



IT Security Awareness Training

15 สิงหาคม 2561

โดย ชาญยุทธ ลือシリพานิชย์



Agenda

01

แบบทดสอบก่อนเรียน

9:00 – 9:10 (10 นาที)

02

Cyber Security คืออะไร ทำไมถึงต้องให้ความสำคัญ

9:10 – 9:30 (20 นาที)

03

ภัยคุกคามประเภทต่าง ๆ และการรับมือ

9:30 – 11:30 (120 นาที)

04

แบบทดสอบหลังเรียน และกิจกรรมเกมส์ตอบคำถาม

แบบทดสอบ 11:30 – 11:40 (10 นาที)

กิจกรรมเกมส์ 11:40 – 12:00 (20 นาที)

Portfolio

Chanyut

Luesiripanit

Experience in

- Risk Management
- Software Developer
- IT Auditor
- IT Security
- ISO 27001 Auditor

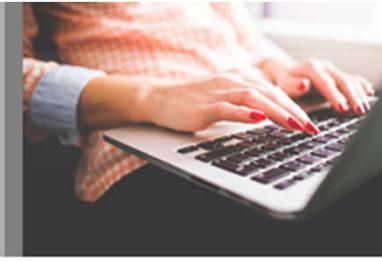


Certificate

- CompTIA Network+
- CompTIA Security+
- Internal Auditing Education Partnership (IAEP)

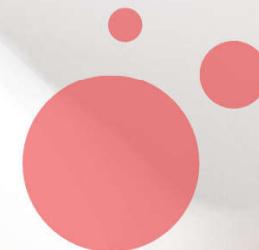


แบบทดสอบ ก่อนเรียน



<https://www.surveymonkey.com/r/G9HQN87>





Viral ?

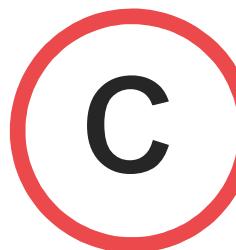
ความปอดภัยทางไซเบอร์ คืออะไร มันสำคัญไหม
ทำไมหลายคนพูดกัน น่ากลัวจริงเหรอ ใจรักก็ถูกเปลี่ยนไป

Cyber Security

ปัญหาภัยคุกคามทางไซเบอร์แบ่งได้เป็น 4 ลักษณะ C.H.E.W.



Cybercrime



วัตถุประสงค์ทางการเงิน

การแฮกบัญชีธนาคารหรือ
ธุรกรรมออนไลน์ต่างๆ
การเรียกค่าไถ่ต่างๆ

Hacktivism



เปิดโปงข้อมูลลับ / อุดมการณ์

เป็นการแฮกข้อมูลลับไม่ว่าจะของทางการ
หรือเอกชนแล้วนำมาเผยแพร่ต่อสาธารณะ
เพื่อเปิดโปงเรื่องบางอย่างหรือสร้างความอับ
อายแก่เจ้าของข้อมูล หรือแสดงจุดยืน
อุดมการณ์

Espionage



จารกรรมข้อมูลเพื่อนำไปใช้
ประโยชน์ต่อ

การเจาะข้อมูลนิเวศน์ต่างๆ การ
เจาะข้อมูลทางการทหาร

War / Cyberwar



การโจมตีทางทหาร /
ความมั่นคงของประเทศ
การทำลายฐานผลิตอาวุธนิวเคลียร์ หรือ
แม้แต่การทำให้ระบบสื่อสารและแหล่ง
พลังงานของปฏิบัติการล่ม



ผลกระทบความมั่นคงฯ มนต์ขลัง^๔
แยกเกอร์เจียระบบธง ไฟฟ้าบุก นับสิบแห่ง



สำนักข่าว นิวยอร์ก ใบเสร็จของสหรัฐฯ รายงานอ้างข้อมูล
จากเจ้าหน้าที่เบี่ยงข่าวกรอง ว่า ผลกระทบความมั่นคง
นาตุนี (เลือกชื่อ) มีรายงานด่วนระดับด้วยความสูงสุด
สำนัก 2 ระบุว่า โรงงานไฟฟ้าบุกเดือดเรื่องค่าไฟ 12 แห่ง^๕
ถูกกลุ่มแยกเกอร์เจียตั้งข้อหา ซึ่งอาจจะเป็นรัฐเชิง
อันน่าอึด...



รัฐบาลแห่งชาติของ USA
สำลักน้ำผ่านบาร์บาร์ของผู้คน
ของสถาบันทางการค้าได้ประกาศว่าผู้คนของ
บริษัทต้องรับภัยคุกคามจากกลุ่มเชื้อ
ไวรัสที่ใช้เวลาเพื่อเข้ารหัสและหักยืด
โดยการติดต่อผ่านเครือข่ายคอมพิวเตอร์

โรงแรม Romantik Seehotel Jaegerwirt

4-Star Superior Hotel เป็นโรงแรมที่ใหญ่ที่สุดใน
ประเทศซึ่งได้รับการยกประดับด้วย
Ransomware แม้จะมีภัยคุกคามที่รุนแรง
กว่าที่เคยมีมา ไม่สามารถต้านทานได้
และบานะที่หายไปนับล้านดอลลาร์
ต้องเสียตัวให้กับกลุ่มเชื้อไวรัส

ATM ธนาคารของลูกค้าในเมืองใหญ่ใน
เดือนที่แล้ว ก่อให้เกิดภัยคุกคามแก่
Jackpotting ฝีมือเชื้อไวรัสที่ต้องการเงินเดือน
ภายใน ATM มาก่อนที่จะเข้าสู่ระบบ
เครื่องจ่ายเงิน ไม่สามารถต้านทานได้
และบานะที่หายไปนับล้านดอลลาร์
ต้องเสียตัวให้กับกลุ่มเชื้อไวรัส

มีผู้คนหลายรายที่ต้องเสียเงินเดือน
ในการซ่อมแซมเครื่องจ่ายเงินเดือน
ของตน ซึ่งเป็นภัยคุกคามที่รุนแรงที่สุดใน
โลกในปัจจุบัน ล่าสุด ลูกค้าที่ต้องเสียเงินเดือน
จำนวนมากต้องเสียเงินเดือนที่ต้องเสียเงินเดือน
ให้กับกลุ่มเชื้อไวรัสที่ต้องการเงินเดือน

ชีวิตเสียไปในชั่ว 24 ชม. !!!

มีรายงานว่าได้มีกลุ่มที่มีบุคคลเข้าร่วมในการซ่อมแซมเครื่องจ่าย
เงินเดือนของลูกค้าที่ต้องเสียเงินเดือน ไม่สามารถต้านทาน
ภัยคุกคาม ซึ่งเป็นภัยคุกคามที่รุนแรงที่สุดใน
โลกในปัจจุบัน ล่าสุด ลูกค้าที่ต้องเสียเงินเดือน



INTERPOL
กองกำลังต่อต้านอาชญากรรมไซเบอร์
ปฏิเสธผู้ต้องหา ให้ทุกคนเข้าร่วม
ชุมชนที่ Webstresser.org

A fake news article from 'Spring News' about the Bitfinex Bitcoin Exchange hack. It features a large Bitcoin logo and a network diagram. The headline reads: 'Bitfinex Bitcoin Exchange Hacked \$72 Million In Bitcoin Stolen Bitcoin sanked 20%' and includes a screenshot of a hacked website with a 'Hacked by #CJapan Anonymous' message.

**Bitfinex Bitcoin Exchange Hacked
\$72 Million In Bitcoin Stolen
Bitcoin sanked 20%**

Hacked by #CJapan Anonymous
#OpSingleGateway

**"Anonymous" เหงาหนัก!
โจมตีเว็บ 4 เว็บไซต์ราชการไทย
ประกาศลั่นเฟชบັກ
เจาะระบบกลาโหม-ลั่งเอกสารลับแล้ว**

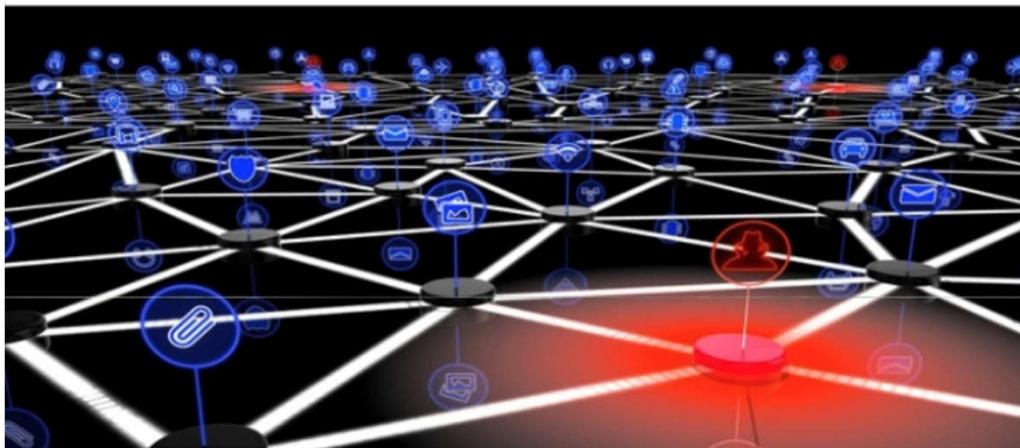
SPRING NEWS

f t g+ LINE

Cyber Security News



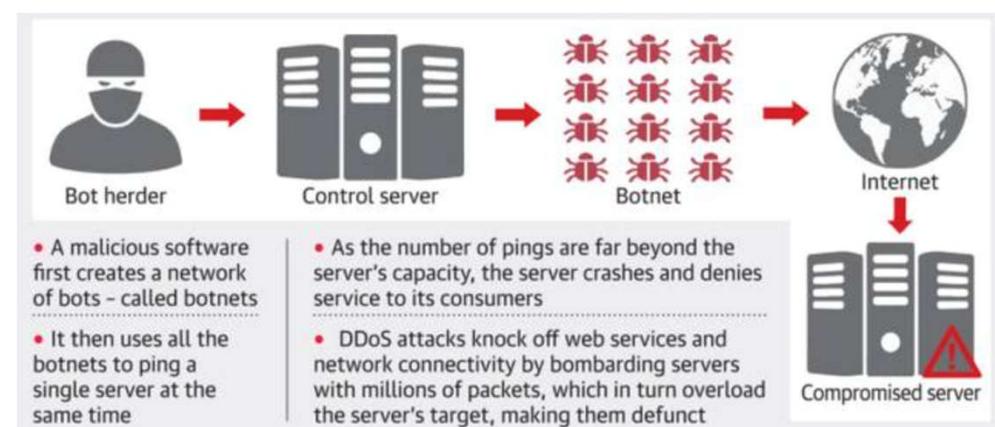
CyberAttack: SberBank - Сбербанк: 8th Nov 2016



**Massive DDoS Attack from 24,000 "Bot" Devices (Internet of Things)
Hits SberBank, Alfa Bank, Moscow Bank, RosBank, Moscow Exchange
- Peak Web IP Requests of 660,000/Sec quoted by Kaspersky Labs -**

โดยเป็นการส่งคำสั่งไปยัง Server จำนวนมากครั้งเพื่อทำให้ระบบทั้งหมดเข้าสู่สถานะ Offline จากนั้นแยกเกอร์เดินเข้ามาสู่ระบบเก็บข้อมูลไปอย่างง่ายดาย

ธนาคารรัสเซียถูกโจมตีทางไซเบอร์ครั้งใหญ่ ซึ่งธนาคาร 5 รายใหญ่ในรัสเซีย ได้แก่ ธนาคาร Sberbank, Alfa-Bank, Bank of Moscow, Rosbank และ Moscow Exchange ตกเป็นเป้าหมายสำคัญของ Botnet โดยพบว่าการโจมตีดังกล่าวมาจากการอุปกรณ์จาก 30 ประเทศ เช่น สหรัฐอเมริกา อินเดีย เป็นต้น ซึ่งการโจมตีดังกล่าวมาในรูปแบบของ DDoS Attack



Cyber Security News



Top Democrat's emails hacked by Russia after aide made typo, investigation finds

In the run-up to the US election, aide to John Podesta spotted phishing email but flagged it as 'legitimate' instead of 'illegitimate'



สหราชอาณาจักรล่าวหารัสเซียว่าแทรกแซงการเมืองประเทศไทยในข่าวระดับโลก เมื่อสำนักงานผู้อำนวยการข่าวกรองแห่งชาติของสหราชอาณาจักรกล่าวว่าผู้นำของประเทศไทยที่ถือว่าเป็นศัตรูกันสหราชอาณาจักรมาช้านานได้สั่งการให้แฮกเกอร์โจกรัฐมีเมลของคณะกรรมการพรรคเดโมแครต (ดีเอนซี) และส่งไปให้วิกิลีกส์เผยแพร่ เพื่อช่วยให้โดนัลด์ทรัมป์ ตัวแทนพรรครีพับลิกันอยู่ในสถานการณ์ได้เปรียบเหนือ希ลารี คลินตัน ตัวแทนจากฝ่ายเดโมแครตในการเลือกตั้งชิงตำแหน่งประธานาธิบดีสหราชอาณาจักร ซึ่งการเผยแพร่ข้อมูลดังกล่าวมีส่วนทำให้ทรัมป์ชนะการเลือกตั้งที่ผ่านมาสำหรับวิธีการนั้นทางสหราชอาณาจักรไม่ได้ออกมาเปิดเผยรายละเอียดใดๆ

Cyber Security News



ภาพจาก <https://www.learnliberty.org/speakers/edward-snowden/>

Edward Snowden หนุ่มชาวอเมริกันที่ออกมายเปิดเผยความลับของประเทศตัวเองให้ทั่วโลกรับรู้ว่าหน่วยงาน NSA ของสหรัฐอเมริกาได้มีการแอบลักลอบข้อมูลการประชุมต่างๆทั่วโลกซึ่งเป็นการกระทำที่ขัดต่อหลักกฎหมายอย่างสิ้นเชิงประชาชนอเมริกันไม่เห็นด้วยกับการกระทำการดังกล่าว เพราะทำให้ประเทศของตนเสียหาย แต่ในทางกลับกันทั่วโลกกลับให้ความสำคัญเพราสหรัฐอเมริกาสามารถสอดแนมได้ถึงระดับข้อมูลบุคคลเกือบทุกประเทศทั่วโลกนอกจากนี้ยังสอดแนมในเรื่องธุรกิจซึ่งเป็นการเอาเปรียบคู่แข่งทางการค้าด้วยที่เห็นได้ชัดคือการดักฟังข่าวสารในการประชุมสุดยอดของ EU และถึงขึ้นมีการวางแผนอุปกรณ์ดักฟังในห้องทำงานส่วนตัวของผู้แทน EU ในสหประชาชาติซึ่งทำให้ประเทศสมาชิกสหภาพยุโรป EU หรือพันธมิตรทางการค้าของสหรัฐอเมริกาเกิดความไม่พอใจเป็นอย่างมากจากเรื่องที่เกิดขึ้น



Cyber Security News



ATM ธนาคารออมสินประเทศไทยโดนขโมยเงินกว่า 12 ล้าน การโจมตีนี้เรียกว่า ATM Jackpotting ซึ่งอาศัยช่องโหว่ของซอฟต์แวร์ภายในตู้ ATM ปล่อยมัลแวร์เข้าไปหลอกเครื่องว่ากำลังมีคนกดเงินทำให้เครื่องจ่ายเงินออกมา ซึ่งแฮกเกอร์ต้องอาศัยระยะเวลาในการรอให้เงินออกมาเรื่อยๆ และต้องทำมากกว่า 1 ตู้ถึงจะได้เงินจำนวน 12 ล้านบาท ซึ่งธนาคารใช้บริการตู้ ATM จากหลายแบรนด์ แต่ในกรณีนี้เป็นตู้ของบริษัท NCR เพียงอย่างเดียว หากมองในแง่ดีเหตุการณ์ในครั้งนี้ทำให้คนไทยหันมาใช้ใจเรื่องซีเคียวริตี้มากขึ้น

Cyber Security News



หนุ่มประดับยนต์โดนแฮกเกอร์หลอกเอาเงินจากบัญชี เรื่องนี้เกิดขึ้นในประเทศไทยซึ่งวิธีการของมิจฉาชีพนั้นได้ปลอมตัวเป็นลูกค้าแล้วใช้รหัสกลในการขอเลขบัตรประชาชนจากเหยื่อจากนั้นนำข้อมูลไปเปลี่ยนแปลงกับเครือข่ายโทรศัพท์ ซึ่งเครือข่ายโทรศัพท์เองก็มีความผิดที่ยอมให้มิจฉาชีพเปลี่ยนแปลงข้อมูลต่อกันนั้นได้ใช้รหัสขอให้เหยื่อสมัคร K-Cyber Banking ซึ่งเป็นบริการแอพพลิเคชันด้านการเงินของธนาคารกรุงไทย ต่อมามิจฉาชีพจึงใช้ข้อมูลส่วนตัวของเหยื่อที่ได้มาล็อกอินเข้าในแอพพริเคชันแล้วโอนเงินไปอย่างง่ายดายเหตุการณ์นั้นทำให้เกิดความตื่นตระหนกอย่างมากในไทย ซึ่งทำให้หลายคนหมดความเชื่อมั่นในระบบดิจิทัล

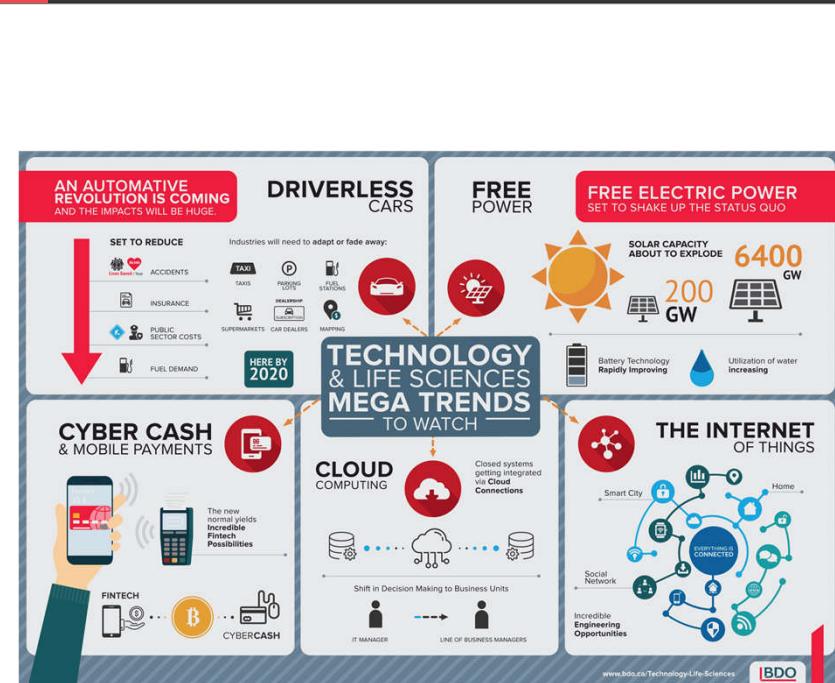
Cyber Security News



นักวิจัยด้านความปลอดภัย **Niall Merrigan** ได้ให้ออกมาเปิดเผยเหตุข้อมูลรั่วไหลที่สร้างความสยองแก่ชาวสยามรับส่งงานต์กับสำนักข่าว [TheRegister.co.uk](https://www.theregister.co.uk) ไว้ว่า เขายังแจ้งรายละเอียดแก่ **TrueMove H** และ แต่เมื่อ恩เครือขยายโทรศัพท์ชื่อดังไม่ได้ตอบสนองอะไรที่เป็นขึ้นเป็นอันตามที่เขาต้องการเท่าไร โดยเขายกบัญชีกข้อมูลกว่า 46,000 รายการขนาดรวมกว่า 32GB ซึ่งเต็มไปด้วยข้อมูลส่วนตัวของลูกค้าทรูมูฟที่สำคัญทั้งสิ้นอย่างรูปสำเนาบัตรประชาชน, ใบขับขี่, หรือแม้แต่พาสปอร์ตหลุดอยู่ในสตอเรจบนคลาวด์ [Amazon S3](https://www.amazon.com) ที่เข้าถึงได้แบบสาธารณะ

ข้อมูลจาก <https://www.enterpriseitpro.net/true-s3-amazon-data-leak/>

คาดการณ์เหตุการณ์ในปี 2561



ข้อมูลจาก ETDA: <https://www.etda.or.th/content/cybersecurity-predictions-2018-by-symantec.html>

คุณคือเป้าหมายของ แฮกเกอร์

You are the Target!



Digital Currency
เป็นแหล่งชุดเงิน
ชน้อยเงิน



Mobile
เป็นแหล่งชุดเงิน
ยืดเครื่อง



IoT
เป็นแหล่งชุดเงิน
และโจมตี DDoS

รับมือกับภัยคุกคามด้านไซเบอร์อย่างไร



ปฏิบัติตามนโยบายด้านความปลอดภัยฯ

องค์กร/หน่วยงาน มีการลงทุนติดตั้งอุปกรณ์รักษาความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ เพียงเราปฏิบัติตามนโยบาย ก็ลดความเสี่ยงที่จะได้รับผลกระทบจากภัยคุกคามต่างๆแล้ว



ไม่กระทำเรื่องสุ่มเสี่ยง

ป้องกันตนเองได้ โดยไม่ต้องพึ่งมืออาชีพ



ไม่ใช้โปรแกรมละเมิดลิขสิทธิ์

โปรแกรมละเมิดลิขสิทธิ์ โดยส่วนใหญ่ มักมาพร้อมกับ ของแడม เช่น ไฟล์อันตราย (Malware virus) หลอกเลี้ยงโปรแกรมที่แชร์อยู่ในแหล่งที่ไม่น่าเชื่อถือ เช่น Torrance ต่างๆ



ไม่เข้าเว็บไซต์พิดภูมาย

บ่อยครั้งเว็บประเภทนี้ จะหารายได้จากการเข้าใช้งานเว็บ ของ คนที่เข้าไป เช่น การแอบใช้งานเครื่องทำการขุด BitCoin หรือ หลอกให้ลงโปรแกรม ซึ่งมาพร้อมกับไฟล์อันตราย



ตั้งรหัสผ่านให้เหมาะสม

หลายครั้งมักพบว่า ผู้ใช้งานในโลก Internet มักตั้งรหัสที่คาดเดาได้ง่าย เช่น ตั้งตามชื่อตอนเอง ชื่อลูก เบอร์โทรศัพท์



ไม่เปิดเผยข้อมูลทุกอย่างลงโลกโซเชียล

รู้หรือไม่ว่า ข้อมูลหลายอย่างในโลกโซเชียล เช่น วันเดือน ปีเกิด สถานที่เกิด สถานที่เรียน มักนำมาใช้ในการเดารหัสผ่าน หรือใช้ในการขอตั้งรหัสใหม่ในบางเว็บได้

ตั้งรหัสผ่านให้ปลอดภัยได้อย่างไร



คาดเดาได้ยาก แต่ต้องจำได้ง่าย
นี่คือ หัวใจสำคัญของการตั้งรหัสผ่านที่ดี



- ความยาว 8 ตัวอักษรขึ้นไป
- ประกอบด้วย ตัวอักษรพิมพ์เล็ก/ใหญ่ ตัวเลข อักษรพิเศษ
- ไม่ใช้ชื่อ เบอร์โทรศัพท์ เป็นรหัสผ่าน

เปลี่ยนรหัสผ่านอย่างสม่ำเสมอ

อย่างน้อยคราวเปลี่ยนทุกๆปี หรือเปลี่ยนทันทีที่สงสัยว่าบัญชีผู้ใช้ถูกแอบน้ำไปใช้



- เปลี่ยนทุก 3 เดือน
- หากเป็นผู้ดูแลระบบ ให้เปลี่ยนทุก 2 เดือน

ไม่ใช้รหัสเดียวกันกับทุกระบบ

วิธีการนี้ช่วยลดความเสี่ยงจากการทำงานของระบบบางตัวที่มีช่องโหว่ หรือไม่มีการป้องกันที่เหมาะสม

มีรหัสผ่านหลายระบบ จึงไม่ได้ใช้โปรแกรมเฉพาะช่วยจำ ปัจจุบันมีโปรแกรมช่วยจัดเก็บรหัสผ่าน เพื่อใช้บันทึกรหัสผ่านระบบต่างๆ ให้ไว้ในฐานข้อมูลที่มีการเข้ารหัส

ใช้คู่กับระบบ 2FA/MFA (ยืนยันตัวตนด้วย 2 วิธีการขึ้นไป)

ระบบสำคัญๆในปัจจุบัน มักออกแบบระบบให้รองรับฟังก์ชันการทำงานนี้ ด้วย เช่น การใส่ OTP การใส่รหัสพิเศษที่ได้จากrangle

ตั้งรหัสผ่านให้ปลอดภัยได้อย่างไร



https://www.youtube.com/watch?time_continue=91&v=aEmF3Iylvr4

ตั้งรหัสผ่านให้ปลอดภัยได้อย่างไร

สิ่งที่ไม่ควรทำอย่างยิ่ง



เดาง่าย

กลุ่มรหัสผ่านที่ถูก Hack ได้สูงสุดในปี 2017

- 123456
- Password
- 12345678
- qwerty
- 12345
- 123456789
- letmein
- 1234567
- football
- iloveyou
- admin
- welcome
- monkey
- login
- abc123
- starwars
- 123123
- dragon
- passw0rd
- maste
- hello
- freedom
- whatever
- qazwsx
- trustno1



รหัสผ่านของเรารวหรือไม่? เช็คได้



[Home](#) [Notify me](#) [Domain search](#) [Who's been pwned](#) [Passwords](#) [API](#) [About](#) [Donate](#)

';-have i been pwned?

Check if you have an account that has been compromised in a data breach

email address pwned?

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?

300	5,371,008,023	76,212	83,050,497
pwned websites	pwned accounts	pastes	paste accounts

<https://haveibeenpwned.com>

เว็บไซต์ที่ทำการรวบรวมชื่อ email ที่เคยมี hacker ทำการ hack หรือมีข่าวว่าระบบมีช่องโหว่ และข้อมูลการเข้าระบบรั่วออกสู่สาธารณะ เช่น yahoo.com, adobe, Drop Box.

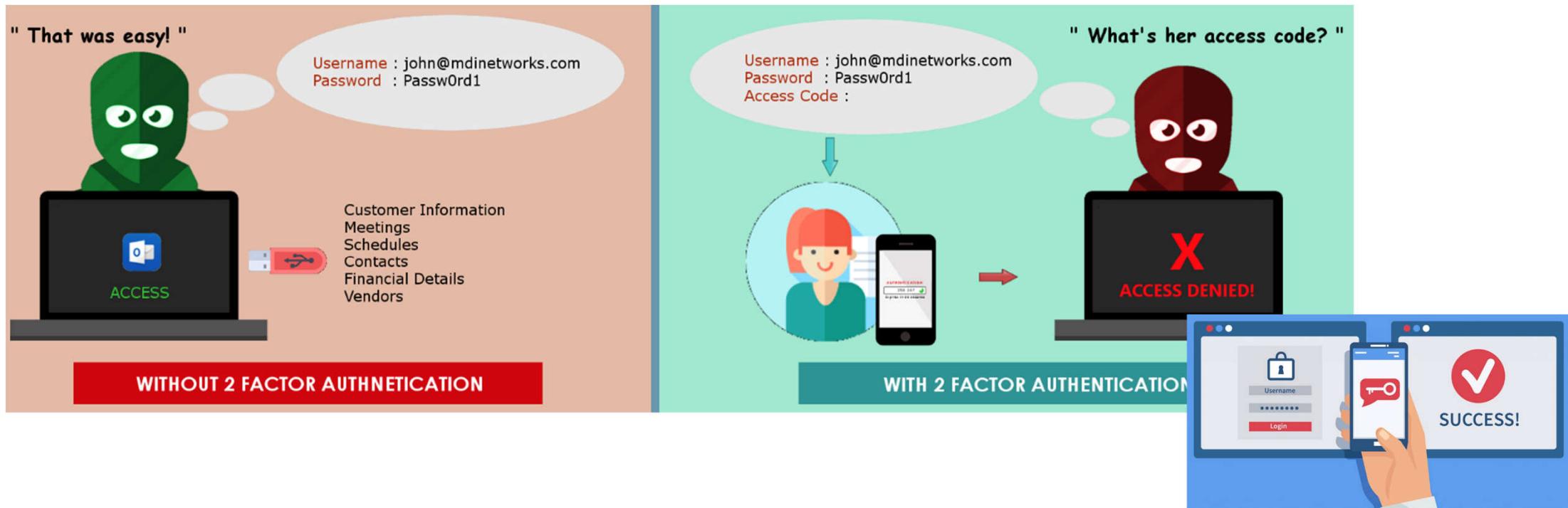
ตั้งรหัสผ่านให้ปลอดภัยได้อย่างไร

การยืนยันตัวตนร่วมกับ 2FA/MFA



การยืนยันตัวตนร่วมกับเทคนิค 2FA/MFA (2 Factor Authentication / Multi Factor Authentication)

2FA/MFA หรือ จำง่ายๆ ก็ชื่อว่า เทคนิคการยืนยันตัวตนด้วยวิธีการ 2 วิธี



ຕິ່ງຮໍສຳຜ່ານໄທ້ປລອດກໍຍໄດ້ຍ່າງໄວ

ກາຣຢືນຍັນຕົວຕະນະມັກ 2FA/MFA



Security and Login > Two-Factor Authentication

Add Extra Security With Two-Factor Authentication

Add extra security to your account every time you log in on a phone or computer we don't recognize.

[Get Started](#)

How Two-Factor Authentication Works

Extra Protection

We'll ask for your password and then a login code any time we notice an unusual login.

Through SMS or an Authentication App

We'll send a text message with a login code, or you can use a security app of your choice.



Login Approval Code

[Continue](#)

[Go Back](#)

ตั้งรหัสผ่านให้ปลอดภัยได้อย่างไร

การยืนยันตัวตนร่วมกับ 2FA/MFA



Google

2-step verification

Help keep the bad guys out of your account by using both your password *and* your phone.



[Get Started](#)

2-step verification adds an extra layer of security to your Google Account

In addition to your username and password, you'll enter a code that Google will send you via text, voice call, or our mobile app.

รู้ทันกลโงง

ป้องกันตนเองได้ โดยไม่ต้องพึ่งมืออาชีพ



หลอกขายของ

ปัจจุบันพบได้บ่อยครั้งใน Facebook บาง Page เปิดเพจนานกว่า 1 ปี



Social Engineering

เป็นการหลอกด้วยเทคนิคต่างๆ เช่น โทรศัพท์ติดต่อไปหาเหยื่อ เพื่อให้เหยื่อเข้าใจว่า เป็นการติดต่อจากบริษัทฯ จากนั้นหลอกขอข้อมูลบางอย่าง



Phishing email

อีเมล์หลอกลวง เป็น 1 ในกลุ่มด้าน Social Engineering ผู้โจมตีมักส่งอีเมล์โดยใช้ชื่อและเนื้อหา เมล์หลอกให้ผู้อ่านเข้าใจว่า เป็นบริษัทปลายทางจริง เพื่อหวังผลบางอย่าง เช่น ขโมยรหัสผ่านในการเข้าใช้งานระบบ หลอกขอหมายเลขบัตรเครดิต ติดตั้งไวรัสเรียกค่าไถ



เว็บผี / ชื่อเว็บ偽冒充 website

หลายครั้งมักพบว่า ผู้ใช้งานในโลก Internet มักตั้งรหัสที่คาดเดาได้ง่าย เช่น ตั้งตามชื่อตนเอง ชื่อลูก เบอร์โทรศัพท์

หลอกขายสินค้าราคาพิเศษ

Facebook



#แฟลชไดร์ฟ
แฟลชไดร์ฟ2TB เทคโนโลยีใหม่ล่าสุดจากомерิกา ชิปหน่วยความจำSLC
ความเร็วในการอ่านและเขียนสูงถึง200M
ใช้เทคโนโลยีใหม่ล่าสุดของชิลิคอนวัลเลอร์
"Flash electronic external storage method" ... See More

แฟลชไดร์ฟ2TB(2048GB)

HTTP://UBOARD.UNNEYI.COM/
แฟลชไดร์ฟ2TB เทคโนโลยีใหม่ล่าสุดจากомерิกา ชิปหน
ราคามาเดิม 5999 บาท ตอนนี้ราคาพิเศษเพียง 1198บาท , ชั้น 1 แ...

Jiran-Shopping
Sponsored • 4
☀️ [ราคาพิเศษ] [Gear S3]
เพียง 1088 บาทเท่านั้น !!!
กิจกรรมนี้มีเพียงเดือนเท่านั้น
500 ตัวสุดท้าย จำกัด เวลาสิ้นเชือ
ลูกค้าที่สั่งซื้อ 50 คนแรกลด 50% 🎉 ... Continue
Reading

GEARS3.MAGICQW.COM
[Gear S3] การดูแลสุขภาพของคุณ
smart watch

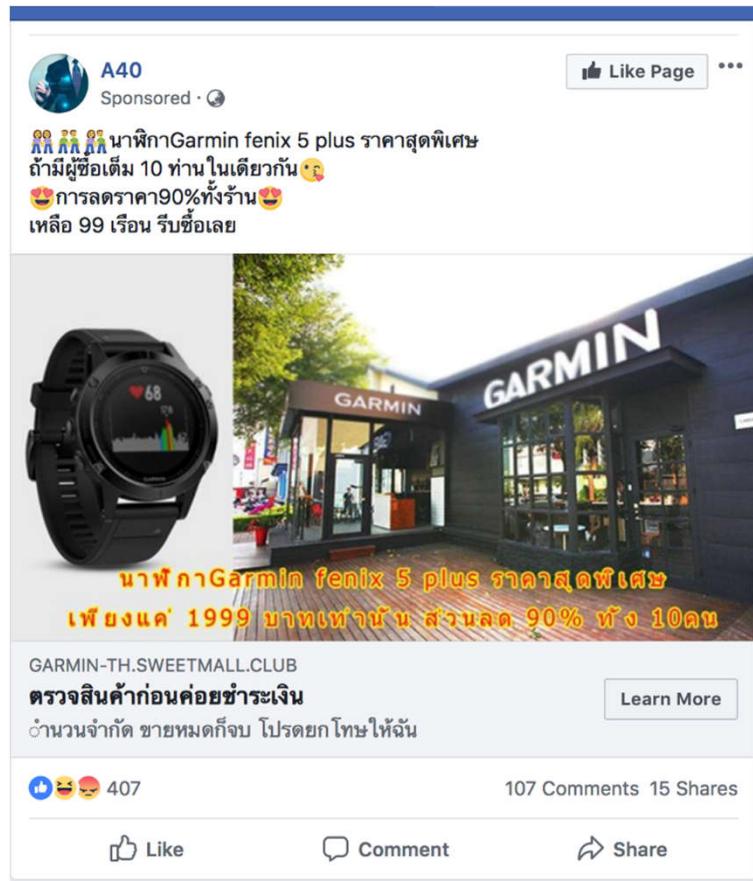
151 Comments 18 Shares
6.6K Like Comment Share

PSGAME.THSHOPTECH.COM
คุณโชคเกมใหม่ PSV2000
ลดราคาอยู่

Learn More

หลักขายสินค้าราคาพิเศษ

Source: Facebook



เพื่อนโคนหลอกมาแล้ว 😞 😞 😞

Like · Reply · 7h

หลอกกันเห็นๆ 555

Like · Reply · 8h

รับสั่งเลยครับ ถูกแบบนี้ มีเจ้าเดียว 2หมื่นเหลือสองพัน

Like · Reply · 3h

โครงสร้างต้องซื้อไปจากชาеля้ว

Like · Reply · 8h

สั้งลักษ์ 20 เรือนครับ

Like · Reply · 3h

ชั่วร์ป่าว

Like · Reply · 1h

เทคนิคการหลอก และการสั่งเกตุ

Source: Facebook



A40
Sponsored · ๔๐
นาฬิกาGarmin fenix 5 plus ราคาสุดพิเศษ
ถ้ามีผู้ซื้อเต็ม 10 ท่านในเดียวันนี้
การลดราคา90%ทั้งร้าน🎉
เหลือ 99 เหรียญ รับซื้อเลย

นาฬิกาGarmin fenix 5 plus ราคาสุดพิเศษ
เพียงแค่ 1999 บาทเท่านั้น ส่วนลด 90% หัง 10คน

GARMIN-TH.SWEETMALL.CLUB
ตรวจสอบสินค้าก่อนค่อยชำระเงิน
จำนวนจำกัด ขายหมดก็จบ โปรดยกโทษให้ฉัน

Like Page Learn More

407 107 Comments 15 Shares

Like Comment Share



สินค้าจำนวนจำกัด

มักจะโฆษณาชวนเชื่อ ว่าสินค้าหลุดจากโรงงาน หรือ มีปัญหากับบริษัทฯ
เจ้าของสินค้า หรือ ช่วงเวลาพิเศษ ได้สินค้ามาจำนวน XX ชิ้นเท่านั้น



ราคาพิเศษ

ราคานี้ขายมักลดลงมากกว่า 50% บางรายการอาจจะถึง 90% สามารถ
จ่ายเงิน เมื่อสินค้ามาส่งที่บ้านได้



Website ปลายทาง เป็นเว็บไม่ได้จดทะเบียน

เว็บที่เข้าไปสั่งซื้อสินค้า จะไม่ใช่เว็บเจ้าของสินค้านั้นๆ แต่จะเป็นเว็บร้านค้า
และไม่ใช่เว็บดัง

อีเมล์หลอกลวง Phishing email



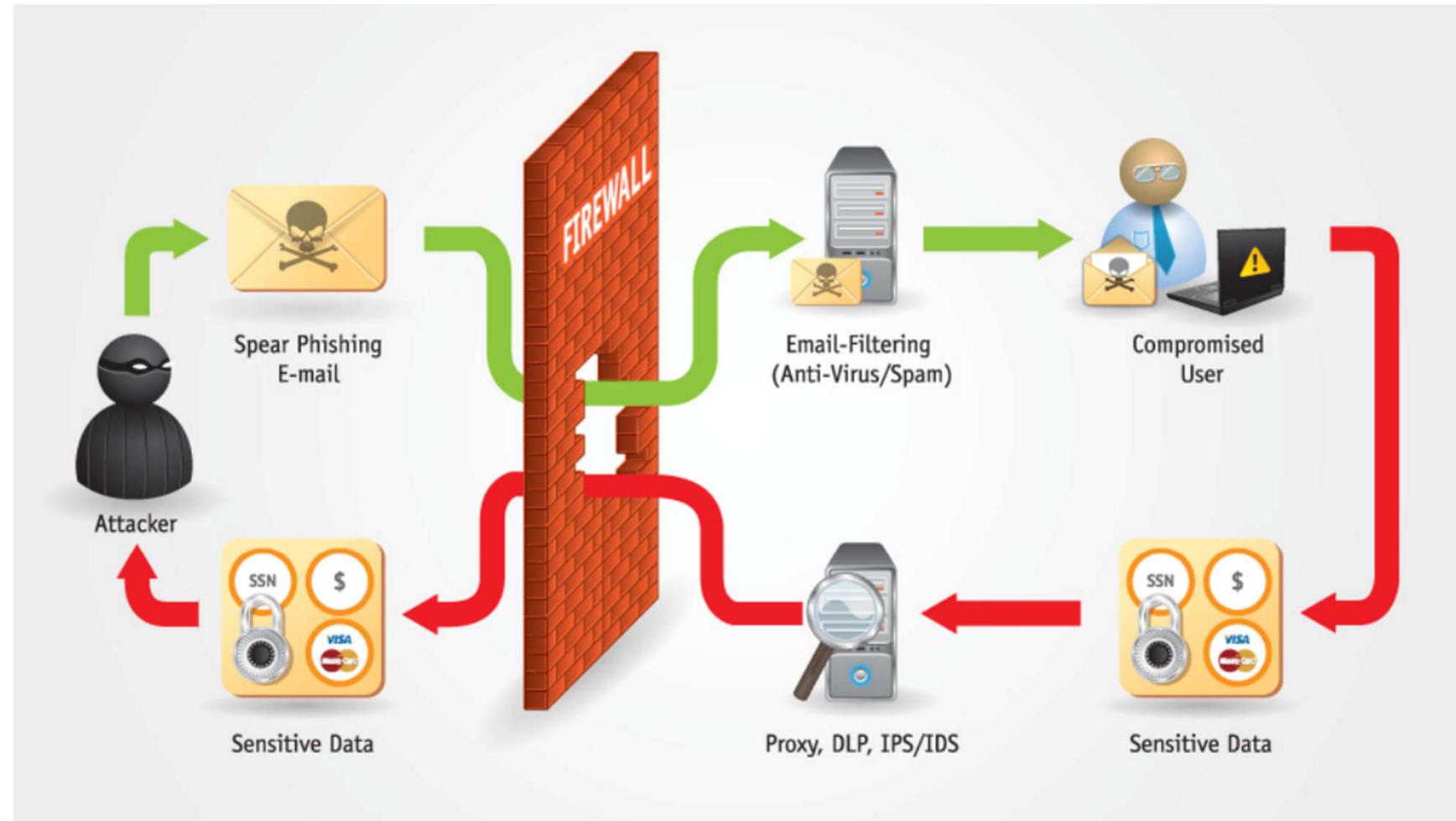
Phishing เป็นรูปแบบหนึ่งของการทำ Social Engineering ซึ่งเป็นเทคนิคการหลอกลวงโดยใช้จิตวิทยาผ่านระบบคอมพิวเตอร์ มักมาในรูปของอีเมลหรือเว็บไซต์เพื่อหลอกให้เหยื่อเผยแพร่องุลความลับต่างๆ เช่น รหัสผ่านหรือหมายเลขบัตรเครดิต เป็นต้น รวมไปถึงหลอกล่อให้เหยื่อ กดลิงค์เพื่อแอบติดตั้งมัลแวร์ลงบนคอมพิวเตอร์โดยที่เหยื่อไม่รู้ตัว



อีเมล Phishing ส่วนใหญ่มักมาในรูปของประกาศแจ้งจากทางธนาคาร หรือจากเว็บ Social Media เช่น Facebook หรือ Twitter เป็นต้น โดยเนื้อหาส่วนใหญ่จะระบุประมาณว่า ชื่อบัญชีของท่านมีปัญหาหรือหมดอายุ จำเป็นต้องอัพเดทชื่อบัญชีใหม่ ให้กดลิงค์ตามที่แนบมาเพื่อกรอกข้อมูล ซึ่งลิงค์ดังกล่าวไม่ได้เชื่อมโยงไปยังหน้าเว็บไซต์ทางการของธนาคารหรือ Social Media แต่อย่างใด แต่จะเป็นเว็บไซต์ที่แฮกเกอร์ปลอมขึ้นมา เพื่อให้คล้ายคลึงกับเว็บไซต์ต้นฉบับ ผู้ใช้ที่ไม่สังเกตถึงความผิดปกติ ดังกล่าวและผลกรอกข้อมูลส่วนตัวลงไป ข้อมูลเหล่านั้นก็จะตกสู่มือของแฮกเกอร์โดยทันที

อีเมล์หลอกลวง Phishing email

ทำไม Hacker ถึงนิยมใช้



ประเภทของการหลอก



PHISHING

The use of email 'lures' to try and entice unsuspecting victims to disclose private information



SPEARPHISHING

A highly targeted phishing attack targeting a specific group of individuals or organization



WHALING

A spear phishing attack focused on 'bigger fish' such as high ranking public or executive figures



SMISHING

Phishing SMS messages sent to smartphones



VISHING

Where an attacker phones the victim

เทคนิคการหลอก และการสั่งเกตฯ

ตรวจจับ Phishing ได้อย่างไร



From : Alertbank@Email.com
To : Sam@email.com

Dear Customer

We need you to verify your account information for your online banking to be re-activated.

Personal Detail

Name - Lastname
Birthdate
Tel.
Password

We've locked your account and **you have 24 hours to verify it.**

Click link to update your account

Click Link
<https://www.alertbank.com>

https://12.345/abank/

1. Email ก่อภัยผู้ส่งไปใช้ก่อภัยผู้คิด แรกกอร์จะใช้ก่อภัยอีเมล์ที่สร้างขึ้นเอง จึงไม่ใช้ชื่ออีเมล์ขององค์กร
2. ข้อต้นด้วยคำว่า “API” แยกกอร์ไม่ทราบบุลของเรางานทำให้ไม่สามารถเจาะจงชื่อผู้รับเอกสารใด
3. ขอพาสวอร์ดและข้อมูลส่วนตัว โดยปกตินาการส่วนนี้ใหญ่จะมีการขอข้อมูลส่วนตัวของลูกค้า ผ่านทางเว็บไซต์
4. ให้รับตอบกลับอย่างรวดเร็ว หรือบางที่ก็อยู่ในลักษณะขั้นชั้น เพื่อให้ผู้ใช้กดเข้าและรับตอบกลับไป
5. Link ที่แบบมาไม่ตรงกับที่อยู่ Link จริงๆ เอาเมาส์ซี้ไปกี Link เพื่อดูว่าอยู่จริงๆ ของ Link นั้น



หากคุณถูก Spear Phishing
เทคนิคในการสั่งเกต ให้คุณ
เพิ่มเติมรายละเอียดด้านล่างนี้

พิจารณารายละเอียดที่ได้รับ

หากโดยปกติแล้ว คุณไม่เคยติดต่อกับผู้ส่งอีเมล์นี้มาก่อนหรือลักษณะการติดต่อ มีความผิดสังเกต เช่น ภาษาที่ใช้ ไม่ใช้รูปแบบที่สื่อสารกันเป็นประจำ ให้คุณทำการติดต่อไปที่บุคคลนั้นๆ โดยตรง ไม่ติดต่อตาม Contact ที่แสดงอยู่ในเนื้อหาของอีเมล์ เพราะ Hacker อาจมีการแก้ไขรายละเอียดบางอย่าง



ตัวอย่างเทคนิคการเช็ค Phishing mail

Sun 4/12/2015 11:55 AM

Internal Revenue Service <office@irs.gov>

[!!Spam KSE]Payment confirmation for tax refund request # 75991792

To [REDACTED]

Attachments: [confirmation_75991792.doc](#) (58 KB); [ATT00001.txt](#) (236 B)

Dear taxpayer,

You are receiving this notification because your tax refund request has been processed. Please find attached a copy of the approved 1040A form you have submitted, containing your personal information. On the last page, you can also find the wire transfer confirmation from the bank.

Transaction type : Tax Refund
Payment method : Wire transfer
Amount : \$7592
Status : Processed
Form : 1040A

Additional information regarding tax refunds can be found on our website: <http://www.irs.gov/Refunds>. Please note that IRS will never ask you to disclose personal or payment information in an email.

Regards,
Internal Revenue Service
Address: 1111 Constitution Avenue, NW
Washington, DC 20224
Website: <http://www.irs.gov>
Phone: 1-800-829-1040

Google search results for "payment confirmation for tax refund request"

About 2,640,000 results (0.51 seconds)

Payment confirmation for tax refund request # ... - Malware
<https://techhelplist.com> › Spam list ▾
Apr 16, 2015 - Email: Fake IRS virus spam email claims your tax refund request has been processed and a copy is attached. You are receiving this notification because your tax refund request has been processed. On the last page, you can also find the wire transfer confirmation from the bank.

Payment confirmation for tax refund request (IRS.gov) | Computing ...
<https://it.brown.edu/alerts/read/payment-confirmation-tax-refund-request-irsgov> ▾
Apr 17, 2015 - Payment confirmation for tax refund request (IRS.gov) Dear taxpayer, You are receiving this notification because your tax refund request has been processed. Please find attached a copy of the approved 1040A form you have submitted, containing your personal information and signature.

Payment confirmation for tax refund request # 3098-2344342 – word ...
<https://myonlinesecurity.co.uk/payment-confirmation-for-tax-refund-request-3098-23...> ▾
Apr 16, 2015 - Carmen Rodriguez RECEIPT – word doc or excel xls spreadsheet malware. ... This email has what appears to be a genuine word doc or Excel XLS spreadsheet attached which is malformed and contains a macro script virus. ... You are receiving this notification because your tax refund ...

ตัวอย่าง Phishing mail



Dear Citibank member,

Due to database operations some online banking accounts and credit cards can be lost. We have to ask you to confirm your online banking or credit card information.

Please follow the link below and submit required information:

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

Thank you
Please do

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



Dear Esteemed Customer,
At Kasikorn Bank Thailand, We take security Seriously. You are receiving This Email as you are a customer with Kasikorn Bank.

Your Account has been flagged for security issues, you must now login and validate your account for your own protection.

[Click here to login and validate your Account](#)

This Email is subject to security From Kasikorn Bank, Please view our privacy policy statement.

Please don't click any link in the phishing e-mail.

Regards,
Technical Service /Internet security,
Kasikorn Bank,
Thailand

Kasikorn Bank © 2012 All Rights Reserved

[Redacted]

TMB
TMB BANK PUBLIC COMPANY LIMITED
3880 PHRAHON YOTHIN ROAD, CHATUCHAK 10900
BANGKOK, THAILAND
SWIFT CODE: TMBKTHBK
E-MAIL: TRANSFER@TMB-THAI.COM
TELEPHONE: (+66-81-629162) (+66-81-6291699)

[RE: PAYMENT AUTHORIZATION AND MEGA MILLIONS BANK DRAFT APPROVAL NOTIFICATION](#)

Attention: Valued Customer,
Hossein Heydari,

SIR, Thank you for your message!

You are welcome to TMB Bank Public Company Limited, we are happy to have you as one of our numerous customers all over the world that uses our advanced Banking services. TMB Bank PLC, is a result bank in the Thailand that has been part of the Bank of Thailand Group Plc since 2000. Traditionally considered one of the major clearing banks, TMB has a large network of 1,600 branches and 3,400 cash machines across Thailand and offers 24-hour telephone telephones and online banking services.

We have received your winning application form and payment application documents from the British Mega Millions Lottery Office, however we are set to verify your eligibility status and commence processing of your fund transfer.

Please print-out and complete the attached [Foreign Exchange Draft Transfer Application Form \(CV-12\)](#) and return the completed copy of your bank account information for verification and transfer of your won prize sum of Four Hundred and Fifty Thousand United States Dollars Only (\$450,000.00 USD). Deposited in our bank by the British Mega Millions Lottery Company.

[Complete Bank Details for Wire Transfer](#)

1. Name of Your Bank
2. Name of Account Holder
3. Address and Phone number of Account Holder

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

3 ขอพิเศษ์ด้วยและข้อมูลส่วนตัว

Sincerely,

Mr. Rajit Supinit | Distributor-West
(Foreign Exchange Operations)
TEL: (+66) 919 688102
MO: (+66) 081 18 3888
© 2012 All Right Reserved
TMB 1558

តែវិយោង Phishing mail



Most bestest Contents for u

Hi sir

I am from content article marketing company to give you deal
of only 3,50\$ USD per 500 words of article. We are na
speakers to delivery fast response of orders. We have
discount for you to order more contents for cheap.

Plz reply with order details.

We wait for you sir.

From: [REDACTED]
Date: 2014-10-13 19:50
To: [REDACTED]
Subject: RE: [REDACTED]

we are interested to buy your product from your company
we are interested to buy your product from your company, kindly quote your best price of the product
in the link <http://productspecification.3owl.com> Please note that Quality is very important to us
because is the secret of our business, click on the link below to see the exact specification of product .
you can also copy and paste on your browser for you to access the
[link http://productspecification.3owl.com](http://productspecification.3owl.com)

Get back to me with your best price and delivery terms of product , feel free to contact me if you have
any more information after you might have seen our specification.

Best Regards
Thank You.
Mrs susan rose
Manage

ตัวอย่าง Phishing mail



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



Dear Paypal valued member,

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

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

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

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

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

Sincerely,
Paypal customer department

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

Wed 10/5/2016 11:21 PM
Microsoft Outlook <msoutlook94@service.outlook.com>
Your Password Has Expired

To

1 2 3 4 5

Password Expired.

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

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

You are now required to [change your password](#) immediately.

Click below to change your password

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

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

ตัวอย่าง Phishing mail



Receipt

APPLE ID		BILLED TO Apple Store	TOTAL \$49.95
DATE	Oct 11, 2017		
ORDER ID	MXJOHL83J1	DOCUMENT NO.	126176719694

iCloud	TYPE	PURCHASED FROM	PRICE
	iCloud: 10 TB Storage Plan Monthly Oct 11, 2017	iCloud Storage	\$49.95
		Subtotal	\$49.95
		Tax	\$0.00
		TOTAL	\$49.95

If you have any questions about your bill, [visit iTunes Support](#). This email confirms payment for the iCloud storage plan listed above. You will be billed each plan period until you cancel by [downgrading](#) to the free storage plan from your iOS device, Mac or PC.

You may contact Apple for a full refund within 15 days of a monthly subscription upgrade or within 45 days after a yearly payment. Partial refunds are available where required by law.

If you did not authorize this purchase, please visit the [Apple Store Cancellation Form](#)

Learn how to [manage your password preferences](#) for iTunes, iBooks, and App Store purchases.

Inbox

From: [iTunes Store](#) > [Hide](#)

Your receipt No.0 [REDACTED]

February 9, 2558 BE at 1:41 PM

Your Apple ID was just used to purchase from the iTunes Store on a computer or device that had not previously been associated with that Apple ID.

This purchase was initiated from Malaysia.

If you made this purchase, you can disregard this email. It was only sent to alert you in case you did not make the purchase yourself.

If you did not make this purchase, we recommend that you go to [apple.validate-id.com](#) to update your Billing address and your card information.

Regards,
Apple

TM and Copyright © 2015 Apple Inc. [1 Infinite Loop, Cupertino CA 95014, United States](#).
[All rights reserved](#) / [Keep Informed](#) / [Privacy Policy](#) / [My Apple ID](#)

ภาพจาก @noonohnoon

Phishing Test

มาจับผิดอีเมลกัน



Someone Has Your Password
Service Customer to: chanyut_l

From:
To:

Service Customer <Paypal-secureupdate-service@freeshare.link>
You abc

PayPai

Dear Value Customer,
Urgent Notice!

Are you in New Zealand? We're detected that someone is trying to log in to your account.
address : 161.65.165.255
City : Wellington
Country : New Zealand
If you are not there, please update your data information to secure your account.

- [Update your data information](#)

What to do next:

Please log in to your PayPal account and update your data information before:
November,20 2016.

If we haven't receive the data information until the specified date time, your account will be deactivated temporary until you update your information.

Login To Your Account

http://paypa.my.webshare.es/d/262436m5/dl=0/ac5c48/?login_id=0bb45d74-433a-4826...

E-mail ผู้ส่ง ไม่ตรงกับเนื้อหา/ข้อความใน e-mail
หากเป็นของจริงต้องมาจาก paypal.com

- คำทักทาย ไม่ระบุถึงใครคนใดคนหนึ่ง
- ใช้ข้อความให้เกิดความสับสนหรือเร่งรีบ

**อีนๆ.
ถ้าคุณไม่เคยสมัครใช้งาน PayPal หรือ
ไม่ได้ใช้เมลนี้สมัคร แสดงว่า นี่คือการ
หลอกลวง

ลิงค์ที่จะเข้าไป ไม่ตรงกับเว็บของ
PayPal.com

Phishing Test

มาจับผิดอีเมล์กัน

From: Krungsri Online Services.
<customerservice@krunbsbank.com>
Sent: Thursday, July 12, 2018 9:29 AM
Subject: การยืนยันการเข้าสู่ระบบ SMS

เรียนลูกค้า

ลูกค้า krungsri ทุกคนควรเปิดใช้การยืนยัน sms otp
ในระหว่างการเข้าสู่ระบบบัญชีของตนเพื่อหลีกเลี่ยง
การใช้แฮกเกอร์ที่ไม่ได้รับอนุญาตซึ่งเข้าถึงบัญชี
ลูกค้าโดยไม่ได้รับความยินยอม

เมื่อคุณเปิดใช้งานการตรวจสอบสิทธิ์ OTP สำหรับ
การเข้าสู่ระบบจะไม่มีใครสามารถเข้าถึงบัญชีของ
คุณได้ยกเว้นคุณ

คลิกที่ <https://www.krungsionline.com>
<<https://apac01.safelinks.protection.outlook.com/>
[url=http%3A%2F%2Fbit.do%2Fepoyq&data=02%](http://url%3A%2F%2Fbit.do%2Fepoyq&data=02%)



Michael Lewis <debian@ocn.ne.jp>
Sun 8/5, 9:12 PM

Deleted Items

Hello Friend

My, name is Mr. Michael Lewis. I work with an off shore branch of one of the leading Banks In the UK, I would need your consent to present you as the next of kin to our late customer who died of heart attack in 2009. He was a wealthy business man who deposited a huge amount in our Bank. He died without any registered next of kin as he was long divorced and had no child.

I was his account officer and have in my possession all the documents required to present you as his beneficiary next of kin. I contacted you because you have same name identity with our late client and can perfectly fit in as next of kin, We can work together to claim this fund. Please listen, this is real and goes on in Banks all over the world without people knowing. Let us utilize this opportunity because it does not come always. A lot of customers open private accounts with different Banks without the knowledge of their families and at their demise or in an event of death or accident such money will be lost to the Bank unless someone makes a claim of it. This is how a lot of Bank Directors make so much money silently.

On your confirmation of this message and indicating your interest, I will furnish you with more details. Please endeavor to provide me with the following so that we can discuss in details

(1) mobile phone numbers
(2) full name
(3) contact address and occupation I urgently hope to get your response as soon as possible.

Yours Sincerely,

Phishing Test

มาจับผิดอีเมลกัน



SCB Credit Card <scbcampaign@mail.scb.co.th>

Thu 8/2/2018 6:20 PM

To: pitbullgroup@hotmail.com ↗

Reply | v

Deleted Items

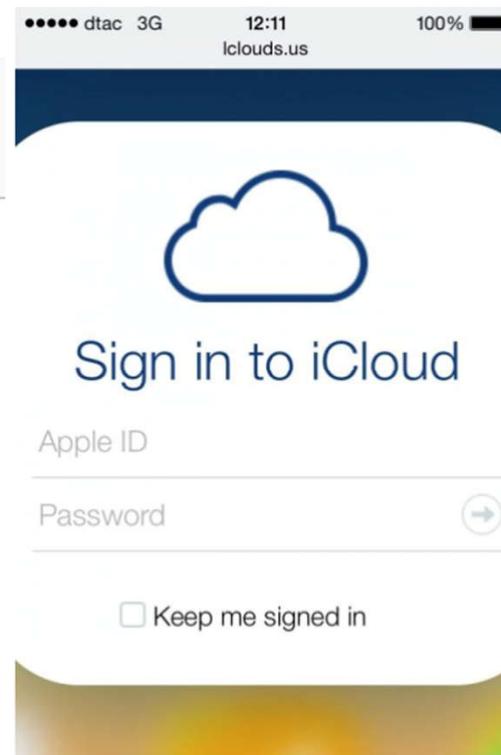
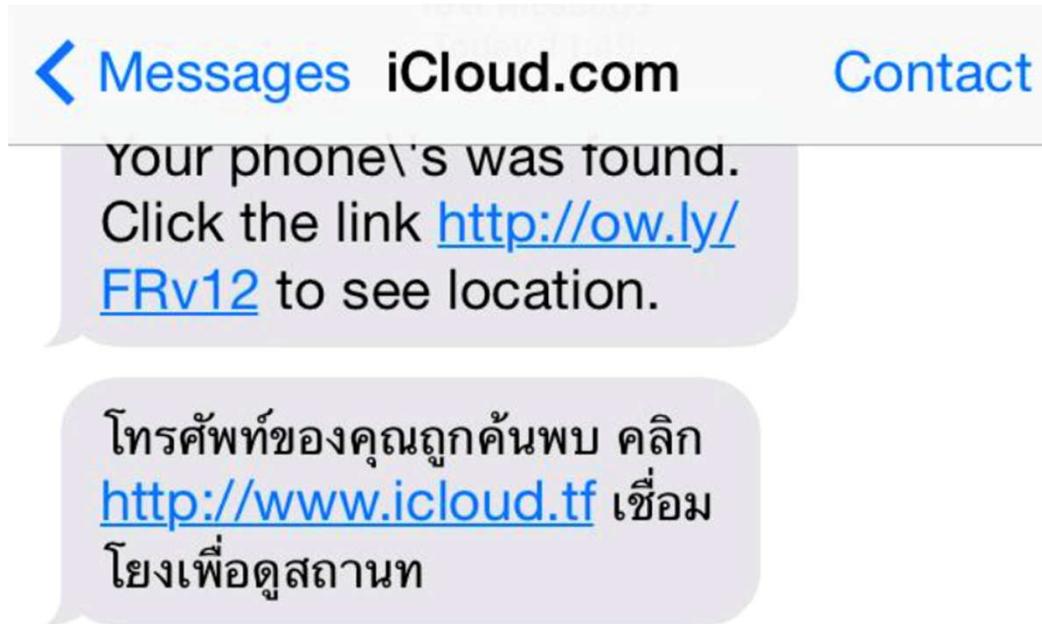
สิงหา พาแม่เที่ยว พักสบาย รับคุ้ม 2 ต่อ กับบัตรเครดิต SCB

The image shows an email header from SCB Credit Card. It features the SCB logo (SCB ไทยพาณิชย์) on the left, followed by the text "SCB Credit Card". Below the header is a large, scenic photograph of a tropical resort. The photo depicts a swimming pool area with several lounge chairs, palm trees, and thatched umbrellas overlooking a clear blue ocean under a bright sky. To the right of the photo, there is promotional text in Thai: "สิงหา พาแม่เที่ยว พักสบาย รับคุ้ม 2 ต่อ" (August, take mom on a trip, stay comfortably, get double value).

ตัวอย่าง Smishing (SMS)

เทคนิคใหม่ของโจรอุโมยมือถือ

ส่ง SMS ไปตามมาถึงเหยื่อที่ถูกโจมตีแล้ว มีคือ พร้อมเลิงค์เพื่อเข้าไปในหน้า iCloud ไปตาม



เทคนิคป้องกัน ไม่ตกเป็นเหยื่อ Phishing



อย่าใจร้อน

ผู้ประสงค์ร้ายมักจะล่อหลอกให้คุณกดลิงค์ หรือ Download ไฟล์ก่อน และคิดทีหลัง โดยใช้ข้อความที่ทำให้คุณเข้าใจว่า ต้องรีบตัดสินใจ เป็นเรื่องเร่งด่วน ต้องทำทันทีทันใด ถ้าเจอข้อความลักษณะนี้ ให้อ่านโดยละเอียด และให้มองไว้ว่ามันอาจเป็น Phishing e-mail

หาความจริง

ถ้า e-mail ดูเหมือนจะถูกส่งมาจากบุคคล บริษัท หรือเว็บไซค์ที่คุณใช้งานอยู่ ให้ใช้ search engine เช่น Google ทำการค้นหาข้อมูลเพิ่มเติม เพื่อตรวจสอบว่า e-mail นี้มาจากเว็บไซค์บริษัทหนึ่งจริงๆ หรือไม่

ลบ e-mail ที่ขอข้อมูลทางการเงินหรือรหัสผ่าน (Password)

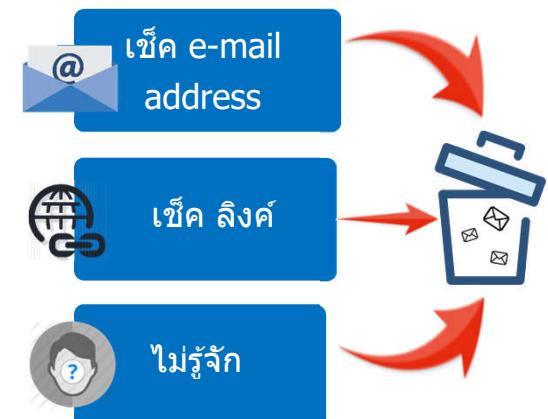
ถ้ามีข้อความที่ขอข้อมูลส่วนตัวของคุณ ข้อมูลทางการเงิน บัญชีเข้าใช้งาน Internet Banking หรือรหัสผ่านต่างๆ ให้เข้าใจไว้ก่อนว่า มันคือ การหลอกลวง

ปฏิเสธคำร้องขอความช่วยเหลือ หรือ การให้ความช่วยเหลือ

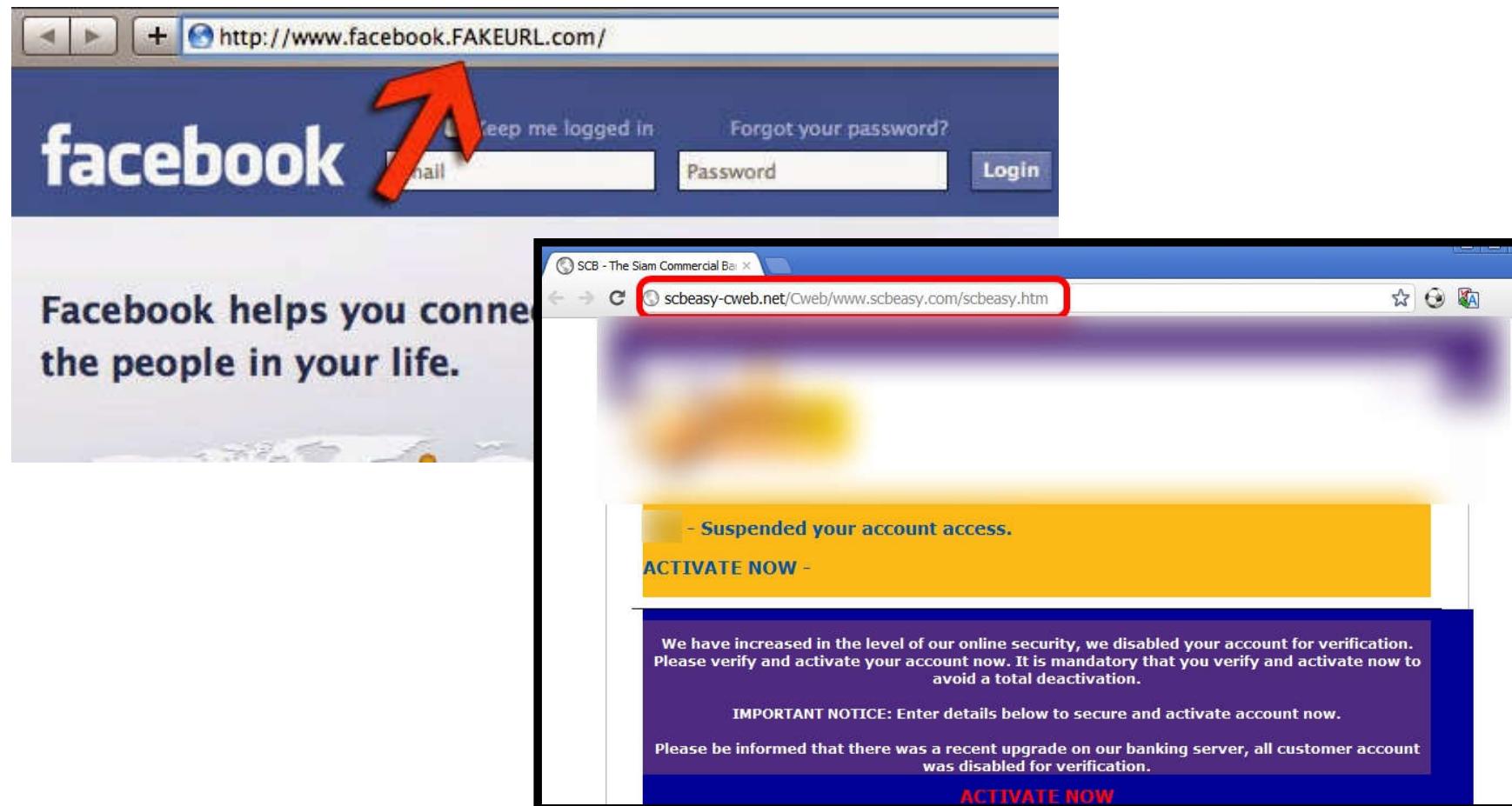
โดยปกติ ถ้าคุณไม่ได้ติดต่อขอความช่วยเหลือจากบริษัทต่างๆ เขามักจะไม่ติดต่อมากาคุณเพื่อขอหรือให้ความช่วยเหลือ ดังนั้นหากได้รับ e-mail ขอหรือให้ความช่วยเหลือในลักษณะนี้ให้ระมัดระวัง

ดูลิงค์ที่คุณจะเข้าไปให้ดีก่อนคลิก

ใช้ search engine เช่น Google ค้นหาลิงค์ที่คุณจะเข้า เพื่อให้มั่นใจว่ามันไม่ใช่เว็บหลอกลวง หรือให้เอาเม้าส์วางบนลิงค์เพื่อดูว่าเว็บที่จะไปเป็นเว็บจริงหรือหลอกลวง



เว็บปลอม



เว็บปลอม

สร้างเว็บปลอมแสนง่าย

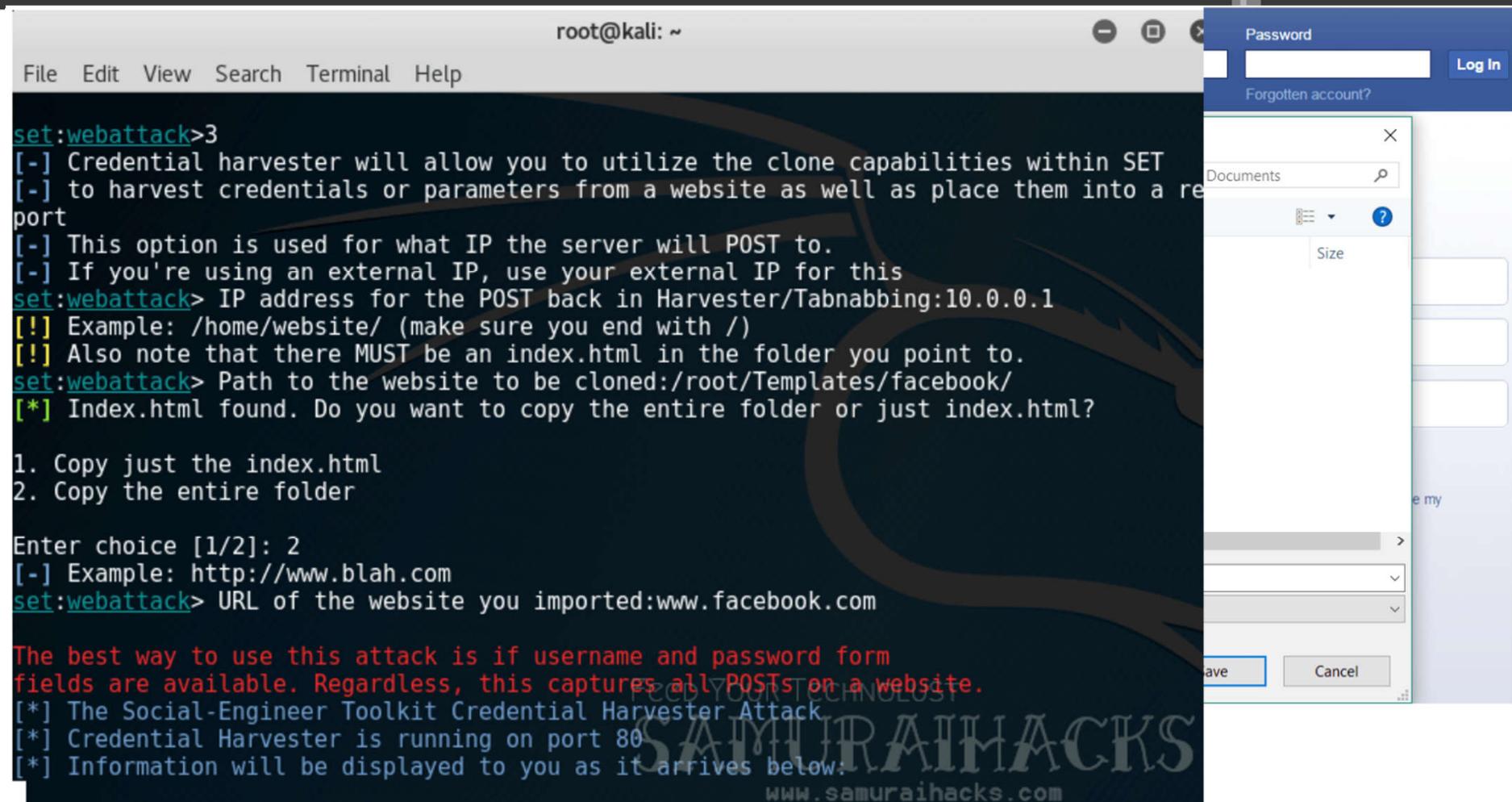
```
root@kali: ~
File Edit View Search Terminal Help
set:webattack>3
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.0.0.1
[!] Example: /home/website/ (make sure you end with /)
[!] Also note that there MUST be an index.html in the folder you point to.
set:webattack> Path to the website to be cloned:/root/Templates/facebook/
[*] Index.html found. Do you want to copy the entire folder or just index.html?

1. Copy just the index.html
2. Copy the entire folder

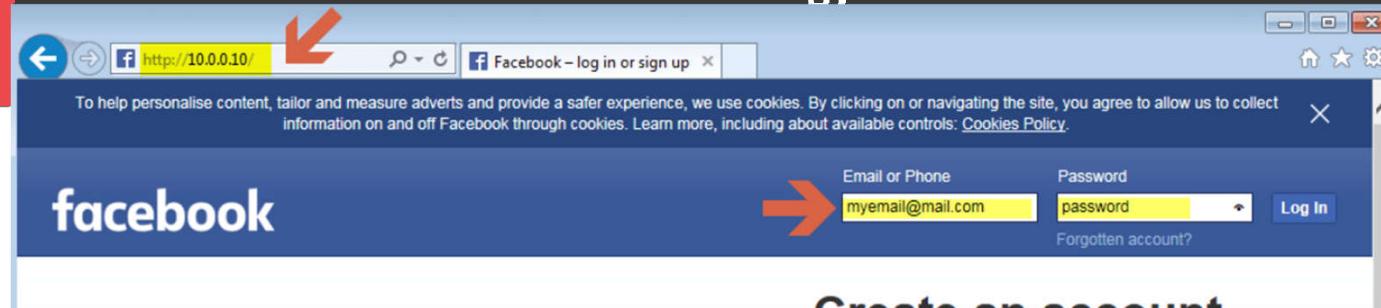
Enter choice [1/2]: 2
[-] Example: http://www.blah.com
set:webattack> URL of the website you imported:www.facebook.com

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below.

  NEED YOUR TECHNOLOGY?  SAMURAIHACKS
  WWW.SAMURAIHACKS.COM
```



ผลหลังบันทึกข้อมูลเข้าเว็บปะลอม



To help personalise content, tailor and measure adverts and provide a safer experience, we use cookies. By clicking on or navigating the site, you agree to allow us to collect information on and off Facebook through cookies. Learn more, including about available controls: [Cookies Policy](#).

facebook

Facebook helps you connect and share with the people in your life.

Email or Phone: myemail@mail.com
Password: password

Create an account

File Edit View Search Terminal Help

```
PARAM: lsd=AVqwBe_o
PARAM: ph=C3
POSSIBLE USERNAME FIELD FOUND: q=[{"user": "0", "page_id": "nwh59l", "posts": [{"time_spent_bit_array": {"tos_id": "nwh59l", "start_time": 1497962505, "tos_array": [308287707, -26804224], "tos_len": 64, "tos_seq": 1, "tos_cum": 26}, 1497962569235, 0]}, {"time_spent_bit_array": {"tos_id": "nwh59l", "start_time": 1497962569, "tos_array": [8389759, 0], "tos_len": 64, "tos_seq": 2, "tos_cum": 35}, 1497962633163, 0}], "trigger": "time_spent_bit_array", "send_method": "ajax"}]
PARAM: ts=1497962711071
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVqwBe_o
POSSIBLE USERNAME FIELD FOUND: email=myemail@mail.com
POSSIBLE PASSWORD FIELD FOUND: pass=password
PARAM: timezone=345
PARAM: lgndim=eyJ3IjoxOTIwLCJ0IjoxMDAwLCJhdYI6MTkyMCwiYWgiOjk2MCwiYyI6MjR9
PARAM: lgnrnd=042802_quM9
PARAM: lgnjs=1497962493
PARAM: ab_test_data=AAVqVAqVqAAVAAAVALAAqqA/AAVVVAVqAAAAAVqVAKq/VPFKAAPAAH
PARAM: locale=en GB
```

A yellow arrow points from the highlighted text area to the bottom right corner of the terminal window.

เทคนิคป้องกัน และการตรวจสอบ



อย่าใจร้อน

กรณีใช้งานระบบสำคัญๆ ให้ตรวจสอบ urls ที่เข้าใช้งานทุกครั้ง และหากเป็นระบบของธนาคาร โดยส่วนใหญ่แล้วชื่อ web urls จะต้องชี้นั้นด้วย https และเมื่อเข้าใช้งานต้องไม่มีข้อความเตือนเรื่องความปลอดภัย หรือ เตือนว่า Certificate Error



หาความจริง

บรา�เซอร์โดยส่วนใหญ่จะตั้งชื่อให้มีความใกล้เคียงกับเว็บจริง อาจจะเปลี่ยนแค่ตัวอักษรตัวใดตัวหนึ่งเท่านั้น เราสามารถตรวจสอบหาเว็บจริงได้โดยพิมพ์ชื่อเว็บไซต์ที่จะเข้าใช้งาน ผ่าน google โดยส่วนใหญ่แล้ว จะพบรายชื่อเว็บที่ถูกต้อง

เว็บปลอม

มาลองจับผิดกัน



Welcome to SCBEasy.com - Internet Explorer

https://www.scbeasy.siamcommercialbank.co.uk/index.asp Certificate Error Welcome to SCBEEasy.com

Welcome to SCBEeasy.com - Internet Explorer

https://www.scbeasy.siamcommercialbank.co.uk/index.asp Certificate Error Welcome to SCBEeasy.com

หน้าหลัก บริการต่างๆ สมัคร แบบฟอร์ม ติดต่อเรา

ไทย | English

สมัครบริการออนไลน์ SCB Easy Net

ເຮືອນນໍາຮູ້

ອໝາລີນ! ອັດເດກ e-mail address ຂອງທ່ານເພື່ອ
ຮັບການຈົນເດືອນ ຂ່າວສາງ ແລະສິຫຼະທີ່ເສີ່ມຕົ່ງາ
ຈາກທາງ SCB Easy Net ໂດຍສາມາດແກ້ໄຂ
email address ໄດ້ທີ່ເມຸນ ແກ້ໄຂຂ່ອມູນ

ແຈ້ງເຊື່ອນ! ໂປຣ ຮະວັງ! ອົມເລຂອນອ້າງ
(Phishing mail) ຈ່າເປັນອົມເລຈາກຮາຄາຮອດລອກ
ລວງໃຫ້ຄຶກເທົ່າໄປຢັງເວັນໄປ່ SCB Easy ປຸລອນ
ເພື່ອຄວາມປຸລອດຂັ້ນກຸຽນາທິ່ມພໍ
www.scbeasy.com

Login to SCB Easy Net

Login Name

Password

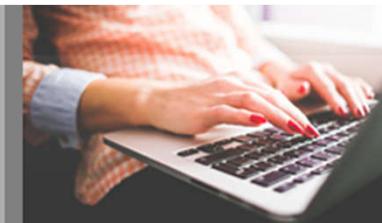
ທ່ານຕ້ອນໄດ້ໃຫ້ຫຼຸດໃຫ້ກຳລັງ Password ເພີ້ມໃນ
ການ log in ຖອນການໃຫ້ Password ໃຫຍ່

ລືມເຮືອນ Password ໄພ ກຳລັກຕິດ

Login

เว็บปลอม

มาลองจับผิดกัน



Welcome to SCBEasy.com - Internet Explorer

http://www.scbeazy.com

Welcome to SCBEeasy.com - Internet Explorer

http://www.scbeazy.com

หน้าหลัก บริการต่างๆ สมัคร แบบฟอร์ม ติดต่อเรา

ไทย | English

สมัครบริการออนไลน์ SCB Easy Net

เรื่องน่ารู้

- อย่าลืม! อพเพด,e-mail address ของคุณเพื่อรับการแจ้งเตือน ข่าวสาร และสิทธิพิเศษต่างๆ จากทาง SCB Easy Net โดยสามารถแก้ไข email address ได้ที่เมนู แก้ไขข้อมูล
- แจ้งเตือน! โปรด ระวัง! อีเมลแอบอ้าง (Phishing mail) ว่าเป็นอีเมลจากธนาคารหลอกลวงให้คลิกเพื่อไปยังเว็บไซต์ SCB Easy ปลอมเพื่อความปลอดภัย กรุณาพิมพ์ www.scbeazy.com

Login to SCB Easy Net

Login Name:

Password:

หากลืมรหัสผ่าน กรุณาตั้ง Password ใหม่ ในการ log in กรุณารีเซ็ต Password ใหม่

ลืมรหัสผ่าน Password ใหม่ คลิกคืน

Login

เว็บปลอม

มาลองจับผิดกัน



Welcome to SCBEasy.com - Internet Explorer

https://www.scbeeasy.com/v1.4/site/presignon/index.asp

The Siam Commercial ...

Welcome to SCBEasy.com

https://www.scbeeasy.com/v1.4/site/presignon/index.asp

The Siam Commercial ...

Welcome to SCBEeasy.com

หน้าหลัก บริการต่างๆ บัตร แบบฟอร์ม ติดต่อเรา

ไทย | English

สมัครบริการออนไลน์ SCB Easy Net

เรื่องน่ารู้

อย่าลืม! อัพเดท e-mail address ของคุณเพื่อ รับการแจ้งเตือน ข่าวสาร และสิทธิพิเศษต่างๆ จากทาง SCB Easy Net โดยสามารถแก้ไข email address ได้ที่เมนู แก้ไขข้อมูล

แจ้งเตือน! โปรด ระวัง! อีเมลแอบอ้าง (Phishing mail) ว่าเป็นอีเมลจากธนาคารหลอก ลวงให้คลิกเพื่อไปยังเว็บไซต์ SCB Easy ปลอม เพื่อความปลอดภัย กรุณาพิมพ์ www.scbeeasy.com

Login to SCB Easy Net

Login Name:

Password:

หากลืมรหัสผ่าน กรุณาตั้ง Password ใหม่ กดที่นี่

ลืมรหัสผ่าน Password ใหม่ กดที่นี่

Login

เว็บปลอม

ข้อควรปฏิบัติเมื่อรู้ว่าตกเป็นเหยื่อ



ข้อมูลบริษัท

- หากให้ข้อมูลการเข้าระบบ ให้แก่ไขรหัสผ่านในระบบต่างๆโดยทันที
- ให้แจ้งหัวหน้างาน และฝ่าย IT โดยทันที

ข้อมูลธนาคาร

- ผู้เสียหายควรแจ้งเรื่องไปยังธนาคารที่ใช้บริการ และทำการปิดบัญชีที่คาดว่าสามารถถอนไม่อยู่ได้ หรือเฝ้าระวังการใช้งานบัญชีอย่างต่อเนื่อง เช่น ได้รับ SMS โอนเงินแต่ไม่ได้ทำการถอนในช่วงเวลาอันนั้น
- เปลี่ยนรหัสการเข้าใช้งานโดยทันที

ข้อมูลการเข้าใช้งานเว็บไซค์ต่างๆ

เปลี่ยนรหัสการเข้าใช้งานโดยทันที

Mobile / IoT Security

การรักษาความปลอดภัยให้กับมือถือและอุปกรณ์ IoT



1

Lock หน้าจอ

ตั้งค่า Lock หน้าจอ เครื่อง เพื่อบังกันบุคคลอื่นแอบใช้งานมือถือ

2

ไม่ Root/Jailbreak เครื่อง

การ Root/Jailbreak นอกจากทำให้เครื่องหมดประกันแล้ว โปรแกรมที่ใช้ใน การ Root/Jailbreak อาจฝังคำสั่งไม่ประสงค์ดีไว้ด้วยเช่นกัน และทำให้ โปรแกรมบางตัวสามารถเข้าถึงไฟล์สำคัญของเครื่องได้

3

ไม่ลงโปรแกรมที่ไม่ได้มาจากการ Google Play Store หรือ Apple AppStore

Google และ Apple มีขั้นตอนในการตรวจสอบโปรแกรมก่อนอนุญาตให้ เผยแพร่ใน Store จึงมั่นใจได้ในระดับหนึ่งว่า โปรแกรมเชื่อถือได้

4

ตรวจสอบ App ที่จะใช้งาน

บางครั้งอาจพบ Application ที่ไม่เหมาะสมใน Store ทางที่ดีที่สุด คือ การ อ่าน Review ของผู้ใช้งานคนอื่น และดูยอดจำนวนคนติดตั้ง

5

ปรับปรุง Software ให้ทันสมัย

มือถือหลายรุ่นในปัจจุบัน ผู้ผลิตเริ่มมีการปรับปรุง Software เครื่อง นอกจากให้ทันสมัยขึ้นแล้ว ยังทำการปิดช่องโหว่ของ Software ตัวเดิม

Mobile / IoT Security

การรักษาความปลอดภัยให้กับมือถือและอุปกรณ์ IoT



Mobile / IoT Security

การรักษาความปลอดภัยให้กับมือถือและอุปกรณ์ IoT



Smart Home



1

เปลี่ยนรหัสโรงงาน เป็นรหัสใหม่

หากอุปกรณ์ IoT สามารถเปลี่ยนรหัสผ่านได้ ต้องทำการเปลี่ยนเป็นรหัสผ่านใหม่ เพื่อป้องกัน Hacker สุมตรวจสอบและใช้เป็นฐานการยิง DDoS

2

ปรับปรุง Software ให้ทันสมัย

IoT หลายรุ่นในบ้าน ผู้ผลิตเริ่มมีการปรับปรุง Software เครื่อง นอกจากให้ทันสมัยขึ้นแล้ว ยังทำการปิดช่องโหว่ของ Software ตัวเดิม

Wireless / Access Point

การรักษาความปลอดภัยให้กับอุปกรณ์ Wifi



- 1 **เปลี่ยนรหัสโรงงาน เป็นรหัสใหม่**
หลังทำการตั้งค่าเสร็จแล้วให้ทำการตั้งค่ารหัสผ่านใหม่โดยทันที
- 2 **ปรับปรุง Software ให้ทันสมัย**
Wireless/Wifi หลายรุ่นในปัจจุบัน ผู้ผลิตเริ่มมีการปรับปรุง Software เครื่อง นอกจากให้ทันสมัยขึ้นแล้ว ยังทำการปิดช่องโหว่ของ Software ด้วย
- 3 **ไม่เปิดฟังก์ชัน WPS**
WPS เป็นฟังก์ชันที่ทำให้การเชื่อมต่อระหว่างอุปกรณ์อื่นๆ กับ Wireless device ทำได้ง่าย แต่ WPS มีช่องโหว่ที่สามารถถูกเจาะได้ง่าย
- 4 **ตั้งรหัสผ่าน Wifi SSID ด้วยรหัสผ่าน WPA2**
ในปัจจุบันมีเครื่องมือที่หาได้โดยง่าย สามารถทำการทดสอบรหัส วิธีการเข้ารหัสแบบ WEP, WPA และลองเข้าใช้งาน Wireless ได้แล้ว
- 5 **SSID Name**
การตั้งชื่อ ควรตั้งเป็นชื่อที่ไม่ได้สื่อให้ทราบได้อย่างชัดเจนว่าเป็น Wireless ของใคร สำหรับการซ่อน SSID นั้น ปัจจุบันไม่ได้ถือว่าเป็นการควบคุมความปลอดภัย เนื่องจากรีเกลย์ Tool ทางด้านล่างนี้ ระบุไว้ ลังกล่าว

เสริมเกรดเล็ก เกรดน้อย



บัตรพนักงาน

ป้อยครั้งที่เรามักษบพนักงานบริษัทฯ นำบัตรพนักงานวางแผนจองโต๊ะทานข้าวในช่วงเที่ยงวัน ซึ่งการกระทำดังกล่าว
เสี่ยงต่อการถูกขโมยบัตร หรือการสำเนาข้อมูลในบัตร และถูกแอบบันนำไปใช้เพื่อเข้าถึงพื้นที่บริษัทฯ



Lock หน้าจอทุกครั้งที่ลูกออกจากโต๊ะ

ทุกครั้งที่เดินออกจากโต๊ะทำงาน ควรทำการ Lock หน้าจอ ทุกครั้งเพื่อป้องกันบุคคล
อื่น แอบเข้าถึงเครื่อง หรือข้อมูลสำคัญของคุณ



ระมัดระวังการใช้งาน Wifi ที่ไม่รู้จัก

หากคุณต้องการใช้ Internet ที่ไม่ใช่ของคุณเอง ความนิ่นใจว่า Wifi ที่จะใช้งานมีความ
น่าเชื่อถือ แต่ทั้งนี้ หากเลี่ยงได้ ควรเลี่ยง และใช้งานผ่าน 3G/4G ในมือถือ

Section Break

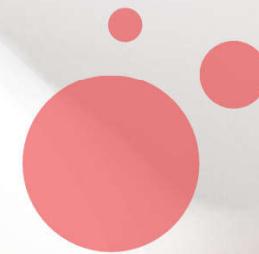


แบบทดสอบ หลังเรียน



<https://www.surveymonkey.com/r/GDYPSPHB>





Thank you