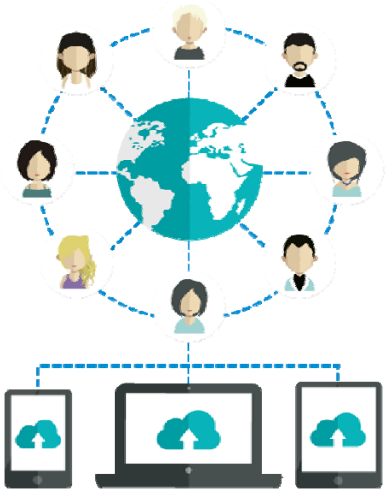
Security Awareness

การสร้างความตระหนักถึงภัยคุกคาม จากการใช้งานอินเทอร์เน็ต และการใช้เทคโนโลยีเพื่อคววามปลอดภัย

นางสาวภัทรกรณ์ สุ่มมาตย์ และทีมงาน

อินเทอร์เน็ต (Internet)



Internet

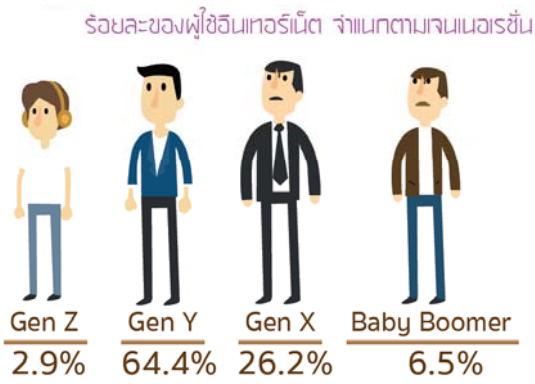
InterConnection Network

เครือข่ายคอมพิวเตอร์ที่ใหญ่ที่สุดในโลก เกิดขึ้นจากระบบเครือข่ายคอมพิวเตอร์เล็ก ๆ รวมกันเป็นระบบเครือข่ายใหญ่ เพื่อใช้ในการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลกันทั่วโลก

ผลการสำรวจพฤติกรรมการใช้งานอินเทอร์เน็ตของประเทศไทย

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) หรือ ETDA (เอ็ตด้า)
"ผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2558"

มีผู้ตอบออนไลน์ที่สมบูรณ์ 10,434 คน จากผู้ตอบออนไลน์ **17,010 คน**
โดยแบ่งออกเป็น 4 กลุ่มได้แก่
Gen z (น้อยกว่า 15 ปี) , **Gen y** (15-34 ปี) , **Gen x** (35-50 ปี) และ **Baby Boomer** (51 ปีขึ้นไป)

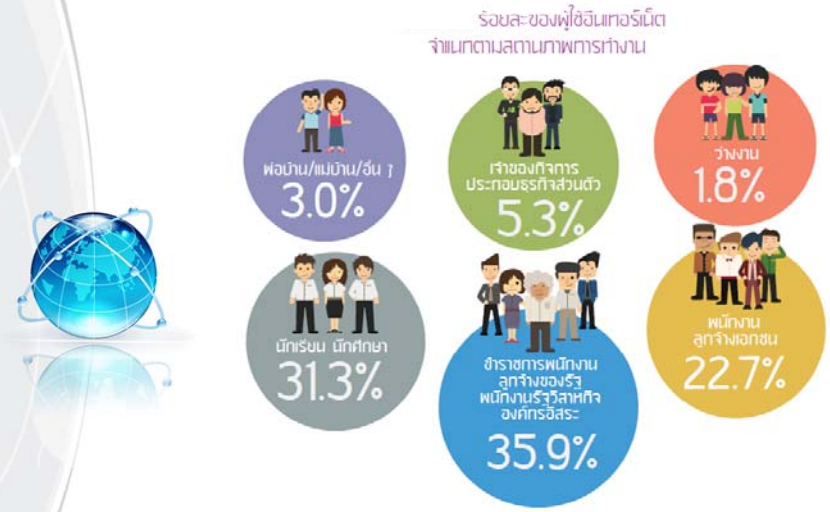


ผลการสำรวจพฤติกรรมการใช้งานอินเทอร์เน็ตของประเทศไทย

เพศ

ผู้ใช้อินเทอร์เน็ต ทั้งหมด ประกอบด้วยเพศชาย ร้อยละ 42.4 เพศหญิง ร้อยละ 55.8 และเพศที่สาม ร้อยละ 1.8 ดังแสดงในภาพ 28

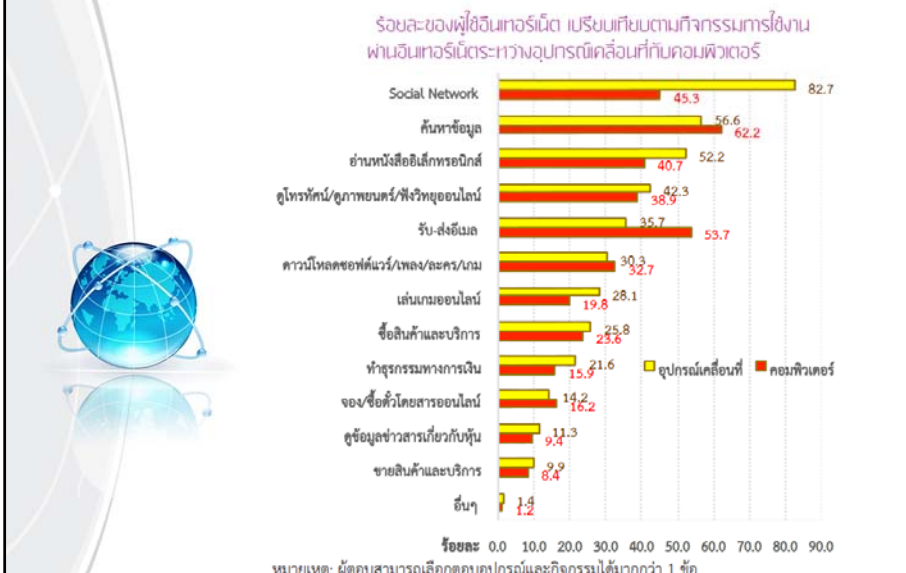
ผลการสำรวจพฤติกรรมการใช้งานอินเทอร์เน็ตของประเทศไทย



ผลการสำรวจพฤติกรรมการใช้งานอินเทอร์เน็ตของประเทศไทย

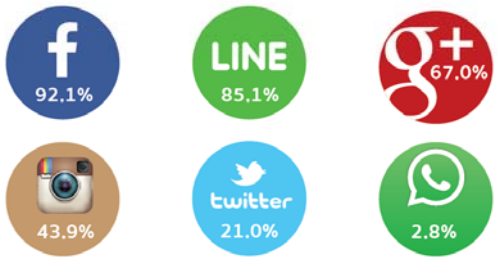
ผลการสำรวจพฤติกรรมการใช้งานอินเทอร์เน็ตของประเทศไทย

ผลการสำรวจพฤติกรรมการใช้งานอินเทอร์เน็ตของประเทศไทย



ผลการสำรวจพฤติกรรมการใช้งานอินเทอร์เน็ตของประเทศไทย

ร้อยละของผู้ใช้อินเทอร์เน็ต
เปรียบเทียบตามเครือข่ายสังคมออนไลน์ที่ใช้บริการเป็นประจำ



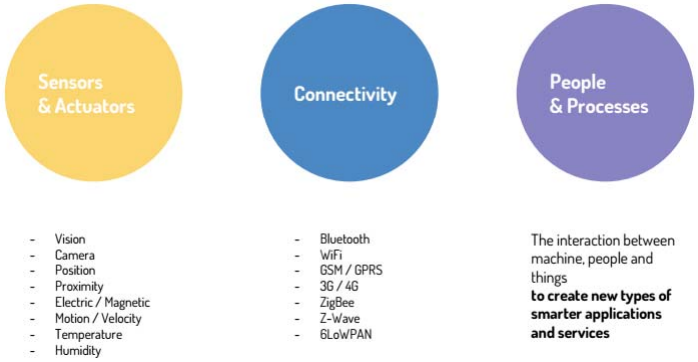
หมายเหตุ: เลือกตอบได้มากกว่า 1 ข้อ

ทุกวันนี้ **"อินเทอร์เน็ต"** เกี่ยวข้องกับชีวิตคนเราตลอดเวลา ตั้งแต่ตื่นเช้าไปจนกระทั่งถึงเข้านอน ทั้งกิจกรรมส่วนตัว การทำธุรกิจ และการทำธุรกรรมต่างๆ ตั้งแต่การรับส่งอีเมล การค้นหาข้อมูลผ่านเว็บไซต์ต่างๆ การอัพโหลดรูปและข้อความขึ้นสู่โซเชียลเน็ตเวิร์ก การฝากถอนและโอนเงินกับธนาคาร รวมทั้งการสั่งซื้อสินค้าโดยไม่ต้องเดินทางไปที่ร้านให้เสียเวลา

Internet of Things (IoT)

Internet of Things (หรือบางที่เรียก Internet of Everything)
แปลตรงๆ คือ"อินเทอร์เน็ตสำหรับสิ่งของ"
(บางแห่งเรียก M2M ย่อมาจาก machine to machine)

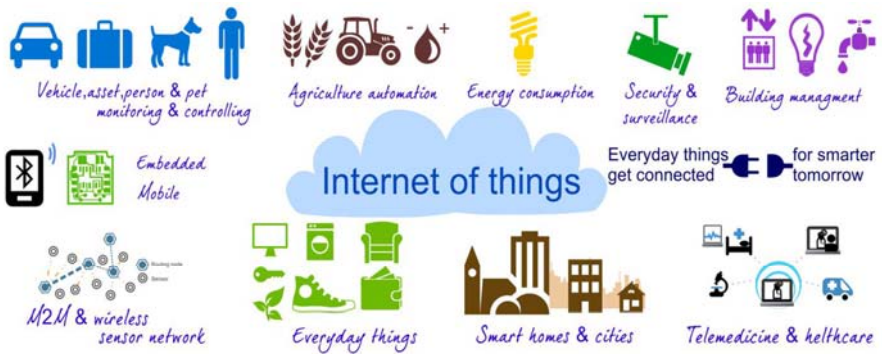
Internet of Things (IoT)



IoT ประกอบด้วย 3 ส่วน

- Sensor & Actuators คือการดึงเอาผลลัพธ์ออกมา
- Connectivity คือการเชื่อมต่ออินเตอร์เน็ตต่างๆ เช่น Wi-Fi ,GPRS, 3G
- People & Process ตัวสำคัญที่สุดที่จะผูกสิ่งต่างๆ เอาไว้รวมกัน โดยสร้างเป็นแอปพลิเคชั่น/บริการใหม่

Internet of Things (IoT)



การเปลี่ยนแปลงรูปแบบการกระทำความผิด

ยุคเก่า

ยุคปัจจุบัน

ภัยคุกคาม

***ภัยคุกคาม* หมายถึง** พฤติกรรมไม่หวังดีต่อผู้ใช้งานคนอื่นๆ ในระบบเครือข่ายอินเตอร์เน็ต โดยกระทำตนเป็นภัยคุกคามต่อข้อมูลและระบบเครือข่าย

ประเภทของภัยคุกคามที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่าย
สามารถจำแนกได้ 2 ประเภทหลัก ๆ ดังนี้

1. **ภัยคุกคามทางตรรกะ (Logical)**
2. **ภัยคุกคามทางกายภาพ (Physical)**

ภัยคุกคามทางตรรกะ (Logical)

ภัยคุกคาม ที่เกิดขึ้นนั้นจะมุ่งเน้นไปทางด้านข้อมูลหรือ สารสนเทศ ไม่ว่าจะเป็นการเข้าใช้ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต หรือขัดขวางไม่ให้ระบบคอมพิวเตอร์ทำงานได้ตามปกติ และอาจเข้าใช้ข้อมูล ลบข้อมูล และแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ซึ่งการกระทำดังกล่าวนั้น *ส่วนใหญ่เกิดจากฝีมือของ ผู้ใช้งานคอมพิวเตอร์แทบทั้งสิ้น*

ภัยคุกคามทางตรรกะ (Logical)

Hacker VS Cracker

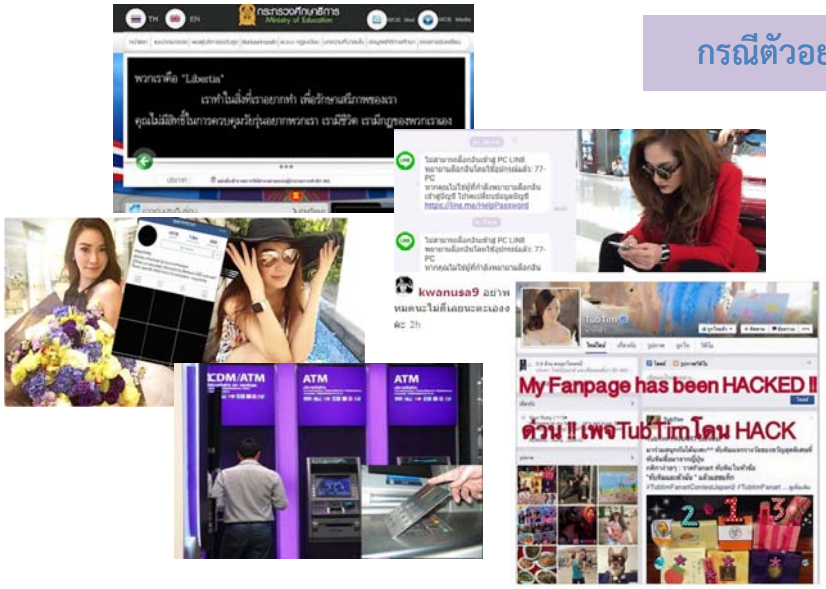
Hacker คือพวกเค้าเป็นบุคคลที่มีความสนใจในเรื่องคอมพิวเตอร์อย่างลึกซึ้ง Hacker นั้นไม่ได้มีเจตนาในการที่จะเจาะระบบเพื่อประโยชน์ส่วนตัว แต่ต้องการที่จะหาช่องโหว่ของระบบ และหาสาเหตุที่ รวมทั้งวิธีการปิดช่องโหว่นั้นด้วย

Cracker จะเป็นบุคคลที่จะพยายามเจาะระบบรักษาความปลอดภัยเพื่อวัตถุประสงค์ไม่ดีต่าง ๆ หรือพยายามจะขโมยข้อมูลและหผลประโยชน์จากผู้เสียหายต่าง ๆ

ไม่ว่าจะเป็นแฮกเกอร์ (Hacker) หรือ แคร็กเกอร์(Cracker)
ถ้ามีการแอบเข้าใช้งานระบบคอมพิวเตอร์เครือข่ายของผู้อื่นโดยไม่ได้รับอนุญาต
แม้ว่าจะไม่ประสงค์ร้ายก็ถือว่าเป็นการกระทำ ที่ไม่ดีทั้งสิ้น เพราะขาดจริยธรรมด้านคอมพิวเตอร์

ภัยคุกคามทางตรรกะ (Logical)

กรณีตัวอย่าง



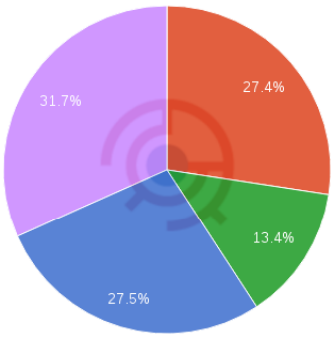
ภัยคุกคามทางตรรกะ (Logical)

ภัยคุกคามทางกายภาพ (Physical)

ภัยคุกคาม ลักษณะนี้มุ่งเน้นอุปกรณ์ ประเภทฮาร์ดแวร์ ที่ใช้ในระบบคอมพิวเตอร์และระบบเครือข่าย เช่น ทำให้ฮาร์ดดิสก์เสีย ทำให้คอมพิวเตอร์ทำงานผิดพลาด *โดยส่วนใหญ่แล้วจะเกิดภัยจากธรรมชาติ* อาจเป็นน้ำท่วม ไฟไหม้ ฟ้าฝ่า แผ่นดินไหว เป็นต้น และบางครั้ง อาจเกิดจากการกระทำของมนุษย์ที่ทำความเสียหายให้กับตัวเครื่องและอุปกรณ์ *ทั้งโดยเจตนาหรือไม่เจตนา*

สถิติภัยคุกคาม

สถิติภัยคุกคาม ตั้งแต่มกราคม – พฤษภาคม 2559



- การพยายามบุกรุก (13.4%)
- การหลอกลวง (27.4%)
- การโจมตี (27.5%)
- การโจมตีด้วยโค้ดอันตราย (31.7%)

ข้อมูลจาก ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทยหรือ ThaiCERT (ไทยเซิร์ต)

ภัยคุกคาม

ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts) (13.4%)

ภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ เพื่อจะได้เข้าครอบครอง หรือทำให้เกิดความขัดข้อง ภัยคุกคามนี้รวมถึงความพยายามจะบุกรุก/เจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่ม/เดาข้อมูล

ภัยคุกคาม

การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) (27.4%)

ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ

ภัยคุกคาม

การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) (27.5%)

ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

ภัยคุกคาม

โปรแกรมไม่พึงประสงค์ (Malicious Code) (31.7%)

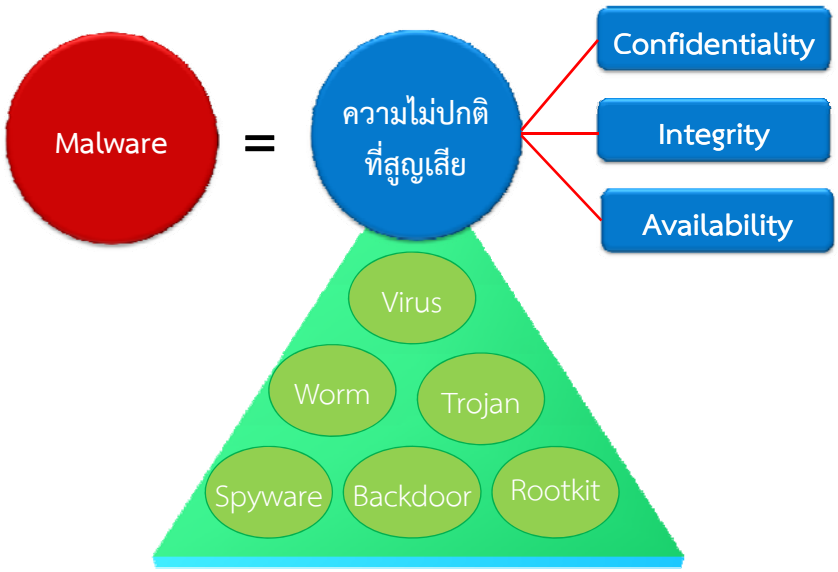
ภัยคุกคาม ที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้น เพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์ กับผู้ใช้งานหรือระบบ (Malicious Code) ทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือซอฟต์แวร์ โดยปกติโปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือซอฟต์แวร์ก่อน จึงจะสามารถติดตั้งตัวเองหรือทำงานได้ เช่น Virus, Worm, Trojan หรือ Spyware ต่างๆ

มัลแวร์ (Malware)

มัลแวร์คืออะไร ?

มัลแวร์ (Malware) ย่อมาจาก Malicious Software หมายถึง ซอฟต์แวร์ไม่พึงประสงค์ เป็นโปรแกรมที่ถูกเขียนขึ้นมาเพื่อทำอันตรายกับระบบ เช่น ทำให้คอมพิวเตอร์ทำงานผิดปกติ ขโมย/ทำลายข้อมูล หรือเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องคอมพิวเตอร์ เป็นต้น

มัลแวร์ (Malware)



มัลแวร์ (Malware)

ในการแบ่งประเภทของมัลแวร์ โดยปกติจะแบ่งตามพฤติกรรมการทำงาน

ตัวอย่างเช่น

- **Virus** - แพร่กระจายตัวเองไปยังเครื่องอื่นๆ ผ่านไฟล์
- **Worm** - แพร่กระจายตัวเองไปยังเครื่องอื่นๆ ผ่านระบบเครือข่าย (เช่น อีเมล หรือระบบแชร์ไฟล์)
- **Trojan** - หลอกว่าเป็นโปรแกรมที่ปลอดภัยแล้วให้ผู้ใช้หลงเชื่อนำไปติดตั้ง
- **Backdoor** - เปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่อง
- **Rootkit** - เปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่อง พร้อมได้สิทธิ์ของผู้ดูแลระบบ
- **Spyware** - แอบดูพฤติกรรมการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัวด้วย

มัลแวร์ (Malware)

การติดมัลแวร์ โดยหลักๆ มีอยู่ 2 วิธีคือ

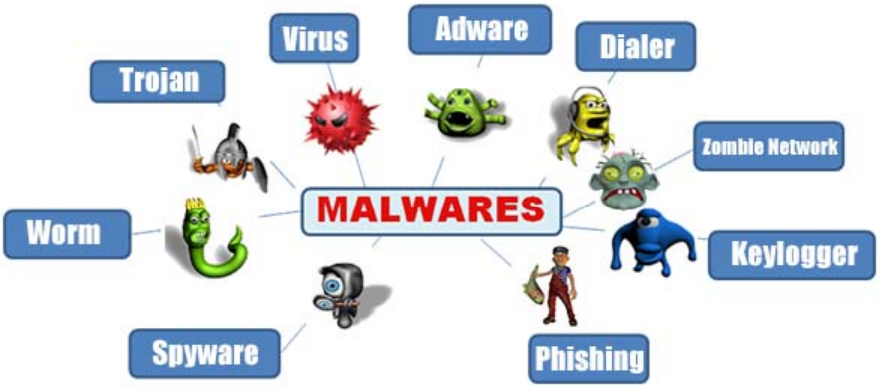
1. หลอกให้ผู้ใช้เป็นคนรันโปรแกรมมัลแวร์เอง
2. ติดตั้งตัวเองลงในเครื่องโดยอัตโนมัติผ่านช่องโหว่ของซอฟต์แวร์ วิธีการแพร่กระจายมัลแวร์

ช่องโหว่ (Vulnerability)

ช่องโหว่ คือ ความอ่อนแอ่ของระบบคอมพิวเตอร์ หรือ ระบบเครือข่ายที่เป็ดโอกาสให้สิ่งที่เป็นภัยคุกคามสามารถเข้าถึงสารสนเทศในระบบได้ซึ่งจะนำไปสู่ความเสียหายแก่สารสนเทศ หรือแม้แต่การทำงานของระบบ

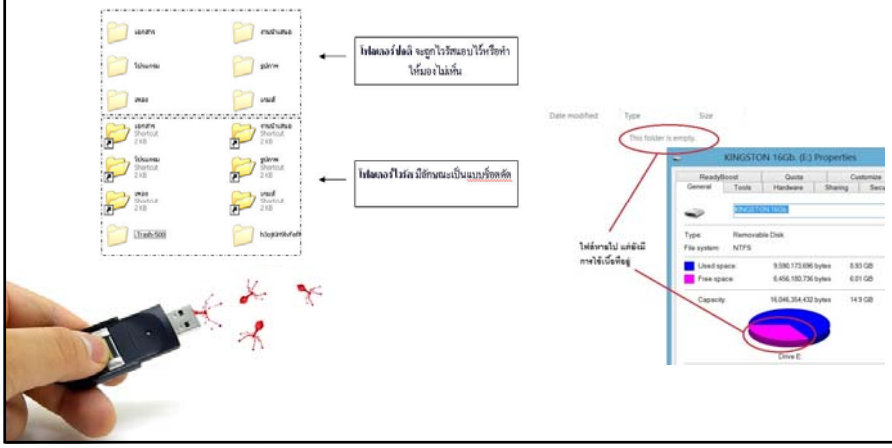
มัลแวร์ (Malware)

ตัวอย่าง



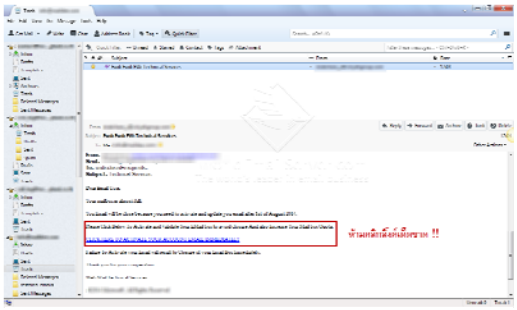
Virus (ไวรัส)

Virus (ไวรัส) แพร่เชื้อไปติดไฟล์อื่นๆในคอมพิวเตอร์ของคุณโดยการเพิ่มจำนวนตัวมันเองขึ้นมาเป็นจำนวนมาก ไวรัสต้องส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ได้ต้องอาศัยไฟล์พาหะ สิ่งที่มันทำคือสร้างความเสียหายให้กับไฟล์



Worm (หนอน)

Worm (หนอน) โปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้สามารถแพร่กระจายตัวเองจากเครื่องคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่งโดยอาศัยระบบเน็ตเวิร์ค (E-mail) ซึ่งการแพร่กระจายสามารถทำได้ด้วยตัวของมันเอง ซึ่งจะแพร่กระจายได้อย่างรวดเร็ว และทำความเสียหายรุนแรงกว่าไวรัสมาก

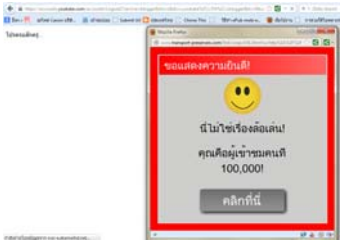


Trojan (ม้าโทรจัน)

Trojan (ม้าโทรจัน) เป็นโปรแกรมที่ถูกเขียนขึ้นมาให้ทำตัวเหมือนว่าเป็น โปรแกรมทั่ว ๆ ไป เพื่อหลอกล่อผู้ใช้ให้ทำการเรียกขึ้นมาทำงาน อาศัยการหลอกคนใช้ให้ดาวน์โหลดเอาไปใส่เครื่องเองหรือด้วยวิธีอื่นๆ สิ่งที่มันทำคือ เปิดโอกาสให้ผู้ไม่ประสงค์ดีเข้ามาควบคุมเครื่องที่ติดเชื้อจากระยะไกล ซึ่งจะทำอะไรก็ได้

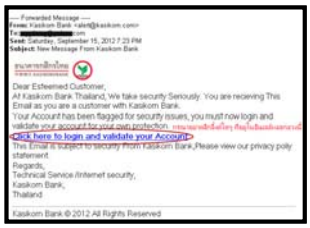
Spyware (สปายแวร์)

Spyware (สปายแวร์) แต่ไม่ได้มีความหมาย ลึกลับเหมือนอย่างชื่อ ในอันที่จริง สปายแวร์จะได้รับความรู้จักในชื่อของ **Adware** ด้วย ดังนั้นคำว่า สปายแวร์ จึงเป็นเพียงการระบุประเภทของซอฟต์แวร์เท่านั้น ส่วนความหมายที่แท้จริง สปายแวร์ หมายถึงโปรแกรมที่แอบเข้ามาติดตั้งในเครื่องคอมพิวเตอร์โดยที่ผู้ใช้อาจไม่ได้เจตนา



Phishing (ฟิชชิง)

Phishing (ฟิชชิง) การหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์

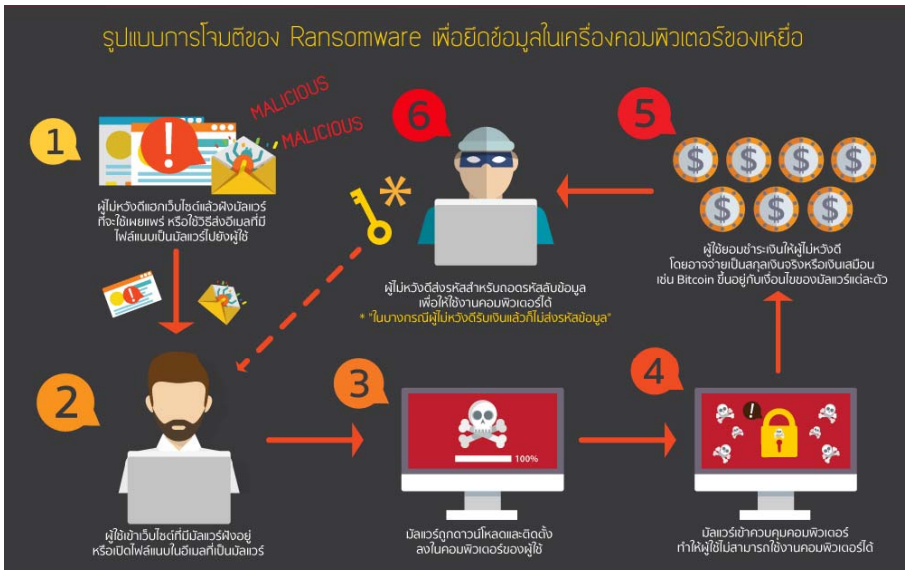


Ransomware (แรนซัมแวร์)

Ransomware (**แรนซัมแวร์**) เป็นมัลแวร์ที่ออกแบบมาเพื่อเรียกค่าไถ่เหยื่อ โดยเฉพาะ โดยส่วนใหญ่เกิดจากการคลิกลิงก์ อันตราย หรือไปดาวน์โหลดไฟล์ ที่แนบใน อีเมลเพื่อเปิดเอกสารแต่กลายเป็นพวกมัลแวร์อันตราย

Ransomware (แรนซัมแวร์)

Ransomware (แรนซัมแวร์)



BitCoin

บิตคอย (bitcoin)

เงินในโลกดิจิตอล (Digital Currency) หรือเงินในยุคคอมพิวเตอร์

BitCoin

ความมั่นคงปลอดภัย SECURITY

ความมั่นคงปลอดภัย (Security)

คือ สถานะที่มีความปลอดภัย ไร้กังวล อยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ

การรักษาความมั่นคงปลอดภัยของสารสนเทศ (Information Security)

คือผลที่เกิดขึ้นจาการใช้ระบบของนโยบายและ/ หรือ ระเบียบปฏิบัติที่ใช้ในการพิสูจน์ทราบ ควบคุม และป้องกันการเปิดเผยข้อมูล (ที่ได้รับคำสั่งให้มีการป้องกัน) โดยไม่ได้รับอนุญาต

ความมั่นคงปลอดภัย SECURITY

การทำให้ระบบคอมพิวเตอร์มีความสามารถตามมีเป้าหมาย 3 ประการดังนี้

1. Confidentiality : ข้อมูลถูกเก็บเป็นความลับ
2. Integrity : ข้อมูลมีความถูกต้องและน่าเชื่อถือ
3. Availability : ระบบมีความเสถียร และทำงานไม่ผิดพลาด

การป้องกันภัยคุกคาม

มาตรการความปลอดภัยขั้นพื้นฐาน (Basic Security Measures)

- ✓ความปลอดภัยบนสภาพแวดล้อมภายนอก (External Security)
- ✓ความปลอดภัยด้านการปฏิบัติงาน (Operational Security)
- ✓การตรวจตราเฝ้าระวัง (Surveillance)
- ✓การใช้รหัสผ่านและระบบแสดงตัวตน (Passwords and ID Systems)
- ✓การตรวจสอบ (Auditing)
- ✓สิทธิ์การเข้าถึง (Access Rights)
- ✓การป้องกันไวรัส (Guarding Against Viruses)

ความปลอดภัยบนสภาพแวดล้อมภายนอก

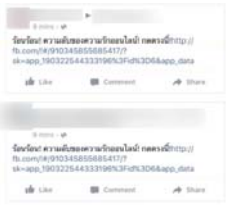
ความปลอดภัยบนสภาพแวดล้อมภายนอก

เป็นลักษณะทางกายภาพที่ต้องการป้องกันระบบคอมพิวเตอร์ อุปกรณ์ หรือเครือข่ายเกิดความเสียหาย ตัวอย่างเช่น การป้องกันไฟไหม้ อุทกภัย แผ่นดินไหว ไฟตก/ไฟกระชาก และการถูกทำลายหรือถูกขโมย

ความปลอดภัยด้านการปฏิบัติงาน

ความปลอดภัยด้านการปฏิบัติงาน

บนเครือข่ายคอมพิวเตอร์ จะเป็นการพิจารณาด้วยการสร้างข้อจำกัดของบุคคลใดบุคคลหนึ่งในการ เข้าถึงระบบ



การตรวจตราเฝ้าระวัง

ผู้บริหารเครือข่ายส่วนใหญ่ต้องมี**กระบวนการตรวจตราเฝ้าระวัง** เพื่อมิให้ระบบคอมพิวเตอร์ถูกทำลายหรือถูกลักขโมย ศูนย์ปฏิบัติการ คอมพิวเตอร์บางศูนย์ ได้มีการติดตั้งกล้องโทรทัศน์วงจรปิดตามจุดสำคัญต่างๆ ในบริเวณห้อง ซึ่งทำให้สามารถตรวจตราเฝ้าระวังผ่าน จอโทรทัศน์ตามบริเวณที่กล้องได้ติดตั้งอยู่ ทำให้สามารถสังเกตพฤติกรรมและเหตุการณ์ความเคลื่อนไหวของบุคคลภายในที่ต้องการ ลักลอบหรือขโมยข้อมูล

การใช้รหัสผ่านและระบบแสดงตัวตน

การใช้รหัสผ่าน ก่อนเข้าสู่ระบบ รวมถึงรหัสผ่านสำหรับเรียกดูข้อมูลสำคัญๆ บางอย่าง การใช้รหัสผ่านเป็น มาตรการหนึ่งของความปลอดภัยขั้นพื้นฐานที่นิยมใช้กันมานาน สำหรับหน่วยงานที่ต้องการระดับความปลอดภัยมากกว่าที่จะใช้รหัสผ่าน จึงได้มีระบบที่ใช้สำหรับแสดงตัวตน โดยใช้คุณสมบัติ ทางกายภาพของแต่ละบุคคลที่มีความแตกต่างกัน

รหัสผ่าน คือ สายอักขระที่บุคคลสามารถใช้เพื่อเข้าสู่ระบบคอมพิวเตอร์ และเข้าถึงแฟ้ม โปรแกรม และทรัพยากรอื่นๆ

***รหัสผ่าน เปรียบเสมือน* กุญแจเข้าบ้านของเรา**

การใช้รหัสผ่านและระบบแสดงตัวตน

การใช้รหัสผ่านและระบบแสดงตัวตน

Rank	Password
1	123456
2	password
3	12345678
4	qwerty
5	12345
6	123456789
7	football
8	1234
9	1234567
10	baseball

การใช้รหัสผ่านและระบบแสดงตัวตน

ทำอย่างไรจึงจะช่วยให้รหัสผ่านคาดเดาได้ยาก

สิ่งที่ท้าทายความสามารถ คือ การสร้างรหัสผ่านที่คุณสามารถจดจำได้ แต่ผู้อื่นสามารถคาดเดาได้ยาก

สิ่งที่ควรทำในการสร้างรหัสผ่าน	สิ่งที่ไม่ควรทำในการสร้างรหัสผ่าน
✓ ใช้รหัสผ่านที่ยาว (อย่างน้อย 7 ตัว)	× อย่าใช้ส่วนใดส่วนหนึ่งหรือทั้งหมดของชื่อผู้ใช้
✓ ใช้ตัวอักษรตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก ตัวเลข รวมทั้งสัญลักษณ์ต่างๆ ประกอบกัน	× อย่าใช้คำที่มีความหมายในภาษาใดๆ
✓ ใช้สัญลักษณ์อย่างน้อยหนึ่งตัวในตำแหน่งที่ 2 - 6	× อย่าใช้ตัวเลขที่อยู่ในตำแหน่งเดียวกับตัวอักษรในการคิดคำ
✓ ใช้ตัวอักษรที่แตกต่างกันอย่างน้อย 4 ตัว (อย่าใช้ตัวอักษรซ้ำกัน)	× อย่าใช้ตัวอักษรหรือหมายเลขที่เรียงต่อกัน (เช่น abcdefg หรือ "234567")
✓ ใช้ตัวเลขและตัวอักษรแบบสุ่ม	× อย่าใช้แป้นพิมพ์ที่อยู่ติดกัน (เช่น "qwerty")

การใช้รหัสผ่านและระบบแสดงตัวตน

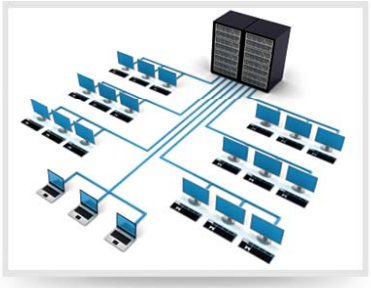
การจัดการรหัสผ่านที่ดีขึ้น

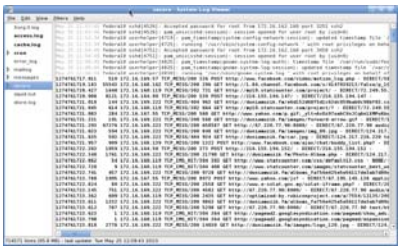
มีคนจำนวนมากเขียนรหัสผ่านที่เป็นความลับของตน แล้วติดไว้ที่หน้าจอคอมพิวเตอร์ หรือพับไว้ในลิ้นชักข้างเครื่องคอมพิวเตอร์ เรามาจัดการรหัสผ่านของคุณอย่างปลอดภัยมากขึ้น

สิ่งที่ควรทำในการจัดการรหัสผ่าน	สิ่งที่ไม่ควรทำในการจัดการรหัสผ่าน
✓ เก็บรหัสผ่านของคุณไว้เป็นความลับ	x อย่าเขียนลงในกระดาษ
✓ ใช้รหัสผ่านที่แตกต่างกันสำหรับแต่ละเว็บไซต์	x อย่าใช้คุณสมบัติ "จำรหัสผ่านของฉัน" บนเว็บ
✓ เปลี่ยนรหัสผ่านของคุณอย่างน้อยทุกๆ 6 เดือน	

การตรวจสอบ

การตรวจสอบระบบคอมพิวเตอร์ เป็นแนวทางหนึ่งที่ใช้งานอย่างได้ผลในกรณีป้องกันผู้ไม่หวังดีหรือก่อการร้าย ระบบการตรวจสอบ ส่วนใหญ่มักใช้ซอฟต์แวร์เพื่อตรวจสอบหรือเฝ้าระวัง การบันทึกเป็นหลักฐานไว้ใน ล็อกไฟล์ (Log File) ซึ่งมีรายละเอียดที่บันทึกไว้ เช่น วันที่ เวลา และบุคคลที่เข้า มาใช้งาน สิ่งเหล่านี้ทำให้เราสามารถตรวจสอบย้อนหลังได้ เข้ามาเมื่อไร เวลาใด ทำให้เราสามารถสังเกตพฤติกรรมนั้นได้

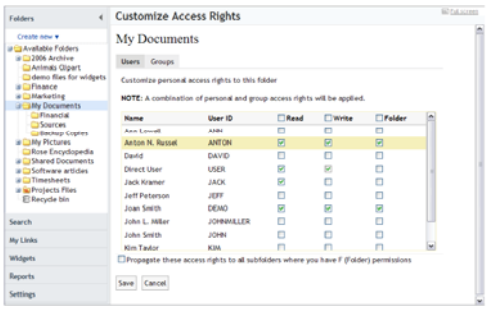




สิทธิ์การเข้าถึง

การกำหนดสิทธิ์การใช้งาน และโดยปกติผู้บริหารเครือข่ายจะเป็นผู้กำหนดอำนาจสิทธิการใช้งานของยูสเซอร์ตามความเหมาะสม หรือปฏิบัติตามนโยบายของฝ่ายบริหารระดับสูง โดยการกำหนดสิทธิการใช้งานจะพิจารณาจากปัจจัยอยู่ 2 ปัจจัย คือ **ใคร และ อย่างไร** (Who and How)

- ❑ **ใคร (Who)** หมายถึง ควรกำหนดสิทธิ์การใช้งานให้กับใคร
- ❑ **อย่างไร (How)** หมายถึง เมื่อใครผู้นั้นได้สิทธิแล้วจะกำหนดให้เขาเข้าถึงข้อมูลได้อย่างไร



การป้องกันไวรัส

โปรแกรมป้องกันไวรัส หรือ แอนติไวรัส (Antivirus Software) เป็นโปรแกรมที่สร้างขึ้นเพื่อคอยตรวจจับ ป้องกัน และกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์หรือมัลแวร์

โปรแกรมป้องกันไวรัสมี 2 แบบหลักๆ คือ

- **แอนติไวรัส (Anti-Virus)** เป็นโปรแกรมโปรแกรมป้องกันไวรัสทั่วๆไป จะค้นหาและทำลายไวรัสในคอมพิวเตอร์ของเรา
- **แอนติสปายแวร์ (Anti-Spyware)** เป็นโปรแกรมป้องกันการโจรกรรมข้อมูล จากไวรัสสปายแวร์ และจากแฮ็กเกอร์ รวมถึงการกำจัด Adsware ซึ่งเป็นป๊อปอัพโฆษณาอีกด้วย

การป้องกันไวรัส

ตารางแสดง 10 อันดับโปรแกรมสแกนไวรัส (Antivirus) ที่ดีที่สุดแห่งปี 2015

Rank	1st Place	2nd Place	3rd Place	4th Place	5th Place	6th Place	7th Place	8th Place	9th Place	10th Place
Score	95%	92%	85%	84%	81%	80%	79%	76%	69%	68%
Overall Protection	Best Overall Antivirus Software of 2015									
Antivirus Software (All Software Available for Instant Download)	VIPRE Antivirus	ESET Antivirus	AVG Anti-Virus	Bitdefender Antivirus	Norton Antivirus	Kaspersky Anti-Virus	Avira Antivirus	Avast Antivirus	McAfee Antivirus	Panda Antivirus
	Read More	Read More	Read More	Read More	Read More	Read More	Read More	Read More	Read More	Read More
	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now

พรบ. คอมพิวเตอร์

พ.ร.บ.คอมพิวเตอร์ คืออะไร

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ มีเพื่อกำหนดความผิดในการกระทำที่มี “ระบบคอมพิวเตอร์” เข้า มาเกี่ยวข้อง ซึ่งระบบคอมพิวเตอร์นี้ เป็นได้ทั้งคอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์วางตัก คอมพิวเตอร์พกพา แท็บเล็ต โทรศัพท์มือถือ และสมาร์ทโฟน รวมถึงระบบต่าง ๆ ที่ควบคุมด้วยระบบคอมพิวเตอร์ เช่น ระบบควบคุมไฟฟ้า น้ำประปา ธนาคาร ฯลฯ

Thank you