

Lecture 3: Computer Crime and พรบ คอมพิวเตอร์ 2550 และ 2560

Computer Ethics : Social and Professional Issues 24.12.67



Computer Crime

Hacking

Computer Criminals

Malwares

- Ransomware
- DoS/ DDoS
- Identity Theft => Phishing



แนะนำให้รู้จัก พรบ คอมพิวเตอร์

Hacking



**Intentional unauthorized access to
computer systems**

Computer security ปกป้อง asset
Computer Crime ละเมิด asset



What is computer System?

Hardware

- computers, printers, scanners, servers, and communication media

software

- application and special programs, system back-ups, and diagnostic programs, and system programs such as operating systems and protocols

data

- in storage, transition, or undergoing modification

people

- users, system administrators, and hardware and software manufacturers

Documentation

- administrative procedures, and policy documents

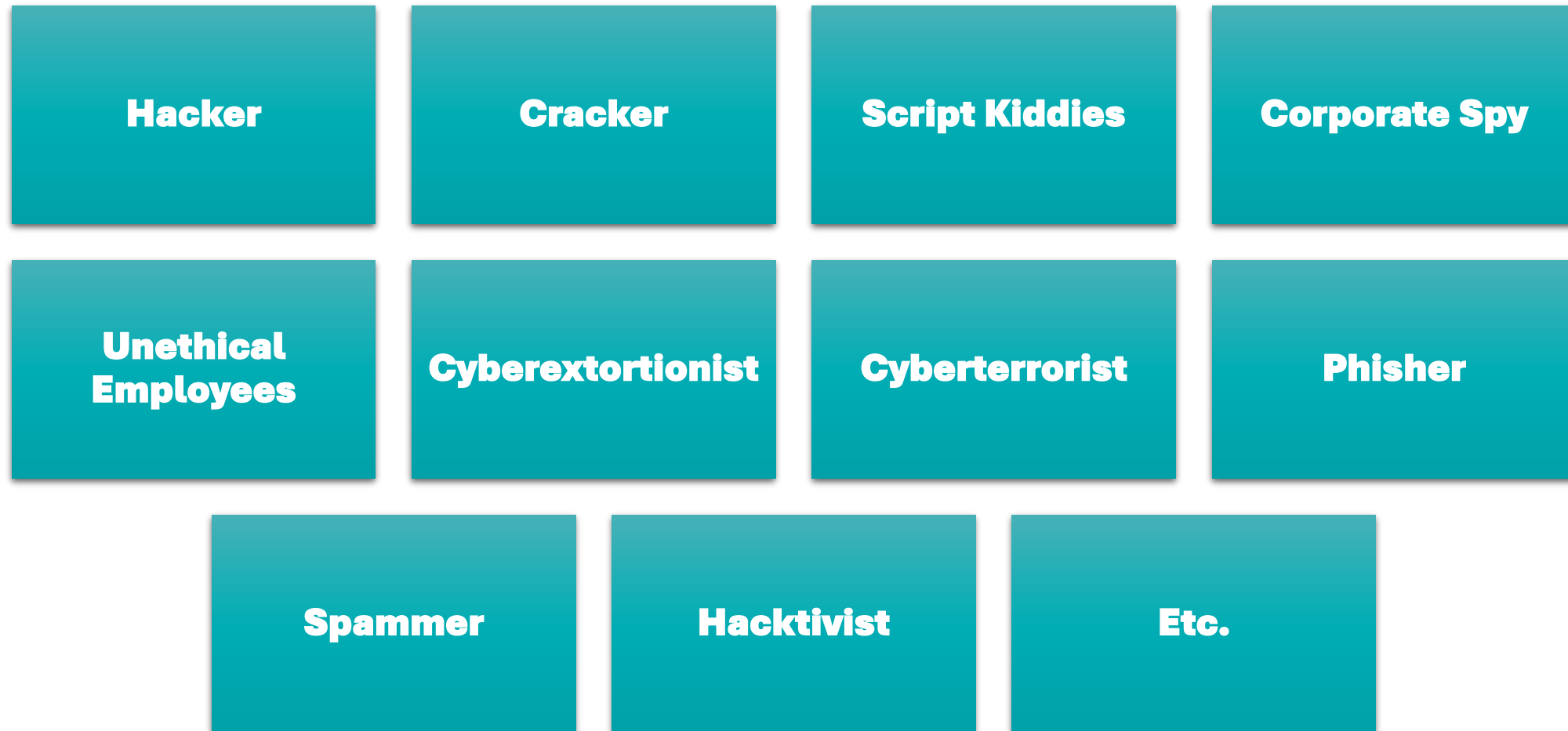


Hacking

- [Base13] categorized into 3 phases:
 - Phase1: The joy of programming Early 1960s-1970s
 - White hat hacker
 - Creative programmer who wrote elegant and clever code
 - Phase2: 1970 – mid 1990
 - Start negative meaning
 - Spreading of computer worms and viruses and phone phreaking
 - Phase3: mid 1990s
 - Growth of Web hacking, virus and worm could spread rapidly
 - DoS to shut down web
 - Large scale of personal and financial information
- Now?
 - Mobile Hacking /IoT security/OT Security

Computer Criminals I

- กลุ่มคนที่เข้าถึงข้อมูลโดยไม่ได้รับอนุญาต



Computer Criminals and their friends. II

Hacker – แฮกเกอร์

มีความรู้ความสามารถเช่นเดียวกับแฮกเกอร์ เข้าถึงคอมพิวเตอร์ หรือ ระบบเครือข่ายโดยไม่ได้รับอนุญาต เช่นกัน

แต่มีเจตนาให้เกิดความเสียหายของข้อมูล มากกว่าแฮกเกอร์

- มุ่งทำลายระบบ หรือ ลักลอบเข้าไปแก้ไข เปลี่ยนแปลงหรือ ทำลายข้อมูลในระบบนั้นทั้ง หรือ ทำการ ขโมยข้อมูล

มักเรียกว่า เป็นกลุ่มคน หมวกดำ (black hat)

ถือว่าเป็นบุคคลที่มีความร้ายแรงมากในปัจจุบัน

Cracker- แครกเกอร์

อาศัยช่องโหว่ของเทคโนโลยีลักลอบดูข้อมูลของผู้อื่น โดยไม่ได้รับอนุญาต

แรกเริ่มความหมายจะไปทางบวก

- ค้นหาช่องโหว่ของระบบ เพื่อนำมาปรับปรุงให้ปลอดภัยขึ้น โดยเจตนาแล้วไม่ได้มุ่งร้ายต่อข้อมูลอย่างใด

ปัจจุบัน ความหมายเอนเอียงไปทางผู้ที่ เข้า access คอมพิวเตอร์หรือเน็ตเวิร์คโดยไม่ถูกต้อง

Ethical Hacker

มีความรู้ความสามารถทางด้านคอมพิวเตอร์และระบบเครือข่าย คอมพิวเตอร์เป็นอย่างดี

Computer Criminals and their friends. III

Script Kiddy:

- มีจุดมุ่งหมายเหมือน แครกเกอร์ แต่ ไม่มีความรู้หรือ ทักษะเหมือนแครกเกอร์
- อาศัยโปรแกรมหรือเครื่องมือบางอย่างที่หามาได้จากแหล่งต่างๆ บนอินเทอร์เน็ต (ที่เขียนโดย แครกเกอร์หรือแฮกเกอร์) และทำตามคู่มือการใช้งาน
- มักเป็นพวกเด็กวัยรุ่นหรือ นักศึกษา
- ปัจจุบันมีจำนวนมากขึ้นอย่างรวดเร็ว มีการนำโปรแกรมหรือ script ที่มีคนเขียนและนำออกมาเผยแพร่ให้ทดลองใช้กันอย่างมากมาทั่วโลก
- เช่น การลอบอ่านอีเมล การขโมยรหัสผ่านของผู้อื่น การใช้โปรแกรมก่อวินาศกรรมอย่างง่าย

Computer Criminals and their friends. III

•Unethical Employees

- => ลูกจ้างที่ฝ่าฝืน code of practices ของบริษัท หรือ นำความลับบริษัทไปเปิดเผย (ขายให้คู่แข่ง เป็นต้น)

Computer Criminals and their friends. IV

- Corporate Spy (Corporate Espionage):
 - <http://www.youtube.com/watch?v=QhIU2uuinI> (See Duplicity)
 - is the act or practice of spying to gain secret information on a government or a business competitor.
 - Is hired to use any means to acquire data that will give the payers a competitive or financial advantage over their competition.
 - Ex.
 - **Key logger**
 - **Fake Wireless AP**
 - downloading free access point (AP) software like, a spy can use his laptop or PDA to impersonate any legitimate wireless hotspot
 - Next use Man-in-the middle attack to steal customer or company data's sent through this network. (see more info in ###)

http://www.sans.org/reading_room/whitepapers/engineering/corporate-espionage-201_512

Computer Criminals and their friends. V

Cyberextortionist

- ส่งอีเมลขู่เรียกเงิน ไม่งั้นจะนำความลับ หรือ ช่องโหว่ของบริษัทที่รู้มาไปเปิดเผย หรือโจมตีให้ระบบเครื่องข่าย /บริษัทล่ม
- ตย <http://www.securityweek.com/cyber-extortion-huge-profits-low-risk>
 - Data the new hostage (จับข้อมูลเป็นตัวประกัน)
 - **technician broke into system to change the access code and pwd. => company and its customers can't get access.**
 - a note posted in 2009 on a public website for the Virginia Department of Health Professions:
 - *"ATTENTION VIRGINIA I have your sh**! In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too. Uhoh :(“*
 - The release of protected or personal data
 - Selling corporate secrets ((i.e., strategies, technologies, relationships)))
 - The release of private corporate or personal information

Computer Criminals and their friends. V

Cyberterrorist

- ใช้อินเทอร์เน็ตในการทำลาย หรือ ทำความเสียหายต่อคอมพิวเตอร์ เพื่อวัตถุประสงค์ทางการเมือง
- ความเสียหายอาจจะส่งผลกระทบในการทำลาย การจราจรทางอากาศของทั้งประเทศ หรือ ทำลายบริษัทที่เป็นผู้ผลิตไฟฟ้า หรือ โครงสร้างทางการสื่อสารของประเทศ
- ปกติแล้ว คนกลุ่มนี้จะ มีทักษะทางคอมพิวเตอร์สูงมาก
- การก่อการร้ายทาง cyber นี้ต้องใช้ ทีมงานที่มีทักษะสูง เงินเป็นจำนวนมาก และ เวลาหลายปี
- See Die Hard 4

Crime Tools: 1. Malicious Software

- Malware ย่อมาจาก malicious software
- โปรแกรมที่มีวัตถุประสงค์ร้ายต่อระบบ ทำให้ระบบทำงานไม่ได้ หรือ ก่อความรำคาญให้กับผู้ใช้ หรือ แอบเปิดทางให้ แฮกเกอร์เข้าระบบ หรือ ล้วงความลับของระบบ หรือ เหยื่อ

Virus

Worm

Trojan

Spyware

BOT

Spam

Ransomware

DDoS

XSS

Sidejacking

Malware

คอมพิวเตอร์ไวรัส (Computer Virus)

อาศัยคำสั่งที่เขียนขึ้นภายในตัวโปรแกรมเพื่อกระจายไปยังเครื่องคอมพิวเตอร์เป้าหมาย

แพร่กระจายโดย

- ผ่านการทำสำเนาข้อมูลด้วยสื่อบันทึกข้อมูลสำรองจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง หรือ
- มีการแลกเปลี่ยนข้อมูลกันระหว่างเครื่องคอมพิวเตอร์ เช่น อีเมล

อาศัยคุณกระทำการอย่างใดอย่างหนึ่งกับพาหะที่โปรแกรมไวรัสนั้นแฝงตัวอยู่เพื่อแพร่กระจาย

- รันโปรแกรม อ่านอีเมล เปิดดูเว็บเพจ หรือ เปิดไฟล์ที่แนบมากับอีเมล

เมื่อแพร่กระจายจะส่งผลให้ไฟล์และคอมพิวเตอร์เป้าหมายติดไวรัส และได้รับความเสียหายตามไปด้วย โดยที่เจ้าของไม่รู้ตัว

การแฝงตัวมากับพาหะ นี้เอง เลยถูกเรียกว่า ไวรัส

Example of Virus

1986

Brain (c. 1986)

- 1st virus to move from one PC to another

1999

Melissa (c. 1999)

- Attached to email, infected 100K computers
- **Author sentenced on charges of computer theft and sending a damaging computer program.**
- 20 months prison, a fine of \$5000 and three years of supervised release, no use of internet during this time

Michelangelo (c. 1991)

- Attacks only on March 6th

1991

Love Bug (c. 2000)

- Another email virus, deletes files and collects passwords
- **Author has no criminal record because his country has no law against computer misuse (that time).**

2000

Malware

Worm (หนอนอินเทอร์เน็ต)

รุนแรงมากกว่าไวรัสแบบดั้งเดิมมาก

สามารถเจาะไชไปยังเครื่องคอมพิวเตอร์ต่างๆ ได้เอง (ไม่ต้องใช้พาหะ)

ตัวโปรแกรมจะคล้ายๆ กับไวรัสคอมพิวเตอร์ แต่

- มุ่งเน้นการกระจายที่แพร่หลายและรุนแรง
- อาศัยเครือข่ายคอมพิวเตอร์ในการแพร่กระจาย

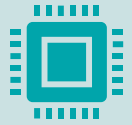
การทำงาน

- ตรวจสอบเพื่อหาเครื่องเป้าหมายที่เชื่อมต่อกับอินเทอร์เน็ตเสียก่อน
- วิ่งเจาะไชไปเครื่องนั้นได้เอง

ลักษณะเด่น

- คือ เวิร์มสามารถสำเนาเข้าตัวมันเองได้อย่างมหาศาลภายในเวลาไม่กี่นาที
- ทำให้ทรัพยากรของระบบของเครื่องคอมพิวเตอร์มีน้อยลง ทำงานผิดพลาด และ อาจส่งผลร้ายแรงได้ เช่น ฮาร์ดดิสก์มีข้อมูลเต็ม หรือ คอมพิวเตอร์ปิดเองโดยไม่มีเหตุผล หรือ shut down network

Morris Worm: the first internet worm



Robert Tappan Morris, Jr.

- Graduate student at Cornell
- Released worm onto Internet from MIT computer



Effect of worm

Spread to significant numbers of Unix computers
Infected computers kept crashing or became unresponsive
Make CERT happens.



Impact on Morris

Suspended from Cornell
3 years' probation + 400 hours community service
\$150,000 in legal fees and fines

Malware

Trojan horse (ม้าโทรจัน)

อาศัยการฝังตัวอยู่ในระบบคอมพิวเตอร์เครื่องนั้น ไม่มีการแพร่กระจายตัวแต่อย่างใด

โปรแกรมจะถูกตั้งเวลาการทำงานหรือควบคุมการทำงานระยะไกลจากผู้ไม่ประสงค์ดี เพื่อให้เข้ามาทำงานยังเครื่องคอมพิวเตอร์เป้าหมายได้

โปรแกรมแบบม้าโทรจันจะแอบเข้าไปอยู่ในเครื่องคอมพิวเตอร์เป้าหมายโดยไม่ให้รู้ตัว โดย

- ซ่อนตัวมากับโปรแกรมมัลแวร์ประโยชน์ให้ใช้งาน เช่น โปรแกรมที่ นศ ไปดาวน์โหลด หรือ เกม หรือ เพลง โดยตัวมันเอง จะประสงค์ร้ายต่อเครื่อง เช่น สั่งให้ เครื่อง เปลี่ยนแปลง ลบ หรือ แก้ไขข้อมูล
- เมื่อนักศึกษาเปิดไฟล์ที่ไป ดาวน์โหลด ตัว โทรจันจะ
 - ฝังตัวอยู่ในเครื่อง เมื่อการทำงานของเครื่องมีเงื่อนไข หรือ ตรงกับเวลาที่ตั้งไว้ไว้ ก็จะทำงานทันที => logic bomb/ Time bomb
 - หรือ ทำการติดต่อไปที่ผู้ไม่ประสงค์ดี และจัดการให้ผู้ไม่ประสงค์ดีสามารถเข้ามาควบคุมการทำงานของเครื่องจากระยะไกล => Remote Admin Trojan (RAT)

ตัวอย่าง

- Keylogger Screen logger

Malware Spyware

คือ โปรแกรมที่เข้ามาอยู่ในคอมพิวเตอร์ โดยที่ผู้เป็นเจ้าของไม่รู้ตัว

จะแอบเก็บข้อมูลของผู้ใช้เครื่อง และ ทำการส่งข้อมูลที่มันเก็บรวบรวมไปให้กับ แหล่งข้อมูลภายนอกในระหว่างที่ผู้ใช้อินเทอร์เน็ตอยู่

ถูกเขียนขึ้นมาใช้งานบนอินเทอร์เน็ตเป็นหลัก

อาจไม่กระทำการร้ายแรง และจุดประสงค์ร้าย เหมือน มัลแวร์พวก ไวรัส หนอน แต่จะสร้างความรำคาญให้กับผู้ใช้เมื่อเชื่อมต่อเข้ากับอินเทอร์เน็ต

เช่น

- การที่นายจ้าง ใช้ โปรแกรม spyware ในการรวบรวมข้อมูลเกี่ยวกับการใช้งานโปรแกรม ของลูกจ้าง
- หรือ การที่บริษัทโฆษณารวบรวมข้อมูลการใช้ บราวซ์เว็บของผู้ใช้

Malware

Spam mail

รูปแบบของจดหมายอิเล็กทรอนิกส์ที่เราไม่ต้องการ

วิธีการก่อกวน

- ส่งอีเมลแบบหว่านแห ให้กับผู้รับจำนวนมากที่อาจไม่รู้จักกันมาก่อน / เชิญชวนให้ซื้อสินค้า หรือ บริการของเว็บ

ส่งมาถึงเราได้อย่างไร

- แฮกเกอร์ที่ได้รับการว่าจ้างในการส่งโฆษณาแบบเหวี่ยงแห นี้ / เราถูกสะกดรอยตามด้วยการใช้โปรแกรมประเภทสปายแวร์

ข้อเสีย

- นำรำคาญ และทำให้พลาดข้อมูลข่าวสารบางฉบับ เนื่องจากเมลล์บ็อกซ์เต็ม

บางประเทศยังไม่จัดว่าเป็น crime

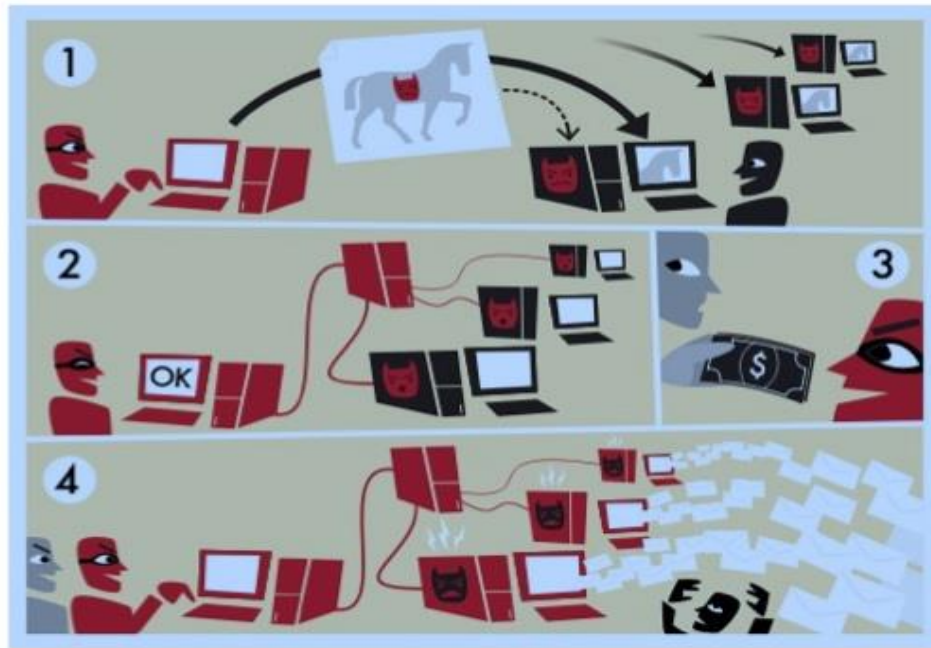
พรบ.คอมพิวเตอร์ 2550 มาตรา 11 “ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท”

Malware

บอตเน็ต (Botnets)

- กลุ่มของเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับเน็ตเวิร์ก เครื่องคอมพิวเตอร์เหล่านี้
 - ถูกควบคุมจาก บุคคลภายนอก (outsider) แบบ ทางไกล (remote)
 - ผู้เป็นเจ้าของเครื่องไม่รู้เลยว่าเครื่องตัวเองถูกคนอื่นแอบเข้ามาใช้
 - Outsider ใช้กลุ่มของเครื่องคอมพิวเตอร์เหล่านี้ในการ โจมตีเน็ตเวิร์กอื่น
- คนร้ายจะติดตั้งโปรแกรมที่ชื่อว่า bots บนเครื่องเหล่านี้เพื่อจะ สร้างเน็ตเวิร์ก botnets หรือที่เรียกว่า zombie army
- หลังจากนั้นจะใช้เครื่องในเน็ตเวิร์กนี้ทำการส่ง สปแอมเมลล์ ไวรัส หรือ มัลแวร์อื่นๆ หรือใช้ในการ ทำ DOS attack

Example of using bot to send SPAM mail.



- 1) A **bot controller** installs bots on vulnerable machines.
- 2) The bots login to a **C&C server**
- 3) A spammer purchases service from the operator
- 4) The operator instructs the botnet to send spam

Denial of Service Attack

- เรียกสั้นๆ ว่า ดอส แอทแทค (DOS attack)
- มีจุดมุ่งหมายในการทำให้ระบบคอมพิวเตอร์ยุ่งยากจนปฏิเสธการให้บริการแก่เครื่องอื่นๆ ตามหน้าที่ปกติ
เช่น
 - ส่งข้อมูลมหาศาล(ที่ไม่มีประโยชน์)ไปให้คอมพิวเตอร์ทำการประมวลผล หรือส่งข้อมูลที่ไม่มีประโยชน์จำนวนมากมายเข้าไปที่ระบบเครือข่ายเพื่อไม่ให้คอมพิวเตอร์สามารถให้บริการอะไรได้เลย
- Distributed DOS (DDOS) ร้ายแรงมากขึ้นไปอีก
 - ซึ่งเครื่องที่เป็น bot (zombie army) จะถูกใช้ในการโจมตีเครื่องคอมพิวเตอร์หลายๆ เครื่องในระบบเครือข่ายซึ่งเคยเกิดขึ้นแล้ว ที่ Yahoo ebay Amazon.com CNN.com โดน DDOS แอทแทค ถึงกับต้องงดให้บริการชั่วคราว

ตย DDoS attack

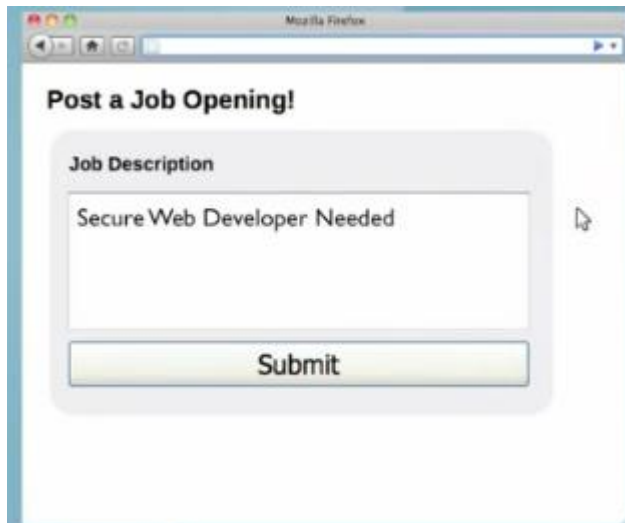
- Massive DDoS attack made Twitter service unavailable for several hours on August 6, 2009
- Three other sites attacked at same time: Facebook, LiveJournal, and Google
- All sites used by a political blogger from the Republic of Georgia
- 4th of July weekend in 2009: DDoS attack on governmental agencies and commercial Web sites in United States and South Korea
- Attack may have been launched by North Korea

Malware SQL injection and Cross Site Scripting Attack (XSS)

- Another way malware may be downloaded without user's knowledge
- Problem appears on Web sites that allow people to read what others have posted
- Attacker injects client-side script into a Web site
- Victim's browser executes script, which may steal cookies, track user's activity, or perform another malicious action

• เกิดจาก Programmer เขียนโค้ดแบบไม่ระวัง !!!

ตัวอย่าง XSS การโพสข้อมูลบนเว็บหางาน [2]



Post a Job Opening!

Job Description

Secure Web Developer Needed

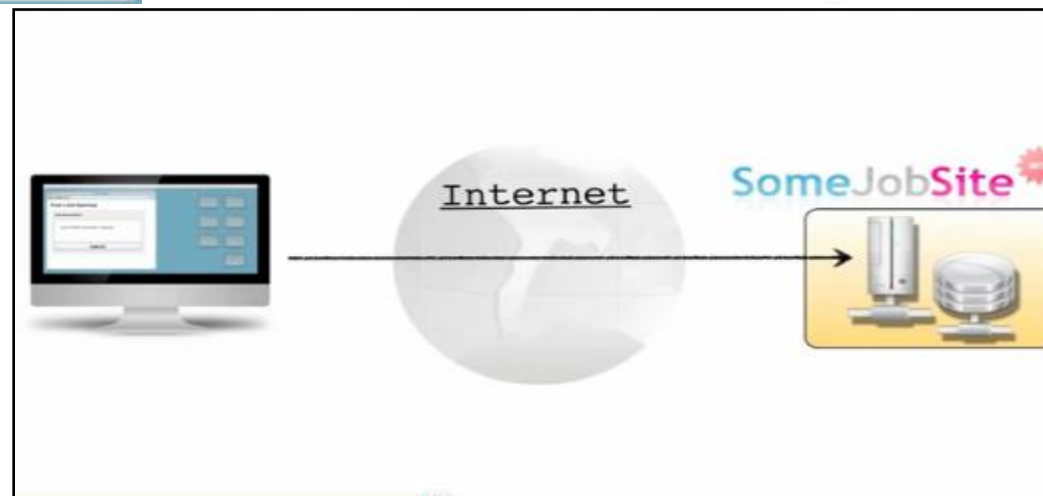
Submit

Static Content

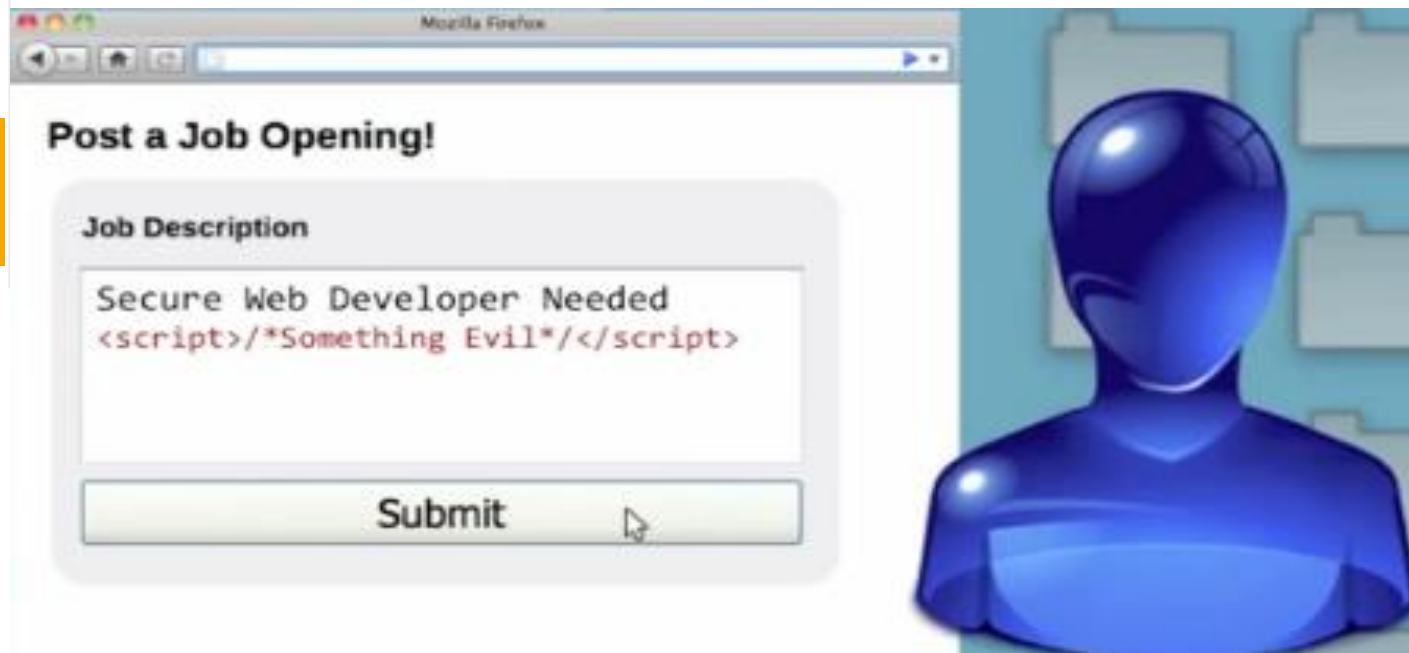
User Supplied Content

```
<html>
<body>
<h1>New Job Posting</h1>
<h2>Job Description</h2>
<hr/>
Secure Web Developer Needed

</body>
</html>
```



<http://www.youtube.com/watch?v=Z9RQSnf8-g&feature=related>



<http://www.youtube.com/watch?v= Z9RQSnf8-g&feature=related>

ที่ browser ของเหยื่อจะไม่เห็น
ในส่วนของ something evil จะ
เห็นแต่ Secure Web Developer
needed

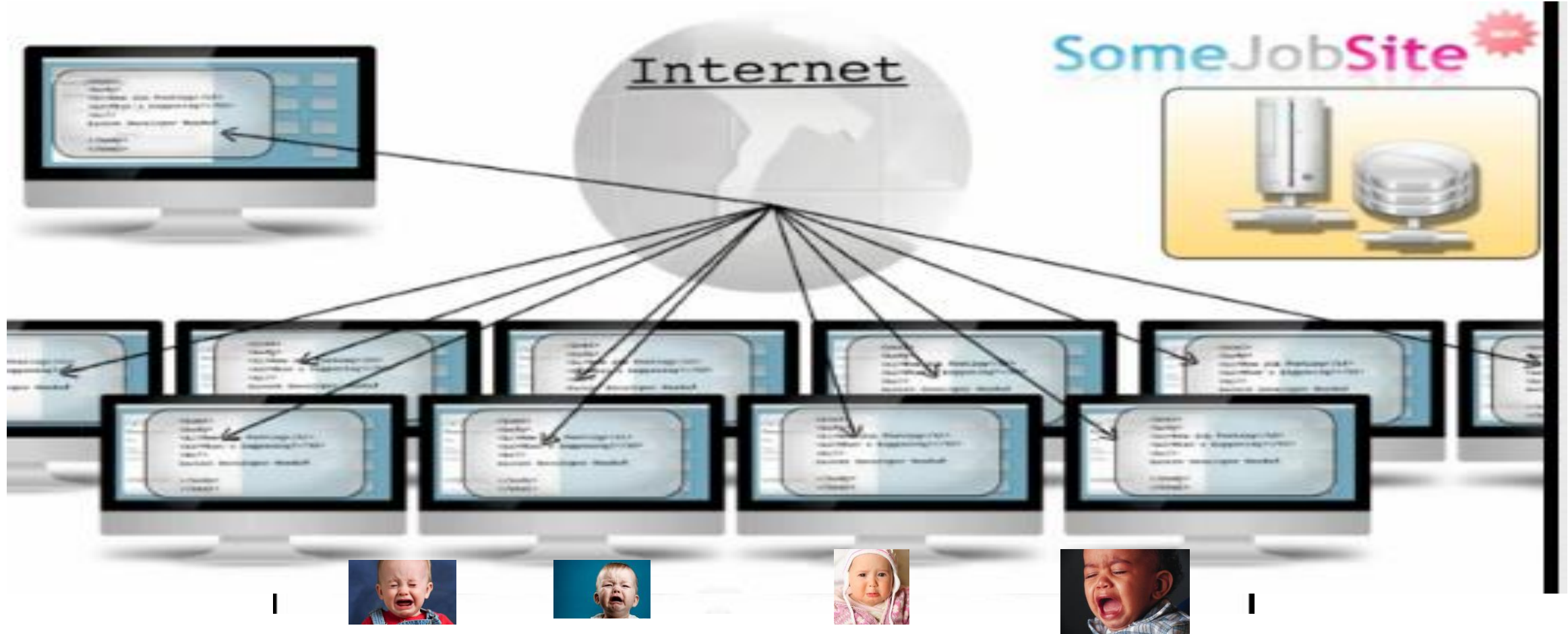
Static Content

User Supplied
Content

```
<html>
<body>
<h1>New Job Posting</h1>
<h2>Job Description</h2>
<hr/>
Secure Web Developer Needed
<script>/*something evil*/</script>
</body>
</html>
```

บรรดาเซิร์ฟเวอร์ของเหยื่อ ไม่สงสัยว่ามีการ
ซ่อนโค้ดอันตรายเพราะคิดว่า script นี้
มาจากเว็บไซต์ที่เชื่อถือได้

script เหล่านี้สามารถที่จะเข้าถึงข้อมูลต่าง ๆ ของเครื่องเหยื่อที่บรรดา
เซิร์ฟเวอร์ของคุณกับเว็บไซต์นี้ !!!!



http://www.youtube.com/watch?v=_Z9RQSnf8-q&feature=related

SQL injection

- Method of attacking a database-driven Web application with improper security
- Attack inserts (injects) SQL query into text string from client to application
- Application returns sensitive information
- Example:
 - statement =
 - "SELECT * FROM users WHERE name = '' + userName + '";" username gets: "" or '1'='1"
 - Result:
 - "SELECT * FROM users WHERE name = " OR '1'='1';"

**Programmer fault : again
!!!**

believed to have played a role in the theft of passwords from LinkedIn, eHarmony and Yahoo. Attack Percentage rose 69% from Q1 to Q2 2012
[<http://www.zdnet.com/sql-injection-attacks-up-69-7000001742/>]

Sidejacking

- Hijacking of an open Web session by capturing a user's cookie
- Sidejacking possible on unencrypted wireless networks because many sites send cookies "in the clear"
- Example: Firesheep
 - extension to Firefox browser
 - made it possible for ordinary computer users to easily sidejack Web sessions

Identity Theft: Phishing

- การ**หลอกลวง**เหยื่อเพื่อล้วงเอาข้อมูลส่วนตัว
- ผู้ที่ต้องการข้อมูลจะส่งอีเมลซึ่งดูเหมือนอีเมลที่มาจากแหล่งข้อมูลนั้นจริง ๆ
- ในอีเมลจะขอข้อมูลบางอย่างที่เป็นข้อมูลส่วนตัวหรือข้อมูลทางการเงินของเหยื่อ
 - เช่น หมายเลขบัตรเครดิต บัญชีเงินฝาก ลอคอิน พาสเวิร์ด
- โดยอาจจะหลอกให้เหยื่อ
 - อีเมลตอบกลับไป
 - ให้ URL มาเพื่อให้เหยื่อไปใส่ข้อมูล โดยจาก URL ดูเหมือน เป็น URL ที่ถูก
- At least 67,000 phishing attacks globally in second half of 2010

ตัวอย่าง การเตือนให้ระวัง phishing จาก Kbank

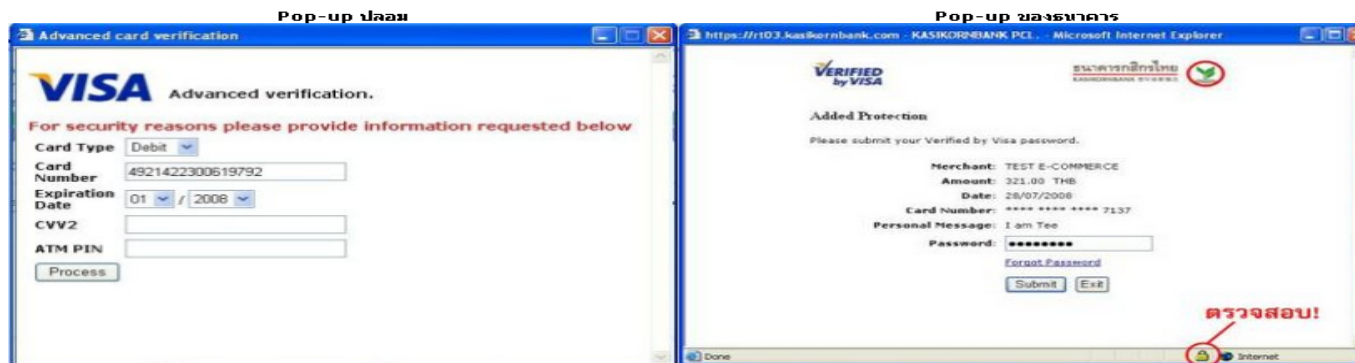


เรียน ลูกค้าผู้ใช้บริการ K-Cyber Banking (บริการธนาคารทางอินเทอร์เน็ตกสิกรไทย)

เรื่อง แจ้งเตือนระวังโจรฉกฉวยข้อมูลบัตรเครดิต/รหัสเอทีเอ็ม

ขณะนี้ มีโจรฉกฉวยข้อมูลชื่อ **"Pws.Sinawal.AU"** ซึ่งนอกจากจะเป็นโปรแกรมที่ฝังตัวในเครื่องคอมพิวเตอร์ เพื่อคัดลอกข้อมูลการพิมพ์แล้ว ยังสามารถติดตามพฤติกรรมผู้ใช้งานทางอินเทอร์เน็ต โดยเมื่อพิมพ์คำว่า "bank" ที่ browser จะมี Pop-up ให้กรอกข้อมูลบัตรเครดิต รวมถึงรหัสเอทีเอ็ม ATM PIN โดยอ้างว่าเพื่อความปลอดภัย ดังภาพ

หากพบ Pop-up ดังกล่าว โปรดอย่าตอบกลับหรือให้ข้อมูลใดๆ ทั้งสิ้น นอกจากนี้ ธนาคารขอให้อ่านหาการตรวจสอบเว็บไซต์ก่อน submit ข้อมูลใดๆ โดยคลิกที่สัญลักษณ์ "รูปแม่กุญแจ" ที่มุมขวาล่างของ browser เพื่อตรวจสอบข้อมูล Certificate ให้แน่ใจว่าเป็นเว็บไซต์ของธนาคารจริง



หากท่านมีข้อสงสัย หรือต้องการสอบถามรายละเอียดเพิ่มเติม โปรดติดต่อ K-Contact Center โทร. 0 2888 8888 กด 03 ทุกวัน ตลอด 24 ชั่วโมง หรืออีเมล eBusinessSupport@kasikornbank.com

ขอแสดงความนับถือ

บมจ. ธนาคารกสิกรไทย

<https://ebank.kasikornbank.com/retailstatic/security/trojan.htm>

Subject ระวังเมลล์ลอคถาม User_Password ครับ

Sender ktnarin@kmitl.ac.th

Date 07.04.2012 03:47

เรียน บุคลากร และนักศึกษาทุกท่าน

หากได้รับ E-mail แจ้งมาถึงท่านว่าอย่างไรก็ตาม แล้วให้ท่านกรอก User และ Password ท่านโปรดอย่ากรอกลงไปเด็ดขาด เพราะมันเป็น mail ที่ลอคเอา User Password จากท่าน สำนักบริการคอมพิวเตอร์ ไม่มีนโยบายดังกล่าวอย่างแน่นอนและจะไม่มีการถาม User Password จากท่านอย่างเด็ดขาด

ตามตัวอย่างข้างล่างที่เห็นเป็น e-mail หลอกว่าโควต้าท่านเดิม และหลอกให้ท่านกรอก user password ซึ่งจริงๆ แล้วระบบ kmitl webmail ท่านสามารถดูว่าโควต้าพื้นที่เหลือเท่าไรได้ที่แถบแสดงด้านซ้าย

จึงเรียนมาเพื่อทราบและโปรดอย่าหลงเชื่อเด็ดขาด

อ.นรินทร์ ธรรมารักษ์วัฒนะ
สำนักบริการคอมพิวเตอร์

Subject: เรียนผู้ใช้ Webmail

Date: Thu, 5 Apr 2012 13:08:10 +0100

From: Webmaster Help Desk <webmailcontrolunit@cyberservices.com>

To:

Reply-To: webmailcontrolunit@cyberservices.com

--

กล่องจดหมายของคุณได้เกินขีด จำกัด
ของการใช้โควต้าซึ่งเป็นที่ตั้งเป็นไปตามที่ผู้จัดการของคุณและการเข้าถึงกล่องจดหมายของคุณผ่านทางพอร์ทัล mail ของเราจะไม่สามารถใช้ได้สำหรับบางครั้ง

ในระหว่างระยะเวลาการบำรุงรักษา

คุณจะไม่สามารถสร้างอีเมลใหม่เพื่อส่งหรือรับอีกครั้งจนกว่าคุณจะตรวจสอบกล่องจดหมายของคุณ

หากต้องการตรวจสอบกล่องจดหมายของคุณคุณสามารถคลิกที่นี่
<http://iohanalander.com/acc/>

ขอบคุณ
ผู้ดูแลระบบ

Copyright (c) 2012 # WEBMASTER ADMIN สิทธิสงวน*

พรบ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

หมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์

ฐานความผิดและบทลงโทษสำหรับการกระทำโดยมิชอบ

มาตรา ๕	การเข้าถึงระบบคอมพิวเตอร์
มาตรา ๖	การล่วงรู้มาตรการป้องกันการเข้าถึง
มาตรา ๗	การเข้าถึงข้อมูลคอมพิวเตอร์
มาตรา ๘	การดักข้อมูลคอมพิวเตอร์โดยมิชอบ
มาตรา ๙	การแก้ไข เปลี่ยนแปลง ข้อมูลคอมพิวเตอร์
มาตรา ๑๐	การรบกวน ขัดขวาง ระบบคอมพิวเตอร์
มาตรา ๑๑	สแปมเมล (Spam Mail)
มาตรา ๑๒	การกระทำความผิดต่อ ประชาชนโดยทั่วไป / ความมั่นคง
มาตรา ๑๓	การจำหน่าย/เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด
มาตรา ๑๔	นำเข้า ปลอม/ เท็จ / ภัยมั่นคง / ลามก/ ส่งต่อ ข้อมูลคอมพิวเตอร์
มาตรา ๑๕	ความรับผิดชอบของผู้ให้บริการ
มาตรา ๑๖	การเผยแพร่ภาพ ดัดต่อ/ดัดแปลง

รวม ๑๒ มาตรา

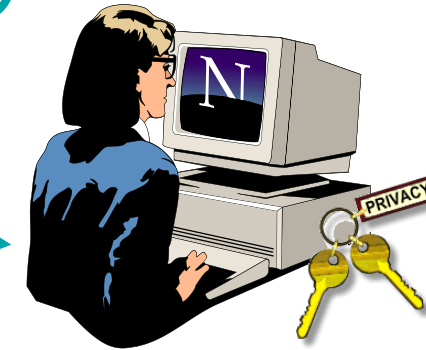
การกระทำความผิดตามมาตรฐานต่างๆ

Unauthorized Access

การแอบเข้าถึง
ข้อมูลคอมพิวเตอร์
มาตรา ๗



การดักข้อมูลคอมพิวเตอร์
มาตรา ๘



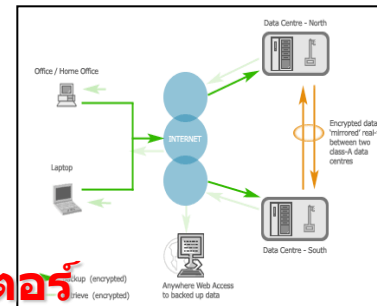
แอบเข้าไปในระบบ
คอมพิวเตอร์ &
แอบรู้มาตรการป้องกัน
ระบบคอมพิวเตอร์
(ขโมย password)
มาตรา ๕ และ
มาตรา ๖



การรบกวน/
แอบแก้ไขข้อมูล
มาตรา ๙



การรบกวนระบบคอมพิวเตอร์
มาตรา ๑๐



สรุปพระราชบัญญัติ (พ.ร.บ.) ว่าด้วยการ
กระทำความผิดเกี่ยวกับคอมพิวเตอร์ พศ
2550 และ พศ **2560**

มาตรา 5 -16

วัตถุประสงค์

- เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์
- หากมีผู้กระทำความผิดประการใด ๆ ให้
 - ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือ
 - ทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือ
 - ใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล
 - แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือ
 - ใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร
- ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน
- สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำความผิดดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

มาตรา	เนื้อหา	จำคุก (หรือ)	ปรับ (บาท)	หมายเหตุ
5	ผู้ใด เข้าถึง โดยมิชอบซึ่ง ระบบคอมพิวเตอร์ ที่มี <u>มาตรการป้องกัน</u> <u>การเข้าถึง</u> โดยเฉพาะและมาตรการนั้น <u>มิได้มีไว้สำหรับตน</u> <i>Unauthorized Access</i>	ไม่เกิน 6 เดือน	ไม่เกิน 10,000	หรือ ทั้งจำและ ปรับ
6	ผู้ใด ล่วงรู้ มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ ที่ ผู้อื่น จัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดย มิชอบ ในประการที่น่าจะ เกิดความเสียหายแก่ผู้อื่น (แอบรู้รหัสเวิร์ดแล้วนำไปให้ผู้อื่น)	ไม่เกิน 1 ปี	ไม่เกิน 20,000	หรือ ทั้งจำและ ปรับ
7	ผู้ใด เข้าถึง โดยมิชอบซึ่ง ข้อมูลคอมพิวเตอร์ ที่มี <u>มาตรการป้องกัน</u> <u>การเข้าถึง</u> โดยเฉพาะและมาตรการนั้น <u>มิได้มีไว้สำหรับตน</u>	ไม่เกิน 2 ปี	ไม่เกิน 40,000	หรือ ทั้งจำและ ปรับ

“ ออกเกือบหัก แอบแฮ็กคอมสามี
จากละครออกเกือบหัก แอบรักคุณสามี ตอนที่ 4 น้องเมย์มีแผนร้าย แอบ
แฮ็ก (Hack) คอมพิวเตอร์ของพี่เจียร์ และก็เอาข้อมูลไปให้บริษัทคู่แข่ง
อีกด้วย แสบไม่เบาเลยนะคะ แต่เห็นร้าย ๆ แบบนี้ แต่สุดท้ายก็ทำไป
เพราะหวังดีนะ ”

#กองปราบปราม #CSD #ออกเกือบหัก #แฮ็ก

”

มาตรา	เนื้อหา	จำคุก (หรือ)	ปรับ (บาท)	หมายเหตุ
8	<p>ผู้ใดกระทำได้ด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดัก รับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบ คอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะ หรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้</p> <p>Eavedropping ดักฟัง Interception</p>	ไม่เกิน 3 ปี	ไม่เกิน 60,000	หรือ ทั้งจำและ ปรับ
9	<p>ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่า ทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ</p> <p>Modification</p>	ไม่เกิน 5 ปี	ไม่เกิน 100,000	หรือ ทั้งจำและ ปรับ
10	<p>ผู้ใดกระทำได้ด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบ คอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่ สามารถทำงานตามปกติได้</p> <p>Interruption DoS</p>	ไม่เกิน 5 ปี	ไม่เกิน 100,000	หรือ ทั้งจำและ ปรับ

มาตรา	เนื้อหา	จำคุก	ปรับ
11	ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข	ไม่มี	ไม่เกิน 100,000 บาท
(เพิ่มเติม 2560)	ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น อันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ ข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย	ไม่มี	ไม่เกิน 200,000 บาท

ปลอมแปลงแหล่งที่มา เช่น IP Spoofing

มาตรา	เนื้อหา	จำคุก(และ)	ปรับ (บาท)
12 แก้ไข ใหม่ใน พรป ปี 2560	ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อ <u>ข้อมูลคอมพิวเตอร์</u> หรือ ระบบคอมพิวเตอร์ ที่เกี่ยวกับการรักษา	1-7 ปี	20,000 – 140,000
	<ul style="list-style-type: none">• <u>ความมั่นคงปลอดภัยของประเทศ</u>• <u>ความปลอดภัยสาธารณะ</u>• <u>ความมั่นคงในทางเศรษฐกิจของประเทศ</u>หรือ• <u>โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ</u>	<div>ความมั่นคงปลอดภัย อันตรายต่อชีวิตและ ทรัพย์สิน ถึงแก่ความตาย</div>	
	ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิด ความเสียหาย ต่อ คอมพิวเตอร์ ดังกล่าว		
	ถ้าการกระทำความผิดตาม มาตรา ๙ หรือ มาตรา ๑๐ เป็นการกระทำต่อ ข้อมูลคอมพิวเตอร์ หรือ ระบบคอมพิวเตอร์ ตามวรรคหนึ่ง	3-15 ปี	60,000-300,000
	ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสาม โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึง แก่ความตาย	5-20 ปี	100,000 – 400,000
12/1 เพิ่มเติม ปี 2560	ถ้าการกระทำความผิดตาม มาตรา ๙ หรือ มาตรา ๑๐ เป็นเหตุให้เกิด อันตราย แก่ บุคคลอื่น หรือ ทรัพย์สินของผู้อื่น	ไม่เกิน 10 ปี	100,000 – 400,000
	ถ้าการกระทำความผิดตาม มาตรา ๙ หรือ มาตรา ๑๐ โดย มิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึง แก่ความตาย	5-20 ปี	100,000 – 400,000

มาตรา	เนื้อหา	จำคุก (หรือ)	ปรับ (บาท)	หมายเหตุ
13	ผู้ใด <u>จำหน่ายหรือเผยแพร่ชุดคำสั่ง</u> ที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม มาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑	ไม่เกิน 1 ปี	ไม่เกิน 20,000	หรือ ทั้งจำและปรับ
เพิ่ม 2560	ผู้ใด <u>จำหน่ายหรือเผยแพร่ชุดคำสั่ง</u> ที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม มาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม	ไม่เกิน 2 ปี	ไม่เกิน 40,000	หรือ ทั้งจำและปรับ
<div><div>ผู้ใด<u>จำหน่ายหรือเผยแพร่ชุดคำสั่ง</u>ที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ หาก ผู้นำไปใช้<ul style="list-style-type: none">ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิด ตาม<ul style="list-style-type: none">- มาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือ- มาตรา ๑๒/๑ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญา ตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย ก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น</div><div><div>ผู้ใด<u>จำหน่ายหรือเผยแพร่ชุดคำสั่ง</u>ที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หาก ผู้นำไปใช้<ul style="list-style-type: none">ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิด ตาม<ul style="list-style-type: none">- มาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือ- มาตรา ๑๒/๑ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญา ตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย ก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น</div><div>ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคหนึ่งหรือวรรคสอง และตามวรรคสาม หรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทางเดียว</div></div></div>				

มาตรา	เนื้อหา	จำคุก(หรือ)	ปรับ (บาท)	หมายเหตุ
14	<p>ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ</p> <p>(1). โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่ง</p> <ul style="list-style-type: none"> ข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือ ข้อมูลคอมพิวเตอร์อันเป็นเท็จ <p>โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน</p> <p>อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา</p> <p>(2). นำเข้าสู่ระบบคอมพิวเตอร์ซึ่ง</p> <ul style="list-style-type: none"> ข้อมูลคอมพิวเตอร์อันเป็นเท็จ <p>โดยประการที่น่าจะเกิดความเสียหายต่อ</p> <ul style="list-style-type: none"> ○ การรักษาความมั่นคงปลอดภัยของประเทศ ○ ความปลอดภัยสาธารณะ ○ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือ ○ โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ <p>หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน</p> <p>(3). นำเข้าสู่ระบบคอมพิวเตอร์ซึ่ง</p> <ul style="list-style-type: none"> ข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับ <ul style="list-style-type: none"> ○ ความมั่นคงแห่งราชอาณาจักร หรือ ○ การก่อการร้ายตามประมวลกฎหมายอาญา <p>(4). นำเข้าสู่ระบบคอมพิวเตอร์ซึ่ง</p> <ul style="list-style-type: none"> ข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก และ ข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้ <p>(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)</p>	ไม่เกิน 5 ปี	ไม่เกิน 100,000	หรือ ทั้งจำ ทั้งปรับ
แก้ไขใหม่ใน พรบ ปี 2560	<p>ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง</p> <p>ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าว</p>	ไม่เกิน 3 ปี	ไม่เกิน 60,000	หรือ ทั้งจำทั้งปรับ หรือ ยอมความได้

นำเข้าข้อมูล => โพสต์ อัฟโหลด

เผยแพร่ => แชร์

มาตรา	เนื้อหา	จำคุก	ปรับ
15 แก้ไข ใหม่ ปี 2560	<u>ผู้ให้บริการ</u> ผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔	ตามมาตรา ๑๔	
	ให้รัฐมนตรีออกประกาศกำหนด <ul style="list-style-type: none"> ขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และ การนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ 		
	ถ้า <u>ผู้ให้บริการพิสูจน์ได้</u> ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้น <u>ไม่ต้องรับโทษ</u> ”		

มาตรา	เนื้อหา	จำคุก(และ)	ปรับ (บาท)	หมายเหตุ
16 แก้ไขใหม่ใน พรบ ปี 2560	ผู้ใด นำเข้าสู่ระบบคอมพิวเตอร์ ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็น ภาพของผู้อื่น ที่ <ul style="list-style-type: none">เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้น<ul style="list-style-type: none">เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี	ไม่เกิน 3 ปี	ไม่เกิน 200,000	ยอมความได้
	ถ้า การกระทำตามวรรคหนึ่ง เป็นการกระทำต่อ ภาพของผู้ตาย และ <ul style="list-style-type: none">การกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำความผิดต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง		<div>นำเข้าข้อมูล => ภาพตัดต่อ</div> <div>ผู้เสียหาย</div> <div>ผู้ตาย ผู้เสียหายเสียชีวิต</div> <div>ยอมความได้</div>	
	ถ้า การกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการ นำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็น <u>การติชมด้วยความเป็นธรรม</u> ซึ่งบุคคลหรือสิ่งใดอัน เป็นวิสัย ของประชาชน ย่อมกระทำ ผู้กระทำ ไม่มีความผิด	ไม่เกิน 3 ปี	ไม่เกิน 200,000	ยอมความได้
	ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้			
	ถ้า ผู้เสียหาย ในความผิดตามวรรคหนึ่งหรือวรรคสอง ตายเสียก่อนร้องทุกข์ ให้ บิดา มารดา คู่สมรส หรือ บุตรของผู้เสียหายร้องทุกข์ได้ และให้ ถือว่าเป็นผู้เสียหาย			

มาตรา	เนื้อหา
16/1	<p>ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่าจำเลย มีความผิด ศาลอาจสั่ง</p> <p>(๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว</p> <p>(๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์</p> <p>วิทยุกระจายเสียง</p> <p>วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณาหรือเผยแพร่</p> <p>(๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากความผิดนั้น</p>
16/2	<p>ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำ</p> <p>ตามมาตรา ๑๖/๑</p> <ul style="list-style-type: none"> • ผู้นั้นต้องทำลายข้อมูลดังกล่าว • หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ตามมาตรา ๑๔ หรือมาตรา ๑๖ แล้วแต่กรณี

ทำลายข้อมูลคำสั่งศาล

มาตรา	เนื้อหา
17	<p>ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ</p> <p>(๑) ผู้กระทำความผิดนั้นเป็ คนไทย และรัฐบาลแห่งประเทศที่ความผิดใด เกิดขึ้นหรือผู้เสียหายใด ร้องขอให้ ลงโทษ หรือ</p> <p>(๒) ผู้กระทำความผิดนั้นเป็ คนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็ ผู้เสียหายและผู้เสียหายใด ร้องขอให้ ลงโทษ จะต้องรับโทษภายในราชอาณาจักร</p>
17/1	<p>ความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๑๑ มาตรา ๑๓ วรรคหนึ่ง</p> <p>มาตรา ๑๖/๒ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๗</p> <p>ให้คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งมีอำนาจเปรียบเทียบได้</p> <p>คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งตามวรรคหนึ่งให้มีจำนวนสามคนซึ่งคนหนึ่งต้องเป็นพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา</p> <p>เมื่อคณะกรรมการเปรียบเทียบได้ทำการเปรียบเทียบกรณีใดและผู้ต้องหาได้ชำระเงินค่าปรับตามคำเปรียบเทียบภายในระยะเวลาที่คณะกรรมการเปรียบเทียบกำหนดแล้ว ให้ถือว่าคดีนั้นเป็นอันเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา</p> <p>ในกรณีที่ผู้ต้องหาไม่ ชำระเงินค่าปรับภายในระยะเวลาที่กำหนด ให้เริ่มนับอายุความในการฟ้องคดีใหม่ นับตั้งแต่วันที่ครบกำหนดระยะเวลาดังกล่าว”</p>

References:

- [Baas08] Sara Baase, A gift of Fire, 3rd, Pearson Prentice Hall, 2008.
- [Tavani07] Ethics & Technology: Ethical Issues in an Age of Information and Communication Technology, 2nd, Wiley, 2007.
- [Reynold07] George W. Reynolds, Ethics in Information Technology, Thomson Course Technology.
- [พนิดา53] พนิดา พานิชกุล, จริยธรรมทางเทคโนโลยีสารสนเทศ, เคทีพี คอมพ์ แอนด์ คอนซัลท์, 2553.
- [Quin13] Michael J. Quinn. Ethics for the Information Age, 4th, Addison Wesley, 2013.