ISO 27001:2013

ระบบการจัดการความปลอดภัยของข้อมูล

ISO27001:2013 มาตรฐานสากล

องค์กร ISO - International Organization for Standardization เป็นหน่วยงานที่ให้กำเนิดมาตรฐาน ISO27001 โดยเวอร์ชั่นล่าสุดคือ ISO27001:2013 ประกาศเมื่อ 1 ต.ค. 2013 ส่วนเวอร์ชั่น แรกประกาศใช้ครั้งแรกเมื่อปี 2550 (ISO27001:2005) หลังจากประกาศใช้ก็ได้รับความสนใจจากองค์กรทั้งภาครัฐและเอกชนทั่วโลก นำมาใช้งานและขอการรับรอง (Certification) ประเทศไทยเองก็ไม่แพ้ชาติใดในโลก มีหน่วยงานรัฐและเอกชนเริ่มทำ ISO27001 และขอการรับรองได้สำเร็จ เช่น บริษัท ไทยออยล์ จำกัด (มหาชน) บริษัท ทรู อินเทอร์เน็ต ดาต้าเซ็นเตอร์ จำกัด (True IDC) และรัฐวิสาหกิจอีกหลายแห่ง มาตรฐานนี้ออกแบบมาให้ใช้ได้ประเภทธุรกิจ หน่วยราชการ สถานศึกษา และใช้ได้กับองค์กรทั้งขนาดเล็กและขนาดใหญ่อย่างบริษัทข้ามชาติ ทำได้เหมือนกันครับ

ทำไมถึงต้องทำ ISO27001:2013

ลองนึกภาพดูสมมติท่านไปใช้บริการหน่วยงานราชการแห่งหนึ่ง ปรากฏว่าระบบไอทีล่มให้บริการไม่ได้ เจอแบบนี้ประชาชนผู้ใช้บริการเดือดร้อนแน่นอน ผู้บริหารหน่วยราชการนั้นคงเหงื่อตกและเร่งแก้ปัญหาเฉพาะหน้าเป็นการด่วน แน่นอนว่าระบบสารสนเทศทุกวันนี้เปรียบเสมือนเส้นเลือดของธุรกิจ คงไม่ดีแน่ถ้าไอทีล่มบ่อย หรือข้อมูลหาย จะดีกว่ามั้ยถ้ามีระบบอะไรซักอย่างที่ทำให้แน่ใจได้ว่าระบบข้อมูลสารสนเทศสามารถให้บริการตามปกติ ข้อมูลได้รับการปกป้อง และหากเกิดขัดข้องก็สามารถรับมือและกู้ระบบคืนได้ ระบบที่ว่านี้ก็คือ ISO27001 พระเอกของเราล่ะครับ

ดังนั้นการที่จะมั่นใจได้ว่าระบบสารสนเทศ ของเรามีความมั่นคงปลอดภัย ก็คือเราจะต้องรู้ว่ามีภัยคุกคามอะไรบ้างที่อาจมาโจมตี ทำให้สารสนเทศของเราเกิดความเสียหาย จากนั้นจึงประเมินความเสี่ยงและกำหนดมาตรการจัดการกับภัยคุกคาม ให้แน่ใจว่าสามารถรับมือภัยคุกคามเหล่านั้นได้อย่างเหมาะสม

ISO27001 ทำยากมั้ย? กลัวจะทำไม่สำเร็จ

นี่เป็นคำถามยอดฮิตเลยครับ คำถามที่ว่าทำยากมั้ย ตอบได้เลยว่าไม่ยาก ถ้ามีความรู้และความเข้าใจ 2 เรื่องใหญ่ๆ คือ

1.เข้าใจองค์กรตัวเอง

2.เข้าใจมาตรฐานว่าต้องทำอะไรบ้าง

ISO27001 ทำยากมั้ย? กลัวจะทำไม่สำเร็จ(ต่อ)

1.เข้าใจองค์กรตนเอง :

ต้องสำรวจข้อมูล ซอฟแวร์ ฮาร์ดแวร์ บุคลากร ในขอบเขตที่จัดทำระบบ ข้อมูลนี้ยิ่งมีรายละเอียดยิ่งดี หากหน่วยงานท่านเป็นราชการ บัญชีครุภัณฑ์เป็นจุดเริ่มต้นที่ดีในการรวบรวมข้อมูล Hardware Software

เข้าใจภาระกิจขององค์กร รู้ว่าระบบงานใดสำคัญที่สุดและระบบงานต่างๆ มีข้อจำกัดและจุดอ่อนอะไรบ้าง รู้ไปทำไมหรือครับ? ก็รู้เพื่อที่จะไปหามาตรการมาจัดการกำจัดจุดอ่อนนั้น เช่น ระบบฐานข้อมูลทำงานอยู่บนเครื่อง Server ที่เก่ามาก ในกรณีนี้จุดอ่อนก็คือ Server ดังนั้นท่านก็ต้องหามาตรการมาจัดการความเสี่ยงนี้ โดยจัดหาเครื่องใหม่

ISO27001 ทำยากมั้ย? กลัวจะทำไม่สำเร็จ (ต่อ)

2.เข้าใจมาตรฐาน :

การนำมาตรฐาน ISO27001 มาใช้งาน ก็ต้องทำความเข้าใจในตัวมาตรฐานเสียก่อน ว่าต้องทำอะไรบ้าง ทั้งเรื่องเอกสาร(Documents) และการนำไปใช้งานจริง (Implementation) ตามข้อกำหนดของ ISO27001:2013

ISO27001 : 2013

Information Security Management System (ISMS)

ระบบการจัดการ
ความมั่นคงปลอดภัยของสารสนเทศ

ประกอบด้วยส่วนสำคัญ 4 ประการ

Focus !!

Treatment of Information Security Risks tailored to the needs of the organization

เน้นการบริหารจัดการ
ความเสี่ยงของสารสนเทศ

Applicability

All type ,size and nature of organizations

นำไปใช้ได้กับองค์กร
ทุกขนาดและทุกประเภท

By : www.club27001.com - Information Seurity Blog

ทำความเข้าใจมาตรฐาน ISO27001:2013

และความสำคัญของการประเมินความเสี่ยงของสารสนเทศ

(Information Security Risk Assessment)

ประเมินความเสี่ยงนั้นสำคัญไฉน

"การประเมินความเสี่ยงของสารสนเทศ(Information Security Risk Assessment)" เป็นหัวใจสำคัญของ การทำ ระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO27001 นั่นคือ หากท่านประเมินความเสี่ยงไม่ถูกต้อง หรือไม่ครอบคลุม ก็จะทำให้การจัดการความเสี่ยงที่ตามมานั้นแก้ปัญหาไม่ตรงจุด และไม่ครอบคลุมตามไปด้วย ว่าไปแล้วการประเมินความเสี่ยงก็เหมือนการตรวจร่างกายถ้าตรวจไม่ครบหรือตรวจไม่ละเอียดก็ไม่พบอาการป่วยและไม่ได้รักษา ปล่อยทิ้งไว้จนสุกงอมอาการป่วยก็แสดงออกมาในที่สุด!!

โมเดล CIA ใน ISO27001

Confidential: การปกป้องสารสนเทศให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ ถ้าหากข้อมูลรั่วไหลแสดงว่าขาดคุณสมบัติในข้อนี้

Integrity: ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง เช่น การแฮกระบบเพื่อแก้ไขข้อมูล เป็นต้น

Availability : สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน

ตัวอย่างความเสี่ยง

การกระทำโดยมนุษย์		สิ่งแวดล้อม
ตั้งใจ	อุบัติเหตุ	
1. วางเพลิง, วางระเบิด	1. ไฟฟ้าดับ, น้ำไม่ไหล	1. แผ่นดินไหว
2. สร้างความเสียหายโดยเจตนา	2. เครื่องปรับอากาศเสีย	2. พายุเฮอริเคน
3. โจรกรรม	3. ฮาร์ดแวร์เสีย	3. ฟ้าผ่า
4. ปลอมตัวเป็นผู้ที่ระบุ	4. ข้อผิดพลาดของเจ้าหน้าที่ปฏิบัติงาน	4. น้ำท่วม
5. ซอฟแวร์ที่เป็นอันตราย	5. ข้อผิดพลาดการบำรุงรักษา	5. อุณหภูมิสูงและความชื้น
6. กฎหมายการใช้ซอฟแวร์	6. ความล้มเหลวของซอฟแวร์	6. ฝุ่นละออง
7. เข้าถึงเครือข่ายโดยผู้ที่ไม่ได้รับอนุญาต	7. การใช้ซอฟต์แวร์ผิดกฎหมาย	7. รังสีแม่เหล็กไฟฟ้า
8. ใช้สิ่งอำนวยความสะดวกทางเครือข่ายโดยไม่ได้รับอนุญาต	8. ความล้มเหลวทางเทคนิคของอุปกรณ์เครือข่าย	8. ไฟฟ้าสถิต
9. แทรกซึมการสื่อสาร, ดักฟังการสนทนา	9. การส่งผิดพลาด	9. การเสื่อมสภาพของสื่อจัดเก็บข้อมูล
10. เปลี่ยนเส้นทางของข้อมูล	10. การส่งข้อมูลเกินพิกัด	
	11. ลบไฟล์, ลบข้อมูล	

สร้างความตระหนักด้านความมั่นคงปลอดภัย

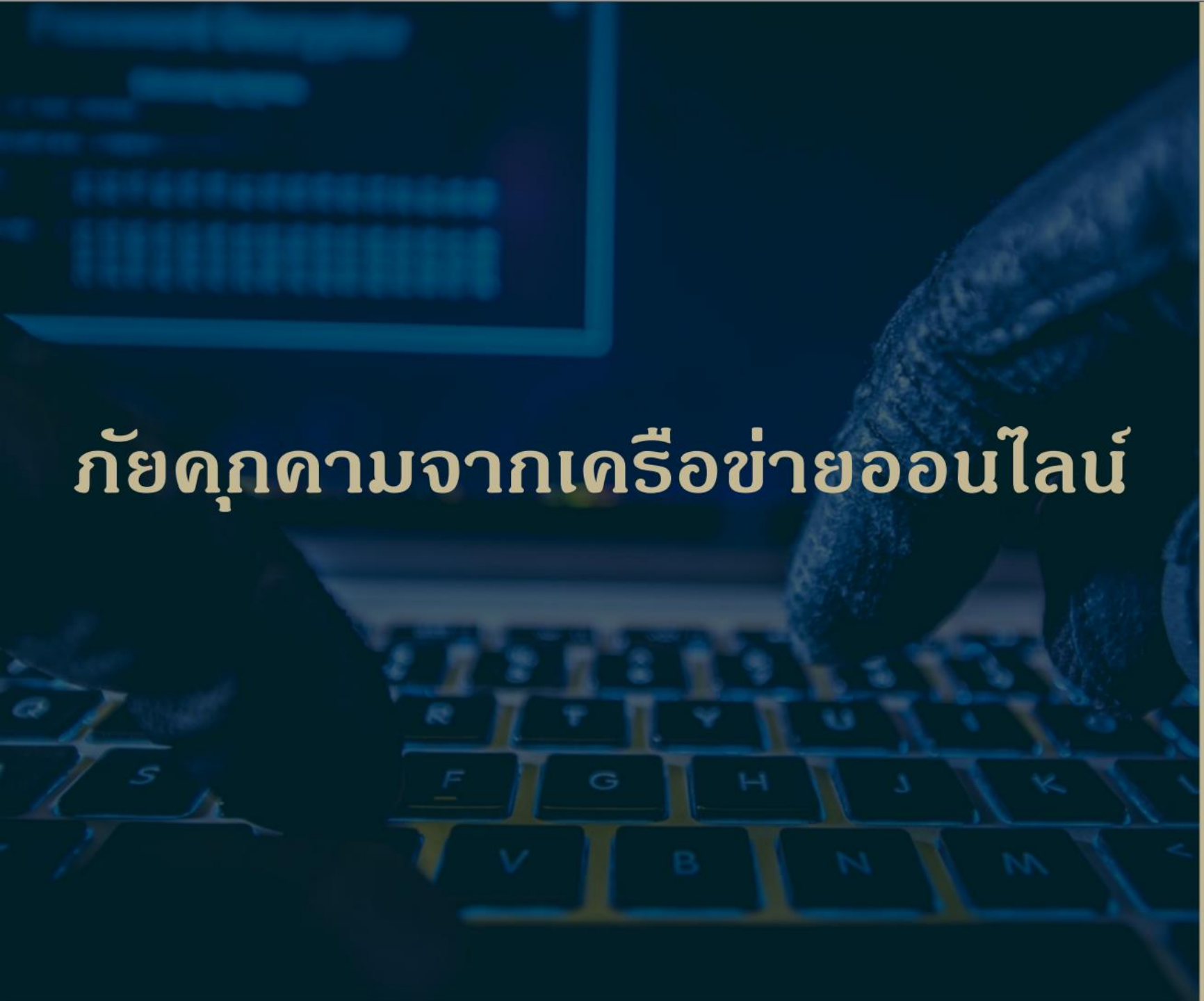
(Security Awareness Training)

ผู้บรรยาย

- นายวีระยุทธ มายุศิริ
- ฝ่ายเทคโนโลยีและสารสนเทศ
- E-Mail : weerayut_mayusiri@hotmail.com
- Facebook : https://www.facebook.com/weerayuth.mayusiri
- @Line : 0869910633

วัตถุประสงค์

- เพื่อสร้างความตระหนักและความเข้าใจถึงภัยคุกคามที่เกิดขึ้นบนระบบเครือข่ายอินเตอร์เน็ตในปัจจุบัน
- เพื่อเรียนรู้แนวทางป้องกันและลดความเสี่ยงจากภัยคุกคามที่เกิดขึ้นบนระบบเครือข่ายอินเตอร์เน็ต
- เพื่อให้ผู้เข้าร่วมอบรมสามารถนำความรู้ที่ได้ไปเผยแพร่ให้ผู้อื่นได้อย่างถูกต้องและมีประสิทธิภาพ



ภัยคุกคามจากเครือข่ายออนไลน์

Scam/Phishing: การล่อลวงทางอินเทอร์เน็ต

- การหลอกลวงทางอินเทอร์เน็ต
- เพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต
- โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ (Chat)
- ตัวอย่างของการฟิชชิ่ง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ
- และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่โดยเว็บไซต์ที่ลิงก์ไปนั้นมักจะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง
- Phishing : PHP + Fishing

Scam/Phishing: การล่อลวงทางอินเทอร์เน็ต

เว็บไซต์หลอกลวง

(ตะขอ)

สแปมเมล์

(เหยื่อล่อปลา)

ID ของผู้ทำธุรกรรมทาง

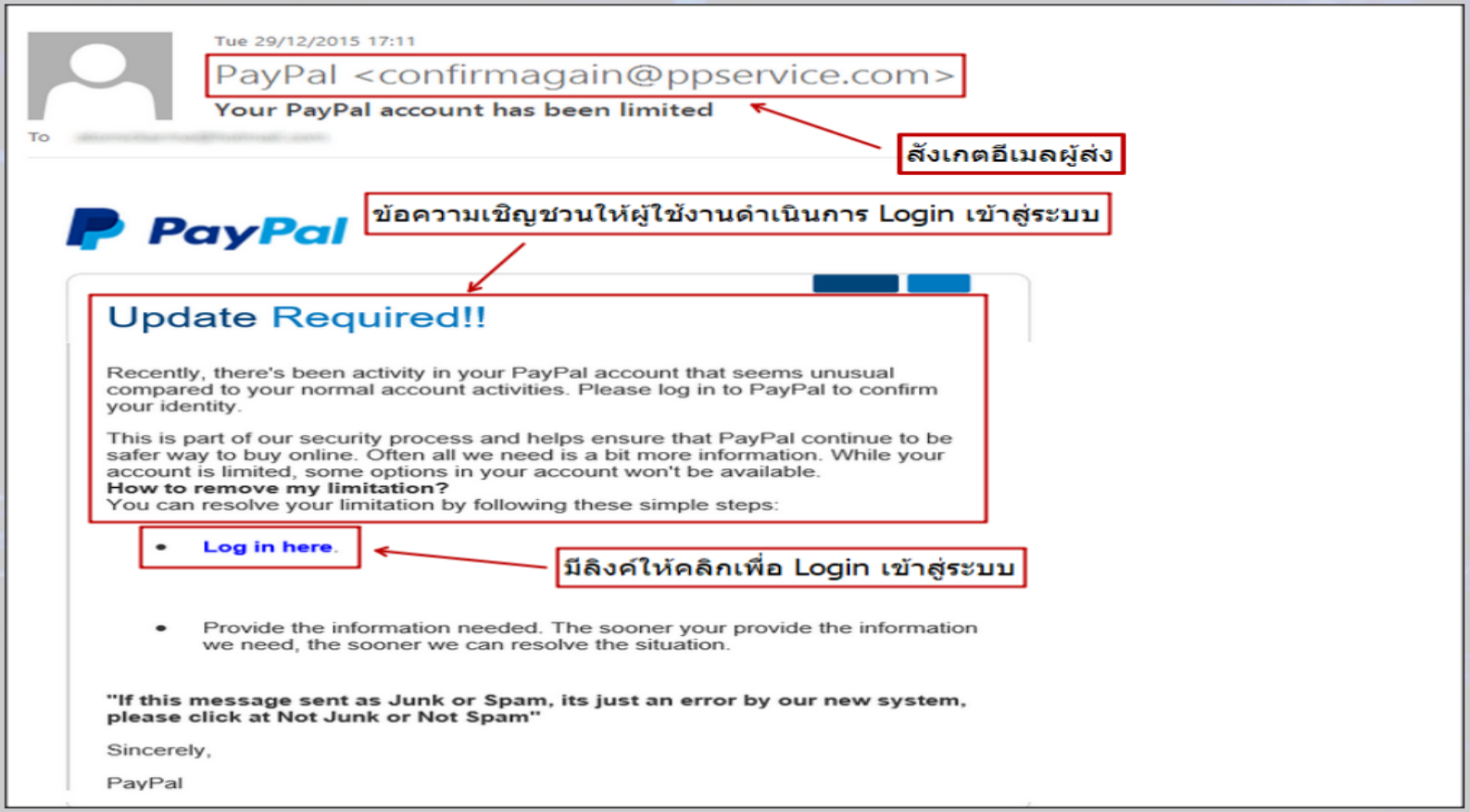
อิเล็กทรอนิกส์

(ปลา)

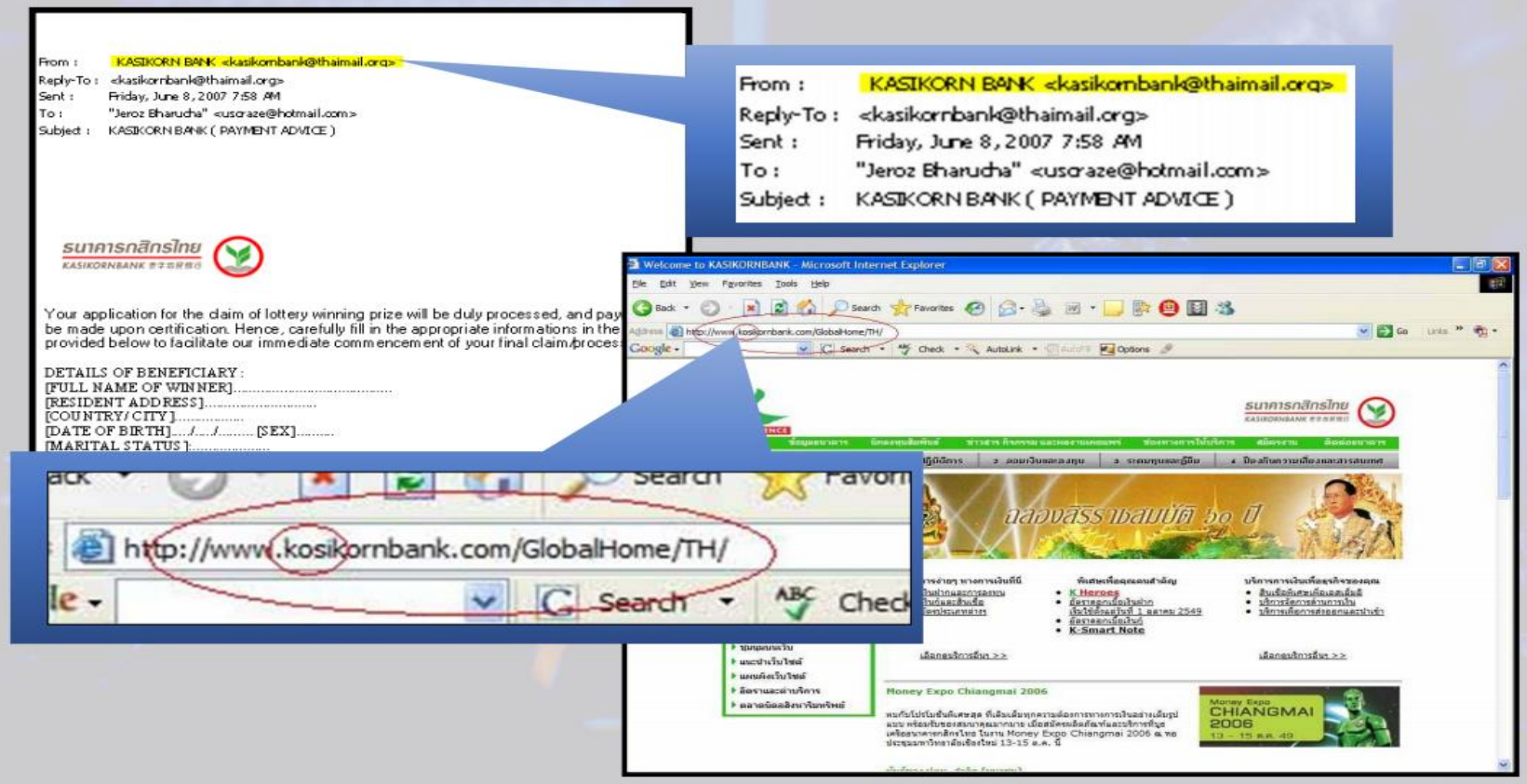
แฮกเกอร์

(ผู้ตกปลา)

ตัวอย่าง Phishing



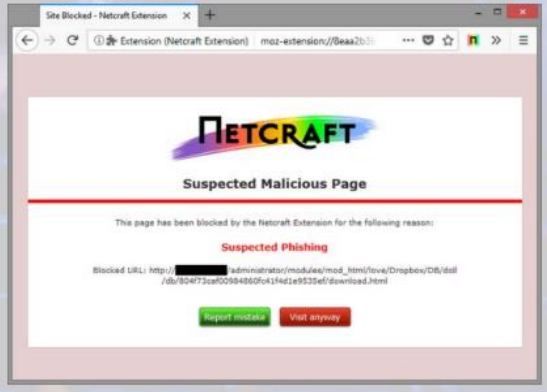
ตัวอย่าง Phishing



ตัวอย่าง Phishing

วิธีแก้ไข / ป้องกัน

- ห้ามคลิกลิงค์ที่ได้รับจากอีเมล์ควรดำเนินกรอกชื่อเว็บไซต์ในช่อง URL บนบราวเซอร์ด้วยตัวท่านเอง
- การเข้าถึงเว็บไซต์ที่มีการ Login เข้าสู่ระบบจะต้องสังเกตสัญญาลักษณ์รูปกุญแจสีเขียว
- ตรวจสอบผ่านเว็บไซต์ www.virustotal.com
- ตรวจสอบโดยใช้ Add on หรือ Extensions บนบราวเซอร์




ภัยคุกคามจาก Malware
[ไม่มีชื่อเรื่อง]
56

เนื้อหา

- รวมฮิต Malware (ซอฟต์แวร์ไม่ประสงค์ดี)
- Ransomware (แรนซัมแวร์) เข้ารหัสข้อมูล เรียกค่าไถ่จากผู้ใช้งาน
- Scareware (สแกร์แวร์) หลอกลวงผู้ใช้งานว่าเป็นผลิตภัณฑ์รักษาความปลอดภัย มีการแจ้งเตือนผู้ใช้ว่า มีการติดเชื้อเกิดขึ้น และให้ดาวน์โหลดโปรแกรมป้องกันไวรัส(ปลอม)มาติดตั้งที่เครื่อง
- Spyware (สปายแวร์) ละเมิดความเป็นส่วนตัวของผู้ใช้
- Trojan (โทรจัน) หลอกว่าเป็นโปรแกรมปกติทั่วไป เมื่อหลงติดตั้งจะขโมยข้อมูลและเปิดให้ผู้ไม่ประสงค์ดีเข้ามาควบคุมเครื่อง

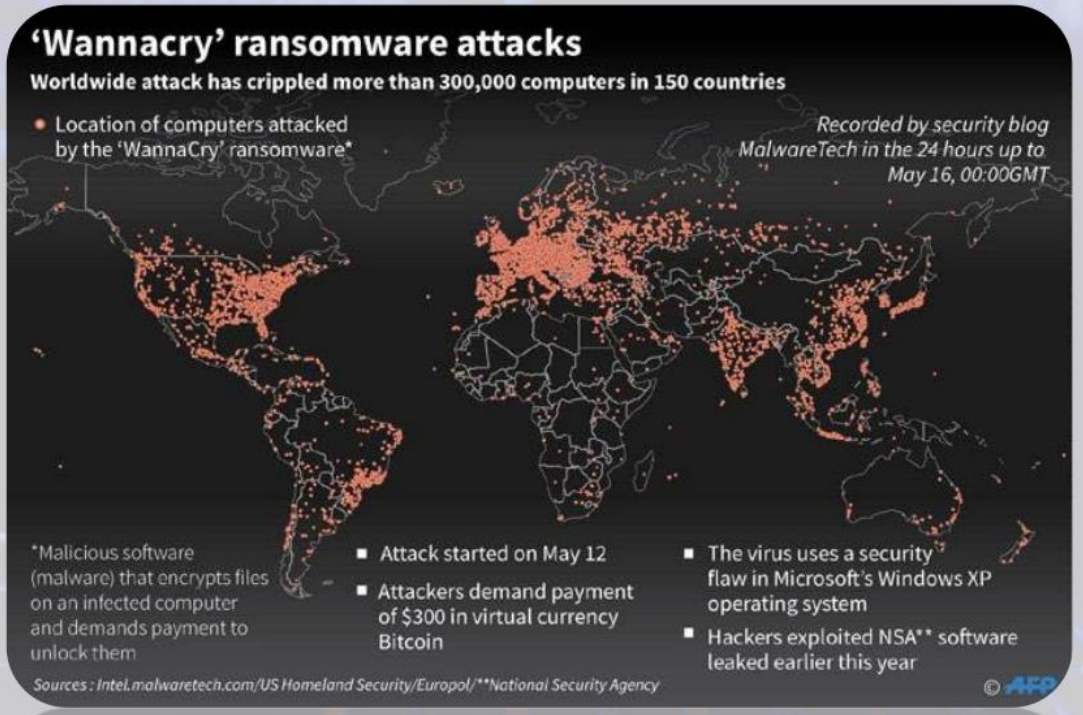
Malware (ซอฟต์แวร์ไม่ประสงค์ดี)

- ย่อมาจากคำว่า Malicious Software ซึ่งหมายถึงโปรแกรมประสงค์ร้ายต่าง ๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล มัลแวร์ แบ่งออกได้หลากหลายประเภท อาทิเช่น ไวรัส (Virus) เวิร์ม (Worm) หรือหนอนอินเทอร์เน็ต ม้าโทรจัน (Trojan Horse) การแอบดักจับข้อมูล (Spyware) คีย์ ล็อกเกอร์ (Key Logger)

WannaCry

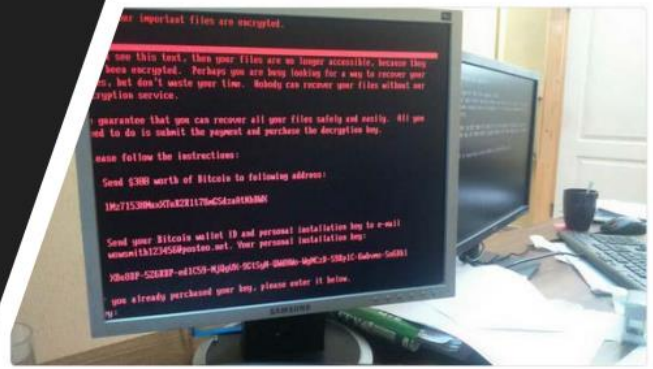

Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

WannaCry


'Wannacry' ransomware attacks
Worldwide attack has crippled more than 300,000 computers in 150 countries
Location of computers attacked by the 'WannaCry' ransomware*
Recorded by security blog MalwareTech in the 24 hours up to May 16, 00:00GMT
*Malicious software (malware) that encrypts files on an infected computer and demands payment to unlock them
Attack started on May 12
Attackers demand payment of $300 in virtual currency Bitcoin
The virus uses a security flaw in Microsoft's Windows XP operating system
Hackers exploited NSA** software leaked earlier this year
Sources : Intel.malwaretech.com/US Homeland Security/Europol/**National Security Agency
© AFP

Petwarp or Petya or NotPetya

- Petya is a family of encrypting ransomware that was first discovered in 2016. The malware targets Microsoft Windows-based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin in order to regain access to the system.



วิธีแก้ไข / ป้องกัน

- https://noransom.kaspersky.com/

วิธีแก้ไข / ป้องกัน

- ***ส่วนใหญ่แก้ไม่ได้ 100%***
- Ransomware แต่ละตัวแก้ไขไม่เหมือนกัน
- จ่ายเงินค่าไถ่ใช่ว่าจะได้ข้อมูลเสมอไป
- ลง Antivirus ที่สำคัญต้อง update
- ไม่เปิดไฟล์มั่ว
- ไม่คลิกลิงค์มั่ว
- สำรองข้อมูลสำคัญไว้ ปลอดภัยที่สุด
- อัพเดตระบบปฏิบัติการที่ใช้งานอย่างสม่ำเสมอ

ซอฟต์แวร์สอดแนม (Spyware)

- เพื่อสังเกตการณ์หรือดักจับข้อมูล หรือควบคุมเครื่องคอมพิวเตอร์
- ผู้ใช้ไม่รับทราบว่าได้ติดตั้งเอาไว้
- มักแพร่กระจายผ่านเว็บไซต์ อีเมล์ USB-Drive
- ข้อมูลที่มักจะถูกดักจับ
  - ข้อมูลบัตรเครดิต
  - รหัสผ่าน
  - อีเมล์

ม้าโทรจัน (Trojan Horse)

- ไม่ทำสำเนาตัวเอง
- เจตนาทำสิ่งที่คาดไม่ถึง
  - ลบไฟล์
  - เปิดประตูลับ หรือ Back Door
  - ขโมยข้อมูลสำคัญ เช่น รหัสผ่าน เลขที่บัตรเครดิต เป็นต้น
  - ทำการเชื่อมต่อสู่ภายนอก

โปรแกรมเปิดไฟล์ PDF ที่ยังไม่ได้รับการแพทช์

- เป็นรูปแบบไฟล์ที่มีความเสี่ยงที่สุด เนื่องจากช่องโหว่ต่าง ๆ ของ Adobe Acrobat และ Reader ได้กลายเป็นส่วนหนึ่งของชุดเครื่องมือในการใช้หาประโยชน์ในทางที่ผิด ๆ เช่น การเข้าควบคุมระบบและทำตามอย่างที่แฮกเกอร์ต้องการ


ภัยคุกคามและความเสี่ยงต่อ
การใช้งาน Mobile Device
76

ภัยคุกคามบนมือถือสมาร์ทโฟนที่เกิดขึ้นในประเทศไทย

เว็บไซต์ข่าวในไทย ถูกฝังโทรจัน ปล่อยโค้ดหลอกโหลดแอพป้องกันไวรัสปลอม ในธนาคารออนไลน์

SMS ดาวน์โหลดโปรแกรม AVG AntiVirus Mobile Pro สำหรับติดตั้งใน Android โดยโปรแกรมดังกล่าวเป็นโปรแกรมแอนตี้ไวรัสปลอม จุดประสงค์เพื่อขโมย SMS OTP จากธนาคาร

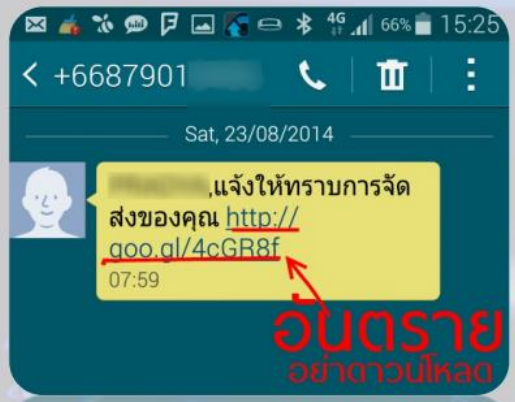
ภัยคุกคามบนมือถือสมาร์ทโฟนที่เกิดขึ้นในประเทศไทย

โทรจันตัวนี้จะเข้าไปแก้ไขข้อมูลที่แสดงผลอยู่ในเบราว์เซอร์ ไม่ใช่การสร้างเว็บไซต์ปลอม ทำให้การเชื่อมต่อแบบ HTTPS และข้อมูลใบรับรองดิจิทัล (Digital Certificate) ที่แสดงอยู่ในเว็บไซต์ เป็นใบรับรองฯ จริงของธนาคาร

[ไม่มีชื่อเรื่อง]

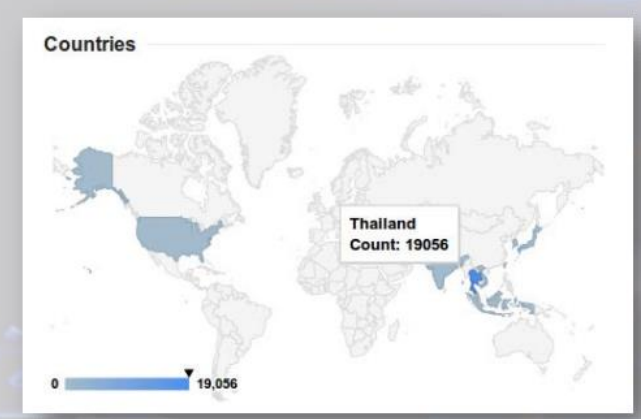
ภัยคุกคามบนมือถือสมาร์ทโฟนที่เกิดขึ้นในประเทศไทย

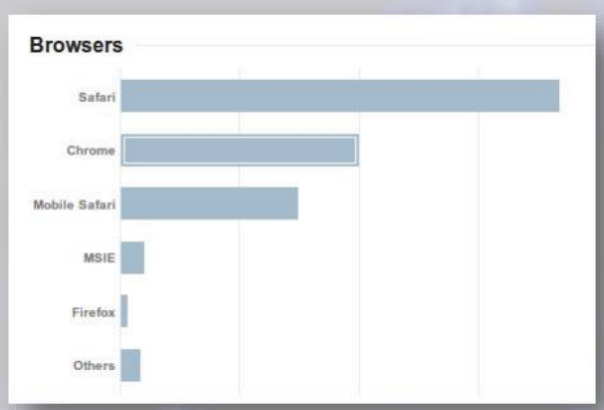
ภัยคุกคามบนมือถือสมาร์ทโฟนที่เกิดขึ้นในประเทศไทย

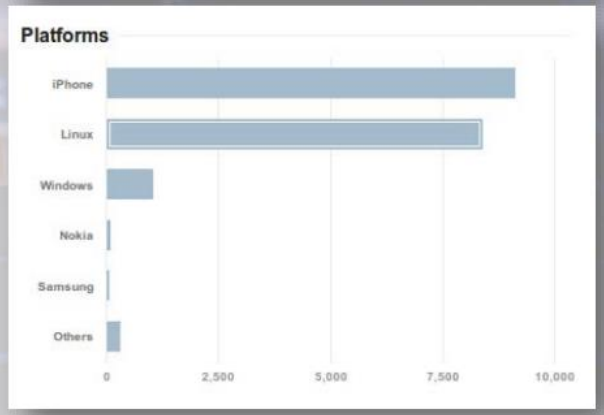


ภัยคุกคามบนมือถือสมาร์ทโฟนที่เกิดขึ้นในประเทศไทย

สถิติการคลิกลิงก์ที่เผยแพร่มัลแวร์







https://www.thaicert.or.th/alerts/user/2014/al2014us017.html

ภัยคุกคามบนมือถือสมาร์ทโฟนที่เกิดขึ้นในประเทศไทย

อีเมลหลอกลวง (Phishing)

From: Bank of Ayudhya [mailto:updatebofa@optusnet.com.au] ①

To: undisclosed-recipients:

Subject: Bank of Ayudhya :- Account Verification Process ②

ธนาคารกรุงศรีอยุธยา
BANK OF AYUDHYA

Dear Customer,
As part of our commitment to satisfy our customers, we always update annually. To ensure you are always protected, we are introducing a new programmed on security called BankSecure-cfx-08 and you'll see a number of initiatives that will be put in place to enhance your Bank of Ayudhya experience.

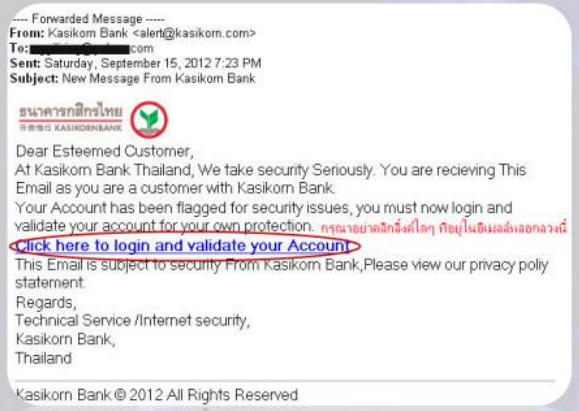
Due to this, you are requested to follow the provided steps and confirm your Krungsri Online details for the safety of your accounts.

To initiate the verification process: Kindly Sign In below. ③
https://www.krungsrionline.com/cgi-bin/bvisapi.dll/krungsri_ib/login/login.jsp

เมื่อคลิกแล้ว จะเข้าสู่หน้าเว็บหลอกลวง เช่น
http://acc.stcosme.free.fr/components/com_expose/expose/img/thumbs/login.eng.html

Sincerely,

Copyright 2001 Bank of Ayudhya PCL. All right reserved

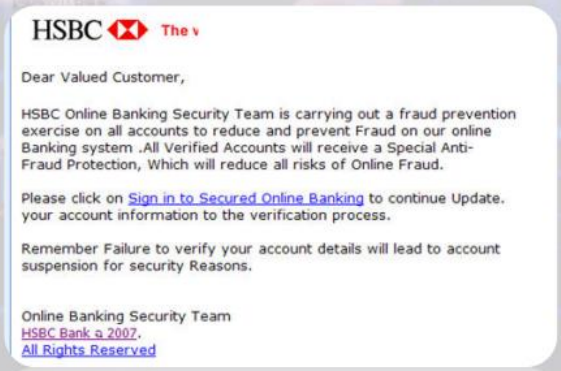


---- Forwarded Message -----
From: Kasikorn Bank <alert@kasikorn.com>
To: [redacted]com
Sent: Saturday, September 15, 2012 7:23 PM
Subject: New Message From Kasikorn Bank

ธนาคารกสิกรไทย KASIKORNBANK

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. กรุณาอย่าคลิกลิ้งค์ใดๆ ที่อยู่ในอีเมลล์หลอกลวงนี้
Click here to login and validate your Account
This Email is subject to security From Kasikorn Bank,Please view our privacy poliy statement.
Regards,
Technical Service /Internet security,
Kasikorn Bank,
Thailand

Kasikorn Bank © 2012 All Rights Reserved



HSBC The v

Dear Valued Customer,

HSBC Online Banking Security Team is carrying out a fraud prevention exercise on all accounts to reduce and prevent Fraud on our online Banking system .All Verified Accounts will receive a Special Anti-Fraud Protection, Which will reduce all risks of Online Fraud.

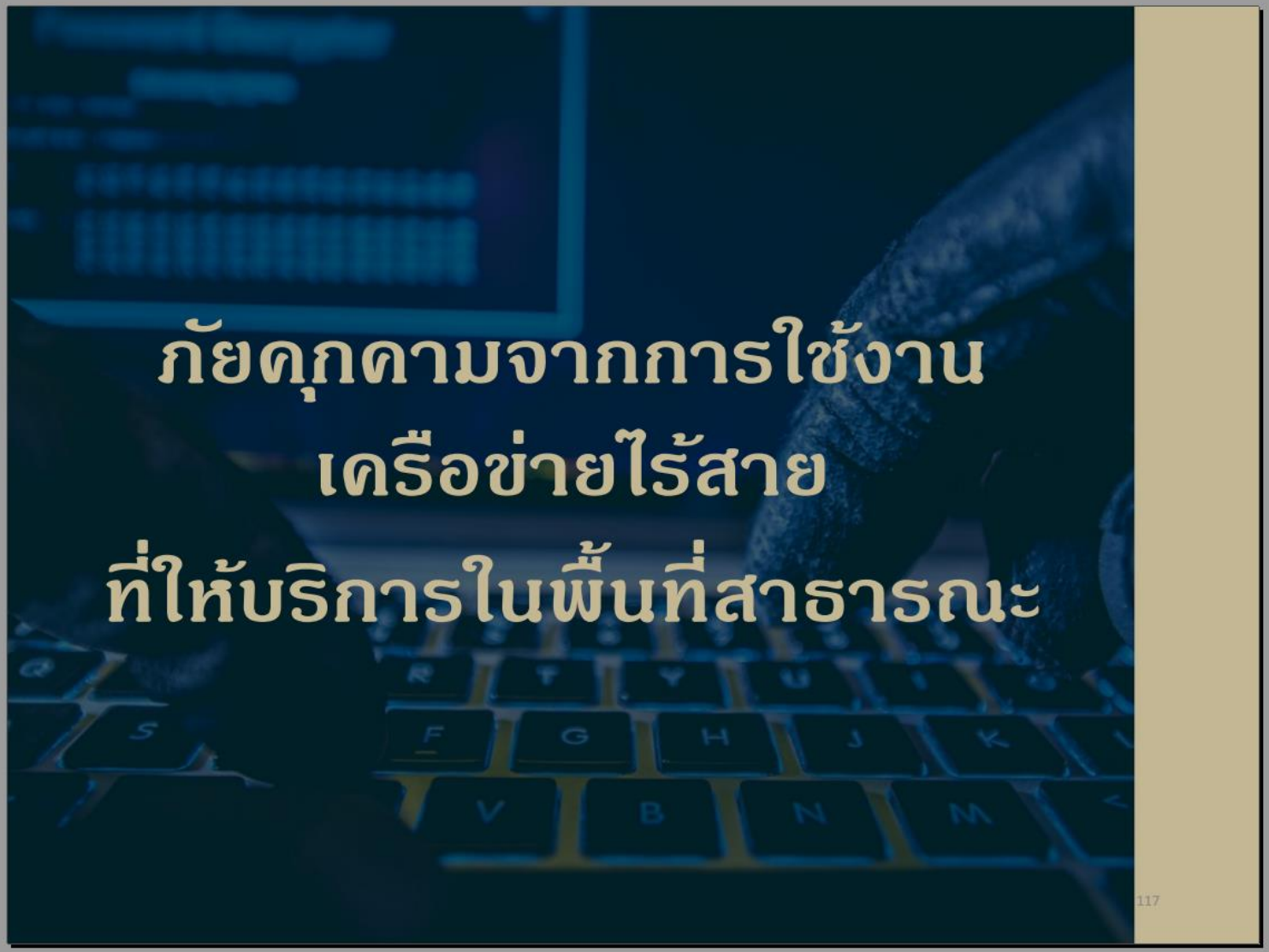
Please click on Sign in to Secured Online Banking to continue Update. your account information to the verification process.

Remember Failure to verify your account details will lead to account suspension for security Reasons.

Online Banking Security Team
HSBC Bank a 2007.
All Rights Reserved

วิธีแก้ไข / ป้องกัน บนมือถือสมาร์ทโฟน

- ดำเนินการอัพเดตแอปพลิเคชันอย่างสม่ำเสมอ
- ไม่ Jailbreak หรือ root เครื่อง
- ดำเนินการติดตั้ง Antivirus บนอุปกรณ์
- ไม่ติดตั้งโปรแกรมจากแหล่งอื่นที่ไม่ใช่ Google Play, App Store
- ดำเนินการตรวจสอบความเหมาะสม และน่าเชื่อถือของแอพก่อนติดตั้ง
- ห้ามคลิกลิงค์ที่ได้รับจากอีเมล์ควรดำเนินกรอกชื่อเว็บไซต์ในช่อง URL บนบราวเซอร์ด้วยตัวท่านเอง
- การเข้าถึงเว็บไซต์ที่มีการ Login เข้าสู่ระบบจะต้องสังเกตสัญญาลักษณ์รูปกุญแจสีเขียว
- ตรวจสอบผ่านเว็บไซต์ www.virustotal.com

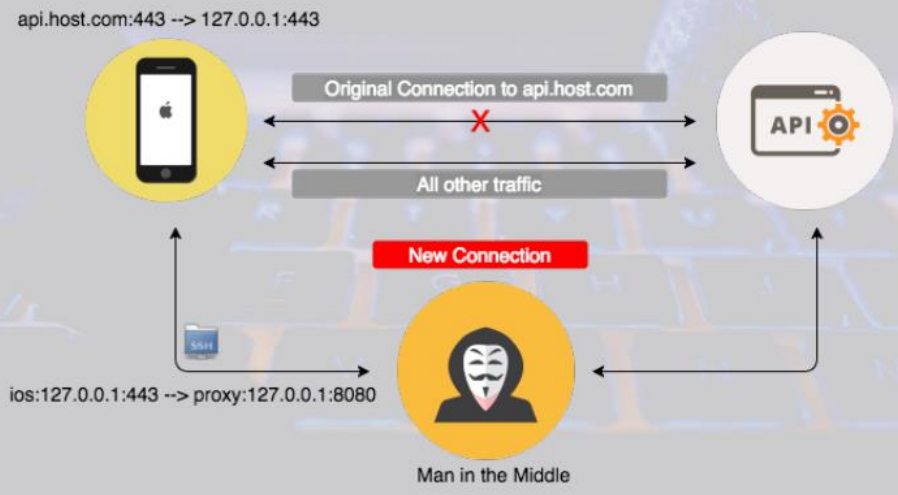

ภัยคุกคามจากการใช้งาน
เครือข่ายไร้สาย
ที่ให้บริการในพื้นที่สาธารณะ
117

คุณคิดว่า https ปลอดภัยหรือไม่ ?

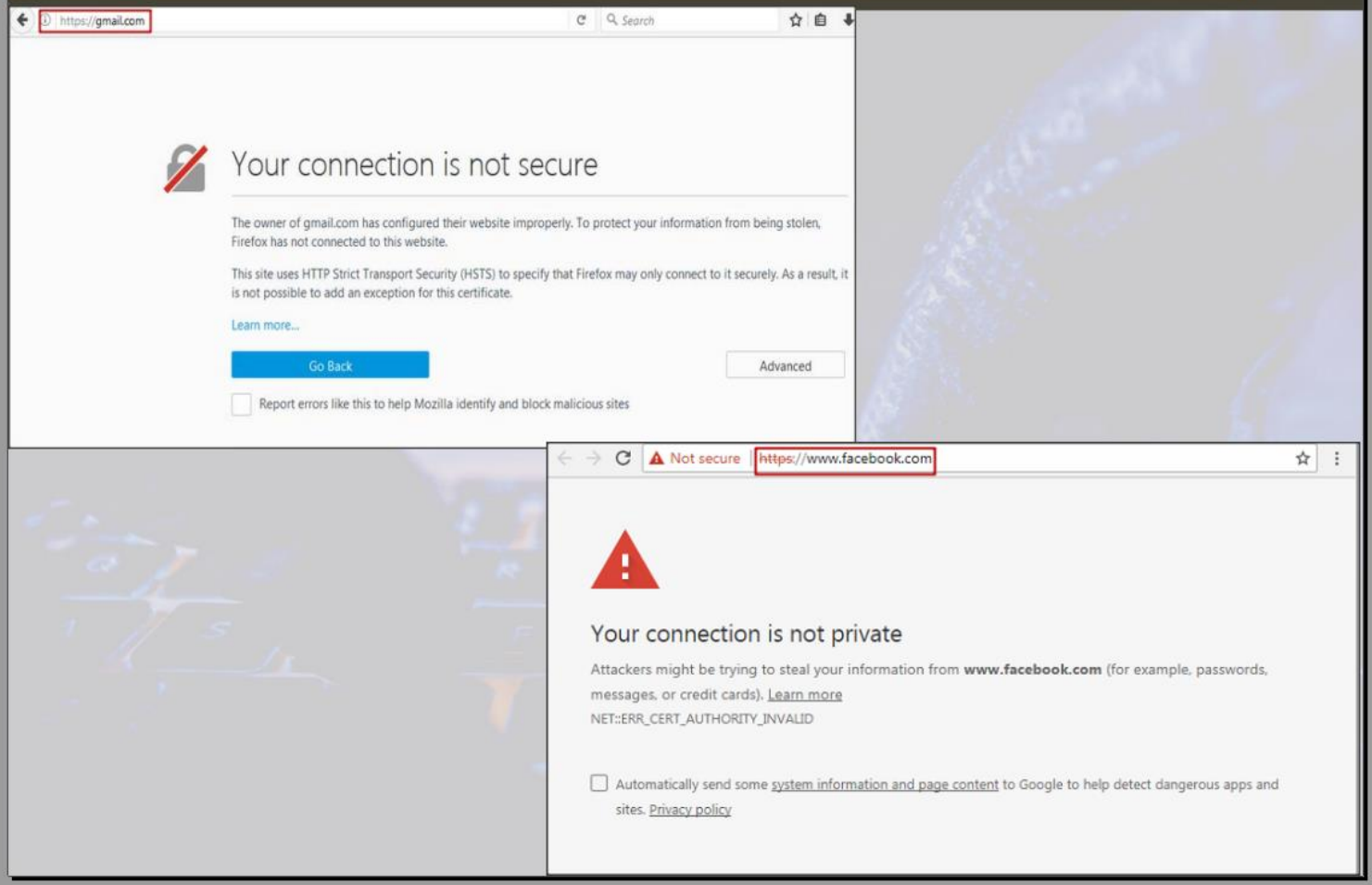
อย่าเพิ่งคิดว่าปลอดภัยเพราะอาจไม่เป็นเช่นนั้น

ภัยคุกคาม และความเสี่ยงต่อการใช้งาน Mobile Device

- Man-in-the-middle attack
  - SSL Strip
  - ARP Spoof
  - Spoof DNS
  - Facebook Phishing



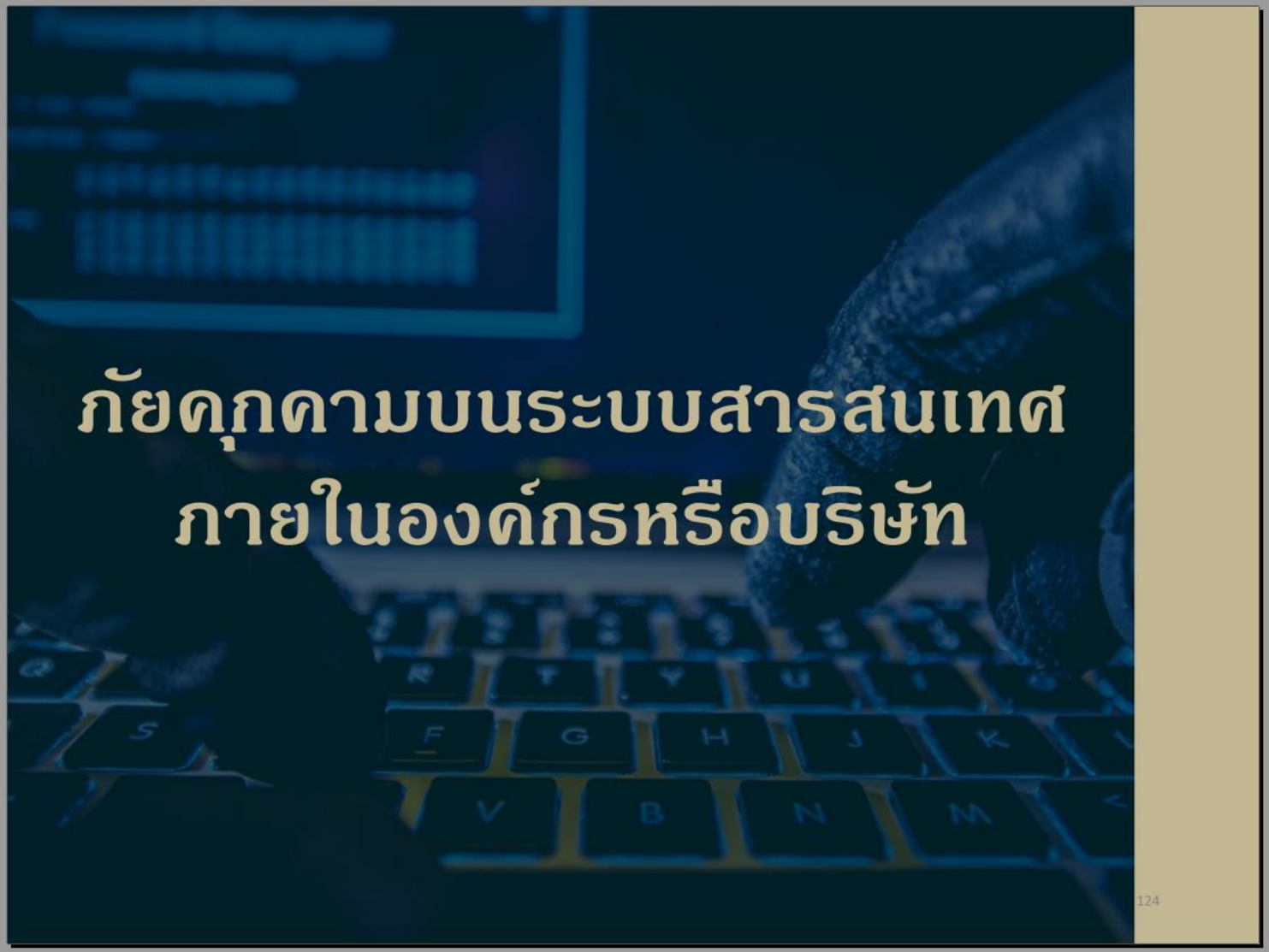
ภัยคุกคาม และความเสี่ยงต่อการใช้งาน Mobile Device



วิธีแก้ไข / ป้องกัน

- ไม่ใช้งาน Wi-Fi สาธารณะในการทำธุรกรรมทางการเงินและเข้าสู่ระบบงานสำคัญภายในองค์กร
- สังเกตหน้า Error ของเว็บบราวเซอร์ในการแจ้งเตือนต่าง ๆ
- การเข้าถึงเว็บไซต์ที่มีการ Login เข้าสู่ระบบจะต้องสังเกตสัญญาลักษณ์รูปกุญแจสีเขียว

- ตรวจสอบผ่านเว็บไซต์ www.virustotal.com
- ตรวจสอบโดยใช้ Add on หรือ Extensions บนบราวเซอร์ “HTTPS Everywhere”


ภัยคุกคามบนระบบสารสนเทศ
ภายในองค์กรหรือบริษัท
124

เนื้อหา

- การตั้งรหัสผ่านให้ปลอดภัย
- โปรแกรมไม่ประสงค์ดี ซึ่งจะเน้นในเรื่องของการปรับปรุงฐานข้อมูลรูปแบบไวรัส
- การตรวจสอบว่าฐานข้อมูลรูปแบบไวรัสมีการอัพเดตหรือไม่การแพร่กระจายของไวรัสผ่านทาง Thumb Drive การป้องกัน Spyware
- การตั้งค่า Windows Update
- การเปิดใช้งาน Personal Firewall
- การตั้ง Screen saver แบบมีรหัสผ่าน
- การรับส่งอีเมลให้ปลอดภัย

การตั้งรหัสผ่านให้ปลอดภัย

- ความยาวรหัสผ่าน 8-16 ตัวอักษร
- ประกอบด้วยตัวอักษร ตัวเลข และอักษระพิเศษ
- ไม่ใช้คำที่มีในพจนานุกรม (Dictionary)
- ควรมีการเปลี่ยนรหัสผ่านตามระยะเวลา
  เช่น 6 เดือนหรือ 1 ปี
- ไม่ใช้งานรหัสผ่านที่เหมือนกันในทุก ๆบริการ
- แยกรหัสผ่านสำหรับระบบงาน(ที่ทำงาน)
  กับระบบที่ใช้งานส่วนตัว

การตั้งรหัสผ่านให้ปลอดภัย

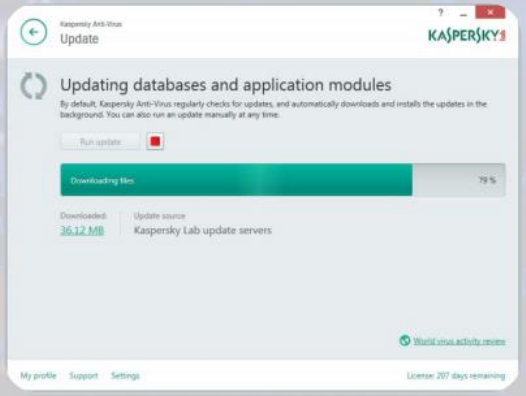
- เทคนิค การกำหนดรหัสผ่านให้จำง่ายเช่น
  - ให้กำหนดเป็นภาษาไทย แต่พิมพ์เป็นภาษาอังกฤษ เช่น
    - คุณทำได้ : 86Imewfh
    - ทำไมเสียบ่อยจัง : mew,glup[jvp0y'
  - ตั้งให้สื่อความหมายเกี่ยวกับระบบที่ใช้
    - งานบัญชีปวดหัว : 'ko[yP=ux;fsy;

การตั้งรหัสผ่านให้ปลอดภัย

- คำที่มักเขียนผิดเฉพาะส่วนตัว
  - ไปไห้วพระ : ไปไห้วพะ : wx>sh;rt
- ผสมคำไทยและอังกฤษ
  - ระบบ@error : it[[@error
- ใช้การแทนที่หรือตัวย่อสื่อความหมาย
  - เงินเดือนเป็นศูนย์: $เดือนเป็น0 : $gfnvogxHo0
  - โอ้แอ็ดมินคนดี : o@มินคนD : o@,bo8oD

การป้องกันไวรัสบนเครื่องคอมพิวเตอร์

- ผู้ใช้งานต้อง : ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัสว่ายังทำงานตามปกติหรือไม่ และมีการปรับปรุงฐานข้อมูลไวรัสอย่างสม่ำเสมอหรือไม่ โดยให้ทำการตรวจสอบอย่างน้อยวันละ 1 ครั้ง หากพบว่าทำงานผิดปกติ ให้รีบแจ้งผู้ดูแลระบบที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยทันที

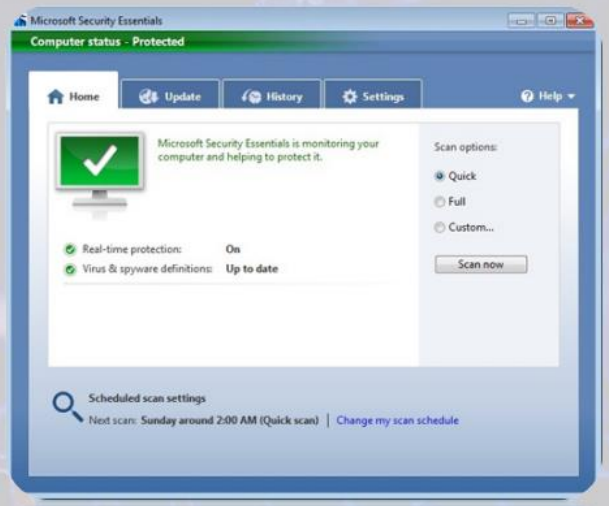


การป้องกัน Spyware

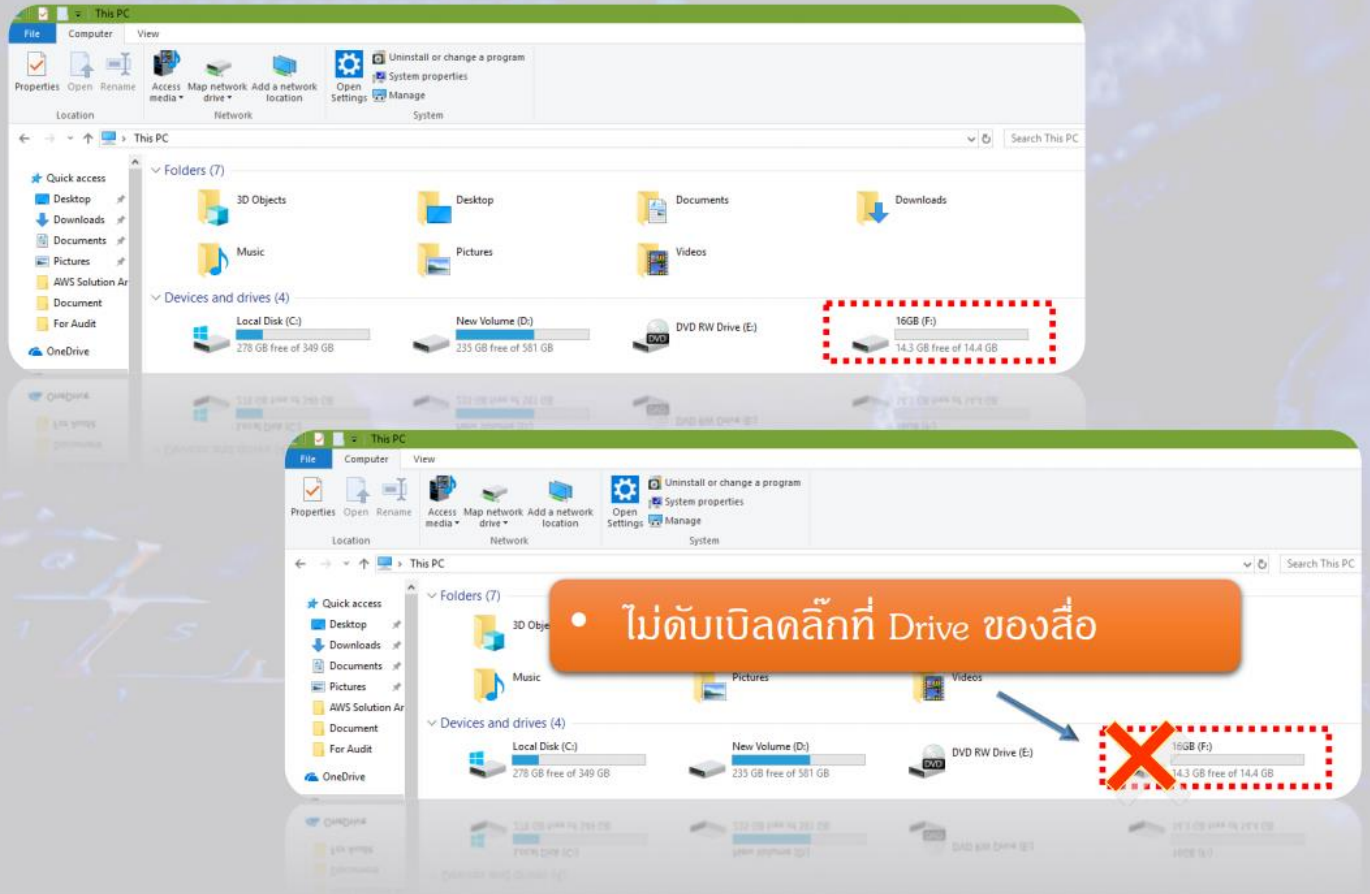
- เวลาที่ผู้ใช้พบหน้าจอในลักษณะนี้ให้คลิกที่กากบาท X ขวาบน เพื่อปิดหน้าต่าง
- ป๊อบอัพนั้น
- อย่าคลิก “yes”หรือ“accept”หรือ“download” เพราะนั่นเท่ากับเป็นการอนุญาตให้ดาวน์โหลดโปรแกรมเหล่านั้นได้
- เพระฉะนั้น “อย่าหลงกล”

การป้องกัน Spyware

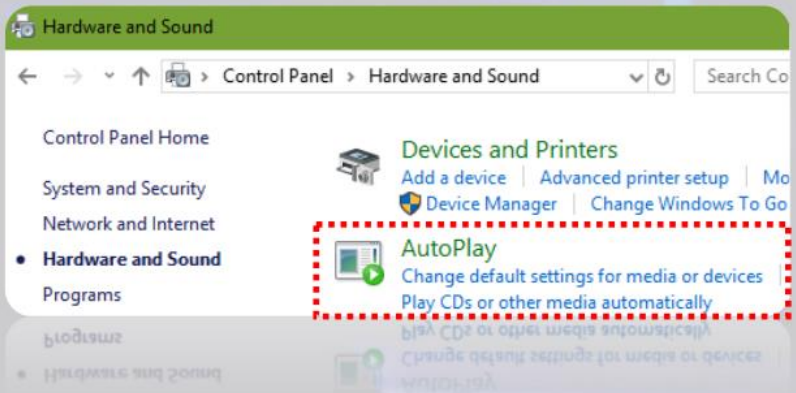
- ใช้ซอฟต์แวร์แอนติสปายแวร์ ซึ่งเป็นเสมือนกำแพงอีกด่านหนึ่งที่ช่วยป้องกันซอฟต์แวร์ที่ไม่รู้จักติดตามคุณเข้ามาขโมยข้อมูลส่วนบุคคลจากเครื่องของคุณระหว่างที่ใช้งานออนไลน์



การป้องกันไวรัสจาก Thumb Drive

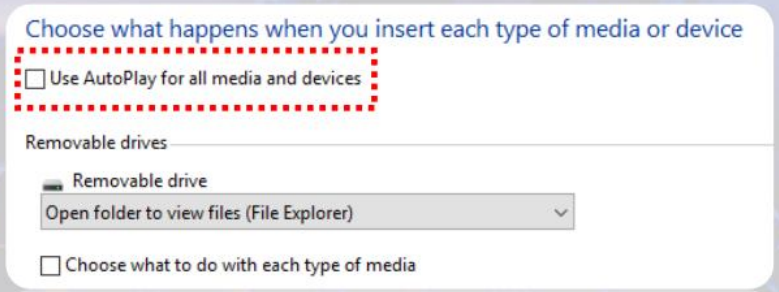


การป้องกันไวรัสจาก Thumb Drive

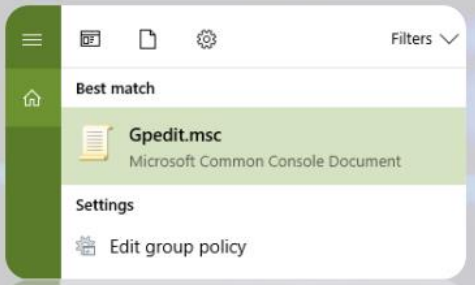


- การปิดการทำงานของ Autoplay ที่มีมาใน Control Panel

- เอาเครื่องหมายถูกออกหน้าหัวข้อ Use AutoPlay for all media and devices แล้วคลิก Save

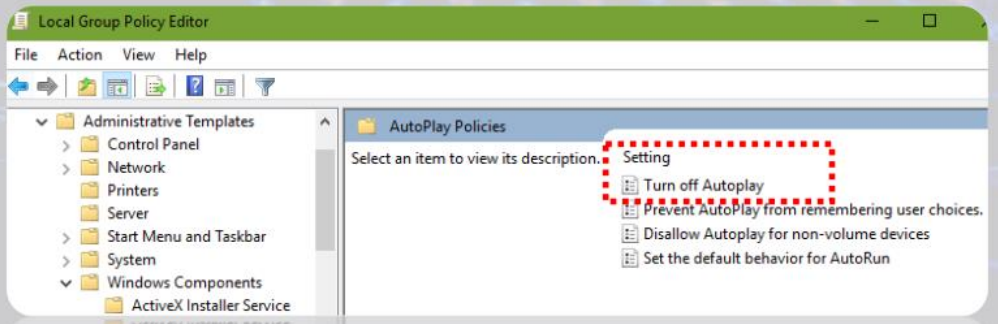


การป้องกันไวรัสจาก Thumb Drive



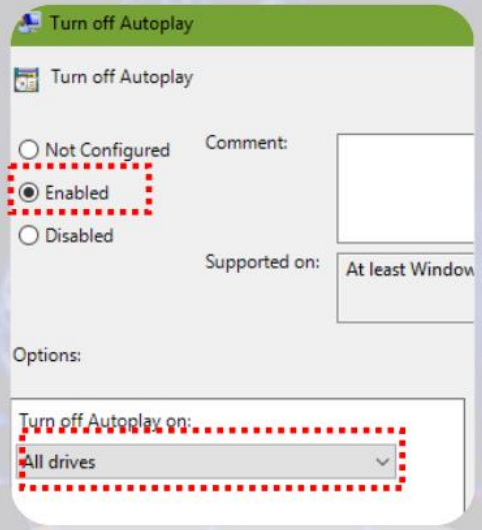
- คลิก Start -> ที่ช่อง Search box พิมพ์คำสั่ง Gpedit.msc -> Enter

- ดับเบิ้ลคลิกหัวข้อ Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies
- ที่พาเนลทางด้านขวา ดับเบิ้ลคลิกหัวข้อ Turn off Autoplay



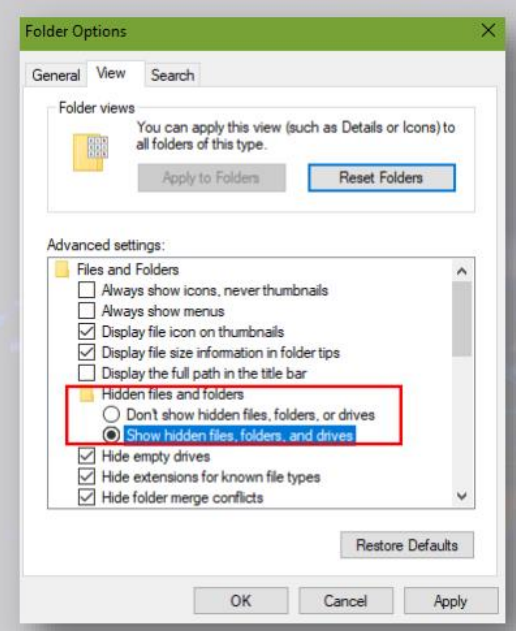
การป้องกันไวรัสจาก Thumb Drive

- ที่หน้าต่างกำหนดคุณสมบัติให้เลือกเป็น Enabled
- และที่หัวข้อ Turn off Autoplay on: ให้เลือก
- All drives หรือ
- CD-Rom and removable media drives
- แล้วคลิก Apply -> OK



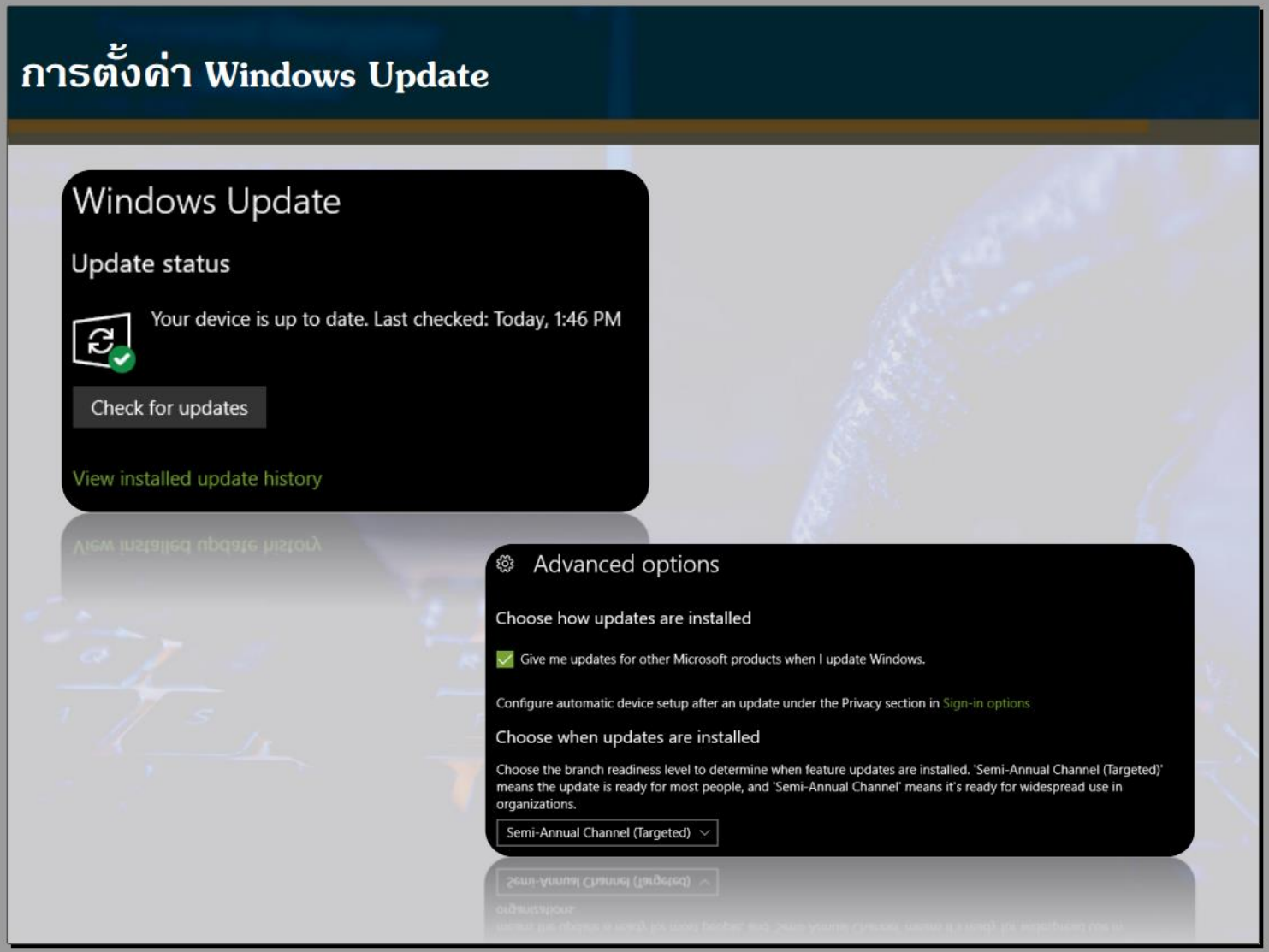
การป้องกันไวรัสจาก Thumb Drive

- การโชว์ไฟล์ที่ถูกซ่อน (HIDDEN FILE)
- เลือกที่ This PC -> View -> Option -> View

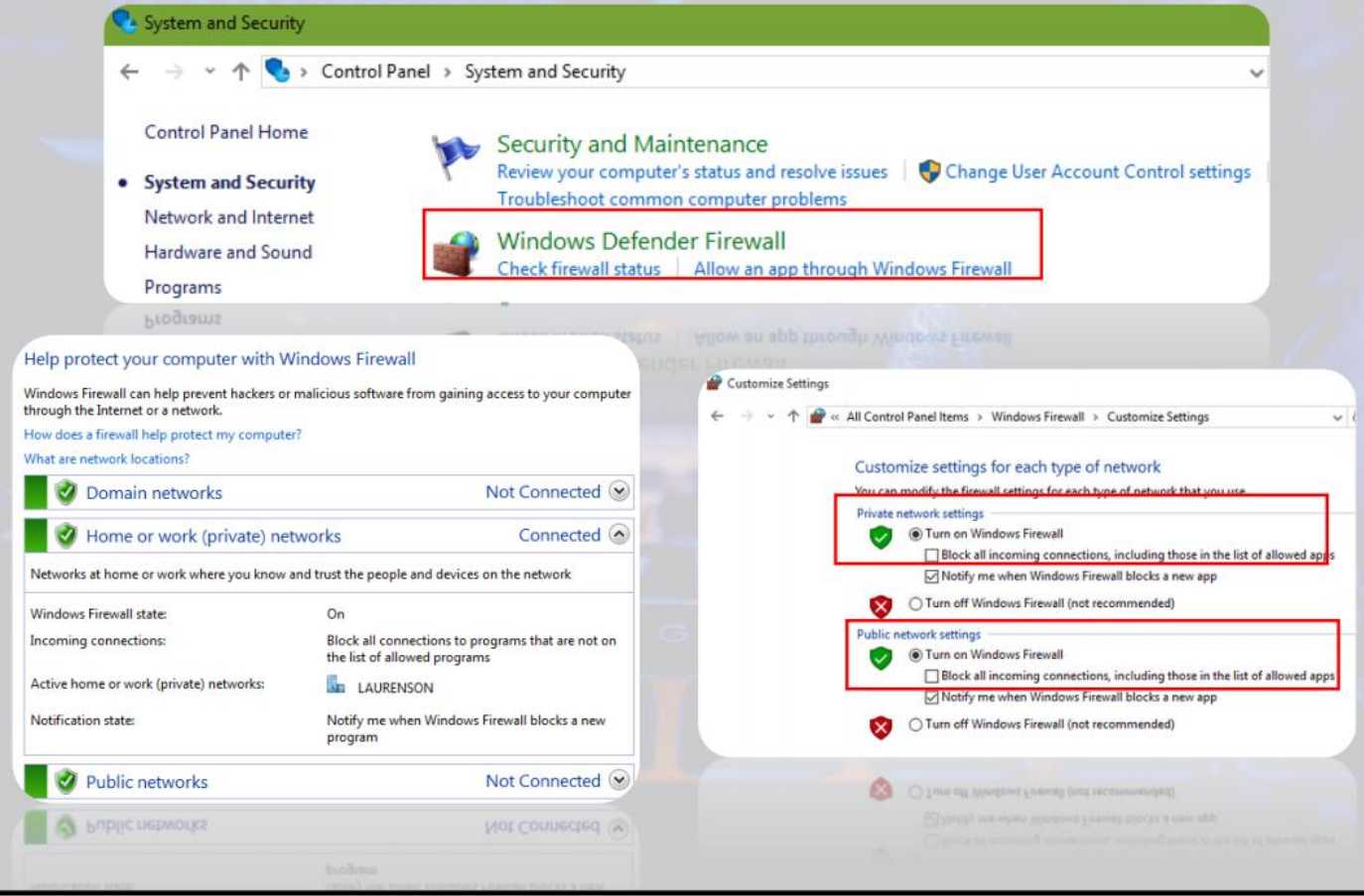


- เลือกที่แถบ View
- แล้วคลิกที่ Show Hidden file,folders, And drivers
- แล้วติกที่ Hide protected operating system file

การตั้งค่า Windows Update



การเปิดใช้งาน Personal Firewall




ภัยคุกคามที่เกิดขึ้นใน
ชีวิตประจำวัน

การดักดูข้อมูลบัตร ATM (ไทย)

- ติดตั้ง Key Board ส่วนบุคคล

การดักดูข้อมูลบัตร ATM (ไทย)

- ถอดประกอบได้

การดักดูข้อมูลบัตร ATM (ไทย)

- ตู้ ATM ไม่ปรกติ

วิธีแก้ไข / ป้องกัน

- สังเกตความผิดปกติต่าง ๆ รอบ ๆ เครื่อง ATM
- การกดเงินสดที่ตู้ ATM ทุกครั้งต้องปกปิดรหัสผ่าน
- สมัครบริการ SMS Alert
- ทำการจำกัดวงเงิน
- ใช้บัตร ATM EMV ชิป
- แจ้งธนาคารทันที่เมื่อพบสิ่งผิดปกติ

Q & A