เรื่องน่ารู้สำหรับลูกเสือไซเบอร์

CYBER SCOUT THAILAND

รู้ไว้ภัยออนไลน์

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

คำนำ

หนังสือที่ท่านกำลังจะเปิดอ่านอยู่นี้ เป็นการค้นคว้า เรียบเรียงเนื้อหาสาระเกี่ยวกับภัยออนไลน์ และ รูปแบบและลักษณะของความผิดเกี่ยวกับคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยบุคลากรกลุ่มงานส่งเสริมและพัฒนาสังคมอิเล็กทรอนิกส์ สำนักส่งเสริมและพัฒนาการใช้เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งเป็นผู้ดูแลโครงการสร้างลูกเสือบนเครือข่ายอินเทอร์เน็ต หรือเรียกสั้นๆ ว่า "ลูกเสือไซเบอร์ (Cyber Scout)" ดังนั้น เนื้อหาในหนังสือเล่มนี้จึงเหมาะสำหรับลูกเสือไซเบอร์ ตลอดจนเด็ก เยาวชน และผู้ที่ต้องการศึกษาหาความรู้เพื่อการรู้เท่าทันภัยที่จะแทรกซึมเข้ามาทางโลกออนไลน์ ซึ่งเป็นที่ทราบกันดีอยู่แล้วว่า "โลกออนไลน์ หรืออินเทอร์เน็ต" เป็นแหล่งของความรู้ ความบันเทิง ฯลฯ ที่หลากหลายไม่มีขอบเขต ผู้คนสามารถติดต่อ ส่งข่าวสารกันได้ทั่วโลกโดยที่ไม่จำเป็นต้องรู้จักกันเลย

ผู้จัดทำหวังเป็นอย่างยิ่งว่า หนังสือเล่มนี้จะเป็นเสมือนภูมิคุ้มกันในการไม่กระทำความผิดทางคอมพิวเตอร์ ซึ่งไม่เฉพาะสำหรับตัวลูกเสือไซเบอร์เอง แต่ยังสามารถแนะนำความรู้นี้ให้กับอาสาสมัครลูกเสือไซเบอร์รุ่นต่อๆ ไป หรือมิตรสหาย ได้อีกด้วย

คณะผู้จัดทำ
กลุ่มงานส่งเสริมและพัฒนาสังคมอิเล็กทรอนิกส์
สำนักส่งเสริมและพัฒนาการใช้เทคโนโลยีสารสนเทศและการสื่อสาร
มีนาคม 2557

สารบัญ

ภัยคุกคามจากการใช้งานอินเทอร์เน็ต

การกระทำผิดกฎหมาย เกิดขึ้นได้ตลอดเวลาบนอินเทอร์เน็ต บางครั้งผู้ใช้กระทำความผิดโดยรู้เท่าไม่ถึงการณ์ เช่น การดาวน์โหลดเพลงมาฟัง หากเพลงที่ดาวน์โหลดเพลงมาฟังนั้นเป็นเพลงที่ละเมิดลิขสิทธิ์มาก็เท่ากับเราทำผิดกฎหมายด้วย , การส่งต่อคลิปวิดีโอหรือเขียนกระทู้ที่ทำให้มีผู้เสียหายก็เป็นความผิด , การประกาศขายไตของเราเองก็ผิดกฎหมายห้ามซื้อขายอวัยวะเป็นต้น ทั้งนี้ มิจฉาชีพก็ยังใช้อินเทอร์เน็ตในการฉ้อโกงเราด้วย ตัวอย่างเช่น การเปิดเว็บไซต์ปลอมเพื่อลวงเอาหมายเลขบัตรเครดิต , โพสต์กระทู้เชิญชวนให้ซื้อโทรศัพท์มือถือราคาถูกซึ่งความเป็นจริงแล้วไม่มีอยู่จริง , การส่งโปรแกรมโจมตีระบบคอมพิวเตอร์หรือขโมยข้อมูลผู้อื่น เป็นต้น

1. วิธีสังเกตภัยคุกคามจากอินเทอร์เน็ต

ปัจจุบันการขยายตัวของเครือข่ายออนไลน์เป็นไปอย่างรวดเร็วและเติบโตอย่างกว้างขวางจนเรียกได้ว่ากลายเป็นศูนย์รวมสินค้าขนาดมหึมา สำหรับกลุ่มนักล่าออนไลน์ที่มุ่งจะล่วงละเมิดทางเพศต่อเยาวชน เว็บไซต์ประเภทต่างๆ ไม่ว่าจะเป็นไดอารี่ออนไลน์ , เว็บหาเพื่อนร่วมโรงเรียนหรือต่างโรงเรียน , เว็บหาคู่ , ชุมชนออนไลน์ หรือการเล่นแชทไลน์ ซึ่งกลายเป็นสื่อร้ายที่ผู้กระทำผิดคิดมิชอบ เข้าไปค้นหาข้อมูลแล้วกระทำการล่อลวง เยาวชนของเราให้กลายเป็นเหยื่อชั้นดีอย่างง่ายดาย ตามข่าวเศร้าที่ได้พบเห็นจากสื่อต่างๆ ทั้งโทรทัศน์ แลหนังสือพิมพ์ เหตุเพราะเยาวชนของเราหลงไปติดกับดัก โพสต์ข้อมูลส่วนตัว วิธีการติดต่อผ่านจดหมายอิเล็กทรอนิกส์ (E-mail) และโปรแกรมรูปแบบต่างๆ

แนวทางการรับมือกับภัยออนไลน์

1) เมื่อตัวเราเอง หรือบุคคลใกล้ชิด ใช้เวลาเล่นอินเทอร์เน็ตมากเกินจำเป็น โดยเฉพาะช่วงเย็นถึงดึก และมักมีพิรุธปิดหน้าจอหรือเปลี่ยนหน้าจอทันทีที่ท่านเดินผ่าน
2) เมื่อพบว่ามีการ Download ภาพลามกไว้ในคอมพิวเตอร์ ซึ่งได้รับจากนักล่าออนไลน์ส่งมากระตุ้นเร้าความรู้สึกให้ผู้รับภาพ
3) เมื่อพบว่าตัวเอง หรือบุคคลใกล้ชิด ได้รับโทรศัพท์ จากบุคคลที่ไม่เคยรู้จักมาก่อนหรือมีการใช้โทรศัพท์ทางไกลไปยังหมายเลขที่ไม่รู้จัก

4) เมื่อมีพัสดุของขวัญ จดหมายลึกลับมาให้ตัวเราหรือบุคคลใกล้ชิดของท่าน
5) เมื่อตัวเราหรือบุคคลใกล้ชิด มีอาการห่างเหินกับกิจกรรมของสมาชิกในครอบครัวแยกตัวจากกลุ่ม หรือเก็บตัวอยู่คนเดียว

2. กรณีศึกษาภัยคุกคามจากอินเทอร์เน็ต

ภัยคุกคามจากอินเทอร์เน็ตถือได้ว่าเป็นภัยอันตรายต่อสังคมในปัจจุบันเป็นอย่างมาก เพราะนอกจากภัยนี้จะเป็นการรบกวนการทำงานของผู้ที่ใช้งานคอมพิวเตอร์และอินเทอร์เน็ตแล้ว ยังส่งผลเสียต่อข้อมูลสำคัญๆ ที่มีอยู่ โดยประเด็นหลักๆ ที่ควรระมัดระวังในการใช้งานอินเทอร์เน็ต อาจแบ่งได้ดังนี้

2.1 การละเมิดลิขสิทธิ์/ทรัพย์สินทางปัญญา

ทรัพย์สินทางปัญญา (Intellectual Property) คือ สิทธิอันชอบธรรมตามกฎหมายที่คุ้มครองการประดิษฐ์ การออกแบบ ยี่ห้อการค้า ต้นฉบับ รวมถึงสิทธิบัตร เครื่องหมายการค้า และลิขสิทธิ์ (Copyright) เป็นการให้สิทธิแก่ผู้สร้างในการป้องกันการนำผลงานไปใช้โดยไม่ได้รับอนุญาต

และอินเทอร์เน็ตช่วยทำให้ข้อมูลข่าวสารแพร่สะพัดไปอย่างรวดเร็ว ในขณะเดียวกันก็เป็นเครื่องมือชั้นเยี่ยมในการละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา ตัวอย่างที่เห็นได้ชัด เช่น การอัพโหลดและดาวน์โหลดเพลงหรือริงโทนโดยไม่ได้รับอนุญาต การจำหน่ายจ่ายแจกซีดีเถื่อน ซอฟต์แวร์ละเมิดลิขสิทธิ์ การคัดลอกบทความ รูปภาพ ข้อมูล เป็นต้น

ผู้ให้บริการพื้นที่ (Space Provider) และผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) มีส่วนต้องรับผิดชอบกรณีรู้เห็นกับผู้ใช้ในการนำผลงานที่ได้มาโดยมิชอบหรือโดยผิดกฎหมายมาเผยแพร่บนเว็บไซต์ แต่ในทางตรงข้ามก็ไม่ต้องรับผิดชอบหากสามารถพิสูจน์ได้ว่าไม่ได้รู้เห็นกับผู้ใช้ อย่างไรก็ตาม เจ้าของเว็บไซต์หรือผู้ให้บริการมีหน้าที่ต้องตรวจสอบเนื้อหาที่เผยแพร่บนเครื่องของตนอย่างสม่ำเสมอ บนเว็บไซต์ควรจัดแสดงข้อความระบุให้ผู้ใช้มีหน้าที่ต้องรับผิดชอบเนื้อหาข้อมูลที่นำมาเผยแพร่เอง

2.2 การสงวนสิทธิ์ผลงานบนอินเทอร์เน็ตมีหลายรูปแบบ **เช่น**

1) Copyright : ผู้ใช้จะไม่สามารถคัดลอก ดัดแปลง หรือแจกจ่ายงานในลักษณะที่ทำให้เจ้าของผลงานเสียประโยชน์ที่พึงได้จากงานนั้น

(เช่น สูญเสียรายได้) โดยไม่ได้รับอนุญาตจากเจ้าของงานเสียก่อน

2) Copyleft : เจ้าของผลงานอนุญาตให้ผู้ใช้คัดลอก ดัดแปลง หรือเผยแพร่งานโดยไม่ต้องขออนุญาต โดยมีเงื่อนไขบางประการ เช่น จะต้องประกาศว่างานชิ้นนี้ใครเป็นเจ้าของต้นฉบับ หรือจะต้องให้สิทธิ์ผู้ใช้คนต่อไปในการคัดลอก ดัดแปลง หรือเผยแพร่ ตามสิทธิ์ที่เจ้าของงานต้นฉบับกำหนดไว้ในสัญญาการให้อนุญาต (License) ซึ่งมีรูปแบบต่างๆ เช่น

- GPL (GNU Public License) ให้สิทธิ์ผู้ใช้ที่จะคัดลอก ดัดแปลง แจกจ่ายงานได้อย่างอิสระ โดยมีข้อแม้ว่าผู้ใช้นั้นจะต้องแนบสัญญาอนุญาตชนิดเดียวกันนี้ไปกับงานที่ตนคัดลอก ดัดแปลง หรือแจกจ่ายด้วย จุดประสงค์คือเพื่อทำให้งานชิ้นนั้นถูกเผยแพร่ พัฒนาต่อยอดไปได้เรื่อยๆ
- GFDL (GNU Free Documentation License) มีลักษณะเช่นเดียวกับ GPL แต่จะใช้กับงานเอกสาร คู่มือ หรือหนังสือ
- Creative Commons เป็นรูปแบบสัญญาอนุญาตที่ยืดหยุ่น ให้เจ้าของงานกำหนดว่าจะให้สิทธิ์อะไรแก่ผู้ใช้บ้าง เช่น ให้สามารถคัดลอก เผยแพร่ได้ แต่ห้ามดัดแปลง หรือให้คัดลอก เผยแพร่ ดัดแปลง แต่ห้ามเอาไปใช้เพื่อประโยชน์ทางการค้า แต่ไม่ว่าจะเป็น Creative Commons รูปแบบใด ก็จะมีเงื่อนไขอันหนึ่งที่เหมือนกัน ก็คือ ผู้ใช้ต้องระบุว่าใครเป็นเจ้าของงานต้นฉบับเมื่อนำงานนั้นไปใช้ เผยแพร่ หรือดัดแปลง

2.3 โปรแกรมอันตราย (Malware)

โปรแกรมอันตราย (Malware) ย่อมาจาก Malicious Software เป็นคำรวมๆ ที่ใช้เรียกโปรแกรมที่มีจุดประสงค์ร้าย มุ่งโจมตีหรือก่อกวนการทำงานของผู้ใช้อื่นหรือระบบอื่น ชนิดหรือประเภทของ Malware จากอดีตจนถึงปัจจุบันตามที่ได้รวบรวมและสืบค้นจากแหล่งข้อมูลต่างๆ ไม่ว่าจะเป็นการค้นคว้าจากหนังสือ บทความ เอกสารจากการสัมมนา เอกสารทางวิชาการ และเอกสารออนไลน์นั้น สามารถแยกตามคุณลักษณะหรือวัตถุประสงค์ในการใช้งานเป็นประเภทได้ ดังนี้

1) ไวรัสคอมพิวเตอร์ (Computer virus)

ไวรัสคอมพิวเตอร์ เป็นโปรแกรมคอมพิวเตอร์ขนาดเล็กชนิดหนึ่งที่สามารถสำเนา (copy) ตัวเองแล้วเกาะติดและแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่นๆ ได้อย่างรวดเร็วโดยมีวัตถุประสงค์ไปในทางที่ไม่ดี ความสามารถของไวรัสนั้นจะมีตั้งแต่การสร้างความรำคาญเล็กๆ น้อยๆ ไปจนถึงกระทั่งทำลายหรือล้างข้อมูลในฮาร์ดดิสก์ (Hard Disk) คำว่า "ไวรัส" นั้นอาจจะหมายถึงโปรแกรมอันตรายชนิดอื่นๆ ด้วย เช่น หนอนคอมพิวเตอร์ (Worm) , ม้าโทรจัน (Trojan Horses) , สปายแวร์ (Spyware) เป็นต้น ทั้งนี้ เพื่อให้เกิดความง่ายต่อการสื่อถึงโปรแกรมอันตรายต่างๆ เหล่านั้น ซึ่งความจริงแล้วควรจะใช้คำว่า "มัลแวร์ (Malware)" อย่างไรก็ตาม ความหมายของไวรัสนั้นก็ขึ้นอยู่กับความตั้งใจของผู้พูดหรือกล่าวถึงว่าต้องการให้หมายถึงโปรแกรมอันตรายทุกชนิด (มัลแวร์) หรือหมายถึงเฉพาะโปรแกรมไวรัสจริงๆ เท่านั้น ถึงแม้ว่าไวรัสไม่ได้มีความหมายรวมถึงโปรแกรมมุ่งร้ายทั้งหมดแต่ความหมายจะครอบคลุมเพียงโปรแกรมที่สามารถแพร่กระจายตัวเองได้เท่านั้น ในบางครั้งก็มักจะทำให้เกิดความสับสนระหว่างไวรัสกับหนอนคอมพิวเตอร์และม้าโทรจัน ซึ่งความแตกต่างระหว่างไวรัสและหนอนคอมพิวเตอร์คือ หนอนคอมพิวเตอร์จะสามารถแพร่กระจายตัวเองไปได้โดยที่ไม่ต้องอาศัยพาหะ (Host) ในการแพร่กระจายแต่อย่างใด ส่วนไวรัสนั้นไม่สามารถแพร่กระจายจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งได้ด้วยตัวมันเองแต่ไวรัสมีความจำเป็นที่จะต้องอาศัยพาหะเพื่อที่จะอาศัยไปสู่เครื่องที่ยังไม่ติดไวรัสโดยมักจะแพร่กระจายผ่านทางระบบสื่อสารต่างๆ เช่น Floppy disk , แผ่นซีดี , USB drive หรือแม้แต่การทำไฟล์แชร์ (File share) ที่เปิดโอกาสให้เครื่องอื่นๆ เข้ามาดูหรือใช้ทรัพยากรประเภทไฟล์ในเครื่องของผู้เป็นเจ้าของได้ ซึ่งปัจจุบันคนจำนวนมากสามารถที่จะเข้าถึงอินเทอร์เน็ตได้อย่างรวดเร็วและง่ายดาย ดังนั้นไวรัสจำนวนมากจึงได้ประโยชน์จากการใช้เครือข่ายอินเทอร์เน็ตในการแพร่กระจาย ตัวอย่างเช่น การแพร่กระจายผ่านการให้บริการในรูปแบบเวิลด์ไวด์เว็บ (World Wide Web : WWW), อีเมล (e-Mail) , โปรแกรมสนทนา (Instant Messaging) หรือไฟล์แชร์ เป็นต้น

ไวรัสคอมพิวเตอร์ในปัจจุบันสามารถแพร่กระจายออกไปอย่างกว้างขวาง รวดเร็วและมีความรุนแรงในการทำลายล้างสูงกว่าในอดีต ส่วนม้าโทรจันนั้นเป็นโปรแกรมที่มีความสามารถในการเปิดแบ็คดอร์ (Backdoor) และทำตัวเองให้เป็นโปรแกรมที่ดูไม่เป็นอันตรายในสายตาของระบบรักษา

ความปลอดภัยของคอมพิวเตอร์ สำหรับความแตกต่างระหว่างหนอนกับม้าโทรจันก็คือ หนอนจะมุ่งเน้นไปที่การทำให้เกิดอันตรายต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ส่วนม้าโทรจันนั้นถือเป็นโปรแกรมที่สอดคล้องกับการทำงานของคอมพิวเตอร์โดยไม่มีคำสั่งหรือการปฏิบัติการที่เป็นอันตรายต่อตัวคอมพิวเตอร์

อย่างไรก็ตาม ไวรัสบางชนิดได้รับ การออกแบบมาเพื่อที่จะทำลายล้างคอมพิวเตอร์ด้วยการโจมตีโปรแกรม การลบไฟล์หรือแม้กระทั่งการเข้าไปแก้ไขข้อมูลต่างๆ ในฮาร์ดดิสก์ แต่ไวรัสบางชนิดไม่ได้ออกแบบมาเพื่อที่จะทำลายล้างแต่ได้รับการออกแบบมาอย่างง่ายๆ เพื่อทำสำเนาตัวเองแล้วแพร่กระจายไปเรื่อยๆ หรือบางทีอาจจะแสดงข้อความหรือวีดีโอ (Video) เล็กๆ เพื่อก่อกวนหรืออาจสร้างปัญหาให้ถึงขั้นที่ระบบปฏิบัติการคอมพิวเตอร์ล่มหรือปฏิเสธการทำงานได้ ทั้งนี้ ประเภทของไวรัสที่สามารถตรวจพบจากอดีตจนถึงปัจจุบัน ได้แก่

ไวรัสตั้งต้น (Germs)

ไวรัสตั้งต้น เป็นโปรแกรมไวรัสรุ่นแรกสุด ก่อนที่จะมีการแพร่กระจาย กล่าวคือ เป็นไวรัสที่ถูกคอมไพล์ (คอมไพล์ (Compile) หมายถึง การแปลภาษาคอมพิวเตอร์ที่มนุษย์เขียนขึ้นเป็นภาษาที่คอมพิวเตอร์เข้าใจโดยผ่านทางโปแกรมแปลโปรแกรมที่เรียกว่าคอมไพเลอร์ (Compiler)) ออกมาจากซอร์สโค้ด (ซอร์สโค้ด (Source Code) หมายถึง รหัสต้นฉบับรหัสต้นทาง) ในครั้งแรกซึ่งจะมีอยู่ในลักษณะพิเศษและไม่จำเป็นต้องมีไฟล์พาหะให้ฝังตัว

ไวรัสบูต (Boot viruses)

ไวรัสประเภทนี้จะฝังตัวที่ส่วนเริ่มต้นของแผ่นดิสก์เก็ตหรือมาสเตอร์บูตเรคคอร์ด (บูตเรคคอร์ด (boot record) หมายถึง ส่วนที่มีการบันทึกข้อมูลเพื่อการปลุกเครื่องไว้) ของฮาร์ดดิสก์ ส่งผลทำให้เครื่องคอมพิวเตอร์โหลดโปรแกรมไวรัสเข้าไปสู่หน่วยความจำก่อนในขณะเปิดเครื่องแทนที่จะโหลดระบบปฏิบัติการ ตัวอย่างของไวรัสประเภทนี้เช่น ไวรัสที่ชื่อว่า Form, Disk Killer, Michelangelo และ Stone เป็นต้น

ไวรัสโปรแกรม (Program viruses)

ไวรัสโปรแกรม เป็นไวรัสที่ฝังตัวเองไว้ในไฟล์โปรแกรมที่สามารถถูกเอ็กซิคิวต์ (Execute) ได้ ซึ่งส่วนใหญ่จะเป็นไฟล์ที่มีนามสกุล .BIN , .COM , .EXE , .OVL , .DRV (driver) และ .SYS (device driver) เป็นต้น โดยโปรแกรมเหล่านี้จะถูกโหลดเข้าสู่หน่วยความจำในขณะเอ็กซิคิวต์ จึงส่งผลให้

โหลดส่วนการทำงานของไวรัสเข้าไปด้วย ตัวอย่างของไวรัสประเภทนี้ เช่น ไวรัสที่มีชื่อว่า Sunday และ Cascade เป็นต้น

Multipartite viruses

เป็นไวรัสที่มีการทำงานหลากหลายรูปแบบ กล่าวคือ สามารถแพร่กระจายทางไฟล์ปกติและสามารถแพร่กระจายในส่วนของบูตเรคคอร์ดได้ เมื่อมีการเอ็กซิคิวต์ไฟล์ไวรัส ก็จะมีการคัดลอกตัวเองไปยังบูตเรคคอร์ด แต่เมื่อมีการบูตเครื่อง ครั้งต่อไปก็จะถูกโหลดเข้าไปยังหน่วยความจำและฝังตัวในไฟล์อื่นๆ ต่อไป ตัวอย่างของไวรัสประเภทนี้ เช่น ไวรัสที่มีชื่อว่า Invader , Flip และ Tequila เป็นต้น

Stealth viruses

ไวรัสเหล่านี้จะใช้เทคนิคเพื่อหลีกเลี่ยงการตรวจจับ โดยทั่วไปจะใช้วิธีการขัดขวาง (Interrupt) การทำงานของกระบวนการอ่านของระบบดิสก์โดยเมื่อไฟล์ที่ไม่มีไวรัสถูกอ่านขึ้นมาก็จะถูกแทรกส่วนโปรแกรมไวรัสเข้าไป (Read Stealth Virus) นอกจากนี้ยังมีไวรัสที่สามารถเปลี่ยนขนาดของไฟล์หรือไดเรกทรอรี่ของข้อมูล (Size Stealth Virus) เมื่อไวรัสทำงานจะทำการแทรกส่วนโปรแกรมไวรัสระหว่างการอ่านข้อมูล เช่นไวรัสมีขนาดข้อมูล 1,024 ไบต์ และไฟล์ข้อมูลเดิมมีขนาด 4,096 ไบต์ ขนาดของไฟล์ที่ถูกไวรัสฝังตัวก็จะมีขนาด (1,024 + 4,096) 5,120 ไบต์ ซึ่งขนาดไฟล์มีการเปลี่ยนแปลงและจะถูกตรวจจับได้ ดังนั้นไวรัสนี้จะเข้าขัดขวางการทำงานระบบของไดเรกทรอรี่ โดยการอ่านค่า 5,120 ไบต์ขึ้นมา และลบออกด้วยขนาดของตัวไวรัสเอง จากนั้นจึงส่งผลที่ได้ไปยังระบบเพื่อแสดงผลอีกครั้ง ตัวอย่างของไวรัสประเภทนี้ เช่น ไวรัสที่ชื่อว่า Frodo , Joshi และ Whale เป็นต้น

Polymorphic viruses

เป็นไวรัสที่สามารถเข้ารหัสที่โค้ดของไวรัสด้วยค่าคีย์เฉพาะส่งผลทำให้การตรวจจับนั้นทำได้ยากมากยิ่งขึ้น ตัวอย่างของไวรัสประเภทนี้ เช่น Involuntary, Stimulate, Cascade, Phoenix, Evil, Proud และ Virus 101 เป็นต้น

Macro viruses

ไวรัสมาโครเป็นไวรัสที่สามารถติดไปกับไฟล์ต่างๆ ที่มีความสามารถในการใช้งานมาโครได้ เช่น ไฟล์เอกสารไมโครซอฟท์ออฟฟิศ (เช่น Word และ Excel เป็นต้น) เมื่อเปิดไฟล์เอกสารที่มีไวรัสมาโครฝังอยู่แล้ว ไวรัสมาโครจะแฝงตัวเข้าไปอยู่ในไฟล์เทมเพลตที่ชื่อ Normal.dot ซึ่งเป็นไฟล์

ที่เอกสารทุกชิ้นต้องอ้างอิงถึง ตัวอย่างของไวรัสประเภทนี้ เช่น ไวรัสที่มีชื่อว่า DMV, Nuclear และ Word Concept เป็นต้น

Active X

ไวรัสประเภทนี้มุ่งโจมตีโดยอาศัยฟังก์ชั่นการทำงานของเว็บบราวเซอร์ที่อนุญาตให้รันโปรแกรมจากเว็บไซต์ได้อย่างอิสระ ตัวอย่างของไวรัสประเภทนี้ เช่น ไวรัสที่ชื่อ JS.ActiveXComponent เป็นต้น

อนึ่ง ยังมีประวัติและความเป็นมาของไวรัสที่น่าสนใจอีกว่า ในปี ค.ศ. 1970 โปรแกรมเมอร์ชื่อ Bob Thomas ได้ทดลองเขียนโปรแกรมที่สามารถคัดลอกตัวเองไปสู่โปรแกรมอื่นบนคอมพิวเตอร์เครื่องอื่นในเน็ตเวิร์กของ ARPANET (Advanced Research Projects Agency Network หมายถึง เครือข่ายสำนักงานโครงการวิจัยชั้นสูง) ได้ โปรแกรมนี้จะแสดงข้อความออกมาว่า "I'm the Creeper, Catch me if you can!" การที่โปรแกรมนี้สามารถแพร่กระจายตัวเองได้ จึงถูกเรียกว่าเป็น "ไวรัสคอมพิวเตอร์" และจากข้อความที่มันแสดงออกมาทางหน้าจอไวรัสตัวนี้จึงมีชื่อเรียกว่า "ไวรัส Creeper" และถือเป็นไวรัสตัวแรก อย่างไรก็ตาม บางแหล่งข้อมูลก็เชื่อว่าไวรัสตัวแรกเกิดขึ้นก่อนปี ค.ศ. 1969 โดยทีมวิศวกรของ Bell Telephone Laboratories ที่ได้สร้างเกมชื่อว่า "Darwin" ที่ฝังตัวในหน่วยความจำ ทำสำเนาตัวเองได้ ซึ่งจุดประสงค์หลักของเกมนี้ก็คือ ทำลายโปรแกรมของคู่แข่งและครอบครองหน่วยความจำ

โปรแกรมไวรัสตัวแรกที่แพร่ตัวเองออกนอกห้องทดลองไปสู่โลกภายนอกได้คือ "Rother J" ซึ่งเขียนขึ้นโดย Richard Skrenta ในปี ค.ศ. 1981 ไวรัสตัวนี้แพร่ตัวเองโดยการเกาะติดไปกับแผ่นฟล็อปปี้ดิสก์ ระบบปฏิบัติการ Apple DOS 3.3 ซึ่งในสมัยนั้นเน็ตเวิร์กหรืออินเทอร์เน็ตยังไม่แพร่หลาย ดังนั้นการถ่ายโอนโปรแกรมจึงต้องใช้วิธีการสำเนาหรือก๊อปปี้ (copy) จากแผ่นหนึ่งไปยังอีกแผ่นหนึ่ง ซึ่งหากแผ่นต้นฉบับมีไฟล์ใดไฟล์หนึ่งที่ติดไวรัสอยู่ก็จะทำให้ไวรัสมีโอกาสแพร่กระจายไปสู่แผ่นอื่นหรือคอมพิวเตอร์เครื่องอื่นได้

อย่างไรก็ตาม ยังมีไวรัส Brain ที่ถูกสร้างขึ้นเมื่อปี ค.ศ. 1986 โดยโปรแกรมเมอร์อายุ 19 ปี ชาวปากีสถานชื่อ Basit Farooq และพี่ชายของเขาชื่อ Amjad ไวรัส Brain เป็นไวรัสคอมพิวเตอร์ตัวแรกที่เกาะบูตเซคเตอร์ (ไวรัสตัวอื่นก่อนหน้านี้จะเกาะที่ไฟล์) กล่าวได้ว่าในยุค 1980-1990 ถือเป็นยุครุ่งเรืองของไวรัสที่เกาะติดไฟล์โปรแกรม (executable file) และบูตเซคเตอร์ (boot sector) ในยุคนี้มีไวรัสใหม่ๆ ถูกเขียนออกมาจำนวนมาก การแพร่กระจาย

ของไวรัสนอกจากจะติดมากับแผ่นฟล็อปปี้ดิสก์ที่สำเนาต่อๆ กันมาแล้ว ไวรัสยังสามารถติดมาจากไฟล์ที่ดาวน์โหลด (Download หมายถึง บรรจุลง) จาก BBS (Bulletin Board System) ได้อีกด้วย

นอกจากนี้ ยังมีไวรัสที่เขียนโดยคนไทยในราวปี ค.ศ. 1990 โดยเป็นไวรัสขนาด 512 ไบต์ ที่เขียนขึ้นด้วยภาษาแอสแซมบลีและติดต่อโดยเกาะที่บูตเซคเตอร์ การทำงานของไวรัสตัวนี้คือ บังคับให้มีเสียงเพลงออกมาที่ลำโพงโดยเพลงที่ไวรัสตัวนี้เล่นออกมาเป็นเพลงไทยเดิมที่ชื่อ "ลาวดวงเดือน" จึงทำให้ไวรัสตัวนี้มีชื่อว่า "ไวรัสลาวดวงเดือน" และในราวๆ ปี ค.ศ. 1995 ได้มีการค้นพบไวรัสที่เกาะติดไฟล์เอกสาร แทนที่จะติด executable file หรือ boot sector ไวรัสดังกล่าวถูกเรียกว่า "มาโครไวรัส (Macro virus)" มาโครไวรัสเป็นไวรัสประเภทหนึ่งที่ถูกเขียนขึ้นด้วยภาษาสคริปต์ที่รันภายใต้โปรแกรม Microsoft Word หรือ Microsoft Excel หลังจากนั้นก็พบว่ามีไวรัสประเภทสคริปต์ถูกเขียนออกมาเป็นจำนวนมากรวมทั้งไวรัสที่โด่งดังอย่างไวรัส "I Love You" ซึ่งถูกเขียนขึ้นมาด้วยภาษาคอมพิวเตอร์ที่ชื่อ VB Script ในปี ค.ศ. 2000

ม้าโทรจัน (Trojan Horses)

ม้าโทรจันเป็นโปรแกรมที่ถูกออกแบบมาให้แฝงตัวเองเข้าไปในระบบคอมพิวเตอร์และจะทำงานโดยการดักจับเอารหัสผ่านต่างๆ หรือข้อมูลจากปุ่มของคีย์บอร์ดที่ถูกกดในเครื่องคอมพิวเตอร์ที่ถูกม้าโทรจันฝังตัวไว้ แล้วส่งกลับไปยังผู้โจมตีเพื่อเข้าใช้หรือโจมตีระบบในภายหลัง ม้าโทรจันบางตัวยังสามารถจะดาวน์โหลดและติดตั้งภัยคุกคามอื่นๆ เพิ่มเติมได้อีก จึงทำให้ผู้โจมตีได้ข้อมูลส่วนบุคคลต่างๆ ของเจ้าของเครื่องไปเช่น ชื่อ รหัสผ่าน หมายเลขบัญชีธนาคาร รวมทั้งหมายเลขบัตรเครดิต แต่ตัวม้าโทรจันเองจะไม่ได้ทำอันตรายใดๆ ต่อระบบ ม้าโทรจันสามารถแฝงตัวเข้ามาได้ในหลายรูปแบบ เช่น เกมส์ การ์ดอวยพร หรือจดหมายต่างๆ เป็นต้น

อย่างไรก็ตาม ด้วยความที่ม้าโทรจันไม่ได้ถูกออกแบบมาเพื่อทำลายระบบหรือสร้างความเสียหายต่อระบบคอมพิวเตอร์ ม้าโทรจันจึงแตกต่างจากไวรัสและหนอน กล่าวคือ ม้าโทรจันจะไม่สามารถทำสำเนาตัวเองและแพร่กระจายตัวเองได้ แต่สามารถที่จะอาศัยตัวกลางซึ่งอาจเป็นโปรแกรมต่างๆ จดหมาย หรือการไปดาวน์โหลดไฟล์จากแหล่งต่างๆ เมื่อเรียกใช้งานไฟล์เหล่านี้ ม้าโทรจันก็จะทำงานและจะเปิดช่องทางต่างๆ ให้ผู้บุกรุกเข้าโจมตีระบบได้ ประเภทของม้าโทรจัน ได้แก่ Backdoor และ Password-Stealing ตัวอย่าง

ม้าโทรจันที่เป็นที่รู้จัก เช่น Backorifice , Downloader-EV , Pest Trap , Sub7 (SubSeven) , Zbot, Fostrem , Swifi , Kuaiput , Bredolab , Ergrun , Keyloggers/Keystrokers และ Password Retrievers เป็นต้น

สปายแวร์ (Spyware)

สปายแวร์ เป็นโปรแกรมที่มีจุดมุ่งหมายเพื่อเก็บรวบรวมข้อมูลส่วนบุคคลที่สำคัญต่างๆ ภายในเครื่องคอมพิวเตอร์ที่ถูกโปรแกรมประเภทนี้ติดตั้งอยู่ และเทคนิคที่ใช้นั้นได้แก่ การดักข้อมูลที่ถูกกดปุ่มคีย์บอร์ด การบันทึกเว็บไซต์ที่เคยเข้าเยี่ยมชมมา หรือไฟล์เอกสารต่างๆ ที่อยู่ภายในเครื่อง เป็นต้น ตัวอย่างโปรแกรมประเภทนี้ เช่น CoolWebSearch เป็นต้น

สปายแวร์มีหลายประเภทนับตั้งแต่ประเภทที่เป็นคุกกี้จากการเข้าดูเว็บไซต์จนกระทั่งถึงประเภทที่เป็นโปรแกรมซึ่งล่วงล้ำเข้าไปในเครื่องคอมพิวเตอร์ของผู้ใช้เพื่อรายงานข้อมูลกลับไปยังผู้ผลิตว่าผู้ใช้ใช้งานโปรแกรมที่ติดตั้งนั้นอย่างไร โปรแกรมที่ล่วงล้ำนี้โดยทั่วไปจะเป็นซอฟต์แวร์ที่ผู้ใช้ดาวน์โหลดมาจากอินเทอร์เน็ตและติดตั้งเพื่อใช้งานในจุดประสงค์หนึ่ง และผู้ผลิตซอฟต์แวร์นั้นก็ย่อมจะต้องการทราบลักษณะการใช้งานของผู้ใช้เพื่อใช้เป็นข้อมูลในการปรับปรุงซอฟต์แวร์ของตนต่อไป จึงล่วงละเมิดผู้ใช้โดยแอบติดตั้งโปรแกรมในส่วนของการรายงานผลกลับไปยังผู้ผลิตด้วย

หนอนคอมพิวเตอร์ (Worm)

หนอนคอมพิวเตอร์ เป็นโปรแกรมประยุกต์ที่ไม่จำเป็นต้องฝังตัวเองในไฟล์ที่เป็นพาหะและมีการแพร่กระจายตัวเองผ่านระบบเครือข่าย โดยทั่วไปแล้วหนอนจะเอ็กซิคิวต์ตัวมันเองบนเครื่องคอมพิวเตอร์ที่อยู่ในระยะไกลอย่างอัตโนมัติหรือถูกผู้ใช้งานเป็นผู้ทำการเอ็กซิคิวต์เองก็ได้ ซึ่งจะทำให้สามารถแพร่กระจายได้อย่างรวดเร็วและทำความเสียหายรุนแรงกว่าไวรัสมาก ซึ่งหนอนสามารถแบ่งแยกย่อยออกไปได้อีก ดังนี้

- **หนอนอีเมล (Email Worms)**

หนอนอีเมล หรือมีอีกชื่อว่า Mass-Mailers Worm เป็นหนอนที่สามารถแพร่กระจายตัวเองโดยอาศัยอีเมล ซึ่งอาจจะใช้การส่งเนื้อหาที่เป็นลิงค์ (ลิงค์ (Link) หมายถึง เชื่อมโยง, โยง) ให้ดาวน์โหลดไฟล์หนอนจากบางเว็บไซต์ หรืออาจจะแนบไฟล์ของหนอนในรูปแบบของเอกสารที่แนบมาพร้อมกับอีเมล ตัวอย่างของหนอนชนิดนี้ เช่น หนอนในตระกูล Mydoom, Netsky และ Bagle เป็นต้น

➢ Instant Messaging Worms

เป็นหนอนที่แพร่กระจายโดยการส่งลิงค์หรือไฟล์ของหนอนไปกับข้อความที่ถูกส่งในโปรแกรมประเภท Instant messaging (อันได้แก่ MSN, Yahoo หรือ ICQ เป็นต้น) ไปให้กับผู้อื่นที่มีรายชื่ออยู่ในเครื่องที่ถูกหนอนประเภทนี้คุกคาม ตัวอย่างของหนอนชนิดนี้ เช่น หนอนตระกูล Bropia เป็นต้น

➢ Internet Worms

เป็นหนอนที่จะสแกนไปทั่วทั้งระบบเครือข่ายเพื่อค้นหาเป้าหมายที่เป็นเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายที่มีช่องโหว่ จากนั้นก็จะพยายามทำการติดต่อเข้าควบคุมเครื่องดังกล่าว เปรียบเสมือนกับการได้ครอบครองเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายนั้น หรืออีกวิธีหนึ่งในการแพร่กระจายของหนอนชนิดนี้คือ หลังจากที่ค้นพบเครื่องคอมพิวเตอร์เป้าหมายที่ยังไม่ได้รับการซ่อมแซมช่องโหว่ ก็จะทำการส่งแพ็กเก็ต (Packet) ที่เป็นไฟล์ของหนอนหรือไฟล์ที่ใช้ในการดาวน์โหลดหนอน ถ้าหากทำได้สำเร็จหนอนก็จะทำการเอ็กซิคิวต์ตัวเองและทำการส่งเช่นนี้อีกต่อๆ ไป ตัวอย่างของหนอนชนิดนี้ เช่น หนอนในตระกูล Blaster , Welchia และ Sasser เป็นต้น

➢ IRC Worms

หนอนที่อาศัยช่องทางสำหรับการสนทนาผ่านอินเทอร์เน็ตทางพอร์ท (พอร์ท (Port) หมายถึง ช่องทางเข้า/ออก มีความหมายเหมือนกับ input/output port) IRC (Internet Relay Chat หมายถึง การคุยผ่านอินเทอร์เน็ต (ไออาร์ซี)) ซึ่งกระบวนการแพร่กระจายนั้น หนอนจะทำการส่งไฟล์หนอนหรือลิงค์ของเว็บไซต์ที่ถูกหนอนฝังตัวอยู่ซึ่งวิธีการนี้จะไม่ค่อยมีผลกระทบมากนักเพราะว่าผู้รับจะต้องมีการยืนยันที่จะจัดเก็บและเปิดไฟล์นั้นก่อน ตัวอย่างของหนอนชนิดนี้ เช่น Aplore , Maldal , Gokar , Spester , Irok และ Nymph เป็นต้น

➢ File-sharing Networks Worms

หนอนชนิดนี้จะใช้วิธีการคัดลอกตัวเองไปยังโฟลเดอร์ที่เปิดแชร์ไว้ เหมือนกับเป็นโฟลเดอร์หนึ่งภายในเครื่องคอมพิวเตอร์ที่ถูกหนอนประเภทนี้คุกคาม โดยชื่อไฟล์ของหนอนนั้นดูเหมือนจะไม่มีอันตราย และในปัจจุบันหนอนประเภทนี้ก็สามารถอาศัยระบบเครือข่ายแบบ P2P ในการแพร่กระจายได้อีกด้วย ตัวอย่างของหนอนชนิดนี้ เช่น หนอน Duload ที่แพร่กระจายผ่าน

เครือข่ายผู้ที่ใช้งานโปรแกรม KaZaA ซึ่งเป็นโปรแกรมช่วยในการแชร์ไฟล์แบบ P2P เป็นต้น

สำหรับประวัติความเป็นมาของหนอนนั้น ใน ปี ค.ศ. 1988 มีการค้นพบหนอนชื่อมอร์ริส (Morris) ที่ทำให้คอมพิวเตอร์จำนวนมากในสหรัฐอเมริกา รวมทั้งคอมพิวเตอร์ในศูนย์วิจัยขององค์การบริหารการบินและอวกาศแห่งชาติ (The National Aeronautics and Space Administration : NASA) ติดเชื้อไปด้วย และส่งผลกระทบให้การปฏิบัติงานหยุดชะงัก การระบาดครั้งนั้นทำให้เกิดความเสียหายเป็นมูลค่าราว 100 ล้านเหรียญสหรัฐ

2) แอดแวร์ (Adware)

แอดแวร์ เป็นโปรแกรมหรือซอฟต์แวร์แบบซ่อนตัวอีกชนิดหนึ่งที่มีรูปแบบการทำงานและการติดเชื้อคล้ายกับสปายแวร์มาก ต่างกันตรงที่สปายแวร์จะเน้นในการขโมยข้อมูลแล้วส่งกลับไปยังเจ้าของสปายแวร์ ส่วนแอดแวร์จะเน้นที่การโฆษณา โดยจะแสดงหรือดาวน์โหลดโฆษณามายังเครื่องคอมพิวเตอร์หลังจากที่ถูกติดตั้งโปรแกรมนี้แล้ว หรือจะสร้างหน้าจอ Pop-up หรือการ์ตูนน่ารักต่างๆ เพื่อหลอกล่อให้เหยื่อเผลอคลิกเข้าไปยังเว็บไซต์ขายสินค้าในขณะที่มีการเรียกใช้งาน เช่น เว็บไซต์ขายภาพหรือวีดีโอโป๊ เว็บไซต์ของธุรกิจขายตรง เป็นต้น ทั้งนี้ แอดแวร์มักจะถูกแนบมากับอีเมลขยะ (spam mail) หรือโปรแกรมประเภทพักหน้าจอ (Screen Saver) โดยแอดแวร์สามารถทำงานได้โดยอัตโนมัติเมื่อเหยื่อเริ่มใช้งานหรือเข้าสู่อินเทอร์เน็ต ตัวอย่างแอดแวร์ เช่น TopMoxie , 123 Messenger , 180 Solutions เป็นต้น

3) โปรแกรมทดสอบช่องโหว่ (Exploits)

โปรแกรมทดสอบช่องโหว่ เป็นโปรแกรมที่ใช้ในการเจาะระบบคอมพิวเตอร์ เพื่อให้ได้มาซึ่งสิทธิ์เพื่อควบคุมระบบดังกล่าวได้ ซึ่งจำเป็นจะต้องอาศัยการโจมตีผ่านทางช่องโหว่ของระบบด้วย แต่แฮกเกอร์ที่เรียกว่า “White hat” จะนำโปรแกรมประเภทนี้ไปใช้ในการ Penetration testing ซึ่งเป็นการทดสอบเจาะระบบคอมพิวเตอร์โดยที่มีการว่าจ้างจากเจ้าของระบบ เพื่อค้นหาว่าในระบบนี้มีช่องโหว่หรือจุดอ่อนหรือไม่ ตัวอย่างเช่น โปรแกรม zgv เป็นต้น

4) โปรแกรมเจาะระบบ (Auto-Rooters)

โปรแกรมประเภทนี้เป็นเครื่องมือในการเจาะระบบ เพื่อให้ได้มาซึ่งสิทธิ์เป็นผู้ดูแลระบบและสามารถควบคุมเครื่องคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่เป็นเป้าหมายจากระยะไกลได้ โปรแกรมประเภทนี้ส่วนใหญ่จะถูกใช้โดยแฮกเกอร์ที่ไม่ดีหรือที่เรียกว่า "Script-Kiddie"

5) โปรแกรมดาวน์โหลดไวรัส (Virus Downloaders)

โปรแกรมดาวน์โหลดไวรัส เป็นโปรแกรมที่ถ้าถูกติดตั้งและถูกเอ็กซิคิวต์จะดาวน์โหลดโปรแกรมอื่นๆ ที่เป็นอันตรายต่อเครื่องคอมพิวเตอร์และระบบเครือข่ายจากเว็บไซต์หรือแหล่งอื่นๆ แล้วทำการรันโปรแกรมนั้นโดยอัตโนมัติด้วย ตัวอย่าง เช่น Luder.A เป็นต้น

6) โปรแกรมปล่อยไวรัส (Virus Droppers)

โปรแกรมปล่อยไวรัส เป็นโปรแกรมที่ใช้ในการปล่อยไวรัสจากโปรแกรมไวรัสเอง เมื่อเครื่องคอมพิวเตอร์ที่ถูกโปรแกรมประเภทนี้ติดตั้งจะถูกดาวน์โหลดไฟล์ไวรัส หนอน หรือม้าโทรจันอื่นๆ มาไว้ในเครื่องคอมพิวเตอร์นั้นได้ ซึ่งโปรแกรมประเภทนี้อาจจะเป็นโปรแกรมธรรมดาที่แอบลักลอบดาวน์โหลดไวรัสมาหรืออาจจะมาพร้อมกับไวรัสหรือหนอนชนิดอื่นๆ ก็ได้ ตัวอย่าง เช่น หนอนที่ชื่อ Klez นั้นจะมีโปรแกรมนี้เพื่อดาวน์โหลดหนอนที่ชื่อ Elkern เป็นต้น

7) โปรแกรมฉีดไวรัส (Virus Injectors)

โปรแกรมฉีดไวรัส เป็นโปรแกรมที่คล้ายกับโปรแกรมปล่อยไวรัส (Droppers) แตกต่างกันที่โปรแกรมประเภทนี้จะทำการติดตั้งและโหลดส่วนของไวรัสไปไว้ในหน่วยความจำได้ เหมือนกับการฉีดไวรัสเข้าไปสู่หน่วยความจำ นอกจากนี้โปรแกรมประเภทนี้อาจจะฉีดไวรัสเข้าไปกับข้อมูลที่เคลื่อนที่อยู่ในระบบเครือข่ายคอมพิวเตอร์ได้ ตัวอย่างของหนอนหรือไวรัสที่มีลักษณะนี้ เช่น CodeRed ที่ใช้โปรแกรมนี้ในการทำสำเนาตัวเองและส่งออกไปในระบบเครือข่ายคอมพิวเตอร์ เป็นต้น

8) โปรแกรมชุดสร้างไวรัส (Kits-Virus Generators)

นักเขียนไวรัสคอมพิวเตอร์ (Virus writers) ได้พัฒนาโปรแกรมชุดสร้างไวรัส เช่น Virus Creation Laboratory (VCL) หรือ PSMPC generator เป็นต้น เพื่อสร้างไวรัสตัวใหม่ๆ โดยอัตโนมัติ ซึ่งจุดมุ่งหมายก็เพื่อให้สามารถสร้างไวรัสตัวใหม่ๆ และไม่จำเป็นต้องมีความรู้ด้านคอมพิวเตอร์มาก ตัวอย่างของไวรัสที่ถูกสร้างด้วยโปรแกรมชุดสร้างไวรัส เช่น VBS/VBSWG.J หรือเป็นที่รู้จักในชื่อของไวรัส Anna Kournikova ที่ถูกสร้างโดยเครื่องมือที่ชื่อ VBSWG ซึ่งผู้ที่สร้างไวรัสนี้ก็ถูกจับและถูกดำเนินการทางกฎหมายไปแล้ว เป็นต้น

9) โปรแกรมสำหรับส่งสแปม (Spammer Programs)

โปรแกรมประเภทนี้ส่วนมากมักถูกใช้เพื่อส่งข้อความในลักษณะของการชักจูงหรือโฆษณาไปยังกลุ่มผู้รับต่างๆ ผ่านทางอีเมล โปรแกรมสนทนา (Instant Messaging) รวมทั้งอีเมลและ SMS ในโทรศัพท์มือถืออีกด้วย

จุดมุ่งหมายของโปรแกรมประเภทนี้ก็เพื่อให้ผู้ส่งได้รับเงินจากผู้ที่ได้รับข้อความและเข้าเว็บไซต์ที่ปรากฏในข้อความ อีกทั้งโปรแกรมประเภทนี้ยังอาจถูกนำไปใช้ในการบุกรุกแบบฟิชชิ่ง (Phishing) ส่งผลให้เหยื่อนั้นสูญเสียทรัพย์สินหรือข้อมูลส่วนตัว เช่น รหัสผ่าน หมายเลขบัตรเครดิต หมายเลขบัญชี เป็นต้น ตัวอย่างโปรแกรม เช่น Harvesters เป็นต้น

10) โปรแกรมระเบิด (Bombs Programs)

โปรแกรมระเบิด เป็นโปรแกรมการทำงานที่ผู้โจมตีตั้งใจพัฒนาขึ้นมาเพื่อให้เกิดการทำงานผิดปกติขึ้น โดยจะแฝงอยู่ในโปรแกรมที่ใช้งานตามปกติ และจะกำหนดให้มีการทำงานภายใต้เงื่อนไขที่กำหนดไว้ เช่น Time Bomb เป็นโปรแกรมที่มีการตั้งเวลาให้ทำงานตามที่กำหนดเวลาไว้ หรือ Logic Bomb เป็นโปรแกรมที่กำหนดเงื่อนไขให้ทำงานเมื่อมีเหตุการณ์หรือเงื่อนไขใดๆ เกิดขึ้น ลักษณะที่พบ เช่น โปรแกรมจะถูกลบเองเมื่อถูกรันไปแล้ว 2-3 ครั้ง เป็นต้น

11) โปรแกรมโทรศัพท์อัตโนมัติ (Dialers Programs)

โปรแกรมโทรศัพท์อัตโนมัติหรือมีชื่อเรียกอีกว่า Porn dialer หากมีการติดตั้งโปรแกรมประเภทนี้ในเครื่องคอมพิวเตอร์ จะมีการต่อโทรศัพท์

อัตโนมัติ ซึ่งจุดมุ่งหมายก็เพื่อที่จะให้เหยื่อนั้นต้องจ่ายค่าโทรศัพท์ในอัตราที่แพงที่สุดหรือทำให้เสียค่าโทรศัพท์ระหว่างประเทศ ตัวอย่าง เช่น โปรแกรมที่ชื่อ Dialer เป็นต้น

12) โปรแกรมล้อกันเล่น (Joke Programs)

โปรแกรมประเภทนี้จัดได้ว่าเป็นโปรแกรมที่ไม่ได้ตั้งใจทำอันตรายต่อเครื่องหรือระบบโดยตรง หากเพียงแค่ต้องการก่อกวนหรือสร้างความรำคาญให้แก่ผู้ใช้งาน โดยการเข้าไปเปลี่ยนพฤติกรรมปกติของเครื่องคอมพิวเตอร์ เช่น หากโปรแกรมนี้เป็นสกรีนเซฟเวอร์ก็อาจจะทำการล็อกหน้าจอได้เองทั้งๆ ที่ผู้ใช้งานเองไม่ได้ปรับแต่งค่าให้ล็อก เป็นต้น

อย่างไรก็ตาม โปรแกรมนี้อาจทำอันตรายได้ในบางกรณี เช่น เมื่อทำการล็อกหน้าจอแต่ไม่ปลดล็อกให้ ดังนั้น อาจจะต้องปิดเครื่องคอมพิวเตอร์โดยที่ไม่ได้บันทึกงานไว้ก่อน ทำให้เกิดความเสียหายต่อผู้ใช้งานได้ เป็นต้น ตัวอย่างของโปรแกรมประเภทนี้ เช่น Joke.Train เป็นต้น

13) ฟลัดเดอร์ (Flooders)

แฮกเกอร์จะใช้โปรแกรมประเภทนี้ในการโจมตีระบบเครือข่ายเป้าหมายด้วยการส่งข้อมูลในปริมาณมหาศาลเพื่อทำให้เกิดความคับคั่งในระบบเครือข่าย ส่งผลให้เครือข่ายเป้าหมายไม่สามารถให้บริการต่อไปได้ เรียกการโจมตีประเภทนี้ว่า Denial of Service (DoS) ถ้าหากว่ามีเครื่องคอมพิวเตอร์ที่ถูกควบคุมและจะถูกใช้โจมตีแบบ DoS พร้อมกันหลายๆ เครื่องไปยังเป้าหมายเดียวกัน จะเรียกการโจมตีแบบนี้ว่า Distributed Denial of Service (DDoS)

14) รูทคิท (Rootkits)

รูทคิท เป็นชุดโปรแกรมเจาะระบบแบบพิเศษที่มักจะถูกใช้หลังจากแฮกเกอร์สามารถเจาะระบบเข้าไปได้สิทธิการควบคุมระบบนั้น จากนั้นก็จะติดตั้งโปรแกรมประเภทนี้โดยการดัดแปลงโปรแกรมใช้งานปกติหรือ Kernel ที่ถูกติดตั้งไว้อยู่แล้ว เพื่อหลอกให้ผู้ดูแลระบบ ไม่ให้สังเกตเห็นไฟล์ผิดปกติที่ถูกสร้างโดยแฮกเกอร์ มีการทำงานอยู่สองแบบคือ User-Mode และ Kernel-Mode ตัวอย่างรูทคิท เช่น Adore เป็นต้น

3. อาการที่แสดงว่าเครื่องอาจโดนโปรแกรมอันตราย

1) ใช้เวลานานผิดปกติในการเปิดเครื่อง หรือเรียกโปรแกรมขึ้นมาทำงาน
2) ขนาดของโปรแกรม หรือ วันเวลาของโปรแกรมเปลี่ยนไป
3) ข้อความที่ปกติไม่ค่อยได้เห็นกลับถูกแสดงขึ้นมาบ่อยๆ
4) เกิดอักษรหรือข้อความประหลาดบนหน้าจอ
5) เครื่องส่งเสียงออกทางลำโพงโดยไม่ได้เกิดจากโปรแกรมที่ใช้งานอยู่
6) แป้นพิมพ์ทำงานผิดปกติหรือไม่ทำงานเลย
7) ไฟแสดงสถานะการทำงานของดิสก์ติดค้างนานกว่าที่เคยเป็น
8) ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้งานสูญหายไป
9) เครื่องบูทตัวเองโดยไม่ได้สั่ง หรือ หยุดทำงานโดยไม่ทราบสาเหตุ
10) มีหน้าต่างปรากฏขึ้นมาบ่อยครั้งที่เปิดดูเว็บไซต์
11) ทูลบาร์ (Tools bar) แถบปุ่มเครื่องมือเพิ่มขึ้น
12) หน้าจอมีไอคอน (Icon) ประหลาดๆ เพิ่มขึ้น
13) เมื่อเปิดเว็บบราวเซอร์ หน้าเว็บแรกที่ปรากฏจะเป็นเว็บที่ไม่เคยเห็นมาก่อน
14) สร้างความรำคาญ โดยการเปิดหน้าเว็บโฆษณาอยู่ตลอดเวลา

4. การป้องกันภัยจากโปรแกรมอันตราย

1) เลือกใช้บริการข้อมูลหรือดาวน์โหลดไฟล์จากแหล่งที่น่าเชื่อถือเท่านั้น
2) ระมัดระวังการเปิดอีเมลหรือไฟล์จากสื่อบันทึกข้อมูลต่างๆ โดยเฉพาะที่มาจากคนที่ไม่รู้จัก
3) หลีกเลี่ยงการใช้แผ่นดิสก์ ซีดี ทรัมป์ไดรว์ จากแหล่งไม่น่าเชื่อถือ หรือไม่ใช้ร่วมกับบุคคลอื่น ควรมีการตรวจเช็คไวรัสและโปรแกรมอันตรายก่อนใช้งานทุกครั้ง
4) ติดตั้งโปรแกรมป้องกันภัยให้เหมาะสม เช่น AntiVirus , Anti Spyware/ Adware ฯลฯ และมีการอัพเดทฐานข้อมูลไวรัสและโปรแกรมอันตรายใหม่ๆ อย่างสม่ำเสมอ ซึ่งโปรแกรมป้องกันภัยมีทั้งแบบที่ต้องเสียเงินซื้อ และแบบที่ใช้ฟรีถาวร (Freeware) หรือใช้ฟรีภ ายในระยะเวลาที่กำหนด (Shareware)

5. วิธีป้องกันภัยคุกคามทางอินเทอร์เน็ต

1) การตั้งสติก่อนเปิดเครื่อง ต้องรู้ตัวก่อนเสมอว่าเราอยู่ที่ไหนที่นั่นปลอดภัยเพียงใด
2) ก่อน login เข้าใช้งานคอมพิวเตอร์ต้องมั่นใจว่าไม่มีใครแอบดูรหัสผ่านของเรา
3) เมื่อไม่ได้อยู่หน้าจอคอมพิวเตอร์ ควรล็อกหน้าจอให้อยู่ในสถานะที่ต้องใส่ค่า login
4) ตระหนักอยู่เสมอว่าข้อมูลความลับและความเป็นส่วนตัวอาจถูกเปิดเผยได้เสมอในโลกออนไลน์
5) การกำหนด password ที่ยากแก่การคาดเดา ควรมีความยาวไม่ต่ำกว่า 8 ตัวอักษร และใช้อักขระพิเศษไม่ตรงกับความหมายในพจนานุกรม เพื่อให้เดาได้ยากมากขึ้นและการใช้งานอินเทอร์เน็ตทั่วไป เช่นการ Login ระบบ e-mail , ระบบสนทนาออนไลน์ (chat) , ระบบเว็บไซต์ที่เป็นสมาชิกอยู่ทางที่ดีควรใช้ password ที่ต่างกันบ้างพอให้จำได้
6) การสังเกตขณะเปิดเครื่องว่ามีโปรแกรมไม่พึงประสงค์ถูกเรียกใช้ขึ้นมาพร้อมๆ กับการเปิดเครื่องหรือไม่ ถ้าสังเกตไม่ทันให้สังเกตระยะเวลาบูทเครื่อง หากนานผิดปกติอาจเป็นไปได้ว่าเครื่องคอมพิวเตอร์ติดปัญหาจากไวรัส หรือภัยคุกคามรูปแบบต่างๆ ได้
7) การหมั่นตรวจสอบและอัพเดท OS หรือซอฟต์แวร์ที่ใช้ให้เป็นปัจจุบัน โดยเฉพาะโปรแกรมป้องกันภัยในเครื่องคอมพิวเตอร์ เช่น โปรแกรมป้องกันไวรัส, โปรแกรมไฟร์วอลล์ และควรใช้ระบบปฏิบัติการและซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย นอกจากนี้ควรอัพเดทอินเทอร์เน็ตบราวเซอร์ให้ทันสมัยอยู่เสมอ
8) ไม่ลงซอฟต์แวร์มากเกินความจำเป็น
   8.1) ซอฟต์แวร์ที่จำเป็นต้องลงในเครื่องคอมพิวเตอร์ ได้แก่
   - อินเทอร์เน็ตบราวเซอร์ เพื่อให้เปิดเว็บไซต์ต่างๆ
   - อีเมลเพื่อใช้รับส่งข้อมูลและติดต่อสื่อสาร
   - โปรแกรมสำหรับงานด้านเอกสาร, โปรแกรมตกแต่งภาพ เสียง วีดีโอ
   - โปรแกรมป้องกันไวรัสคอมพิวเตอร์และโปรแกรมไฟร์วอลล์

8.2) ซอฟต์แวร์ที่ไม่ควรมีบนเครื่องคอมพิวเตอร์ที่ใช้งาน ได้แก่

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

9) ไม่ควรเข้าเว็บไซต์เสี่ยงภัยเว็บไซต์ประเภทนี้ ได้แก่

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

10) สังเกตความปลอดภัยของเว็บไซต์ที่ให้บริการธุรกรรมออนไลน์ เว็บไซต์ E-Commerce ที่ปลอดภัยควรมีการทำ HTTPS มีใบรับรองทางอิเล็กทรอนิกส์และมีมาตรฐานรองรับ

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

12) ศึกษาถึงข้อกฎหมายเกี่ยวกับการใช้สื่ออินเทอร์เน็ต ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยมีหลักการง่ายๆ ที่จะช่วยให้สังคมออนไลน์สงบสุข คือให้คำนึงถึงใจเขาใจเรา ไม่หลงเชื่อโดยง่าย อย่าเชื่อในสิ่งที่เห็น และงมงายกับข้อมูลบนอินเทอร์เน็ต ควรหมั่นศึกษาหาความรู้จากเทคโนโลยีอินเทอร์เน็ต และศึกษาข้อมูลให้รอบด้าน ก่อนปักใจเชื่อในสิ่งที่ได้รับรู้

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"ผู้ให้บริการ" หมายความว่า

(1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

"ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา 5 ผู้ใดเข้าถึงโดยมิชอบซึ่ง**ระบบคอมพิวเตอร์**ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 6 ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึง**ระบบคอมพิวเตอร์**ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่ง**ข้อมูลคอมพิวเตอร์**ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 8 ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่ง**ข้อมูลคอมพิวเตอร์**ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้น มิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกิน สามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 9 ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมด หรือบางส่วน ซึ่ง**ข้อมูลคอมพิวเตอร์**ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 10 ผู้ใดกระทำด้วยประการใดโดยมิชอบเพื่อให้การทำงานของ**ระบบคอมพิวเตอร์**ของผู้อื่น ถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุก ไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำ

มาตรา 11 ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของ บุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา 12 ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10

(1) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันที หรือในภายหลัง และไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปีและปรับไม่เกินสองแสนบาท

(2) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง ในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

มาตรา 13 ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือ ในการกระทำความผิดตามมาตรา ถ มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

ทั้งปรับ

มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิด ความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

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

มาตรา 15 ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มี การกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

มาตรา 16 ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา 17 ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(1) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทย หรือคนไทยเป็นผู้เสียหาย และผู้เสียหายได้ร้องขอให้ลงโทษ

จะต้องรับโทษภายในราชอาณาจักร

หมวด 2 พนักงานเจ้าหน้าที่

มาตรา 18 ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจง เป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูล คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูล คอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็น เฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่ง

มาตรา 19 การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ (8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิดเท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็วเมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา 18 (4) (5) (6) (7) และ (8) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือ ผู้ครอบครองดังกล่าวในทันทีที่กระทำได้ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา 18 (4) (5) (6) (7) และ (8) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน การทำสำเนาข้อมูล คอมพิวเตอร์ตามมาตรา 18 (4) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น การยึดหรืออายัดตามมาตรา 18 (8) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน หนังสือแสดงการยึดหรือ

ความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

มาตรา 20 ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสองลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้อง พร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้ ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

มาตรา 21 ในกรณีที่พนักงานเจ้าหน้าที่พบว่าข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติมขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวงทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

อายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา 22 ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา 18 ให้แก่บุคคลใดความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบหรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาลพนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 23 พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา 18 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 24 ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา 18 และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 25 ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจมีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใดให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา 27 ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา 18 หรือมาตรา 20 หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา 21 ต้องระวางโทษปรับไม่เกินสองแสนบาทและปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรา 28 การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา 29 ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้ ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป ให้นายก รัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา 30 ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

สรุปแบบแยกบทลงโทษตามมาตรา

มาตรา	โทษปรับ	โทษจำคุก
มาตรา 5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน	<=10,000	<=6เดือน
มาตรา 6 ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น	<=20,000	<=1ปี
มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน	<=40,000	<=2ปี
มาตรา 8 ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้	<=60,000	<=3ปี
มาตรา 9 ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมด หรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ	<=100,000	<=5ปี
มาตรา 10 ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่น ถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้	<=100,000	<=5ปี
มาตรา 11 ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของ บุคคลอื่นโดยปกติสุข	<=100,000	-
มาตรา 12 ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10 (1) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันที หรือในภายหลัง และไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่	<=200,000	<=10ปี
(2) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบ คอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง ในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ	60,000 - 300,000	3 - 5 ปี

มาตรา	โทษปรับ	โทษจำคุก
ถ้าการกระทำความผิดตาม (2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย	-	10 - 20 ปี
มาตรา 13 ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือ ในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11	<=20,000	<=1ปี
มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ (1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน (2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิด ความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน (3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา (4) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้ (5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ(4)	<=100,000	<=5ปี
มาตรา 15 ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มี การกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตาม มาตรา 14	<=100,000	<=5ปี
มาตรา 16 ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูล คอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้น เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้ ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้และให้ถือว่าเป็นผู้เสียหาย	<=60,000	<=3ปี

มาตรา	โทษปรับ	โทษจำคุก
มาตรา 17 ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ (1) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้น หรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ (2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหาย และผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร	จะต้องรับโทษภายในราชอาณาจักร	

รูปแบบและลักษณะของความผิดที่ได้กระทำต่อคอมพิวเตอร์โดยแท้ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

1. การเข้าถึงโดยมิชอบ ตามมาตรา 5 และมาตรา 7

การกระทำความผิดฐานเข้าถึงโดยมิชอบหรือโดยฝ่าฝืนต่อบทบัญญัติแห่งกฎหมายนี้ อาจเกิดขึ้นได้หลายวิธี เช่น การเจาะระบบ (hacking or cracking) หรือการบุกรุกทางคอมพิวเตอร์ (computer trespass) เพื่อทำลายระบบคอมพิวเตอร์หรือเปลี่ยนแปลงแก้ไขข้อมูลหรือการเข้าถึงข้อมูลที่เก็บรักษาไว้เป็นความลับ (secret) การส่งชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจัน (Trojan Horses) สปายแวร์ (spyware) ผ่านช่องโหว่ต่างๆ โดยเข้าไปฝังตัวในระบบคอมพิวเตอร์เพื่อขโมยข้อมูลรหัสผ่านหรือข้อมูลส่วนบุคคลของผู้อื่นเพื่อใช้บุกรุกเข้าไปในระบบคอมพิวเตอร์ของผู้นั้น หรือนำข้อมูลดังกล่าวไปก่ออาชญากรรมอื่นต่อไป เป็นต้น จนอาจเป็นที่มาของการกระทำความผิดฐานอื่นและอาจก่อให้เกิดความเสียหายต่อเนื่องเป็นมูลค่ามหาศาล ซึ่งสามารถเรียกวิธีการเข้าถึงประเภทนี้ว่า “การเข้าถึงทางอิเล็กทรอนิกส์ หรือ การเข้าถึงทางดิจิทัล” ซึ่งอาจเป็นการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ไม่ว่าทั้งหมดหรือแต่บางส่วนก็ได้ เช่น การเข้าถึงฮาร์ดแวร์ซึ่งเป็นส่วนประกอบต่างๆ ของคอมพิวเตอร์หรือข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง หรือข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น นอกจากนี้ยังหมายความรวมถึงการเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์ที่แม้ว่าตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้ไม่ว่าจะเข้าถึงนั้นจะผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เป็นต้น หรือโดยผ่านทางระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบ LAN (Local Area Network หมายถึง เครือข่ายคอมพิวเตอร์โดยการเชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้เคียงเข้าด้วยกัน) เป็นต้น

นอกจากจะมีการเข้าถึงทางอิเล็กทรอนิกส์แล้ว หากพิจารณาถึงความหมายและเจตนารมณ์ของกฎหมายแล้ว ย่อมหมายความรวมถึง "การเข้าถึงในระดับกายภาพ" ด้วย เช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์ แล้วผู้กระทำผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้น เป็นต้น

อย่างไรก็ตาม ยังมีประเด็นที่ต้องพิจารณาเกี่ยวกับการกระทำความผิดฐานนี้อีกว่า หากเพียงแค่มีการเข้าถึงโดยไม่ได้รับอนุญาตจะถือว่าเป็นการก่ออาชญากรรมได้หรือไม่ หรือผู้กระทำจะต้องมีมูลเหตุจูงใจที่จะกระทำให้เกิดความเสียหายด้วยจึงจะถือเป็นการก่ออาชญากรรม เช่น บุคคลซึ่งมิได้มีมูลเหตุจูงใจดังกล่าวแต่มีความอยากรู้อยากเห็นหรืออยากทดลอง จึงทดลองเจาะระบบคอมพิวเตอร์ของผู้อื่นโดยมิได้มีมูลเหตุจูงใจที่จะก่อให้เกิดความเสียหาย กรณีดังกล่าวควรกำหนดให้ต้องรับผิดและมีบทลงโทษหรือไม่ และกรณีที่มีการเข้าถึงแม้โดยไม่มีมูลเหตุจูงใจที่จะก่อให้เกิดความเสียหาย เช่น การเข้าไปในระบบคอมพิวเตอร์ของสายการบินแล้วทำการเปลี่ยนแปลงระบบจองตั๋วเครื่องบินและสลับตารางการบินของลูกค้าที่จองไว้ จนเกิดความเสียหายต่อสายการบินและตัวลูกค้า กรณีดังกล่าวนี้จะกำหนดขอบเขตในการพิจารณาว่าเป็นความผิดอย่างไร เป็นต้น

ประเด็นนี้มีนักกฎหมายเห็นว่า....[1] การเข้าถึงโดยมิชอบตามมาตรา 5 และมาตรา 7 นี้ ถือเป็นความผิดในตัวเอง (mala inse) กล่าวคือ แม้ว่าผู้กระทำจะมิได้มีมูลเหตุจูงใจเพื่อก่อให้เกิดความเสียหาย หรือการกระทำดังกล่าวจะยังมิได้ก่อให้เกิดความเสียหายก็ตาม ทั้งนี้ เพราะเห็นว่าการกระทำดังกล่าวนั้นสามารถก่อให้เกิดการกระทำผิดฐานอื่นหรือฐานที่ใกล้เคียงค่อนข้างง่ายและอาจก่อให้เกิดความเสียหายร้ายแรงทั้งการพิสูจน์มูลเหตุจูงใจทำได้ค่อนข้างยาก และที่สำคัญจะต้องเป็นการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีวิธีการป้องกันการเข้าถึงโดยเฉพาะจึงจะถือเป็นความผิด

[1] แนวทางการจัดทำกฎหมายอาชญากรรมคอมพิวเตอร์, ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค), พ.ศ.2546 หน้า 22

2. การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะโดยมิชอบ ตามมาตรา 6

การล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ไม่ว่าจะล่วงรู้โดยชอบหรือมิชอบก็ตาม ตัวอย่างการล่วงรู้โดยมิชอบ เช่น การใช้ชุดคำสั่งไม่พึงประสงค์ประเภทโปรแกรมดักข้อมูลผ่านปุ่มคีย์บอร์ด (Keylogger หรือ Keystroker) แอบบันทึกการกดรหัสผ่านของผู้อื่นแล้วนำไปเปิดเผยต่อ เป็นต้น เพียงแค่นี้ก็ถือว่าเป็นการนำมาตรการป้องกันหรือรหัสผ่านนั้นไปเปิดเผยโดยมิชอบซึ่งเข้าองค์ประกอบของความผิดฐานนี้แล้ว ไม่ว่าบุคคลที่สามซึ่งล่วงรู้มาตรการป้องกันหรือรหัสผ่านนั้นจะนำไปใช้เพื่อเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นหรือไม่ก็ตาม

3. การดักรับข้อมูลคอมพิวเตอร์โดยมิชอบ ตามมาตรา 8

ในปัจจุบันข้อมูลได้ถูกจัดเก็บในรูปแบบอิเล็กทรอนิกส์และมีการโอนข้อมูลทางอิเล็กทรอนิกส์กันมากขึ้น โอกาสที่จะถูกดักรับหรือล่วงรู้ข้อมูลนั้นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์จึงมีมากขึ้นตามไปด้วย ดังนั้น การลักลอบดักข้อมูลโดยฝ่าฝืนกฎหมาย (Illegal interception) จึงเป็นปัญหาสำคัญอีกปัญหาหนึ่งที่อาจส่งผลกระทบต่อความเป็นส่วนตัวในการติดต่อสื่อสาร (the right of privacy of data communication) ของประชาชนในทำนองเดียวกับการให้ความคุ้มครองสิทธิความเป็นส่วนตัวในการติดต่อสื่อสารรูปแบบเดิมที่ห้ามดักฟังโทรศัพท์ การลักลอบดักข้อมูลในที่นี้หมายถึงการลักลอบดักข้อมูลโดยใช้วิธีการทางเทคนิค (technical means) เพื่อลักลอบดักฟัง ตรวจสอบหรือติดตามเนื้อหาสาระของข้อมูลข่าวสารที่สื่อสารถึงกันระหว่างบุคคล หรือกรณีเป็นการกระทำอันเป็นการล่อลวงหรือจัดหาข้อมูลดังกล่าวให้กับบุคคลอื่นรวมทั้งการแอบบันทึกข้อมูลที่สื่อสารถึงกันนั้นด้วย ตัวอย่าง เช่น การใช้ชุดคำสั่งไม่พึงประสงค์ประเภทสนิฟเฟอร์ (sniffer) แอบดักแพ็คเกต (packet) ซึ่งเป็นชุดของข้อมูลที่เล็กที่สุดที่อยู่ระหว่างการส่งไปให้ผู้รับ เป็นต้น ทั้งนี้ วิธีการทางเทคนิคก็หมายถึงอุปกรณ์ที่มีสายเชื่อมต่อกับระบบเครือข่ายต่างๆ และหมายรวมถึงอุปกรณ์ประเภทไร้สายด้วย เช่น การติดต่อผ่านทางโทรศัพท์มือถือหรืออุปกรณ์ชนิดพกพาต่างๆ เป็นต้น อย่างไรก็ตามการกระทำที่จะถือเป็นความผิดฐานลักลอบดักข้อมูลนั้น ข้อมูลที่ส่งจะต้องมิใช่ข้อมูลที่อาจเปิดเผยให้สาธารณชนสามารถรับรู้ได้ (non-public transmissions) การกระทำความผิดฐานนี้จึงจำกัดเฉพาะแต่เพียงวิธีการส่งที่ผู้ส่งข้อมูลประสงค์จะส่งข้อมูลนั้นให้แก่บุคคลหนึ่งบุคคลใดโดยเฉพาะเจาะจงเท่านั้นจึงจะได้รับ

ความคุ้มครองแม้จะเป็นการส่งข้อมูลผ่านทางเครือข่ายสาธารณอย่างอินเทอร์เน็ตก็ตาม ดังนั้น จึงไม่ต้องพิจารณาถึงเนื้อหาสาระของข้อมูลที่ส่งด้วยแต่อย่างใด เพราะเนื้อหาสาระของข้อมูลที่ส่งนั้นอาจมีเนื้อหาสาระที่หาได้โดยทั่วไปหรือมีอยู่ทั่วไป รวมทั้งข้อมูลที่เป็นความลับทางการค้า หรือเป็นข้อมูลส่วนบุคคลที่เจ้าของข้อมูลประสงค์จะปกปิดเป็นความลับก็ได้

อนึ่ง หากพิจารณาถึงลักษณะหรือพฤติการณ์แห่งการกระทำความผิดฐานลักลอบดักรับข้อมูลคอมพิวเตอร์และฐานเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบแล้ว จะเห็นได้ว่าความผิดทั้งสองฐานดังกล่าวมีลักษณะหรือพฤติการณ์แห่งการกระทำที่ใกล้เคียงกันอย่างยิ่ง แต่มีความแตกต่างกันที่เจตนาภายใน กล่าวคือ การกระทำความผิดฐานลักลอบดักรับข้อมูลต้องเป็นการกระทำโดยมีมูลเหตุจูงใจเพื่อให้ได้มาซึ่งข้อมูลคอมพิวเตอร์ ส่วนการกระทำความผิดฐานเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบนั้น แม้จะกระทำโดยมิได้มีเจตนาหรือมีมูลเหตุจูงใจหรือมิได้ประสงค์ต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ใดโดยเฉพาะเจาะจง และแม้จะมิได้มีความเสียหายใดๆ เกิดขึ้น ผู้กระทำก็ต้องรับผิดในการกระทำดังกล่าว

4. การรบกวนข้อมูลคอมพิวเตอร์และรบกวนระบบคอมพิวเตอร์ ตามมาตรา 9 และมาตรา 10

ความผิดฐานรบกวนหมายถึงการรบกวนข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์โดยจงใจก่อให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมทั้งระบบคอมพิวเตอร์และระบบการสื่อสารด้วย ทั้งนี้ประโยชน์ที่กฎหมายมุ่งประสงค์จะคุ้มครองคือ ความครบถ้วนสมบูรณ์ของข้อมูลและเสถียรภาพในการใช้งานหรือการใช้ข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่บันทึกเก็บไว้บนสื่อคอมพิวเตอร์ได้เป็นไปโดยปกติสุข โดยไม่ต้องการให้มีการทำให้เสียหาย หรือทำให้ข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์เสื่อมค่าหรือไร้ประโยชน์ รวมถึงการลบหรือทำลายข้อมูลคอมพิวเตอร์ หรือกระทำการใดๆ ให้ไม่สามารถเข้าถึงข้อมูลคอมพิวเตอร์หรือใช้โปรแกรมคอมพิวเตอร์นั้นได้รวมทั้งการเปลี่ยนแปลงข้อมูลใดๆ ที่มีอยู่ด้วย

ตัวอย่างของการกระทำความผิดในฐานนี้ ได้แก่ การป้อนโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ เช่น ไวรัส เพื่อทำลายข้อมูลคอมพิวเตอร์ หรือการป้อน

ชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันเข้าไปในระบบเพื่อขโมยรหัสผ่านของผู้ใช้คอมพิวเตอร์ สำหรับนำไปใช้ในการกระทำความผิดอื่นต่อไป เช่น การนำรหัสผ่านที่เกี่ยวกับธุรกรรมทางการเงินบนอินเทอร์เน็ตหรืออินเทอร์เน็ตแบงก์กิ้งของผู้ใช้คอมพิวเตอร์ไปก่ออาชญากรรมทางการเงิน หรือ การเข้าไปลบ เปลี่ยนแปลงแก้ไขข้อมูลหรือกระทำการใดๆ อันเป็นการรบกวนข้อมูลคอมพิวเตอร์ เป็นต้น นอกจากนั้น กฎหมายยังมุ่งคุ้มครองการทำงานของระบบคอมพิวเตอร์และระบบการติดต่อสื่อสารให้เป็นไปตามปกติสุขซึ่งรูปแบบหรือวิธีการรบกวนหรือขัดขวางหรือทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้เป็นปกติสุขนั้นอาจเกิดขึ้นได้ในขั้นตอนต่างๆ ตั้งแต่การป้อนข้อมูลเข้าไปในระบบหรือในการส่ง ทำลาย ลบ หรือเปลี่ยนแปลงแก้ไขข้อมูลคอมพิวเตอร์ ซึ่งผลของการกระทำจะก่อให้เกิดความเสียหายที่ร้ายแรงหรือรุนแรงต่อการใช้ระบบดังกล่าวหรือต่อการติดต่อสื่อสารกับระบบอื่น เช่น การโจมตีจากชุดคำสั่งไม่พึงประสงค์เพื่อทำให้ระบบทำงานหนักและปฏิเสธการทำงาน (Denial of service) หรือทำให้ระบบทำงานช้าลง เป็นต้น

5. การรบกวนการใช้ระบบคอมพิวเตอร์โดยปกติสุข ตามมาตรา 11

การรบกวนการใช้งานระบบคอมพิวเตอร์โดยปกติสุขในที่นี้ก็คือ การทำสแปมเมล (Spam Mail) ซึ่งเป็นรูปแบบการโจมตีระบบคอมพิวเตอร์ด้วยการใช้โปรแกรมสำหรับส่งสแปม (Spammer Programs) ส่งข้อความในลักษณะของการชักจูงหรือโฆษณาไปยังกลุ่มผู้รับต่างๆ เป็นจำนวนมหาศาลผ่านทางอีเมลหรือโปรแกรมสนทนา (Instant Messaging) รวมทั้งอีเมลและ SMS ในโทรศัพท์มือถือโดยปกปิดแหล่งที่มา เช่น ไม่ปรากฏหมายเลข IP address หรือชื่อของผู้ส่งไม่ว่าจะเป็นชื่อเล่นหรือชื่อจริง เป็นต้น ซึ่งการโจมตีของพวกสแปมเมอร์นี้จึงไม่ใช่ปัญหาเล็กๆ ที่เป็นแค่ทำให้เกิดความรำคาญแก่ผู้ใช้คอมพิวเตอร์ทั่วไป แต่กำลังกลายเป็นปัญหาใหญ่ที่ส่งผลกระทบและสร้างความเสียหายในเชิงเศรษฐกิจ กล่าวคือ สแปมเมลมักก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการใช้ทรัพยากรของระบบคอมพิวเตอร์ รวมทั้งระบบคอมพิวเตอร์และระบบการสื่อสาร จนอาจต้องเสียค่าใช้จ่ายในการซื้อซอฟต์แวร์สำหรับใช้กำจัดสแปมเมล หรืออาจถึงขั้นทำให้เครื่องเมลเซิร์ฟเวอร์ (เครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่ในการให้บริการจดหมายอิเล็กทรอนิกส์) ของฝ่ายผู้รับอีเมลต้องทำงานหนักจนไม่สามารถทำงานต่อไปได้และหยุดให้บริการในที่สุดซึ่งมักจะมีค่าใช้จ่ายในการซ่อมแซมหรือการดูแลรักษาตามมา ทั้งนี้ โดยภาพรวมแล้วโปรแกรมสำหรับส่งสแปมเมลดังกล่าว

ถือเป็นชุดคำสั่งไม่พึงประสงค์อีกประเภทหนึ่งด้วย เพราะการส่งอีเมลจำนวนมากๆ ในคราวเดียวกันหรือต่อเนื่องกันเป็นจำนวนมหาศาลนั้นมนุษย์คงไม่สามารถกระทำได้ จึงต้องใช้โปรแกรมสำหรับส่งสแปมเป็นเครื่องมือพิเศษช่วยในการส่งดังกล่าว

อย่างไรก็ตาม มีข้อน่าสังเกตว่า ผลกระทบจากการรบกวนด้วยการทำ สแปมเมลที่ถึงขั้นทำให้เครื่องเมลเซิร์ฟเวอร์ของฝ่ายผู้รับอีเมลต้องทำงานหนักจนไม่สามารถทำงานต่อไปได้และหยุดให้บริการในที่สุดนั้น อาจคล้ายคลึงกับการรบกวนข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ ตามมาตรา 9 และ มาตรา 10 แต่แตกต่างกันที่วิธีการ เจตนา และการประสงค์ต่อผลหรือย่อมเล็งเห็นผลของการกระทำ กล่าวคือ ในการส่งสแปมเมลนั้นผู้ส่งอีเมลอาจเพียงแต่ต้องการก่อให้เกิดความรำคาญแก่ผู้รับอีเมลหรือต้องการโฆษณาเชิญชวนเพื่อให้ทำการอย่างใดอย่างหนึ่งหรือหลอกให้ตกเป็นเหยื่อเท่านั้น แต่หากผลที่เกิดจากการกระทำนั้นถึงขั้นที่ทำให้เครื่องเมลเซิร์ฟเวอร์ของฝ่ายผู้รับอีเมลไม่สามารถทำงานต่อไปได้และหยุดให้บริการนั้น ย่อมเป็นการทำให้ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ของเครื่องเมลเซิร์ฟเวอร์ฝ่ายผู้รับอีเมลได้รับความเสียหายและเข้าข่ายเป็นการรบกวนข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ด้วย

6. การรบกวนระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่ก่อให้เกิดความเสียหายต่อประชาชนหรือสาธารณะ ตามมาตรา 12

การรบกวนระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่ก่อให้เกิดความเสียหายต่อประชาชนหรือกระทบต่อความมั่นคงของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจ และการบริการสาธารณะ ตามมาตรา 12 นี้ ปัจจุบันเป็นปัญหาการกระทำความผิดทางคอมพิวเตอร์ที่ประเทศส่วนใหญ่วิตกกังวล กล่าวคือ การใช้โปรแกรมหรือชุดคำสั่งเจาะเข้าไปในระบบคอมพิวเตอร์และแอบเติมหรือทำลายข้อมูลคอมพิวเตอร์ หรือแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ อันอาจส่งผลกระทบต่อระบบสาธารณูปโภคหรือระบบการเงินของประเทศ หรือแม้กระทั่งเป็นที่มาของการทำสงครามข้อมูลข่าวสาร (Information Warfare) ที่กำลังเกิดขึ้นกับสังคมไทยอยู่ในปัจจุบันโดยผ่านทางโปรแกรมเครือข่ายสังคมออนไลน์อย่าง Facebook เป็นต้น

รูปแบบและลักษณะของความผิดเกี่ยวกับคอมพิวเตอร์

เมื่อได้ทราบถึงรูปแบบและลักษณะของความผิดที่ได้กระทำต่อคอมพิวเตอร์โดยแท้ไปแล้ว ต่อไปนี้จะเป็นการกล่าวถึงรูปแบบและลักษณะของความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งผู้กระทำความผิดหรืออาชญากรได้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์เป็นเครื่องมือหรือเป็นปัจจัยในการกระทำความผิด โดยจะยึดถือตามหลักการและนัยแห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นสำคัญเช่นกัน ได้แก่

การนำเข้าหรือเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะที่ไม่เหมาะสม ตามมาตรา 14 และมาตรา 15

การนำเข้าข้อมูลคอมพิวเตอร์ตามมาตรา 14 และมาตรา 15 นี้ เป็นลักษณะอันเกิดจากการนำเข้าข้อมูลคอมพิวเตอร์ที่เป็นเท็จหรือมีเนื้อหาไม่เหมาะสมในรูปแบบต่างๆ โดยในมาตรา 14 นั้น กำหนดไว้ให้ครอบคลุมทั้งการปลอมแปลงข้อมูลคอมพิวเตอร์หรือทำข้อมูลคอมพิวเตอร์อันเป็นเท็จ หรือก่อให้เกิดความเสียหายหรือก่อให้เกิดความตื่นตระหนกกับประชาชน หรือเนื้อความที่กระทบต่อความมั่นคงของประเทศหรือการก่อการร้าย รวมทั้งข้อมูลคอมพิวเตอร์อันลามกทั้งหลาย และรวมถึงการส่งข้อมูลที่ได้รับให้ผู้อื่นอีกทอดหนึ่งด้วย อย่างไรก็ตาม นอกจากการกำหนดโทษสำหรับผู้กระทำความผิดตามมาตรา 14 แล้ว ยังมีการกำหนดโทษของผู้ให้บริการที่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ไว้ในในมาตรา 15 ด้วย โดยผู้ให้บริการที่สนับสนุนหรือให้ความยินยอมดังกล่าวต้องรับโทษเช่นเดียวกับผู้กระทำความผิดด้วย โดยท่านอาจารย์พรเพชร วิชิตชลชัย ได้ให้คำอธิบายเกี่ยวกับองค์ประกอบของฐานความผิดทั้งสองมาตราดังกล่าว ดังนี้

> ***มาตรา 14*** *ผู้ใดกระทำด้วยประการใดๆ ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ*
>
> *(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน*

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็น ความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิด เกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะ อันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็น ข้อมูลคอมพิวเตอร์ ตาม (1) (2) (3) หรือ (4)

ปกติแล้วความผิดเกี่ยวกับคอมพิวเตอร์จะหมายความเฉพาะความผิดที่กระทำต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ดังที่บัญญัติไว้ในมาตราก่อนหน้านี้ อย่างไรก็ตาม คอมพิวเตอร์หรือระบบคอมพิวเตอร์อาจถูกใช้เป็นเครื่องมือในการประกอบอาชญากรรมได้แทบทุกประเภท ที่เห็นได้ชัดเจนก็คือความผิดฐาน ดูหมิ่น หมิ่นประมาทหรือเผยแพร่ภาพลามก ซึ่งการกระทำความผิดเหล่านั้นก็จำต้องพิจารณาจากองค์ประกอบความผิดสำหรับความผิดนั้นๆ เช่น พิจารณาบทบัญญัติจากบทบัญญัติของประมวลกฎหมายอาญา เป็นต้น

ถึงแม้ว่าการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดจะเป็นความผิดตามกฎหมายอื่นอยู่แล้ว แต่ผู้ร่างกฎหมายคงเห็นว่ามีความผิดหลายลักษณะที่ควรบัญญัติเป็นความผิดตามพระราชบัญญัตินี้อีกประการหนึ่ง จึงได้บัญญัติมาตรา 14 โดยมีองค์ประกอบความผิดที่สำคัญคือ “นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์” การกระทำผิดตามมาตรานี้จึงต้องพิจารณาว่าอาจเป็นความผิดตามกฎหมายอื่นอีกด้วยหรือไม่ ความผิดตามมาตรา 14 มี 5 อนุมาตรา จึงเปรียบเสมือนการบัญญัติความผิดขึ้นมาอีก 5 ลักษณะ ดังนี้

1. *นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน*

ความผิดตามมาตรา 14 (1) มีองค์ประกอบความผิด ดังนี้

(1) นำเข้าสู่ระบบคอมพิวเตอร์

การนำเข้าสู่ หมายถึงการนำข้อมูลคอมพิวเตอร์หรือโปรแกรมซอฟต์แวร์ต่างๆ เข้าสู่ระบบคอมพิวเตอร์

(2) ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ

ข้อมูลคอมพิวเตอร์ปลอม หมายถึง ข้อมูลคอมพิวเตอร์ที่มีการเปลี่ยนแปลงแก้ไข ไม่ว่าการเปลี่ยนแปลงแก้ไขนั้นจะทั้งหมดหรือแต่เพียงบางส่วน ส่วนข้อมูลคอมพิวเตอร์เป็นเท็จนั้น น่าจะหมายถึงข้อมูลคอมพิวเตอร์ที่ไม่ใช่ของจริง เช่นข้อมูลคอมพิวเตอร์ที่ระบุว่าเป็นเครื่องมือป้องกันไวรัสของบริษัทหนึ่ง แต่แท้จริงแล้วไม่ใช่ เป็นต้น

(3) โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

องค์ประกอบความผิดนี้มีใช้อยู่ในความผิดตามประมวลกฎหมายอาญาหลายฐานความผิด เช่น ความผิดฐานปลอมเอกสารตามมาตรา 264 หรือความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ตามมาตรา 269/1 องค์ประกอบนี้ไม่ใช่เจตนาพิเศษของผู้กระทำ แต่เป็นเรื่องที่จะต้องพิจารณาจากลักษณะของการกระทำในเรื่องของเจตนาด้วย

(4) เจตนาตามประมวลกฎหมายอาญา มาตรา 59

เจตนาในที่นี้ต้องครอบคลุมองค์ประกอบทั้ง 3 ประการข้างต้นกล่าวคือ ผู้กระทำต้องมีเจตนานำเข้าสู่ระบบคอมพิวเตอร์ ในขณะเดียวกันผู้กระทำต้องรู้ถึงข้อเท็จจริงในองค์ประกอบความผิดว่าเป็นข้อมูลคอมพิวเตอร์ปลอมหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จและต้องรู้ว่าการกระทำดังกล่าวเป็นการกระทำที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

2. นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

ความผิดตามมาตรา 14 (2) มีองค์ประกอบความผิด ดังนี้

(1) นำเข้าสู่ระบบคอมพิวเตอร์

องค์ประกอบความผิดเดียวกันกับข้อ 14 (1)

(2) ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ

มาตรา 14 (2) เน้นที่ข้อมูลคอมพิวเตอร์อันเป็นเท็จ จึงไม่ใช่เรื่องที่ไปปลอมแปลงข้อมูลที่มีอยู่

(3) โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

ความจริงแล้วองค์ประกอบความผิดตามมาตรา 14 (2) ก็ใกล้เคียงและเกลื่อนกลืนกัน การกระทำที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน ก็น่าจะถือได้ว่าเข้าองค์ประกอบความผิดที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชนตามมาตรา 14 (1) อยู่แล้วด้วย

(4) เจตนาตามประมวลกฎหมายอาญา มาตรา 59

3. นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

ความผิดตามมาตรา 14 (3) มีองค์ประกอบความผิด ดังนี้

(1) นำเข้าสู่ระบบคอมพิวเตอร์

(2) ข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

องค์ประกอบความผิดข้อนี้พิจารณาจากลักษณะของข้อมูลคอมพิวเตอร์กล่าวคือเป็นข้อมูลคอมพิวเตอร์ที่ใช้กระทำความผิดเกี่ยวกับความมั่นคงแห่ง

ราชอาณาจักรตามประมวลกฎหมายอาญา มาตรา 107 ถึงมาตรา 135 หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา มาตรา 135/1 ถึงมาตรา 135/3

ความผิดตามมาตรา 14 (3) นี้จึงเป็นการบัญญัติเอาผิดเพิ่มขึ้นจากการกระทำซึ่งเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายโดยในการกระทำความผิดดังกล่าวได้ใช้วิธีการทางคอมพิวเตอร์นำข้อมูลคอมพิวเตอร์อันเป็นความผิดตามมาตราดังกล่าวเข้าสู่ระบบคอมพิวเตอร์ ดังนั้นการกระทำความผิดตามมาตรา 14 (3) นี้ผู้กระทำอาจต้องรับผิดตามประมวลกฎหมายอาญาตามบทมาตราที่กล่าวมาด้วย

(3) เจตนาตามประมวลกฎหมายอาญา มาตรา 59

ซึ่งหมายถึงเจตนาในการนำเข้าสู่ระบบคอมพิวเตอร์ตาม (1) และรู้ถึงข้อเท็จจริงอันเป็นองค์ประกอบความผิดตาม (2)

4. นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูล คอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

ความผิดตามมาตรา 14 (4) มีองค์ประกอบความผิด ดังนี้

(1) นำเข้าสู่ระบบคอมพิวเตอร์

(2) ข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

องค์ประกอบความผิดข้อนี้พิจารณาจากลักษณะของข้อมูลคอมพิวเตอร์เช่นกัน คือเป็นข้อมูลคอมพิวเตอร์ที่มีลักษณะอันลามก

คำว่า *"ลามก"* เป็นคำสามัญที่ไม่มีการนิยามศัพท์ แต่เป็นคำที่ใช้เป็นองค์ประกอบความผิดตามประมวลกฎหมายอาญา มาตรา 287 ซึ่งเป็นความผิดฐานเผยแพร่วัตถุอันลามก ดังนั้นข้อมูลคอมพิวเตอร์ใดจะเข้าองค์ประกอบความผิด *"ลามก"* หรือไม่ จึงใช้มาตรฐานเดียวกันกับความผิดตามประมวลกฎหมายอาญา มาตรา 287 ดังกล่าว ศาลฎีกาได้มีคำพิพากษาไว้เป็นบรรทัดฐานหลายเรื่องแล้วในเรื่องการพิจารณาลักษณะอันลามก

(3) ข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

การจะเป็นความผิดตามมาตรา 14 (4) นอกจากข้อมูลคอมพิวเตอร์นั้นมีลักษณะอันลามกแล้ว ยังต้องเป็นข้อมูลคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้อีกด้วย ดังนั้นหากเป็นการนำข้อมูลคอมพิวเตอร์ของตนโดยเฉพาะที่ไม่ได้ประสงค์จะให้ผู้ใดเข้าถึง แต่บังเอิญนำเครื่องคอมพิวเตอร์ไปซ่อม แล้วช่างซ่อมตรวจพบเข้าจึงนำไปเข้าสู่ระบบคอมพิวเตอร์และเผยแพร่ดังที่เป็นข่าวคราว เช่นนี้ เฉพาะช่างซ่อมเท่านั้นที่มีความผิดตามมาตรา 14 (4)

5. เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นความผิดตามมาตรา 14 (1) (2) (3) หรือ (4)

ความผิดตามมาตรา 14 (5) มีองค์ประกอบความผิด ดังนี้

(1) เผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์

องค์ประกอบความผิดนี้แตกต่างจากอนุมาตรา (1) (2) (3) หรือ (4) ซึ่งเป็นเรื่องการนำเข้าสู่ระบบคอมพิวเตอร์ แต่องค์ประกอบความผิดข้อนี้เป็นเพียงการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ ซึ่งเป็นวิธีการที่ระบบคอมพิวเตอร์สร้างขึ้นมาเพื่อให้มีการส่งต่อหรือเผยแพร่ข้อมูลได้โดยง่าย

คำว่า *"เผยแพร่หรือส่งต่อ"* เป็นคำสำคัญที่เข้าใจได้แต่ต้องระลึกว่าเป็นการเผยแพร่หรือส่งต่อในระบบคอมพิวเตอร์ ไม่หมายความรวมถึงการส่งต่อทางกายภาพ เช่นการส่งดิสเก็ต หรือสั่งพิมพ์ออก (printout)

(2) โดยรู้อยู่แล้วว่าเป็นความผิดตามมาตรา 14 (1) (2) (3) หรือ (4)

การจะเป็นความผิดตามมาตรา 14 (5) ต้องพิสูจน์ด้วยว่าผู้กระทำรู้อยู่แล้วว่าข้อมูลคอมพิวเตอร์ที่ตนเผยแพร่หรือส่งต่อนั้น เป็นข้อมูลซึ่งเป็นความผิดตามมาตรา 14 (1) (2) (3) หรือ (4)

(3) เจตนาตามประมวลกฎหมายอาญา มาตรา 59

หมายถึง ผู้กระทำต้องมีเจตนาในการเผยแพร่หรือส่งต่อ

ผู้ให้บริการจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14

มาตรา 15 ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

มาตรา 15 เป็นการเอาผิดกับ *"ผู้ให้บริการ"* มีองค์ประกอบความผิด ดังนี้

1) ผู้ให้บริการ

ผู้ที่จะมีความผิดตามมาตรา 15 ต้องเป็น *"ผู้ให้บริการ"* ซึ่งมีนิยามศัพท์ไว้ในมาตรา 3 ผู้ให้บริการจึงหมายถึงผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ตหรือให้สามารถติดต่อถึงกันโดยประการอื่นโดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น และยังหมายความรวมถึงผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

2) จงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14

บทบัญญัติมาตรานี้ใช้ถ้อยคำ *"จงใจ"* ซึ่งเป็นคำที่เพิ่มขึ้นมาจาก *"เจตนา"* โดยมีเจตนารมณ์ที่จะเน้นให้เห็นว่า *"จงใจ"* นั้นหมายถึงต้องรู้ว่ามีการกระทำความผิดตามมาตรา 14 เช่นมีการเตือนหรือแจ้งให้ทราบแล้วว่าข้อมูลคอมพิวเตอร์นั้นเป็นความผิดต่อกฎหมายตามบทบัญญัติมาตรา 14 เมื่อผู้ให้บริการยังปล่อยให้มีการเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นความผิดในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ก็จะถือได้ว่าเป็นการจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิด

3) ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

ข้อนี้เป็นเรื่องที่กฎหมายบัญญัติเอาผิดเฉพาะผู้ให้บริการที่กระทำความผิดในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตนเท่านั้น

อย่างไรก็ตาม ผู้ให้บริการหรือผู้ใดก็ตามหากมีการกระทำอันเป็นการสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ไม่ว่าในระบบคอมพิวเตอร์ของตนหรือของผู้ใดก็อาจต้องรับผิดตามหลักเรื่องตัวการ หรือผู้สนับสนุนตามหลักในประมวลกฎหมายอาญาได้

4) เจตนาตามประมวลกฎหมายอาญา มาตรา 59

มีข้อสังเกตว่า ถึงแม้มาตรา 15 จะได้บัญญัติองค์ประกอบความผิดว่า *"จงใจ"* แล้วก็ตาม แต่ผู้กระทำจะต้องมีเจตนาตามประมวลกฎหมายอาญา มาตรา 59 ด้วย ซึ่งถึงแม้จะดูเป็นองค์ประกอบความผิดที่ซ้ำซ้อนกัน แต่คณะกรรมาธิการเห็นควรให้คงไว้เพื่อเน้นย้ำว่าการที่จะเอาผิดกับผู้ให้บริการตามมาตรานี้ได้จะ ต้องเป็นเรื่องที่ผู้ให้บริการรู้อยู่แล้วว่าข้อมูลคอมพิวเตอร์ที่อยู่ในระบบคอมพิวเตอร์ซึ่งอยู่ในความควบคุมของตนเป็นข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามมาตรา 14 แล้วยังยินยอมหรือสนับสนุนให้ข้อมูลคอมพิวเตอร์นั้นอยู่ในระบบคอมพิวเตอร์ของตนอยู่

การนำเข้าภาพของผู้อื่นที่เกิดจากการตกแต่ง ตามมาตรา 16

มาตรา 16 *ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ*

ถ้ากระทำตามวรรคหนึ่งเป็นการนำเข้าข้อมูลคอมพิวเตอร์ โดยสุจริต ผกระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

ความผิดตามมาตรา 16 นี้เป็นลักษณะของการดูหมิ่นหรือหมิ่นประมาทด้วยการตกแต่งภาพของบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด มีองค์ประกอบความผิด ดังนี้

1) นำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้

หมายความว่า ผู้กระทำได้มีการกระทำอันเป็นการนำข้อมูลคอมพิวเตอร์เข้าสู่ระบบคอมพิวเตอร์ และระบบคอมพิวเตอร์นั้นเป็นระบบที่ประชาชนทั่วไปอาจเข้าถึงได้ ถ้าเป็นระบบคอมพิวเตอร์ของตนเองก็ไม่เป็นความผิด

2) ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด

องค์ประกอบความผิดข้อนี้ต้องเป็นข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น หมายถึงการแสดงข้อมูลคอมพิวเตอร์นั้นออกเป็นภาพของบุคคล และภาพนั้นอาจเกิดจากการสร้างขึ้นใหม่ หรือเป็นภาพที่มีอยู่แต่ได้มีการตัดต่อ เติม หรือดัดแปลง ซึ่งเป็นการทำด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด

คำว่า *"วิธีการอื่นใด"* เขียนไว้เพื่อให้ครอบคลุมการเปลี่ยนแปลงแก้ไขข้อมูลคอมพิวเตอร์ที่เป็นภาพบุคคลนั้นด้วยวิธีการใดๆ ก็ได้ซึ่งจะมีผลทำให้เกิดการเปลี่ยนแปลงต่อข้อมูลคอมพิวเตอร์ จึงไม่น่าจะหมายความรวมถึงการตัดต่อเติมหรือดัดแปลงภาพบุคคลซึ่งเป็น printout จากคอมพิวเตอร์

3) โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

องค์ประกอบความผิดข้อนี้ใช้ข้อความทำนองเดียวกับความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา มาตรา 326 แต่เพิ่มคำว่า *"ได้รับความอับอาย"* เข้าไปด้วย จึงมีความหมายกว้างกว่าความผิดฐานหมิ่นประมาท

4) เจตนาตามประมวลกฎหมายอาญา มาตรา 59

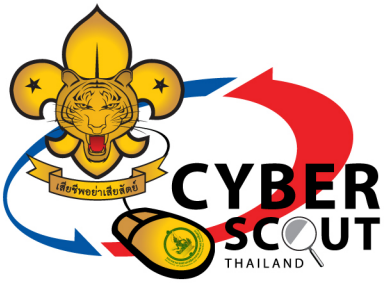
หมายถึงเจตนาในการนำภาพบุคคลเข้าสู่ระบบคอมพิวเตอร์

การนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริตไม่เป็นความผิด การกระทำใดเป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริตน่าจะพิจารณาเทียบได้กับบทบัญญัติในประมวลกฎหมายอาญา มาตรา 326 ที่บัญญัติว่า *"ผู้ใดแสดงความคิดเห็นหรือข้อความโดยสุจริต...ผู้นั้นไม่มีความผิดฐานหมิ่นประมาท"*

ข้อสังเกตประการต่อไปสำหรับความผิดตามมาตรา 16 ก็คือความผิดตามมาตรานี้เป็นความผิดอันยอมความได้ และเป็นความผิดมาตราเดียวที่บัญญัติให้เป็นความผิดอันยอมความได้ ทั้งนี้เนื่องจากเห็นได้ชัดเจนว่าความเสียหายที่เกิดขึ้นนั้นเป็นความเสียหายเฉพาะบุคคล

เมื่อเป็นความผิดอันยอมความได้ กฎหมายจึงต้องบัญญัติในเรื่องผู้เสียหายไว้ในลักษณะทำนองเดียวกับความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา มาตรา 333 ดังปรากฏความในวรรคสี่ ดังนี้

"ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย"



สำนักส่งเสริมและพัฒนาการใช้เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
120 หมู่3 ชั้น 7 อาคารรัฐประศาสนภักดี ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา
ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ : 0 21417036 , 0 21417045-47
โทรสาร : 0 21438043
เว็บไซต์กระทรวงฯ : http://www.mict.go.th
เว็บไซต์ลูกเสือไซเบอร์ : http://www.cyberscoout.in.th