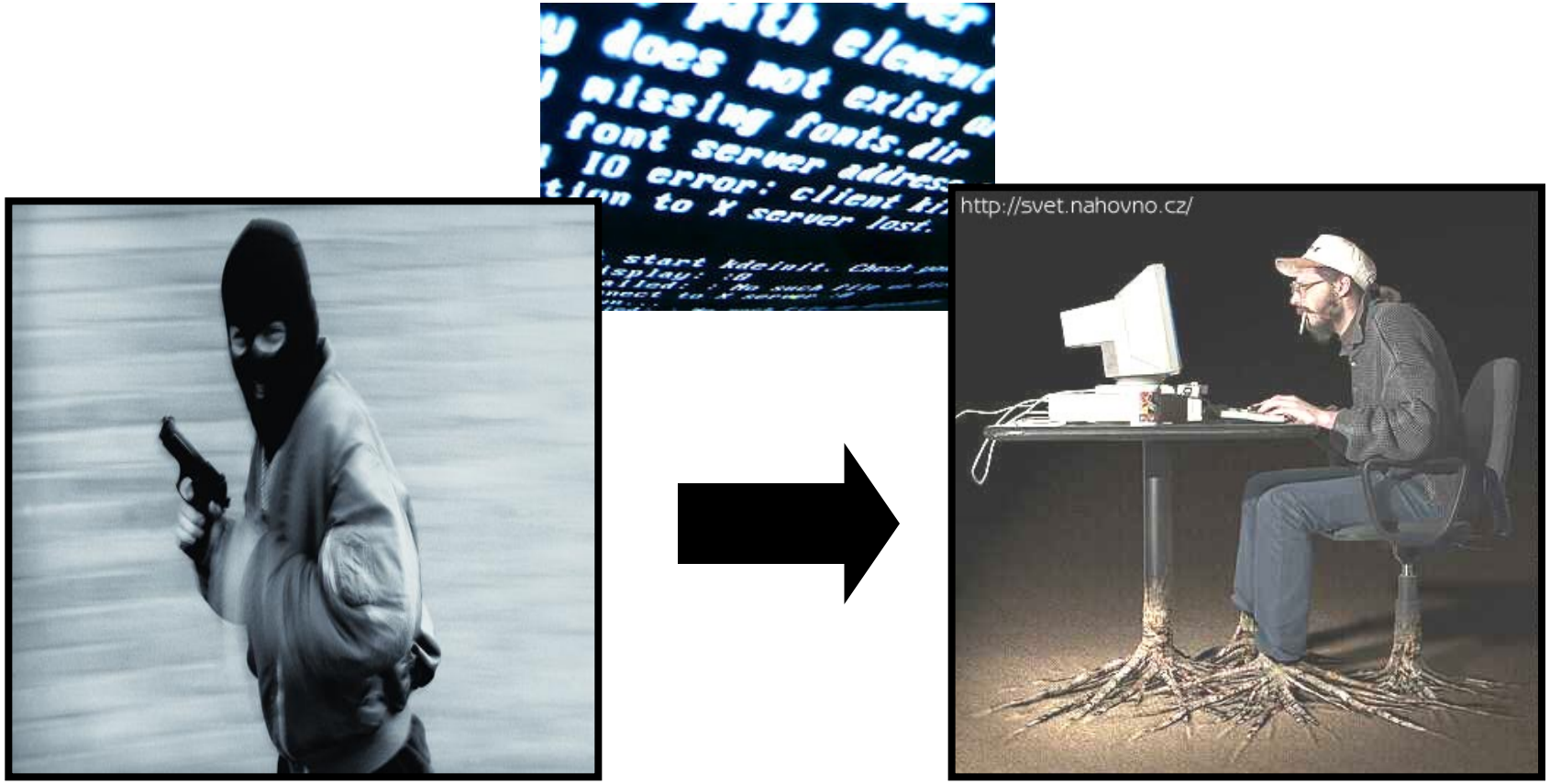
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ 2550

การเปลี่ยนรูปแบบการกระทำความผิด

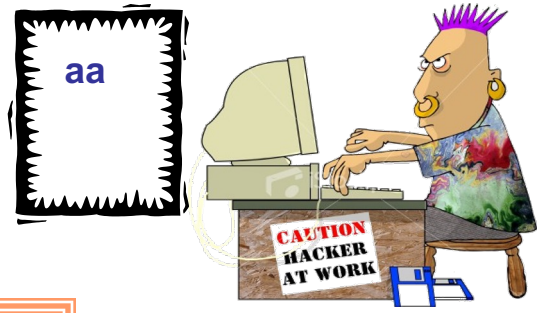


ยุคเก่า

ยุคปัจจุบัน

การกระทำความผิดตามมาตราต่างๆ

การแอบเข้าถึงข้อมูลคอมพิวเตอร์
มาตรา ๗

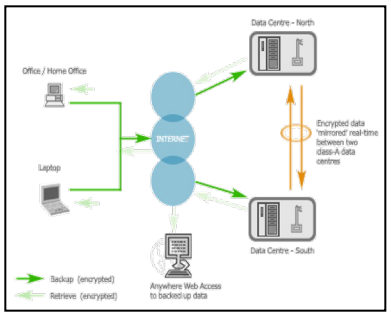


การดักข้อมูลคอมพิวเตอร์
มาตรา ๘

แอบเข้าไปในระบบคอมพิวเตอร์ &
แอบรู้มาตรการป้องกันระบบคอมพิวเตอร์
(ขโมย password)
มาตรา ๕ และ
มาตรา ๖

การรบกวน/
แอบแก้ไขข้อมูล
มาตรา ๙

การรบกวนระบบคอมพิวเตอร์
มาตรา ๑๐



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

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

คำนิยาม ม.๓

- ระบบคอมพิวเตอร์
- ข้อมูลคอมพิวเตอร์
- ข้อมูลจราจรทางคอมพิวเตอร์
- ผู้ให้บริการ
- ผู้ใช้บริการ
- พนักงานเจ้าหน้าที่
- รัฐมนตรี

หมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์

กระทำต่อคอมพิวเตอร์

- ม.๕ การเข้าถึงระบบคอมฯ
- ม.๖ การล่วงรู้มาตรการการป้องกันการเข้าถึง
- ม.๗ การเข้าถึงข้อมูลคอมฯ
- ม.๘ การดักรับข้อมูลคอมฯ
- ม.๙ การรบกวนข้อมูลคอมฯ
- ม.๑๐ การรบกวนระบบคอมฯ
- ม.๑๓ การจำหน่าย/ เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด

ม.๑๒ บทหนัก

ใช้คอมพิวเตอร์กระทำความผิด

- ม.๑๑ Spam mail
- ม.๑๔ การปลอมแปลงข้อมูลคอมพิวเตอร์/ เผยแพร่เนื้อหาอันไม่เหมาะสม
- ม.๑๕ ความรับผิดของผู้ให้บริการ
- ม.๑๖ การเผยแพร่ภาพจากการตัดต่อ/ดัดแปลง

มีผลบังคับใช้ภายหลังประกาศใช้ ๓๐ วัน (ม.๒)

การกระทำผิดนอกราชอาณาจักร รับโทษในราชอาณาจักร (ม.๑๗)

การรับฟังพยานหลักฐานที่ได้มาตาม พ.ร.บ. ฉบับนี้ (ม. ๒๕)

หมวด ๒ พนักงานเจ้าหน้าที่

พนักงานเจ้าหน้าที่

อำนาจหน้าที่ (ม.๑๘) (๑) มีหนังสือ/เรียกเพื่อให้ถ้อยคำ/เอกสาร (๒) เรียกข้อมูลจราจร (๓) สั่งให้ส่งมอบข้อมูลที่อยู่ในครอบครอง (๔) ทำสำเนาข้อมูล (๕) สั่งให้ส่งมอบข้อมูล/อุปกรณ์ (๖) ตรวจสอบ/เข้าถึง (๗) ถอดรหัสลับ (๘) ยึด/อายัดระบบ

การตรวจสอบการใช้อำนาจ (ม.๑๙) ยื่นคำร้องต่อศาลในการใช้อำนาจตามม.๑๘ (๔)-(๘),ส่งสำเนาบันทึกรายละเอียดให้แก่ศาลภายใน ๔๘ ชม., ยึด/อายัดห้ามเกิน ๓๐ วัน ขอขยายได้ ๖๐ วัน (ม.๑๘(๘))

การ block เว็บไซต์ โดยความเห็นชอบของ รมว.ทก.ยื่นคำร้องต่อศาล, ห้ามจำหน่าย/เผยแพร่ malicious code (ม.๒๐-ม.๒๑)

ความรับผิดของพนักงานเจ้าหน้าที่: (ม. ๒๒ ถึง มาตรา ๒๔)

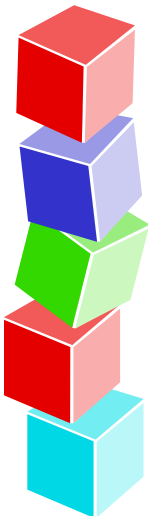
พยานหลักฐานที่ได้มาโดยมิชอบ อ้างและรับฟังมิได้ (ม.๒๕)

การแต่งตั้ง/กำหนดคุณสมบัติพนักงานเจ้าหน้าที่/การประสานงาน (ม.๒๘-๓๐)

ผู้ให้บริการ

ม.๒๖ เก็บข้อมูลจราจร ๙๐ วันไม่เกิน ๑ ปี

ม.๒๗ ไม่ปฏิบัติตามคำสั่งพนักงานเจ้าหน้าที่หรือคำสั่งศาล ระวางโทษปรับ



บทกำหนดโทษ

ฐานความผิด	โทษจำคุก	โทษปรับ
มาตรา ๕ เข้าถึงคอมพิวเตอร์โดยมิชอบ	ไม่เกิน ๖ เดือน	ไม่เกิน ๑๐,๐๐๐ บาท
มาตรา ๖ ล่วงรู้มาตรการป้องกัน	ไม่เกิน ๑ ปี	ไม่เกิน ๒๐,๐๐๐ บาท
มาตรา ๗ เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ	ไม่เกิน ๒ ปี	ไม่เกิน ๔๐,๐๐๐ บาท
มาตรา ๘ การดักข้อมูลคอมพิวเตอร์	ไม่เกิน ๓ ปี	ไม่เกิน ๖๐,๐๐๐ บาท
มาตรา ๙ การรบกวนข้อมูลคอมพิวเตอร์	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๐ การรบกวนระบบคอมพิวเตอร์ มาตรา ๑๑ สแปมเมล์	ไม่เกิน ๕ ปี ไม่มี	ไม่เกิน ๑๐๐,๐๐๐ บาท ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๒ การกระทำต่อความมั่นคง (๑) ก่อความเสียหายแก่ข้อมูลคอมพิวเตอร์ (๒) กระทบต่อความมั่นคงปลอดภัยของประเทศ/เศรษฐกิจ วรรคท้าย เป็นเหตุให้ผู้อื่นถึงแก่ชีวิต	ไม่เกิน ๑๐ ปี ๓ ปี ถึง ๑๕ ปี ๑๐ ปี ถึง ๒๐ ปี	+ ไม่เกิน ๒๐๐,๐๐๐ บาท ๖๐,๐๐๐-๓๐๐,๐๐๐ บาท ไม่มี
มาตรา ๑๓ การจำหน่าย/เผยแพร่ชุดคำสั่ง	ไม่เกิน ๑ ปี	ไม่เกิน ๒๐,๐๐๐ บาท
มาตรา ๑๔ การเผยแพร่เนื้อหาอันไม่เหมาะสม	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๕ ความรับผิดของ ISP	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๖ การตัดต่อภาพผู้อื่น ถ้าสุจริต ไม่มีความผิด	ไม่เกิน ๓ ปี	ไม่เกิน ๖๐,๐๐๐ บาท

รูปแบบการกระทำความผิด (๑)

ฐานความผิด	ตัวอย่าง รูปแบบการกระทำความผิด	ตัวอย่างผลกระทบต่อ ความมั่นคงปลอดภัย (Information Security) & ความเสียหาย
มาตรา ๕ เข้าถึงระบบคอมพิวเตอร์ มาตรา ๖ เปิดเผยมาตรการป้องกันระบบ มาตรา ๗ เข้าถึงข้อมูลคอมพิวเตอร์ มาตรา ๘ ดักรับข้อมูลคอมพิวเตอร์	**สปายแวร์ (Spyware)** **สนิฟเฟอร์ (Sniffer)**	- การสอดแนมข้อมูลส่วนตัว - การแอบดักฟัง packet
มาตรา ๙ รบกวน/ทำลายข้อมูลคอมพิวเตอร์ มาตรา ๑๐ รบกวน/ทำลายระบบคอมพิวเตอร์	**การใช้ชุดคำสั่งในทางมิชอบ (Malicious Code) เช่น Viruses, Worms, Trojan Horses**	- การตั้งเวลาให้โปรแกรมทำลายข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ - การทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม หรือหยุดทำงาน (Denial of Service)
มาตรา ๑๑ สแปมเมล์	**การทำสแปม (Spamming)**	-รบกวนการใช้ระบบคอมพิวเตอร์ตามปกติ อาจถึงขั้นทำให้เป็น Zombie
มาตรา ๑๒ เหตุฉกรรจ์ อันเกิดจากการกระทำข้างต้น	**BOT หรือ BOTNET**	- ผลกระทบต่อความมั่นคงปลอดภัยของประเทศ หรือทางเศรษฐกิจ -ความปลอดภัยสาธารณะ -การบริการสาธารณะ -อาจเกิดสงครามข้อมูลข่าวสาร (Information Warfare)

รูปแบบการกระทำความผิด (๒)

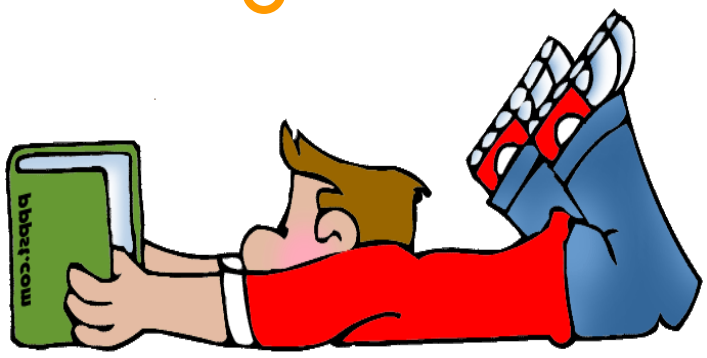
ฐานความผิด	ตัวอย่าง รูปแบบการกระทำความผิด	ตัวอย่างผลกระทบต่อความมั่นคงปลอดภัย (Information Security) & ความเสียหาย
มาตรา ๑๓ การจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์	**Hacking Tools**	- การสอดแนมข้อมูลส่วนตัว - การแอบดักฟัง packet
มาตรา ๑๔ การนำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ปลอม, เท็จ หรือไม่เหมาะสม หรือการส่งต่อข้อมูล (forward) นั้น	**การใช้ชุดคำสั่งในทางมิชอบ (Malicious Code) เช่น Viruses, Worms, Trojan Horses, Phishing**	- การตั้งเวลาให้โปรแกรมทำลายข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ - การทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม หรือหยุดทำงาน (Denial of Service)
มาตรา ๑๕ ความรับผิดฐานสนับสนุนการกระทำความผิดของผู้ให้บริการ	**การโพสต์หรือนำเข้าข้อมูลคอมพิวเตอร์ตามมาตรา ๑๔**	ความเสียหายกับบุคคลอื่น
มาตรา ๑๖ การตัดต่อภาพ เป็นเหตุให้ถูก ดูหมิ่น ถูกเกลียดชัง หรืออับอาย	**การตัดต่อภาพ**	ผู้ถูกกระทำถูกดูหมิ่น ถูกเกลียดชัง หรืออับอาย

ตัวอย่างรูปแบบการกระทำความผิดทางคอมพิวเตอร์

มาตรา 5 + มาตรา 7
การเข้าถึงระบบคอมพิวเตอร์+ข้อมูลคอมพิวเตอร์

กรณีไหนบ้างถือว่าเป็นการเข้าถึงคอมพิวเตอร์ครับ?

- **เข้าถึงโดยมิชอบ (illegal Access)**
- **ระบบคอมพิวเตอร์/ข้อมูลคอมพิวเตอร์**
- **ที่มีมาตรการป้องกันโดยเฉพาะ**
  - **ตั้ง Password**
  - **ตรวจสอบลายนิ้วมือ**



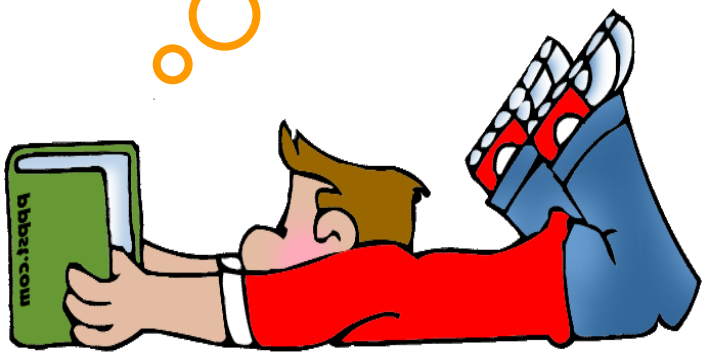
HACK IS A CRIME

มาตรา 6
เปิดเผยมาตรการป้องกันระบบ

รู้มาตรการป้องกัน
แล้วนำไปเปิดเผย

หากรู้วิธีการเข้าถึงระบบคอมพิวเตอร์ของคนอื่นแล้วนำไปบอกคนอื่นจะผิดหรือไม่ ?

- รู้มาตรการป้องกันการเข้าถึง
- ระบบคอมพิวเตอร์
- นำมาตรการดังกล่าวไปเปิดเผย

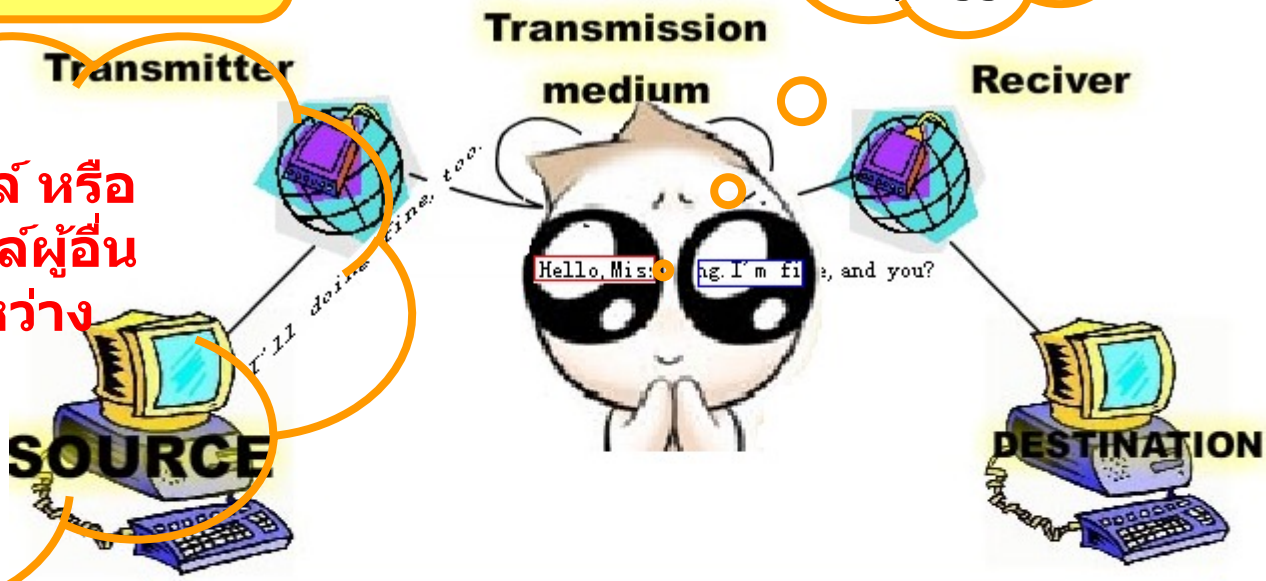


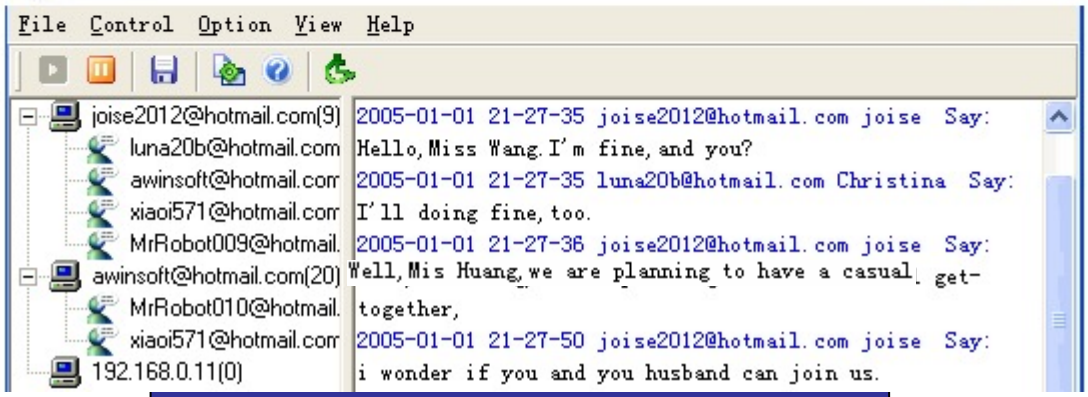
รู้ password เพื่อนโดยบังเอิญ แล้วเอาไปโพสต์ในเว็บ บอกรหัสผ่าน เข้าเล่นเกมส์ออนไลน์แก่เพื่อน

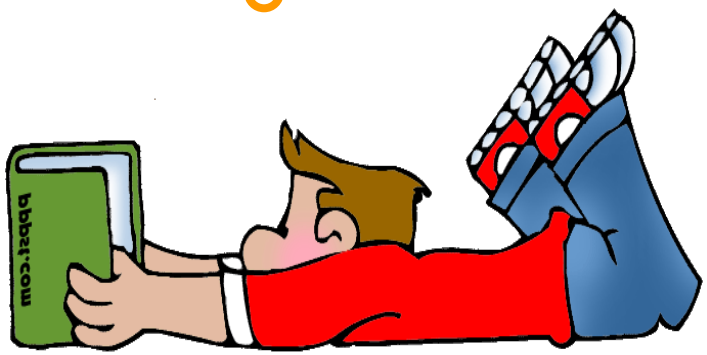
มาตรา 8
ดักรับข้อมูลคอมพิวเตอร์

Spyware
Sniffer
Keylogger

อยากรู้ว่าคนอื่นส่งเมล์ หรือข้อมูล อะไรเลยดักเมล์ผู้อื่นในขณะที่กำลังส่งระหว่างกันผิดหรือไม่?



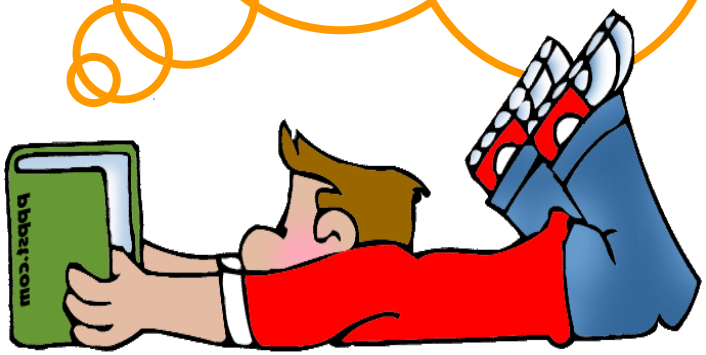




มาตรา 9+10
รบกวน/ทำลาย
ข้อมูลหรือระบบคอมพิวเตอร์

Viruses,
Worms,
Trojan Horses

การเข้าไปลบหรือเขียนเพิ่มเติม
ข้อมูลคอมพิวเตอร์ของคนอื่นผิดหรือไม่ ?
ทำให้เสียหาย /ทำลาย
แก้ไข /เปลี่ยนแปลง
ข้อมูลหรือระบบ
คอมพิวเตอร์ของผู้อื่น

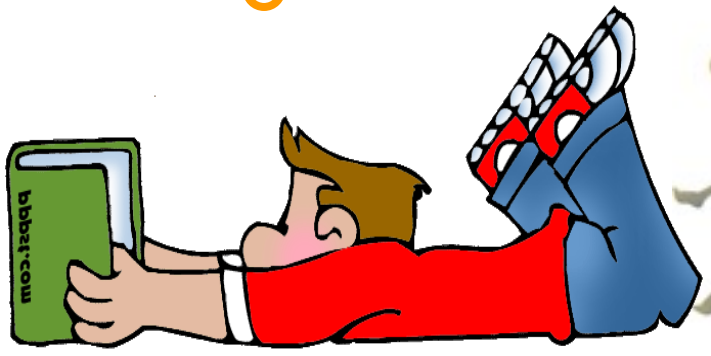


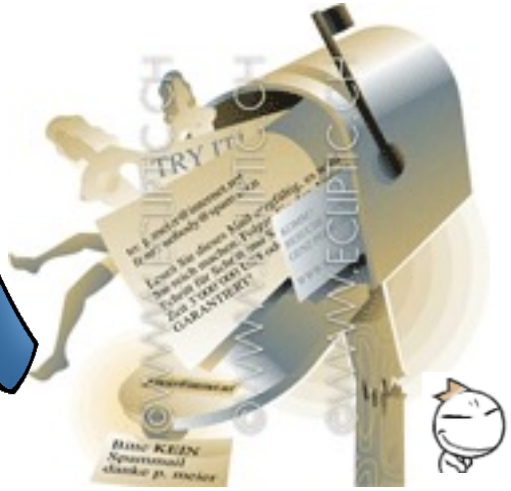
อย่าลบหรือแก้ไขข้อมูลในคอมคนอื่นซี้ซั้วขอรับ

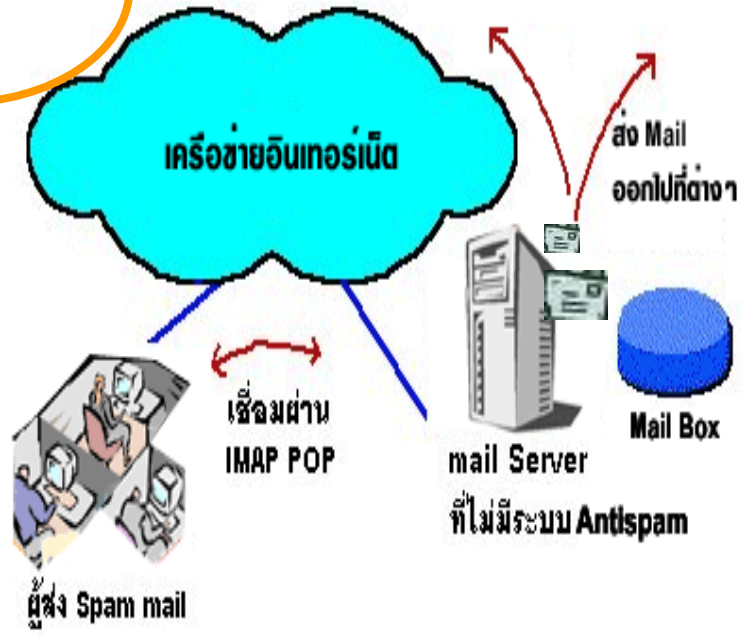
Denial of service attack: DoS คือ การทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม หรือหยุดทำงาน

มาตรา 11
ส่ง Spam mail

- ส่งข้อมูลคอมพิวเตอร์/ e-Mail
- โดยปกปิด/ ปลอมแปลงแหล่งที่มาหรือผู้ส่ง
- ทำให้ระบบคอมพิวเตอร์ของผู้อื่นใช้งานไม่ได้ หรือใช้งานได้ช้า



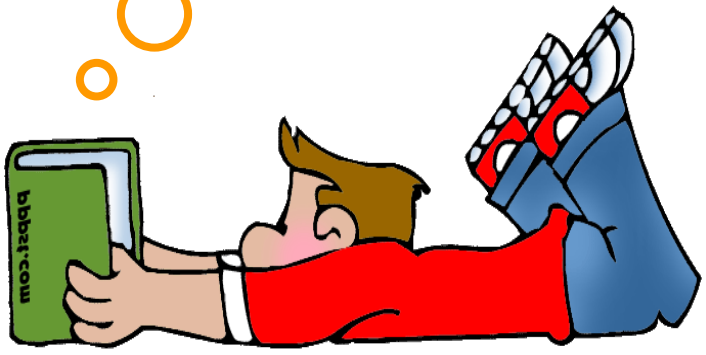


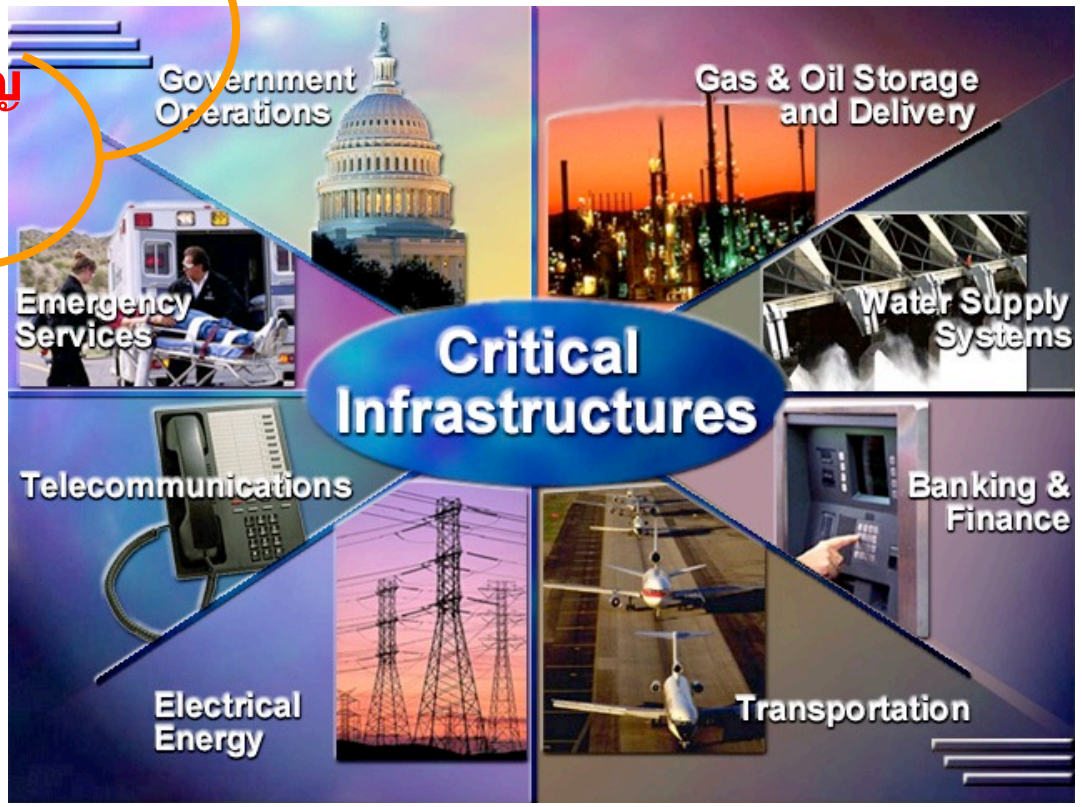


มาตรา 12
การทำความผิด
ต่อระบบโครงสร้างพื้นฐาน

- ทำความผิดตามมาตรา 9 และ 10
- ทำความเสียหายต่อประชาชน
- ทำความเสียหายต่อ

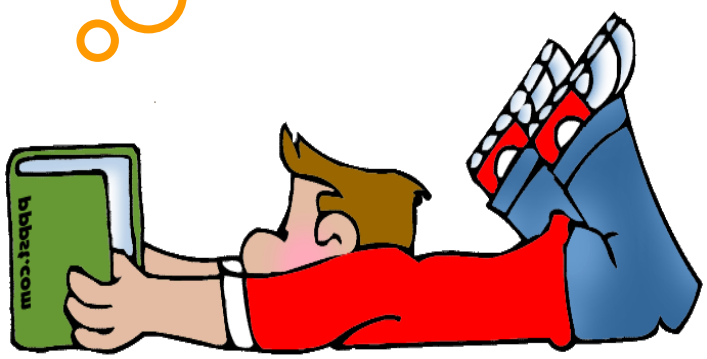
ระบบโครงสร้างพื้นฐานสำคัญ เช่น ไฟฟ้า, ประปา, Banks





มาตรา 13
จำหน่าย/เผยแพร่ชุดคำสั่ง ที่ใช้ในการกระทำความผิด

คนที่ขาย แจก หรือ เผยแพร่ **Hardware** หรือ **Software** ที่ใช้ในการกระทำความผิดได้ไหมครับ ?

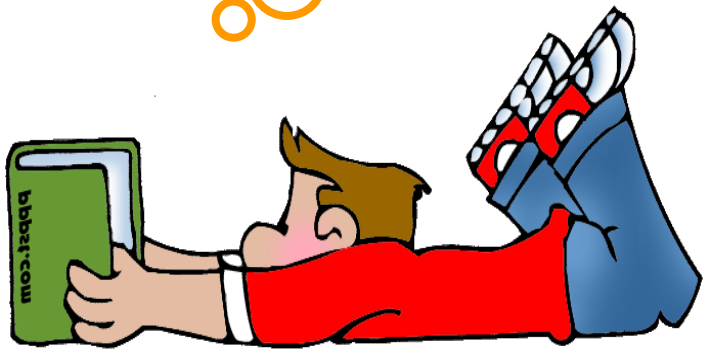


ขาย CD สอนป้องกันแฮคเกอร์ และสอนเขียนโปรแกรม

ขาย แจก หรือ เผยแพร่ Hardware หรือ Software ที่ใช้ในการกระทำความผิด ถือว่ามีส่วนช่วยให้คนอื่นทำผิด ก็ไม่รอดหรอก จะบอกให้

มาตรา 14
การเผยแพร่เนื้อหาที่ไม่เหมาะสม

- สร้างข่าวลือทำให้ผู้อื่นเสียหาย
- กระทบต่อความมั่นคง
- กล่าวว่าร้ายสถาบันกษัตริย์ การเผยแพร่ความคิดการก่อการร้าย การก่อกบฏ
- Forward Mail รูปลามก คลิปฉาว



อ๊ะอ๊ะ ดูได้ อ่านได้ เก็บได้ แต่อย่าเขียน โพสต์ หรือ ส่งต่อนะจะบอกให้

มาตรา 14 ว่าด้วยเรื่องไม่จริง เรื่องโป้ปดมดเท็จ เรื่องความมั่นคง และเรื่องลามก

ขี้จุ๊ เบบี้ ขี้จุ๊ ตาลาลา
ขี้ฮก เบบี้ ขี้ฮก ตาลาลา

เรื่องไม่จริง

ฟ้าถล่มแล้วจ้า
หนีเร็ว

เรื่องโป้ปดมดเท็จ

ภาพลามก

ความมั่นคงของประเทศ และก่อการร้าย

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ
โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือ
ก่อให้เกิดความตื่นตระหนกแก่ประชาชน

การติดต่อสื่อสาร

การทหาร

การเมืองการปกครอง

การป้องกันภัยสาธารณะ

ความมั่นคง
ของประเทศ

การต่างประเทศ

การคมนาคม

การพลังงาน

การสาธารณสุข

การเงิน

ก่อให้เกิดความตื่นตระหนกแก่ประชาชน

เกิดโรคระบาด

อาหารจะขาดแคลน

จะปลดคนงาน

เกิดการปฏิวัติ

เกิดภัยพิบัติ

หุ้นจะตก

การเข้าถึงคอมพิวเตอร์โดยมิชอบ

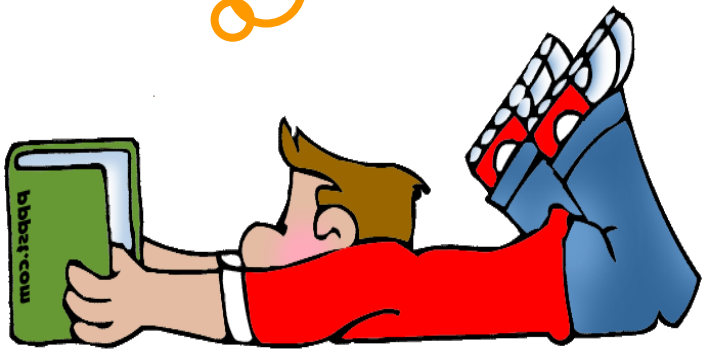
เช่น การเจาะระบบทั้งแบบ hacking และ cracking การบุกรุกทางคอมพิวเตอร์ เพื่อทำลายระบบคอมพิวเตอร์ หรือเปลี่ยนแปลงแก้ไขข้อมูล หรือเข้าถึงข้อมูลที่ได้มีการเก็บรักษาเป็นความลับ เช่น รหัสผ่าน (password) หรือความลับทางการค้าที่อาจะเป็นที่มาของการใช้คอมพิวเตอร์เพื่อฉ้อโกงหรือปลอมแปลงเอกสารที่อาจก่อให้เกิดความเสียหายต่อเนื่องเป็นมูลค่ามหาศาลได้

ภาพลามกอนาจารคืออะไร

ภาพนี้ลามกหรือไม่?

มาตรา 16
โชว์ภาพตัดต่อของคนอื่น

- โชว์ภาพของผู้อื่นในคอมพิวเตอร์
- เป็นภาพที่ทำเอง ตัดต่อ หรือ เพิ่มสัดส่วน
- ทำด้วยคอมพิวเตอร์/อิเล็กทรอนิกส์
- ทำให้คนนั้นอับอาย/เสียชื่อเสียง ถูกเกลียดชัง



มาตรการที่พึงดำเนินการ

มาตรการส่วนบุคคล

- ควรกำหนด Password ในการใช้ระบบคอมพิวเตอร์โดยกำหนดอย่างน้อย 8 ตัว และเปลี่ยนเป็นระยะๆ
- ลง & Update โปรแกรม Anti-Virus
- ไม่โพสต์หรือส่งต่อ Contents ไม่เหมาะสม
- ไม่ตัดต่อภาพที่อาจเป็นเหตุให้ผู้อื่นอับอาย
- ควรตรวจสอบการบังคับใช้กฎหมายของพนักงานเจ้าหน้าที่/พนักงานสอบสวนว่า กำลังใช้อำนาจตามกฎหมายใด

1) กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

2) กฎหมายอาญา – บัตรอิเล็กทรอนิกส์

3) กฎหมายทรัพย์สินทางปัญญา – ลิขสิทธิ์, เครื่องหมายการค้า

มาตรการเชิงนโยบายระดับองค์กร

- การจัดทำนโยบายด้านความมั่นคงปลอดภัย (ICT Security Policy)
- การจัดทำ Code of Conduct/Best Practices
- ควรมีการ Monitor และ Patch หรือ Harden ระบบ
- ควรมีการตั้งคณะทำงานกำกับหรือติดตามดูแลการปฏิบัติตามกฎหมาย, นโยบาย และ Code of Conduct/Best Practices
- ควรตรวจสอบการบังคับใช้กฎหมายของพนักงานเจ้าหน้าที่/พนักงานสอบสวนว่า กำลังใช้อำนาจตามกฎหมายใด

1) กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

2) กฎหมายอาญา – บัตรอิเล็กทรอนิกส์

3) กฎหมายทรัพย์สินทางปัญญา – ลิขสิทธิ์, เครื่องหมายการค้า

10 อย่าง....อย่าทำ

ถ้าไม่มีหน้าที่หรือ
ไม่ได้รับอนุญาต

1. อย่า..เข้าระบบที่คนอื่นตั้ง password ไว้
2. อย่า..เอามาตรการป้องกันการแก้ไข password ที่คนอื่นตั้งไว้ไปเผยแพร่
3. อย่า..เข้าไปดูหรือเข้าไปเอาข้อมูลของผู้อื่นที่มีมาตรการรักษาความปลอดภัย
4. อย่า..ใช้ sniffer ดัก E-mail คนอื่น
5. อย่า..ลองวิชาด้วยการรบกวนระบบคอมพิวเตอร์หรือข้อมูลผู้อื่น
6. อย่า..สร้างเมล์เท็จเพื่อให้ผู้อื่นแตกตื่นตกใจ
7. อย่า..ร้อนวิชาด้วยการรบกวนระบบโครงสร้างสำคัญของประเทศ
8. อย่า..เผยแพร่เน็ตที่เป็นภาพลามกหรือเป็นภัยต่อความมั่นคงของประเทศ
9. อย่า..ตัดต่อภาพเพื่อให้ผู้อื่นอับอาย
10. อย่า..เผยแพร่โปรแกรมสำหรับใช้กระทำความผิด

10 ข้อแนะนำ...ควรทำ

1. **เปลี่ยน**..password ทุกๆ 3 เดือน
2. **ไม่แชร์**..password กับผู้อื่น
3. **ใช้**..password เสร็จต้องออกจากโปรแกรมทันที
4. **ตั้ง**..ระบบป้องกันการเจาะข้อมูล
5. **เก็บรักษา**..ข้อมูลของตนอย่างดีและต้องไม่ให้ข้อมูลส่วนตัวกับผู้อื่น
6. **อ่าน**..เงื่อนไขให้ละเอียดก่อนดาวน์โหลดโปรแกรม
7. **แจ้ง**..พนักงานเจ้าหน้าที่เมื่อพบเจอการกระทำความผิด
8. **บอกต่อ**..คนใกล้ชิด เช่น เพื่อน คนในครอบครัว ให้ใช้อินเทอร์เน็ตอย่างระมัดระวัง
9. **ไม่ใช้**..โปรแกรมที่ผิดกฎหมาย
10. **ไม่**..หลงเชื่อโฆษณาหรือเนื้อหาในเว็บไซต์ที่ไม่เหมาะสม จนอาจถูกหลอกได้

อย่าใจอ่อน (ง่าย) อย่าไว้ใจคนแปลกหน้า อย่าโลภ อย่าหมกมุ่น อย่ารั้น อย่าคิดว่าไม่มีใครรู้

แหล่งข้อมูลอ้างอิง

- หนังสือความรู้เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
- เอกสารประกอบการบรรยาย โดยฝ่ายศึกษาวิจัยประเด็นด้านจริยธรรม กฎหมาย และผลกระทบทางสังคมของเทคโนโลยีสารสนเทศ (ELS) ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ค้นรายละเอียดเพิ่มเติมได้ที่

- **http://wiki.nectec.or.th/**
- **http://www.nectec.or.th/**
- **http://www.mict.go.th/**
- **http://www.dsi.go.th/**
- **http://www.royalthaipolice.go.th**