10301112 เทคโนโลยีสารสนเทศและการสื่อสาร

บทที่ 6: ความมั่นคงคอมพิวเตอร์ และ ภัยคุกคามทางด้านไซเบอร์

ผู้ช่วยศาสตราจารย์ ดร. ปวีณ เขื่อนแก้ว

สาขาวิชาวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์ มหาวิทยาลัยแม่โจ้

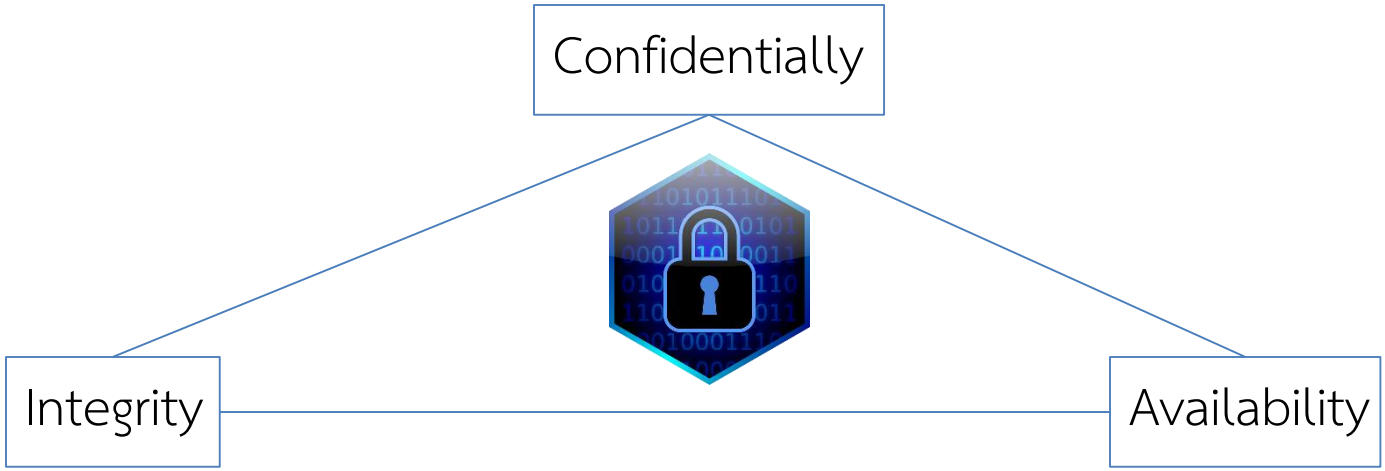
CyberSecurity หรือ **ความมั่นคงปลอดภัยทางไซเบอร์** คือการนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย, โครงสร้างพื้นฐานทางสารสนเทศ, ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

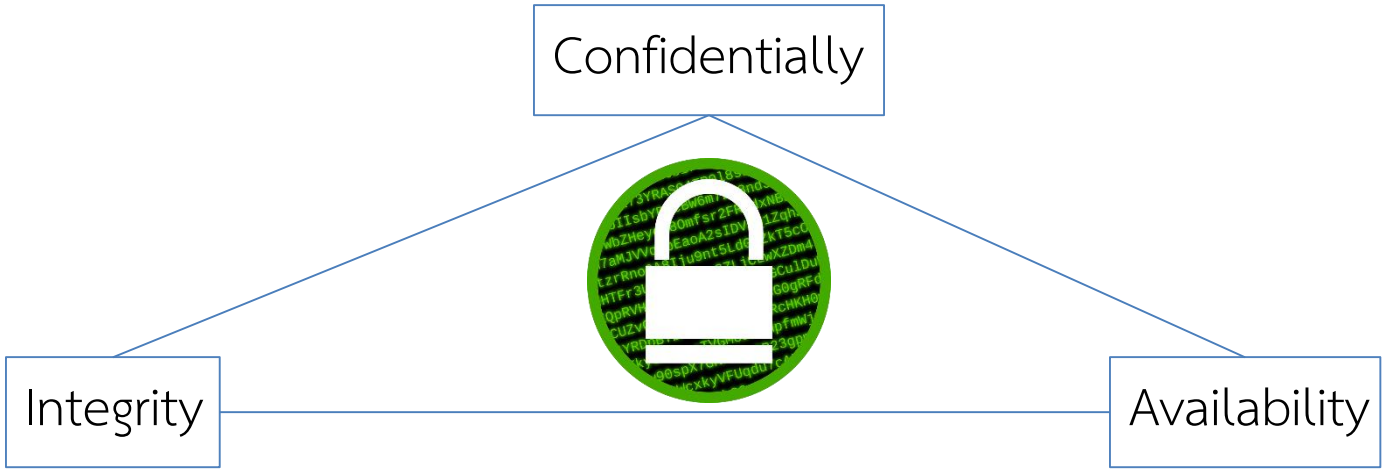
พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล
มาตรฐานด้านความปลอดภัย ISO 2700127001(ระบบบริหารจัดการความปลอดภัยของข้อมูล)

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์

CIA Triad



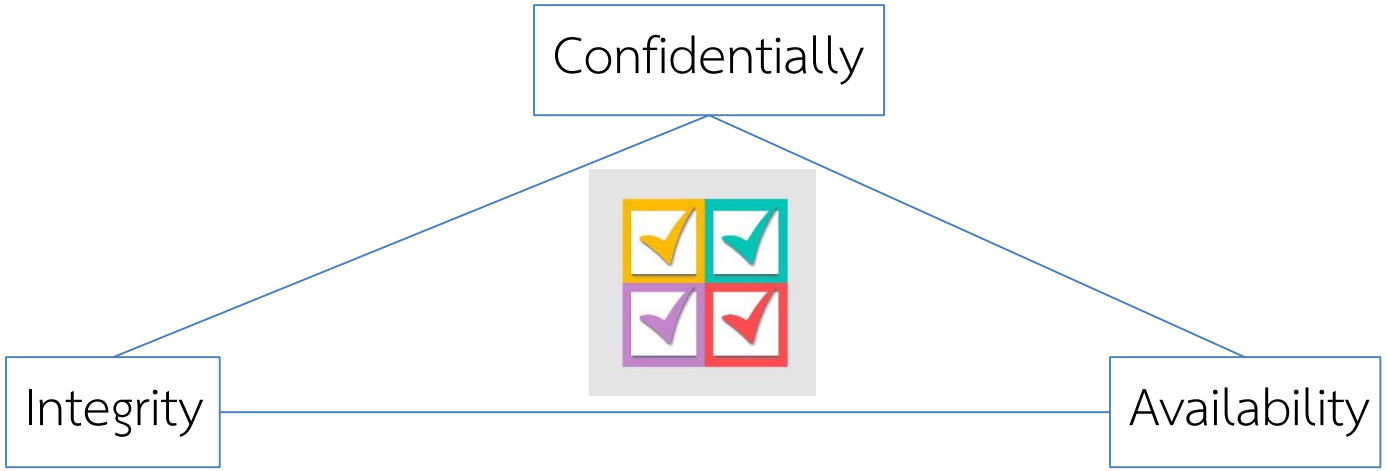
CIA Triad



Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น **ความลับสูงสุด**ผู้ที่สามารถเข้าถึงได้ คือ **ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น**
- เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

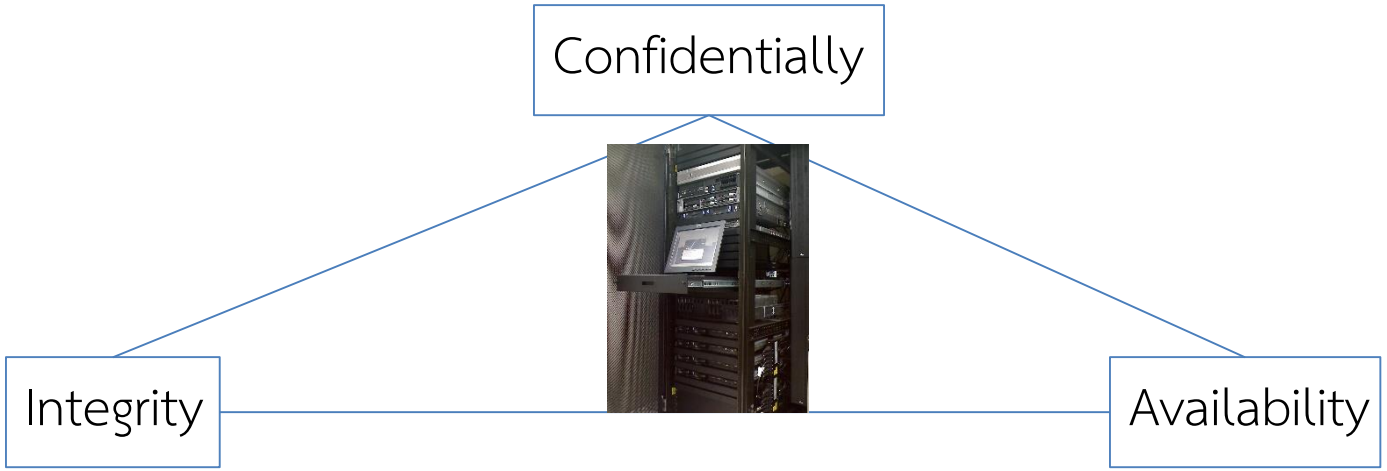
CIA Triad



Integrity หรือการรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูลและการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

CIA Triad



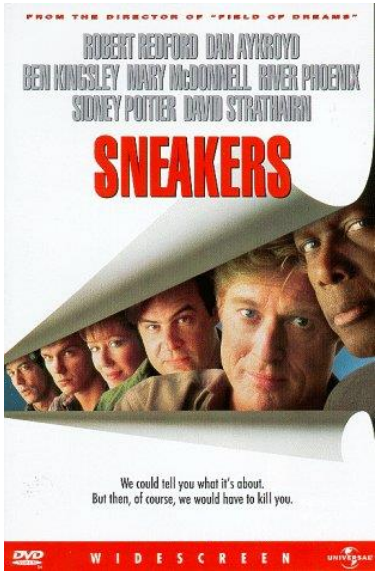
Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

Ian Murphy หรือ Captain Zap

เจาะระบบของ **AT&T** ในปี 1981
เพื่อเปลี่ยนนาฬิกาของเครื่องคิดเงินค่าโทร

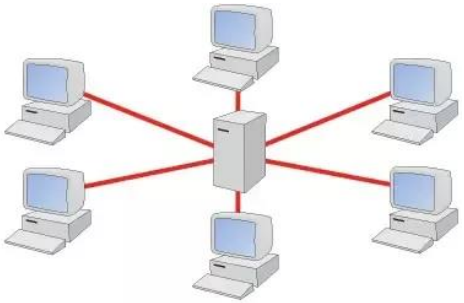
Hack ด้วยวิธีการคุ้ยขยะ

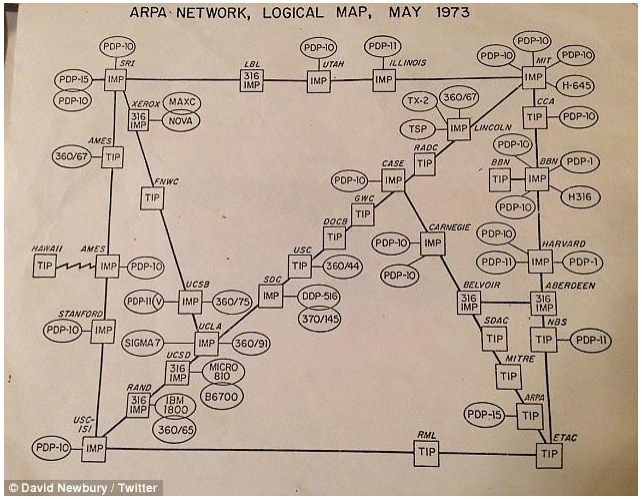


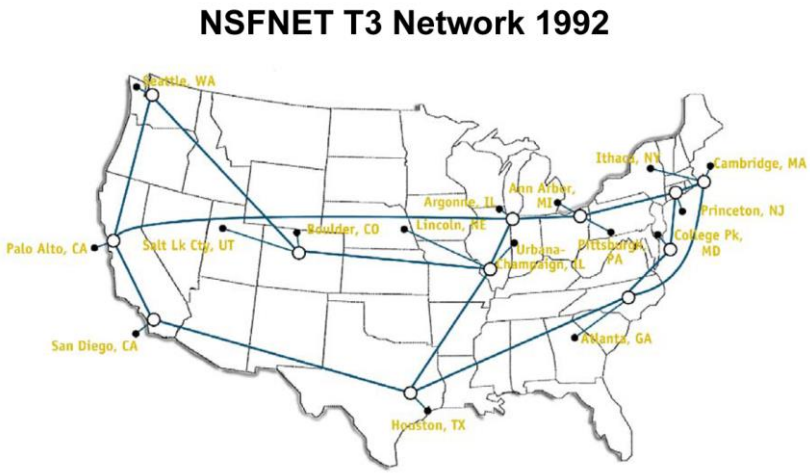
ทำให้เกิดอาชีพ **Dumpster Diver** คือคนที่รับจ้างคุ้ยขยะ เพื่อหาข้อมูลลับต่าง ๆ ของบริษัทห้างร้าน ให้กับบริษัทคู่แข่งที่จ้าง

อินเตอร์เน็ต (Internet) นั้นย่อมาจากคำว่า “International network” หรือ “Inter Connection network” ซึ่งหมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายคอมพิวเตอร์ทั่วโลกเข้าไว้ด้วยกัน เพื่อให้เกิดการสื่อสาร และการแลกเปลี่ยนข้อมูลร่วมกัน โดยอาศัยตัวเชื่อมเครือข่ายภายใต้มาตรฐานการเชื่อมโยงเดียวกัน นั่นก็คือ TCP/IP Protocol ซึ่งเป็นข้อกำหนดวิธีการติดต่อสื่อสารระหว่างคอมพิวเตอร์ในระบบเครือข่าย ซึ่งโปรโตคอลนี้จะช่วยให้คอมพิวเตอร์ที่มีฮาร์ดแวร์ที่แตกต่างกันสามารถติดต่อถึงกันได้

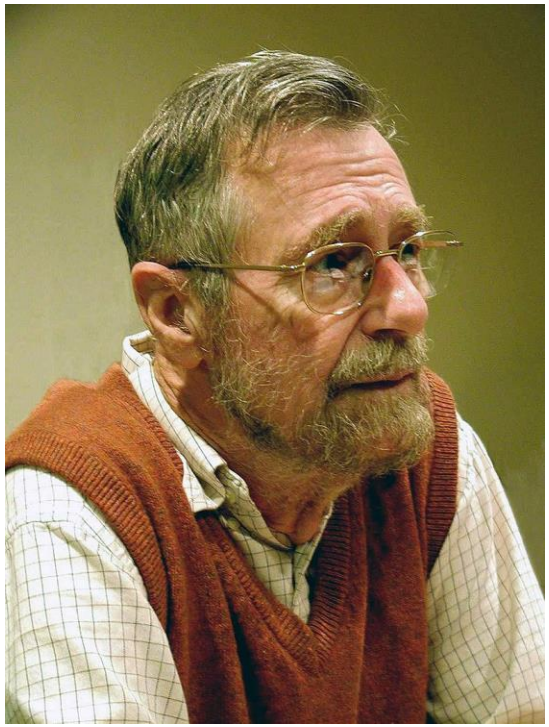
เดิมเครือข่ายคอมพิวเตอร์จะสื่อสารกันได้ จำเป็นต้องมีศูนย์กลางการเชื่อมต่อ ซึ่งเป็นจุดอ่อนของเครือข่าย หากศูนย์กลางถูกทำลายการสื่อสารจะล้มเหลวทั้งหมด
ต่อมามีการค้นพบ Dijkstra algorithm จึงสามารถพัฒนาเครือข่ายคอมพิวเตอร์ให้สามารถหาเส้นทางได้เอง โดยไม่ต้องมีศูนย์กลาง







Edsger W. Dijkstra

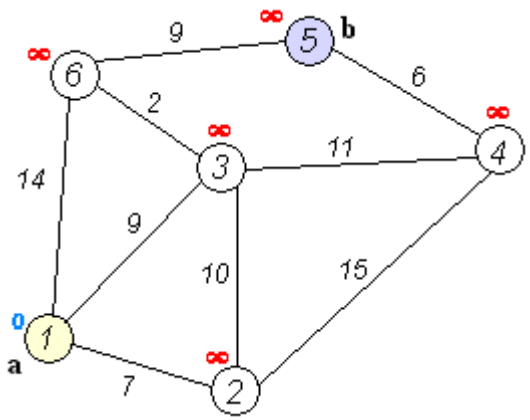


เกิด วันที่ 11 พ.ค. 1930 ชาวเนเธอร์แลนด์

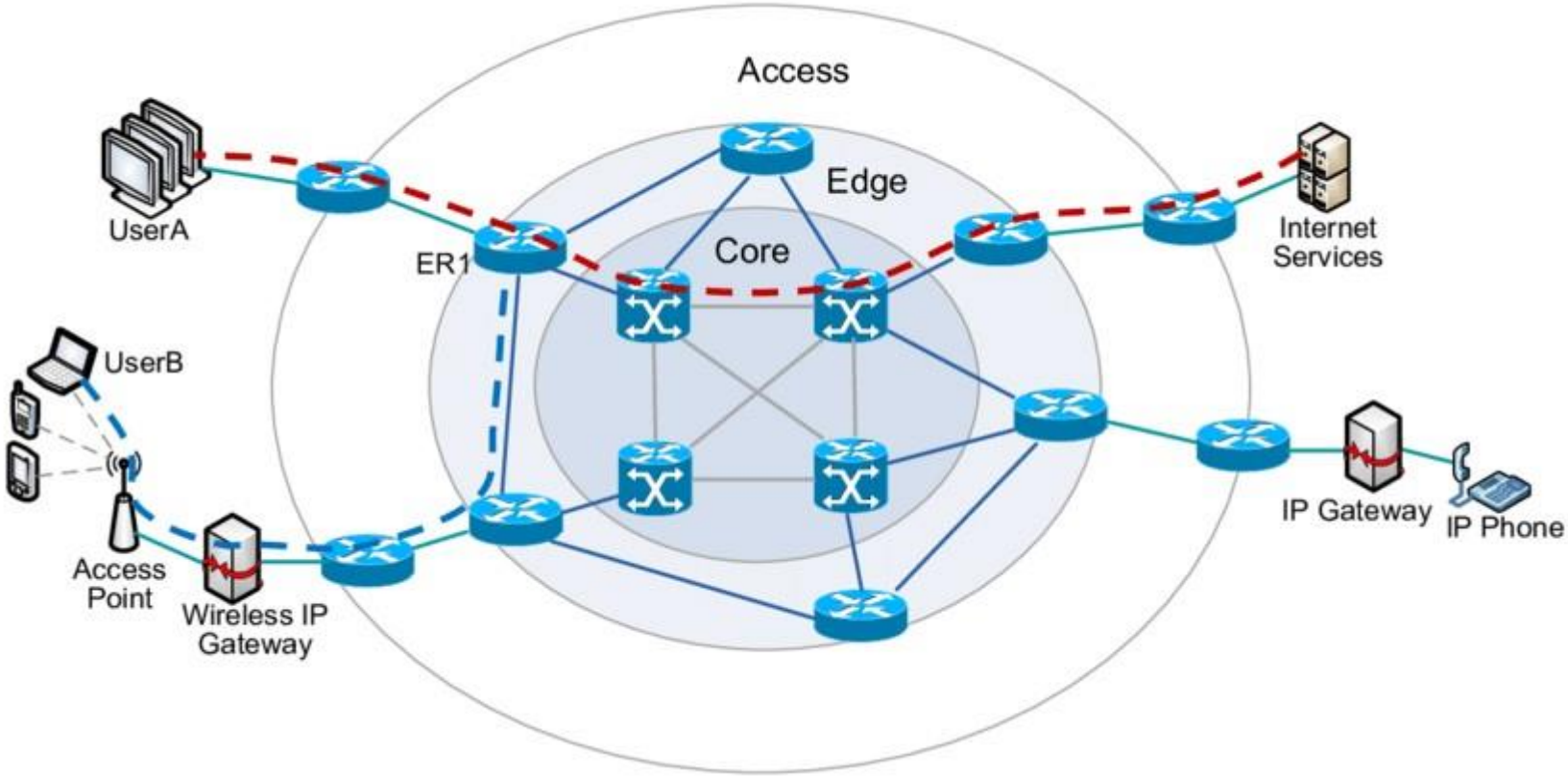
เสียชีวิต วันที่ 6 สิงหาคม 2002

ผลงาน : วิทยาศาสตร์คอมพิวเตอร์ (หนังสือชุด ศิลปะแห่งการเขียนโปรแกรม, อัลกอริทึม) การเข้ารหัสขอมูล

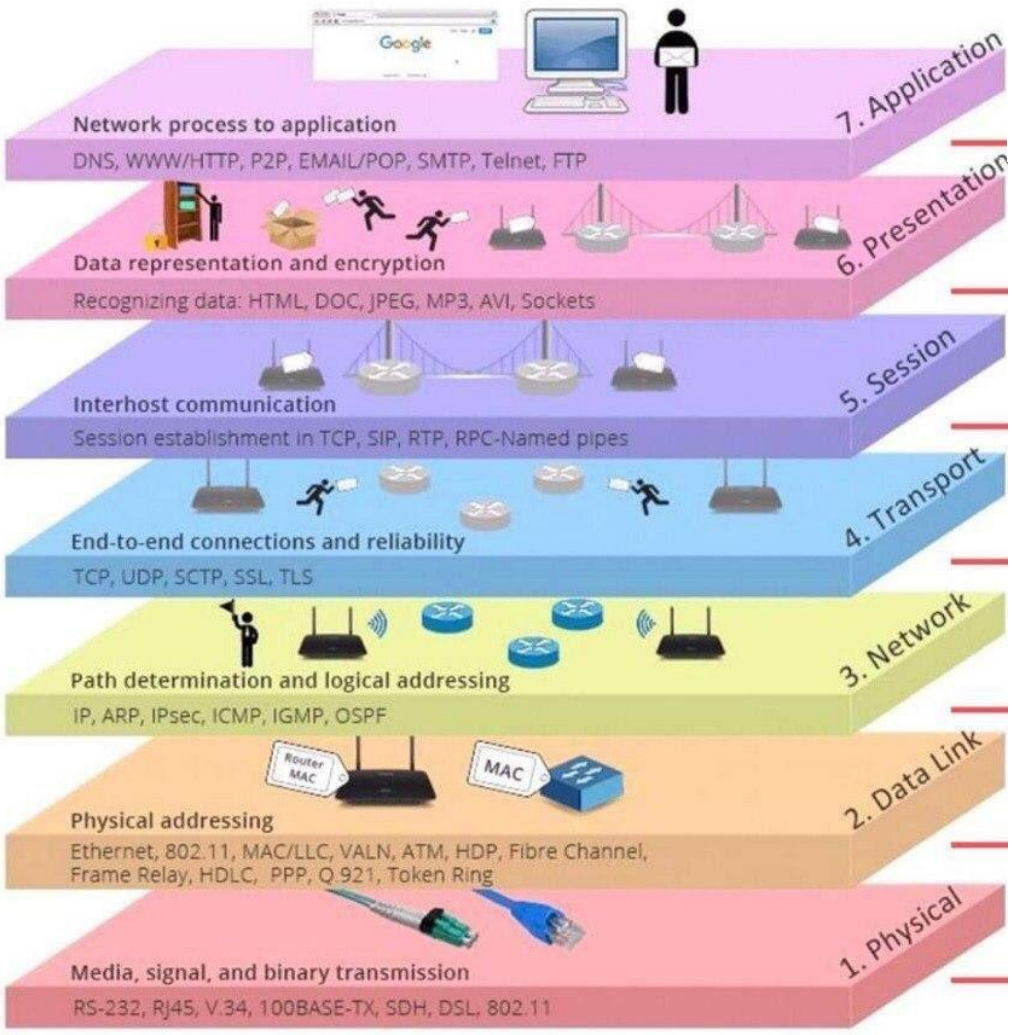
- Structured programming
- Shortest path algorithm (**Open Shortest Path First** (**OSPF**)) ใช้ใน AS
- Banker's algorithm
- Parallel processing
- Distributed computing



สถาปัตยกรรมเครือข่ายอินเตอร์เน็ตในปัจจุบัน

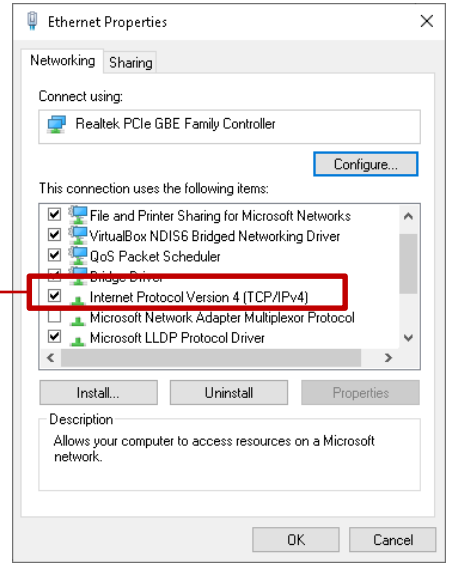


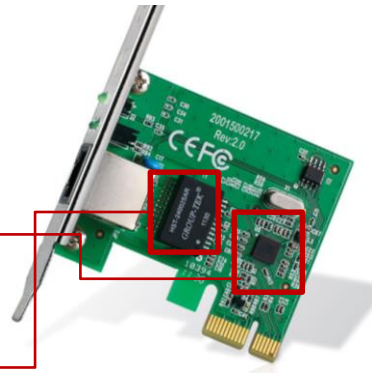
OSI Model (Open Systems Interconnection Model) คือ รูปแบบความคิดที่พรรณาถึงคุณสมบัติพิเศษและมาตรฐานการทำงานภายในของระบบการสื่อสาร

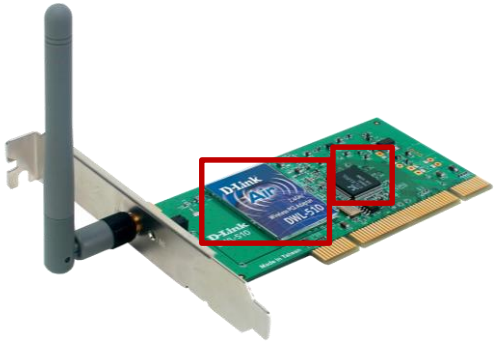


Winsock.dll

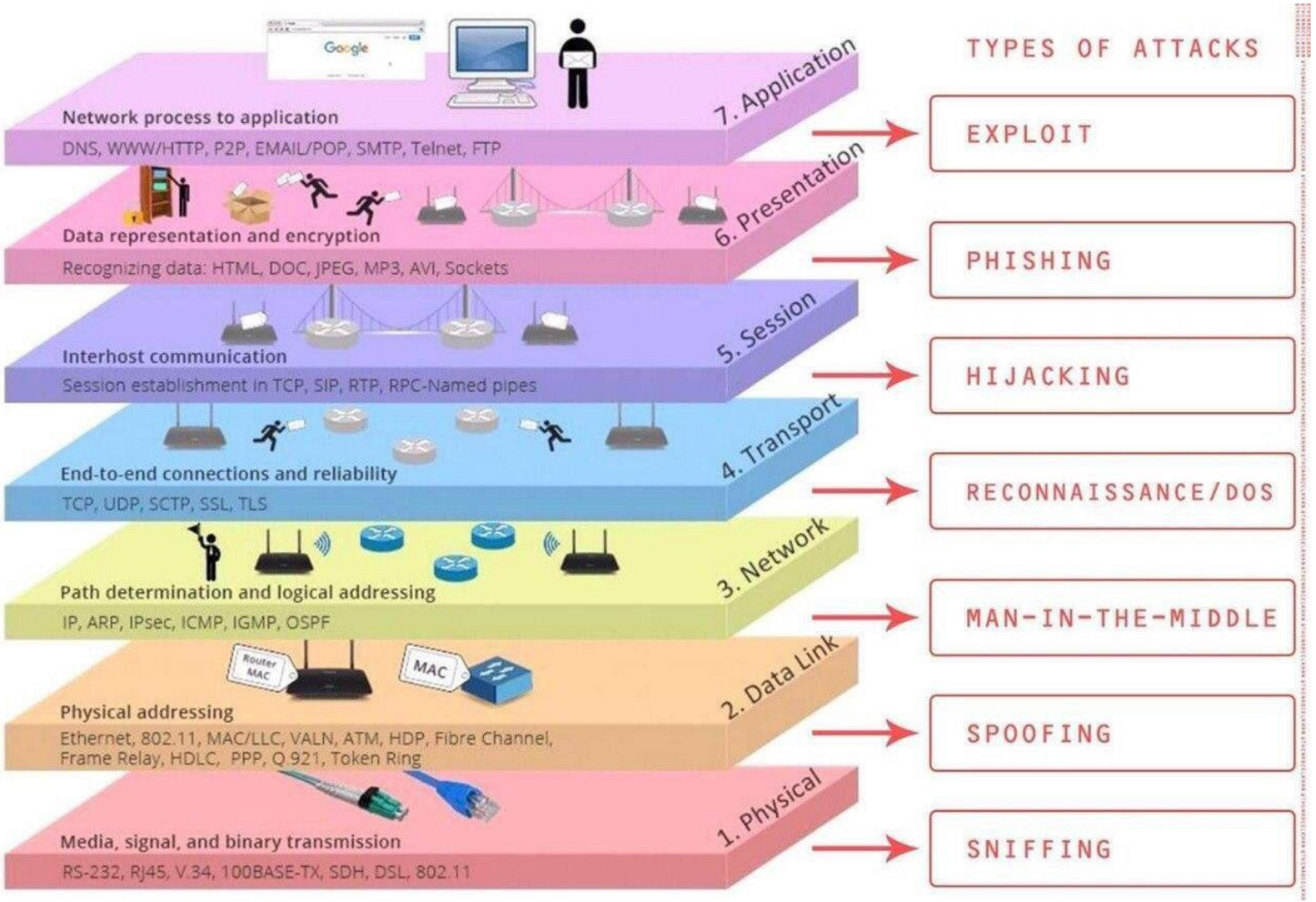
YouTube







OSI Model (Open Systems Interconnection Model) คือ รูปแบบความคิดที่พรรณาถึงคุณสมบัติพิเศษและมาตรฐานการทำงานภายในของระบบการสื่อสาร



รูปแบบภัยคุกคามของ Cybersecurity

Malware

Web-based attacks

Phishing

Web application attacks

Spam

DDoS

Data breach

Insider threat

Botnets

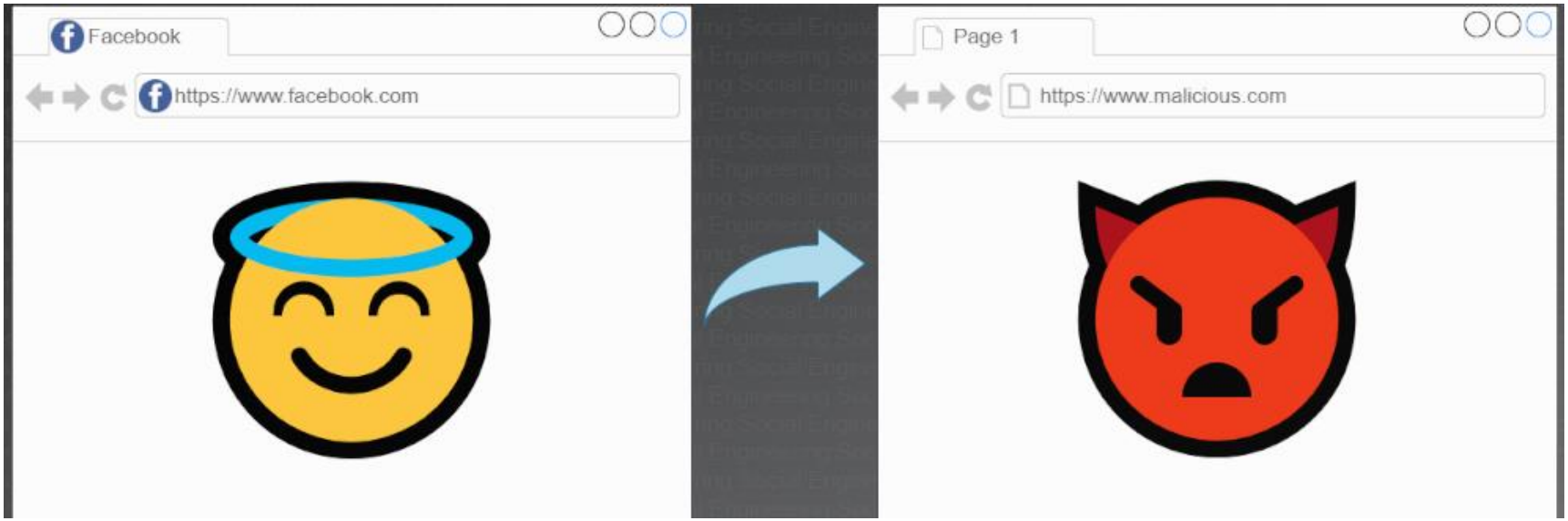
Ransomware

Crypto jacking

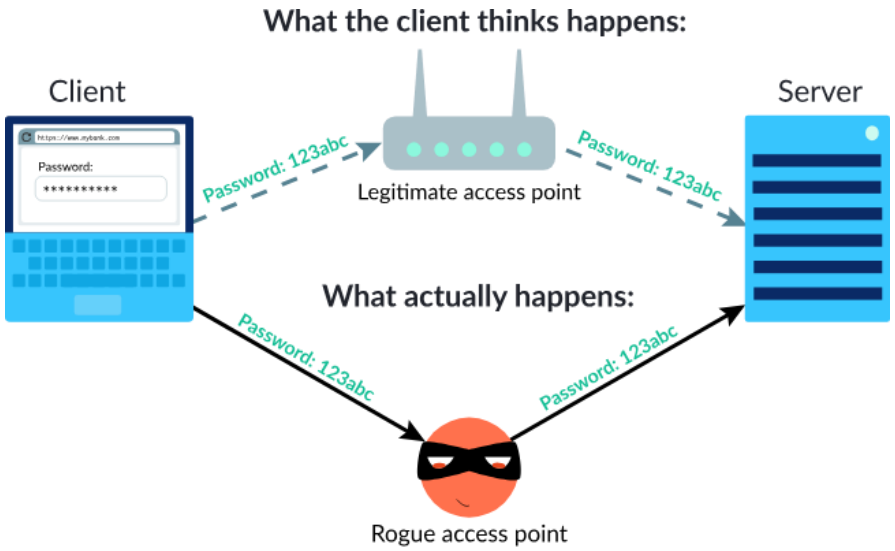
Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่ เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง

- ไวรัส (Virus)
- เวิร์ม (Worms)
- โทรจัน (Trojans)

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยสร้างเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware



Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social
โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่น ๆ
เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการประกอบธุรกรรม



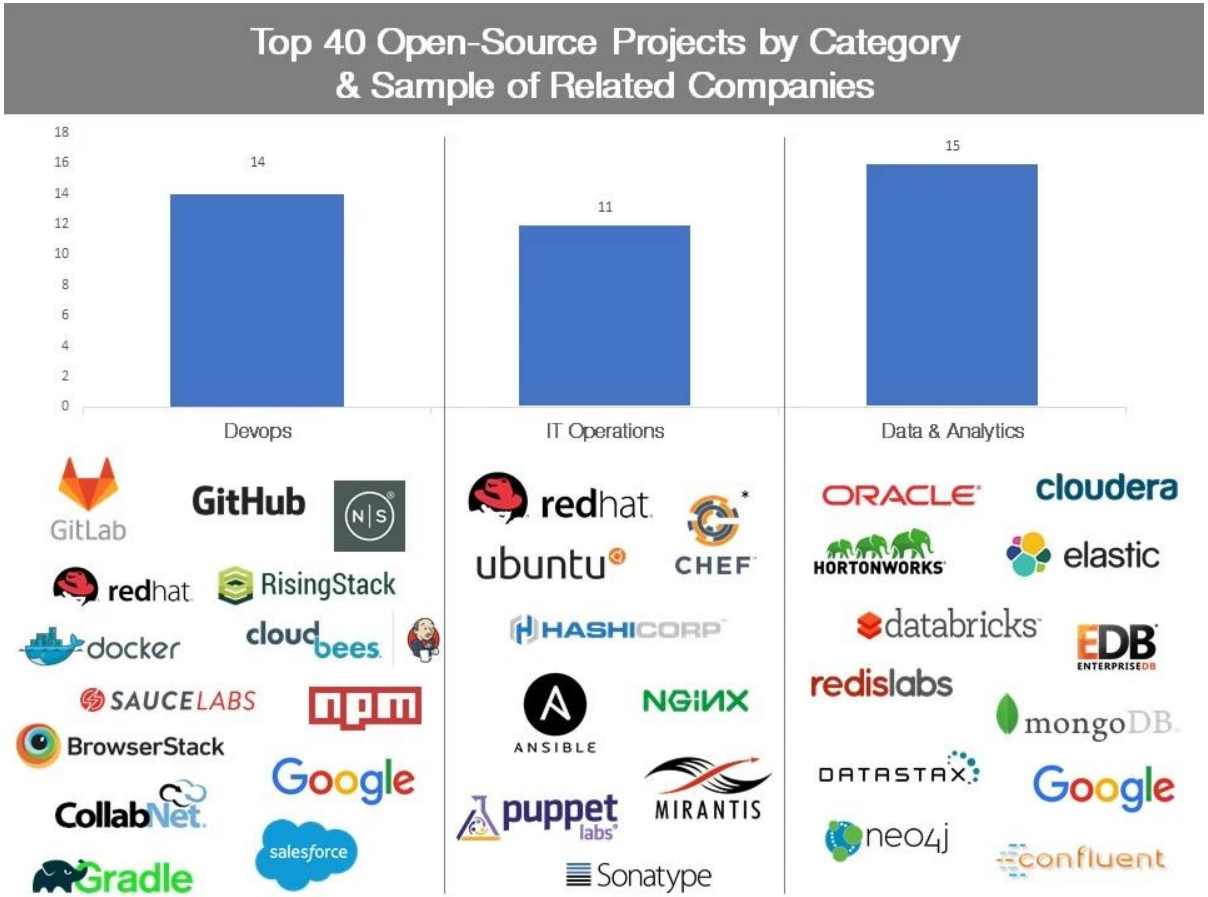
Web application attacks

Web application attacks
คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น

- Code ของเว็บไซต์เช่น CMS
- Web Server หรือ Database Server

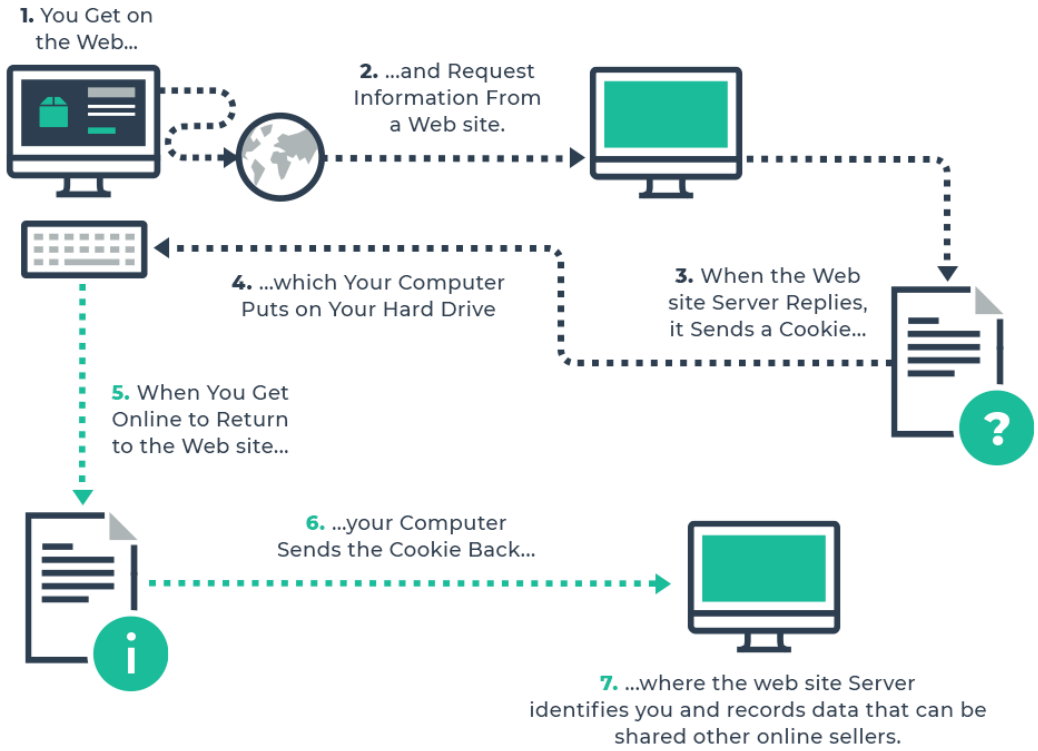
วิธีการโจมตีที่นิยมใช้

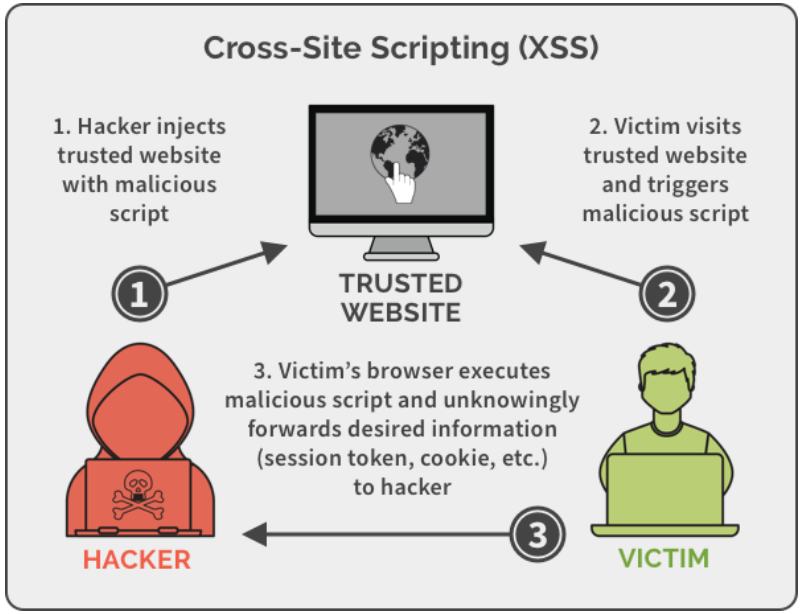
- Cross Site Scripting
- SQL Injection
- Path Traversal



Web application attacks

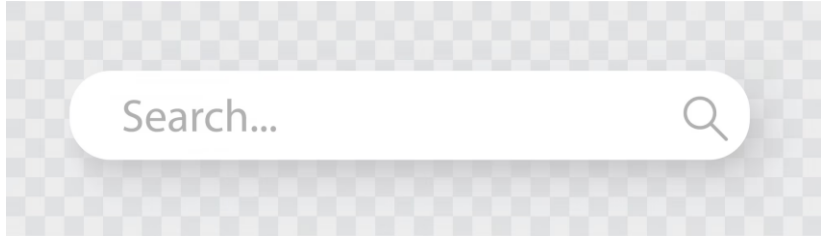
- Cross Site Scripting

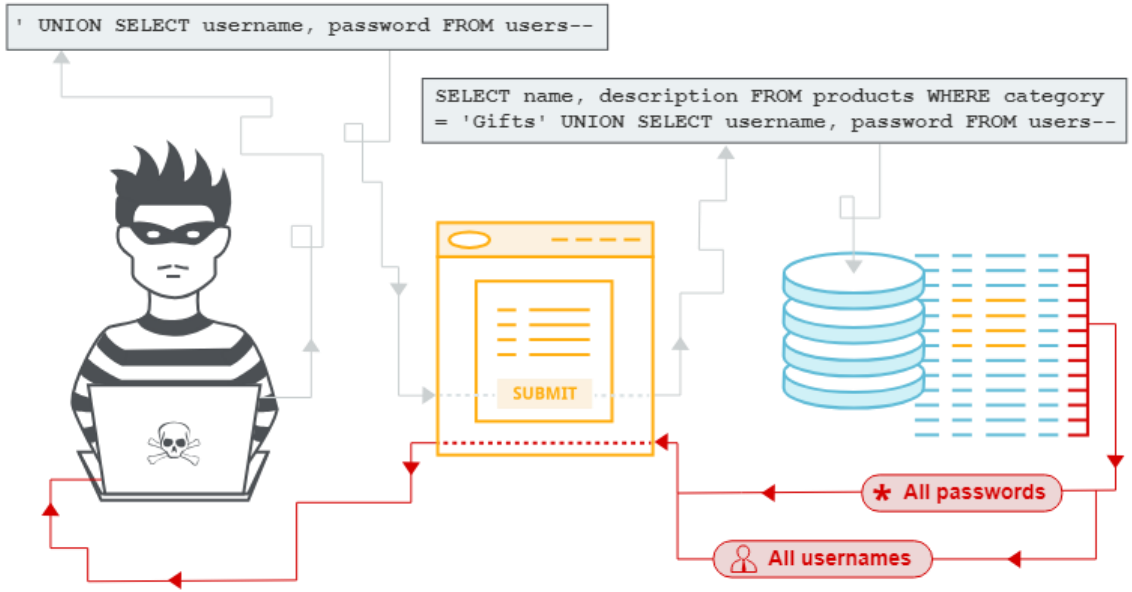




Web application attacks

- SQL Injection

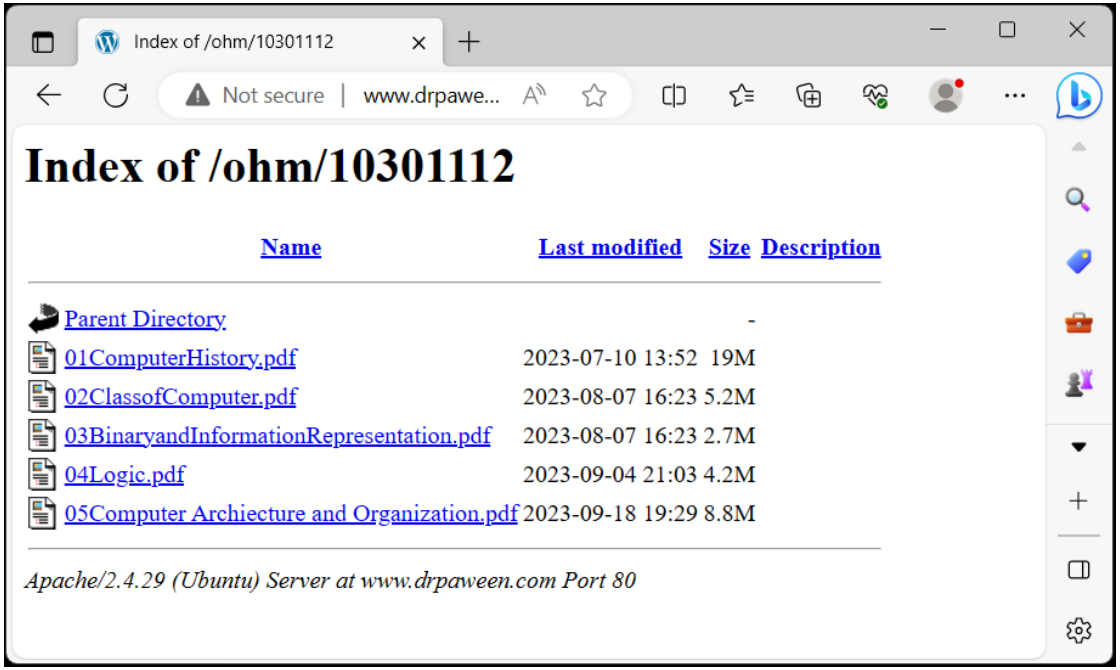


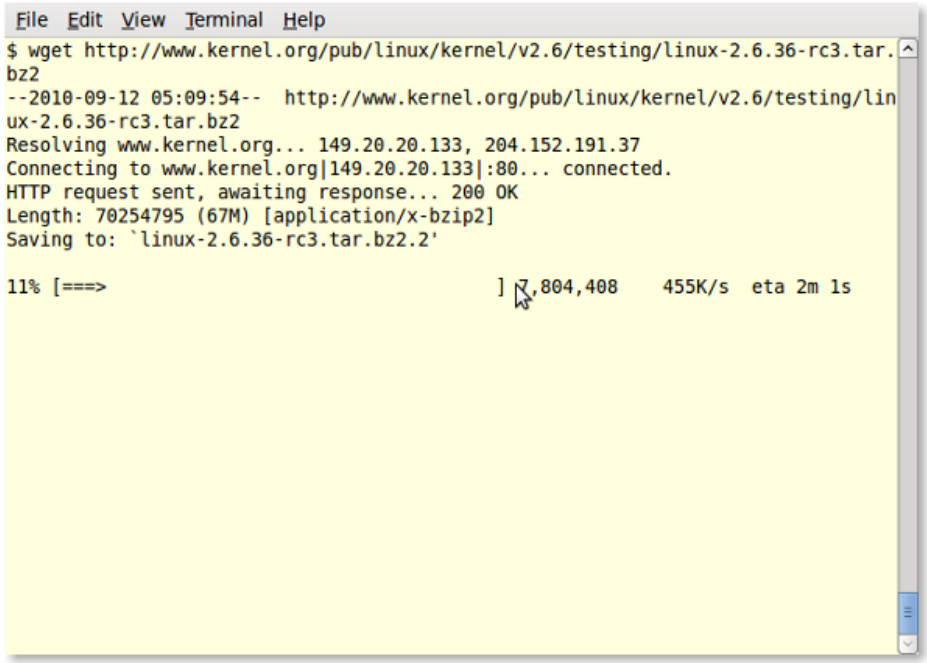



```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.3.4.44#dev}
|_ -| . [,]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent i
s illegal. It is the end user's responsibility to obey all applicable local, state and fed
eral laws. Developers assume no liability and are not responsible for any misuse or damage
 caused by this program

[*] starting @ 10:44:53 /2019-04-30/

[10:44:54] [INFO] testing connection to the target URL
[10:44:54] [INFO] heuristics detected web page charset 'ascii'
[10:44:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:44:54] [INFO] testing if the target URL content is stable
[10:44:55] [INFO] target URL content is stable
[10:44:55] [INFO] testing if GET parameter 'id' is dynamic
[10:44:55] [INFO] GET parameter 'id' appears to be dynamic
[10:44:55] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
 (possible DBMS: 'MySQL')
```

Web application attacks

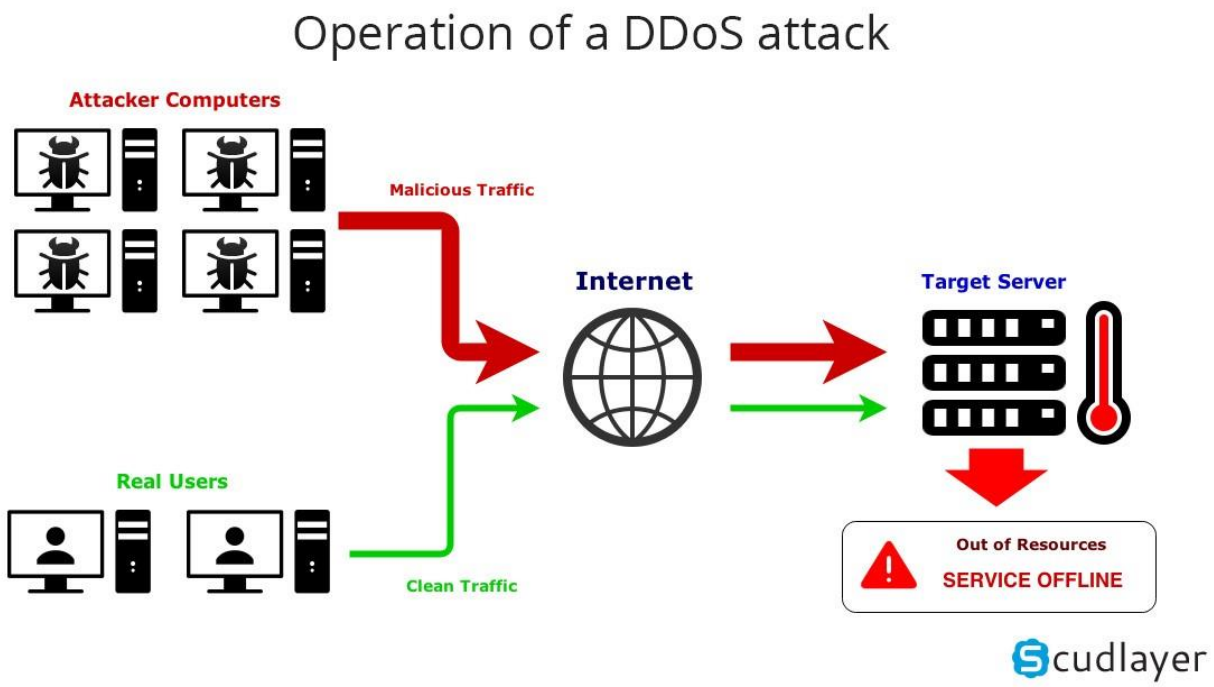
- Path Traversal





Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจานวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้าง ความรำคาญ หรือก่อกวน

DDoS(Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม



Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

ผลกระทบ

- ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ
ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น
ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย
และผลลัพธ์ของภัยนี้มีความรุนแรง

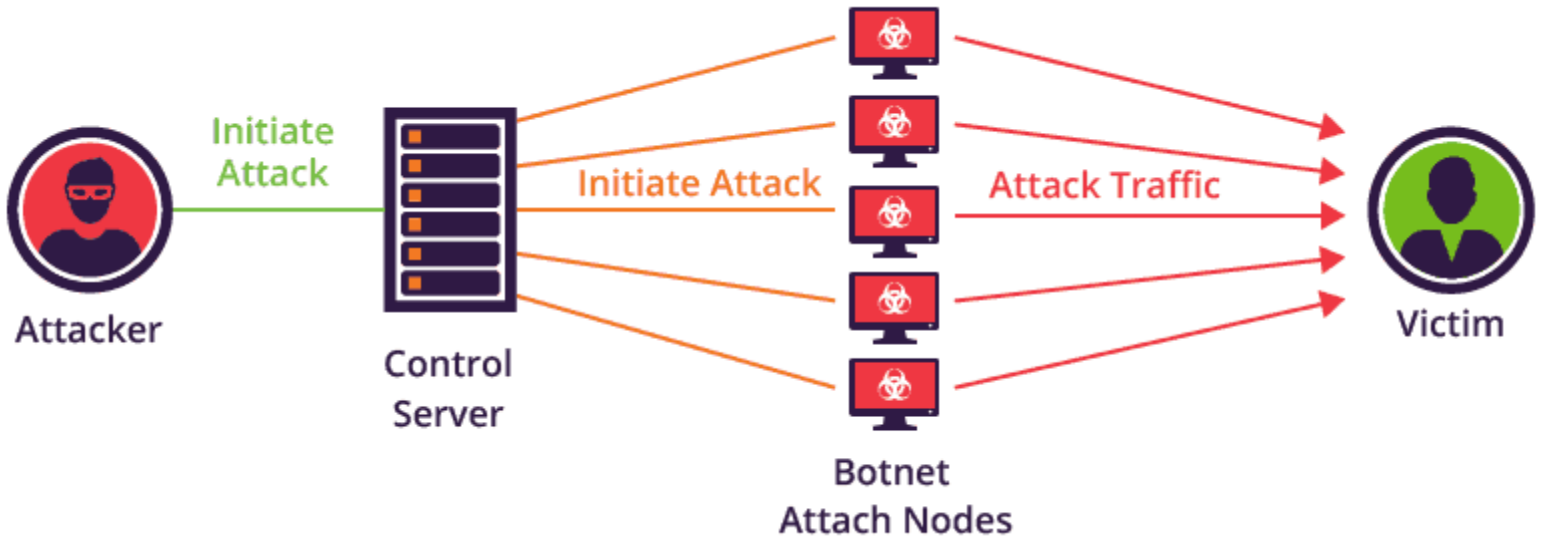
วิธีการป้อง

นำหลักการ Zero Trust มาใช้งานภายในองค์กร

Social Engineering “วิศวกรรมสังคม” เป็นศิลปะในการหลอกลวง ด้วยหลักการพื้นฐานทางจิตวิทยาให้เหยื่อเปิดเผยข้อมูล เพื่อให้ได้ผลประโยชน์ตามที่แฮกเกอร์ต้องการโดยอาศัยจุดอ่อน ความรู้เท่าไม่ถึงการณ์ ความไม่รู้ ความประมาท ซึ่งการโจมตีนี้จะได้ผลดีมากเมื่อเทียบกับการโจมตีทางไซเบอร์ลักษณะอื่น ๆ โดยเฉพาะกับคนที่ไม่มีความรู้ทางด้านไอทีหรือความปลอดภัยทางไซเบอร์ วิธีการสื่อสารมักจะมีรูปแบบดังนี้

- การสร้างสถานการณ์ให้มีความเร่งด่วนเช่น เช่น ใกล้จะหมดเวลาแล้ว ให้เหยื่อควรรีบตัดสินใจก่อนโปรโมชันจะหมดลง
- ปลอมแปลงตัวเองเป็นผู้อื่นที่มีความสำคัญกับองค์กร หรือบุคคลสำคัญต่างๆ เช่น CEO หรือ เจ้าของบริษัท
- พูดถึงเหตุการณ์ต่างๆ เพื่อความสมจริง หรือนำสถานการณ์ฉุกเฉิน ณ เวลานั้น มาใช้ในการอ้างอิง เช่น การขอรับบริจาคเงินน้ำท่วม หรือจากสถานการณ์โรคระบาดโควิด19
- ซ่อน หรืออำพราง URL, Domain หรือ Address อันตราย ให้เหมือน URL ของจริง
- เสนอผลตอบแทนหรือโปรโมชันเพื่อสร้างแรงจูงใจ
- ในบางครั้งใช้วิธีการแฮก Account ของผู้ใกล้ชิดเหยื่อแล้วติดต่อเหยื่อผ่าน Social Network เพื่อขอยืมเงิน
- การหลอกลวงทางโทรศัพท์
- การค้นข้อมูลจากถังขยะ
- ฟิชชิง (Phishing) เพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้
ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets
เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

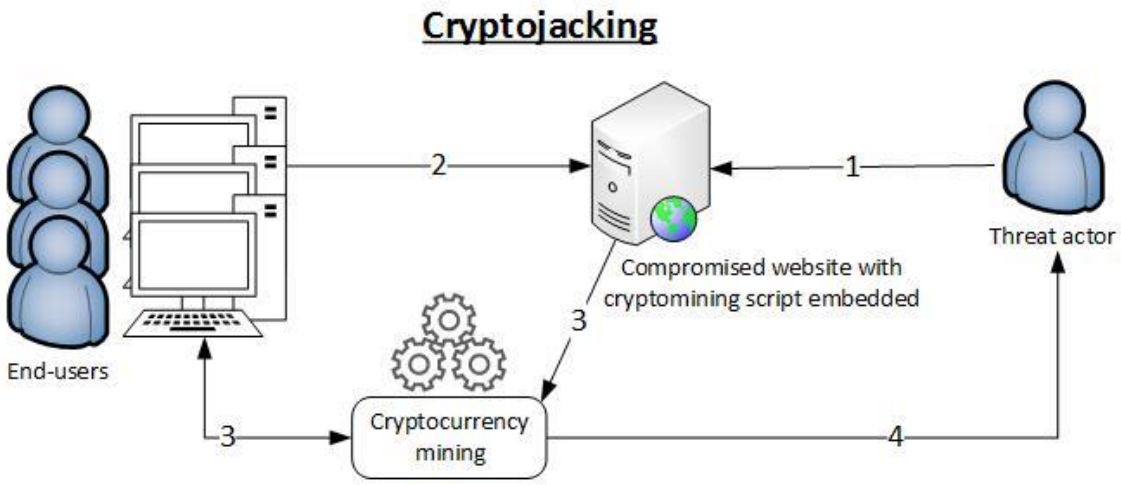


Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่าน ที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

- สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล
- ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทาการเปิด

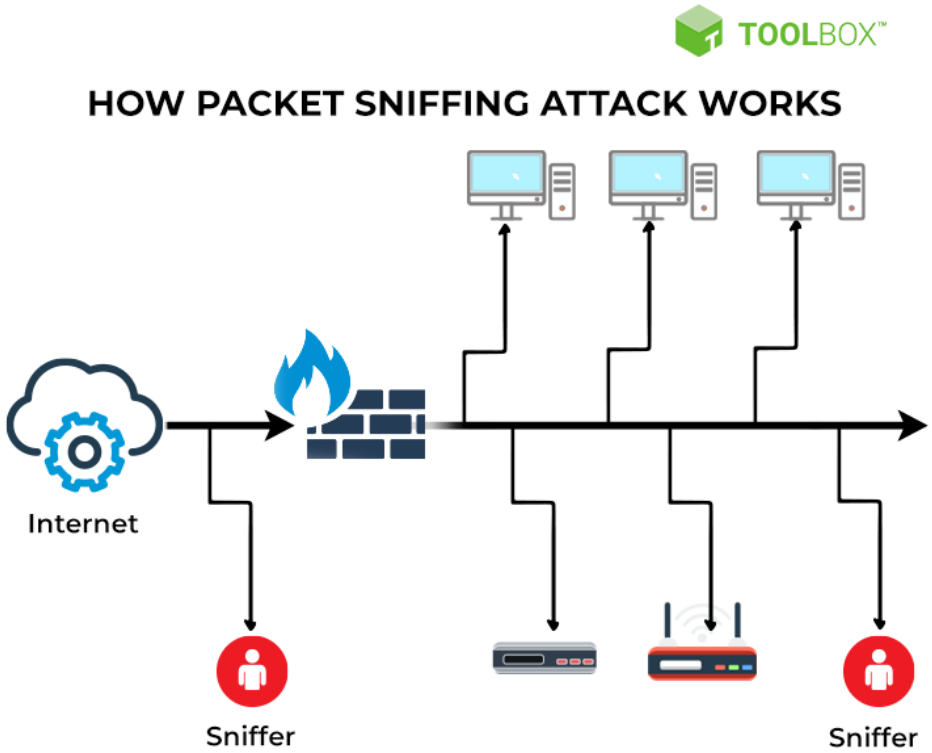
Crypto jacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker

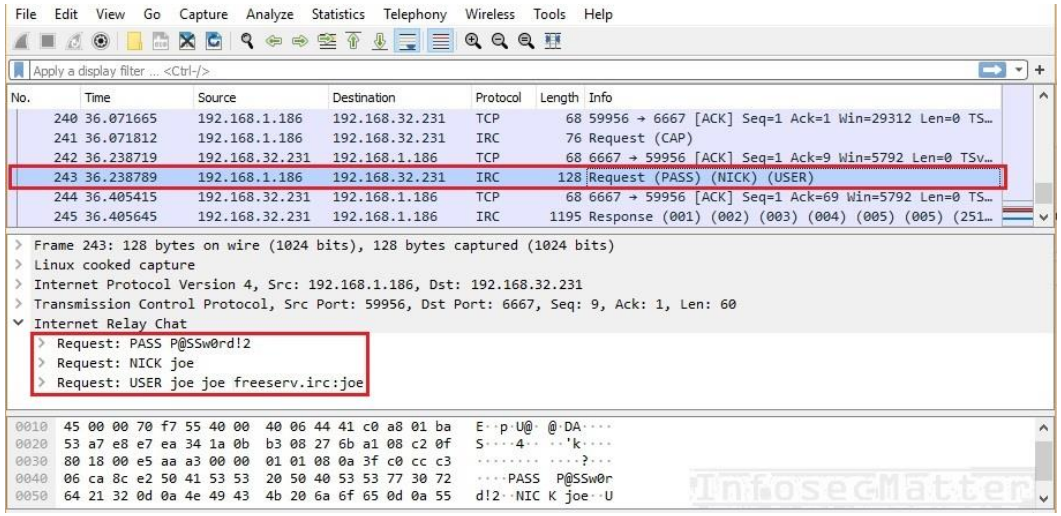


Steps

1. The threat actor compromises a website
2. Users connect to the compromised website and the cryptomining script executes
3. Users unknowingly start mining cryptocurrency on behalf of the threat actor
4. Upon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins

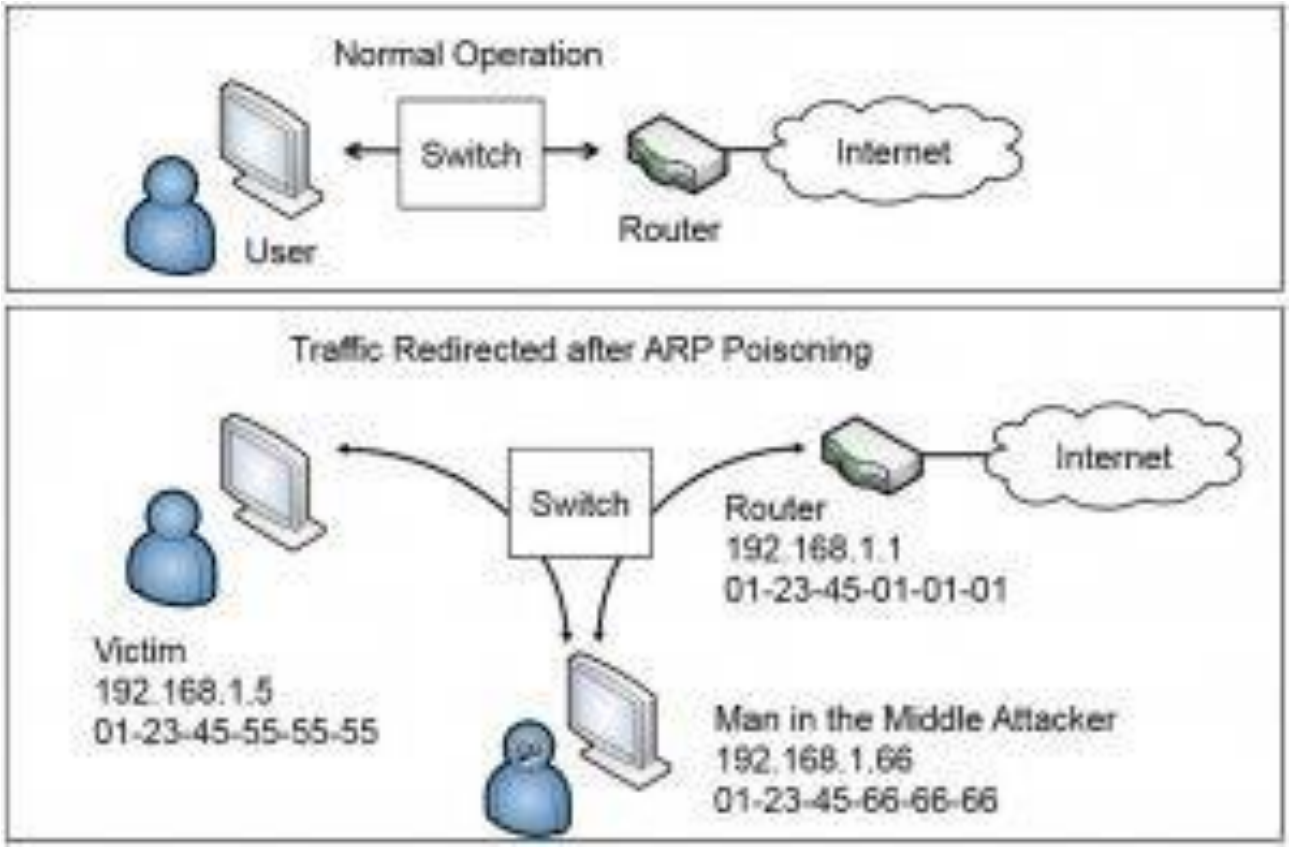
การสอดแนมหรือสนิฟฟง (Sniffing) บางที่ก็ใชคำวา สนูปปง (Snooping), อีฟดร อปปง (Eavesdropping) หมายถึง การดักเพื่อแอบดูขอมูล ซึ่งจัดอยูใน ประเภทการเปดเผย การสอดแนมเปนการโจมตีแบบพาสซีฟ(Passive) เปนการกระทำที่ไมมีการเปลี่ยนแปลง หรือแกไขขอมูล ยกตัวอยางเชน การดักอานขอมูล ในระหวาง การอานไฟลที่จัดเก็บอยูใน ระบบ การแท็ปสายขอมูล (Wiretapping) เปนวิธีการหนึ่งของการสนูปปงเพื่อเฝาดูขอมูลที่ วิ่งบนเครือขาย การรักษา ความลับของขอมูล เชน การเขารหัสขอมูล (Encryption) จะเปน สิ่งที่ปองกันได

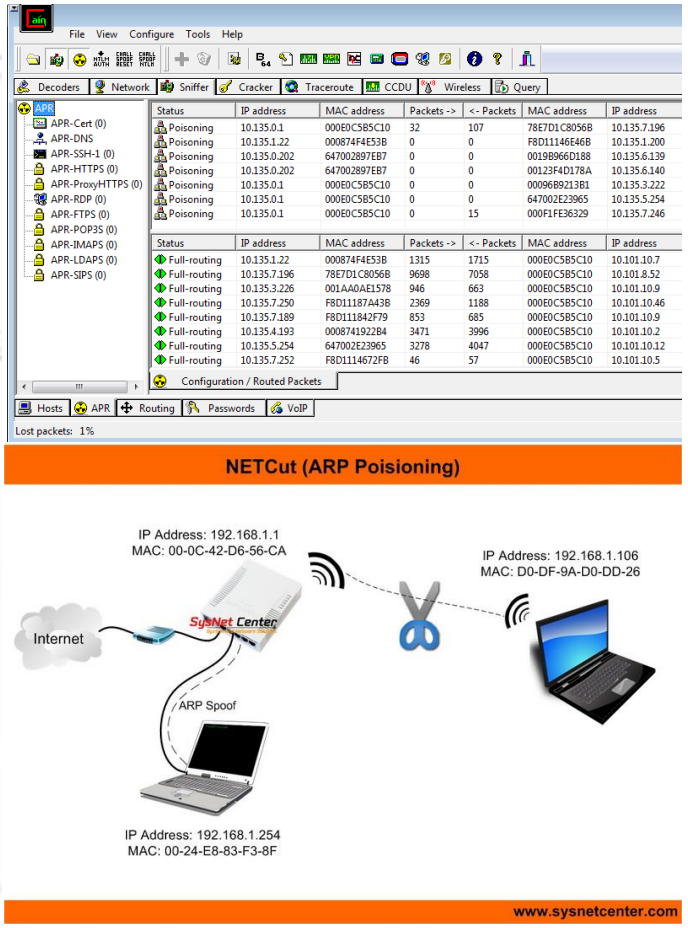




ARP Poisoning Attacks

ARP Spoofing หรือ ARP cache poisoning คือ การโจมตีโดยใช้ช่องโหว่ของโปรโตคอล ARP (Address Resolution Protocol เป็นโปรโตคอลสำหรับการจับคู่ (map) ระหว่าง Internet Protocol address (IP address) กับตำแหน่งของอุปกรณ์ในระบบเครือข่าย) เพื่อหลอกเหยื่อ โดยมีจุดประสงค์หลักคือ การจู่โจมแบบ DOS (Denial of Service) เป็นการทำให้เครื่องเหยื่อไม่สามารถสื่อสารกับปลายทาง ได้อย่างถูกต้องเป็นผลทำให้ไม่สามารถใช้งาน Internet ได้ และ MITM (Man In The Middle) เป็นการจู่โจมเพื่อดักจับข้อมูล (Sniffer) ของเหยื่อ





ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจาวัน

Computer

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1.ควรมีการแยก User ใช้งานกันของแต่ละบุคคล

2.ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

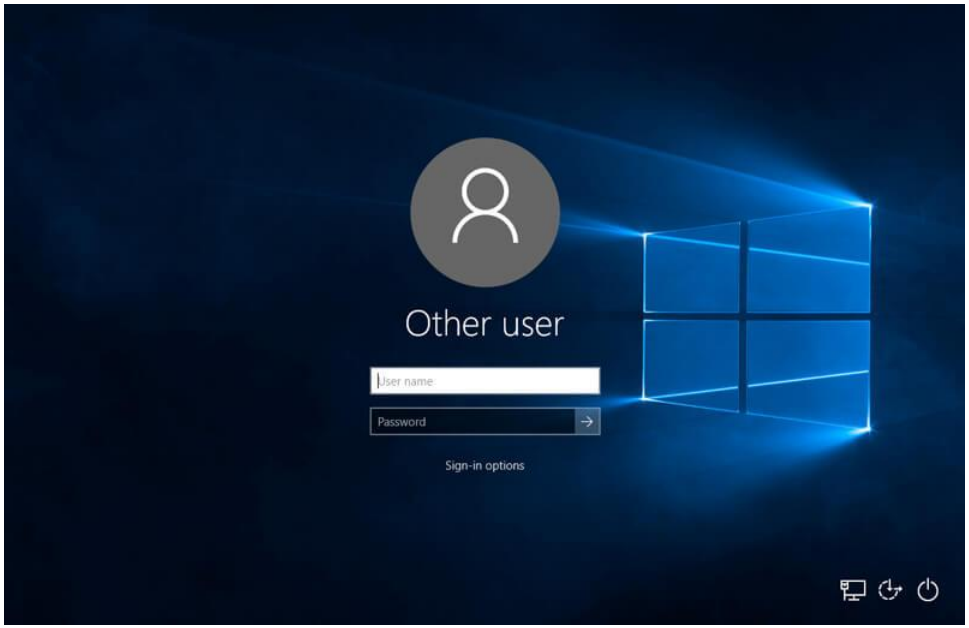
3.ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

4.มีการ Update Patch ระบบปฏิบัติการ(OS) อย่างสม่ำเสมอ

5.มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

6.ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

7.มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น



การใช้ Password ที่ดี คือ

1. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #)
2. มีความยาวของ Password อย่างน้อย 8 ตัวอักษร
3. ควรหลีกเลี่ยงการใช้ Common password หรือ **Default password**หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, 123456, วันเกิด, หมายเลขโทรศัพท์, คำที่มีในพจนานุกรม
4. มีการเปลี่ยน Password อย่างสม่ำเสมอ
5. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
6. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
7. **ไม่ควรบอก Password แก่ผู้อื่น**

```
[root@arch01 ~]# cat /etc/shadow | sed 's/michael/test/' | sed 's/mbo/joe/'
root:$6$4GxAA08J$AB7vFkLSCxtVdVMcPav8jZ5u4ZsyG22hy1cqWPdnQgqL84VesJNQYFXSwhfwkhT
UeHNxYwjjUGe8U/sjITBhq/:16672::::::
bin:x:14871::::::
daemon:x:14871::::::
mail:x:14871::::::
ftp:x:14871::::::
http:x:14871::::::
uuidd:x:14871::::::
dbus:x:14871::::::
nobody:x:14871::::::
systemd-journal-gateway:x:14871::::::
systemd-timesync:x:14871::::::
systemd-network:x:14871::::::
systemd-bus-proxy:x:14871::::::
systemd-resolve:x:14871::::::
systemd-journal-upload:!!:16672::::::
systemd-journal-remote:!!:16672::::::
avahi:!:16672::::::
polkitd:!:16672:0:99999:7:::
joe:$6$TA4PslzF$ch961z/ppk1VrmVAqSjSEDf75FIahttselx/bsDdjSXLt8cmsIoX9eAKfVm8epuD
KGvYV1xkohA37aeEvmu8d1:16672:0:99999:7:::
git:!:16683::::::
test:$6$PNkLwU7L$2Hm8YRMGgRoxxt4srAzGBZJFxU7SnlDbaUwb6APg5dyXSiQvQwSxHY1jOi5t2eM
kZ1PwBzY1aHAvZu29wSBpJ0:16735:0:99999:7:::
                                                    linux-audit.com
```

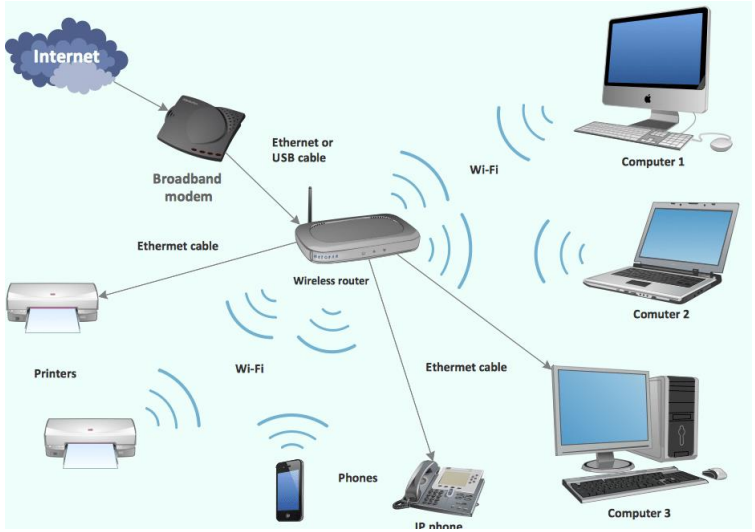
ตัวอย่าง MySQL password hash

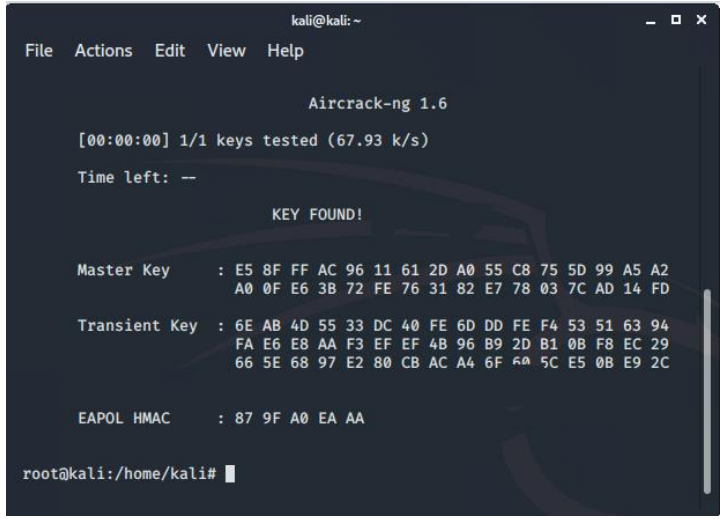
*D35DB127DB631E6E27C6B75E8D376B04F64FAF83

https://crackstation.net

รหัส WIFI สามารถดักจับได้

wpa2-handshake





E-mail

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1.ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

2.ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

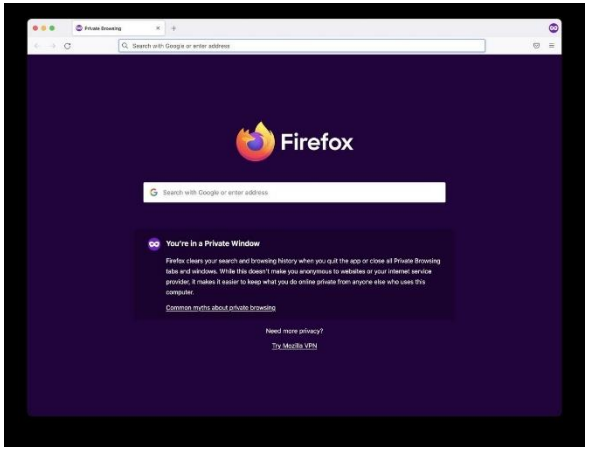
3.ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค

4.เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านทางช่องทางอื่น ๆ เพิ่มเติม

Website

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

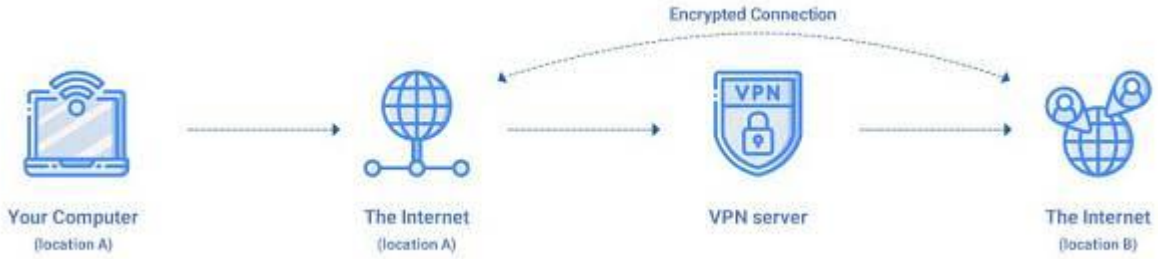
1. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ
2. ไม่ควรทำการบันทึก Password ต่าง ๆ บน Browser
3. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
4. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น
5. ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ
6. ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing
7. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ



VPN

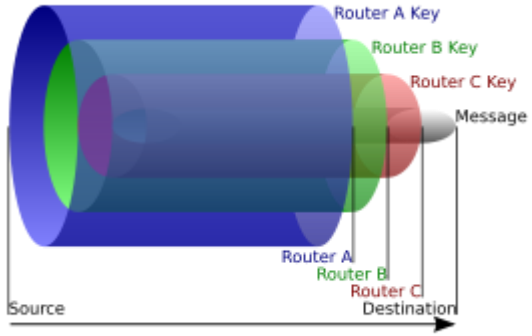
เครือข่ายเสมือน (Virtual Private Network) โปรแกรม VPN จะสร้างการเชื่อมต่อที่ปลอดภัยระหว่างคุณและอินเทอร์เน็ต มันมอบชั้นความเป็นส่วนตัวและความเป็นนิรนามเพิ่มเติมให้กับคุณ ดังนั้นคุณจึงสามารถ:

- ซ่อนกิจกรรมบนอินเทอร์เน็ตและตำแหน่งของคุณเพื่อหลีกเลี่ยงการถูกติดตามได้ (โดยเฉพาะอย่างยิ่งบนเครือข่าย WiFi สาธารณะ)
- ก้าวข้ามการเซ็นเซอร์ทางออนไลน์และท่องอินเทอร์เน็ตได้อย่างอิสระ
- Torrent อย่างปลอดภัยและเป็นนิรนามได้โดยไม่มีการควบคุมความเร็ว
- ปลดบล็อกแพลตฟอร์มสตรีมมิ่งอย่าง Netflix, Disney+ และอื่น ๆ ได้อีกมากมาย

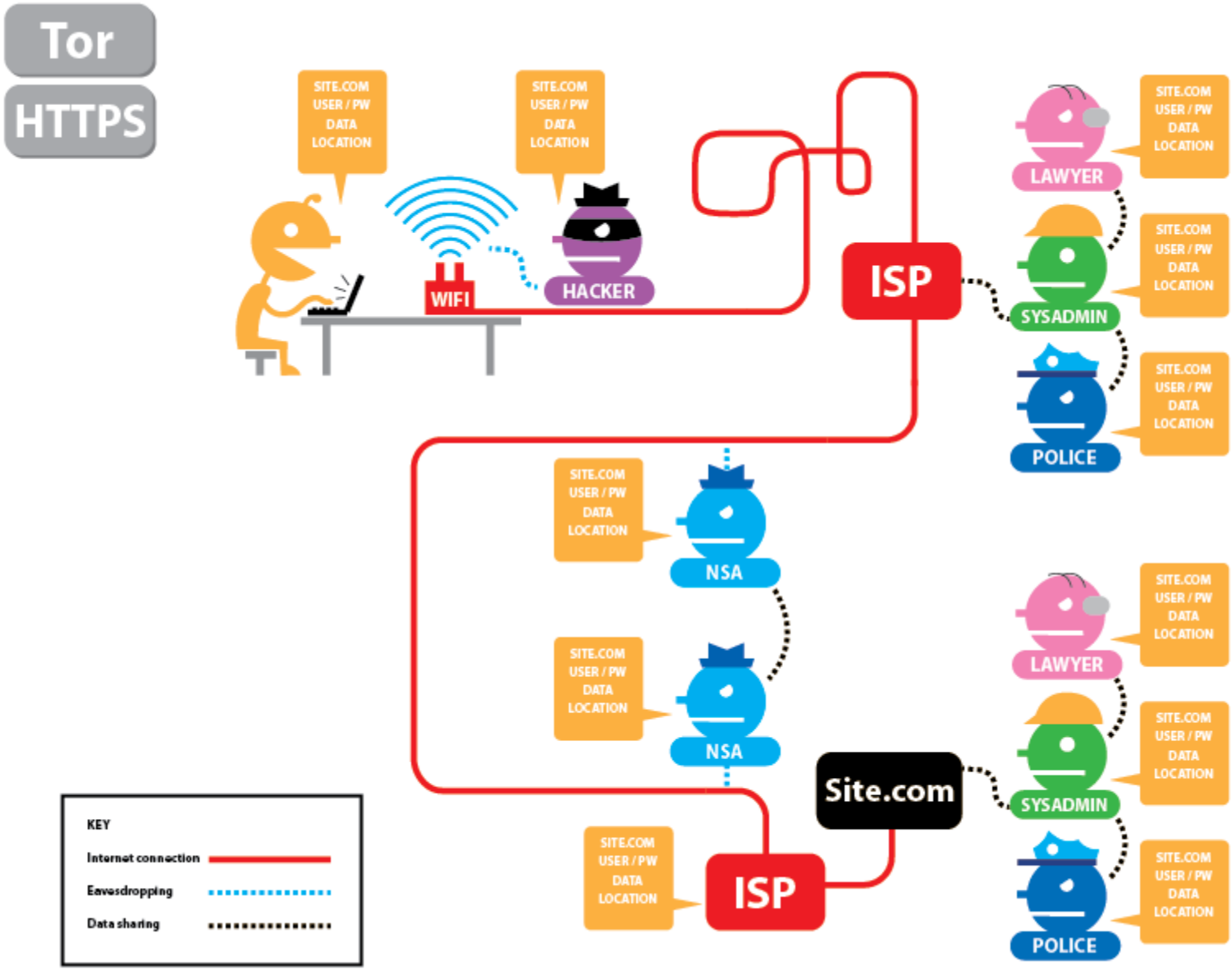


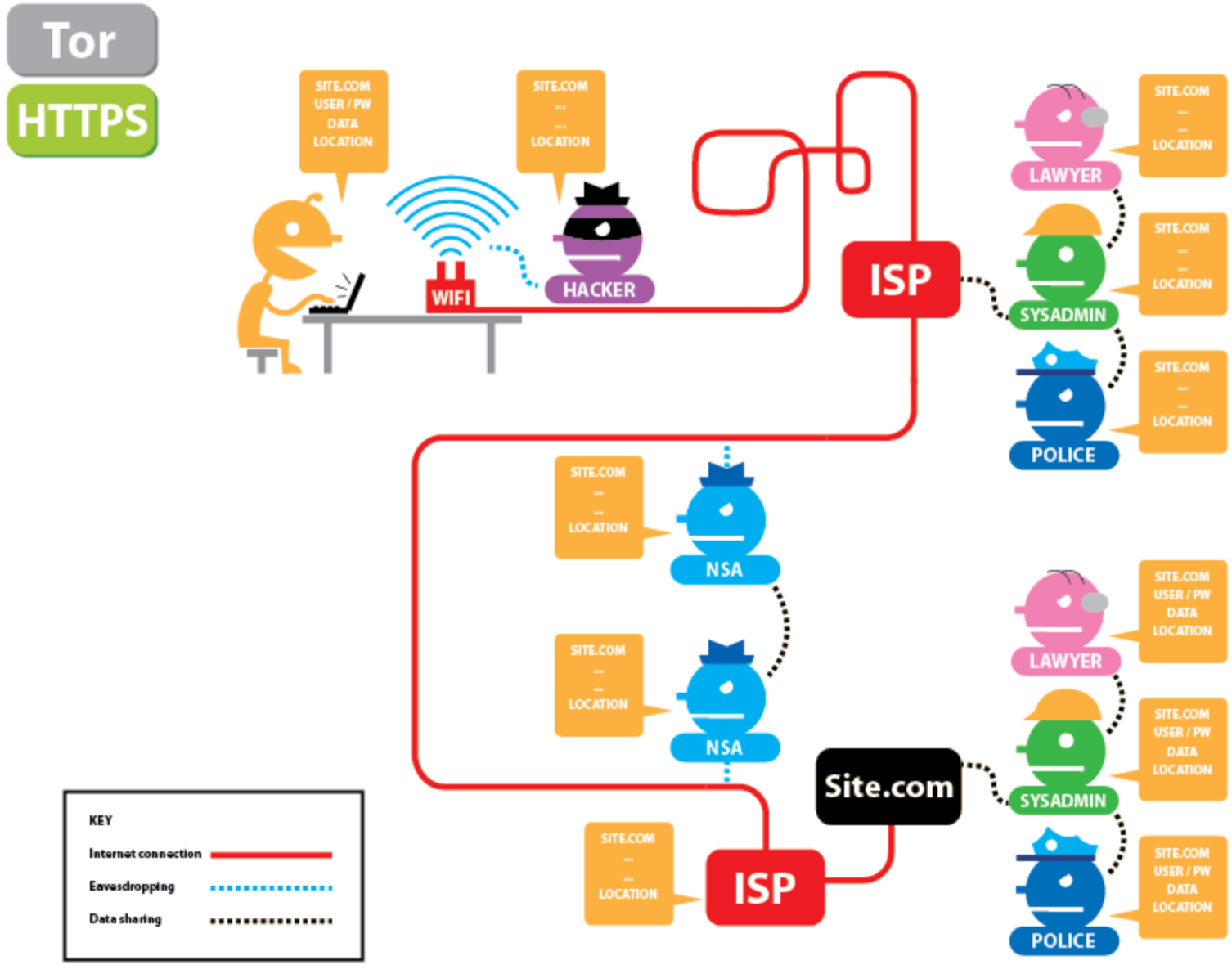
← บริการ VPN ของมหาวิทยาลัยแม่โจ้

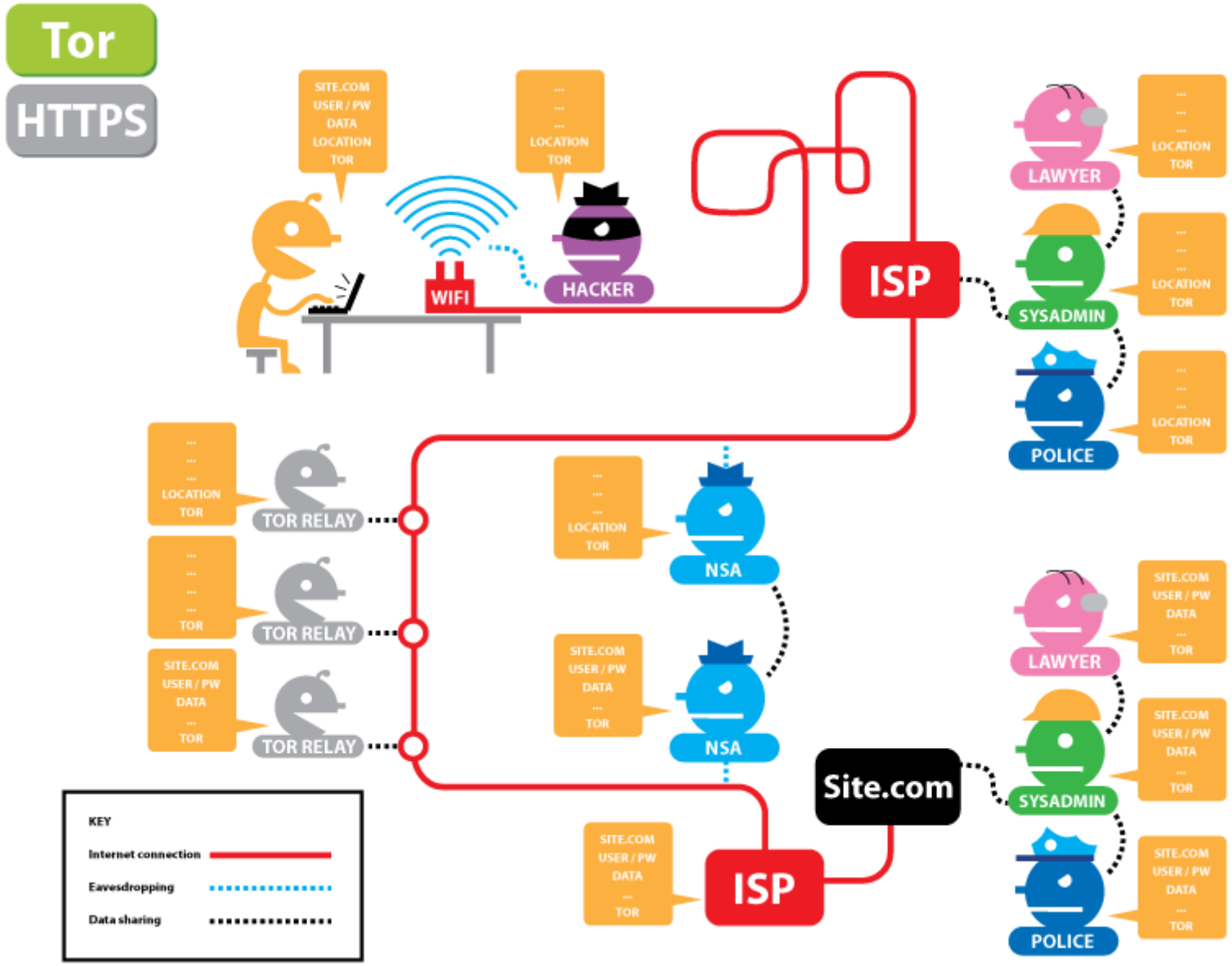
ทอร์ (อังกฤษ: Tor) เป็นซอฟต์แวร์เสรี (ฟรี) ที่ช่วยให้สื่อสารทางอินเทอร์เน็ตอย่างนิรนามได้ รวมทั้งช่วยให้สามารถเรียกดูเว็บไซต์บางแห่งที่ถูกเซ็นเซอร์ได้ โดยอาศัยการจัดเส้นทางแบบหัวหอม คือการจัดส่งการสื่อสารผ่านสถานีส่งต่อเป็นลำดับ ๆ ตามที่โปรแกรมผู้ใช้เลือกเองโดยสุ่มและเข้ารหัสลับเป็นชั้น ๆ (คล้ายหัวหอม) ส่วนชื่อเป็นอักษรย่อจากโปรเจ็กต์ดั้งเดิมคือ "The Onion Router" (เราเตอร์หัวหอม)

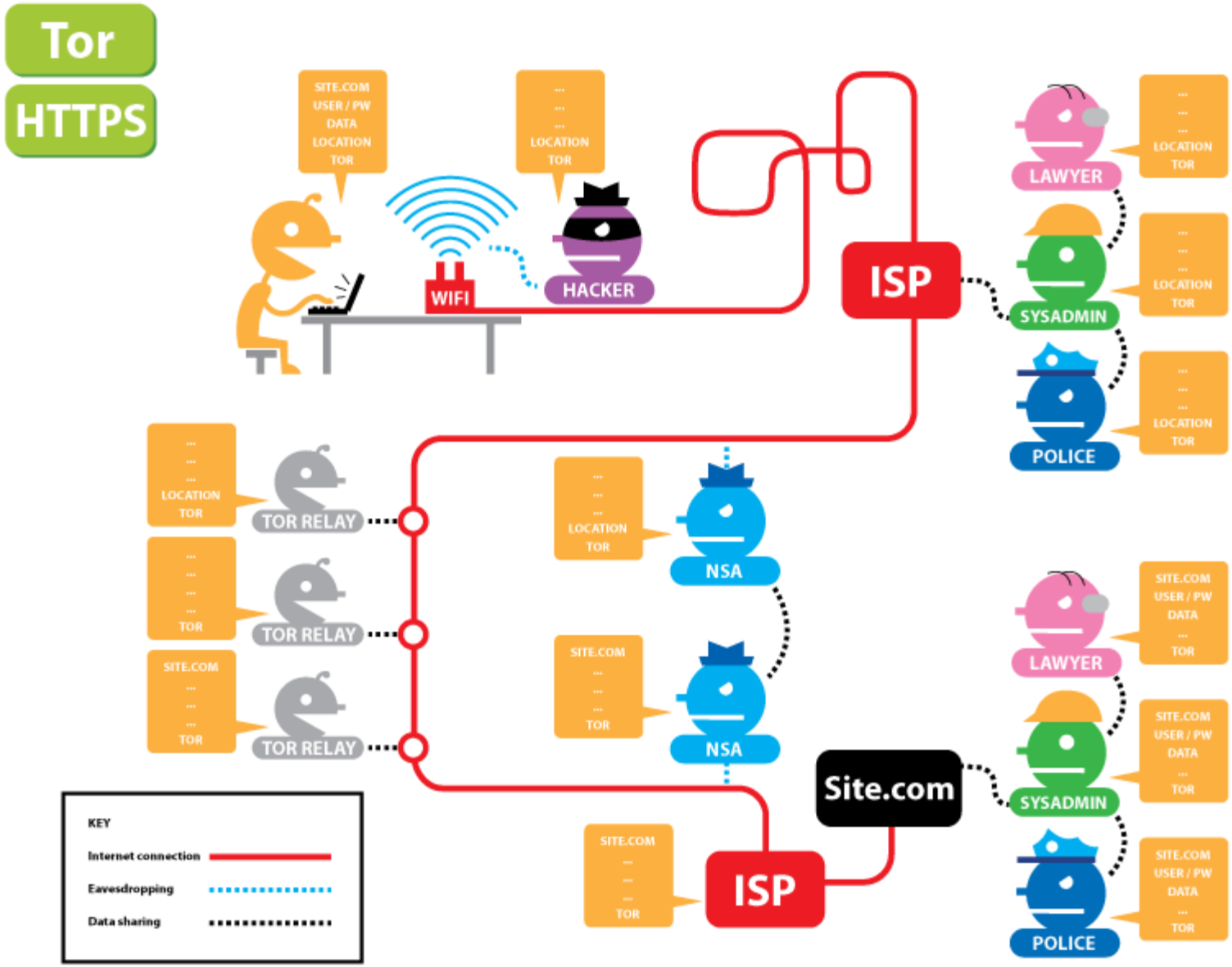


TOR คือ VPN ที่วิ่งอยู่ภายใน VPN หลายๆชั้น


Tor
HTTPS
SITE.COM USER / PW DATA LOCATION
SITE.COM USER / PW DATA LOCATION
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
NSA
NSA
ISP
Site.com
KEY
Internet connection
Eavesdropping
Data sharing


Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
SITE.COM
...
...
LOCATION
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
NSA
NSA
Site.com
ISP
KEY
Internet connection
Eavesdropping
Data sharing


Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
TOR
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
TOR RELAY
TOR RELAY
TOR RELAY
NSA
NSA
Site.com
ISP
KEY
Internet connection
Eavesdropping
Data sharing


Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
TOR
...
LOCATION
TOR
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
TOR RELAY
TOR RELAY
TOR RELAY
NSA
NSA
Site.com
ISP
KEY
Internet connection
Eavesdropping
Data sharing

Messaging

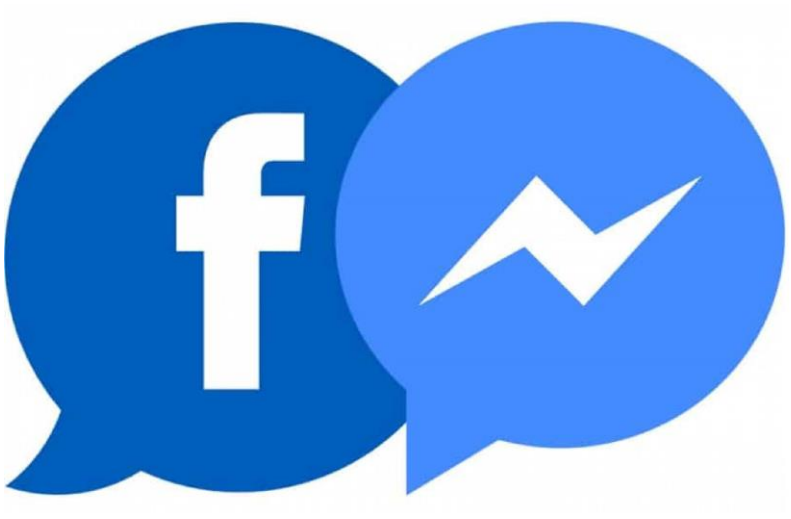
สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1.ไม่ควรบันทึก Password ไว้ที่โปรแกรม

2.กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง

3.มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่าง ๆ ที่ได้รับมา

4.มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ



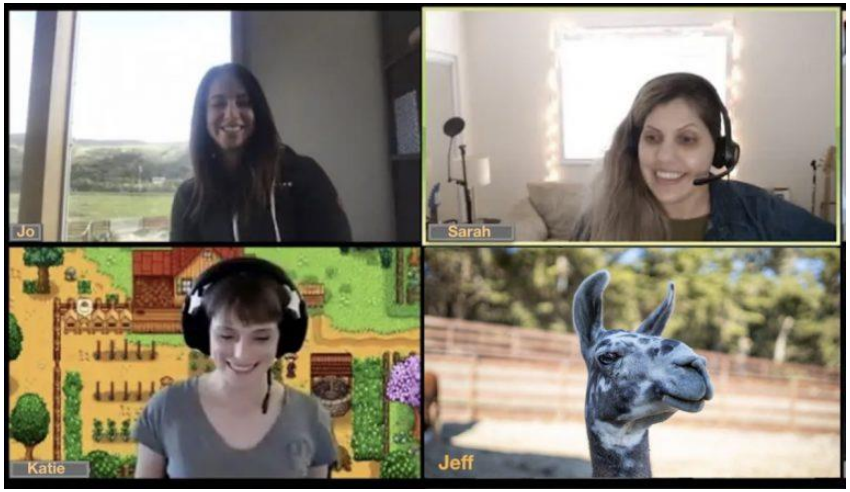
Fake News

Fake News หรือ ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมากเนื่องจากข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือ ซึ่งทาให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตุข่าวปลอม

1. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ
2. ระบุที่มาของข่าวไม่ได้
3. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
4. สำนวนการเขียนออกแนวการโฆษณา

Conference



สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1.ใช้สถานที่เหมาะสมกับการ Conference
2.ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
3.แชร์เอกสารต่าง ๆ อย่างระมัดระวัง
4.ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
5.มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

Cloud Storage

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

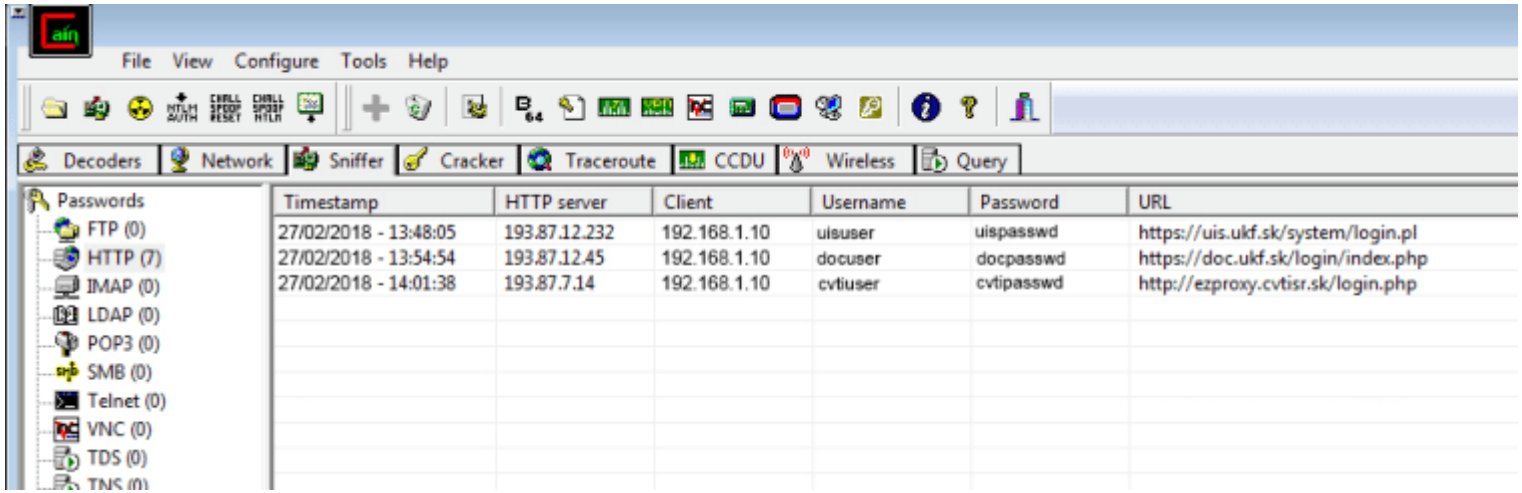
1.แยก User ในการใช้งานของแต่ละบุคคล
2.ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
3.ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
4.ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ
5.มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ
6.มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

Free WIFI

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

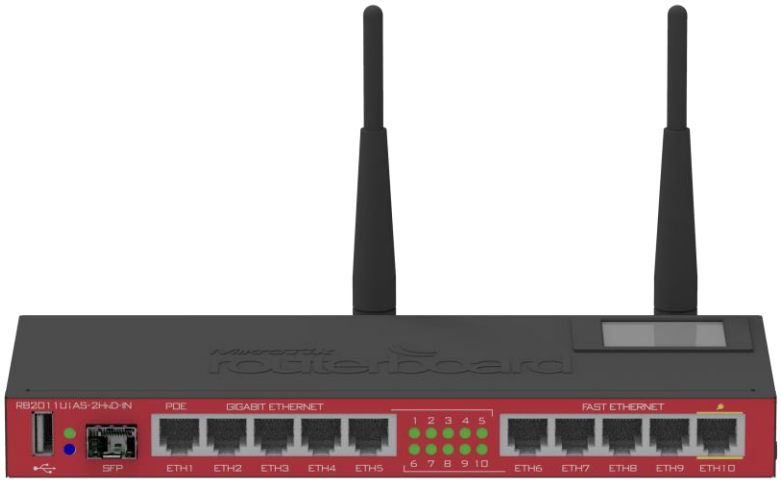
1.ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน

2.หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ



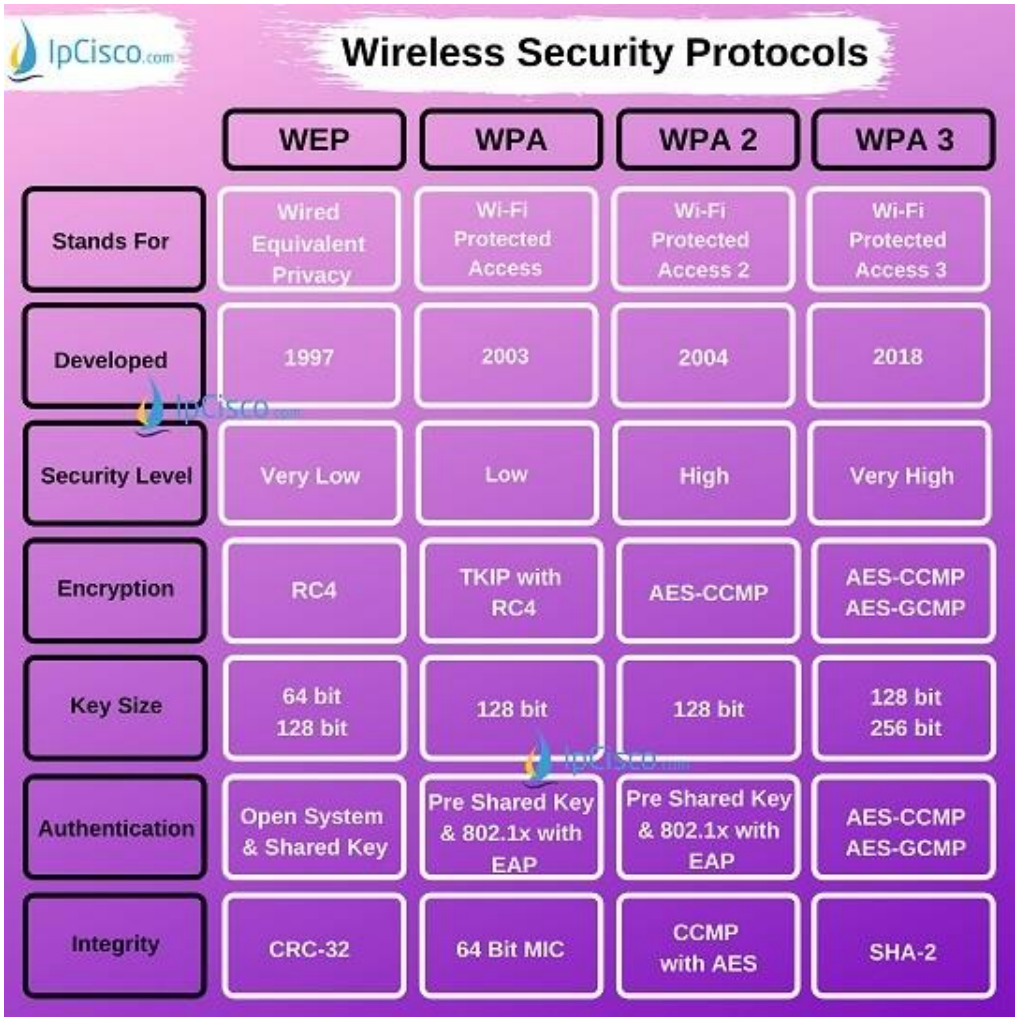
Home WIFI

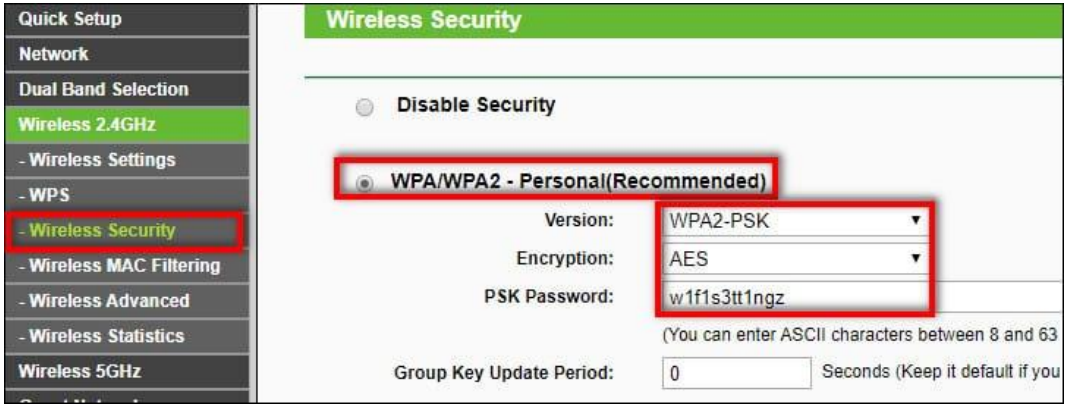
Home WIFI router



Business WIFI router

Home WIFI





RADIUS Supported

Mobile

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1.เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์

2.ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา

3.กำหนด Application permission ให้เหมาะสม

4.มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

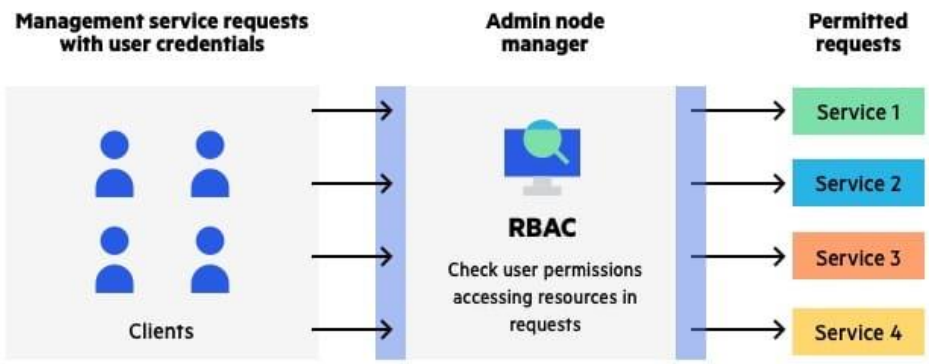
5.มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

Internet Connection

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน
2. เปลี่ยน SSID และรหัสผ่านของ WIFIที่กำหนดมาจากผู้ให้บริการ
3. กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น

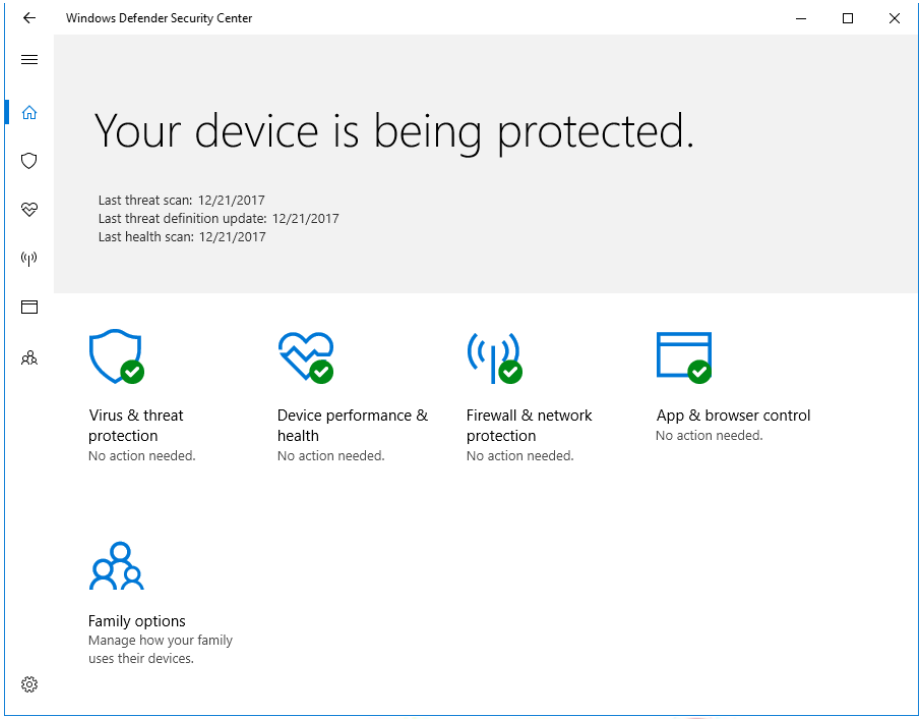
Sn.	CCTV Company Name	Default Username	Default Password	Default IP Address
1.	Hikvision	admin	12345	192.0.0.64
2.	TVT	admin	123456	192.168.226.1
3.	Sony	admin	admin	192.168.0.100
4.	Samsung	root	4321 or admin	192.168.1.200
5.	Samsung	admin	4321 or 1111111	192.168.1.200
6.	FLIR	admin	fliradmin	192.168.250.116
7.	Avigilon	admin	admin	no default/DHCP
8.	Panasonic	admin	12345	192.168.0.253
9.	Panasonic	admin1	password	192.168.0.253
10.	ACTi	Admin or admin	123456	192.168.0.100
11.	Axis	root	pass or no set password	192.168.0.90



IoT Devices

IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทางานร่วมกับระบบต่าง ๆ หรือแอปพลิเคชันต่าง ๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่ายเปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

“Antivirus” ยังมีความจำเป็นหรือไม่?

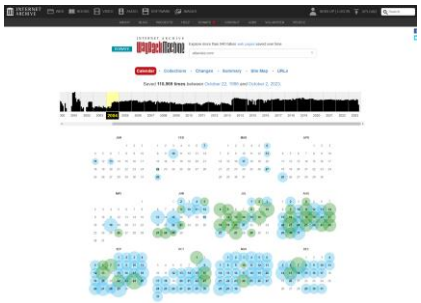


Symantec
McAfee
KASPERSKY lab
AVG Anti-Virus
COMODO SSLCERTIFICATE
Malwarebytes
WEBROOT SecureAnywhere
BullGuard
SOPHOS Silver Partner
bitdefender
AVIRA
panda
eset
F-Secure
TREND MICRO
VIPRE ANTIVIRUS
avast! be free
GDATA

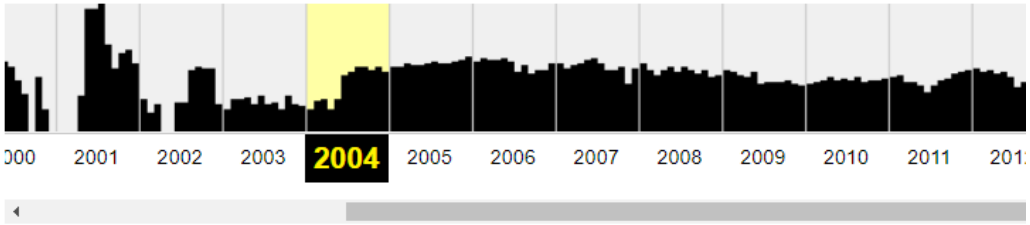
ร่องรอยดิจิทัล (Digital Footprint)

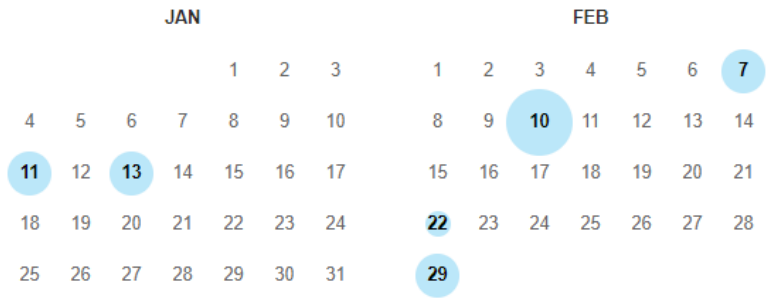
ร่องรอยดิจิทัล คือ ร่องรอยที่ผู้ใช้อินเทอร์เน็ตและโลกไซเบอร์กระทำการต่าง ๆ ในโลกดิจิทัล เช่น การใช้งานอัปโหลดข้อมูลส่วนตัว ไฟล์งาน รูปภาพ การใช้งานสมาร์ตโฟน แท็บเล็ต และคอมพิวเตอร์ โดยระบบต่าง ๆ ของอินเทอร์เน็ตจะบันทึกข้อมูลของผู้ใช้งาน เช่น ชื่อ และข้อมูลส่วนตัว วันเดินปีเกิด ตำแหน่งงาน ผลงาน ข้อมูลการศึกษา ประวัติส่วนตัว ของผู้ใช้งาน ร่องรอยดิจิทัล สามารถบอกให้ผู้อื่นทราบถึงสิ่งที่เราชอบ สิ่งที่สนใจ และสิ่งที่เราอยากทำ

- ร่องรอยดิจิทัล **ที่ผู้ใช้เจตนาบันทึก** (Active Digital Footprints) ร่องรอยดิจิทัล ของผู้ใช้งานที่เจตนาบันทึกไว้ในโลกออนไลน์ ข้อมูลที่เราตั้งใจเปิดเผยโดยที่รู้ตัว เช่น อีเมล เบอร์โทร ชื่อโปรไฟล์ เฟซบุ๊ก หรือสิ่งที่เราตั้งใจโพสต์ลงในโซเชียลมีเดีย เช่น สิ่งที่เราพูดหรือโพสต์ รูปที่เราเคยลง สิ่งที่เรากดไลก์ รีทวิต หรือแชร์ ที่ตั้งสถานที่ที่เราอยู่หรือเคยไป
- ร่องรอยดิจิทัล **ที่ผู้ใช้ไม่เจตนาบันทึก** (Passive Digital Footprints) ร่องรอยดิจิทัล ของผู้ใช้งานที่ไม่มีเจตนาบันทึกเอาไว้ในโลกออนไลน์ หรือข้อมูลแบบที่ไม่ได้ตั้งใจหรือไม่ได้รู้ตัว เช่น IP Address หรือ Search History ต่าง ๆ ที่เราถูกจัดเก็บเอาไว้ สิ่งที่เราเคยคลิกเข้าไป การซื้อสินค้าออนไลน์ของเรา การเปิดระบบ GPS เป็นต้น



Internet Archive





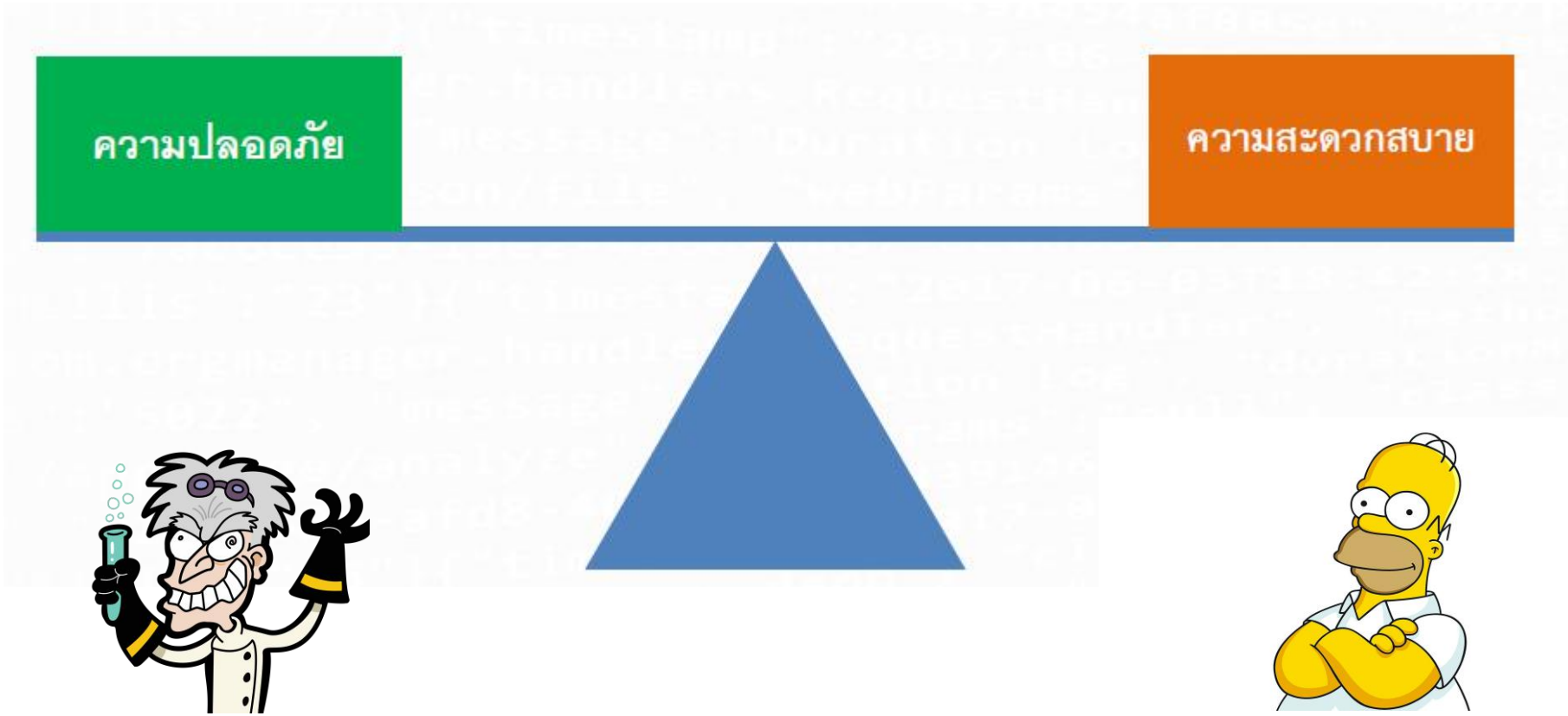
ร่องรอยดิจิทัล (Digital Footprint)

2 March 1997

ร่องรอยดิจิทัล (Digital Footprint)

9 Jan 2005

เราควรเลิกใช้อินเตอร์เน็ตดีหรือไม่ ?



สิ่งที่เราต้องทำคือเราต้องพยายามถ่วงน้ำหนัก ในส่วนของความปลอดภัย และความสะดวกสบาย ให้สมดุลกัน