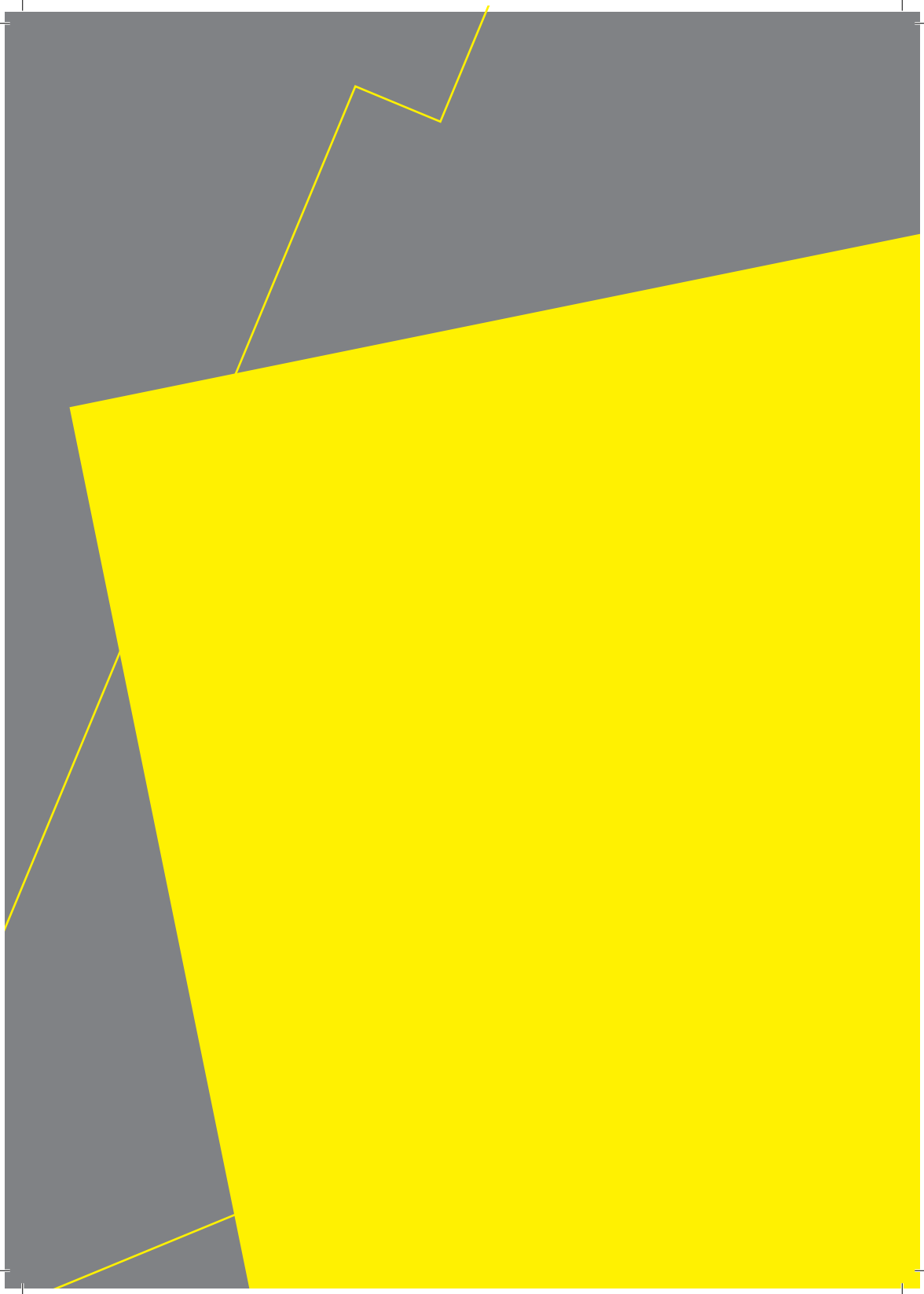
คู่มือการปฏิบัติและแนวทางการป้องกันเพื่อหลีกเลี่ยงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์



คู่มือการปฏิบัติและแนวทางการป้องกัน เพื่อหลีกเลี่ยงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พิมพ์ครั้งที่ 1 (สิงหาคม 2551)
จำนวน 30,000เล่ม
เอกสารเผยแพร่

อาคาร 9 บริษัท ทีโอที จำกัด (มหาชน)
ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ : 0-2505-7370

จัดทำโดย
สำนักกำกับการใช้เทคโนโลยีสารสนเทศ
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

สารบัญ

บทที่ 1

ความรู้ความเข้าใจพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ความเป็นมาของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1. สภาพปัญหาเกี่ยวกับการกระทำความ ผิดทางคอมพิวเตอร์ในปัจจุบัน

1.1 ความสำคัญของคอมพิวเตอร์ในชีวิตประจำวัน สังคมในปัจจุบันเป็นสังคมไอที[1] ที่คอมพิวเตอร์เป็นเครื่องมือที่สำคัญ ซึ่งช่วยอำนวยความสะดวกให้แก่ผู้ใช้ไม่ว่าจะเป็นการทำงานด้านการส่งข้อมูลข่าวสารระหว่างที่หนึ่งไปยังอีกที่หนึ่ง ในรูปแบบสื่อ ทั้งภาพเสียง ตัวอักษรและมัลติมีเดีย[2]ได้อย่างรวดเร็วฉับไวทันเวลาที่ต้องการ หากแต่ในปัจจุบันมีการใช้คอมพิวเตอร์ในทางไม่เหมาะสม เช่น นำไปใช้แพร่ภาพ ลามกอนาจาร นำภาพไปตัดต่อเข้าสู่ระบบคอมพิวเตอร์ทำให้ผู้อื่นเสียหาย ปลอมแปลง ข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต ก่อกวนทำร้ายผู้ใช้คอมพิวเตอร์อื่นๆ หลอกลวง ก่อการร้ายเป็นต้น การป้องกันปราบปราม และจับกุมดำเนินคดีแก่ผู้ที่ใช้คอมพิวเตอร์ในทางที่ทำให้เกิดความเสียหายแก่ผู้อื่น หรือเกิดความเสียหาย แก่ประเทศชาติ จึงเป็นเรื่องจำเป็นที่จะต้องมีการแก้ไขปัญหาดังกล่าว

1.2 ผลของการกระทำผิดกระทบหรือความเสียหายในวงกว้างและรวดเร็ว ซึ่งส่งผลกระทบทั้งด้านเศรษฐกิจ, สังคม (ความสงบสุข และศีลธรรม) รวมถึงด้านความมั่นคงปลอดภัยของประเทศชาติด้วย

1.3 ยังไม่มีกฎหมายกำหนดความผิดมาก่อน เนื่องจากการประกอบอาชญากรรม ทางคอมพิวเตอร์นั้น มีความแตกต่างไป จากการประกอบอาชญากรรมแบบเดิมมาก และกฎหมาย

ที่มีอยู่เดิมไม่สามารถนำมาปรับใช้กับพฤติกรรมใหม่ๆ ที่ก่อเกิดความเสียหายต่อเศรษฐกิจ, สังคม และความมั่นคงได้

1.3.1 การที่กฎหมายอาญามุ่งคุ้มครองวัตถุที่มีรูปร่างเท่านั้น แต่ในยุคไอทีนั้นข้อมูลข่าวสารเป็นวัตถุที่ไม่มีรูปร่าง เอกสารไม่ได้อยู่ในแผ่นกระดาษอีกต่อไป ซึ่งกฎหมายที่มีอยู่ไม่อาจขยายการคุ้มครองไปถึงได้ตัวอย่างของการก่ออาชญากรรมทาง คอมพิวเตอร์ได้แก่ การโจรกรรมเงินในบัญชีลูกค้าของธนาคาร, การโจรกรรม ความลับของบริษัทต่างๆที่เก็บไว้ใน คอมพิวเตอร์, การปล่อยไวรัสเข้าไปใน คอมพิวเตอร์, การใช้คอมพิวเตอร์ในการ ปลอมแปลงเอกสารต่างๆ, การเผยแพร่ภาพลามกอนาจาร รวมไปถึงการใช้ คอมพิวเตอร์เพื่อการก่อวินาศกรรมด้วยซึ่งรูปแบบ

1 IT ไอที (information technology) เทคโนโลยีสารสนเทศ, เทคโนโลยีข้อมูล

2 Multimedia มัลติมีเดีย สื่อประสม, สื่อหลายแบบ การใช้สื่อหลาย ๆ ประเภทร่วมกันเช่นสื่อการสอน ที่มีการนำเสนอด้วยภาพและเสียง พร้อมทั้งมีคำอธิบายด้วย

การก่ออาชญากรรมทาง คอมพิวเตอร์ในปัจจุบัน ทวีความซับซ้อน และรุนแรงมากขึ้นเรื่อยๆ ทำให้การสืบสวนมีความยากลำบาก หากอาศัยกฎหมายอาญาแบบเดิมซึ่งยากที่จะเอาตัวผู้กระทำความผิดมาลงโทษ ตัวอย่างเช่น การขโมยโดเมนเนม (Domain Name) ซึ่ง ไม่มีรูปร่าง ไม่สามารถจับต้องและถือเอาได้ แต่ก็ถือเป็นทรัพย์ทรัพย์สินอย่างหนึ่งตาม ประมวลกฎหมายแพ่งและพาณิชย์ และยอมรับกันว่ามีมูลค่าทางศาล

1.3.2 พยานหลักฐานที่เกี่ยวกับคอมพิว-เตอร์นั้นสามารถเปลี่ยนแปลงได้ตลอดเวลาและถูกกระทำได้ง่าย แต่ยากต่อการสืบหา รวมทั้งยังสูญหายได้ง่ายอีกด้วย เช่น ข้อมูลที่ถูกบันทึกอยู่ในสื่อบันทึกข้อมูลถาวรของเครื่อง (Hard Disk) นั้น หากระหว่างการเคลื่อนย้ายได้รับความกระทบกระเทือนหรือเกิดการกระแทก หรือเคลื่อนย้ายผ่านจุดที่เป็นสนามแม่เหล็กข้อมูลที่บันทึกใน Hard Disk ดังกล่าวก็อาจสูญหายได้

1.3.3 ปัญหาเรื่องขอบเขตพื้นที่ ซึ่งเป็นเรื่องที่มีความสำคัญ เพราะผู้กระทำความผิดอาจกระทำจากที่อื่นๆ ที่ไม่ใช่ประเทศไทย ซึ่งอยู่นอกเขตอำนาจของศาลไทย ดังนั้น กฎหมายควรบัญญัติให้ชัดเจนด้วยว่าศาลมี เขตอำนาจที่จะลงโทษผู้กระทำผิดได้ถึงไหนเพียงไร และถ้ากระทำความผิดในต่างประเทศจะถือเป็นความผิดในประเทศไทยด้วยหรือไม่

จากสภาพปัญหาต่างๆ ที่กล่าวมาข้างต้น ประเทศไทยจึงต้องบัญญัติกฎหมายอาชญา-กรรมทางคอมพิวเตอร์เป็นกฎหมายเฉพาะแทนที่จะแก้ไขประมวลกฎหมายอาญา เนื่องจากลักษณะการก่ออาชญากรรมลักษณะพิเศษ จึงควรมีกฎหมายใหม่ที่ไม่กระทบต่อโครงสร้างประมวลกฎหมายอาญาเดิมเพียงแต่กฎหมายนี้จะเข้ามาทำหน้าที่อุดช่องว่างทางกฎหมายของประมวลกฎหมายอาญาที่ไม่สามารถนำตัวผู้กระทำความผิดมาลงโทษได้ นอกจากนี้นการบังคับใช้กฎหมายอาชญากรรมทางคอมพิวเตอร์จำเป็นต้องมีอำนาจพิเศษของเจ้าพนักงานบางประการ อาทิ การถอดรหัสลับข้อมูล การเรียกข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น อีกทั้งการแก้ไขประมวลกฎหมายอาญาจำเป็นต้องใช้เวลาค่อนข้างนานจึงเห็นควรให้มีกฎหมายเฉพาะในลักษณะพระราชบัญญัติ เพื่อให้ทันต่อการกระทำผิดรูปแบบใหม่ที่ทวีความรุนแรงเพิ่มมากขึ้น

2. เจตนารมณ์ในการร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

เนื่องจากปัญหาภัยคุกคามที่เกิดจากไวรัส[3]คอมพิวเตอร์ แฮกเกอร์[4] การเผยแพร่รูปภาพ ข้อความ ที่มีลักษณะลามก อนาจาร หรือข้อมูลอันเป็นเท็จที่ก่อให้เกิดความเสียหายต่อบุคคล ต่อความมั่นคงทางการเมือง สังคม และเศรษฐกิจของประเทศ จึงเป็นเหตุให้เกิดการร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้น โดยมีเจตนารมณ์ดังนี้

1. เพื่อเป็นการใช้กรอบแห่งกฎหมายในการกำหนดฐานความผิดและบทลงโทษในการเรียกร้องค่าเสียหายแก่ผู้กระทำความผิดเพื่อคุ้มครองสิทธิให้แก่ประชาชน
2. เพื่อกำหนดบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของเจ้าพนักงานเจ้าหน้าที่ทั้งด้านนโยบาย มาตรฐาน แนวปฏิบัติ และกำหนดหน้าที่ของผู้ให้บริการไม่ว่าจะแก่ตนเองหรือบุคคลอื่นในการเข้าสู่อินเทอร์เน็ต[5] หรือให้สามารถติดต่อถึงกันโดยผ่านระบบคอมพิวเตอร์ก็ตาม โดยให้มีแนวทางการปฏิบัติการดำเนินงานให้เกิดความชัดเจนถูกต้องในแนวทางเดียวกัน

3 Virus ไวรัส หรือไวรัสคอมพิวเตอร์ (Computer virus) คือโปรแกรมคอมพิวเตอร์ที่บุกรุกเข้าไปในเครื่องคอมพิวเตอร์โดยไม่ได้รับความยินยอมจากผู้ใช้ ส่วนมากมักจะมีประสงค์ร้ายและสร้างความเสียหายให้กับระบบของเครื่องคอมพิวเตอร์นั้นๆ ไวรัสนั้นเป็นประเภทหนึ่งของโปรแกรมประเภทมัลแวร์ (malware) หรือโปรแกรมที่มีประสงค์ร้าย ในความหมายที่ใช้กันทั่วไปนั้น

4 Hacker แฮกเกอร์ ผู้ที่พยายามหาวิธีการหรือหาช่องโหว่ของระบบ เพื่อแอบลักลอบเข้าสู่ระบบเพื่อล้วงความลับหรือแอบดูข้อมูลข่าวสาร

5 Internet อินเทอร์เน็ต, เครือข่ายระหว่างกัน, เครือข่ายคอมพิวเตอร์ขนาดยักษ์ที่เชื่อมต่อกันทั่วโลก โดยมีมาตรฐานการ รับส่งข้อมูลระหว่างกัน เป็นหนึ่งเดียว

3. ขั้นตอนการร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (9 ปีของกฎหมายนี้)

2541	ครม. เห็นชอบให้คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติดำเนินการโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ
ต.ค. - 49	ครม. เห็นชอบตามที่คณะกรรมการกฤษฎีกาพิจารณา
พ.ย. - 49	สภานิติบัญญัติแห่งชาติลงมติรับหลักการ
พ.ค. - 50	สภานิติบัญญัติแห่งชาติลงมติเห็นชอบ
18-มิ.ย. - 50	ประกาศในราชกิจจานุเบกษา เล่ม 124 ตอน 27 ก หน้า 4-13
18-ก.ค. - 50	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550ฯ มีผลบังคับใช้

ที่มา http://www.etcommission.go.th/ict_law_step.php

4. การจัดตั้งหน่วยงานรองรับ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที) ได้มีการแบ่งส่วนราชการภายใน กำหนดหน่วยงานขึ้นใหม่เป็นหน่วยงานระดับสำนัก ใช้ชื่อว่า “สำนักกำกับการใช้เทคโนโลยีสารสนเทศ” ซึ่งจะเป็นหน่วยงานปฏิบัติที่มารองรับภารกิจตามพระราชบัญญัติฯ โดยหน่วยงานที่จัดตั้งขึ้นนี้จะต้องมีการเตรียมความพร้อมทั้งด้านการพัฒนาบุคลากรและการจัดเตรียมเครื่องมือในการดำเนินการด้านนิติวิทยาศาสตร์ทางคอมพิวเตอร์ และการสืบสวนสอบสวนภัยอาชญากรรมทางคอมพิวเตอร์

5. ผลกระทบเมื่อมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

เนื่องด้วย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ได้มีผลบังคับใช้ตั้งแต่ วันที่ 18 กรกฎาคม 2550 ดังกล่าวมีผลต่อการบังคับใช้ก่อให้เกิดผลกระทบต่อผู้ใช้งานคอมพิวเตอร์ในวงกว้าง ดังนี้

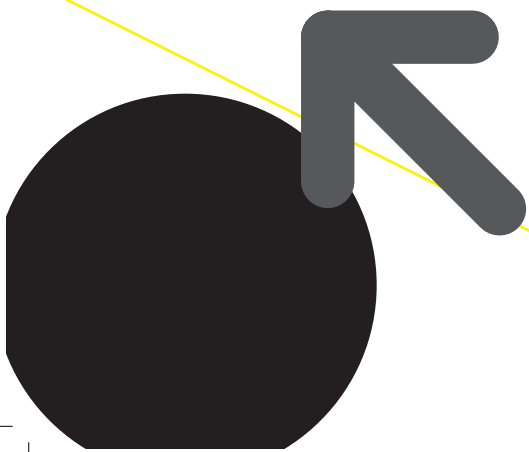
1. ปัญหาด้านการเตรียมความพร้อมของหน่วยงานต่าง ๆ เมื่อมีประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักการเก็บข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ 2550 ออกมา ทำให้ข้อมูลจราจรทางคอมพิวเตอร์เป็นพยานหลักฐานสำคัญการดำเนินคดี ผู้ให้บริการซึ่งประกอบด้วย ผู้ประกอบการกิจการโทรคมนาคม ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (ISP หน่วยงานราชการ บริษัท สถาบันการศึกษา ผู้ให้บริการในการเข้าถึงระบบเครือข่ายในหอพัก ร้านอาหาร โรงแรม) ผู้ให้บริการเช่าระบบคอมพิวเตอร์ ผู้ให้บริการร้านอินเทอร์เน็ต ต้องมีการเตรียมจัดหาระบบและอุปกรณ์ต่าง ๆ ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ให้ครอบคลุมตามที่กฎหมายกำหนด โดยการเก็บบันทึกต้องตอบให้ได้ว่า ใคร ทำอะไร ที่ไหน อย่างไร และเวลาใด (Who What

Where When Why) ซึ่งปัญหาดังกล่าวจะแบ่งออกเป็นปัญหาของ 2 ส่วน ได้แก่

1.1 องค์กรขนาดเล็ก ไม่มีเจ้าหน้าที่ผู้เชี่ยวชาญคอมดูแลระบบ และไม่มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์มาก่อน ผู้ให้บริการประเภทนี้ เช่น ร้านอินเทอร์เน็ต คาเฟ่ ขนาดเล็ก บริษัทขนาดเล็ก แต่ด้วยเป็นกิจการขนาดเล็กทำให้มีการจัดการเรื่องนี้ได้ง่ายกว่าบริษัทใหญ่ที่ต้องมีการลงทุน มากมาย โดยข้อมูลที่จะต้องจัดเก็บ ได้แก่ ข้อมูลล็อกที่มีการบันทึกเมื่อมีการเข้างานเครือข่ายโดยระบุตัวตน และสิทธิในการเข้าถึง วัน เวลา การติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ ยูสเซอร์ไอดี ซึ่งเป็นชื่อระบุตัวตนผู้ใช้งาน หมายเลขไอพีแอดเดรส หมายเลขที่ระบุในอีเมล์แอดเดรสของชื่อที่อยู่บนอีเมล์ใช้งาน โปรแกรม ปัญหาด้านการใช้งานอินเทอร์เน็ตไร้สายในการก่ออาชญากรรมไม่ว่าจะเป็นอินเทอร์เน็ต คาเฟ่ หรือการให้บริการฟรีอินเทอร์เน็ตไร้สายต่างๆ ผู้ให้บริการดังกล่าวต้องมี การบันทึกการใช้งาน ถ้าหากไม่ทำตาม กฎหมายจะถูกดำเนินตามกฎหมายจนทำให้ร้านอินเทอร์เน็ตหลายรายต้องปิดตัวลงเพราะขาดเงินซื้ออุปกรณ์ แต่หากมองในมุมกลับกันกฎหมายดังกล่าวก็มีข้อดีในการช่วยป้องกันผู้ใช้บริการอินเทอร์เน็ตทำความผิด ตัวอย่างเช่นกรณีรูปลามกอนาจารถูกส่งกันเป็นว่าเล่นไม่ว่าจะเป็นการกลั่นแกล้ง หรือแบล็กเมล์ก็ตามและยังมีการส่งข้อความหมิ่นประมาท แต่เมื่อพรบ.ประกาศใช้ก็ทำให้มีปัญหาลดลงบ้าง

1.2 องค์กรขนาดใหญ่ต้องมีภาระต้นทุนในการบริหารจัดการ ที่ผ่านมาปัญหาอาชญา- กรรมทางคอมพิวเตอร์เกิดขึ้นในประเทศไทย มาก มาย แต่ผู้ที่ได้รับความเสียหาย โดยเฉพาะ กลุ่มธนาคารที่อาจมีค่าใช้จ่ายความเสียหายจากภัยคุกคามทางคอมพิวเตอร์ปีละกว่า 100 ล้านบาท มักจะไม่เปิดเผย เพราะส่งผลกระทบต่อความเชื่อมั่นส่วนปัญหาการได้รับสแปมเมล์นั้น เฉพาะผู้ให้บริการอินเทอร์เน็ต หรือ ไอเอสพี มีค่าใช้จ่ายกลั่นกรองอีเมล์หลักหลายล้านบาท การเก็บข้อมูลจราจรและข้อมูลกิจกรรมต่างๆ ที่เกิดขึ้นในระบบสารสนเทศอย่างครบถ้วนตามพรบ. การซื้ออุปกรณ์และซอต์ฟแวร์เพื่อความสะดวกในการเก็บข้อมูลจราจรและสามารถตรวจสอบจากส่วนกลาง ให้สามารถระบุตัวบุคคลได้ ผู้บริหารอาจยังไม่มีความเข้าใจพอที่จะเลือกอุปกรณ์ที่ตรงกับการประกาศ เพราะโซลูชั่นต่างๆ นั้นมีราคาที่ต่างกันจากผู้ผลิตอุปกรณ์หลายค่ายที่ต้องการทำกำไรจึงเป็นปัญหาที่ต้องการคำแนะนำจาก

ผู้ดูแลกฎหมายออกมาประชาสัมพันธ์ให้ผู้ให้บริการเลือกการใช้งานได้อย่างเหมาะสมและคุ้มค่ามากที่สุด การให้ความรู้ความเข้าใจอย่างถูกต้องเกี่ยวกับพระราชบัญญัติฯ รวมถึงการกำหนดในการใช้งานคอมพิวเตอร์และระบบสารสนเทศขององค์กรจะช่วยลดความเสี่ยงต่อการเกิดความผิดตามพระราช-บัญญัติ รวมถึงปัญหาด้านการเก็บข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งในอนาคตจะต้องมีการเก็บข้อมูลจราจรทางคอม-พิวเตอร์เพิ่มมากขึ้น และจำนวนวันในการเก็บอาจจะต้องมีการเพิ่มพื้นที่ในการเก็บเพื่อใช้ในการสืบค้น



2. ปัญหาการสร้างความตระหนักและปลูกฝังความเข้าใจให้กับบุคลากรภายในองค์กร การใช้งานอินเทอร์เน็ตภายในองค์กร ต้องสร้างวัฒนธรรมการใช้งานคอมพิวเตอร์และอินเทอร์เน็ต อย่างปลอดภัย เช่น การตั้งรหัสผ่านเครื่องเพื่อป้องกันการเข้าถึงข้อมูล หลีกเลี่ยงส่งต่อภาพ ข้อความหรือภาพเคลื่อนไหวที่ผิดกฎหมาย ห้ามเข้าสู่อินเทอร์เน็ตด้วย “ชื่อผู้ใช้งาน” และ“รหัสผ่าน” ที่ไม่ใช่ของเรา นอกจากนี้ การตั้งกฎเกณฑ์ภายในองค์น่าจะเป็นวิธีที่ช่วยแก้ไขปัญหาได้เป็นอย่างดี ประกอบกับการประชาสัมพันธ์ให้ทุกส่วนเกิดความตระหนัก ผู้ใช้บริการต้องมีการปรับตัว เช่น ความระมัดระวังการให้ข้อมูลส่วนตัว การรักษาความปลอดภัยการส่งต่อจดหมายอิเล็กทรอนิค (forward mail) เพราะหากเมื่อมีการกระทำความผิดเกิดขึ้นจะไม่สามารถระบุตัวผู้กระทำความผิดได้ การใช้บริการเว็บบอร์ดมีขั้นตอนมากขึ้น เช่น การสมัครสมาชิก การกรอกข้อมูลพร้อมหลักฐาน เป็นต้น ฉะนั้นเพื่อที่จะสร้างความปลอดภัยในการใช้งานคอมพิวเตอร์ควรต้องจัดทำให้เป็นเรื่องวาระแห่งชาติ เป็นเรื่องที่ทุกๆ คนในสังคมต้องรู้และปฏิบัติตามนำมาสู่การพัฒนาระบบโทรคมนาคมที่ยั่งยืน

3. ปัญหาความไม่พร้อมและการขาดแคลนบุคลากรในการสืบสวนสอบสวน

3.1 หน้าที่ความรับผิดชอบ ซึ่งเราปฏิเสธไม่ได้ว่าพรบ.ฉบับนี้มีความชัดเจนในการปฏิบัติงานและความร่วมมือกับพนักงานเจ้าหน้าที่มากขึ้น ในเรื่องการให้ข้อมูลและการระงับการแพร่หลายของข้อมูลคอมพิวเตอร์ ควรมีการอนุญาตให้เจ้าหน้าที่สามารถเก็บ ข้อมูลหรือซอฟต์แวร์ที่เป็นหลักฐานหรือเป็นประโยชน์ต่อการปฏิบัติหน้าที่ไว้ได้ พร้อมทั้งมีการกำหนดอาณาเขตให้แน่นอน เพราะถ้าหากกฎหมายระบุกว้างเกินไป เจ้าหน้าที่อาจต้องดูแลทุกเว็บไซต์ในโลก

3.2 ความเสียหายเกิดในวงกว้าง อาชญากรรมอินเทอร์เน็ตในปัจจุบันเป็นปัญหาสำคัญ และแก้ไม่ตกของประเทศทั้งหลาย ระยะหลังๆ ที่ผ่านมาจากการเก็บสถิติการกระทำความผิดที่เกิดขึ้นในหลาย ๆ ประเทศพบว่าการกระทำความผิดเกิดต่อ "ข้อมูลข่าวสาร" อย่างไรก็ตาม คดีการกระทำความผิดต่อข้อมูลข่าวสารที่เกิดขึ้น มักมีระดับของภยันตรายที่แตกต่างกันไปขึ้นอยู่กับว่าข้อมูลที่ถูกละเมิดนั้น เป็นของใครหรือหน่วยงานใด เช่น การจารกรรมข้อมูลข่าวสารที่เกี่ยวกับระบบความปลอดภัยของรัฐ อันตรายที่เกิดขึ้นอาจกว้างกว่า การขโมยข้อมูลส่วนบุคคลบางอย่าง เพื่อผู้กระทำความผิดจะนำไปใช้ในการข่มขู่ หรือรีดไถจากเจ้าของข้อมูล เช่น หากเป็นความผิดด้านการเผยแพร่ภาพลามกอนาจาร ต้องสืบสวนจากบุคคลหลายฝ่าย ซึ่งก่อให้เกิดความยากลำบาก และอาจไม่คุ้มกับการลงทุนสืบสวน

3.3 ความชำนาญในการสื่อสาร พนักงานเจ้าหน้าที่ต้องมีความรู้ทางด้านไอที มีประสบการณ์ เพื่อใช้ในการพิสูจน์หลักฐาน ต้องสามารถสืบค้นย้อนหลังเพื่อใช้ในการตรวจสอบ สืบหา ตามจับตัวผู้กระทำความผิด ทำให้ผู้เชี่ยวชาญอยู่มีจำนวนจำกัด อีกทั้งเทคโนโลยีก็มีการพัฒนาเปลี่ยนแปลงทุกวัน การจัดหาเทคโนโลยีการจัดหาซอต์ฟแวร์ฮาร์ดแวร์ก็เป็นไปอย่างจำกัด

3.4 ความเสียหายต่างกัน เนื่องจากกฎหมายเกี่ยวกับคอมพิวเตอร์เป็นกฎหมายที่ค่อนข้างใหม่ อีกทั้งการกระทำความผิดเกิดขึ้นได้ง่ายเห็นได้จากสถิติการใช้งานอินเทอร์เน็ตที่มีจำนวนผู้ใช้งานเพิ่มขึ้นทุกวันและส่งผลกระทบในต่อภาคส่วนต่างๆ เช่น การเมือง เศรษฐกิจ

ความมั่นคง ศีลธรรม จรรยาบรรณ ในปัจจุบันการดำเนินคดีได้มีการดำเนินการจัดการกับคดีความที่ส่งผลในวงกว้าง หรือมีผลกระทบกับหมู่คนหมู่มากก่อน อันเนื่องจากจำนวนพนักงานเจ้าหน้าที่ที่ทำการดูแลและรับผิดชอบ มีจำนวนจำกัด

3.5 ข้อมูลที่อยู่ภายในคอมพิวเตอร์มีการเปลี่ยนแปลงได้ ข้อมูลในฮาร์ดดิสก์มีความเสี่ยงต่อการสูญเสียข้อมูลได้ เพราะข้อมูลของคอมพิวเตอร์ที่เก็บในฮาร์ดดิสก์นั้นปกติมักมีข้อมูลที่ผู้ใช้งานเพิ่มเข้าไปใหม่เสมอๆ จากการผิดพลาดในการจัดเก็บข้อมูล และการเข้าถึงข้อมูลจากผู้ที่ไม่ได้รับอนุญาต หรืออาจเกิดจากปัญหาไวรัสที่ติดเข้ามาในเครื่อง ความพยายามของแฮกเกอร์ที่ต้องการให้ข้อมูลเกิดการเปลี่ยนแปลง สูญหาย

3.6 กฎหมายไม่มีบทคุ้มครองพนักงานเจ้าหน้าที่ เช่น เมื่อเจ้าหน้าที่ได้งานมาจะไม่สามารถให้ผู้อื่นช่วยเหลือได้ หากพนักงานเจ้าหน้าที่ไม่มีความถนัดในการทำงานนั้น จึงมีความจำเป็นต้องมอบหมายให้ผู้อื่น ซึ่งอาจเป็นการกระทำความผิดในมาตราที่22 ที่ห้ามมิให้พนักงานเจ้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่ได้มาตามมาตรา 18ให้แก่บุคคลใด ซึ่งการออกกฎเพื่อคุ้มครองพนักงานเจ้าหน้าที่ประชาชนก็อาจมองได้ว่าเป็นการทำให้พนักงานเจ้าหน้าที่ขาดความปลอดภัยในการทำงาน ยกตัวอย่างเช่น หากต้องนำเครื่องเซิฟเวอร์ของบริษัทใดมาพิสูจน์หลักฐานซึ่งอาจมีข้อมูลที่สำคัญทางการเงิน เมื่อพนักงานเจ้าหน้าที่อาจจะกระทำโดยรู้เท่าไม่ถึงการทำสำเนาข้อมูลเป็นผลทำให้ข้อมูลการเงินที่สำคัญของบริษัทรั่วไหลสู่ภายนอก การกระทำเช่นนี้พนักงานเจ้าหน้าที่อาจถูกฟ้องร้อง ทำให้ไม่มีความปลอดภัยกับพนักงานเจ้าหน้าที่ในการปฏิบัติงาน

3.7 ปัญหาการประสานงานกับผู้ให้บริการต่างประเทศ ซึ่งไม่สามารถควบคุมให้ผู้ให้บริการในต่างประเทศปฏิบัติตามกฎหมายเราได้ ดังนั้นจึงต้องมีการประสานงานระหว่างสำนักงานตำรวจแห่งชาติกับสำนักงานสืบสวนของสหรัฐอเมริกา (FBI) เพื่อทำการแลกเปลี่ยนข้อมูลอันเป็นประโยชน์ในการติดตามผู้กระทำความผิดโดยเป็นการแลกเปลี่ยนข้อมูลแบบไม่เป็นทางการ หรือการใช้เวทีระหว่างประเทศในการสร้างข้อตกลงให้ความร่วมมือระหว่างประเทศเกี่ยวกับการแลกเปลี่ยนข้อมูลด้านคอมพิวเตอร์

4. ปัญหาของกระบวนการยุติธรรม

4.1 ความน่าเชื่อถือของพยานหลักฐาน ซึ่งนับวันคอมพิวเตอร์ยิ่งมีส่วนเกี่ยวข้องกับชีวิตประจำวันของคนมากขึ้น โดยเฉพาะคนรุ่นใหม่ ดังนั้น โอกาสที่บุคคลเหล่านี้ ที่ต้องใช้คอมพิวเตอร์เป็นประจำจะไปกระทำการที่เป็นความผิดได้โดยง่าย ดังนั้น องค์ประกอบความผิดที่สำคัญและจำเป็นเสมอสำหรับความผิดตามกฎหมายฉบับนี้ คือ คำว่าโดยมิชอบ ที่หมายถึงการกระทำจะผิด หรือไม่ผิดกฎหมายจะต้องดูที่เจตนาด้วย ทั้งนี้เองทางศาลก็ต้องมีเจ้าหน้าที่ที่มีความรู้ทั้งทางด้านตัวกฎหมายและด้านคอมพิวเตอร์ควบคู่กันไปด้วย ซึ่งบุคลากรที่มีความเชี่ยวชาญทั้งสองด้านในเวลาเดียวกันนั้นมีจำนวนน้อยในปัจจุบัน

4.2 การดำเนินการทางด้านการระงับการเผยแพร่เว็บไซต์ มีการดำเนินการที่ล่าช้า ซึ่งทางศาลได้เร่งทยอยอบรมศาลชั้นต้นทั่วประเทศให้มีความรู้ความเข้าใจในกฎหมายฉบับนี้ รวมถึงการอนุมัติหมายค้นให้กับพนักงานเจ้าหน้าที่ตามกฎหมายฉบับนี้ ปัจจุบันการใช้อินเทอร์เน็ตในประเทศไทยมีแนวโน้มเพิ่มขึ้นทุกปี เนื่องจากมีเทคโนโลยีที่ทำให้การเข้าถึงอินเทอร์เน็ตง่าย สะดวก และราคาถูกลง รวมทั้งการทำธุรกิจออนไลน์มากขึ้นจึงเกิดการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มากขึ้นด้วย ซึ่งมีแนวโน้มที่มูลค่าความเสียหายที่เกิดแต่ละคดีจะมากขึ้นเช่นกัน จึงต้องรีบหาทางแก้ไข

5. ปัญหาการตีความหมายของพรบฯ ฉบับนี้ เช่น

5.1 ข้อมูล “ลามกอนาจาร”ลักษณะไหนที่จะเรียกว่าข้อมูลลามกอนาจาร หากเราตีความหมายจากคำพิพากษาฎีกาว่าสิ่งใดลามกหรือไม่ลามกนั้น จะต้องไม่เป็นภาพที่นำไปสู่ความใคร่ทางกามอารมณ์ ความตื่นเต้นทางเพศ และต้องไม่ปรากฏอวัยวะเพศให้เห็นได้ชัด “สิ่งอันลามก คือ น่าอับอายในทางเพศต่อตา น่าอุจาดบัดสี ตรงกันข้ามกับสิ่งที่เป็นศิลปะอันแสดงถึงความงามและฝีมือของศิลปิน ศิลปะหรือลามกพิจารณาตามความรู้สึกของวิญญูชนรูปหญิงเปลือยกาย เห็นเด่นชัดเฉพาะถัน ส่วนโยนีถูกระบายให้ลบเลือนหรือเพียงฐานแสดงสุขภาพอนามัยของการอาบแดดสอนวิธีเขียนส่วนสัดความงามของร่างกายไม่น่าเกลียดอุจาดบัดสีที่นิยมนำไปสู่ความใคร่ทางกามารมณ์ ไม่เป็นลามกอนาจาร (ฎีกาที่ 978/2492 ฎ.675)”

5.2 ข้อมูลที่เกี่ยวกับ “ความมั่นคง” ซึ่งบัญญัติไว้ใน 3 มาตรา ซึ่งมีความหมายถึง ความมั่นคงปลอดภัยของประเทศ ข้อมูลที่เป็นความผิดต่อ ชาติ ศาสนา และองค์พระมหากษัตริย์ พระราชินี รัชทายาท ซึ่งเป็นผลเสียหายต่อประเทศชาติก่อให้เกิดการล้มล้างหรือการเปลี่ยนแปลงรัฐธรรมนูญ

5.3 ข้อมูล “ก่อให้เกิดความตื่นตระหนกแก่ประชาชน” โดยเจตนารมณ์ของการบัญญัติต้องการให้หมายถึงข้อความที่ส่งผลกระทบต่อบุคคลทั่วไป ไม่ว่าจะในทางสังคม ทางความมั่นคง ทางเศรษฐกิจ หรือทางความรู้สึกก็ตาม ซึ่งกรเขียนกฎหมายลักษณะเช่นนี้เป็นการให้อำนาจแก่ศาลในการใช้ดุลพินิจพิจารณาคดีความได้

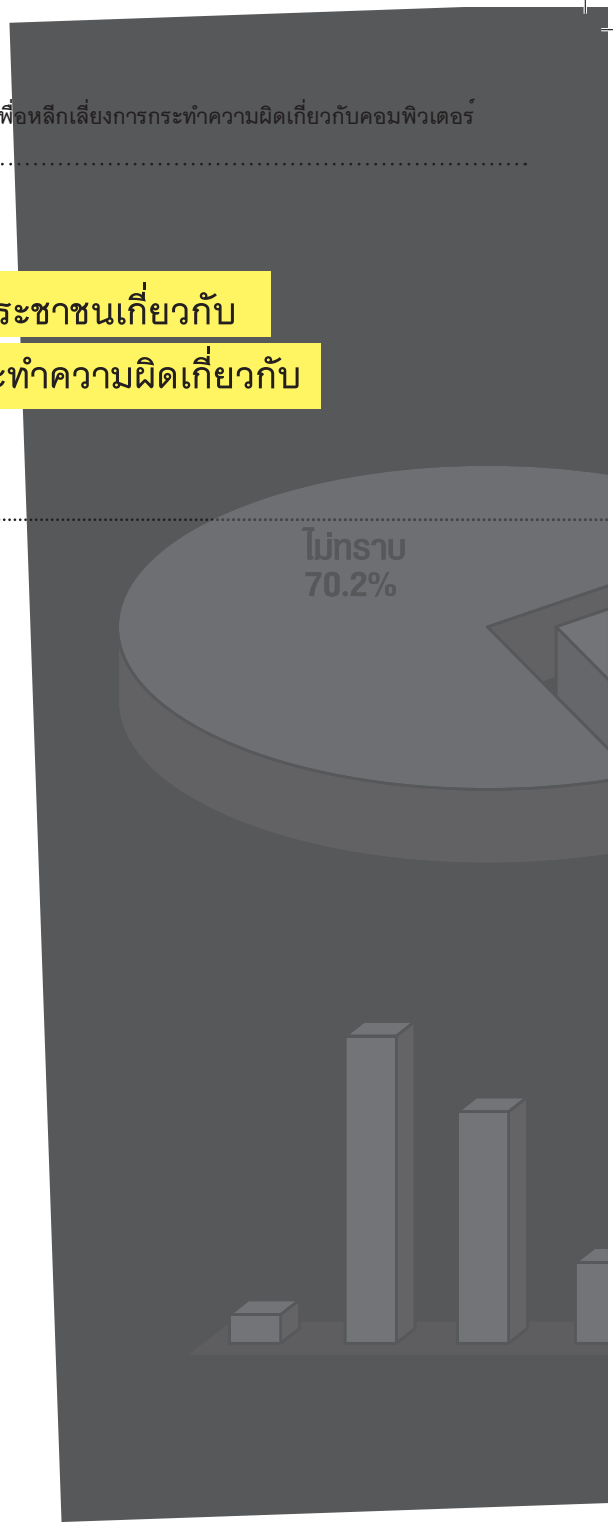
6. การขอความร่วมมือส่วนผู้ให้บริการในต่างประเทศในการขอข้อมูลจราจรทำได้ยาก เนื่องจาก ปัจจุบันมีการติดต่อสื่อสารผ่านระบบเครือข่ายอินเทอร์เน็ตทั้งในประเทศและต่างประเทศกันอย่างกว้างขวาง หากการกระทำความผิดเกิดที่ผู้ให้บริการต่างประเทศในการใช้งานในทางที่เหมาะสม การเผยแพร่ข้อมูลที่ไม่เป็นจริง ผู้ให้บริการในต่างประเทศไม่ได้บังคับใช้กฎหมายของไทย ทำให้ผู้ให้บริการต่างประเทศไม่ให้ร่วมมือ หากเมื่อมีการกระทำความผิดจากผู้ให้บริการต่างประเทศการขอข้อมูลจารจรรวมถึงการแจ้งการปิดกั้นข้อความรูปภาพที่ไม่เหมาะสมจะทำด้วยความยากลำบาก ซึ่งจะต้องไปดูที่กฎหมายระหว่างประเทศ

7. ปัญหาความผิดฐานทำให้เสียทรัพย์ของกฎหมายคอมพิวเตอร์ที่เกิดจากไวรัสคอมพิวเตอร์ แฮกเกอร์ ได้สร้างความเสียหายต่อเครื่องคอมพิวเตอร์ โครงข่ายคอม-พิวเตอร์ หรือวัตถุที่ได้รับจากการประมวลของคอมพิวเตอร์ ความเสียหายมักเกิดกับข้อมูลและโปรแกรมคอมพิวเตอร์ ซึ่งไม่ได้สร้างความเสียหายกับระบบฮาร์ดแวร์เลย จึงไม่สามารถนำความผิดฐานทำให้เสียทรัพย์มาปรับใช้กับความเสียหายที่เกิดขึ้นจากไวรัส แฮกเกอร์ได้ แต่อย่างไรก็ตามมีข้อน่าสังเกตประการหนึ่งคือ แม้การกระทำดังกล่าวไม่สร้างความเสียหายต่อคอมพิวเตอร์ฮาร์ดแวร์ แต่การทำงานของเครื่องคอมพิวเตอร์ต้องประกอบด้วย 3 ส่วน คือ ฮาร์ดแวร์ ซอฟท์แวร์และข้อมูล หากขาดส่วนใดส่วนหนึ่งของการทำงานก็จะไม่สามารถทำงานได้เลย จึงสามารถตีความได้ว่าเป็นการทำให้ฮาร์ดแวร์ไร้ประโยชน์ อันเป็นความผิดทำให้เสียทรัพย์

8. ปัญหาความไม่เข้าใจของประชาชนเรื่องการแจ้งความดำเนินคดี ซึ่งตั้งแต่กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มีผลบังคับใช้ ประชาชนสามารถแจ้งความได้ที่สถานีตำรวจทั่วประเทศ อย่างไรก็ตามยังเห็นว่ายังมีประชาชนเข้ามาร้องเรียนที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารซึ่งสามารถทำได้ แต่หากประชาชนที่อยู่ห่างไกลก็สามารถแจ้งความได้ที่สถานีตำรวจใกล้บ้านท่าน โดยส่วนใหญ่เป็นการหมิ่นประมาทและเผยแพร่ภาพลามกอนาจาร ส่วนคดีที่มีมูลค่าความเสียหายมาก แต่ก็ยังเป็นปัญหาของทางสถานีตำรวจท้องที่ซึ่งอาจไม่มีเจ้าหน้าที่ที่มีความรู้ด้านคอมพิวเตอร์ทำให้การดำเนินงาน การประสานงานเกิดความล่าช้า ต้องมีการแก้ไขกันต่อไป

9. ปัญหาการซื้ออุปกรณ์ต่าง ๆ ที่มีประสิทธิภาพสูงในการทำงานจากต่างประเทศ เช่น การนำเครื่องมือมาใช้งานในการตรวจจับการกระทำผิด จะต้องมีการควบคุมจากภาครัฐในการนำเข้ามาใช้ การจดทะเบียนเพื่อควบคุมเพื่อง่ายต่อการตรวจสอบ การหาตัวผู้กระทำความผิด เป็นการตัดปัญหาที่ต้นเหตุ เนื่องจากเป็นการสร้างช่องทางให้อาชญากรทางเทคโนโลยีมาก่อปัญหาการจรกรรมข้อมูล การสร้างความเสียหาย หรือ อาชญากรรมต่างๆ ได้

การสำรวจความคิดเห็นของประชาชนเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550



สำนักงานสถิติแห่งชาติ ดำเนินการสำรวจความคิดเห็นของประชาชนเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อใช้เป็นแนวทางในการปรับปรุงการประชาสัมพันธ์เผยแพร่เกี่ยวกับพระราชบัญญัติให้แก่สาธารณะชนได้เข้าใจอย่างแท้จริง และเป็นผลให้การบังคับใช้พระราชบัญญัติมีประสิทธิภาพสูงสุด

โดยการสัมภาษณ์สมาชิกในครัวเรือนตัวอย่างที่มีอายุ 18 ปีขึ้นไป ครัวเรือนละ 1 คน รวมทั้งสิ้น 5,800 คน ระหว่างวันที่ 1 – 20 พฤษภาคม 2551 และนำเสนอผลในระดับกรุงเทพฯ ภาค และทั่วประเทศ

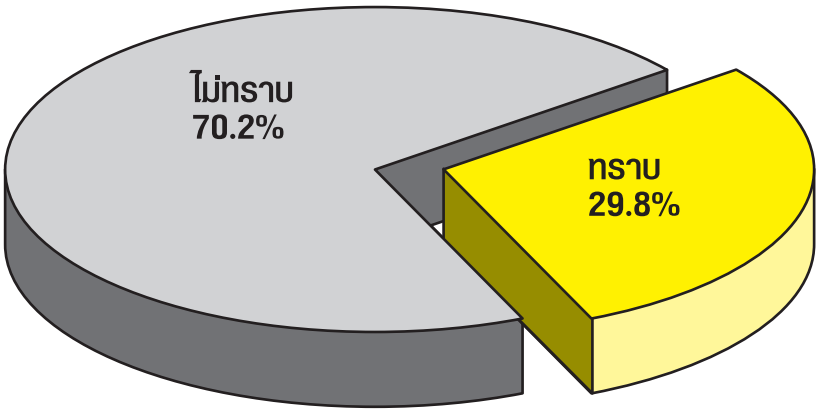
ข้อมูลทั่วไปของผู้ตอบสัมภาษณ์

ผู้-ตอบสัมภาษณ์ เป็นชาย ร้อยละ 47.5 เป็นหญิงร้อยละ 52.5 และมีอายุระหว่าง 18 – 29 ปี ร้อยละ 26.4 อายุ 30 – 39 ปี ร้อยละ 25.2 อายุ 40 – 49 ปี ร้อยละ 24.1 อายุ 50 – 59 ปี ร้อยละ 15.9 อายุ 60 ปี ขึ้นไป ร้อยละ8.4 สำหรับการศึกษามีการศึกษาต่ำกว่าปริญญาตรี ร้อยละ 81.7 ปริญญาตรี ร้อยละ 17.0 สูงกว่าปริญญาตรี ร้อยละ 1.3 ส่วนสถานภาพการทำงานของผู้ตอบสัมภาษณ์ เป็นเกษตรกร ร้อยละ 19.9 ค้าขาย / ประกอบธุรกิจส่วนตัว ร้อยละ18.6 พนักงาน/ลูกจ้างเอกชน ร้อยละ 18.1 แม่บ้าน/ไม่ได้ประกอบอาชีพ ร้อยละ 12.1 ข้าราชการ/พนักงานรัฐวิสาหกิจ ร้อยละ10.4 รับจ้างทั่วไป/กรรมกร ร้อยละ 10.2 และอื่น ๆ ร้อยละ 10.7

1. ความคิดเห็นเกี่ยวกับ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1) การทราบว่ามี พ.ร.บ.

หลังจากที่ได้มีการบังคับใช้ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตั้งแต่วันที่ 18 กรกฎาคม 2550 ผลการสำรวจความคิดเห็นของประชาชน 18 ปีขึ้นไป พบว่า มีประชาชนถึงร้อยละ 70.2 ไม่ทราบว่ามี พ.ร.บ. ออกมาบังคับใช้ มีเพียงร้อยละ 29.8 เท่านั้นที่ทราบว่ามี โดยช่องทางที่ทำให้ประชาชนทราบว่ามี พ.ร.บ. ออกมาบังคับใช้นั้น ส่วนใหญ่ทราบมาจากสื่อโทรทัศน์มากที่สุด ร้อยละ 23.9 รองลงมา สื่อสิ่งพิมพ์ ร้อยละ 10.0 เว็บไซต์ ร้อยละ 8.6 เพื่อน/คนรู้จัก/บุคคลทั่วไป ร้อยละ 7.0 สื่อวิทยุ ร้อยละ 4.2 บุคลากรของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) โดยตรง ร้อยละ 1.3 และอื่นๆ อีกร้อยละ 0.4

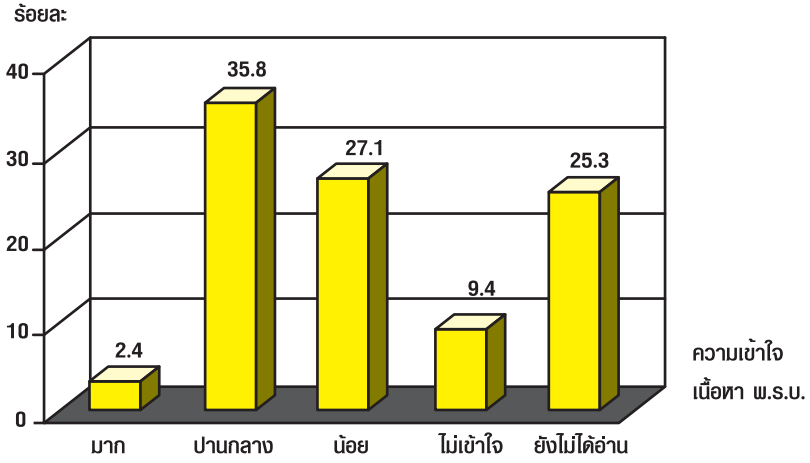


แผนภูมิ 1
ร้อยละของประชาชน จำแนกตามการทราบว่ามี พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ออกมาบังคับใช้ทั่วประเทศ

2)ความเข้าใจในเนื้อหาของ พ.ร.บ.

สำหรับประชาชนที่ทราบว่ามี พ.ร.บ. ดังกล่าวออกมาบังคับใช้แล้ว เมื่อสอบถามถึงความเข้าใจในเนื้อหาของ พ.ร.บ. ประชาชนส่วนใหญ่ระบุว่ามีความเข้าใจอยู่ในระดับปานกลางถึงมาก ร้อยละ 38.2 เข้าใจน้อย ร้อยละ 27.1 ส่วนที่ไม่มีความเข้าใจใน พ.ร.บ.ดังกล่าวเลย มีร้อยละ 9.4 และเป็นที่น่าสังเกตว่ายังมีประชาชนอีกถึงร้อยละ 25.3 ที่ทราบว่ามี พ.ร.บ. ฉบับนี้แต่ยังไม่มีโอกาสได้อ่านหรือทำความเข้าใจ

นอกจากนั้น ยังได้สอบถามถึงการเตรียมตัวของประชาชนเพื่อป้องกันไม่ให้กระทำความผิดตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ผลสำรวจ พบว่า ประชาชนถึงร้อยละ 80.5 ยังไม่ได้มีการเตรียมตัว มีเพียงร้อยละ 19.5 ที่มีการเตรียมตัว

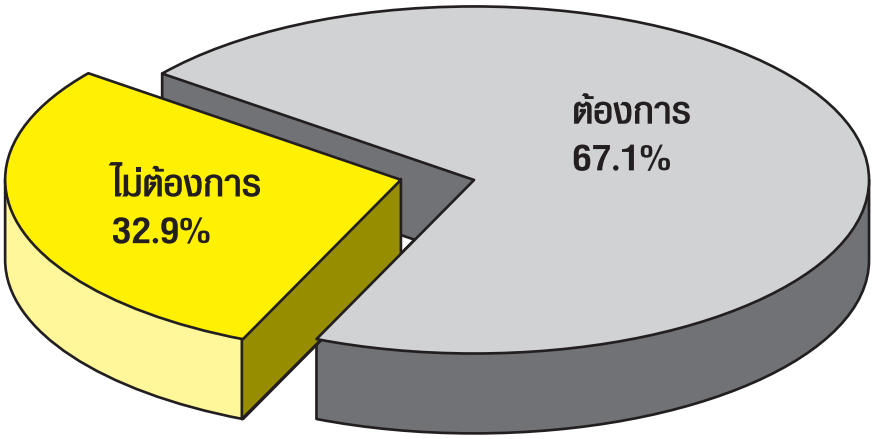


หมายเหตุ : 1/ ถามเฉพาะผู้ที่ทราบว่ามี พ.ร.บ.

3) ความต้องการทราบข้อมูลเกี่ยวกับ พ.ร.บ.

ประชาชนส่วนใหญ่ทั่วประเทศถึงร้อยละ 67.1 มีความต้องการทราบข้อมูลเกี่ยวกับ พ.ร.บ. โดยต้องการให้เผยแพร่ทางสื่อโทรทัศน์มากที่สุด รองลงมา สื่อสิ่งพิมพ์ เว็บไซต์ สื่อวิทยุ บุคลากรของกระทรวง ICT โดยตรง งานสัมมนา และอื่นๆ ตามลำดับ

ช่องทาง	ร้อยละ
• สื่อโทรทัศน์	47.0
• สื่อสิ่งพิมพ์	9.4
• เว็บไซต์	4.4
• สื่อวิทยุ	2.9
• บุคลากรของกระทรวง(ICT)	1.7
• งานสัมมนา	1.2
• อื่น ๆ	0.5



แผนภูมิ 3
ร้อยละของประชาชน จำแนกตามความต้องการทราบข้อมูลเกี่ยวกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ทั่วประเทศ

2. การทราบความหมายของคำที่เกี่ยวกับคอมพิวเตอร์

จากการสอบถามประชาชนว่าทราบความหมายของคำที่เกี่ยวกับคอมพิวเตอร์ ได้แก่ “ซอฟแวร์ลิขสิทธิ์” “การเข้าถึงอินเทอร์เน็ต” “พนักงานเจ้าหน้าที่” “ระบบคอมพิวเตอร์” “ข้อมูลคอมพิวเตอร์” “ข้อมูลจราจรคอมพิวเตอร์” “ผู้ให้บริการ” “ผู้ใช้บริการ” ปรากฏว่า ประชาชนโดยรวมทั่วประเทศทราบความหมายของคำว่า “ผู้ใช้บริการ” มากที่สุด (52.2%) ส่วนคำที่ประชาชนทราบความหมายน้อยที่สุด คือ “ข้อมูลจราจรคอมพิวเตอร์” (14.9%)

คำ/ประโยค	รวม	การทราบความหมาย	
		ทราบ	ไม่ทราบ
ซอฟแวร์ลิขสิทธิ์	100.0	30.5	69.5
การเข้าถึงอินเทอร์เน็ต	100.0	36.2	63.8
พนักงานเจ้าหน้าที่	100.0	38.3	61.7
ระบบคอมพิวเตอร์	100.0	39.4	60.6
ข้อมูลคอมพิวเตอร์	100.0	40.3	59.7
ข้อมูลจราจรคอมพิวเตอร์	100.0	14.9	85.1
ผู้ให้บริการ	100.0	48.0	52.0
ผู้ใช้บริการ	100.0	52.2	47.8

ตาราง 1
ร้อยละของประชาชนจำแนกตามการทราบความหมายของคำ/ประโยคที่เกี่ยวข้องกับคอมพิวเตอร์ ทั่วประเทศ

3. การทราบการกระทำที่มีความผิดตาม พ.ร.บ.

เมื่อสอบถามถึงการทราบการกระทำที่มีความผิดตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ประชาชนส่วนใหญ่ไม่ทราบว่ามีความผิด โดยมีความคิดเห็นของประชาชนมีสัดส่วนตาม ตาราง 2

ความผิดตาม พ.ร.บ. คอมพิวเตอร์	รวม	การทราบว่ามีความผิด	
		ทราบ	ไม่ทราบ
" การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน	100.0	39.2	60.8
" การเปิดเผยวิธีการที่จะเข้าไปยังระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน	100.0	36.1	63.9
" การเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน	100.0	37.5	62.5
" การดักข้อมูลคอมพิวเตอร์ที่อยู่ระหว่างการส่งของระบบคอมพิวเตอร์	100.0	32.0	68.0
" การทำลาย แก้ไข เปลี่ยนแปลงเพิ่มเติมข้อมูลผู้อื่นโดยไม่ได้รับ อนุญาต	100.0	40.5	59.5
" การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ที่มีการปกปิดหรือปลอมแปลงแหล่งที่มาของข้อมูลเพื่อรบกวนการทำงานของผู้อื่น	100.0	31.4	68.6
" การเผยแพร่ข้อมูลที่เป็นเท็จเข้าสู่ระบบคอมพิวเตอร์	100.0	35.3	64.7
" การเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงของชาติเข้าสู่ระบบคอมพิวเตอร์	100.0	43.1	56.9
" การเผยแพร่ข้อมูลความผิดที เกี่ยวกับการก่อการร้ายเข้าสู่ระบบคอมพิวเตอร์	100.0	41.3	58.7
" การเผยแพร่ข้อมูลที่มีลักษณะ ลามกอนาจารเข้าสู่ระบบคอมพิวเตอร์	100.0	50.1	49.9
" การเผยแพร่ภาพตัดต่อที่เป็นการหมิ่นประมาทเข้าสู่ระบบ คอมพิวเตอร์	100.0	45.6	54.4
" ผู้ให้บริการการเข้าถึงอินเทอร์เน็ต ไม่มีการเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ 90 วัน	100.0	13.9	86.1

ตาราง 2
ร้อยละของประชาชนจำแนกตามการทราบความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ทั่วประเทศ

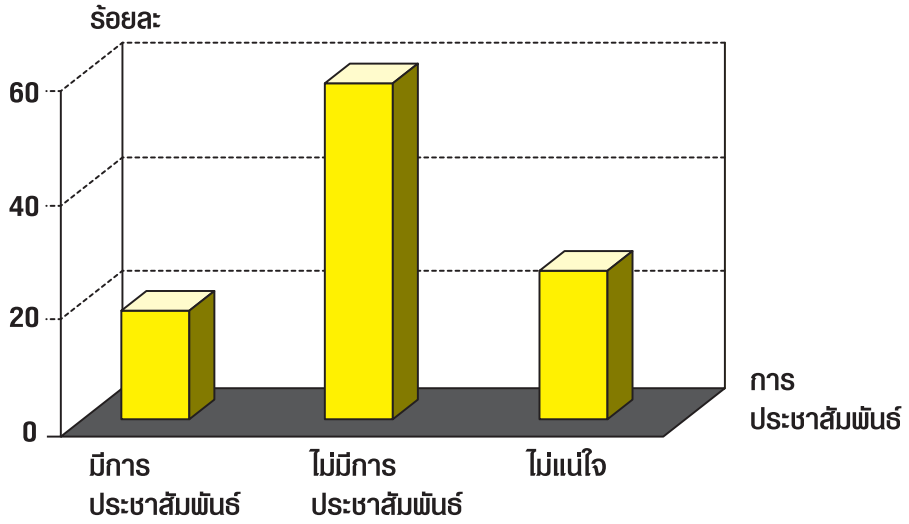
4. การดำเนินการด้านการรักษาความปลอดภัยของหน่วยงาน

จากการสำรวจได้สอบถามประชาชนที่มีสถานภาพการทำงานเป็นข้าราชการ/พนักงานรัฐวิสาหกิจ พนักงาน/ลูกจ้างเอกชน ค้าขาย/ประกอบธุรกิจส่วนตัว ถึงการดำเนินการเกี่ยวกับมาตรการรักษาความปลอดภัยของหน่วยงาน/ที่ทำงานเพื่อรับมือกับพ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ตามมาตรการที่ปรากฏในตาราง 3 พบว่า ประชาชนประมาณ ร้อยละ 42 – 55 ระบุว่าหน่วยงาน/ที่ทำงานยังไม่มีการดำเนินการ

มาตรการรักษาความปลอดภัย	รวม	การดำเนินการของหน่วยงาน		
		มี	ไม่มี	ไม่แน่ใจ
" จัดทำแผนพัฒนาระบบคอมพิวเตอร์ทางด้านความปลอดภัย	100.0	16.4	53.8	29.8
" จัดเก็บข้อมูลจราจรคอมพิวเตอร์	100.0	13.2	54.6	32.2
" จัดให้มีโปรแกรมรักษาความปลอดภัย	100.0	36.6	42.7	20.7
" จัดให้มีอุปกรณ์รักษาความปลอดภัย	100.0	28.8	47.4	23.8
" จัดทำแผนงบประมาณการจัดซื้อจัดจ้าง	100.0	16.0	52.3	31.7

ตาราง 3
ร้อยละของประชาชน จำแนกตามการดำเนินการด้านรักษาความปลอดภัยของหน่วยงาน/ที่ทำงาน ทั่วประเทศ

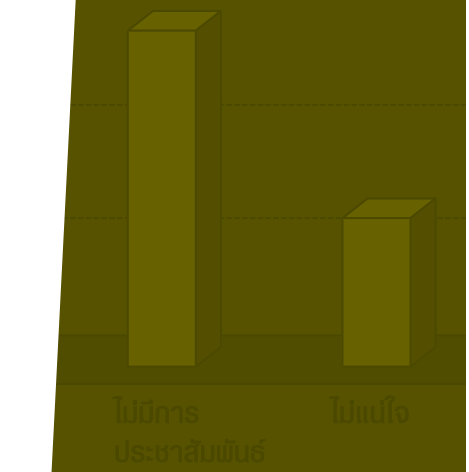
นอกจากนั้นยังได้สอบถามถึงการประชาสัมพันธ์หรือการมีนโยบายของหน่วยงานเพื่อให้เจ้าหน้าที่ในหน่วยงานปฏิบัติตาม พ.ร.บ. ฉบับนี้ พบว่า ประชาชนส่วนใหญ่ ร้อยละ 59.4 ระบุว่าหน่วยงานยังไม่มี ร้อยละ 17.6 มี และร้อยละ 23.0 ไม่แน่ใจ



แผนภูมิ 4
ร้อยละของประชาชนจำแนกตามการประชาสัมพันธ์ของหน่วยงานเพื่อให้เจ้าหน้าที่ปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ทั่วประเทศ

5. ข้อคิดเห็นและข้อเสนอแนะ

สำหรับข้อคิดเห็นและข้อเสนอแนะมีผู้แสดงความคิดเห็น (18.7%) ต่อ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ดังนี้ ประชาสัมพันธ์สร้างความรู้ ความเข้าใจเกี่ยวกับ พ.ร.บ. ฉบับนี้ให้มากขึ้น ทั้งในรูปเอกสารและผ่านสื่ออื่น ๆ ควรลงโทษผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างจริงจัง ควรมีมาตรการควบคุมเยาวชนในการใช้อินเทอร์เน็ต และร้านค้าผู้ให้บริการอินเทอร์เน็ตควรมีมาตรการควบคุม/ตรวจสอบการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเข้มงวดและมีคุณภาพ เป็นต้น



ที่มา : สำนักสถิติเศรษฐกิจสังคมและประชามติ 3 สำนักงานสถิติแห่งชาติ. 2551. สำรวจความคิดเห็นของประชาชนเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. กรุงเทพฯ.

บทที่ 2

ฐานความผิด องค์ประกอบความผิด และบทกำหนดโทษ

ความก้าวหน้าทางเทคโนโลยีสารสนเทศและการสื่อสาร ได้เข้ามามีบทบาทในการดำเนินชีวิตของคนทุกคนในสังคม ทำให้บุคคลไม่หวังดีนำมาใช้เป็นช่องทางเพื่อสร้างประโยชน์ส่วนตน จนก่อให้เกิดปัญหาทางอาชญากรรมทางคอมพิวเตอร์ เมื่อมีการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อย่างเป็นทางการเมื่อวันที่ 18 กรกฎาคม พ.ศ. 2550 ประชาชน หน่วยงานทุกภาคส่วนจึงจำเป็นที่ต้องปฏิบัติตาม

ดังนั้น การสร้างความรู้ และความเข้าใจที่เกี่ยวกับฐานความผิด องค์ประกอบความผิดและบทกำหนดโทษ จึงเป็นสิ่งที่จำเป็นสำคัญอย่างยิ่ง เพื่อให้ผู้ใช้งาน ผู้ปฏิบัติงานและผู้ดูแลระบบคอมพิวเตอร์จะได้สามารถนำมาเป็นแนวทางในการปฏิบัติตามกฎหมาย โดยได้รวบรวมรายละเอียดและอธิบายฐานความผิด องค์ประกอบความผิดและบทกำหนดโทษ ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อให้ทุกคนเข้าใจสาระสำคัญของกฎหมายมากขึ้น ลักษณะความผิดและบทกำหนดโทษของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แบ่งได้ 2 หมวด ได้แก่ ความผิดเกี่ยวกับคอมพิวเตอร์ และพนักงานเจ้าหน้าที่

ลักษณะความผิดเกี่ยวคอมพิวเตอร์ ประกอบด้วย 13 มาตรา กล่าวคือตั้งแต่มาตราที่ 5 ถึงมาตราที่ 17 มีฐานความผิดครอบคลุมว่าด้วยการกระทำความความผิดที่เกี่ยวกับคอมพิวเตอร์ ดังรายละเอียดดังต่อไปนี้

ความผิดเกี่ยวกับคอมพิวเตอร์

ฐานความผิด	โทษจำคุก	โทษปรับ
มาตรา 5 เข้าถึงคอมพิวเตอร์โดยมิชอบ	ไม่เกิน 6 เดือน	ไม่เกิน 10,000 บาท
มาตรา 6 ล่วงรู้มาตรการป้องกัน	ไม่เกิน 1 ปี	ไม่เกิน 20,000 บาท
มาตรา 7 เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ	ไม่เกิน 2 ปี	ไม่เกิน 40,000 บาท
มาตรา 8 การดักข้อมูลคอมพิวเตอร์	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท
มาตรา 9 ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 10 ทำให้ระบบไม่สามารถทำงานได้ตามปกติ	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 11 สแปมเมล์	ไม่มี	ไม่เกิน 100,000 บาท
มาตรา 12 กระทำผิดมาตรา 9 หรือมาตรา 10	ไม่เกิน 10 ปี	ไม่เกิน 200,000 บาท
(1) ก่อให้เกิดความเสียการแก่ประชาชน (2) กระทบต่อความมั่นคงปลอดภัยของประเทศ/เศรษฐกิจ วรรคท้าย เป็นเหตุให้ผู้อื่นถึงแก่ชีวิต	3 ปี ถึง 15 ปี 10 ปี ถึง 20 ปี	60,000 - 300,000 บาท ไม่มี
มาตรา 13 การจำหน่าย/เผยแพร่ชุดคำสั่ง	ไม่เกิน 1 ปี	ไม่เกิน 20,000 บาท
มาตรา 14 การเผยแพร่เนื้อหาอันไม่เหมาะสม	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 15 และ มาตรา 26 ความรับผิดชอบของผู้ให้บริการ(ISP7)	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 16 การตัดต่อภาพผู้อื่น	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท
มาตรา 17 การกระทำความผิดนอกราชอาณาจักรต้องได้รับโทษในราชอาณาจักร		

7ISP (Internet Service Provider) คือ ผู้ให้บริการอินเทอร์เน็ต

การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ

มาตรา 5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

โทษ ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

การเจาะระบบคอมพิวเตอร์ หรือการบุกรุกทางคอมพิวเตอร์ เช่น การใช้โปรแกรมสปายแวร์ (spyware[8]) ขโมยข้อมูลรหัสผ่านส่วนบุคคลของผู้อื่นเพื่อใช้บุกรุกเข้าไปในระบบคอมพิวเตอร์ของผู้นั้นผ่านช่องโหว่ของระบบดังกล่าวโดยไม่ได้รับอนุญาต

การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์

มาตรา 6 ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

โทษ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ เช่น การใช้โปรแกรม keystroke[9] แอบบันทึกการกดรหัสผ่านของผู้อื่น แล้วนำไปโพสต์ในกระทู้ต่าง ๆ เพื่อให้บุคคลที่สามสามารถใช้รหัสผ่านเข้าไปในระบบคอมพิวเตอร์ของผู้ที่เป็นเหยื่อได้

การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ

มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

โทษ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ เช่น การกระทำการใด ๆ ที่กล่าวว่าไว้ในมาตราข้างต้น เพื่อเข้าถึงแฟ้มข้อมูลที่มีชั้นความลับโดยไม่ได้รับอนุญาต

8 Spy ware เป็นซอฟต์แวร์ที่เขียนมาเพื่อส่งข้อมูลส่วนบุคคลของคุณไปยังคน หรือสิ่งที่ได้กำหนดไว้ ลักษณะจะคล้ายกับ Cookies แต่ว่า spy ware จะเป็น Cookies ที่แอบแฝงเข้ามา โดยที่คุณไม่รู้ตัว เพื่อวัตถุประสงค์เพื่อการโฆษณา หรือแอบนำข้อมูลส่วนตัวของคุณส่งออกไป

9 keystroke คือ เป็น spyware ชนิดหนึ่ง เมื่อเวลาเข้าเว็บต่างๆ เช่น MSN WLM Yahoo เป็นต้น ที่ต้องใช้ รหัสในการเข้า keystroke จะแผงมากับผู้ไม่หวังดี จะจดจำการกระทำของเราทุกๆ อย่างทำให้ข้อมูลของเราถูกเปิดเผย

การพิจารณาฐานความผิด

- การกระทำซึ่งเป็นความผิดตามมาตรา 7 อาจต้องมีการกระทำความผิดตามมาตรา 5 เสียก่อน

การดักข้อมูลคอมพิวเตอร์โดยมิชอบ

มาตรา 8 ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

โทษ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

การดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นในระหว่างการส่ง เช่น การใช้สนิฟเฟอร์ (sniffer[10]) แอบดัก (packet[11]) ซึ่งเป็นชุดของข้อมูลที่เล็กที่สุดอยู่ระหว่างการส่งไปให้ผู้รับ

การรบกวนข้อมูลคอมพิวเตอร์

มาตรา 9 ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

โทษ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

การรบกวนระบบคอมพิวเตอร์

มาตรา 10 ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

โทษ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

เหตุผล การกำหนดฐานความผิดคำนึงถึงการก่อให้เกิดการปฏิเสธการให้บริการ (Denial of Service) เป็นสำคัญ

การรบกวนข้อมูลหรือระบบคอมพิวเตอร์ เช่น การใช้โปรแกรมไวรัสส่ง e-mail[12] จำนวนมหาศาล ส่งไปยังคอมพิวเตอร์ผู้อื่น เพื่อรบกวนทำให้ระบบคอมพิวเตอร์นั้น ไม่สามารถทำงานได้ตามปกติ

10 Sniffer เป็นโปรแกรมที่กำหนดขึ้นเพื่อลักลอบดักข้อมูลที่ส่งผ่านระบบเครือข่าย ทำให้ทราบรหัสผ่านของบุคคลหรือส่งโอนข้อมูลผ่านระบบเครือข่าย

11 Packet (แพ็คเกต) เป็นหน่วยของข้อมูลที่ส่งระหว่างจุดเริ่มต้นกับปลายบนอินเทอร์เน็ต

12 E-Mail (Electronic Mail) จดหมายอิเลคทรอนิกส์ เป็นข้อมูลที่มีการรับและส่งโดยเครื่องคอมพิวเตอร์โดยผ่านเครือข่ายของ การสื่อสาร

สแปมเมล์ (Spam Mail[13])

มาตรา 11 ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

โทษ ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

การกระทำใกล้เคียงกับมาตรา 10 กระทำความผิดโดยใช้โปรแกรมหรือชุดคำสั่งส่งไปให้เหยื่อเป็นจำนวนมาก ๆ โดยปกปิดแหล่งที่มา เช่น IP address[14] เป็นต้น ซึ่งมักก่อให้เกิดความเสียหายเชิงเศรษฐกิจ หรือส่งผลกระทบต่อการใช้ทรัพยากรของระบบคอมพิวเตอร์

การกระทำซึ่งก่อให้เกิดผลกระทบต่อความมั่นคง

มาตรา 12 ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10

(1) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันที หรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(2) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะหรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์[15]ที่มีไว้เพื่อประโยชน์สาธารณะ

โทษ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

เหตุผล กำหนดโทษหนักขึ้นตามความเสียหายที่เกิดขึ้น

การรบกวนระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์อันเป็นเท็จ เช่น การเจาะเข้าไปในระบบคอมพิวเตอร์และแอบเติมหรือทำลายข้อมูลคอมพิวเตอร์ ที่ก่อให้เกิดความเสียหายต่อประเทศชาติหรือสร้างความตื่นตระหนกแก่ประชาชน

13 Spam Mail คือ การส่ง mail จำนวนมาก ๆ ในครั้งหนึ่ง หรือการทยอยส่งแต่ส่งจำนวนมากฉบับ สำหรับวัตถุประสงค์นั้นมีหลายหลาก ตั้งแต่โฆษณาสินค้า การโจมตีระบบ การแก้แค้นส่วนตัว การกลั่นแกล้งฯลฯ

14 IP Address คือ หมายเลขอินเตอร์เน็ต หรือหมายเลขประจำตัวของคอมพิวเตอร์ ซึ่งจะมีหมายเลขที่ไม่ซ้ำกันเลย ประกอบด้วยตัวเลข 4 ชุด ที่คั่นด้วยจุลภาค (.) โดยตัวเลขแต่ละชุดจะมี ค่าได้ตั้งแต่ 0 จนถึง 255 เช่น 158.108.2.71

15 ระบบคอมพิวเตอร์ อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

จัดจำหน่าย เผยแพร่ชุดคำสั่งที่ใช้ในการกระทำความผิด

มาตรา 13 ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11

โทษ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

เหตุผล จำกัดเฉพาะกรณีโปรแกรมคอมพิวเตอร์เท่านั้น ซึ่งแต่เดิมรวมถึงฮาร์ดแวร์ (อุปกรณ์) ด้วย

ตัวอย่างโปรแกรมคอมพิวเตอร์ที่ก่อให้เกิดความเสียหายหรืออันตรายได้

Virus สร้างขึ้นเพื่อทำลายระบบและมักมีการแพร่กระจายตัวได้อย่างรวดเร็ว

Trojan Horse คือ โปรแกรมที่กำหนดให้ทำงานโดยแฝงอยู่กับโปรแกรมทั่วไป เพื่อจุดประสงค์ใดจุดประสงค์หนึ่ง เช่น การขโมยข้อมูล เป็นต้น

Bombs คือ โปรแกรมที่กำหนดให้ทำงานภายใต้เงื่อนไขที่กำหนดขึ้น เช่น Logic Bomb เป็นโปรแกรมที่กำหนดเงื่อนไขให้ทำงานเมื่อมีเหตุการณ์หรือเงื่อนไขใดๆเกิดขึ้น

Rabbit เป็นโปรแกรมที่กำหนดขึ้นเพื่อให้สร้างตัวมันเองซ้ำๆ เพื่อให้ระบบไม่สามารถทำงานได้ เช่น พื้นที่หน่วยความจำเต็ม

Sniffer เป็นโปรแกรมที่กำหนดขึ้นเพื่อลักลอบดักข้อมูลที่ส่งผ่านระบบเครือข่าย ทำให้ทราบรหัสผ่านของบุคคลหรือส่งโอนข้อมูลผ่านระบบเครือข่าย

การนำเข้า/เผยแพร่เนื้อหาอันไม่เหมาะสม

มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

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

โทษ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

บทลงโทษผู้ให้บริการ[16]

มาตรา 15 ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

โทษ ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

เหตุผล ผู้ให้บริการในที่นี้มุ่งประสงค์ถึงเจ้าของเว็บไซต์[17] ซึ่งมีการพิจารณาว่าควรต้องมีหน้าที่ลบเนื้อหาอันไม่เหมาะสมด้วย

มาตรา 16 ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

โทษ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้ ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดามารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

การหมิ่นประมาทโดยภาพหรือข้อมูล การตัดต่อ ดัดแปลงบนกระดานข่าว18, เว็บไซต์โดยเจตนาทำให้ประชาชนทั่วไปสถาบันพระมหากษัตริย์ ความมั่นคงของประเทศได้รับความเสียหาย

16ผู้ให้บริการ
(1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น แบ่งได้เป็น

กลุ่ม 1: ผู้ประกอบกิจการโทรคมนาคมและกิจการกระจายภาพและเสียง ได้แก่ โทรศัพท์พื้นฐาน มือถือ ดาวเทียม สื่อสารไร้สาย เป็นต้น

กลุ่ม 2: ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ได้แก่ สถานศึกษา หน่วยงานราชการ บริษัท โรงแรม หอพัก ร้านอาหาร เป็นต้น

กลุ่ม 3: ผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อการให้บริการโปรแกรมประยุกต์ต่างๆ ได้แก่ Web hosting, Internet Data Center

กลุ่ม 4: ผู้ให้บริการร้านอินเทอร์เน็ต ได้แก่ Internet Café เกมออนไลน์

(2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น คือ ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ ได้แก่ ผู้ให้บริการ Web board, Web blog, Internet Banking, e-Commerce, Web services เป็นต้น

17 Web Site หรือ Website คือ หน้าเว็บเพจหลายหน้า ซึ่งเชื่อมโยงกันผ่านทางไฮเปอร์ลิงก์ ส่วนใหญ่จัดทำขึ้นเพื่อนำเสนอข้อมูลผ่านคอมพิวเตอร์ โดยถูกจัดเก็บไว้ในเวิลด์ไวด์เว็บ หน้าแรกของเว็บไซต์ที่เก็บไว้ที่ชื่อหลักจะเรียกว่า โฮมเพจ

การเผยแพร่ภาพซึ่งตัดต่อในลักษณะหมิ่นประมาท

มาตรา 16 ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

โทษ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริตผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้ ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

การหมิ่นประมาทโดยภาพหรือข้อมูล การตัดต่อ ดัดแปลงบนกระดานข่าว18, เว็บไซต์โดยเจตนาทำให้ประชาชนทั่วไปสถาบันพระมหากษัตริย์ ความมั่นคงของประเทศได้รับความเสียหาย

18 WebBoard กระดานข่าวกระดานสนทนา เป็นโปรแกรมที่ทำหน้าที่ในลักณะเป็นกระดานสนทนา เป็นกระดานแจ้งข่าวสาร ข้อมูล และแลกเปลี่ยนความคิดเห็นกัน โดยใช้รูปแบบการแสดงผล HTML ที่นิยมใช้ใน World Wide Web. WebBoard อนุญาตให้ผู้เยี่ยมชมเวปไซต์ และผู้พัฒนาเวปไซต์สามารถตั้งหัวข้อกระทู้เพื่อประกาศข่าวสาร แลกเปลี่ยนความคิดเห็นกันได้

ที่มา : บทวิเคราะห์มาตราทางกฎหมายที่เกี่ยวข้องกับระบบคอมพิวเตอร์จากภัยไวรัส แฮกเกอร์

พนักงานเจ้าหน้าที่

ฐานความผิด	โทษจำคุก	โทษปรับ
มาตรา 5 เข้าถึงคอมพิวเตอร์โดยมิชอบ	ไม่เกิน 6 เดือน	ไม่เกิน 10,000 บาท
มาตรา 6 ล่วงรู้มาตรการป้องกัน	ไม่เกิน 1 ปี	ไม่เกิน 20,000 บาท
มาตรา 7 เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ	ไม่เกิน 2 ปี	ไม่เกิน 40,000 บาท
มาตรา 8 การดักข้อมูลคอมพิวเตอร์	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท
มาตรา 9 ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 10 ทำให้ระบบไม่สามารถทำงานได้ตามปกติ	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 11 สแปมเมล์	ไม่มี	ไม่เกิน 100,000 บาท
มาตรา 12 กระทำผิดมาตรา 9 หรือมาตรา 10	ไม่เกิน 10 ปี	ไม่เกิน 200,000 บาท
(1) ก่อให้เกิดความเสียการแก่ประชาชน (2) กระทบต่อความมั่นคงปลอดภัยของประเทศ/เศรษฐกิจ วรรคท้าย เป็นเหตุให้ผู้อื่นถึงแก่ชีวิต	3 ปี ถึง 15 ปี 10 ปี ถึง 20 ปี	60,000 - 300,000 บาท ไม่มี
มาตรา 13 การจำหน่าย/เผยแพร่ชุดคำสั่ง	ไม่เกิน 1 ปี	ไม่เกิน 20,000 บาท
มาตรา 14 การเผยแพร่เนื้อหาอันไม่เหมาะสม	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 15 และ มาตรา 26 ความรับผิดชอบของผู้ให้บริการ(ISP7)	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 16 การตัดต่อภาพผู้อื่น	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท
มาตรา 17 การกระทำความผิดนอกราชอาณาจักรต้องได้รับโทษในราชอาณาจักร		

อำนาจของพนักงานเจ้าหน้าที่

มาตรา 18 อำนาจทั่วไปของพนักงานเจ้าหน้าที่ที่ได้รับการแต่งตั้ง แบ่งเป็น

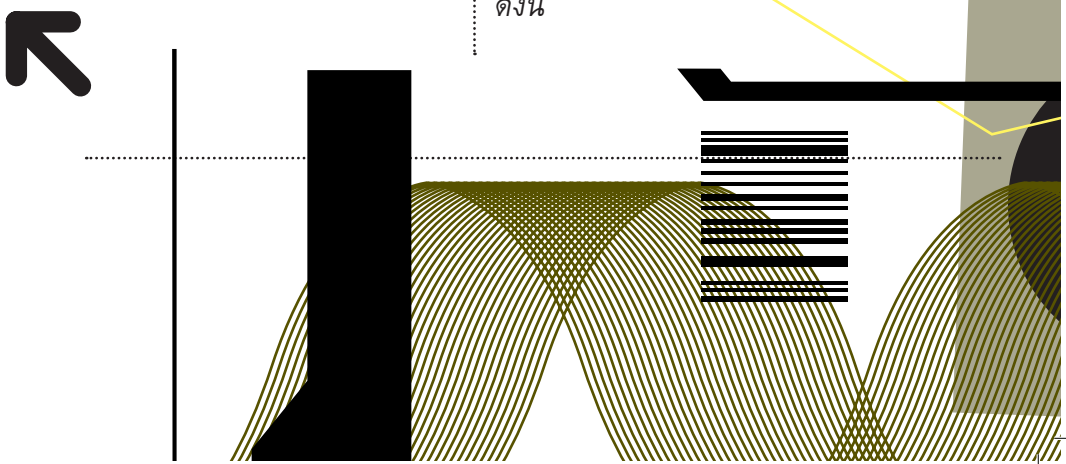
1. อำนาจที่ดำเนินการได้โดยไม่ต้องใช้อำนาจศาล
   - มีหนังสือสอบถาม เพื่อให้ส่งคำชี้แจงให้ข้อมูล
   - เรียกข้อมูลจราจรคอมพิวเตอร์
   - สั่งให้ส่งมอบข้อมูลตาม ม.26
2. อำนาจที่ต้องขออนุญาตศาล
   - ทำสำเนาข้อมูล
   - เข้าถึงระบบคอมพิวเตอร์/ข้อมูลคอมพิวเตอร์
   - ถอดรหัสลับ
   - ยึดอายัดระบบคอมพิวเตอร์

ข้อจำกัด/การตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่

มาตรา 19 การจำกัดการใช้อำนาจของพนักงานเจ้าหน้าที่ ซึ่งมีเงื่อนไขการใช้อำนาจทั่วไปตามมาตรา 18

- การขออนุญาตศาล
- การส่งคำร้องขอศาล
- ระยะเวลาในการยึด/อายัดระบบคอมพิวเตอร์ 30 วัน หรือ 60 วัน

หน้าที่ของพนักงานเจ้าหน้าที่ในการดำเนินการหาตัวผู้กระทำความผิดที่ต้องได้รับอนุญาตจากศาลก่อนดำเนินการ โดยมีหลักเกณฑ์และเงื่อนไขการขออนุญาตจากศาลดังนี้



1. ยื่นคำร้องต่อศาลที่มีเขตอำนาจ

2. ระบุรายละเอียดเกี่ยวกับการกระทำความผิด เหตุที่ต้องใช้อำนาจลักษณะการกระทำความผิด อุปกรณ์ที่ใช้และผู้กระทำความผิด

3. ส่งสำเนาบันทึกให้แก่เจ้าของหรือผู้ครอบครอง

4. พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าส่งสำเนาบันทึกรายละเอียดการดำเนินการแก่ศาลภายใน 48 ชั่วโมงนับแต่เวลาลงมือดำเนินการ

5. การยึดหรืออายัดระบบคอมพิวเตอร์สามารถกระทำได้ 30 วัน หรือ 90 วัน หากมีความจำเป็น

การ Block Website[19]

มาตรา 20 ในกรณีที่การกระทำความผิดเป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่

1.อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร

2. มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

พนักงานเจ้าหน้าที่อาจยื่นขอต่อศาลให้มีคำสั่งระงับการแพร่หลายของข้อมูลคอมพิวเตอร์นั้นได้

ลักษณะข้อมูลคอมพิวเตอร์ที่อาจจำเป็นต้องระงับการเผยแพร่

1. ข้อมูลความผิดต่อองค์พระมหากษัตริย์ พระราชินี รัชทายาท และผู้สำเร็จราชการ

2. ความผิดต่อความมั่นคงภายในราชอาณาจักร

3. ความผิดเกี่ยวกับความมั่นคงนอกราชอาณาจักร

4. ความผิดต่อความสัมพันธ์ไมตรีกับต่างประเทศ

5. ลักษณะข้อมูลที่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น ภาพลบหลู่ศาสนาภาพลามกอนาจาร

ฐานความผิด	โทษจำคุก	โทษปรับ

ชุดคำสั่งไม่พึงประสงค์

มาตรา 21

ในกรณีที่พบว่าข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งที่ไม่พึงประสงค์รวมอยู่ด้วย

พนักงานเจ้าหน้าที่อาจยื่นขอต่อศาลให้มีคำสั่งระงับการแพร่หลายของข้อมูลคอมพิวเตอร์นั้นได้

ห้ามมิให้พนักงานเผยแพร่ข้อมูลที่ได้มาตามมาตรา 18

มาตรา 22 ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์[20] ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา 18 ให้แก่บุคคลใด ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำ

1. เพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้
2. เพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ
3. เป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาลพนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่ง

โทษ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

พนักงานเจ้าหน้าที่ประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูล

มาตรา 23 พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ[21] ที่ได้มาตามมาตรา 18

โทษ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

19Block website คือ ปิดกั้นเว็บไซต์

20ข้อมูลคอมพิวเตอร์ คือ ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

21ผู้ใช้บริการ ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

ความรับผิดของผู้ล่วงรู้ข้อมูล

มาตรา 24 ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา 18 และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด

โทษ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

การรับฟังพยานหลักฐาน

มาตรา 25 ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญา หรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้

แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

หน้าที่ของผู้ให้บริการ

มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่ง ให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกิน 90 วันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

โทษ ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า 90 วันนับตั้งแต่การใช้บริการสิ้นสุดลง

หากฝ่าฝืนคำสั่งศาล หรือพนักงานเจ้าหน้าที่

มาตรา 27 ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา 18 หรือมาตรา 20 หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา 21

โทษ ต้องระวางโทษปรับ ไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

การแต่งตั้งพนักงานเจ้าหน้าที่

มาตรา 28 การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

การรับคำร้องทุกข์กล่าวโทษ จับ ควบคุม คัน และการกำหนดระเบียบ/แนวทางและวิธีปฏิบัติ

หลักเกณฑ์เกี่ยวกับคุณสมบัติพนักงานเจ้าหน้าที่ แบ่งเป็น

(1) พนักงานเจ้าหน้าที่ซึ่งรับผิดชอบงานด้านกฎหมายและการปราบปราม

คุณวุฒิ - ป.โท, เอกสาขานิติศาสตร์/เนติบัณฑิต/ หรือ ป.ตรีนิติศาสตร์ หรือรัฐศาสตร์และเคยเป็นพนักงานสอบสวน

(2) พนักงานเจ้าหน้าที่ซึ่งรับผิดชอบงานด้านเทคนิค

คุณวุฒิ - วิศวกรรมศาสตร์ วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ หรือ สาขาที่เกี่ยวข้อง

(3) ข้อยกเว้นจากคุณวุฒิสองข้อข้างต้น

คุณสมบัติ

1) ผ่านการทดสอบจากรัฐมนตรี ข้อเขียน หรือ สอบปฏิบัติ

2) ผ่านการอบรมหลักสูตร Cyber Security Management[22] / CISSP[23], CompTIA Security+, CISM

3) ผ่านการอบรม computer forensics พนักงานเจ้าหน้าที่ พนักงานเจ้าหน้าที่ตามพ.ร.บ./ DSI/ เจ้าพนักงานตำรวจ

มาตรา 29 ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญา มีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

22 Cyber-Security Management
การจัดการและวิธีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
23CISSP (Certified Information Systems Security Professional)
ระบบความปลอดภัยข้อมูลสารสนเทศ

บทที่ 3

ข้อควรปฏิบัติเพื่อป้องกันการกระทำความผิด

Safety net คู่มือการใช้งานเครือข่ายอินเทอร์เน็ตอย่างปลอดภัย สำหรับผู้ใช้งานทั่วไป

ไฟร์วอลล์ส่วนตัว (Personal Firewall)

ไฟร์วอลล์ส่วนตัวคือซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ส่วนตัวซึ่งทำหน้าที่ช่วยป้องกันผู้บุกรุกหรือผู้ไม่ประสงค์ดีเข้ามาในเครื่องคอมพิวเตอร์ส่วนตัวของเราหรือช่วยป้องกันโปรแกรมที่ไม่ประสงค์ดีทั้งหลาย เช่น ไวรัส โทรจัน สปายแวร์ ถูกติดตั้งลงไปในเครื่องคอมพิวเตอร์ส่วนตัวโดยที่เราเองอาจไม่ทราบหรือไม่รู้ตัว

ไฟร์วอลล์ทำงานโดยทำการตรวจสอบข้อมูลทั้งหมด (ไวรัส โทรจัน สปายแวร์ ก็ถือเป็นข้อมูลด้วย ที่เข้าหรือออกจากเครื่องคอมพิวเตอร์ส่วนตัวและจะอนุญาตให้ผ่านไปได้ก็ต่อเมื่อตรวจสอบแล้วและพบว่าไม่ละเมิดกับกฎเกณฑ์ของไฟร์วอลล์ที่กำหนดไว้ ในทางตรงกันข้าม หากมีการละเมิดไฟร์วอลล์ก็จะไม่อนุญาติให้ผ่านไป

ผู้ใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลอาจคิดว่าเครื่องของตนไม่มีทรัพย์สินหรือข้อมูลใดๆ ที่จะเป็นประโยชน์ต่อผู้บุกรุก ดังนั้นจึงไม่มีเหตุผลที่จะบุกรุกเข้ามาแต่มีเหตุผลอยู่อีกจำนวนหนึ่งดังนี้ ซึ่งมีความสำคัญสำคัญที่ผู้ใช้อาจต้องทบทวนความคิดนี้ใหม่อีกครั้ง

การทำลายทรัพย์สินสารสนเทศให้เสียหาย

เมื่อบุกรุกเข้ามาได้แล้ว ผู้บุกรุกอาจทำให้เครื่องคอมพิวเตอร์นั้นเกิดความ เสียหายได้ เช่น ทำให้เครื่องบูตไม่ได้

การขโมยข้อมูลในเครื่องคอมพิวเตอร์

เมื่อบุกรุกเข้ามาได้แล้ว ผู้บุกรุกอาจทำการขโมยข้อมูลที่สำคัญๆ ของผู้ใช้งาน ได้แก่ บัญชีผู้ใช้ (account) และรหัสผ่าน (Password) ข้อมูลส่วนตัวที่ไม่ต้องการเปิดเผย หรือข้อมูลสำคัญอื่นๆ

การจู่โจมเครื่องคอมพิวเตอร์อื่นบนอินเทอร์เน็ต

เมื่อบุกรุกเข้ามาได้แล้ว ผู้บุกรุกจะใช้เครื่องของผู้ใช้นั้นเพื่อทำการบุกรุกเครื่องคอมพิวเตอร์อื่นๆต่อไป หรือเพื่อทำการส่งสแปมเมล์ออกไปมีซอฟต์แวร์ทูล (Software Tool) บนอินเทอร์เน็ตมากมายที่ผู้บุกรุกสามารถดาวน์โหลดมาใช้งานได้ เช่น ทูลประเภทที่สามารถสแกนหาเครื่องคอมพิวเตอร์ที่ต่ออินเทอร์เน็ตอยู่ รวมทั้งช่องทางการสื่อสารคอมพิวเตอร์ที่เปิดอยู่หรือที่เรียกกันว่ามีพอร์ต (Port) เปิดอยู่ ซึ่งผู้บุกรุกสามารถใช้เป็นทางเข้าไปสู่เครื่องคอมพิวเตอร์ของผู้ใช้ได้ เมื่อเข้าไปได้แล้ว ผู้บุกรุกจะสามารถสร้างความเสียหายทั้งสามนั้นได้

คำแนะนำ

ให้ตัดการเชื่อมต่อจากอินเทอร์เน็ตทันทีที่ไม่มีการใช้งานเครื่องคอมพิวเตอร์ส่วนตัว

อย่าแอบเข้าใช้งานระบบคอมพิวเตอร์ของอื่น โดยของไม่อนุญาต

ให้ติดตั้งไฟร์วอลล์ส่วนตัวโดยสามารถดาวน์โหลดได้จากเว็บ

แหล่งข้อมูลเพิ่มเติม

www.zonelabs.com

www.symantec.com

www.sygate.com

การสวมรอยบุคคล (Identity Theft)

การขโมยเอกสารสำคัญที่ใช้ในการระบุตัวตน เช่น บัตรประจำตัวประชาชนและกระทำการฉ้อฉลต่อเอกสารดังกล่าว หรือแม้กระทั่งปลอมแปลงเอกสารสำคัญนั้นถือเป็นคดีที่มีความผิดทางกฎหมาย โดยที่ผู้กระทำฉ้อฉลนั้นมักจะมีแรงจูงใจทางด้านการเงินเป็นเหตุผลสำคัญ

ในปัจจุบันการขโมยและการกระทำการฉ้อฉลนั้นสามารถกระทำได้กับเอกสารอิเล็กทรอนิกส์ที่อยู่ในเครื่องคอมพิวเตอร์ (นอกเหนือจากการขโมยและการกระทำการฉ้อฉลกับเอกสารกระดาษที่เกิดขึ้นอยู่แล้ว) ซึ่งเป็นเรื่องที่จะมีความสำคัญเพิ่มมากขึ้นเรื่อยๆ ทั้งนี้เนื่องจากในปัจจุบันเอกสารสำคัญที่ใช้ระบุตัวตนมากมายได้ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์และอาจเข้าถึงได้อาทิ โดยผู้บุกรุกโดยผ่านเครือข่ายอินเทอร์เน็ต

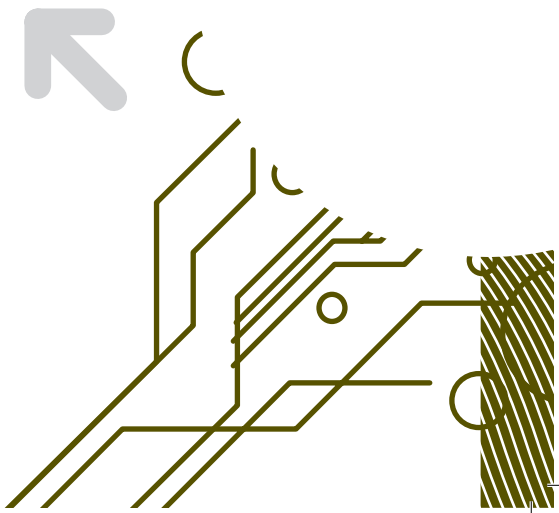
การขโมยเอกสารสำคัญนั้น เมื่อเกิดขึ้นแล้ว อาจนำไปสู่การสวมรอยเป็นตัวบุคคลผู้เป็นเจ้าของเอกสารนั้น และอาจใช้ในการดำเนินการเรื่องต่างๆ แทนตัวผู้เป็นเจ้าของโดยมิได้รับมอบหมายซึ่งเป็นการกระทำที่ผิดกฎหมาย เช่น การขโมยบัญชีผู้ใช้และรหัสผ่าน (Password) เพื่อทำการล็อกอินเข้าไปซื้อสินค้าในเว็บแห่งหนึ่งผลที่จะเกิดขึ้นต่อผู้ที่ถูกสวมรอย ได้แก่ เสียประวัติทางด้านการเงิน ก่อให้เกิดหนี้สินมากมาย ต้องคดีที่มิได้เป็นผู้ก่อ เสียชื่อเสียง และอื่นๆ

แหล่งข้อมูลเพิ่มเติม

www.idtheftcenter.org

www.privacyrights.org/identity.htm

www.consumer.gov/idtheft/



คำแนะนำ

- ให้ระมัดระวังไม่เปิดเผยข้อมูลส่วนตัวเกินความจำเป็น ซึ่งรวมถึงเลขที่บัตรต่างๆ เช่น บัตรประจำตัวประชาชน บัตรเครดิต ใบขับขี่ บัตรประจำตัวผู้เสียภาษีอากร เป็นต้น หมายเลขดังกล่าวในหลายๆ กรณี จะถูกใช้เป็นข้อมูลสำคัญในการล็อกอินเข้าสู่เว็บไซต์ หรือจะถูกสอบถามทางโทรศัพท์ก่อนที่เจ้าหน้าที่ของธนาคารจะเปิดเผยข้อมูลทางการเงินของผู้สอบถามให้ทราบ
- ให้ระมัดระวังข้อมูลบัญชีธนาคาร หรือข้อมูล Statement รายเดือนที่ธนาคารส่งมา มิให้เปิดเผยล่วงรู้โดยไม่มีความจำเป็น
- ให้ระมัดระวังการให้ข้อมูลเกี่ยวกับบัตรเครดิต จะให้ก็ต่อเมื่อมีความจำเป็นจริงๆ เท่านั้น
- ในกรณีที่ต้องให้ตัวบัตรเครดิตแก่ผู้ขาย เช่น ที่สถานีเติมน้ำมันเชื้อเพลิง ให้คอยจับตาดูพฤติกรรมการนำบัตรนั้นไปรูดเพื่อชำระเงิน
- ในการซื้อสินค้าทางเว็บ นอกจากระมัดระวังการให้ข้อมูลบัตรเครดิตแล้ว ต้องตรวจสอบก่อนที่จะสั่งซื้อว่าการประมวลผลการสั่งซื้อของเว็บนั้นมีความปลอดภัยพอเพียงหรือไม่ (การประมวลผลที่ไม่ปลอดภัยอาจนำไปสู่การแอบดักดู ข้อมูลส่วนตัวของผู้ซื้อได้)
- ให้ยกเลิกบัญชีธนาคารที่ไม่ได้มีการใช้งานมาเป็นระยะเวลานาน เช่น นาน กว่า 6 เดือน
- ให้ระมัดระวังไม่ให้ผู้อื่นซึ่งอาจยืนอยู่ในบริเวณข้างเคียง เห็นรหัสผ่านของบัตร ATM ส่วนตัว
- ให้ใช้รหัสผ่านที่ยากต่อการเดาและเปลี่ยนรหัสผ่านบ่อยๆ
- หมั่นตรวจตรา Statement ทางการเงินที่ได้รับจากธนาคารเพื่อดูว่ามีความผิดปกติเกิดขึ้นในบัญชีธนาคารของเราหรือไม่

ข้อความฉับพลัน ห้องสนทนา และการแชร์ไฟล์บนอินเทอร์เน็ต (Instant Messaging, Chat Rooms, File Sharing)

การสนทนากันบนอินเทอร์เน็ตทำได้หลายวิธี วิธีการหนึ่งคือการสนทนาบนเว็บ ซึ่งจะมีการจัดเป็นห้องสนทนาบนเว็บไว้ให้ โดยวิธีนี้ผู้ใช้มีเพียงเว็บบราวเซอร์ก็สามารถเข้าไปสนทนาในห้องสนทนาที่จัดไว้ให้ได้ วิธีที่สองคือการใช้โปรแกรม Instant Relay Chat (IRC) ซึ่งทำให้ผู้ใช้จำเป็นต้องติดตั้งโปรแกรม IRC ก่อนที่จะใช้งานได้ โปรแกรมดังกล่าวอาจดาวน์โหลดได้จากทางเว็บหรือไม่ก็ต้องทำการจัดซื้อ มาแล้วทำการติดตั้ง

การส่งข้อความฉับพลันหรือที่เรียกกันว่า Instant Messaging เป็นวิธีการสนทนาอีกรูปแบบหนึ่งซึ่งผู้ใช้ต้องทำการติดตั้งโปรแกรมก่อนใช้งานเช่นกันโปรแกรมนี้จะทำให้ผู้ใช้สามารถสนทนากับเพื่อนที่ล็อกอินเข้ามาใช้งานได้อย่างทันทีทันใด รวมทั้งจะอนุญาตให้ผู้ใช้เก็บรายชื่อของเพื่อนที่มีความสนใจร่วมกันหรือเรามักสนทนาด้วยกันบ่อยๆ เอาไว้ในโปรแกรมและยังสามารถตรวจสอบดูได้ว่ามีเพื่อนคนใดบ้าง ณ ขณะนี้ที่ได้ทำการล็อกอินเข้ามาแล้วทั้งการสนทนาในห้องสนทนาและการใช้ข้อความฉับพลันได้มีการใช้งานกันอย่างแพร่หลายในธุรกิจหลากหลายประเภทไม่ว่าจะเป็นภาครัฐหรือภาคเอกชน ถึงแม้ว่าการสนทนาในทั้งสองรูปแบบจะมีประโยชน์มากในการแลกเปลี่ยนความคิดเห็นหรือข้อมูลต่างๆ กันทว่าหากมิได้เตรียมการป้องกันไว้ให้ดีแล้ว ผลในทางลบก็อาจเกิดขึ้นได้ เช่น การติดไวรัสหรือโทรจันในเครื่องของผู้ที่รับไฟล์ที่ส่งมาให้ การเปิดเผยข้อมูลส่วนตัว เป็นต้น การแชร์ไฟล์ระหว่างเพื่อนบนอินเทอร์เน็ตเป็นรูปแบบหนึ่งของการแลกเปลี่ยนข้อมูลบนอินเทอร์เน็ต (การสนทนาทั้งสองประเภทที่ได้กล่าวถึงไปแล้วนั้นก็อาจนำไปสู่การแลกเปลี่ยนข้อมูลระหว่างผู้ใช้ด้วย) ซึ่งหากไม่ได้เตรียมการป้องกันไวรัสไว้ให้ดีแล้ว อาจเปิดโอกาสให้ผู้บุกรุกเข้ามานำไฟล์ในเครื่องของผู้ใช้งานไปได้ หรือแม้แต่เครื่องคอมพิวเตอร์ที่ใช้งานได้รับความเสียหายได้ โปรแกรมสำหรับการแชร์ไฟล์นี้ ได้แก่ Kazaa, Morpheus, LimeWire เป็นต้น ซึ่งจะทำให้สามารถเข้าไปเอาไฟล์ในเครื่องของเพื่อนได้โดยตรง

คำแนะนำ

- ให้หลีกเลี่ยงไม่ใช้งานทั้งการส่งข้อความฉับพลัน การสนทนาในห้องสนทนา และการแชร์ไฟล์บนอินเทอร์เน็ต ทั้งนี้เนื่องจากวิธีการทั้งสามนี้อาจก่อให้เกิดการละเมิดความเป็นส่วนตัว การติดตั้งโปรแกรมที่ไม่ประสงค์ดี และการแพร่ กระจายของไวรัสได้ ถ้าจำเป็นต้องใช้ ให้ทำการศึกษาให้ดีก่อนเริ่มต้นใช้งาน
- ให้ติดตั้งไฟร์วอลล์ส่วนบุคคล
- ให้ติดตั้งโปรแกรมป้องกันไวรัสและหมั่นทำการปรับปรุงไฟล์รูปแบบไวรัสอย่างสม่ำเสมอ
- สำหรับการแชร์ไฟ ล์ ให้ตรวจสอบการปรับแต่งค่าที่ใช้งานในโปรแกรมแชร์ไฟล์และให้แชร์เฉพาะไฟล์ที่ตนต้องการให้ผู้อื่นได้รับทราบข้อมูลจริง ๆ
- ให้ระมัดระวังการไม่ละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของไฟล์
- ให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการสอบสวน สอบสวนตัวผู้กระทำความผิด หากพบเว็บไซต์ที่มีการเผยแพร่ภาพลามก อนาจารสามารถแจ้งให้พนักงานเจ้าหน้าที่ดำเนินการหาตัวผู้กระทำความผิดได้

แหล่งข้อมูลเพิ่มเติม

www.tio.com.au/FAQ/int_dumping.htm

อีเมล์หลอกลวง
(Instant Scams)

ในปัจจุบันได้มีอีเมล์ประเภทหลอกลวงให้ผู้ที่ได้รับอีเมล์หลงเชื่อซึ่งหลายๆ ครั้งจะทำให้ผู้รับอีเมล์ได้รับความเสียหาย เช่น เสียเงิน เสียเวลา และจะเป็นการยากที่จะเรียกร้องหรือขอกลับคืนเมื่อได้เสียไปแล้ว ในปัจจุบันองค์กร Federal Trade Commision (FTC) ของสหรัฐอเมริกาได้ระบุอีเมล์ประเภทหลอกลวงนี้ไว้ 12 ประเภท ซึ่งผู้ใช้ต้องให้ความระมัดระวัง

1. การสร้างโอกาสทางธุรกิจ อีเมล์ประเภทนี้จะเสนอรายได้ก้อนใหญ่โดย ที่ไม่ต้องทำอะไรมากหรือไม่มีค่าใช้จ่ายในการลงทุน

2. อีเมล์ขายสินค้าที่มีกลุ่มผู้ใช้งานเป็นจำนวนมาก (Bulk E-mail) อีเมล์ประเภทนี้จะเสนอรายชื่อกลุ่มผู้ใช้งานอีเมล์ซึ่งมีเป็นจำนวนมากและ ชักชวนว่าสามารถโฆษณาหรือขายสินค้าลงไปยังกลุ่มผู้ใช้งานอีเมล์นี้ได้ ผู้ให้บริการอินเทอร์เน็ตส่วนใหญ่จะไม่อนุญาตอีเมล์ขายสินค้าใน ลักษณะเช่นนี้

3. อีเมล์ลูกโซ่ อีเมล์ประเภทนี้จะชักชวนให้ผู้รับส่งเงินจำนวนเล็กน้อยไปยังผู้ส่งและส่งต่ออีเมล์นี้ไปให้เพื่อนหรือผู้อื่นต่อไป

4. การทำงานที่บ้านโดยลงแรงเพียงเล็กน้อย (Work-at-home Schemes) อีเมล์ประเภทนี้จะเสนอการมีรายได้อย่างสม่ำเสมอโดยลงแรงเพียง เล็กน้อย ผู้รับอีเมล์จะต้องจ่ายค่าธรรมเนียมแรกเข้าและทำงานตามที่ในอีเมล์ขอให้ทำ (โดยหวังจะได้รับค่าตอบแทนก้อนใหญ่) แต่ผู้รับก็จะไม่มีทางได้รับค่าตอบแทนใดๆ ทั้งสิ้นกลับคืน

5. การรักษาสุขภาพและการควบคุมน้ำหนัก อีเมล์ประเภทนี้จะเสนอยาประเภทต่างๆ อาทิ สูตรสมุนไพร การรักษาการหมดสมรรถภาพ การ รักษาอาการผมร่วง เป็นต้น การหลงเชื่อคำโฆษณาและซื้อผลิตภัณฑ์ มาใช้งานส่วนใหญ่แล้วจะเป็นการเสียเงินไปโดยเปล่าประโยชน์

6. รายได้ก้อนใหญ่โดยไม่ต้องเสียแรงมากนัก อีเมล์ประเภทนี้จะเสนอวิธี ที่จะร่ำรวยได้อย่างรวดเร็ว

7. สินค้าฟรีอีเมล์ประเภทนี้จะเสนอให้สินค้าฟรีโดยชำระเงินเพียง เล็กน้อย เช่น เพื่อเข้าเป็นสมาชิก เป็นต้น

8. โอกาสในการลงทุนที่มีผลตอบแทนสูง อีเมล์ประเภทนี้จะเสนอผล ตอบแทนที่สูงกับการลงทุนที่ไม่มีความเสี่ยง เงินที่ลงทุนไปก็จะสูญไปโดยเปล่าประโยชน์

9. ชุดอุปกรณ์เชื่อมต่อเคเบิลทีวี (Cable De-scambler Kits) อีเมล์ ประเภทนี้จะเสนอขายชุดอุปกรณ์สำหรับเชื่อมต่อเข้ากับเคเบิลทีวีได้โดยไม่ต้องเสียค่าสมาชิกอีก เช่น เป็นรายเดือน ชุดอุปกรณ์ดังกล่าวแม้ว่าจะทำได้จริงก็เป็นสิ่งผิดกฎหมาย

10. การให้เงินกู้หรือสินเชื่อโดยมีเงื่อนไขง่ายๆ อีเมล์ประเภทนี้จะเสนอ เงินกู้หรือสินเชื่อโดยมีเงื่อนไขง่ายๆ สถาบันทางการเงินที่ถูกต้องตามกฎหมายจะไม่ใช้วิธีนี้ในการให้เงินกู้หรือสินเชื่อ

11. การเคลียร์สินเชื่อ อีเมล์ประเภทนี้จะเสนอช่วยเคลียร์หรือล้างข้อมูลสินเชื่อที่ติดลบในบัญชีธนาคาร การทำตามที่เสนอถือเป็นการกระทำที่มีความผิดทางกฎหมาย

12. การเสนอให้รางวัลไปเที่ยวฟรี อีเมล์ประเภทนี้จะเสนอว่าท่านเป็นผู้ที่ได้รับรางวัลชนะเลิศให้ไปท่องเที่ยวฟรีในภายหลัง ท่านจะพบว่า ข้อเสนอนั้นไม่ได้เป็นอย่างที่คิด หรือไม่ก็ต้องชำระเงินเพิ่มเติม ซึ่งมิได้มีการอธิบายหรือแจ้งให้ทราบเอาไว้ก่อน

คำแนะนำ

- ให้ระมัดระวังโฆษณาชวนเชื่อในลักษณะดังกล่าว ซึ่งมักจะไม่มีทางเป็นจริงได้
- ให้หมั่นคอยติดตามดูประเภทของอีเมล์หลอกลวงได้จากเว็บไซต์ในแหล่งข้อมูลเพิ่มเติม

แหล่งข้อมูลเพิ่มเติม

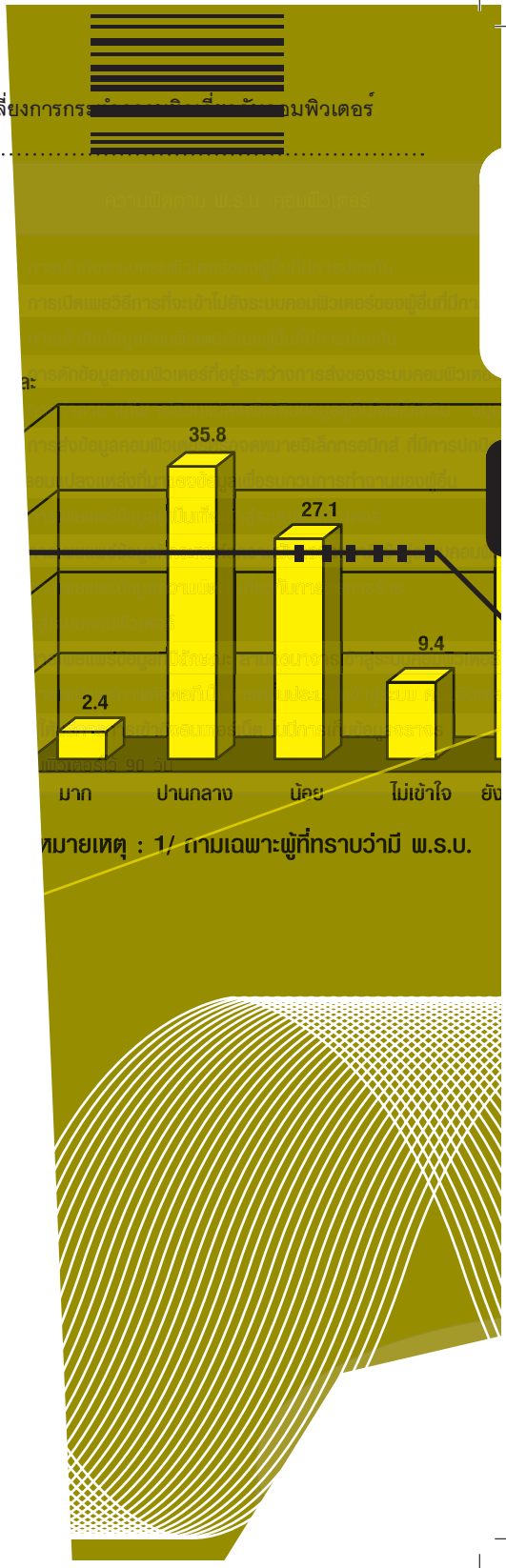
www.ftc.gov

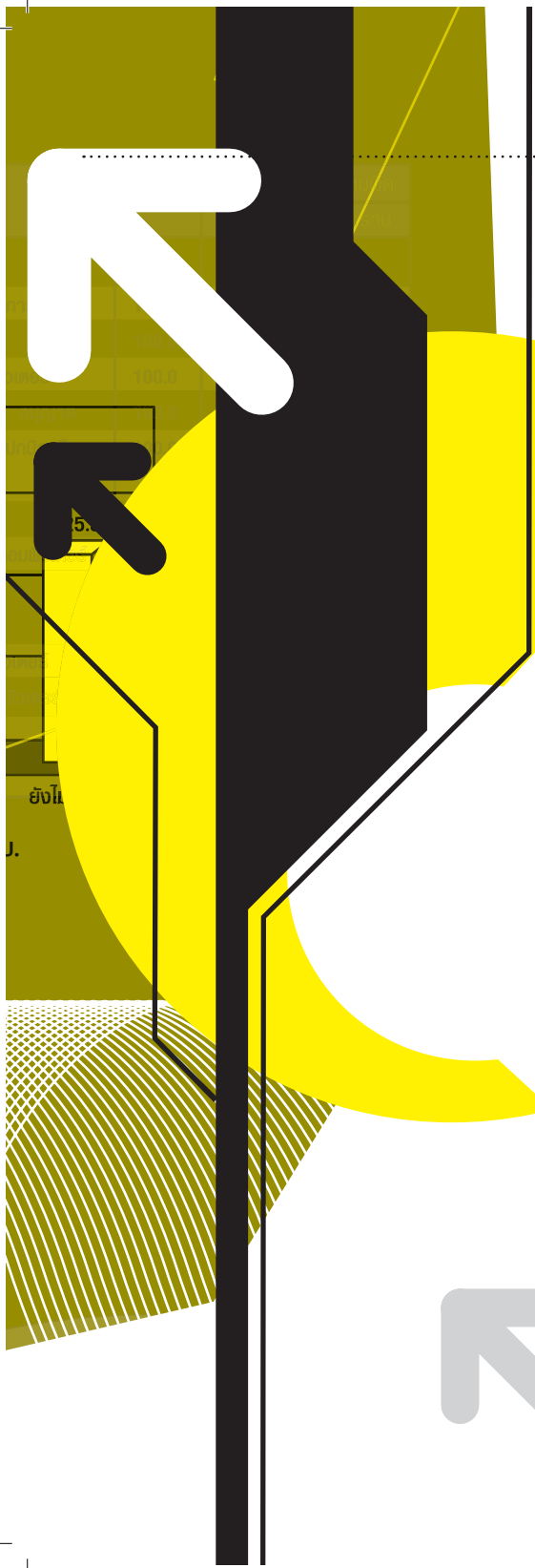
www.crimes-of-persuasion.com

ประเด็นทางกฎหมาย
(Legal Issues)

การใช้งานอินเทอร์เน็ตในแต่ละประเทศมีกฎหมายที่รองรับการใช้งานที่แตกต่างกัน บางเรื่องเป็นสิ่งที่ผิดกฎหมายในทุกประเทศทั่วโลก อาทิ ปัญหาสื่อลามกซึ่งเป็นภาพของเยาวชน การบุกรุกเครื่องคอมพิวเตอร์ เป็นต้น ในขณะที่บางเรื่อง เช่น การพนัน อาจจะเป็นสิ่งที่ผิดกฎหมายหรือไม่ผิดกฎหมายได้ในบางประเทศ ผู้ใช้จึงต้องระมัดระวังและศึกษากฎหมายที่รองรับการใช้งานอินเทอร์-เน็ตในประเทศของตน กิจกรรมบนอินเทอร์-เน็ตที่โดยทั่วไปถือเป็นความผิดทางกฎหมายได้แก่

- การเล่นการพนัน
- การซื้ออาวุธปืน
- การซื้อขายยาเสพติด
- การนำเสนอสื่อลามกทุกประเภท
- การบุกรุกคอมพิวเตอร์หรือเครือข่าย
- การพัฒนา และแพร่ไวรัสคอมพิวเตอร์
- การทำให้เครือข่ายหรือเครื่องคอมพิวเตอร์ของผู้อื่นไม่สามารถใช้งานหรือ ให้บริการได้
- การสวมรอยบุคคลเพื่อทำการฉ้อฉล





คำแนะนำ

- ไม่เข้าไปยุ่งเกี่ยวกับกิจกรรมที่ถือเป็นความผิดทางกฎหมายดังกล่าว
- ให้ปฏิบัติตามกฎหมายของประเทศทั้งในเรื่องทั่ว ๆ ไปและที่เกี่ยวข้องกับการใช้งานอินเทอร์เน็ต รวมทั้งกฎหมายในระดับนานาชาติด้วย
- ให้หมั่นคอยติดตามดูเว็บไซต์ในแหล่งข้อมูลเพิ่มเติม

แหล่งข้อมูลเพิ่มเติม

www.eclip.org

www.ilpf.org

www.uncitral.org

www.bmck.com/ecommerce

www.gipiproject.org

www.cybercrime.gov

การเฝ้าดูการใช้งานอินเทอร์เน็ต
(Monitoring Internet Usage)

อินเทอร์เน็ตนอกจากจะเป็นสิ่งที่มีประโยชน์ต่อสำนักงานหรือองค์กรแล้วยังเป็นแหล่งบันเทิงใจสำหรับพนักงานในองค์กรด้วย แต่การที่พนักงานใช้เวลาไปกับการบันเทิงมากจนเกินไปจนกลายเป็นผลเสียต่อการทำงาน หรือการที่พนักงานอาจเข้าไปยุ่งเกี่ยวกับกิจกรรมที่ส่อไปในทางผิดกฎหมาย จะเกิดเป็นผลในทางลบต่อองค์กรได้ จึงมีความจำเป็นอย่างยิ่งที่จะต้องคอยเฝ้าดูและสอดส่องกิจกรรมการใช้งานอินเทอร์เน็ตของพนักงาน

สำหรับการใช้งานอินเทอร์เน็ตจากที่บ้าน แม้อินเทอร์เน็ตจะมีประโยชน์ต่อการเรียนรู้เป็นสิ่งบันเทิงเชิงสร้างสรรค์ และส่งเสริมการเจริญเติบโตทางด้านวัยวุฒิของบุตรหลานในครอบครัว แต่พ่อแม่ก็ควรหมั่นสอดส่องและดูแลการเข้าไปในเว็บไซต์ที่ไม่เหมาะสมของบุตรหลาน ทั้งนี้เนื่องจากมีเว็บไซต์เป็นจำนวนมากที่ส่อไปในทางที่ไม่เหมาะสมต่อบุตรหลานของเรานั่นเอง

คำแนะนำสำหรับการใช้งานอินเทอร์เน็ตภายในองค์กร

- ให้ความรู้แก่พนักงานเกี่ยวกับการใช้งานอินเทอร์เน็ตอย่างสม่ำเสมอ
- ให้จัดทำนโยบายการใช้งานอินเทอร์เน็ตขององค์กรอย่างเป็นลายลักษณ์อักษร โดยอย่างน้อยต้องมีเนื้อหาดังนี้ปรากฏอยู่ในนโยบายด้วย
    - o การใช้งานอินเทอร์เน็ตมีจุดประสงค์เพื่อผลประโยชน์ขององค์กร ไม่ใช่ใช้เพื่อผลประโยชน์ส่วนตัว
    - o การใช้งานอินเทอร์เน็ตจะได้รับการเฝ้าดูแลอย่างใกล้ชิด เช่น โดยผู้ดูแลระบบ
    - o มีแนวทางการใช้งานอีเมล์อย่างเหมาะสม
- ให้หมั่นคอยติดตามดูเว็บไซต์ในแหล่งข้อมูลเพิ่มเติม

คำแนะนำสำหรับการใช้งานอินเทอร์เน็ตจากที่บ้าน

- พ่อแม่จะต้องให้ความรู้แก่บุตรหลานเกี่ยวกับการใช้งานอินเทอร์เน็ตอย่างเหมาะสม
- ให้ใช้ซอฟต์แวร์เพื่อคอยตรวจสอบการเข้าเว็บไซต์ของบุตรหลาน รวมทั้งกรองการเข้าเว็บไซต์บางเว็บไม่ให้สามารถทำได้
- ให้หมั่นคอยติดตามดูเว็บไซต์ในแหล่งข้อมูลเพิ่มเติม
- ป้องกันเว็บที่ไม่เหมาะสมสำหรับเยาวชน ด้วยการติดตั้งโปรแกรม ICT House Keeper

แหล่งข้อมูลเพิ่มเติม

สำหรับการใช้งานอินเทอร์เน็ตภายในองค์กร ให้ดูข้อมูลเพิ่มเติมที่

www.email-policy.com

www.epolicyinstitute.com

www.fatline.com

สำหรับการใช้งานอินเทอร์เน็ตจากที่บ้าน ให้ดูข้อมูลเพิ่มเติมที่

www.icthousekeeper.com

www.getnetwise.org

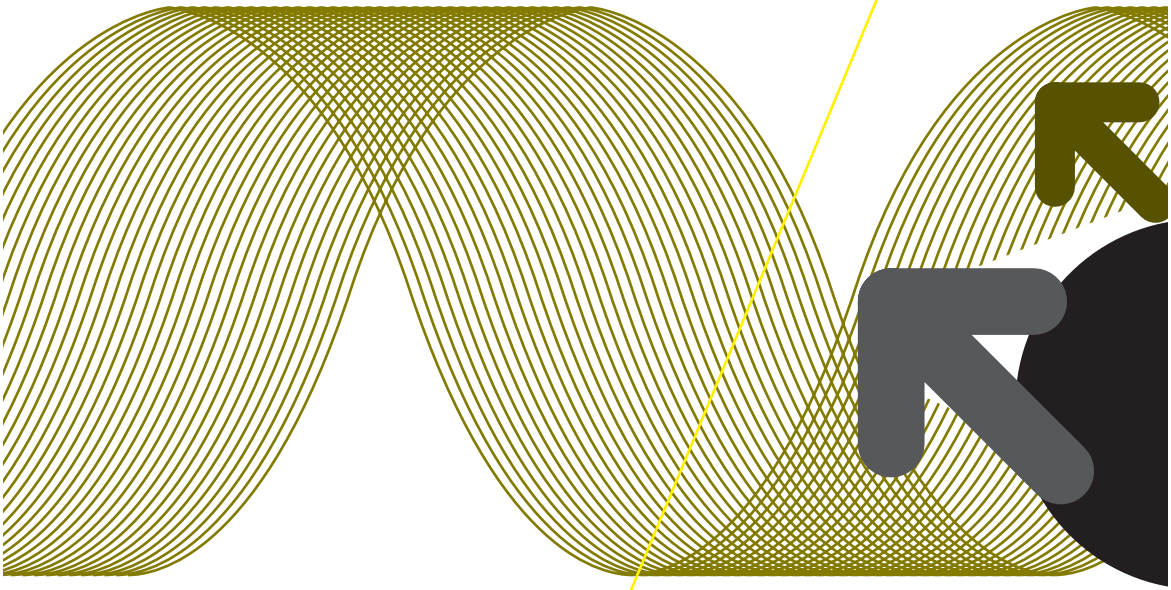
www.wiredpatrol.org

www.childnet-int.org

การหมิ่นประมาทหรือการทำให้ผู้อื่นเสียชื่อเสียง

(Online Defamation)

ข้อความทุกรูปแบบที่ใช้งานบนอินเทอร์เน็ต ไม่ว่าจะเป็นในอีเมล์ เว็บบอร์ดห้องสนทนา บนเว็บไซต์ ต้องระมัดระวังไม่ให้เป็นข้อความเท็จหรือก่อให้เกิดความ เสียหายต่อตัวบุคคลหรือองค์กรที่ถูกพาดพิง กล่าวถึง หรืออ้างอิง



คำแนะนำ

- ให้กล่าวเฉพาะสิ่งที่มีหลักฐานความจริงสนับสนุนเท่านั้น ห้ามใช้อารมณ์หรือความรู้สึกมากล่าวลงไป
- อีเมล์เมื่อส่งไปยังผู้รับแล้วจะไม่มีทางเรียกกลับคืนมาได้ ฉะนั้นให้ระมัดระวังทุกถ้อยคำในอีเมล์ที่ส่งถึงผู้รับ
- ให้ระมัดระวังการกล่าวคำในเว็บบอร์ด ห้องสนทนา ข้อความฉับพลันที่จะไม่ละเมิดผู้อื่น
- ให้ความรู้แก่พนักงานหรือบุตรหลานเกี่ยวกับการระมัดระวังการใช้ถ้อยคำของตนบนอินเทอร์เน็ต
- ไม่นำเข้าข้อมูลหรือภาพลามกอนาจาร เข้าไปในระบบคอมพิวเตอร์
- การตัดต่อและเผยแพร่ภาพตัดต่อของผู้อื่น ที่ทำให้เขาเสื่อมเสียชื่อเสียง
- ก่อนที่จะกล่าวถึงผู้อื่นในเชิงลบให้พิจารณาถึงสาเหตุที่ต้องทำ รวมทั้งประเมินผลที่จะเกิดขึ้นด้วย
- ให้หมั่นคอยติดตามดูเว็บไซต์ในแหล่งข้อมูลเพิ่มเติม

แหล่งข้อมูลเพิ่มเติม

www.onlinepolicy.org/defamation.shtml

www.wiredpatrol.org/law/freespeech/defamation.html

www.spawn.org/marketing/slander.html

www.cyberlaw.com

สแปม
(Spam)

ในปัจจุบันเราทุกคนส่วนใหญ่ล้วนได้รับจดหมายขยะ ตู้จดหมายของเราจะ เต็มไปด้วยจดหมายโฆษณาที่เราไม่ได้ขอให้ส่งมาให้ และเราก็ทิ้งจดหมายเหล่านั้น ไปโดยไม่ได้แม้แต่จะเปิดอ่าน สิ่งที่เทียบเท่ากันนี้กำลังเกิดขึ้นกับระบบอีเมล์ที่เรา ใช้งานกันอยู่ กล่าวคือข้อความอีเมล์ที่เราไม่ได้ขอให้ส่งมาให้จะมาอยู่ในตู้จดหมายอิเล็กทรอนิกส์ของเราเกือบทุกวันและกลายเป็นสิ่งที่ค่อน-ข้างจะน่ารำคาญ เราเรียกข้อความอีเมล์ที่เป็นขยะดังกล่าวว่าสแปมเมล์ หรือเรียกสั้นๆ ว่าสแปม

สแปมเป็นปัญหาที่หนักกว่าจดหมายขยะในตู้จดหมาย เนื่องจากสแปม ก่อให้เกิดค่าใช้จ่ายต่อผู้รับตามสาเหตุที่จะได้กล่าวถึงด้านล่าง ในขณะที่จดหมายขยะ จะก่อให้เกิดค่าใช้จ่ายต่อผู้ส่งซึ่งต้องใช้เงินในการตีพิมพ์โฆษณาเพื่อส่งมายังผู้รับ นอกจากนั้นแล้วผู้ส่งสแปมจะเสียค่าใช้จ่ายเท่าเดิมไม่ว่าสแปมเมล์นั้นจะถูกส่งไปยังผู้รับเพียงคนเดียวหรือล้านคนก็ตาม ส่วนจดหมายขยะผู้ส่งจะต้องเสียค่าใช้จ่ายเท่ากับจำนวนผู้รับ สแปมทำให้บุคคลและองค์กรสิ้นเปลืองทั้งเวลาและเงินตามที่จะได้กล่าวถึง

- ผู้รับสแปมส่วนใหญ่จะต้องเสียค่าใช้จ่ายในการเชื่อมต่อกับอินเทอร์เน็ตเป็นรายชั่วโมง หากต้องรับสแปมเป็นจำนวนมาก ก็เป็นที่แน่นอนว่าผู้รับจะต้องเสียค่าใช้จ่ายในการนี้สูงมากขึ้น
- ผู้รับอาจต้องใช้เวลาในการจัดการกับสแปมเป็นจำนวนมากในแต่ละวัน (ทั้งนี้เนื่องจากผู้ส่งสามารถส่งได้ง่ายโดยมีค่าใช่จ่ายเท่าเดิม)
- สแปมกีดขวางการทำงานของเมล์เซิร์ฟเวอร์ทั่วโลกซึ่งทำให้ทุกคน ประสบกับการเชื่อมต่อที่ช้าลงและเสียค่าใช้จ่ายในการเชื่อมต่อที่สูงขึ้น ถึงแม้ว่าจะไม่สามารถกำจัดสแปมได้อย่างเด็ดขาดแต่เราอาจลดระดับความรุนแรงลงได้โดยให้ปฏิบัติตามคำแนะนำด้านล่าง

คำแนะนำ

- ไม่ส่งอีเมล์เพื่อตอบกลับสแปมที่ส่งมา การตอบสแปมนั้นเท่ากับเป็นการยืนยันอีเมล์แอดเดรสของผู้รับว่าเป็นแอดเดรสที่มีอยู่จริงและจะทำให้ผู้รับนั้นตกเป็นเป้าหมายที่ชัดเจนมากยิ่งขึ้น
- ให้ใช้อีเมล์แอดเดรสที่ใช้ในงานประจำวันเพื่อติดต่อกับผู้ที่ติดต่ออยู่ด้วย

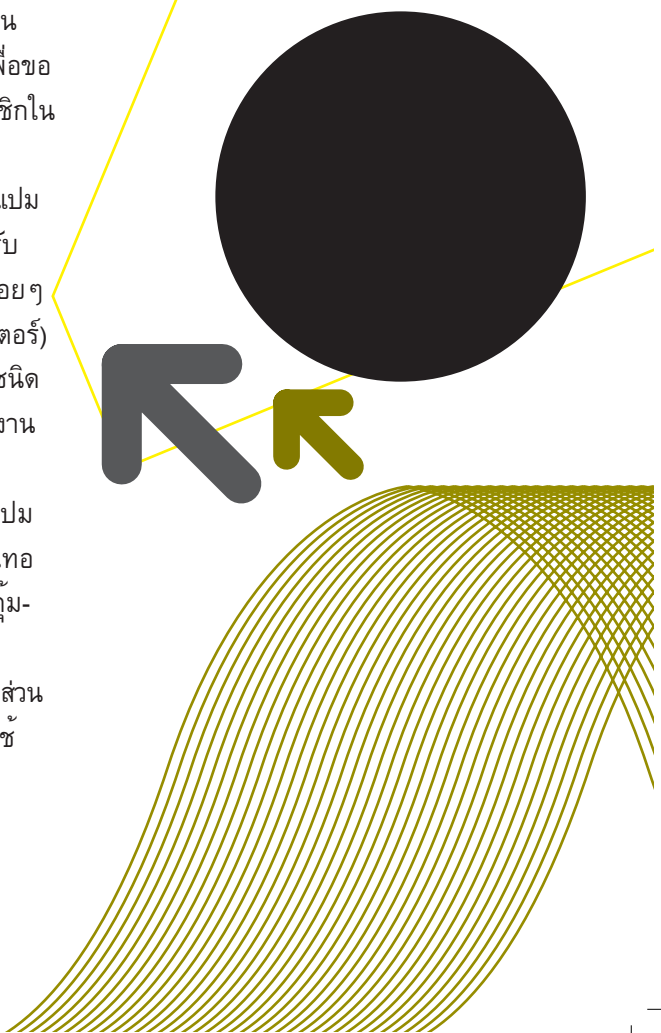
เป็น ประจำ เช่น ผู้ร่วมงาน เพื่อน และครอบครัว สำหรับการส่งอีเมล์เพื่อ จุดประสงค์อื่นๆ ให้ใช้อีเมล์แอดเดรสต่างหากอีกอันหนึ่ง

- ไม่ใช้อีเมล์แอดเดรสที่ใช้ในงานประจำวันเพื่อสมัครสมาชิกอีเมล์เพื่อขอรับ ข้อมูลข่าวสารหรือเข้าเป็นสมาชิกในเมล์ลิ่งลิสต์ต่างๆ
- ไม่ซื้อสินค้าใดๆ ที่โฆษณาในสแปมเนื่องจากจะยิ่งทำให้ผู้ส่งสแปมได้รับผลตอบแทนและจะใช้วิธีนี้ต่อไปเรื่อยๆ
- ใช้ตัวกรองสแปม (สแปมฟิลเตอร์) ซึ่งมีให้เลือกหลากหลายและเลือกชนิดที่เหมาะสมกับโปรแกรมอีเมล์ที่ใช้งานอยู่ให้มากที่สุด
- ให้รายงานร้องเรียนปัญหาสแปมกลับไปยังผู้ให้บริการเครือข่ายอินเทอร์เน็ต เว็บไซต์ต่สแปมหรือองค์กรคุ้มครองผู้บริโภค
- ตรวจสอบนโยบายการใช้ข้อมูลส่วนตัวของลูกค้าของเว็บไซต์ที่เข้าไปใช้บริการ เพื่อดูว่าเว็บนั้นจะนำอีเมล์แอดเดรสของลูกค้าไปทำอะไรบ้าง

แหล่งข้อมูลเพิ่มเติม

spam.abuse.net

www.cauce.org



การปลอมแปลงอีเมล์ (Spoofing)

การปลอมแปลงบนระบบคอมพิวเตอร์ที่สำคัญมีด้วยกันสองประเภทประเภทแรกคือการปลอมแปลงหมายเลข IP Address (IP Address Spoofing) ผู้ให้บริการอินเทอร์เน็ต (ISP) ในปัจจุบันจะสามารถป้องกันลูกค้าของตนจากการปลอมแปลงประเภทนี้ได้แล้ว ดังนั้นผู้ใช้ที่บ้านและธุรกิจจึงไม่จำเป็นจะต้องกังวลกับปัญหา นี้ อย่างไรก็ตาม องค์กรหรือธุรกิจที่ต้องดูแลระบบเครือข่ายเองอาจมีความจำเป็นต้องปรึกษากับผู้ขายอุปกรณ์เครือข่ายที่องค์กรจัดซื้อมาใช้งานเพื่อปกป้องตนเองจากปัญหานี้การปลอมแปลงอีกประเภทหนึ่งคือการปลอมแปลงอีเมล์ (Email Spoofing) ผลที่เกิดขึ้นคือผู้ใช้จะได้รับอีเมล์ที่ระบุว่ามาจากผู้ส่งคนหนึ่งแต่แท้จริงแล้วเป็นอีเมล์ที่มาจากผู้ส่งอีกคนหนึ่ง การปลอมแปลงอีเมล์นี้โดยทั่วไปแล้วจะมีวัตถุประสงค์ที่จะหลอกให้เหยื่อกระทำการที่อาจก่อให้เกิดความเสียหายหรือบอกข้อมูลที่มีความสำคัญออกมา (เช่น รหัสผ่าน หรือข้อมูลส่วนตัว)

คำแนะนำ

- เมื่อได้รับแจ้งเตือนถึงการปลอม-แปลงอีเมล์ที่กล่าวว่าผู้ส่งคือท่าน หรือได้ รับทราบถึงการปลอมแปลงจากการตีกลับของอีเมล์ของท่านทั้งๆ ที่ท่านไม่ได้เป็นผู้ส่งไป ให้เก็บรวบรวมหลักฐานทั้งหมดที่เกี่ยวกับการปลอมแปลงนั้นและส่งไปให้กับผู้ให้บริการอินเทอร์เน็ตของท่านเพื่อใช้ในการสืบสวนต่อไป
- ให้ใช้ลายมือชื่ออิเล็กทรอนิกส์กับผู้ที่ติดต่อด้วย หากไม่มั่นใจว่าอีเมล์ที่ได้รับมาจากแหล่งที่เชื่อถือได้หรือไม่ สำหรับข้อมูลเพิ่มเติมในเรื่องนี้โปรดดูที่หัวข้อลายมือชื่ออิเล็กทรอนิกส์
- ให้ระมัดระวังอีเมล์ที่ระบุว่าส่งมาจากเพื่อนหรือผู้ร่วมงานและใช้ subject ของอีเมล์ที่แปลกๆ อีเมล์ดังกล่าวนี้อาจส่งมาโดยอัตโนมัติจากซอฟต์แวร์ที่ไม่ประสงค์ดีต่างๆ เช่น หนอนเครือข่าย เป็นต้น
- ให้ดูวิธีการหลอกลวงต่างๆ จากเว็บไซต์ด้านล่างซึ่งเป็นเว็บของเซิร์ต (CERT-Computer Emergency Response Team) ซึ่งเป็นหน่วยงานที่ได้รับรายงานจากทั่วโลกเกี่ยวกับการหลอกหลวงในรูปแบบต่างๆ ที่เกิดขึ้น มีวิธีการหลอกลวงหลากหลายวิธีที่นำมาใช้หลอกให้เหยื่อเปิดเผยข้อมูลสำคัญ เช่น รหัสผ่าน การหลอกลวงดังกล่าวอาจจะมาในรูปของการปลอมแปลงอีเมล์ การหลอกให้เข้าไปดูเว็บไซต์ การโทรศัพท์ถาม หรือแม้แต่การส่งจดหมายมาถามทางไปรษณี ย์ ทั้งนี้ก่อนที่จะให้ข้อมูลใดๆ เกี่ยวกับผ่านหรือข้อมูลส่วนตัวของตน ให้ตรวจสอบให้มั่นใจก่อนว่าผู้สอบถามเป็นผู้ที่รู้จักหรือ สามารถพิสูจน์ตัวตนได้

แหล่งข้อมูลเพิ่มเติม
www.cert.org/tech_tips/email_spoofing.html

สปายแวร์ (Spyware)

สปายแวร์คือซอฟต์แวร์ใดๆ ที่ใช้ช่องทางการเชื่อมต่อกับอินเทอร์เน็ตในเครื่องคอมพิวเตอร์ของผู้ใช้เพื่อแอบส่งข้อมูลส่วนตัวของผู้ใช้นั้นไปให้กับบุคคลหรือองค์กรหนึ่ง โดยที่ผู้ใช้เองไม่ทราบ หรือไม่ได้รับอนุญาตจากผู้ใช้ก่อน สปายแวร์ สามารถเข้าสู่เครื่องคอมพิวเตอร์ที่ใช้งานได้โดยผ่านทางไวรัสคอมพิวเตอร์ เว็บเพจที่ เข้าไปดู หรืออีเมล์ที่เปิดอ่าน

สปายแวร์นั้นมีหลายประเภทนับตั้งแต่ประเภทที่เป็นคุกกี้จากการเข้าดูเว็บ(ดูรายละเอียดในหัวข้อคุกกี้) จนกระทั่งถึงประเภทที่เป็นโปรแกรมที่ล่วงล้ำเข้ามาใน เครื่องคอมพิวเตอร์ของผู้ใช้เพื่อรายงานข้อมูลกลับไปยังผู้ผลิตว่าผู้ใช้ใช้งานโปรแกรมที่ติดตั้งนั้นอย่างไร โปรแกรมที่ล่วงล้ำนี้โดยทั่วไปจะเป็นซอฟต์แวร์ที่ผู้ใช้ ดาวน์โหลดมาจากอินเทอร์เน็ตและติดตั้งเพื่อใช้งานในจุดประสงค์หนึ่ง และผู้ผลิต ซอฟต์แวร์นั้นก็ย่อมจะต้องการทราบลักษณะการใช้งานของผู้ใช้เพื่อใช้เป็นข้อมูลใน การปรับปรุงซอฟต์แวร์ของตนต่อไป จึงล่วงละเมิดผู้ใช้โดยแอบติดตั้งโปรแกรมใน ส่วนของการรายงานผลกลับไปยังผู้ผลิตด้วย ผู้ใช้โดย ส่วนใหญ่จะไม่เห็นด้วยกับการละเมิดนี้เนื่องจากเห็นว่าเป็นการละเมิดสิทธิและความเป็นส่วนตัว และ ก็ได้มีการฟ้องร้องบริษัทผู้ผลิตที่กระทำเช่นนี้มา หลายกรณี แล้วและส่งผลให้มีการแก้ไข ซอฟต์แวร์เพื่อมิให้กระทำการล่วงละเมิดผู้ใช้อีก ต่อไป

อย่างไรก็ตามก็ยังคงมีบริษัทผู้ผลิตซอฟต์แวร์อีกหลายบริษัทที่ยังคงรวบรวมข้อมูลส่วนตัวของผู้ใช้อยู่อย่างลับๆ ผู้ใช้จึงต้องระมัดระวังและอ่านข้อมูลและเงื่อนไขการติดตั้งของโปรแกรมใดๆ ที่ต้องการติดตั้ง โดยส่วนใหญ่แล้วในระหว่างการติดตั้งผู้ใช้สามารถเลือกที่จะไม่ให้ทำการรายงานข้อมูลกลับไปยังบริษัทได้ แต่จะต้องใช้ความระมัดระวังว่ามีขั้นตอนใดที่เป็นตัวเลือกดังกล่าว เนื่องจากบางบริษัทมีความต้องการที่จะได้รับทราบข้อมูลของผู้ใช้งานเป็นอย่างมากจึงใช้วิธีการต่าง ๆ ที่จะปกปิดการติดตั้งสปายแวร์ลงไปยังเครื่องคอมพิวเตอร์ของผู้ใช้

เว็บบัก (Web Bug) ก็เป็นอีกรูปแบบหนึ่งของสปายแวร์ เว็บบักเป็นโปรแกรมเล็กๆ ที่มองเห็นเป็นไฟล์รูปภาพเล็กๆ อยู่บนเว็บเพจหรือในข้อความอีเมล์ที่ส่งมาเป็นแบบ HTML ซึ่งโดยส่วนใหญ่แล้วผู้ใช้จะไม่สามารถสังเกตเห็นได้อย่าง ชัดเจน เว็บบักจะทำงานร่วมกับคุกกี้เพื่อเก็บรวบรวมข้อมูลลักษณะนิสัยการท่องเว็บ ของผู้ใช้ การป้องกันเว็บบักที่ดีที่สุดคือการตั้งค่าการรับคุกกี้ในบราวเซอร์ที่ใช้งานให้ค่าความปลอดภัยสูงที่สุดเท่าที่จะยอมรับได้

คำแนะนำ

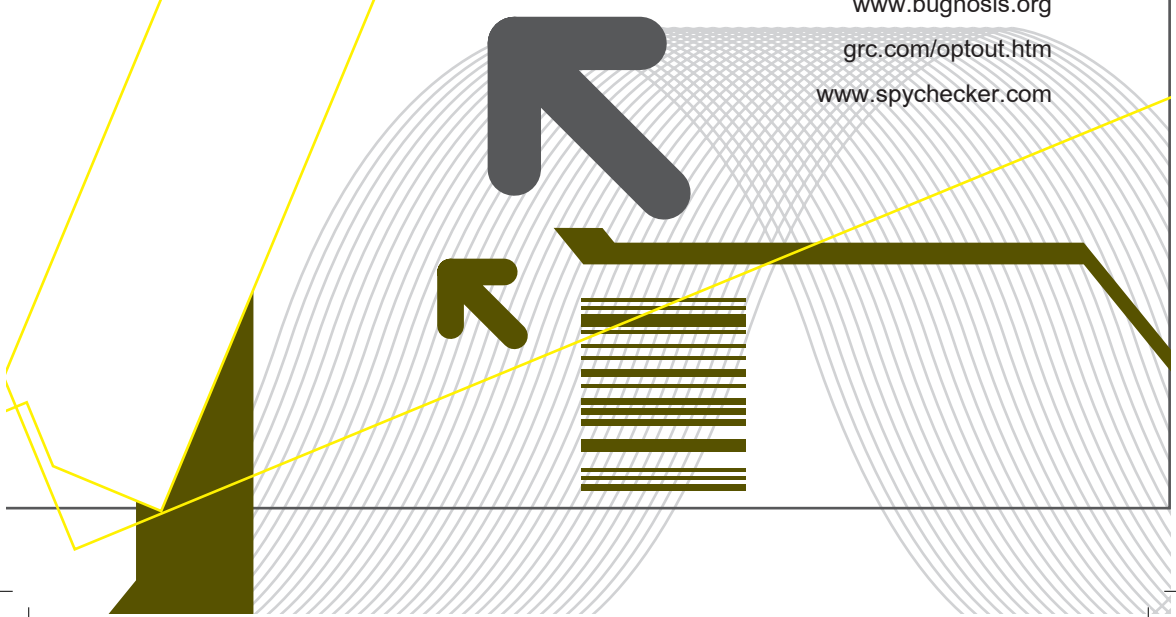
- ตรวจสอบและปรับแต่งการตั้งค่าสำหรับคุกกี้ในเว็บบราวเซอร์ที่ใช้งานให้มี ความเหมาะสม
- ดาวน์โหลดโปรแกรมตรวจสอบสปายแวร์มาใช้งาน เช่นโปรแกรม "Ad-aware" (www.lavasoft.de)
- อ่านนโยบายของเว็บไซต์ที่เข้าไปชมว่าเว็บนั้นจะนำข้อมูลส่วนตัวของผู้ใช้ ไปใช้งานอย่างไรและเว็บนั้นใช้สปายแวร์ในการเก็บรวบรวมข้อมูลหรือไม่
- ติดตั้งโปรแกรมไฟร์วอลล์และปรับปรุงให้ทันสมัยอยู่เสมอ

แหล่งข้อมูลเพิ่มเติม

www.bugnosis.org

grc.com/optout.htm

www.spychecker.com



โปรแกรมโทรจัน

(Trojan Programs)

โปรแกรมโทรจันเข้ามาสู่เครื่องที่ใช้งานโดยที่ผู้ใช้อาจจะไม่รู้ตัวและจะทำงานอยู่เบื้องหลังซึ่งทำให้เป็นการยากที่จะตรวจจับได้ โดยทั่วไปแล้วโปรแกรมโทรจันจะแฝงมากับโปรแกรมอื่น สาเหตุที่เราเรียกกันว่า "โทรจัน" นั้น เป็นการอุปมาอุปไมยซึ่งเทียบได้กับม้าโทรจันในนิยายปรัมปราของกรีกม้าโทรจันนี้เมื่อดูจากภายนอกแล้วก็ เหมือนม้าที่ทำด้วยไม้ธรรมดาๆ ที่ถูกส่งเข้าไปในตัวเมือง แต่ข้างในตัวม้าจะแฝงไว้ด้วยข้าศึกติดเข้ามาด้วย ซึ่งเมื่อเข้าไปในตัวเมืองแล้ว ก็จะสามารถเข้าไปเปิดประตูเมืองให้กับฝ่ายศัตรูเข้ามาได้ โปรแกรมโทรจันจึงทำงานเป็น "ไส้ศึก" ในลักษณะเดียวกับม้าโทรจันนั่นเอง โปรแกรมโทรจันอาจจะติดมากับไฟล์ที่ส่งมาทางอีเมล์ มาจากการแลกเปลี่ยนโปรแกรมกันในห้องสนทนา มาจากไฟล์ที่อยู่ในฟล็อปปีดิสก์ หรือโปรแกรมที่ก็อปปีกันมา และวิธีอื่นๆ อีกมากมาย

โปรแกรมโทรจันแบ่งออกเป็น 3 ชนิดหลักๆ ดังนี้

- โปรแกรมเข้าถึงเครื่องคอมพิวเตอร์จากทางไกล (Remote Access Tools - RATs) โปรแกรมประเภทนี้จะทำให้ผู้บุกรุกระบบจากทางไกล เช่น โดยผ่านทางเครือข่ายเข้ามา สามารถเข้าถึงเครื่องคอมพิวเตอร์ที่ ถูกติดตั้งโทรจันลงไป
- ตัวจับการพิมพ์แป้นคีย์บอร์ด (Key Loggers) โปรแกรมประเภทนี้ จะบันทึกการพิมพ์จากแป้นคีย์บอร์ดทั้งหมดที่ป้อนเข้าเครื่อง แล้วรวบ รวมส่งเป็นไฟล์ให้ผู้บุกรุกต่อไป
- ตัวจับรหัสผ่าน (Password Retrievers) โปรแกรมประเภทนี้จะนำส่งไฟล์รหัสผ่านในเครื่องของผู้ใช้ให้แก่ผู้บุกรุก

การดาวน์โหลดไฟล์โปรแกรมโทรจันมาแต่ยังไม่ได้สั่ง "รัน" หรือ "เอ็กซีคิวต์" ไฟล์นั้น จะยังไม่ทำให้โปรแกรมโทรจันเริ่มต้นการทำงาน ผู้ใช้ต้องระมัดระวัง ในการทำงานกับไฟล์ประเภทเวิร์ด หรือ สเปรดชีตด้วย ทั้งนี้เนื่องจากไฟล์ประเภทนี้ อาจมีมาโครที่สามารถสั่งให้เครื่องทำงานได้ มีไวรัสหรือโทรจันแอบแฝงมาด้วย

โปรแกรมโทรจันกับไวรัสคอมพิวเตอร์ (ให้ดูในหัวข้อไวรัส) แม้ไม่ใช่เป็น สิ่งเดียวกัน แต่โปรแกรมป้องกันไวรัสหลายโปรแกรมจะสามารถตรวจจับหา โปรแกรมโทรจันได้

คำแนะนำ

- ติดตั้งโปรแกรมไฟร์วอลล์บนเครื่องคอมพิวเตอร์ที่ใช้งาน
- หมั่นปรับปรุงไฟล์รูปแบบไวรัสของโปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ
- ใช้โปรแกรมป้องกันไวรัสตรวจสอบโปรแกรมที่กำลังจะติดตั้งและใช้งานก่อนทุกครั้ง
- ใช้โปรแกรมป้องกันไวรัสตรวจสอบเครื่องคอมพิวเตอร์ที่ใช้งานทั้งเครื่องอย่างน้อยสัปดาห์ละหนึ่งครั้ง

แหล่งข้อมูลเพิ่มเติม

www.cert.org

การติดต่อสอบถามเรื่องพ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

- สามารถสืบค้นข้อมูลเพิ่มเติม ได้ที่ http://www.mict.go.th

- ติดต่อสอบถามหรือร้องเรียน ผ่านทางเบอร์โทรศัพท์ 1111 หรือ ติดต่อโดยตรง ได้ที่ สำนักกำกับการใช้เทคโนโลยีสารสนเทศ กระทรวง ICT โทรศัพท์ 02 505 7223
- การแจ้งความเพื่อดำเนินคดี สามารถแจ้งความได้ ณ สถานีตำรวจ ทั่วราชอาณาจักร หรือมาแจ้งความด้วยตนเองโดยตรง ที่กระทรวง ICT จะมีหน่วยงานรับเรื่องเกี่ยวกับการกระทำความผิดตาม พ.ร.บ. นี้ (เฉพาะในวันและเวลาราชการ)

อ้างอิง

1. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร : www.mict.go.th
2. คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ : www.etcommission.go.th
3. ศูนย์ตรวจสอบและวิเคราะห์การกระทำผิดทางเทคโนโลยี (High-Tech Crime Center) : http://htcc.police.go.th
4. กองบัญชาการเทคโนโลยีสารสนเทศและการสื่อสาร : http://ict.police.go.th
5. สำนักงานตำรวจแห่งชาติ : www.royalthaipolice.go.th
6. กรมสอบสวนคดีพิเศษ : http://www.dsi.go.th/
7. ประชาชนเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กรุงเทพฯ, พ.ศ. 2551.
8. เว็บไซต์ NECTEC เพื่อประชาคมความรู้ (NECTEC PEDIA) : http://wiki.nectec.or.th/nectecpedia/index.php
9. Safety net คู่มือการใช้งานเครือข่ายอินเทอร์เน็ตอย่างปลอดภัย สำหรับผู้ใช้งานทั่วไป , 2548
10. คุยสบาย ฯ ครั้งที่ 7 (อาชญากรรมคอม ฯ) : http://biolawcom.de/?/article/44
11. สถิติเศรษฐกิจสังคมและประชามติ 3 สำนักงานสถิติแห่งชาติ. สำรวจความคิดเห็นของ

ภาคผนวก

พระราชบัญญัติว่าด้วย การกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติ
ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
พ.ศ. ๒๕๕๐

ภูมิพลอดุลยเดช ป.ร.
ให้ไว้ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๕๐

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐"

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงาน เข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์ด้วย

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"ผู้ให้บริการ" หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

"ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑
ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาทหรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลัง และไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี หรือปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิด

ความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

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

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

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

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่งเป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความกันได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ

จะต้องรับโทษภายในราชอาณาจักร

หมวด ๒
พนักงานเจ้าหน้าที่

มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกตัวบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสารข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ใช้บริการเกี่ยวกับการติดต่อสื่อสาร ผ่านระบบคอมพิวเตอร์ หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการ ที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าว ให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘(๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจ

เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๘(๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้น ไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๘(๔) (๕) (๖) (๗) และ (๘) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการ ให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการเพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘(๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๖(๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือ ถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา ๒๐ ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสอง ลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายวิธีพิจารณาความอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้น ได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

มาตรา ๒๑ ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้มีไว้ในครอบครอง หรือเผยแพรชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้นตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือ ข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดความจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปี เป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการ นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า เก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา ๒๗ ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามตามมาตรา ๑๘ หรือมาตรา ๒๐ หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา ๒๑ ต้องระวางโทษปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรา ๒๘ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้

และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา ๒๕ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตาม พระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงาน สอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรี ในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา ๓๐ ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง

บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไขหรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการพ.ศ. ๒๕๕๐

ด้วยในปัจจุบันการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์เริ่มเข้าไปมีบทบาทและทวีความสำคัญเพิ่มขึ้นตามลำดับต่อระบบเศรษฐกิจและคุณภาพชีวิตของประชาชน แต่ในขณะเดียวกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีแนวโน้มขยายวงกว้าง และทวีความรุนแรงเพิ่มมากขึ้น ข้อมูลจราจรทางคอมพิวเตอร์นับเป็นพยานหลักฐานสำคัญในการดำเนินคดีอันเป็นประโยชน์อย่างยิ่งต่อการสืบสวน สวนสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ จึงสมควรกำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าว

อาศัยอำนาจตามความในมาตรา ๒๖ วรรค ๓ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ดังนั้น รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้กำหนดหลักเกณฑ์ไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามประกาศนี้

ข้อ ๔ ในประกาศนี้

"ผู้ให้บริการ" หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการหรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนด คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ "ผู้ใช้บริการ"

หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

ข้อ ๕ ภายใต้บังคับของมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ประเภทของผู้ให้บริการซึ่งมีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์แบ่งได้ ดังนี้

(๑) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือ เพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ ๔ ประเภท ดังนี้

ก. ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก.แนบท้ายประกาศนี้

ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่างๆ (Host Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ง. ผู้ให้บริการร้านอินเทอร์เน็ต ดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

(๒) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม (๑) (Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ (Application Service Provider) ประกอบด้วยผู้ให้บริการดังภาคผนวก ก. แนบท้ายประกาศนี้

ข้อ ๖ ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการต้องเก็บรักษา ปรากฏดังภาคผนวก ข. แนบท้ายประกาศนี้

ข้อ ๗ ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ดังนี้

(๑) ผู้ให้บริการตามข้อ ๕ (๑) ก. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๑

(๒) ผู้ให้บริการตามข้อ ๕ (๑) ข. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๒ ตามประเภท ชนิดและหน้าที่การให้บริการ

(๓) ผู้ให้บริการตามข้อ ๕ (๑) ค. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๒ ตามประเภท ชนิดและหน้าที่การให้บริการ

(๔) ผู้ให้บริการตามข้อ ๕ (๑) ง. มีหน้าที่เก็บ

ข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๓

(๕) ผู้ให้บริการตามข้อ ๕ (๒) มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๔

ทั้งนี้ ในการเก็บรักษาข้อมูลจราจรตามภาคผนวกต่างๆ ที่กล่าวไปข้างต้นนั้น ให้ผู้ให้บริการเก็บเฉพาะในส่วนที่เป็นข้อมูลจราจรที่เกิดจากส่วนที่เกี่ยวข้องกับบริการของตนเท่านั้น

ข้อ ๘ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัยดังต่อไปนี้

(๑) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

(๒) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือ ทำ Data Hashing เป็นต้น เว้นแต่ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์กรกำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบ ระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้งพนักงานเจ้าหน้าที่ ตามพระราชบัญญัตินี้

(๓) จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อให้การส่งมอบข้อมูลนั้น เป็นไปด้วยความรวดเร็ว

(๔) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือ บริการ 1222 หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

(๕) ในกรณีที่ผู้ให้บริการประเภทหนึ่งประเภทใด ในข้อ ๑ ถึงข้อ ๔ ข้างต้น ได้ให้บริการในนามตนเอง แต่บริการดังกล่าวเป็นบริการที่ใช้ระบบของผู้ให้บริการซึ่งเป็นบุคคลที่สาม เป็นเหตุให้ผู้ให้บริการในข้อ ๑ ถึงข้อ ๔ ไม่สามารถรู้ได้ว่า ผู้ใช้บริการที่เข้ามาในระบบนั้นเป็นใคร ผู้ให้บริการเช่นว่านั้นต้องดำเนินการให้มีวิธีการระบุและยืนยันตัวบุคคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย

ข้อ ๙ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

ข้อ ๑๐ ผู้ให้บริการซึ่งมีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามข้อ ๗ เริ่มเก็บข้อมูลดังกล่าวตามลำดับ ดังนี้

(๑) ผู้ให้บริการตามข้อ ๕ (๑) ก. เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นสามสิบวันนับจากวันประกาศในราชกิจจานุเบกษา

(๒) ให้ผู้ให้บริการตามข้อ ๕ (๑) ข. เฉพาะผู้ให้บริการเครือข่ายสาธารณะหรือผู้ให้บริการอินเทอร์เน็ต (ISP) เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งร้อยแปดสิบวันนับจากวันประกาศในราชกิจจานุเบกษา

ผู้ให้บริการอื่นนอกจากที่กล่าวมาในข้อ ๑๐ (๑) และข้อ ๑๐ (๒) ข้างต้น ให้เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งปีนับจากวันประกาศในราชกิจจานุเบกษา

ประกาศ ณ
วันที่ ๒๑ สิงหาคม พ.ศ. ๒๕๕๐
นายสิทธิชัย โภไคยอุดม
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ภาคผนวก ก

แนบท้ายประกาศ
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์
ของผู้ให้บริการพ.ศ. ๒๕๕๐

๑. ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่นโดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น ตามข้อ ๕ (๑) จำแนกได้ ๔ ประเภท ดังนี้

ประเภท	ตัวอย่างของผู้ให้บริการ
ก.ผู้ประกอบกิจการโทรคมนาคมและกิจการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier)	๑) ผู้ให้บริการโทรศัพท์พื้นฐาน (Fixed Line Service Provider) ๒) ผู้ให้บริการโทรศัพท์เคลื่อนที่ (Mobile Service Provider) ๓) 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 เว้นแต่ผู้ให้บริการนั้น ให้บริการแต่เพียง Physical Media หรือสายสัญญาณอย่างเดียว (Cabling) เท่านั้น (เช่น ผู้ให้บริการ Dark Fiber, ผู้ให้บริการสายใยแก้วนำแสง ซึ่งอาจไม่มีสัญญาน Internet หรือไม่มี IP Traffic) ๔) ผู้ให้บริการดาวเทียม (Satellite Service Provider)
ข.ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)	๑) ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ทั้งมีสายและไร้สาย ๒) ผู้ประกอบการซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรม หรือร้านอาหารและเครื่องดื่ม ในแต่ละกลุ่มอย่างหนึ่งอย่างใด ๓) ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัทหรือ สถาบันการศึกษา
ค.ผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อให้บริการโปรแกรมประยุกต์ต่างๆ (Hosting Service Provider)	๑) ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (Web Hosting), การให้บริการเช่า Web Server ๒) ผู้ให้บริการแลกเปลี่ยนแฟ้มข้อมูล (File Server หรือ File Sharing) ๓) ผู้ให้บริการการเข้าถึงจดหมายอิเล็กทรอนิกส์ (Mail Server Service Provider) ๔) ผู้ให้บริการศูนย์รับฝากข้อมูลทางอินเทอร์เน็ต (Internet Data Center)
ง.ผู้ให้บริการร้านอินเทอร์เน็ต	๑.ผู้ให้บริการร้านอินเทอร์เน็ต (Internet Caf?) ๒.ผู้ให้บริการร้านเกมออนไลน์ (Game Online)

๒. ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม ข้อ ๕ (๒) ประกอบด้วยผู้ให้บริการดังภาคผนวก ก แนบท้ายประกาศนี้

ประเภท	ตัวอย่างของผู้ให้บริการ
ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ (Content and Application Service Provider)	๑) ผู้ให้บริการเว็บบอร์ด (Web board) หรือ ผู้ให้บริการบล็อค (Blog) ๒) ผู้ให้บริการการทำธุรกรรมทางการเงินทางอินเทอร์เน็ต (Internet Banking) และผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ (Electronic Payment Service Provider) ๓) ผู้ให้บริการเว็บเซอร์วิส (Web Services) ๔) ผู้ให้บริการพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) หรือธุรกรรมทางอิเล็กทรอนิกส์ (e-Transactions)

ภาคผนวก ข

แนบท้ายประกาศ
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการพ.ศ. ๒๕๕๐

๑. ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ก. มีหน้าที่ต้องเก็บรักษามีดังต่อไปนี้

ประเภท	รายการ
ก.ข้อมูลที่สามารถระบุและติดตามถึงแหล่งกำเนิดต้นทาง 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	วันที่ รวมทั้งเวลาเริ่มต้นและสิ้นสุดของการใช้งาน (Fixed Network Telephony and Mobile Telephony, the Date and Time of the Start and End of the Communication)
ค.ข้อมูลซึ่งสามารถระบุที่ตั้งในการใช้โทรศัพท์มือถือหรืออุปกรณ์ติดต่อสื่อสารแบบไร้สาย (Mobile Communication Equipment)	๑) ที่ตั้ง label ในการเชื่อมต่อ (Cell ID) ณ สถานที่เริ่มติดต่อสื่อสาร
	๒) ข้อมูลซึ่งระบุที่ตั้งทางกายภาพของโทรศัพท์มือถืออันเชื่อมโยงกับข้อมูลที่ตั้งของ Cell ID ขณะที่มีการติดต่อสื่อสาร
	๓) จัดให้มีระบบบริการตรวจสอบบุคคลผู้ใช้บริการ

๒. ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ข. ถึง ค. มีหน้าที่ต้องเก็บรักษามีดังต่อไปนี้

ประเภท	รายการ
ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย	๑) ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่าย ซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย (Access Logs Specific to Authentication and Authorization Servers เช่น TACACS (Terminal Access Controller Access-Control System) or RADIUS (Remote Authentication Dial-In User Service) or DIAMETER (Used to Control Access to IP Routers or Network Access Servers)
	๒) ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server) ๓) ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID)
	๔) ข้อมูลหมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดให้โดยระบบผู้ให้บริการ (Assigned IP Address)
	๕) ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (Calling Line Identification)

ข. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)	๑) ข้อมูล Log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็กทรอนิกส์ (Simple Mail Transfer Protocol : SMTP Log) ซึ่งได้แก่ - ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID) - ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender E-mail Address) - ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver E-mail Address) - ข้อมูลที่บงบอกถึงสถานะในการตรวจสอบ (Status Indicator) ซึ่งได้แก่ จดหมายอิเล็กทรอนิกส์ที่ส่งสำเร็จ จดหมายอิเล็กทรอนิกส์ที่ส่งคืน จดหมายอิเล็กทรอนิกส์ที่มีการส่งล่าช้า เป็นต้น
	๒) ข้อมูลจดหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ใช้บริการที่เชื่อมต่ออยู่ขณะเข้ามาใช้บริการ (IP Address of Client Connected to Server)
	๓) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server)
	๔) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ ที่ถูกเชื่อมต่ออยู่ในขณะนั้น (IP Address of Sending Computer)
	๕) ชื่อผู้ใช้งาน (User ID) (ถ้ามี)
	๖) ข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือการเข้าถึงเพื่อเรียกข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิก โดยยังจัดเก็บข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึงไปนั้น ไว้ที่เครื่องให้บริการ (POP3 (Post Office Protocol Protocol Version 3) Log or IMAP4 (Internet Message Access Protocol Version 4) Log)

ค. ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องให้บริการโอนแฟ้มข้อมูล
	๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
	๓) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น (IP Source Address)
	๔) ข้อมูลชื่อผู้ใช้งาน (User ID) (ถ้ามี)
	๕) ข้อมูลตำแหน่ง (Path) และ ชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการ ส่งขึ้นมาบันทึก หรือให้ดึงข้อมูลออกไป (Path and Filename of Data Object Uploaded or Downloaded)
ง) ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ให้บริการเว็บ
	๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ
	๓) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น
	๔) ข้อมูลคำสั่งการใช้งานระบบ
	๕) ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI: Uniform Resource Identifier) เช่น ตำแหน่งของเว็บเพ็จ
จ. ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย (NNTP (Network News Transfer Protocol) Log)
	๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
	๓) ข้อมูลหมายเลข Port ในการใช้งาน (Protocol Process ID)
	๔) ข้อมูลชื่อเครื่องให้บริการ (Host Name)
	๕) ข้อมูลหมายเลขลำดับข้อความที่ได้ถูกส่งไปแล้ว (Posted Message ID)
ฉ. ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Messaging (IM) เป็นต้น	ข้อมูล Log เช่น ข้อมูลเกี่ยวกับวัน เวลาการติดต่อของผู้ใช้บริการ (Date and Time of Connection of Client to Server) และ ข้อมูลชื่อเครื่องบนเครือข่าย และ หมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ในขณะนั้น (Hostname and IP Address) เป็นต้น

๓. ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ง. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก. ผู้ให้บริการร้านอินเทอร์เน็ต	๑) ข้อมูลที่สามารถระบุตัวบุคคล ๒) เวลาของการเข้าใช้ และเลิกใช้บริการ ๓) หมายเลขเครื่องที่ใช้ IP Address (Internet Protocol address)

๔. ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๒) มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ (Content Service Provider)	๑) ข้อมูลรหัสประจำตัวผู้ใช้หรือข้อมูลที่สามารถระบุตัวผู้ใช้บริการได้ หรือ เลขประจำตัว (User ID) ของผู้ขายสินค้าหรือบริการ หรือ เลขประจำตัวผู้ใช้บริการ (User ID) และที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการ
	๒) บันทึกข้อมูลการเข้าใช้บริการ
	๓) กรณีผู้ให้บริการเว็บบอร์ด (Web board) หรือผู้ให้บริการบล็อค (Blog) ให้เก็บข้อมูลของผู้ประกาศ (Post) ข้อมูล

ประกาศกระทรวง
เทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติ
ของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติ
ว่าด้วยการกระทำความผิดเกี่ยวกับ
คอมพิวเตอร์ พ.ศ.2550

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

เพื่อให้การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ มีความชัดเจนและเป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๒๘ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้กำหนดหลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

"รัฐมนตรี" หมายความว่า รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ ๒ พนักงานเจ้าหน้าที่ ต้องมีคุณสมบัติดังต่อไปนี้

(๑) มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์

(๒) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรีทางวิศวกรรมศาสตร์ วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือรัฐประศาสนศาสตร์

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

(๔) มีคุณสมบัติอื่นอย่างหนึ่งอย่างใดดังต่อไปนี้

ก. รับราชการหรือเคยรับราชการไม่น้อยกว่าสองปีในตำแหน่งเจ้าหน้าที่ตรวจพิสูจน์พยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์หรือพยานหลักฐานอิเล็กทรอนิกส์

ข. สำเร็จการศึกษาตามข้อ ๒ (๒) ในระดับปริญญาตรี และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสี่ปี

ค. สำเร็จการศึกษาตามข้อ ๒ (๒) ในระดับปริญญาโท หรือสอบไล่ได้เป็นเนติบัณฑิตตามหลักสูตรของสำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสามปี

ง. สำเร็จการศึกษาตามข้อ ๒ (๒) ในระดับปริญญาเอก หรือมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงาน ตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสองปี

จ. เป็นบุคคลที่ทำงานเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ หรือมีประสบการณ์ในการดำเนินคดีเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ไม่น้อยกว่าสองปี

ข้อ ๓ ในกรณีที่มีความจำเป็นเพื่อประโยชน์ของทางราชการในการสืบสวนและสอบสวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จำเป็นต้องมีบุคลากรซึ่งมีความรู้ ความชำนาญ หรือประสบการณ์สูงเพื่อดำเนินการสืบสวนและสอบสวนการกระทำผิดหรือคดีเช่นว่านั้น หรือเป็นบุคลากรในสาขาที่ขาดแคลน รัฐมนตรีอาจยกเว้นคุณสมบัติตามข้อ ๒ ไม่ว่าทั้งหมดหรือบางส่วนสำหรับการบรรจุและแต่งตั้งบุคคลใดเป็นการเฉพาะก็ได้

ข้อ ๔ การแต่งตั้งบุคคลหนึ่งบุคคลใดเป็นพนักงานเจ้าหน้าที่ให้แต่งตั้งจากบุคคลซึ่งมีคุณสมบัติตามข้อ ๒ หรือ ข้อ ๓ โดยบุคคลดังกล่าวต้องผ่านการประเมินความรู้ความสามารถหรือทดสอบตามหลักสูตรและหลักเกณฑ์ที่รัฐมนตรีประกาศกำหนด

การแต่งตั้งบุคคลใดเป็นพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ดำรงตำแหน่งในวาระคราวละ ๔ ปี และการแต่งตั้งให้ประกาศในราชกิจจานุเบกษา

ข้อ ๕ พนักงานเจ้าหน้าที่ต้องไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) เป็นบุคคลล้มละลาย บุคคลไร้ความสามารถหรือบุคคลเสมือนไร้ความสามารถ

(๒) เป็นสมาชิกสภาผู้แทนราษฎร สมาชิกวุฒิสภา

ข้าราชการการเมือง สมาชิกสภาท้องถิ่น ผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งที่รับผิดชอบในการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่ในพรรคการเมือง

(๓) เป็นผู้อยู่ระหว่างถูกสั่งให้พักราชการหรือถูกสั่งให้ออกจากราชการไว้ก่อน

(๔) ถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หน่วยงานของรัฐหรือรัฐวิสาหกิจเพราะทำผิดวินัย หรือรัฐมนตรีให้ออกจากการเป็นพนักงานเจ้าหน้าที่ เพราะมีความประพฤติเสื่อมเสีย บกพร่องหรือไม่สุจริตต่อหน้าที่หรือหย่อนความสามารถ

(๕) ได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษ สำหรับความผิดที่กระทำโดยประมาทหรือความผิดลหุโทษ

(๖) ต้องคำพิพากษาหรือคำสั่งของศาลให้ทรัพย์สินตกเป็นของแผ่นดิน เพราะร่ำรวยผิดปกติหรือมีทรัพย์สินเพิ่มขึ้นผิดปกติ

ข้อ ๖ พนักงานเจ้าหน้าที่พ้นจากตำแหน่งเมื่อ

(๑) ตาย

(๒) ลาออก

(๓) ถูกจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก

(๔) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามข้อ ๕

(๕) รัฐมนตรีให้ออก เพราะมีความประพฤติเสื่อมเสีย บกพร่องหรือไม่สุจริตต่อหน้าที่หรือหย่อนความสามารถ

(๖) ครบวาระการดำรงตำแหน่ง

ข้อ ๗ ประกาศนี้มีผลใช้บังคับตั้งแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๒๑ สิงหาคม พ.ศ.๒๕๕๐
นายสิทธิชัย โภไคยอุดม
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ภาคผนวก

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

ผู้ที่จะได้รับการแต่งตั้งให้เป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ จะต้องผ่านการอบรมด้านจริยธรรม สืบสวน สอบสวนความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) แล้วแต่กรณี ดังต่อไปนี้

๑. หลักสูตรมาตรฐานสากล (International Standard Courses)

วัตถุประสงค์ : เพื่อใช้เป็นแนวทางในการจัดอบรมให้กับบุคคลซึ่งจะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ในกรณีทั่วไป (หลักสูตรเต็มเวลาประมาณ ๑ เดือน ทั้งภาคทฤษฎีและปฏิบัติ ทั้งนี้ ไม่รวมด้านที่สาม ข. และด้านที่สี่ ข. ซึ่งเป็นหลักสูตรความเชี่ยวชาญเฉพาะทาง)

เนื้อหาหลักสูตรที่อบรม :

ด้านแรก การอบรมด้านจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทและอำนาจหน้าที่ของพนักงานเจ้าหน้าที่

ด้านที่สอง ความรู้พื้นฐานด้านการสืบสวนและสอบสวนเพื่อการบังคับใช้กฎหมาย (Law Enforcement)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑.	กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๒.	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๓.	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)
๔.	การสืบสวนทางเทคนิค เช่น การตรวจสอบหมายเลข IP Address หรือแหล่งที่มาของการกระทำความผิด การขอข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) จากผู้ให้บริการ การวิเคราะห์และเชื่อมโยงข้อมูล/พยานหลักฐานข้างต้น
๕.	แนวทางปฏิบัติในการดำเนินคดี/การทำสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ (การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การรวบรวมพยานหลักฐาน และแสวงหาข้อเท็จจริง การตรวจสถานที่เกิดเหตุ การยื่นคำร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน การเก็บรักษาพยานหลักฐาน การเก็บรักษาพยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการ การเปรียบเทียบปรับและการดำเนินคดี เป็นต้น
๖.	การบริหารจัดการคดีให้เป็นไปอย่างมีประสิทธิภาพ

ด้านที่สาม ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security)

ก. เนื้อหาหลักสูตรภาคบังคับสำหรับพนักงานเจ้าหน้าที่

ข. หลักสูตรความมั่นคงปลอดภัยของระบบ

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑.	General security concepts
๒.	Security Architecture
๓.	Access Controls
๔.	Applications Security
๕.	Operation Security
๖.	Security Management
๗.	Cryptography
๘.	Physical Security
๙.	Telecommunications and Network Security
๑๐.	Business Continuity Planning
๑๑.	Law, Investigations, and Ethics

สารสนเทศขั้นสูง (Advanced Information Security Course) สำหรับพนักงานเจ้าหน้าที่สายผู้เชี่ยวชาญด้านเทคนิค

ลำดับ	เนื้อหาหลักสูตร (ความชำนาญเฉพาะทาง)
๑.	Audit and Monitoring
๒.	Risk, Response and Recovery
๓.	Malicious Code Analysis
๔.	Vulnerabilities Assessment & Penetration Testing

ด้านที่สี่ การพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics)

ก.ความรู้ด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics)

ข.ความเชี่ยวชาญเฉพาะทางด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Professional Computer Forensics และ Certified Forensic Computer Examiner (CFCE))

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑.	The needs for Computer Forensics
๒.	Principles of Computer Forensics and Digital/Electronic Evidence
๓.	Crime scene, Digital/Electronic Evidence and Chain of Custody
๔.	Capturing the Data Image and Volatile Data
๕.	Extracting Information from Captured Data
๖.	Breaking Password and Encryption
๗.	Using Computer Forensics Tools
๘.	Investigation and Interrogation
๙.	Digital/Electronic Evidence Analysis and Synthesis
๑๐.	Testify in Court, Admissibility requirements
๑๐.	Different between Computer Forensics and Network/Internet Forensics
๑๒.	Network/Internet Forensics
๑๓.	Using Network/Internet Forensics Tools

๒. หลักสูตรเร่งรัด (Intensive Courses) (๕ วัน)

วัตถุประสงค์ : เพื่อใช้เป็นแนวทางในการจัดการอบรมระยะสั้นแบบเร่งรัดให้กับบุคคลซึ่งจะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ในกรณีพิเศษ ซึ่งได้รับการยกเว้นตามหลักเกณฑ์ในการกำหนดคุณสมบัติของพนักงานเจ้าหน้าที่ตามปกติทั่วไป

เนื้อหาหลักสูตรที่อบรม :

ด้านแรก การอบรมด้านจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทและอำนาจหน้าที่ของพนักงานเจ้าหน้าที่

ลำดับ	เนื้อหาหลักสูตร (ความชำนาญเฉพาะทาง)
๑.	Using Computer Forensic Tools เช่น Encase, Forensics Toolkits, ILook
๒.	Using Network / Internet Forensic Tools เช่น Encase Field Intelligence Model (FIM)
๓.	Wireless Forensic Tools เช่น Netstumbler, Kismet, Aircrack
๔.	Using Handheld Forensics Tools (Cell & PDA) Paraben, MobilEdit, Vogon
๕.	Cryptology ได้แก่ Cryptography และ Cryptanalysis

ด้านที่สอง ความรู้พื้นฐานด้านการสืบสวนและสอบสวนเพื่อการบังคับใช้กฎหมาย (Law Enforcement)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑.	กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๒.	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๓.	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)
๔.	การสืบสวนทางเทคนิค เช่น การตรวจสอบหมายเลข IP Address หรือแหล่งที่มาของการกระทำความผิด การขอข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) จากผู้ให้บริการ การวิเคราะห์และเชื่อมโยงข้อมูล/ พยานหลักฐานข้างต้น
๕.	แนวทางปฏิบัติในการดำเนินคดี/การทำสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ (การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การรวบรวมพยาน หลักฐาน และแสวงหาข้อเท็จจริง การตรวจสถานที่เกิดเหตุ การยื่นคำร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน การเก็บรักษาพยานหลักฐาน การเก็บรักษาพยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการ การเปรียบเทียบปรับและการดำเนินคดี เป็นต้น
๖.	การบริหารจัดการคดีให้เป็นไปอย่างมีประสิทธิภาพ

ด้านที่สาม การพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑.	The needs for Computer Forensics
๒.	Principles of Computer Forensics and Digital/Electronic Evidence
๓.	Crime scene, Digital/Electronic Evidence and Chain of Custody
๔.	Capturing the Data Image and Volatile Data
๕.	Extracting Information from Captured Data
๖.	Breaking Password and Encryption
๗.	Using Computer Forensics Tools
๘.	Investigation and Interrogation
๙.	Digital/Electronic Evidence Analysis and Synthesis
๑๐.	Testify in Court, Admissibility requirements
๑๑.	Different between Computer Forensics and Network/Internet Forensics
๑๒.	Network/Internet Forensics
๑๓.	Using Network/Internet Forensics Tools

ประกาศกระทรวงเทคโนโลยีสารสนเทศ
และการสื่อสาร
เรื่อง กำหนดแบบบัตรประจำตัวพนักงานเจ้าหน้าที่
ตามพระราชบัญญัติว่าด้วยการกระทำความผิด
เกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ประกาศ
กระทรวงเทคโนโลยีสารสนเทศ และการสื่อสาร

เรื่อง กำหนดแบบบัตรประจำตัวพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

อาศัยอำนาจตามความในมาตรา ๓๐ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกำหนดแบบบัตรประจำตัวพนักงานเจ้าหน้าที่ไว้ ดังต่อไปนี้

ข้อ ๑ บัตรประจำตัวพนักงานเจ้าหน้าที่ให้มีพื้นสีขาว ขนาดและลักษณะตามแบบท้ายประกาศนี้

ข้อ ๒ ให้ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้ออกบัตรประจำตัวพนักงานเจ้าหน้าที่

ข้อ ๓ ให้พนักงานเจ้าหน้าที่ยื่นคำขอมีบัตรประจำตัว พร้อมกับแนบรูปถ่ายไม่เกินหกเดือนก่อนวันยื่นคำขอมีบัตร ขนาด ๒.๕ x ๓ เซนติเมตร ครึ่งตัว หน้าตรง ไม่สวมหมวก แต่งเครื่องแบบปฏิบัติราชการหรือเครื่องแบบพิธีการหรือแต่งกายสุภาพ จำนวน ๒ รูป ต่อสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ ๔ คำขอมีบัตรตามข้อ ๓ ให้เป็นไปตามแบบท้ายประกาศนี้

ข้อ ๕ บัตรประจำตัวตามประกาศนี้ ให้ใช้ได้สี่ปีนับแต่วันออกบัตร

ข้อ ๖ เมื่อได้ออกบัตรประจำตัวให้แก่ผู้ใด ให้ผู้ออกบัตรประจำตัวจัดให้มีสำเนาข้อความและรายการบัตรประจำตัวซึ่งติดรูปถ่ายของผู้นั้นไว้ด้วยหนึ่งฉบับ และเก็บไว้เป็นหลักฐานที่สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ ๗ การออกบัตรประจำตัว ในกรณีบัตรประจำตัวหมดอายุ สูญหายหรือชำรุดในสาระสำคัญ หรือผู้ถือบัตรประจำตัวนั้นได้ยายสังกัด ให้นำความในข้อ ๑ ข้อ ๒ ข้อ ๓ ข้อ ๔ ข้อ ๕ และข้อ ๖ มาบังคับใช้โดยอนุโลม

ข้อ ๘ ผู้ใดได้รับบัตรประจำตัวใหม่ หรือผู้ถือบัตรไม่มีสิทธิใช้บัตรประจำตัวนั้นต่อไป ให้คืนบัตรต่อสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารโดยพลัน ในวันที่ได้รับบัตรประจำตัวใหม่หรือไม่มีสิทธิใช้บัตรประจำตัวนั้น

ประกาศ ณ วันที่ ๒๑ สิงหาคม พ.ศ. ๒๕๕๐
นายสิทธิชัย โภไคยอุดม
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

แบบคำขอมีบัตรประจำตัวพนักงานเจ้าหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

เขียนที่.....

วันที่.....เดือน.....พ.ศ.....

ข้าพเจ้า.....เกิดวันที่.....เดือน.....พ.ศ.....

อายุ.....ปี เลขที่บัตรประจำตัวประชาชน.....

มีชื่ออยู่ในทะเบียนบ้านเลขที่.....ซอย.....ถนน.....

ตำบล/แขวง.....อำเภอ/เขต.....จังหวัด.....

รหัสไปรษณีย์.....โทรศัพท์.....โทรศัพท์มือถือ.....

ที่อยู่ตามภูมิลำเนา บ้านเลขที่.....ซอย.....ถนน.....

ตำบล/แขวง.....อำเภอ/เขต.....จังหวัด.....

รหัสไปรษณีย์.....

หน่วยงาน.....

ทำคำขอยื่นต่อปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อขอมีบัตรประจำตัวพนักงานเจ้าหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และได้แนบรูปถ่ายสองรูปมาพร้อมกับคำขอนี้แล้ว

ข้าพเจ้าขอรับรองว่าข้อความดังกล่าวข้างต้นเป็นความจริงทุกประการ

ลายมือชื่อ).....ผู้ทำคำขอ

(.....)

ลงชื่อ .....

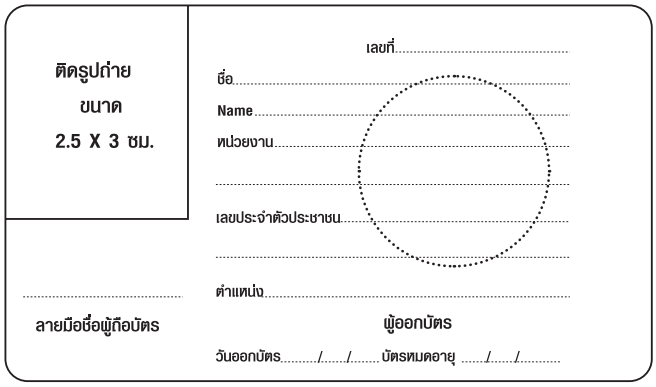
ตำแหน่ง.....

(ผู้บังคับบัญชา ผู้ให้ความยินยอม)

(...../...../.....)

แบบบัตรประจำตัวพนักงานเจ้าหน้าที่

ด้านหน้า



กว้าง 5.4 ซม.

ยาว 8.5 ซม.

ด้านหลัง

หมายเหตุ

(1) ด้านหน้าบัตรแสดงข้อมูลผู้ถือบัตรได้แก่ ชื่อ ชื่อภาษาอังกฤษ หมายเลขบัตรประจำตัวประชาชน ชื่อหน่วยงานต้นสังกัด ภาพถ่าย ลายมือชื่อผู้ถือบัตร และแสดงเลขที่บัตรพร้อมวันที่ออกและวันที่หมดอายุ

(2) ด้านหน้าบัตรมีตราครุฑสีแดง เป็นวงกลมสองวงซ้อนกัน ขนาดเส้นผ่าศูนย์กลาง 3.5 ซม. วงใน 2.5 ซม. ล้อมครุฑขนาดตัวครุฑ 2 ซม. ระหว่างวงนอกและวงในให้มีอักษรไทยระบุกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารอยู่ขอบล่างของตรา

(3) ด้านหลังมีแถบแม่เหล็กสำหรับบรรจุข้อมูล

(4) ด้านหลังระบุว่าเป็นบัตรประจำตัวพนักงานเจ้าหน้าที่ตามพระราชบัญญัติฯ

(5) ด้านหลังบัตรด้านล่างมีข้อความระบุว่าหากเก็บบัตรนี้ได้กรุณาส่งคืนกระทรวงฯ หรือโทร. 1111

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง แต่งตั้งพนักงานเจ้าหน้าที่ ตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. ๒๕๕๐

เพื่อให้การปฏิบัติและการดำเนินงานด้านการสืบสวนสอบสวน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เป็นไปด้วยความเรียบร้อย มประสิทธิภาพและสัมฤทธิ์ผลในทางปฏิบัติ

อาศัยอำนาจตามความในมาตรา ๒๘ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารจึงประกาศแต่งตั้งพนักงานเจ้าหน้าที่ ดังต่อไปนี้

๑. นายวรพัฒน์ ทิวถนอม
๒. นายอาจิน จิรชีพพัฒนา
๓. นายวินัย อยู่สบาย
๔. นายธนิต ประภาตนันท์
๕. นายอารีย์ จิวรรักษ์
๖. นายสมศักดิ์ ศุภจิราวัฒน์
๗. นายสุรชัย นิลแสง
๘. นายณัฐวุฒิ ภัทรประยูร
๙. นายไพรัช อิงคสิทธิ์
๑๐. นายสมญา พัฒนวรพันธ์
๑๑. นายจิโรภาส พูลสุวรรณ
๑๒. นายทรงกลด บ่ายเจริญ
๑๓. นายอิทธิฤทธิ์ ไชยขันธ์
๑๔. พันตำรวจโท วิวัฒน์ สิทธิสรเดช
๑๕. พันตำรวจโท อัยฎางค์ ม่วงศรี

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๓ สิงหาคม พ.ศ. ๒๕๕๐
สิทธิชัย โภไคยอุดม
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศ
และการสื่อสาร

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง แต่งตั้งพนักงานเจ้าหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (ฉบับที่ ๒)

เพื่อให้การปฏิบัติและการดำเนินงานด้านการสืบสวนสอบสวน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เป็นไปด้วยความเรียบร้อย มีประสิทธิภาพ และสัมฤทธิ์ผลในทางปฏิบัติ

อาศัยอำนาจตามความในมาตรา ๒๘ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงประกาศแต่งตั้งพนักงานเจ้าหน้าที่ ดังต่อไปนี้

๑. พันตำรวจเอก ญาณพล ยั่งยืน
๒. พันโท นราวิทย์ เปาอินทร์
๓. พันตำรวจโท ชาญชัย ลิขิตคันทะสร
๔. พันตำรวจโท ชาญชัย ยิ่งยง
๕. พันตำรวจตรี นิติ สัมฤทธิ์เดชขจร
๖. พันตำรวจโทหญิง พรรณทิพย์ เต็มเจริญ
๗. นางสาวสุรวรรณ บุญญาศิริรัตน์
๘. นายรองฤทธิ์ พุกกะเวส
๙. นายจิรโรจน์ นิราศนภาภัย
๑๐. นายลักษมณ์ เฉลิมชัย
๑๑. นายมงคล มีลุน
๑๒. นายธีรศักดิ์ มาตาเดิม
๑๓. นายปัญญา ว่องไว
๑๔. นางสาวศิริวรรณ เทพอารักษ์กุล
๑๕. นางศศินี ชื่นชม
๑๖. นางสาวศุภวรรณ ภู่ธนะพิบูล
๑๗. นายรัชพร วรอินทร์
๑๘. นางสาวกีรติ บุญโชติ
๑๙. นายกิตติ ศรีบุญญากร
๒๐. นายสถาพร สอนเสนา

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๙ กันยายน พ.ศ. ๒๕๕๐
สิทธิชัย โภไคยอุดม
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

(ร่าง)
กฎกระทรวงว่าด้วย
การยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ. ....

อาศัยอำนาจตามความในมาตรา ๔ มาตรา ๑๘ และมาตรา ๑๙ วรรค ๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ออกกฎกระทรวงไว้ ดังต่อไปนี้

ข้อ ๑ เมื่อศาลมีคำสั่งอนุญาตให้ยึดหรืออายัดระบบคอมพิวเตอร์แล้ว ก่อนทำการยึดหรืออายัดให้พนักงานเจ้าหน้าที่แสดงบัตรประจำตัว และส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ดำเนินการยึดหรืออายัดโดยให้เจ้าพนักงานตำรวจหรือพนักงานฝ่ายปกครองแห่งท้องที่นั้นมาร่วมเป็นพยานด้วย

ข้อ ๒ ให้พนักงานเจ้าหน้าที่ดำเนินการยึดหรืออายัดระบบคอมพิวเตอร์ได้ทุกวันในเวลาระหว่างพระอาทิตย์ขึ้นถึงพระอาทิตย์ตก เว้นแต่ในกรณีที่มีเหตุอันควรเชื่อได้ว่าหากไม่ดำเนินการทันที ระบบคอมพิวเตอร์นั้นจะสูญหายหรือถูกยักย้าย ให้มีอำนาจดำเนินการยึดหรืออายัดในเวลาอื่นได้

ข้อ ๓ ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการยึดหรืออายัด ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

ข้อ ๔ ให้พนักงานเจ้าหน้าที่ทำบัญชีแสดงรายละเอียดเกี่ยวกับระบบคอมพิวเตอร์ที่ตรวจยึดหรืออายัด เช่น ประเภทอุปกรณ์ ชนิด รุ่น หมายเลขเครื่อง(S/N) จำนวน โดยกรอกข้อมูลลงในแบบ ทก.ยค. ที่แนบท้ายกฎกระทรวงนี้ และให้ถ่ายสำเนาแบบนั้น ติดที่บรรจุภัณฑ์ ตามลำดับหมายเลขไว้และให้แสดงเครื่องหมายไว้ที่ระบบคอมพิวเตอร์นั้นให้เห็นเป็นที่ประจักษ์แจ้งว่าได้มีการยึดหรืออายัดแล้วตามวิธีที่เห็นสมควร

ข้อ ๕ เมื่อยึดหรืออายัดระบบคอมพิวเตอร์แล้ว ให้พนักงานเจ้าหน้าที่จัดการให้เจ้าของ หรือผู้ครอบครองระบบคอมพิวเตอร์นั้นลงลายมือชื่อรับรองในแบบ ทก.ยค. แนบท้ายกฎกระทรวงนี้ หากผู้นั้นไม่ยินยอมลงลายมือชื่อ หรือในกรณีที่ไม่มีบุคคลดังกล่าว

ให้จดแจ้งลงในแบบนั้น และให้เจ้าพนักงานตำรวจหรือพนักงานฝ่ายปกครองแห่งท้องที่นั้นลงลายมือชื่อรับรองแทน

ข้อ ๖ เมื่อยึดหรืออายัดระบบคอมพิวเตอร์แล้ว ให้พนักงานเจ้าหน้าที่จัดให้มีบรรจุภัณฑ์ที่เหมาะสมสำหรับการจัดเก็บระบบคอมพิวเตอร์นั้นเพื่อป้องกันความเสียหายและการเปลี่ยนแปลงของข้อมูลที่อาจเกิดขึ้น แล้วทำการปิดผนึก (Seal) ด้วยวัสดุที่สามารถป้องกันการเปิดบรรจุภัณฑ์โดยไม่ได้รับอนุญาตได้

ข้อ ๗ ในกรณีที่พนักงานเจ้าหน้าที่ดำเนินการยึดหรืออายัดระบบคอมพิวเตอร์ใดแล้วไม่สามารถขนย้ายมาเก็บรักษาไว้ ณ สำนักงาน หรือสถานที่เก็บรักษาได้ หรือระบบคอมพิวเตอร์นั้นมีสภาพไม่เหมาะสมที่จะนำมาเก็บรักษา ให้รายงานพนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าพร้อมเสนอความเห็นเพื่อพิจารณาสั่งการตามที่เห็นสมควร ในกรณีที่พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้ายังไม่สั่งการตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ผู้ดำเนินการยึดหรืออายัดนั้นจัดการเก็บรักษาทรัพย์สินไว้ตามที่เห็นสมควรไปพลางก่อน

ข้อ ๘ ในการดำเนินการยึดหรืออายัดระบบคอมพิวเตอร์ ให้พนักงานเจ้าหน้าที่มีหนังสือแจ้งแก่เจ้าของ ผู้มีสิทธิหรือผู้ครอบครองระบบคอมพิวเตอร์นั้น

ข้อ ๙ ถ้ามูลค่าแห่งระบบคอมพิวเตอร์ที่ได้ยึดหรืออายัดไว้นั้น ต้องเสื่อมเสียไปเพราะความผิดของบุคคลภายนอกเนื่องจากการไม่ปฏิบัติตามคำสั่งยึดหรืออายัดไม่ว่าด้วยประการใด ๆ ให้พนักงานเจ้าหน้าที่ เรียกให้บุคคลภายนอกนั้นรับผิดชดใช้ค่าสินไหมทดแทนเพื่อความเสียหายใดๆ อันเกิดขึ้นแต่การนั้น

ให้ไว้ ณ วันที่ พ.ศ. ....

(นายสิทธิชัย โภไคยอุดม)
รัฐมนตรีว่าการ
กระทรวงเทคโนโลยีสารสนเทศ
และการสื่อสาร