



ISO 27001:2013

ระบบการจัดการความปลอดภัยของข้อมูล

ISO27001:2013 มาตรฐานสากล

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

ทำไมถึงต้องทำ ISO27001:2013

ลองนึกภาพคุณสมบัติท่านไปใช้บริการหน่วยงานราชการแห่งหนึ่ง ปรากฏว่าระบบไอทีล่มให้บริการไม่ได้ เจอแบบนี้ประชาชนผู้ใช้บริการเดือดร้อนแน่นอน ผู้บริหารหน่วยราชการนั้นคงเหงื่อตกและเร่งแก้ปัญหาเฉพาะหน้าเป็นการด่วน แน่แน่นอนว่าระบบสารสนเทศทุกวันนี้เปรียบเสมือนเส้นเลือดของธุรกิจ คงไม่ดีแน่ถ้าไอทีล่มบ่อย หรือข้อมูลหาย จะดีกว่ามั้ยถ้ามีระบบอะไรซักอย่างที่ทำให้แน่ใจได้ว่าระบบข้อมูลสารสนเทศสามารถให้บริการตามปกติ ข้อมูลได้รับการปกป้อง และหากเกิดขัดข้องก็สามารถรับมือและกู้ระบบคืนได้ ระบบที่ว่านี้ก็คือ ISO27001 พระเอกของเราละครับ

ดังนั้นการที่จะมั่นใจได้ว่าระบบสารสนเทศ ของเรามีความมั่นคงปลอดภัย ก็คือเราจะต้องรู้ว่ามียักษ์คุกคามอะไรบ้างที่อาจมาโจมตี ทำให้สารสนเทศของเราเกิดความเสียหาย จากนั้นจึงประเมินความเสี่ยง และกำหนดมาตรการจัดการกับภัยคุกคาม ให้แน่ใจว่าสามารถรับมือภัยคุกคามเหล่านั้นได้อย่างเหมาะสม

ISO27001 ทำยากมั๊ย? กลัวจะทำไม่สำเร็จ

นี่เป็นคำถามยอดฮิตเลยครับ คำถามที่ว่าทำยากมั๊ย ตอบได้เลยว่าไม่ยาก ถ้ามีความรู้และความเข้าใจ 2 เรื่องใหญ่ๆ คือ

1. เข้าใจองค์กรตัวเอง
2. เข้าใจมาตรฐานว่าต้องทำอะไรบ้าง

ISO27001 ทำยากมั๊ย? กลัวจะทำไมไม่สำเร็จ(ต่อ)

1.เข้าใจองค์กรตนเอง :

ต้องสำรวจข้อมูล ซอฟต์แวร์ ฮาร์ดแวร์ บุคลากร ในขอบเขตที่จัดทำระบบ ข้อมูลนี้ยังมีรายละเอียดยิ่งดี หากหน่วยงานท่านเป็นราชการ บัญชีครุภัณฑ์เป็นจุดเริ่มต้นที่ดีในการรวบรวมข้อมูล Hardware Software

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

ISO27001 ทำยากมั๊ย? 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

Establish จัดทำระบบ

ปรับปรุง
อย่างต่อเนื่อง
Continual
Improvement



Implement
นำไปใช้

Maintain
รักษาระบบ

นำไปใช้ได้กับองค์กร
ทุกขนาดและทุกประเภท



Focus !!

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

เน้นการบริหารจัดการ
ความเสี่ยงของสารสนเทศ



Applicability

All type ,size and nature
of organizations

The background is a solid teal color. In the four corners, there are decorative white line-art patterns resembling circuit traces or network connections, with small circles at the end of the lines.

ทำความเข้าใจมาตรฐาน ISO27001:2013

และความสำคัญของการประเมินความเสี่ยงของสารสนเทศ

(Information Security Risk Assessment)

ประเมินความเสี่ยงนั้นสำคัญไฉน

"การประเมินความเสี่ยงของสารสนเทศ(Information Security Risk Assessment)" เป็นหัวใจสำคัญของการทำ ระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO27001 นั่นคือ หากท่านประเมินความเสี่ยงไม่ถูกต้อง หรือไม่ครอบคลุม ก็จะทำให้การจัดการความเสี่ยงที่ตามมานั้นแก้ปัญหาไม่ตรงจุด และไม่ครอบคลุมตามไปด้วย ว่างไปแล้วการประเมินความเสี่ยงก็เหมือนการตรวจร่างกายถ้าตรวจไม่ครบหรือตรวจไม่ละเอียดก็ไม่พบอาการป่วยและไม่ได้รับการ ปล่อยทิ้งไว้จนสูงงอมอาการป่วยก็แสดงออกมาในที่สุด!!

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. ซอฟต์แวร์ที่เป็นอันตราย | 5. ข้อผิดพลาดการบำรุงรักษา | 5. อุณหภูมิสูงและความชื้น |
| 6. กฎหมายการใช้ซอฟต์แวร์ | 6. ความล้มเหลวของซอฟต์แวร์ | 6. ฝุ่นละออง |
| 7. เข้าถึงเครือข่ายโดยผู้ที่ไม่ได้รับอนุญาต | 7. การใช้ซอฟต์แวร์ผิดกฎหมาย | 7. รั้งสีแม่เหล็กไฟฟ้า |
| 8. ใช้สิ่งอำนวยความสะดวกทางเครือข่ายโดยไม่ได้รับอนุญาต | 8. ความล้มเหลวทางเทคนิคของอุปกรณ์เครือข่าย | 8. ไฟฟ้าสถิต |
| 9. แทรกซึมการสื่อสาร, ดักฟัง การสนทนา | 9. การส่งผิดพลาด | 9. การเสื่อมสภาพของสื่อจัดเก็บข้อมูล |
| 10. เปลี่ยนเส้นทางของข้อมูล | 10. การส่งข้อมูลเกินพิกัด | |
| | 11. ลบไฟล์, ลบข้อมูล | |

สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย

(Security Awareness Training)



ผู้บรรยาย

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

วัตถุประสงค์

- เพื่อสร้างความตระหนักและความเข้าใจถึงภัยคุกคามที่เกิดขึ้นบนระบบเครือข่ายอินเทอร์เน็ตในปัจจุบัน
- เพื่อเรียนรู้แนวทางป้องกันและลดความเสี่ยงจากภัยคุกคามที่เกิดขึ้นบนระบบเครือข่ายอินเทอร์เน็ต
- เพื่อให้ผู้เข้าร่วมอบรมสามารถนำความรู้ที่ได้ไปเผยแพร่ให้ผู้อื่นได้อย่างถูกต้องและมีประสิทธิภาพ



ภัยคุกคามจากเครือข่ายออนไลน์

Scam/Phishing: การล่อลวงทางอินเทอร์เน็ต

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

Scam/Phishing: การล่อลวงทางอินเทอร์เน็ต



ตัวอย่าง Phishing

The image shows a screenshot of a phishing email. At the top left is a generic person icon. To its right, the date and time 'Tue 29/12/2015 17:11' are displayed. The sender is identified as 'PayPal <confirmagain@ppservice.com>', with the email address highlighted by a red box and an arrow pointing to the Thai annotation 'สังเกตอีเมลผู้ส่ง' (Observe the sender's email). The subject line reads 'Your PayPal account has been limited'. Below this is the PayPal logo and the text 'ข้อความเชิญชวนให้ผู้ใช้งานดำเนินการ Login เข้าสู่ระบบ' (Invitation message for users to perform login system operation). The main body of the email features a large red-bordered box with the heading 'Update Required!!'. The text inside explains that account activity is unusual and that the account is limited. It includes a section titled 'How to remove my limitation?' and lists steps to resolve the issue. The first step is 'Log in here.', which is highlighted by a red box and an arrow pointing to the Thai annotation 'มีลิงค์ให้คลิกเพื่อ Login เข้าสู่ระบบ' (There is a link to click for login system operation). The second step is to provide needed information. At the bottom, there is a warning: 'If this message sent as Junk or Spam, its just an error by our new system, please click at Not Junk or Not Spam'. The email ends with 'Sincerely, PayPal'.

Tue 29/12/2015 17:11

PayPal <confirmagain@ppservice.com>

Your PayPal account has been limited

To [redacted]

สังเกตอีเมลผู้ส่ง

PayPal

ข้อความเชิญชวนให้ผู้ใช้งานดำเนินการ Login เข้าสู่ระบบ

Update Required!!

Recently, there's been activity in your PayPal account that seems unusual compared to your normal account activities. Please log in to PayPal to confirm your identity.

This is part of our security process and helps ensure that PayPal continue to be safer way to buy online. Often all we need is a bit more information. While your account is limited, some options in your account won't be available.

How to remove my limitation?

You can resolve your limitation by following these simple steps:

- **Log in here.** มีลิงค์ให้คลิกเพื่อ Login เข้าสู่ระบบ
- Provide the information needed. The sooner your provide the information we need, the sooner we can resolve the situation.

"If this message sent as Junk or Spam, its just an error by our new system, please click at Not Junk or Not Spam"

Sincerely,
PayPal

ตัวอย่าง Phishing

From : KASIKORN BANK <kasikombank@thaimail.org>
Reply-To : <kasikornbank@thaimail.org>
Sent : Friday, June 8, 2007 7:58 AM
To : "Jeroz Bharucha" <usoraze@hotmail.com>
Subject : KASIKORN BANK (PAYMENT ADVICE)



Your application for the claim of lottery winning prize will be duly processed, and pay be made upon certification. Hence, carefully fill in the appropriate informations in the provided below to facilitate our immediate commencement of your final claim process.

DETAILS OF BENEFICIARY :

[FULL NAME OF WINNER].....
[RESIDENT ADDRESS].....
[COUNTRY/CITY].....
[DATE OF BIRTH]..... [SEX].....
[MARITAL STATUS].....

From : KASIKORN BANK <kasikombank@thaimail.org>
Reply-To : <kasikornbank@thaimail.org>
Sent : Friday, June 8, 2007 7:58 AM
To : "Jeroz Bharucha" <usoraze@hotmail.com>
Subject : KASIKORN BANK (PAYMENT ADVICE)



ตัวอย่าง Phishing

Tue 5/16/2017 10:29 AM
admin@Kasikorn.com
ลงทะเบียนรับ iPhone 7


To: Damrongsak Chairattanasong
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

ประกาศปรับปรุงระบบ K-Cyber เนื่องจากธนาคารมีการปรับปรุงระบบรักษาความปลอดภัย จึงขอให้ผู้ใช้งานทุกท่านทำการลงทะเบียน
เพื่อรักษาข้อมูล **ลงทะเบียน**
(สำหรับผู้ที่ลงทะเบียนภายในวันที่ 19 พฤษภาคม 2560 สิ้นรับ iPhone 7 ประกาศในวันที่ 26 พฤษภาคม 2560)



ลงทะเบียนรับ iPhone 7

เนื่องจากธนาคารมีการปรับปรุงระบบรักษาความปลอดภัยภายใน
ทางธนาคารจึงขอให้ผู้ใช้งานทุกท่านทำการลงทะเบียนเพื่ออัปเดตข้อมูล



สมัครรับข้อมูลระบบ security iphone 7

ชื่อ

นามสกุล

หมายเลข

อีเมล

* กรุณาตรวจสอบข้อมูลก่อนกดปุ่ม

Sign up

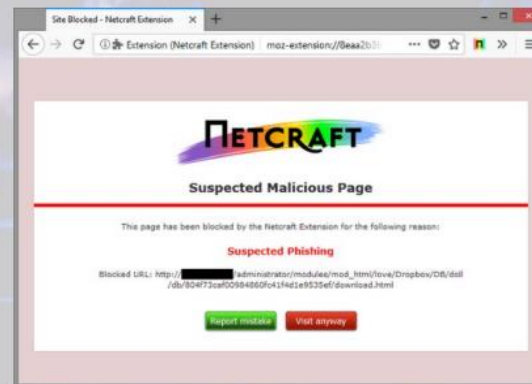
***ลงทะเบียนภายในวันที่ 19 พ.ค. 2560 สิ้นรับ iPhone 7 จำนวน 3 รางวัล
ประกาศผล 26 พ.ค. 2560**

www.kasikornbank.com
K-Contact Center 01-2582000

Facebook: KBank Line
Twitter: EBank Line
YouTube: EBank Line
WhatsApp: KBank Line

วิธีแก้ไข / ป้องกัน

- ห้ามคลิกลิงค์ที่ได้รับจากอีเมลควรดำเนินการกรอกชื่อเว็บไซต์ในช่อง URL บนเบราว์เซอร์ด้วยตัวท่านเอง
- การเข้าถึงเว็บไซต์ที่มีการ Login เข้าสู่ระบบจะต้องสังเกตสัญญาณลักษณะรูปกุญแจสีเขียว
- ตรวจสอบผ่านเว็บไซต์ www.virustotal.com
- ตรวจสอบโดยใช้ Add on หรือ Extensions บนเบราว์เซอร์



ภัยคุกคามจาก Malware

[ไม่มีชื่อจริง]



เนื้อหา

- รวมฮิต Malware (ซอฟต์แวร์ไม่ประสงค์ดี)
- Ransomware (แรนซัมแวร์) เข้ายึดข้อมูล เรียกค่าไถ่จากผู้ใช้งาน
- Scareware (สแกร์แวร์) หลอกหลวงผู้ใช้งานว่าเป็นผลิตภัณฑ์รักษาความปลอดภัย มีการแจ้งเตือนผู้ใช้ว่า มีการติดเชื่อเกิดขึ้น และให้ดาวน์โหลดโปรแกรมป้องกันไวรัส(ปลอม)มาติดตั้งที่เครื่อง
- Spyware (สปายแวร์) ละเมิดความเป็นส่วนตัวของผู้ใช้
- Trojan (โทรจัน) หลอกว่าเป็นโปรแกรมปกติทั่วไป เมื่อหลงติดตั้งจะขโมยข้อมูลและเปิดให้ผู้ใช้ไม่ประสงค์ดีเข้ามาควบคุมเครื่อง

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 GMT from Monday to Friday.

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](#)

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

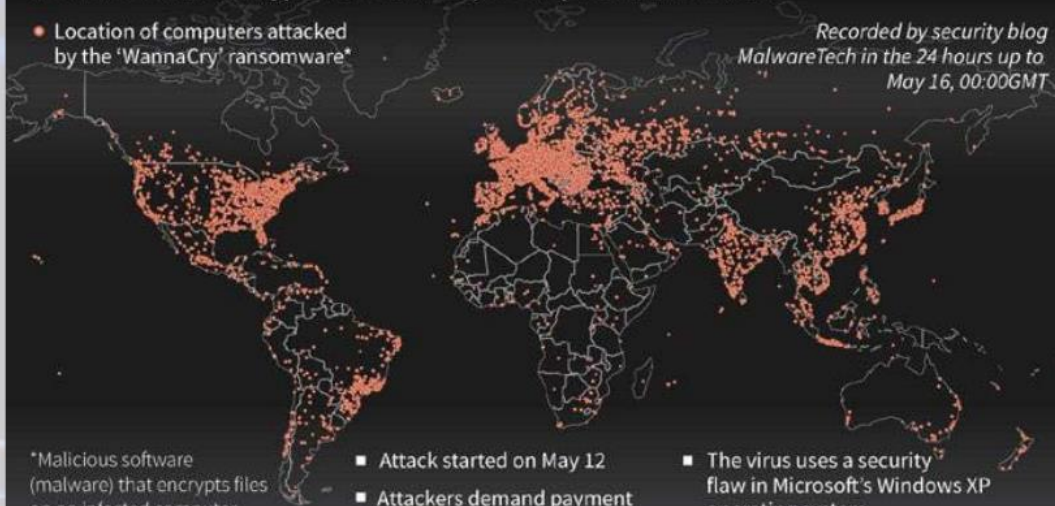
WannaCry

'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



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/>

KASPERSKY EN RU **FAQ**

Free Ransomware Decryptors

Welcome to No Ransom, the place to find the latest decryptors, ransomware removal tools, and information on ransomware protection.

What is ransomware? It's a malware (a Trojan or another type of virus) that locks your device or encrypts your files, and then tells you that you have to pay ransom to get your data back. It's not cheap, and there's no guarantee of success. If you become a victim of ransomware, try our free decryption tools and get your digital life back.

Remove the ransomware first (you can use **Kaspersky Internet Security**) or else it will lock up your system again.

Before starting the decryptor, read the associated **how-to guide**.

Type the file extension, email or any other information mentioned on the locked screen **SEARCH**

| TOOL NAME | DESCRIPTION | UPDATED |
|-----------|-------------|---------|
| LOOF MYKE | DESCRIPTION | UPDATED |

วิธีแก้ไข / ป้องกัน

- *****ส่วนใหญ่แก้ไม่ได้ 100%*****
- Ransomware แต่ละตัวแก้ไขไม่เหมือนกัน
- จ่ายเงินค่าไถ่ใช้ว่าจะได้ข้อมูลเสมอไป
- ลง Antivirus **ที่สำคัญต้อง update**
- ไม่เปิดไฟล์มั่ว
- ไม่คลิกลิงค์มั่ว
- สำรองข้อมูลสำคัญไว้ ปลอดภัยที่สุด
- อัปเดตระบบปฏิบัติการที่ใช้งานอย่างสม่ำเสมอ

ซอฟต์แวร์สอดแนม (Spyware)

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



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

ภัยคุกคามบนมือถือสมาร์ทโฟนที่เกิดขึ้นในประเทศไทย

เว็บไซต์ข่าวในไทย ถูกฝังโทรจัน ปล่องัดตัดทลออกโหลดแอปป้องกันไวรัสปลอม
ในธนาคารออนไลน์



SMS ดาวน์โหลดโปรแกรม AVG AntiVirus Mobile Pro สำหรับติดตั้งใน Android โดยโปรแกรม
ดังกล่าวเป็นโปรแกรมแอนตี้ไวรัสปลอม จุดประสงค์เพื่อขโมย SMS OTP จากธนาคาร

ภัยคุกคามบนมือถือสมาร์ทโฟนที่เกิดขึ้นในประเทศไทย

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



ภัยคุกคามบนมือถือสมาร์ทโฟนที่เกิดขึ้นในประเทศไทย



✓ วิธีสังเกต แอป จริง

1. ชื่อแอป ต้องเป็น "Bualong mBanking"
2. ไอคอนของแอป 
3. ชื่อผู้พัฒนาต้องเป็น "Bangkok Bank PCL"

✗ วิธีสังเกต แอป ปลอม

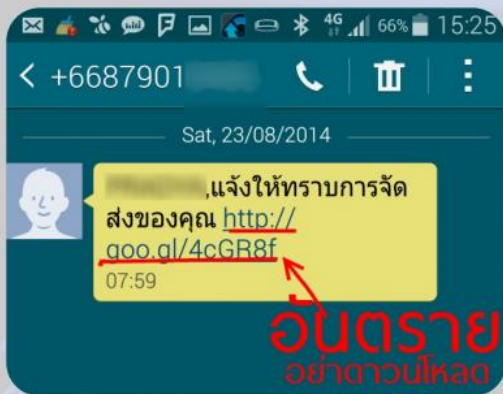
ชื่อผู้พัฒนาไม่ใช่ "Bangkok Bank PCL"
ไม่ว่าจะภาษาไทยหรืออังกฤษ

ระวัง! แอปปลอม



วิธีสังเกตให้ดูชื่อ Developer
ต้องเป็นของ Siam Commercial Bank PCL. เท่านั้น

ภัยคุกคามบนมือถือสมาร์ทโฟนที่เกิดขึ้นในประเทศไทย



อันตราย
อย่าดาวน์โหลด

ขั้นตอนการโจมตีไวรัส SMS

เกิดกับผู้ใช้แอนดรอยด์เท่านั้น

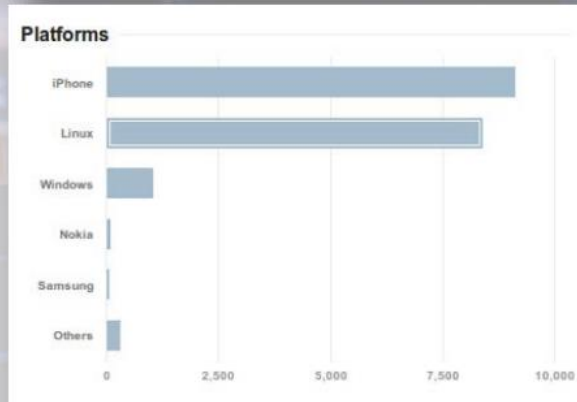
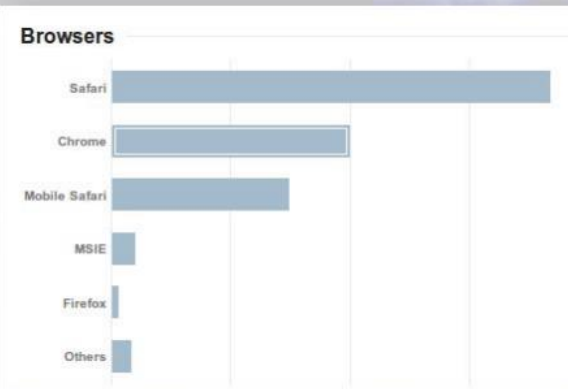
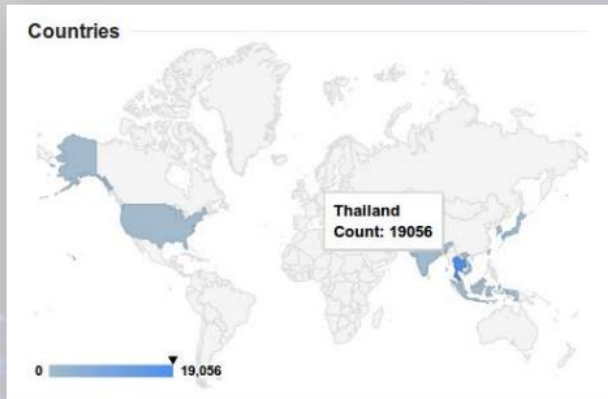
- 01** มี SMS จากคนรู้จัก ส่งเข้ามาที่สมาร์ทโฟน ให้คลิกลิงก์ไปดาวน์โหลด แอปพลิเคชันมาติดตั้ง โดยมีข้อความ เช่น (ชื่อผู้ติดต่อในโทรศัพท์), รับประทานในการดำเนินคดี ของคุณ <http://goo.gl/q87XnM>
- 02** เมื่อติดตั้งแล้ว แอปจะเข้าหารายชื่อผู้ติดต่อ และส่งข้อความสั้น ออกต่อไป
- 03** เกิดค่าใช้จ่าย ในการส่ง SMS ทำให้ผู้ใช้โรคเข้าห้องเรียน ทางโอเปอเรเตอร์
- 04** โอเปอเรเตอร์ ร่วมกันปิดกั้น ลิงก์ดาวน์โหลด และเฝ้าระวัง การส่งข้อความ

วิธีป้องกัน
ไม่ควรคลิกลิงก์ที่ไม่รู้แหล่งที่มา และคอยตรวจสอบค่าบริการอย่างสม่ำเสมอ

ASTV infoGraphics
www.manager.co.th
ที่มา : ASTV ผู้จัดการออนไลน์

ภัยคุกคามบนมือถือสมาร์ทโฟนที่เกิดขึ้นในประเทศไทย

สถิติการคลิกลิงก์ที่เผยแพร่มาแวร์



ภัยคุกคามบนมือถือสมาร์ทโฟนที่เกิดขึ้นในประเทศไทย

อีเมลหลอกลวง (Phishing)

From: Bank of Ayudhya [mailto:updatebof@optu.net.com.au] ❶
To: undisclosed-recipients:
Subject: Bank of Ayudhya :: Account Verification Process. ❷

 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.
https://www.krungsrionline.com/cgi-bin/bvisapi.dll/krungsri_ib/login/login.jsp ❸

แนบไฟล์มา จะนำส่งเจ้าหน้าที่ของทาง 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: Kasikom Bank <alert@kasikom.com>
To: [REDACTED]
Sent: Saturday, September 15, 2012 7:23 PM
Subject: New Message From Kasikom Bank



Dear Esteemed Customer,
At Kasikom Bank Thailand, We take security Seriously. You are receiving This Email as you are a customer with Kasikom Bank.
Your Account has been flagged for security issues, you must now login and validate your account for your own protection. กรุณาเข้าหลักสิทธิ์ใดๆ ก็อยู่ในขั้นแจ้งเตือนแล้ว
Click here to login and validate your Account
This Email is subject to security From Kasikom Bank, Please view our privacy policy statement.
Regards,
Technical Service /Internet security,
Kasikom Bank,
Thailand

Kasikom Bank © 2012 All Rights Reserved



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 © 2007.
All Rights Reserved

วิธีแก้ไข / ป้องกัน บนมือถือสมาร์ทโฟน

- ดำเนินการอัปเดตแอปพลิเคชันอย่างสม่ำเสมอ
- ไม่ Jailbreak หรือ root เครื่อง
- ดำเนินการติดตั้ง Antivirus บนอุปกรณ์
- ไม่ติดตั้งโปรแกรมจากแหล่งอื่นที่ไม่ใช่ Google Play, App Store
- ดำเนินการตรวจสอบความเหมาะสม และนำเชือกของแอปก่อนติดตั้ง
- ห้ามคลิกลิงค์ที่ได้รับจากอีเมลควรดำเนินการกรอกชื่อเว็บไซต์ในช่อง URL บนเบราว์เซอร์ด้วยตัวท่านเอง
- การเข้าถึงเว็บไซต์ที่มีการ Login เข้าสู่ระบบจะต้องสังเกตสัญญาณลักษณะรูปกุญแจสีเขียว
- ตรวจสอบผ่านเว็บไซต์ www.virustotal.com



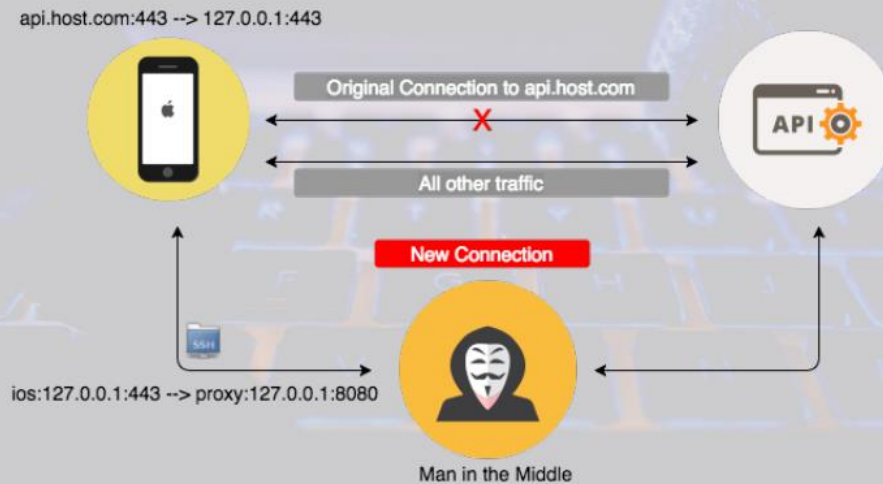
ภัยคุกคามจากการใช้งาน
เครือข่ายไร้สาย
ที่ให้บริการในพื้นที่สาธารณะ



คุณคิดว่า **https** ปลอดภัยหรือไม่ ?
อย่าเพิ่งคิดว่าปลอดภัยเพราะอาจไม่เป็นเช่นนั้น

ภัยคุกคาม และความเสี่ยงต่อการใช้งาน Mobile Device

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



ภัยคุกคาม และความเสี่ยงต่อการใช้งาน Mobile Device

The image displays two browser windows illustrating security warnings. The top window shows a Firefox browser with the address bar containing `https://gmail.com`. The main content area displays a warning: "Your connection is not secure". Below this, it states: "The owner of gmail.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website." It further explains: "This site uses HTTP Strict Transport Security (HSTS) to specify that Firefox may only connect to it securely. As a result, it is not possible to add an exception for this certificate." There are buttons for "Go Back" and "Advanced", and a checkbox for "Report errors like this to help Mozilla identify and block malicious sites".

The bottom window shows a browser with the address bar containing `https://www.facebook.com`. The main content area displays a warning: "Your connection is not private". Below this, it states: "Attackers might be trying to steal your information from **www.facebook.com** (for example, passwords, messages, or credit cards). [Learn more](#)". The error code "NET::ERR_CERT_AUTHORITY_INVALID" is shown. There is a checkbox for "Automatically send some system information and page content to Google to help detect dangerous apps and sites. [Privacy policy](#)".

วิธีแก้ไข / ป้องกัน

- ไม่ใช้งาน Wi-Fi สาธารณะในการทำธุรกรรมทางการเงินและเข้าสู่ระบบงานสำคัญภายในองค์กร
- สังเกตหน้า Error ของเว็บเบราว์เซอร์ในการแจ้งเตือนต่าง ๆ
- การเข้าถึงเว็บไซต์ที่มีการ Login เข้าสู่ระบบจะต้องสังเกตสัญญาณลักษณะรูปกุญแจสีเขียว
- ตรวจสอบผ่านเว็บไซต์ www.virustotal.com
- ตรวจสอบโดยใช้ Add on หรือ Extensions บนเบราว์เซอร์ “HTTPS Everywhere”





ภัยคุกคามบนระบบสารสนเทศ ภายในองค์กรหรือบริษัท

6C6974746
Data Breac
6368657320
Attack696
7368 06
7468652A



เนื้อหา

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

การตั้งรหัสผ่านให้ปลอดภัย

- ความยาวรหัสผ่าน 8-16 ตัวอักษร
- ประกอบด้วยตัวอักษร ตัวเลข และอักขระพิเศษ
- ไม่ใช่คำที่มีในพจนานุกรม (Dictionary)
- ควรมีการเปลี่ยนรหัสผ่านตามระยะเวลา เช่น 6 เดือนหรือ 1 ปี
- ไม่ใช่งานรหัสผ่านที่เหมือนกันในทุก ๆ บริการ
- แยกรหัสผ่านสำหรับระบบงาน(ที่ทำงาน) กับระบบที่ใช้งานส่วนตัว



การตั้งรหัสผ่านให้ปลอดภัย



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

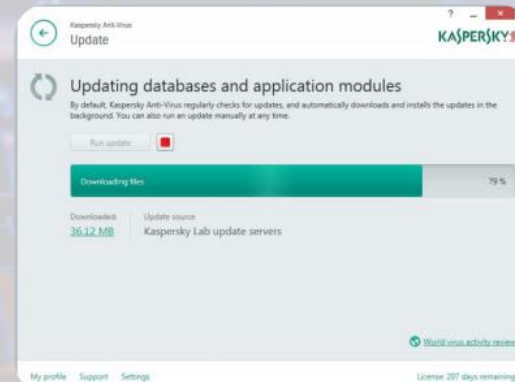
การตั้งรหัสผ่านให้ปลอดภัย

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



การป้องกันไวรัสบนเครื่องคอมพิวเตอร์

- ผู้ใช้งานต้อง : ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัสว่า**ยังทำงานตามปกติหรือไม่** และ**มีการปรับปรุงฐานข้อมูลไวรัส**อย่างสม่ำเสมอหรือไม่ โดยให้ทำการ**ตรวจสอบอย่างน้อยวันละ 1 ครั้ง** หากพบว่าทำงานผิดปกติ ให้รีบแจ้งผู้ดูแลระบบที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยทันที



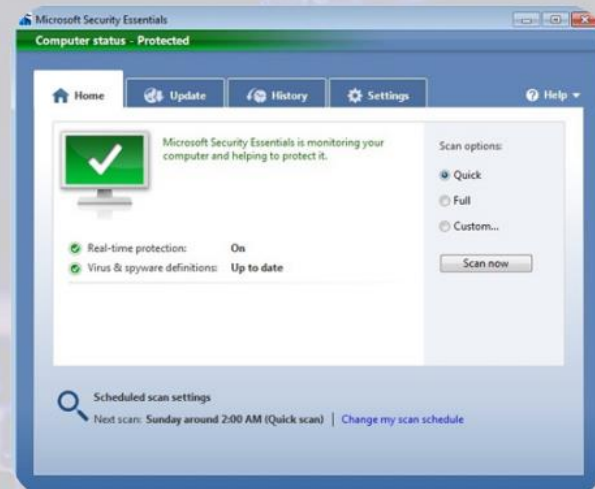
การป้องกัน Spyware

- เวลาที่ผู้ใช้พบหน้าจอในลักษณะนี้ให้คลิกที่กากบาท X ขวบน เพื่อปิดหน้าต่าง
- ปิดอ็อปชั่น
- อย่าคลิก “yes” หรือ “accept” หรือ “download” เพราะนั่นเท่ากับเป็นการอนุญาตให้ดาวน์โหลดโปรแกรมเหล่านั้นได้
- เพราะฉะนั้น “อย่าหลงกล”

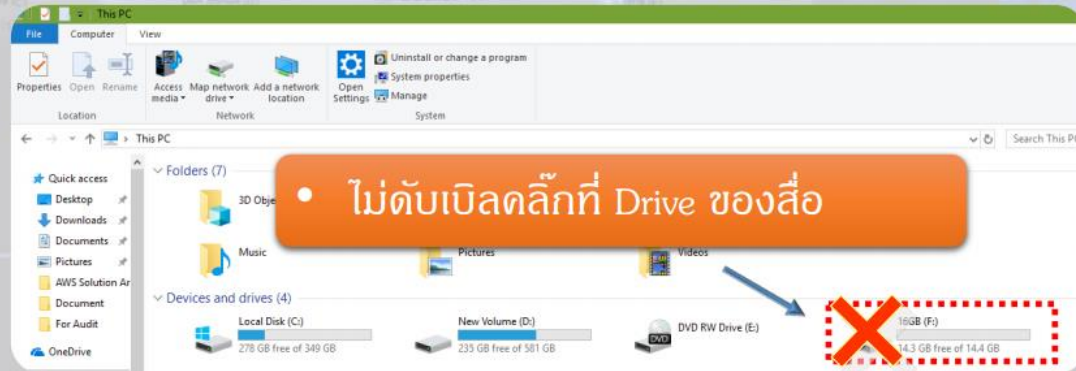
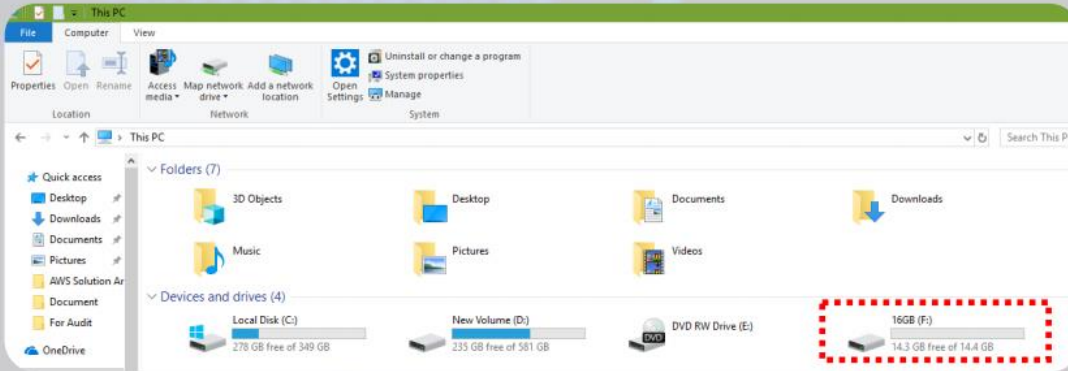


การป้องกัน Spyware

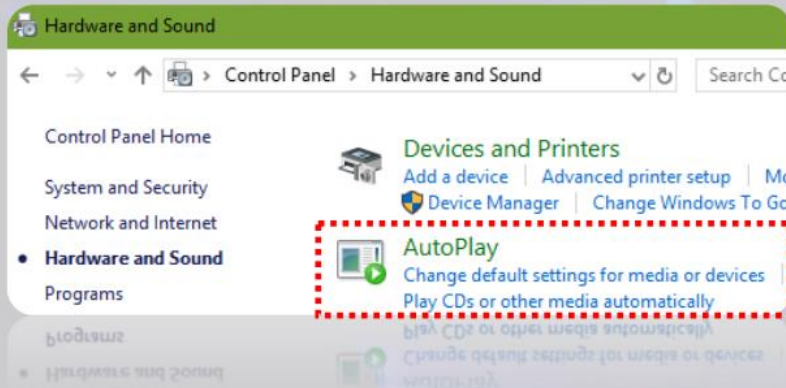
- ใช้ซอฟต์แวร์แอนติสไปยาแวร์ ซึ่งเป็นเสมือนกำแพงอีกด้านหนึ่งที่ช่วยป้องกันซอฟต์แวร์ที่ไม่รู้จักติดตามคุณเข้ามาขโมยข้อมูลส่วนบุคคลจากเครื่องของคุณระหว่างที่ใช้งานออนไลน์



การป้องกันไวรัสจาก Thumb Drive

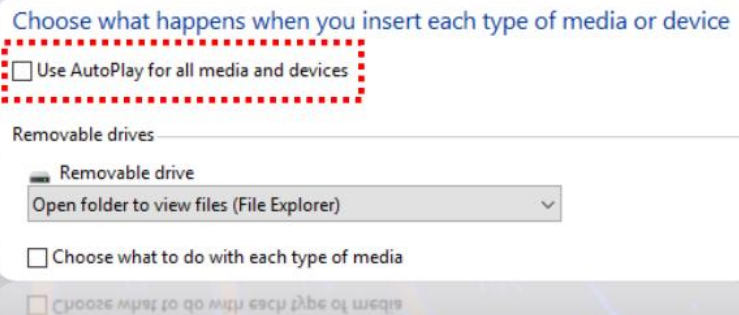


การป้องกันไวรัสจาก Thumb Drive

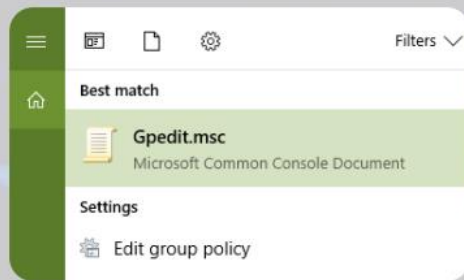


- การปิดการทำงานของ Autoplay ที่มีมาใน Control Panel

- เอาเครื่องหมายถูกออกหน้าหัวข้อ Use AutoPlay for all media and devices แล้วคลิก Save

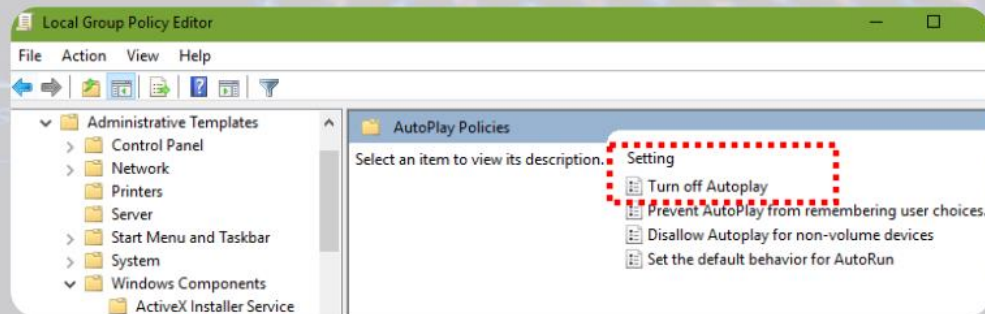


การป้องกันไวรัสจาก Thumb Drive



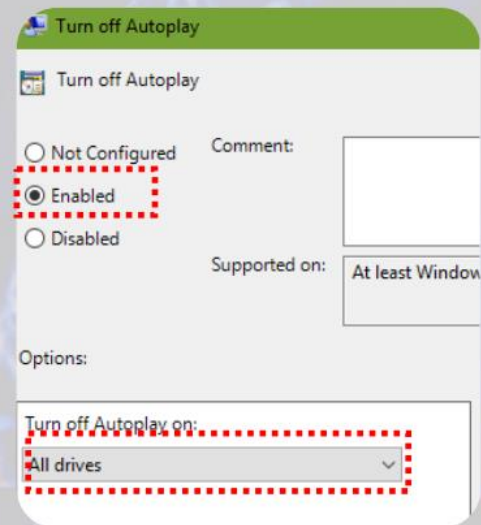
- คลิก Start -> ที่ช่อง Search box พิมพ์คำสั่ง Gpedit.msc -> Enter

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



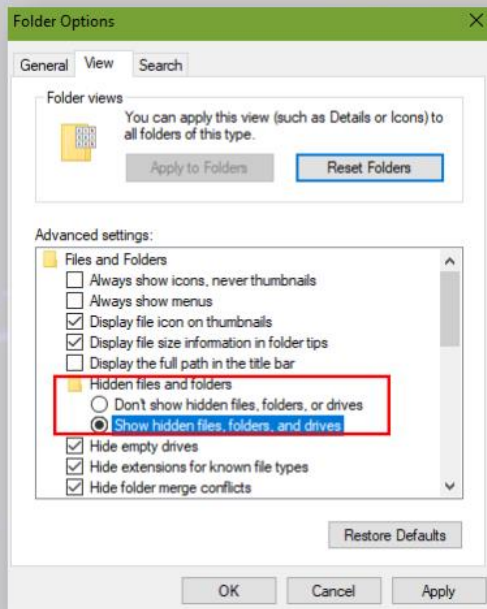
การป้องกันไวรัสจาก Thumb Drive

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



การป้องกันไวรัสจาก Thumb Drive

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



- เลือกที่แถบ View
- แล้วคลิกที่ Show Hidden file, folders, And drives
- แล้วติ๊กที่ Hide protected operating system file

การตั้งค่า Windows Update

Windows Update

Update status



Your device is up to date. Last checked: Today, 1:46 PM

Check for updates

[View installed update history](#)

⚙️ Advanced options

Choose how updates are installed

Give me updates for other Microsoft products when I update Windows.

Configure automatic device setup after an update under the Privacy section in [Sign-in options](#).

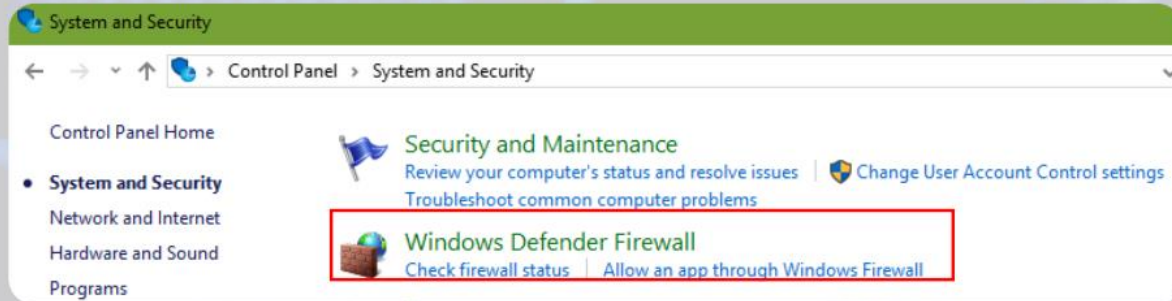
Choose when updates are installed

Choose the branch readiness level to determine when feature updates are installed. 'Semi-Annual Channel (Targeted)' means the update is ready for most people, and 'Semi-Annual Channel' means it's ready for widespread use in organizations.

Semi-Annual Channel (Targeted) ▾

Semi-Annual Channel (Targeted) ▾

การเปิดใช้งาน Personal Firewall



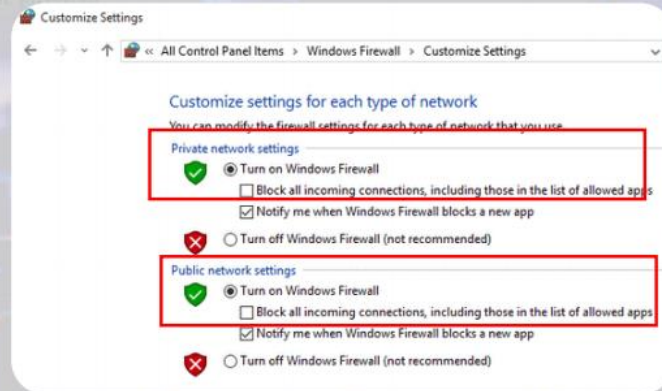
Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

| | | |
|---|--|---------------|
| | Domain networks | Not Connected |
| | Home or work (private) networks | Connected |
| Networks at home or work where you know and trust the people and devices on the network | | |
| Windows Firewall state: | On | |
| Incoming connections: | Block all connections to programs that are not on the list of allowed programs | |
| Active home or work (private) networks: | LAURENSON | |
| Notification state: | Notify me when Windows Firewall blocks a new program | |
| | Public networks | Not Connected |





ภัยคุกคามที่เกิดขึ้นใน ชีวิตประจำวัน

การดักดูข้อมูลบัตร ATM (ไทย)

- ติดตั้ง Key Board ส่วนบุคคล



การตรวจจับข้อมูลบัตร ATM (ไทย)

- กดประกอบได้



การตรวจจับข้อมูลบัตร ATM (ไทย)

- ตู้ ATM ไม่ปรกติ



วิธีแก้ไข / ป้องกัน

- สังเกตความผิดปกติต่างๆ รอบๆ เครื่อง ATM
- การกดเงินสดที่ตู้ ATM ทุกครั้งต้องปกปิดรหัสผ่าน
- สมัครบริการ SMS Alert
- ทำการจำกัดวงเงิน
- ใช้บัตร ATM EMV ชิป
- แจ้งธนาคารทันทีเมื่อพบสิ่งผิดปกติ



Q & A

