



กสท.กร.ทบ.

การสร้างความตระหนักรู้ด้านความปลอดภัยสารสนเทศ



สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี (2538) ทรงอธิบายคำว่า “เทคโนโลยีสารสนเทศ (Information Technology) หรือเรียกว่าๆ ว่าไอที (IT)” เน้นถึงการจัดกระบวนการดำเนินงานสารสนเทศหรือสารนิเทศในขั้นตอนต่างๆ ตั้งแต่ การเสาะแสวงหา การวิเคราะห์ การจัดเก็บ การจัดการ และการเผยแพร่เพื่อเพิ่มประสิทธิภาพ ความถูกต้อง ความแม่นยำ และความรวดเร็วทันต่อการนำไปใช้ ประโยชน์ ”

Cyberspace หมายถึง พื้นที่ ที่สร้างขึ้นด้วยระบบอิเล็กทรอนิกส์ ที่ใช้เพื่อสื่อสาร ติดต่อกัน ซึ่งสามารถติดต่อกันได้ทั่วโลก เมื่อมีคนท่องไปในอวกาศ เช่น การส่งไปรษณีย์ อิเล็กทรอนิกส์ เป็นต้น



Cyber Warfare เป็น Domain ที่ 5
แห่งการทำสงครามทางการทหาร (The Fifth Domain of Warfare)
นอกเหนือจาก พื้นดิน, ผืนฟ้า, อากาศ และ อวกาศ
มีความสำคัญถึงกับ
เพนตากอน ได้จัดตั้งกองบัญชาการไซเบอร์ (Cyber Command)
เมื่อ พฤษภาคม 2010



“สารสนเทศ” (Information) กำลังกลายเป็นอาวุธที่สามารถนำมาใช้ในการโจมตีฝ่ายตรงข้ามได้ ดังตัวอย่างที่เห็นได้ชัดเจนจากปรากฏการณ์ “Arab Spring” ในการใช้เครือข่ายสังคมออนไลน์โซเชียลมีเดีย เช่น Facebook และ Twitter สร้างกระแสต่อต้านรัฐบาล มีผลกระทบเต็มๆ ต่อการบริหารงานของรัฐบาล และ มีผลกระทบต่อภาพลักษณ์ของผู้นำในระดับประเทศ





กรณีตัวอย่าง wikileaks

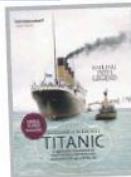


Irish Independent

IRELAND'S BEST-SELLING DAILY NEWSPAPER

METROEDITION
www.independent.ie Tuesday 31 May 2011 €1.90 (€1.20 in Northern Ireland)

WIKILEAKS THE IRELAND CABLES DAY ONE 10-PAGE SPECIAL



FREE
SPECIAL
TITANIC
MAGAZINE

How the US taps into our secrets

WikiLeaks



● How Mary Hanafin slagged the Greens



● Mystery Sinn Fein/DUP talks finally revealed



● How Maire Geoghegan-Quinn landed top €240,000 EU job

LIFTING THE RED

THIS is Julian Assange, founder and editor-in-chief of WikiLeaks, the international website which is exposing organisations.

He has released secret documents obtained from confidential sources and has become known for some of the largest leaks of classified information in history.

No w, the Irish Independent has obtained exclusive access to more than 1,000 US embassy cables.

Over the next days we will give readers a unprecedented insight into what really goes on at the highest levels of government, both at home and abroad.

THE IRELAND CABLES:
PAGES 22 TO 31

Shane Phelan
Investigative Correspondent

THE United States is routinely given access to sensitive information by the highest levels of the Irish Government through an extensive network of official - but highly confidential - coalitions.

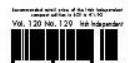
America's official coalition partners, senior civil servants and top diplomats among them, are secretly giving away US embassy cables reveal.

Their actions are disclosed in the Ireland Cables, a massive 1,000 classified documents exclusively obtained by the Irish Independent from the whistleblowing organisation WikiLeaks.

One leaked cable reveals how former minister and current Taoiseach, prime minister Mary Hanafin briefed the American embassy on tense ongoing coalition negotiations.

The word "PROTECT" appears beside her name in the cable, meaning her identity and/or her comments were not to be made public.

Continued on page 22



26/27/2011



สถิติมัลแวร์โดย Microsoft DCU ในช่วงต้นปี พ.ศ.2558

จาก Top 25 ประเทศ ประเทศไทยเราติดมัลแวร์เป็นอันดับที่ 5 ของ

ทวีปเอเชีย รองจาก อินเดีย อินโดนีเซีย จีน เวียتنาม

โดยมัลแวร์ส่วนใหญ่ติดมาตั้งแต่ปี พ.ศ.2557 จนถึงปี พ.ศ.2559

เป็น เวลากว่า 2 ปี ก็ยังไม่ได้รับการแก้ไข



Top 10 in Asia under Cyber Threats

This index shows the highest ranked Asian markets, with some on a global list of top 25 countries, and is ranked by the number of malware detections through unique IP addresses.

1. (1)	India	
2. (5)	Indonesia	
3. (8)	China	
4. (9)	Vietnam	
5. (11)	Thailand	
6. (17)	Philippines	
7. (19)	Malaysia	
8.	Taiwan	
9.	Japan	
10.	South Korea	

Noteworthy: There are 7 Asian countries in the global top 25 list

เป้าหมายที่ถูกโจมตี

Year 2015

Medical / Health care

Government / Military

Education / Research

Banking / Financial

Small , Medium , Large Business

/ \$

129 / 100 Mil

27 / 47 Mil

31 / 724 K

39 / 408K

154 / 121K



กรณีตัวอย่าง ประเทศของจีน ที่ใช้การจารกรรมในทางสร้างสรรค์
โดยการ Hack ข้อมูลงานวิจัย เพื่อนำมาสร้างการผลิตในระดับสูงต่างๆ



กลุ่ม Anonymous



สถานการณ์ด้านไซเบอร์



แผนที่แสดงรำมไซเบอร์สเปส

Map.norsecorp.com

หัวข้อด้านความปลอดภัยสารสนเทศ



Single Gateway

change.org

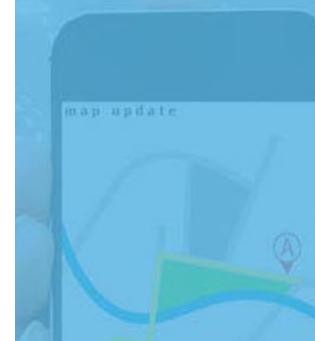
เริ่มเรื่องรบเรกต์ ค้นหา

เข้าสู่ระบบ

รัฐบาล The Government of Thailand

ต่อต้านการตั้งชิงเกิลเกตเวย์ Go against Thai govt to use a Single Internet Ga ท่วง.

Coconut Shell Thailand



404 Page Not Found
ขออภัย ไม่พบหน้าที่ต้องการ กรุณาลองใหม่อีกครั้ง

Pawoot Pom Pongvitayapanu
9 hrs · Edited · ดู

ไม่เห็นด้วยเลยกับการซื้อขายการให้รัฐ เพื่อแสวงผลอุตสาหกรรมด้วยช่องทางเดียว นั่นคือ Single Gateway หมายความว่าจะได้ จึงมีเนื้อหาให้รัฐเข้าไปสักการะ แต่อารยธรรมไทย มีความคุณไม่ได้ จึงมีเนื้อหาให้รัฐเข้าไปสักการะ ไม่ใช่ทางเดียวแต่การกระทำนี้จะครอบครอง ในที่เดียวฯ ก่อนเรื่องจะเป็นปัญหา ไม่ใช่เรื่องของคนอื่นๆ ไม่ใช่เรื่องของประเทศค่าครองการนี้ ใจเย็นๆ ครับ

Soraj Hongladarom @Sonamsangbo · 21h
รัฐบาลบอกให้ศึกษา ก่อนให้รับคอมเรื่อง #singlegateway จะให้ศึกษาจากในประเทศ ทางที่ดี รบ. ควรเปิดข้อมูลแผนรายละเอียด นโยบาย เรื่องนี้มาให้หมุน



กลุ่ม Anonymous ประกาศโจมตีระบบราชการไทย

 **Anonymous**
@YourAnonNews

+ Follow

#Anonymous targets CAT in
#OpSingleGateway [telecomasia.net/content/
anonym ...](http://telecomasia.net/content/anonym...) #Thailand #Asia [pastebin.com/
SL0ZaMxT](http://pastebin.com/SL0ZaMxT)

The following media may contain sensitive material.
If you'd prefer not to see these warnings, log in to change your Tweet media settings.
Don't have an account? [Sign up!](#)

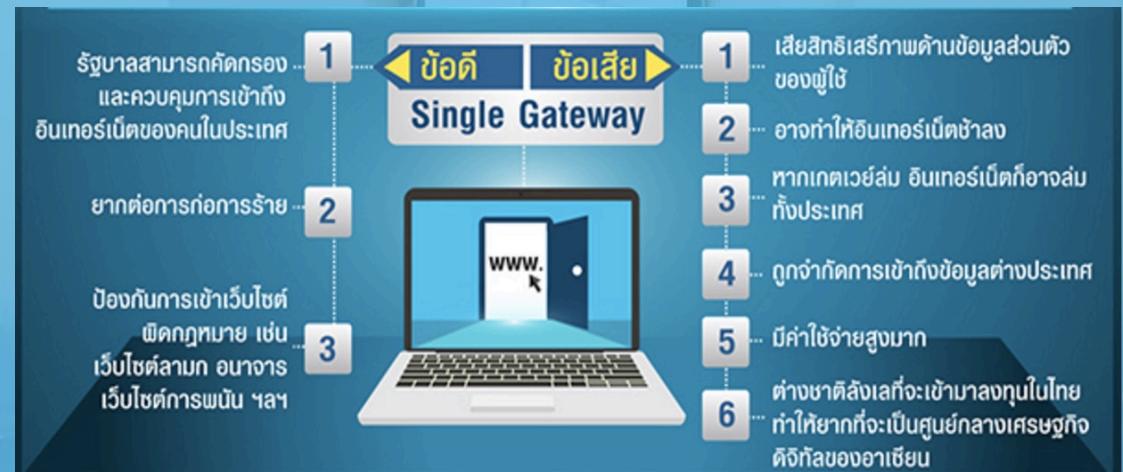
[View content](#) [Learn more](#)



Single Gate way

คืออะไร ?

เกี่ยวข้องกับเราอย่างไร ?



Promptpay , AnyID

ถ้าใช้ **PromtPay**
ชีวิตดีขึ้นยังไง ?

A hand holds a smartphone, which is connected by lines to various icons representing different services or applications. These include a cloud with an upward arrow, a document with a bar chart, a magnifying glass over a map, a computer monitor, a camera, a game controller, and a person icon. To the right, a cartoon bull is shown running with a shopping bag full of groceries, including a strawberry and a sandwich, and a small gift box.

MONEY BUFFALO

ເນື່ອກ່ອນ

985+
259251
94576
ເຢວະເໄຍະ
21871329

ພວມື້ PromptPay

ບັດປະຈາກ

ຈຳເຄີຍບັດປະຈາກ
ຊື່ອື່ນຄົວແທນ



MONEY
BUFFALO

ເຄີ່ງເຮັດໂວນເຈີນຜ່ານ



ເລີບປະຈາກ
ຊື່ອເບອຣໂກຣສັບທີ່ໄດ້

ດີ່ຕິ່



PromptPay

MONEY
BUFFALO

ແຄ່ງເຕາ

3

ອຍ່າງນີ້ຈຸກກັນ

ບັນຫຼິນຄາກ
ອັນດັບ

+

ບັດປະຈາກ

+



MONEY
BUFFALO

PromptPay

ເນື່ອກ່ອນ



ພວມື້ PromptPay

ຄ່າຮຽນເນື້ອງ

ດູກຄາກກາ



MONEY
BUFFALO



ข้อพิจารณาเกี่ยวกับ Promtpay

ร้านค้ารับเงินเข้าผ่าน prompt pay จะมีบันทึกไว้หมดว่าร้านมีรายได้เท่าไร
ร้านจะหลบสรรพากรมากขึ้น

คนธรรมดาก็เป็นผู้รับ - ผู้โอน/ผู้จ่าย ผ่านระบบ prompt pay ก็จะปรากฏ
บันทึกรับจ่ายเป็นหลักฐานด้วยเช่นกัน ก็จะทำให้ภาครัฐรู้มากขึ้นว่าโครงสร้าง
หรือโครงสร้างราย (ยอดใช้จ่ายมากแต่แจ้งว่ารายได้น้อย) ทำให้หลบเสี่ยงภาษี
เงินได้บุคคลธรรมดามากขึ้น



Mobile Application Security

สถิติ Mobile OS ที่ถูก Hack ในปี 2015



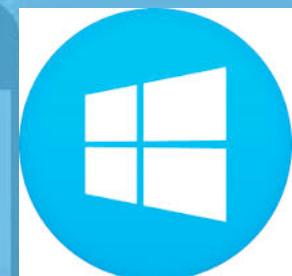
IOS 84%



Android 16%



Blackberry OS <1%



Windows <1%

ข้อควรระวัง Mobile Application ที่ไม่ปลอดภัย



มีการขอ Permission Device & AppHistory
และ Device ID & Call information
Permission ทั้ง 2 นี้จะทำให้อแอปสามารถ
ดึงข้อมูลแอปอื่นๆ ที่กำลังเปิดอยู่ในขณะนั้น
ประวัติการใช้เว็บและ bookmark
เบอร์โทรศัพท์ (แต่ไม่รวมถึง Contact)
ID ของสมาร์ทโฟน !!!

“

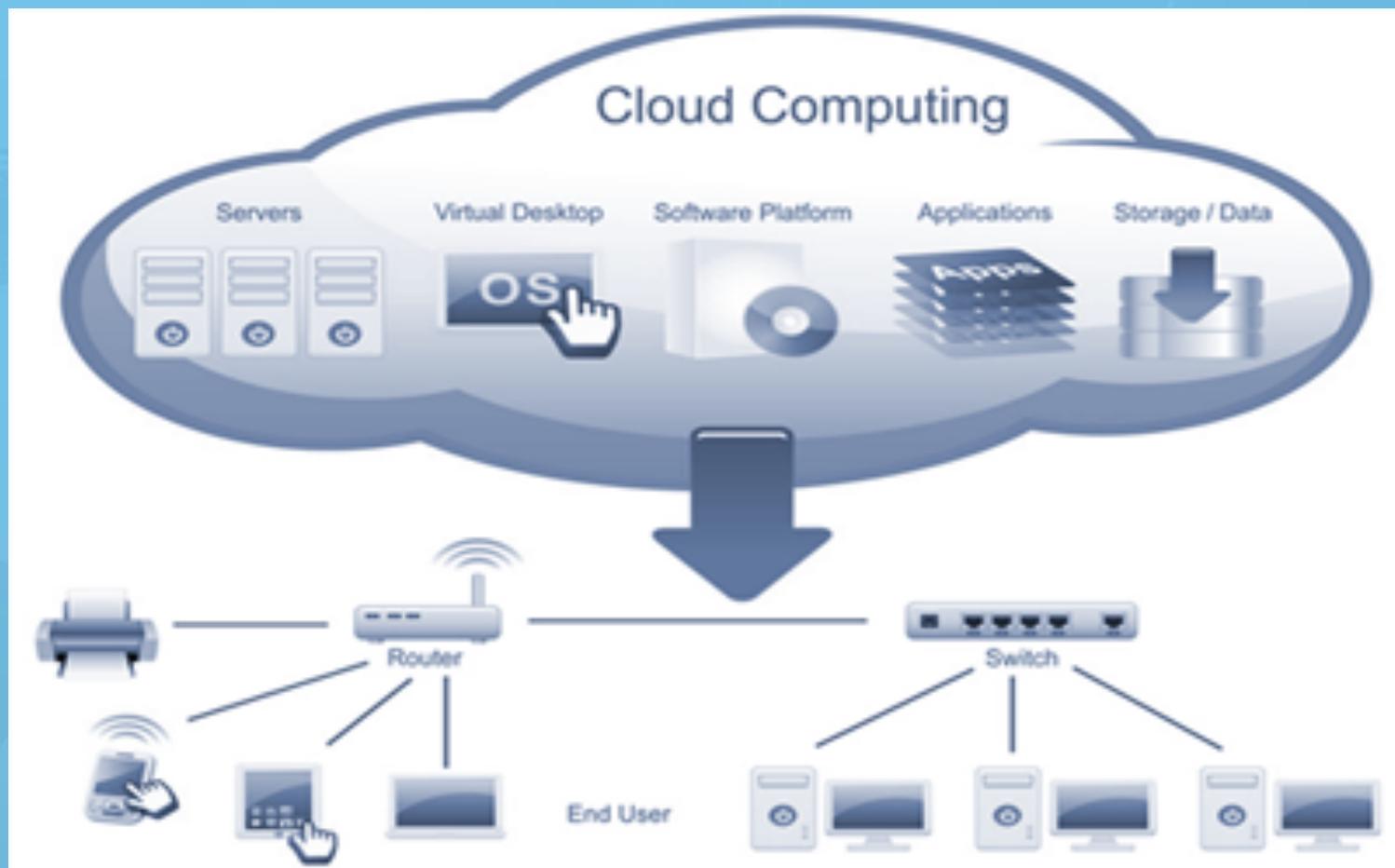
เจอ ใจระครับ แอพฯ MakeupPlus ทันทีที่แต่งภาพเสร็จมันจะอัพโหลดรูปเข้าเว็บ
<http://qiniu.com/> ซึ่งเป็น Cloud Storage ของจีน...

Posted by nuuneoi.com on Saturday, September 5, 2015

Cloud Computing



Cloud Computing คืออะไร?





ข้อควรระวังจากการใช้ Cloud ที่ไม่ปลอดภัย

Hacker โจมตีผ่านแอพ
Find My Phone
โดยอาศัยช่องโหว่ iCloud API
เพื่อขโมยข้อมูลสำคัญ รูปภาพต่างๆ



3 NEWS 12° 9° Auckland Shows iWitness

HOME VIDEO NZ NEWS DECISION 14 WORLD ENTERTAINMENT SPORT

Jennifer Lawrence, others exposed in nude photo leak

Monday 1 Sep 2014 11:46 a.m. 1 Comment

- Crime Scene - Do Not Cross



Gmail by Google msn YAHOO! AOL



การใช้งาน Cloud ที่มีความปลอดภัย

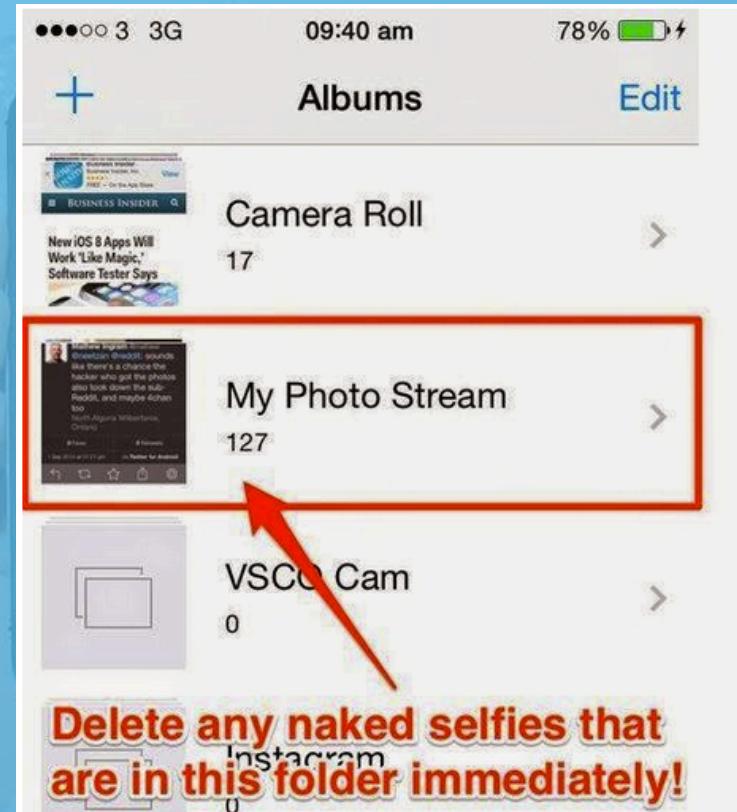
อัพเดต iOS และ APP ให้เป็นเวอร์ชันล่าสุดอยู่เสมอ

เพิ่มความปลอดภัยด้วย Two-step verification

เปลี่ยนรหัสผ่าน Apple ID / iCloud

ลบภาพออกจาก Photo Stream

ปิด Photo Sync



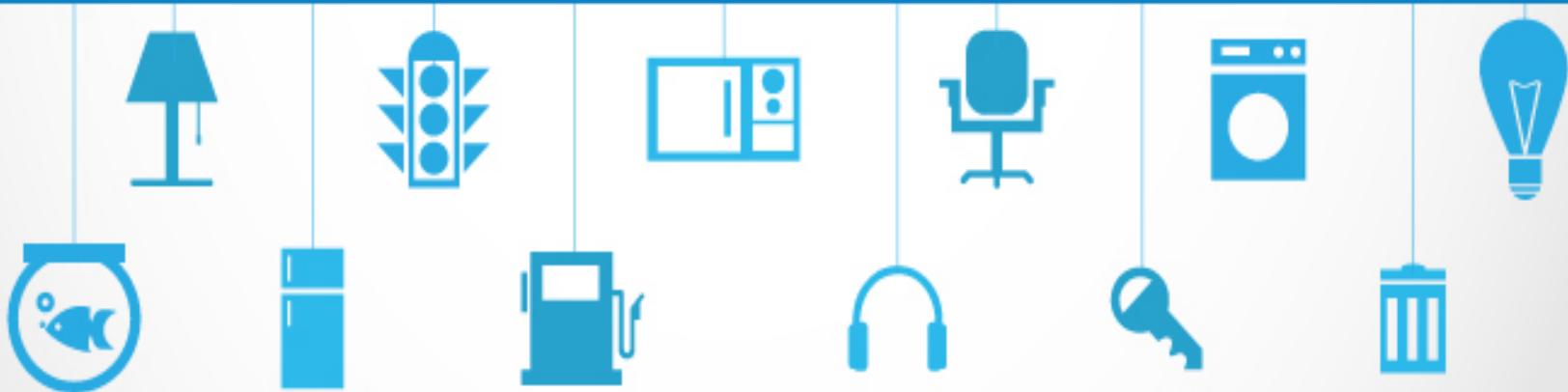
Internet of things



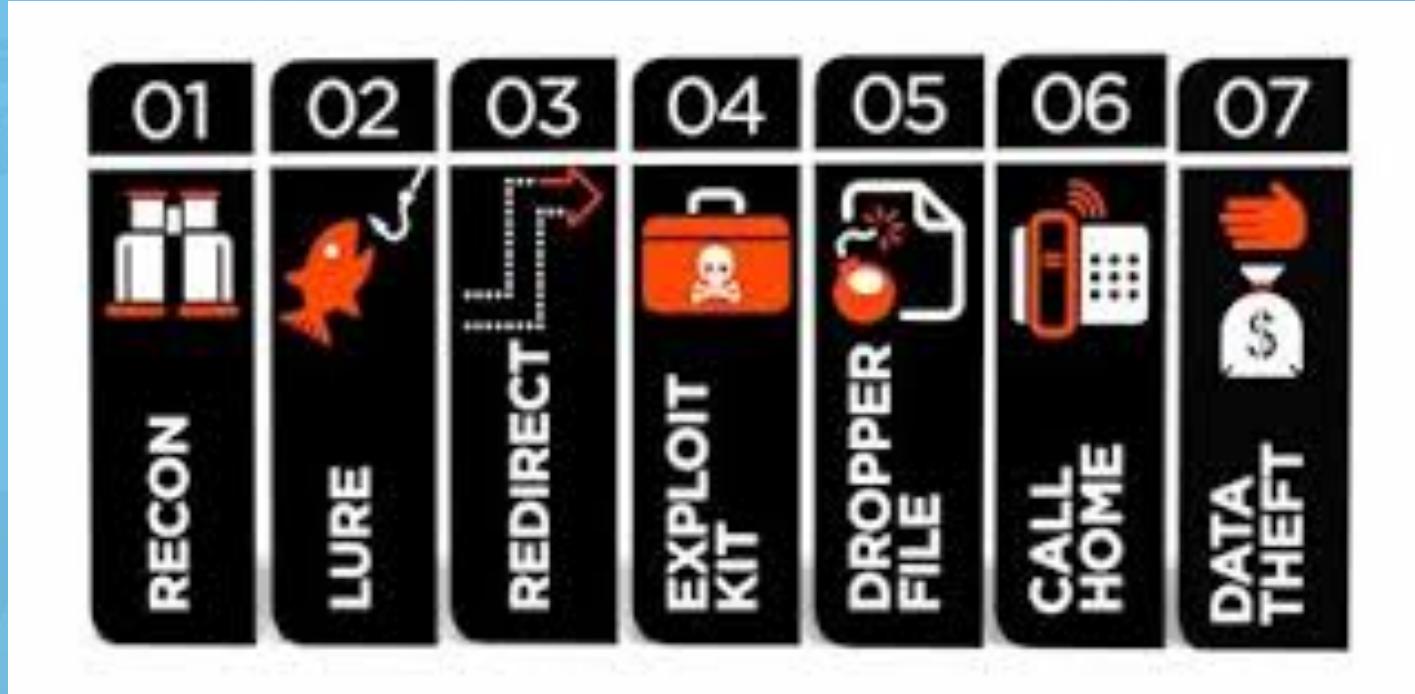
เทคโนโลยีอินเตอร์เน็ตที่เชื่อมต่ออุปกรณ์และ เครื่องมือต่างๆ เช่น โทรศัพท์มือถือ รถยนต์ ตู้เย็น โทรทัศน์ และอื่นๆ เข้าไว้ด้วยกัน



There is expected to be **75 billion**
connected devices by 2020.



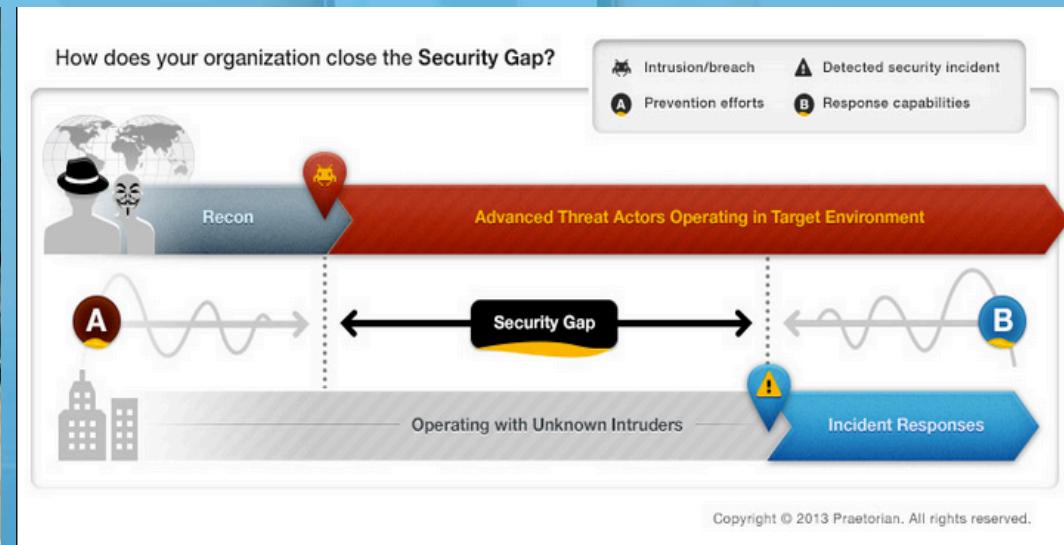
ภัยคุกคามทางไซเบอร์ต่างๆ ที่เกิดขึ้นได้ในชีวิตประจำวัน



APT : Advancepersistance Threat



แผงตัวเข้าไปอยู่ในระบบโดยไม่ให้เป้าหมายรู้ตัว อาจใช้เวลาแค่วันเดียว เป็นสัปดาห์ เป็นเดือนหรือนานจนเป็นปี เพื่อจุดประสงค์ที่จะสร้างความเสียหาย หรือรวมข้อมูลสำคัญที่ต้องการให้ได้มากที่สุดเท่าที่จะทำได้



Advanced Persistent Threat (APT): The Uninvited Guest

How attackers remain in your network harvesting information and avoiding detection over time

1. INCURSION

Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

2. DISCOVERY

Once in, the attackers stay "low and slow" to avoid detection. They then map the organization's defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.



3. CAPTURE

Attackers access unprotected systems and capture information over an extended period. They may also install malware to secretly acquire data or disrupt operations.

4. EXFILTRATION

Captured information is sent back to the attack team's home base for analysis and further exploitation fraud—or worse.



ATTACK METHODS

- = Social Engineering
- = Zero-Day Vulnerability
- = SQL Injection

Ransomware

มัลแวร์ชนิดหนึ่งที่ออกแบบมาเพื่อเรียกค่าไถ่เหยื่อ โดยเกิดจากการสร้าง link ปลอม หรือไฟล์ที่แนบในอีเมลเพื่อเปิดเอกสาร มาให้เหยื่อไปคลิกหรือดาวน์โหลด จากนั้นมัลแวร์ Ransomware จะกันนั้นจะเข้ารหัสข้อมูลในคอมพิวเตอร์ แล้วเรียกค่าไถ่ ทำให้ไม่สามารถใช้งานคอมพิวเตอร์ได้ จำเป็นจะต้องจ่ายเงิน จึงจะได้ข้อมูลคืน





Time left

71:01:05



Transaction ID

ATTENTION!

Private key will be destroyed on 2014-07-21 [10:24:57]

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain a private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files.

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 1 Bitcoin to



DDOS : Distributed Denial of Service



มีจุดประสงค์เพื่อให้ระบบหยุดการทำงานไม่สามารถใช้เครื่องคอมพิวเตอร์ได้ทั้งระบบ
หรือเครื่องเดียว โดยใช้วิธีการ ส่ง Request จากหลายๆเครื่องเข้าไปยังเป้าหมาย
เพื่อให้เครื่องเป้าหมายรับภาระหนักและหยุดทำงานในที่สุด

กรณีเว็บทางการ ICT ล่ม กรณี F5



Anonymous
@LatestAnonNews

+ Follow

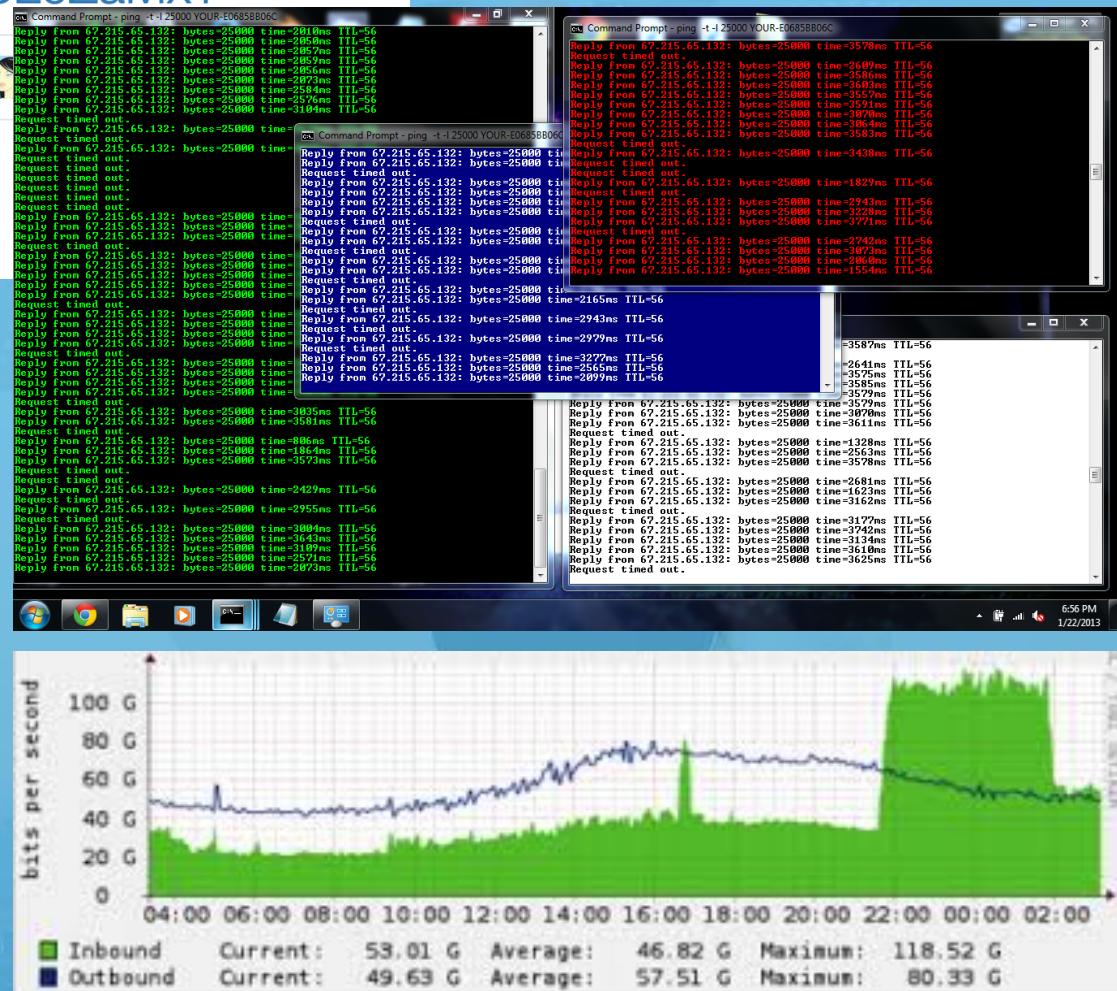
#OpSingleGateway Thailand Statement.
#Anonymous pastebin.com/SL0ZaMxT

RETWEETS FAVORITES
48 **10**

1:32 PM - 21 Oct 2015



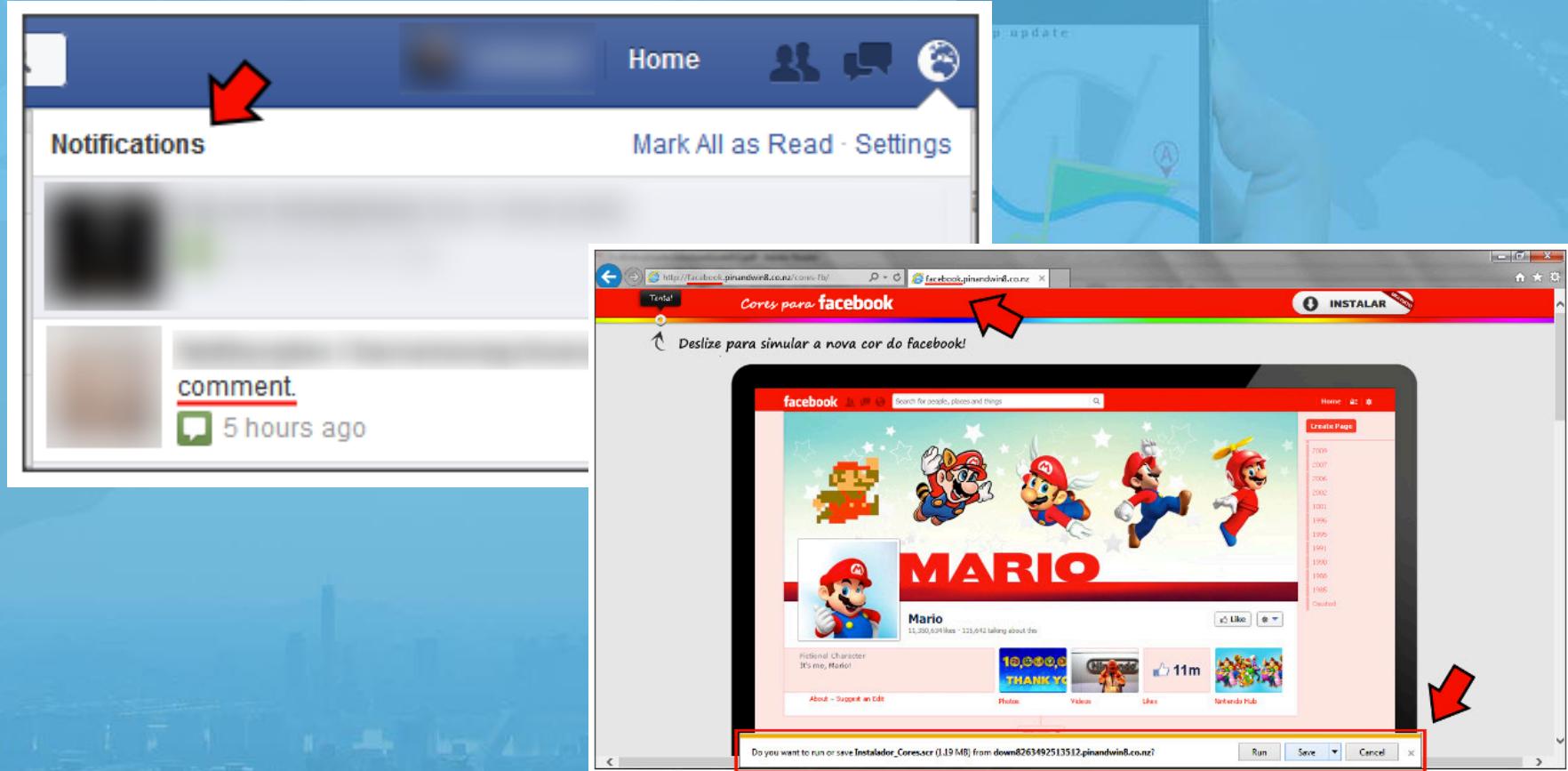
เป้าหมายของถูกใจมติ
สภาพการการทำงานของ
เครื่องเพิ่มขึ้นจนถึงขั้นรับไม่
ได้และหยุดทำงานในที่สุด



Malware บน FaceBook

มัลแวร์บน FaceBook ที่จะแสดงเหมือนมีคนมา Comment กับเรา แต่ว่าเมื่อกดเข้าไป จะติด มัลแวร์ หรือเปิดหน้าเว็บอื่น

- 50% ของโฆษณาบนเว็บไซต์ Live-Streaming มีมัลแวร์





ที่มาของ ม้าโทรจัน หรือ ม้าไม้เมืองทรอย เกิดขึ้นจากอุบายของ โอดิสเซียส ในการบุกเข้าเมืองทรอย แล้วลากไปวางไว้หน้ากำแพงเมืองทรอย แล้วให้ทหารกรีกแสร้งทำเป็นล่าถอยออกไป ชาวทรอยเห็นแล้วเข้าใจว่าเป็นบรรณาการที่ทางฝ่าย กรีก สร้างขึ้นมาเพื่อบุชาเทพเจ้าและล่าถอยไปแล้ว จึงลากเข้าไปไว้ในเมือง ตกดึก ทหารกรีกที่ซ่อนตัวอยู่ในม้าไม้ ก็ได้ลงมาเผาเมืองและปล้นเมืองทรอยได้เป็นที่สำเร็จ

การทำงานของ Trojan จะส่งข้อมูลหลอกภัยมายังเครื่องว่า ไม่มีพิษภัย
หลักจากนั้น เครื่องเหลือ โทรจันก็ จะส่งสคริปท์ ที่ถูกออกแบบมาเพื่อการโจมตี
ตามเป้าหมายที่ต้องการ ออกทำงาน



ภัยจาก E-mail ปลอม

Hacker สามารถปลอมตัวเป็น E-mail ของใครก็ได้เพื่อส่งมาหลอกลวงเหยื่อ โดยในรูปของ E-mail ธนาคาร หรือ คนรู้จัก

----- Forwarded Message -----

From: Kasikorn Bank <alert@kasikorn.com>

To: [REDACTED]@[REDACTED].com

Sent: Saturday, September 15, 2012 7:23 PM

Subject: New Message From Kasikorn Bank

 Kasikorn Bank Thailand
开泰银行 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. กรุณาอย่าคลิกลิ้งค์ใดๆ ก็อยู่ในอีเมลล์หลอกลวงนี้

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

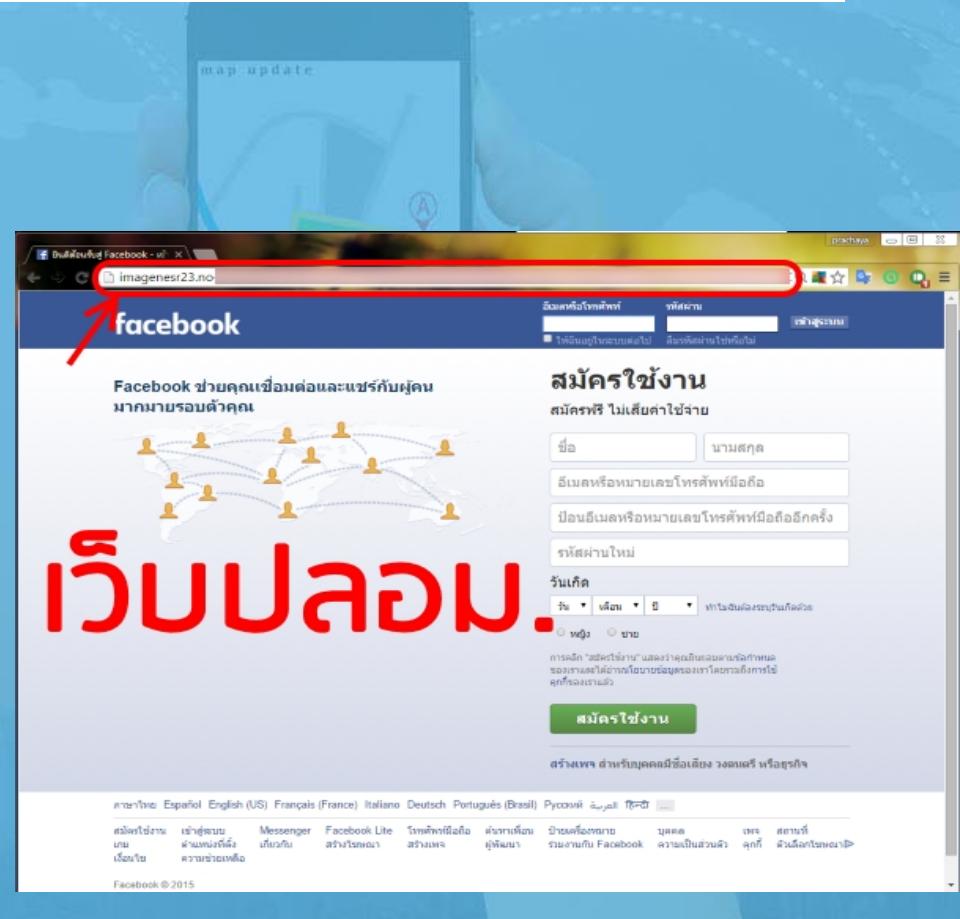
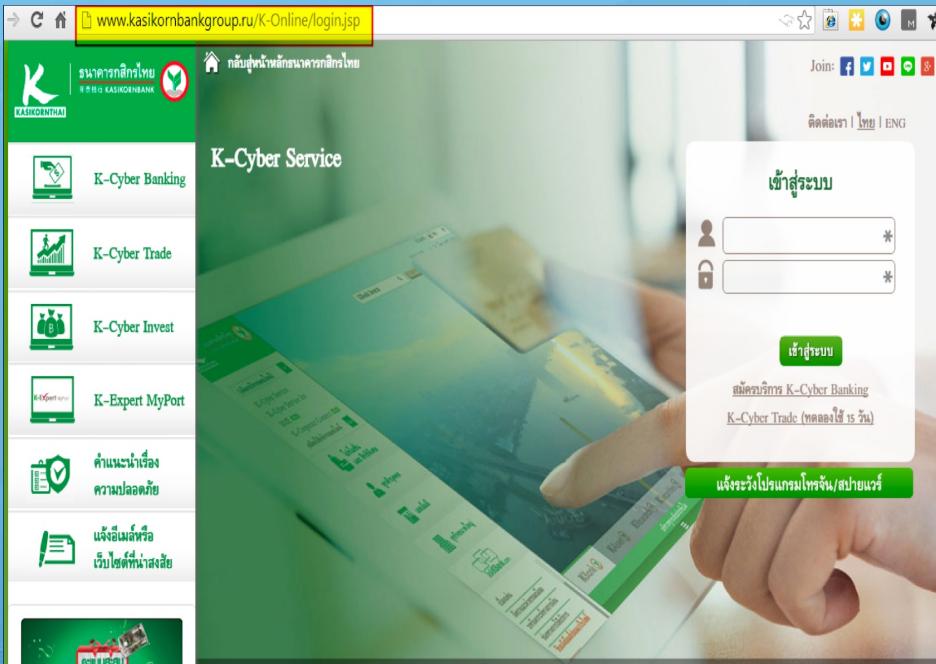
This Email is subject to security From Kasikorn Bank,Please view our privacy poliy statement.

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

Kasikorn Bank © 2012 All Rights Reserved

เว็บปลอม , I-Bank ปลอม

Hacker จะสร้างหน้าเว็บปลอมให้คล้ายกับของจริงที่สุด หรือหลอกให้ เข้าเว็บ
แล้ว Redirect ไปที่เว็บปลอมอื่นๆ
บางครั้งเป็นเว็บจริง แต่มี Popup ปลอมครอบเพื่อหลอกให้เหยื่อเข้าใจผิด





ธนาคารกสิกรไทย
开泰银行 KASIKORN BANK

KASIKORNTHAI

บ้านค้ากสิกรไทย
Kasikorn Home



K-Cyber Banking



K-Cyber Trade



K-Cyber Invest



K-Expert MyPort



คำแนะนำเรื่อง
ความปลอดภัย



แจ้งอิเมลหรือ
เว็บไซต์ที่น่าสงสัย

K-Cyber Service



เข้าสู่ระบบ



*



*

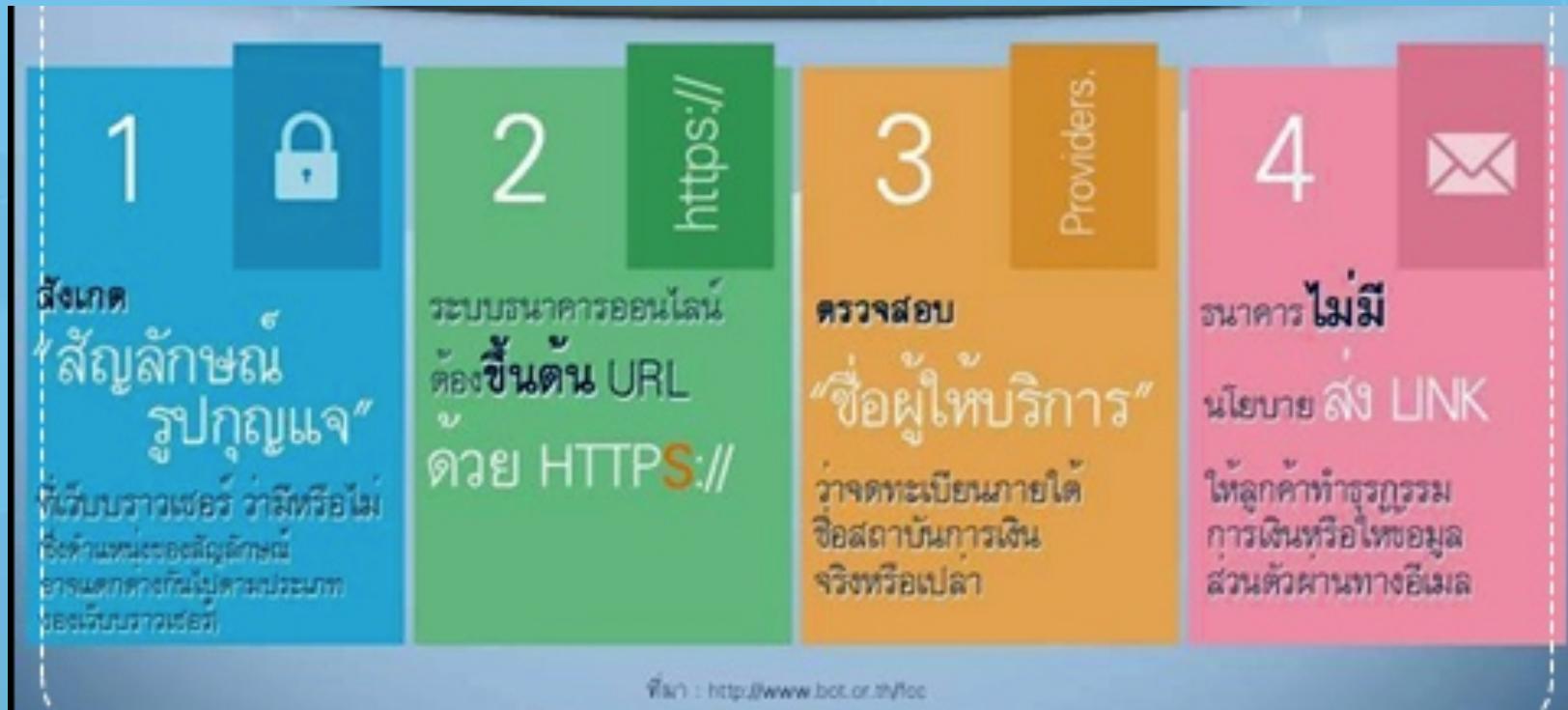
เข้าสู่ระบบ

สมัครบริการ K-Cyber Banking

K-Cyber Trade (ทดลองใช้ 15 วัน)

แจ้งรหัสง๊อปแกรมโจรจัน/สปายแวร์

เมื่อทำธุรกรรมผ่าน Internet Banking ให้สังเกตดังต่อไปนี้



** หากรู้ตัวให้รีบติดต่อ ร. เจ้าของบัญชี
หรือตั้งค่าการทำธุรกรรมให้มี OTP ร่วมด้วย

URL Shortener

รูปแบบการแปลง URL ของเว็บเพื่อให้สั้นและจำจ่ายขึ้น เช่น Bit.ly , Goo.gl

The screenshot shows the Google URL Shortener interface. At the top, it says "Google url shortener". Below that, there is a text input field with the placeholder "Paste your long URL here:" followed by a long URL: "94%E0%B8%9B%E0%B8%B5-2011.html". To the right of this input field is a "Shorten" button. Further to the right, the shortened URL "http://goo.gl/..." is displayed. Below the input field, there is a note: "All goo.gl URLs and click analytics are public and can be shared by anyone." The background of the slide features a blue gradient with a faint silhouette of a person working at a desk.

Paste your long URL here:

94%E0%B8%9B%E0%B8%B5-2011.html

Shorten

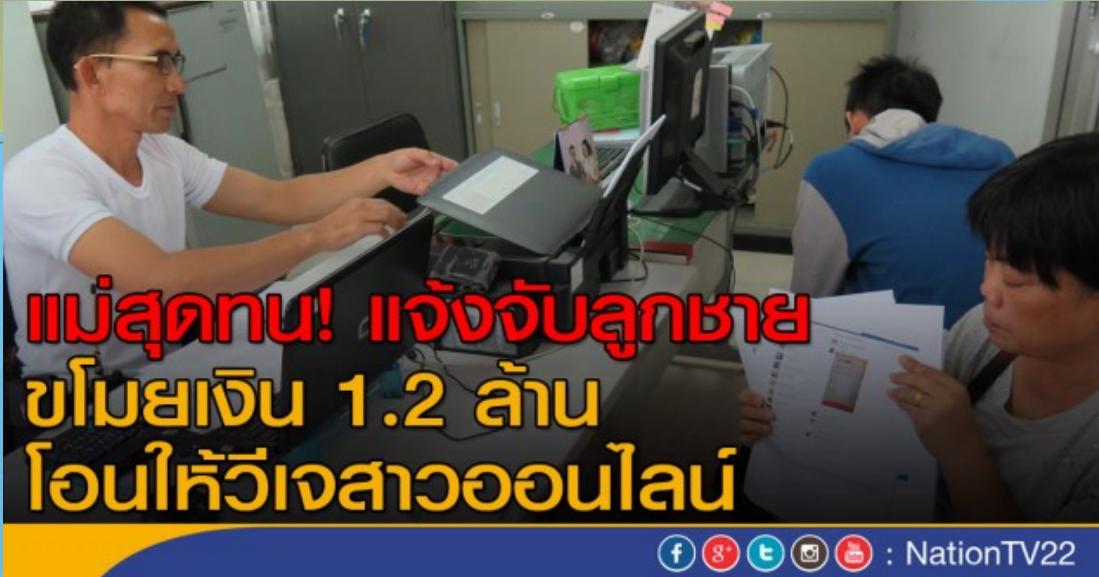
http://goo.gl/...

All goo.gl URLs and click analytics are public and can be shared by anyone.

ภัยจาก Social Network

ปัจจุบันมี Application Social Network เกิดขึ้นเป็นจำนวนมาก และให้บริการในหลายรูปแบบ รวมถึงการให้ผู้ใช้งานเข้ามา มีปฏิสัมพันธ์ กับเครือข่ายผู้ใช้งาน จนมีการหลอกลวงเกิดขึ้น





[f](#) [g](#) [t](#) [i](#) [y](#) : NationTV22



[/ DBH Productions](#)

แหล่งข้อมูลเพิ่มเติม

<https://www.thaicert.or.th>

<http://plan.rta.mi.th/armycert/>

ดาวน์โหลดเอกสารประกอบการบรรยาย

<http://doca-rta-mi-th.com/km.php>