจนมากนัก ทั้งนี้ขึ้นอยู่กับวัฒนธรรมของสังคมในแต่ละประเทศนั้น ๆ ด้วย

ตัวอย่างของการกระทำที่ยอมรับกันโดยทั่วไปว่าเป็นการกระทำที่ผิดจริยธรรม ในการใช้งานคอมพิวเตอร์คือ ใช้ทำร้ายผู้อื่นให้เกิดความเสียหาย หรือก่อความรำคาญ เช่น การใช้คอมพิวเตอร์และ

เทคโนโลยีสารสนเทศในการขโมยข้อมูลของผู้อื่น การนำภาพหรือข้อมูลส่วนตัวของบุคคลไปลงบนอินเทอร์เน็ตโดยไม่ได้รับอนุญาต การเข้าถึงข้อมูลหรือคอมพิวเตอร์ของบุคคลอื่นโดยไม่ได้รับอนุญาต การละเมิดลิขสิทธิ์ซอฟต์แวร์ เป็นต้น

โดยทั่วไปเมื่อพิจารณาถึงจริยธรรมเกี่ยวกับการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศ มักจะกล่าวถึงใน 4 ประเด็นดังต่อไปนี้

6.1.1 ความเป็นส่วนตัว (Privacy)

ในปัจจุบันยุคดิจิทัลข้อมูลและสารสนเทศจำนวนมากสามารถสืบค้นได้อย่างสะดวก โดยผ่านระบบเครือข่ายอินเทอร์เน็ตมีทั้งข้อมูลที่เผยแพร่เป็นสาธารณะ ข้อมูลที่ผู้ใช้ต้องเสียค่าบริการ และด้วยความสามารถของเครือข่ายคอมพิวเตอร์ที่อำนวยความสะดวกและรวดเร็วในการเข้าถึงข้อมูลและสารสนเทศให้กับผู้ใช้ หลายคนจึงเริ่มวิตกกังวลถึงความเป็นส่วนตัวของข้อมูลที่อาจถูกจัดเก็บและเปิดเผยโดยไม่มีเหตุอันควร ตัวอย่างข้อมูลที่ได้รับผลกระทบจากความเป็นส่วนบุคคล เช่น ข้อความในอีเมลที่ถูกควบคุมและจัดการโดยผู้ให้บริการอีเมลหรือข้อมูลที่ผู้ใช้ลงทะเบียนในการเข้าเยี่ยมชมเว็บไซต์ หรือสมัครใช้บริการในเรื่องต่าง ๆ เป็นต้น

ความเป็นส่วนตัวของข้อมูลและสารสนเทศ โดยทั่วไปหมายถึงสิทธิที่จะอยู่ตามลำพังและเป็นสิทธิที่เจ้าของสามารถที่จะควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น สิทธินี้ได้ครอบคลุมทั้งปัจเจกบุคคล กลุ่มคนและองค์การต่าง ๆ

ซึ่งประเด็นเกี่ยวข้องกับความเป็นส่วนตัวที่เป็นที่น่าสังเกตดังนี้

6.1.1.1 การเข้าไปดูข้อความในอีเมลและการบันทึกข้อมูลในเครื่องคอมพิวเตอร์ รวมทั้งการบันทึกแลกเปลี่ยนข้อมูลที่บุคคลเข้าไปใช้บริการเว็บไซต์และกลุ่มข่าวสาร การใช้เทคโนโลยีในการติดตามความเคลื่อนไหวหรือพฤติกรรมของบุคคล เช่น บริษัทใช้คอมพิวเตอร์และกล้องวงจรปิดในการตรวจจับหรือเฝ้าดูการปฏิบัติงานหรือการให้บริการของพนักงาน ถึงแม้ว่าจะเป็นการติดตามการทำงานเพื่อการพัฒนาคุณภาพการให้บริการ แต่กิจกรรมหลายอย่างของพนักงานก็ถูกเฝ้าดูด้วย พนักงานสูญเสียความเป็นส่วนตัวซึ่งการกระทำเช่นนี้ถือเป็นการผิดจริยธรรม

6.1.1.2 การใช้ข้อมูลของลูกค้าจากแหล่งต่าง ๆ เพื่อประโยชน์ในการขยายตลาด

6.1.1.3 การรวบรวมหมายเลขโทรศัพท์ ที่อยู่อีเมล หมายเลขบัตรเครดิต และข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำไปสร้างฐานข้อมูลประวัติลูกค้าขึ้นมาใหม่ แล้วนำไปขายให้กับบริษัทอื่น

ดังนั้น เพื่อเป็นการป้องกันการละเมิดสิทธิความเป็นส่วนตัวของข้อมูลและสารสนเทศ ผู้ใช้บริการจึงต้องระมัดระวังการให้ข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน วันเดือนปีเกิด ข้อมูลบัตรเครดิต ที่อยู่อีเมล เบอร์โทรศัพท์ เป็นต้น

6.1.2 ความถูกต้อง (Accuracy)

ในการใช้คอมพิวเตอร์เพื่อรวบรวม จัดเก็บ และเรียกดูข้อมูล คุณลักษณะที่สำคัญประการหนึ่งคือความน่าเชื่อถือของข้อมูล ทั้งนี้ข้อมูลจะมีความน่าเชื่อถือมากน้อยเพียงใดย่อมขึ้นอยู่กับความถูกต้องในการบันทึกข้อมูล การเก็บรักษาข้อมูลด้วย ประเด็นด้านจริยธรรมที่เกี่ยวข้องกับความถูกต้องของข้อมูล โดยทั่วไปจะพิจารณาว่าใครจะเป็นผู้รับผิดชอบความถูกต้องของข้อมูลที่จัดเก็บและเผยแพร่ เช่น ในกรณีที่องค์การให้ลูกค้าลงทะเบียนด้วยตนเอง หรือกรณีของข้อมูลที่เผยแพร่ทางเว็บไซต์ จะทราบได้อย่างไรว่าข้อผิดพลาดที่เกิดขึ้นนั้นไม่ได้เกิดจากความจงใจ และผู้ใดจะเป็นผู้รับผิดชอบหากเกิดข้อผิดพลาด ดังนั้นในการจัดทำข้อมูลรวมถึงการปรับปรุงข้อมูลให้มีความทันสมัยอยู่เสมอ นอกจากนี้ควรให้สิทธิ์แก่บุคคลในการเข้าไปตรวจสอบความถูกต้องของข้อมูลของตนเองได้ เช่น ในระบบ MIS ของมหาวิทยาลัย อาจารย์ผู้สอนต้องสามารถดูคะแนน หรือเกรดของนักศึกษาในความรับผิดชอบหรือที่สอนเพื่อตรวจสอบว่าคะแนนที่ป้อนไปนั้นถูกต้อง ไม่ถูกแก้ไขเปลี่ยนแปลง เป็นต้น

6.1.3 ความเป็นเจ้าของ (Intellectual Property)

สิทธิความเป็นเจ้าของ หมายถึง กรรมสิทธิ์ในการถือครองทรัพย์สิน ซึ่งอาจเป็นทรัพย์สินทั่วไปที่จับต้องได้ เช่น คอมพิวเตอร์ โทรศัพท์มือถือ รถยนต์ หรืออาจเป็นทรัพย์สินทางปัญญา (ความคิด) ที่จับต้องไม่ได้ เช่น โปรแกรมคอมพิวเตอร์ บทเพลง แต่สามารถถ่ายทอดและบันทึกลงสื่อต่าง ๆ ได้ เช่น สื่อสิ่งพิมพ์ ซีดีรอม ดีวีดีรอม ฮาร์ดดิสก์ เป็นต้น

ทรัพย์สินทางปัญญาอาจคิด หรือสร้าง หรือผลิตขึ้นจากบุคคลหรือองค์การ ซึ่งทรัพย์สินเหล่านั้นจะได้รับการคุมครองสิทธิภายใต้กฎหมาย ได้แก่

6.1.3.1 ความลับทางการค้า (Trade secret) คือ ข้อมูลการค้าซึ่งยังไม่รู้จักกันโดยทั่วไปและมีประโยชน์ในเชิงพาณิชย์ เป็นข้อมูลต่าง ๆ ที่เกิดจากความคิดของบุคคลหรือกลุ่มบุคคลเกี่ยวกับข้อมูลการค้า สูตร โปรแกรม วิธีการเทคนิคหรือกรรมวิธีต่าง ๆ เช่น สูตรยา สูตรอาหาร สูตรเครื่องดื่ม สูตรเครื่องสำอาง กรรมวิธีการผลิต บัญชีรายชื่อลูกค้า ข้อมูลการบริหารธุรกิจ กลยุทธ์การโฆษณาสินค้า เป็นต้น ผู้ควบคุมความลับทางการค้าจะต้องมีมาตรการ ที่เหมาะสมในการเก็บความลับทางการค้า กฎหมายที่เกี่ยวข้องกับความลับทางการค้าคือ พระราชบัญญัติความลับทางการค้า พ.ศ. 2545 ซึ่งเป็นกฎหมายที่มีผลบังคับใช้เมื่อวันที่ 22 กรกฎาคม พ.ศ. 2545 โดยให้ความคุ้มครอง ข้อมูลที่เป็นความลับทางการค้าอย่างกว้างขวางและมีประสิทธิภาพ ผู้ที่เป็นเจ้าของความลับทางการค้าจะได้รับความคุ้มครองตลอดไป ตราบเท่าที่ความลับทางการค้านั้นยังคงเป็นความลับอยู่ การละเมิดสิทธิในความลับทางการค้า ได้แก่ การกระทำที่เป็นการเปิดเผย เอาไป หรือใช้ซึ่งความลับทางการค้าโดยไม่ได้รับความยินยอมจากเจ้าของความลับทางการค้านั้น ความลับทางการค้าจะได้รับความคุ้มครองโดยไม่ต้องมีการจดทะเบียนแต่อย่างใด เจ้าของความลับทางการค้าสามารถเลือกที่

จะแจ้งจอข้อมูลความลับทางการค้าได้ ศึกษาเพิ่มเติมเกี่ยวกับพระราชบัญญัติความลับทางการค้า พ.ศ. 2545 ได้ที่ http://www.ratchakitcha.soc.go.th/DATA/PDF/00054000.PDF

6.1.3.2 ลิขสิทธิ์ (Copyright) เป็นสิทธิในการกระทำใด ๆ (ตีพิมพ์ แสดงผลงาน หรือแจกจ่ายผลงาน) เกี่ยวกับงานที่สร้างสรรค์ขึ้น โดยการใช้สติปัญญาความรู้ ความสามารถ โดยไม่ลอกเลียนงานของผู้อื่น กฎหมายที่คุ้มครองลิขสิทธิ์ แบ่งงานที่สร้างสรรค์ทั้งหมด 9 ประเภท คือ

1) งานวรรณกรรม (หนังสือ จุลสาร สิ่งพิมพ์ โปรแกรมคอมพิวเตอร์ ฯลฯ)

2) งานนาฏกรรม (ท่าเต้น ท่ารำ ฯลฯ)

3) งานศิลปกรรม (จิตกรรม ประติมากรรม ภาพพิมพ์ ภาพถ่าย ศิลปประยุกต์ ฯลฯ)

4) งานดนตรีกรรม (ทำนอง ทำนองและเนื้อร้อง ฯลฯ)

5) งานสิ่งบันทึกเสียง (เทป ซีดี)

6) งานโสตทัศนวัสดุ (วีซีดี ดีวีดี ที่มีภาพหรือมีทั้งภาพและเสียง)

7) งานภาพยนตร์

8) งานแพร่เสียงแพร่ภาพ

9) งานอื่นใดในแผนกวรรณคดี วิทยาศาสตร์ หรือศิลปะ

ซึ่งเป็นสิทธิที่ได้รับการคุ้มครองในการคัดลอกหรือทำซ้ำผลงาน ถึงแม้ว่าผลงานนั้นจะนำเสนอทางอินเทอร์เน็ต และตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 จะคุ้มครองผลงานนั้น ๆ เป็นเวลา 50 ปี หลังจากที่งานได้คิดค้นขึ้น หรือตั้งแต่ที่มีการแสดงผลงานเป็นครั้งแรก ผลงานชิ้นนั้นจะแจ้งจดหรือไม่แจ้งจดลิขสิทธิ์ก็ได้ สามารถดูรายละเอียดของพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 เพิ่มเติมได้ที่

http://www.ratchakitcha.soc.go.th/DATA/PDF/2537/A/059/1.PDF

6.1.3.3 สิทธิบัตร (Patent) เป็นหนังสือสำคัญที่ออกรับรองให้เพื่อคุ้มครองการประดิษฐ์ หรือออกแบบผลิตภัณฑ์ต่าง ๆ ซึ่งพระราชบัญญัติสิทธิบัตร พ.ศ. 2522 จะคุ้มครอง

สิทธิบัตรที่แจ้งจด 20 ปี นับตั้งแต่วันขอรับสิทธิบัตร สามารถดูรายละเอียดของพระราชบัญญัติสิทธิบัตร พ.ศ. 2522 ได้ที่ http://www.ratchakitcha.soc.go.th/DATA/PDF/2522/A/035/1.PDF

ความลับทางการค้า ลิขสิทธิ์ และสิทธิบัตร แตกต่างกันตรงที่ ผลงานที่ได้รับความคุ้มครองจากลิขสิทธิ์และสิทธิบัตรเป็นสิ่งที่เปิดเผยต่อสาธารณะ เพราะสร้างขึ้นเพื่อให้คนทั่วไปใช้ และโปรแกรมคอมพิวเตอร์จะได้รับความคุ้มครองภายใต้กฎหมายลิขสิทธิ์เนื่องจากถูกจัดอยู่ในประเภทเดียวกับงานเขียน ในสังคมของเทคโนโลยีสารสนเทศมักจะกล่าวถึงการละเมิดลิขสิทธิ์ซอฟต์แวร์ เมื่อซื้อโปรแกรมคอมพิวเตอร์ที่มีการจดลิขสิทธิ์ นั่นหมายความว่าได้จ่ายค่าลิขสิทธิ์ในการใช้ซอฟต์แวร์นั้น สำหรับผู้ใช้หลังจากเปิดกล่องหรือบรรจุภัณฑ์แล้ว หมายถึงว่า ได้ยอมรับข้อตกลงเกี่ยวกับลิขสิทธิ์ในการใช้สินค้านั้น ซึ่งลิขสิทธิ์ในการใช้จะแตกต่างกันไปในแต่ละสินค้าและบริษัท บางโปรแกรมคอมพิวเตอร์จะอนุญาตให้ติดตั้งได้เพียงครั้งเดียว หรือไม่อนุญาตให้ใช้กับคอมพิวเตอร์เครื่องอื่น ๆ ถึงแม้ว่าเครื่องนั้น ผู้ใช้เป็นเจ้าของและไม่มีผู้อื่นใช้ก็ตาม ในขณะที่บางบริษัทอนุญาตให้ใช้โปรแกรมนั้นได้ในหลาย ๆ เครื่อง ตราบใดที่ผู้ใช้ยังเป็นบุคคลที่มีสิทธิในโปรแกรมคอมพิวเตอร์ที่ซื้อมา

การคัดลอกโปรแกรมคอมพิวเตอร์ให้กับบุคคลอื่น เป็นการกระทำที่จะต้องพิจารณาให้รอบคอบก่อนว่า โปรแกรมที่จะทำการคัดลอกนั้นเป็นโปรแกรมคอมพิวเตอร์ที่ผู้ใช้มีสิทธิในระดับใด ตัวอย่างเช่น

Copyright software เป็นซอฟต์แวร์ลิขสิทธิ์ ที่ผู้ใช้ซื้อลิขสิทธิ์มา และมีสิทธิ์ใช้

Shareware เป็นซอฟต์แวร์ที่ให้ทดลองใช้ได้ ก่อนที่จะตัดสินใจซื้อ

Freeware เป็นซอฟต์แวร์ที่ให้ใช้งานได้ฟรี คัดลอก และเผยแพร่ให้ผู้อื่นได้

ความลับทางการค้ากับสิทธิบัตรจะมีความแตกต่างกันหลายเรื่องไม่ว่าจะเป็นในเรื่องของระบบการให้ความคุ้มครอง สิทธิที่ได้รับ หรือในเรื่องของอายุการคุ้มครอง แต่ในบางกรณีผู้ที่เป็นเจ้าของข้อมูลความลับทางการค้าบางอย่าง เช่น ข้อมูลการค้าที่เกี่ยวกับตัวสินค้า หรือตัวผลิตภัณฑ์ เช่น สูตรอาหาร สูตรส่วนผสมของยา หรือข้อมูลการค้าที่เกี่ยวกับวิธีการผลิตสินค้า เช่น ข้อมูลเกี่ยวกับกรรมวิธีการถนอมอาหาร กรรมวิธีการผลิตสีย้อมผ้า อาจเห็นว่าข้อมูลการค้าของตนที่มีอยู่นอกจากจะเป็นความลับทางการค้าแล้วยังอาจจะอยู่ในเงื่อนไขที่จะได้รับการคุ้มครองตามกฎหมายสิทธิบัตรอีกด้วย แต่ไม่แน่ใจว่าควรจะให้การคุ้มครองสิ่งเหล่านั้นทางไหนดี ในเรื่องนี้ ผู้ที่เป็นเจ้าของข้อมูลดังกล่าวควรพิจารณาเรื่องต่าง ๆ ดังต่อไปนี้ประกอบด้วย คือ

1) การให้ความคุ้มครองโดยการยื่นคำขอจดทะเบียนสิทธิบัตร ผู้ที่เป็นเจ้าของต้องเปิดเผยข้อมูลที่เป็นรายละเอียดของการประดิษฐ์เพื่อแสดงให้เห็นว่าสิ่งที่นำมาขอรับสิทธิบัตรเป็นของใหม่ไม่เคยมีมาก่อน แต่การให้ความคุ้มครองความลับทางการค้าไม่จำเป็นต้องเปิดเผยรายละเอียดของข้อมูลที่เป็นความลับ เนื่องจากไม่ได้เป็นระบบจดทะเบียน ดังนั้นถ้าเจ้าของความลับทางการค้านำข้อมูลการค้าที่เป็นความลับมาจดทะเบียนขอรับความคุ้มครองทางด้านสิทธิบัตร ความเป็นความลับของข้อมูลนั้นก็จะหมดไป จะเปลี่ยนใจนำข้อมูลการค้านั้นมาขอรับความคุ้มครองตามกฎหมายความลับทางการค้าอีกไม่ได้

2) ถ้าเจ้าของข้อมูลการค้าสามารถเก็บข้อมูลการค้าของตนไว้เป็นความลับได้ ข้อมูลนั้นก็จะยังคงเป็นความลับต่อไปไม่มีกำหนดเวลาสิ้นสุด แต่ถ้านำไปจดทะเบียนขอรับความคุ้มครองทางด้าน

สิทธิบัตร กฎหมายจะให้การคุ้มครองภายในเวลาที่จำกัด เมื่อพ้นระยะเวลาตามที่กฎหมายกำหนด สิ่งนั้นก็จะตกเป็นของสาธารณะ ทุกคนก็สามารถนำไปใช้ได้ สิทธิผูกขาดแต่เพียงผู้เดียวที่เคยมีอยู่ก็จะหมดสิ้นไป

3) ถ้าผู้ที่เป็นเจ้าของความลับทางการค้าเลือกที่จะเก็บความลับทางการค้าของตนไว้ต่อมา หากปรากฏว่ามีคนอื่นมาขโมยข้อมูลที่เป็นความลับทางการค้านั้นไปเปิดเผยให้บริษัทคู่แข่งรายอื่นๆ ข้อมูลการค้านั้นก็จะสูญเสียการเป็นความลับไป ผู้ที่เป็นเจ้าของจะต้องพิสูจน์ให้ศาลเห็นได้ว่าความลับทางการค้านั้นเป็นของตน มีการขโมยไป และสูตร วิธีการ หรือกรรมวิธีในการผลิตสินค้าของคู่แข่งรายอื่นๆ เป็น สูตร วิธีการ หรือกรรมวิธีของตน ซึ่งค่อนข้างจะพิสูจน์ได้ยาก แต่ถ้าเจ้าของข้อมูลเลือกที่จะนำข้อมูลดังกล่าวไปจดทะเบียนขอรับการคุ้มครองทางด้านสิทธิบัตร หากมีบริษัทคู่แข่งรายใดมาผลิตสินค้าเลียนแบบโดยใช้ ข้อมูล สูตร วิธีการ หรือกรรมวิธีเดียวกับที่ได้จดทะเบียนสิทธิบัตรไว้ ผู้ที่เป็นเจ้าของสิทธิบัตรก็จะได้รับการคุ้มครองตามกฎหมาย

6.1.4 การเข้าถึงข้อมูล (Data Accessibility)

การเข้าใช้งานโปรแกรมหรือระบบคอมพิวเตอร์มักจะมีการกำหนดสิทธิตามระดับของผู้ใช้งาน ทั้งนี้เพื่อเป็นการป้องกันการเข้าไปดำเนินการต่าง ๆ กับข้อมูลของผู้ใช้ที่ไม่มีส่วนเกี่ยวข้อง และเป็นการรักษาความลับของข้อมูล ตัวอย่างสิทธิในการใช้งานระบบ เช่น การบันทึก การแก้ไข ปรับปรุง และการลบ เป็นต้น ดังนั้นในการพัฒนาระบบคอมพิวเตอร์จึงได้มีการออกแบบระบบรักษาความปลอดภัยไว้ การเข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับความยินยอมนั้นก็ถือเป็นการทำผิดจริยธรรมเช่นเดียวกับการละเมิดข้อมูลส่วนตัว

ในการใช้งานคอมพิวเตอร์และเครือข่ายร่วมกันให้เป็นระเบียบ ผู้ใช้ร่วมใจกันปฏิบัติตามระเบียบและข้อบังคับของแต่ละหน่วยงานอย่างเคร่งครัดแล้ว การกระทำผิดจริยธรรมทางคอมพิวเตอร์ก็คงจะไม่เกิดขึ้น

6.2 อาชญากรรมทางคอมพิวเตอร์

คอมพิวเตอร์และเทคโนโลยีสารสนเทศมีการพัฒนาอย่างรวดเร็วและต่อเนื่องทำให้การดำเนินชีวิตประจำวัน โดยเฉพาะการติดต่อสื่อสารระหว่างกันจากทุกมุมโลกทำได้อย่างสะดวก อย่างไรก็ตามโลกของไซเบอร์ที่มีการใช้เครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตอย่างมากมายนั้น ต้องยอมรับว่า เทคโนโลยีก็สามารถก่อให้เกิดปัญหาได้เช่นกัน เพราะมีการก่ออาชญากรรมทางคอมพิวเตอร์เพิ่มมากขึ้นเรื่อย ๆ

อาชญากรรมทางคอมพิวเตอร์ (Computer crime) หรืออาชญากรรมไซเบอร์ (Cyber crime) เป็นการกระทำที่ผิดกฎหมายโดยใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศเป็นเครื่องมือ เช่น

การโจรกรรมข้อมูลหรือความลับของบริษัทคู่แข่ง การบิดเบือนข้อมูล การฉ้อโกง การหลอกลวง การฟอกเงิน การถอดรหัสโปรแกรมคอมพิวเตอร์ ไวรัสคอมพิวเตอร์ การทำลายข้อมูลและระบบการป้องกันในระบบเครือข่าย การก่อกวนโดยกลุ่มแฮกเกอร์ (Hacker) รวมไปถึง การก่อการร้ายในโลกไซเบอร์ (Cyber terrorist) เป็นต้น

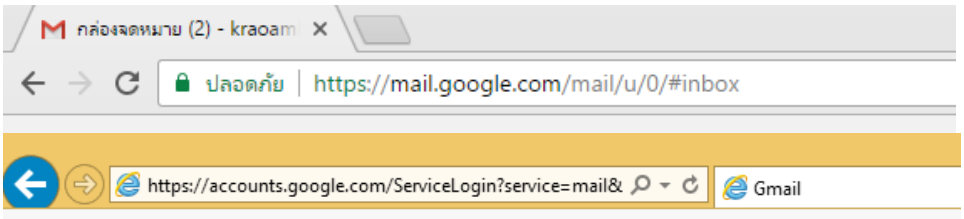
แฮกเกอร์ หรือนักเลงคอมพิวเตอร์ คือ บุคคลที่มีความรู้ในระบบคอมพิวเตอร์เป็นอย่างดี สามารถเข้าไปถึงข้อมูลในคอมพิวเตอร์ โดยเจาะผ่านระบบรักษาความปลอดภัยของคอมพิวเตอร์ ซึ่งเป็นการใช้ความรู้ความสามารถในทางที่ไม่ถูกต้อง เช่น การลักลอบเข้าไปยังคอมพิวเตอร์เครื่องอื่นผ่านการสื่อสารบนระบบเครือข่าย โดยไม่ได้รับอนุญาต อาจจะมีวัตถุประสงค์เข้าไปเพื่อหาช่องโหว่ของระบบเครือข่าย หรืออาจกระทำไปด้วยความสนุก ต้องการทดสอบความสามารถของตนเอง รวมถึงการอวดความสามารถกับเพื่อน ๆ ส่วน แครกเกอร์ (Cracker) หรือนักเจาะระบบ คือแฮกเกอร์ที่มีความชำนาญทางด้านคอมพิวเตอร์ ระบบเครือข่าย หรือการเขียนโปรแกรมคอมพิวเตอร์มากเป็นพิเศษ ลักลอบเข้าไปยังคอมพิวเตอร์ของผู้อื่นเพื่อมุ่งทำลายระบบ เจาะระบบเพื่อล้วงข้อมูล คัดลอก เปลี่ยนแปลง ลบ หรือทำลายข้อมูลให้เสียหาย จะสร้างความเสียหายที่รุ่นแรง เพื่อประโยชน์ของตนเองหรือพวกพ้อง แครกเกอร์จะสร้างความเสียหายที่ร้ายแรงกว่าแฮกเกอร์มาก การกระทำของแฮกเกอร์หรือแครกเกอร์ เป็นการกระทำที่ผิดกฎหมายทั้งสิ้น

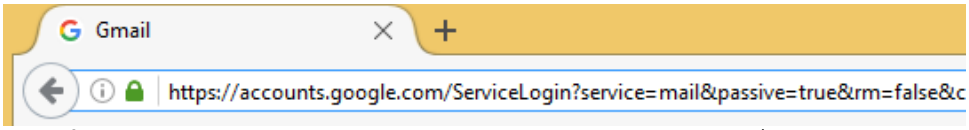
6.2.1 การใช้คอมพิวเตอร์ในฐานะเป็นเครื่องมือในการก่ออาชญากรรม

การก่ออาชญากรรมโดยการใช้คอมพิวเตอร์เป็นเครื่องมือมีหลายรูปแบบ เช่น

6.2.1.1 การขโมยหมายเลขบัตรเครดิต (Credit card theft)

หากบัตรเครดิตหาย จะด้วยทำหายเองหรือถูกขโมยก็ตาม เมื่อเจ้าของบัตรรู้ต้องรีบแจ้งระงับการใช้บัตรในทันที แต่ถ้าถูกขโมยหมายเลขบัตรเครดิตทางอิเล็กทรอนิกส์แล้ว เป็นการยากที่เจ้าของจะรู้จนกว่าจะได้รับใบแจ้งยอดการใช้เงินจากบัตรนั้น ในบางครั้งขโมยอาจนำหมายเลขบัตรไปใช้สำหรับการเข้าฐานข้อมูลเครดิต และบัญชีธนาคาร เพื่อจะกระทำการอื่น ๆ ต่อไป ดังนั้นเมื่อจะซื้อสินค้าและชำระเงินด้วยบัตรเครดิตผ่านทางอินเทอร์เน็ตจะต้องแน่ใจว่าระบบมีการรักษาความปลอดภัย เช่น ถ้าทำธุรกรรมผ่านเว็บไซต์หรือกำลังใช้เว็บไซต์ให้สังเกตว่าที่ Address bar ของ Web browser จะมีรูปแม่กุญแจล็อกอยู่ และที่อยู่เว็บไซต์หรือ URL จะระบุ https:// ดังภาพ 6.1





ภาพที่ 6.1 สัญลักษณ์รูปแม่กุญแจล็อก หรือ https:// ปรากฏอยู่ที่แอดเดรสบาร์ของเว็บเบราว์เซอร์

6.2.1.2 การแอบอ้างตัว (Identity theft)

เป็นการแอบอ้างตัวของผู้กระทำต่อบุคคลที่สามว่าตนเป็นอีกคนหนึ่ง การกระทำในลักษณะนี้จะใช้ลักษณะเฉพาะตัว ได้แก่ หมายเลขบัตรประชาชน หมายเลขบัตรเครดิต หนังสือเดินทาง และข้อมูลส่วนบุคคลอื่น ๆ ของผู้ถูกกระทำหรือเหยื่อไปใช้แอบอ้างเพื่อหาผลประโยชน์ ตัวอย่างเช่น นายดำแอบอ้างตัวว่าเป็นนายแดง โดยการส่งอีเมลและเอกสารปลอมที่แสดงตนว่าเป็นนายแดงจริง เพื่อขอเปลี่ยนแปลงเจ้าของเว็บไซต์จากนายแดงเป็นนายดำ ดังนั้นนายดำก็จะได้รับผลประโยชน์ต่าง ๆ โดยที่ไม่ต้องจ่ายค่าสิทธิในการใช้ที่อยู่อินเทอร์เน็ตนั้น หรือนางสาวหน่อยตั้งชื่อ Facebook เหมือนชื่อของดารานักแสดง เพื่อลอกให้ผู้อื่นหลงเชื่อว่าเป็นดารานักแสดงคนนั้นจริง แล้วก็หลอกให้ผู้อื่นโอนเงินให้ เป็นต้น

6.2.1.3 การสแกมทางคอมพิวเตอร์ (Scam)

เป็นการกระทำโดยใช้คอมพิวเตอร์เป็นเครื่องมือในการหลอกลวงผู้อื่น ปัจจุบันมีรูปแบบที่แตกต่างกันมากมาย เช่น

1) การส่งข้อความ หรือโฆษณาบนเว็บไซต์ว่าผู้ใช้สามารถเดินทางเข้าพักหรือท่องเที่ยวแบบหรูในราคาถูกแต่เมื่อเข้าไปใช้บริการจริง กลับไม่เป็นอย่างที่บอกไว้ หรือบางครั้งอาจต้องมีการจ่ายเพิ่มเติม ซึ่งไม่ได้แจ้งไว้ล่วงหน้า ดังนั้นหากเกิดกรณีเช่นนี้ ก่อนตัดสินใจควรจะต้องมีข้อตกลงเป็นลายลักอักษร รวมทั้งข้อตกลงเกี่ยวกับการยกเลิกสัญญาให้ชัดเจนเสียก่อน

2) การเสนอให้ผู้ใช้สามารถเข้าไปใช้บริการเว็บไซต์เฉพาะผู้ใหญ่ได้ฟรี หากผู้ใช้ระบุหมายเลขบัตรเครดิตเพื่อเป็นการยืนยันอายุของผู้ใช้ หลังจากนั้นผู้ใช้ก็จะได้รับใบเรียกเก็บเงินจากบัตรเครดิตโดยที่ผู้ใช้ไม่ได้ซื้อสินค้าหรือรับบริการใด ๆ เลย ดังนั้นก่อนที่ผู้ใช้จะกรอกหมายเลขบัตรเครดิตจะต้องอ่านรายละเอียดหรือข้อตกลงให้รอบคอบเสียก่อน

6.2.2 การใช้คอมพิวเตอร์ในฐานะเป็นเป้าหมายของอาชญากรรม

นอกจากการใช้คอมพิวเตอร์เป็นเครื่องมือในการก่ออาชญากรรมแล้ว คอมพิวเตอร์ก็อาจเป็นเป้าหมายของอาชญากรรมได้ด้วย ตัวอย่างลักษณะการกระทำที่เป็นอาชญากรรมคอมพิวเตอร์ใน 4 ลักษณะประเด็นคือ

6.2.2.1 การเข้าถึงและการใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาต

การเข้าถึงและการใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นการกระทำต่าง ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์หรือข้อมูลของผู้อื่นโดยที่เจ้าของไม่อนุญาต การเข้าถึงอาจใช้วิธีขโมยรหัสส่วนตัว (Personal identification number : PIN) หรือการเข้ารหัสผ่าน (Password) ซึ่งการกระทำโดยมิชอบนี้อาจก่อให้เกิดความเสียหายแก่บุคคลหรือองค์การ เช่น การเข้าถึงข้อมูลส่วนบุคคลเกี่ยวกับประวัติทางการแพทย์ การรักษาพยาบาล ข้อมูลทางการเงิน หรือการเข้าถึงข้อมูลที่เป็นความลับทางการค้า ซึ่งหากนำข้อมูลเหล่านี้ไปเผยแพร่ในทางที่ไม่ถูกต้องแล้ว ย่อมก่อให้เกิดความเสียหายแก่เจ้าของอย่างแน่นอน อาชญากรรมประเภทนี้มีเหตุจูงใจในการกระทำที่แตกต่างกัน เช่น พวกที่มีมูลจูงใจทางการเงินและโจรกรรมความลับทางการค้า หรือลิขสิทธิ์ต่าง ๆ ส่วนพวกที่ทำเพื่อสนองความพอใจส่วนตัวก็จะเข้าไปเพื่อสืบความลับของคู่รักหรือศัตรู ในขณะพวกที่เคียดแค้น เช่น พนักงานที่ถูกไล่ออกจะกระทำไปเพื่อที่จะต้องการแก้แค้นนายจ้าง เป็นต้น

6.2.2.2 การก่อกวนหรือการทำลายข้อมูล

ข้อมูลและสารสนเทศเป็นทรัพย์สินที่มีคุณค่าของบุคคล ของบริษัท หรือหน่วยงานภาครัฐ การถูกขโมยข้อมูลหรือข้อมูลถูกทำลาย อาจสร้างความเสียหายให้กับองค์การมากกว่าการถูกขโมยโปรแกรมหรืออุปกรณ์คอมพิวเตอร์ ผู้ใช้สามารถที่จะตกเป็นเหยื่อของการถูกขโมยข้อมูลได้เนื่องจากบางบริษัทต้องการนำข้อมูลนั้น ๆ เพื่อใช้ในการแข่งขันทางธุรกิจ การขโมยข้อมูลจะเกี่ยวข้องกับอาชญากรรมประเภทอื่น ๆ เช่น การเข้าถึงข้อมูลหรือเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต เป็นต้น

มัลแวร์ (Malware) ย่อมาจากคำว่า Malicious Software หมายถึงโปรแกรมประสงค์ร้ายต่าง ๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล มัลแวร์ แบ่งออกได้หลากหลายประเภท อาทิเช่น ไวรัส (Virus) เวิร์ม (Worm) หรือหนอนอินเทอร์เน็ต ม้าโทรจัน (Trojan Horse) การแอบดักจับข้อมูล (Spyware) คีย์ล็อกเกอร์ (Key Logger) บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน ตลอดจนโปรแกรมประเภทขโมยข้อมูล (Cookie) และการฝัง Malicious Mobile Code (MMC) ผ่านทางช่องโหว่ของโปรแกรม Internet Browser โดยโปรแกรมจะทำการควบคุมการทำงานโปรแกรม Internet Browser ให้เป็นไปตามความต้องการของผู้ที่ไม่หวังดี เช่น การแสดงโฆษณาในลักษณะของการ Pop-Up หน้าต่างโฆษณาออกมาเป็นระยะ เรียกโปรแกรมประเภทนี้ว่า แอ็ดแวร์ (Adware) ซึ่งภัยเหล่านี้ในปัจจุบันได้เพิ่มขึ้นอย่างรวดเร็ว ซึ่งอาจจะเกิดผลกระทบแก่ผู้ใช้งานได้ ถ้ารับโปรแกรมเหล่านี้เข้ามาในเครื่องคอมพิวเตอร์

การก่อกวนหรือการทำลายข้อมูลเป็นอาชญากรรมคอมพิวเตอร์ที่เข้าไปปั่นป่วนและแทรกแซงการทำงานของคอมพิวเตอร์ฮาร์ดแวร์และซอฟต์แวร์โดยไม่ได้รับอนุญาต เช่น

1) ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นโปรแกรมที่สามารถติดต่อจากไฟล์หนึ่งไปยังอีกไฟล์หนึ่งภายในระบบเดียวกัน หรือจากคอมพิวเตอร์เครื่องหนึ่งไปยัง

เครื่องอื่นโดยการแนบตัวเองไปกับโปรแกรมอื่น สามารถทำลายฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล เมื่อโฮสต์รันโปรแกรมที่ติดไวรัส ส่วนที่เป็นไวรัสก็จะถูกรันด้วยและทำให้แพร่กระจายไปยังเครื่องอื่นหรือบางทีก็สร้างโค้ดใหม่ เป็นโปรแกรมที่ออกแบบมาเพื่อดัดแปลงโปรแกรมคอมพิวเตอร์อื่น โปรแกรมที่ติดไวรัสจะเพิ่มจำนวนตัวเองอย่างรวดเร็ว ซึ่งอาจแฝงตัวอยู่ในไฟล์หรือสื่อเก็บข้อมูล เช่น ฮาร์ดดิสก์ แฟลชไดร์ฟ การสร้างความเสียหายจะแบ่งเป็น 2 ลักษณะคือ ไวรัสที่แสดงข้อความรบกวนหรือทำให้คอมพิวเตอร์ทำงานช้าลง แต่จะไม่ทำลายข้อมูล อีกประเภทหนึ่งจะทำลายการทำงานของระบบคอมพิวเตอร์ ได้แก่ การลบไฟล์ การสั่งปิดเครื่องคอมพิวเตอร์ หรือการรบกวนการทำงานของโปรแกรมอื่น ๆ ที่ติดตั้งอยู่ในเครื่องที่ติดไวรัส เป็นต้น

โดยทั่วไปไวรัสคอมพิวเตอร์จะแบ่งเป็น 3 ชนิดคือ 1) ไวรัสที่ทำงานบน Boot sector หรือบางครั้งเรียก System Virus ไวรัสประเภทนี้จะแฝงตัวอยู่ที่ Boot sector ของฮาร์ดดิสก์ แล้วยังสามารถที่จะฝังตัวอยู่ในหน่วยความจำของเครื่องคอมพิวเตอร์ได้ด้วย จะทำงานเมื่อเริ่มเปิดระบบ 2) ไวรัสที่เกาะติดที่แฟ้มงานหรือโปรแกรม ไวรัสชนิดนี้จะแฝงตัวอยู่ตามไฟล์ต่าง ๆ ส่วนใหญ่จะเป็นไฟล์ที่มีนามสกุลเป็น .exe และ .com เพราะเป็นไฟล์ที่ถูกเรียกใช้งานเป็นประจำ การทำงานของไวรัสจะเกิดขึ้นเมื่อผู้ใช้เรียกใช้ไฟล์ที่ติดไวรัส จากนั้นไวรัสจะฝังตัวเองในหน่วยความจำของคอมพิวเตอร์ โดยปกติการติดไวรัสประเภทนี้มักมาจากการดาวน์โหลดไฟล์หรือโปรแกรมจากอินเทอร์เน็ตในแหล่งที่ไม่ปลอดภัย หรือการเปิดไฟล์ที่แนบมากับอีเมล 3) แมโครไวรัส (Macro Virus) เป็นไวรัสที่ทำงานบนโปรแกรมที่ใช้ภาษาแมโคร เช่น โปรแกรมประมวลคำ (Word processing) และโปรแกรมตารางคำนวณ (Spreadsheet) เป็นต้น ไวรัสแมโครเป็นอันตรายได้โดยที่ไม่ต้องเรียกใช้งานไฟล์ที่มีนามสกุล .exe

ไวรัสส่วนใหญ่จะทำงานเมื่อเปิดเครื่องคอมพิวเตอร์ใช้งานหรือเรียกไฟล์ที่ติดไวรัส มีไวรัสประเภทหนึ่งเรียกว่า ลอจิกบอมบ์ (logic bomb) หรือ ระเบิดเวลา (Time bomb) ซึ่งเป็นไวรัสที่ออกแบบมาให้ทำงานตามเงื่อนไขหรือเวลาที่กำหนดไว้ จะทำงานเมื่อนาฬิกาของเครื่องเดินถึงเวลาที่ถูกเขียนให้ไวรัสตื่นขึ้นมาทำงานนั่นเอง

ไวรัสคอมพิวเตอร์ที่ระบาดไปทั่วโลกและมีความรุนแรงมาก เป็นมัลแวร์เรียกค่าไถ่ ชื่อ วอนนา คราย (WannaCry) ถูกค้นพบเมื่อเดือนกุมภาพันธ์ พ.ศ. 2560 และระบาดหนักไปทั่วโลกช่วงต้นเดือนพฤษภาคม พ.ศ. 2560 โดย โดยมัลแวร์ดังกล่าวมีจุดประสงค์หลักเพื่อเข้ารหัสลับข้อมูลในคอมพิวเตอร์เพื่อเรียกค่าไถ่ หากไม่จ่ายเงินตามที่เรียกจะไม่สามารถเปิดไฟล์ได้ มัลแวร์เรียกค่าไถ่ตัวนี้ ระบาดผ่านช่องโหว่ของวินโดวส์ซอฟต์แวร์ ทำให้ผู้ไม่ประสงค์ดีสามารถติดตั้งซอฟต์แวร์ลงบนคอมพิวเตอร์ของเราได้และนอกจากนี้ตัวมัลแวร์เอง ยังสามารถกระจายตัวจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งได้อัตโนมัติอีกด้วย ดูข้อมูลและ

การป้องกันเพิ่มเติมได้ที่ https://www.thaicert.or.th/alerts/user/2017/al2017us001.html

2) เวิร์ม (Worm) หรือหนอน คุณสมบัติพิเศษของเวิร์ม คือ สามารถแพร่กระจายตัวของมันเองได้โดยอัตโนมัติและไม่ต้องอาศัยโปรแกรมอื่นในการแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่นๆ ผ่านทางเครือข่าย เวิร์ม สามารถทำอันตรายให้กับระบบ เวิร์มบางประเภทสามารถแพร่กระจายตัวเองโดยที่ไม่ต้องอาศัยการช่วยเหลือจากผู้ใช้เลย หรือบางตัวก็อาจแพร่กระจายเมื่อผู้ใช้รันโปรแกรมบางโปรแกรม นอกจากความสามารถในการแพร่กระจายด้วยตัวเองแล้ว เวิร์มยังสามารถทำลายระบบได้อีกด้วย เป็นโปรแกรมคอมพิวเตอร์ที่กระจายตัวเองเช่นเดียวกับไวรัส แต่แตกต่างกันที่ไวรัสต้องให้มนุษย์สั่งการเรียกใช้งาน ในขณะที่เวิร์มจะแพร่กระจายตัวเองจากคอมพิวเตอร์สู่คอมพิวเตอร์เครื่องอื่นๆ โดยผ่านทางอีเมลและเครือข่ายอินเทอร์เน็ต เวิร์มจะแพร่กระจายโดยการค้นหาที่อยู่อีเมลของผู้ใช้จาก E-mail Address Book จากนั้นก็จะส่งตัวมันเองไปกับอีเมลนั้น ๆ เมื่อผู้ใช้เปิดไฟล์อ่าน เวิร์มก็จะเริ่มทำงานโดยการคัดลอกตัวเองและส่งอีเมลอิเล็กทรอนิกส์ไปยังคนอื่น ๆ ที่มีรายชื่ออยู่ใน E-mail Address Book ของผู้ใช้เหมือนกับการส่งอีเมลลูกโซ่ถึงคนอื่น ๆ ต่อไปเรื่อย ๆ เวิร์มจะทำลายไฟล์ โดยโปรแกรมจะตรวจสอบว่าระบบมีไฟล์ที่สามารถคัดลอกตัวมันเองลงไปแทนที่ได้หรือไม่ ถ้ามีก็จะคัดลอกลงไปแทนที่ และเมื่อมีการเรียกใช้ไฟล์นั้น เวิร์มก็จะกระจายต่อไปเรื่อย ๆ ตัวอย่างเวิร์มที่รู้จักกันอย่างแพร่หลาย เช่น “Nimda”, “W32.Sobig”, “W32.bugbear”, “W32.Blaster” และ “Love Bug” (ซึ่งเป็นไฟล์ที่แนบมากับอีเมลที่กำหนดหัวเรื่องว่า “I LOVE YOU”)

3) ม้าโทรจัน (Trojan Horse) เป็นโปรแกรมที่ดูเหมือนจะมีประโยชน์หรือไม่เป็นอันตราย แต่ในตัวโปรแกรมจะแฝงโค้ดสำหรับการใช้ประโยชน์หรือทำลายระบบที่รันโดยโปรแกรมนี้ส่วนใหญ่จะถูกแนบมากับ E-mail และเมื่อดูเผิน ๆ ก็เป็นโปรแกรมอรรถประโยชน์ทั่ว ๆ ไป แต่จริง ๆ แล้ว ข้างในจะแฝงส่วนที่เป็นอันตรายต่อระบบเมื่อรันโปรแกรมนี้ ม้าโทรจันจะแตกต่างจากไวรัสและเวิร์ม ตรงที่ม้าโทรจันจะไม่กระจายตัวมันเองไปยังคอมพิวเตอร์เครื่องอื่น ๆ ได้โดยโปรแกรมม้าโทรจันจะแฝงตัวอยู่กับโปรแกรมอื่น ๆ ที่อาจส่งผ่านมาทางอีเมล เช่น Zipped_files.exe และเมื่อมีการเรียกใช้ไฟล์ โปรแกรมจะลบไฟล์ที่อยู่ในฮาร์ดดิสก์

4) ข่าวหลอกลวง (Hoax) เป็นการส่งข้อความต่อ ๆ กันเหมือนอีเมลลูกโซ่เพื่อให้เกิดความเข้าใจผิดโดยอาศัยเทคนิคทางจิตวิทยาทำให้ข่าวนั้นน่าเชื่อถือ

การก่ออาชญากรรมโดยใช้ไวรัส เวิร์ม และม้าโทรจัน มีข้อสังเกตเพื่อใช้ในการตรวจสอบว่าเครื่องคอมพิวเตอร์ที่กำลังใช้งานอยู่ติดไวรัสหรือไม่ เช่น มีข้อความหรือภาพแปลก ๆ แสดงบนจอภาพ มีเสียงที่ผิดปกติหรือเสียงเพลงเปิดขึ้นเป็นบางเวลา หน่วยความจำคอมพิวเตอร์ลดน้อยลงกว่าที่ควรจะเป็น เครื่องคอมพิวเตอร์ที่กำลังใช้งานอยู่ทำงานช้าผิดปกติ

โปรแกรมหรือไฟล์หายไปโดยที่ผู้ใช้ไม่ได้ลบทิ้ง มีโปรแกรมแปลกปลอมเข้ามา ขนาดของไฟล์ใหญ่ผิดปกติ การทำงานของไฟล์หรือโปรแกรมผิดปกติไปจากเดิมที่เคยใช้

6.2.2.3 การทำให้ระบบปฏิเสธการให้บริการ (Denial of Service)

การทำให้ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ หรือ DoS เป็นการโจมตีเว็บไซต์เพื่อไม่ให้เว็บไซต์นั้นติดต่อสื่อสารกับคอมพิวเตอร์เครื่องอื่น ๆ ได้ การโจมตีอาจมาจากคอมพิวเตอร์เพียงเครื่องเดียว หรือจากคอมพิวเตอร์จำนวนมากที่ถูกควบคุมสั่งการ (Distributed Denial of Service : DDoS) โดยผู้กระทำหรือแฮกเกอร์จะเข้าไปยังระบบคอมพิวเตอร์ที่ไม่ใช่เป้าหมายหลักของการจู่โจม แต่จะเข้าไปเพื่อติดตั้งรหัสซึ่งจะเปลี่ยนทั้งระบบให้กลายเป็นตัวแทน (Agents) หรือทาส (Zombies or Slaves) ของแฮกเกอร์ (ซึ่งแฮกเกอร์สามารถควบคุมตัวแทนได้หลายตัวในเวลาเดียวกัน) ในขณะเดียวกันแฮกเกอร์ก็จะสั่งให้ตัวแทนส่งข้อความ หรือการขอใช้บริการจำนวนมากพร้อม ๆ กันไปยังเครื่องคอมพิวเตอร์แม่ข่ายของเหยื่อ (Victims) ทำให้ระบบเกิดการติดขัดจนต้องปิดบริการชั่วคราว ส่งผลเสียต่อการดำเนินธุรกิจ โดยปกติแล้ว Dos / DDoS จะเป็นการโจมตีเว็บไซต์ที่ให้บริการทางธุรกิจ หรือเว็บไซต์ราชการ เป็นต้น

6.2.2.4 การขโมยคอมพิวเตอร์

การขโมยเครื่องคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องก็เป็นปัญหาอาชญากรรมอย่างหนึ่ง โดยเฉพาะเครื่องคอมพิวเตอร์ที่อยู่ตามสำนักงานของหน่วยงานภาครัฐ หรือเอกชน ที่เก็บข้อมูลสำคัญ ๆ เอาไว้ อาจจะมีผู้ประสงค์ร้ายต้องการนำข้อมูลที่เก็บอยู่ในเครื่องนั้นมาใช้งาน หรือทำลายทิ้งเพื่อปกปิดความลับบางอย่าง หลาย ๆ หน่วยงานต้องปกป้องโดยการติดตั้งกล้องวงจรปิด ติดตั้งเหล็กดัด หรือเก็บคอมพิวเตอร์และอุปกรณ์ที่มีความสำคัญนั้นไว้ในห้องนิรภัย ที่มีการป้องกันหลายชั้นกว่าจะเข้าไปถึงได้ หรือมีการสำรองข้อมูลไว้ในเครื่องอีกที่หนึ่ง เป็นต้น

6.3 วิธีการป้องกันการเข้าถึงข้อมูลและคอมพิวเตอร์

การป้องกันการเข้าถึงข้อมูลและคอมพิวเตอร์จากบุคคลที่ไม่ได้รับอนุญาต ได้แก่

6.3.1 การใช้ User name หรือ User ID และรหัสผ่าน (Password) บางระบบจะกำหนดชื่อผู้ใช้และรหัสผ่านมาให้เพื่อความสะดวก ในขณะที่บางระบบจะให้ผู้ใช้กำหนดเอง หากระบบใดมีการกำหนดรหัสผ่านมาให้ ผู้ใช้ควรเปลี่ยนแปลงรหัสผ่านนั้นใหม่ด้วยตนเองในภายหลัง และควรหลีกเลี่ยงการกำหนดรหัสที่เป็นวันเดือนปีเกิด เบอร์โทรศัพท์ หรือรหัสอื่น ๆ ที่แฮกเกอร์สามารถเดาได้ง่าย ควรตั้งรหัสผ่านที่มีทั้งตัวอักษรและตัวเลข

6.3.2 การใช้วัตถุใด ๆ เพื่อการเข้าสู่ระบบ ได้แก่ บัตร หรือกุญแจ ตัวอย่างเช่น การใช้บัตร ATM เพื่อทำธุรกรรมเกี่ยวกับบัญชีธนาคาร ซึ่งโดยปกติจะใช้บัตรควบคู่กับ PIN (Personal

Identification Number) ประกอบด้วยตัวเลข 4 หลักและ PIN ก็เป็นรหัสผ่านที่เจ้าของควรให้ความสำคัญไม่ควรใช้ตัวเลขที่เกี่ยวกับวันเดือนปีเกิดหรือการจดรหัสลงในบัตร

6.3.3 การใช้อุปกรณ์ทางชีวะภาพ (Biometric Devices) เป็นการใช้อุปกรณ์ตรวจสอบลักษณะส่วนตัวของบุคคลเพื่อการอนุญาตใช้โปรแกรม ระบบ อุปกรณ์ หรือการเข้าใช้ห้องคอมพิวเตอร์ เช่น การตรวจสอบด้วยเสียง ลายนิ้วมือ ฝ่ามือ ลายเซ็น ม่านตา และรูปหน้า เป็นต้น โดยอุปกรณ์จะทำการแปลงลักษณะส่วนบุคคลให้อยู่ในรูปข้อมูลดิจิทัลแล้วเปรียบเทียบกับข้อมูลที่จัดเก็บในคอมพิวเตอร์ ถ้าข้อมูลไม่ตรงกันคอมพิวเตอร์ก็จะปฏิเสธการเข้าสู่ระบบ

6.3.4 ระบบเรียกกลับ (Callback System) หรือ OTP (On Time Password) เป็นระบบที่ผู้ใช้ระบุชื่อและรหัสผ่าน เพื่อขอเข้าใช้ระบบปลายทาง หากข้อมูลถูกต้อง คอมพิวเตอร์ก็จะเรียกกลับให้เข้าใช้งานเอง ระบบในลักษณะนี้เป็นการเพิ่มความปลอดภัยให้คอมพิวเตอร์อีกระดับหนึ่ง คือ คอมพิวเตอร์จะตรวจสอบหมายเลขโทรศัพท์ของผู้ใช้เมื่อเรียกกลับ อย่างไรก็ตามการใช้งานลักษณะนี้จะมีประสิทธิภาพมากขึ้นถ้าผู้ขอใช้ระบบใช้เครื่องคอมพิวเตอร์จากตำแหน่งเดิม (หมายเลขโทรศัพท์เดิม) ในขณะที่การใช้เครื่องคอมพิวเตอร์แบบพกพาอาจต้องเปลี่ยนหมายเลขโทรศัพท์ ทำให้เกิดความเสี่ยงมากกว่า

6.3.5 เครื่องคอมพิวเตอร์ที่ใช้งานต้องติดตั้งโปรแกรมสแกนไวรัส สแกนสิ่งแปลกปลอมที่จะเข้ามาในเครื่อง และอัพเดตฐานข้อมูลไวรัสอย่างสม่ำเสมอ

6.3.6 อย่าดาวน์โหลดโปรแกรม ในเว็บไซต์ที่มีความเสี่ยง

6.3.7 สำรองข้อมูลต่าง ๆ ที่มีในเครื่องไว้ กรณีฉุกเฉินจะสามารถนำกับมาใช้ใหม่ได้ หรือใส่รหัสผ่านในการเปิดไฟล์ รหัสผ่านสำหรับแก้ไขเปลี่ยนแปลงไฟล์ ที่สำคัญ ๆ

6.4 ข้อควรระวังในการเข้าไปยังโลกไซเบอร์หรือใช้งานอินเทอร์เน็ต

ถ้าใช้บริการต่าง ๆ ผ่านอินเทอร์เน็ต ให้พิจารณาข้อพึงระวังต่อไปนี้

6.4.1 บัตรเครดิตและการแอบอ้าง

1) ถ้ามีการกรอกข้อมูลส่วนตัวควรใช้เฉพาะเว็บไซต์ที่มีระบบรักษาความปลอดภัย เช่น https:// หรือตรวจสอบชื่อเว็บไซต์หรือ URL ว่าเป็นชื่อเดียวกันกับเว็บที่เคยใช้บริการหรือไม่ทุกครั้ง เพราะมิจฉาชีพอาจจะทำเว็บไซต์ปลอมที่ตั้งชื่อเว็บและมีหน้าตาของเว็บเหมือนหรือคล้ายกับเว็บไซต์ที่เราเคยใช้มาก ถ้าไม่สังเกตดี ๆ เพื่อหลอกให้ผู้ใช้ กรอกข้อมูลส่วนตัวในการทำธุรกรรมต่าง ๆ ผ่านเว็บ

2) ให้หมายเลขบัตรเครดิตเฉพาะบริษัทที่ผู้ใช้ไว้วางใจได้เท่านั้น

3) ใช้รหัสผ่านอย่างน้อย 10 ตัวอักขระ (ควรผสมระหว่างตัวอักษรและตัวเลข)

4) ใช้รหัสผ่านที่แตกต่างกันในแต่ละระบบหรือเว็บไซต์

6.4.2 การป้องกันข้อมูลส่วนบุคคล

พิจารณาอย่ารอบคอบก่อนการให้ข้อมูลส่วนตัว และให้ข้อมูลในส่วนที่จำเป็น เฉพาะบุคคลนั้น ๆ เท่านั้น

6.4.3 การหลีกเลี่ยงสแปมเมล

สแปมเมลอาจก่อความรำคาญแก่ผู้ใช้อินเทอร์เน็ตได้อย่างมาก เนื่องจากมันจะทวีจำนวนขึ้นเรื่อย ๆ ถ้าผู้ใช้ให้ที่อยู่อีเมลแก่บริษัทที่ทำธุรกิจออนไลน์ ดังนั้นจึงต้องระมัดระวังการลงทะเบียนเพื่อรับข่าวสารกลับมายังอีเมลของผู้ใช้

6.4.4 การป้องกันระบบคอมพิวเตอร์และเครือข่าย

ใช้ไฟร์วอลล์ (Firewall) ที่เป็นฮาร์ดแวร์หรือซอฟต์แวร์เพื่อทำหน้าที่เป็นยามประตูตรวจสอบการเข้าระบบของผู้บุกรุกที่ไม่หวังดี ติดตั้งโปรแกรมสแกนไวรัส สแกนหนอนและม้าโทรจันที่เครื่องคอมพิวเตอร์ หรือโทรศัพท์มือถือ

6.4.5 อย่ารับหรือเปิดอ่านอีเมล หรือไฟล์ที่แนบมากับอีเมล จากคนที่ไม่รู้จัก

6.4.6 ติดตั้งโปรแกรมป้องกันเด็กเข้าถึงเว็บไซต์ที่ไม่พึงประสงค์ เช่น เว็บลามก อาจาร

6.4.7 ติดตามข่าวสารเกี่ยวกับการก่ออาชญากรรมทางคอมพิวเตอร์ จากสื่อต่าง ๆ หรือติดตามข่าวสารเกี่ยวกับการป้องกันการก่อกวนและทำลายข้อมูลได้ที่ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย ที่เว็บไซต์ https://www.thaicert.or.th/

6.5 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

สำหรับประเทศไทยมีกฎหมายที่ใช้ลงโทษผู้ที่กระทำความผิดเกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศ คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 18 มิถุนายน 2550 เริ่มมีผลบังคับใช้ 18 กรกฎาคม 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 จะขอนำข้อความในบางส่วนของพระราชบัญญัติฉบับนี้มาให้ทราบ หากต้องการดูรายละเอียดเนื้อหาทั้งหมดของพระราชบัญญัตินี้สามารถศึกษาเพิ่มเติมได้ที่ http://www.ratchakitcha.soc.go.th/DATA/PDF/2550/A/027/4.PDF และ http://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF

มาตรา ๓ ในพระราชบัญญัตินี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดา

ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบ

คอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ผู้ให้บริการ” หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

.....

หมวด ๑

ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มี

ไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิด ความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับ สามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ต้องระวางโทษปรับไม่เกิน สองแสนบาท

ให้รัฐมนตรีออกประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับและลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่ สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึง สองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาท ถึงสามแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่น ถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท

มาตรา ๑๒/๑ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นเหตุให้เกิดอันตราย แก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่น ถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำ ความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำ ความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญา ตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย ก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำ ความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่ง หรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่าย หรือเผยแพร่ชุดคำสั่งดังกล่าวต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นนั้นด้วย

ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคหนึ่งหรือวรรคสอง และตามวรรคสาม หรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทงเดียว

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่

น่าจะเกิดความเสียหาย แก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิด ความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

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

ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใด บุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้

มาตรา ๑๕ ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิด ตามมาตรา ๑๔

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้อง รับโทษ

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลง ด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็น การติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๖/๑ ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่าจำเลย มีความผิด ศาลอาจสั่ง

(๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว

(๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณา หรือเผยแพร่

(๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น

มาตรา ๑๖/๒ ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลาย ตามมาตรา ๑๖/๑ ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ ในมาตรา ๑๔ หรือมาตรา ๑๖ แล้วแต่กรณี

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร

มาตรา ๑๗/๑ ความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๑๑ มาตรา ๑๓ วรรคหนึ่ง มาตรา ๑๖/๒ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๗ ให้คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้ง มีอำนาจเปรียบเทียบได้

คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งตามวรรคหนึ่งให้มีจำนวนสามคนซึ่งคนหนึ่งต้องเป็น พนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา

เมื่อคณะกรรมการเปรียบเทียบได้ทำการเปรียบเทียบกรณีใดและผู้ต้องหาได้ชำระเงินค่าปรับตามคำเปรียบเทียบภายในระยะเวลาที่คณะกรรมการเปรียบเทียบกำหนดแล้ว ให้ถือว่าคดีนั้นเป็นอันเลิกกัน ตามประมวลกฎหมายวิธีพิจารณาความอาญา

ในกรณีที่ผู้ต้องหาไม่ชำระเงินค่าปรับภายในระยะเวลาที่กำหนด ให้เริ่มนับอายุความในการฟ้องคดีใหม่ นับตั้งแต่วันที่ครบกำหนดระยะเวลาดังกล่าว

.....

หมวด ๒

พนักงานเจ้าหน้าที่

.....

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใด เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

.....

ตัวอย่างการกระทำที่เข้าข่ายมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และฉบับที่ ๒ พ.ศ. ๒๕๖๐ เช่น

6.5.1 ความผิดฐานเป็นแฮกเกอร์ หรือแอบเข้าไปในเครื่องของผู้อื่น นักเจาะระบบ

บุรุกเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกันโดยไม่ได้รับอนุญาต จะมีความผิดตาม มาตรา 5 โทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 10,000 บาท หรือทั้งจำทั้งปรับ ถ้ารู้วิธีการป้องกันในการเข้าถึงข้อมูลข้องผู้อื่นแล้วนำไปเผยแพร่ ทำให้ผู้อื่นเสียหาย มีความผิดตาม มาตรา 6 โทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท หรือทั้งจำทั้งปรับ ขโมยหรือแอบใช้ Username และ Password ในการเข้าถึงข้อมูลของผู้อื่น มีความผิดตามมาตรา 7 โทษจำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 40,000 บาท หรือทั้งจำทั้งปรับ

6.5.2 ความผิดเพราะมือบอน ชอบลองของสร้างหรือปล่อยไวรัส หรือแฮกเกอร์ที่เข้าไปจงใจแก้ไข ทำลายข้อมูลของผู้อื่น จะมีความผิดตาม มาตรา 9 โทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ มาตรา 10 โทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

6.5.3 ความผิดเพราะอิจฉา ก่อกวนหรือกลั่นแกล้งผู้อื่น ส่งอีเมลขยะไปรบกวนผู้อื่น จะมีความผิดตาม มาตรา 11 โทษปรับไม่เกิน 100,000บาท

6.5.4 ความผิดเพราะชอบโพสต์กระทู้ ฟอร์เวิร์ดอีเมล ส่งต่อข้อความ เนื้อหา รูปภาพที่ไม่เหมาะสม หรือแอบอ้าง ใส่ร้ายป้ายสีผู้อื่น เช่น

1) ปลอมแปลงไฟล์เพื่อแฝงตัวเข้าไปทำลายระบบคอมพิวเตอร์ผู้อื่น

2) การหลอกลวง ฉ้อโกง ผู้อื่นผ่านเว็บไซต์

3) ชอบโพสต์แสดงความคิดเห็น ข้อมูลโคมลอย โพสต์ข้อความอันเป็นเท็จใส่ร้ายป้ายสีผู้อื่นแบบไม่มีหลักฐาน หรือหมิ่นประมาทผู้อื่น

4) ส่งต่ออีเมล ส่งต่อรูปภาพ ข้อความ คลิปวิดีโอทั้งหลายที่ไม่เหมาะสมกระทบต่อความมั่นคงของประเทศ

จะมีความผิดตามมาตรา 14 ต้องโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

6.5.5 จัดทำหรือเผยแพร่เว็บไซต์ลามกอนาจาร โพสต์หรือส่งต่อภาพหรือวิดีโอที่ลามกอนาจาร จะมีความผิดตาม มาตรา 14 โทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

6.5.6 ความผิดของผู้ดูแลเว็บไซต์ หรือเจ้าของเว็บไซต์ที่ปล่อยปะละเลย

ถ้าเป็นเว็บไซต์ที่เปิดให้สมาชิกสามารถโพสต์ ถาม ตอบ แสดงความคิดเห็น ไม่ว่าจะอยู่ในรูปของข้อความ รูปภาพ หรือคลิปวิดีโอ ที่เข้าข่ายความผิดตามมาตรา 14 แล้วเจ้าของเว็บหรือผู้ดูแลเว็บไม่รีบทำการลบข้อมูลดังกล่าว ก็จะมีความผิดตาม มาตรา 15 โทษเช่นเดียวกับผู้โพสต์คือจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ ผู้ให้บริการหรือเจ้าของเว็บ ต้องเก็บข้อมูลของผู้ใช้บริการไว้อย่างน้อย 90 วัน เพื่อให้สามารถหาตัวผู้กระทำความผิด หากเจ้าหน้าที่ขอตรวจสอบแล้วไม่ได้ทำการเก็บข้อมูลการใช้งานดังกล่าว ก็จะมีความผิดตามมาตรา 26 โทษปรับไม่เกิน 500,000 บาท

6.5.7 ความผิดของผู้ที่ชอบโพสต์ภาพผู้อื่น ไม่ว่าภาพนั้นจะเป็นภาพจริงหรือภาพตัดต่อ

ถ้าภาพนั้นทำให้ผู้อื่นเสื่อมเสียชื่อเสียง อับอาย ถูกเกลียดชัง จะมีความผิดตามมาตรา 16 โทษจำคุกไม่เกิน 3 ปี และปรับไม่เกิน 200,000 บาท แต่ถ้าโพสต์ภาพนั้นโดยสุจริต ก็ถือว่าไม่มีความผิด ความผิดตามมาตรา 16 นี้ สามารถยอมความกันได้

ทั้งนี้จากตัวอย่างที่กล่าวมาอาจจะมีความผิดตามมาตราอื่น ๆ อีก หากเป็นการกระทำที่สร้างความเสียหายต่อความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ เช่น ความผิดตามมาตรา 12 มาตรา 13 เป็นต้น

6.6 บทสรุป

จริยธรรมทางคอมพิวเตอร์ หมายถึง แนวทางการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศอย่างมีศีลธรรม มีความรู้สึกผิดชอบชั่วดี หรือใช้งานในสิ่งที่บุคคลในสังคมยอมรับ ไม่ทำให้เกิดความวุ่นวายในสังคม มีสามัญสำนึกต่อสังคมในทางที่ดี จริยธรรมที่เกี่ยวข้องกับสังคมยุคคอมพิวเตอร์และเทคโนโลยีสารสนเทศ จะเกี่ยวข้องกับกรอบแนวคิด ที่ตั้งอยู่บนพื้นฐาน 4 ประการ คือ ความเป็นส่วนตัว ความถูกต้อง ความเป็นเจ้าของ และการเข้าถึงข้อมูล

อาชญากรรมคอมพิวเตอร์เป็นปัญหาที่เกิดขึ้นทั่วโลก โดยนอกจากจะเป็นการกระทำที่ขาดจริยธรรมทางคอมพิวเตอร์แล้ว ยังถือว่าผิดกฎหมายด้วย การก่ออาชญากรรมทางคอมพิวเตอร์มีหลายรูปแบบ เช่น การลักลอบเข้าไปในระบบที่มีการป้องกัน การลักลอบเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การขโมยและทำลายอุปกรณ์ การขโมยโปรแกรมคอมพิวเตอร์ การก่อกวนระบบด้วยโปรแกรมประสงค์ร้าย เป็นต้น วิธีป้องกันและรักษาความปลอดภัยระบบคอมพิวเตอร์อาจทำได้หลายแบบเช่น การติดตั้งโปรแกรมป้องกันไวรัส การใช้ระบบไฟล์วอลล์ การเข้ารหัสข้อมูล และการสำรองข้อมูลเป็นต้น

6.7 แบบฝึกหัดท้ายบท

1. จงยกตัวอย่างการกระทำผิดจริยธรรมทางคอมพิวเตอร์

2. จงอธิบายความแตกต่างของความลับทางการค้า ลิขสิทธิ์ และสิทธิบัตร ว่ามีความแตกต่างกันอย่างไร

3. จงยกตัวอย่างปัญหาอาชญากรรมทางคอมพิวเตอร์มาอย่างน้อย 1 ตัวอย่าง พร้อมทั้งบอกวิธีการป้องกันและแก้ไข

4. จงอธิบายความแตกต่างของแฮกเกอร์กับแครกเกอร์มาให้เข้าใจ

5. ปัจจุบันประเทศไทยใช้กฎหมายหลักอะไรที่ลงโทษผู้กระทำความผิดโดยใช้คอมพิวเตอร์เทคโนโลยีสารสนเทศ และบอกเหตุผลด้วยว่าทำไมต้องมีการตรากฎหมายดังกล่าวขึ้นมาใช้

เอกสารอ้างอิง

พนิดา พานิชกุล. (2553). ความมั่นคงปลอดภัยของสารสนเทศและการจัดการ. กรุงเทพฯ : เคทีพี คอมพ์ แอนด์ คอนซัลท์.

. (2553). **จริยธรรมทางเทคโนโลยีสารสนเทศ**. กรุงเทพฯ : เคทีพี คอมพ์ แอนด์ คอนซัลท์.

ไพบูลย์ อมรภิญโญเกียรติ. (2553). **คำอธิบาย พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2550**. กรุงเทพฯ : โปรวิชั่น.

ราชบัณฑิตยสถาน. (2546). **ศัพท์คอมพิวเตอร์และเทคโนโลยีสารสนเทศ.** พิมพ์ครั้งที่ 6. กรุงเทพฯ : สหมิตรพริ้นติ้ง.

วิโรจน์ ชัยมูล และสุพรรษา ยวงทอง. (2558). **ความรู้เบื้องต้นเกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศ**. กรุงเทพฯ : โปรวิชั่น.