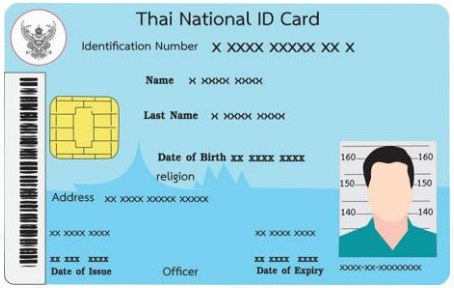
อาชญากรรมคอมพิวเตอร์

นฤดม เพชรทองบุญ
นักวิชาการสิ่งแวดล้อมชำนาญการ

การใช้คอมพิวเตอร์เป็นเครื่องมือในการก่ออาชญากรรม

1. การขโมยหมายเลขบัตรเครดิต

2. การแอบอ้างตัว เป็นการแอบอ้างตัวของผู้กระทำต่อบุคคลที่สามว่าตนเป็นอีกคนหนึ่ง การกระทำในลักษณะนี้จะใช้ลักษณะเฉพาะตัว ได้แก่ หมายเลขบัตรประชาชน



3. การสแกมทางคอมพิวเตอร์ เป็นการกระทำโดยใช้คอมพิวเตอร์เป็นเครื่องมือในการหลอกลวงผู้อื่น เช่นการส่งข้อความ หรือโฆษณาแต่ไม่เป็นความจริงเป็นต้น

ลักษณะของอาชญากรรมคอมพิวเตอร์

ตัวอย่างลักษณะการกระทำที่เป็นอาชญากรรมคอมพิวเตอร์ใน 3 ประเด็น คือ

1. การเข้าถึงและการใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาต
2. การก่อกวนหรือการทำลายข้อมูล
3. การขโมยข้อมูลและอุปกรณ์คอมพิวเตอร์

การก่อกวนหรือการทำลายข้อมูลด้วยโปรแกรมประสงค์ร้าย

เป็นการใช้โปรแกรมที่มุ่งเน้นเพื่อการก่อกวนและทำลายระบบข้อมูลคอมพิวเตอร์โดยเฉพาะ พบมากในปัจจุบันและสร้างความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์เป็นอย่างมาก

กลุ่มโปรแกรมประสงค์ร้ายต่าง ๆ มีดังนี้

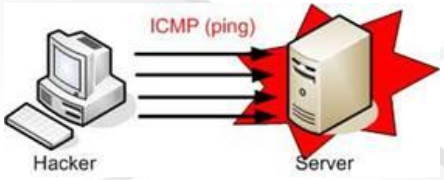
1. ไวรัสคอมพิวเตอร์ (Computer Virus)

2. เวิร์มหรือหนอนอินเทอร์เน็ต (Worm)

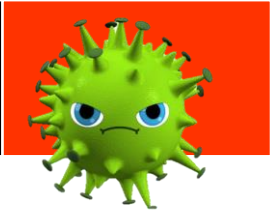
3. ม้าโทรจัน (Trojan horses)

4. ข่าวหลอกลวง (Hoax)

5. การทำให้ระบบปฏิเสธการให้บริการ (Denial of Service หรือ DoS)

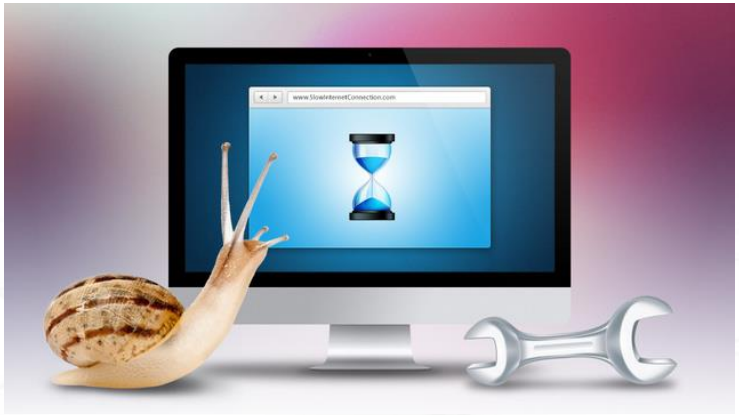


ไวรัสคอมพิวเตอร์ (Computer Virus)



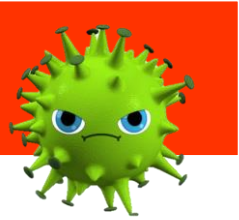
ลักษณะของไวรัสคอมพิวเตอร์

1. ไวรัสที่แสดงข้อความรบกวนหรือทำให้คอมพิวเตอร์ทำงานช้าลง แต่จะไม่ทำลายข้อมูล



2. ทำลายการทำงานของระบบคอมพิวเตอร์ ได้แก่ การลบไฟล์ การปิดเครื่องคอมพิวเตอร์

ไวรัสคอมพิวเตอร์ (Computer Virus)



ไวรัสคอมพิวเตอร์จะแบ่งออกเป็น 3 ชนิดคือ

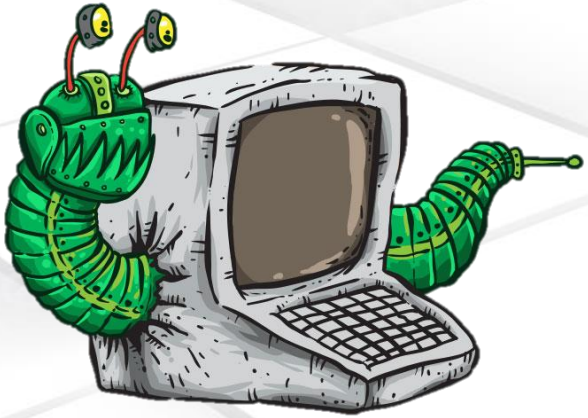
1. ทำงานบน Boot sector เรียกว่า ไวรัสระบบ (system virus) จะทำงานเมื่อเริ่มเปิดระบบ

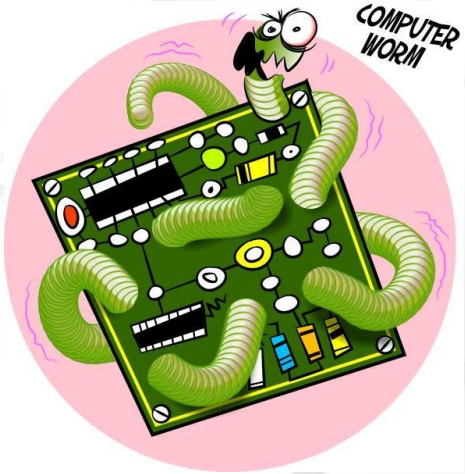
2. ไวรัสติดที่แฟ้มงานหรือโปรแกรม ไวรัสชนิดนี้จะฝังตัวอยู่ตามไฟล์ต่าง ๆ ส่วนใหญ่จะเป็นไฟล์ที่มีนามสกุลเป็น .exe และ .com โดยปกติการติดไวรัสประเภทนี้มาจากการดาวน์โหลดไฟล์หรือโปรแกรมจากอินเทอร์เน็ต หรือการเปิดไฟล์ที่แนบมากับอีเมล์

3. แมโครไวรัส (Macro virus) เป็นไวรัสที่ทำงานบนโปรแกรมที่ใช้ภาษาแมโคร เช่น โปรแกรมประมวลผลคำ และโปรแกรมตารางคำนวณ

เวิร์มหรือหนอนอินเทอร์เน็ต (Worm)

- เป็นโปรแกรมคอมพิวเตอร์ที่จะกระจายตัวเองเช่นเดียวกับไวรัส แต่แตกต่างกันที่ไวรัสต้องให้มนุษย์สั่งการเรียกใช้งาน ในขณะที่เวิร์มจะแพร่กระจายจากคอมพิวเตอร์สู่คอมพิวเตอร์เครื่องอื่น ๆ โดยผ่านทางอีเมล์ และอินเทอร์เน็ต
- ลักษณะที่เด่นของเวิร์ม คือ สามารถสำเนาซ้ำตัวมันเองได้อย่างมหาศาลภายในเวลาเพียงไม่กี่นาที
- ตัวอย่างเวิร์มที่รู้จักกันแพร่หลาย เช่น "Nimda","W32.Sobig", "W32.bugbear", "W32.blaster“ และ "Love Bug" เป็นต้น

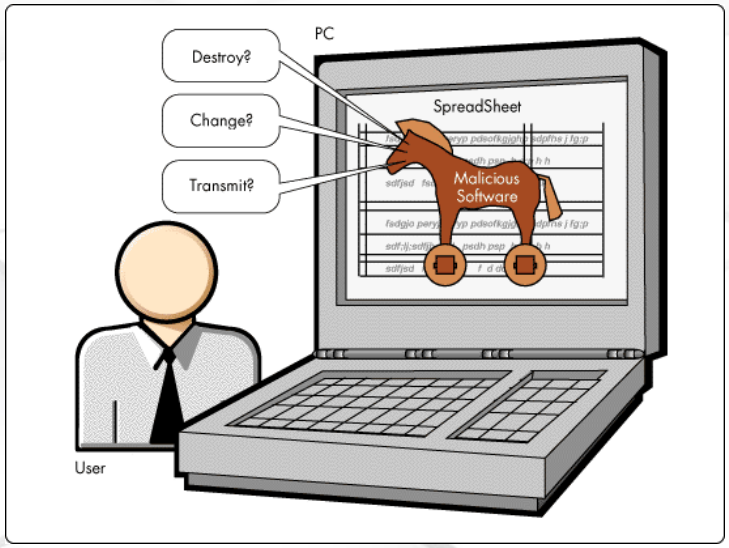




ม้าโทรจัน (Trojan horses)

- โปรแกรมคอมพิวเตอร์ที่ถูกบรรจุเข้าไปในคอมพิวเตอร์เพื่อลอบเก็บข้อมูลของคอมพิวเตอร์เครื่องนั้น เช่น ข้อมูลชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร หมายเลขบัตรเครดิต และข้อมูลส่วนบุคคลอื่น ๆ

โดยส่วนใหญ่แฮกเกอร์จะส่งโปรแกรมเข้าไปในคอมพิวเตอร์เพื่อดักจับข้อมูลดังกล่าว แล้วนำไปใช้ในการเจาะระบบ และเพื่อโจมตีคอมพิวเตอร์, เซิร์ฟเวอร์, หรือระบบเครือข่ายอีกที ซึ่งเป็นที่รู้จักกันในชื่อการโจมตีเพื่อ "ปฏิเสธการให้บริการ" (Denial of Services)

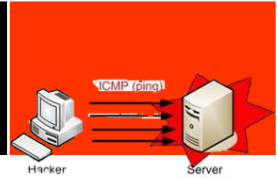


ข่าวหลอกลวง (Hoax)

เป็นการส่งข้อความต่อ ๆ กันเหมือนจดหมายลูกโซ่เพื่อให้เกิดความเข้าใจผิด โดยอาศัยเทคนิคทางจิตวิทยาทำให้ข่าวสารนั้น น่าเชื่อถือ เช่น

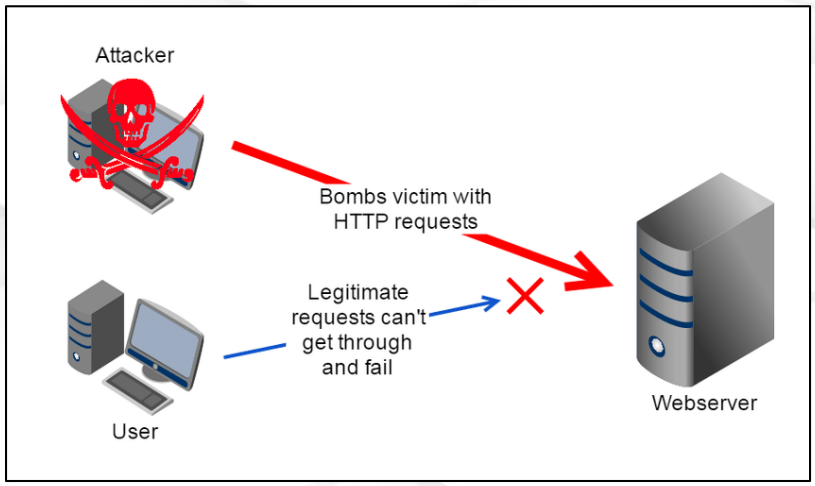
- "Virtual Card for You"
- "Life is Beautiful"
- "FAMILY PICTURES"
- โปรดอย่าดื่ม.....
- เครื่องดื่มยี่ห้อ.....
- โปรดอย่าใช้มือถือยี่ห้อ.....

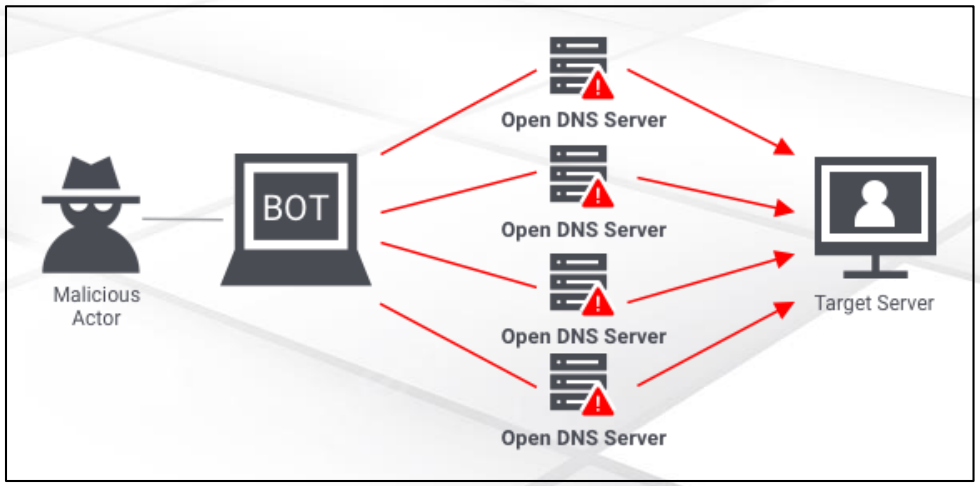
การทำให้ระบบปฏิเสธการให้บริการ (Denial of Service)



- เป็นการพยายามทำให้เครื่องหรือทรัพยากรเครือข่ายเป้าหมาย ใช้บริการไม่ได้
  เช่น ขัดขวางหรือชะลอบริการของแม่ข่ายที่เชื่อมโยงกับอินเทอร์เน็ตอย่างชั่วคราวหรือถาวร

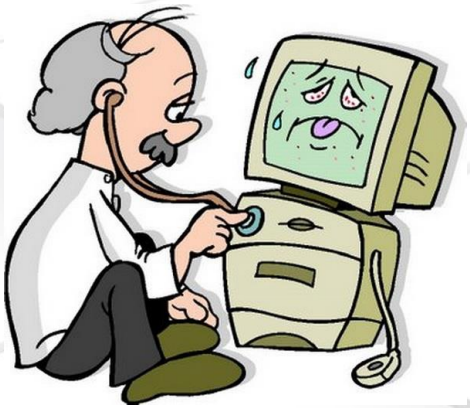
- การโจมตีโดยปฏิเสธการให้บริการแบบกระจาย (distributed denial-of-service (DDoS) attack)
  คือ การโจมตีซึ่งใช้แหล่งต้นทางเป็นเลขที่อยู่ไอพีจำนวนมาก ส่งปริมาณการเข้าชมจำนวนมากไปยังเครื่องหรือทรัพยากรเครือข่ายเป้าหมายให้ใช้บริการไม่ได้





ข้อสังเกตเพื่อการตรวจสอบว่าเครื่องคอมพิวเตอร์ได้รับไวรัส เวิร์ม และม้าโทรจัน หรือไม่

1. มีข้อความหรือภาพแปลก ๆ แสดงบนจอภาพ
2. มีเสียงที่ผิดปกติหรือเสียงเพลงเปิดขึ้นเป็นบางเวลา
3. หน่วยความจำคอมพิวเตอร์ลดน้อยกว่าที่ควรจะเป็น
4. โปรแกรมหรือไฟล์หายไป โดยที่ผู้ใช้ไม่ได้ลบทิ้ง
5. มีโปรแกรมแปลกปลอมเข้ามา
6. ขนาดของไฟล์ใหญ่ผิดปกติ
7. การทำงานของไฟล์หรือโปรแกรมผิดปกติจากเดิม



Phishing


Password:


ชำระเงินออนไลน์อุ่นใจ...
ต้องรู้จักคำว่า
PHISHING
Phishing เป็นคำพ้องเสียงจากคำว่า Fishing หมายถึงการตกปลา เปรียบเทียบง่าย ๆ
ลองจินตนาการว่าเหยื่อล่อที่ใช้ตกปลาคือกลวิธีที่ผู้ไม่หวังดีใช้หลอกลวง โดยมักเป็นการปลอมอีเมล
หรือหน้าเว็บไซต์ที่มีข้อความทำให้ผู้อ่านหลงเชื่อว่าเป็นของจริง จนตกเป็นเหยื่อ
ปลอมอีเมล
ให้ดูเหมือนของหน่วยงานที่น่าเชื่อถือ เช่น ธนาคาร
โดยเขียนข้อความในอีเมลเชิงหลอกล่อ
เพื่อให้เหยื่อส่งข้อมูลส่วนตัวกลับไปให้ผู้ไม่หวังดี
หรือให้เหยื่อคลิกลิงก์ไปยังหน้าเว็บไซต์ปลอม
FAKE
ปลอมเว็บไซต์
ให้ดูเหมือนเว็บไซต์ทางการเงิน เช่น ธนาคารออนไลน์
ซึ่งเป็นช่องทางที่นำไปสู่บัญชีเก็บเงินของลูกค้า
เมื่อเหยื่อหลงเชื่อกรอกข้อมูลรหัสประจำตัว และ Password
ผู้ไม่หวังดีก็สามารถเข้าถึงและทำธุรกรรมทางการเงินของเราได้ทันที

Phishing

คำแนะนำ

1 URL

ไม่คลิกลิงก์ที่แนบมาในอีเมลของคนที่เรา
ไม่รู้จัก ถ้าต้องการเข้าเว็บไซต์นั้นจริง ๆ
ขอให้พิมพ์ URL ด้วยตัวเอง

2 E-Mail

ระวังอีเมลที่ขอให้ส่งข้อมูลส่วนตัวกลับไป
หรือ อีเมลที่มาพร้อมกับลิงก์

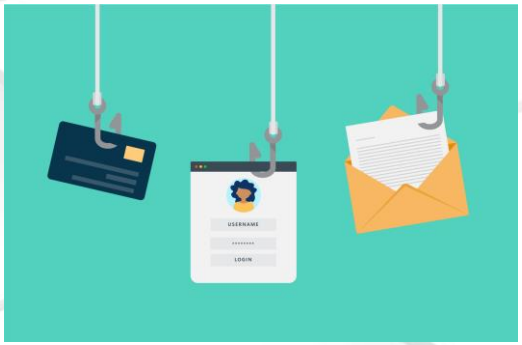
3 HTTPS

โดยปกติธนาคารจะใช้งาน HTTPS เพื่อป้องกันการโจมตี
ทางเครือข่าย ดังนั้นควรสังเกตให้แน่ใจว่าเว็บไซต์ที่ทำ
ธุรกรรมออนไลน์เป็น HTTPS ก่อนให้ข้อมูลส่วนตัว

*แต่บางครั้งหน้าเว็บไซต์ปลอมก็มีการนำใช้งาน HTTPS เช่นกัน ดังนั้นผู้ใช้ควรตรวจสอบ URL ให้ถูกต้องด้วย

4 ANTI-VIRUS

ติดตั้งโปรแกรมแอนติไวรัส แอนติสแปม และไฟร์วอลล์
และหมั่นอัปเดตโปรแกรมให้เป็นเวอร์ชันล่าสุดเสมอ



Phishing

ตัวอย่าง Phishing mail

citi

Dear Citibank member,
Due to database operations some online banking accounts and credit cards can be lost. We have to ask you to confirm your online banking or credit card information.
Please follow the link below and submit required information:

https://web.da-us.citibank.com/signin/citifi/scripts/login2/user_setup.jsp

Thank you
Please do

---- Forwarded Message ----
From: Kasikorn Bank <alert@kasikorn.com>
To: [redacted]com
Sent: Saturday, September 15, 2012 7:23 PM
Subject: New Message From Kasikorn Bank

ธนาคารกสิกรไทย

Dear Esteemed Customer,
At Kasikorn Bank Thailand, We take security Seriously. You are recieving This Email as you are a customer with Kasikorn Bank.
Your Account has been flagged for security issues, you must now login and validate your account for your own protection.
Click here to login and validate your Account
This Email is subject to security From Kasikorn Bank,Please view our privacy polly statement.
Please don't click any link in the phishing e-mail.
Regards,
Technical Service /Internet security,
Kasikorn Bank,
Thailand

Kasikorn Bank © 2012 All Rights Reserved

TMB

TMB BANK PUBLIC COMPANY LIMITED

* Your Login Username: .....
* Your Login Password: .....
* Your Date of Birth: .....
* Your Country Or Territory: .....
* Send to : webmail_accountlogin@instructor.net

3 ขอพาสเวิร์ดและข้อมูลส่วนตัว

Sincerely,

Mr. Rajit Supinit | Distributor-West
(Foreign Exchange Operations)

TMB 1558

Phishing

ตัวอย่าง Phishing mail

From: PayPal Billing Department <Billing@PayPal.com>
Subject: **Credit/Debit card update**
Date: May 4, 2006 08:16:08 PDT
To: [redacted]@bustspammers.com
Reply-To: Billing@PayPal.com

PayPal

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

http://66.160.154.156/catalog/paypal/

Sincerely,
Paypal customer department

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

Wed 10/5/2016 11:21 PM

MO

Microsoft Outlook <msoutlook94@service.out1ook.com>

Your Password Has Expired

To

Password Expired.

Your password for the Microsoft Outlook account [redacted] has expired.

For your account's security, your current password will cease to work shortly .

You are now required to **change your password** immediately.

Click below to change your password

http://msoutlook.service.outlook.com/msacks/reset.html

This is a system notification not an email message and you can't reply to it.

Phishing

จับผิดอีเมลลวงให้ตกเป็นเหยื่อฟิชชิง

Phishing (ฟิชชิง) คือ

การปลอมแปลงอีเมลให้เหมือนว่าส่งมาจากหน่วยงาน องค์กร หรือสถาบันที่มีชื่อเสียง เพื่อหลอกให้เหยื่อหลงกลใส่ข้อมูลสำคัญส่วนตัว จากนั้น ก็จะนำข้อมูลที่ได้จากเราไปสวมรอยสร้างความเสียหายที่เกี่ยวข้องกับเรื่องเงิน

ลักษณะที่น่าสงสัยของฟิชชิงอีเมล

1. อีเมลที่ไม่น่าเชื่อถือ
2. มีไฟล์แนบมาด้วยเช่น .zip
3. ไม่มีการระบุชื่อ-นามสกุล หรือข้อมูลสำคัญ
4. มีคำสะกดผิด
5. มีลิงก์น่าสงสัย
6. มีข้อความแจ้งเตือนว่า ด่วน หรือสำคัญมาก

บัญชีเมลแบบไหนคือเป้าหมาย?

- บัญชีเมลที่ไม่มีการเคลื่อนไหวเกิน 6 เดือน
- บัญชีที่ใช้ล็อกอินหลาย ๆ แอคเคาท์
- บัญชีธุรกิจติดต่องานสำคัญ
- บัญชีที่ไม่เคยเปลี่ยนรหัสผ่าน

Phishing

เว็บปลอม

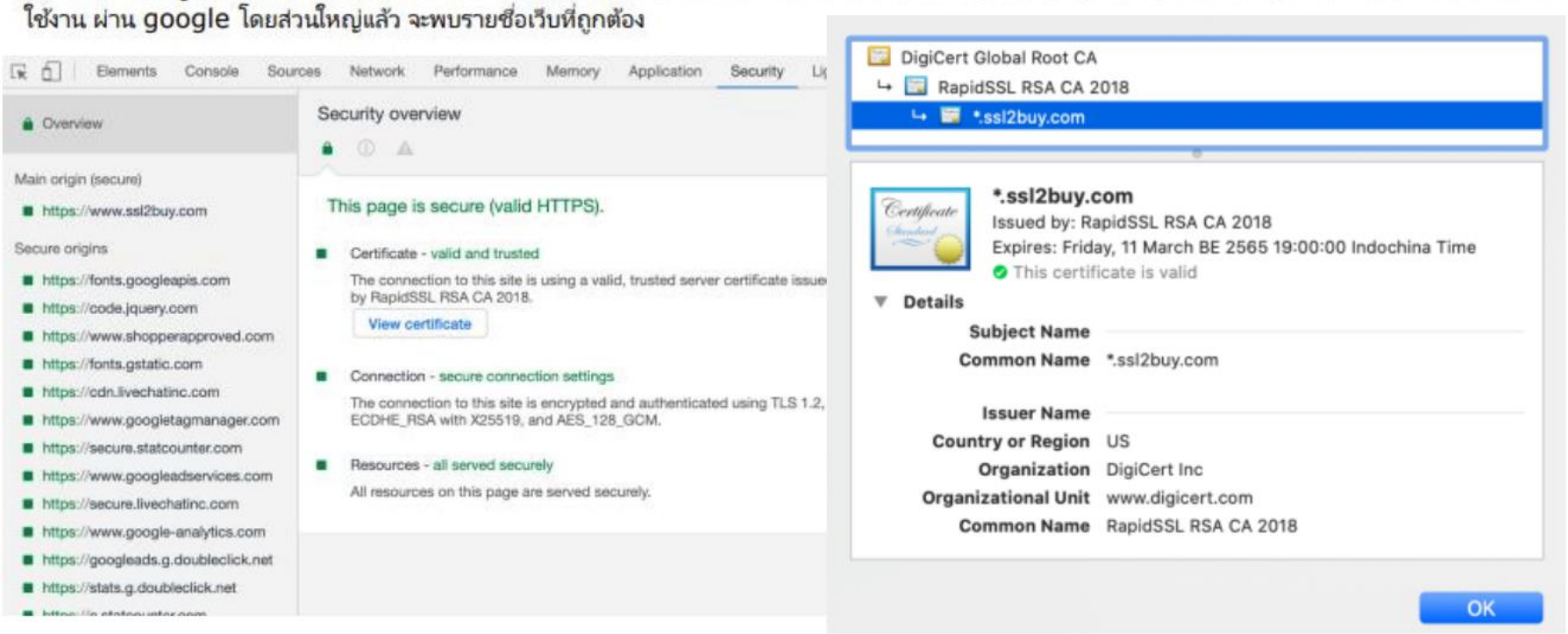
เทคนิคป้องกัน และการตรวจสอบ

อย่าใจร้อน

กรณีใช้งานระบบสำคัญๆ ให้ตรวจเช็ค urls ที่เข้าใช้งานทุกครั้ง และหากเป็นระบบของธนาคาร โดยส่วนใหญ่แล้วชื่อ web urls จะต้องขึ้นต้นด้วย https และเมื่อเข้าใช้งานต้องไม่มีข้อความเตือนเรื่องความปลอดภัย หรือ เตือนว่า Certificate Error

หาความจริง

url โดยส่วนใหญ่มักจะตั้งชื่อให้มีความใกล้เคียงกับเว็บจริง อาจจะเปลี่ยนแค่ตัวอักษรตัวใดตัวหนึ่งเท่านั้น เราสามารถตรวจสอบหาเว็บจริง ได้โดยพิมพ์ชื่อเว็บไซค์ที่จะเข้าใช้งาน ผ่าน google โดยส่วนใหญ่แล้ว จะพบรายชื่อเว็บที่ถูกต้อง



Ransomware

Ransomware เป็นมัลแวร์(Malware) ประเภทหนึ่งที่มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่นๆ คือ ไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้ใช้งานแต่อย่างใด

ทำการเข้ารหัสหรือล็อกไฟล์ ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ

ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใดๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา

ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ

Ransomware

รูปแบบการโจมตีของ Ransomware เพื่อยึดข้อมูลในเครื่องคอมพิวเตอร์ของเหยื่อ

1
MALICIOUS
MALICIOUS
ผู้ไม่หวังดีแฮกเว็บไซต์แล้วฝังมัลแวร์
ที่จะใช้เผยแพร่ หรือใช้วิธีส่งอีเมลที่มี
ไฟล์แนบเป็นมัลแวร์ไปยังผู้ใช้

2
ผู้ใช้เข้าเว็บไซต์ที่มีมัลแวร์ฝังอยู่
หรือเปิดไฟล์แนบในอีเมลที่เป็นมัลแวร์

3
100%
มัลแวร์ถูกดาวน์โหลดและติดตั้ง
ลงในคอมพิวเตอร์ของผู้ใช้

4
มัลแวร์เข้าควบคุมคอมพิวเตอร์
ทำให้ผู้ใช้ไม่สามารถใช้งานคอมพิวเตอร์ได้

5
ผู้ใช้ยอมชำระเงินให้ผู้ไม่หวังดี
โดยอาจจ่ายเป็นสกุลเงินจริงหรือเงินเสมือน
เช่น Bitcoin ขึ้นอยู่กับเงื่อนไขของมัลแวร์แต่ละตัว

6
ผู้ไม่หวังดีส่งรหัสสำหรับถอดรหัสลับข้อมูล
เพื่อให้ใช้งานคอมพิวเตอร์ได้
* "ในบางกรณีผู้ไม่หวังดีรับเงินแล้วก็ไม่ส่งรหัสข้อมูล"

Ransomware

ข้อแนะนำในการป้องกันความเสียหายจากภัย Ransomware

ดำเนินการทันทีเพื่อรักษาความพร้อมใช้งานของข้อมูล

- สำรองข้อมูลสำคัญที่ใช้งานอย่างสม่ำเสมอ
- ติดตั้ง/อัปเดตโปรแกรมป้องกันไวรัส (Antivirus) รวมถึงอัปเดตโปรแกรมอื่น ๆ

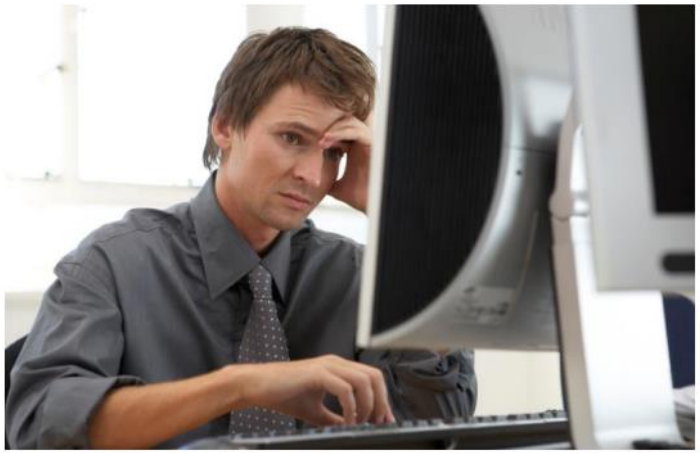
สร้างความตระหนักในการใช้อีเมลและเปิดเว็บไซต์

- ไม่คลิกลิงก์หรือเปิดไฟล์ที่มาพร้อมกับอีเมลที่น่าสงสัย
- ดาวน์โหลดซอฟต์แวร์จากแหล่งที่น่าเชื่อถือเท่านั้น

ในกรณีที่ตกเป็นเหยื่อ

- ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อและอุปกรณ์เก็บข้อมูลเคลื่อนที่
- ให้ติดต่อกับเจ้าหน้าที่ IT ของหน่วยงานในทันที

รายงานปัญหาคอมพิวเตอร์ที่น่าสงสัย



If your system acts unusual!

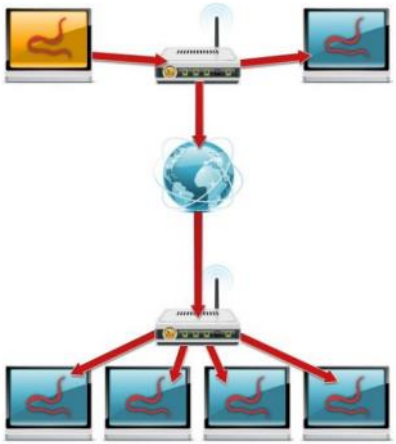
พบอุบัติการณ์ที่ไม่ปกติ

Report immediately

รายงานผู้เกี่ยวข้องโดยด่วน

Trojan Horse

Spyware



Worm

พ.ร.บ. คอมพิวเตอร์ 2550 และ พ.ร.บ. คอมพิวเตอร์ 2560

สาระสำคัญของ พ.ร.บ. คอมพิวเตอร์ 2550

- หลักการสำคัญในการกำหนดฐานความผิดและบทลงโทษต่อการกระทำที่อาศัยคอมพิวเตอร์ในการสร้างความเสียหายต่อบุคคลอื่นหรือส่วนรวม รวมทั้งกลไกในการติดตามและปราบปราม
- กำหนดให้มี "พนักงานเจ้าหน้าที่" เป็นผู้มีอำนาจในการดำเนินการ
- ภาระหน้าที่หลักของผู้ประกอบการคือจะต้องเก็บ Log ข้อมูลจราจรทางคอมพิวเตอร์ที่สามารถ map IP เพื่อยืนยันตัวตนของผู้ก่อเหตุอย่างน้อย 90 วัน และต้องมอบให้เจ้าพนักงานเมื่อมีการร้องขอ

สาระสำคัญของ พ.ร.บ. คอมพิวเตอร์ 2560 (สิ่งที่เปลี่ยนแปลง)

- ฐานความผิดในกฎหมายปี 2550 ไม่ครอบคลุมถึงรูปแบบการกระทำความผิดที่เปลี่ยนแปลงไป โดยเฉพาะการฉ้อโกง หลอกลวง ผ่านโซเชียลเน็ตเวิร์กชื่อดังอย่าง Facebook, Instagram, Line เป็นต้น
- พ.ร.บ. นี้ทำให้สามารถเอาผิดกับคนแชร์ได้ แต่คนแชร์ต้องรู้ก่อนว่าข้อมูลนั้นเป็นเท็จและเจตนาแชร์ (ต่อให้ไม่ได้เป็นคนทำหรือคนเขียน แต่การแชร์ก็มีความผิดเท่ากับคนทำ)
- Spam ไม่ใช่เพียงแค่ email ขายของ แต่การฝากร้านใน Facebook, IG หรือ ส่ง SMS โฆษณา โดยไม่รับความยินยอม ให้ผู้รับสามารถปฏิเสธข้อมูลนั้นได้
- ไม่โพสต์สิ่งลามกอนาจาร ที่ทำให้เกิดการเผยแพร่สู่ประชาชนได้ (แต่เซฟเก็บไว้ดูเองไม่ถือว่าผิด)

สรุป 13 ข้อ พ.ร.บ.คอมพิวเตอร์ 2560

1. การฝากร้านใน Facebook, IG ถือเป็นสแปม ปรับ 200,000 บาท
2. ส่ง SMS โฆษณา โดยไม่รับความยินยอม ให้ผู้รับสามารถปฏิเสธข้อมูลนั้นได้ ไม่เช่นนั้นถือเป็นสแปม ปรับ 200,000 บาท
3. ส่ง Email ขายของ ถือเป็นสแปม ปรับ 200,000 บาท
4. กด Like ได้ไม่ผิด พ.ร.บ.คอมพ์ฯ ยกเว้นการกดไลค์ที่เป็นเรื่องเกี่ยวกับสถาบัน เสี่ยงเข้าข่ายความผิดมาตรา 112 หรือมีความผิดร่วม
5. กด Share ถือเป็นการเผยแพร่ หากข้อมูลที่แชร์มีผลกระทบต่อผู้อื่น อาจเข้าข่ายความผิดตาม พ.ร.บ.คอมพ์ฯ โดยเฉพาะที่กระทบต่อบุคคลที่ 3
6. พบข้อมูลผิดกฎหมายอยู่ในระบบคอมพิวเตอร์ของเรา แต่ไม่ใช่สิ่งที่เจ้าของคอมพิวเตอร์กระทำเอง สามารถแจ้งไปยังหน่วยงานที่รับผิดชอบได้ หากแจ้งแล้วลบข้อมูลออกเจ้าของก็จะไม่มีความผิดตามกฎหมาย เช่น ความเห็นในเว็บไซต์ต่าง ๆ รวมไปถึงเฟซบุ๊ก ที่ให้แสดงความคิดเห็น หากพบว่าการแสดงความเห็นผิดกฎหมาย เมื่อแจ้งไปที่หน่วยงานที่รับผิดชอบเพื่อลบได้ทันที เจ้าของระบบเว็บไซต์จะไม่มีความผิด

สรุป 13 ข้อ พ.ร.บ.คอมพิวเตอร์ 2560

7. สำหรับ แอดมินเพจ ที่เปิดให้มีการแสดงความเห็น เมื่อพบข้อความที่ผิด พ.ร.บ.คอมพ์ฯ เมื่อลบออกจากพื้นที่ที่ตนดูแลแล้ว จะถือเป็นผู้พ้นผิด

8. ไม่โพสต์สิ่งลามกอนาจาร ที่ทำให้เกิดการเผยแพร่สู่ประชาชนได้

9. การโพสเกี่ยวกับเด็ก เยาวชน ต้องปิดบังใบหน้า ยกเว้นเมื่อเป็นการเชิดชู ชื่นชม อย่างให้เกียรติ

10. การให้ข้อมูลเกี่ยวกับผู้เสียชีวิต ต้องไม่ทำให้เกิดความเสื่อมเสียเชื่อเสียง หรือถูกดูหมิ่น เกลียดชัง ญาติสามารถฟ้องร้องได้ตามกฎหมาย

11. การโพสต์ด่าว่าผู้อื่น มีกฎหมายอาญาอยู่แล้ว ไม่มีข้อมูลจริง หรือถูกตัดต่อ ผู้ถูกกล่าวหา เอาผิดผู้โพสต์ได้ และมีโทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 200,000 บาท

12. ไม่ทำการละเมิดลิขสิทธิ์ผู้ใด ไม่ว่าข้อความ เพลง รูปภาพ หรือวิดีโอ

13. ส่งรูปภาพแชร์ของผู้อื่น เช่น สวัสดี อวยพร ไม่ผิด ถ้าไม่เอาภาพไปใช้ในเชิงพาณิชย์ หารายได้

Thank you

Cyber Security