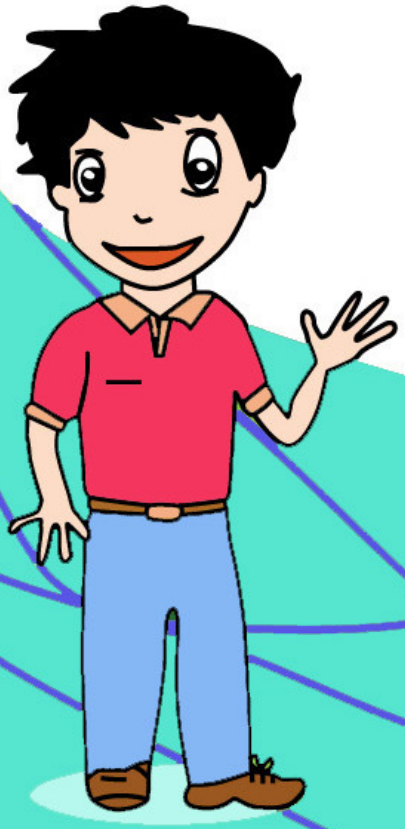
กิจกรรมส่งเสริมและพัฒนาความรู้ด้าน ICT

การปฏิบัติและการป้องกัน เพื่อหลีกเลี่ยงการกระทำความผิด เกี่ยวกับคอมพิวเตอร์

www.mict4u.net



สำนักส่งเสริมและพัฒนาการใช้เทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เอกสารประกอบการอบรม

การปฏิบัติและการป้องกันเพื่อหลีกเลี่ยง
การกระทำความผิดเกี่ยวกับคอมพิวเตอร์

www.mict4u.net

กิจกรรมส่งเสริมและพัฒนาความรู้ด้าน ICT

จัดโดย กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เอกสารประกอบการอบรม หลักสูตรการปฏิบัติและการป้องกันเพื่อหลีกเลี่ยงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

เอกสารเผยแพร่ สงวนลิขสิทธิ์ พ.ศ. 2554
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เขียนโดย
ดร.สานนท์ ฉิมมณี (CEH ECSA)
อาจารย์คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต
นายภส จันทรศิริ (CEH ECSA)
อาจารย์คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต

จัดทำและเผยแพร่โดย
สำนักส่งเสริมและพัฒนาการใช้เทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม 2550
อาคารรวมหน่วยราชการ บี (ชั้น 6) ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง
เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ (02) 141 7041, (02) 141 7046 โทรสาร (02) 141
เว็บไซต์ www.mict4u.net

จัดพิมพ์โดย
บริษัท ล็อกซเล่ย์ จำกัด (มหาชน)
102 ถนน ณ ระนอง แขวงคลองเตย เขตคลองเตย กรุงเทพฯ 10110
โทรศัพท์ (02) 515 8343 โทรสาร (02) 515 8342

คำนำ

ในปัจจุบันนี้ทุกท่านคงปฏิเสธไม่ได้ว่าตนเองไม่มีส่วนเกี่ยวข้องใดๆกับคอมพิวเตอร์เลย จะด้วยทางตรงคือเป็นผู้ใช้คอมพิวเตอร์เอง หรือทางอ้อมคือเกี่ยวข้องกับผู้ที่ใช้คอมพิวเตอร์เช่นต้องทำงานที่มีกระบวนการบางอย่างที่ต้องมีคอมพิวเตอร์เข้ามาเกี่ยวข้อง ซึ่งแต่เดิมการกระทำความผิดต่างๆเกี่ยวกับคอมพิวเตอร์ จะไม่มีกฎหมายที่เฉพาะมารองรับ จึงใช้ได้แค่กฎหมายอาญาที่มีความใกล้เคียงในแต่ละกรณีไป ทำให้การเอาผิดต่างๆที่เกี่ยวกับคอมพิวเตอร์อาจยังไม่สามารถทำได้อย่างชัดเจนนัก แต่ในปัจจุบันประเทศไทยได้มี “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550” มีสามารถใช้เอาผิดกับผู้ที่กระทำความผิดทางคอมพิวเตอร์ได้อย่างชัดเจนมากยิ่งขึ้น และเมื่อมีการกระทำความผิดก็จะไม่สามารถอ้างได้ว่าไม่ทราบว่ามีกฎหมายนั้นๆกำหนดอยู่ เพราะกฎหมายถือว่าเป็นซึ่งที่ประชาชนทุกคนในประเทศต้องปฏิบัติตาม

เอกสารฉบับนี้ได้จัดทำขึ้นเพื่อใช้ประกอบการอบรมหลักสูตร **การปฏิบัติและการป้องกันเพื่อการหลีกเลี่ยงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์** ที่จัดทำขึ้นโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีจุดมุ่งหมายเพื่อแนะนำแนวทางหรือวิธีปฏิบัติที่เหมาะสมเพื่อให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยแบ่งเนื้อหาตามจุดประสงค์ของกฎหมายฉบับนี้ทั้ง 3 อย่างได้แก่ ฐานความผิดและบทลงโทษ, อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ และหน้าที่ของผู้ให้บริการ อย่างไรก็ตามอาจมีรายละเอียดของการอบรมบางส่วนที่แตกต่างไปจากในเอกสารฉบับนี้ ทำให้เอกสารฉบับนี้สามารถใช้อ่านเพิ่มเติมหลังการอบรมได้ แต่จะไม่สามารถใช้อ่านทดแทนการเข้าอบรมตามหลักสูตรได้ นอกจากนี้เอกสารเกี่ยวกับข้อบังคับต่างๆสามารถดาวน์โหลดได้ทางเว็บไซต์ที่ http://www.mict.go.th

ภส จันทรศิริ

สารบัญ

บทที่ 1
ความหมายและผลกระทบของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ในบทแรกนี้เป็นการกล่าวถึงส่วนอธิบายและนิยามคำศัพท์ที่มีการบังคับใช้ตามกฎหมายฉบับนี้ อันได้แก่มาตราที่ 1 ถึงมาตราที่ 4

มาตราที่ 1

พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550"

พระราชบัญญัติฉบับนี้เป็นกฎหมายอาญาที่ระบุความผิดที่เกี่ยวข้องกับการใช้คอมพิวเตอร์โดยผิดกฎหมายซึ่งเกือบทุกมาตราของกฎหมายฉบับนี้ระบุให้เป็นความผิดทางอาญาที่ยอมความไม่ได้ (ยกเว้นมาตรา 16 เพียงมาตราเดียวที่เป็นความผิดอาญาที่ยอมความได้) ดังนั้นในการวินิจฉัยในประเด็นเรื่องการกระทำความผิดอาญาแต่ละมาตราซึ่งเป็นสาระสำาคัญของ พ.ร.บ. ฉบับนี้จึงใช้หลักเกณฑ์พื้นฐานตามกฎหมายอาญาหลักทั่วไปอันได้แก่

1. ต้องมีการกระทำความผิด
2. การกระทำความผิดนั้นเข้าองค์ประกอบการกระทำความผิดของแต่ละมาตรา
3. ผู้กระทำความผิดต้องมีเจตนาประลงค์ต่อผลและเล็งเห็นผล
4. พิจารณาเรื่องความสัมพันธ์ในเรื่องการกระทำกับผล (causatlon)

มาตราที่ 2

พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

กฎหมายฉบับนี้มีผลบังคับใช้ตั้งแต่วันที 18 กรกฎาคม 2550 ดังนั้นหากมีการกระทำความผิดทีเขาองค์ประกอบความผิดก่อนหน้าวันที่กฎหมายฉบับนี้มีผลบังคับใช้ก็ไม่ถือว่าเป็นความผิดอาญาตามกฎหมายฉบับนี้ เว้นแต่การกระทำความผิดดังกล่าวนั้นเป็นความผิดที่คาบเกี่ยวหรือต่อเนื่องเรื่อยมาตั้งแต่ก่อนวันที่ 18 กรกฎาคม 2550 จนถึงและอยู่ระหว่าง หรือหลังวันบังคับใช้กฎหมายดังกล่าวเป็นต้นไป

มาตราที่ 3

ในพระราชบัญญัตินี้

"ระบบคอมพิวเตอร์" **หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ**

"ข้อมูลคอมพิวเตอร์" **หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย**

"ข้อมูลจราจรทางคอมพิวเตอร์" **หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น**

"ผู้ให้บริการ" **หมายความว่า**

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

"ผู้ใช้บริการ" **หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม**

"พนักงานเจ้าหน้าที่" **หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้**

"รัฐมนตรี" **หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้**

ความหมายของ "ระบบคอมพิวเตอร์" ตามความหมายในกฎหมายฉบับนี้ หมายถึงบรรดาอุปกรณ์ หรือชุดอุปกรณ์ใดๆก็ตาม ที่มีสิ่งอื่นใดหรือชุดคำสั่ง (โปรแกรมคอมพิวเตอร์ซอฟต์แวร์ (Software) หรือ Application) ซึ่งชุดคำสั่งดังกล่าวสามารถทำให้อุปกรณ์ หรือชุดอุปกรณ์นั้นประมวลผล(Process) ข้อมูลคอมพิวเตอร์ได้เองโดยอัตโนมัติ เช่น เครื่องคอมพิวเตอร์ที่มีโปรแกรม Operating system (เช่น Microsoft windows, Mac OS X) โปรแกรมหรือชุดคำสั่งดังกล่าวทำให้อุปกรณ์ของคอมพิวเตอร์นั้นสามารถประมวลผลข้อมูลดอมพิวเตอร์ในรูปแบบของภาพ เสียง ข้อความให้สามารถอ่านและฟังข้อความได้โดยอัตโนมิตทันที แต่ในกรณีที่อุปกรณ์หรือชุดอุปกรณ์ใดๆที่แม้มีชุดคำสั่ง แต่ไม่สามารถประมวลผลข้อมูลคอมพิวเตอร์เองได้ ก็ไม่ถือว่าเป็น "ระบบคอมพิวเตอร์" ในหมายของกฎหมายฉบับนี้

"ข้อมูลคอมพิวเตอร์" ในกฎหมายฉบับนี้ยังรวมถึงข้อมูลอิเล็กทรอนิกส์ทุกประเภทที่ระบุไว้ในมาตราที่ 4 ของ พรบ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 ซึ่งระบุว่า *"ข้อมูลอิเล็กทรอนิกส์" หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร*

ในด้าน "ข้อมูลจราจรทางคอมพิวเตอร์" นั้นจะต้องมีองค์ประกอบของการสื่อสารที่สำคัญดังนี้

ผู้ส่งข้อมูล (Sender) คือสิ่งที่ทำหน้าที่ส่งข้อมูลไปยังจุดหมายที่ต้องการ

ผู้รับข้อมูล (Receiver) คือสิ่งที่ทำหน้าที่รับข้อมูลที่ถูกส่งมาให้

ข้อมูล (Data) คือข้อมูลที่ผู้ส่งข้อมูลต้องการส่งไปยังผู้รับข้อมูล ข้อมูลอาจอยู่ในรูปของข้อความ เสียง ภาพเคลื่อนไหว และอื่น ๆ

สื่อนำข้อมูล (Medium) คือสิ่งที่ทำหน้าที่เป็นตัวกลางในการขนถ่ายข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล เช่น สายเคเบิ้ล สายใยแก้วนำแสง อากาศ ฯลฯ

โปรโตคอล (Protocol) คือกฎหรือวิธีที่ถูกกำหนดขึ้นเพื่อการสื่อสารข้อมูล ซึ่งผู้ส่งข้อมูลจะต้องส่งข้อมูลในรูปแบบตามวิธีการสื่อสาร ที่ตกลงไว้กับผู้รับข้อมูล จึงจะสามารถสื่อสารข้อมูลกันได้

ตัวอย่างการสื่อสารข้อมูลด้วยโทรศัพท์

ผู้ส่งข้อมูล: ผู้ที่ทำการส่งข้อความในรูปแบบของเสียงรวมถึงตัวเครื่องโทรศัพท์ที่ใช้ในการติดต่อด้วย

ผู้รับข้อมูล: ผู้ที่ทำการรับข้อความเสียงรวมถึงตัวเครื่องโทรศัพท์ที่ใช้ในการรับข้อมูลด้วย

ข้อมูล: ข่าวสารที่ถูกส่งในการสนทนาระหว่างสองฝ่าย ในรูปแบบของเสียง

สื่อนำข้อมูล: สายโทรศัพท์ ชุมสายโทรศัพท์

โปรโตคอล: ในการเริ่มการสื่อสาร (establishment) ผู้เริ่ม (ผู้โทร) จะต้องแนะนำตัวก่อน ในระหว่าง การสนทนา ทั้งสองฝ่ายจะผลัดกันเป็นผู้ส่ง และผู้รับข้อมูล เมื่อผู้ส่งพูดจบ ให้เว้นจังหวะให้ผู้สนทนาพูดตอบ ถ้ารับข้อมูลไม่ชัดเจนให้ทำการแก้ไขข้อผิดพลาด (error detection) ด้วยการส่งข้อความว่า "อะไรนะ?" เพื่อให้คู่สนทนาส่งข้อมูลซ้ำอีกครั้ง ในการจบการสื่อสาร (termination) ให้พูดคำว่า "แค่นี้นะ" และอีกฝ่ายตอบว่า "ตกลง" เป็นการตอบรับ (acknowledgement)

ในบางกรณี ผู้ส่งข้อมูลอาจเปลี่ยนสถานะเป็นผู้รับข้อมูล เช่น การสื่อสารข้อมูลด้วยโทรศัพท์ เมื่อฝ่ายหนึ่งเป็นผู้ส่งข้อมูลไปให้แล้ว ฝ่ายรับข้อมูลได้ส่งข้อมูลกลับมาให้ในขณะนั้น ผู้ส่งข้อมูลจะเปลี่ยนสถานภาพเป็นผู้รับข้อมูล

คำอธิบายเพิ่มเติมเกี่ยวกับ “ผู้ให้บริการ” ตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับลงวันที่ 23 สิงหาคม 2550 ในภาคผนวก ก. ได้ขยายความเพิ่มเติมไว้ดังนี้

(1) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ ๔ ประเภท ดังนี้

ก. ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier) ประกอบด้วยผู้ให้บริการดังนี้

- ผู้ให้บริการโทรศัพท์พื้นฐาน (Fixed Line Service Provider)
- ผู้ให้บริการโทรศัพท์เคลื่อนที่ (Mobile Service Provider)
- ผู้ให้บริการวงจรเช่า (Leased Circuit Service Provider) เช่น ผู้ให้บริการ Leased Line, ผู้ให้บริการสายเช่า Fiber Optic, ผู้ให้บริการ ADSL (Asymmetric Digital Subscriber Line), ผู้ให้บริการ Frame Relay, ผู้ให้บริการ ATM (Asynchronous Transfer Mode), ผู้ให้บริการ MPLS (Multi Protocol Label Switching) เป็นต้น เว้นแต่ผู้ให้บริการนั้นให้บริการแต่เพียง Physical Media หรือสายสัญญาณอย่างเดียว (Cabling) เท่านั้น (เช่น ผู้ให้บริการ Dark Fiber, ผู้ให้บริการสายใยแก้วนำแสง ซึ่งอาจไม่มีสัญญาน Internet หรือไม่มี IP Traffic)
- ผู้ให้บริการดาวเทียม (satellite seญice provider)

ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ประกอบด้วยผู้ให้บริการดังนี้

- ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ทั้งมีสายและไร้สาย
- ผู้ประกอบการซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรม หรือร้านอาหารและเครื่องดื่ม ในแต่ละกลุ่มอย่างหนึ่งอย่างใด
- ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเดอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัทหรือ สถาบันการศึกษา

ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่าง ๆ (Host Service Provider) ประกอบด้วยผู้ให้บริการดังนี้

- ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (web Hosting), การให้บริการเช่า Web Server
- ผู้ให้บริการแลกเปลี่ยนแฟ้มข้อมูล (File Server หรือ File Sharing)
- ผู้ให้บริการการเข้าถึงจดหมายอิเล็กทรอนิกส์ (Mail Sever Service Provider)
- ผู้ให้บริการศูนย์รับฝากข้อมูลทางอินเทอร์เน็ต (Internet Data Center)

ง. ผู้ให้บริการร้านอินเทอร์เน็ต ประกอบด้วยผู้ให้บริการดังนี้

- ผู้ให้บริการร้านอินเทอร์เน็ต (Internet Cafe)
- ผู้ให้บริการร้านเกมออนไลน์ (Game Online)

(2) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม (1) (Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่าง ๆ (Application Service Provider) ประกอบด้วยผู้ให้บริการดังนี้

- ผู้ให้บริการเว็บบอร์ด (web board) หรือ ผู้ให้บริการบล็อค (Blog)
- ผู้ให้บริการการทำธุรกรรมทางการเงินทางอินเทอร์เน็ต (Internet Banking) และผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ (Electronic Payment Service Provider)
- ผู้ให้บริการเว็บเซอร์วิส (web services)
- ผู้ให้บริการพาณิชย์อิเล็กทรอนิกส์ (e-commerce) หรือ ธุรกรรมทางอิเล็กทรอนิกส์ (e-Transactions)

และโดยทั่วไปแล้วทุกครั้งที่ต้องมีการติดต่อกับ “พนักงานเจ้าหน้าที่” ควรมีการตรวจสอบด้วย โดยการตัวสอบในเบื้องต้นก็คือบัตรประจำตัว ซึ่งต้องมีลักษณะตามประกาศรูปที่ 1.1 แต่ถ้าไม่แน่ใจจริงๆอาจทำการตรวจสอบกับทางกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้โดยตรง

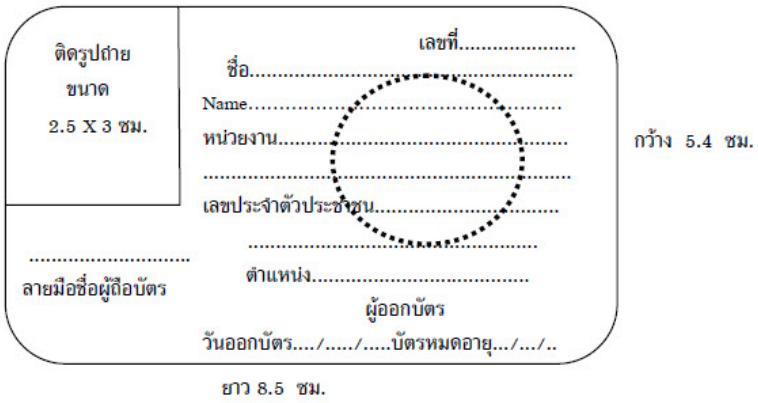
ส่วน “รัฐมนตรี” ในกฎหมายฉบับนี้หมายถึง รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (MICT) ตามมาตราที่ 4

มาตราที่ 4

ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

ด้านหน้า



ด้านหลัง

รูปที่ 1.1 แสดงแบบบัตรประจำตัวพนักงานเจ้าหน้าที่

บทที่ 2

บทลงโทษที่เกี่ยวข้องกับการกระทำความผิดตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ในบทนี้เป็นการกล่าวถึงหมวดที่ 1 ความผิดเกี่ยวกับคอมพิวเตอร์ อันได้แก่ มาตราที่ 5 ถึงมาตราที่ 17

มาตราที่ 5

ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

ในมาตรานี้มีจุดที่น่าสนใจอยู่ 3 ประเด็นคือ

1. ความผิดตามมาตราที่ 5 และมาตราที่ 7 ไม่มีองค์ประกอบเรื่อง “ความเสียหาย” ดังนั้นแม้จะมีการเข้าถึงโดยมีชอบซึ่งข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ แต่ไม่มีความเสียหารเกิดขึ้น ก็เป็นความผิดสำเร็จตามมาตราที่ 5 และ7 แล้ว
2. ความหมายของคำว่า “โดยมิชอบ” ตามกฎหมายฉบับนี้เดิมมีการกำหนดนิยามความหมายไว้ในร่างกฎหมายฉบับเดิม ต่อมากรรมธิการฯ ได้ตัดนิยามความหมายคำว่า “โดยมิชอบ” และ “เข้าถึงโดยมิชอบ” ออกไป โดยให้เหตุผลว่าไม่มีความจำเป็นเนื่องจากคำว่า “โดยมิชอบ” มีการระบุไว้แล้วในประมวลกฎหมายอาญาในหมวดฐานความผิดไว้หลายมาตรา โดยเฉพาะประมวลกฎหมายอาญา,k9ik 269/1-7 อันว่าด้วยความผิด

เกี่ยวกับบัตรอิเล็กทรอนิกส์ ตัวอย่างเช่น *มาตรา 269/5 ผู้ใดใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาทหรือทั้งจำทั้งปรับ*

3. หากระบบคอมพิวเตอร์ไม่มีระบบรักษาความมั่นคงปลอดภัยหรือมาตรการป้องกันการเข้าถึง แม้ว่าจะมีการเข้าถึงโดยมิชอบก็ไม่เป็นความผิดตามมาตราที่ 5 และ 7 เช่น มือถือประเภทคอมพิวเตอร์พกพา หากไม่มีการกำหนดรหัสผ่านก็ไม่ได้รับความคุ้มครองตามกฎหมายฉบับนี้ แม้ผู้กระทำผิดจะมีเจตนาและกระทำการเข้าถึงโดยไม่ได้รับความยินยอมก็ตาม เพราะไม่เข้าองค์ประกอบความผิดตามมาตราทั้ง 2 นี้

มาตราที่ 6

ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

การกระทำความผิดตามมาตรานี้ ต้องมีองค์ประกอบพิเศษ คือ “ต้องเปิดเผยในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น” ตัวอย่างเช่น นาย A เป็นเพื่อนกับนาย B (ซึ่งนาย B เป็นผู้จัดการฝ่ายคอมพิวเตอร์ของบริษัท C) นาย B บอกชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ของพนักงานทุกคนของบริษัท C ให้กับนาย A ทราบ นาย A นำข้อมูลรหัสลับดังกล่าวไปจำหน่ายให้คู่แข่งทางธุรกิจและก่อให้เกิดความเสียหาย การกระทำของทั้งนาย A และนาย B ถือเป็นความผิดตามมาตรานี้

มาตราที่ 7

ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

ความหมายและองค์ประกอบความผิดทั้งหมดของมาตรานี้ มีความหมายเช่นเดียวกับมาตรา 5 แต่มีข้อแตกต่าง คือ องค์ประกอบความผิดของมาตรา 5 แตกต่างจากมาตรา 7 คือวัตถุที่ถูกกระทำโดยการเข้าถึงโดยมิชอบตามมาตรา 7 คือ “ข้อมูลคอมพิวเตอร์” ขณะทีมาตรา 5 คือ “ระบบคอมพิวเตอร์” เท่านั้น

โดยปกติการกระทำความผิดตามมาตรา 7 นั้น มักเกิดขึ้นควบคู่กับการกระทำความผิดตามมาตรา 5 เนื่องจากการเจาะรหัสข้อมูลคอมพิวเตอร์ตามมาตรา 7 ในทางปฏิบัติจะเป็นการกระทำความผิดสำเร็จได้ก็ต่อเมื่อมีการความผิดตามมาตรา 5 มาก่อน กล่าวคือ ผู้กระทำความผิดต้องเข้าถึงระบบคอมพิวเตอรได้ก่อนจึงจะเข้าดูหรือเข้าถึงข้อมูลคอมพิวเตอรได้

นอกจากนี้ ในทางปฏิบัติ ผู้กระทำความผิดโดยการเจาะรหัส หรือเข้าถึงโดยมิชอบ (Hacker) ซึ่งข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์นั้น อาจใช้ “โปรแกรมคอมพิวเตอร์ประสงค์ร้าย (Malware)” ที่อยู่ในรูปแบบของไวรัส (Virus) เพื่อทำลายระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์อันเป็นความผิดตามมาตรา 9 ก่อน จึงจะสามารถเข้าถึงข้อมูลคอมพิวเตอร์ภายในของบุคคลอื่นได้

มาตราที่ 8

ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้น มิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

การสอดแนมหรือการดักจับข้อมูล (Snooping) และบางทีก็มักจะใช้คำว่า *สนิฟฟิง (Sniffing)* หรืออาจเรียกว่า *อีฟดรอปปิง (Eavesdropping)* แทนก็ได้ ซึ่งหมายถึงการดักเพื่อแอบดูข้อมูล ซึ่งจัดอยู่ในประเภทการเปิดเผย การสอดแนมเป็นการโจมตีแบบไม่แสดงตัวตน (Passive) คือการกระทำที่ไม่มีการเปลี่ยนแปลงหรือแก้ไขข้อมูล

ยกตัวอย่างเช่น การดักอ่านข้อมูลในระหว่างที่ส่งผ่านเครือข่าย การอ่านไฟล์ที่จัดเก็บอยู่ในระบบ และการแท็ปสายข้อมูล (Wiretapping) ก็เป็นอีกวิธีหนึ่งของการสอดแนมเพื่อเฝ้าดูข้อมูลที่วิ่งบนเครือข่าย เป็นต้น

การรักษาความลับของข้อมูล เช่น การเข้ารหัสข้อมูล (Encryption) จะเป็นสิ่งที่ช่วยป้องกันภัยคุกคามประเภทนี้ได้ และนอกจากนี้การดักจับแพ็กเก็ต (Packet Sniffer) ก็อีกเป็นอีกรูปแบบหนึ่งของการโจมตีแบบสอดแนม ข้อมูลที่คอมพิวเตอร์ส่งผ่านเครือข่ายนั้นจะถูกย่อยเป็นชุดเล็กๆ ซึ่งเรียกว่า แพ็กเก็ต (Packet) แอพพลิเคชันหลายชนิดจะส่งข้อมูลโดยที่ไม่ได้เข้ารหัส (Clear Text) ดังนั้น ข้อมูลอาจถูกคัดลอกและจัดการโดยเครื่องอื่นที่ไม่ใช่เครื่องปลายทางก็ได้ ทั้งนี้เน็ตเวิร์คโปรโตคอลจะเป็นตัวกำหนดหมายเลขของแต่ละแพ็กเก็ต ซึ่งเป็นสิ่งที่คอมพิวเตอร์ใช้สำหรับระบุว่าแพ็กเก็ตนั้นส่งจากไหนไปไหน เนื่องจากโปรโตคอลที่ใช้ส่วนใหญ่ เช่น TCP/IP เป็นโปรโตคอลมาตรฐานและเป็นที่รู้จักกันโดยทั่วไป ทำให้มีการพัฒนาแอพพลิเคชันที่สามารถดักจับแพ็กเก็ตที่วิ่งบนเครือข่ายได้ และที่น่ากลัวคือสามารถหาดาวน์โหลดได้จากอินเทอร์เน็ตอย่างง่ายดาย โดยที่ผู้ใช้งานไม่จำเป็นต้องมีความรู้เกี่ยวกับคอมพิวเตอร์มากก็สามารถใช้ซอฟต์แวร์เหล่านี้ได้ แพ็กเก็ตสนิฟเฟอร์เป็นโปรแกรมใช้ “เน็ตเวิร์คการ์ด (Network card หรือ LAN card)” ในโหมดโพรมิสเซียส (Promiscuous Mode) ซึ่งในโหมดนี้เน็ตเวิร์คการ์ดจะรับทุกๆแพ็กเก็ตที่วิ่งบนสายสัญญาณแล้วส่งต่อไปยังแอพพลิเคชันเพื่อวิเคราะห์ต่อไป

ข้อสังเกตของมาตราข้อนี้ได้แก่

1. หากเป็นการเผยแพร่ข้อมูลโดยภาครัฐหรือเอกชนเพื่อประโยชน์สาธารณะและมีการดักรับไม่เป็นความผิดตามกฎหมายฉบับนี้ แต่อาจเป็นความผิดตามกฎหมายมาตราอื่นหรือกฎหมายฉบับอื่น
2. มาตรา 8 ตามกฎหมายฉบับนี้บัญญัติขึ้นมาเพื่ออุดช่องว่างทางกฎหมายของการดำเนินคดีกับอาชญากรรมที่ใช้เทคโนโลยีในการดักหรือรับไว้ซึ่งข้อมูลที่มีการส่งผ่านระบบการสื่อสารโทรคมนาคม ในรูปแบบอีเมล์ หรือ

เทคโนโลยีไร้สาย (Wireless LAN) ซึ่งแต่เดิมมีระบุไว้เพียงความผิดที่เกี่ยวข้องกับการดักฟังโทรศัพท์ตามมาตรา 74 ของ พ.ร.บ. การประกอบกิจการโทรคมนาคม พ.ศ. 2544 เท่านั้น โดระบุไว้ว่า "ผู้ใดกระทำด้วยประการใดๆ เพื่อดักรับไว้ใช้ประโยชน์ หรือเปิดเผยข้อความข่าวสาร หรือข้อมูลอื่นใดที่มีการสื่อสารทางโทรคมนาคมโดยไม่ชอบด้วยกฎหมายต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่แสนบาท หรือทั้งจำทั้งปรับ

มาตราที่ 9

ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

สิ่งที่กฎหมายมาตรานี้ต้องการคุ้มครองคือ ความสมบูรณ์ครบถ้วนถูกต้องของข้อมูลคอมพิวเตอร์ (Integrity of Computer Data)

การรักษาความถูกต้องและสมบูรณ์ของข้อมูล (Integrity of Data) หมายถึงการทำให้ข้อมูลมีความน่าเชื่อถือได้ ซึ่งประกอบด้วย 2 ส่วนคือ ข้อมูลนั้นไม่ได้ถูกแก้ไขหรือเปลี่ยนแปลงจากแหล่งที่มาเดิม ส่วนที่สองคือ ความน่าเชื่อถือของแหล่งที่มา ตัวอย่างเช่น หนังสือพิมพ์รายงานข่าวว่าอาจมีการก่อการร้ายเกิดขึ้น ซึ่งข่าวนี้อาจรั่วมาจากสำนักข่าวกรองของรัฐบาล แต่เนื่องจากหนังสือพิมพ์ได้ข่าวมาด้วยวิธีการที่ผิด จึงรายงานว่าข่าวนี้ได้มาจากแหล่งอื่น เนื้อข่าวที่ตีพิมพ์ไปนั้นยังคงสภาพเดิมจากแหล่งที่มา ซึ่งเป็นการรักษาความถูกต้องและสมบูรณ์ของข้อมูล แต่แหล่งข้อมูลที่ได้มานั้นเปลี่ยนไป ดังนั้น ความถูกต้องและสมบูรณ์ของข้อมูลนี้ก็จะถูกกทำลายไปเช่นกัน

กลไกในการรักษาความถูกต้องและสมบูรณ์ของข้อมูลนั้นประกอบด้วย 2 ส่วน คือ

- *การป้องกัน (Prevention)* เป็นความพยามยามที่จะแก้ไขหรือเปลี่ยนแปลงข้อมูลโดยผู้ที่ไม่ได้รับอนุญาต ตัวอย่างเช่น องค์กรหนึ่งใช้ระบบงานบัญชี ถ้ามีพนักงานคนหนึ่งได้เจาะเข้าระบบ และแก้ไขเงินโบนัสของตัวเอง

- *การตรวจสอบ (Detection)* เป็นความพยายามที่จะแก้ไขหรือเปลี่ยนแปลงข้อมูลโดยผู้ที่ได้รับอนุญาตแต่พยายามแก้ไขข้อมูลนอกเหนือขอบเขตที่ตัวเองมีสิทธิ์ ตัวอย่างเช่น องค์กรหนึ่งใช้ระบบงานบัญชี โดยผู้ดูแลระบบบัญชีของบริษัทเองซึ่งได้รับอนุญาตให้ใช้งานระบบ แต่ได้ดำเนินการแก้ไขข้อมูลโดยการโอนเงินเข้าบัญชีตัวเองและพยายามปกปิดการกระทำนี้

กลไกในการป้องกันนี้มีจุดมุ่งหมายเพื่อรักษาความถูกต้องและสมบูรณ์ของข้อมูล ซึ่งทำได้โดยการป้องกันความพยายามที่จะเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต หรือความพยายามที่จะเปลี่ยนแปลงข้อมูลในรูปแบบที่ไม่ถูกต้องหรือได้รับอนุญาต โดยใช้ *การพิสูจน์ตัวตน (Authentication)* และ *การควบคุมการเข้าถึง (Access Control)* จะเป็นกลไกที่ใช้สำหรับการป้องกันการบุกรุกประเภทแรกได้เป็นอย่างดี ส่วนการป้องกันความพยายามจากผู้ที่ได้รับอนุญาตนั้นต้องใช้ *กลไกการตรวจสอบสิทธิ์ (Authorization)* และกลไกอื่นๆเพิ่มขึ้นมา

ทั้งนี้กลไกในการตรวจสอบความถูกต้องและสมบูรณ์ของข้อมูล (Integrity Detection) นั้นไม่ใช่กลไกในการรักษาให้ข้อมูลคงสภาพเดิม แต่เป็นกลไกที่ตรวจสอบว่าข้อมูลยังคงมีความเชื่อถือได้อยู่หรือไม่ ซึ่งสามารถทำได้โดยการตรวจเช็คและวิเคราะห์เหตุการณ์ต่างๆ ที่เกิดขึ้นในระบบ หมายรวมถึงทั้งที่เกิดจากระบบเองและผู้ใช้งานระบบด้วย เพื่อตรวจสอบว่ามีปัญหาเกิดขึ้นหรือไม่ หรืออาจจะตรวจสอบและวิเคราะห์ข้อมูลว่ามีคุณสมบัติที่สำคัญหรือที่คาดหวังไว้ยังคงสภาพเดิมอยู่หรือไม่ และกลไกนี้อาจมีรายงานด้วยว่าส่วนไหนของข้อมูลหรือไฟล์มีการแก้ไขหรืออาจรายงานว่าทั้งไฟล์นั้นถูกเปลี่ยนไปจากสภาพเดิมโดยสิ้นเชิง

การทำงานของการรักษาความถูกต้องและสมบูรณ์ของข้อมูลนั้นแตกต่างจากการรักษาความลับของข้อมูลมาก การรักษาความลับของข้อมูลนั้นเป็นการตรวจสอบว่าข้อมูลถูกขโมยหรือไม่ แต่การรักษาความถูกต้องและสมบูรณ์ของข้อมูลนั้นเกี่ยวกับการรักษาความถูกต้องของข้อมูลและการรักษาความน่าเชื่อถือของข้อมูลด้วยแหล่งที่มาของข้อมูล (ข้อมูลได้มาอย่างไรและจากใคร) ข้อมูลถูกป้องกันดีแค่ไหนก่อนที่จะมาถึง

ปลายทาง และข้อมูลถูกป้องกันอย่างไรในระหว่างที่จัดเก็บอยู่ในระบบนั้น ซึ่งทั้งหมดนี้เป็นผลกระทบต่อความถูกต้องและสมบูรณ์ของข้อมูลทั้งสิ้น ดังนั้น การตรวจสอบความถูกต้องและสมบูรณ์ของข้อมูลนั้นเป็นสิ่งที่กระทำได้ยาก เนื่องจากมันจะขึ้นอยู่กับสมมติฐานเกี่ยวกับแหล่งที่มาและความน่าเชื่อถือของแหล่งที่มานั้น ซึ่งเป็นจุดหนึ่งที่มักจะถูกมองข้ามบ่อย

"การเปลี่ยนแปลง" หมายถึง การแก้ไขข้อมูลโดยที่ไม่ได้รับอนุญาต ซึ่งภัยนี้จะจัดอยู่ใน 3 ประเภท คือ อาจเป็นการหลอกหลวง (Deception) ถ้าฝ่ายรับต้องใช้ข้อมูลที่ถูกเปลี่ยนแปลงแล้ว หรือข้อมูลที่ได้รับเป็นข้อมูลที่ผิดแล้วนำไปใช้งาน ถ้าการเปลี่ยนแปลงข้อมูลแล้วทำให้ระบบถูกควบคุมได้ก็จะจัดอยู่ในประเภทการทำให้ยุ่งและการควบคุมระบบ และการเปลี่ยนแปลงข้อมูลถือเป็นการแบบปลอมแปลงตัวตน (Active) ตัวอย่างเช่น การโจมตีแบบผ่านคนกลาง (Man-in-the-middle attack) เป็นต้น

โดยการโจมตีแบบผ่านคนกลาง เป็นการพยายามที่จะใช้บัญชีผู้ใช้ที่ถูกต้องในการล็อกอินเข้าไปในระบบ ซึ่งการให้ได้มาซึ่งข้อมูลเหล่านี้ก็โดยการใช้การโจมตีแบบคนกลาง (Man-in-the-middle) กล่าวคือ สมมติว่าอลิสเป็นนักเรียนชั้นประถมซึ่งสอบได้คะแนนไม่ดี ครูประจำชั้นก็เลยส่งจดหมายไปให้พ่อแม่ของอลิสให้มาพบครู อลิสทราบดีและคอยดูว่าจะมีจดหมายส่งมาถึงพ่อแม่ตัวเองเมื่อไร เมื่อจดหมายมาถึงอลิสทำการเปลี่ยนข้อความในจดหมายบอกถึงความชื่นชมในตัวอลิสที่ทำคะแนนได้ดีในวิชาคณิตศาสตร์ แล้วเธอก็เขียนจดหมายปลอมว่ามาจากพ่อแม่ของตัวเองว่าไม่สามารถเข้าร่วมประชุมได้ เมื่อพ่อแม่ได้อ่านจดหมายแล้วก็รู้สึกภาคภูมิใจในตัวลูก ในขณะที่ครูก็ไม่สงสัยว่าทำไมพ่อแม่ของอลิสไม่ยอมมาพบ อลิสใช้วิธีการโจมตีแบบคนกลางในการสื่อสารระหว่างครูกับพ่อแม่ของตัวเอง

การโจมตีแบบคนกลางของการสื่อสารผ่านระบบคอมพิวเตอร์เป็นรูปแบบที่พบเห็นได้ทั่วไป การโจมตีประเภทนี้จะทำให้คอมพิวเตอร์สองเครื่องดูเหมือนว่าจะสื่อสารกันอยู่โดยที่ไม่รู้ว่ามีคนกลางคอยเปลี่ยนแปลงข้อมูลอยู่ การป้องกันการโจมตีแบบคนกลางก็อาจใช้วิธีการเข้ารหัสข้อมูลควบคู่กับการพิสูจน์ทราบตัวจริงของคู่รับคู่ส่ง การ

โจมตีแบบนี้แบ่งออกเป็น 2 ประเภทคือ แบบปลอมแปลงตัวตน (Active) คือ ข้อความที่ส่งถึงคนกลางจะถูกเปลี่ยนแปลงแล้วค่อยส่งต้อถึงผู้รับ และแบบไม่แสดงตัวตน (Passive) คือการส่งต่อข้อความเดิมที่ได้รับ

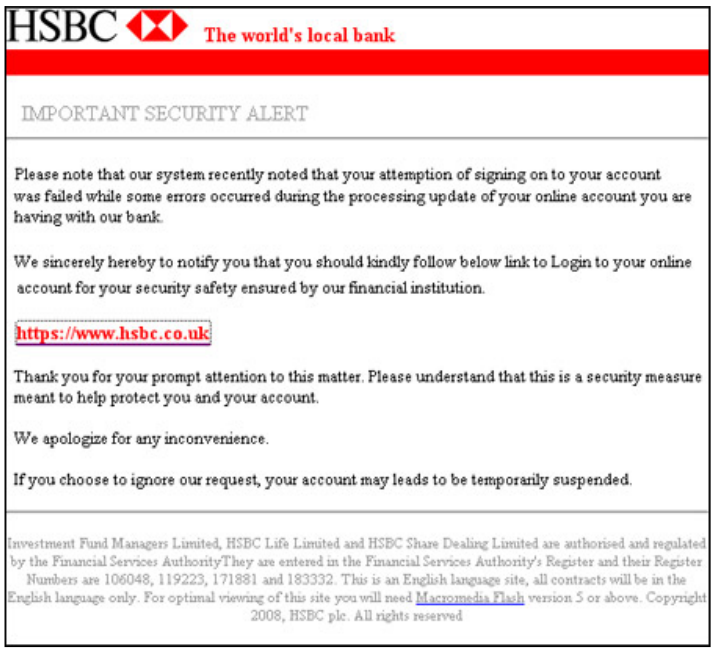
การโจมตีอีกแบบหนึ่งซึ่งคล้ายกับการโจมตีแบบคนกลางคือ การโจมตีแบบทำซ้ำ (Replay Attack) คือ ข้อความที่ได้รับจากผู้ส่งจะถูกจัดเก็บไว้แล้วส่งต่อไปอีกครั้งหนึ่งเมื่อเวลาผ่านไประยะหนึ่ง

นอกจากนี้ยังมีการโจมตีวิศวกรรมสังคม (Social Engineering) ซึ่งเป็นปฏิบัติการทางจิตวิทยาซึ่งเป็นวิธีที่เรียบง่ายที่สุดในการโจมตี เนื่องจากไม่จำเป็นต้องใช้ความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์มากนัก และส่วนใหญ่จะใช้ได้ผลดี การโจมตีแบบวิศวกรรมสังคมจะเกี่ยวกับการหลอกให้บางคนหลงกลเพื่อเข้าถึงระบบ เช่น การหลอกถามรหัสผ่าน การหลอกให้ส่งข้อมูลที่สำคัญให้ เป็นต้น วิศวกรรมสังคมถือเป็นจุดอ่อนที่ป้องกันยากเพราะเกี่ยวข้องกับคน

การโจมตีแบบวิศวกรรมสังคมโดยส่วนใหญ่จะใช้โทรศัพท์ถามข้อมูลโดยหลอกว่าตนเป็นผู้ที่ได้รับอนุญาตหรือเป็นผู้มีอำนาจ อีกวิธีหนึ่งก็โดยการค้นหาข้อมูลจากถังขยะ (Dumpster Diving) เพื่อค้นหาข้อมูลจากเอกสารที่ถูกทิ้งแล้ว ซึ่งในนั้นอาจมีคู่มือการใช้งาน รหัสผ่านที่เขียนไว้ในเศษกระดาษ เป็นต้น อีกวิธีหนึ่งคือ **ฟิสชิ่ง** (Phising) ซึ่งทำโดยการส่งอีเมลเพื่อหลอกให้ส่งข้อมูลให้โดยหลอกว่ามาจากผู้ที่ได้รับอนุญาต ดังรูปที่ 2.1 ยกตัวอย่างเช่น ผู้โจมตีอาจส่งอีเมลและบอกว่ามาจากองค์กรที่ถูกกฎหมายแล้วหลอกให้คลิกเข้าไปยังเว็บไซต์อื่น แทนที่จะไปเว็บไซต์จริงๆ แต่กลับเป็นเว็บไซต์หลอกที่มีหน้าตาเหมือนเว็บไซต์จริง ผู้ใช้จะถูกถามให้กรอกชื่อผู้ใช้ และรหัสผ่านเพื่อยืนยันเจ้าของบัญชีธนาคาร หรือข้อมูลเกี่ยวกับบัตรเครดิต ซึ่งผู้โจมตีก็จะได้ข้อมูลนั้นไป

การป้องกันวิศวกรรมสังคมสามารถทำได้สองทาง วิธีแรกก็โดยการทำให้องค์กรมีขั้นตอนการปฏิบัติที่เข้มงวด หรือนโยบายที่เข้มงวดเกี่ยวกับการบอกรหัสผ่านให้กับคนอื่นทราบ ส่วนอีกวิธีหนึ่งก็โดยการจัดให้มีการอบรมพนักงานเกี่ยวกับนโยบาย และการบังคับให้เป็นไปตามนโยบายการรักษาความปลอดภัย อย่างไรก็ตาม Web Browser รุ่น

ใหม่ส่วนใหญ่ในปัจจุบันมักที่ฟังก์ชันในการป้องกัน Phising อยู่ด้วย โดยใช้การเปรียบเทียบระหว่าง Hyper Link ที่ผู้ใช้คลิกเลือก (ไม่ใช่เว็บไซต์ที่เชื่อมไป) กับ IP Address ที่ไปจริงๆว่าตรงกันหรือไม่ ถ้าไม่ตรงก็จะมีการแจ้งเตือนเพื่อให้ผู้ใช้ตัดสินใจเองอีกครั้ง รวมถึงเทียบกับฐานข้อมูลของการโจมตีจาก Web Browser นั้นๆ ดังรูปที่ 2.2


HSBC The world's local bank

IMPORTANT SECURITY ALERT

Please note that our system recently noted that your attemption of signing on to your account was failed while some errors occurred during the processing update of your online account you are having with our bank.

We sincerely hereby to notify you that you should kindly follow below link to Login to your online account for your security safety ensured by our financial institution.

https://www.hsbc.co.uk

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account.

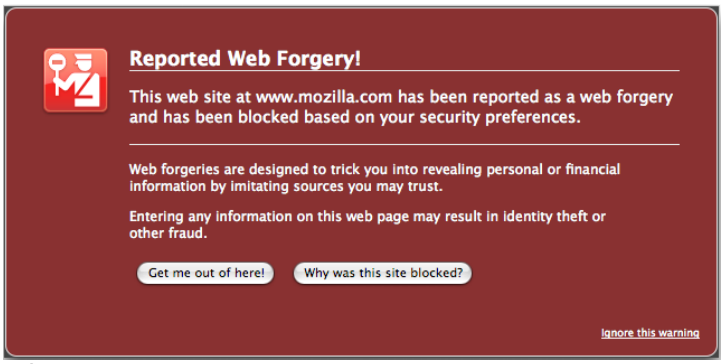
We apologize for any inconvenience.

If you choose to ignore our request, your account may leads to be temporarily suspended.

Investment Fund Managers Limited, HSBC Life Limited and HSBC Share Dealing Limited are authorised and regulated by the Financial Services AuthorityThey are entered in the Financial Services Authority's Register and their Register Numbers are 106048, 119223, 171881 and 183332. This is an English language site, all contracts will be in the English language only. For optimal viewing of this site you will need Macromedia Flash version 5 or above. Copyright 2008, HSBC plc. All rights reserved

รูปที่ 2.1 ตัวอย่างอีเมล์ของการโจมตีแบบ Phising

(ที่มา: http://blog.activeservers.com/CategoryView,category,Dev.aspx)


Reported Web Forgery!

This web site at www.mozilla.com has been reported as a web forgery and has been blocked based on your security preferences.

Web forgeries are designed to trick you into revealing personal or financial information by imitating sources you may trust.

Entering any information on this web page may result in identity theft or other fraud.

Get me out of here! Why was this site blocked?

Ignore this warning

รูปที่ 2.2 ตัวอย่างการแจ้งเตือนการโจมตีแบบ Phising จาก Web Browser

(ที่มา: http://blog.activeservers.com/CategoryView,category,Dev.aspx)

มาตราที่ 10

ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

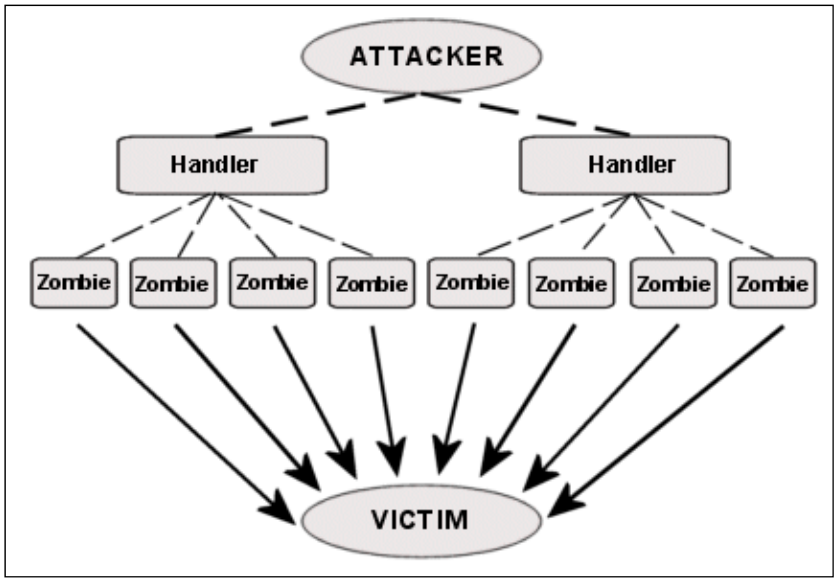
เจตนารมณ์ในการร่างกฎหมายมาตรานี้ก็เพื่อป้องกันการโจมตีในรูปแบบของ "*การปฏิเสธการให้บริการ (Denial of Service)*" และ "*การหน่วงเวลา (Delay)*"

ทั้งนี้หากบริษัท A ทำการอัพเดท (update) ข้อมูลคอมพิวเตอร์ของตนเองหรือเจ้าของเว็บไซต์ต้องการตรวจสอบว่ามีไวรัสอยู่ในระบบคอมพวเตอร์ของตนหรือไม่ และทำการอัพโหลดซอฟต์แวร์เพิ่มเติมในเว็บไซต์ของตนเอง ซึ่งในทางเทคนิคจะมีผลทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง อันมีผลให้ผู้ใช้บริการของบริษัท A ใช้เครื่องคอมพิวเตอร์ของตนในการดาวน์โหลดข้อมูลคอมพิวเตอร์ช้าลง กรณีดังกล่าวไม่ถือว่าเป็นความผิดตามมาตรา 10 เพราะขาดองค์ประกอบเรื่อง "เจตนาและการกระทำโดยมิชอบ"

การปฏิเสธการให้บริการ หมายถึง การที่เซิร์ฟเวอร์ไม่สามารถให้บริการได้เป็นเวลานาน การโจมตีแบบนี้อาจเกิดที่เครื่องเซิร์ฟเวอร์ โดยการขัดขวางไม่ให้เซิร์ฟเวอร์ใช้ทรัพยากร (Resources) ที่ทำเป็นสำหรับการให้บริการหรืออาจเกิดที่ปลายทาง โดยการขัดขวางช่องสื่อสารไปยังเซิร์ฟเวอร์ หรืออาจเกิดในระหว่างทางโดยการละทิ้งแพ็กเก็ตข้อมูลที่รับส่งระหว่างเซิร์ฟเวอร์ การรักษาความพร้อมใช้งานเป็นวิธีที่ใช้ป้องกันการโจมตีแบบนี้ได้ การโจมตีแบบปฏิเสธการให้บริการหรือการหน่วงเวลาอาจเป็นการโจมตีระบบโดยตรง หรืออาจจะเกิดปัญหาที่ไม่เกี่ยวข้องกับระบบการรักษาความปลอดภัยก็ได้

การโจมตีแบบกระจายเพื่อให้เกิดการปฏิเสธการให้บริการ (DDoS: Distributed Denial of Service) หมายถึง การโจมตีเซิร์ฟเวอร์โดยการทำให้เซิร์ฟเวอร์นั้นไม่สามารถให้บริการได้ ซึ่งโดยปกติจะทำโดยการใช้ทรัพยากรของเซิร์ฟเวอร์จนหมดหรือถึงขีดจำกัดของเซิร์ฟเวอร์ ทั้งนี้การโจมตีมักทำโดยผู้โจมตี (Attacker) จะทำการให้ผู้ใช้งานระบบอินเทอร์เน็ตทั่วไปสามารถเข้ามาเลือกใช้บริการต่างๆของเค้าได้ เช่นการดาวน์โหลด

โปรแกรมต่างๆ เป็นต้น ผ่านทางเว็บไซต์หรือวิธีการอื่น เรียกว่า เครื่องมือ (Handler) และจะมีการแนบ Malware จำพวกม้าโทรจันไปด้วย ซึ่งเครื่องที่ติดจะเรียกว่า เครื่องผีดิบ (Zombie) ซึ่งเครื่องผีดิบเหล่านี้จะไม่แสดงอาการผิดปกติใดๆทั้งสิ้น แต่เมื่อมีการติดมากพอตามความต้องการของผู้โจมตีแล้ว (ในบางครั้งอาจเป็นล้านเครื่อง) ผู้โจมตีจะมีการสั่งให้เครื่องผีดิบเหล่านั้นทำการเรียกใช้บริการเดียวกันจากเครื่องเซิร์ฟเวอร์ของเหยื่อ (Victim) พร้อมๆกัน ดังรูปที่ 2.3 ทำให้ผู้ใช้ที่ต้องการใช้บริการจริงๆไม่สามารถใช้งานได้ หรือบางครั้งอาจทำให้เครื่องเซิร์ฟเวอร์ที่ถูกโจมตีนั้นไม่สามารถให้บริการใดๆได้อีกเลย การโจมตีแบบนี้อาจใช้โปรโตคอลที่ใช้บนอินเทอร์เน็ตทั่วไป เช่น TCP (Transmission Control Protocol) หรือ ICMP (Internet Control Message Protocol) เป็นต้น นอกจากนี้การโจมตีแบบนี้มักเป็นการโจมตีจุดอ่อนของระบบหรือเซิร์ฟเวอร์ มากกว่าการโจมตีจุดบกพร่อง (Bug) หรือช่องโหว่อื่นของระบบรักษาความปลอดภัย อย่างไรก็ตามการโจมตีอาจทำให้ประสิทธิภาพของระบบเครือข่ายลดลงด้วย เนื่องจากการส่งแพ็กเก็ตจำนวนมากที่ถือว่าเป็นข้อมูลขยะเข้าไปในระบบเครือข่ายนั้นย่อมไปแย่งการใช้ทรัพยากรของข้อมูลที่ใช้งานอยู่จริงอย่างมาก



รูปที่ 2.3 แสดงโครงสร้างการโจมตีแบบ DDos (Distributed Denial of Service)

การหน่วงเวลา หมายถึง การยับยั้งไม่ให้ข้อมูลส่งถึงตามเวลาที่ควรจะเป็น การส่งข้อความหรือข้อมูลนั้นต้องใช้เวลาในการส่ง สมมติว่าโดยปกติข้อความนั้นจะส่งถึงปลายทางภายในเวลา t แต่ถ้าผู้บุกรุกสามารถหน่วงเวลาให้ข้อมูลส่งถึงปลายทางมากกว่าเวลา t แล้ว แสดงว่าการโจมตีแบบหน่วงเวลาเป็นผลสำเร็จ ซึ่งการโจมตีแบบนี้ผู้บุกรุกต้องสามารถควบคุมระบบบางส่วนได้ เช่น เซิร์ฟเวอร์หรือเครือข่าย เป็นต้น ยกตัวอย่างเช่น สมมติว่าผู้ใช้ต้องการที่จะเข้าควบคุมเซิร์ฟเวอร์ที่ให้บริการอยู่ 2 เซิร์ฟเวอร์ คือ เซิร์ฟเวอร์หลัก (Primary Server) และเซิร์ฟเวอร์สำรอง (Secondary Server) โดยเมื่อเซิร์ฟเวอร์หลักไม่สามารถให้บริการได้เซิร์ฟเวอร์สำรองก็จะทำหน้าที่แทนทันที สมมติว่าผู้บุกรุกสามารถเจาะเข้าระบบและสามารถควบคุมเซิร์ฟเวอร์สำรองได้ เมื่อผู้ใช้พยายามที่จะล็อกอินเข้าเซิร์ฟเวอร์หลัก ผู้บุกรุกก็พยายามหน่วงเวลาไว้จนทำให้ผู้ใช้เข้าใจว่าเซิร์ฟเวอร์หลักไม่สามารถให้บริการในขณะนั้นได้ จะเปลี่ยนไปล็อกอินเข้าเซิร์ฟเวอร์สำรอง ซึ่งผู้บุกรุกได้ควบคุมไว้ ดังนั้น การโจมตีแบบหน่วงเวลาก็เป็นผลสำเร็จ การรักษาความพร้อมใช้งานจะสามารถป้องกันการโจมตีแบบนี้ได้

มาตราที่ 11

ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

จดหมายอิเล็กทรอนิกส์ในปัจจุบันถือได้ว่าเป็นช่องทางในการติดต่อสื่อสารกันอย่างแพร่หลาย ไม่ว่าจะเป็นในระดับของการสื่อสารกันในเรื่องทั่วๆไป, การติดต่อกันเรื่องทางธุรกิจที่สำคัญต่างๆ จนถึงการติดต่อระหว่างหน่วยงานราชการต่างๆ ดังนั้นนี้จึงถือได้ว่าเป็นช่องทางให้ผู้โจมตีทั้งหลายส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมต่างๆ ให้แก่ผู้ใช้ในทุกๆระดับเพื่อจุดมุ่งหมายที่ต่างกันออกไป และจดหมายอิเล็กทรอนิกส์เหล่านี้นี้เองที่ทำให้ผู้ใช้ต้องเสียทั้งเงินและเวลาในการคัดกรองออกจากจดหมาย

อิเล็กทรอนิกส์ที่ใช้งานอยู่จริง ทั้งนี้จดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมและสามารถพบเห็นได้อยู่เป็นประจำได้แก่

จดหมายหลอกหลวง (Hoax Mail) เป็นจดหมายอิเล็กทรอนิกส์ที่ส่งมาโดยปราศจากโปรแกรมประสงค์ร้ายใดๆทั้งหมด แต่จะเป็นการแจ้งข่าวสารซึ่งโดยส่วนมากจะเกี่ยวกับความปลอดภัยทางเทคโนโลยีสารสนเทศ โดยบอกถึงการมาของโปรแกรมประสงค์ร้ายตัวใหม่และแนะนำวิธีในการแก้ไข ซึ่งแน่นอนทั้งหมดนี้เป็นเรื่องหลอกอยู่แล้ว ดังนั้นแล้วถ้าคุณได้รับจดหมายอิเล็กทรอนิกส์ที่มีการแจ้งเตือนไม่ว่าเรื่องอะไรควรทำการตรวจสอบข้อมูลนั้นก่อนทำการใดๆตามที่จดหมายนั้นแนะนำ ซึ่งการตรวจสอบที่ง่ายที่สุดก็โดยการค้นหาในอินเทอร์เน็ตด้วยคำสำคัญในจดหมาย เช่น ชื่อไวรัส หรือชื่อผู้ส่ง เป็นต้น

จดหมายขยะ (Spam Mail) เป็นจดหมายอิเล็กทรอนิกส์ที่ผู้ใช้ไม่ต้องการไม่ว่าจดหมายนั้นจะแนบโปรแกรมประสงค์ร้ายมาด้วยหรือไม่ก็ตาม ซึ่งโดยส่วนใหญ่แล้วจะในรูปแบบของการโฆษณาสินค้าและบริการต่างๆ และเป็นการยากที่จะสามารถแยกจดหมายขยะจากจดหมายปกติ เนื่องจากจดหมายขยะของคนหนึ่งอาจเป็นจดหมายที่อีกคนหนึ่งต้องการอ่านโฆษณานั้นอยู่ก็ได้

จดหมายรำคาญ (Bacon Mail หรือ Bacn Mail) เป็นจดหมายอิเล็กทรอนิกส์ที่ผู้ใช้รู้จักกับแหล่งที่มา โดยอาจเคยติดต่อกันอยู่หรือได้ไปลงทะเบียนไว้กับบริษัทที่ส่งจดหมายนั้น แต่ทั้งนี้จดหมายเหล่านี้เป็นจดหมายที่ผู้ใช้ยังไม่ต้องการหรือไม่สนใจในขณะที่ได้รับ

มาตราที่ 12

ถ้าการกระทำความผิดตามมาตรา 9 **หรือมาตรา** 10

(1) **ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท**

(2) **เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท**

ถ้าการกระทำความผิดตาม (2) **เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี**

มาตรา 12 เป็นบทบัญญัติเพิ่มโทษกับผู้กระทำความผิด ซึ่งผู้กระทำความผิดต้องกระทำความผิดตามที่ระบุไว้ในมาตรา 9 หรือมาตรา 10 เสียก่อน และผลแห่งการกระทำความผิดดังกล่าวนั้นก่อให้เกิดความเสียหายกับประชาชนหรือก่อให้เกิดความเสียหายในวงกว้างต่อความมั่นคงในประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจ หรือบริการสาธารณูปโภคต่างๆ

การปรับใช้ มาตรา 12 ใช้หลักเกณฑ์เกี่ยวกับเรื่องหลักเรื่องความสัมพันธ์ระหว่างการกระทำกับผล (causation) ในประมวลกฎหมายอาญาทั่วไปมาเป็นหลักในการวินิจฉัยประเด็นเรื่องเพิ่มโทษ

มาตราที่ 13

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8

มาตรา 9 มาตรา 10 หรือมาตรา 11 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

"Malicious logic เป็นชุดของคำสั่งที่สร้างปัญหาในการละเมิดนโยบายด้านความปลอดภัยทางเทคโนโลยีสานสรเทศ" หรือส่วนใหญ่แล้วเรามักเรียกกันว่า "โปรแกรมประสงค์ร้าย (Malware)" เนื่องจากที่พบเห็นจริงๆมักอยู่ในรูปของโปรแกรม (Software) แล้ว ทั้งนี้ที่ผ่านมาภัยคุกคามของชุดคำสั่งประสงค์ร้ายนั้นดูจะเป็นสิ่งที่สร้างปัญหาและมีการกล่าวถึงมากที่สุดในบรรดารูปแบบของภัยคุกคามที่มีทั้งหมด

ไวรัส (Virus) หมายถึง โปรแกรมที่ทำลายระบบคอมพิวเตอร์ โดยจะแพร่กระจายไปยังไฟล์อื่นๆที่อยู่ในเครื่องเดียวกัน ไวรัสสามารถทำลายเครื่องได้ตั้งแต่ลบไฟล์ทั้งหมดที่อยู่ในฮาร์ดดิสก์ไปจนถึงเป็นแค่โปรแกรมที่สร้างความรำคาญให้กับผู้ใช้เครือข่าย เช่น แค่เปิดวินโดวส์แล้วเปิดป๊อปอัพเพื่อแสดงข้อความบางอย่าง โดยธรรมชาติแล้วไวรัสไม่สามารถที่จะแพร่กระจายไปยังเครื่องอื่นๆ ได้ตัวตัวเอง แต่การแพร่กระจายไปยังเครื่องอื่นต้องอาศัยโปรแกรมอื่นหรือมนุษย์ เช่น การแชร์ไฟล์โดยใช้ Flash Dive เป็นต้น และไวรัสนั้นไม่สามารถรันได้ด้วยตัวเอง ต้องอาศัยคนเปิดไฟล์ที่ติดไวรัสนั้นจึงจะทำงานได้

หนอน (Worm) หมายถึง โปรแกรมที่เป็นอันตรายต่อระบบคอมพิวเตอร์ โดยจะแพร่กระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆที่อยู่ในเครือข่าย หนอนจะใช้ประโยชน์จากแอพพลิเคชั่นที่รับส่งไฟล์โดยอัตโนมัติ และไม่ต้องอาศัยคนเพื่อเปิดไฟล์ใดๆ เพราะหนอนมีส่วนของโปรแกรมที่สามารถรันตัวเองเพื่อสร้างความเสียหายได้ เวิร์มนั้นบางที่อาจอาศัยอีเมล์ในการแพร่กระจายตัวเองเหมือนไวรัส โดยแนบไฟล์ไปกับอีเมล์เมื่อผู้รับเปิดจดหมายอ่านหนอนก็จะเริ่มทำงานทันที อย่างไรก็ตามในครั้งแรกที่เกิดหนอนขึ้นในวงการคอมพิวเตอร์นั้นเพื่อใช้ช่วยเพิ่มความสะดวกในการลงโปรแกรมให้กับเครื่องคอมพิวเตอร์ที่มีอยู่ในระบบของตนเอง ซึ่งในบางครั้งอาจมีกว่าร้อยเครื่อง โดยหนอนจะทำการส่งตัวเองไปพร้อมกับโปรแกรมที่จะทำการลงไปยังทุกๆเครื่องในระบบแล้วทำการลงโปรแกรมนั้นๆให้เองโดยอัตโนมัติไปเรื่อยๆจนครบทุกเครื่อง

ม้าโทรจัน (Trojan horse) นี้เป็นคำที่มาจากสงครามโทรจันระหว่างทรอย (Troy) และกรีซ (Greek) ซึ่งเปรียบถึงม้าโครงไม้ขนาดใหญ่ที่ชาวกรีซสร้างทิ้งไว้แล้วซ่อนทหารไว้ข้างใน จากนั้นทำทีเป็นว่าถอนทัพกลับ เมื่อชาวทรอยออกมาดูเห็นม้าโครงไม้ทิ้งไว้และคิดว่าเป็นบรรณาการที่ทหารกรีซทิ้งไว้ให้เพื่อไม่ให้ตามไปโจมตีคืน จึงนำกลับเข้าเมืองไปด้วย แต่พอตกดึกทหารกรีซที่ซ่อนอยู่ในม้าโครงไม้ก็ออกมาและเปิดประตูให้กับทหารกรีซเข้าไปทำลายเมืองทรอยได้ในที่สุด สำหรับในความหมายทางคอมพิวเตอร์แล้ว ม้าโทรจัน หมายถึง โปรแกรมที่ทำลายระบบความปลอดภัยของคอมพิวเตอร์ไม่ทางใดก็ทางหนึ่ง โดยแฝงมากับโปรแกรมอื่นๆ เช่น เกม, สกรีนเซิร์ฟเวอร์ เป็นต้น ซึ่งผู้ใช้อาจจะดาวน์โหลดโปรแกรมต่างๆเหล่านี้มา และเมื่อติดตั้งแล้วรันโปรแกรม ม้าโทรจันที่แฝงมาด้วยก็จะทำลายระบบความปลอดภัยของคอมพิวเตอร์ เช่น เปิดช่องทางการสื่อสาร (Port) ที่ไม่ได้ใช้เอง เพื่อเป็นการสร้างประตูหลังให้กับโปรแกรมอื่นเข้ามาทำลายระบบได้ หรืออาจทำการบันทึกการใช้งานต่างๆของผู้ใช้งาน (Logs) เพื่อให้เจ้าของม้าโทรจันนั้นสามารถเข้ามาดูข้อมูลที่บันทึกไว้ได้ เป็นต้น

ทั้งนี้ม้าโทรจันอาจมีชื่อเรียกอื่นซึ่งอธิบายถึงลักษณะการทำงานของมัน เช่น

รูทคิท (Rootkits) เป็นชุดโปรแกรมขนาดเล็กที่หลอกให้ผู้ใช้เชื่อว่าจำเป็นต่อการทำงานของระบบคอมพิวเตอร์ โดยพวกผู้โจมตีนิยมใช้สำหรับเจาะเข้าระบบเพื่อควบคุมระบบหรือขโมยข้อมูล โปรแกรมประเภทนี้อาจใช้เทคนิคต่างๆ เช่น การเฝ้าดูสิ่งที่ผู้ใช้พิมพ์บนคีย์บอร์ด (Key Stroke), แก้ไขไฟล์บันทึก (Log file) ของระบบ, สร้างประตูหลัง (Back door) เพื่อสำหรับการเจาะเข้าระบบในภายหลัง หรืออาจใช้ระบบนี้เพื่อเป็นฐานในการโจมตีระบบอื่นๆผ่านทางเครือข่าย โดยทั่วไปรูทคิทจะถูกจัดไว้เป็นชุดเพื่อใช้สำหรับโจมตีระบบปฏิบัติการประเภทใดประเภทหนึ่งโดยเฉพาะ รูทคิทเกิดขึ้นครั้งแรกในปี 1990 โดยในช่วงนั้นระบบปฏิบัติการซันยูนิกซ์ (SUN Unix) และลีนุกซ์ (Linux) เป็นเป้าหมายของการโจมตี แต่ในปัจจุบันมีรูทคิทหลายประเภทเพื่อใช้กับระบบปฏิบัติการต่างๆ ซึ่งรวมถึงไมโครซอฟท์วินโดวส์ (Microsoft Window) และแม็คอินทอช (Mac OS) ด้วย

Remote Access Trojan (RAT) เป็นม้าโทรจันที่จะสร้างประตูหลัง (Back door) ให้ผู้โจมตีสามารถเข้ามาในระบบเพื่อขโมยข้อมูลหรือควบคุมระบบจากระยะไกล ตัวอย่างเช่น แบ็คออริไฟซี (Back Orifice), คาฟีน (Cafeene) และซับเซเว่น (SubSeven) เป็นต้น

ข้อสังเกตอย่างหนึ่งคือ ถึงแม้ว่าชุดโปรแกรม RAT หรือรูทคิดบางโปรแกรมเป็นเครื่องมือที่สามารถใช้งานอย่างถูกต้องตามกฎหมายเพื่อจุดประสงค์สำหรับการดูแลระบบ (Monitoring System) อย่างไรก็ตามเครื่องมือเหล่านี้อาจเป็นอันตรายต่อระบบหรือองค์กรได้ถ้ามีการใช้งานในทางที่ผิด

รูปที่ 2.4 แสดงภาพม้าโทรจันที่มีการซ่อนคนไว้ภายใน

นอกจากโปรแกรมประสงค์ร้ายที่ได้กล่าวมาแล้วยังมีการแยกโปรแกรมที่มีลักษณะพิเศษออกไปอีกหลายอย่างแต่ที่มักพบเจอหรือได้ยินก็คือ Spyware และ Adware ซึ่งถ้าจะวัดกันตามลักษณะทั้ง 3 แล้วโปรแกรมประสงค์ร้ายเหล่านี้จะถือว่าจัดอยู่ในพวกของ “ม้าโทรจัน” แต่อย่างไรก็ตามโดยมากแล้วจะไม่ถือว่าโปรแกรมเหล่านี้เป็น Malware เนื่องจากจุดประสงค์ที่แท้จริงไม่ได้สร้างมาเพื่อจุดประสงค์ร้าย แต่ถึงกระนั้นก็มักสร้างความรำคาญต่อผู้ใช้ไม่มากก็น้อย

สปายแวร์ (Spyware) เป็นโปรแกรมขนาดเล็กที่มักมากับการที่ผู้ใช้เข้าใช้บริการในเว็บไซต์ที่ให้บริการบนอินเทอร์เน็ตด้านต่างๆ เช่น รับฝากไฟล์, เกมฟรี, ภาพลามก, การพนัน, ดาวน์โหลดโปรแกรมฟรี เป็นต้น โดยอาจมาในรูปของให้ผู้ใช้ทำการดาวน์โหลดโปรแกรม ActiveX มาติดตั้งก่อนจึงจะสามารถใช้บริการได้ แต่ทั้งนี้เมื่อเราได้ติดตั้งไปแล้วก็จะมีการติดตั้งสปายแวร์ลงไปด้วย ซึ่งโปรแกรมนี้จะทำการส่งข้อมูลการใช้งานของผู้ใช้ไว้ตามที่กำหนดไปยังเจ้าของสปายแวร์ หรือก็คือบริษัทของผู้ให้บริการที่ผู้ใช้ได้ใช้บริการไปนั้นเอง และการทำงานทั้งหมดนี้จะเป็นการทำงานที่อยู่เบื้องหลังทั้งสิ้น ทั้งนี้ข้อมูลที่บริษัทเหล่านี้ได้ไปมักเป็นไปเพื่อประโยชน์ทางด้านธุรกิจ เช่น ผู้ใช้ชอบเข้าเว็บไซต์แบบใด, ใช้โปรแกรมแบบใด, ชอบฟังเพลงหรือใช้สื่อแบบใด เป็นต้น นอกจากผลกระทบเรื่องความเป็นส่วนตัวของผู้ใช้แล้ว สปายแวร์ยังมีส่วนทำให้การใช้งานทั่วไปภายในเครื่องตลอดจนการใช้งานระบบเครือข่ายได้ช้าหรือในบางครั้งอาจใช้งานไม่ได้เลย เนื่องจากสปายแวร์ได้ใช้ทรัพยากรของระบบอยู่ด้านหลังนั้นเอง

แอดแวร์ (Adware) เป็นโปรแกรมขนาดเล็กที่มีลักษณะการติดมาและการทำงานคล้ายกับสปายแวร์ แต่จะทำการแสดงหน้าต่างป็อปอัพ (Popup) โฆษณาขึ้นมาโดยดูจากพฤติกรรมของผู้ใช้ และมักจะไม่ทำการส่งข้อมูลไปยังเจ้าของแอดแวร์มากเท่ากับสปายแวร์นอกจากเพื่อปรับปรุงข้อมูลในการแสดงผลของป็อปอัพกับเครื่องของผู้ถูกโจมตีเท่านั้น

ทั้งนี้ Malware ต่างๆไม่สามารถทำงานข้าม OS (ระบบปฏิบัติการ: Operating System) กันได้ เนื่องจากในแต่ละ OS จะมีการใช้นามสกุลของไฟล์ที่เรียกใช้งานได้ไม่เหมือนกัน เช่นใน Window OS จะใช้ไฟล์ .exe แต่ใน MAC OS นั้นจะไม่สามารถรันไฟล์ .exe ได้ ดังนั้น Malware บน Window OS จึงไม่มีผลกระทบต่อ MAC OS อย่างไรก็ตามในทำนองเดียวกัน Malware บน MAC OS ก็ไม่มีผลกับ Window OS เช่นกัน

อย่างไรก็ตามนอกจากโปรแกรมประสงค์ร้ายที่เรารู้จักในปัจจุบันแล้ว กลุ่มนักวิชาการทางคอมพิวเตอร์หลายท่านคาดการณ์ว่า *"ในปัจจุบันอาจมีชุดคำสั่งประสงค์ร้ายบางอย่างที่เราไม่รู้จักและไม่สามารถอธิบายได้ในปัจจุบัน ได้แฝงตัวอยู่ในระบบ*

เครือข่ายที่พวกเรากำลังใช้งานอยู่ และรอเพียงเวลาที่มันจะทำงานอย่างเต็มรูปแบบโดยที่พวกเราไม่สามารถจะคาดเดาได้เลยว่าผลกระทบของมันจะออกมาเป็นอย่างไร"

มาตราที่ 14

ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) **นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน**

(2) **นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิด ความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน**

(3) **นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา**

(4) **นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้**

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

ความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา หมายถึง ความผิดที่ระบุไว้ในประมวลกฎหมายอาญาทั่วไป

- ในหมวดความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันได้แก่
  - ก) ความผิดต่อองค์พระมหากษัตริย์ พระราชินี รัชทายาท และผู้สำเร็จราชการแทนพระองค์ (มาตรา 107-112)
  - ข) ความผิดต่อความมั่นคงภายในราชอาณาจักร (มาตรา 113-118)
  - ค) ความผิดต่อความมั่นคงภายนอกราชอาณาจักร (มาตรา 119-129)

ง) ความผิดต่อสัมพันธไมตรีกับต่างประเทศ (มาตรา 130-138)

- ความผิดเกี่ยวกับการก่อการร้าย (มาตรา 135/1-135/4)

และคำว่า “ลามก” ได้มีคำพิพากษาฎีกาที่วินิจฉัยเกี่ยวกับประเด็นเรื่องความหมายของคำนี้ดังนี้

คำพิพากษาฎีกาที 3510/2531 ภาพหญิงยืนเปลือยกายกอดชาย ภาพหญิงสวมกางเกงในโป่งตามีผู้ชายนอนกอดมือโอบบริเวณทรวงอก ภาพหญิงเปลือยกายท่อนบนใช้มือจับหูโทรศัพท์กดที่อวัยวะเพศ ภาพหญิงเปลือยกายมีแหคลุมตัวมือข้างกุมนมอีกข้างหนึ่งกุมอวัยวะเพศ ภาพหญิงเปิดเสื้อให้เห็นนม ล้วงมือเข้าโปในกระโปรง ภาพหญิงเปลือยอกสวมกางเกงในมือล้วงที่อวัยวะเพศ และภาพหญิงเปลือยอกสวมกางเกงขาสั้น มือข้างหนึ่งล้วงไปจับที่อวัยวะเพศ ภาพดังกล่าวแม้ไม่เห็นอวัยวะเพศชัดเจน แต่ก็มีลักษณะส่อไปในด้านยั่วยุกามารมณ์ และภาพหญิงเปลือยตลอดร่างซึ่งพอเห็นอวัยวะเพศได้บ้างถือได้ว่าเป็นภาพอันลามก ไม่ใช่ภาพศิลปะ ทีแสดงถึงสัดส่วนความสมบูรณ์ของร่างกาย

ข้อความต่างๆ ที่ได้บรรยายถึงการร่วมประเวณีของชายและหญิงอย่างชัดเจนละเอียดลออ โดยบรรยายถึงอารมณ์ของชายและหญิงไปในทางยั่วยุกามารมณ์ แม้จะมิได้ใช้ถ้อยคำหยาบคาย ถือได้ว่าเป็นข้อความอันลามก

นอกจากนี้คำว่า “ประชาชน” ในที่นี้ไม่ได้มีความหมายหมายถึงบุคคลจำนวนมาก ในชั้นกรรมาธิการฯ มีข้อถกเถียงว่าควรจะใช้คำว่า “ผู้อื่น” หรือคำว่า “ประชาชน” และท้ายที่สุดกรรมาธิการฯ ตกลงใช้คำว่า “ประชาชน” โดยได้รับคำชี้แจงจากตัวแทนจากเนักงานอัยการสูงสุดและที่ปรึกษากฎหมายของกรรมาธิการฯ ว่า คำว่า “ประชาชน” ที่ระบุไว้ในมาตรา 14 (4) นั้นมีความหมายหมายถึง *“บุคคลที่มากกว่า 1 คนขึ้นไป”* ก็ถือว่าเป็น “ประชาชน” ในความหมายของกฎหมายฉบับนี้แล้ว ทั้งนี้โดยอ้างอิงจากคำพิพากษาฎีกาและข้อกฎหมายทีเกี่ยวข้อง ดังนี้

คำพิพากษาฎีกาที 3213/2426 “มีวีดีโอเทปลามกไว้ให้เช่า หรือ แลกเปลี่ยนระหว่าง “สมาชิก” ผิดตามมาตรานี้”

คำพิพากษาฎีกาที 2875/2531 "มีโทรทัศน์สีและเครื่องเล่นวีดีโอเทปที่ใช้ฉายภาพยนตร์ลามกเพื่อแสดงอวดแก่ประชาชน โดยเก็บเงิน ผิดตามมาตรานี้"

ดังนั้น หากเว็บไซต์ A ให้บริการจำหน่ายภาพลามกอนาจารผ่านอินเตอร์เน็ต เฉพาะสมาชิกเท่านั้น การกระทำของเว็บไซต์ A ก็ถือว่าเป็นความผิดตามมาตรา 14 (4)

มาตราที่ 15

ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

"ผู้ให้บริการ" หมายความว่า

1. ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

2. ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

ส่วนคำว่า "ยินยอม" ในกฎหมายฉบับนี้หมายถึง *"ยินยอมโดยชัดแจ้งและยินยอมโดยปริยาย"* ซึ่งในการปรับใช้กฎหมายอาจจะมีปัญหาเกียวกับการพิสูจน์องค์ประกอบเรื่องเจตนาว่า

ก) หากนาย ก. ซึ่งเป็นพนักงานของบริษัท Z ส่งข้อมูลคอมพิวเตอร์ปลอม เท็จ หรือลามกอนาจารภายในองค์กรของตนเอง ผู้บริหารของบริษัท Z จะมีความผิดตามมาตรา 15 หรือไม่หรือ

ข) เว็บไซต์ท่า (Portal Website) หรือเว็บไซต์ทั่วโปที่ให้บริการพื้นที่แก่ผู้ใช้บริการ (User) ในการแสดงความคิดเห็นได้ แต่ปรากฏว่านาย ข. มาโพสต์ภาพลามก อนาจาร เว็บไซต์นั้นต้องรับผิดตามมาตรา 15 หรือไม่

ในทางปฏิบัติการพิสูจน์เรื่องเจตนาเป็นสิ่งที่ค่อนข้างยุ่งยาก เพื่อป้องกันปัญหาในเรื่องดังกล่าวบริษัทและเว็บไซต์ทั่วไป ซึ่งเป็นผู้ให้บริการตามกฎหมายฉบับนี้จึงควรจัดทำนโยบายการใช้อินเทอร์เน็ต (Internet Policy) สำหรับพนักงานในองค์กรของตน

หรือกรณีเว็บไซต์ก็ควรมีการระบุข้อกำหนด เงื่อนไข (Terms & Conditions) ในเว็บไซต์ของตน โดยระบุห้ามมิให้ใช้เผยแพร่ข้อมูลที่ผิดกฎหมาย เพื่อป้องกันปัญหาเรื่องการพิสูจน์เรื่องเจตนาหรือการยินยอมโดยปริยายให้พนักงานในองค์กรกระทำความผิดตามมาตรา 14

มาตราที่ 16

ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้น เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรานี้ถือเป็นมาตราเดียวในหมวดฐานความผิดทั้งหมดที่เป็นความผิดที่ "สามารถยอมความได้" วัตถุประสงค์ของร่างกฎหมายมาตรา 16 คือแก้ไขปัญหาช่องว่างในกฎหมายอาญาเรื่องหมิ่นประมาท ในมาตรา 326 และ328 เนื่องจากในปัจจุบันการใช้สื่อเทคโนโลยีและโปรแกรมคอมพิวเตอร์ในการสร้าง ตัดต่อ หรือดัดแปลงภาพของบุคคลที่มีชื่อเสียงไปในทางที่ก่อให้เกิดความเสียหายมีค่อนข้างมาก อาทิเช่น ตัดต่อภาพของบุคคลผู้มีชื่อเสียงในลักษณะภาพลามกอนาจาร หรือตัดต่อเพื่อใส่ความให้เกิดความเสียหาย ซึ่งกฎหมายฐานหมิ่นประมาทตามประมวลกฎหมายอาญาไม่สามารถเอาผิดกับบุคคลดังกล่าวได้

แต่ทั้งนี้ ความผิดตามมาตรานี้จะไม่ปรับใช้กับกรณีสื่อมวลชนตัดต่อหรือทำภาพล้อเลียนดาราหรือนักการเมืองในลักษณะรูปการ์ตูนเพื่อประกอบการเสนอข่าว (Parody) ดังตัวอย่างในรูปที่ 2.5

รูปที่ 2.5 ภาพตัวอย่างของ Parody

มาตราที่ 17

ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(1) **ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ**

(2) **ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ**

จะต้องรับโทษภายในราชอาณาจักร

ทั้งนี้ในมาตรานี้มักเกิดปัญญาในเรื่องการเข้าผิดได้ง่าย ซึ่งความเป็นจริงนั้นเริ่มตั้งแต่การนำสืบหาหลักฐานต่างๆ เนื่องจากกฎหมายในแต่ละประเทศมีความแตกต่างกัน ทำให้การที่หน่วยงานที่รับผิดชอบจะเข้าไปตรวจสอบหลักฐานในต่างประเทศนั้นในหลายๆกรณีมักทำได้ยาก หรือเกิดความล่าช้าในการประสานงานต่างๆ ทำให้การบังคับใช้จริงในทางปฏิบัติจึงเกิดขึ้นได้ค่อนข้างลำบาก

บทที่ 3
บทบาท และอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ในบทที่ 3 นี้จะเป็นการกล่าวถึงกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่และหน้าที่ของผู้ให้บริการที่มีการบังคับใช้ตามกฎหมายฉบับนี้ อันได้แก่มาตราที่ 18 ถึงมาตราที่ 30

มาตราที่ 18

ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตาม

พระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) **สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่**

(6) **ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใดอันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้**

(7) **ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการ**
เข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ใน
การถอดรหัสลับดังกล่าว

(8) **ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้**

บทบัญญัติในมาตรานี้ให้อำนาจพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งและอบรมโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (กระทรวงไอซีที) ที่เรียกว่า “Cyber Cop” ซึ่งแบ่งขอบเขตอำนาจของพนักงานเจ้าหน้าที่ออกเป็น 2 ส่วนใหญ่ดังนี้

1. อำนาจของพนักงานเจ้าหน้าที่ที่สามารถดำเนินการได้เองโดยไม่ต้องยื่นคำร้องขอต่อศาล จะได้แก่อำนาจในวรรคที่ (1) (2) และ (3)
2. อำนาจของพนักงานเจ้าหน้าที่ที่จะใช้ได้ในกรณีที่ร้องขอต่อศาลเท่านั้น จะได้แก่อำนาจในวรรคที่ (4) (5) (6) (7) และ (8)

ทั้งนี้แล้ว เจ้าหน้าที่ตำรวจตาม ป.วิ.อ. ซึ่งไม่ได้รับการแต่งตั้งให้เป็น “พนักงานเจ้าหน้าที่” ตามกฎหมายฉบับนี้ไม่มีอำนาจตามมาตรา 18

มาตราที่ 19

การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) **และ** (8) **ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิดเท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว**

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา 18 (4) (5) (6) (7) **และ** (8) **มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของ หรือ ผู้ครอบครองดังกล่าวในทันทีที่กระทำได้**

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา 18 (4) (5) (6) (7) **และ** (8) **ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน**

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา 18 (4) **ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น**

การยึดหรืออายัดตามมาตรา 18 (8) **นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้วพนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยาย**

เวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรานี้เป็นมาตรานี้เป็นการอธิบายถึงรายละเอียดในกรณีที่พนักงานเจ้าหน้าที่จะใช้อำนาจในการทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ถอดรหัสลับ ยึดหรืออายัดระบบคอมพิวเตอร์ ซึ่งต้องขออำนาจจากศาลเท่านั้น เนื่องจากเป็นกรณีที่พนักงานเจ้าหน้าที่ต้องใช้อำนาจกระทบถึงสิทธิ เสรีภาพ และทรัพย์สินของประชาชนทั่วไป จึงต้องให้ศาลเป็นองค์กรที่เข้ามาตรวจสอบอีกขั้นตอนหนึ่ง

มาตราที่ 20

ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลาย ซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสองลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้อง พร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

ตามมาตรานี้จะต้องมีลักษณะเป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่

1. อาจกระทบต่อความมั่นคงในราชอาณาจักร เฉพาะที่บัญญัติไว้ในภาค 2 ลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญาอันได้แก่ หมวด

ความผิดเกี่ยวกับพระมหากษัตริย์ และหมวดความผิดเกี่ยวกับความมั่นคง ซึ่งมีรายละเอียดดังนี้

ก) ความผิดต่อองค์พระมหากษัตริย์ พระราชินี รัชทายาท และผู้สำเร็จราชการแทนพระองค์ (มาตรา 107-112)

ข) ความผิดต่อความมั่นคงภายในราชอาณาจักร (มาตรา 113-118)

ค) ความผิดต่อความมั่นคงภายนอกราชอาณาจักร (มาตรา 119-129)

ง) ความผิดตอสัมพันธไมตรีกับต่างประเทศ (มาตรา 130-138)

2. ข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน คำว่า “ขัดต่อความสงบเรียบร้อย และศีลธรรมอันดีของประชาชน” ซึ่งตามแนวคำพิพากษาฎีกา หมายถึง

ก) เว็บไซต์ที่เผยแพร่ข้อมูลลามกอนาจาร

ข) เว็บไซต์ที่เผยแพร่ข้อมูลเกี่ยวกับการพนัน

ค) เว็บไซต์ที่เผยแพร่ข้อมูลเกี่ยวกับการค้ามนุษย์ ค้าทาส

ทั้งนี้แล้วการปิดปล็อคเว็บไซต์ตามมาตรา 20 นั้น ศาลเท่านั้นที่มีอำนาจในการปิดปล็อคเว็บไซต์ โดยในชั้นกรรมาธิการฯ มีข้อตกลงร่วมกันว่า การปรับใช้มาตรา 20 นั้นจะไม่ใช้กับกรณีเว็บไซต์ที่แสดงความคิดเห็นเกี่ยวกับทางการเมือง ซึ่งเป็นสิทธิโดยชอบของประชาชนที่พึงกระทำได้ อันไม่ขัดต่อกฎหมายแต่อย่างใด

และหากมีการปิดปล็อคเว็บไซต์ที่มิได้เป็นการกระทำผิดตามกฎหมายฉบับนี้ คำสั่งปล็อคเว็บไซต์ดังกล่าวถือว่ามิชอบ ผู้มีส่วนได้เสียสามารถร้องขอให้ศาลเพิกถอนและเรียกร้องค่าเสียกายได้

มาตราที่ 21

ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้

หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวงทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

"Malicious logic เป็นชุดของคำสั่งที่สร้างปัญหาในการละเมิดนโยบายด้านความปลอดภัยทางเทคโนโลยีสานสรเทศ" หรือส่วนใหญ่แล้วเรามักเรียกกันว่า "โปรแกรมประสงค์ร้าย (Malware)" เนื่องจากที่พบเห็นจริงๆมักอยู่ในรูปของโปรแกรม (Software) แล้ว

มาตราที่ 22

ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา 18 ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

กฎหมายต้องการคุ้มครอง "ข้อมูลส่วนบุคคล" อันได้แก่ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้แต่ละคน จึงจำกัดสิทธิ์ให้เฉพาะเจ้าหน้าที่เท่านั้นที่รับทราบรายละเอียดข้อมูลดังกล่าวได้ และหากพนักงานเจ้าหน้าที่มีการเปิดเผยข้อมูล

ดังกล่าวกับบุคคลภายนอก เจ้าหน้าที่ดังกล่าวจะมีโทษในทางอาญา ซึ่งเป็นความผิดที่ยอมความไม่ได้

มาตราที่ 23

พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา 18 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรานี้เป็นการกำหนดโทษกับพนักงานเจ้าหน้าที่ที่กระทำโดยประมาทและทำให้บุคคลอื่นซึ่งไม่ใช่พนักงานเจ้าหน้าที่ล่วงรู้ถึงข้อมูลคอมพิวเตอร์ ข้อมูลจราจรคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่ได้มาตามมาตรา 18

มาตราที่ 24

ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

เป็นการกำหนดความรับผิดชอบกับบุคคลภายนอกที่ล่วงรู้ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลจราจรคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาโดยอาศัยอำนาจตามกฎหมายฉบับนี้ แล้วนำไปเปิดเผย

มาตราที่ 25

ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

ตามมาตรานี้ กรรมาธการฯ ผู้ร่างนำเอาข้อความและหลักเกณฑ์มาจากมาตรา 226 ของประมวลกฎหมายวิธีพิจารณาความอาญาในเรื่อง “การห้ามรับฟังพยานหลักฐานที่ได้มาโดยมิชอบ” โดยหลักกฎหมายเรียกว่า “หลักผลไม้มีพิษ” ซึ่งในที่สุดแล้วศาลจะเป็นผู้ใช้ดุลพินิจในการพิจารณาตามหลักการพิจารณาคดีอาญาทั่วไปเป็นกรณีๆไป

มาตราที่ 26

ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใดให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

คำอธิบายเพิ่มเติมเกี่ยวกับ “หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ” ตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับลงวันที่ 23 สิงหาคม 2550 ในภาคผนวก ข. ได้ขยายความเพิ่มเติมไว้ดังนี้

1. ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ 5 (1) ก. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก.ข้อมูลที่สามารถระบุและติดตามถึงแหล่งกำเนิด ต้นทาง ปลายทาง และทางสายที่ผ่านของการติดต่อสื่อสารของระบบคอมพิวเตอร์	- ข้อมูลระบบชุมสายโทรศัพท์พื้นฐาน โทรศัพท์วิทยุมือถือ และระบบตู้โทรศัพท์สาขา (fixed network telephony and mobile telephony) - หมายเลขโทรศัพท์ หรือ เลขหมายวงจร รวมทั้งบริการเสริมอื่นๆ เช่น บริการโอนสาย และหมายเลขโทรศัพท์ที่ได้โอนสาย รวมทั้งหมายเลขโทรศัพท์ซึ่งถูกเรียกจากโทรศัพท์ที่มีการโอน - ชื่อ ที่อยู่ของผู้ใช้บริการหรือผู้ใช้งานที่ลงทะเบียน (name and address of subscriber or registered user) - ข้อมูลเกี่ยวกับวันที่, เวลา และที่ตั้งของ Cell ID ซึ่งมีการใช้บริการ (date and time of the initial activation of the service and the location label (Cell ID))
ข.ข้อมูลที่สามารถระบุวันที่ เวลา และระยะเวลาของการติดต่อสื่อสารของระบบคอมพิวเตอร์	- วัน ที่ รวมทั้งเวลาเริ่มต้นและสิ้นสุดของการใช้งาน (fixed network telephony and mobile telephony, the date and time of the start and end of the communication)
ค.ข้อมูลซึ่งสามารถระบุที่ตั้งในการใช้	- ที่ตั้ง label ในการเชื่อมต่อ (Cell ID) ณ สถานที่เริ่มติดต่อสื่อสาร

โทรศัพท์มือถือ หรืออุปกรณ์ติดต่อสื่อสารแบบไร้สาย (Mobile communication equipment)	- ข้อมูลซึ่งระบุที่ตั้งทางกายภาพของโทรศัพท์มือถืออันเชื่อมโยงกับข้อมูลที่ตั้งของ Cell ID ขณะที่มีการติดต่อสื่อสาร - จัดให้มีระบบบริการตรวจสอบบุคคลผู้ใช้บริการ

2. ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ 5 (1) ข. ถึง ค. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย	1) ข้อมูล log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่ายซึ่งระบุถึงตัวตนและสิทธิ ในการเข้าถึงเครือข่าย (Access logs specific to authentication and authorization servers, such as TACACS+ or RADIUS or DIAMETER used to control access to IP routers or network access servers) 2) ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server 3) ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID) 4) ข้อมูลหมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดให้โดย

	ระบบผู้ให้บริการ (Assigned IP address) 5) ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (Calling line Identification)
ข. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)	1) ข้อมูล log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็กทรอนิกส์ (Simple Mail Transfer Protocol : SMTP log) 2) ข้อมูลจดหมายอิเล็กทรอนิกส์ที่บันทึกการใช้บริการเรียกข้อมูลจดหมาย อิเล็กทรอนิกส์ ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือการดึงข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิกโดยยังคงจัดเก็บ ข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึงไปนั้นไว้ที่เครื่องให้บริการ (POP3 log or IMAP4 log) 3) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server) 4) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ ที่ถูกเชื่อมต่ออยู่ในขณะนั้น (IP address of sending computer) 5) ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID)

	6) ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender e-mail address) 7) ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver e-mail address) 8) ข้อมูลที่บอกถึงสถานะในการตรวจสอบ (Status indicator) 9) ข้อมูลที่บอกถึงวันเวลาในการเชื่อมต่อของเครื่องที่เข้าใช้บริการเชื่อมกับ เครื่องให้บริการ (Date and time of connection of client to server) 10) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ใช้บริการที่เชื่อม ต่ออยู่ขณะเข้ามาใช้บริการ (IP address of client connected to server) 11) ชื่อผู้ใช้งาน (User ID) ถ้ามี 12) ข้อมูลจดหมายอิเล็กทรอนิกส์ที่ถูกส่งคืน
ค. ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล	1) ข้อมูล log ที่บันทึกเมื่อมีการเข้าถึงเครื่องให้บริการโอนแฟ้มข้อมูล 2) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server)

	3) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น (IP source address) 4) ข้อมูลชื่อผู้ใช้งาน (User ID) (ถ้ามี) 5) ข้อมูลตำแหน่ง (path) และ ชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการ ส่งขึ้นมาบันทึก หรือให้ดึงข้อมูลออกไป (Path and filename of data object uploaded or downloaded)
ง ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ	1) ข้อมูล log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ให้บริการเว็บ 2) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ 3) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น 4) ข้อมูลคำสั่งการใช้งานระบบ 5) ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI : Uniform Resource Identifier) ดูภาษาไทยใหม่
จ. ชนิดของข้อมูลบนเครือข่าย	1) ข้อมูล log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย (NNTP log)

คอมพิวเตอร์ขนาดใหญ่ (Usenet)	2) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server) 3) ข้อมูลหมายเลข port ในการใช้งาน (Protocol process ID) 4) ข้อมูลชื่อเครื่องให้บริการ (Host name) 5) ข้อมูลหมายเลขลำดับข้อความที่ได้ถูกส่งไปแล้ว (Posted message ID)
ฉ. ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Messaging (IM) เป็นต้น	ข้อมูล log เช่นข้อมูลเกี่ยวกับวัน เวลาการติดต่อของผู้ใช้บริการ (Date and time of connection of client to server) และ/หรือข้อมูลชื่อเครื่องบนเครือข่าย และ/หรือหมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ ในขณะนั้น (Hostname and/or IP address) เป็นต้น

3. ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ 5 (1) ง. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก. ผู้ให้บริการร้านอินเทอร์เน็ต	1)ข้อมูลที่สามารถระบุตัวบุคคล 2)เวลาของการเข้าใช้ และเลิกใช้บริการ 3)หมายเลขเครื่องที่ใช้ IP Address

4. ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ 5 (2) มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ (Content Service Provider)	1) ข้อมูลรหัสประจำตัวผู้ใช้หรือข้อมูลที่สามารถระบุตัวผู้ใช้บริการได้ และ/หรือเลขประจำตัว (User ID) ของผู้ขายสินค้าหรือบริการและ/หรือเลขประจำตัวผู้ใช้บริการ (User ID) และ/หรือที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการ 2) บันทึกข้อมูลการเข้าใช้บริการ 3) กรณีผู้ให้บริการเว็บบอร์ด (Web board) หรือผู้ให้บริการบล็อค (Blog) ให้เก็บข้อมูลของผู้ประกาศ (Post) ข้อมูล 4) ข้อมูลที่จำเป็นต่อการทำธุรกรรมเฉพาะด้าน เช่น ชื่อ สกุล รหัสประจำตัวประชาชนของผู้ใช้บริการหรือเอกสารอื่นที่มีผลใช้บังคับได้ตาม กฎหมาย หรือรหัส

	ประจำตัวผู้ใช้ ที่สามารถระบุตัวผู้ใช้บริการได้ และ/หรือ เลขบัญชีธนาคารของผู้ใช้บริการ และ/หรือข้อมูลที่เป็นประโยชน์ต่อการชำระเงิน เช่น เลขบัญชีธนาคาร หรือ เลขบัตรเครดิต และ/หรือข้อมูลที่สามารถแสดงถึงการซื้อขายสินค้าหรือบริการ โดยข้อมูลที่กล่าวมาต้องได้รับการเข้ารหัสลับเพื่อป้องการสำเนาไปใช้ ประโยชน์จากผู้ไม่มีสิทธิ

ทั้งนี้รายละเอียดของการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่กฎหมายระบุไว้นั้น เป็นเพียงแนวทางในการจัดเก็บเพื่อระบุตัวผู้กระทำความผิดและวันเวลาที่กระทำความผิด โดยต้องมีมาตรการที่รักษาความสมบูรณ์ของข้อมูลตามสมควร ซึ่งขึ้นอยู่กับประเภทและขนาดขององค์กร รวมถึงงบประมาณแต่ละกรณีๆไป แต่ไม่ได้หมายความว่าผู้ให้บริการทุกรายต้องจัดเก็บในมาตรฐานแบบเดียวกัน ทั้งหมดตามทีระบุไว้ในประกาศของกระทรวงไอซีที

มาตราที่ 27

ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา 18 หรือมาตรา 20 หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา 21 ต้องระวางโทษปรับไม่เกินสองแสนบาทและปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรานี้เป็นเรื่องบทกำหนดโทษที่ให้อำนาจศาลหรือพนักงานเจ้าหน้าที่ในการดำเนินคดีกับบุคคลที่ปฏิเสธไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่ที่สั่งให้มีการส่งมอบข้อมูลจราจรคอมพิวเตอร์หรือคำสังอื่นใดตามที่ระบุไว้ในมาตรา 18 หรือในกรณีที่รัฐมนตรีว่าการกระทรวงไอชทีมีคำสั่งให้ปิดบล็อคเว็บไต์ หรือระงับการเผยแพร่ข้อมูลคอมพิวเตอร์ และเจ้าของเว็บไซต์หรือผู้ให้บริการไม่ปฏิบัตตาม รวมถึงกรณีที่

รัฐมนตรีว่าการกระทรวงไอซีทีมีประกาศว่าชุดคำสั่งใดเป็นคำสั่งประสงค์ร้ายที่ห้ามจำหน่ายและเผยแพร่

มาตราที่ 28

การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้ และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

ซึ่งมีรายละเอียดเพิ่มเติมตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ดังนี้

ข้อ 1 ในประกาศนี้

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

“รัฐมนตรี” หมายความว่า รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ 2 พนักงานเจ้าหน้าที่ ต้องมีคุณสมบัติ ดังต่อไปนี้

(1) มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์

(2) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรีทางวิศวกรรมศาสตร์ วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือรัฐประศาสนศาสตร์

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

(4) มีคุณสมบัติอื่นอย่างหนึ่งอย่างใด ดังต่อไปนี้

ก. รับราชการหรือเคยรับราชการไม่น้อยกว่าสองปีในตำแหน่งเจ้าหน้าที่ตรวจพิสูจน์พยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์หรือพยานหลักฐานอิเล็กทรอนิกส์

ข. สำเร็จการศึกษาตามข้อ 2 (2) ในระดับปริญญาตรี และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสี่ปี

ค. สำเร็จการศึกษาตามข้อ 2 (2) ในระดับปริญญาโท หรือสอบไล่ได้เป็นเนติบัณฑิตตามหลักสูตรของสำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสามปี

ง. สำเร็จการศึกษาตามข้อ 2 (2) ในระดับปริญญาเอก หรือมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงาน ตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสองปี

จ. เป็นบุคคลที่ทำงานเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ หรือมีประสบการณ์ในการดำเนินคดีเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ไม่น้อยกว่าสองปี

ข้อ 3 ในกรณีที่มีความจำเป็นเพื่อประโยชน์ของทางราชการในการสืบสวนและสอบสวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จำเป็นต้องมีบุคลากรซึ่งมีความรู้ความชำนาญ หรือประสบการณ์สูง เพื่อดำเนินการสืบสวนและสอบสวนการกระทำผิดหรือคดีเช่นว่านั้น หรือเป็นบุคลากรในสาขาที่ขาดแคลน รัฐมนตรีอาจยกเว้นคุณสมบัติตามข้อ 2 ไม่ว่าทั้งหมดหรือบางส่วนสำหรับการบรรจุและแต่งตั้งบุคคลใดเป็นการเฉพาะก็ได้

ข้อ 4 การแต่งตั้งบุคคลหนึ่งบุคคลใดเป็นพนักงานเจ้าหน้าที่ให้แต่งตั้งจากบุคคลซึ่งมีคุณสมบัติตามข้อ 2 หรือข้อ 3 โดยบุคคลดังกล่าวต้องผ่านการประเมินความรู้ความสามารถหรือทดสอบตามหลักสูตรและหลักเกณฑ์ที่รัฐมนตรีประกาศกำหนดการแต่งตั้งบุคคลใดเป็นพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ ดำรงตำแหน่งในวาระคราวละ 4 ปี และการแต่งตั้งให้ประกาศในราชกิจจานุเบกษา

ข้อ 5 พนักงานเจ้าหน้าที่ต้องไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(1) เป็นบุคคลล้มละลาย บุคคลไร้ความสามารถ หรือบุคคลเสมือนไร้ความสามารถ

(2) เป็นสมาชิกสภาผู้แทนราษฎร สมาชิกวุฒิสภา ข้าราชการการเมือง สมาชิกสภาท้องถิ่นผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งที่รับผิดชอบในการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่ในพรรคการเมือง

(3) เป็นผู้อยู่ระหว่างถูกสั่งให้พักราชการหรือถูกสั่งให้ออกจากราชการไว้ก่อน

(4) ถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หน่วยงานของรัฐหรือรัฐวิสาหกิจเพราะทำผิดวินัย หรือรัฐมนตรีให้ออกจากการเป็นพนักงานเจ้าหน้าที่ เพราะมีความประพฤติเสื่อมเสียบกพร่องหรือไม่สุจริตต่อหน้าที่หรือหย่อนความสามารถ

(5) ได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษ สำหรับความผิดที่กระทำโดยประมาทหรือความผิดลหุโทษ

(6) ต้องคำพิพากษาหรือคำสั่งของศาลให้ทรัพย์สินตกเป็นของแผ่นดิน เพราะร่ำรวยผิดปกติหรือมีทรัพย์สินเพิ่มขึ้นผิดปกติ

ข้อ 6 พนักงานเจ้าหน้าที่พ้นจากตำแหน่งเมื่อ

(1) ตาย

(2) ลาออก

(3) ถูกจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก

(4) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามข้อ ๕

(5) รัฐมนตรีให้ออก เพราะมีความประพฤติเสื่อมเสีย บกพร่องหรือไม่สุจริตต่อหน้าที่หรือหย่อนความสามารถ

(6) ครบวาระการดำรงตำแหน่ง

ข้อ 7 ประกาศนี้มีผลใช้บังคับตั้งแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

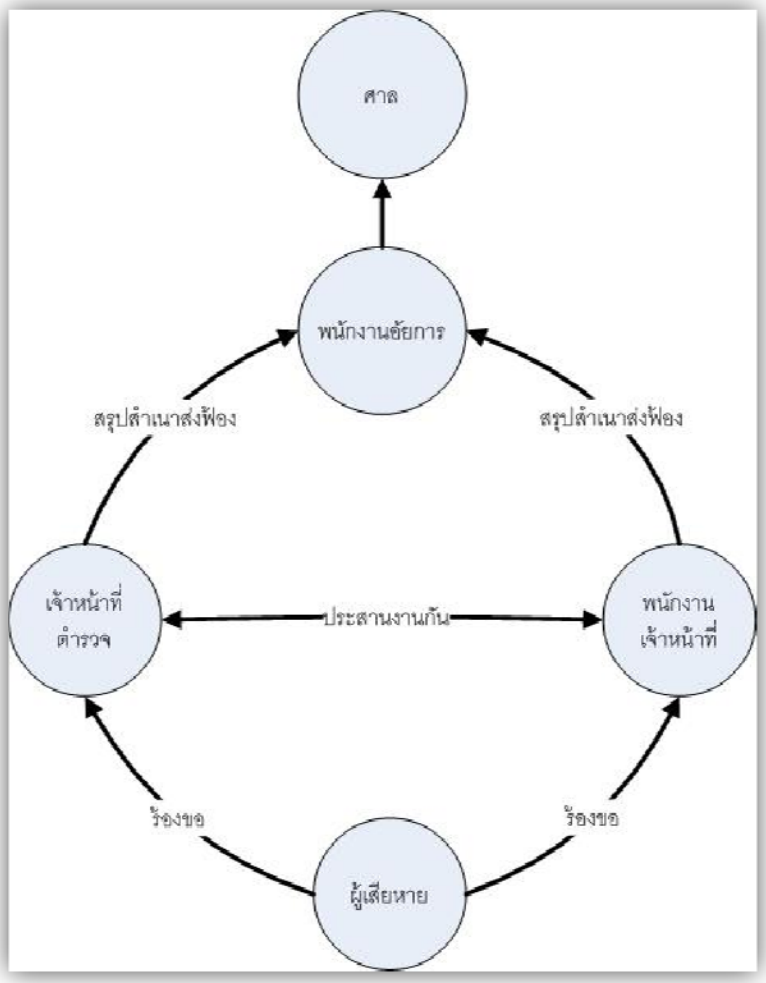
มาตราที่ 29

ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์ หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

ตามที่ พ.ร.บ. ว่าด้วยการกระทำความผิดเยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งทำขึ้นระหว่างสำนักงานตำรวจแห่งชาติและกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งจะระบุขอบเขตของอำนาจหน้าที่ของพนักงานเจ้าหน้าที่และเจ้าหน้าที่ตำรวจไว้ ดังรูปที่ 3.1



รูปที่ 3.1 ขอบเขตอำนาจหน้าที่ของพนักงานเจ้าหน้าที่และเจ้าหน้าที่ตำรวจ

มาตราที่ 30

ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง

บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

บทที่ 4
กรณีศึกษาของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ตั้งแต่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้มีผลบังคับใช้ตั้งแต่ 18 กรกฎาคม 2550 ก็ได้มีการนำมาใช้จับกุมดำเนินคดีอยู่หลายกรณี ซึ่งในบทนี้จะยกตัวอย่างข้อมูลจากที่สื่อต่างๆได้มีการเผยแพร่ข้อมูลการจับกุมออกมา

กรณีศึกษาที่ 1

จับ ผอ.เว็บประชาไทคาสุวรรณภูมิหมิ่นเบื้องสูง

ฐานนำข้อมูลเท็จใส่ร้ายทำให้เกิดความเสียหายต่อผู้อื่น แก่ประเทศ เจอแค่คนดูแลเว็บ ยังให้การปฏิเสธ

เมื่อเวลาประมาณ 15.00 น. วันที่ 6 มี.ค. เจ้าหน้าที่ตำรวจทั้ง ในและนอกเครื่องแบบ 5 คน เจ้าหน้าที่ตำรวจหญิง 1 คน และเจ้าหน้าที่ในเครื่องแบบ 1 คน เดินทางด้วยรถยนต์ จำนวน 2 คัน เข้าแสดงตนพร้อมหมายค้นและหมายจับ น.ส. จีรนุช เปรมชัยพร ผู้ดูแลเว็บไซต์ประชาไท ด้วยข้อหากระทำความผิดตามมาตรา 15 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ขณะนี้อยู่ระหว่างการสอบสวน โดย น.ส. จีรนุช ปฏิเสธให้การใดๆ จนกว่าจะมีทนายความให้คำปรึกษา

สำหรับมาตรา 15 ว่าด้วยพ.ร.บ.กระทำความผิดเกี่ยวกับคอมพิวเตอร์ ระบุว่า ผู้ให้บริการผู้ใดจงใจสนับสนุน หรือ ยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ 1) นำข้อมูลปลอมไม่ว่าทั้งหมด บางส่วน หรือ ข้อมูลเท็จ ที่น่าจะเกิดความเสียหายแก่ผู้อื่น หรือ ประชาชน 2) ข้อมูลเท็จที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือ ก่อให้เกิดความตื่นตระหนกแก่ประชาชน 3) ข้อมูลคอมพิวเตอร์อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือ ความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา 4) ข้อมูลคอมพิวเตอร์ที่มีลักษณะลามกและข้อมูลนั้นประชาชนทั่วไปสามารถเข้าถึง ได้ เข้าสู่ระบบคอมพิวเตอร์ รวมถึง 5) เผยแพร่ หรือ ส่งต่อ ข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูล คอมพิวเตอร์ตามข้อ 1, 2, 3 หรือ 4 ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 1 แสนบาท หรือ ทั้งจำทั้งปรับ

ข้อมูลจาก ข่าวสด วันที่ 6 มี.ค. 2552

ตม.สุวรรณภูมิ จับ"จีรนุช เปรมชัยพร" ผอ.เว็บไซต์ประชาไท อ้างตามหมายจับจากศาลขอนแก่น

พ.ต.อ. ภัคพงศ์ สายอุบล ผกก.สืบสวนปราบปราม บก.ตม.2 เปิดเผยว่า นางสาวจีรนุช เปรมชัยพร อายุ 43 ปี บรรณาธิการเว็บไซต์ประชาไท ตามหมายจับศาลจังหวัดขอนแก่น ที่ จ.311/2552 ลงวันที่ 8 กันยายน 2552 ซึ่งต้องหาว่ากระทำความผิดฐาน “ร่วมกันประกาศแก่บุคคลทั่วไปให้กระทำความผิด, ร่วมกันหมิ่นประมาท ดูหมิ่นหรือแสดงความอาฆาตมาดร้าย พระมหากษัตริย์ พระราชินี รัชทายาทหรือผู้สำเร็จราชการแทนพระองค์, ทำให้ปรากฏแก่ประชาชนด้วยวาจา หนังสือหรือวิธีอื่นใด อันมิใช่เป็นการกระทำภายในความมุ่งหมายแห่งรัฐธรรมนูญ หรือมิใช่เพื่อแสดงความคิดเห็นหรืออติชมโดยสุจริต เพื่อให้เกิดความปั่นป่วนหรือกระด้างกระเดื่องในหมู่ประชาชนถึงขนาดที่จะก่อ ความไม่สงบขึ้นในราชอาณาจักร หรือเพื่อให้ประชาชนล่วงละเมิดกฎหมายแผ่นดิน, นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการ ก่อการร้ายตามประมวลกฎหมายอาญา และเป็นผู้ให้บริการจงใจสนับสนุนหรือยินยอมให้มีการกระทำผิดในระบบ คอมพิวเตอร์ในความควบคุมของตนเอง” พ.ต.อ.ภัคพงศ์ กล่าวว่า

เจ้าหน้าที่สืบสวนปราบปราม บก.ตม.2 ได้รับแจ้งจากแหล่งข่าวจะมีผู้ต้องหาตามหมายจับเดินทางเข้ามาในราชอาณาจักร จึงได้ออกตรวจสอบภายในท่าอากาศยานสุวรรณภูมิ โดยประสานกับฝ่าย ตม.ขาเข้าร่วมตรวจสอบ กระทั่งพบผู้ต้องหาเดินทางกลับมาจากประเทศฟินแลนด์ ด้วยสายการบินฟินแอร์ เที่ยวบินที่ AY 095 และขณะที่นำหนังสือเดินทางมาขอรับการตรวจอนุญาตเดินทางเข้าราชอาณาจักร ตำรวจจึงแสดงหมายจับ เข้าจับกุมตัว จากการสอบสวนในเบื้องต้นผู้ต้องหาให้การว่าเป็นเพียง WEB MASTER ผู้ควบคุมดูแลระบบคอมพิวเตอร์ในเว็บไซต์ และให้การปฏิเสธตลอดข้อกล่าวหา จึงควบคุมตัวส่งพนักงานสอบสวน สภ.เมืองขอนแก่น ดำเนินคดีตามกฎหมายต่อไป กักตัว ผอ.ประชาไท ที่สุวรรณภูมิ ความผิดตาม พรบ.คอมพิวเตอร์ มาตรา 14-15 เบื้องต้นแจ้งว่ามีหมายจับจากศาลจังหวัดขอนแก่น และจะต้องส่งตัวไปยังขอนแก่น ขณะนี้ยังไม่ทราบข้อกล่าวหาที่ชัดเจน โดยที่ผ่านมา บก.ประชาไท ระบุว่า ยังไม่เคยได้รับหมายเรียกแต่อย่างใด

ผู้สื่อข่าวรายงานหมายเลขคดีของ นส.จีรนุช คือ ปจว.ข้อ ก. หรือคดีที่ 4371/2551วันที่ 11 ส.ค. 51 เป็นการฟ้องโดยผู้กำกับการ สภ.อ.เมืองขอนแก่น ผู้ดูแลระบบร่วมกับผู้ใช้กระทำความผิดมาตรา 14 และมาตรา 15 พรบ.คอมพิวเตอร์ หมายระบุว่า ข้อความที่ผิดเกิดขึ้นเมื่อวันที่ 27 เม.ย. 2552 ระบุสถานที่เกิดเหตุ ขอนแก่น โดยหมายจับลงวันที่ 8 ก.ย. 2552 มีพ.ตท.ชัชพงษ์ พงษ์สุวรรณ เป็นพนักงานสอบสวน ผู้สื่อข่าวรายงานว่า วันที่เดินทางไปยุโรปเพื่อร่วมการประชุมเมื่อ 2 อาทิตย์ก่อน น.ส.จีรนุช ได้ถูกเจ้าหน้าที่ ตม.กักตัวตรวจสอบโดยระบุว่า มีชื่อซ้ำกับคนที่จ.ขอนแก่น และในวันที่เดินทางกลับ ก็ถูกกักไว้ด้วยเหตุผลเดียวกัน ก่อนจะแจ้งว่ามีหมายจับ จากศาลขอนแก่นล่าสุด รายงานแจ้งว่า เจ้าหน้าที่กำลังทำบันทึกจับกุมที่สนามบิน จากนั้น จะส่งตัวไปที่ สภ.อ.ขอนแก่น ทางรถยนต์ทันที

ข้อมูลจาก http://www.posttoday.com **วันที่** 24 **กันยายน** 2553

กรณีศึกษาที่ 2

จับแพทย์หญิงโยงโพสต์ข่าวลือทุบหุ้น ผิดตาม พ.ร.บ.คอมพิวเตอร์

กทม. 17 พ.ย. เมื่อช่วงเย็นที่ผ่านมา พนักงานสอบสวนกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทาง เทคโนโลยี หรือ ปอท. ร่วมกับเจ้าหน้าที่กระทรวงไอซีที นำหมายจับของศาลอาญา เข้าตรวจค้นห้องพักรอยัลปาร์ค คอนโดมิเนียม ซอยพหลโยธิน 8 ซึ่งเป็นห้องพักของแพทย์หญิง ธัศพร รัตนวงศา แพทย์รังสีวิทยาโรงพยาบาลแห่งหนึ่งย่านฝั่งธนฯ เนื่องจากมีหลักฐานยืนยันว่า มีการโพสต์ข้อความไม่เป็นมงคลมาจากห้องพักของคอนโดฯ ดังกล่าว และพบว่าเป็นห้องพักของแพทย์หญิงธัศพร ซึ่งยอมรับว่าเป็นผู้โพสต์ข้อความ จน ส่งผลให้หุ้นตกติดต่อกัน 3 วัน คือระหว่างวันที่ 13-15 ตุลาคมที่ผ่านมา สร้างความเสียหายให้ตลาดหลักทรัพย์ฯ หลายร้อยล้านบาท พร้อมยึดของกลางคอมพิวเตอร์โน้ตบุ๊คจำนวน 1 เครื่อง ก่อนควบคุมตัวมาสอบปากคำที่ ปอท. ภายในศูนย์ราชการแจ้งวัฒนะ พร้อมตั้งข้อหาตามความผิด พ.ร.บ.คอมพิวเตอร์ ฐานนำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ ซึ่งก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

พล.ต.ต.เกรียงศักดิ์ อรุณศรีโสภณ ผู้บังคับการ ปอท. กล่าวว่าเบื้องต้นผู้ต้องหาให้การรับสารภาพ โดยยอมรับว่าเป็นผู้โพสต์ข้อความดังกล่าวลงในเว็บไซต์ประชาไท เบื้องต้นยังไม่พบว่ามีความเชื่อมโยงกับผู้ต้องหา 3 คนที่ถูกจับกุมไปก่อนหน้านี้ และยังไม่ได้สอบลึกถึงสาเหตุที่โพสต์ข้อความดังกล่าว ซึ่งพนักงานสอบสวนจะสอบสวนให้ละเอียดเพื่อให้ได้ข้อเท็จจริง ทั้งนี้ได้ตั้งหลักทรัพย์ประกันตัวไว้ 1 แสนบาท โดยมีเงื่อนไขต้องมารายงานตัวตามกำหนดและห้ามเดินทางออกนอกประเทศ

ข้อมูล วันที่ 19 พฤศจิกายน 2009 จาก

http://news.mcot.net/crime/inside.php?value=bmlkPTEyNjEwMiZudHlwZT10ZXh0

กรณีศึกษาที่ 3

ตำรวจสอบสวนกลาง รวบ 2 ผู้ต้องหาปล่อยข่าวมิบังควร ทุบหุ้น บ่อนทำลายความมั่นคง ลงเว็บไซต์ "ประชาไท-ฟ้าเดียวกัน" เจ้าตัวยังอ้างแค่แปลข่าวจากสำนักข่าวต่างประเทศ ไม่มีเจตนาทุบหุ้น

วันนี้ (1 พ.ย.) เมื่อเวลา 15.25 น.ที่สนามบินสุวรรณภูมิ พล.ต.ต.ปัญญา มาเม่น รอง ผบช.ก.พร้อมด้วย พ.ต.อ.พิสิษฐ์ เปาอินทร์ รอง ผบก.ปอท., พ.ต.อ.อาชยน ไกรทอง ผกก.1 บก.ทท., พ.ต.ท.พันธนะ นุชนารถ รอง ผบก.1บก.ทท.นำหมายศาลอาญา ที่ 3089/2552 ลงวันที่ 30 ต.ค.2552 ในความผิดตาม พ.ร.บ.ว่าด้วยการทำผิดเกี่ยวกับคอมพิวเตอร์ เข้าจับกุม น.ส.ธีรนันต์ วิภูชนิน อายุ 43 ปี อดีตกรรมการผู้จัดการบริษัทหลักทรัพย์ ยูบีเอส จำกัด อยู่บ้านเลขที่ 368 แขวงจันทรเกษม เขตจตุจักร กทม. ขณะเดินทางกลับจากกรุงเวียนนา ประเทศออสเตรีย โดยสายการบินออสเตรียแอร์ไลน์ เที่ยวบินที่ OS 0025 ก่อนควบคุมตัวสอบปากคำที่ศูนย์ร่วมบริการประชาชน กองบังคับการตำรวจท่องเที่ยวสุวรรณภูมิ

ทั้งนี้ เจ้าหน้าที่ได้ทำการสอบปากคำ น.ส.ธีรนันต์ เป็นเวลานานประมาณ 1 ชั่วโมง ก่อนแจ้งข้อหา "นำเข้าข้อมูลคอมพิวเตอร์อันเป็นเท็จโดยประการที่น่าจะก่อให้เกิดความเสีย หายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน พ.ร.บ.ว่าด้วยการทำผิดเกี่ยวกับคอมพิวเตอร์ มาตรา 14" พร้อมควบคุมตัว น.ส.ธีรนันต์ ไปยังกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)

ด้าน น.ส.ธีรนันต์ กล่าวเพียงสั้นๆ ด้วยสีหน้ายิ้มแย้มไม่มีท่าทีวิตกกังวลว่า ตนได้แปลข้อความจากเว็บไซต์สำนักข่าวต่างประเทศ และนำไปโพสต์ลงในเว็บไซต์ เนื่องจากวันดังกล่าวหุ้นตกลงอย่างรุนแรงมาก ประชาชนอยากรู้ว่าเกิดจากอะไรขึ้น ไม่ได้มีเจตนาเผยแพร่ข้อความเพื่อทำให้หุ้นตก

ทั้งนี้ ตำรวจได้ตรวจยึดคอมพิวเตอร์โน้ตบุ๊กยี่ห้อเอชพี 1 เครื่อง กล้องดิจิตอลลูมิกซ์ 1 ตัว เมมโมรีการ์ด 1 อัน โทรศัพท์มือถือยี่ห้อโซนี่อีริคสัน 1 เครื่อง ของ น.ส.ธีรนันต์ ไว้ตรวจสอบ พร้อมกับนำกำลังส่วนหนึ่งเข้าตรวจสอบฮาร์ดดิสก์ เครื่องคอมพิวเตอร์ที่

บ้านของ น.ส.ธีรนันต์ ตั้งอยู่เลขที่ 368 ซอยเสือใหญ่อุทิศ ถนนรัชดาภิเษก แขวงจอมพล เขตจตุจักร กทม.ซึ่งเป็นบ้านเดี่ยว เนื้อที่ 200 ตารางวา โดยผู้สื่อข่าวรายงานว่า เว็บไซต์ที่ น.ส.ธีรนันต์ นำข้อความไปโพสต์ คือ เว็บประชาไทดอตคอม

ผู้สื่อข่าวรายงานด้วยว่า เมื่อเวลา 13.30 น.วันเดียวกัน เจ้าหน้าที่ตำรวจได้นำหมายศาลอาญา ในข้อหาเดียวกันเข้าจับกุม นายคธา ปาจริยพงษ์ อายุ 37 ปี พนักงานบรษัทหลักทรัพย์ซิมิโก้ จำกัด (มหาชน) ได้ที่ อาคารลิเบอร์ตี้ ถ.สีลม แขวงและเขตบางรัก กทม.ซึ่งเป็นผู้นำข้อความที่เข้าข่ายความผิดโพสต์ลงในเว็บไซต์ฟ้าเดียวกัน ก่อนขยายผลเข้าตรวจค้นบ้านพัก และนำตัวควบคุมตัวไปสอบที่ บก.ปอท.

ผู้สื่อข่าวรายงานว่า สำหรับเว็บไซต์ประชาไทดอตคอม และ ฟ้าเดียวกัน เป็นสองเว็บไซต์ได้รับความนิยมในกลุ่มคนเสื้อแดง และมักมีการนำเสนอบทความที่หมิ่นเหม่ต่อการจาบจ้วงสถาบันมาแล้วหลายครั้ง

ต่อมาเวลา 18.45 น.ที่กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) พล.ต.ท.ไถง ปราศจากศัตรู ผู้บัญชาการตำรวจสอบสวนกลาง (ผบช.ก.) พร้อมด้วย พล.ต.ต.ปัญญา มาเม่น รอง ผบช.ก. และ พ.ต.อ.พิสิษฐ์ เปาอินทร์ รอง ผบก.ปอท.ได้ทำการแถลงข่าว โดยไม่ได้นำตัว 2 ผู้ต้องหามาร่วมแถลงด้วย

พล.ต.ท.ไถง กล่าวว่า หลังเกิดเหตุกรณีการปล่อยข่าวลืออันไม่เป็นมงคล และส่งผลทำให้ตลาดหุ้นได้รับผลกระทบอย่างรุนแรง พล.ต.อ.ปทีป ตันประเสริฐ รักษาราชการแทนผู้บัญชาการตำรวจแห่งชาติ (รรท.ผบ.ตร.) ได้สั่งการให้ตนตั้งคณะพนักงานสอบสวนขึ้นมาเพื่อดำเนินการสืบสวนสอบสวนเอา ผิดกับผู้ที่ดำเนินการ

โดยตำรวจจะดำเนินคดีเฉพาะในส่วนของการปล่อยข่าวลือ ซึ่งเป็นความผิดตาม พ.ร.บ.ว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ มาตรา 14 แต่หากพบว่าการกระทำเข้าข่ายเป็นความผิดเกี่ยวกับหลักทรัพย์และตลาดหลัก ทรัพย์ ซึ่งเป็นกฎหมายอีกฉบับก็จะส่งข้อมูลให้กรมสอบสวนคดีพิเศษ หรือ ดีเอสไอ ซึ่งเป็นผู้รับผิดชอบ รับไป

ดำเนินการ สำหรับ 2 ผู้ต้องหาที่ถูกจับกุม ในชั้นนี้ได้แจ้งข้อหาตามความผิด พ.ร.บ.ว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ มาตรา 14

"ทางคณะพนักงานสอบสวนได้ร่วมกับกระทรวงไอซีที จับกุมผู้จ้องหาได้ 2 คน ซึ่งได้นำข้อความอันเป็นเท็จ เข้าสู่ระบบคอมพิวเตอร์ ซึ่งเป็นความผิดตาม พ.ร.บ.นี้"

ด้าน พล.ต.ต.ปัญญา มาเม่น รอง ผบช.ก.กล่าวว่า ตำรวจได้นำหมายศาลเข้าจับกุมผู้ต้องหา 2 คน และหลังจากจับกุมได้กระจายกำลังเจ้าหน้าที่ออกตรวจค้น เพื่อหาพยานหลักฐานที่ทำงาน และบ้านพักของผู้ต้องหาทั้ง 2 ซึ่งก็ได้พยานหลักฐานมาจำนวนหนึ่ง แต่ไม่สามารถเปิดเผยในรายละเอียดได้ เนื่องจากจะต้องทำการตรวจสอบของกลาง และควบคุมตัวผู้ต้องหาไว้ทำการสอบสวนขยายผลไปยังผู้ร่วมขบวนการที่เหลือต่อ ไป

เมื่อผู้สื่อข่าวถามว่า การกระทำของทั้ง 2 คน เชื่อมโยงกันหรือไม่ พล.ต.ต.ปัญญา กล่าวว่า อยู่ระหว่างทำการการตรวจสอบ เมื่อถามว่า มีใครได้ประโยชน์หรือไม่ ก็อยู่ระหว่างการตรวจสอบเช่นกัน

ส่วนจะมีการขยายผลและออกหมายจับเพิ่มเติมหรือไม่ รอง ผบช.ก.กล่าวว่า ขณะนี้ได้ประสานกับสำนักงานข่าวกรองแห่งชาติ และกระทรวงไอซีที เพื่อทำการสอบสวนว่ามีผู้ต้องสงสัย บางกลุ่ม มีพฤติกรรมในการโพสข้อความลงในอินเตอร์เน็ตหรือไม่ ซึ่งหากพบก็จะดำเนินการรวบรวมพยานหลักฐานเพื่อขอศาลออกหมายจับและหมายค้นต่อ ไป เนื่องจากหากปล่อยให้เนิ่นนานเกรงว่า กลุ่มบุคคลดังกล่าว อาจจะทำลายหลักฐานได้

อย่างไรก็ตาม สำหรับ 2 ผู้ต้องหาที่ถูกจับกุมได้ พนักงานสอบสวนได้ควบคุมตัวไว้ทำการสอบสวนเพื่อขยายผลที่กองบังคับการปราบ ปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) โดยไม่อนุญาตให้ประกันตัว

ข้อมูล วันที่ 1 พฤศจิกายน 2552 จาก

http://www.manager.co.th/Crime/ViewNews.aspx?NewsID=9520000130815

กรณีศึกษาที่ 4

ปดส.บุกรวบ นศ.สาว ม.ดังมือโพสต์แพร่คลิปอนาจาร นร.หญิงสำเร็จความใคร่ด้วยปากให้เพื่อนชายบนรถเมล์ปรับอากาศ สารภาพ รับคลิปมาจากเพื่อนทางอีเมล ก่อนนำไปโพสต์ลงในเว็บไซต์ต่าง ๆ หลายแห่ง อ้างรู้เท่าไม่ถึงการณ์ และไม่ทราบว่าการกระทำดังกล่าวจะมีความผิด เผย การจับกุมมือโพสต์เผยแพร่คลิปวิดีโอลามกอนาจารทางอินเทอร์เน็ตเป็นครั้งแรกหลังจากที่มีการบังคับใช้ พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

วันนี้ (11 มี.ค.) ที่ บก.ปดส.พล.ต.ต.วิมล เปาอินทร์ ผบก.ปดส.สั่งการให้ พ.ต.อ.วรพงษ์ ทองไพบูลย์ ผกก.ฝป.10 บก.ปดส. พ.ต.ท.ปัญญา ชะเอมเทศ สว.ฝป.10 บก.ปดส.นำหมายค้นศาลอาญา เข้าตรวจค้นบ้านเลขที่ 9/36 หมู่ 3 แขวงและเขตลาดพร้าว หลังสืบทราบว่าเป็นสถานที่ใช้เผยแพร่คลิปวิดีโอนักเรียนหญิงกำลังสำเร็จความ ใคร่ด้วยปากให้กับเพื่อนชายบนรถโดยสารประจำทางปรับอากาศ ซึ่งกลายเป็นข่าวโด่งดังไปแล้วก่อนหน้านี้

เมื่อไปถึงเจ้าหน้าที่ตำรวจพบ น.ส.แสงดาว (นามสมมติ) อายุ 20 ปี นักศึกษาชั้นปีที่ 3 คณะบริหารคอมพิวเตอร์ มหาวิทยาลัยเอกชนชื่อดังแห่งหนึ่ง อยู่ในบ้าน จึงเชิญมาสอบสวน พร้อมตรวจยึดเครื่องคอมพิวเตอร์ 1 เครื่อง และอุปกรณ์ที่เกี่ยวข้องรวมทั้งเอกสารรวมทั้งสิ้น 8 รายการ

น.ส.แสงดาว รับสารภาพว่า ได้รับคลิปดังกล่าวจากเพื่อนที่ส่งอีเมลมาให้ เมื่อต้นปีที่ผ่านมา จากนั้นก็นำไปโพสต์ลงเว็บไซต์ต่างๆ หลายแห่ง โดยไม่ได้เป็นการกระทำในเชิงพาณิชย์ ทั้งนี้ตนรู้เท่าไม่ถึงการณ์ ไม่ทราบมาก่อนว่าการกระทำเช่นนี้จะเป็นความผิด

“หนูไม่ทราบว่า การส่งอีเมลและโพสต์ลงเว็บไซต์ต่างๆ จะมีความผิดตามกฎหมาย ซึ่งหากทราบว่าผิดหนูคงไม่ทำแน่นอน” น.ส.แสงดาว กล่าว

เจ้าหน้าที่จึงแจ้งข้อหานำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูล คอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้น ประชาชนทั่วไปอาจเข้าถึงได้และเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดย รู้อยู่แล้วว่าเป็นคอมพิวเตอร์ ตาม พ.ร.บ.ว่าด้วยการ

กระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14(5), (1) หรือ (4) มีโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ

สำหรับการจับกุมครั้งนี้ถือว่าเป็นการจับกุมผู้ที่เผยแพร่คลิปวิดีโอลามกอนาจารทางอินเทอร์เน็ตเป็น ครั้งแรก หลังจากที่มีการบังคับใช้ พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ อย่างไรก็ตาม เป็นที่น่าสังเกตว่า ในการจับกุมผู้กระทำความผิดลักษณะนี้ มักจะจับกุมได้แต่ผู้ที่เผยแพร่ แต่ยังไม่เคยมีการขยายผลจับกุมเจ้าของเว็บไซต์เหล่านั้นได้แต่อย่างใด ทั้งนี้ อาจเป็นเพราะเว็บไซต์เหล่านั้นไปจดทะเบียนอยู่ต่างประเทศ ทำให้ยากต่อการติดตามจับกุม

ข้อมูล วันที่ 11 มีนาคม 2551 จาก

http://www.manager.co.th/Crime/ViewNews.aspx?NewsID=9510000030042

บทที่ 5
ความรู้เบื้องต้นเกี่ยวกับคอมพิวเตอร์

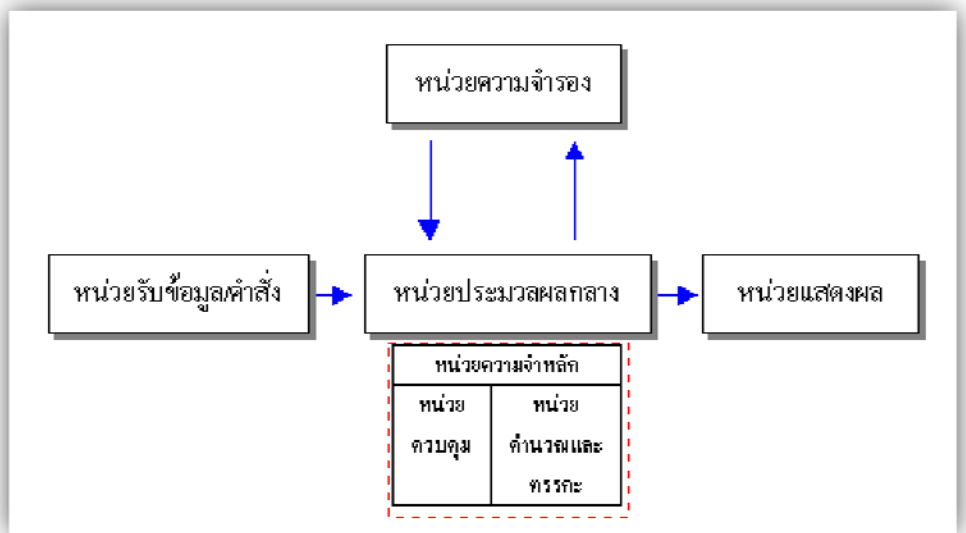
ในสังคมความรู้ (Knowledge-based Society) ข้อมูล ข่าวสาร และสารสนเทศ (Information) เป็นสิ่งสำคัญอย่างยิ่งต่อการดำเนินงานทั้งของภาครัฐและเอกชน โดยเฉพาะอย่างยิ่งการประกอบธุรกิจในยุคดิจิทัลที่มีการนำเทคโนโลยีสารสนเทศเข้ามาช่วยประกอบการตัดสินใจ (Decision Making) ในการจัดการและบริหารงานด้านต่างๆ ข้อมูลและสารสนเทศนับเป็นทรัพยากรหลักที่ได้รับความสนใจจากบุคลากรทุกระดับ ทั้งนี้เนื่องมาจากการดำเนินงานทางธุรกิจมีความซับซ้อนมากขึ้นและเทคโนโลยีคอมพิวเตอร์ที่มีประสิทธิภาพเพิ่มขึ้นด้วยเช่นกัน ทำให้ข่าวสารเป็นสิ่งที่ทุกคนจำเป็นจะต้องได้รับทราบและเข้าถึงได้อย่างรวดเร็ว

5.1 วงจรการทำงานของคอมพิวเตอร์

ในการทำงานของคอมพิวเตอร์ จะมีขั้นตอนการทำงานพื้นฐาน 4 ขั้นตอน ซึ่งประกอบด้วย การรับข้อมูลการประมวลผล การแสดงผล และการจัดเก็บข้อมูล หรือที่เรียกย่อๆว่า IPOS Cycle (Input Process Output Storage Cycle)

- **รับข้อมูล (input)** คอมพิวเตอร์จะทำหน้าที่รับข้อมูลเพื่อนำไปประมวลผล อุปกรณ์ที่ทำหน้าที่รับข้อมูลที่นิยมใช้ในปัจจุบัน เช่น แป้นพิมพ์ (Keyboard) เมาส์ (Mouse) สแกนเนอร์ (Scanner) ไมโครโฟน (Microphone) และกล้องดิจิตอล (Digital Camera) เป็นต้น
- **ประมวลผล (Process)** เมื่อคอมพิวเตอร์รับข้อมูลเข้าสู่ระบบแล้ว จะทำการประมวลผลตามโปรแกรมหรือคำสั่งที่กำหนด เช่น การคำนวณภาษี การคำนวณเกรดเฉลี่ย เป็นต้น

- **แสดงผล** (Output) คอมพิวเตอร์จะแสดงผลลัพธ์ที่ได้จากการประมวลผลไปยังหน่วยแสดงผล อุปกรณ์ทำหน้าที่แสดงผลที่ใช้แพร่หลายในปัจจุบัน ได้แก่ จอภาพ (Monitor) ลำโพง (Speaker) และเครื่องพิมพ์ (Printer) เป็นต้น
- **จัดเก็บข้อมูล** (Storage) คอมพิวเตอร์จะทำการจัดเก็บข้อมูลลงในอุปกรณ์เก็บข้อมูล เช่น ฮาร์ดดิสก์ (hard disk) แผ่นซีดีรอม (CD-ROM) และ USB Flash Drive เป็นต้น



รูปที่ 5.1 วงจรการทำงานของระบบคอมพิวเตอร์ (NECTEC)

5.2 ประเภทของคอมพิวเตอร์

คอมพิวเตอร์สามารถจำแนกได้หลายประเภท ขึ้นอยู่กับความแตกต่างของขนาดเครื่อง ความเร็วในการประมวลผล และราคาเป็นข้อพิจารณาหลัก โดยทั่วไปนิยมจำแนกประเภทคอมพิวเตอร์เป็น 7 ประเภทดังนี้

1. **ซูเปอร์คอมพิวเตอร์** (Supercomputer) เป็นคอมพิวเตอร์ที่มีขนาดใหญ่ที่สุด รุ่นแรกสร้างในปี ค.ศ. 1960 ที่องค์การทหารของสหรัฐอเมริกา สร้างสามารถประมวลผลได้กว่า 100 ล้านคำสั่งต่อวินาที จึงทำให้ทำงานได้รวดเร็วและมี

ประสิทธิภาพสูง มีราคาแพงที่สุด เป็นเครื่องคอมพิวเตอร์ที่เหมาะกับงานคำนวณที่ต้องคำนวณตัวเลขจำนวนมหาศาลให้เสร็จภายในระยะเวลาอันสั้น โดยต้องอยู่ในห้องที่มีการควบคุมอุณหภูมิและปราศจากฝุ่นละออง มักใช้กับองค์การที่มีขนาดใหญ่เท่านั้น เนื่องจากสามารถรองรับการใช้งานของผู้ใช้จำนวนมากพร้อม ๆ กันได้ เรียกว่า *มัลติโปรเซสซิ่ง (Multiprocessing)* อันเป็นการใช้หน่วยประมวลผลหลายตัว เพื่อให้คอมพิวเตอร์สามารถทำงานหลายงานพร้อม ๆ กันได้ จึงนิยมใช้กับงานที่การคำนวณที่ซับซ้อน เช่น การพยากรณ์อากาศ การทดสอบทางอวกาศ การคำนวณทางวิทยาศาสตร์ การบินอุตสาหกรรมน้ำมัน ตลอดจนการวิจัยในห้องปฏิบัติการ ทั้งของภาครัฐบาลและเอกชน เป็นต้น โดยหน่วยงานที่มีการใช้ซูเปอร์คอมพิวเตอร์ ได้แก่ องค์การนาซา (NASA) และหน่วยงานธุรกิจขนาดใหญ่ เช่น บริษัท General Motors และ AT&T เป็นต้น

รูปที่ 5.2 ซูเปอร์คอมพิวเตอร์

2. **เมนเฟรมคอมพิวเตอร์** (Mainframe Computer) เป็นเครื่องคอมพิวเตอร์ขนาดใหญ่มีความเร็วในการประมวลผลสูงรองลงมาจากซูเปอร์คอมพิวเตอร์ ต้องอยู่ในห้องที่ควบคุมอุณหภูมิและปราศจากฝุ่นละออง และได้รับการ

พัฒนาให้มีหน่วยประมวลผลหลายหน่วยทำงานพร้อม ๆ กันเช่นเดียวกับซูเปอร์คอมพิวเตอร์ แต่มีจำนวนหน่วยประมวลผลที่น้อยกว่า จึงทำให้สามารถประมวลผลคำสั่งได้หลายสิบล้านคำสั่งต่อวินาที ระบบคอมพิวเตอร์ของเครื่องเมนเฟรมส่วนมากจะมีระบบคอมพิวเตอร์ย่อย ๆ ประกอบอยู่ด้วย เพื่อช่วยในการทำงานบางประเภทให้กับเครื่องหลัก มีราคาแพงมาก (แต่น้อยกว่าซูเปอร์คอมพิวเตอร์) เหมาะกับงานที่มีข้อมูลที่มีปริมาณมากต้องประมวลผลพร้อมกันโดยผู้ใช้นับพันคน (Multi-user) ใช้กับองค์การใหญ่ ๆ ทั่วไป เช่น งานด้านวิศวกรรมคอมพิวเตอร์ วิทยาศาสตร์ การควบคุมระบบเครือข่าย งานพัฒนาระบบ งานด้านธุรกิจ ธนาคาร งานสำมะโนประชากร งานสายการบิน งานประกันชีวิต และมหาวิทยาลัย เป็นต้น

รูปที่ 5.3 เมนเฟรมคอมพิวเตอร์

3. **มินิคอมพิวเตอร์ หรือ คอมพิวเตอร์ขนาดกลาง** (Minicomputer) **หรือเรียกว่า** Mid-range Computer/Server เป็นเครื่องคอมพิวเตอร์ที่มีขนาดกลางที่มีประสิทธิภาพในการทำงานน้อยกว่าเมนเฟรมแต่สูงกว่าไมโครคอมพิวเตอร์ สามารถรองรับการทำงานจากผู้ใช้หลายร้อยคน (Multi-user) ในการทำงานที่แตกต่างกัน (Multi Programming) เช่นเดียวกับเครื่องเมนเฟรม แต่สิ่งที่แตกต่างกันระหว่างเครื่องเมนเฟรมและเครื่องมินิคอมพิวเตอร์ คือ ความเร็วในการทำงาน เนื่องจากมินิคอมพิวเตอร์ทำงานได้ช้ากว่า และควบคุมผู้ใช้งานต่าง ๆ ในจำนวนที่น้อยกว่า

รวมทั้งสื่อที่เก็บข้อมูลมีความจุน้อยกว่าเมนเฟรม จึงเหมาะกับองค์การขนาดกลาง เพราะมีราคาถูกกว่าเครื่องเมนเฟรมมาก ทำงานเฉพาะด้าน เช่น การคำนวณทางด้านวิศวกรรม การจองห้องพักของโรงแรม การทำงานด้านบัญชีขององค์การธุรกิจ เป็นต้น ซึ่งในสถานศึกษาต่าง ๆ และบางหน่วยงานของรัฐนิยมใช้คอมพิวเตอร์ประเภทนี้

รูปที่ 5.4 มินิคอมพิวเตอร์

4. **ไมโครคอมพิวเตอร์** (Microcomputer) เป็นเครื่องคอมพิวเตอร์ขนาดเล็ก ราคาถูกสามารถเรียกได้อีกอย่างหนึ่งว่า ***เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer หรือ PC)*** มีการพัฒนาขึ้นในปี ค.ศ. 1975 ซึ่งได้รับความนิยมเป็นอันมาก เมื่อ IBM ได้สร้างเครื่อง IBM PC ออกมา สามารถใช้งานโดยใช้คนเดียว (Stand-alone) หรือเชื่อมต่อเป็นเครือข่ายเพื่อติดต่อสื่อสารกับคอมพิวเตอร์เครื่องอื่นได้ จากการที่เทคโนโลยีที่ก้าวนำสมัยทำให้ PC สามารถเชื่อมโยงเข้ากับระบบเครือข่ายอินเทอร์เน็ตติดต่อสื่อสารกับคนอื่นได้ทั่วโลก เหมาะกับงานทั่วไป เช่น การประมวลผลคำ (Word Processing) การคำนวณ (Spreadsheet) การบัญชี (Accounting) จัดทำสิ่งพิมพ์ (Desktop Publishing) และงานที่เกี่ยวข้องกับฐานข้อมูล เป็นต้น ซึ่งทั้งหมดนี้ทำให้คอมพิวเตอร์แบบนี้เป็นที่นิยมอย่างแพร่หลายมากที่สุด ส่งผลให้การพัฒนาเครื่องไมโครคอมพิวเตอร์มีลักษณะและรูปแบบที่แตกต่างกัน เช่น คอมพิวเตอร์ตั้งโต๊ะ (desktop computer) คอมพิวเตอร์พกพา (portable computer) ซึ่งมีรายละเอียดดังนี้

- **คอมพิวเตอร์แบบตั้งโต๊ะ** (Desktop Computer) เป็นคอมพิวเตอร์ส่วนบุคคล ที่มีรูปแบบพื้นฐาน เหมาะสำหรับตั้งโต๊ะทำงานทั่วไป และได้รับความนิยมเป็นอย่างมาก แบ่งเป็น 2 รูปแบบ คือ Desktop Model และ Tower Model โดย Desktop Model จะวางหน้าจอไว้บน Case และลักษณะการวาง Case จะเป็นแนวนอน ส่วน Tower Model จะวาง Case ในแนวตั้ง และปัจจุบันได้ประยุกต์ Case ทั้งสองลักษณะให้สามารถวางได้ทั้ง 2 รูปแบบ เพื่อความยืดหยุ่นต่อพื้นที่ในการใช้งาน

รูปที่ 5.5 คอมพิวเตอร์แบบตั้งโต๊ะ

- **เวิร์คสเตชันคอมพิวเตอร์** (Workstation Computer) เป็นเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ ที่สนับสนุนการทำงานของคอมพิวเตอร์เครือข่าย ซึ่งใช้ในการจัดสรรและใช้ทรัพยากรร่วมกัน เช่น แฟ้มข้อมูลโปรแกรมประยุกต์ อุปกรณ์คอมพิวเตอร์ เช่น เครื่องพิมพ์และอุปกรณ์อื่น ๆ โดยการเชื่อมโยงกับเทอร์มินัล (Terminal) หลาย ๆ เครื่อง อีกทั้งได้ถูกออกแบบมาให้มีความสามารถในการคำนวณด้านวิศวกรรม สถาปัตยกรรม หรืองานอื่น ๆ ที่เน้นการแสดงผลด้านกราฟิก เช่น การนำมาช่วยออกแบบภาพกราฟิกที่มีความละเอียดสูง ทำให้เวิร์คสเตชันใช้หน่วยประมวลผลที่มีประสิทธิภาพสูงและมีหน่วยเก็บข้อมูลสำรองจำนวนมากด้วย ผู้ใช้บางกลุ่มจะเรียกเครื่องระดับเวิร์คสเตชันนี้ว่า ***ซูเปอร์ไมโคร*** *(Supermicro)* เพราะถูก

ออกแบบให้ใช้งานแบบตั้งโต๊ะ แต่ชิปที่ใช้ทำงานนั้นแตกต่างกันมาก เนื่องจากเวิร์คสเตชันส่วนมากใช้ชิปที่ลดจำนวนคำสั่งที่สามารถใช้สั่งงานให้เหลือเฉพาะที่จำเป็น เพื่อให้สามารถทำงานได้ด้วยความเร็วสูง

รูปที่ 5.6 เวิร์คสเตชันคอมพิวเตอร์

- **โน๊ตบุ๊คคอมพิวเตอร์** (Notebook Computer) เป็นคอมพิวเตอร์ขนาดเล็ก มีน้ำหนักเบาประมาณ 2-4 กิโลกรัม และบางกว่าแบบตั้งโต๊ะ สามารถพกพาไปยังสถานที่ต่าง ๆ ได้สะดวก โดยมีหน้าจอและคีย์บอร์ดติดกัน ส่วนเม้าส์ (Mouse) และลำโพงจะอยู่ติดกับตัวเครื่อง โดยสามารถหาอุปกรณ์ดังกล่าวติดตั้งภายนอกเพิ่มเติมก็ได้ มีเครื่องอ่านแผ่นดิสก์ (Floppy Disk Drive) และเครื่องอ่านแผ่นซีดีรอม (CD-ROM drive) และพัฒนาให้มีขนาดเล็กกว่าเดิมในขนาดที่สามารถวางบนตักได้

รูปที่ 5.7 โน๊ตบุ๊คคอมพิวเตอร์

- **คอมพิวเตอร์แทปเลท** (Tablet Computer) มีลักษณะคล้ายโน๊ตบุ๊ค คือ มีขนาดเล็ก มีน้ำหนักเบา มีความบาง และสามารถเคลื่อนย้ายและพกพาได้สะดวก แต่จะมีความแตกต่างกันที่แทปเลทสามารถป้อนข้อมูลทางจอภาพได้ตามเทคโนโลยีของผู้ผลิต เช่น การใช้ปากกาชนิดพิเศษที่สามารถเขียนลงบนจอภาพ และใช้โปรแกรมในการช่วยแปลงตัวเขียนเหล่านั้นให้เป็นตัวอักษรที่เหมือนกับการพิมพ์จากคีย์บอร์ด

รูปที่ 5.8 คอมพิวเตอร์แทปเลท

- **คอมพิวเตอร์พกพา** (Handheld Computer) มีขนาดเล็กกว่าโน๊ตบุ๊คและแทปเลท คือ มีขนาดเท่าฝ่ามือ ถือเพียงมือเดียวได้ และใช้อีกมือถือปากกาที่เรียกว่า สไตล์ลัส (Stylus) เขียนข้อความบนจอเพื่อป้อนข้อมูลเข้าสู่เครื่องได้ด้วยเทคโนโลยีการรับรู้ลายมือ (Hand writing recognition) พกพาสะดวกมากกว่า สามารถจัดเก็บข้อมูลได้มาก คีย์บอร์ดและหน้าจอมีขนาดเล็ก บางรุ่นใช้ปากกาชนิดพิเศษในการนำเข้าข้อมูล มีน้ำหนักเพียงร้อยกว่ากรัม และจอสีที่มีความละเอียดสูงถึง 320x320 และสามารถต่อเข้ากับอินเทอร์เน็ต และบางรุ่นสามารถใช้ฟังเพลง MP3 หรือใช้เป็นโทรศัพท์เคลื่อนที่ได้ด้วย คอมพิวเตอร์ชนิดนี้ถูกออกแบบมาเพื่อทำหน้าที่เป็นอุปกรณ์จัดเก็บและจัดการสารสนเทศส่วนบุคคล (Personal Information Manager: PIM หรือ Personal Organizer) เช่น ตารางเวลา ปฏิทินนัดหมาย สมุดโทรศัพท์ และสมุดบันทึก เป็นต้น คอมพิวเตอร์ชนิดนี้นิยมเรียกว่า **PDA (Personal Digital Assistant)** PDA ในปัจจุบันที่นิยมได้แบ่งออกเป็นสองแบบ คือ พีดีเอในกลุ่มของปาล์ม (Palm) ซึ่งใช้ Palm OS จากบริษัทปาล์มต่างๆ และ PDA ในกลุ่มของพ๊อกเก็ตพีซี (Pocket PC) ซึ่งใช้ Window Mobile OS

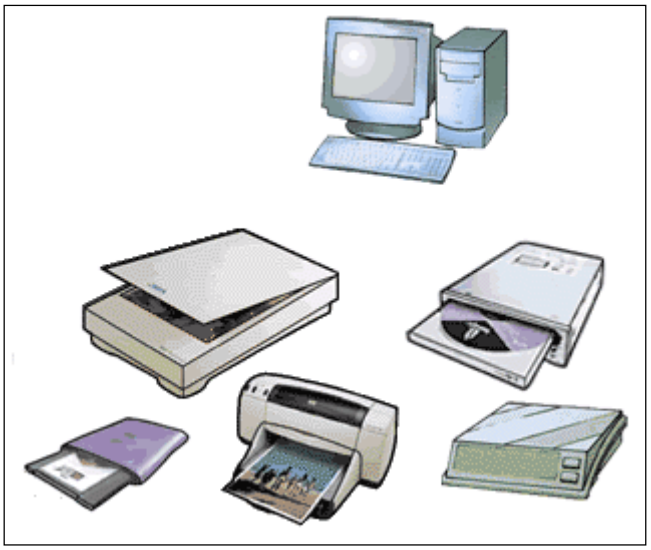
รูปที่ 5.9 Palm และ Pocket PC

- **คอมพิวเตอร์แบบฝัง** (embedded computer) เป็นคอมพิวเตอร์ที่ฝังในอุปกรณ์ต่างๆ นิยมนำมาใช้ทำงานเฉพาะด้าน พิจารณาจากภายนอกจะไม่เห็นว่าเป็นคอมพิวเตอร์แต่จะทำหน้าที่ควบคุมการทำงานบางอย่างของอุปกรณ์นั้นๆ คอมพิวเตอร์ประเภทนี้ เช่น เครื่องเล่นเกม ระบบเติมน้ำมันอัตโนมัติ โทรศัพท์มือถือ เป็นต้น

รูปที่ 5.10 อุปกรณ์ที่มี Embedded computer บนรถยนต์

5.3 เทคโนโลยีฮาร์ดแวร์

เมื่อกล่าวถึง ฮาร์ดแวร์คอมพิวเตอร์ (Hardware) โดยทั่วไปจะหมายถึง อุปกรณ์อิเล็กทรอนิกส์และอุปกรณ์อื่นๆ ที่ต่อพ่วงเข้ากับเครื่องคอมพิวเตอร์ ได้แก่ โมเด็ม, เครื่องพิมพ์, สแกนเนอร์ และลำโพง เป็นต้น



รูปที่ 5.11 ตัวอย่างฮาร์ดแวร์คอมพิวเตอร์

1. **อุปกรณ์รับข้อมูล** (Input devices)

อุปกรณ์รับข้อมูลเป็นอุปกรณ์ที่ใช้รับข้อมูลต่างๆ เข้าสู่คอมพิวเตอร์หรือเข้าสู่อุปกรณ์ประมวลผล ปกติเมื่อพูดถึงอุปกรณ์รับข้อมูลจะหมายถึง แป้นพิมพ์ (Keyboard) ซึ่งสามารถที่จะรับตัวอักษร ตัวเลข อักขระต่าง ๆ รวมทั้งคำสั่งจากผู้ใช้ และเมาส์ (Mouse) ที่ใช้คลิก (Click) เพื่อส่งคำสั่งเข้าไปประมวลผล นอกจากนี้ยังมีอุปกรณ์รับข้อมูลอื่นๆ อีกเช่น แทร็กบอล (trackball) จอยสติก (joystick) เครื่องสแกน (scanner) กล้องถ่ายรูปดิจิตอล (digital camera) ไมโครโฟน (microphone) และจอภาพแบบสัมผัส (Touch Screen) เป็นต้น

รูปที่ 5.12 ตัวอย่างแป้นพิมพ์

รูปที่ 5.13 ตัวอย่างเมาส์

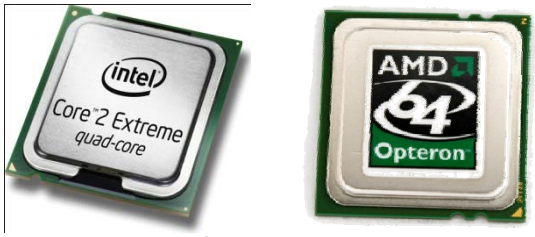
รูปที่ 5.14 ตัวอย่างอุปกรณ์รับข้อมูล

2. **อุปกรณ์ประมวลผล** (Processing devices)

อุปกรณ์ประมวลผล โดยทั่วไปเรียกรวมๆว่า หน่วยประมวลผลกลาง (CPU: Central Processing Unit) หรือ ซีพียู ถือว่าเป็นฮาร์ดแวร์ที่สำคัญที่สุดของระบบคอมพิวเตอร์ ทำหน้าที่ประมวลผลข้อมูลและสารสนเทศด้วยชุดคำสั่งที่ผู้ใช้ส่งเข้าไปให้ทำงานตามที่ผู้ใช้ต้องการ ส่วนของหน่วยประมวลผลนี้เป็นฮาร์ดแวร์ที่ประกอบด้วยแผงวงจรที่สำคัญ 2 ส่วนด้วยกัน คือ หน่วยประมวลผล และหน่วยความจำ

- *หน่วยประมวลผล* เปรียบเสมือนกับเป็นสมองของคอมพิวเตอร์ ในเครื่องคอมพิวเตอร์ส่วนบุคคล หน่วยประมวลผลจะประกอบไปด้วยหน่วยประมวลผลขนาดเล็ก ซึ่งเรียกว่า ไมโครโปรเซสเซอร์ (Microprocessor) จำนวน 1 ตัวหรือมากกว่า ประกอบอยู่บนแผงวงจรหลัก (Main board หรือ Motherboard) และมีวงจรอิเล็กทรอนิกส์เล็กๆ อีกมากมายรวมอยู่ด้วยโดยทั่วไปตัวประมวลผลหรือไมโครโปรเซสเซอร์จะเรียกว่า ซีพียู

- *หน่วยความจำ* เปรียบเสมือนกับโต๊ะทำงาน หากไม่มีโต๊ะทำงาน เอาไว้กองเอกสารต่าง ๆ คงจะยุ่งยากไม่น้อยกับการจัดการกับข้อมูลเหล่านั้น อย่างไรก็ตาม ชนิดของหน่วยความจำ ที่เราคุ้นเคยกันมากที่สุด ได้แก่ แรม (RAM : Random Access Memory) การทำงานของแรมนั้น จะควบคู่ไปกับ ซีพียู โดยที่ข้อมูลแทบทั้งหมดจะต้องถูกส่งผ่านมายังแรมเสียก่อน แล้วจึงค่อยส่งต่อไปให้ ซีพียู และในขณะที่ ซีพียู ประมวลผลข้อมูลเสร็จก็จะส่งมายังแรมเพื่อรอส่งต่อไปยังหน่วยอื่นๆ แรมจึงเป็นตัวเก็บและพักข้อมูลชั่วคราว แรมจะต้องมีไฟเลี้ยง เมื่อปิดเครื่องข้อมูลทั้งหมดในแรมก็จะหายไป ดังนั้นถ้าต้องการจะเก็บข้อมูลหรือสารสนเทศนั้นไว้ จะต้องบันทึกข้อมูลลงหน่วยความจำสำรองทุกครั้งเมื่อจะปิดเครื่อง ประสิทธิภาพของคอมพิวเตอร์ส่วนใหญ่นอกจากจะขึ้นอยู่กับความสามารถและความเร็วของซีพียูแล้วยังขึ้นอยู่กับขนาดของแรมด้วย



รูปที่ 5.15 ตัวอย่างซีพียู

3. **อุปกรณ์หน่วยความจำหลัก** (Main memory unit devices)

เป็นวงจรรวมหรือชิปที่ใช้บันทึกโปรแกรมและข้อมูล หน่วยความจำหลักจะบรรจุอยู่บนเมนบอร์ดหรือแผงวงจรหลัก หน่วยความจำบางประเภทก็ถูกออกแบบให้อยู่ในชิปซีพียูเลยหน่วยของข้อมูลที่จัดเก็บในหน่วยความจำเรียกว่าไบต์ (byte) 1 ไบต์ จะประกอบไปด้วย 8 บิต นอกจากนี้ยังมีหน่วยเป็นกิโลไบต์ (kilobyte หรือ KB) ซึ่งมีค่าเท่ากับ 1,024 ไบต์ , เมกะไบต์ (megabyte หรือ MB) มีค่าโดยประมาณหนึ่งล้านไบต์หรือ 1,024 KB , กิกะไบต์ (gigabyte หรือ GB) มีค่าประมาณหนึ่งพันล้านไบต์หรือ

หนึ่งล้านกิโลไบต์และเทราไบต์ (terabyte หรือ TB) มีค่าประมาณหนึ่งล้านล้านไบต์ หน่วยความจุของข้อมูลในหน่วยความจำสรุปได้ดังนี้

8	bits	=	1	Byte
1024	Bytes	=	1	kilobyte (KB)
1024	KB	=	1	megabyte (MB)
1024	MB	=	1	gigabyte (GB)
1024	GB	=	1	terabyte (TB)

หน่วยความจำหลักที่เป็นที่รู้จักกันอย่างกว้างขวางมี 3 ประเภท คือ แรม (RAM) รอม (ROM) และซีมอส (CMOS)

- **แรม (RAM)**

  Random access memory หรือ RAM เป็นอุปกรณ์หรือแผงวงจรที่ทำหน้าที่เก็บข้อมูลและโปรแกรมคอมพิวเตอร์ หน่วยความจำแรม บางครั้งเรียกว่าหน่วยความจำชั่วคราว (volatile) ทั้งนี้เนื่องจากโปรแกรมและข้อมูลที่ถูกเก็บในหน่วยความจำแรมจะถูกลบหายไป เมื่อปิดเครื่องคอมพิวเตอร์ ดังนั้นถ้าต้องการเก็บข้อมูลและโปรแกรมที่อยู่ในแรมไว้ใช้งานในอนาคตจะต้องบันทึกข้อมูลเหล่านั้น ลงในหน่วยความจำสำรอง (secondary storage) ก่อนที่จะปิดเครื่องคอมพิวเตอร์ทุกครั้ง เครื่องคอมพิวเตอร์พกพาบางประเภทจะใช้หน่วยความจำ ที่เรียกว่า flash ROM หรือ flash memory ซึ่งสามารถจัดเก็บข้อมูลและโปรแกรมไว้ได้ ถึงแม้ว่าจะปิดเครื่องคอมพิวเตอร์แล้วก็ตาม ซึ่ง RAM ที่นิยมใช้ในปัจจุบันนี้แบ่งเป็น 2 ประเภทคือ static RAM (SRAM) และ dynamic RAM (DROM)

  - **Static RAM**

    เป็นหน่วยความจำที่นิยมใช้เป็นหน่วยความจำแคช (cache memory) เพราะ SRAM มีความเร็วสูงกว่า DRAM รวมทั้งราคาก็สูง

กว่าด้วยหน่วยความจำแคช คือหน่วยความจำแรมที่ช่วยเพิ่มความเร็วให้กับอุปกรณ์คอมพิวเตอร์ เช่น เครื่องพิมพ์

- Dynamic RAM

หน่วยความจำที่นำมาใช้งานกันในปัจจุบันส่วนใหญ่จะเป็น DRAM ซึ่งเป็นหน่วยความจำที่มีความเร็วอยู่ระหว่าง 10-100 nanoseconds ราคา DRAM จะต่ำกว่า SRAM ซึ่งชนิดของ DRAM เช่น EDO RAM (extended data output RAM) SDRAM (synchronous DRAM)

- **รอม (ROM)**

Read - 0nly memory หรือ ROM เป็นหน่วยความจำที่บันทึกข้อสนเทศและคำสั่งเริ่มต้น (start -up) ของระบบ คุณสมบัติเด่นของรอมคือ ข้อมูลและคำสั่งจะไม่ถูกลบหายไป ถึงแม้ว่าจะปิดเครื่องคอมพิวเตอร์ หรือไม่มีกระแสไฟฟ้าหล่อเลี้ยงแล้วก็ตามข้อมูลหรือคำสั่งที่จัดเก็บในหน่วยความจำรอม ส่วนใหญ่จะถูกบันทึกมาจากโรงงานผู้ผลิตเครื่องคอมพิวเตอร์ และข้อมูลเหล่านี้จะไม่สามารถลบหรือแก้ไขได้ แต่สามารถอ่านได้ เรียกว่า PRAM (programmable read-only memory)

- **หน่วยความจำ CMOS**

CMOS ย่อมาจาก complementary metal-oxide semiconductor เป็นหน่วยความจำที่ใช้เก็บข้อสนเทศที่ใช้เป็นประจำของระบบคอมพิวเตอร์ เช่น ประเภทของแป้นพิมพ์ เมาส์ จอภาพ และเครื่องอ่านแผ่นดิสก์ (disk drive) CMOS ใช้กระแสไฟจากแบตเตอรี่ ดังนั้นเมื่อปิดเครื่องคอมพิวเตอร์ ข้อสนเทศใน CMOS จึงไม่สูญหาย ลักษณะเด่นของ CMOS อีกอย่างหนึ่งคือ ข้อสนเทศที่บันทึกใน CMOS สามารถเปลี่ยนแปลงได้เมื่อมีการเปลี่ยนแปลงอุปกรณ์ให้กับเครื่องคอมพิวเตอร์ เช่น การเพิ่ม RAM และฮาร์ดแวร์อื่น ๆ

รูปที่ 5.16 ตัวอย่างแรม

รูปที่ 5.17 ตัวอย่าง CMOS Timer

3. **อุปกรณ์แสดงผล** (Output devices)

อุปกรณ์แสดงผลเป็นอุปกรณ์ที่ส่งผลการทำงานกลับมาให้ผู้ใช้ ส่วนมากเมื่อพูดถึงอุปกรณ์แสดงผลจะนึกถึง จอภาพ (Monitor) และ เครื่องพิมพ์ (Printer) เครื่องคอมพิวเตอร์จะส่งผลลัพธ์ไปให้จอภาพเมื่อผู้ใช้ต้องการเห็นผลลัพธ์ และจะส่งผลลัพธ์ไปเครื่องพิมพ์เมื่อผู้ใช้ต้องการผลลัพธ์ออกทางกระดาษ ในขณะเดียวกันถ้าคอมพิวเตอร์ประมวลผลข้อมูลทางเสียงก็จะถ่ายทอดเสียงออกทางลำโพง (Speaker)

รูปที่ 4.18 ตัวอย่างจอภาพ, เครื่องพิมพ์ และลำโพง

4. **อุปกรณ์หน่วยความจำสำรอง** (Secondary storage devices **หรือ** External storage devices)

อุปกรณ์หน่วยความจำสำรอง เป็นอุปกรณ์ที่ใช้เก็บข้อมูลสารสนเทศและชุดคำสั่งมีอยู่หลายประเภทที่ใช้อยู่ในปัจจุบัน ได้แก่ จานแม่เหล็ก (Magnetic disk)

แถบแม่เหล็ก (Magnetic tape) และจานแสง (Optical disk) สามารถเก็บสารสนเทศรูปแบบต่างๆได้อย่างมหาศาล และสามารถนำสารสนเทศกลับมาใช้ในระบบคอมพิวเตอร์ในครั้งต่อๆ ไปได้เมื่อต้องการ

รูปที่ 5.19 ตัวอย่างจานแม่เหล็ก (Floppy disk และ Hard disk)

รูปที่ 5.20 ตัวอย่างแถบแม่เหล็ก

รูปที่ 5.21 ตัวอย่างจานแสง (DVD, HD-DVD และ Blue-Ray disc)

5. **อุปกรณ์สื่อสารข้อมูล** (Communication devices)

อุปกรณ์สื่อสารข้อมูล เป็นอุปกรณ์ที่ทำการต่อเชื่อมเข้ากับเครือข่าย ไม่ว่าจะเป็น โมเด็ม (Modem) หรือการ์ดเน็ตเวิร์ก (Network card) สำหรับโมเด็มนั้น เป็นอุปกรณ์ที่จำเป็น สำหรับการติดต่อ กับเครือข่ายอินเตอร์เน็ต ซึ่งก็มีตั้งแต่ โมเด็มแบบอนาล็อก 56 kbps ไปจนถึงโมเด็มดิจิตอล ทั้งแบบ DSL Modem Cable Modem และอินเตอร์เน็ตผ่านดาวเทียม ในขณะที่การ์ดเน็ตเวิร์กนั้นก็ช่วยให้เครื่องคอมพิวเตอร์เชื่อมต่อเข้ากับเครือข่ายระยะใกล้ (LAN : Local Area Network) ได้ ซึ่งก็แบ่งออกเป็นหลายชนิดเช่นเดียวกัน ตั้งแต่ความเร็ว 10 / 100 Mbps ไปจนถึงความเร็วในระดับ 1 Gbps

นอกจากนี้บนตัวเครื่องคอมพิวเตอร์ยังมีช่องสำหรับต่อเชื่อม เรียกว่า พอร์ต (Ports) ซึ่งถูกออกแบบมา สำหรับเชื่อมต่ออุปกรณ์ต่าง ๆ ตั้งแต่ เครื่องพิมพ์ สแกนเนอร์ โมเด็ม หรือแม้แต่ ฮาร์ดดิสก์ แบบติดตั้งภายนอก พอร์ตเหล่านี้ถือว่าเป็นช่องทางสำหรับสื่อสารข้อมูลระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์รอบข้าง ตัวอย่าง พอร์ตที่มีใช้งานกันในปัจจุบัน ได้แก่

- **Parallel Port**

  เป็นพอร์ตรุ่นเก่า ที่ให้ความเร็วในการต่อเชื่อมที่ดีในระดับหนึ่ง ส่วนใหญ่จะใช้ต่อเชื่อมกับเครื่องพิมพ์ และสแกนเนอร์ เป็นต้น

- **Serial Port**

  เป็นพอร์ตรุ่นเก่าเช่นเดียวกับ Parallel Port นิยมใช้ต่อเชื่อมกับโมเด็มรุ่นแรกๆ

- **USB Port**

  เป็นพอร์ตที่มีความอเนกประสงค์ เพราะมีอุปกรณ์รองรับกับ USB มากมาย ไม่ว่าจะเป็นเครื่องพิมพ์ สแกนเนอร์ โมเด็ม กล้องดิจิตอล หรือแม้แต่ CD-RW ด้วย ข้อดีที่ติดตั้งได้ง่าย และให้ความเร็วที่น่าพอใจ

- **Fire wire (IEEE 1394)**

เป็นพอร์ตที่มีความเร็วสูงที่สุด จากความเร็วของมันทำให้มีผู้พัฒนา อุปกรณ์ ให้ทำงานรองรับ Fire wire ตั้งแต่ฮาร์ดดิสก์ แบบติดตั้งภายนอก CD-RW ไปจนถึง กล้องวิดีโอ

รูปที่ 5.22 ตัวอย่าง Parallel Port, Serial Port, USB Port และ Fire wire (IEEE 1394)

5.4 เทคโนโลยีซอฟต์แวร์

คอมพิวเตอร์ฮาร์ดแวร์ไม่สามารถทำงานได้โดยปราศจากคำสั่งหรือโปรแกรม ที่เรียกว่า ซอฟต์แวร์ (Software) ซึ่งมีหน้าที่ในการควบคุมให้เครื่องคอมพิวเตอร์ทำงานให้ได้ตามผลลัพธ์ที่ต้องการ ซอฟต์แวร์หรือโปรแกรมเขียนขึ้นด้วยภาษาต่างๆ และการเลือกใช้โปรแกรมที่เหมาะสมกับลักษณะของงานนั้น จะช่วยให้การใช้เทคโนโลยีสารสนเทศเกิดประสิทธิภาพได้อย่างสูงสุด

ซอฟต์แวร์แบ่งออกเป็น 2 ประเภท คือ ซอฟต์แวร์ระบบ (System Software) และ ซอฟต์แวร์ประยุกต์ (Application Software) ในการทำงานใดๆ ผู้ใช้จะติดต่อกับซอฟต์แวร์ระบบหรือซอฟต์แวร์ประยุกต์เพื่อควบคุมการทำงานของฮาร์ดแวร์

รูปที่ 5.23 การทำงานของซอฟต์แวร์

1. **ซอฟต์แวร์ระบบ** (System software)

ซอฟต์แวร์ระบบ หมายถึง โปรแกรมหรือคำสั่งที่ทำหน้าควบคุมการปฏิบัติงานของส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ฮาร์ดแวร์ ตลอดเวลาควบคุม การสื่อสารข้อมูลในระบบเครือข่ายคอมพิวเตอร์ แบ่งเป็น 2 ประเภทคือ

- **ระบบปฏิบัติการ** (operating system **หรือ** OS)

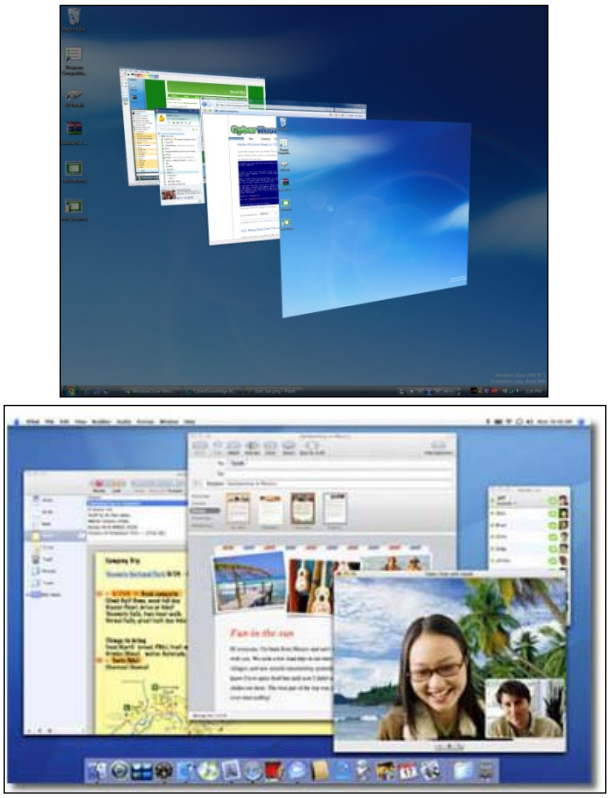
  เป็นชุดคำสั่งที่ทำหน้าที่เป็นสื่อกลางระหว่างโปรแกรมประยุกต์และอุปกรณ์คอมพิวเตอร์ ตัวอย่างระบบปฏิบัติการที่ใช้ในปัจจุบัน เช่น ระบบปฏิบัติการดอส (Disk Operating System หรือ DOS), Windows 98, UNIX เป็นต้น

  ระบบปฏิบัติการสามารถแบ่งออกตามลักษณะการทำงานได้ดังนี้

- **ระบบปฏิบัติการแบบมีลิขสิทธิ์** ได้แก่

ระบบปฏิบัติการเอ็มเอสดอส (Microsoft Disk Operating System หรือ MS - DOS) เอ็มเอสดอส เป็นระบบการปฏิบัติการที่ทำหน้าที่ดูแลการทำงานต่าง ๆ ของระบบคอมพิวเตอร์ เช่น ควบคุมหน่วยความจำ จอภาพ เครื่องพิมพ์ และอุปกรณ์ต่อพ่วงอื่น ๆ โปรแกรมเอ็มเอสดอส จะทำหน้าที่ประสานงานให้โปรแกรมประยุกต์ต่าง ๆ ทำหน้าที่ได้เหมาะสมตามคุณสมบัติของโปรแกรมนั้น ๆ

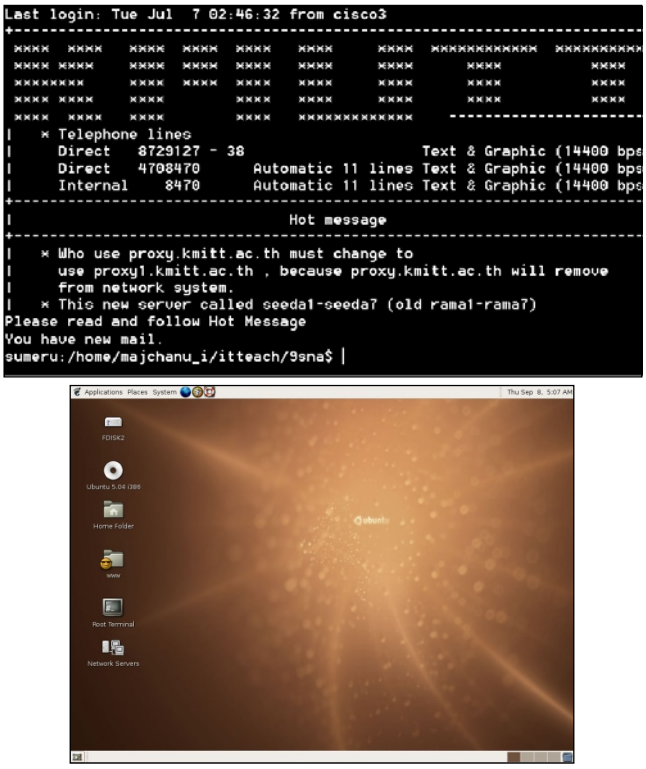
ไมโครซอฟต์วินโดวส์ (Microsoft Windows) เป็นระบบปฏิบัติการที่ผลิตโดยบริษัทไมโครซอฟต์ ประเทศสหรัฐอเมริกา การทำงานของระบบจะมีลักษณะเดียวกับระบบดอส แต่ต่างกันที่ระบบปฏิบัติการ ไมโครซอฟต์วินโดวส์จะติดต่อกับผู้ใช้ในลักษณะของภาพกราฟิกที่สวยงาม ที่เรียกว่า Graphical user หรือ GUI ผู้ใช้จะติดต่อกับระบบวินโดวส์ผ่านเมนูคำสั่ง (menu) และรูปภาพที่เป็นสัญลักษณ์ที่ใช้แทนคำสั่ง ซึ่งเรียกว่าไอคอน (Icon) ไมโครซอฟต์แวร์วินโดวส์ได้พัฒนาประสิทธิภาพอย่างต่อเนื่อง และเป็นระบบปฏิบัติการที่มีผู้ใช้มากที่สุด ปัจจุบันไมโครซอฟต์วินโดวส์ที่ใช้งานอยู่ ได้แก่ Windows 2003 server, Windows XP, Windows Vista และ MAC OSX 10.5



รูปที่ 4.24 หน้าจอ Windows Vista และ MAC OSX 10.5

- **ระบบปฏิบัติการแบบเปิด** (Open operating system)

เป็นระบบที่พัฒนาจากแนวคิดที่ต้องการใช้ระบบปฏิบัติการกับเครื่องคอมพิวเตอร์ต่าง ๆ ได้ซึ่งแต่เดิมการใช้ระบบปฏิบัติการไม่ว่าจะเป็นเครื่อง คอมพิวเตอร์ของบริษัทนั้น ๆ แต่ในปัจจุบันแนวโน้มการพัฒนาให้ระบบปฏิบัติการสามารถใช้งานร่วมกับฮาร์ดแวร์ที่แตกต่างกันได้แพร่หลายมากขึ้น ตัวอย่างระบบปฏิบัติการประเภทนี้ เช่น ระบบปฏิบัติการยูนิกซ์ และลีนุกซ์



รูปที่ 4.25 หน้าจอ UNIX และ LENUX Ubuntu 5.04

- **ตัวแปลภาษาคอมพิวเตอร์** (translator)

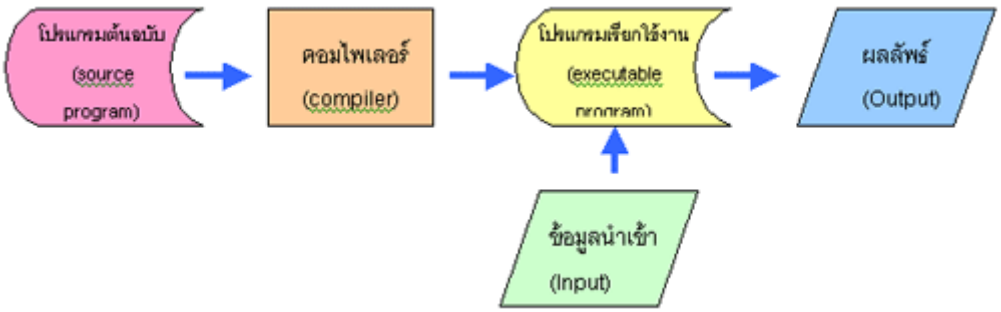
การพัฒนาโปรแกรมคอมพิวเตอร์ ผู้เขียนโปรแกรมหรือที่เรียกว่าโปรแกรมเมอร์นั้น จะเลือกใช้ภาษาให้เหมาะสมกับลักษณะงานและความถนัด ของผู้เขียนโปรแกรม โปรแกรมที่เขียนขึ้นหรือที่เรียกว่าโปรแกรมต้นฉบับ จึงมีลักษณะโครงสร้างของภาษาที่แตกต่างกันออกไป ในการทำงานของคอมพิวเตอร์นั้น คอมพิวเตอร์จะไม่สามารถเข้าใจภาษาที่ใกล้เคียงกับภาษามนุษย์ที่เรียกว่า ภาษาระดับสูง เนื่องจากคอมพิวเตอร์จะรับข้อมูลที่เป็นสัญญาณไฟฟ้าซึ่งแทนด้วยเลขฐานสอง (0 หรือ 1) หรือที่เรียกว่า ภาษาเครื่อง เท่านั้น

ดังนั้นในการสั่งให้คอมพิวเตอร์ทำงาน จึงจำเป็นจะต้องมีตัวกลางที่ทำหน้าที่เสมือนเป็นนักแปลภาษา โปรแกรมที่นำมาใช้

เรียกว่าโปรแกรมแปลภาษาคอมพิวเตอร์ ซึ่งจะทำหน้าที่แปลภาษาระดับสูงที่เป็นโปรแกรมต้นฉบับ ให้อยู่ในรูปของโปรแกรมเรียกใช้งานที่เครื่องคอมพิวเตอร์เข้าใจและสามารถทำงานได้ ตัวแปลภาษาสามารถแบ่งตามลักษณะการทำงานได้เป็น 3 ประเภท

- **คอมไพเลอร์** (Compiler)

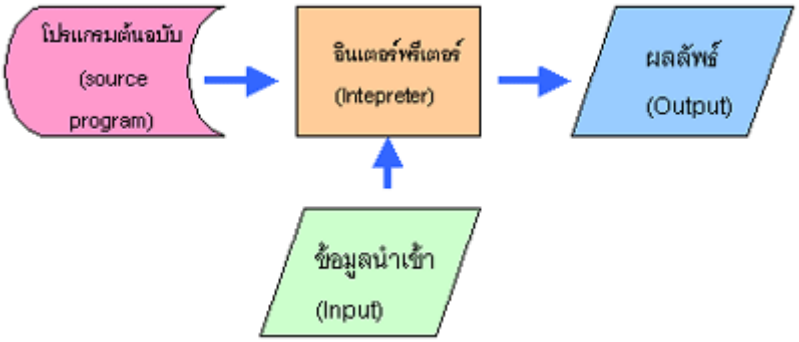
เป็นตัวแปลภาษาระดับสูง เช่น ภาษาปาสคาล ภาษาโคบอลและภาษาฟอร์แทรนให้เป็นภาษาเครื่อง การทำงานจะใช้หลักการแปลโปรแกรมต้นฉบับ ทั้งโปรแกรมเรียกใช้งาน ซึ่งจะถูกบันทึกไว้ในลักษณะของแฟ้มข้อมูลหรือไฟล์ เมื่อต้องการเรียกใช้งานโปรแกรมก็สามารถเรียกจากไฟล์เรียกใช้งาน โดยไม่ต้องทำการแปลหรือคอมไพล์อีก ทำให้การทำงานเป็นไปอย่างรวดเร็ว และขณะที่คอมไพล์โปรแกรมต้นฉบับที่เขียนขึ้นด้วยภาษาระดับสูง คอมไพเลอร์จะตรวจสอบโครงสร้างไวยากรณ์ของคำสั่งและข้อมูลที่จะใช้ในการคำนวณ และเปรียบเทียบต่อจากนั้นคอมไพเลอร์จะสร้างรายการข้อผิดพลาดของโปรแกรม (Program listing) เพื่อใช้เก็บโปรแกรมต้นฉบับและคำสั่งที่เขียนไม่ถูกต้องตามกฎ หรือโครงสร้างของภาษานั้น ๆ ไฟล์นั้นมีประโยชน์ในการช่วยโปรแกรมเมอร์ในการแก้ไขโปรแกรม (debug)



รูปที่ 5.26 กระบวนการการแปลงโปรแกรมต้นฉบับของคอมไพเลอร์

- **อินเตอร์พรีเตอร์** (Interpreter)

เป็นตัวแปลระดับสูงเช่นเดียวกับคอมไพเลอร์แต่จะแปลพร้อมกับทำงานตามคำสั่งทีละคำสั่งตลอดไปทั้งโปรแกรม ทำให้การแก้ไขโปรแกรมกระทำได้ง่าย และรวดเร็ว การแปลโดยใช้อินเตอร์พรีเตอร์จะไม่สร้างโปรแกรมเรียกใช้งาน ดังนั้นจะต้องทำการแปลใหม่ทุกครั้งที่มีการเรียกใช้งาน ตัวอย่างภาษาที่ใช้ตัวแปลอินเตอร์พรีเตอร์ เช่น ภาษาเบสิก (BASIC)



รูปที่ 5.27 กระบวนการการแปลงโปรแกรมต้นฉบับของอินเตอร์พรีเตอร์

- **แอสเซมบลีลี** (Assembler)

เป็นตัวแปลภาษาแอสเซมบลี (assembly) ซึ่งเป็นภาษาระดับต่ำให้เป็นภาษาเครื่อง

2. **ซอฟต์แวร์ประยุกต์** (APPLICATION SOFTWARE)

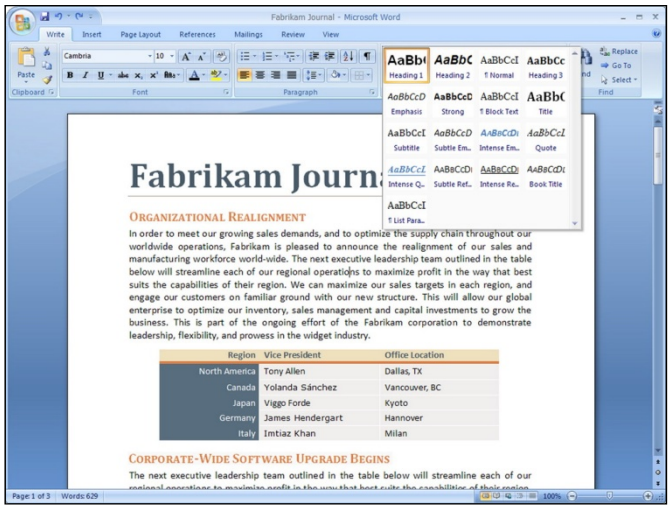
ซอฟต์แวร์ประยุกต์เป็นโปรแกรมที่พัฒนาขึ้นเพื่อให้คอมพิวเตอร์ทำงานด้านต่างๆ ตามความต้องการของผู้ใช้ ซึ่งถ้าโปรแกรมพัฒนาขึ้น เพื่อความต้องการเฉพาะขององค์การใดองค์การเหนึ่ง จะเรียกซอฟต์แวร์ประเภทนี้ว่า ซอฟต์แวร์เฉพาะงาน (Custom program หรือ tailor-made software) ซึ่งข้อดีคือโปรแกรมสามารถใช้งานได้

อย่างมีประสิทธิภาพตามความประสงค์ ของหน่วยงาน แต่ข้อเสียคือซอฟต์แวร์ประเภทนี้จะใช้เวลาในการพัฒนานาน และค่าใช้จ่ายค่อนข้างสูง ด้วยเหตุผลดังกล่าว จึงได้มีการพัฒนาโปรแกรมที่ใช้สำหรับงานทั่ว ๆ ไปที่เรียก general-purpose software หรือบางครั้งเรียกว่า โปรแกรมสำเร็จรูป (package software) เป็นซอฟต์แวร์เชิงพาณิชย์ (commercial software) ที่ผู้ใช้สามารถซื้อไปประยุกต์ใช้งานได้ทันที

ซอฟต์แวร์ประยุกต์ที่นิยมใช้สำหรับงานทั่วไป สามารถแบ่งตามประเภทของงานได้ดังนี้

- **โปรแกรมประมวลผลคำ** (word processor)

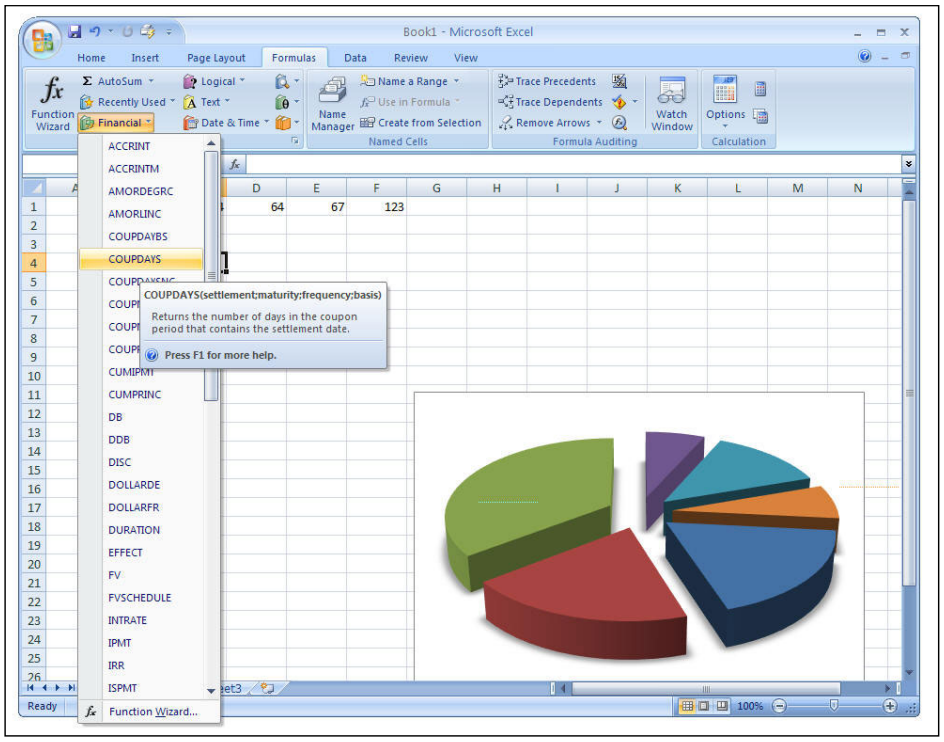
  เป็นโปรแกรมด้านการจัดทำเอกสาร นิยมเรียกสั้น ๆ ว่า Word ซึ่งเป็นโปรแกรมที่ได้รับความนิยมอย่างแพร่หลายเพื่อการผลิตเอกสาร ในรูปแบบต่าง ๆ เช่น รายงานจดหมาย บันทึกข้อความ หนังสือ และ สิ่งพิมพ์ทั่วไป โปรแกรมประมวลผลคำในปัจจุบันมีความสามารถในการใส่รูปภาพ ตาราง อักษรศิลป์ต่างๆ รวมทั้งยังมีเครื่องมือช่วยในการทำงานได้อย่างสะดวก เช่น ระบบการตรวจตัวสะกดและไวยากรณ์ เป็นต้น โปรแกรมประมวลผลคำที่นิยมใช้ในปัจจุบันนี้ ได้แก่ โปรแกรม Microsoft Word, WordPerfect และ Lotus Word Pro เป็นต้น



รูปที่ 5.28 หน้าจอ Microsoft Word 2007

- **โปรแกรมด้านการคำนวณ** (Spreadsheet)

เป็นโปรแกรมที่มีลักษณะตารางทำการ (Worksheet) เหมาะสำหรับงานการคำนวณตัวเลขในรูปแบบต่าง ๆ ตารางทำการประกอบด้วย ช่องตาราง หรือเซลล์ (Cell) ที่เรียงเป็นแถวและคอลัมน์ สามารถป้อข้อมูลตัวอักษร ตัวเลข และสูตรการคำนวณได้ นอกจากนี้ยังสามารถ ใส่รูปภาพและจัดทำกราฟสถิติได้อย่างสวยงาม ลักษณะงานที่ใช้ซอฟต์แวร์ประเภทนี้ เช่น การทำบัญชีงบกำไร - ขาดทุน รายงานการขาย การบันทึกคะแนนนักศึกษา ตัวอย่างซอฟต์แวร์สำเร็จรูปด้านการคำนวณ ได้ Microsoft Excel, Lotus 1-2-3 และ Quattro Pro เป็นต้น

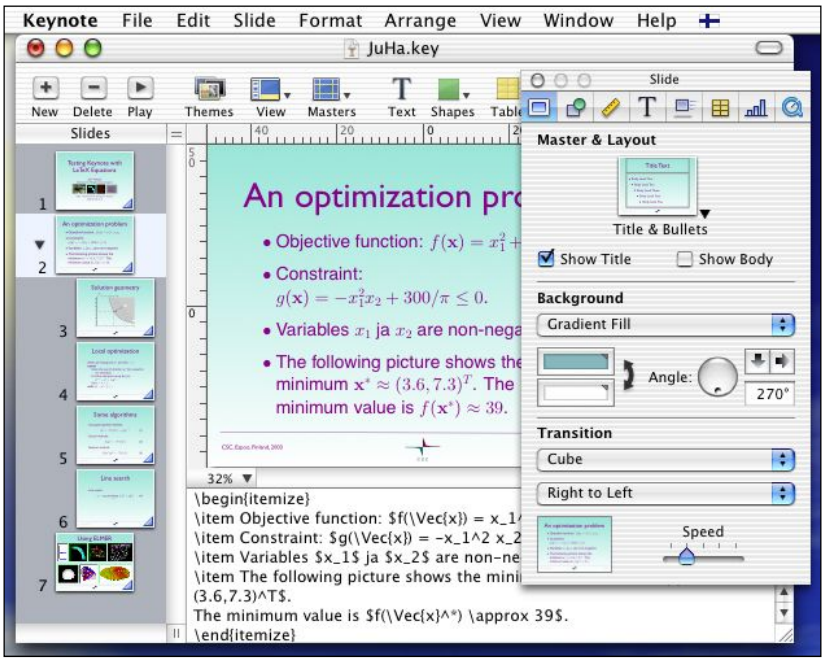


รูปที่ 5.29 หน้าจอ Microsoft Excel 2007

- **โปรแกรมการนำเสนอข้อมูล** (Presentation)

เป็นโปรแกรมประยุกต์ที่ช่วยงานด้านการนำเสนอข้อมูลด้วยคอมพิวเตอร์ซึ่งอาจเป็นการนำเสนอข้อมูลให้กับผู้เข้าฟังการประชุม สัมมนา หรือการบรรยาย ในการเรียนการสอน โดยทั่วไปนิยมที่จะนำคอมพิวเตอร์ไปพ่วงต่อกับเครื่องฉายวีดีทัศน์ (LCD projector) หรือจอทีวีขนาดใหญ่ เพื่อนำเสนอข้อมูลให้กับผู้ฟังที่มีจำนวนมากได้ด้วย

โปรแกรมนำเสนอข้อมูล จะมีต้นแบบสไลด์ (Template) ให้เลือกใช้ได้หลายรูปแบบ มีแบบตัวอักษรและรูปภาพประกอบต่าง ๆ จำนวนมาก สามารถใส่เทคนิคและลูกเล่นต่าง ๆ โดยเฉพาะภาพเคลื่อนไหว แผนผังองค์การ และใช้สื่อประสม เช่น วิดีโอและเสียงประกอบได้ ซึ่งโปรแกรมการนำเสนอข้อมูลที่นิยมใช้ในปัจจุบัน ได้แก่ Microsoft PowerPoint ของบริษัท Microsoft, โปรแกรม Freelance Graphics ของบริษัท Lotus Development และโปรแกรม Keynote ของ บริษัท Apple เป็นต้น



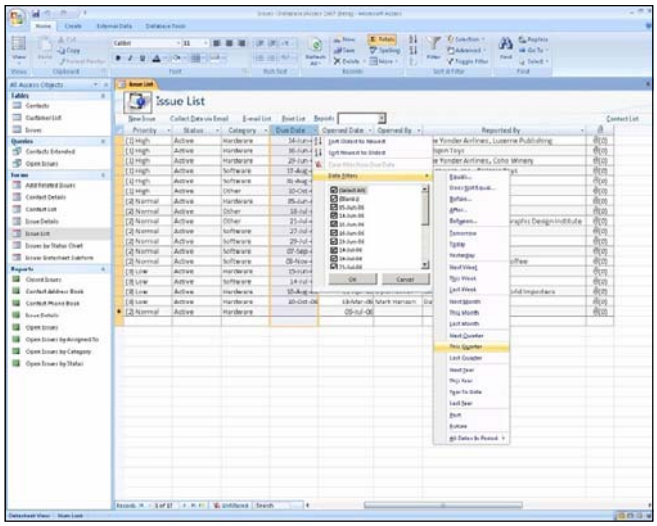
รูปที่ 5.30 หน้าจอ Apple Keynote

- **โปรแกรมจัดการฐานข้อมูล** (Database)

เป็นโปรแกรมที่ใช้ในการสร้างข้อมูล เพื่อจัดเก็บและจัดการข้อมูลได้อย่างสะดวกและรวดเร็ว ไม่ว่าจะเป็นการเพิ่ม แก้ไข หรือลบข้อมูล ตลอดจนการค้นหาข้อมูลตามเงื่อนไขที่กำหนด นอกจากนี้โปรแกรมยังสามารถพิมพ์รายงานได้อย่างสวยงามอีกด้วย

ผู้ใช้โปรแกรมยังสามารถประยุกต์โปรแกรมจัดการฐานข้อมูลกับงานด้านต่าง ๆ เช่น การจัดเก็บข้อมูลลูกค้า สินค้าคงคลัง ข้อมูลบุคลากร เป็นต้น

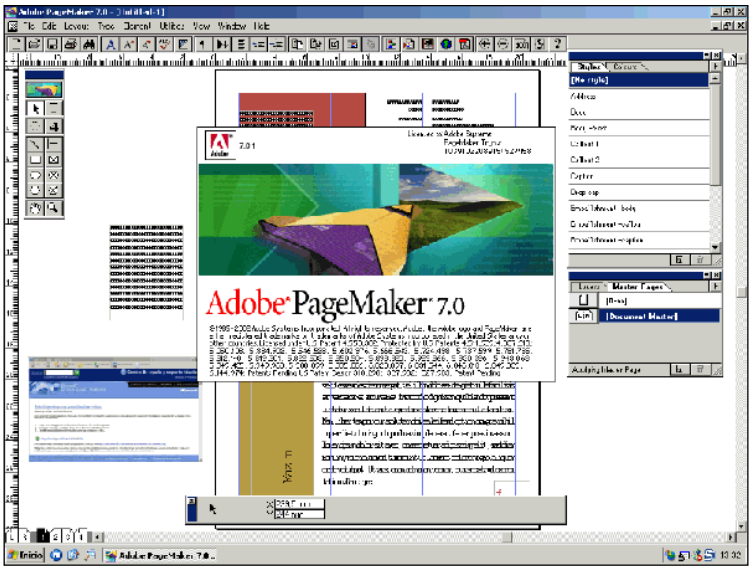
โปรแกรมจัดการฐานข้อมูลที่นิยมใช้ในปัจจุบัน ได้แก่ Microsoft Access และ FoxPro เป็นต้น



รูปที่ 5.31 หน้าจอ Microsoft Access 2007

- **โปรแกรมด้านงานพิมพ์** (Desktop publishing)

เป็นโปรแกรมที่ใช้จัดหน้าสิ่งพิมพ์ต่าง ๆ เช่น แผ่นพับ หนังสือ นามบัตร ใบประชาสัมพันธ์ การออกแบบแผ่นพับ (Brochure) โปรแกรมสามารถนำรูปภาพเข้ามาเป็นส่วนประกอบของงานได้ด้วย โปรแกรมที่ใช้สำหรับงานพับงานพิมพ์ในปัจจุบัน เช่น Adobe PageMaker เป็นต้น



รูปที่ 5.32 หน้าจอ Adobe PageMaker 7.0

- **โปรแกรมกราฟิก** (Graphics)

เป็นโปรแกรมที่ช่วยในการตกแต่งงานกราฟิกต่าง ๆ ซึ่งสามารถจำแนกได้เป็น 2 ประเภทคือ

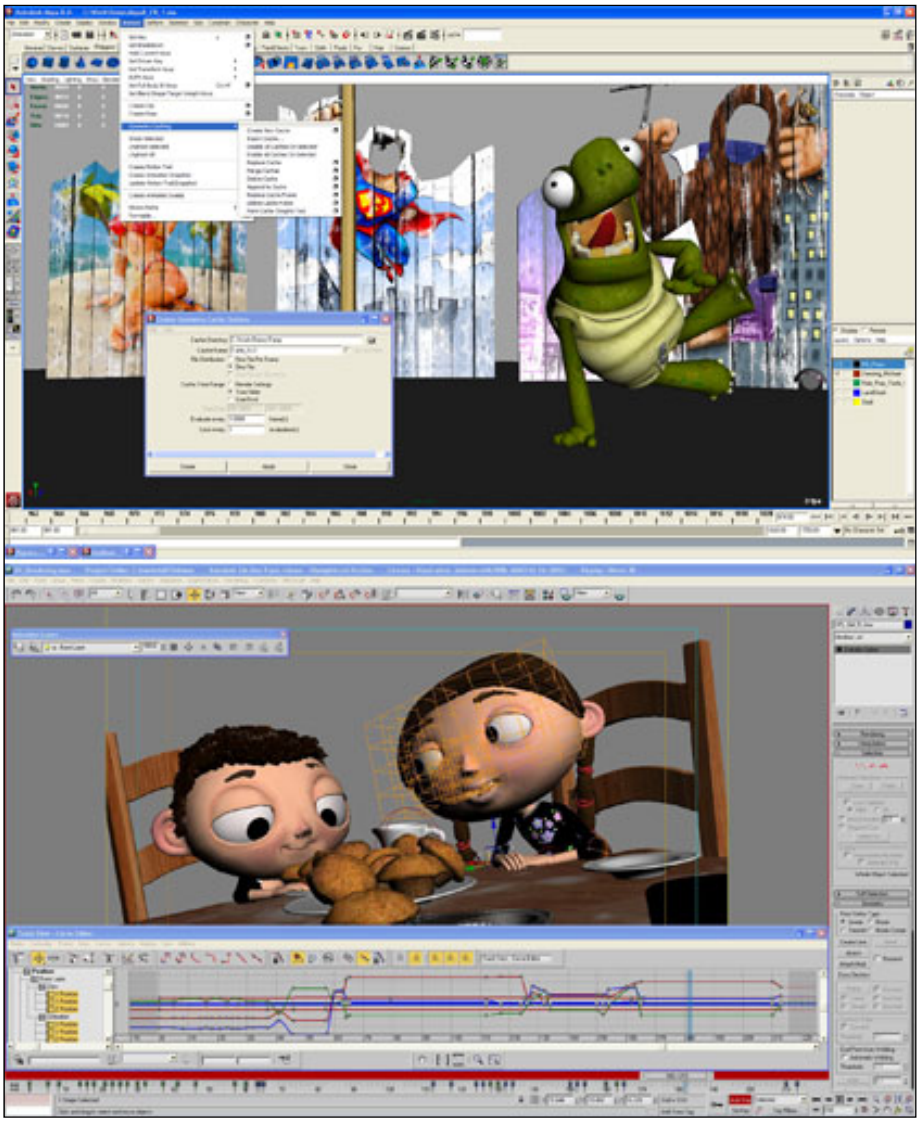
- **โปรแกรมสำหรับตกแต่งภาพ**

เป็นโปรแกรมช่วยในการวาดภาพและตกแต่งภาพให้สวยงาม โดยใช้เครื่องมือที่มีลักษณะเหมือนดินสอ แปรง พู่กัน จานสี และอุปกรณ์ตกแต่ง ภาพอื่น ๆ ที่เลียนแบบของจริง นอกจากนี้ยังสามารถนำภาพที่ได้จากการสแกนภาพด้วยเครื่องสแกนเนอร์ (Scanner) มาเชื่อมต่อในโปรแกรม เพื่อนำมาตกแต่งภาพได้ ซึ่งโปรแกรมด้านกราฟิกที่ใช้ตกแต่งภาพที่นิยมใช้ ได้แก่ Adobe PhotoShop, Microsoft Paint, CorelDraw เป็นต้น

รูปที่ 5.33 หน้าจอของ Adobe PhotoShop CS3 (for MAC OSX)

- **โปรแกรมช่วยออกแบบ**

เป็นโปรแกรมที่ใช้ช่วยในการออกแบบงานด้านสถาปัตยกรรมและวิศวกรรม โปรแกรมช่วยออกแบบที่นิยมใช้ เช่น AutoCAD ซึ่งสามารถใช้ออกแบบงานต่าง ๆ เช่น บ้าน รถยนต์ ระบบไฟฟ้า แผงวงจร หรือโปรแกรมออกแบบ 3 มิติเคลื่อนไหวต่างๆ เช่น Alias Maya, 3D MAX เป็นต้น นอกจากนี้ยังมีโปรแกรมออกแบบขนาดเล็กกว่า เช่น Generic Cadd และ Design Your Own Home เป็นต้น



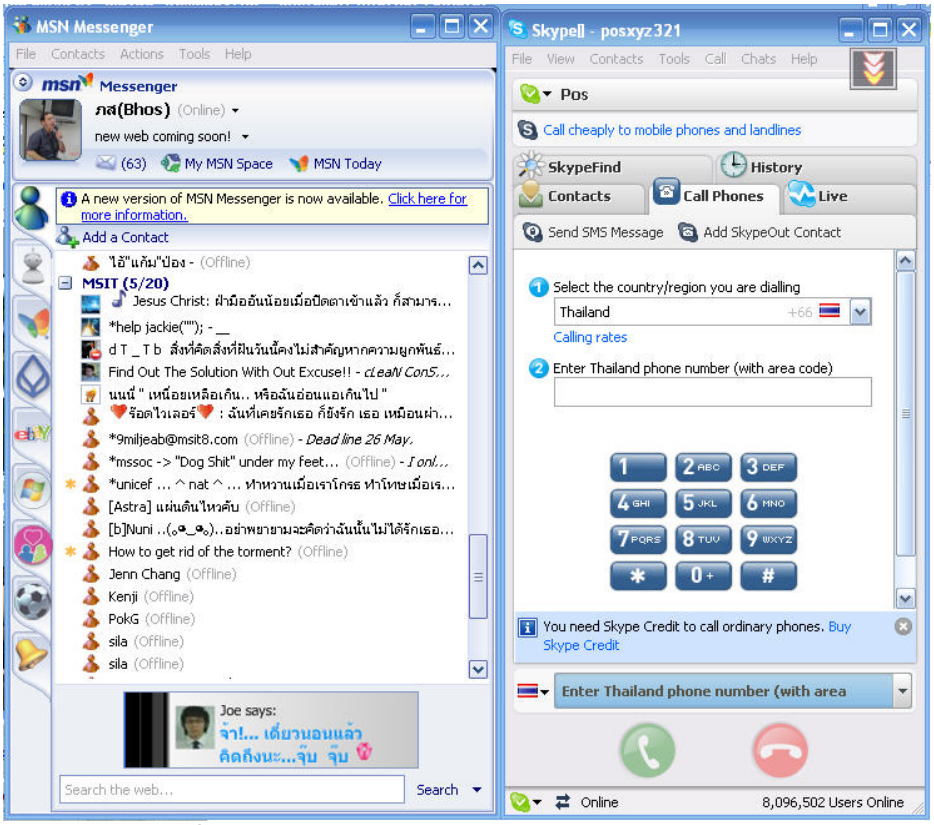
รูปที่ 5.34 หน้าจอของ Alias Maya 8 และ 3Ds MAX 9

- **โปรแกรมด้านติดต่อสื่อสาร** (Communication software)

เป็นโปรแกรมที่ใช้ในการติดต่อสื่อสารกับผู้อื่นได้สะดวก รวดเร็ว และช่วยประหยัดเวลาและค่าใช้จ่ายได้ด้วย การสื่อสารอาจอยู่ในรูปของไปรษณีย์อิเล็กทรอนิกส์ ที่สามารถส่งจดหมายถึงผู้รับได้ในทันที สามารถใช้แทนการส่งข้อความ โทรศัพท์ หรือแฟกซ์ เช่น บางองค์การธุรกิจใช้ไปรษณีย์ อิเล็กทรอนิกส์

ในการรับ - ส่งใบซื้อสินค้าระหว่างประเทศ ทำให้ช่วยลดค่าใช้จ่ายลงไปได้มาก โปรแกรมในกลุ่มด้านการสื่อสาร ได้แก่

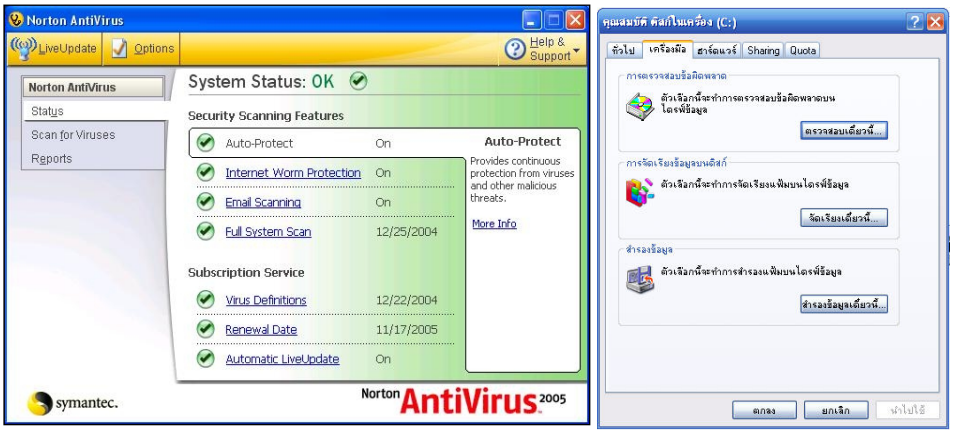
- โปรแกรมที่ช่วยในการโอนย้ายโปรแกรมหรือแฟ้มข้อมูลจากแหล่งข้อมูลในเครือจ่ายอินเทอร์มาใช้งานที่เครื่องของตนเองได้ด้วย เช่น FTP (file transfer protocol) เป็นต้น
- โปรแกรมที่ใช้สนทนาพูดคุยโต้ตอบกัน เช่น ICQ, miRC, MSN Messenger และ Skype เป็นต้น เป็นการสนทนากันโดยผ่านแป้นพิมพ์หรือสื่อประสมอื่น ๆ โดยสามารถโต้ตอบกันแบบคำต่อคำได้แบบทันทีด้วย ซึ่งปัจจุบันเป็นที่นิยมอย่างแพร่หลาย



รูปที่ 5.35 หน้าจอของ MSN Messenger 7.5 และ Skype 3.1

- **โปรแกรมอรรถประโยชน์** (Utility)

เป็นโปรแกรมที่เรียกใช้งานเพื่อช่วยเพิ่มประสิทธิภาพการทำงานของเครื่องคอมพิวเตอร์ ดูแลรักษาความปลอดภัยและเสถียรภาพของ เครื่องคอมพิวเตอร์ เช่น โปรแกรมสำหรับสำรองข้อมูลที่สำคัญในฮาร์ดดิสก์ (Backup) โปรแกรมตรวจสอบความถูกต้องของข้อมูล ในฮาร์ดดิสก์ โปรแกรมที่ช่วยในการจัดระเบียบข้อมูลในฮาร์ดดิสก์ (Disk Defragmenter) เพื่อสามารถอ่านและบันทึกข้อมูลได้รวดเร็วขึ้น โปรแกรมตรวจสอบไวรัส (Virus Scan) โปรแกรมบีบอัดข้อมูล (Compression Utility) เพื่อเพิ่มเนื้อที่ใช้งานในดิสก์หรือฮาร์ดดิสก์ให้มากขึ้น หรือโปรแกรมบีบอัดข้อมูลที่ต้องขยายก่อนจึงเรียกใช้งานได้ เช่น WinZip เป็นต้น ซึ่งโปรแกรมอรรถประโยชน์เหล่านี้หลายโปรแกรมจะให้มาพร้อมกับระบบปฏิบัติการ Microsoft Windows แล้ว



รูปที่ 5.36 หน้าจอของ Norton Antivirus 2007 และโปรแกรมอรรถประโยชน์บน Window XP

บทที่ 6
จริยธรรมที่พึงมีในการใช้คอมพิวเตอร์

ตามพจนานุกรมฉบับราชบัณฑิตยสถานฉบับ พ.ศ. 2542 จริยธรรมนิยามว่า "ธรรมที่เป็นข้อประพฤติปฏิบัติ, ศีลธรรม, กฎศีลธรรม" ซึ่งในทางปฏิบัติแล้ว การระบุว่าการกระทำสิ่งใดผิดจริยธรรมนั้น อาจกล่าวได้ไม่ชัดเจนมากนัก ทั้งนี้ย่อมขึ้นอยู่กับวัฒนธรรมของสังคมในแต่ละประเทศหรือแต่ละกลุ่มสังคมด้วย ในปัจจุบันคอมพิวเตอร์ถูกการใช้กันอย่างแพร่หลาย ทั้งในด้านการทำงาน, สนทนา, ธุรกิจ, การป้องกันภัย รวมถึงเพื่อความบันเทิงด้วย ทำให้ปัจจุบันมีคนใช้คอมพิวเตอร์ในทางที่ไม่ถูกต้อง และก่อให้เกิดโทษตามมามากมาย เพราะผู้ใช้เหล่านั้นยังไม่มีคุณธรรมและจริยธรรมในการใช้คอมพิวเตอร์ ซึ่งคุณสมบัติดังกล่าวนี้หากบุคคลผู้ใช้คอมพิวเตอร์ผู้ใดยังไม่มีแล้วจะก่อให้เกิดความเสียหายตามมาอีกมาก ดังนั้นไม่ว่าใครก็ตามที่จะใช้คอมพิวเตอร์ในทางใดก็ตาม ก็ควรจะมีจริยธรรมในการใช้คอมพิวเตอร์เพื่อให้เกิดความสงบต่อสังคมโดยรวม

จริยธรรม (Ethics) เป็นเรื่องของการกำหนดพฤติกรรมที่กลุ่มสังคมให้การยอมรับ หรือเป็นการระบุถึงสิ่งที่ควรหรือไม่ควรทำ โดยขึ้นอยู่กับสภาพแวดล้อมทางวัฒนธรรมของแต่ละกลุ่มสังคม และโดยมากแล้วจริยธรรมมักไม่มีการระบุเป็นเอกสารที่ชัดเจนเท่าไรนัก แต่มักจะเป็นการแสดงออกซึ่งพฤติกรรมที่คนส่วนใหญ่ในสังคมนั้นๆให้การยอมรับแต่ปฏิบัติกันต่อๆมา โดยนอกจากที่จะเกี่ยวของกับวัฒนธรรมแล้ว อาจยังขึ้นอยู่สภาพพื้นที่ที่อยู่อาศัย ศาสนา การศึกษา หรือความต้องการของผู้ที่มีอำนาจในแต่ละพื้นที่นั้นๆด้วย *ทั้งนี้ในสังคมขนาดเล็กแล้ว ระดับการศึกษาจะสามารถใช้เป็นตัวระบุถึงจริยธรรมได้อย่างใกล้เคียงกว่าในสังคมขนาดใหญ่ที่มีปัจจัยอื่นๆเข้ามาเกี่ยวข้องอยู่มากกว่า*

ฉะนั้นแล้วจริยธรรมที่พึงมีในการใช้คอมพิวเตอร์ก็ควรเกิดขึ้นจากพฤติกรรมที่ผู้คนในสังคมการใช้คอมพิวเตอร์ส่วนใหญ่ให้การยอมรับ และยึดถือเป็นแนวทางปฏิบัติกันต่อๆมา ซึ่งสังคมของผู้ใช้คอมพิวเตอร์ก็ต้องนับว่าเป็นสังคมขนาดใหญ่ที่ผู้คนมีความหลากหลายทั้งทางวัฒนธรรม ศาสนา และการศึกษา ก็โดยทั่วไปแล้วก็มีบัญญัติอยู่ 10 ข้อที่เป็นที่ยอมรับโดยทั่วไปว่าเป็นจริยธรรมในการใช้คอมพิวเตอร์ที่พึงมี อันได้แก่

1. ท่านต้องไม่ใช้คอมพิวเตอร์ในการทำร้ายผู้อื่น
2. ท่านต้องไม่รบกวนการงานของคอมพิวเตอร์ของผู้อื่น
3. ท่านต้องไม่แอบดูแฟ้มข้อมูลของผู้อื่น
4. ท่านต้องไม่ใช้คอมพิวเตอร์เพื่อการลักขโมย
5. ท่านต้องไม่ใช้คอมพิวเตอร์เพื่อเป็นการสร้างพยานเท็จ
6. ท่านต้องไม่ใช้หรือทำสำเนาซอฟต์แวร์ของผู้อื่นโดยไม่ได้จ่ายค่าใช้สิทธิ์นั้น
7. ท่านต้องไม่ใช้คอมพิวเตอร์ของผู้อื่นโดยไม่ได้กับอนุญาต
8. ท่านต้องไม่ฉวยเอาทรัพย์ทางปัญญาของผู้อื่นมาเป็นของตน
9. ท่านต้องคิดถึงผลต่อเนื่องที่จะเกิดขึ้นต่อสังคมในโปรแกรมที่เขียน หรือระบบที่ออกแบบขึ้นมา
10. ท่านต้องใช้คอมพิวเตอร์ในทางที่แสดงถึงความใคร่ครวญและเคารพต่อความเป็นมนุษย์

จากทั้ง 10 ข้อที่กล่าวมาจะเห็นได้ว่าในบางข้อนั้นแม้จะผิดจริยธรรมแต่จะไม่ผิดกฎหมาย ตัวอย่างเช่น ในข้อที่ 3 การแอบดูข้อมูลคอมพิวเตอร์ของผู้อื่นที่มีการเปิดทิ้งไว้และไม่ได้มีการตั้งรหัสป้องกันแต่อย่างใด แม้ว่าจะผิดต่อจริยธรรมดังที่ได้กล่าวมาแต่จะไม่ผิดตามมาตราที่ 7 ของพ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นต้น

“There’s no essential different between Computer Security Awareness and Life Security Awareness”

Pos Chandrasiri
Lecturer of Information Technology, Rangsit University

“ความตระหนักในความปลอดภัยทางคอมพิวเตอร์ก็ไม่ต่างอะไรกับความตระหนักในความปลอดภัยของชีวิตประจำวัน”

ภส จันทรศิริ
อาจารย์คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต

บรรณานุกรม

[1] Matt Bishop. **Introduction to Computer Security.** U.S.: Addison-Wesley: 2005

[2] ผศ.ดร. ศรีไพร ศักดิ์รุ่งพงศากุลม เจษฎาพร ยุทธนวิบูลย์ชัย. **ระบบสารสนเทศและเทคโนโลยีการจัดการความรู้**. กรุงเทพฯ: บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน), 2549

[3] ไพบูลย์ อมรภิญโญเกียรติ. **คำอธิบาย พ.ร.บ. คอมพิวเตอร์ พ.ศ.2550**. กรุงเทพฯ: บริษัท โปรวิชั่น จำกัด, 2553