กฎหมายเทคโนโลยีสารสนเทศ : กฎหมายอาชญากรรมทางคอมพิวเตอร์

Unit 5

กฎหมายอาชญากรรมทางคอมพิวเตอร์

- กฎหมายอาชญากรรมทางคอมพิวเตอร์ (Computer Crime Law) เป็นการกำกับดูและควบคุมความสงบสุขของระบบสารสนเทศเพื่อสร้างความเชื่อมั่น และความปลอดภัย ในเรื่องของสิทธิ์การใช้ การละเมิด และผู้บุกรุก
- กฎหมายอาชาญากรรมทางคอมพิวเตอร์ค่อนข้างล่าช้าในการออกกฎหมายมาจากหลายสาเหตุ
  1) จะต้องดูตัวอย่างกฎหมายจากหลายๆประเทศที่บังคับใช้ไปก่อนแล้ว
  2) การคัดลอกกฎหมายไม่สามารถคัดลอกมาพูดได้ เนื่องจากต้องปรับให้เหมาะแก่ประเทศไทยและคำนึกถึงวัฒนธรรม คำนึกถึงความเท่าเทียมกันของประชาชน
  3) อีกสาเหตุด้วยหน่วยงานราชการที่ซับซ้อนหลายหน่วยงานมีขั้นตอนระเบียบปฏิบัติหลายขั้นตอน รวมทั้งการพิจารณาของระบบรัฐสภาด้วย
- บางเรื่องต้องใช้เวลานานถึง 5 ปีกว่าจะออกมาใช้บังคับได้ บางเรื่องใช้เวลาถึง 10 ปีเลยทีเดียว

การบัญญัติกฎหมายอาชยากรรมคอมพิวเตอร์

มี 2 วิธี ขึ้นอยู่ว่าต่างประเทศจะเลือกแบบใด

- เลือกที่จะแก้ไขประมวลกฎหมายอาญาเพื่อให้รับผิดแบบใหม่ เพื่อกำหนดฐานความผิดและการลงโทษที่รองรับแบบใหม่ได้ และเพื่อให้มีความเหมาะสมและปรับเข้ากับผู้กระทำความผิดได้ เช่น เยอรมัน อิตาลี สวิสเซอร์แลนด์
- มีการบัญญัติกำหนดไว้เป็นการเฉพาะ เช่น อังกฤษ สิงคโปร์ มาเลเซีย สหรัฐอเมริกา และ ไทย (รูปแบบต่างกันในแต่ละประเทศ แต่ฐานความผิดมีความใกล้เคียงกัน)

เพิ่มเติม

- หลักกฎหมายถ้าไม่มีโทษจะไม่มีกฎหมาย
- กฎหมายอาญามุ่งคุ้มครองเฉพาะวัตถุที่มีรูปร่างเท่านั้น (วัตถุทางกฎหมาย หมายถึง สิ่งที่มีราคาและยึดถือได้)
- สื่อไอทีไม่ได้อยู่ในแผ่นกระดาษ ดังนั้นกฎหมายอาญาที่มีอยู่จึงไม่สามารถขยายความคุ้มครองที่เป็นอยู่ได้ทั้งหมด ตัวอย่าง

  1) การโจรกรรมเงินในบัญชีลูกค้าในธนาคาร 2) การโจรกรรมความลับของบริษัทต่าง ๆ 3) การปล่อยไวรัสเข้าไปยังคอมพิวเตอร์ 4) การใช้คอมพิวเตอร์ปลอมแปลงเอกสารต่าง ๆ

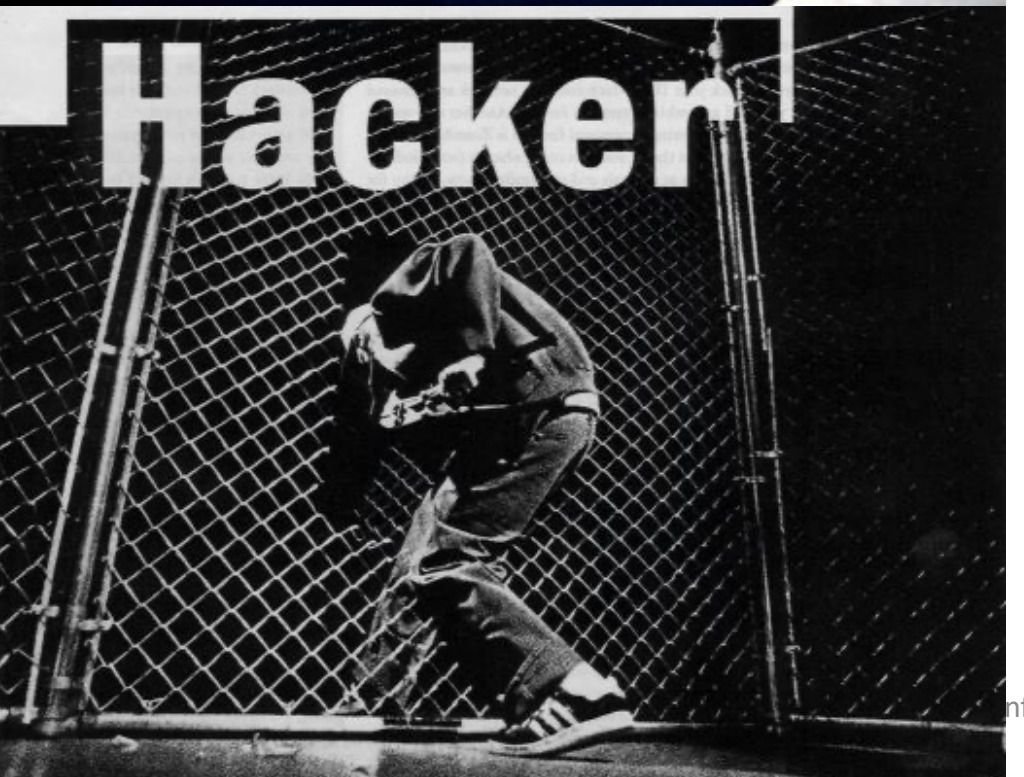
การใช้คอมพิวเตอร์ในการก่อวินาศกรรม

- ที่ต้องมีความผิดทางอาญา เนื่องจากต้องมีพยานหลักฐานเพื่อความผิดทางคอมพิวเตอร์มีการเปลี่ยนแปลงได้ตลอดเวลาและเปลี่ยนแปลงได้ง่าย จึงเป็นการยากต่อการหาพยานหลักฐาน
- เช่น ข้อมูลที่ถูกบันทึกอยู่ในสื่อบันทึกข้อมูลถาวรของเครื่องคอมพิวเตอร์ฮาร์ดิสหากเคลื่อนย้ายได้รับการกระเทียนจะทำให้สูญหายได้
- ดังนั้น หากต้องการสืบหลักฐานจากเครื่องคอมพิวเตอร์ฮาร์ดิส ต้องให้ศาลออกหมายค้นเพื่อเป็นพยานหลักฐาน
- ในประเทศไทยอายุของผู้กระทำความผิด หากเป็นเด็ก (เด็ก = ต่ำกว่า 7 ปี , เยาวชน = อายุไม่เกิน 18 ปี) จะขึ้นศาลเยาวชน เนื่องจากว่าทำไปด้วยความอยากรู้อยากลอง กฎหมายจึงกำหนดโทษดังนี้
  - ไม่จำคุก / มีคุมประพฤติ (สามารถรอการกำหนดโทษเหมือนไม่มีโทษ)
  - รอการลงโทษ (มีโทษแต่รอ) / ลงโทษ (ถ้าทำผิดอีกในระหว่างรอให้เพิ่มโทษ)

ผู้กระทำความผิดทางกฎหมายอาชญากรรมทางคอมพิวเตอร์

Hacker vs Cracker

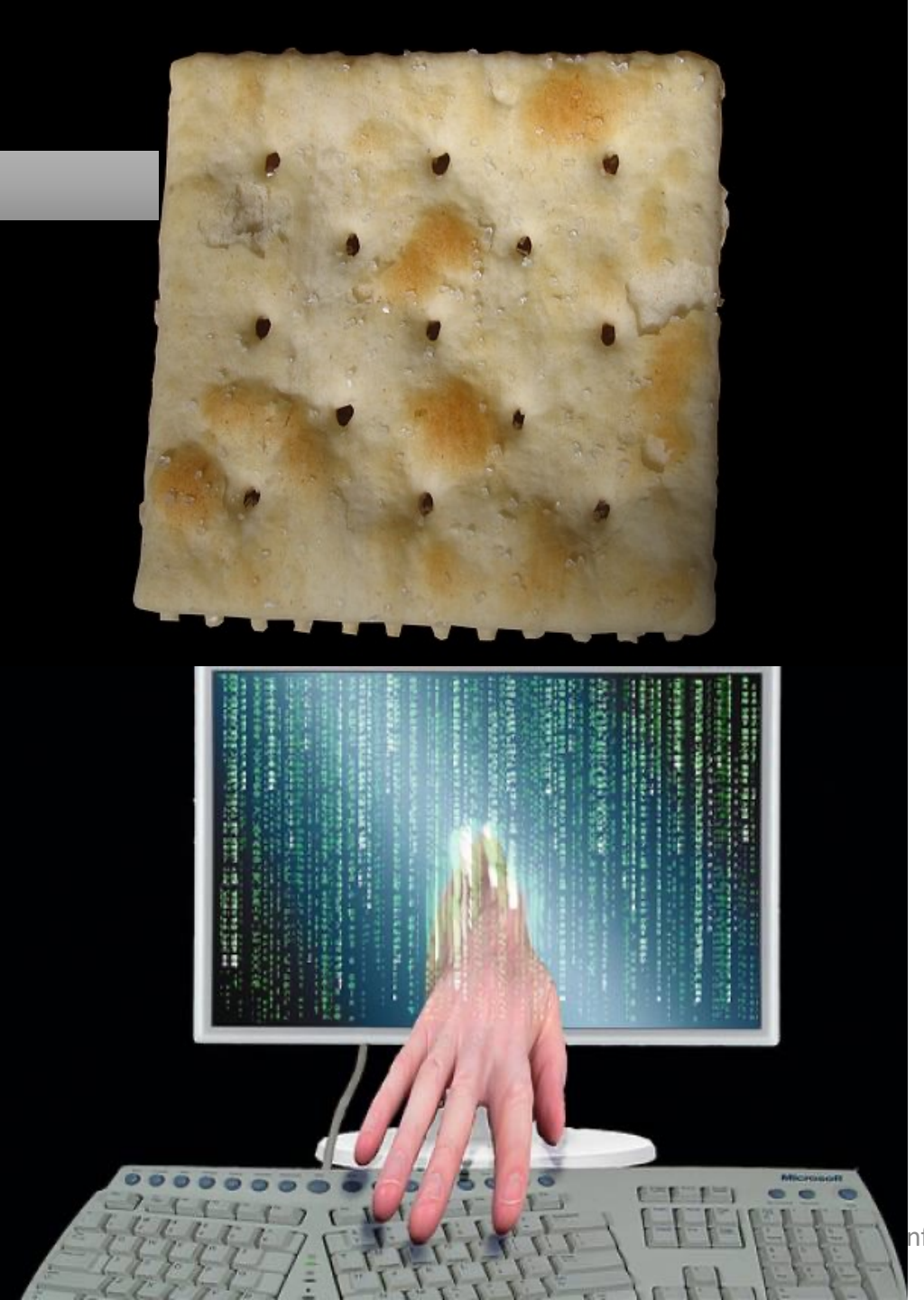
- ความเหมือน หรือ แตกต่าง
- ผลทางกฎหมาย



Hacker

ผู้เชี่ยวชาญในด้านคอมพิวเตอร์อย่างมาก และเชี่ยวชาญทางด้านการใช้ (เซียนคอมพิวเตอร์) จนสามารถเจาะรหัสความปลอดภัยคนอื่นได้ โดยมีวัตถุประสงค์หรือการงานหน้าที่ของตนเอง เพื่อวัดขีดความสามารถ เช่น

- มีหน้าที่รักษาความปลอดภัยของเครือข่ายหรือองค์กร
- ทำเพื่อทดสอบประสิทธิภาพระบบขององค์กร



Cracker

ผู้มีความรู้ความสามารถในการเจาะระบบข้อมูลทางคอมพิวเตอร์ ซึ่งมีคล้าย Hacker แต่ต่างในทางวัตถุประสงค์ โดย Cracker มีจุดประสงค์ในทางไม่ดีที่ต้องการทำร้ายหรือขโมยข้อมูลผู้อื่น ไปใช้ในทางไม่ดีจนเกิดความเสียหาย

ผู้กระทำความผิดทางกฎหมายอาชญากรรมทางคอมพิวเตอร์ [ต่อ]

ความเหมือน

- คือ การเข้าถึงข้อมูลโดยมิชอบ, การเข้าถึงข้อมูลคอมพิวเตอร์ของบุคคลอื่นโดยไม่มีอำนาจ (Unauthorized Access)

ข้อยกเว้น

- หากเป็นการเข้าถึงข้อมูลโดยการทดสอบข้อมูล และหน้าที่ของตนถือว่าไม่ผิด เฉพาะในองค์การหรือหน่อยงานของตนเท่านั้น

อาชญากรทางคอมพิวเตอร์

- พวกเด็กหัดใหม่ (Novice)
- พวกวิกลจริต (Deranged persons)
- อาชญากรที่รวมกลุ่มกระทำผิด (Organized crime)
- อาชญากรอาชีพ (Career)
- พวกหัวพัฒนา มีความก้าวหน้า (Con artists)
- พวกคลั่งลัทธิ (Dremer) / พวกช่างคิดช่างฝัน(Ideologues)
- ผู้ที่มีความรู้และทักษะด้านคอมพิวเตอร์อย่างดี (Hacker/Cracker)

ลักษณะของการกระทำผิดหรือทำให้เกิดภยันตรายหรือความเสียหาย

อันเนื่องมาจากการก่ออาชญากรรมทางคอมพิวเตอร์แบ่งออกได้เป็น 3 ลักษณะ จำแนกตามวัตถุหรือระบบที่ถูกกระทำ

- **การกระทำต่อระบบคอมพิวเตอร์ (Computer System)**
- **การกระทำต่อระบบข้อมูล (Information System)**
- **การกระทำต่อระบบเครือข่ายซึ่งใช้ในการติดต่อสื่อสาร (Computer Network)**

ศัพท์นิยามทางกฎหมาย

- **“ระบบคอมพิวเตอร์”**
  หมายถึง อุปกรณ์อิเล็กทรออิกส์หรือชุดอุปกรณ์อิเล็กทรอนิกส์ใด ๆ
  ซึ่งมีการตั้งโปรแกรมให้ทำหน้าที่ในการประมวลผลข้อมูลโดยอัตโนมัติ ดังนั้น “ระบบคอมพิวเตอร์” จึงได้แก่ ฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่พัฒนาขึ้นเพื่อประมวลผลข้อมูลดิจิทัล (Digital Data) อันประกอบด้วยเครื่องคอมพิวเตอร์ และอุปกรณ์รอบข้าง (Peripheral) ต่างๆ ในการเข้ารับหรือป้อนข้อมูล (Input) นำออกหรือแสดงผลข้อมูล (Output) และบันทึกหรือเก็บข้อมูล (Store and Record)
- **“โปรแกรมคอมพิวเตอร์”**
  คือ ชุดคำสั่งที่ทำให้คอมพิวเตอร์ทำงาน

ศัพท์นิยามทางกฎหมาย [ต่อ]

- **“ระบบข้อมูล”**
  หมายถึง กระบวนการประมวลผลด้วยคอมพิวเตอร์หรือระบบคอมพิวเตอร์ สำหรับสร้าง ส่ง รับ เก็บรักษาหรือประมวลผลข้อมูลอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ ~~โทรเลข โทรพิมพ์~~ โทรสาร เป็นต้น
  - “ข้อมูลดิจิทัล (Digital Data)” ข้อมูลจะมีลักษณะหลากหลาย แล้วแต่การสร้างและวัตถุประสงค์ของการใช้งาน
  - “ข้อมูลจราจร (Traffic Data)” เป็นข้อมูลที่บันทึกวงจรการติดต่อสื่อสาร ตั้งแต่ต้นทางถึงปลายทาง ทำให้ทราบถึงจำนวนปริมาณข้อมูลที่ส่งผ่านระบบคอมพิวเตอร์ในแต่ละช่วงเวลา สำหรับข้อมูลต้นทางนั้น
  - “เลขที่อยู่ไอพี (Internet Protocol Address) หรือ IP Address” ที่อยู่ของเครื่องคอมพิวเตอร์ในการเชื่อมโยงในระบบเครือข่าย

ศัพท์นิยามทางกฎหมาย [ต่อ]

- **“ระบบเครือข่าย”**
  หมายถึง การเชื่อมต่อเส้นทางการสื่อสารระหว่างคอมพิวเตอร์หรือระบบคอมพิวเตอร์เข้าด้วยกันเป็นทอดๆ ซึ่งอาจเป็นระบบเครือข่ายแบบปิด หรือระบบเครือข่ายแบบเปิด
  - **“ระบบเครือข่ายแบบปิด”** คือ ให้บริการเชื่อมต่อเฉพาะสมาชิกเท่านั้น
  - **“ระบบเครือข่ายแบบเปิด”** คือ การเปิดกว้างให้ผู้ใดก็ได้ใช้บริการในการเชื่อมต่อระบบเครือข่าย

การกระทำความผิดทางคอมพิวเตอร์

การคุกคาม ลักลอบ การเข้าไปในระบบโดยไม่ได้รับอนุญาต การบุกรุก มีวิวัฒนาการได้แก่

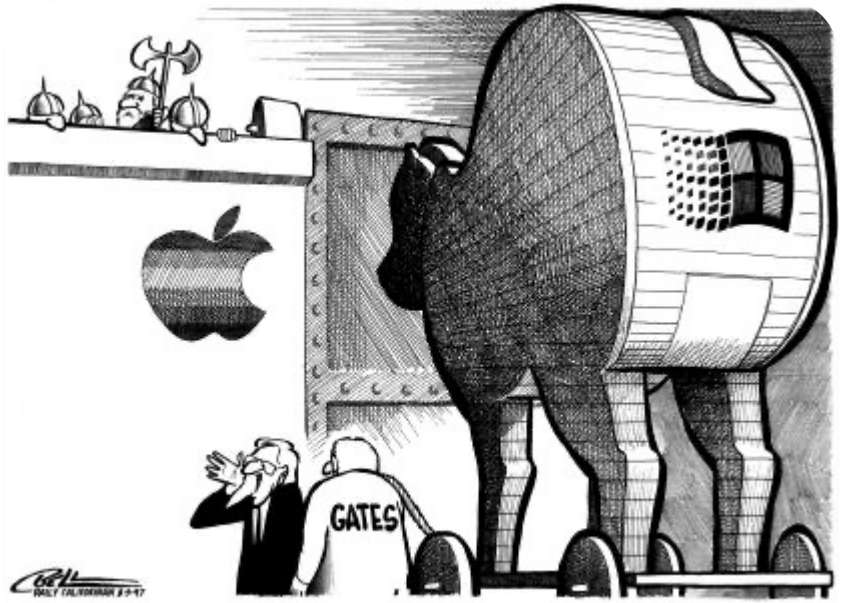
- Virus Computer
- Trojan Horse
- Bomb
- Rabbit
- Sniffer
- Spoofing
- The Hole in the Web

Virus Computer

- สร้างมาเพื่อทำร้ายระบบ และมีการกระจายตัวอย่างรวดเร็ว เพราะ Virus Computer ติดเชื้อและแพร่กระจายได้รวดเร็วมาก และทวีความรุนแรงมากขึ้นเรื่อยๆ โดยอาจทำให้เครื่อง Computer ใช้งานไม่ได้ หรืออาจทำให้ข้อมูลใน Hard Disk เสียหายไปเลย

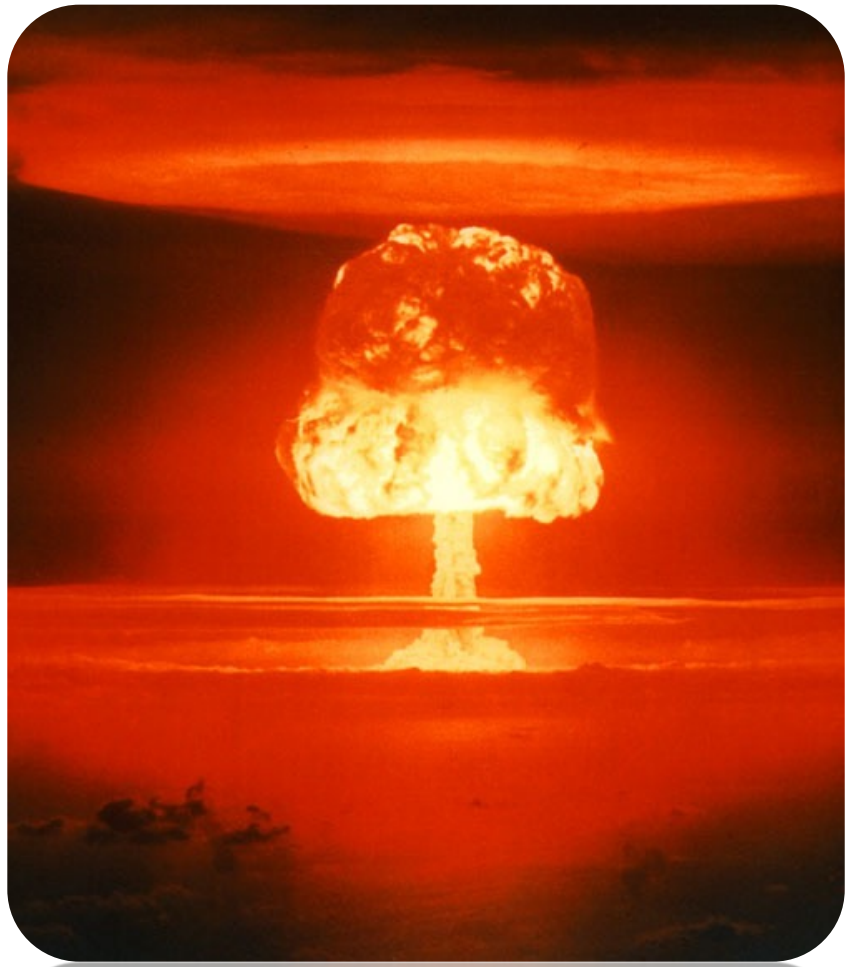
Trojan Horse

- โปรแกรมที่ทำงานโดยแผงอยู่ กับการทำงานของโปรแกรมทั่วไป โดยมีวัตถุประสงค์หนึ่ง เช่น การลักลอบขโมยข้อมูล เป็นต้น



Bomb

- เป็นโปรแกรมที่ถูกกำหนดขึ้นให้ทำตาม เงื่อนไขที่กำหนดเหมือนระเบิดเวลา เช่น Time Bomb ซึ่งเป็นโปรแกรมที่มีการตั้งเวลาให้ทำงานตามที่กำหนดเวลาไว้ หรือ Logic Bomb ซึ่งเป็นโปรแกรมที่กำหนดเงื่อนไขให้ทำงานเมื่อมีเหตุการณ์หรือเงื่อนไขใดๆเกิดขึ้น เป็นต้น

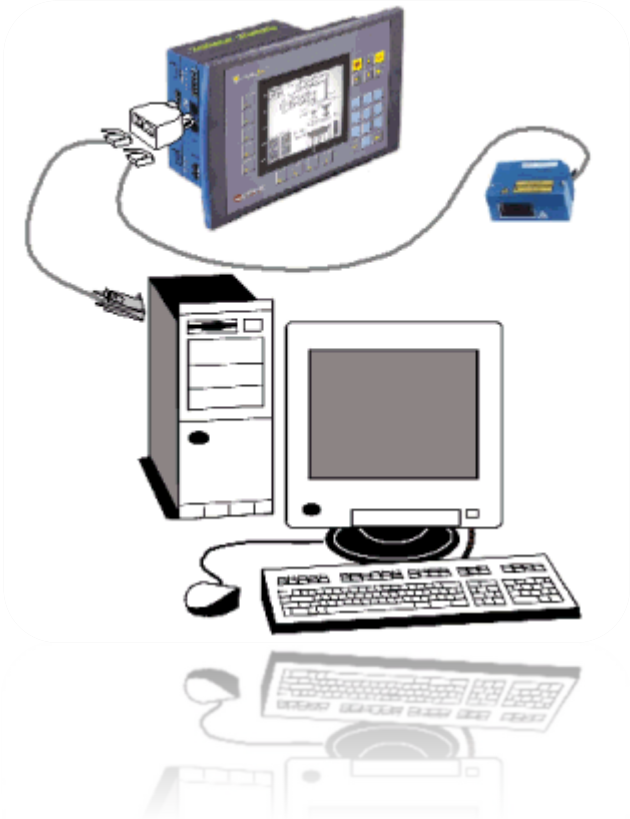


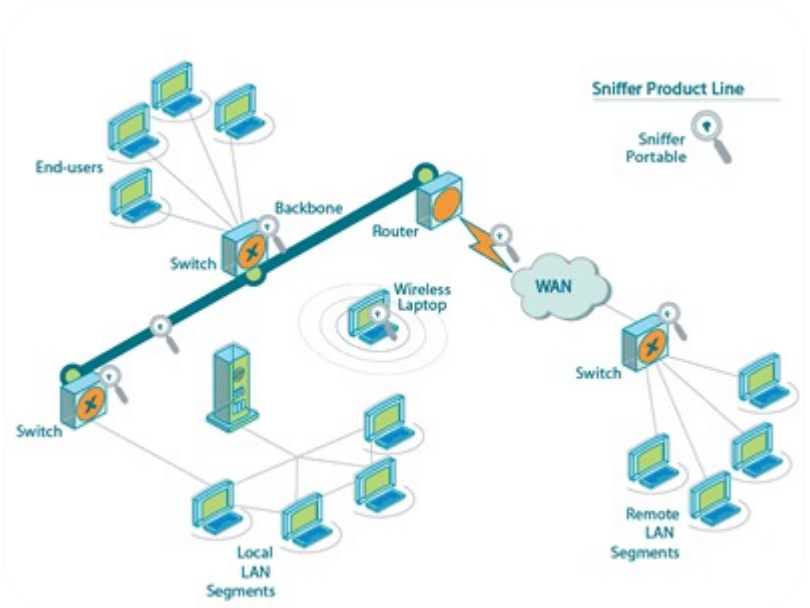
Rabbit

- เป็นโปรแกรมที่กำหนดขึ้นเพื่อให้สร้างตัวมันเองซ้ำๆ เพื่อไม่ให้ระบบทำงานได้ เช่น ทำให้พื้นที่ในหน่วยความจำเต็มเพื่อให้ Computer ไม่สามารถทำงานต่อไปเป็นต้น เป็นวิธีการที่ผู้ใช้มักจะใช้เพื่อทำให้ระบบของเป้าหมายล่ม หรือไม่สามารถทำงานหรือให้บริการได้

Sniffer

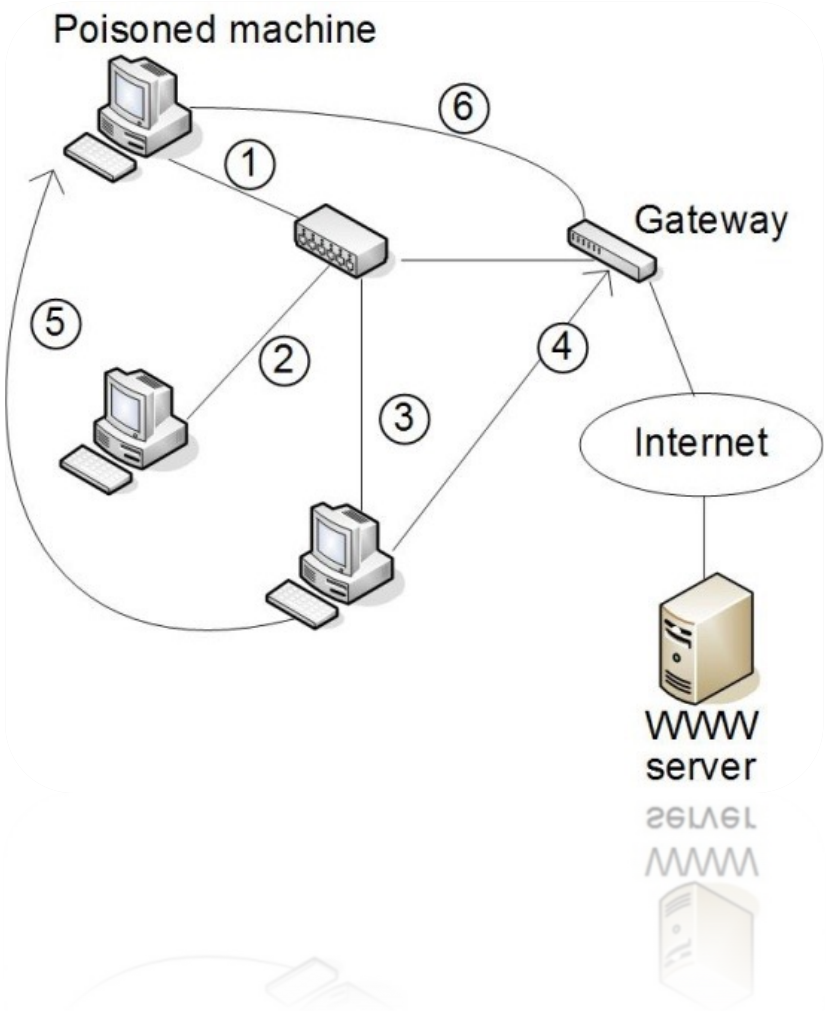
- เป็นโปรแกรมเล็กๆที่ถูกสร้างขึ้นมาเพื่อทำการลักลอบดักข้อมูล ผ่านเครือข่ายที่บันทึกในการ Login ไว้ จึงทำให้ทราบ Password ของบุคคลซึ่งส่งหรือโอนข้อมูลผ่านระบบเครือข่าย โดยจะนำไปเก็บไว้ในแฟ้มลับที่สร้างขึ้น





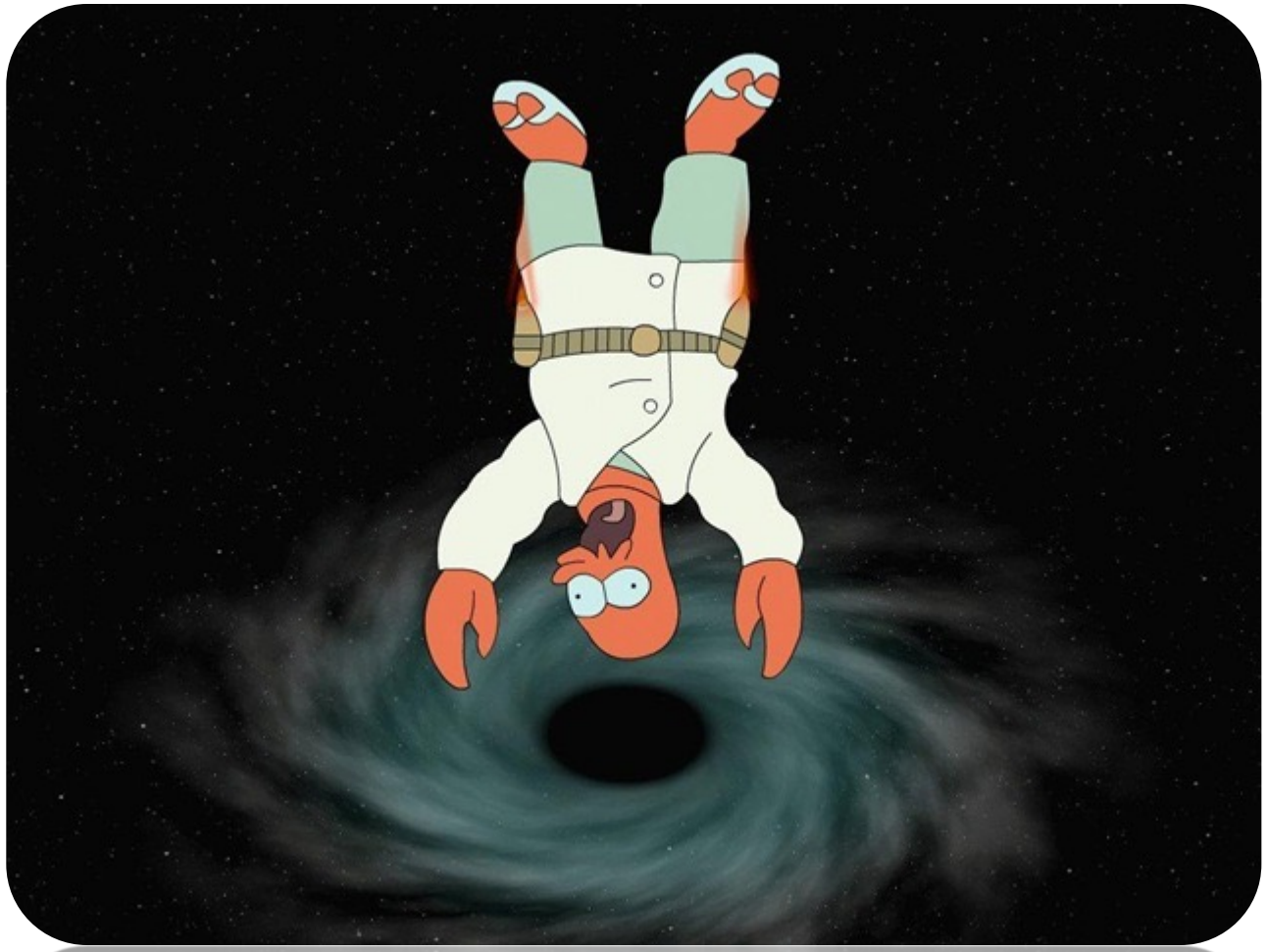
Spoofing

- เป็นการเข้าสู่คอมพิวเตอร์ระยะไกล โดยปลอมแปลงที่อยู่บนอินเตอร์เน็ต (Internet Address) ของเครื่องที่เข้าได้ง่ายหรือเครือข่ายเดียวกัน โดยการเข้าค้นหาระบบความปลอดภัย แล้วเข้าไปยังเครื่องคอมพิวเตอร์นั้น



The Hole in the Web

- การปฏิบัติการของเว็ปไซต์ที่มีช่องว่าง ที่ผู้บุกรุกหรือบุคคลอื่นเข้าไปจัดการหรือเจ้าของเว็ปไซต์ทำได้



การก่ออาชญากรรมคอมพิวเตอร์ในขั้นของกระบวน

แบ่งกระบวนการออกเป็น 3 ส่วน

- Input Process
- Data Processing
- Output Process

การก่ออาชญากรรมคอมพิวเตอร์ในขั้นของกระบวนการนำเข้า (Input Process)

- **การสับเปลี่ยน Disk** คือ การสับเปลี่ยนดิสทุกอย่าง ไม่ว่าจะเป็น Hard Disk, Floppy Disk รวมทั้ง Disk ชนิดอื่น ๆ ด้วย
- **การทำลายข้อมูล** คือไม่ว่าจะใน Hard Disk หรือสื่อบันทึกข้อมูลชนิดอื่นที่ใช้ร่วมกับ โดยไม่มีอำนาจหรือมิชอบ
- **การป้อนข้อมูลเท็จ** คือ ผู้มีอำนาจหน้าที่อันอาจเข้าถึงเครื่องคอมพิวเตอร์และข้อมูลและผู้ไม่มีอำนาจ ป้อนข้อมูลเท็จโดยมิชอบ
- **การลักข้อมูลข่าวสาร** (Computer Espionage) คือ การลักข้อมูลข้าวสารไม่ว่าการกระทำใดใดให้ได้ข้อมูลยังตัวเองโดยมิชอบ *(บางทีคือการลักทรัพย์ดูตามการวิเคราะห์)*
- **การลักใช้บริการหรือเข้าไปใช้โดยไม่มีอำนาจ** (Unauthorized Access) คือ การเจาะระบบเข้าไป หรือใช้วิธีการอย่างใดๆเพื่อให้ได้โดยไม่ต้องลงทะเบียนเสียค่าใช้จ่าย *(ถือว่าเป็นคดีอาญาลักทรัพย์/ผู้ใช้ข้อมูลถือว่ารับข้องโจร)*

การก่ออาชญากรรมคอมพิวเตอร์ในส่วนกระบวนการ (Data Processing)

เป็นการกระทำตัวข้อมูลระบบ เช่น

- **การทำลายข้อมูลและระบบโดยใช้ไวรัส** (Computer Subotage) คือ การแพร่ข้อมูลซึ่งกระจายได้ง่ายและรวดเร็ว
- **การทำลายข้อมูลและโปรแกรม** (Damage to Data and Program) การทำลายข้อมูลโดยไม่ชอบย่อมจะต้องเป็นความผิด
- **การเปลี่ยนแปลงข้อมูลและโปรแกรม** (Alteration of Data and Program) คือ การเปลี่ยนแปลงข้อมูลและโปรแกรมจนทำให้เกิดความเสียหาย

การก่ออาชญากรรมคอมพิวเตอร์ในส่วนกระบวนการนำออก (Output Process)

เป็นการกระทำโดยนำออก เช่น

- **การขโมยขยะ** (Sewaging) คือ ข้อมูลที่เราไม่ใช้แล้ว แต่ยังไม่ได้ทำลาย ถ้าขยะที่ถูกขโมยไปนั้นอาจทำให้เจ้าของต้องเสียหายอย่างใดๆ
- **การขโมย** Printout คือ การขโมยงานหรือข้อมูลที่ Print ออกมาแล้ว (ผิดฐานลักทรัพย์)

รับโดยไม่รู้ที่มา... ต้องผิดด้วยหรือ?


อ่ะ... ถือว่าช่วยเหลือเพื่อนมนุษย์ครับ
1000
โอ้โห! เงินเยอะขนาดนี้ ได้มาสุจริตหรือเปล่าเนี่ย
เอาคืนซะเลยดีไหมเนี่ย
เดี๋ยวๆ จะรีบไปไหนล่ะท่าน

การกำหนดฐานความผิดและบทกำหนดโทษ

การพัฒนากฎหมายอาชญากรรมคอมพิวเตอร์ในเบื้องต้น พัฒนาขึ้นโดยคำนึงถึงลักษณะการกระทำความผิดต่อระบบคอมพิวเตอร์ ระบบข้อมูล และระบบเครือข่าย ซึ่งสรุปความผิดสำคัญได้ 3 ฐานความผิด

- **การเข้าถึงโดยไม่มีอำนาจ (Unauthorized Access)**
- **การใช้คอมพิวเตอร์โดยไม่ชอบ (Computer Misuse)**
- **ความผิดเกี่ยวข้องกับคอมพิวเตอร์ (Computer Related Crime)**

ความผิดแต่ละฐานที่กำหนดขึ้น

การกระทำความผิดด้วยการเข้าถึงโดยไม่มีอำนาจหรือโดยฝ่าฝืนกฎหมาย และการใช้คอมพิวเตอร์ในทางมิชอบ ถือเป็นการกระทำที่คุกคามหรือเป็นภัยต่อความปลอดภัย (Security) ของระบบคอมพิวเตอร์และระบบข้อมูล เมื่อระบบไม่มีความปลอดภัยก็จะส่งผลกระทบต่อความครบถ้วน (Integrity) การรักษาความลับ (Confidential) และเสถียรภาพในการใช้งาน (Availability) ของระบบข้อมูลและระบบคอมพิวเตอร์

- **การเข้าถึงโดยไม่มีอำนาจ**
  ตาม พรบ.คอมพิวเตอร์ ระบุไว้ดังนี้ การเข้าถึงข้อมูลหรือระบบ (Hacking หรือ Cracking) หรือบุกรุกทางคอมพิวเตอร์เพื่อทำร้ายระบบคอมพิวเตอร์หรือเปลี่ยนแปลงแก้ไขข้อมูล เช่น Password หรือ ข้อมูลทางการค้า

  “การเข้าถึง” ยังหมายถึง การเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เนต อันเป็นการเชื่อมโยงระหว่างเครือข่ายหลายๆเครือข่ายเข้าด้วยกัน และยังหมายถึง การเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบ LAN (Local Area Network) อันเป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ๆกันเข้าด้วยกัน

ความผิดแต่ละฐานที่กำหนดขึ้น [ต่อ]

- **การลักลอบดักข้อมูล**
  (Illegal Interception) เนื่องจากมีวัตถุประสงค์เพื่อคุ้มครองสิทธิความเป็นส่วนตัวในการติดต่อสื่อสาร (The Right of Privacy of Data Communication) เช่น การดักฟังโทรศัพท์หรือแอบบันทึกเทปลับ เป็นต้น

  การกระทำที่เป็นความผิดฐานลักลอบดักข้อมูลนั้น ข้อมูลที่ส่งต้องมิใช่ข้อมูลที่ส่งและเปิดเผยให้สาธารณชนรับรู้ได้ (Non-Public Transmissions) การกระทำความผิดฐานนี้จึงจำกัดเฉพาะแต่เพียงวิธีการส่งที่ผู้ส่งข้อมูลประสงค์จะส่งข้อมูลนั้นให้แก่บุคคลหนึ่งบุคคลใดโดยเฉพาะเจาะจงเท่านั้น

ความผิดแต่ละฐานที่กำหนดขึ้น [ต่อ]

- **ความผิดฐานรบกวนระบบ**
  การรบกวนทั้งระบบข้อมูลและระบบคอมพิวเตอร์ (Data and System Interference) โดยมุ่งลงโทษผู้กระทำความผิดที่จงใจก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ โดยมุ่งคุ้มครอง ความครบถ้วนของข้อมูล และเสถียรภาพในการใช้งานหรือการใช้ข้อมูลหรือโปรแกรมคอมพิวเตอร์ที่บันทึกไว้บนสื่อคอมพิวเตอร์ได้เป็นปกติ

ความผิดแต่ละฐานที่กำหนดขึ้น [ต่อ]

- **การใช้อุปกรณ์ในทางมิชอบ**
  ต่างกันตรงที่ผลิต จ่าย จำหน่วย หรือ ครอบครองคอมพิวเตอร์ที่ใช้กระทำความผิด หรือ อุปกรณ์ในการแจะระบบ (Hasher Tools) รวมถึงรหัสผ่านคอมพิวเตอร์ รหัสการเข้าถึง หรือข้อมูลอื่นในลักษณะคล้ายคลึงกันด้วย

  สำหรับการแจกจ่ายนั้น ให้รวมถึงการส่งข้อมูลที่ได้รับเพื่อให้ผู้อื่นอีกทอดหนึ่ง (Forward) หรือการเชื่อมโยงฐานข้อมูลเข้าด้วยกัน (Hyperlinks) ด้วย

รูปแบบของอาชญากรรมทางคอมพิวเตอร์

ทั่วโลกได้จำแนกประเภทอาชญากรรมทางคอมพิวเตอร์ได้ 9 ประเภท (ตามข้อมูลคณะอนุกรรมการเฉพาะกิจร่างกฎหมายอาชญากรรมทางคอมพิวเตอร์)

- การขโมยข้อมูลทางอินเตอร์เน็ต รวมถึงการขโมยประโยชน์ในการลักลอบใช้บริการ
- การปกปิดความผิดของตัวเอง โดยใช้ระบบการสื่อสาร
- การละเมิดลิขสิทธิ์ ปลอมแปลงรูปแบบเลียนแบบระบบซอฟแวร์โดยมิชอบ
- การเผยแพร่ภาพ เสียง ลามก อนาจาร และข้อมูลที่ไม่เหมาะสม
- การฟอกเงิน

รูปแบบของอาชญากรรมทางคอมพิวเตอร์ [ต่อ]

- การก่อกวน ระบบคอมพิวเตอร์ เช่น ทำลายระบบสาธารณูปโภค เช่น ระบบจ่ายน้ำ จ่ายไฟ จราจร แอปกระเป๋าตังค์
- การหลอกลวงให้ร่วมค้าขาย หรือ ลงทุนปลอม (การทำธุรกิจที่ไม่ชอบด้วยกฎหมาย)
- การลักลอบใช้ข้อมูลเพื่อแสวงหาผลประโยชน์ในทางมิชอบ เช่น การขโมยรหัสบัตรเครดิต
- การใช้คอมพิวเตอร์ในการโอนเงิน/บัญชีผู้อื่นเป็นของตัวเอง

มาตรา และ โทษ

มาตรา 5-8 (แฮกเกอร์) การกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงชาติ

5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบ

ระวางโทษ จำคุก ไม่เกิน 6 เดือน หรือ ปรับไม่เกิน 1 หมื่นบาท

6 ล่วงรู้มาตรการเข้าถึงระบบ

ระวางโทษ จำคุก ไม่เกิน 1 ปี หรือ ปรับไม่เกิน 2 หมื่นบาท

7 เข้าถึงข้อมูลโดยมิชอบ

ระวางโทษ จำคุก ไม่เกิน 2 ปี หรือ ปรับไม่เกิน 4 หมื่นบาท

8 ผู้ใดกระทำด้วยประการใดๆ

ระวางโทษ จำคุก ไม่เกิน 3 ปี หรือ ปรับไม่เกิน 6 หมื่นบาท

ต้องระวางโทษจำคุกตั้งแต่ 1 ปี ถึง 10/ ปรับตั้งแต่ 2 หมื่น ถึง 2 แสน

มาตรา และ โทษ [ต่อ]

มาตรา 9-10 (ทำลายซอฟแวร์) **เป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบ**

จนเป็นเหตุให้บุคคลอื่นถึงแก่ความตาย (แต่มิได้เจตนาฆ่า)

9 ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง

ระวางโทษ จำคุก ไม่เกิน 5 ปี หรือ ปรับไม่เกิน 1 แสนบาท

10 ทำการโดยใดๆมิชอบ

ระวางโทษ จำคุก ไม่เกิน 5 ปี หรือ ปรับไม่เกิน 1 แสนบาท

ต้องระวางโทษจำคุกตั้งแต่ 3 ปี ถึง 15/ ปรับตั้งแต่ 6 หมื่น ถึง 3 แสน

ต้องระวางโทษจำคุกตั้งแต่ 5 ปี ถึง 20/ ปรับตั้งแต่ 1 แสน ถึง 4 แสน

มาตรา 11 (ปกปิด เปลี่ยนแปลง E-mail)

11 ส่งเมล์ ปลอมแปลง รบกวน

ระวางโทษ ปรับไม่เกิน 1 แสนบาท.

มาตรา และ โทษ [ต่อ]

มาตรา 13 (ผู้ค้าซอฟแวต์สนับสนุนการทำผิด) เพิ่มโทษสูงขึ้นจากใน พรบ.คอม 50

13 ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่ทำขึ้นเฉพาะ

ระวางโทษ จำคุก ไม่เกิน 1 ปี หรือ ปรับไม่เกิน 2 หมื่นบาท

ต้องระวางโทษจำคุกไม่เกิน 2 ปี / ปรับไม่เกิน 4 หมื่น

*** มาตรา 14 (ผู้ใช้งานทั่วไปกระทำการ)** ยกเลิกและเพิ่มเติมให้ครอบคลุมกับปัจจุบัน

14 ต้องระวางโทษ จำคุก ไม่เกิน 5 ปี หรือ ปรับไม่เกิน 1 แสนบาท

ต้องระวางโทษจำคุกไม่เกิน 3 ปี / ปรับไม่เกิน 6 หมื่น

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน โดยทุจริตหรือหลอกลวง

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยน่าจะเกิดความเสียหายต่อความมั่นคงชาติ

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงชาติ หรือต่อประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก และข้อมูลที่อาจเข้าถึงได้

(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้ว (1-4)

มาตรา และ โทษ [ต่อ]

*** มาตรา 15 (ผู้ให้บริการผู้ใดจงใจสนับสนุนให้กระทำความผิด)** ยกเลิกและเพิ่มเติมให้ครอบคลุมกับปัจจุบัน

15 ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14 ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิด

มาตรา 16 (ตัดต่อ เผยแพร่ภาพอนาจาร) ยกเลิกและเพิ่มเติมให้ครอบคลุมกับปัจจุบัน

16 ปลอมแปลงดัดแปลงภาพผู้อื่น จนทำให้เสียหาย ถูกดูหมิ่น

- ทั้งบิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูถูก หรือถูกเกลียดชัง
- ศาลให้อำนาจในการ ทำลาย โฆษณาเผยแพร่ และพิจารณาตามที่ศาลเห็นสมควร

ระวางโทษ จำคุก ไม่เกิน 3 ปี หรือ ปรับไม่เกิน 6 หมื่นบาท

ต้องระวางโทษจำคุกไม่เกิน 3 ปี / ปรับไม่เกิน 2 แสน

*** มาตรา 18-30 (การให้อำนาจแก่เจ้าหน้าที่)** ยกเลิกและเพิ่มเติมให้ครอบคลุมกับปัจจุบัน

คำถาม

- Q1 : การนำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น จะได้รับโทษอย่างไร

- Q2 : การนำรูปของเพื่อนไปตัดต่อแล้วส่งรูปไปยังเว็บบอร์ด ทำให้เพื่อนเสื่อมเสียชื่อเสียง จะได้รับโทษอย่างไร

- Q3 : การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน จะได้รับโทษอย่างไร

- Q4 : การแสดงการแจ้งเตือนภาพย้อนอดีตของ Facebook ที่ผู้ใช้โพสต์รูปทั้งที่เป็นรูปตนเองกับคนอื่น หรือ รูปคนอื่นผิดหรือไม่

บริบททางสังคมของเทคโนโลยีสารสนเทศ

เทคโนโลยีสารสนเทศกับการพัฒนาสังคม

- อุตสาหกรรมเทคโนโลยีสารสนเทศกลายเป็นอุตสาหกรรมการผลิตที่มีขนาดใหญ่ที่สุดในโลก มีการประมาณการว่าตลาดโลกสำหรับอุปกรณ์ ทั้งฮาร์ดแวร์ และซอฟต์แวร์ โทรคมนาคม และผลิตภัณฑ์ที่เกี่ยวข้องอื่นๆ จะมีบทบาทสูงในการกำหนดทิศทางของเทคโนโลยี เป็นที่ทราบกันดีว่าเทคโนโลยีการสื่อสารในอดีตและปัจจุบันได้เปลี่ยนไปอย่างมาก อนาคตธุรกิจบันเทิงจะเป็นธุรกิจอีกประเภทหนึ่งที่ทำเงิน เนื่องจากเป็นธุรกิจที่มีอิทธิพลอย่างสูงกับแนวความคิด ความอ่านของผู้คนในสังคม

สารสนเทศกับบุคคล

- การพัฒนาของเทคโนโลยีสารสนเทศ ทำให้เกิดความต้องการและการใช้สารสนเทศของบุคคลเพิ่มมากขึ้น สารสนเทศมีการใช้เพื่อให้เกิดความรู้และความเข้าใจในเรื่องที่ตนเกี่ยวข้อง และนำความรู้ความเข้าใจมาตัดสินใจแก้ไขปัญหาที่เกิดขึ้นได้อย่างถูกต้อง แม่นยำ และรวดเร็ว ทันเวลากับสถานการณ์ต่างๆ ที่เกิดขึ้นได้อย่างเหมาะสม
- เทคโนโลยีสารสนเทศเป็นเรื่องที่ใกล้ชิดและเกี่ยวพันกับชีวิตประจำวันของมนุษย์ เช่น การถอนเงินอัตโนมัติ ธนาคารอิเล็กทรอนิกส์ การซื้อขายสินค้าทางพาณิชย์อิเล็กทรอนิกส์ การประชุมทางไกล การศึกษาทางไกล ระบบห้องสมุดดิจิตอล การเข้าถึงบริการและสารสนเทศต่างๆ ผ่านระบบโทรศัพท์มือถือ เป็นต้น

สารสนเทศกับสังคม

- สารสนเทศนอกจากมีความสำคัญต่อตัวบุคคล แล้วยังมีความสำคัญต่อสังคมในด้านต่างๆ ได้แก่ ด้านการศึกษา ด้านสังคม ด้านเศรษฐกิจ และด้านวัฒนธรรม

1.**ด้านการศึกษา** การจัดการเรียนการสอนในปัจจุบันมุ่งเน้นผู้เรียนเป็นศูนย์กลาง สารสนเทศที่ดีมีคุณค่าและทันสมัย จะช่วยให้การเรียนการสอนมีประสิทธิภาพและประสิทธิผล เพื่อพัฒนาองค์ความรู้ใหม่ๆ

2. **ด้านสังคม** สารสนเทศช่วยพัฒนาสติปัญญาของมนุษย์ ช่วยพัฒนาบุคลิกภาพส่วนบุคคลให้อยู่ร่วมกับผู้อื่นได้อย่างมีความสุข อีกทั้งช่วยให้เกิดความคิดสร้างสรรค์ เกิดการประดิษฐ์คิดค้นเทคโนโลยีใหม่ๆ

3.**ด้านเศรษฐกิจ** สารสนเทศมีความสำคัญในการขับเคลื่อนเศรษฐกิจยุคใหม่ที่เรียกว่า เศรษฐกิจบนฐานความรู้ หน่วยงานหรือผู้ประกอบการธุรกิจให้ความสำคัญกับ “การจัดการความรู้” เพื่อรักษาองค์ความรู้ขององค์กรไว้ สารสนเทศด้านธุรกิจการค้าจึงถือเป็นต้นทุนการผลิตที่สำคัญ

4.**ด้านวัฒนธรรม** สารสนเทศเป็นรากฐานที่จำเป็นสำหรับความก้าวหน้าของอารยธรรม สารสนเทศช่วยสืบทอดค่านิยม ทัศนคติ ศิลปะ และวัฒนธรรมที่เป็นเอกลักษณ์อันดีงามของชาติ ก่อให้เกิดความภาคภูมิใจ ความสามัคคี ความมั่นคงในชาติ

ผลกระทบด้านบวก

1. การสร้างเสริมคุณภาพชีวิตที่ดีขึ้น
2. เสริมสร้างความเท่าเทียมในสังคมและการกระจายโอกาส
3. สารสนเทศกับการเรียนการสอน
4. เทคโนโลยีสารสนเทศกับสิ่งแวดล้อม
5. เทคโนโลยีสารสนเทศกับการป้องกันประเทศ
6. การผลิตในอุตสาหกรรม และการพาณิชยกรรม
7. เทคโนโลยีสารสนเทศมีผลเกี่ยวข้องกับทุกเรื่องในชีวิตประจำวัน

ผลกระทบด้านลบ

1. ก่อให้เกิดความเครียดในสังคมมากขึ้น
2. ก่อให้เกิดการรับวัฒนธรรม
3. ก่อให้เกิดผลด้านศีลธรรม
4. การมีส่วนร่วมของคนในสังคมลดน้อยลง
5. การละเมิดสิทธิเสรีภาพส่วนบุคคลโดยการเพยแพร่ข้อมูลหรือรูปภาพต่อสาธารณชน
6. เกิดช่องว่างทางสังคม
7. อาชญากรรมบนเครือข่าย
8. ก่อให้เกิดปัญหาด้านสุขภาพ

1. กฎหมายคืออะไร / มีกี่ระบบ / อะไรบ้าง (อธิบายพอสังเขป)
2. ทำความผิดโดยไม่รู้ผิดหรือไม่ / เพราะอะไร (อธิบายพอสังเขป)
3. ธุรกรรมทางอิเล็กทรอนิกส์ กับ การพาณิชย์อิเล็กทรอนิกส์ ต่างกันอย่างไร (อธิบายพอสังเขป)
4. พรบ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ฉบับปัจจุบันคือ / มีกี่หมวดอะไรบ้าง (อธิบายพอสังเขป)
5. ทำไมการเขียนโปรแกรมคอมพิวเตอร์ถึงสามารถจดลิขสิทธิ์ได้ (อธิบายพอสังเขป)
6. ลิขสิทธิ์ กับ สิทธิบัตร ต่างกันอย่างไร (อธิบายพอสังเขป)
7. พ.ร.บ.คอมพิวเตอร์ คืออะไร / มีวัตถุประสงค์เพื่ออะไร / ฉบับปัจจุบันคือ (อธิบายพอสังเขป)
8. พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ.2550 มีกี่หมวด / อะไรบ้าง (อธิบายพอสังเขป)
9. พรบ.คอม ปี 50 กับ พรบ.คอม ปี 60 ต่างกันอย่างไร (อธิบายพอสังเขป)
10. กฎหมายเทคโนโลยีสารสนเทศ จำนวน 6 ฉบับ มีอะไรบ้าง (อธิบายพอสังเขป)
11. EDI คืออะไร (อธิบายพอสังเขป)
12. Hacker กับ Cracker ต่างกันอย่างไร (อธิบายพอสังเขป)
13. การกระทำความผิดทางคอมพิวเตอร์มีกี่ชนิด / อะไรบ้าง (อธิบายพอสังเขป)
14. ความผิดแต่ละฐานที่กำหนดขึ้นของ พรบ.คอม อะไรบ้าง (อธิบายพอสังเขป)