การวิเคราะห์กลุ่มผู้กระทำความผิดอาชญากรรมทางคอมพิวเตอร์ ในรูปแบบ Fake e-mail

คุณปรเมศร์ เพียรสกุล

8 กันยายน 2559


ประกอบธุรกิจอย่างไรไม่ให้ถูกหลอกลวงจากอาชญากรรมทางคอมพิวเตอร์
กรณีอาชญากรรมทางคอมพิวเตอร์ในรูปแบบ fake e-mail
วันพฤหัสบดีที่ 8 กันยายน 2559 เวลา 08.30-16.00 น.
ณ โรงแรมอมารี ดอนเมือง แอร์พอร์ต ถนนวิภาวดีรังสิต กรุงเทพมหานคร
FAKE

สถิติการปลอมอีเมล์

https://blog.cloudmark.com/2016/04/14/the-top-5-email-wire-fraud-email-attacks-rising-in-frequency-increasing-in-financial-losses/

สถิติภัยคุกคาม ประจำปี พ.ศ. 2559 (ThaiCERT)

ETDA สพธอ www.etda.or.th ThaiCERT Thailand Computer Emergency Response Team a member of ETDA

TH EN แผนผังเว็บไซต์ ค้นหา

แจ้งเหตุภัยคุกคาม กิจกรรม แจ้งเตือนและข้อแนะนำ เอกสารเผยแพร่ บริการ เว็บไซต์ที่เกี่ยวข้อง เกี่ยวกับไทยเซิร์ต

หน้าแรก > เอกสารเผยแพร่ > สถิติภัยคุกคาม 2559

สถิติภัยคุกคาม

ดูสถิติภัยคุกคามปี 2559

สถิติภัยคุกคาม ประจำปี พ.ศ. 2559

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	0	0	0	0	0	0	0	0					**0**
Availability	0	0	0	0	0	0	0	0					**0**
Fraud	98	95	66	73	164	125	104	52					**777**
Information gathering	0	0	0	0	0	0	0	0					**0**
Information security	0	0	0	0	0	0	0	0					**0**
Intrusion Attempts	35	39	36	62	69	70	59	82					**452**
Intrusions	175	51	122	96	53	44	158	60					**759**
Malicious code	97	123	80	104	168	167	49	14					**802**
Other	0	0	0	0	0	0	0	0					**0**
รวม	**405**	**308**	**304**	**335**	**454**	**406**	**370**	**208**					**2790**

สถิติภัยคุกคาม (ETDA)

Cyber Crime. Why Small Businesses Can Lose Big

Whether you run a florist shop, a courier service or a small manufacturing business, you're an attractive target to cyber criminals. You've also got a lot to protect: an estimated 40% of a small business's worth is derived from the information it owns.[1]

Take a stroll down the street to learn where you're vulnerable and what you can do about it.

No business is too small to be a target.[2]

90% of small businesses believe a cyber attack would have a serious impact.

BUT 50% of small businesses don't think that they're targets of cyber crime.

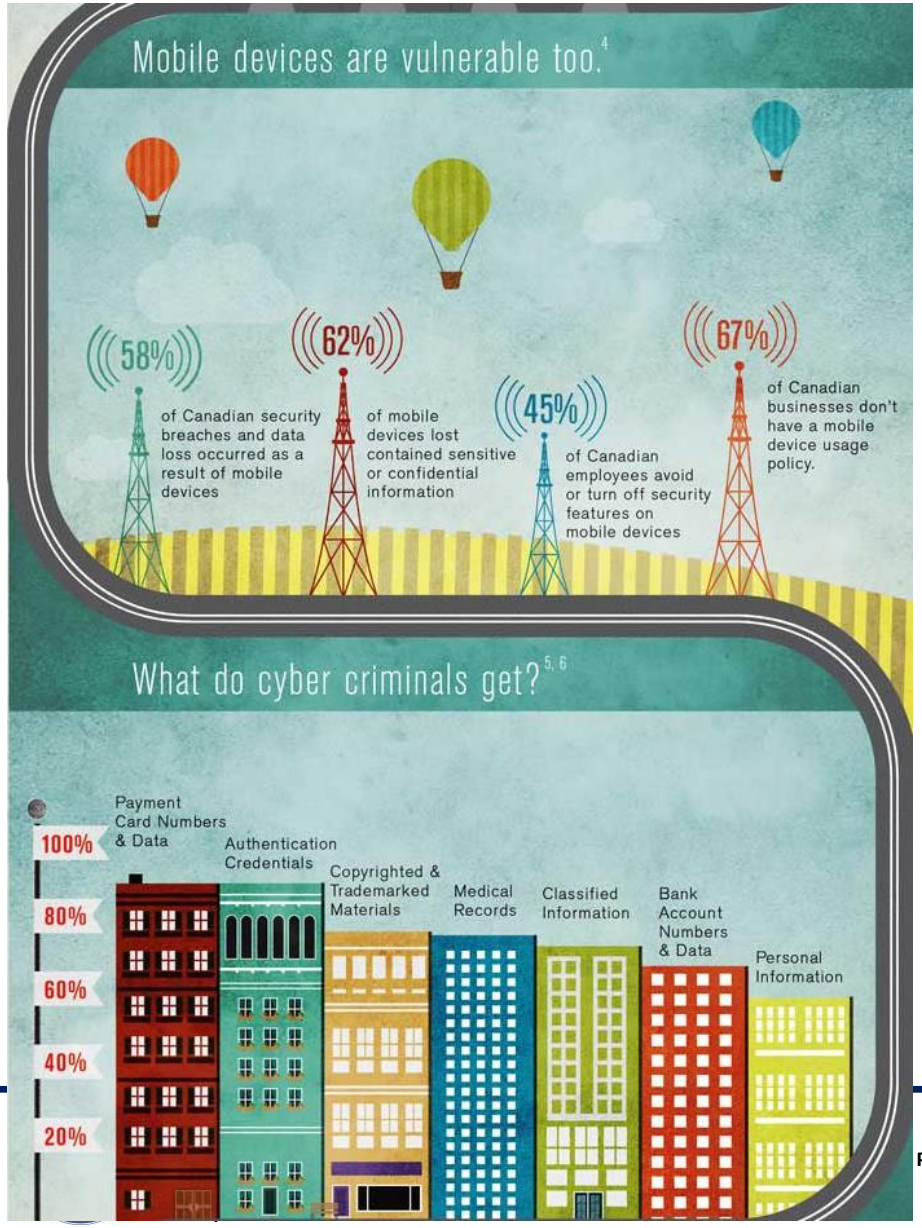
40% of all cyber attacks in 2011 were on small to medium sized businesses.

What are cyber criminals after?

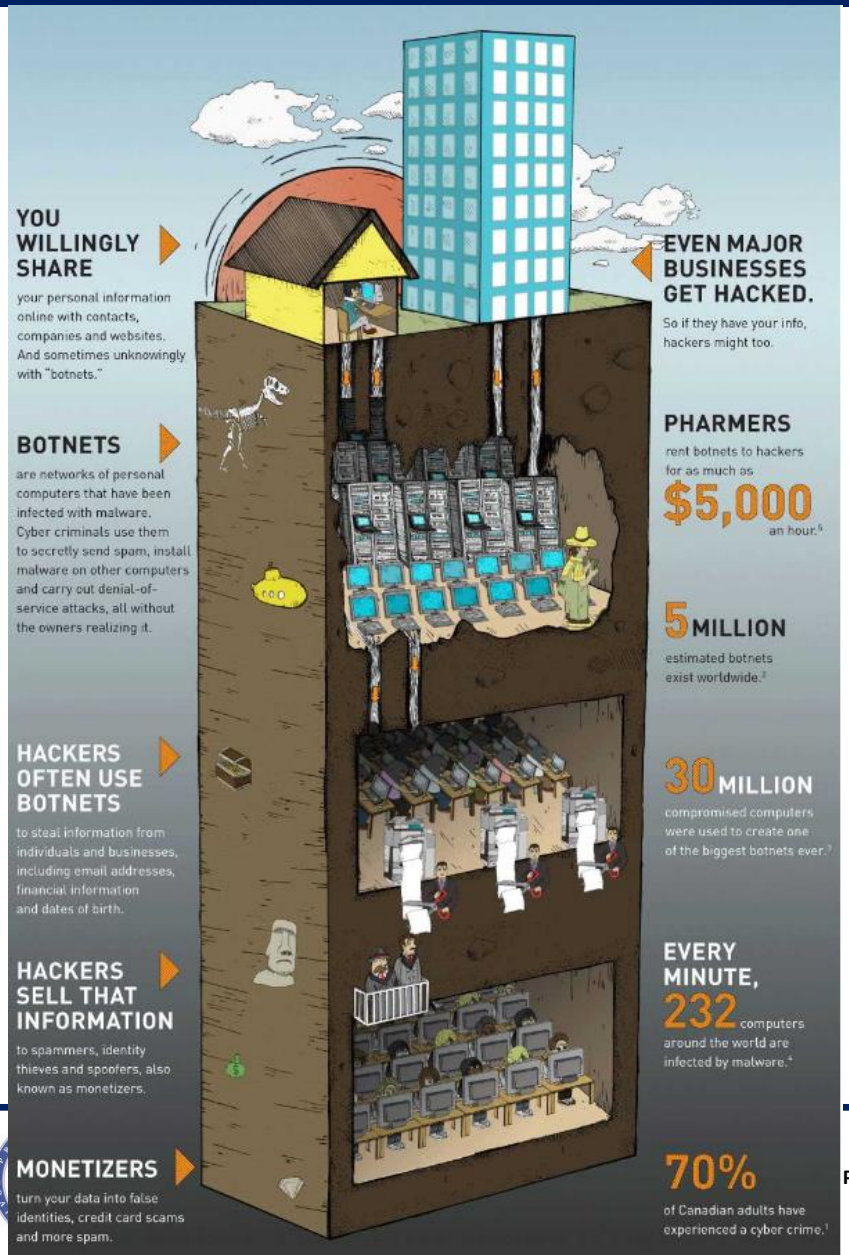
- CUSTOMER RECORDS
- CONTACT LISTS
- EMPLOYEE INFORMATION
- COMPANY BANKING INFO
- SERVERS
- COMPUTER ACCESS

What attacks do businesses face?[3]

Cyber Crime. Why Small Businesses Can Lose Big



The Underground E-economy: Cyber Crime Exposed



Know how to protect yourself online.

Be wary of emails from financial institutions and other organizations that ask for your personal information. If in doubt, call the company to verify the email.

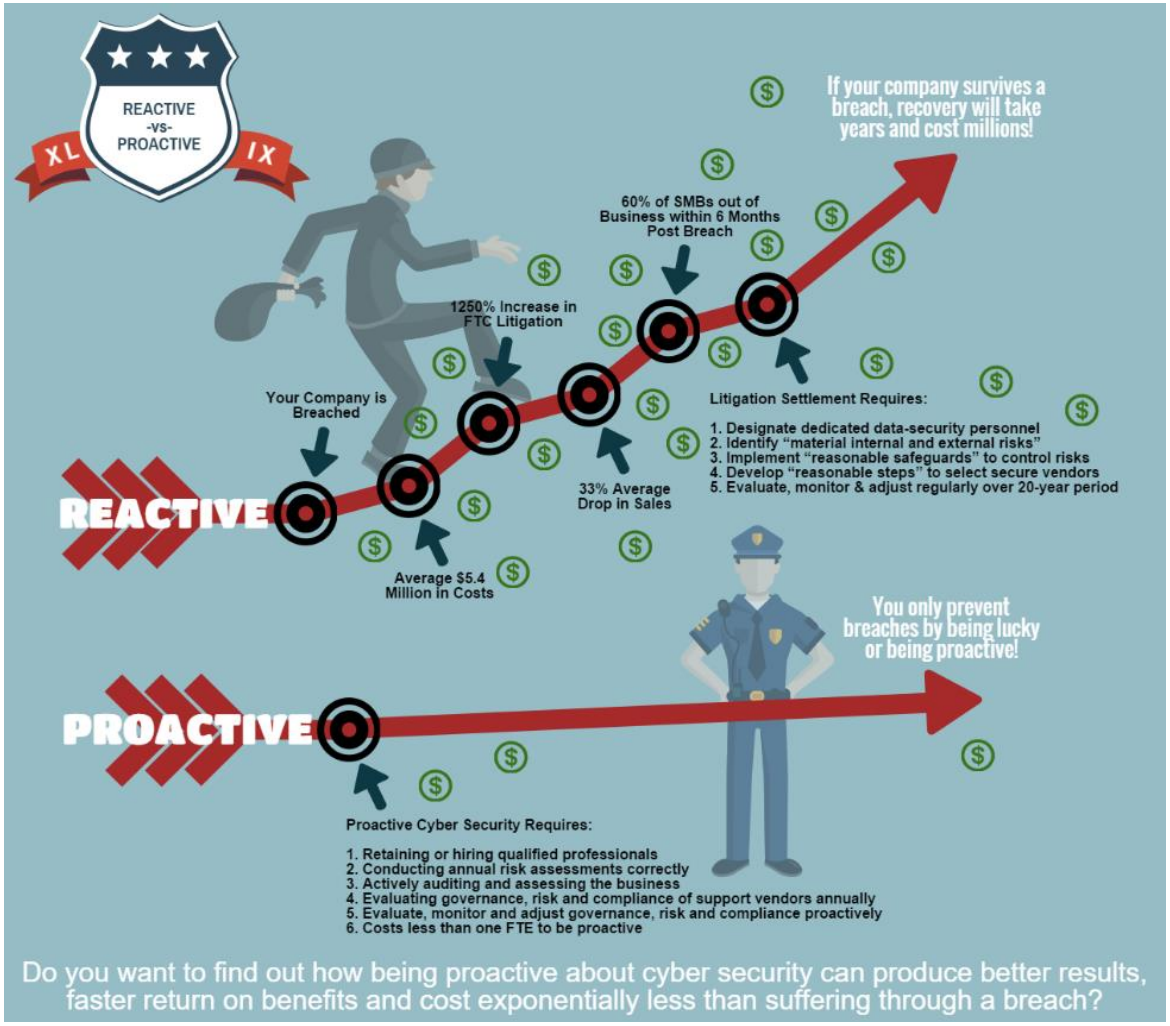
- Don't use your credit card number online unless you know the company you're dealing with is reputable and the website is secure.
- Set different passwords for all the websites you use. And don't forget to update your antivirus software regularly.

Keep your info out of the Underground E-economy.

- Be careful with sharing your personal information like your cell number, address, workplace and social insurance number (SIN). Your SIN number is virtually a key to your identity and credit reports.
- Keep your social media profiles private. Cyber criminals scan them for your personal information.
- Visit Getcybersafe.gc.ca for more tips on how to protect your personal information online.

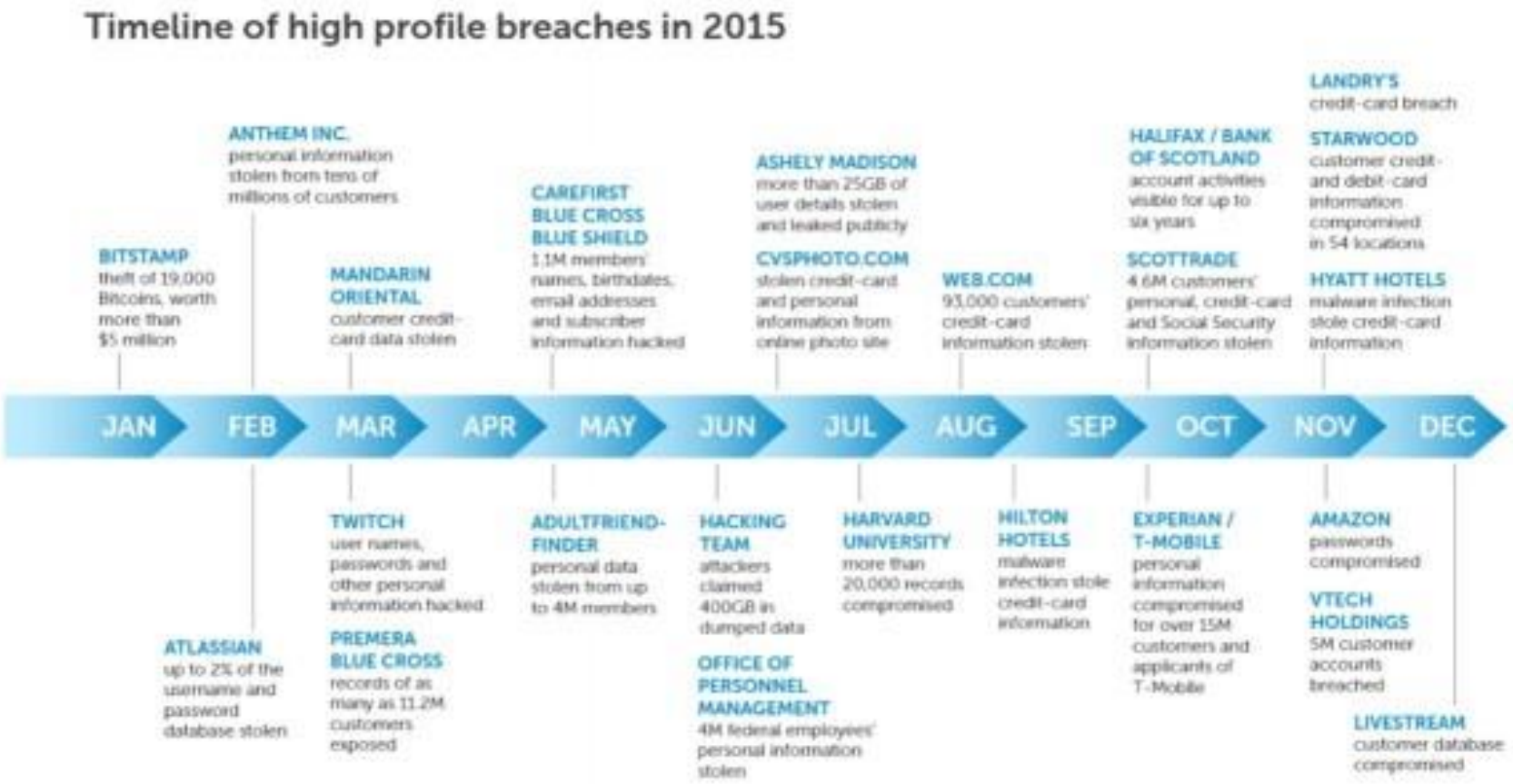
Securing Mail Servers and Content (NIST 800-45) Guidelines on Electronic Mail Security

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce




******
OK

ภัยจากอาชญากรรมไซเบอร์



ภัยจากอาชญากรรมไซเบอร์

แฮคเกอร์เจาะระบบ ATM ออมสินฉกเงิน 12 ล้านสั่งระงับใช้ตู้ชั่วคราว 3 พันเครื่องใช้ตู้ธนาคารอื่นได้ไม่เสียค่าบริการ

ธนาคารออมสินสั่งระงับใช้ตู้เอทีเอ็มเพื่อตรวจสอบหลังถูกกลุ่มคนร้ายแฮกข้อมูลและได้เงินไปกว่า 12 ล้านบาทตั้งแต่ภาคใต้ถึงกทม.

Last updated: 24 สิงหาคม 2559 | 16:12

ออมสิน ปิดบริการตู้ ATM บางส่วน หลังพบเงินของธนาคารที่ใส่ในตู้เอทีเอ็มหายไป21ตู้ ยอดเงิน 12,291,000 บาท แจงเงินหายจากตู้ธนาคาร ย้ำไม่กระทบกับบัญชีหรือเงินฝากลูกค้า ในระหว่างนี้ใช้ตู้เอทีเอ็มธนาคารอื่นได้ไม่เสียค่าธรรมเนียม

ภัยจากอาชญากรรมไซเบอร์

รวบ 6 ผู้ต้องหาขบวนการแฮกเงินหนุ่มอยุธยา 9 แสนจากแบงก์กสิกร-รับสารภาพทำมาแล้ว 9 ครั้งเรียนรู้ช่องโหว่ระบบธนาคารมาเป็นอย่างดี

Last updated: 25 สิงหาคม 2559 | 13:25

เจ้าหน้าที่ตำรวจรวบยกแก๊งคนร้ายฉกเงินหนุ่มอยุธยาสูญเงินในบัญชีกว่า 9 แสน ธนาคารกสิกร รับสารภาพย่ามใจทำมาแล้ว 9 ครั้ง เรียนรู้ระบบของธนาคารมาเป็นอย่างดี-ตร.แจ้งข้อหาลักทรัพย์ผู้อื่น

ภัยจากอาชญากรรมไซเบอร์

ขโมยเงินออนไลน์ อันตรายผ่านมือถือ โดย ประวิทย์ ลี่สถาพรวงศา กรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.)

Last updated: 26 สิงหาคม 2559 | 07:07

ข่าวมิจฉาชีพขโมยเงินเกือบล้านบาทออกจากบัญชีธนาคารของร้านขายอุปกรณ์ประดับยนต์ โดยการหลอกขอสำเนาบัตรประชาชนเจ้าของร้าน แล้วไปติดต่อขอออกซิมการ์ดมือถือเลขหมายของเจ้าของร้าน เพื่อใช้มือถือไปสวมรอยขอรหัสเข้าระบบอินเทอร์เน็ตแบงก์กิ้งหรือธนาคารออนไลน์ของเจ้าของร้านอีกต่อหนึ่ง แล้วโอนเงินเกือบล้านบาทออกไปในเวลาอันรวดเร็ว เป็นข่าวที่สะเทือนขวัญและสร้างความกังวลแก่ผู้ใช้ระบบธนาคารออนไลน์ หรือผู้ที่กำลังจะขอใช้บริการอย่างหลีกเลี่ยงไม่ได้

ภัยจากอาชญากรรมไซเบอร์

แก๊งคอลเซ็นเตอร์

เตือน! แก๊งคอลเซ็นเตอร์ แอบอ้างเป็นเจ้าหน้าที่ DSI ระบาดหนัก มีผู้เสียหายแล้วกว่า1.2ล้านบาท

Last updated: 29 สิงหาคม 2559 | 14:45

ดีเอสไอเตือนประชาชนระวังถูกแก๊งคอลเซนเตอร์อ้างเป็นเจ้าหน้าที่รัฐหลอกโอนเงินผ่านบัญชี ล่าสุดมีผู้เสียหายแล้ว2รายมูลค่ากว่า1.2ล้านบาท

ภัยจากอาชญากรรมไซเบอร์

สตม.รวบ 2 เกาหลีใต้แก๊งคอลเซ็นเตอร์หลอกตุ๋นเงินเหยื่อกว่า 500 รายสูญเงินกว่าพันล้านวอน ก่อนหนีมาซ่อนตัวในไทย

พล.ต.ท.ณัฐธร เพราะสุนทร ผบช.สตม. แถลงผลจับกุม นายซุกวู ยางและนายซางจี ยูน ผู้ต้องหาตามหมายจับตำรวจสากลในความผิดฐานอาชญากรทางการเงินข้ามชาติ (ขอบคุณภาพจาก คม ชัด ลึก)

Last updated: 26 สิงหาคม 2559 | 19:34

ตำรวจตรวจคนเข้าเมืองรวบ 2 หนุ่มแก๊งคอลเซ็นเตอร์ชาวเกาหลีใต้ผู้ต้องหาตามหมายจับของตำรวจสากลตั้งแก๊งคอลเซนเตอร์หลอกโกงเงินข้ามประเทศกว่า 500 ราย เหยื่อสูญเงินกว่า 1,700 ล้านวอนประมาณ 53 ล้านบาท ก่อนหนีมาซ่อนตัวในไทย

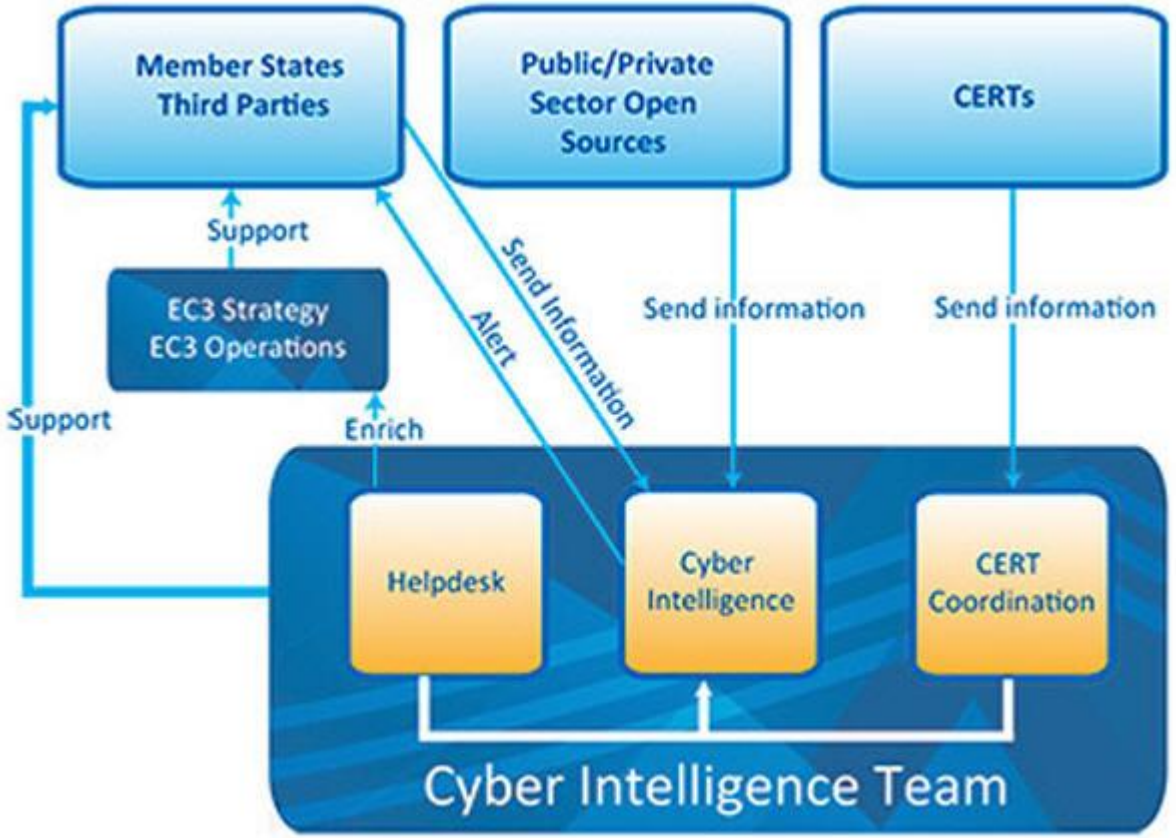
ภัยจากอาชญากรรมไซเบอร์

ผู้เชี่ยวชาญรัสเซียแนะธนาคารไทยจัดตั้งหน่วยสืบราชการลับไซเบอร์ตอบโต้กลุ่มแฮก ATM

Last updated: 4 กันยายน 2559 | 10:39

ภายหลังจากการปล่อยไซรัสมัลแวร์เพื่อแฮกเงินจากตู้เอทีเอ็มของธนาคารออมสิน ผู้เชี่ยวชาญด้านความมั่นคงไซเบอร์ของรัสเซียแนะนำธนาคารไทยต้องพัฒนาหน่วยสืบราชการลับไซเบอร์ขึ้นมาศึกษาและรับมือกับกลุ่มอาชญากรรมเลือดใหม่ในโลกไซเบอร์

ภัยจากอาชญากรรมไซเบอร์



ภัยจากอาชญากรรมไซเบอร์

TEEN WHO HACKED CIA DIRECTOR'S EMAIL TELLS HOW HE DID IT

CIA director John Brennan. CHRIS MAGDALONI/AP

A HACKER WHO claims to have broken into the AOL account of CIA Director John Brennan says he obtained access by posing as a Verizon worker to trick another employee into

https://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/

ภัยจากอาชญากรรมไซเบอร์

อาชญากรรมไซเบอร์ (Cyber Crime) ภัยคุกคามของเศรษฐกิจรูปแบบใหม่

ภัยคุกคามทางไซเบอร์ได้เพิ่มระดับความรุนแรง และมีความซับซ้อนในการโจมตีมากขึ้น ความเสียหายที่เกิดจากการอาชญากรรมและการโจมตีทางไซเบอร์จะมีผลต่อธุรกิจอย่างร้ายแรง ซึ่งในทุกองค์กรทั้งภาครัฐ และภาคเอกชน จะต้องตระหนักและต้องมีการกำหนดมาตรการในการป้องกันภัยคุกคามทางไซเบอร์ดังกล่าว

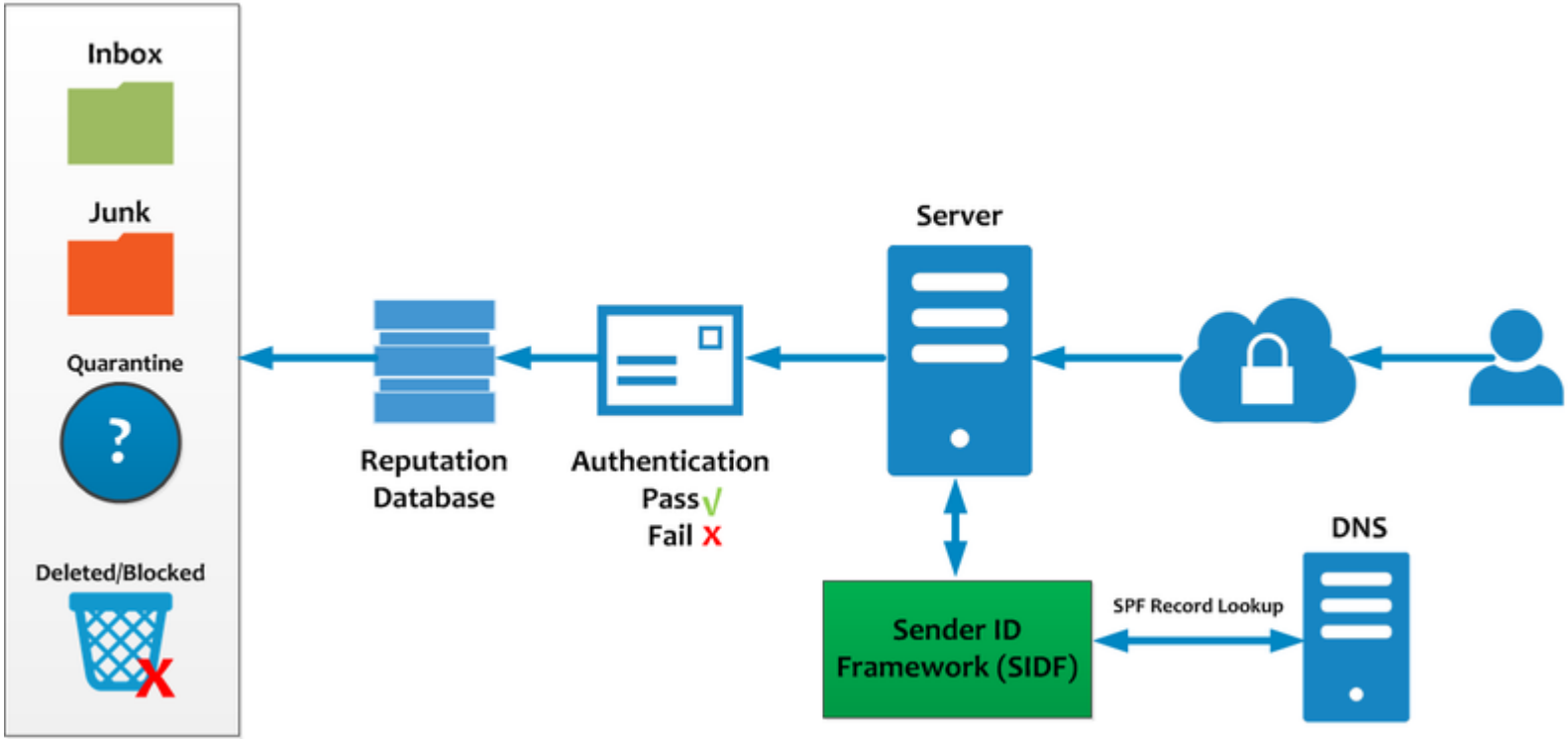
1. **มีการคุกคามอย่างไร้ขอบเขต**
    1. การเปลี่ยนแปลง
    2. Mobility and consumerization
    3. ระบบ Cloud
2. **ความสามารถของอาชญากรทางไซเบอร์ที่มีจำนวนเพิ่มมากขึ้นอย่างไม่น่าเชื่อ**
3. **อุปสรรคที่องค์กรต้องเผชิญในปัจจุบัน เพื่อให้องค์กรสามารถเอาชนะอาชญากรทางไซเบอร์**
    1. ไม่มีความคล่องตัวในการดำเนินการ
    2. องค์กรไม่มีงบประมาณสำหรับความมั่นคงปลอดภัยไซเบอร์
    3. ขาดทักษะด้านความมั่นคงปลอดภัยไซเบอร์
4. **การใช้งานเทคโนโลยีทำให้เกิดภัยคุกคามเพิ่มมากขึ้น**

ภัยจากอาชญากรรมไซเบอร์

Fake Email คือ อะไร ?

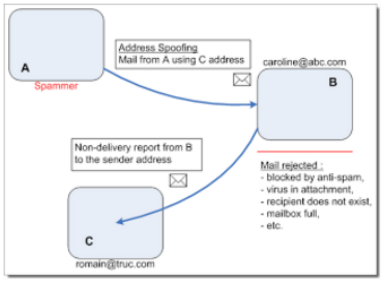
Fake Email คือ การที่ Hacker ทำการสร้าง Email เลียนแบบชื่อ Email ของคุณขึ้นมา เพื่อมีวัตถุประสงค์ใช้ชื่อ Email ของคุณส่งข้อมูลไปหาบุคคลอื่นๆ เช่น ส่งเลขที่บัญชีของ Hacker ไปหาลูกค้า เพื่อให้ลูกค้าของคุณหลงเชื่อว่าคุณมีการเปลี่ยนแปลงเลขที่บัญชี และทำการโอนเงินมายังบัญชีของ Hacker แทน

อีเมล์ทำงานอย่างไร



Fake Emails Or Email Spoofing in DOS

Fake Emails Or Email Spoofing in DOS



Well, let's get started then. Well in order to fake (spoof) an email, you first need to have an SMTP (Simple Mail Transfer Protocol) server that you can use to send the email from. How do you find one? Simple

First decide what server you want to use to send email from, for this example I will use Hotmail. Now go to Start --> Run --> Type the word 'cmd' without the '
Now that you have DOS open, type the following command:

```
nslookup -querytype=mx hotmail.com
```

You can replace hotmail.com with whatever site's mail servers you want to use. Anyway, when you execute that command, the following output comes out:

```
Non-authoritative answer:
hotmail.com     MX preference = 5, mail exchanger = mx2.hotmail.com
hotmail.com     MX preference = 5, mail exchanger = mx3.hotmail.com
hotmail.com     MX preference = 5, mail exchanger = mx4.hotmail.com
hotmail.com     MX preference = 5, mail exchanger = mx1.hotmail.com
```

The SMTP servers are mx2.hotmail.com, mx3.hotmail.com, etc. Now, for the next part of the tutorial, I will be using mx2.hotmail.com.

Now, let's get started spoofing the actual email! You still have DOS open right, good. Now type the following command to connect with Hotmail's SMTP server. You can replace the server name with your preferred server.

```
telnet mx2.hotmail.com 25
```

You will see whatever welcome message they give. Now type the following command:

```
HELO
```

You'll get a message, usually with your IP. Now the next command shows what email you want to pretend to be sending from. I'll use the fake email lala@lala.org

```
MAIL FROM: lala@lala.org
```

You should get a 250 OK. Now we will type a command to choose who we want the email to go to. I will use the fake email blah@blah.com

```
RCPT TO: blah@blah.com
```

Now you get another 250 OK. Now we will start the actual message. Type:

```
DATA
```

Then type your message. Be sure to add title headers, like Subject, To, From, etc. so the email looks real. After you are done typing the email, press Enter, then type a . then press Enter again. Your email has been sent!

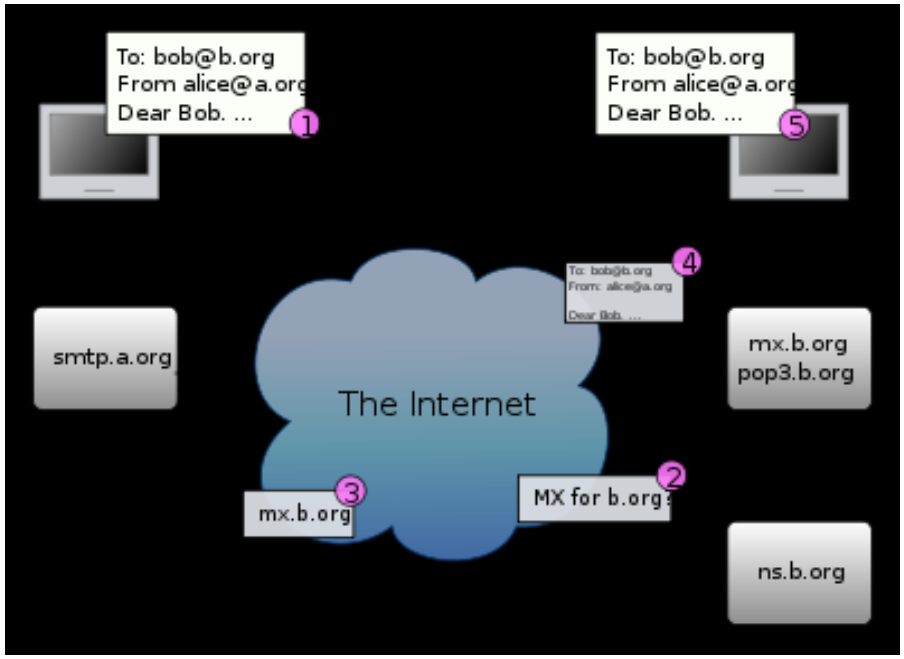
Now type **quit** to end the connection to the server.

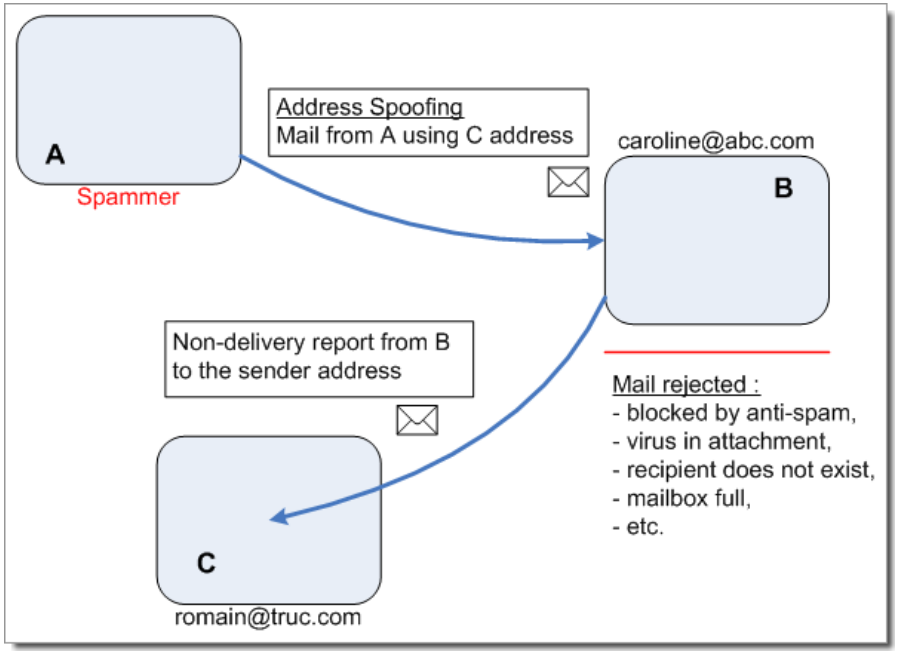
That's all for now, hope you learned something!

SPAMBOG ALTERNATIVES

http://www.alternativesoftwares.com/spambog/

E-mail Spoofing



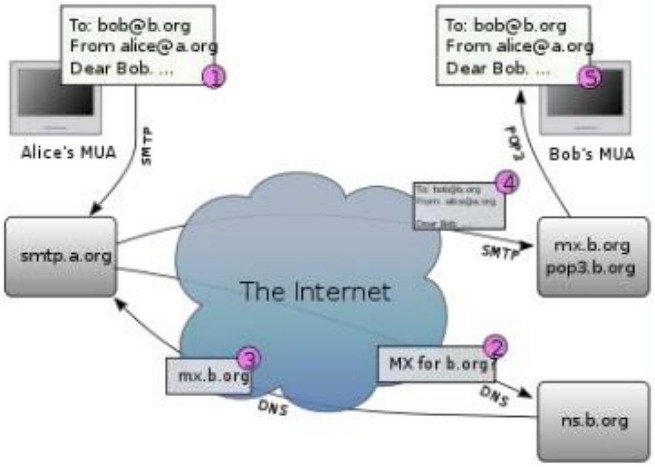


E-mail Spoofing

8K Miles Cloud Solutions

How Email is sent?

- Internet was built on trust and email also works in the same fashion
- No authentication exists between ISP to send emails
- SPAM abuse is high as this trust is misused



3

E-mail Spoofing

From: onlinebanking@ealerts.bankofamerica.com
Subject: Bank Of America Alert : Account Suspended
Date: Tue, 26 Apr 2011 05:41:38 +0200

Bank of America Higher Standards Online Banking

Dear Valued Member,

We noticed invalid login attempts into you account online from an unknown IP address .
Due to this, we have temporarily suspended your account.
We need you to update your account information for your online banking to be re-activ
please update your billing information today by clicking

here www.bankofamerica.com/account/re-activation/ After a few clicks,

just verify the information you entered is correct.
Sincerely,

BOA Member Services Team
P.S. The link in this message will be expire within 24 Hours . You have to update your pay

© 2010 BOA LLC. All Rights Reserved.

TSB Bank
expect more

Dear Customer,

Getting the picture?

Statement of account dated for 15-04-2013 to 15-05-2013 of your account

Your Bank Account Statement Is Now Available To Be Viewed Online.

To View Your Statement, Please click the "Log In" below to access your TSB Bank Account Online.

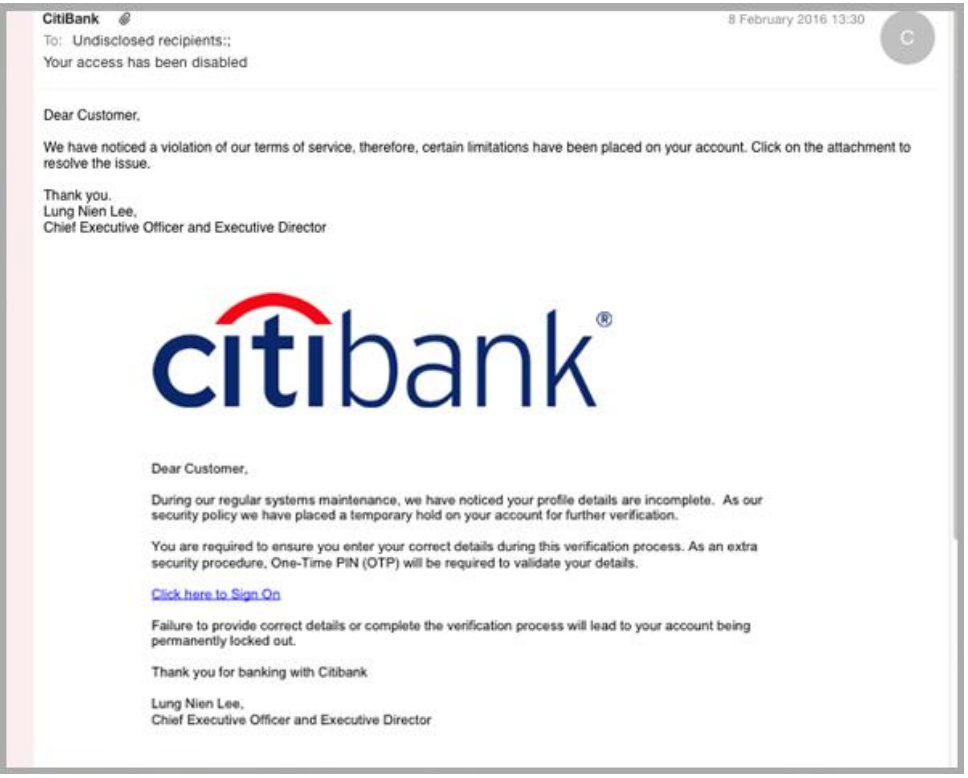
Overly enthusiastic use of capitals

Log In

TSB Bank Customer Service.

Â© 2013 Copyright TSB Bank. All rights reserved.

E-mail Spoofing



CitiBank 8 February 2016 13:30

To: Undisclosed recipients::

Your access has been disabled

Dear Customer,

We have noticed a violation of our terms of service, therefore, certain limitations have been placed on your account. Click on the attachment to resolve the issue.

Thank you.
Lung Nien Lee,
Chief Executive Officer and Executive Director

citibank®

Dear Customer,

During our regular systems maintenance, we have noticed your profile details are incomplete. As our security policy we have placed a temporary hold on your account for further verification.

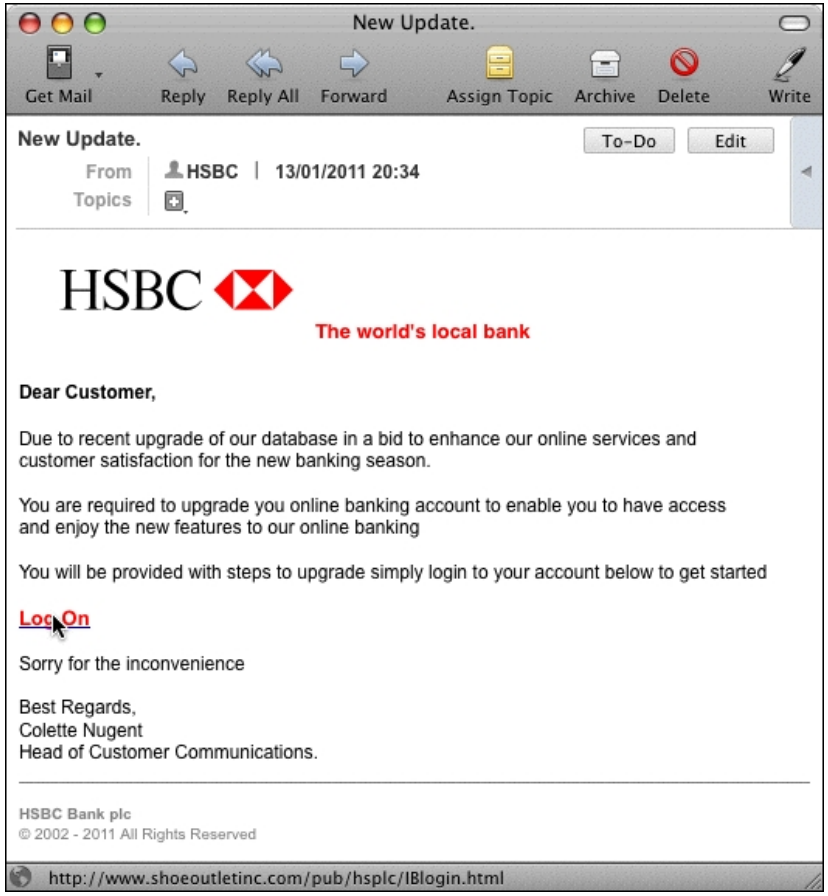
You are required to ensure you enter your correct details during this verification process. As an extra security procedure, One-Time PIN (OTP) will be required to validate your details.

Click here to Sign On

Failure to provide correct details or complete the verification process will lead to your account being permanently locked out.

Thank you for banking with Citibank

Lung Nien Lee,
Chief Executive Officer and Executive Director



New Update.

Get Mail | Reply | Reply All | Forward | Assign Topic | Archive | Delete | Write

New Update. To-Do Edit

From HSBC | 13/01/2011 20:34

Topics

HSBC

The world's local bank

Dear Customer,

Due to recent upgrade of our database in a bid to enhance our online services and customer satisfaction for the new banking season.

You are required to upgrade you online banking account to enable you to have access and enjoy the new features to our online banking

You will be provided with steps to upgrade simply login to your account below to get started

Log On

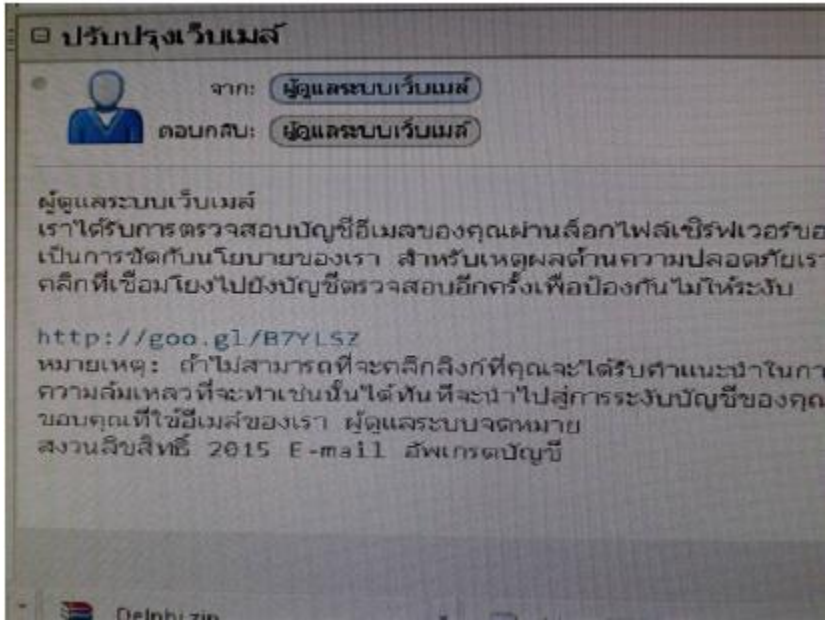
Sorry for the inconvenience

Best Regards,
Colette Nugent
Head of Customer Communications.

HSBC Bank plc
© 2002 - 2011 All Rights Reserved

http://www.shoeoutletinc.com/pub/hsplc/IBlogin.html

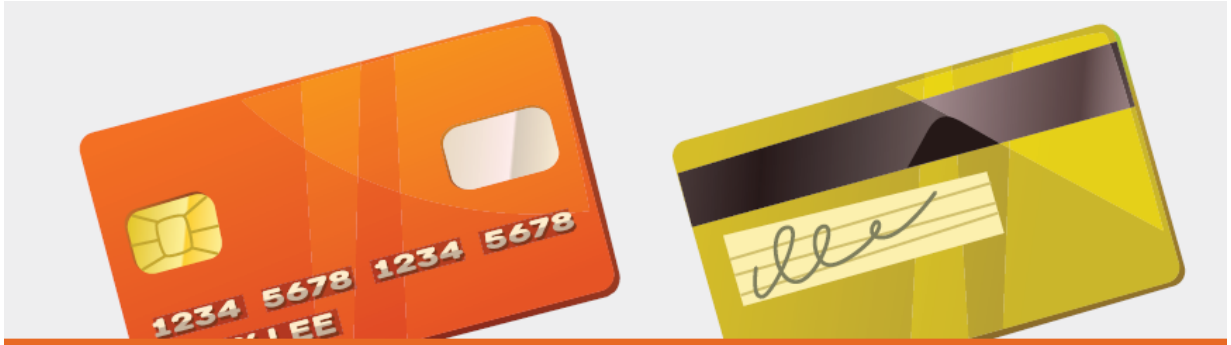
ระวังอีเมลหลอกลวง (Phishing) มุ่งโจมตีหน่วยงานภาครัฐในประเทศไทย



เหยื่อหรือผู้ใช้งานอีเมลที่หลงเชื่อ คลิกลิงก์ดังกล่าว จะถูกพาไปยังหน้า เว็บ **Phishing** (หน้าเว็บเพจที่ผู้ไม่หวังดีสร้างขึ้นเพื่อหลอกลวง) ดังรูป โดยเป็นแบบฟอร์มสอบถามข้อมูลส่วนบุคคล ได้แก่ ชื่อเต็ม ที่อยู่อีเมล ชื่อผู้ใช้ และรหัสผ่าน และหากผู้ใช้งานหลงเชื่อกรอกข้อมูล ดังกล่าวก็จะทำให้ข้อมูลส่วนตัวถูกส่งไปยังผู้ไม่หวังดีทันที

https://www.thaicert.or.th/alerts/user/2015/al2015us003.html

แฮกเกอร์ใช้มัลแวร์เจาะ ATM ขโมยเงินหลายประเทศ



ขยายจากเม็กซิโก แฮกเกอร์ใช้มัลแวร์เจาะ ATM ขโมยเงินในหลายประเทศ

จากเหตุการณ์ก่อนหน้าที่แฮกเกอร์เคยเจาะระบบ ATM ใน Mexico เพื่อขโมยเงินในตู้ ปัจจุบันพบเหตุการณ์ในลักษณะเดียวกันทั่วโลกโดยเฉพาะในภูมิภาคเอเชียและประเทศรัสเซีย นอกจากนี้ยังพบตู้ ATM จำนวน 50 เครื่องในแถบยุโรปตะวันออกถูกโจมตีด้วย ซึ่งตำรวจอินเตอร์โปลกำลังดำเนินการสืบสวน

สำหรับวิธีการเจาะระบบของแฮกเกอร์นั้น มีดังนี้คือ

1. แฮกเกอร์แอบเชื่อมต่อมือถือที่มีมัลแวร์ชื่อ Ploutus กับ ATM ผ่าน USB แล้วตั้งมือถือทิ้งเอาไว้ในตู้ เมื่อ ATM ถูกเชื่อมต่อกับมือถือก็จะติดมัลแวร์และตกอยู่การควบคุมของแฮกเกอร์

2. แฮกเกอร์ส่งคำสั่งผ่าน SMS ไปยังมือถือที่เชื่อมต่อกับ ATM ให้ ATM ถอนเงินที่อยู่ในตู้ เพื่อให้แนบเนียนอาจให้คนหนึ่งแกล้งทำเป็นกดเงิน ในขณะที่อีกคนซึ่งอยู่ห่างออกไปส่ง SMS ทำให้สังเกตความผิดปกติได้ยาก

การโจมตีนี้เป็นการขโมยเงินในตู้โดยตรง ต่างจาก ATM Skimming ที่ขโมยเงินจากบัญชีของผู้ใช้งาน และสะดวกกว่าเพราะไม่ต้องขโมย PIN และข้อมูลเพื่อสร้างบัตรปลอม

ระวังภัย ระวังภัย อีเมลหลอกลวง "Your Facebook login is currently removed" มีไฟล์แนบเป็นมัลแวร์ขโมยข้อมูล

43 SMEs ไทย ตกเป็นหนึ่งในเป้าหมายของปฏิบัติการสอดแนมทางไซเบอร์ Grabit

บริษัทด้านความมั่นคงปลอดภัย Kaspersky ค้นพบภัยคุกคามทางไซเบอร์ชื่อว่า Grabit ซึ่งเป็นปฏิบัติการที่มุ่งเน้นสอดแนมข้อมูลเชิงธุรกิจ และสามารถขโมยไฟล์ได้กว่า 10,000 ไฟล์จากผู้ประกอบการธุรกิจขนาดกลางและขนาดย่อมที่ตั้งอยู่ในประเทศไทย อินเดีย และสหรัฐอเมริกา เป็นส่วนใหญ่ โดยมีเป้าหมายเป็นกลุ่มประเภทธุรกิจ เช่น ธุรกิจเคมีภัณฑ์ นาโนเทคโนโลยี การศึกษา การเกษตร สื่อ การก่อสร้าง ฯลฯ

ในโลกไซเบอร์นั้นทุกองค์กรมีความเสี่ยงที่จะถูกภัยคุกคามโจมตีเท่ากันหมด และภัยคุกคามทางไซเบอร์ Grabit ก็ได้แสดงให้เห็นว่าเป้าหมายของการโจมตีเพื่อสอดแนมและขโมยข้อมูลนั้นไม่ได้จำกัดอยู่เพียงแค่องค์กรใหญ่ที่มีชื่อเสียงเท่านั้น ธุรกิจขนาดกลางและขนาดย่อมก็สามารถตกเป็นเป้าการโจมตีได้เช่นกัน ถ้าหากธุรกิจเหล่านั้นมีสิ่งที่ผู้ไม่หวังดีต้องการ เช่น เงิน และข้อมูลลับ

การทำงานของการโจมตี Grabit นั้นจะเริ่มจากการส่งอีเมลเป็นไฟล์เอกสาร (.doc) เข้ามายังกล่องจดหมายของเหยื่อ โดยหลังจากที่เหยื่อหลงเชื่อดาวน์โหลดไฟล์แนบโปรแกรมสอดแนมจะถูกส่งมาจากเซิร์ฟเวอร์ ซึ่งส่วนใหญ่จะเป็นเซิร์ฟเวอร์ทั่วไปที่ถูกแฮกและเข้าควบคุมโดยแฮกเกอร์ จากการรายงานนั้นโปรแกรมสอดแนมที่แฮกเกอร์ใช้คือโปรแกรม HawkEye ซึ่งมีความสามารถในการตรวจจับการใช้งานของผู้ใช้ด้วยการบันทึกการกดแป้นพิมพ์ โดยแฮกเกอร์สามารถใช้เซิร์ฟเวอร์เพียงหนึ่งเซิร์ฟเวอร์ในการขโมยข้อมูลต่าง ๆ ของเหยื่อได้เป็นจำนวนมาก ดังนี้ ชื่อบัญชี 3,023 ชื่อ รหัสผ่าน 2,887 รหัส อีเมล 1,053 อีเมล จาก 4,928 ระบบทั้งภายในและภายนอก โดยเป็นข้อมูลที่สามารถใช้เพื่อยืนยันตัวตนกับบริการต่าง ๆ เช่น Outlook, Facebook, Skype, Google mail, Yahoo, LinkedIn และ Twitter เป็นต้น อีกทั้งยังรวมไปถึงเลขบัญชีธนาคารของเหยื่อ

บริษัท Kaspersky ได้ให้วิธีการตรวจสอบ และป้องกันจากปฏิบัติการสอดแนมทางไซเบอร์ Grabit มาดังนี้

1. ตรวจสอบไฟล์ที่ได้รับการเก็บไว้ใน “C:\Users\\AppData\Roaming\Microsoft” ว่ามีไฟล์ประเภท executable file (นามสกุลของไฟล์คือ .exe) หรือไม่

62 ระวังภัย อีเมลหลอกลวง "Your Facebook login is currently removed" มีไฟล์แนบเป็นมัลแวร์ขโมยข้อมูล

ขณะนี้มีอีเมลปลอมซึ่งอ้างว่าส่งมาจากทาง Facebook กำลังระบาด โดยใช้หัวเรื่อง "Your Facebook login is currently removed" (หรือแปลเป็นภาษาไทยว่า "บัญชีเฟซบุ๊กของคุณถูกลบออก") เพื่อดึงดูดความสนใจและหลอกล่อให้ผู้รับเปิดอ่าน อีเมลดังกล่าวมีไฟล์แนบที่เป็นมัลแวร์ ซึ่งหากผู้ใช้เปิดไฟล์ดังกล่าว จะถูกติดตั้งมัลแวร์ลงในเครื่องเพื่อสอดแนมและดักเก็บข้อมูลของผู้ใช้ เช่น ข้อมูลส่วนตัวหรือข้อมูลทางการเงิน เป็นต้น

หากผู้ใช้ได้รับอีเมลที่มีหัวเรื่องดังกล่าวและเผลอเปิดไฟล์แนบไปแล้ว ให้รีบทำการสแกนไวรัสบนคอมพิวเตอร์และกำจัดไวรัสทิ้งโดยทันที วิธีการป้องกันจากอีเมลอันตรายนี้คือตรวจสอบรายละเอียดก่อนเปิดอ่านอีเมลทุกครั้ง และถ้าหากพบความผิดปกติ ให้ลบอีเมลเหล่านี้ทิ้งทันที โดยห้ามเปิดไฟล์ที่แนบมากับอีเมล นอกเหนือจากนี้ ผู้ใช้ควรต้องอัปเดตโปรแกรมแอนติไวรัสให้ทันสมัยอยู่เสมออีกด้วย

เตือนระวังเปิดอีเมลเจอมัลแวร์เรียกค่าไถ่ระบาด

63 เตือนระวังเปิดอีเมล
เจอมัลแวร์เรียกค่าไถ่ระบาด
ภัยท้าทายความมั่นคงโลกไซเบอร์

ไทยเซิร์ต ออกประกาศแจ้งเตือนให้ระวังภัย รวมถึงแนะนำวิธีการป้องกันความเสียหายจากมัลแวร์หรือโปรแกรมประสงค์ร้าย ที่เรียกว่า Ransomware หรือมัลแวร์เรียกค่าไถ่ สืบเนื่องจากกรณีล่าสุดที่ สำนักเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ กรมสอบสวนคดีพิเศษ (ดีเอสไอ) มีหนังสือแจ้งเตือนแก่เจ้าหน้าที่ภายในดีเอสไอ เรื่อง "แจ้งเตือนการเปิดอ่านจดหมายอิเล็กทรอนิกส์" ซึ่งมีมัลแวร์/ไวรัสส่งผ่านจดหมายอิเล็กทรอนิกส์ การเปิดไฟล์แนบจะทำให้ติดมัลแวร์เรียกค่าไถ่นี้ทันที

เมื่อเปิดไฟล์แนบ มัลแวร์จะโจมตีด้วยวิธีการเข้ารหัสลับ (Encryption) ไฟล์เอกสารต่าง ๆ บนคอมพิวเตอร์ที่ติดมัลแวร์ รวมถึงเอกสารที่แชร์ผ่านเครือข่ายและจากอุปกรณ์ External Drive ที่เสียบอยู่กับเครื่องคอมพิวเตอร์ ซึ่งไฟล์ของเครื่องเหยื่อจะยังอยู่ แต่ไม่สามารถ

ระวังภัย แอพปลอม

รูปที่ 1 ประกาศใน Twitter ของธนาคารไทยพาณิชย์

จากการตรวจสอบเพิ่มเติม พบว่าแอปพลิเคชันปลอมดังกล่าวสร้างโดยนักพัฒนาที่ใช้ชื่อ ว่า SCIENTIFIKA MEDIA โดยนำ ขึ้นสู่ Google Play Store เมื่อวันที่ 25 มีนาคม และยังพบว่าผู้พัฒนารายนี้ ได้พัฒนาแอปพลิเคชันปลอมของธนาคารไทยรวม 5 แห่งคือ

ธนาคารกรุงไทย

ธนาคารกรุงเทพ

ธนาคารไทยพาณิชย์

ธนาคารกรุงศรีอยุธยา และ

ธนาคารธนชาต

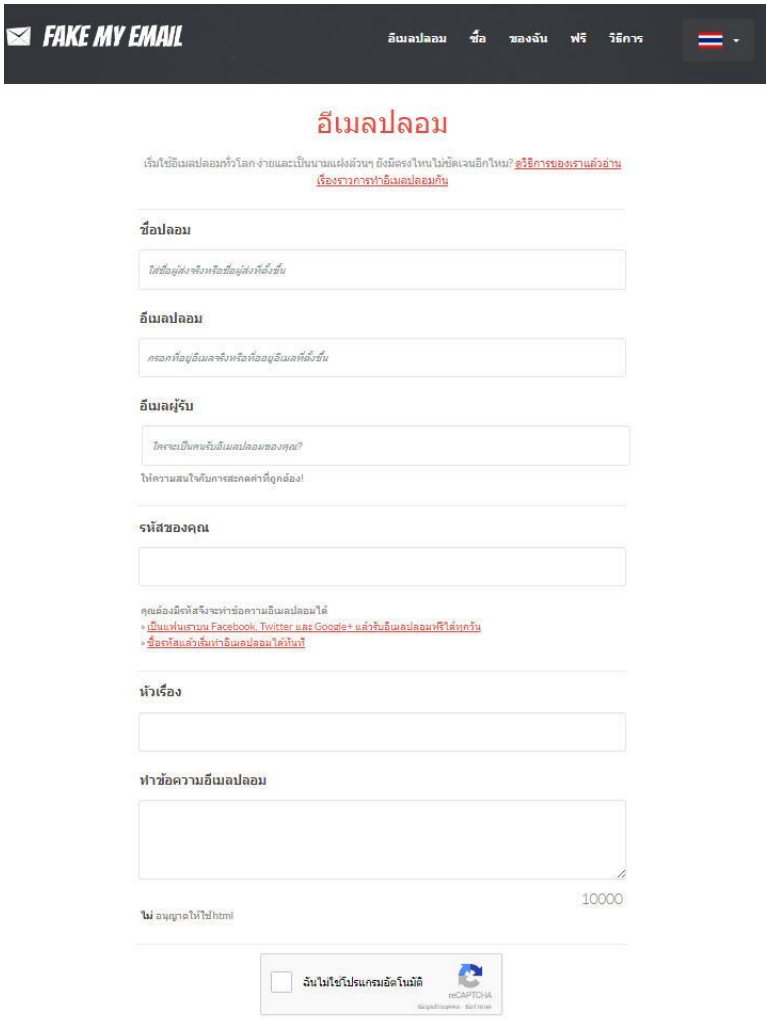
รวมถึงแอปพลิเคชันปลอมของธนาคารอื่น ๆ ในต่างประเทศด้วย

อีเมลปลอม


FAKE MY EMAIL
อีเมลปลอม
ซื้อ
ของฉัน
ฟรี
วิธีการ
อีเมลปลอม
ที่อยู่และข้อความอีเมลปลอม ระบุผู้ส่งเล่นตลกใด ๆ ที่อยู่อีเมล และส่งข้อความอีเมลเล่นตลก จริง
อีเมลปลอม »
เจมส์ส่งอีเมลปลอมถึงลิซ่าด้วยที่อยู่อีเมลของเดวิด เพราะเขาขี้อายมาก
จาก: David@gmail.com 13:37 PM
สวัสดีลิซ่า ผมตกหลุมรักคุณเข้าแล้ว! จุ๊บๆ
ลิซ่าอ่านเมลปลอมแล้วมีความสุข
ตอบกลับ: David@gmail.com 14:15 PM
:) มาดื่มกาแฟหรืออะไรกันหน่อยไหม?
» รับคุณสมบัติในการเปลี่ยนหรือปลอมสิ่งที่คนอื่นเห็นบนข้อความอีเมลเวลาได้รับเมลจากคุณ เขาจะไม่รู้เลยว่าเป็นคุณ! คุณสามารถเลือกที่อยู่อีเมลและชื่อที่อยู่ในใจของคุณ เพื่อส่งข้อความอีเมลปลอมได้ อีกฝ่ายจะคิดว่าคุณเป็นคนอื่น สิ่งนี้ทำได้ง่ายๆ และได้ผลกับทุกอีเมล ทั่วโลก!


ฉันจะเริ่มได้อย่างไร?
คุณสามารถเริ่มทำอีเมลปลอมได้ฟรี ง่ายๆ แค่เป็นแฟนบน Facebook, Twitter หรือ Google+ เราให้คุณส่งข้อความอีเมลปลอมฟรีทุกวันแก่ทุกคนที่กดถูกใจบนหน้าแฟนเพจของเรา
หากคุณซื้อรหัส คุณจะสามารถเริ่มใช้ที่อยู่อีเมลปลอมได้ทันที
ซื้ออีเมลปลอม
รายละเอียด
ทันทีที่คุณซื้อรหัสอีเมลปลอม คุณจะสามารถวางข้อความอีเมลปลอมได้ คุณสามารถตั้งชื่อที่อยู่อีเมลอื่นเป็นผู้ส่งและจัดเตรียมข้อความอีเมลของคุณได้
ดูขั้นตอนการส่งข้อความเมลปลอมเหล่านี้
1. กรอกข้อมูลที่จำเป็นทั้งหมด ที่อยู่อีเมลปลอม ชื่ออีเมลปลอม และที่อยู่อีเมลผู้รับ
2. ป้อนรหัสที่ถูกต้อง หัวเรื่อง และเตรียมข้อความอีเมลปลอมของคุณ
3. เรียบร้อย! ผู้รับจะได้รับอีเมลปลอมของคุณในไม่ช้า
รับแอป Fake my Email ฟรีบนมือถือของคุณ

อีเมลปลอม



ง่ายขนาดนี้จริงหรือ?

จริง การส่งข้อความอีเมลปลอมทำได้ง่ายดายมาก เราอยากอวดให้คุณเห็นว่าการเลียนแบบอีเมลคนอื่นทำได้ง่ายแค่ไหน โปรดระวังหากคุณเป็นคนหนึ่งที่จะได้รับข้อความอีเมลที่อาจก่อให้เกิดความเข้าใจผิดได้มาก อาจมีบุคคลที่สามที่ประสงค์ร้ายเข้ามาได้เสมอ

ปลอดภัยไหม?

อีเมลปลอมและข้อมูลทั้งหมดของคุณจะถูกส่งแบบเข้ารหัส ผ่านทางโปรโตคอลความปลอดภัย HTTPS (SSL หรือ Secure Sockets Layer) ซึ่งเป็นเทคโนโลยีเดียวกับที่ธนาคารใช้ปกป้องข้อมูลของคุณ บุคคลที่สามไม่สามารถเข้ามาอ่านได้แน่นอน นอกจากนี้เรายังเก็บรักษาข้อมูลการชำระเงิน ข้อมูลส่วนตัว และอีเมลปลอมของคุณไว้เป็นความลับให้อีกด้วย

แล้วการส่งข้อความ โทร หรือ WhatsApp ปลอมล่ะ?

อย่างที่คุณคิดนั่นละ ถูกต้อง! เราช่วยส่งข้อความ โทรออก และ WhatsApp ปลอมด้วย! แค่ช่วยปรับปรุงประสบการณ์การปลอมของคุณเท่านั้น:

» https://www.fakemytextmessage.com
» https://www.fakemycallid.com
» http://www.fakewhats.com

โปรดทราบ

บริการอีเมลปลอมของเราขอเรียนชี้แจงว่า ผู้ใช้งานต้องรับผิดชอบความเสียหายที่อาจเกิดขึ้นเองทั้งหมด โปรดทำการส่งอีเมลปลอมด้วยความระมัดระวัง

เป้าหมาย บุคคล และผู้มีตำแหน่งในบริษัท ธุรกิจ

- คณะกรรมการบริษัท (Board Member)
- ประธานเจ้าหน้าที่บริหาร/ประธาน/กรรมการผู้จัดการ (Chief Executive Officer/President/Managing Director)
- ประธานเจ้าหน้าที่ปฏิบัติ (Chief Operating Officer)
- ประธานเจ้าหน้าที่การเงิน/นักบริหารเงิน/ผู้ตรวจสอบบัญชี (Chief Financial Officer/Treasurer/Comptroller)
- ประธานเจ้าหน้าที่ฝ่ายบริหาร/ผู้อานวยการฝ่ายเทคโนโลยี (Chief Information Officer/Technology Director)
- ประธานเจ้าหน้าที่ฝ่ายรักษาความปลอดภัย (Chief Security Officer)
- เจ้าหน้าที่อาวุโสอื่นๆ (โปรดระบุ) Other Senior Executive (please specify)
- รองประธานกรรมการอาวุโส/รองประธานกรรมการ/กรรมการ (Senior Vice President/Vice President/Director)
- หัวหน้าหน่วยธุรกิจ (Head of Business Unit)
- หัวหน้าแผนก (Head of Department)
- หัวหน้าแผนกทรัพยากรบุคคล (Head of Human Resources)
- ผู้จัดการ (Manager)

โอกาสที่เกิด

บุคคลที่มีชื่อเสียง

บุคคลที่มีอำนาจ

บุคคลที่เกี่ยวข้องการการเงิน

เป้าหมาย ภาคธุรกิจ

- การบิน อวกาศ และการป้องกันประเทศ (Aerospace and Defense)
- ยานยนต์ (Automotive)
- เคมีภัณฑ์ (Chemicals)
- การสื่อสาร (Communication)
- พลังงาน, การไฟฟ้า, การประปา และเหมืองแร่ (Energy, Utilities and Mining)
- วิศวกรรมและการก่อสร้าง (Engineering and Construction)
- บันเทิงและสื่อโฆษณา (Entertainment and Media)
- บริการด้านการเงิน (Financial Services)
- หน่วยงานภาครัฐ/รัฐวิสาหกิจ (Government / State Owned Enterprises)
- การรักษาพยาบาลและการพักผ่อน (Hospitality and Leisure)
- การผลิต (Manufacturing)
- ประกัน (Insurance)
- ยาและวิทยาศาสตร์เพื่อสุขภาพ (Pharmaceuticals and Life Sciences)
- บริการวิชาชีพ (Professional Services)
- ธุรกิจค้าปลีกและผู้บริโภค (Retail and Consumer)
- เทคโนโลยี (Technology)
- การขนส่งและโลจิสติกส์ (Transportation and Logistics)

โอกาสที่เกิด
ทุกธุรกิจที่ใช้ IT และ
Internet
โดยเฉพาะสถาบันการเงิน
องค์กรที่มีชื่อเสียง

เตือนภัย เรื่องเมล์ เมล์

อีเมลจาก Hilton หน้าตาเหมือน Phishing มาก จนพนักงานในเครือก็เข้าใจผิด

By: mk on 22 August 2016 - 08:11 Tags: Hilton E-mail Phishing Security

ในบางครั้ง อีเมลด้านการตลาดของหน่วยงานก็อาจหน้าตาดูเหมือนอีเมลหลอกลวง (scam/phishing) เสียจนฝ่ายอื่นๆ ของหน่วยงานเข้าใจว่าเป็นเช่นนั้นจริงๆ

เรื่องนี้เกิดกับกลุ่มธุรกิจโรงแรม Hilton Worldwide โดยลูกค้าที่เป็นสมาชิกสะสมแต้ม HHonors ได้รับอีเมลขอให้ยืนยันข้อมูลในบัญชีว่าถูกต้อง โดยให้ล็อกอินบัญชีตามลิงก์ที่แนบมากับอีเมล เพื่อตรวจสอบข้อมูลที่อยู่และหมายเลขโทรศัพท์ของลูกค้า

ลูกค้ารายหนึ่งเกิดไม่แน่ใจว่านี่คืออีเมล phishing หลอกเอาข้อมูลบัญชีหรือไม่ จึงจับภาพหน้าจอแล้วทวีตไปถาม @HiltonHHonors ซึ่งก็ได้รับคำตอบว่านี่ไม่ใช่อีเมลของบริษัท และขอให้ลูกค้าไม่แชร์ข้อมูลบัญชีให้ใคร

เพียงแต่เคสนี้มันคืออีเมลของ Hilton ของจริง!

เล่นดีดับทแตก! จอมแหกตาส่งอีเมลขู่โจมตี DDoS เรียกเอาเงินได้เพียบ ทั้งที่ไม่เคยโจมตีจริงสักครั้ง

By: ตะโร่งโต้ง on 27 April 2016 - 10:51 Tags: DDoS Scam E-mail Crime

ช่วงเวลาไม่ถึง 2 เดือนที่ผ่านมา มีบริษัทท่าธุรกิจออนไลน์หลายแห่งได้รับอีเมลจากผู้ที่อ้างตัวว่าเป็นกลุ่ม *"Armada Collective"* ข่มขู่ว่าจะโจมตีบริการออนไลน์ของบริษัทเหล่านั้นด้วยวิธี DDoS และยื่นเงื่อนไขให้บริษัทจ่ายเงินเป็น bitcoin เพื่อแลกกับการละเว้นไม่ลงมือโจมตี ซึ่งผลก็คือมีหลายบริษัทยอมจ่ายเงินแต่โดยดี ขนาดที่ว่ารวมมูลค่าแล้วเป็นเงินกว่า 100,000 ดอลลาร์ ทั้งที่ในความเป็นจริงผู้ส่งอีเมลข่มขู่นั้นยังไม่เคยโจมตีใครเลยสักครั้ง

ใจความของอีเมลข่มขู่กรรโชกนั้น ระบุจำนวนเงินที่ต้องการไว้ที่ 10 bitcoin (หรือประมาณ 165,000 บาท) โดยมีการหลอกล่อให้ผู้รับอีเมลกดเข้าไปดูข้อมูลผลการค้นหาของชื่อ *"Armada Collective"* ซึ่งคาดว่าเป็นการแอบอ้างเอาชื่อมาขู่มากกว่าจะเป็นฝีมือกลุ่มดังกล่าวจริง (*"Armada Collective"* เป็นชื่อของกลุ่มที่ลงมือโจมตี ProtonMail ผู้ให้บริการอีเมลแบบเข้ารหัสที่โฆษณาตัวเองว่า "NSA เจาะไม่เข้า" โดยลงมือโจมตีเพื่อเรียกค่าไถ่เป็น bitcoin ไปเมื่อปีก่อน)

เตือนภัย เรื่องเมล์ เมล์

มุขใหม่แฮ็กเกอร์ปลอมตัวเป็น CEO แล้วอีเมลหลอกให้พนักงานโอนเงินให้

By: mk on 10 April 2016 - 22:29 Tags: E-mail Fraud Scam Security FBI

FBI ออกมาเตือนภัยออนไลน์แบบใหม่ที่กำลังได้ความนิยม นั่นคือแฮ็กเกอร์ปลอมตัวเป็นซีอีโอหรือผู้บริหารระดับสูงของบริษัท แล้วอีเมลหาพนักงานที่รับผิดชอบเรื่องเงิน หลอกให้โอนเงินไปตามที่สั่ง การหลอกลวงแบบนี้มีชื่อเรียกว่า Business Email Scam (BEC) หรือ "CEO Fraud"

รูปแบบการโจมตีมีทั้งการปลอมอีเมล หรือการหลอกบัญชีผู้บริหารด้วย social engineering จากนั้นใช้วิธีการสั่งงานที่ดูน่าเชื่อถือ ขอให้โอนเงินในปริมาณที่ไม่เยอะจนผิดสังเกต จากสถิติของ FBI นับตั้งแต่ปี 2013 เป็นต้นมา มีเหยื่อมากถึง 17,642 ราย มูลค่าความเสียหายรวมกันถึง 2.3 พันล้านดอลลาร์ และ FBI พบว่านับตั้งแต่ปี 2015 เป็นต้นมา พบรูปแบบการโจมตีลักษณะนี้มากขึ้นถึง 270%

เอกสาร Panama Papers หลุดออกมาได้อย่างไร อาจเป็นเพราะโดนแฮ็กเมลเซิร์ฟเวอร์

By: mk on 6 April 2016 - 15:44 Tags: E-mail Hacking Security

ข่าวใหญ่รอบโลกสัปดาห์นี้คือการหลุดของเอกสาร Panama Papers ครั้งประวัติศาสตร์ รายละเอียดของเนื้อหาในเอกสารมีสื่อกระแสหลักรายงานไปเยอะแล้ว ประเด็นฝั่งไอทีคือเอกสารเหล่านี้หลุดออกมาได้อย่างไร

ตอนนี้เรายังมีข้อมูลเรื่องนี้ไม่เยอะนัก แต่เท่าที่หาได้คือ Wikileaks มีภาพหน้าจออีเมลของบริษัท Mossack Fonseca (แหล่งที่มาของเอกสารเหล่านี้) ที่ส่งถึงลูกค้าเพื่ออธิบายเรื่องข้อมูลหลุด ในอีเมลอธิบายว่าปัญหาเกิดจาก "โดนแฮ็กเมลเซิร์ฟเวอร์"

Mossack Fonseca ระบุในประกาศว่าจ้างผู้เชี่ยวชาญมาสืบสวน และยืนยันว่าโดนแฮ็กเมลเซิร์ฟเวอร์จริงๆ โดยจะพยายามหามาตรการป้องกันไม่ให้เกิดปัญหาแบบนี้อีก

เตือนภัย เรื่องเมล์ เมล์

Gmail เริ่มเตือนการส่งเมลไปยังปลายทางที่ไม่เข้ารหัส, รับเมลจากผู้ส่งที่ยืนยันตัวตนไม่ได้

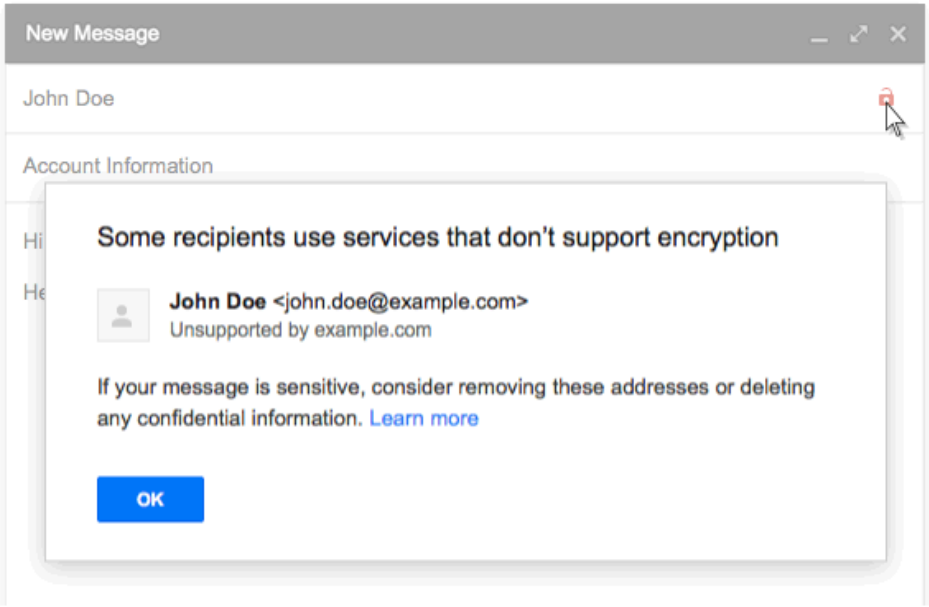
By: mk on 10 February 2016 - 07:48 Tags: Google Security Gmail E-mail TLS

Gmail ออกมาตรการเพิ่มความปลอดภัยให้ผู้ใช้ 2 อย่างดังนี้

- ถ้ารับหรือส่งเมลไปยังปลายทาง ที่เมลเซิร์ฟเวอร์ไม่รองรับการเข้ารหัสผ่าน TLS เราจะเห็นไอคอนแม่กุญแจสีแดงโผล่ขึ้นมาในหน้าจอเขียนเมล พร้อมคำเตือนว่าเนื้อหาในอีเมลอาจถูกดักฟังได้
- ถ้าได้รับเมลจากผู้ส่งที่ยืนยันตัวตนไม่ได้ (authentication) ไอคอนประจำตัวผู้ส่งจะกลายเป็นรูปเครื่องหมายคำถามสีแดง เพื่อให้เรารู้ว่าอาจเป็นผู้ส่งตัวปลอม

ที่มา - Gmail Blog

ไอคอนแม่กุญแจสีแดงที่มุมด้านขวามือของหน้า New Message กดแล้วจะขึ้นคำเตือน



เตือนภัย เรื่องเมล์ เมล์

จันทวรรณ

ดร. จันทวรรณ ปิยะวัฒน์

ผู้ติดตาม 818 ติดตาม 1121

ติดต่อ

เขียน
สมุด
บันทึก
อนุทิน

แลกเปลี่ยน
ความเห็น
ดอกไม้

Email ปลอม (Spam) ส่งถึงสมาชิก GotoKnow.org

ดิฉันขออธิบายเหตุการณ์การเกิด Spam ดังนี้คะ
-ทีมงานได้จัดตั้งเครื่องแม่ข่ายชั่วคราว และ สร้างโปรแกรมส่ง Email แบบชั่วคราวขึ้นมา เพื่อส่งถึงสมาชิก GotoKnow.org ทุกท่าน
-Email ฉบับดังกล่าวถูกส่งออกไปยังระบบ Email ของท่าน ซึ่งมีทั้งระบบฟรีและไม่ฟรี ซึ่งอาจจะไม่มีระบบการกรอง Email หรือไม่มีระบบรักษาความปลอดภัยที่ดีพอ
-โปรแกรม Spammer ที่แพร่กระจายอยู่ทั่วไปบนอินเตอร์เน็ต ซึ่งคอยแอบสุ่มเข้ามาดึงเอา ชื่อ และ Email address จากระบบ Email ของท่านออกไปบังเอิญสุ่มไปเจอ gotoknow(@)planet.mgt.psu.ac.th
-โปรแกรม Spammer นี้ ก็สุ่มสร้างชื่อปลอมขึ้นมาโดยอัตโนมัติ เช่น info, support, admin แล้วต่อด้วยชื่อ host ซึ่งในกรณีนี้คือ planet.mgt.psu.ac.th แล้วใช้เป็นตัวส่งออกไป
ยัง gotoknow(@)planet.mgt.psu.ac.th โดย support(@)planet.mgt.psu.ac.th ซึ่งเป็นอีเมลปลอม
- ทีนี้ เนื่องจากระบบ Mailing list แบบชั่วคราวที่ทีมงานเราสร้างขึ้นมาเอง ไม่ได้ตรวจสอบ Email address ของผู้ส่งที่แน่ชัด คือ Email address จาก jantawan.n(@)psu.ac.th เท่านั้นที่สามารถนำส่งไปยัง gotoknow(@)planet.mgt.psu.ac.th ได้ ก็เลยทำให้ Spammer แอบส่งออกอีเมลไปได้
ทีมงานต้องขอภัยท่านสมาชิกมา ณ ที่นี้ และขอเรียนชี้แจงว่า
ระบบการส่ง Email จาก Planet.mgt.psu.ac.th เป็น server ที่ทีมงานเราจัดตั้งขึ้นมาเองแบบชั่วคราวเพื่อใช้ส่ง Email เป็นคนละระบบกันกับระบบบล็อก GotoKnow.org ซึ่งมีความปลอดภัยสูง และบริหารด้วยทีมงาน Web hosting service มืออาชีพติด top ten ของอเมริกา ชื่อว่า ServePath.com

และเพื่อป้องกันการแอบเข้ามาส่งอีเมลอีก ทีมงานจึงได้ทำการยกเลิกการใช้งานการส่ง Mailing list ผ่านทาง gotoknow(@)planet.mgt.psu.ac.th เป็นที่เรียบร้อยแล้ว
..... อ่านต่อได้ที่: https://www.gotoknow.org/posts/8157

ดิฉันไม่ได้บล็อกซะหลายวัน หลังจากกลับจากแถลงข่าวงานมหกรรมฯ ก็ยุ่งซะจนไม่มีเวลานั่งอยู่หน้าอินเตอร์เน็ตครั้งละนานๆ เหมือนที่ผ่านมา แต่ก็ยังดูแลชุมชน GotoKnow.org อยู่ห่างๆ คะ

ส่วนเมื่อวานนี้กะว่าจะเข้ามาบล็อกและตอบ Email จาก users ทั้งหลาย ก็ทำไม่ได้ เพราะไฟฟ้าดับทั้งวิทยาเขตแบบไม่มีปี่มีขลุ่ย ถามเจ้าหน้าที่ก็ไม่มีใครทราบว่าจะติดกี่โมง ก็เลยไปทำธุระอย่างอื่นนอกวิทยาเขตเสียดีกว่า สุดท้ายปรากฏว่า ไฟฟ้าดับก็ตอนประมาณเหนึ่งทุ่ม รวมเป็นเวลา 10 ชั่วโมง

สำหรับบันทึกฉบับนี้ ดิฉันมีเรื่องต้องมาชี้แจงท่านสมาชิกโดยด่วนคะ คือ ดิฉันได้รับ Email จากผู้ใช้ท่านหนึ่งแจ้งว่าได้รับ Email ที่มีไวรัสจาก GotoKnow

ดิฉันลองตรวจสอบดูพบว่าเกิดการ Email Spam หรือ การส่ง Email โดยไม่ได้ส่งจริงจากเจ้าของ Email ขึ้น

ดิฉันจึงขอย้ำว่า ปกติท่านจะได้รับ Email จาก **jantawan.n (@) psu.ac.th** เท่านั้น หากท่านEmail ได้รับจาก **support (@) planet.mgt.psu.ac.th** ขอให้ลบ Email นั้นทิ้งทันทีคะ

ดิฉันขออธิบายเหตุการณ์การเกิด Spam ดังนี้คะ

-ทีมงานได้จัดตั้งเครื่องแม่ข่ายชั่วคราว และ สร้างโปรแกรมส่ง Email แบบชั่วคราวขึ้นมา เพื่อส่งถึงสมาชิก GotoKnow.org ทุกท่าน

-Email ฉบับดังกล่าวถูกส่งออกไปยังระบบ Email ของท่าน ซึ่งมีทั้งระบบฟรีและไม่ฟรี ซึ่งอาจจะไม่มีระบบการกรอง Email หรือไม่มีระบบรักษาความปลอดภัยที่ดีพอ

-โปรแกรม Spammer ที่แพร่กระจายอยู่ทั่วไปบนอินเตอร์เน็ต ซึ่งคอยแอบสุ่มเข้ามาดึงเอา ชื่อ และ Email address จากระบบ Email ของท่านออกไปบังเอิญสุ่มไปเจอ gotoknow(@)planet.mgt.psu.ac.th

-โปรแกรม Spammer นี้ ก็สุ่มสร้างชื่อปลอมขึ้นมาโดยอัตโนมัติ เช่น info, support, admin แล้วต่อด้วยชื่อ host ซึ่งในกรณีนี้คือ planet.mgt.psu.ac.th แล้วใช้เป็นตัวส่งออกไปยัง gotoknow(@)planet.mgt.psu.ac.th โดย support(@)planet.mgt.psu.ac.th ซึ่งเป็นอีเมลปลอม

- ทีนี้ เนื่องจากระบบ Mailing list แบบชั่วคราวที่ทีมงานเราสร้างขึ้นมาเอง ไม่ได้ตรวจสอบ Email address ของผู้ส่งที่แน่ชัด คือ Email address จาก jantawan.n(@)psu.ac.th เท่านั้นที่สามารถนำส่งไปยัง gotoknow(@)planet.mgt.psu.ac.th ได้ ก็เลยทำให้ Spammer แอบส่งออกอีเมลไปได้

ทีมงานต้องขออภัยท่านสมาชิกมา ณ ที่นี้ และขอเรียนชี้แจงว่า

- ระบบการส่ง Email จาก Planet.mgt.psu.ac.th เป็น server ที่ทีมงานเราจัดตั้งขึ้นมาเองแบบชั่วคราวเพื่อใช้ส่ง Email เป็นคนละระบบกันกับระบบบล็อก GotoKnow.org ซึ่งมีความปลอดภัยสูง และบริหารด้วยทีมงาน Web hosting service มืออาชีพติด top ten ของอเมริกา ชื่อว่า ServePath.com
-
- และเพื่อป้องกันการแอบเข้ามาส่งอีเมลอีก ทีมงานจึงได้ทำการยกเลิกการใช้งานการส่ง Mailing list ผ่านทาง gotoknow(@)planet.mgt.psu.ac.th เป็นที่เรียบร้อยแล้ว

ขอบคุณคะ

ดร.จันทวรรณ น้อยวัน

จับแก๊งแฮกเกอร์ปลอมอีเมล์ ลวงคู่ค้าโอนเงิน 6 ล้าน

จับแฮกเกอร์แสบ! ปลอมเมล์ตุ๋นโอนเงินสูญ 6 ล้าน

โดย ไทยรัฐออนไลน์ 16 ก.ค. 2557 19:30

2,301 ครั้ง

แชร์ 39 Tweet

โหวตข่าวนี้

ชอบ 22.2%

ไม่ชอบ 11.1%

สนุก 0.0%

ประหลาดใจ 0.0%

เสียใจ 0.0%

ให้กำลังใจ 66.7%

ปอท.รวบแฮกเกอร์หัวใส ปลอมอีเมล์บริษัทให้โอนเงิน 6 ล้านเข้าบัญชี ก่อนเดินเข้าตู้เอทีเอ็มเสียบบัตรเชิดเงิน 2 ผู้ต้องหายังให้การปฏิเสธทุกข้อกล่าวหา ยันเปิดบัญชีรับแรงงานต่างด้าว...

เมื่อเวลา 10.45 น. วันที่ 16 ก.ค.57 ที่กองบัญชาการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) พ.ต.อ.สมพร แดงดี รอง.ผบก.ปอท. พ.ต.อ.โยธิน โตสง่า ผกก.3 บก.ปอท. ร่วมกันแถลงการจับกุม นายจอห์น อายุ 33 ปี สัญชาติไนจีเรีย และ นางนวลจันทร์ ชาฤทธิ์ อายุ 43 ปี ผู้ต้องหาขบวนการแฮกเกอร์ปลอมอีเมล์

พ.ต.อ.สมพร เปิดเผยว่า สืบเนื่องจากเมื่อวันที่ 1 ก.ค.ที่ผ่านมา มีบริษัทเอกชนแห่งหนึ่งในประเทศไทย ได้เข้าแจ้งความว่า ถูกขบวนการแฮกข้อมูลของบริษัทปลอมแปลงอีเมล์ ก่อนส่งข้อความแจ้งว่ามีการเปลี่ยนแปลงบัญชีรับโอนเงินค่าสินค้า ไปยังคู่ค้าของบริษัทในประเทศญี่ปุ่นจำนวน 6 ล้านบาท ทำให้บริษัทได้รับความเสียหายเป็นอย่างมาก

จากการสอบสวน ทราบว่า ขบวนการของกลุ่มแฮกข้อมูลนี้ จะทำบัญชีปลอมโดยหลอกให้ผู้เสียหายโอนเงินชำระค่าสินค้าไปให้ โดยเจ้าหน้าที่ติดตามจนทราบว่าบัญชีที่ลูกค้าผู้เสียหายโอนไปนั้นเป็นของนางนวลจันทร์ ซึ่งหลังจากได้รับเงินโอนแล้ว นายจอห์นจะมาถอนเงินจากตู้เอทีเอ็มบัญชีที่เปิดไว้ โดยมีการวางแผนทำกันเป็นขบวนการมีบัญชีธนาคารเชื่อมโยงหลายบัญชี รวมถึงไอทีแอดเดรสของอีเมล์ปลอมก็อยู่ในประเทศไนจีเรียด้วย

ทั้งนี้ ผู้ต้องหาทั้ง 2 ราย ได้ปฏิเสธทุกข้อกล่าวหา โดยนายจอห์นอ้างว่า มีเพื่อนจะโอนเงินมาให้ จึงให้เลขบัญชีไปเท่านั้น ไม่มีส่วนรู้เห็นเรื่องแฮกเกอร์อีเมล์ปลอม หรือที่มาของเงินว่า เป็นการหลอกมาจากบริษัทญี่ปุ่น และไม่เกี่ยวข้องกับคนที่อยู่ในไนจีเรียแต่อย่างใด ส่วนนางนวลจันทร์ ยอมรับว่า เป็นเจ้าของบัญชีดังกล่าวจริง แต่เปิดไว้ให้นายจอห์นทำบริษัทรับแรงงานต่างด้าวมาทำงานในประเทศไทย เบื้องต้นเจ้าหน้าที่ได้แจ้งข้อหา ร่วมกันนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมข้อมูลอันเป็นเท็จโดยประการน่าจะเกิดความเสียหายแก่ประชาชน จากนั้นจะดำเนินคดีกับผู้ต้องหาทั้ง 2 รายต่อไป

ปอท.รวบแฮกเกอร์หัวใส ปลอมอีเมล์บริษัทให้โอนเงิน 6 ล้านเข้าบัญชี ก่อนเดินเข้าตู้เอทีเอ็มเสียบบัตรเชิดเงิน 2 ผู้ต้องหายังให้การปฏิเสธทุกข้อกล่าวหา

DSI เตือนระวังอีเมล์ปลอมหลอกโอนเงิน มูลค่าความเสียหายกว่า 50 ล้านบาท

DSI เตือนระวังอีเมล์ปลอมหลอกโอนเงิน มูลค่าความเสียหายกว่า 50 ล้านบาท ลวงคนไทยผ่านเฟสบุครูปแบบโรมานซ์สแกม ผู้เสียหาย 7 รายมูลค่าความเสียหาย 19 ล้านบาท

PICTURE

แหล่งที่มา : Radio-สถานีวิทยุกระจายเสียงแห่งประเทศไทย

วันที่ข่าว : 11 เมษายน 2559

กรมสอบสวนคดีพิเศษ แถลงเตือนระวังอีเมล์ปลอมหลอกโอนเงิน มูลค่าความเสียหายกว่า 50 ล้านบาท ผ่านเฟสบุคโรมานซ์สแกม มีผู้เสียหาย 7 รายความเสียหาย 19 ล้านบาท

พ.ต.ต.สุริยา สิงหกมล รองอธิบดีกรมสอบสวนคดีพิเศษ (ดีเอสไอ) พร้อมด้วย พ.ต.ท. พเยาว์ ทองเสน ผู้บัญชาการสำนักคดีอาญาพิเศษ 1 และนายนิธิต ภูริคุปต์ ผู้บัญชาการสำนักคดีเทคโนโลยีและสารสนเทศ แถลงผลการดำเนินคดีหลอกลวงคนไทย ผ่านเฟสบุคในรูปแบบโรมานซ์สแกม สร้างโปรไฟล์เป็นชาวต่างชาติผิวขาวหน้าตาดี มีผู้ต้องหา 30 ราย เป็นชาวต่างชาติ 4 ราย เป็นชาวไนจีเรีย 3 ราย อินเดีย 1 ราย หลอกลวงให้เหยื่อโอนเงินให้มูลค่าความเสียหายประมาณ 19 ล้านบาท ผู้เสียหาย 7 ราย มีบัญชีใช้หลอกโอนเงินกว่า 30 บัญชี มีเงินหมุนเวียนกว่า 50 ล้านบาท ศาลอนุมัติหมายจับผู้ต้องหาแล้ว 15 ราย พร้อมทั้งประสานกับทางการมาเลเซียติดตามตัวผู้ต้องหา นอกจากนี้ กรมสอบสวนคดีพิเศษยังสืบทราบว่า ขณะนี้มีกลุ่มมิจฉาชีพชาวต่างชาติ ร่วมกับคนไทย ปลอมอีเมล์หลอกลวงให้คู่ค้าโอนเงินชำระสินค้าไปยังบัญชีของคนร้าย เหยื่อส่วนใหญ่เป็นผู้ประกอบการจำหน่ายสินค้าไปต่างประเทศ โดยคนร้ายใช้วิธีส่งอีเมล์สวมรอยเป็นบริษัทจากประเทศไทยส่งไปหาคู่ค้า ตั้งชื่ออีเมล์ใหม่ที่คล้ายกัน หลังจากเหยื่อหลงเชื่อ คนร้ายจะเป็นตัวกลางระหว่างเหยื่อกับคู่ค้า ติดตามความเคลื่อนไหวส่งมอบสินค้าและรับเงิน จากนั้นจะแจ้งเปลี่ยนบัญชีให้โอนเงินเข้าบัญชีคนร้าย มีผู้เสียหาย กว่า 10 ราย มูลค่าความเสียหายกว่า 50 ล้านบาท

รองอธิบดีกรมสอบสวนคดีพิเศษ ยังกล่าวถึงการดำเนินคดีพิเศษ ที่เกี่ยวข้องกับความผิดแชร์ลูกโซ่ว่า กรมสอบสวนคดีพิเศษ ได้ส่งสำนวนสั่งฟ้องผู้ต้องหาในคดีหลอกลวงประชาชนซื้อขายทองแดง 2 ราย และคดีหลอกลวงให้ลงทุนธุรกิจเด้นท์รถ ให้ซื้อขายรถยนต์มือสองและรับจำนำรถยนต์ โดยให้กำไรสูง ส่งสำนวนสั่งฟ้องผู้ต้องหา 3 ราย

ตร.แถลงจับแก๊งแบล็คอีเกิลลวงหญิงไทยสูญ9ล.

พล.ต.ท.ฐิติราช หนองหารพิทักษ์ ผู้บัญชาการตำรวจสอบสวนกลาง แถลงผลจับกุมผู้ต้องหา 8 ราย ในจำนวนนี้เป็นชายชาวแอฟริกันตะวันออก 5 ราย และหญิงไทย 3 ราย พร้อมของกลาง รวม 87 รายการ อาทิ โทรศัพท์มือถือ 27 เครื่อง สมุดบัญชีธนาคาร 30 เล่ม และคอมพิวเตอร์โน้ตบุ๊ก 5 เครื่อง หลังทยอยจับกุมตัวได้ในพื้นที่ย่านประชาชื่น เพชรเกษม และนนทบุรี จากปฏิบัติการกวาดล้างอาชญากรรมข้ามชาติ Black Eagle โดยพฤติกรรมของผู้ต้องหาแก๊งค์ปลอมอีเมล์ หรือที่เรียกว่า Email Scram จะแสดงตัวเป็นบริษัทผู้ขายสินค้าหลอกลวงให้ผู้เสียหายโอนเงินชำระค่าสินค้า ซึ่งได้สร้างความเสียหายให้กับผู้ค้ากว่า 9 ล้านบาท

ผู้บัญชาการตำรวจสอบสวนกลาง กล่าวว่า ขณะนี้ยังพบกลุ่มชาวต่างชาติ ใช้สื่อออนไลน์ หรือ Romance Scram แสดงตนว่ามีบุคคลิกและฐานะทางสังคมดี เพื่อหลอกหลวงหญิงไทยให้โอนเงินเข้าบัญชี โดยล่าสุดมีผู้เสียหายเป็นหญิงไทยเข้าแจ้งความกว่า 80 รายแล้ว ว่าตกเป็นเหยื่อขบวนการนี้ จึงขอประชาสัมพันธ์ให้หญิงไทยโดยเฉพาะที่มีอายุตั้งแต่ 40 ปีขึ้นไป ที่โสด หรือหย่าร้าง ซึ่งมีแนวโน้มที่จะตกเป็นเหยื่อได้มากกว่ากลุ่มอื่น โดยอย่าหลงเชื่อชาวต่างชาติที่ติดต่อผ่านช่องทางโซเชียลมิเดีย ส่วนกลุ่มของผู้ค้าควรติดต่อทางช่องทางแบบคู่ขนาน เพราะบางกรณีอีเมล์ของบริษัทคู่ค้าอาจถูกแฮกได้ เพื่อป้องกันไม่ให้ตกเป็นเหยื่อของขบวนการดังกล่าว

ทั้งนี้ จากการตรวจสอบพบว่าในช่วง 6 เดือนที่ผ่านมา
มีผู้ตกเป็นเหยื่อโดยพบเงินหมุนเวียนกว่า 100 ล้านบาท

เจออีกแล้ว!! ปลอมอีเมล์หลอกโอนเงินค่าสินค้า.. เพิ่มอัตราความถี่แผ่ขยายสู่หลายพื้นที่

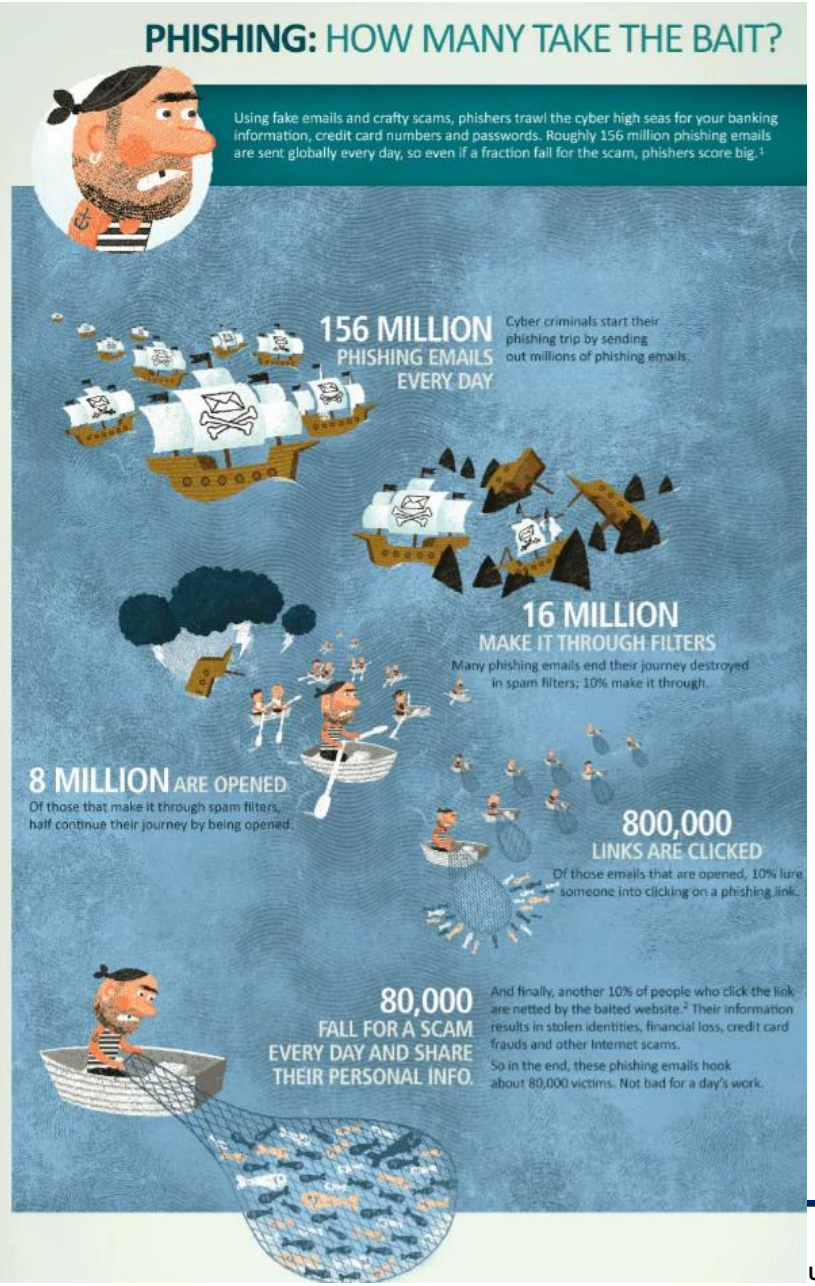
กรณีที่ 1 เกิดขึ้นกับนักธุรกิจไทยที่ทำการซื้อขายสินค้ากับบริษัทจีนในนครเซี่ยงไฮ้ โดยได้ติดต่อกันผ่านอีเมล์จนเริ่มเกิดความคุ้นเคย ต่อมาได้รับแจ้งทางอีเมล์ว่าให้โอนเงินค่ามัดจำสินค้ากว่า 30,000 ดอลลาร์สหรัฐไปยังเลขที่บัญชีของธนาคารแห่งหนึ่งในจีน ภายหลังบริษัทในเซี่ยงไฮ้แจ้งว่าไม่ได้รับเงินค่ามัดจำแต่อย่างใด จึงได้เริ่มมีการตรวจสอบ ผลปรากฏว่าเลขที่บัญชีดังกล่าวเป็นของธนาคารในเมืองเซินเจิ้น มณฑลกวางตุ้ง ทำให้นักธุรกิจไทยต้องเสียทั้งเงินและเวลาในการเดินทางยังประเทศจีนเพื่อดำเนินการแจ้งความ แถมยังไม่รู้ด้วยว่าตำรวจจะติดตามคนร้ายและได้เงินมัดจำกลับคืนมาหรือไม่

กรณีที่ 2 เกิดขึ้นกับบริษัทเวียดนามที่ได้ทำการสั่งซื้อสินค้าจากบริษัทหนึ่งในประเทศไทย ในเวลาต่อมาได้รับอีเมล์แจ้งให้โอนเงินค่าสินค้ารวมจำนวนกว่า 40,000 ดอลลาร์สหรัฐไปยังธนาคารแห่งหนึ่งในนครเซี่ยงไฮ้ ซึ่งผู้ซื้อสินค้าในเวียดนามโอนไปด้วยดีโดยที่ไม่ได้สะดุดใจแต่อย่างใด ภายหลังจึงพบว่าบริษัทไทยมิได้รับเงินจำนวนนั้น ซึ่งความเสียหายไม่เพียงเกิดขึ้นกับบริษัทเวียดนามที่ต้องสูญเสียค่าสินค้าเท่านั้น แต่บริษัทไทยยังได้รับความเสียหายจากการที่ได้ผลิตสินค้าไว้แล้ว และอาจต้องเสีย order หากไม่สามารถติดตามเงินจำนวนดังกล่าวกลับมาได้ และกระบวนการแจ้งความก็ซับซ้อนมากขึ้น เนื่องจากเกี่ยวข้องกับประเทศที่ 3 ที่ผู้ซื้อและผู้ขายมิได้มีบริษัทตั้งอยู่

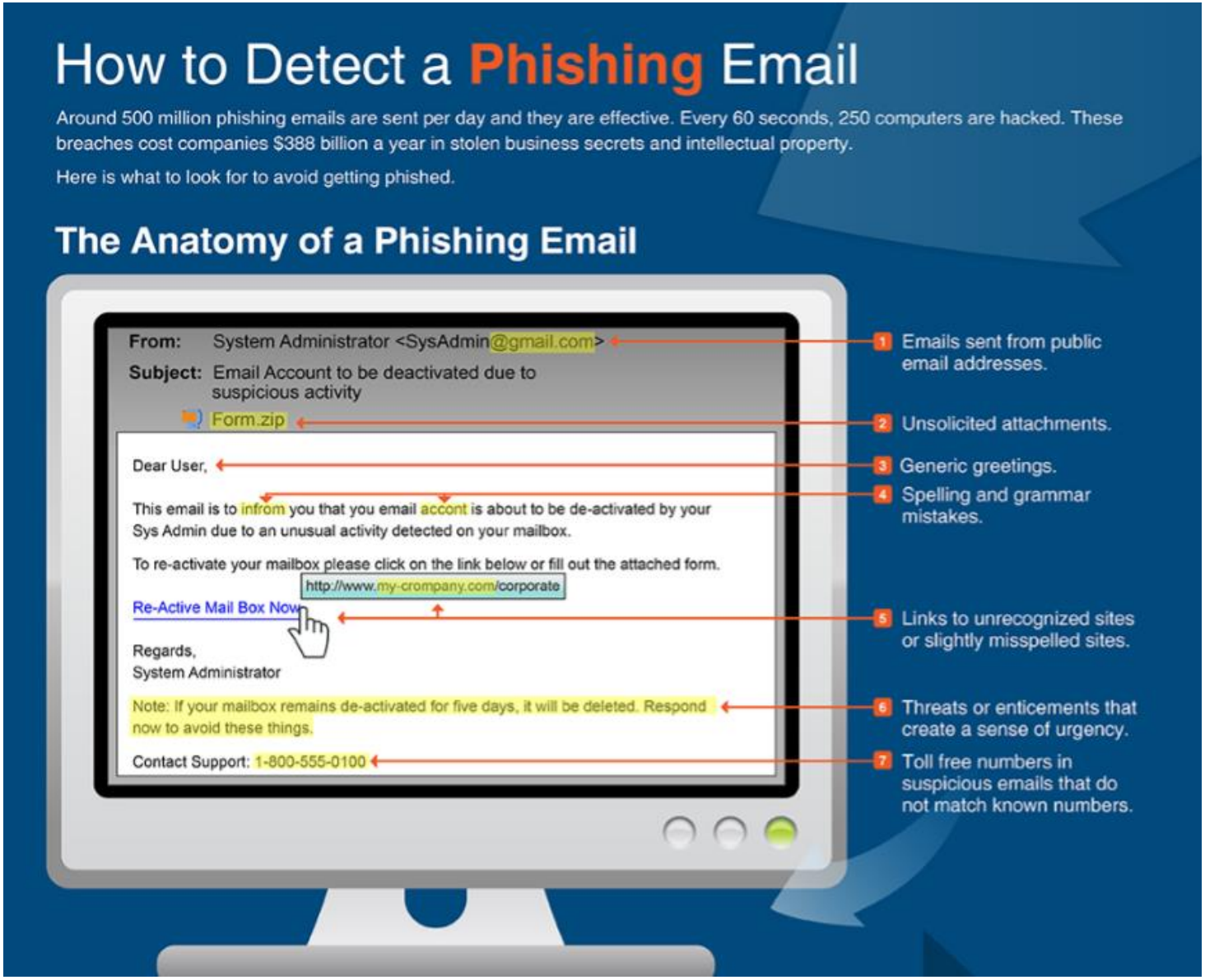
เตือนภัยธุรกิจในจีน (มณฑลเจ้อเจียง) : ระวัง! อีเมล์ถูกแฮ็ก มือที่สามแทรกซึมแทนคู่ค้า หลอกโอนเงินเข้าบัญชีใหม่

กรณีที่ 3 บริษัทไทยแห่งหนึ่งได้ทำธุรกิจการค้ากับบริษัทจีนในมณฑลเจ้อเจียงเป็นระยะเวลาหนึ่งโดยใช้การส่งอีเมล์เจรจาตกลงทางธุรกิจเสมอมา ซึ่งไม่เคยเกิดปัญหาหรืออุปสรรคใด ๆ แต่เมื่อไม่นานมานี้ บริษัทไทยแห่งนี้ได้รับอีเมล์ฉบับหนึ่ง (ซึ่งมีชื่ออีเมล์และชื่อผู้ส่งในตอนท้ายของอีเมล์เป็นชื่อเดียวกันกับคนของบริษัทมณฑลเจ้อเจียงที่ติดต่อกันเป็นประจำ) แจ้งว่า ให้โอนเงินค่าสินค้าตามจำนวนที่ได้ตกลงกันแล้วในช่วงที่ผ่านมาเข้าเลขที่บัญชีธนาคารใหม่ของบริษัท โดยอ้างว่าขณะนี้บริษัทอยู่ในระหว่างการตรวจสอบบัญชีภายใน และไม่สะดวกที่จะตรวจสอบเงินที่โอนเข้ามาในบัญชีเก่าได้ จึงขอใช้บัญชีใหม่ในการโอนเงินแทน ซึ่งบริษัทฝ่ายไทยไม่ได้ชะล่าใจและได้ดำเนินการโอนเงินเข้าบัญชีใหม่ดังกล่าว

ผ่านมาระยะเวลาหนึ่ง เมื่อฝ่ายไทยยังไม่ได้รับสินค้าหลังจากที่โอนเงินไปแล้ว จึงได้ติดต่อสอบถามไปยังบริษัทมณฑลเจ้อเจียง ในที่สุดทั้งสองฝ่ายถึงรู้ว่ามีบุคคลที่สามปลอมแปลงอีเมล์ของบริษัทมณฑลเจ้อเจียง เพื่อใช้สนทนาลวงหลอกให้บริษัทไทยโอนเงินเข้าในบัญชีของตนเอง



- 156 Million Phishing Emails Every Day
- 16 million make it through filters
- 8 million are opened.
- 800,000 links are clicked
- 80,000 fall for a scam every day and share their personal information.
- And finally, another 10% of people who click the link are netted by the baited website.2 Their information results in stolen identities, financial loss, credit card frauds and other Internet scams. So in the end, these phishing emails hook about 80,000 victims. Not bad for a day's work.


How to Detect a Phishing Email
Around 500 million phishing emails are sent per day and they are effective. Every 60 seconds, 250 computers are hacked. These breaches cost companies $388 billion a year in stolen business secrets and intellectual property.
Here is what to look for to avoid getting phished.
The Anatomy of a Phishing Email
From: System Administrator <SysAdmin@gmail.com>
Subject: Email Account to be deactivated due to suspicious activity
Form.zip
Dear User,
This email is to infrom you that you email accont is about to be de-activated by your Sys Admin due to an unusual activity detected on your mailbox.
To re-activate your mailbox please click on the link below or fill out the attached form.
http://www.my-crompany.com/corporate
Re-Active Mail Box Now
Regards,
System Administrator
Note: If your mailbox remains de-activated for five days, it will be deleted. Respond now to avoid these things.
Contact Support: 1-800-555-0100
1 Emails sent from public email addresses.
2 Unsolicited attachments.
3 Generic greetings.
4 Spelling and grammar mistakes.
5 Links to unrecognized sites or slightly misspelled sites.
6 Threats or enticements that create a sense of urgency.
7 Toll free numbers in suspicious emails that do not match known numbers.

Phishing By the Numbers

- 91% of cyber-attacks begin with a spear phishing email.
- 94% of spear phishing emails use malicious file attachments

What Is Phishing?

Phishers typically create fake emails that appear to come from someone you trust, such as a bank, credit card company, or a popular website. These emails typically try to trick you into giving away sensitive information, such as your username, password, or credit card details.

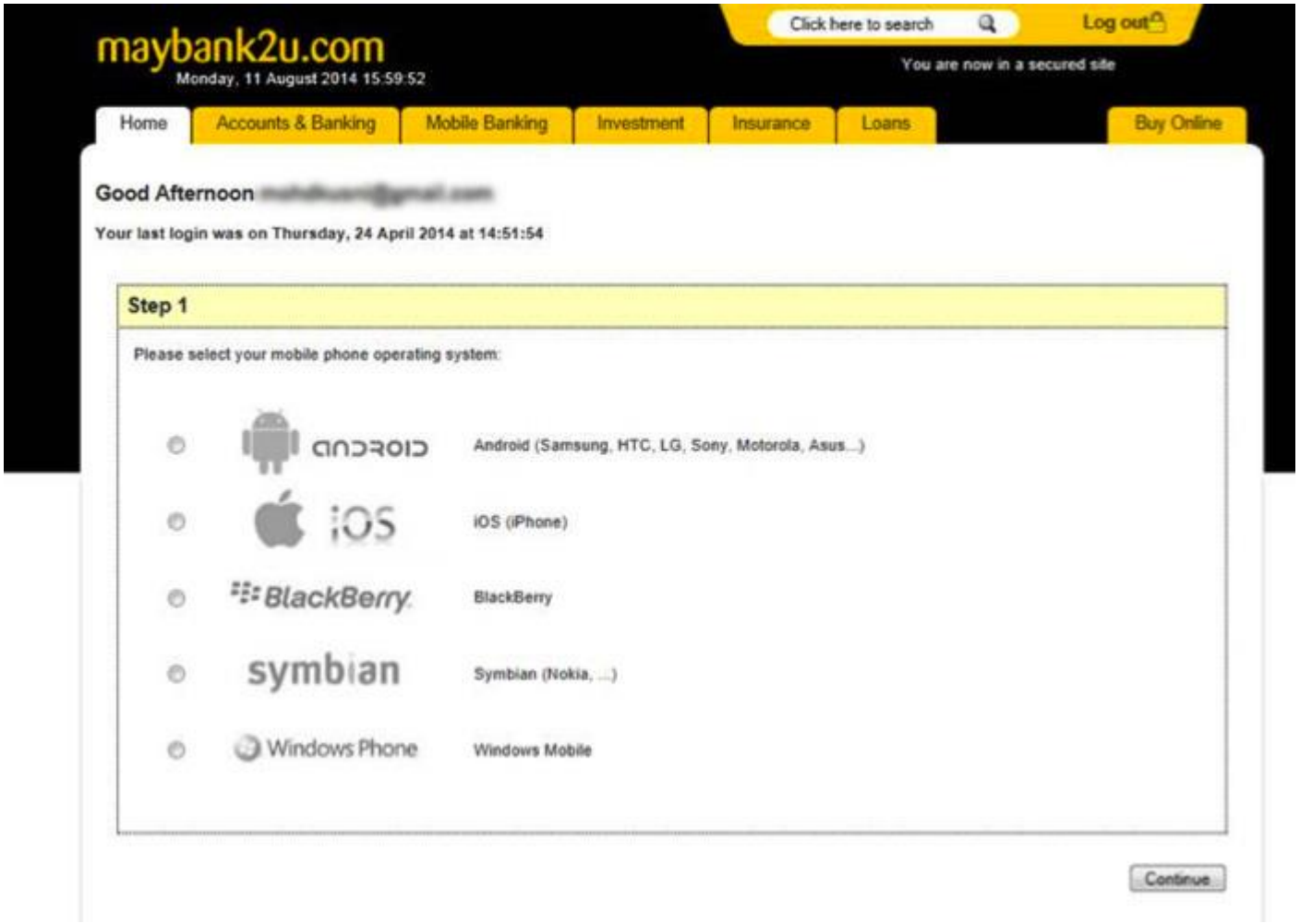
They may also try to get you to inadvertently install malicious programs on your computer, which can happen when you click on an infected link or open an infected attachment. Once infected, the phisher can monitor all of your activity, including all of your keystrokes.

10 Tips for Safe Online Banking

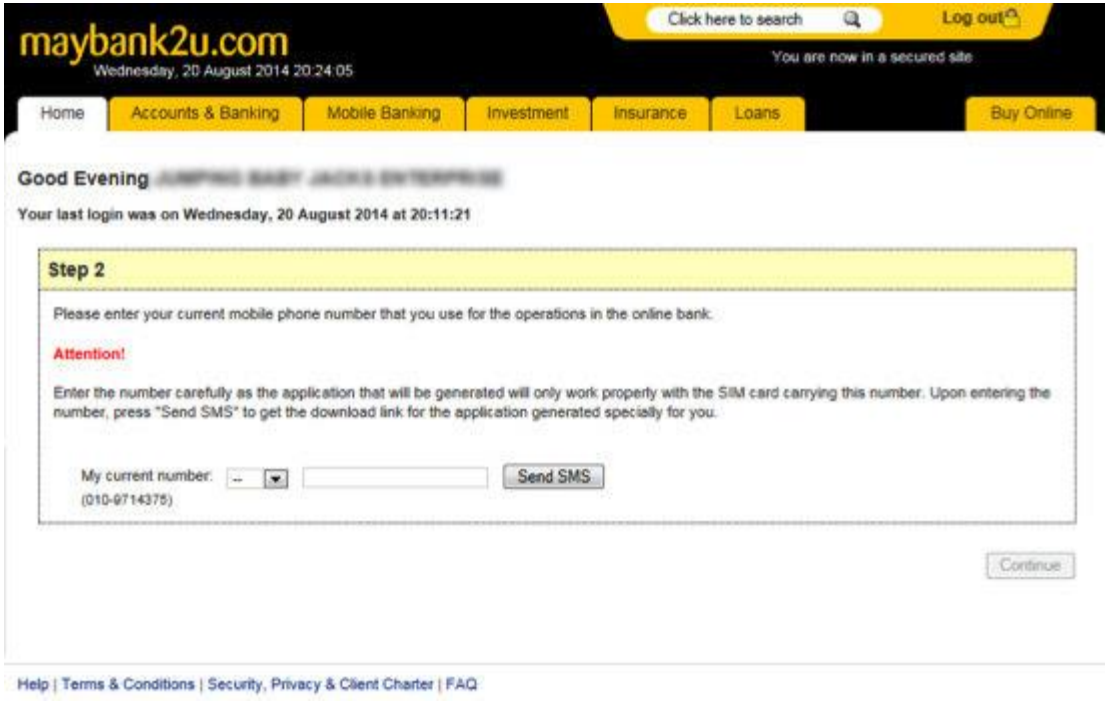
iPhone Scam

Phone scam happens when a customer receives phone call from a "bank" confirm a credit card transaction, such as a transaction at XXX Jewelry purportedly charged the customer's credit card.

Malware

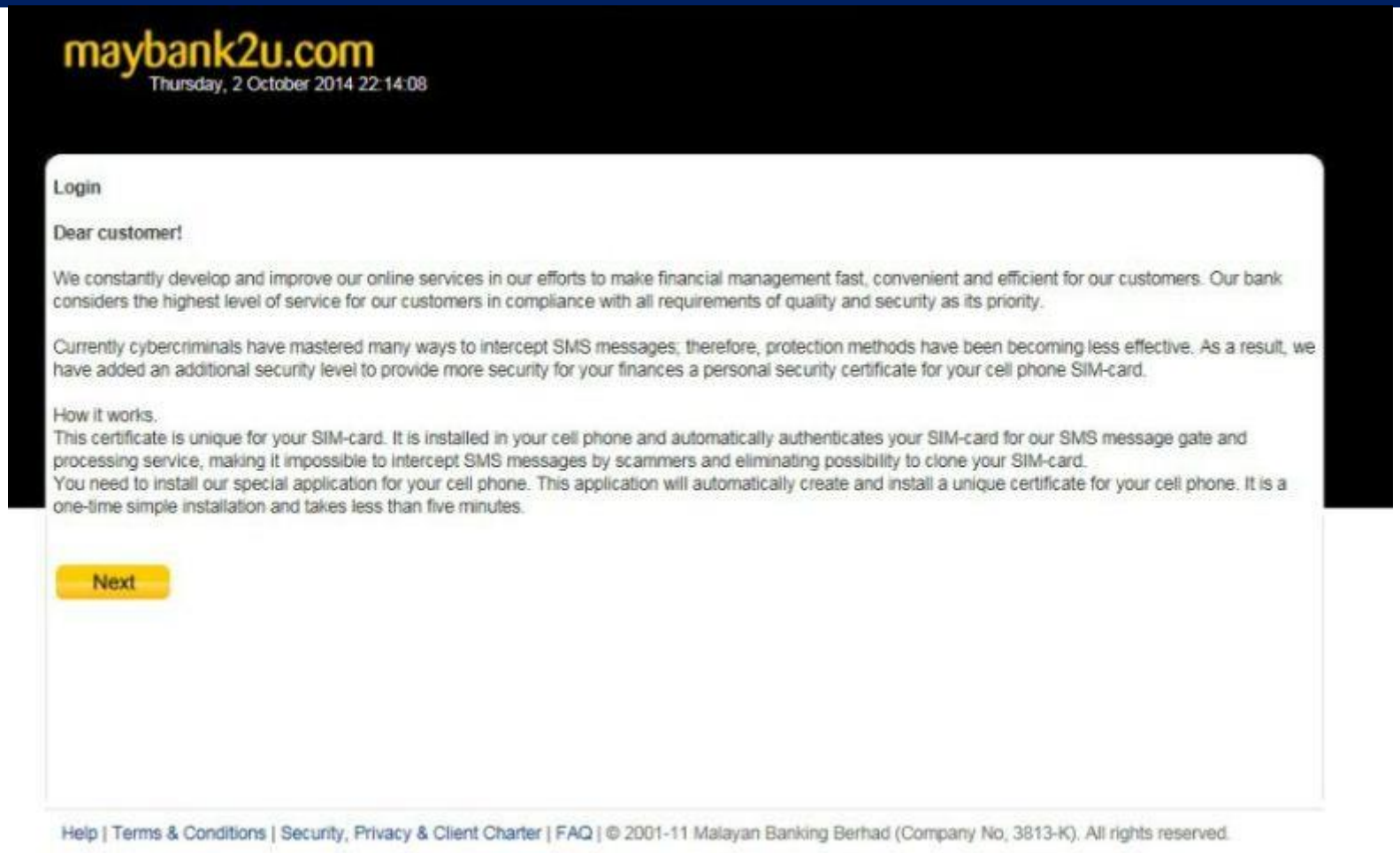

maybank2u.com
Monday, 11 August 2014 15:59:52
Click here to search
Log out
You are now in a secured site
Home
Accounts & Banking
Mobile Banking
Investment
Insurance
Loans
Buy Online
Good Afternoon
Your last login was on Thursday, 24 April 2014 at 14:51:54
Step 1
Please select your mobile phone operating system:
android
Android (Samsung, HTC, LG, Sony, Motorola, Asus...)
iOS
iOS (iPhone)
BlackBerry
BlackBerry
symbian
Symbian (Nokia, ...)
Windows Phone
Windows Mobile
Continue

Malware

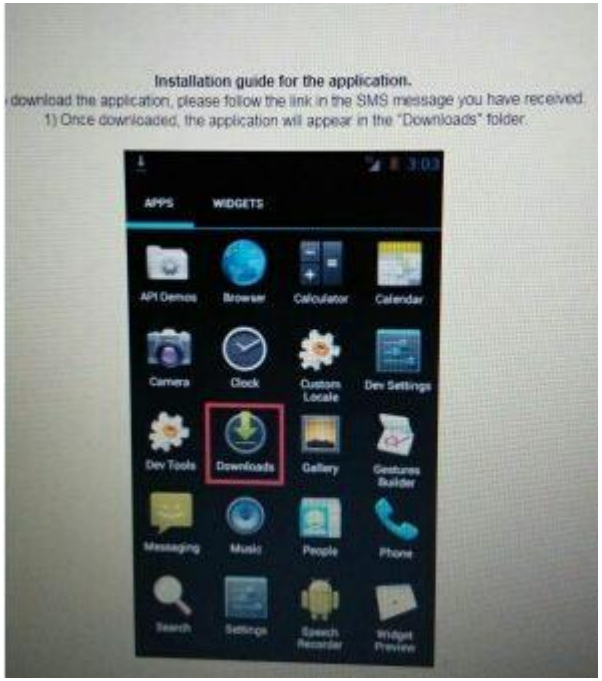

maybank2u.com
Wednesday, 20 August 2014 20:24:05
Click here to search
Log out
You are now in a secured site
Home
Accounts & Banking
Mobile Banking
Investment
Insurance
Loans
Buy Online
Good Evening
Your last login was on Wednesday, 20 August 2014 at 20:11:21
Step 2
Please enter your current mobile phone number that you use for the operations in the online bank.
Attention!
Enter the number carefully as the application that will be generated will only work properly with the SIM card carrying this number. Upon entering the number, press "Send SMS" to get the download link for the application generated specially for you.
My current number:
(010-9714375)
Send SMS
Continue
Help | Terms & Conditions | Security, Privacy & Client Charter | FAQ


maybank2u.com
1
Please select your mobile phone operating system
Android (Samsung, HTC, LG, Sony...)
iOS (iPhone)
Windows Mobile
BlackBerry
Symbian (Nokia, ...)
Next

Malware


maybank2u.com
Thursday, 2 October 2014 22:14:08
Login
Dear customer!
We constantly develop and improve our online services in our efforts to make financial management fast, convenient and efficient for our customers. Our bank considers the highest level of service for our customers in compliance with all requirements of quality and security as its priority.
Currently cybercriminals have mastered many ways to intercept SMS messages; therefore, protection methods have been becoming less effective. As a result, we have added an additional security level to provide more security for your finances a personal security certificate for your cell phone SIM-card.
How it works.
This certificate is unique for your SIM-card. It is installed in your cell phone and automatically authenticates your SIM-card for our SMS message gate and processing service, making it impossible to intercept SMS messages by scammers and eliminating possibility to clone your SIM-card.
You need to install our special application for your cell phone. This application will automatically create and install a unique certificate for your cell phone. It is a one-time simple installation and takes less than five minutes.
Next
Help | Terms & Conditions | Security, Privacy & Client Charter | FAQ | © 2001-11 Malayan Banking Berhad (Company No. 3813-K). All rights reserved.

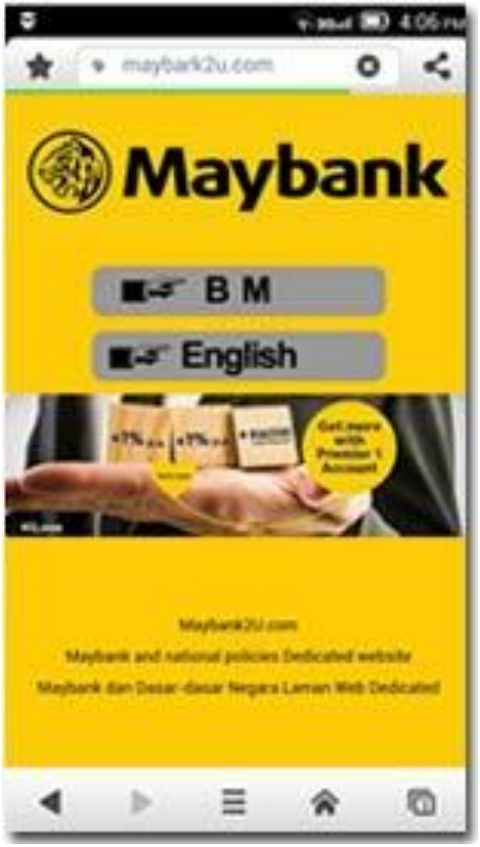
Malware


Installation guide for the application.
download the application, please follow the link in the SMS message you have received.
1) Once downloaded, the application will appear in the "Downloads" folder.
APPS
WIDGETS
API Demos
Browser
Calculator
Calendar
Camera
Clock
Custom Locale
Dev Settings
Dev Tools
Downloads
Gallery
Gestures Builder
Messaging
Music
People
Phone
Search
Settings
Speech Recorder
Widget Preview


3G
2:30 AM
66628
Maybank pemberitahuan kecemasan, http://maybank2u-my.com confirm identity


maybankk2u.com
Go Back
Ignore this Warning

Malware


maybank2u.com
Maybank
B M
English
Maybank2U.com
Maybank and national policies Dedicated website
Maybank dan Dasar-dasar Negara Laman Web Dedicated

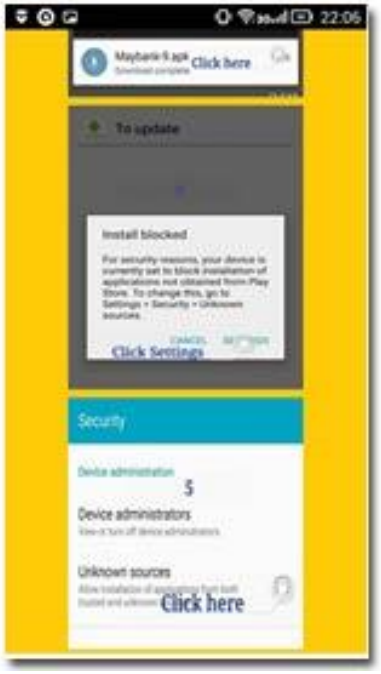

Maybank
Maybank emergency notice, in line with national policy, please confirm again, Maybank user. Log Maybank card is your own, please click Maybank system is confirmed, Maybank card is confirmed! Personally identifiable information, complete if wrong personal information, Maybank card can not be used! To remind you once again! The state's policy is to protect your personal information. Maybank obliged to inform you, please confirm immediately.
Immediately transaction
Please cooperate Otherwise, you can not use Maybank card


Maybank
dear user: Maybank policy: To re-confirm your registration of Maybank. Causing inconvenience sorry: make sure cooperation. Otherwise can not use Maybank card
submit

Malware


www.maybankk2u.com
Maybank
ANDROID
Download Update
Maybank remind you, Android,
need to be updated installation,
please read 1-9 instructions,
installation is complete
Remind you ,If you not
download installation is
complete, not confirm the
identity, maybank card cannot


used
1
Please pull down,if download complete
2
Skype
3
Click here


Click here
To update
Install blocked
Click Settings
Security
Device administrators
5
Unknown sources
Click here


Unknown sources
Click OK
To upda
Do you want to in
will get access to
Click NEXT
To update

Step on how identify and protect from Malware

Step on how identify and protect from Malware

- Open your anti-virus software and check for the latest updates. It is strongly recommended for you have anti-virus software installed in your computer/devices.
- Run a full system scan using your anti-virus software.
- If the scan finds the virus or malware and successfully removes it, you must reset your password and memorable information. Then only you can login your Internet Banking as usual.

Basic Signs your smartphones is infected

- Unexplainable draining of battery
- Pop up dialogs install other applications/ unwanted Ads
- Your antivirus not running (some malware disables antivirus)
- Your monthly data / phone usage increased (check your bill for unknown transactions)
- Overall performance of the smartphone reduced
- Apps crash unexpectedly
- SMS doesn’t get delivered/Calls disrupted

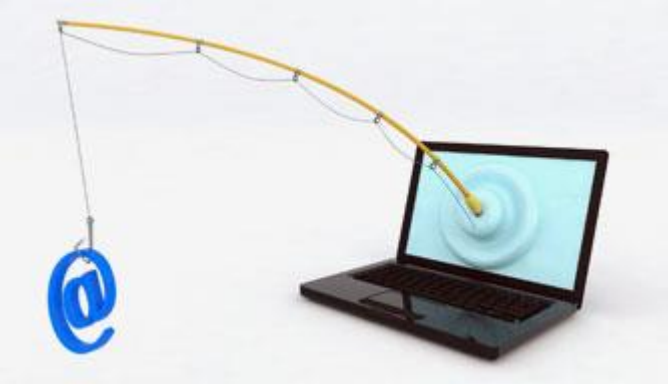
Step on how protect device from Malware

The best protection from malware:

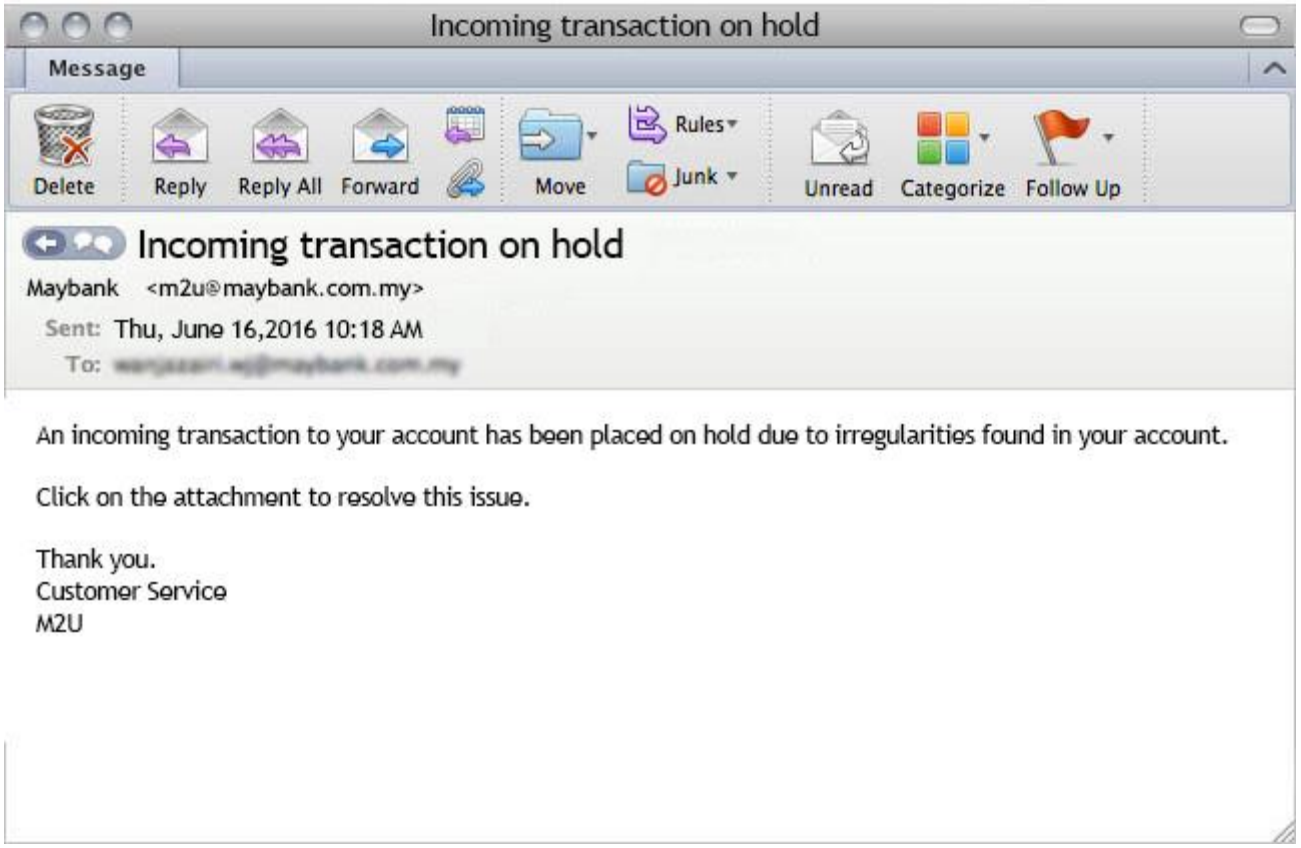
- Use anti-virus software. Install and maintain an updated, quality antivirus program.
- Be choosy. Think before you download any files or programs. Ask yourself if you can trust the source and whether the site is genuine.
- Install updates regularly. Things are always changing, sit's important keep your operating system (e.g. Windows), Internet browser, applications (e.g. Adobe Acrobat, Java) and firewalls up to date.
- Stay safe online. Always use websites and programs that you can trust. Be sure of what you're agreeing to before clicking ‘OK'.
- Be careful. Do not open spam email messages containing attachments or click links on suspicious websites.
- Keep yourself updated. Regularly check security alerts and advisories to obtain the necessary information to protect your device. This helps to prevent you from becoming a victim of common security threats such as banking fraud and identity theft.

What is Phishing?

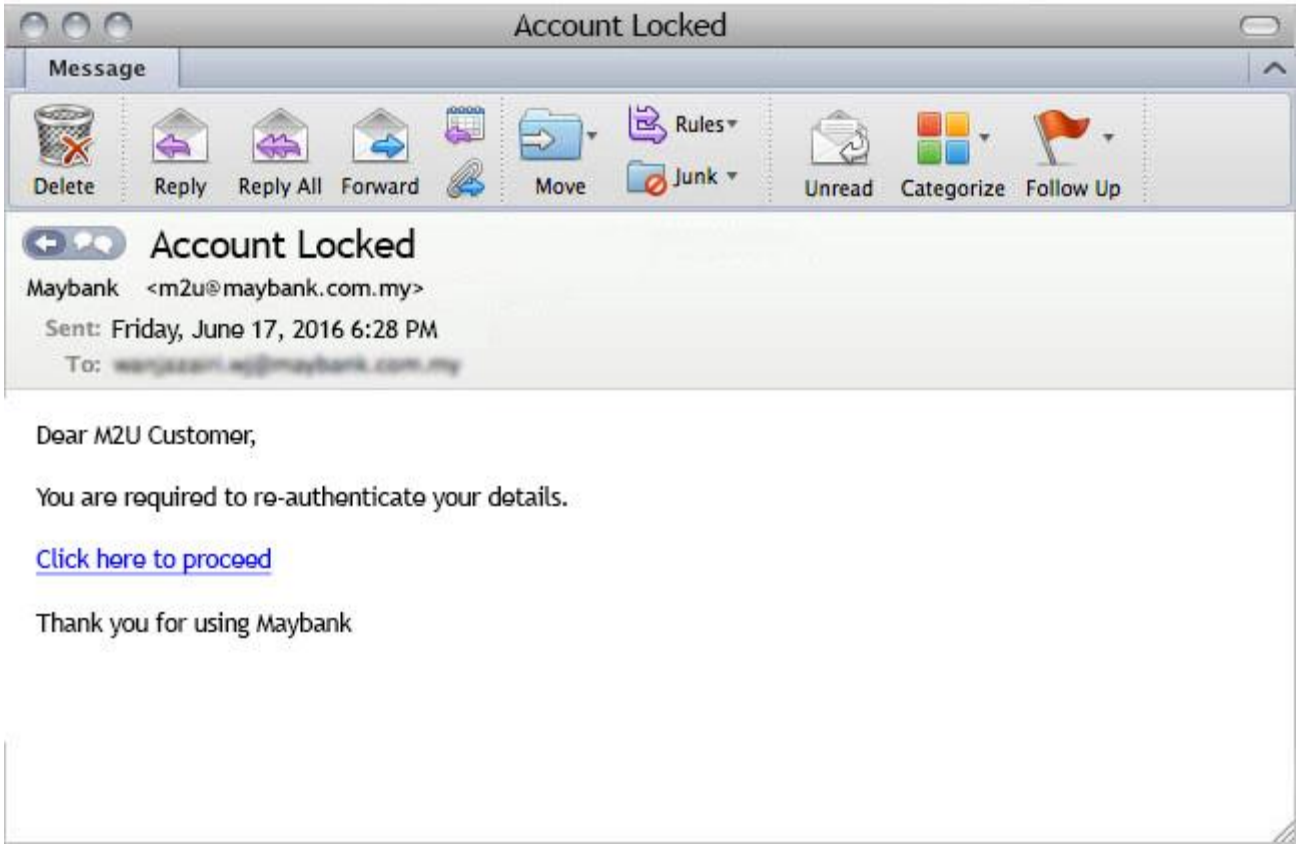
- **Phishing** is a word stemmed from **password + fishing**.
- Phishing scams are a form of **identity theft**, where spam emails are sent out the victims to update their banking credentials.
- The victims are tricked to click on a bogus hyperlink provided by the fraudster as long as they maintain an email account.
- The victims will then be r**edirected to fake login site that is identical the Bank website**.



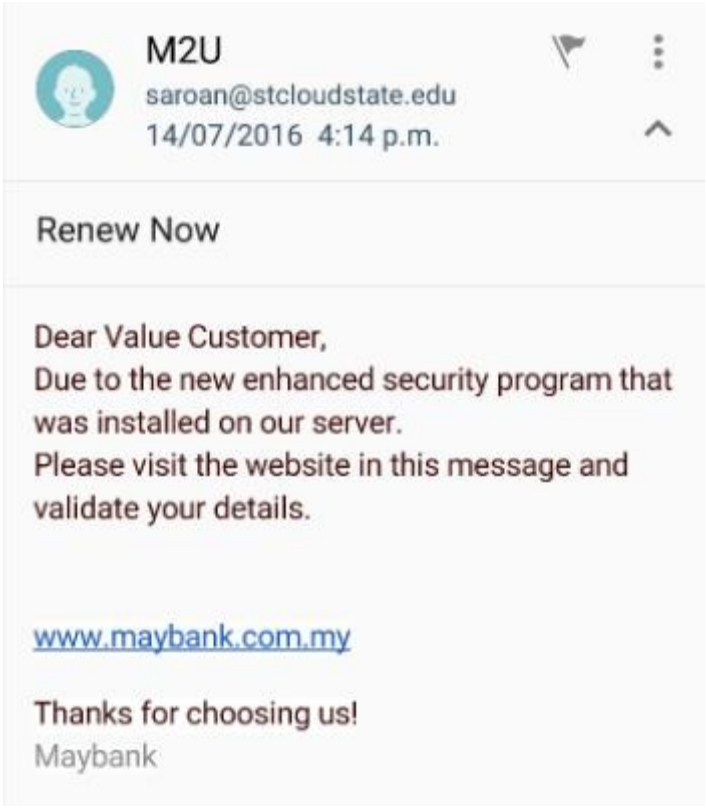
Latest Phishing Emails in Circulation



Latest Phishing Emails in Circulation



Latest Phishing Emails in Circulation



M2U
saroan@stcloudstate.edu
14/07/2016 4:14 p.m.

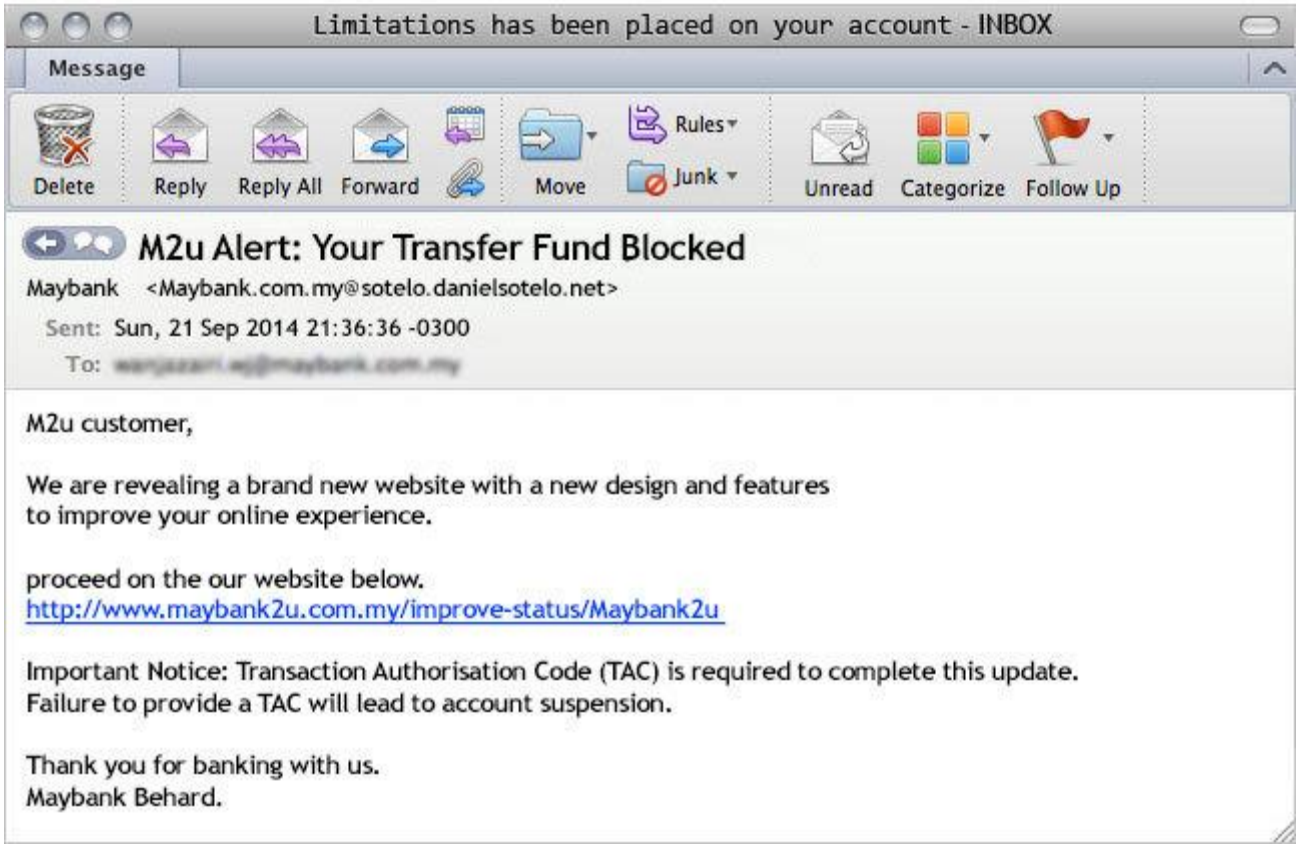
Renew Now

Dear Value Customer,
Due to the new enhanced security program that was installed on our server.
Please visit the website in this message and validate your details.

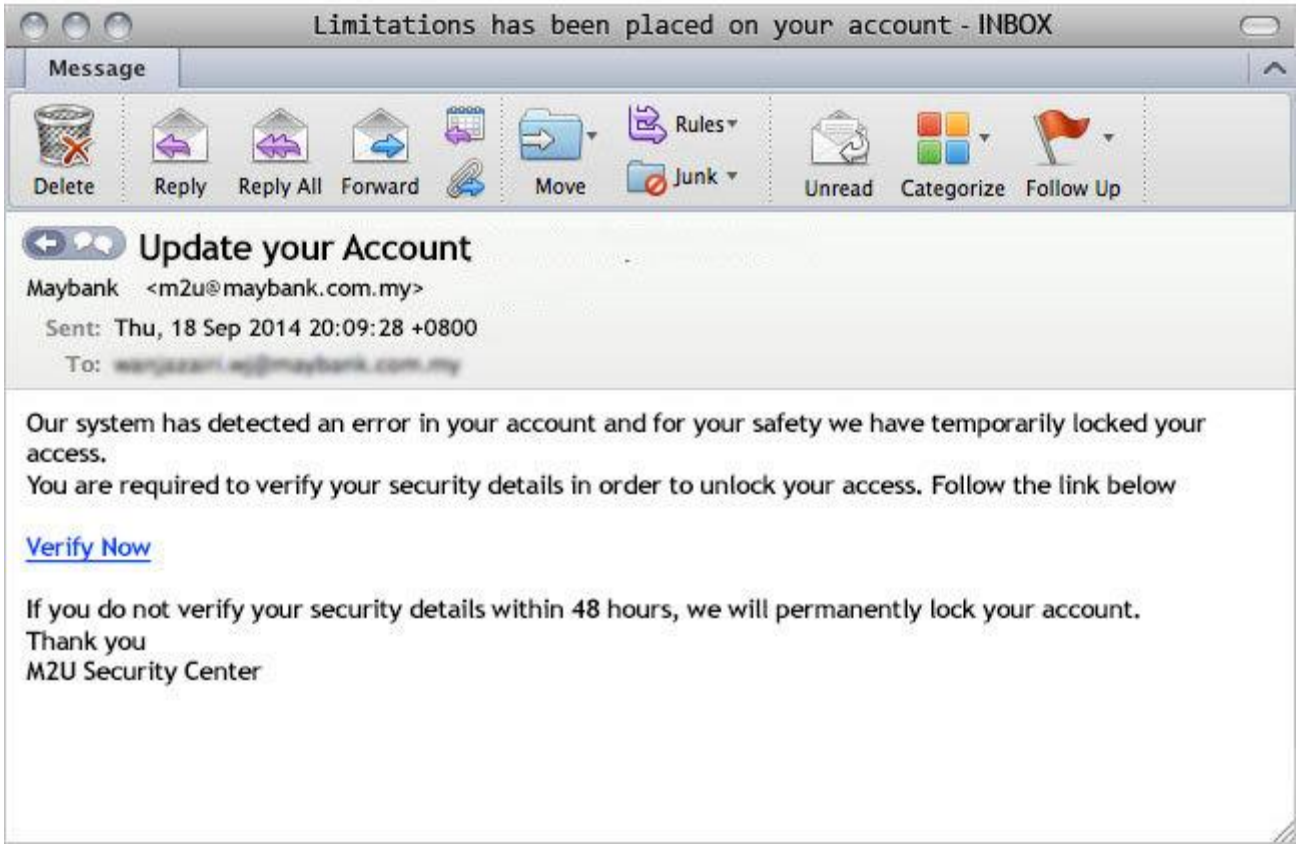
www.maybank.com.my

Thanks for choosing us!
Maybank

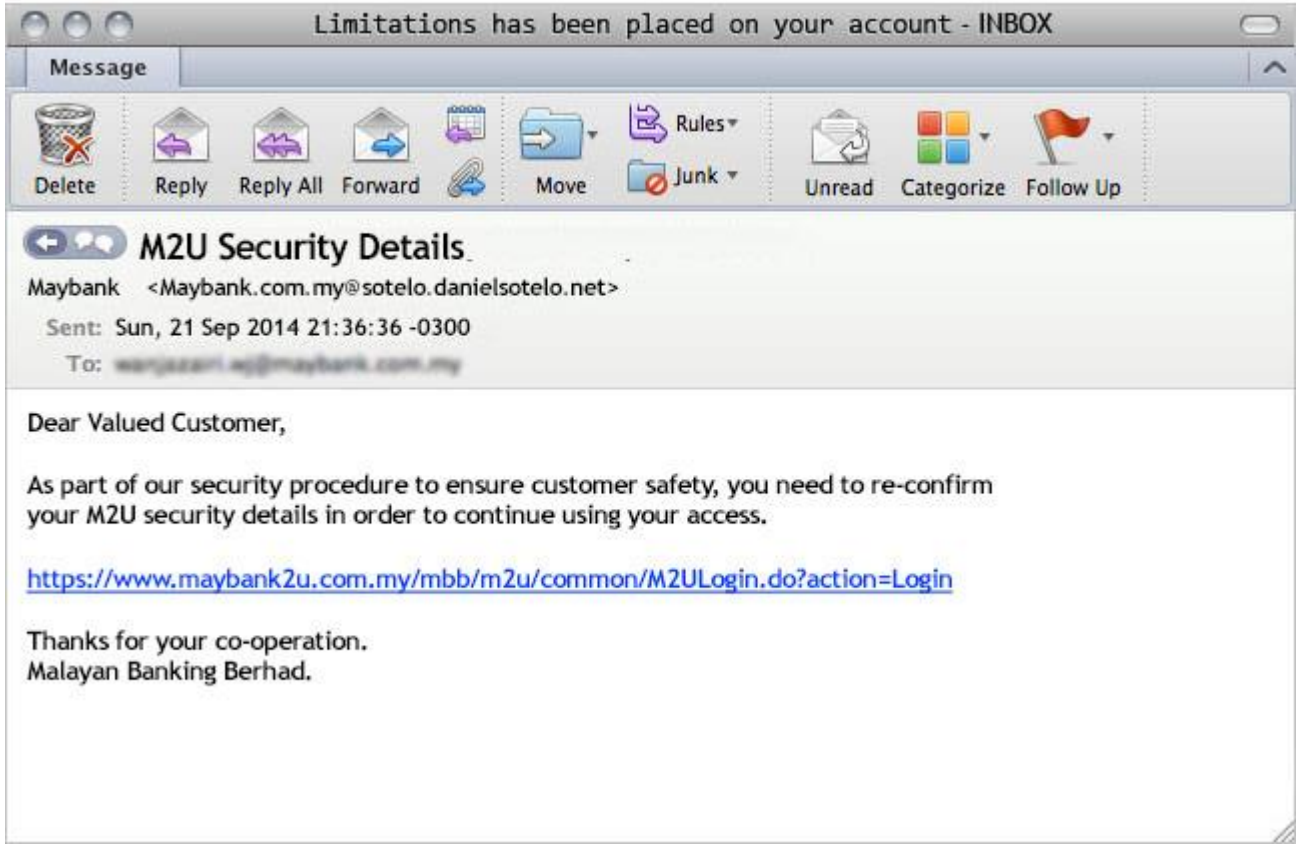
Latest Phishing Emails in Circulation



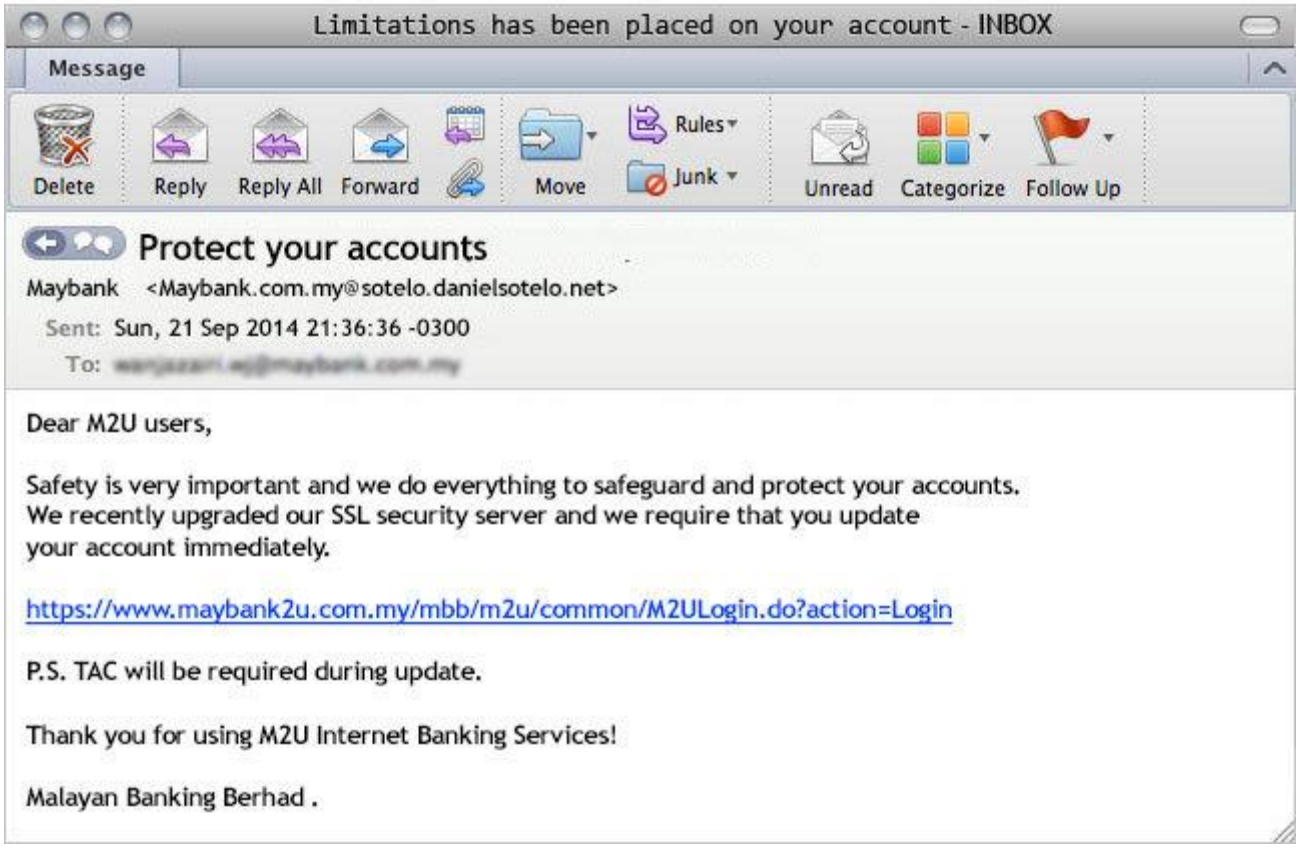
Latest Phishing Emails in Circulation



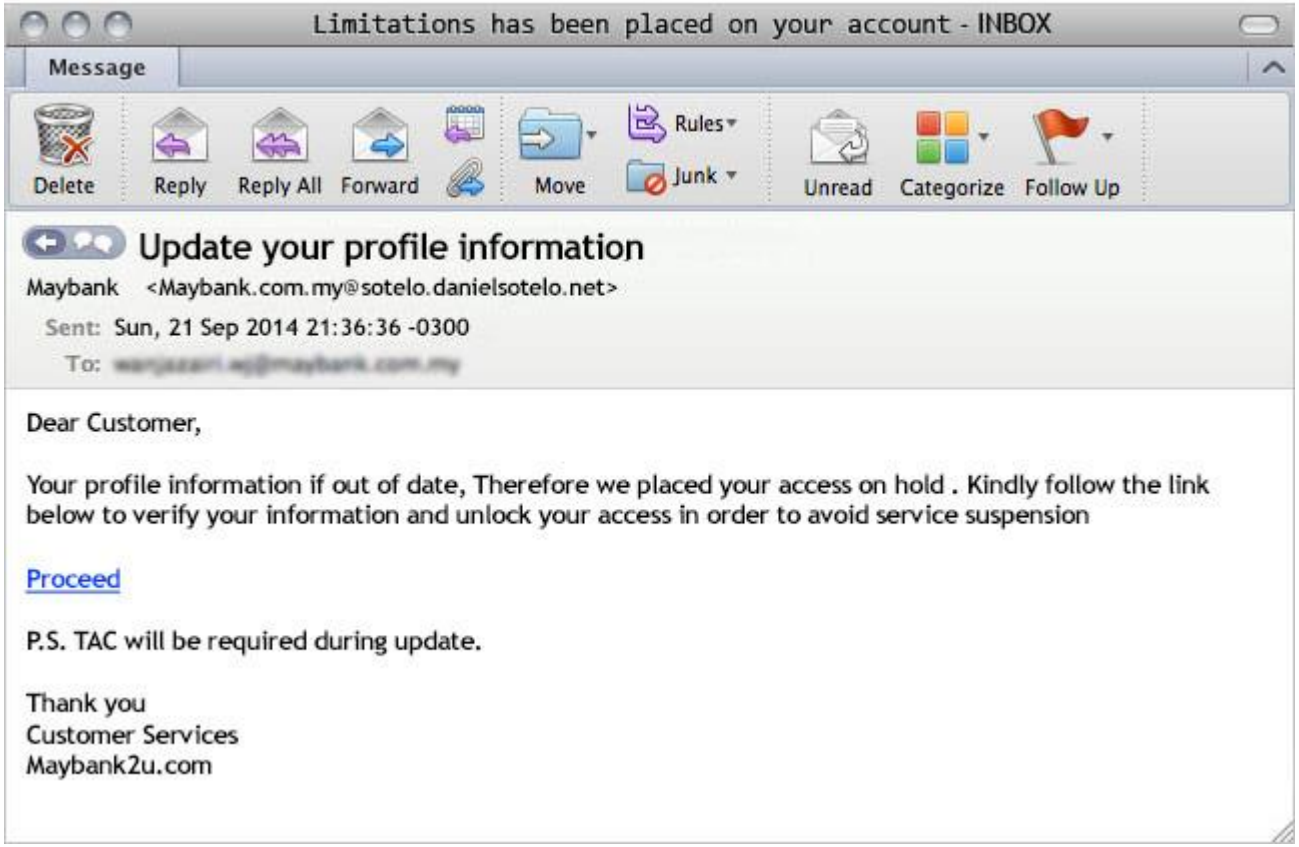
Latest Phishing Emails in Circulation



Latest Phishing Emails in Circulation



Latest Phishing Emails in Circulation



Latest Phishing Emails in Circulation

Maybank Alert: Enhanced Security Features - INBOX

Message

Delete Reply Reply All Forward Move Rules Junk Unread Categorize Follow Up

Maybank Alert: Enhanced Security Features

Maybank Group <security.alert@maybank2u.com.my>

Sent: Thursday, 7 July 2011 15:53:23 +0000

To: [redacted]

Dear valued customer,

We have enhanced our security features. With this enhancement, Transaction Authorisation Code (TAC)* will only be valid per transaction. For any subsequent transactions, you will need to request new TAC.

We therefore, require that all customers verify their data. You will be required to select a new security and also required to verify your security questions and answers. Kindly ensure you enter correct details to avoid service suspension.

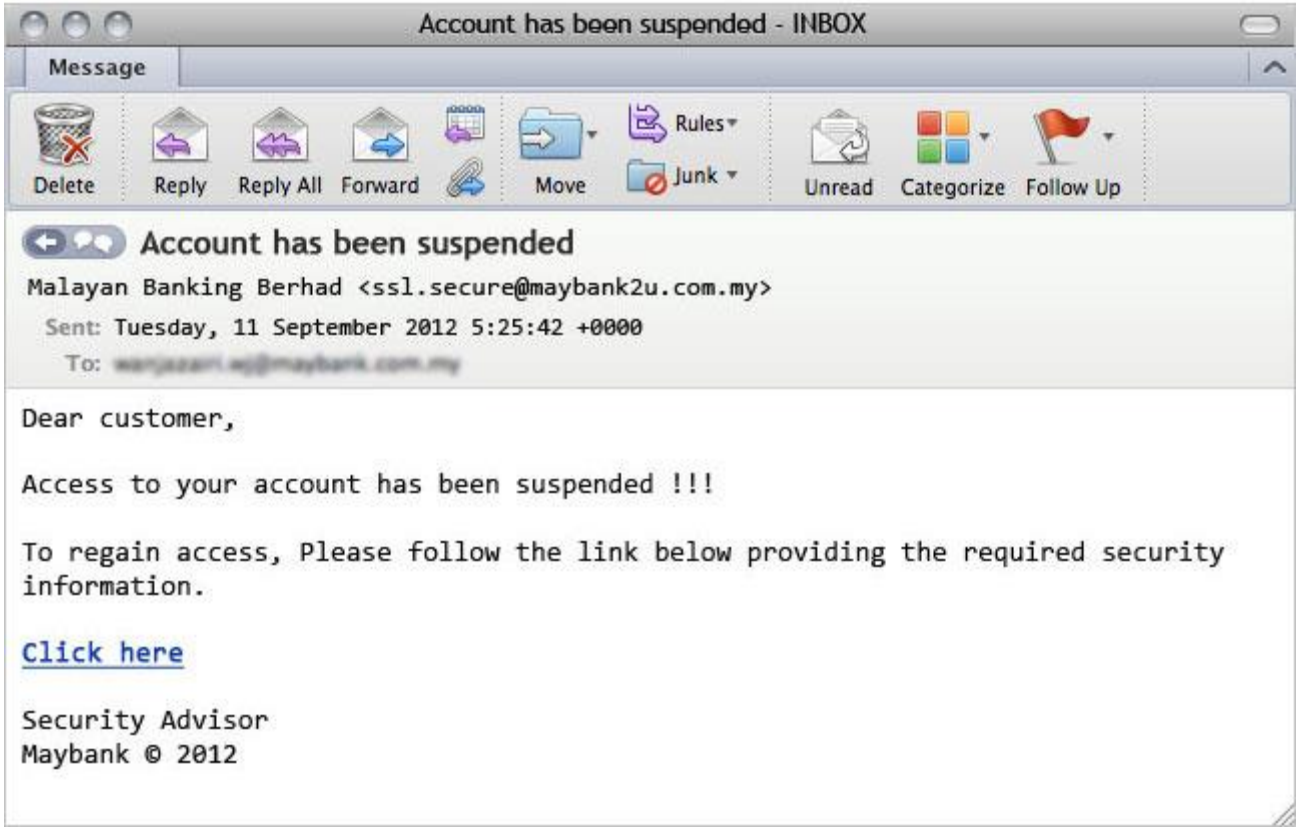
Click on the link below to continue

Click here to proceed

We apologise for any inconvinience this might cause you.

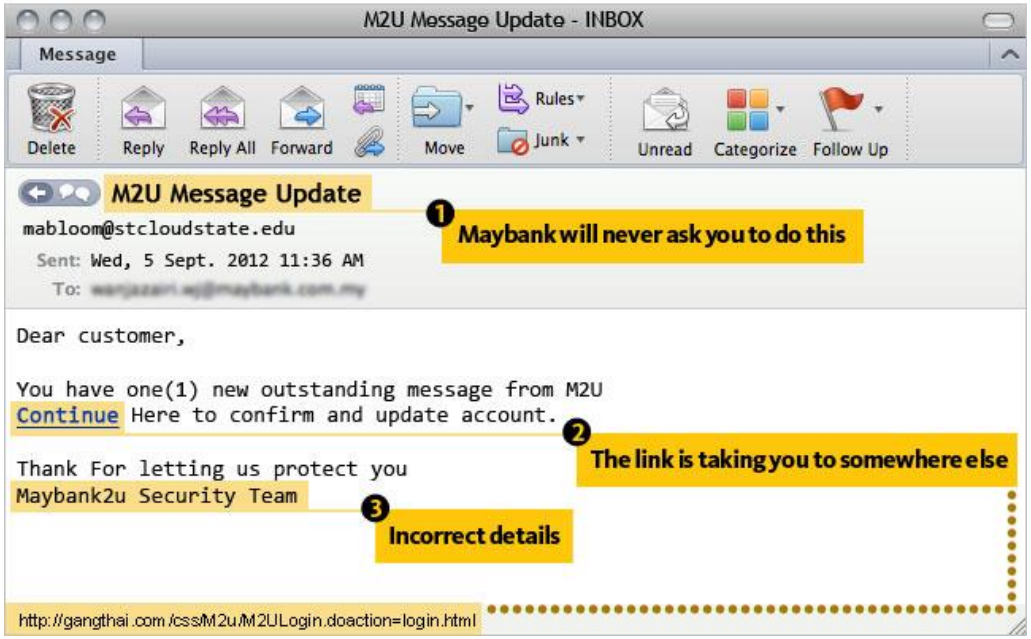
Thank you for using Maybank2u.com

Latest Phishing Emails in Circulation



Latest Phishing Emails in Circulation

Latest Phishing Emails in Circulation



Never respond emails that:

1. Requires you submit your personal information directly in the e-mail or online.
2. Requires you reregister your security image, caption and challenge questions.
3. Threatens close or suspend your accounts if you don't respond.
4. Claims there are unauthorized transactions on your account and requires your account information.
5. Claims that your account has been compromised and requests you enter, validate or verify your account information.
6. Requires you enter your card number, password, user ID or account numbers in email, pop-up window or non-secure webpage.
7. Requires you confirm, validate, verify and/or update your account or credit card information.
8. Requires you confirm your IP address.

Malware

An SMS Scam happens when a customer receives an SMS claiming they have won “cash rewards”.
They are then lured respond by following the fraudster/syndicate’s instructions apply for internet banking.
These SMS Scams have been sent out by fraudsters pretending the from well known organizations.

Malware

Read carefully before you proceed

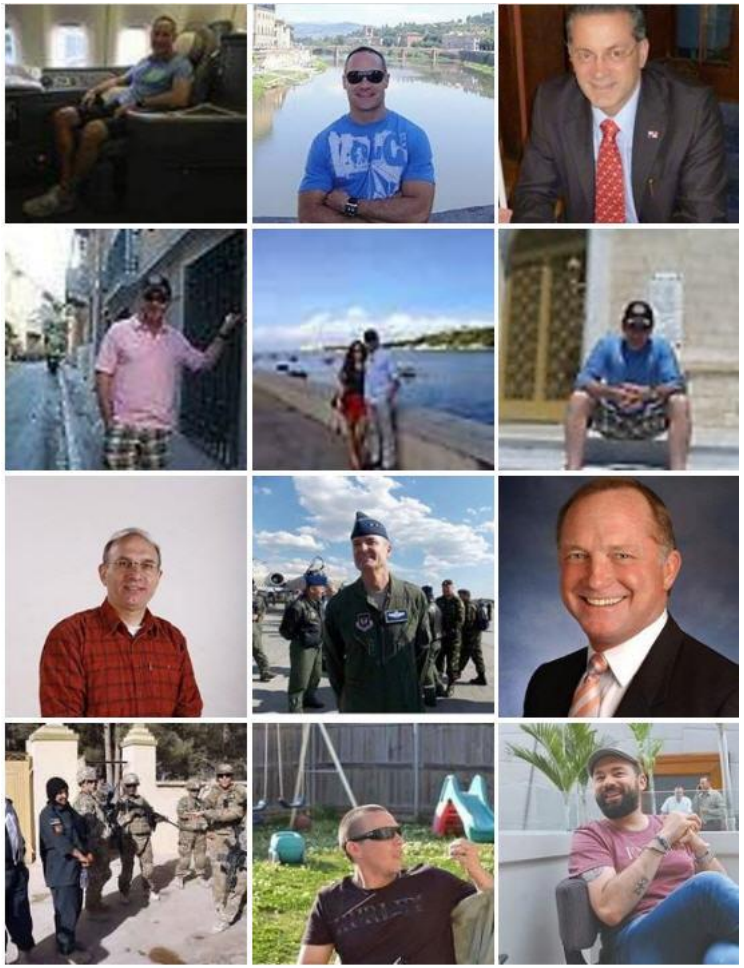
เตือนภัย ใช้อีเมลปลอมหลอกให้โอนเงิน

SCAMMER

- Scam คืออะไร?การหลอกลวงทางอินเทอร์เน็ตอีกแบบหนึ่ง เช่น หลอกให้ร่วมทำธุรกิจด้วย หลอกว่าเป็นผู้โชคดีถูกรางวัล หลอกให้ช่วยเหลือแล้วจะตอบแทนด้วยเงินก้อนโต จนปัจจุบันมันก็ยังมีขบวนการนี้อยู่ มันมีการหลอกลวงหลายรูปแบบ ที่มากสุดคือการใช้ความรักมาล้อเล่นและล่อลวงแบบข้ามประเทศ หลอกว่าคุณเป็นทายาทของมหาเศรษฐีที่เพิ่งเสียชีวิตไป วิธีการหลอกก็คือ มิจฉาชีพจะส่งอีเมลจำนวนมาก ไปหาเหยื่อกลุ่มใหญ่ ภายในอีเมลจะมีเนื้อหาเชิญชวน โน้มน้าว ทำให้เหยื่อเชื่อมั่น (confidence trick) อยากทำตามข้อความเชิญชวนหรือโน้มน้าว เช่น ร่วมลงทุนด้วย ลงทุนเพียงนิดเดียวแต่ได้กำไรกลับคืนมหาศาล บางครั้งยอมโอนเงินค่าดำเนินการไปให้เพื่อหวังได้รางวัลก้อนโตกลับมาในเวลาอันสั้น

- วิธีการสร้างกลลวงของ Scamมิจฉาชีพจะทำการส่งอีเมลหว่านออกไปเป็นจำนวนมาก แล้วก็รอให้เหยื่อเชื่อคำหวานที่เขียนไปในอีเมล เหยื่อเพียง 3 หรือ 5% ที่หลงกลก็คุ้มเกินคุ้ม เมื่อเหยื่อตอบกลับมา พวก scammer ก็จะติดต่อกลับเพื่อดำเนินการหลอกลวงอย่างอื่นต่อไปทันที เช่น หากคุณต้องการร่วมลงทุนกับเรา คุณจะต้องจ่ายค่ามัดจำสินค้าก่อน โปรดโอนเงินให้เป็นจำนวนเงิน **XXX,XXX** บาท เป็นต้น หากเหยื่อเริ่มระแวง ก็อาจจะเชิญให้มาพบที่สำนักงานเพื่อหลอกล่อให้ตายใจ ซึ่งจะมีหลากหลายวิธีในการหลอกลวง

- ความเสียหายที่เกิดขึ้นหากผู้เสียหายหลงเชื่อข้อความทางอีเมล อยากรวยทางลัด ก็จะโอนเงินไปก่อน สุดท้ายคือถูกโกงหน้าตาเฉย ทำให้สูญเสียทรัพย์สินเป็นจำนวนมาก เหยื่อบางราย ระยะแรกๆ ก็อาจจะได้รับกำไรคืนกลับมาบ้าง แต่พอนานๆ เข้า ก็ขาดการติดต่อ และโดนโกงไปเช่นกัน



SCAMMER

แก้งค์ Scammer อาชญากรรมทางการเงินและจิตใจ ข้ามชาติ

ปัญหาสังคม

กระทู้สนทนา

เริ่มจากนี่เลยค่ะ อยากมีแฟนชาวต่างชาติ (หวังสูงไปนิดค่ะ อยากสบาย 555) ทีนี้เลยไปเข้าไปเวปไซด์หาคู่แห่งหนึ่ง มีค่ะ ได้ค่ะ คุยทางเมล์กัน เราก็ยิ้มแป้นเลย (ยอมรับตามตรง เพิ่งเคยสนใจ ไม่ได่ดูรีอ่านข่าวสารเกี่ยวกับพวกนี้เลย) เค้าส่งมาหาเราทุกเมล์นี้หวานหยดย้อย เป็นพ่อหม้ายวัย 45 เมียตาย ลูกติด 1 สาวน้อยน่ารักวัย 6 ขวบ รูปที่ส่งมา (ไปก๊อปใครเค้ามาไม่รู้) ดูดีมาก โปรไฟล์นี้รักลูกสุดๆ หลายรูปมาก คุยไปคุยมา เราก็แอบเพ้อ แหม่ๆก็ต้องมีบ้าง ก็เราขี้เหร่นี่ คุยโน่นนี่นั่นได้สัก 3 อาทิตย์กว่าๆได้ มีข่าวดีมาก ต้องไปซื้อของเข้าแกเลอรี่ที่แอฟริกา (เค้าบอกทำธุรกิจเกี่ยวกับของเก่า ของโบราณ อยู่อังกฤษ เป็นคนอังกฤษ) ทีนี้เค้าบอก ไปแอฟริกาน่าจะ 2-3 วัน มีเวลาเหลือว่างประมาณเกือบ 2 อาทิตย์ อยากมาหาเราที่เมืองไทย พร้อมลูกสาว ลูกสาวอยากเจอ อยากทำความรู้จัก รักคิดถึงอยากสานสัมพันธ์อยากใช้ชีวิตบั้นปลาย บราๆๆๆๆ เยอะค่ะเยอะ เราก็งงสิ่ค้ะ เป็นไปได้เหรอ ก็กล้าๆกลัวๆ ปรึกษาหมดเลยพ่อแม่พี่น้องพ้องเพื่อน ก็มีเตือนบ้าง แต่ก็อ๊ะ ลองดู เค้าก็ส่งเมล์มาเล่าโน่นนี่นั่นที่แอฟริกา เนียนด้วยนะ ส่งรูปบนเครื่องมาด้วย ใกล้จะเสร็จธุระและ ใกล้มาหาและ เรานี่นับวันเลย 555 แต่ก็ยังเอะใจ เป็นไงเป็นกัน แต่เอ๊ะ!! เข้า google ดีกว่า ถามเลย ภัยจากการหาคู่ตามเวปไซด์ ทีนี้มาพรึบเลย แก้งค์ scammer คือไรว๊า ก็อ่านค่ะ เอ๊า!! คล้ายเราเลย แต่แตกต่างกันไปหลายรูปแบบ เอ่อนะ?? เข้าเคล้า อ่านไปหลายกระทู้ หลายคนที่เจอมา ส่วนใหญ่เป็นหญิง เสียรู้พวกมันไปกันเยอะเลยค่ะ สูญเงินนับหมื่นนับแสน เราก็อ่านๆๆๆ มาสะดุดตรงเรื่องลูก เอาลูกมาทำธุรกิจด้วย เอิ่มคล้ายๆ ส่วนใหญ่จะมา ไนจีเรีย เราเชครหัสเบอร์มือถือที่ให้เรามา +234 เอิ่ม ใช่เลย อ่านถึงลูกป่วยเชคที่ได้มาขึ้นเงินไม่ได้บ้าง ถูกปล้นบ้าง โน่นนี่นั่น เนียนแบบประมาณว่าจองตั๋วเครื่องบินมาไทย จะส่งมาให้ดูรายละเอียดเวลาการเดินทาง เยอะค่ะเยอะ เข้าไปอ่านกันดูนะค้ะ จะแนบลิ้งค์ไว้ให้....อ่ะต่อ ทีนี้เมลเด้งขึ้นมาเลยค่ะ ส่งข่าวเป็นยังไง อยู่ยังไง กินยังไง สักพักสะดุดก็กเลยค่ะ แม่เจ้า!! ลูกป่วยค่ะ ส่งคลีนิคแล้ว เย้ยยยย!! เป๊ะๆเด๊ะๆ ทีนี้เอาไงต่อดี โดนกะเค้าแล้วเรา เข้ามาโทรหาเพื่อนเลยค่ะ เล่าๆๆๆ เลยตัดสินใจคุยต่อ ไม่ใช่หลงนะค้ะ อยากรู้ จะมายังไงต่อ ตอนนี้ถึงลูกป่วยแล้วค้าาาา พ่อแม่พี่น้องพ้องเพื่อนแนะนำกันหน่อย จะคอยดูเหมือนกัน เมล์ต่อไปจะเป๊ะอีกมั้ย....ทีเนี้ยอยากให้มันโดนจับอ่ะค่ะ จะหลอกล่อยังไงดี ใครมีข้อมูลแนะนำบ้าง ช่วยๆหน่อย อีกอย่างขอเตือนภัยสาวๆหลายคนด้วย อาจจะรู้ช้ายืดยาดกว่าชาวบ้านชาวช่องเค้า แต่เราก็เชื่อว่า ยังมีบ้างที่ตกเป็นเหยื่อกันอยู่ตอนนี้

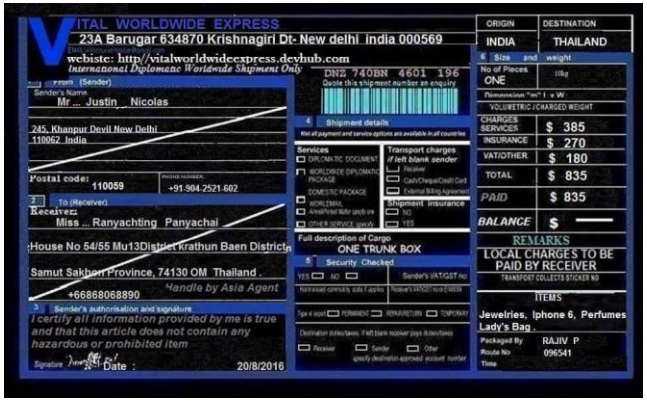
http://newtampo.wordpress.com/2009/05/26/%E0%B8%AB%E0%B8%B2%E0%B8%81%E0%B8%B4%E0%B8%99%E0%B8%81%E0%B8%B1%E0%B8%9A%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B8%A3%E0%B8%B1%E0%B8%81-%E0%B8%AA%E0%B9%81%E0%B8%81%E0%B8%A1%E0%B8%A5%E0%B8%A7%E0%B8%87/

0 0 | koykamol
5 กันยายน 2556 เวลา 05:19 น.

SCAMMER

วิธีการป้องกัน

1. เมื่อได้รับอีเมลข้อความแปลกๆ ให้วิเคราะห์ข้อความที่ส่งมา หากเป็นการเชิญชวนให้ร่วมลงทุน หรือเสนอช่องทางรวยให้กับคุณ ให้สันนิษฐานได้เลยว่า หลอกลวงแน่นอน เพราะไม่มีบริษัทไหน จะเชิญลงทุนผ่านอีเมล
2. ไม่ตอบกลับอีเมลแปลกๆ ที่คุณไม่รู้จัก
3. ติดตั้งโปรแกรมต้านไวรัสและ **Firewall** ซึ่งสามารถป้องกันการรับอีเมลที่ไม่พึงประสงค์หรือการสื่อสารจากผู้ที่ไม่ ได้รับอนุญาต การติดตั้งโปรแกรมปรับปรุงช่องโหว่ (**patch**) ก็สามารถป้องกันผู้ลักลอบ (**hacker**) หรือผู้ส่งอีเมลปลอมได้
4. ป้องกัน **Malware** ที่จะเข้ามาฝังตัว ทำความผิดปกติให้กับเครื่อง หรือเจาะรหัสผ่านต่างๆ โปรแกรมเหล่านี้แอบเข้ามาง่ายมาก บางครั้งการเข้าเว็บบางแห่งก็ติดโปรแกรมไม่พึงประสงค์แฝงตัวเข้ามาด้วย



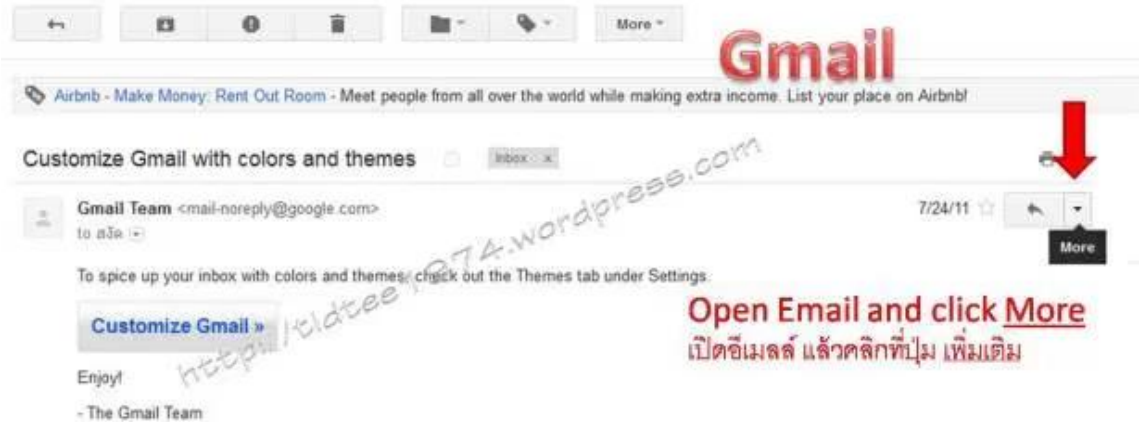
How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- วิธีหา IP Address จากอีเมลล์ที่คนอื่นส่งมาให้เราจาก Gmail, Yahoo, Hotmail หรือ Outlook Express และเมลล์อื่นๆ
- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
- ขั้นตอนที่ 2 ค้นหาจากรูปถ่าย (Searching from Images)

How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)

- Log In your email ลงชื่อเข้าใช้อีเมลล์ เช่น hotmail, yahoo, gmail, และเมลล์อื่นๆ
- Click on view message source (Hotmail+Outlook) or Show original (Gmail) and View Full Header (Yahoo) คลิกที่ดูข้อความต้นฉบับ Hotmail+Outlook หรือ ดูส่วนหัวแบบเต็ม Yahooและ แสดงต้นฉบับ Gmail
- Look at X–originating-IP or Received: from
- ♦ Hotmail → Hotmail → Look at X–originating-IP
- ♦ Other mail → Hotmail → Look at Received: from
- ♦ Yahoo→ Yahoo→ Look at X–originating-IP
- ♦ Other mail → Yahoo→ Look at Received: from
- ♦ Gmail → Gmail → Look at X–originating-IP
- ♦ Other mail → Gmail → Look at Received: from
- Log in at Gmail and click at More ลงชื่อเข้าใช้ Gmail แล้วกดที่ปุ่ม เพิ่มเติม



How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

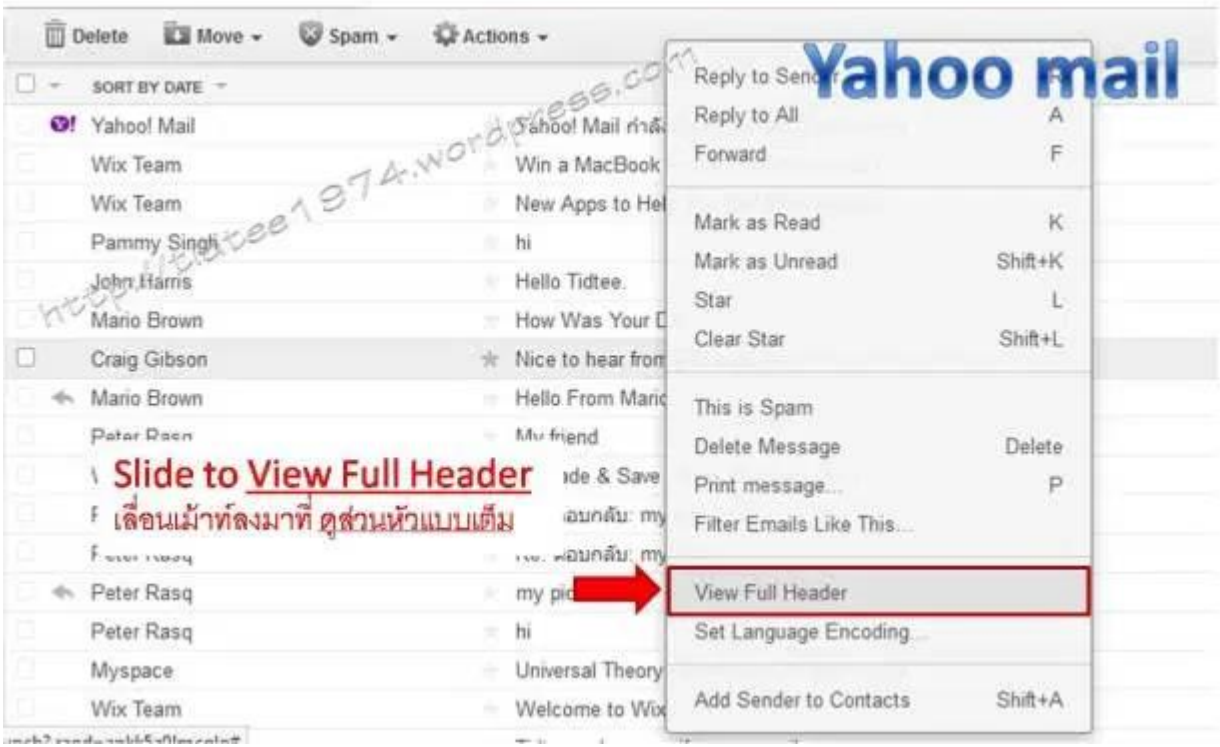
- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
  - Slide tShow original เลื่อนเม้าท์ลงมาที่ แสดงต้นฉบับ

How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
  - -เช็คจาก IP Address (Checking from IP Address) By Yahoo
  - Log in at Yahoo and right click on subject ลงชื่อเข้าใช้ Yahoo แล้วคลิกขวาที่ หัวข้อเมลล์ หรือชื่อเรื่อง

How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
  - Slide down to View Full Header เลื่อนเม้าท์ลงมาที่ ดูส่วนหัวแบบเต็ม

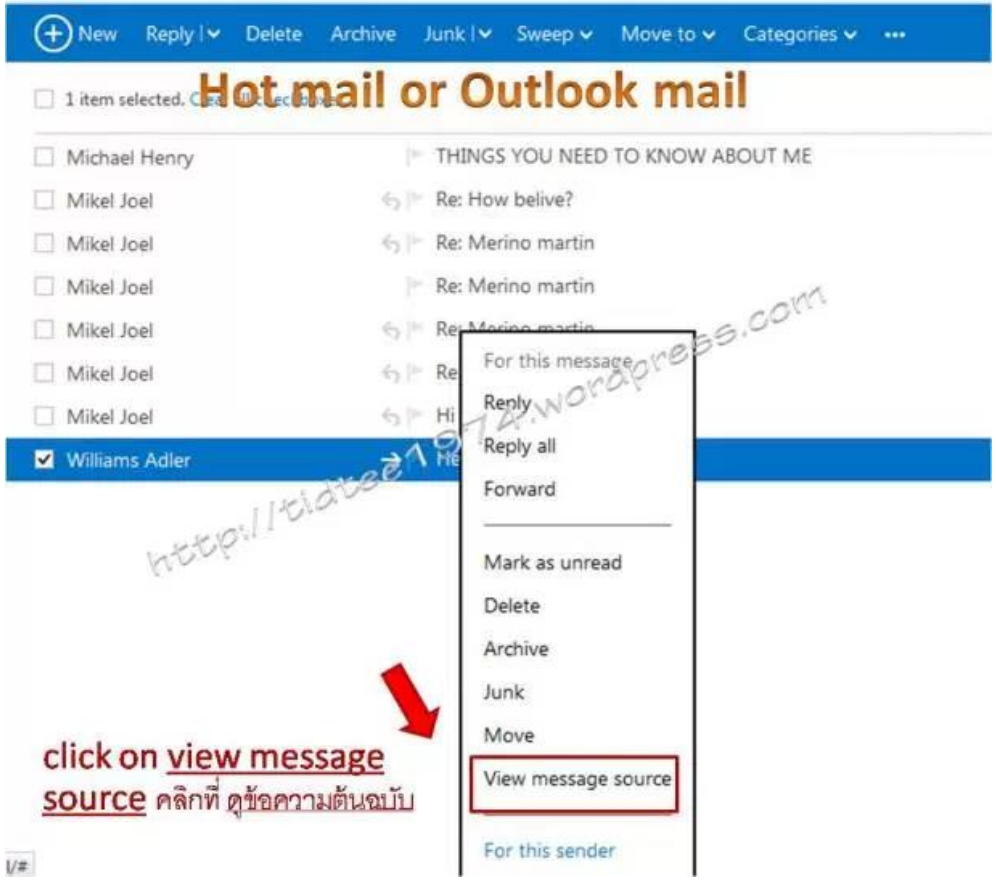


How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
- ♥ -เช็คจาก IP Address (Checking from IP Address) By Hotmail or Outlook

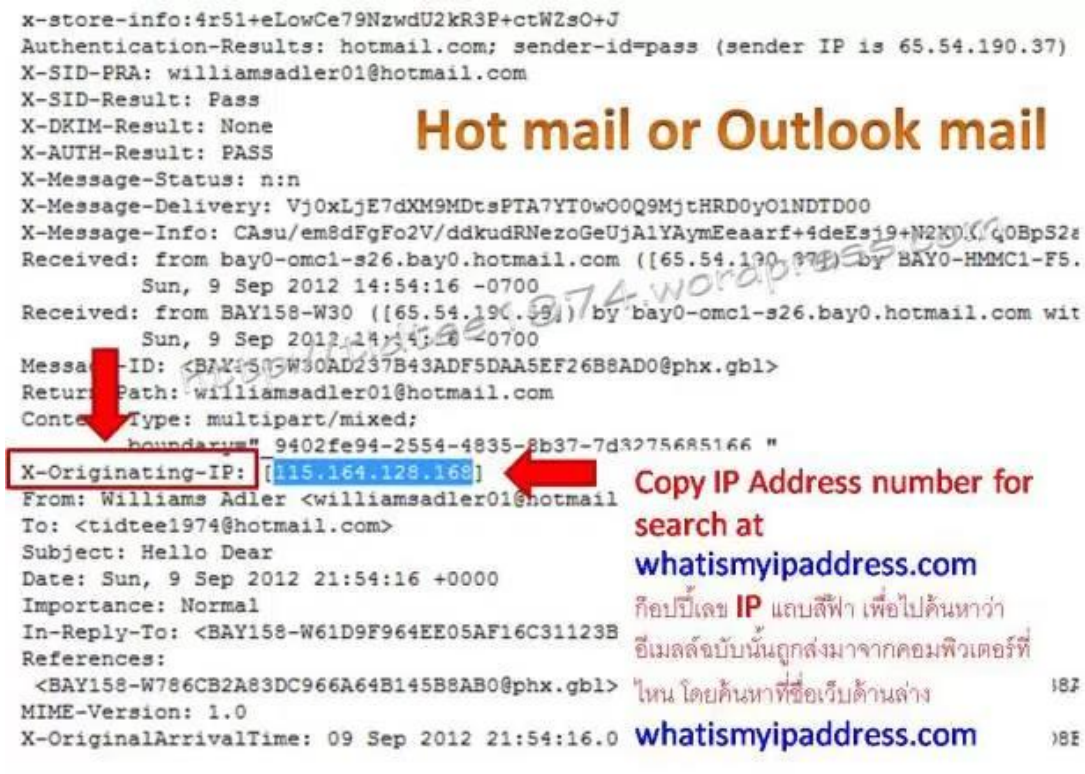
How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
  - 1.2 Click on View message source เลื่อนเม้าท์ลงมาที่ ดูข้อความต้นฉบับ



How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
- 1.3 Copy IP address number for search on www.whatismyipaddress.com
- ก๊อปปี้ IP address เพื่อไปค้นหาที่เว็บ www.whatismyipaddress.com



How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
- 1.3 Copy IP address number for search on www.whatismyipaddress.com
- ก๊อปปี้ IP address เพื่อไปค้นหาที่เว็บ www.whatismyipaddress.com

How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

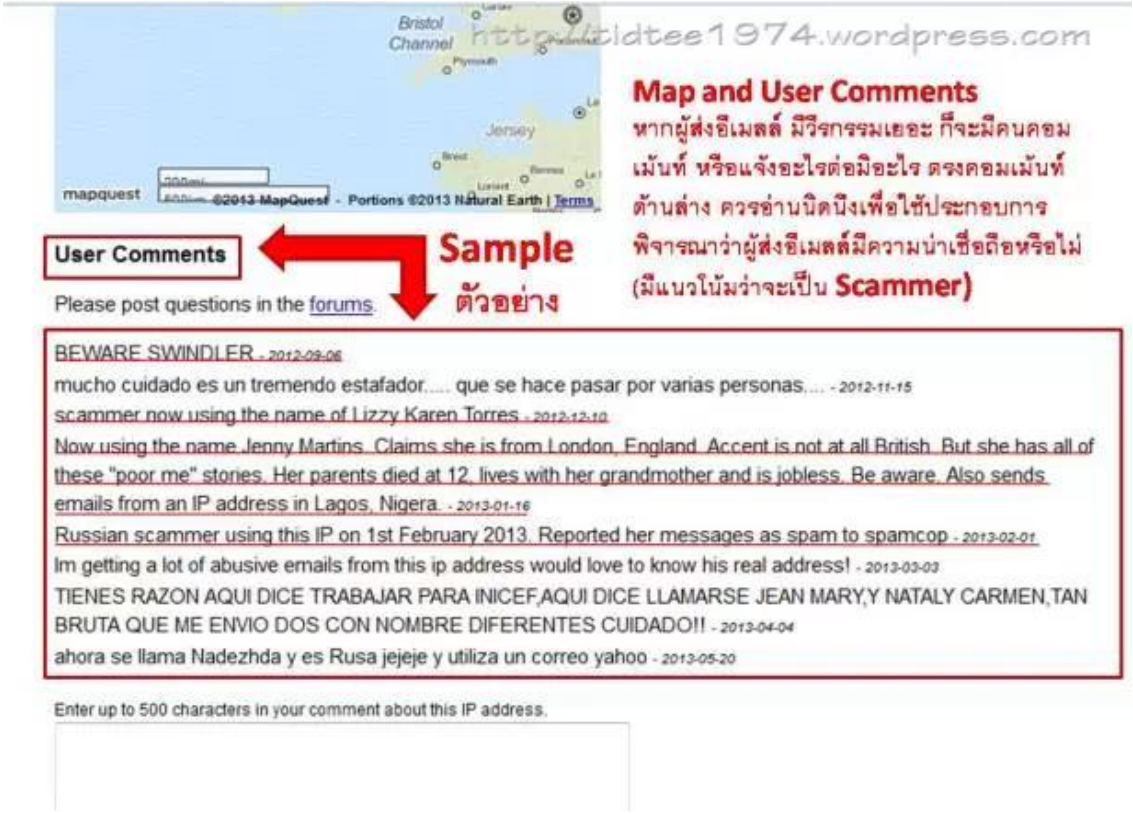
- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
  - 1.4 Click for lookup Ip address ใส่เลข IP ที่ก๊อปปี้มาก่อนหน้านี้ แล้วกดปุ่ม lookup Ip address
  - This site for check IP Address
  - www.whatismyipaddress.com

How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
  - 1.5 General IP Information and Geolocation Information ข้อมูลทั่วไปของเลข IP และที่ตั้งของคอมพิวเตอร์ผู้ส่งอีเมลล์

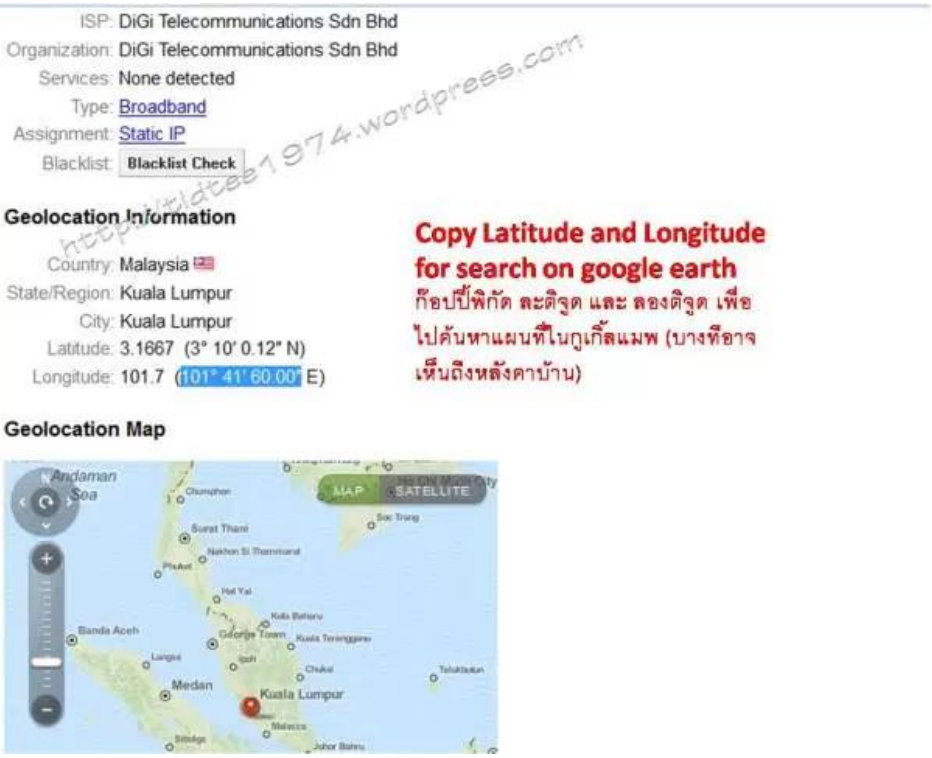
How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
  - 1.6 Geolocation Map and User Comments (must read comment from user) หาก IP นี้ มีวีรกรรมไว้เยอะ ก็จะมีคอมเม้นท์ หรือมีการแจ้งเตือนจากผู้ที่เคยเช็ค IP นี้ ในช่องคอมเม้นด้านล่าง และคอมเม้นท์เหล่านี้แหละก็จะเป็นข้อมูลเพิ่มเติมให้เราอีกด้วย (ควรอ่านนิดนึงนะ เพื่อใช้ประกอบการพิจารณาว่าผู้ส่งเมลล์ให้เรานั้นน่าเชื่อถือหรือไม่? อย่างไร?)



How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
  - 1.7 Copy Latitude, Longitude for search on Google Earth ก๊อปปี้ ละติจูด, ลองจิจูด เพื่อไปค้นหาในกูเกิ้ลเอิร์ธ

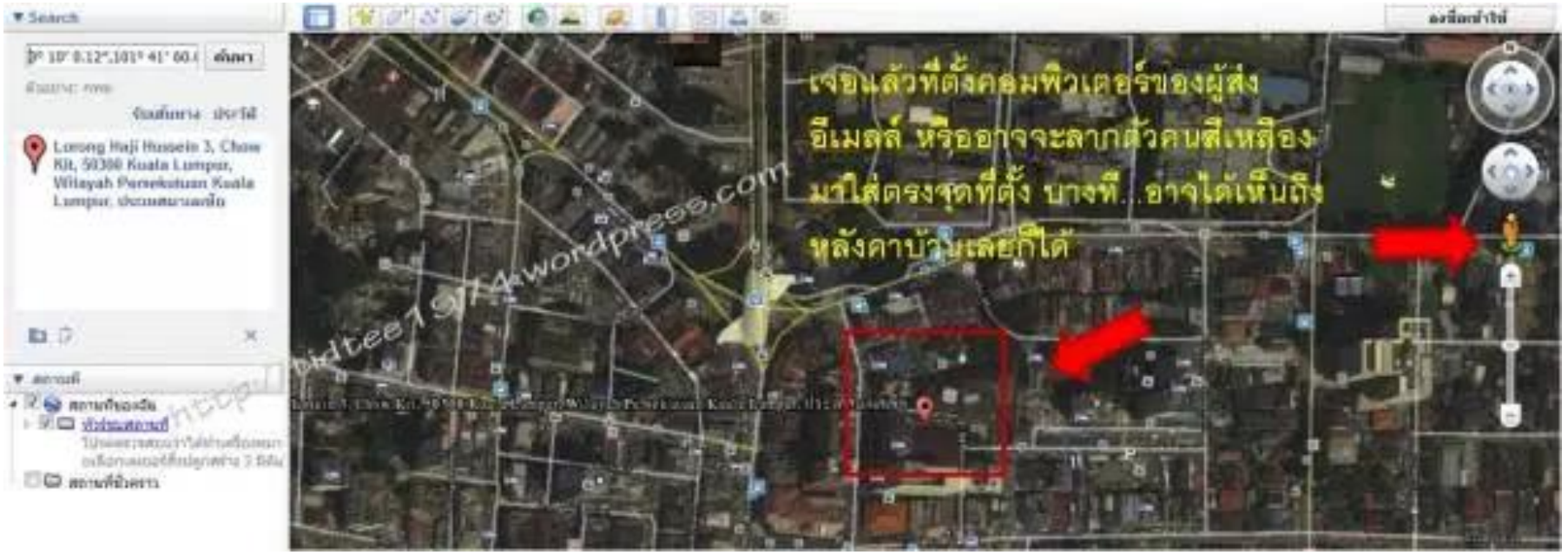


How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
- 1.8 Click on Google Earth (must install Google Earth program first) เปิด Google Earth แต่ต้องลงโปรแกรมก่อนนะ แป๊บเดียวเอง!
- 1.9 Latitude,Lonitude for search วางพิกัดที่ได้คือ ละติจูด,ลองจิจูด โดยใช้เครื่องหมายคอมม่า หรือลูกน้ำ คั่นกลางระหว่างลองติจูด กับ ลองจิจูด ในช่องค้นหา

How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 1 เช็คจาก IP Address (Checking from IP Address)
- 1.10 Finished! we found email sender เจอที่ตั้งคอมพิวเตอร์ของผู้ที่ส่งอีเมลล์มาหาเราแล้ว



How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 2 ค้นหาจากรูปถ่าย (Searching from Images)
  - 2.1 Search on Google and click on Images at menu bar เปิดกูเกิ้ล แล้วคลิกที่ค้นรูป ตรงเมนูด้านบน

How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

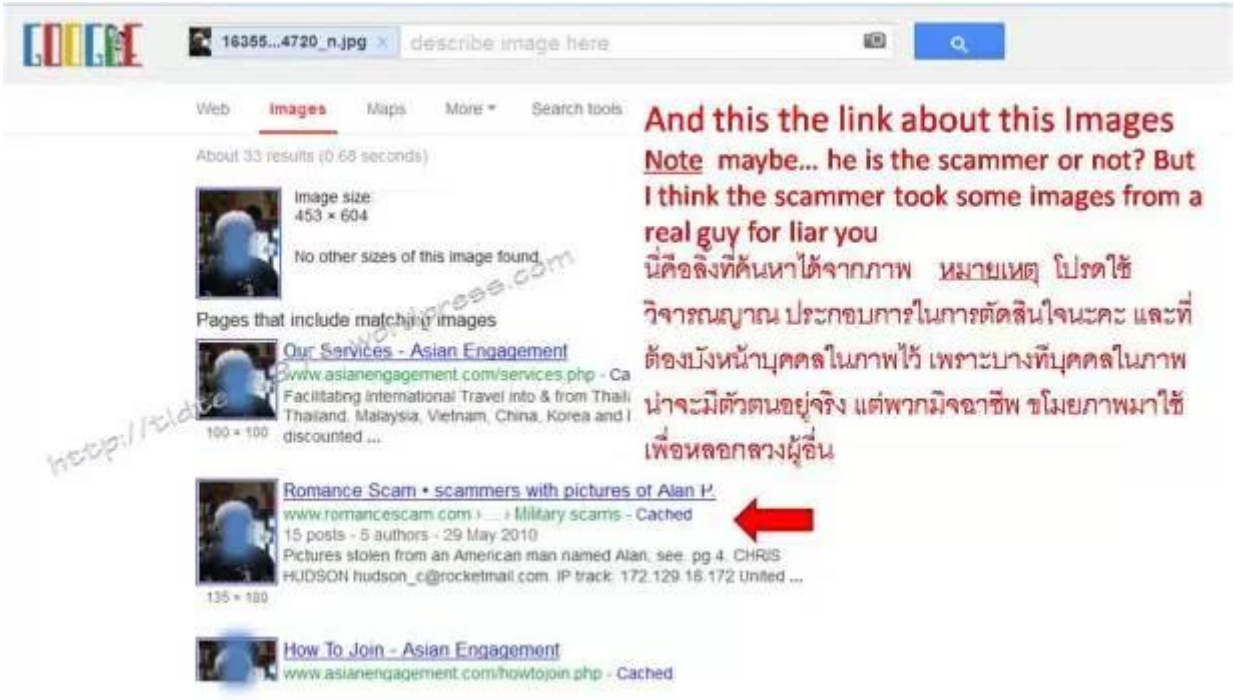
- ขั้นตอนที่ 2 ค้นหาจากรูปถ่าย (Searching from Images)
  - 2.2 Click on camera and browse an images from your computer for upload กดปุ่มเรียกดูเพื่ออัปโหลดรูปภาพ

How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 2 ค้นหาจากรูปถ่าย (Searching from Images)
  - 2.3 Click on upload and image คลิกที่อัปโหลดภาพ

How to check the IP Address of the e-mail sender วิธีหา IP Address จากอีเมลล์ที่ผู้อื่นส่งมา (Scam Hunter)

- ขั้นตอนที่ 2 ค้นหาจากรูปถ่าย (Searching from Images)
  - 2.4 A link about this Images My Note : maybe…he is the scammer or not? But i think the scammer them took some images from a real guy for liar you Link ที่ค้นหาได้จากรูปภาพที่ scammer ส่งให้
  - หมายเหตุส่วนตัว : โปรดใช้เหตุผล และวิจารณญาณในการตัดสินใจ และที่ต้องบังหน้าบุคคลในภาพไว้ เพราะบางทีบุคคลในภาพน่าจะมีตัวตนอยู่จริง แต่พวกมิจฉาชีพแอบขโมยภาพของเค้าเอามาใช้หลอกลวงผู้อื่น



เตือนภัย Scams target you protect yourself

Internet Corporation
Listing Service

ICLS.NET

Domain Name: [redacted].com
Reference Number: DS070132
Letter Date: July 15, 2009

DESCRIPTION OF SERVICES — ANNUAL WEBSITE SEARCH ENGINE LISTING
FROM July 15, 2009 THRU July 15, 2010 $65.00
TOTAL $65.00

SUBSCRIPTION INCLUDES — WITH PAYMENT YOU WILL BECOME A CUSTOMER AND RECEIVE: DOMAIN NAME SUBMISSION TO 25 ESTABLISHED SEARCH ENGINES, QUARTERLY SEARCH ENGINE POSITION AND RANKING REPORTS FOR EIGHT KEYWORD/PHRASE LISTINGS FROM 25 MAJOR SEARCH ENGINES.

INQUIRIES — E-mail: inquiries@icls.net Website: www.icls.net

SCAM

THIS INTERNET LISTING OFFER IS PROVIDED TO MILLIONS OF WEBSITES THROUGHOUT THE UNITED STATES THIS IS A SOLICITATION FOR THE ORDER OF GOODS OR SERVICES, OR BOTH, AND NOT A BILL, INVOICE, OR STATEMENT OF ACCOUNT DUE. YOU ARE UNDER NO OBLIGATION TO MAKE ANY PAYMENTS ON ACCOUNT OF THIS OFFER UNLESS YOU ACCEPT THIS OFFER.

Please make checks payable to: Internet Corporation Listing Service.

Reference Number	Listing Date	Amount	Amount Paid
DS070132	July 15, 2009	$65.00	

Service Options

☐ 1 Year ($65.00) ☐ 2 Years ($120.00) ☐ 5 Years ($260.00)

IMPORTANT
Please provide us with your current e-mail address. Submission instructions will be sent to you when payment is processed.

E-MAIL ADDRESS:

Please remit payment to address on reverse side, do not staple

**********AUTO**ALL FOR AADC 040 T231 P2
Maine Hosting Solutions - Web Hosting Made Easy
Maine's Hostmaster
122 Front St.
Bath, ME 04530-2626

THIS IS A SOLICITATION FOR THE ORDER OF GOODS OR SERVICES, OR BOTH, AND NOT A BILL, INVOICE, OR STATEMENT OF ACCOUNT DUE. YOU ARE UNDER NO OBLIGATION TO MAKE ANY PAYMENTS ON ACCOUNT OF THIS OFFER UNLESS YOU ACCEPT THIS OFFER.

ภายใน1 สัปดาห์ เว็บไซต์ของ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) ได้รับการแจ้งข้อมูลจากผู้เสียหายที่ถูกหลอกให้โอนเงินถึง 4ราย แต่ละรายเสียหายกว่า 30,000 บาท บางรายเป็นแสน และมีแนวโน้มที่จะมีผู้ถูกหลอกลวงอีกจำนวนมาก

มิจฉาชีพจะหลอกลวงด้วยการอ้างตนเป็นบุคคลมีชื่อ มีตัวตน มีอาชีพ ในหลายรูปแบบสร้างข้อมูลต่าง ๆ เกี่ยวกับตนเองเพื่อให้เกิดความน่าเชื่อถือ จะสร้างเอกสารราชการปลอม ส่งภาพถ่าย ปลอม กล่าวโดยสรุปคือ คนร้ายจะสร้างโปรไฟล์ต่าง ๆ ที่เป็นเท็จทั้งหมด เพื่อให้คู่สนทนาเห็นว่า น่าเชื่อถือ คบหาและสนทนาอย่างต่อเนื่อง เริ่มต้นคนร้ายจะทำความรู้จักกับเหยื่อด้วยการสื่อสารผ่าน E-mail , Facebook การ chat ผ่านระบบเครือข่ายต่างๆหรือการเข้าไปในเว็บไซต์หาคู่ หรือแม้แต่การทำทีเข้าไปติดต่อเรื่องงานในโลกไซเบอร์เป็นต้น ด้วยความที่คนร้ายส่วนหนึ่งเป็นต่างชาติ (ส่วนใหญ่พวกผิวดำ) การติดต่อ สื่อสารจึงใช้ภาษาอังกฤษดังนั้นผู้ที่ตกเป็นเหยื่อมักจะเป็นผู้ที่สามารถในการเขียนอ่านภาษาอังกฤษได้หลังจากได้เริ่มทำความรู้จักแล้ว ก็จะติดต่อพูดคุยเรื่อยมา สร้างความสนิทสนม แล้วจะพัฒนาความสัมพันธ์ไปเรื่อย ๆโดยพยายามทำให้เห็นว่าเป็นผู้มีความจริงใจ บางรายถึงเอ่ยปากรักใคร่ชอบพอ ในเชิงชู้สาว บางรายอาจบอกว่าอยากจะร่วมทำธุรกิจด้วย ซึ่งส่วนใหญ่จะอ้างว่ามีฐานะทางการเงิน มีทรัยพ์สินมากแต่อยู่ในสถานภาพที่ไม่สามารถใช้จ่ายในประเทศของตนได้อย่างสะดวกเพื่อหลอกให้เหยื่อคาดหวังคนร้ายพวกนี้หากเราตรวจสอบที่มาของอีเมล์ด้วยการตามไอพีแอดเดรส ก็จะพบว่ามาจากต่างประเทศจริง

เตือนภัย Scams target you protect yourself

คนร้ายจะไม่รีบร้อนในการพูดคุยกับเหยื่อ จะรอจนคิดว่าเหยื่อตายใจ จากนั้นจะเริ่มแผนต่อไป คือ อ้างว่าได้ส่งของมาให้ อาจเป็น ของใช้ต่าง ๆ น้ำหอม เครื่องประดับมีราคา หลายรายการผ่านบริษัทที่รับจ้างส่งสินค้า โดยอาจเป็นทางเครื่องบินหรือทางเรือแล้วแต่คนร้ายจะสร้างเรื่อง และเพื่อให้เหยื่อหลงเชื่ออย่างสนิทใจและเพื่อตอกย้ำให้เหยื่อเชื่ออย่างสนิทใจ คนร้ายได้ส่ง Account ที่มี Username และ Password เพื่อให้เหยื่อเข้าไปตรวจสอบกับเว็บไซต์ของบริษัทที่เป็นผู้ส่งสินค้าหรือสิ่งของนั้นมาให้ด้วย ซึ่งโดยแท้จริงแล้วเว็บไซต์ของบริษัทผู้ส่งสินค้า Account ที่มี Username และ Password ล้วนเป็นสิ่งที่คนร้ายได้สร้างขึ้นมาเองเพื่อไว้หลอกลวงทั้งสิ้นเหล่านี้เรียกว่า Phising Mail นั่นเอง ไม่นานนักเหยื่อก็จะได้รับโทรศัพท์ที่มีเลขหมายในประเทศไทย (ถ้าใช้โทรศพท์มือถือจะใช้แบบที่ไม่จดทะเบียนหรือใช้เบอร์โทรจากระบบโทรศัพท์VOiP ผ่านเครือข่ายระบบอินเตอร์เน็ตเพื่อป้องกันการติดตาม) จากคนไทยที่อยู่ในประเทศไทยหรือคนต่างชาติที่อยู่ในประเทศไทยแล้วแต่กรณี ซึ่งมันคือผู้ร่วมขบวนการหลอกลวงกับคนร้ายที่คุยกับเหยื่อทางอีเมล์ โดยผู้ที่โทรมาจะแจ้งกับเหยื่อว่า เป็นตัวแทนหรือเจ้าหน้าที่ของบริษัทที่จัดส่งสินค้า มีสินค้าส่งถึงท่านแต่การรับของดังกล่าวจะต้องจ่ายค่าธรรมเนียม เป็นเงินจำนวนหลักหลายหมื่นบาท (ส่วนใหญ่ประมาณ 30,000 บาทหรือกว่านั้น) โดยกำหนดให้โอนเงินเข้าบัญชีปลายทางที่คนร้ายกำหนด ซึ่งอาจเป็นบัญชีธนาคารของคนไทย (บัญชีที่คนร้ายนำมาใช้รับเงิน โดยส่วนใหญ่ไม่ใช่เจ้าของบัญชีจริง) หรือโอนเงินไปยังบัญชี คนร้ายที่อยู่ต่างประเทศผ่าน Western Union และแน่นอนในเวลาอันรวดเร็ว คนร้ายจะรีบเอาเงินออกจากบัญชีนั้น ด้วยการไปกดเงินที่ตู้เอทีเอ็ม ในทันทีระหว่างนี้เหยื่ออาจจะเริ่มคิดว่าทำไมต้องจ่ายเงินค่าธรรมเนียมในการส่งของด้วยก็จะติดต่อกลับไปหาคนร้ายที่ติดต่อกันอยู่อย่างต่อเนื่อง ซึ่งก็จะได้รับคำยืนยันว่ามีของที่ส่งมาให้จริง ๆ และมีมูลค่ามากกว่าค่าธรรมเนียมที่ต้องจ่ายหลายเท่านักจะด้วยเหตุผลอะไรก็แล้วแต่ (หลงรัก/อยากได้ ฯลฯ) เหยื่อยังคงหลงเชื่อและไปโอนเงินเข้าบัญชีตามที่คนร้ายกำหนด และรอเพื่อติดต่อกับเจ้าหน้าที่ผู้ส่งของให้มารับของและนี่คือเสียเงินครั้งแรก

เตือนภัย Scams target you protect yourself

ครั้งต่อไป เมื่อเห็นว่าเหยื่อได้จ่ายเงินครั้งแรก กลุ่มคนร้ายจะเริ่มแผนหลอลวงขั้นต่อไป ด้วยการอ้างว่าของที่ส่งมาให้เหยื่อถูกส่งมาที่ศุลกากรแล้ว แต่เจ้าหน้าที่ศุลกากรตรวจพบว่ามีการส่งเงินสดสกุลต่างประเทศมาด้วย ซึ่งการนำเงินเกินจำนวนเข้ามาในราชอาณาจักรโดยไม่แจ้ง เป็นความผิดตามกฎหมาย จะต้องเสียค่าปรับถึงจะนำเงินจำนวนนั้น ออกไปได้ เหยื่อเริ่มสงสัยจึงได้ติดต่อกลับไปยังคนร้ายที่พูดคุยทางเมล์อีกครั้ง ซึ่งก็จะได้รับคำตอบว่าได้ส่งเงินจำนวนดังกล่าวมาด้วยจริง(อีกแล้ว) โดยซ่อนมาไม่คิดว่าเจ้าหน้าที่ศุลกากรจะตรวจพบ แต่ที่ไม่ได้บอกที่แรกเพราะอยากจะเซอร์ไพรส์และแนะนำว่าเสียค่าปรับไปเถอะ เงินจำนวนมากนะไม่อยากให้ต้องส่งกลับมา ถึงตรงนี้ หากเหยื่อไหวตัวทันก็จะเริ่มติดต่อเจ้าหน้าที่ตำรวจ หรือหาข้อมูลทางอินเตอร์เน็ต ว่าน่าจะถูกหลอกหรือไม่ บางรายไหวตัวทันก็เสียเงินจำนวนเดียวในครั้งแรก แต่ถ้ายังงมงายหลงเชื่อ อยากได้เงินหรือสิ่งของ ก็จะสูญเสียเงินเพิ่มในที่สุด (ยอดเงินสูงกว่าครั้งแรกด้วย) รูปแบบการกระทำผิดลักษณะนี้ มีมานานแล้ว

คนร้ายซึ่งเป็นชาวคองโก (ผิวดำ) ในคดีนั้นคนร้ายอ้างตนเป็นหญิงอยู่ในศูนย์อพยพของประเทศกาน่าติดต่อกับผู้เสียหายชายไทยทางอีเมลล์ประมาณ1 เดือน สนิทสนมชอบพอรับเป็นแฟนกัน ฝ่ายหญิงบอกมีเงินสดประมาณ 11.5ล้านเหรียญสหรัฐฯ (ลองคิดเป็นเงินไทย) แต่ในประเทศกาน่า ไม่สามารถใช้เงิน หรือนำออกไปใช้ได้ จึงได้ฝากให้บาทหลวงที่เข้ามาเยี่ยมนำเงินออกไป และจะส่งมาให้ที่ประเทศไทยพร้อมของขวัญมากมาย ซึ่งพฤติกรรมการหลอกลวงคล้ายที่กล่าวข้างต้น รายนี้โดนหลอกเงินสูญไป 150,000 บาท โดยโอนเงินไปต่างประเทศผ่าน Western Unionคดีนี้สามารถจับคนร้ายที่อ้างตนเป็นเจ้าหน้าที่ของบริษัทส่งของ ได้เพียงคนเดียวในประเทศไทย ส่วนผู้ร่วมแก๊งค์คนอื่นอยู่ต่างประเทศ โดยการจับกุมคนร้าย สืบเนื่องจากผู้เสียหายเริ่มสงสัยว่าตนเองน่าจะถูกหลอก เนื่องจากคนร้ายขอให้มา จ่ายเงินเพิ่มอีก จึงได้แจ้งมายัง บก.ปอศ. ผู้เขียนจึงได้สอบถามรายละเอียดของข้อเท็จจริงที่เกิดขึ้น จากนั้นได้วางแผนเพื่อส่งมอบเงินให้คนร้ายอย่างแนบเนียน คนร้ายชะล่าใจหลงกลมาปรากฏตัว มารับเงินจึงถูกจับกุมได้ในที่สุด ส่วนเพื่อนร่วมแก๊งค์ไหวตัวทันหนีออกไปต่างประเทศก่อนซึ่งจากกรณีนี้คนร้ายได้เรียนรู้เช่นกันว่า ไม่ควรไปรับเงินด้วยตนเองทำให้ระยะหลังการติดตามจับกุมยากขึ้นและได้พัฒนารูปแบบการกระทำผิดไปเรื่อย ๆ เช่นกัน ผลคดีนี้ศาลสั่งจำคุกผู้ต้องหา 2 ปี รับสารภาพลดเหลือ 1ปีและศาลสั่งให้คืนเงินเต็มจำนวน แต่จากการสอบถามไปยังผู้เสียหาย ปรากฏว่า จำเลยไม่มีเงินคืนอีกรายเมื่อเร็ว ๆ นี้ **คนร้ายอ้างตนเป็นทหารอยู่ในกองทัพสหรัฐ** ปลอมรูปถ่าย เอกสารราชการต่าง ๆ ของกองทัพทั้งหมด แม้แต่เอกสารที่รับรองสถานภาพทางการเงิน รายได้ ทรพย์สินต่างๆ ที่มีสิทธิ์ได้รับจากกองทัพสหรัฐ โดยออกมาจากผู้บังคับบัญชา ทั้งยังให้เว็บไซต์หน่วยงานทหารอีเมลล์ของ ผู้บังคับบัญชาที่สามารถติดต่อเพื่อยืนยันได้ด้วย เหยื่อเป็นหญิงไทย ที่ประสงค์จะมีสามี เป็นชาวต่างชาติ ได้ส่งของมาให้รูปแบบการหลอกลวงแบบเดียวกันกับข้างต้น อนึ่ง นอกจากนี้ผู้เขียน ได้แนบข้อมูลการหลอกลวงเท่าที่สามารถเผยแพร่ได้ จากการที่ได้รับแจ้งผ่านเว็บไซต์มาเพื่อให้ได้ทราบแผนประทุษกรรมของคนร้ายด้วยส่วนหนึ่งแล้ว

เตือนภัย แก็งค์ Call center

แก็งค์ Call center คนร้ายจะอ้างเป็นเจ้าหน้าที่ของหน่วยงานรัฐ เช่น ตำรวจ ,DSI , ปปง. หรือเจ้าหน้าที่จากธนาคารแห่งประเทศไทยธนาคารพานิชย์ต่าง ๆซึ่งทำเป็นขบวนการโดยแบ่งหน้าที่กันทำแต่ละคนจะรับบทบาทตามที่ได้หัวหน้าแก๊งค์มอบหมายติดต่อกับเหยื่อทางโทรศัพท์ระบบ VOiP ที่สามารถจะกำหนดให้โชว์หมายเลขโทรศัพท์ของหน่วยงาน นั้น ๆ ได้ การสร้างเรื่องของพวก Call Center จะเริ่มด้วยการที่กล่าวหาว่า เหยื่อเป็นหนี้การใช้บัตรเครดิตหรือเกี่ยวข้องกับยาเสพติดหรือการฟอกเงิน แม้เหยื่อจะบอกว่าไม่เคยเป็นหนี้ ไม่เคยทำบัตรเครดิตกับธนาคารตามที่คนร้ายกล่าวอ้าง หรือแม้จะบอกว่าไม่เคยทำบตรเลยก็ตาม คนร้ายก็จะแจ้งว่าอาจมีคนอื่นเอาชื่อท่านไปเปิดบัญชีธนาคาร ซึ่งจะต้องถูกอายัดเงินในบัญชีของท่าน หรือถูกดำเนินการทางกฎหมาย ดังนั้นเพื่อป้องกันไม่ให้บัญชีของเหยื่อได้รับผลกระทบ คนร้ายพวกนี้มีจิตวิทยาการพูดคุยสูงมาก สามารถกดดันให้เหยื่อต้องรีบดำเนินการ โดยจะหลอกให้เหยื่อไปทำธุรกรรมทางการเงินหน้าตู้เอทีเอ็มจากนั้นกดทำรายการตามที่คนร้ายบอก ซึ่งนั่นเป็นการทำรายการโอนเงินเข้าบัญชีปลายทางที่คนร้ายเตรียมไว้แล้ว หลังจากนั้นคนร้ายจะนำเงินออกจากบัญชีปลายทางในทันทีเช่นกันกรณีแก็งค์ Call Center เหยื่อส่วนใหญ่จะเป็นบุคคลทั่วไป ที่ไม่จำเป็นต้องมีความรู้ด้านภาษาอังกฤษเลยก็ได้ จะเห็นได้ว่ารูปแบบแตกต่างจาก แก๊งค์ Scam Mail ที่ต้องมีการสร้างเรื่องติดต่ออย่างใจเย็น ใช้ภาษาอังกฤษในการสื่อสารแต่ที่เหมือนกันคือ เหยื่อไม่ได้ใช้วิจารณญานในการวิเคราะห์เรื่องราว ความเป็นไปได้ว่าเป็นเรื่องจริงหรือไม่

1. **พึงระลึกไว้เสมอ ในโลก Cyber ทุกอย่างหลอกลวงไว้ก่อน เว้นแต่จะรู้จักหรือมีพื้นฐานกันมาก่อนอย่าได้หลงเชื่อ เด็ดขาด ก็ขนาดคนรู้จักเคยเห็นหน้าเห็นตากันมาก่อนยังไว้ใจไม่ค่อยได้ นับประสาอะไรกับคนแปลกหน้า คนที่ไม่เคยรู้จักไม่เคยเห็นหน้ามาก่อนกันจะไว้ใจหรือเชื่อใจได้อย่างไร**
2. **คนที่ท่านกำลังคุยเห็นหน้าตาผ่านเว็บแคมนั้น เป็นตัวจริงหรือไม่ ลองทดสอบง่าย ๆ ระหว่างกำลังสนทนาลองให้ คู่สนทนายกมือหรือลุกขึ้นยืนเพื่อให้แน่ใจว่าท่าน ไม่ได้คุยอยู่กับคลิปวีดีโอที่ถูกบันทึกไว้ก่อน**
3. **ก่อนจะจ่ายเงินที่ใด ตรวจสอบหน่วยงานภาครัฐให้แน่ใจด้วยตนเอง โดยไม่ผ่านลิงค์ที่ถูกส่งจากคนร้ายเข้ามายังอีเมลล์ของเราดังนั้น การเข้าเว็บไซต์ที่เกี่ยวกับ การเงิน การติดต่อหน่วยงานภาครัฐต่าง ๆ ควรพิมพ์จากURL หรือหน้าเว็บไซต์โดยตรง**
4. **ศึกษารูปแบบของ Phising Mail , Scam Mailต่าง ๆ กรณีศึกษาที่มีผู้นำมาเผยแพร่ เพื่อป้องกันการตกเป็นเหยื่อ ทางสื่อต่างๆ โดยเฉพาะสื่อทางอินเตอร์เน็ต**
5. **หากสงสัยว่าท่านกำลังถูกหลอกอยู่หรือไม่ หรือ ตกเป็นเหยื่อได้รับความเสียหายสูญเงิน ไปแล้วจะต้องทำอย่างไร ติดต่อไปยังกองบังคับการปราบปราม**

เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

Scammer (เบื้องหลังเป็นกลุ่มคนคนสัญชาติ ไนจีเรีย กานา คองโก ส่วนใหญ่อาศัยอยู่ในประเทศไทยและประเทศมาเลเซีย)ได้ใช้ช่องทาง Facebook Skype และ e-mail ในการหลอกลวงหญิงไทย เพจใน Facebook ของพวก scammer จะเป็นเพจที่แทบจะไม่มีข้อมูลอะไรและรูปที่ปรากฏมักจะเอารูปบุคคลที่มีชื่อเสียง เป็นดารา นักธุรกิจ หน้าตาดี ผิวขาว มาโพสต์ในFacebook แล้วจะadd เข้ามาเป็นเพื่อนพร้อมทั้งเข้ามาพูดคุยสร้างความสนิทสนมและอ้างว่าเป็นวิศวกรท างานอยู่ที่ ประเทศอังกฤษ ค าถามที่พวก scammer มักจะถามเหยื่อก่อน นั่นคือ มีอายุเท่าไหร่ มีอาชีพอะไร และ เหยื่อที่ตกเป็นเป้าหมายคือ หญิงไทย วัยกลางคนมีอาชีพการงานดี ส่วนใหญ่จะมีสถานภาพโสด หย่าร้าง สมรส ตามลาดับ <u>เหยื่อเหล่านี้มักจะหลงเชื่อและโอนเงินให้ แต่ละรายสูญเงินตั้งแต่หลักแสน-หลักล้านบาท</u>

เว็บไซต์ที่มักจะพบพวก scammer ได้แก่ www.facebook.com ,www.tagged.com, www.WAYN.com www.Thailovelink.com,www.Thaikiss.com,www.Baboo.com

รูปแบบพฤติการณ์ของชาวผิวสีที่ใช้หลอกลวงทางอินเทอร์เน็ต

1.การหลอกลวงทางอีเมล์ (E-mail)ได้มีการส่งอีเมล์ให้แก่เหยื่อ

1.1 หลอกลวงโดยจะส่งของมาให้ พวก scammer อ้างตัวเป็นชายชาวต่างชาติผิวขาว มาขอเพิ่มเป็นเพื่อนใน Facebook ของเหยื่อ และ คุยกันในกล่องข้อความเป็นระยะเวลาตั้งแต่ 1-2 ปีแล้วแต่ละกรณี เบอร์โทรที่ใช้มักเป็นเบอร์โทรต่างประเทศ เช่น +14046471339 โดย scammer ได้อ้างตัวเป็นคนสัญชาติอเมริกา มีอาชีพเป็นวิศวกร ท างานที่บริษัท น้ ามันซึ่งอยู่กลางทะเล จนเริ่มคุยและสนิทกันมากขึ้น scammer จะคุยในลักษณะของชายจีบหญิง แล้ว อ้างว่าคุยกับเหยื่อแล้วรู้สึกดีและอยากจะมาอยู่ประเทศไทยกับเหยื่อ แต่ก่อนมาประเทศไทย จะส่งของมาให้ และช่วยหาบ้านให้scammer สัก 1 หลัง โดยจะส่งเงินมาให้ ประมาณ $750,000 ซึ่ง scammer จะส่งของพร้อมเงินมาให้ในกล่องพัสดุ ซึ่งประกอบด้วย เงินจ านวน $750,000 ,สร้อยทอง ,นาฬิกา, น้ าหอม มาให้เหยื่อ

จากนั้น จะขอที่อยู่ของเหยื่อ พร้อมอีเมล์ของเหยื่อ เพื่อแจ้งการส่งพัสดุ

เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

จากนั้นประมาณ 3 วัน จะมีผู้หญิงไทยคนหนึ่งชื่อว่า xxxx โทรมาหาเหยื่อ อ้างว่าขณะนี้ของได้มาถึง ที่บริษัทขนส่งแล้ว ให้เหยื่อจ่ายค่าธรรมเนียมรับสินค้า $1,500 หรือคิดเป็นเงินไทย ประมาณ 45,000 บาท โดยในอีเมล์ของเหยื่อก็จะมีเอกสารยืนยันว่าได้มีการส่งของมาจากบริษัทดังกล่าวจริง


UNITED DELIVERY AND SECURITY SERVICE

Reaching out to the world- Anywhere, Anytime

INTERNATIONAL DIPLOMATIC WORLD WIDE SHIPMENTS ONLY

AIR WAY BILL

AIR WAY BILL

Quote This Shipment Number At Enquiry

1 FROM (SENDER)

Sender's name:

Address:

Postcodes:

Tel:

2 TO (RECEIVER)

Receiver's name:

XXXX XXXX

Address:

XXXXXXXXXXXXXX..

Delivery destination: Thailand

Postcodes: Bangkhae District Bangkok 10160

Tel: + 66 81 773 2788

3 SENDER'S AUTHORISATION AND SIGNATURE

I/we agree that AEAC standard terms apply to this shipment and limit AEAC liability. The warsaw convention may also apply (see reverse)
I/we understnad that AEAC transport diplomatic goods (see reverse)

4 SHIPMENT DETAILS

All payment and services are available in selected countries

Services

- DIPLOMATIC DOCUMENT
- WORLD WIDE DIPLOMATIC PACKAGE
- DOMESTIC PACKAGE
- WORLD MAIL
- OTHER SERVICE

Specify

Transport Charges
If left blank sender
Days transport charges

- Receiver
- Cash/Cheque/Credit Card
- For approved customers only
- External Billing Agreement

SHIPMENT INSURANCE

- YES
- NO

Full Description Of Cargo
One Trunk Box Containning Bank Values

ORIGINAL

5 SECURITY CHECKED

YES NO

Sender's VAT/GST No.

HARMONISED COMMODITY CODE IF APPLIES

Receiver's VAT.GST No. Or ENSSN

Type of export PERMANENT REPAIR/RETURN TEMPORARY

Destination duties/taxes, if left blank receiver pay duties/tax

Reciever Sender Other

Specify destination approved account number

ORIGIN: MARSHALL ISLAND

DESTINATION: THAILAND

4 SIZE AND WEIGHT

NO. OF PIECES: 1 TRUCK BOX

WEIGHT: 10.020KG

X-PAY SCAN RESULT.....NON-HARMFULL CONTENT (NEGATIVE)

VOLUME TRIC/CHARGED WWEGHT

CODES | CLEARING CHARGES SERVICE

Shipment	GBP: 835.00
Handling Charge	GBP: 820.00
Total Charges:	GBP:545.00
Currency Code:	BRITISH GBP POUNDS
Sender Paid :	GBP: 2000.00

TRANSPORT COLLECT STICKERS NO

PAYMENT DETAILS
Payment at destination
YES NO

PACKAGED BY

ROUTE NO MA004

Date: 10/08/2012

Time: 8:25am

เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

1.2 หลอกลวงว่าได้รับเงินจำนวนหนึ่ง อีเมลล์ส่งมาจาก patrick.delaney@alrahjibank.org ภายหลังได้มีจดหมายมาถึงโดยให้โอนเงินค่าธรรมเนียม พร้อมแนบเอกสารให้ลงลายมือชื่อตอบกลับไป

TO

Prechaporn meekaew ,

We have prepared your transfer document which is attached to this email, please kindly print it out and check the transfer document before you sign it and scan it back to us.

The Malaysia LAW require that all transfer of US$30,000.00 and above must be signed

and accept by the receiver in order to cub money laundry. Please feel free to contact me directly on +601123716994 ,ext 225.

Regards,

PATRICK DELANEY

(PP) Disclaimer:This message is intended only for the use of the person to whom it is expressly addressed and may contain information that is confidential and legally privileged. If you are not the intended recipient, you are hereby notified that any use, reliance on, reference to, review, disclosure or copying of the message and the information it contains for any purpose is prohibited. If you have received this message in error, please notify the sender by reply e-mail of the redelivery and delete all its contents.

TO

Prechaporn meekaew,

The cost of your transfer is MYR10,000.00 payable through our local agent account details below:

BANK NAME: CIMB BANK, MALAYSIA

ACCOUNT NAME: SARINA BINTI ABDUL MAJID

ACCOUNT NUMBER: 13020156096520

AMOUNT TO PAY: MYR 10,000.00

Once you make your payment, then your money will be transfer into your account immediately.

Regards,

PATRICK DELANEY .

+601123716994 ,ext 225.

เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

1.2 หลอกลวงว่าได้รับเงินจำนวนหนึ่ง อีเมลล์ส่งมาจาก patrick.delaney@alrahjibank.org ภายหลังได้มีจดหมายมาถึงโดยให้โอนเงินค่าธรรมเนียม พร้อมแนบเอกสารให้ลงลายมือชื่อตอบกลับไป

Al Rajhi Bank مصرف الراجحي

www.alrahjibank.org

Member Wire Transfer Form

Date of Request: 10/07/2013
Sending Member's Name (Originator) (Your Name) Micheal Joe
Bank Account# (To Charge) (Your Account Number) 02771832673
Member Address/City/State: *104 A-B, Jalan Sultan Ismail, 20200 Kuala Lumpur, Malaysia*
Government Issued ID Number*** _ ID on File
Phone Number (_____) Not APPLICABLE

Signature is Required for US$30,000.00 and Above (Receiver's Signature)

Receiver's Signature (Your Signature) Date

Wire Transfer Instructions

Wire Amount US$50,000.00 (1,564,230 THB)
Receiving Institution: *Siam Commercial Bank*
Your Bank Name: *Siam Commercial Bank* (Siamcquar Branch Bangkok Thailand).
City/State: *333 Silom Road, Bangkok 10500*
Routing/Transit Code) SICOTHBK
Account Name (Beneficiary): xxxxx xxxx
Account Number: *038-453937-3*

To Be Completed By Your Bank

Are Wired Funds Collected? Yes/No
Fee: ____Domestic/___International

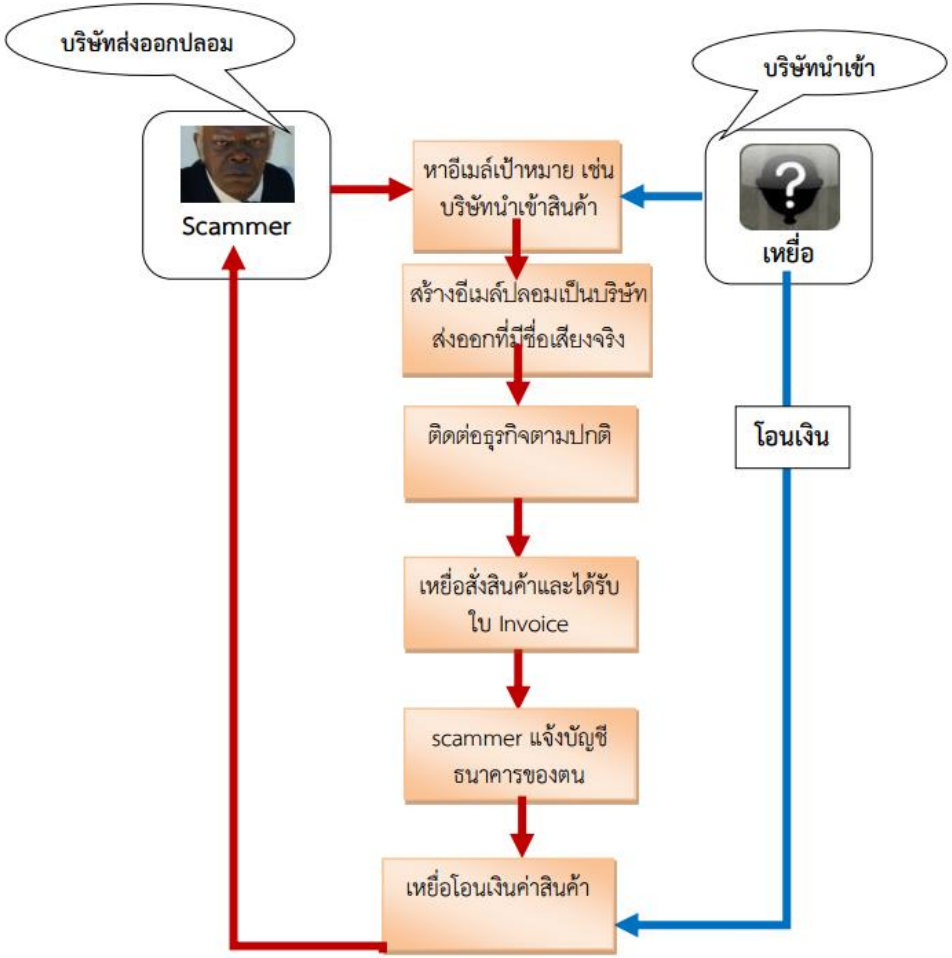
For Bank Use Only:

Wire Initiated by: Saima Rana Majid Date: 10-07-2013 Time: 10.55AM
Wire Verified by: Patrick Delaney Date: 10/7/2013 Time: 10.57AM

COASTAL CREDIT UNION FORM 6438

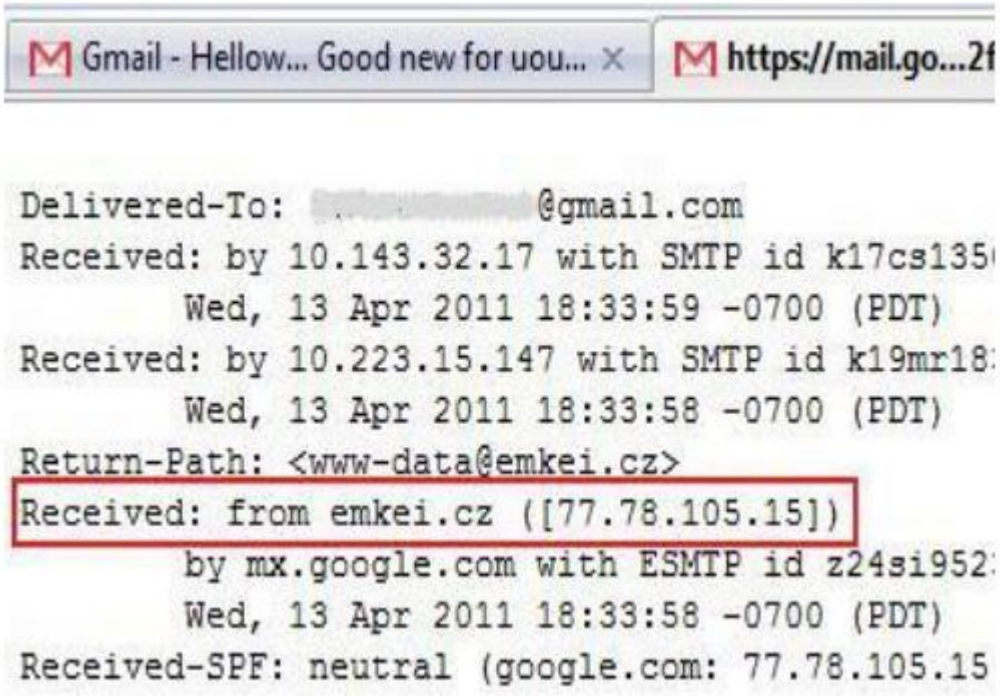
เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

1.3 หลอกลวงโดยการหลอกลวงทางอีเมล์ (Fake E-Mail) ส่วนใหญ่จะเกิดในกรณีที่มีการติดต่อซื้อขาย สินค้าระหว่างประเทศ ทางอีเมล์(E-mail) ระหว่างบุคคล 2 ฝ่ายซึ่งฝ่ายหนึ่งเป็นนิติบุคคล และอีกฝ่ายหนึ่งเป็นนิติบุคคลหรือบุคคลธรรมดา โดยในระหว่างการโต้ตอบทางอีเมล์ เหยื่อจะไม่ทราบว่ามีบุคคลไม่ประสงค์ดีเข้ามาแอบแฝงปลอมตัวเป็นฝ่ายใด ฝ่ายหนึ่ง และทาการโต้ตอบแทนเหยื่อ เมื่อถึงขั้นตอนที่จะต้องโอนเงินค่าสินค้า หรือเงินอื่น จึงเปลี่ยนแปลงบัญชีที่ใช้ในการโอนเงินเดิมมาเป็นบัญชีใหม่ โดยที่เหยื่อไม่ทันระวัง ดังตัวอย่างพฤติการณ์ต่อไปนี้



เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

เมื่อสังเกต Mail Header ของเหยื่อที่ถูกปลอมแปลงอีเมล์จะมีลักษณะดังนี้

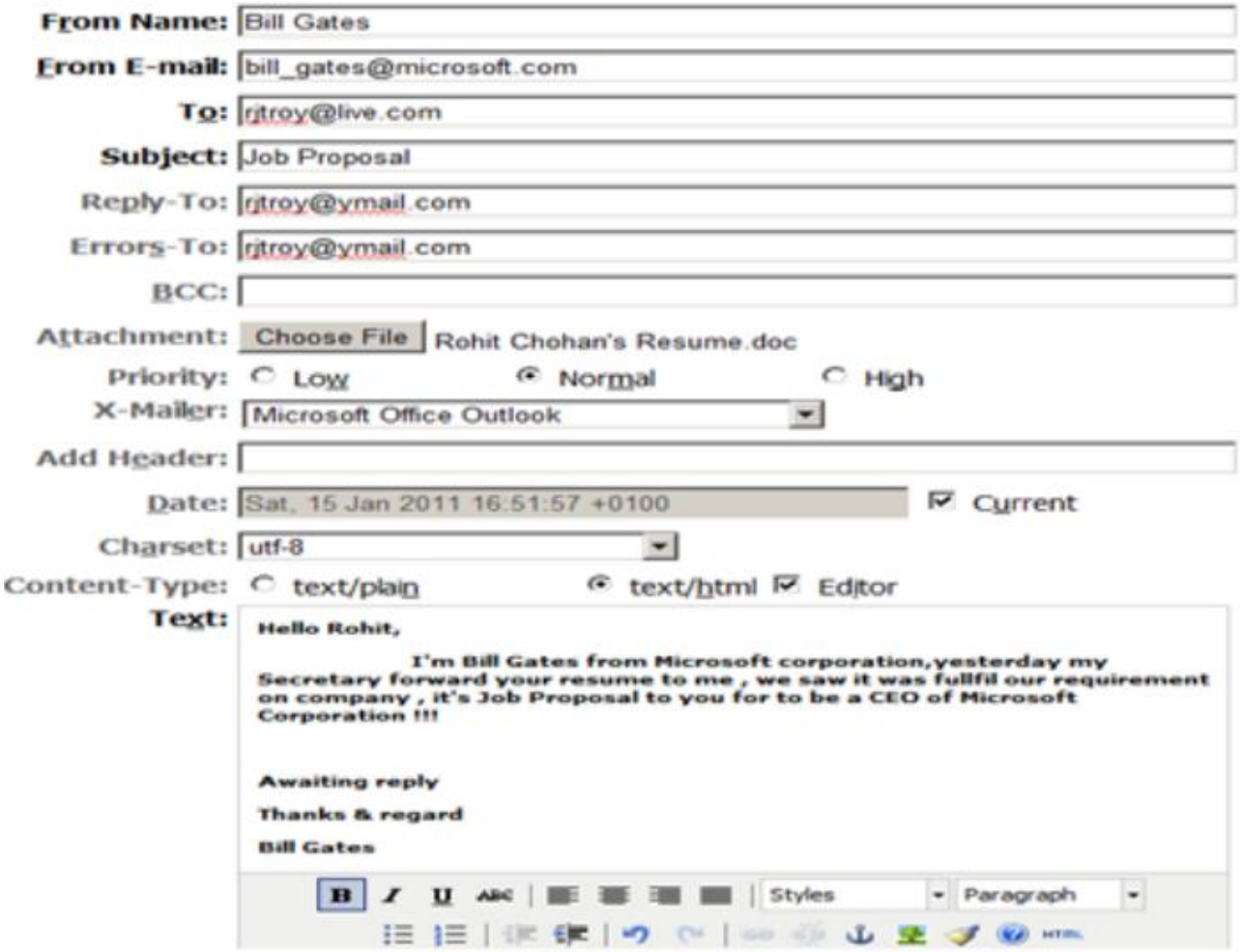


เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

การปลอมแปลงนี้มาจากเว็บไซต์หนึ่งชื่อว่า https://emkei.cz/ โดยมีหน้าเว็บไซต์ดังนี้

เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

การปลอมแปลงนี้มาจากเว็บไซต์หนึ่งชื่อว่า https://emkei.cz/ โดยมีหน้าเว็บไซต์ดังนี้



เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

1.4 หลอกลวงเรื่องการจัดหางาน เหยื่อได้ไปลงทะเบียนไปทำงานต่างประเทศ ที่ศูนย์ทะเบียนคนหางาน กรมการจัดหางาน ในการลงทะเบียนนั้นเหยื่อได้ให้รายละเอียด ชื่อ สกุล ที่อยู่ และหมายเลขโทรศัพท์ พร้อมทั้งแจ้งความประสงค์ ว่าต้องการจะไปทำงานที่ต่างประเทศ เช่น เยอรมัน เกาหลีใต้ อังกฤษ เป็นต้น ในต าแหน่งที่ต่างกันออกไป ซึ่งเมื่อลงทะเบียนแล้วเหยื่อจะได้รับบัตรประจำตัวผู้ต้องการไปท างานต่างประเทศ (ศท.1) ซึ่งเป็นขั้นตอนของทางราชการ

เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

1.4 หลอกลวงเรื่องการจัดหางาน เหยื่อได้ไปลงทะเบียนไปทำงานต่างประเทศ ที่ศูนย์ทะเบียนคนหางาน กรมการจัดหางาน ในการลงทะเบียนนั้นเหยื่อได้ให้รายละเอียด ชื่อ สกุล ที่อยู่ และหมายเลขโทรศัพท์ พร้อมทั้งแจ้งความประสงค์ ว่าต้องการจะไปทำงานที่ต่างประเทศ เช่น เยอรมัน เกาหลีใต้ อังกฤษ เป็นต้น ในต าแหน่งที่ต่างกันออกไป ซึ่งเมื่อลงทะเบียนแล้วเหยื่อจะได้รับบัตรประจำตัวผู้ต้องการไปท างานต่างประเทศ (ศท.1) ซึ่งเป็นขั้นตอนของทางราชการ

W HOTELS WORLDWIDE

W London – Leicester Square
10 Wardour Street, Leicester Square, London, W1D 6QF

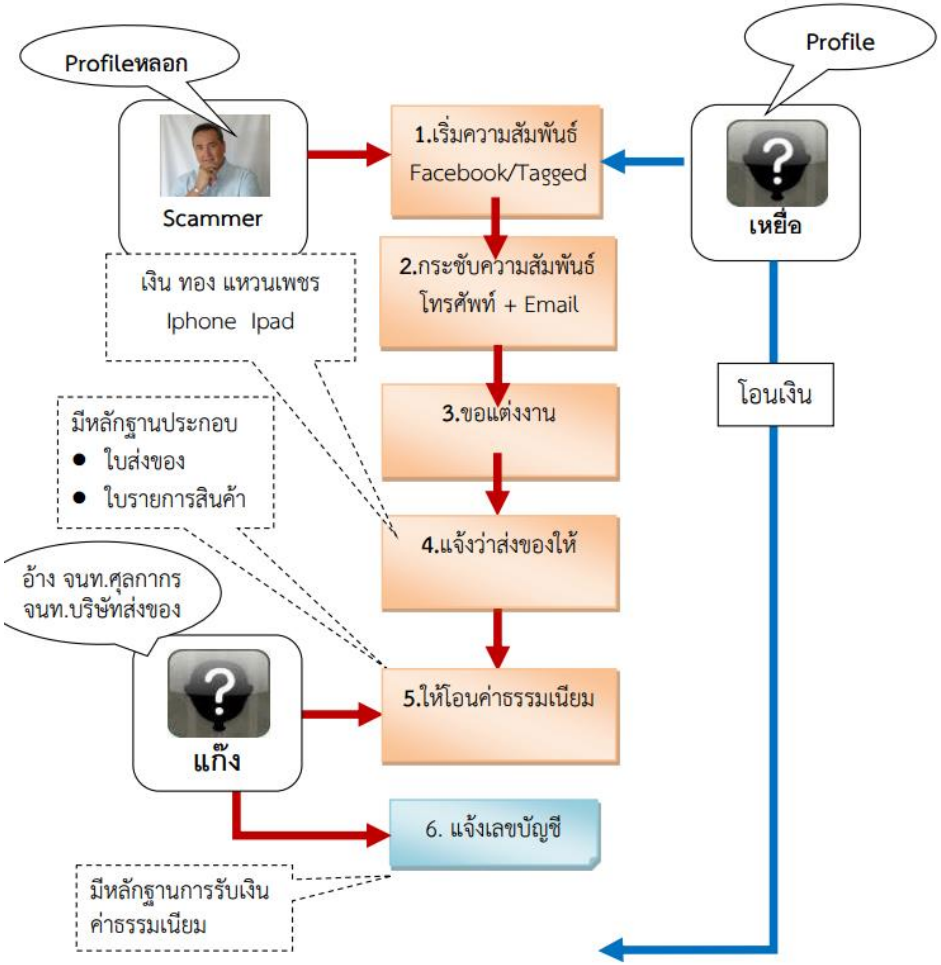
Dear
We thank you for email you sent to us .this is Rules and regulations guiding the operations of the
W London – Leicester Square L LONDON ENGLAND
(1)The contract agreement will last only two years
(2) our diplomat travel agency in Thailand will help you to process your visa and work permit when all documentation submit
(3)the Hotel Management offer every selected candidate Air Ticket. Free accommodation, and feeding only.
(4) HOUSEKEEPING DEPARTMENT

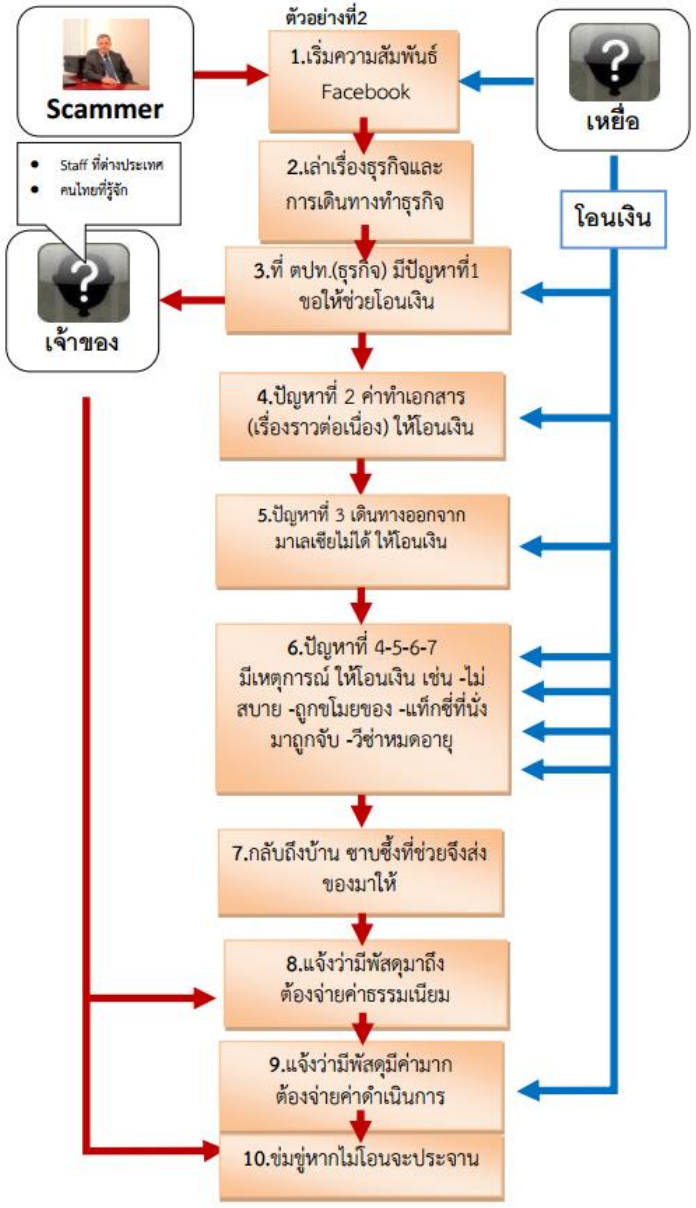
BEAUTY SALON DEPARTMENT

Room service attendant.....(2,650.00 GBP)
Utility cleaner.....(2,650.00 GBP)
Laundry staff.....(2,750.00 GBP)
Floor supervisors.....(2,650.00 GBP)
Pool attendant .....(2,650.00 GBP)
Beautician.....(2,700.00 GBP)
Hair stylists.....(2,700.00 GBP)
Hairdresser.....(2,700.00 GBP)
Massage therapist.....(2,550.00 GBP)
Cosmetologist.....(2,700.00 GBP)
Nail technicians.....(2,650.00 GBP)
Alterative instructors.....(2,650.00 GBP)

เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

การหลอกลวงทาง Social Media เช่น Facebook / Line/Instragram





ACIS PROFESSIONAL CENTER COMPANY LIMITED
62 THE MILLENNIA BUILDING, ROOM 2101, 21ST FLOOR, LUNGSUAN RD., LUMPINI, PATHUMWAN, BANGKOK
TEL +66 0 2650 5771 FAX +66 0 2650 5776
http://www.acisonline.net

เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

2.1หลอกลวงด้วยการขอแต่งงาน เริ่มจากการแสดงความคุ้นเคยโดยการพูดคุยผ่านทางFacebookโทรศัพท์มาหาบ่อยๆ ส่งอีเมล์ (บางกรณี)ด้วยข้อความที่รักใคร่ชอบพอกับเหยื่อ โดยใช้เวลาสร้างความสนิทสนมประมาณ 1-2 เดือน ก็ออกปากว่า จะขอแต่งงาน มีการส่งของมาให้ เช่น เงิน ทอง แหวนเพชร Ipad Iphone แต่จะมีบุคคลซึ่งมักจะเป็นหญิงไทยที่ร่วมกระบวนการอ้างตัวว่าเป็นเจ้าหน้าที่ของศุลกากร แจ้งมาว่ามีพัสดุมาถึง แต่ตรวจสอบพบว่าข้างในมีเงิน จึงต้องเสียค่าธรรมเนียมและค่าภาษี จึงให้เหยื่อโอนเงินไปให้ โดยผ่านบัญชี ของ น.ส. A (นามสมมติ) ธนาคาร B ตัวอย่างรูปภาพที่ได้ส่งมาหาเหยื่อทางอีเมล์

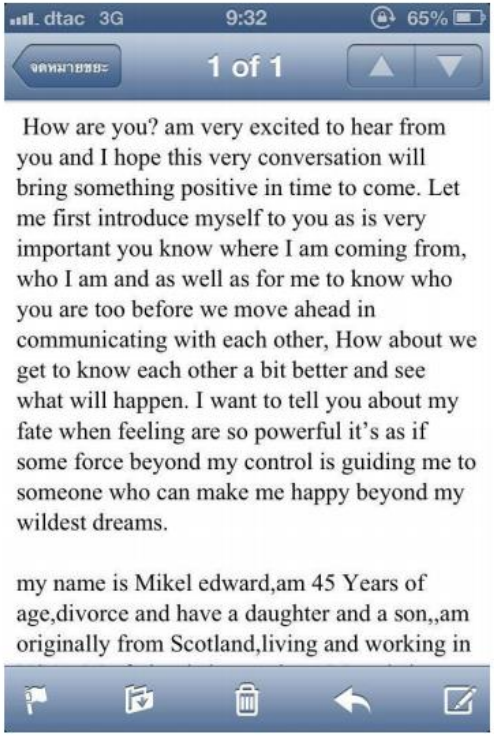
เอกสารที่ใช้อ้างถึงการขนส่ง ตัวอย่าง1

เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

2.2 หลอกลวงด้วยการอาศัยความไว้เนื้อเชื่อใจและความสงสารของเหยื่อ scammerแจ้งกับเหยื่อว่าต้องจ่ายเงินให้บริษัทประกันชื่อ MSIG เป็นเงิน70,000ปอนด์ หรือ 3,416,000บาท เพื่อจะเอาเช็คจากบริษัทประกัน และยังแจ้งว่าขาดเงินอยู่อีก 2000 ปอนด์หรือประมาณ 95,000 บาทจึงขอร้องให้เหยื่อช่วย เนื่องจากเตรียมเงินสดมาไม่พอและก็ได้ถอนเงินสดออกมาจากบัตร มาสเตอร์การ์ดจนหมดแล้ว

เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

2.3 หลอกลวงด้วยการอ้างถึงการเจ็บป่วย เกิดเหตุการณ์ที่ไม่คาดคิดเกิดขึ้นอ้าง บุตรสาวเกิดอาการปวดท้องเนื่องจากกินอาหารและเจอสภาพอากาศที่ไม่ดี ซึ่งเหยื่อคิดว่าเป็นเรื่องจริง พร้อมให้เบอร์โทรแก่เหยื่อไว้ให้ติดต่อ ซึ่งเบอร์โทรนั้นคือ +2348137360089 3วันต่อมาscammerได้ e-mail แจ้งแก่เหยื่อว่าบุตรสาวได้พักรักษาตัวอยู่ที่โรงพยาบาลเนื่องจากอาการปวดท้องจากสาเหตุเดิม ขณะนี้อาการดีขึ้นแล้ว หมอก็อนุญาตให้ออกจากโรงพยาบาลได้ แต่ scammerติดปัญหาเรื่องค่ารักษาพยาบาลของบุตรสาว ซึ่งค่ารักษาทั้งหมด$1,865 ซึ่งscammerได้จ่ายไปแล้ว$1,000 และยังคงเหลืออีก $865 หากไม่ช าระทั้งหมดหมอจะไม่ให้บุตรสาวออกจากโรงพยาบาล ถึงแม้ว่ามีบัตรเครดิตแต่ไม่สามารถใช้งานได้ใน Africa เนื่องจากระบบ Banking ไม่รองรับบัตรใดๆ scammerจึงขอความช่วยเหลือจากเหยื่อ ขอร้องให้เหยื่อโอนเงินส่วนที่เหลือจ านวน $865 เพื่อช่วยจ่ายค่ารักษาพยาบาลของบุตรสาว



เตือนภัย พฤติการณ์ที่ชาวผิวสีมักใช้หลอกลวงผ่านทางอินเทอร์เน็ต

2.4 หลอกลวงว่ามีธุรกิจส่วนตัว เหยื่อรู้จัก Scammer ใน Facebook และติดต่อกับเหยื่อสักระยะ และ ก็ได้เปลี่ยนมาคุยกันใน Skype ซึ่งScammerแนะน าตนเองว่าท าธุรกิจส่วนตัว เป็นคนอิตาลี แต่มาอยู่ใน UKเปิดร้าน ขายรถมือสอง และมือหนึ่ง คุยกันได้สักระยะ Scammer บอกว่าต้องการมาประเทศมาเลเซีย เพื่อมาดูรถ และซื้อรถยี่ห้อ โปตอน ให้กับลูกค้า หลังจากนั้นจะเดินทางมาประเทศไทย เมื่อScammer ได้ด าเนินการซื้อรถ

2.4.1อ้างมีปัญหาเรื่องเอกสารในการขนส่งรถลงเรือเพื่อส่งไปให้ลูกค้าที่ UK จึงให้เหยื่อช่วยเหลือด้วยการโอนเงินก้อนแรกจ านวน30,000 บาท ไปยังบัญชีผู้หญิงไทย หญิงคนนี้อ้างว่าเป็น สต๊าฟ ในร้านขายรถภายหลังจากที่scammer ได้เงินจากเหยื่อ

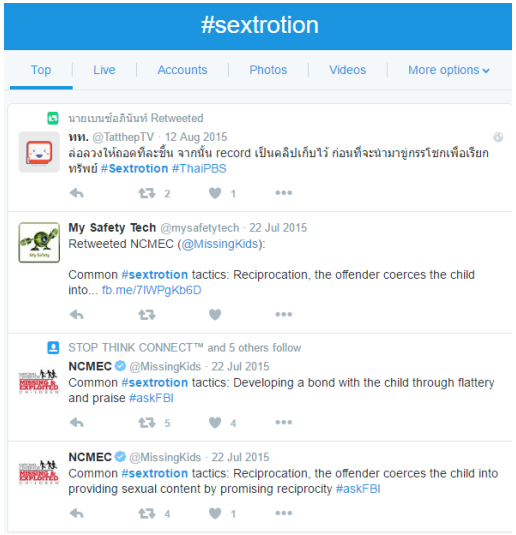
2.4.2อ้างมีปัญหาเกิดขึ้นมาอีกว่า เงินไม่พอในการทำเอกสารให้เหยื่อโอนเงินให้อีกจ านวน 25,000 บาท

.....

2.5 ขู่ว่าจะเอาภาพโป๊ขึ้นเว็บ แล้วให้โอนเงินให้ (Sextrotion) ** เล่าประสบการณ์ส่วนตัว*

2.6 หลอกลวงว่าจะร่วมทำธุรกิจ

2.7 หลอกให้โอนเงิน เพื่อนเดือดร้อน ไม่สะดวก **เล่าประสบการณ์ส่วนตัว*



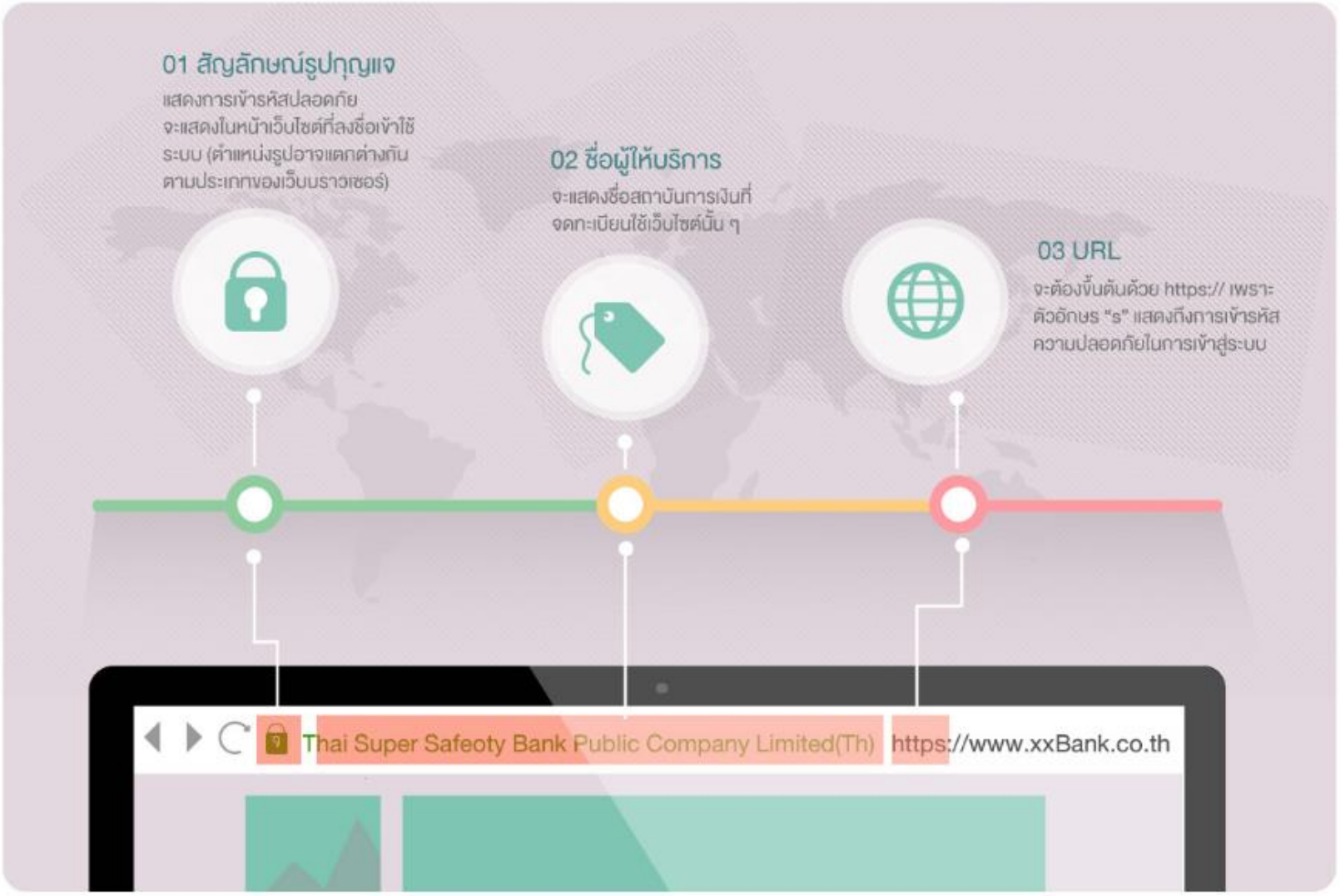
จากพฤติการณ์ทั้งหมดที่ได้กล่าวไปนั้น ได้สร้างความเสียหายให้แก่ธุรกิจเชิงพาณิชย์ต่างๆ เช่น บริษัทที่มีการซื้อขายสินค้าระหว่างประเทศ ความสัมพันธ์ในครอบครัว ซึ่งความเสียหายนี้โดยเฉลี่ยไม่ต่ำ กว่าคนละ 5 แสนบาท และในแต่ละวันมีผู้ที่ถูกหลอกลวง ไม่ต่ ากว่า 100 ราย มูลค่าความเสียหายในแต่ละปี ไม่ต่ ากว่า 2,000 ล้านบาท

เตือนภัย IG ปลอม ลิงค์ไป Web ปลอม เตือนระดมทุนรูปแบบใหม่ ตอบแทนสูง ล่อเหยื่อ

อีก 1 ตัวอย่าง ของ IG ปลอม และ Web ปลอม โดยอ้างใช้ Logo ของบริษัทชื่อดัง เพื่อสร้างความน่าเชื่อถือ และชวนเข้าร่วมทำธุรกิจ

จุดสังเกตอีเมล์ปลอม

จุดสังเกตเว็บไซต์ปลอม



ระวังการทำ Transaction เกี่ยวกับเงิน ๆ ทอง ๆ บนอินเทอร์เน็ต กรณีศึกษา Paypal

เตือนภัยสาว ๆ ให้ระวังการทำ Transaction เกี่ยวกับเงิน ๆ ทอง ๆ บนอินเทอร์เน็ต กรณีศึกษา Paypal

ปกติเราเป็นสมาชิกของ Ebay ซึ่งถ้าใครเคยซื้อ/ขายสินค้าบน Ebay จะต้องรู้จัก Paypal เป็นอย่างดี

ล่าสุดเมื่อไม่กี่วันมานี่ เราได้รับ email จาก paypal ให้เข้าไปอัพเดตข้อมูลล่าสุด ซึ่งจริง ๆ แล้วไอ้ mail ที่ว่านั่น มันเป็น Fraud email

เราดัน Click link ตามมันเข้าไป และ login เข้าไปใน account Paypal ของเรา ก็ดูเหมือนไม่มีอะไร แล้วเราก็ logout ออกจากระบบ Paypal ตามปกติ

วันนี้ได้คุยกับเพื่อนไปเรื่อยเปื่อย เผอิญว่า เพื่อนเราคนนี้เป็นเจ้าพ่อ Ebay ซื้อของบน Ebay อยู่เป็นประจำ และตอนที่คุยกันมันกำลังทำ Transaction บน Ebay และ Paypal ก็บอกเพื่อนไปว่า เราเพิ่งเข้าไป update ข้อมูล paypal ตาม mail ที่ paypal แจ้งมา

ทีนี้ เพื่อนเราคนนี้ก็บอกว่า ไม่เห็นได้รับเมลล์นี้เลย แล้วทักว่า มันเป็น mail หลอกหรือเปล่า

อื่มมมม ไอ้เราก็เลยลอง login เข้าไปตรวจสอบ Account Paypal อีกที ปรากฏว่า ไม่มี Transaction อะไรแปลกปลอม

หลังจากนั้นนึกเฉลียวใจก็เลยโทรไปที่ Call Center ของบัตรเครดิตที่ผูกอยู่กับ Account Paypal ปรากฏว่า มี Transaction ที่เราไม่ได้ทำ พูดง่าย ๆ ก็คือ รายการซื้อของที่เราไม่ได้ใช้แน่ ๆ เพิ่มมา 2 รายการ

รายการแรก น่าจะเป็นซื้อของผ่านเวป ส่วนอีกรายการ เป็นการซื้อกาแฟจากสตาร์บัค ซึ่งปกติเราไม่กินกาแฟ

ก็เลยรู้ตัวว่าโดน Fraud แน่ ๆ ก็เลยอายัดบัตรเครดิตไปเลยค่ะ พร้อมทั้งรีบเปลี่ยน password ของ Paypal

ถึงแม้ว่าจะสามารถยกเลิกรายการที่เราไม่ได้ใช้แน่ ๆ กับเจ้าหน้าที่บัตรเครดิต แต่มันก็เสียเวลาคอยตรวจสอบและต้องคอยระวัง ก็เลยอายัดบัตรไปเลยอย่างที่บอกข้างต้นค่ะ

โดยส่วนตัว ปกติก็ทำ Transaction บนอินเตอร์เน็ตบ่อยพอควร แต่ส่วนใหญ่จะใช้ผ่าน Paypal ไม่เคยเจอเหตุการณ์แบบนี้

ได้ข่าวมาก็เยอะว่ามันมีการฉ้อฉลแบบนี้อยู่เป็นประจำ แต่ไม่นึกว่าจะเกิดกับตัวเอง

ก็เลยตั้งกระทู้มาเพื่อเตือนสาว ๆ นะคะ ว่าอย่าไป click link จาก spam mail อะไรสุ่มสี่สุ่มห้านะคะ

เตือนภัย “Internet Banking” ปล้นวันละแสน

"ช่วยด้วย!!! ผมถูกแฮกเงิน 343,000 บาท..." คือสเตตัสบนเฟซบุ๊กของ ร.ศ.ยุทธพร อิสรชัย นักวิชาการทางการเมืองชื่อดัง ที่เขียนเล่าเหตุการณ์น่าใจหายให้คนบนโลกออนไลน์ได้อ่าน เพื่อบอกว่า เขาตกเป็นเหยื่อ "การโจรกรรมทางการเงินบนอินเทอร์เน็ต" เสียแล้ว

คนที่ยังไม่รู้รายละเอียด อาจนึกสงสัยว่าเป็นถึงรองศาสตราจารย์ เหตุใดจึงโดนหลอกได้ แต่ถ้าลองอ่านรายละเอียดดูจะรู้ว่า เป็นการโจรกรรมที่แยบยลที่สุดตั้งแต่เคยมีมา ถึงขนาดผู้เชี่ยวชาญด้านความปลอดภัยระบบสารสนเทศ ยืนยันว่า "เคสนี้เป็นเคสที่แปลกมาก เป็นครั้งแรกที่เกิดขึ้นในประเทศไทยเลยครับ!!"

แปลกแต่จริง... เงินเกลี้ยงบัญชี

"ผมเข้าไปทำธุรกรรมบนหน้าเว็บไซต์ของ **SCB ครั้งสุดท้าย วันที่ 16 ก.พ.** สักประมาณ 5 โมงครึ่ง **เข้าไปเปลี่ยนอีเมล เพื่อให้อีเมลใหม่นี้ส่งข้อมูลติดต่อถึงผมได้** เขาก็ส่งข้อมูลตอบกลับมายืนยันว่าการเปลี่ยนอีเมลสมบูรณ์แล้ว วันที่เข้าไปเปลี่ยนอีเมล ผมยังเห็นยอดเงินอยู่ที่ 3 แสนกว่าบาท และผมก็ไม่ได้ทำธุรกรรมอะไรเลย จนวันที่ 21 ก.พ. สัก 4-5 โมงเย็น มีโทรศัพท์เข้ามา โทร.มาจากศูนย์ข้อมูลของไทยพาณิชย์ **แจ้งว่ามีการทำธุรกรรมที่ผิดปกติเกิดขึ้น ถามว่าผมทำหรือเปล่า ผมก็บอก เอ๊ะ! ผมไม่ได้ทำนะ**

บอกให้เขาช่วยส่งข้อมูลมาให้หน่อยว่า ผมทำธุรกรรมอะไรไป โอนเข้าบัญชีของใคร เขาก็บอกว่าจะรีบตรวจสอบ แล้วก็ส่งอีเมลมาให้ดู บอกว่าผมทำไป 7 รายการ **เป็นการโอนเงินไปที่ธนาคารกรุงเทพฯ มีชื่อและเลขเจ้าของบัญชีด้วย ชื่อ น.ส.สนธยา ชมชื่น ซึ่งผมไม่รู้จัก** ธนาคารก็แนะนำให้ผมไปแจ้งความ ทำหนังสือถึงธนาคารเพื่อปฏิเสธการทำธุรกรรม ขอให้ทางธนาคารชดเชยค่าเสียหาย" **ร.ศ.ยุทธพร อิสรชัย** คณบดีรัฐศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช เล่ารายละเอียดให้ฟังผ่านรายการ คมชัด ลึก เมื่อไม่กี่วันที่ผ่านมา

อาจารย์ยืนยันด้วยน้ำเสียงหนักแน่นว่า **ทุกครั้งที่จะทำธุรกรรมทางการเงินบนอินเทอร์เน็ต เขาจะตั้งสติและระมัดระวังเป็นพิเศษ ไม่ใช้โน้ตบุ๊กสาธารณะ และเลือกใช้เฉพาะโน้ตบุ๊กส่วนตัวเท่านั้น** โดยเครื่องที่ใช้ในครั้งนี้คือ "แม็คบุ๊กโปร" ซึ่งถือว่ามีระบบป้องกันการแฮกต่างๆ ในระดับสูง จึงชวนให้สงสัยว่าเหตุการณ์ทั้งหมดที่เกิดขึ้น เกิดขึ้นได้อย่างไร?

เพราะมันเกิดขึ้นปุบปับจนตั้งรับไม่ทัน **ไม่มีแม้แต่ sms ส่งรหัส OTP มาจากธนาคารเพื่อให้คอนเฟิร์มการโอนเงิน หรือส่งผลการทำธุรกรรมแล้วเสร็จมาบอกอีกที** อย่างที่ควรจะเป็น ไม่มีกระทั่งการแจ้งเตือนทางอีเมล **มารู้ตัวอีกที เงินก็เกลี้ยงบัญชีเสียแล้ว... 343,000 บาท บวกค่าโอนด้วย สูญเงินไป 343,245 พอดี**

โจรกรรมแบบนี้ ครั้งแรกในไทย!!

นอกจากคำมั่นสัญญาว่าจะตามรอยแฮกเกอร์ สืบค้นความจริงให้ถึงที่สุดแล้ว **ความคืบหน้าล่าสุดจากทางธนาคารไทยพาณิชย์ ผู้ให้บริการ Internet Banking** ของเหยื่อคือการส่งจดหมายถึงลูกค้าทุกคน ผ่านทางเว็บไซต์และสื่อแขนงต่างๆ

"**แจ้งเตือน: ขณะนี้มีการโจรกรรมในรูปแบบของการส่ง SMS โดยใช้หมายเลข 02-777-7777 ซึ่งเป็นหมายเลข Call Center** ของธนาคารไทยพาณิชย์เป็นผู้ส่งและมีลิงก์เพื่อให้ดาวน์โหลดหรือติดตั้งโปรแกรมทางการเงิน หมายเลขดังกล่าวถูกปลอมขึ้นเพื่อหวังหลอกลวงประชาชนโดยตรง

ทั้งนี้ ธนาคารฯ ไม่มีนโยบายในการส่งลิงก์เพื่อให้ดาวน์โหลดโปรแกรมใดๆ ผ่านมือถือ ดังนั้น **เพื่อความปลอดภัยควรใช้งาน mobile banking application ที่ดาวน์โหลดจาก Google Play หรือ App Store เท่านั้น**"

การออกมาให้เตือนให้สมาชิกระมัดระวังแบบนี้ ก็ถือเป็นเรื่องดี แต่แค่อาจจะยังไม่ตรงจุดเท่าที่ควร เพราะในกรณีของอาจารย์ยุทธพร **ซึ่งตกเป็นเหยื่อครั้งใหญ่ครั้งนี้ ไม่ได้เกิดจากการติดตั้งโปรแกรมผ่านมือถือ หรือถูกหลอกจากหมายเลข Call Center ของทางธนาคาร** แต่เกิดจากสาเหตุใด ยังคงเป็นปริศนาคาใจที่ **ปริญญา หอมเอนก** ประธานผู้ก่อตั้ง บริษัท ACIS Professional Center และเลขานุการสมาคมความมั่นคงปลอดภัยสารสนเทศ (TICA) ได้แต่ตั้งข้อสังเกตุอย่างประหลาดใจซ้ำแล้วซ้ำเล่า

"เหตุการณ์นี้เกิดขึ้นที่ไทยพาณิชย์ที่เดียว และเป็นครั้งแรกของเมืองไทยด้วย เป็นเคสที่แปลกมาก ผมเพิ่งคุยกับธนาคาร ทางด่ารวจ แล้วก็เหมือ ตอนนี้ก็ยังหาข้อสรุปไม่ได้ว่าเพราะอะไร **ปกติแล้ว คนที่จะโดนแฮกธุรกรรมทางอินเทอร์เน็ตได้ จะต้องมีโทรจัน (Trojan) อยู่บนเครื่องพีซี มีการสร้างหน้าจอเว็บไซต์หลอกลวงให้ลูกค้าเข้าไปใช้บริการ** และค่าเนินการตามขั้นตอน จนสุดท้าย ใส่รหัส OTP. (รหัสที่จะส่งมายืนยันผ่าน sms มือถือ เพื่อยืนยอมให้ตัดเงินจากบัญชี) **แต่กรณีนี้ ไม่มี sms ส่งมา คอนเฟิร์มแม้แต่อันเดียวเลย แต่ดันถูกโจรกรรมเงินจากบัญชีไป 7 ครั้งรวด** ครั้งละ 5 หมื่น ครั้งสุดท้าย เงินมีไม่พอ เลยโดนไปอีก 4 หมื่นกว่าบาท"

และนี่ไม่ใช่เคสเดียวที่โดน ยังมีอีกรายหนึ่งที่ตกเป็นเหยื่อจากธนาคารเดียวกัน ในระยะเวลาไล่เลี่ยกัน เพียงแต่รายนี้ เลือกที่จะไม่ให้ข้อมูลออกสื่อ "แต่พอเอามือถือไปเช็กดู พบว่า**เครื่องของเขาลงโปรแกรมเอนดรอยด์เอาไว้ตัวหนึ่ง ซึ่งเป็นโปรแกรมเอาไว้ดัก sms ของเครื่องและฟอร์เวิร์ดรหัสที่ธนาคารส่งมา ส่งไปให้โจรอีกที** ซึ่งถ้าตรวจสอบแน่ชัดว่าเป็นเพราะแบบนี้ นั่นก็แสดงว่าเหยื่อรายนี้ไม่น่าจะมีสิทธิได้เงินคืนจากธนาคาร เพราะเขาพลาดเอง เขายินยอมดาวน์โหลดโปรแกรมด้วยมือของเขาเอง ก็เท่ากับยอมรับให้แฮกเกอร์มาโจรกรรมเงินของตัวเอง **เหมือนเป็นการยื่นกุญแจเซฟให้โจรนั่นแหละครับ**

จริงๆ แล้ว ในต่างประเทศก็มีปรากฏการณ์นี้เหมือนกันครับ โดนไป 30 ล้านกว่ายูโร โดนเพราะตัวโทรจัน เป็น malware ดัก sms ซึ่งข่อนอยู่ในมือถือประเภทแอนดรอยด์เป็นส่วนใหญ่ 80 เปอร์เซ็นต์ **ตัวโปรแกรมนี้จะดัก sms ของเหยื่อ ทำให้แฮกเกอร์**

เตือนภัย “Internet Banking” ปล้นวันละแสน

ระวัง!! ตกเป็นเหยื่อ

ให้ลองวิเคราะห์กลโกง ขโมยเงินจากแบงก์ออนไลน์ในหลายๆ รูปแบบว่าเกิดขึ้นเพราะอะไรได้บ้าง? ผู้เชี่ยวชาญด้านความปลอดภัยระบบสารสนเทศ จึงเริ่มยกตัวอย่างหนทางที่พอจะเป็นไปได้ให้ฟัง **เริ่มจากช่องโหว่ที่แทบทุกธนาคารมีในตอนนี้ คือ รหัส OTP**

"ถ้าโอนข้ามธนาคาร **มันจะไม่โชว์ชื่อบัญชีของคนที่โอนเข้า จะบอกแค่ว่ามีเงินจำนวนเท่านี้ โอนเข้าบัญชี แต่ไม่โชว์ชื่อ และคนส่วนใหญ่ก็เฉลเล่อ** ไม่ได้ตรวจสอบบัญชีปลายทางให้ดีๆ เขาส่ง password ยืนยันมาทาง sms ให้กรอก โอนเสร็จปุ๊บ ปรากฏว่าบัญชีปลายทางไม่ใช่บัญชีที่เราอยากจะโอนก็มี

หรืออาจเป็นเพราะบางธนาคารออกแบบระบบเอาไว้ให้ช่วยจำ username กับ password ของลูกค้า และถ้าเห็นว่าเป็นบัญชีเดิมที่เคยโอน **เคยมีธุรกรรมทางการเงิน ระบบจะไม่ส่ง sms มาถามซ้ำอีก เพื่อความสะดวกของลูกค้า ซึ่งมันเป็นดาบสองคม** เป็นระบบที่ออกแบบมาอย่างบกพร่องและแฮกเกอร์จะชอบมาก **แต่ก็มีบางธนาคารที่ระบบต่างกันนะครับ ถามแล้วถามอีก เพื่อรักษาความปลอดภัยของผู้ใช้** ซึ่งผมกำลังพยายามเข้าไปคุยกับทางแบงก์ชาติอยู่ครับ ให้ธนาคารออกกฎรักษาความปลอดภัยของลูกค้าให้มากขึ้นอยู่ครับ”

ส่วนคอไอทีที่ใช้สมาร์ทโฟน-โน้ตบุ๊ก-พีซี ทำธุรการออนไลน์เป็นกิจวัตร ก็ต้องมีสติกันให้มากขึ้น “**ประการแรก** ไม่ว่าเราจะได้รับ sms อะไรก็ตาม อย่าเพิ่งคลิก ต้องโทร.เช็กกับทางธนาคารก่อน คิดดูว่าจู่ๆ จะมีใครส่งลิงก์มาให้เราโหลดนั่นโหลดนี่ มันน่าสงสัยอยู่แล้ว และถ้าลองสังเกตดีๆ ตัวแอปฯ (application) เขาส่งมาให้โหลด

พอคลิกเข้าไป หน้าแรกที่เข้า มันคือหน้าของ Google Play หรือ Apple App Store ก็จริง แต่พอคลิกเข้าไปหน้าที่โหลด **มันจะส่งให้เราไปโหลดอีกหน้าลิงก์หนึ่งแทน เป็นเว็บฝากไฟล์ โหลดเกม อะไรแบบนั้น เราก็ต้องสังเกตดีๆ** ว่าถ้าเป็นแบบนั้น ถ้าไม่ใช่แอปฯ ที่โหลดจาก Google Play กับ Apple Store โดยตรง ก็อย่าไปโหลดเลยดีกว่า มันมีความเสี่ยงที่จะถูกแฮกสูง

หรือถึงแม้เป็นแอปฯ ในกูเกิลเองก็ตาม แต่คุณก็ต้องรู้ข้อมูลเชิงลึกก่อนว่า แอปฯ ที่วางไว้ในนั้น เขาเปิดกว้างมากๆ เพราะฉะนั้น **จะมีพวกแอปฯ โจรปลอมแปลงซ่อนตัวอยู่ในนั้นเยอะมาก** เพราะคนตรวจสอบเขาไม่มีเวลาตรวจและตรวจไม่ละเอียดพอ

เพราะฉะนั้น **ประการที่สอง**คือ **อย่าไปโหลดแอปฯ หรือโปรแกรมชี้ชั่ว** ให้โหลดเฉพาะโปรแกรมดังๆ ที่เขาเล่นกัน จะเป็น Whatsapp หรือ Line ก็เล่นไป แต่โปรแกรมหรือเกมชื่อแปลกๆ ที่ชาวบ้านเขาไม่เล่นกัน ก็อย่าไปโหลดมาเล่น มีโอกาสจะโดนแฮกสูงมาก

ประการที่สาม คือพยายามหาเวลาอัปเดตไวรัสและสแกนในมือถือด้วย จะช่วยให้ค้นหาแอปฯ แปลกๆ หรือแอปฯ โจรได้ในระดับหนึ่ง แต่ไม่ได้ทั้งหมด แต่ว่าวิธีการนี้ คนส่วนใหญ่ไม่ค่อยทำ เพราะคิดว่ามือถือเป็นมือถือ ไม่ได้คิดว่ามือถือเป็นคอมพิวเตอร์

ประการที่สี่ เพื่อความเซฟ **ให้ใช้ platform โปรแกรมที่เป็น IOS เอาไว้ก่อน จะปลอดภัยกว่าแบบเอนดรอยด์** พูดไปทางกูเกิลก็อาจจะไม่ค่อยพอใจ แต่มันคือเรื่องจริง คุณทำระบบออกมาห่วยไปหน่อย ตรวจสอบแย่ เน้นเรื่อง make money เป็นหลัก **พอพื้นที่มันเปิดมาก ก็มีแฮกเกอร์มากมายมาทำ malware มาลงในสโตร์คุณเยอะแยะ เพราะคุณไม่มีกระบวนการกลั่นกรองที่ดี**

กลายเป็นความชวยของผู้บริโภค เพราะถ้าธนาคารตรวจสอบพบว่า เหยื่อที่ถูกโจรกรรมทางมือถือเป็นเพราะโหลดแอปฯ พวกนี้มา เขาก็จะไม่รับผิดชอบอะไรเลย ไม่คืนแม้แต่บาทเดียว หมดสิทธิฟ้องร้องเลย เพราะเหมือนเราเอารหัสบัตรเอทีเอ็มไปบอกเพื่อน ให้เขาไปกดเงินเอง ถ้าเป็นแบบนั้น ก็คงช่วยอะไรไม่ได้แล้วล่ะครับ”

กลโกงธนาคารออนไลน์

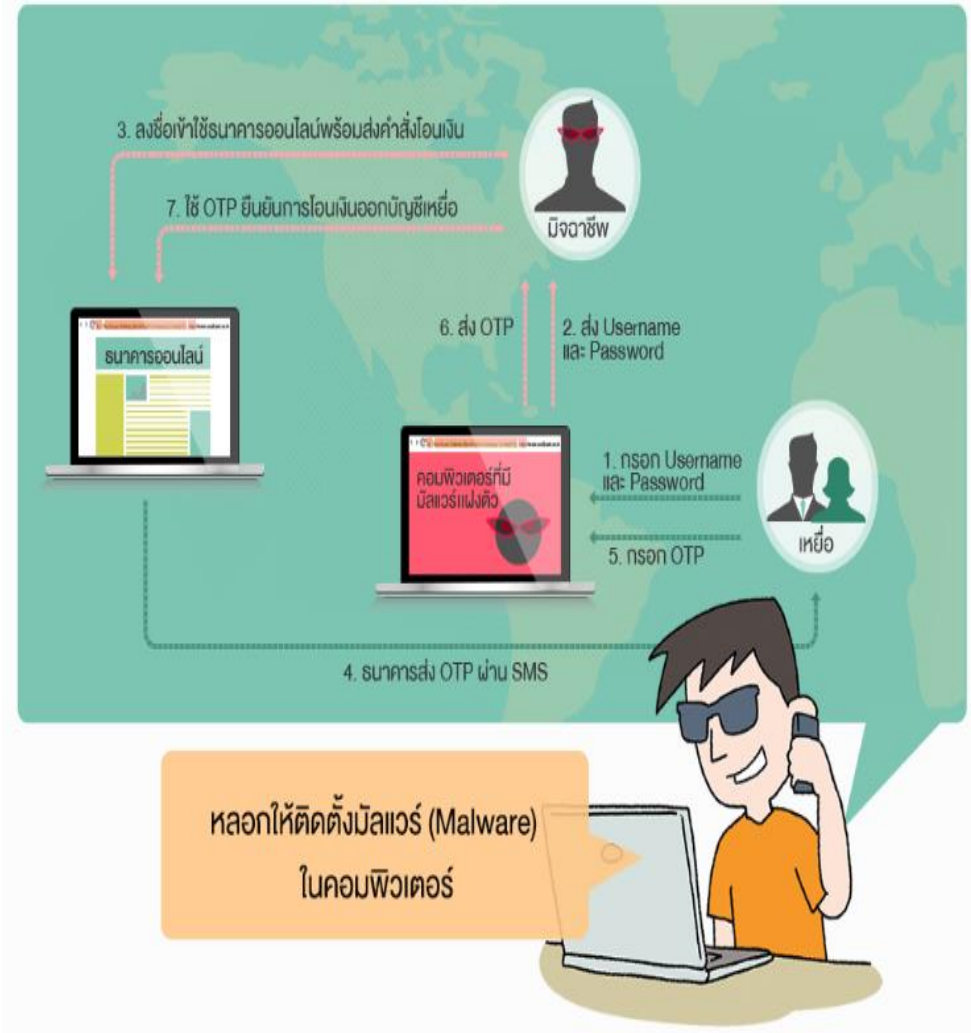
ลักษณะกลโกง

มิจฉาชีพจะหลอกขอรหัสผู้ใช้งาน (username) และรหัสผ่าน (password) จากเหยื่อเพื่อเข้าใช้บัญชีธนาคารออนไลน์ของเหยื่อ แล้วส่งคำสั่งโอนเงินออกจากบัญชีเงินฝาก โดยมีหลายวิธีที่มิจฉาชีพมักใช้ดังนี้

1. หลอกให้ติดตั้งมัลแวร์ในคอมพิวเตอร์

มิจฉาชีพมักแฝงมัลแวร์ (Malware) ไว้ตามลิงก์ดาวน์โหลด หรือเว็บไซต์ต่าง ๆ โดยใช้ข้อความเชิญชวนหลอกล่อให้เหยื่อคลิกเพื่อติดตั้งโปรแกรม เช่น “คุณเป็นผู้โชคดี คลิกที่นี่เพื่อรับรางวัล” เมื่อเหยื่อหลงเชื่อทำตามที่มิจฉาชีพบอก เช่น คลิกไปที่ลิงก์มัลแวร์จะถูกติดตั้งในคอมพิวเตอร์ และทำการบันทึกข้อมูลการใช้งานธนาคารออนไลน์ของเหยื่อ เช่น รหัสผ่านผู้ใช้งาน (username) รหัสผ่าน (password) เพื่อนำไปปลอมแปลงคำขอโอนเงินให้เหมือนเป็นคำสั่งของเจ้าของบัญชี เมื่อธนาคารได้รับคำขอโอนเงินที่จริง ๆ แล้วมาจากมิจฉาชีพ ธนาคารก็จะส่งรหัสผ่านชั่วคราวผ่านระบบ SMS ให้แกเหยื่อ ซึ่งมิจฉาชีพจะสร้างหน้าต่างหรือหน้าจอ pop-up ขึ้นมาบนหน้าจอคอมพิวเตอร์ของเหยื่อเพื่อหลอกถามรหัสผ่านชั่วคราวที่ถูกส่งมายังโทรศัพท์มือถือของเหยื่อ หรืออาจใช้โปรแกรมบันทึกการกดรหัสผ่านแล้วนำมาใช้ยืนยันการโอนเงินออกจากบัญชีของเหยื่อ

มิจฉาชีพจะพยายามหลอกล่อเหยื่อให้ติดตั้งมัลแวร์เพื่อใช้ขโมยข้อมูล แต่เมื่อเหยื่อได้ติดตั้งมัลแวร์แล้ว มิจฉาชีพก็จะยังไม่สามารถโอนเงินของเหยื่อออกจากบัญชีได้ หากเหยื่อไม่กรอกรหัสผ่านชั่วคราวเพื่อใช้ในการยืนยันการทำธุรกรรมของมิจฉาชีพ



กลโกงธนาคารออนไลน์

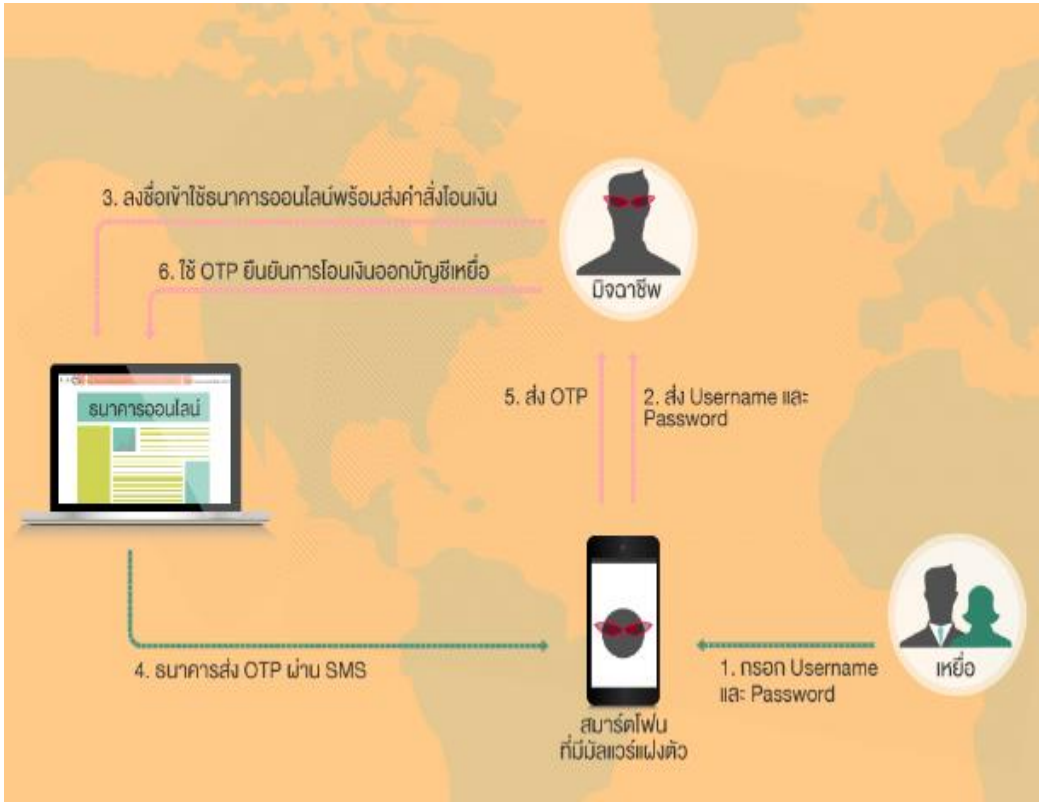
ลักษณะกลโกง

มิจฉาชีพจะหลอกขอรหัสผู้ใช้งาน (username) และรหัสผ่าน (password) จากเหยื่อเพื่อเข้าใช้บัญชีธนาคารออนไลน์ของเหยื่อ แล้วส่งคำสั่งโอนเงินออกจากบัญชีเงินฝาก โดยมีหลายวิธีที่มิจฉาชีพมักใช้ดังนี้

2. หลอกติดตั้งมัลแวร์ในสมาร์ตโฟน

ความแตกต่างจะอยู่ที่มิจฉาชีพไม่จำเป็นต้องหลอกขอรหัสผ่านชั่วคราวจากเหยื่ออีก มิจฉาชีพจะส่งลิงก์ผ่าน SMS หรืออีเมลให้เหยื่อคลิก เพื่อติดตั้งและเปิดใช้งานมัลแวร์ในสมาร์ตโฟนหรือแท็บเล็ต แล้วหลอกให้เหยื่อกรอกรหัสผ่านผู้ใช้งาน (username) และรหัสผ่าน (password) ในหน้าจอที่คล้ายกับแอปพลิเคชันของธนาคารออนไลน์จริง เมื่อเหยื่อเลือกทำรายการต่อ มัลแวร์จะทำให้เครื่องสมาร์ตโฟนของเหยื่อค้างและใช้งานไม่ได้ ทำให้เหยื่อไม่ได้รับ SMS แจ้งรหัสผ่านชั่วคราว จากธนาคารออนไลน์จริง แต่รหัสผ่านชั่วคราวนั้นจะถูกส่งให้แก่มิจฉาชีพแทน

การหลอกลวงวิธีนี้ เมื่อเหยื่อหลงกลติดตั้งมัลแวร์ มิจฉาชีพไม่จำเป็นต้องหลอกขอรหัสผ่านชั่วคราวจากเหยื่ออีก เพราะมัลแวร์จะทำหน้าที่ดัก SMS แจ้งรหัสผ่านชั่วคราวไว้แล้วส่งให้แก่มิจฉาชีพ มิจฉาชีพจึงสามารถโอนเงินออกจากบัญชีเหยื่อได้



กลโกงธนาคารออนไลน์

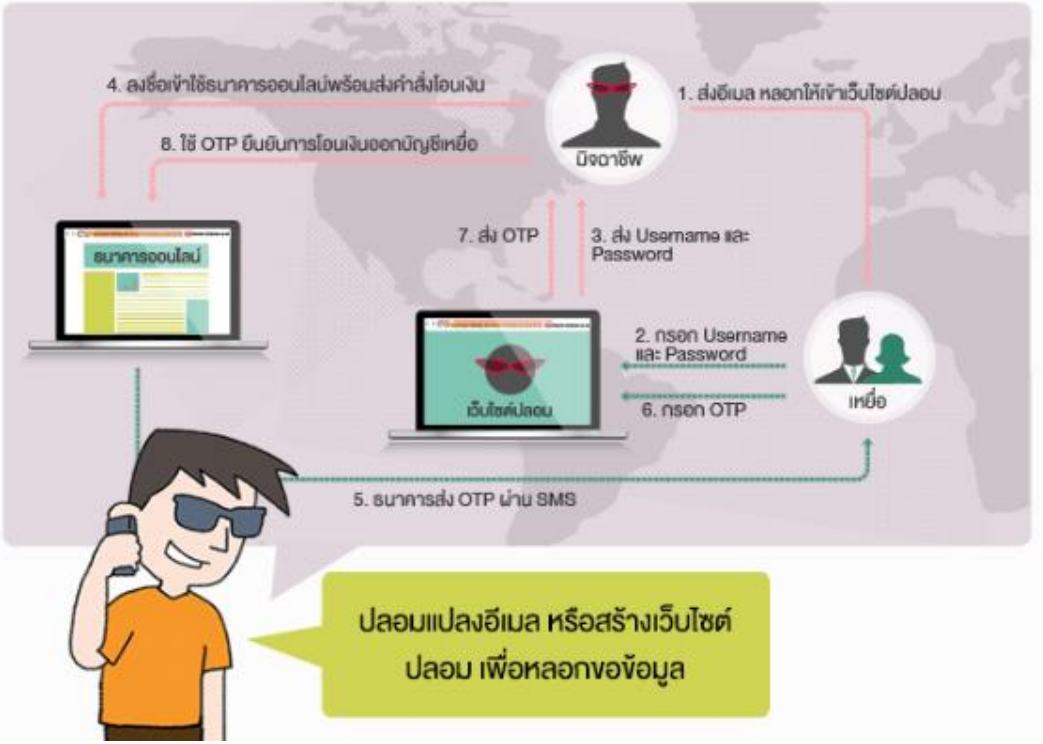
ลักษณะกลโกง

มิจฉาชีพจะหลอกขอรหัสผู้ใช้งาน (username) และรหัสผ่าน (password) จากเหยื่อเพื่อเข้าใช้บัญชีธนาคารออนไลน์ของเหยื่อ แล้วส่งคำสั่งโอนเงินออกจากบัญชีเงินฝาก โดยมีหลายวิธีที่มิจฉาชีพมักใช้ดังนี้

3. ปลอมแปลงอีเมลหรือสร้างเว็บไซต์ปลอม เพื่อหลอกขอข้อมูล

อีเมลปลอมก็เป็นอีกวิธีหนึ่งที่มิจฉาชีพมักใช้เพื่อหลอกเอาข้อมูลที่จำเป็นในการใช้งานธนาคารออนไลน์จากเหยื่อ โดยมิจฉาชีพจะทำอีเมลแอบอ้างเป็นอีเมลของธนาคารอ้างการปรับปรุงระบบรักษาความปลอดภัย แล้วหลอกให้เหยื่อยืนยันการใช้งานบัญชีธนาคารออนไลน์ผ่านการกรอกข้อมูลในอีเมล หรือคลิกลิงก์เชื่อมโยงไปยังเว็บไซต์ธนาคารออนไลน์ปลอมที่มี URL ที่คล้ายหรือเกือบเหมือนเว็บไซต์จริง ซึ่งเมื่อเหยื่อบอกรหัสผ่านผู้ใช้งาน (username) และรหัสผ่าน (password) ในลิงก์ปลอมเหล่านั้น มิจฉาชีพก็สามารถนำข้อมูลไปใช้แอบอ้างเป็นเจ้าของบัญชีแล้วส่งคำสั่งโอนเงิน และสร้างหน้าต่างปลอมหรือหน้าจอ pop-up หลอกให้เหยื่อกรอกรหัสผ่านชั่วคราว ในหน้าจอคอมพิวเตอร์ของเหยื่ออีก ทำให้มิจฉาชีพสามารถโอนเงินออกจากบัญชีของเหยื่อสำเร็จ

มิจฉาชีพมักหลอกขอข้อมูลจากเหยื่อผ่านอีเมลหรือเว็บไซต์ปลอมที่ลักษณะคล้ายกับเว็บไซต์จริงเกือบทุกประการ แต่อีเมลหรือเว็บไซต์ปลอมมีจุดน่าสังเกตดังนี้



วิธีป้องกันการใช้งานธนาคารออนไลน์ทั่วไป

- ไม่ควรใช้รหัสผ่าน (password) ที่ง่ายต่อการคาดเดา เช่น 123456 หรือ วัน/เดือน/ปีเกิด
- ก่อนเข้าใช้ธนาคารออนไลน์ จะต้องมั่นใจหรือตรวจสอบให้แน่ใจว่าเป็นอุปกรณ์ที่ใช้นั้นไม่มีมัลแวร์ (Malware) แฝงอยู่
- ติดตั้งโปรแกรมป้องกันไวรัสที่ถูกกฎหมาย พร้อมตรวจสอบและอัพเดตโปรแกรมอยู่เสมอ
- ไม่ติดตั้งหรือดาวน์โหลดโปรแกรมแปลก ๆ หรือโปรแกรมที่ไม่ถูกกฎหมาย เพราะอาจเป็นช่องทางให้มัลแวร์เข้ามาในคอมพิวเตอร์ สมาร์ตโฟน หรือแท็บเล็ตได้
- ไม่ใช้ลิงก์เชื่อมโยงที่มากับอีเมลหรือในเว็บไซต์ต่าง ๆ เพื่อเข้าสู่ระบบธนาคารออนไลน์ แต่ควรพิมพ์ URL ด้วยตัวเอง
- ไม่ทำธุรกรรมการเงินผ่านอินเทอร์เน็ตสาธารณะ แต่หากจำเป็น ให้เปลี่ยนรหัสผ่านหลังจากใช้งานทันที
- ตรวจสอบรายการเคลื่อนไหวในบัญชี และการเข้าใช้ระบบธนาคารออนไลน์อยู่เสมอ ว่าเป็นรายการที่ได้ทำไว้หรือไม่
- ควร "ออกจากระบบ" (logout) ทุกครั้งเมื่อไม่ใช้งาน
- จำกัดวงเงินในการทำธุรกรรมผ่านธนาคารออนไลน์ เพื่อลดความเสี่ยงในกรณีถูกมิจฉาชีพขโมยรหัสผ่าน
- ธนาคารไม่มีนโยบายส่ง SMS หรือ email เพื่อให้ดาวน์โหลด ติดตั้งโปรแกรม หรือเข้าสู่ระบบธนาคารออนไลน์
- หากคลิกลิงก์ต้องสงสัย ให้รีบติดต่อเจ้าหน้าที่ธนาคารหรือฝ่ายบริการลูกค้าของธนาคารทันทีและขอคำปรึกษาเกี่ยวกับการใช้งานที่ปลอดภัย
- ติดตามข่าวสารกลโกงธนาคารออนไลน์เป็นประจำ เพื่อรู้เท่าทันเล่ห์เหลี่ยมกลโกง

วิธีป้องกันการใช้งานธนาคารออนไลน์ทั่วไป สำหรับการใช้งานธนาคารออนไลน์ผ่านสมาร์ตโฟนหรือแท็บเล็ต

- ไม่เก็บเอกสารหรือข้อมูลสำคัญไว้ในสมาร์ตโฟนหรือแท็บเล็ต เช่น เลขที่บัตรประชาชน เลขที่บัญชีเงินฝาก จดรหัส
- หลีกเลี่ยงการดาวน์โหลด หรือติดตั้งโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ โดยเฉพาะอุปกรณ์ที่ใช้งานธนาคารออนไลน์
- หลีกเลี่ยงการใช้งานธนาคารออนไลน์ผ่านอุปกรณ์ที่มีการดัดแปลง หรือแก้ไขระบบปฏิบัติการ (jailbreak หรือ root) เพราะมีความเสี่ยงสูงที่จะถูกขโมยข้อมูล

สิ่งที่ควรทำเมื่อตกเป็นเหยื่อ

- หากพบเว็บไซต์ปลอมของธนาคาร ให้รีบแจ้งสถาบันการเงินนั้น ๆ ทันที เพื่อดำเนินการปิดเว็บไซต์ดังกล่าว
- หากได้รับข้อความหรือได้คลิกลิงก์เพื่อดาวน์โหลดโปรแกรมต้องสงสัยหรือให้ข้อมูลในเว็บไซต์ปลอมไปแล้ว ให้รีบติดต่อเจ้าหน้าที่ธนาคารทันที
- หากได้รับรหัสผ่านชั่วคราวโดยที่ไม่ได้ส่งคำสั่งโอนเงิน ให้แจ้งเหตุการณ์ที่เกิดขึ้นแก่เจ้าหน้าที่ธนาคารหรือฝ่ายบริการลูกค้าของธนาคารทันทีและขอคำปรึกษาเกี่ยวกับการใช้งานที่ปลอดภัย

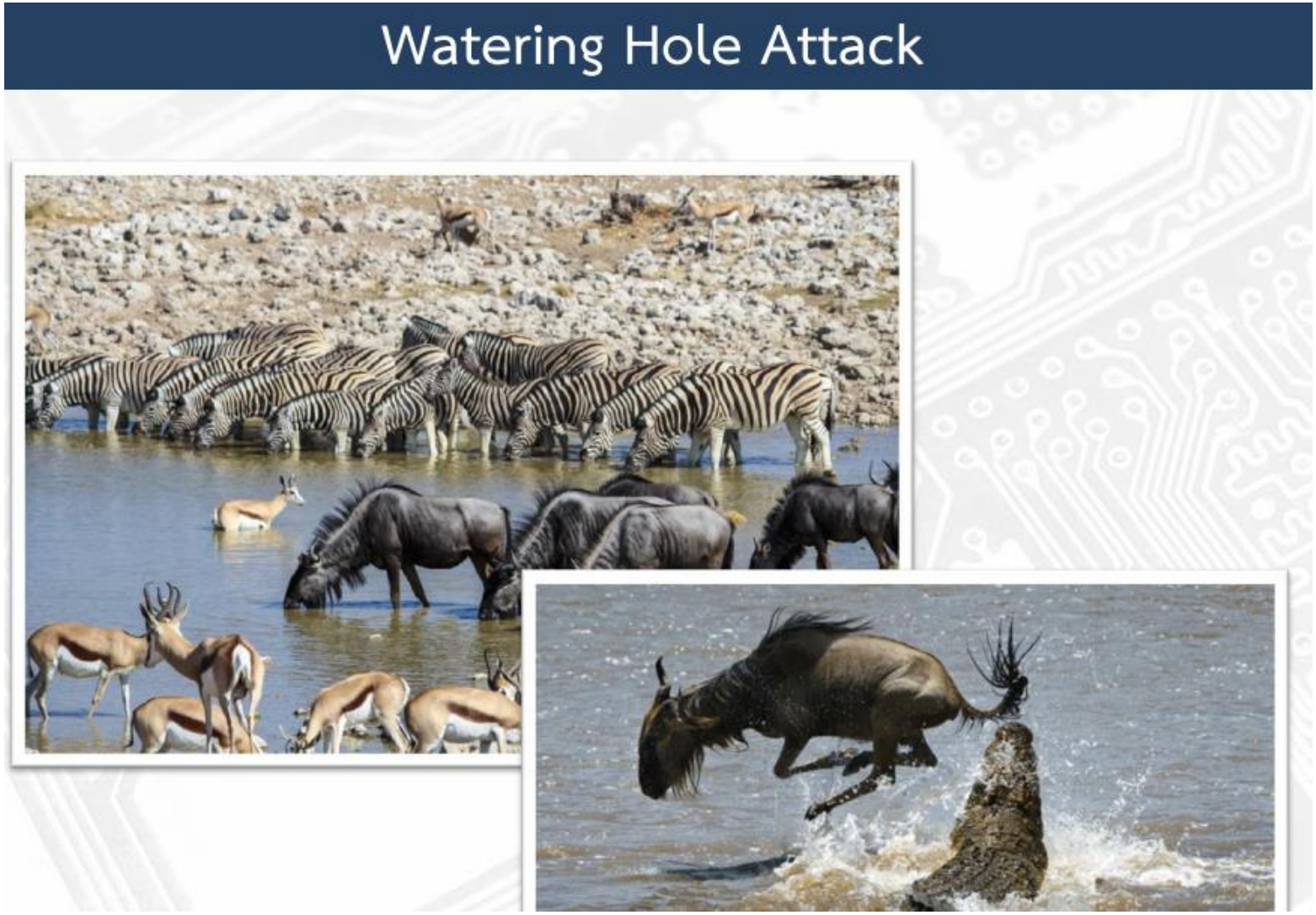
เงินที่ถูกมิจฉาชีพโอนไปจากบัญชีเงินฝากจะได้คืนหรือไม่

การจะได้เงินคืนจากมิจฉาชีพเป็นเรื่องที่ค่อนข้างยาก เพราะทันทีที่มิจฉาชีพได้รับเงินในบัญชี ก็จะรีบถอนออกไป รวมทั้งบัญชีที่โอนไปมักเป็นบัญชีของผู้รับจ้างเปิดบัญชี ไม่ใช่ของมิจฉาชีพ จึงทำให้ยากต่อการติดตาม

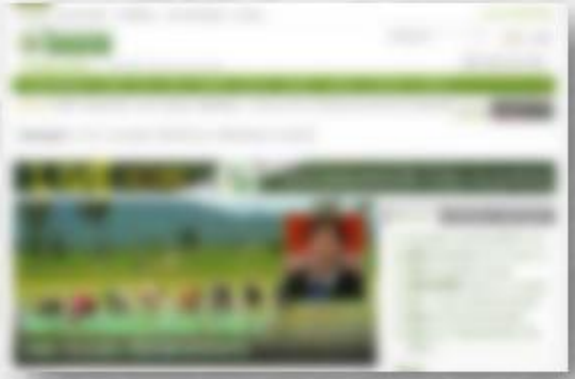
กรณีที่มิจฉาชีพหลอกให้ติดตั้งมัลแวร์ในสมาร์ตโฟน มิจฉาชีพทราบเบอร์โทรศัพท์ของเราได้อย่างไร

มิจฉาชีพอาจได้เบอร์โทรจากหลายแหล่ง เช่น ข้อมูลจากการสมัครสมาชิกตามเว็บไซต์ต่าง ๆ หรือเบอร์โทรศัพท์ของเหยื่อที่แสดงในโซเชียลมีเดียต่าง ๆ หรืออีกกรณีคือ เครื่องคอมพิวเตอร์ของเหยื่อติดมัลแวร์ซึ่งหลอกถามข้อมูลโทรศัพท์มือถือจากเหยื่อ

เตือนภัย Watering Hole Attack



เตือนภัย Watering Hole Attack



1 เหยื่อเปิดเว็บไซต์หนังสือพิมพ์ที่มีมัลแวร์

2 มัลแวร์ถูกติดตั้งบนเครื่องคอมพิวเตอร์เหยื่อโดยอัตโนมัติ

3 มัลแวร์ทำงานเมื่อเหยื่อเข้าใช้งาน e-banking โดยแฝงโฆษณาเรื่องการแจกโปรแกรม antivirus บนโทรศัพท์มือถือ

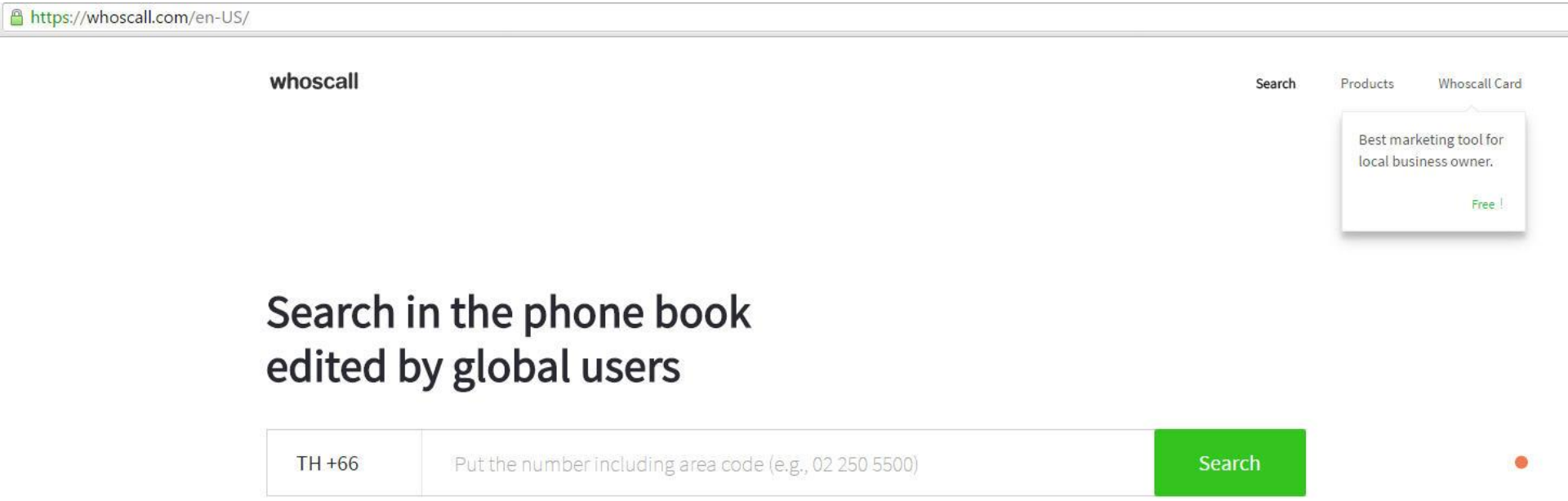
4 เหยื่อหลงเชื่อและติดตั้ง Antivirus ปลอมทำให้ถูกขโมย SMS ที่ใช้ในระบบ e-banking

5 ผู้ไม่หวังดีเข้าถึงระบบ e-banking เพื่อขโมยเงินออกจากบัญชีเหยื่อ

WhoCall

- เพื่อป้องกันเบอร์ และรายงานเบอร์คนไทยที่ร่วมมือกับชาวต่างชาติหลอกโอนเงิน ในรูปแบบต่างๆ ค่าส่งของ หรือ เงินลงทุนในในต่างประเทศ หรือคนไทยหลอกคนไทยด้วยกันเอง เช่นโอนค่าทำเนียมอนุมัติเงินกู้บัตรเงินสด บางพวกแกล้งป่วยหนักขอยืมเงิน พวกเราควร ติดตั้ง app whocall มีทั้งระบบ ios และ android ให้ค้นหาแอปชื่อ whocall และติดตั้ง ทุกครั้งที่มีเบอร์แปลกๆ โทรมา และมีการรายงานว่าเป็นเบอร์เหล่ามิฉาชีพ บอร์เหล่านั้นมันจะแจ้งเราด้วยตามรายงาน..เป็นแอปที่ดีมาก ๆ

WhoCall


https://whoscall.com/en-US/
whoscall
Search
Products
Whoscall Card
Best marketing tool for local business owner.
Free !
Search in the phone book edited by global users
TH +66
Put the number including area code (e.g., 02 250 5500)
Search

WhoCall

TH +66 | 090 972 0999

090 978 0999

No results found

Thailand, True Move

Are you the owner of this number?

หลอกให้โอนเงินผ่าน Facebook

ตำรวจท่องเที่ยวรวบเครือข่ายหลอกลวงหญิงไทยผ่าน facebook ให้โอนเงิน
โดยอ้างตัวเป็นต่างชาติทำทีตีสนิทจะขอแต่งงาน - ทำธุรกิจร่วมกัน ฯลฯ
มูลค่าความเสียหายกว่า17ล้านบาท!!!

รับชม 88,405 ครั้ง

Matichon Online ได้แพร่ภาพสด
3 พฤษภาคม ·

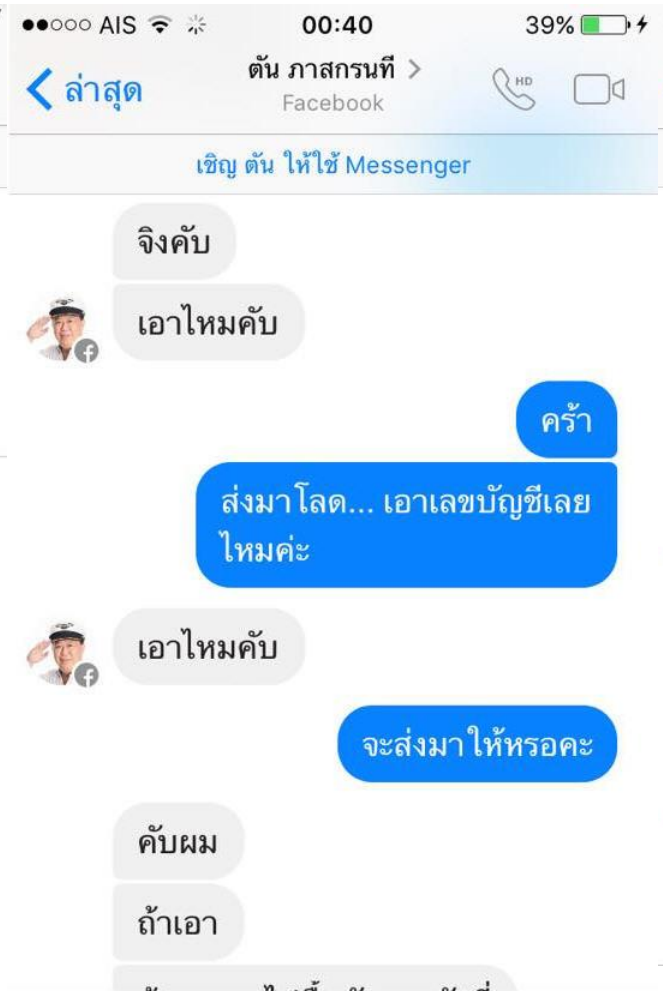
LIVE (สด) ตำรวจท่องเที่ยวรวบเครือข่ายหลอกลวงหญิงไทยผ่าน facebook ให้โอนเงิน โดยอ้างตัวเป็นต่างชาติทำทีตีสนิทจะขอแต่งงาน - ทำธุรกิจร่วมกัน -ปัญหาสุขภาพ ฯลฯ
มูลค่าความเสียหายมากกว่า20ล้านบาท!!!

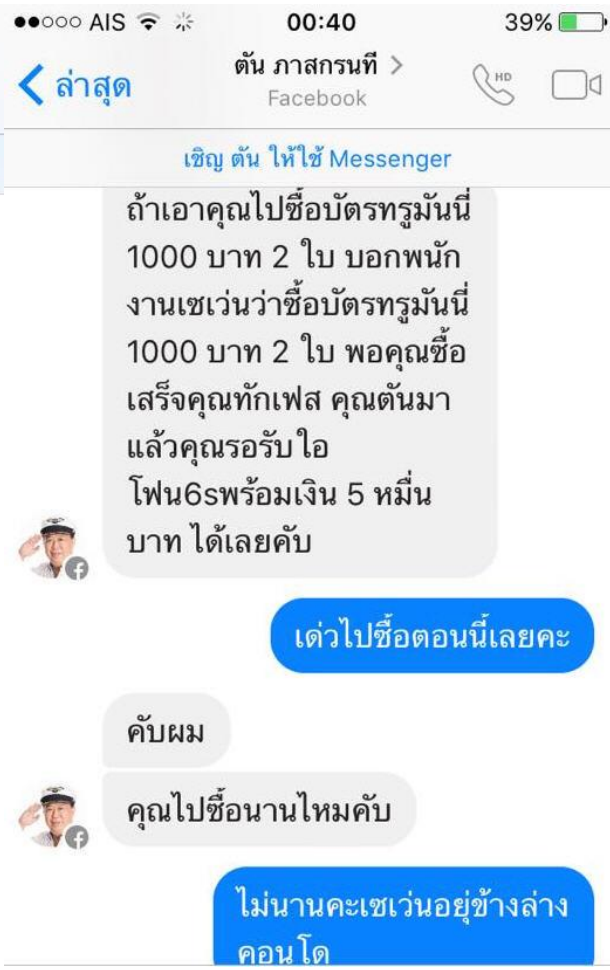
สุภาพสตรีเสื้อสีชมพู (1ในผู้เสียหาย ซึ่งถูกหลอกลวง)

LIVE (สด) ตำรวจท่องเที่ยวรวบเครือข่ายหลอกลวงหญิงไทยผ่าน facebook ให้โอนเงิน โดยอ้างตัวเป็นต่างชาติทำทีตีสนิทจะขอแต่งงาน - ทำธุรกิจร่วมกัน -ปัญหาสุขภาพ ฯลฯ
มูลค่าความเสียหายมากกว่า 20 ล้านบาท!!!
สุภาพสตรีเสื้อสีชมพู (1ในผู้เสียหาย ซึ่งถูกหลอกลวง)

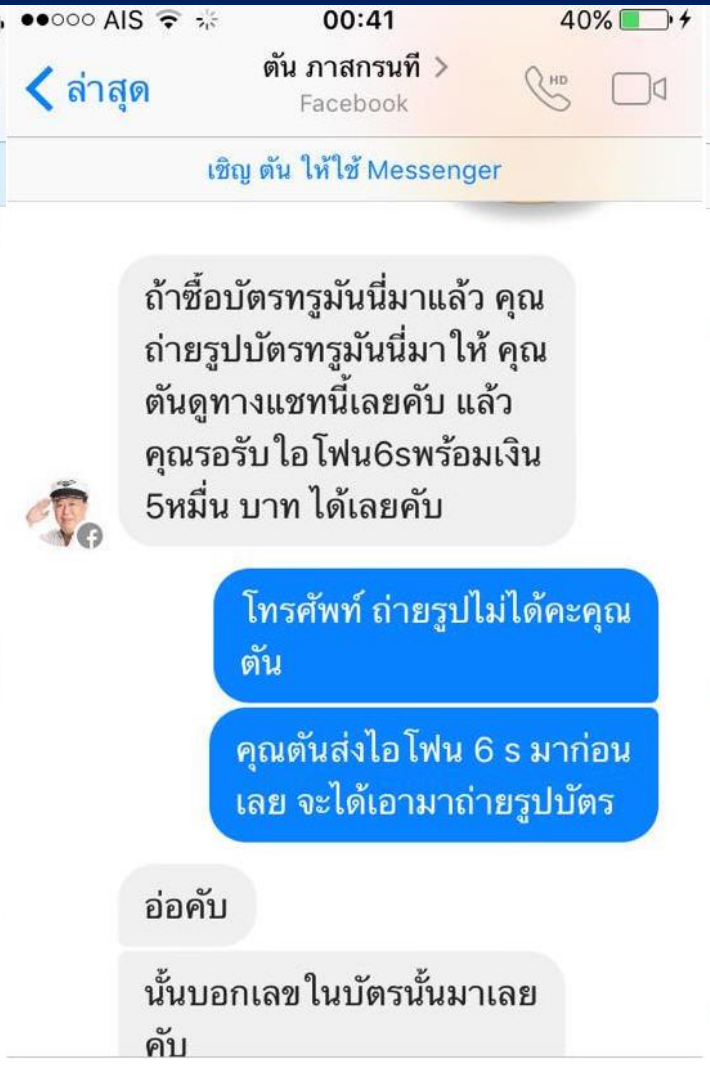
อยากให้ข่าวนี้ไปถึงคนที่กำลังคุยกับฝรั่ง จริงๆแล้วพวกนี้คนไทยด้วยกันทั้งนั้น

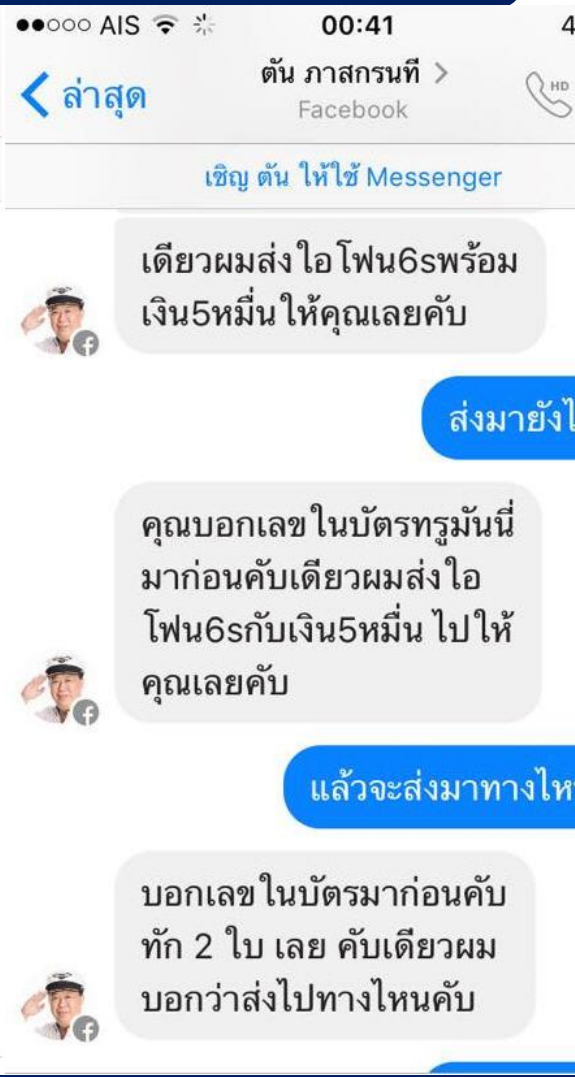
Profile ปลอมอ้างเป็น คุณตัน ภาสกรนที



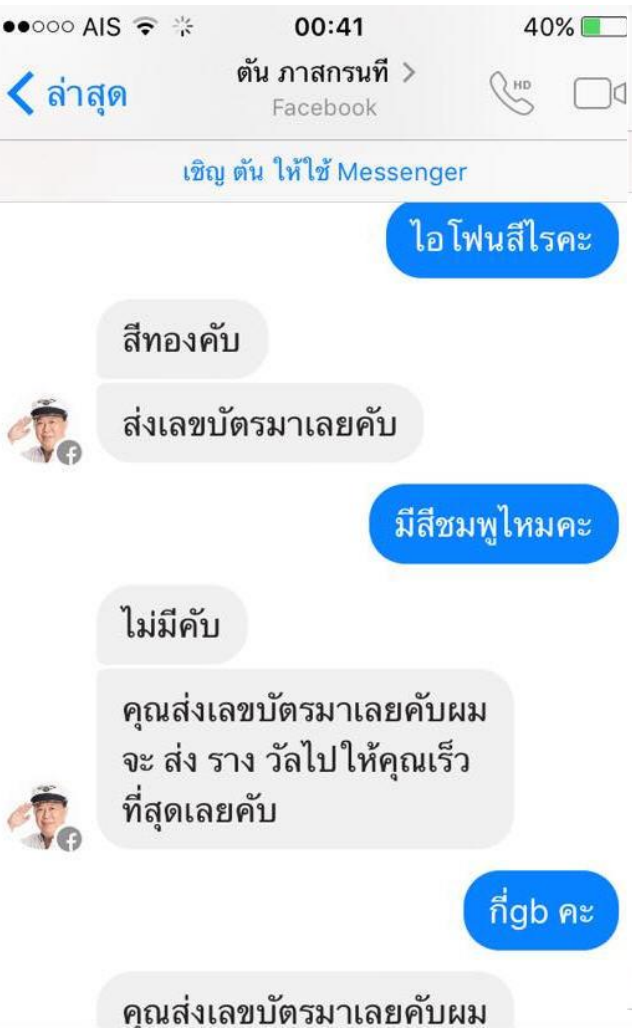


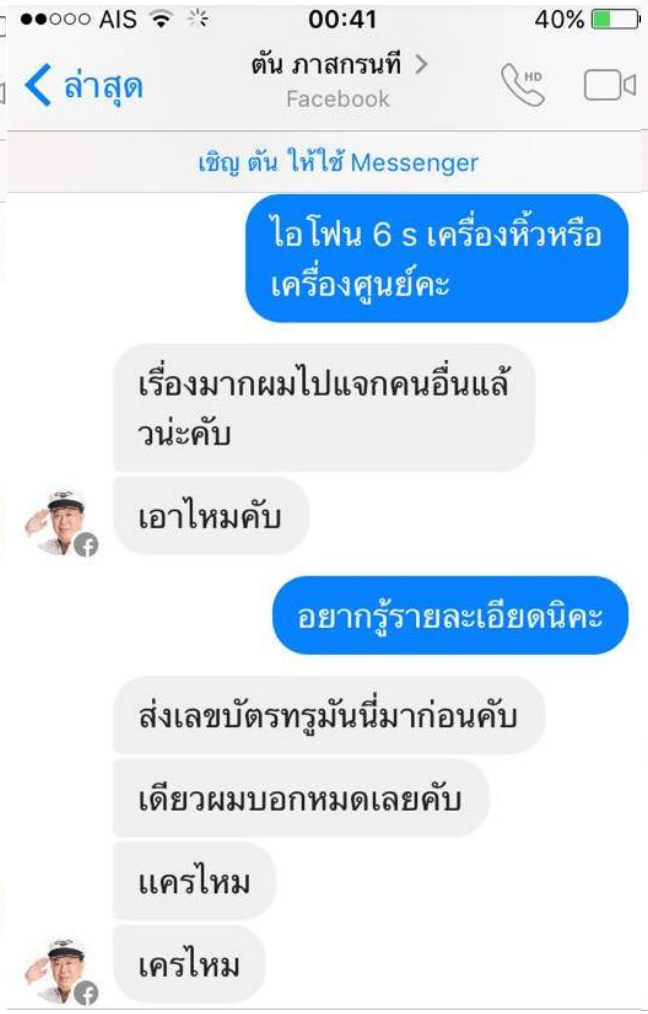
Profile ปลอมอ้างเป็น คุณตัน ภาสกรนที

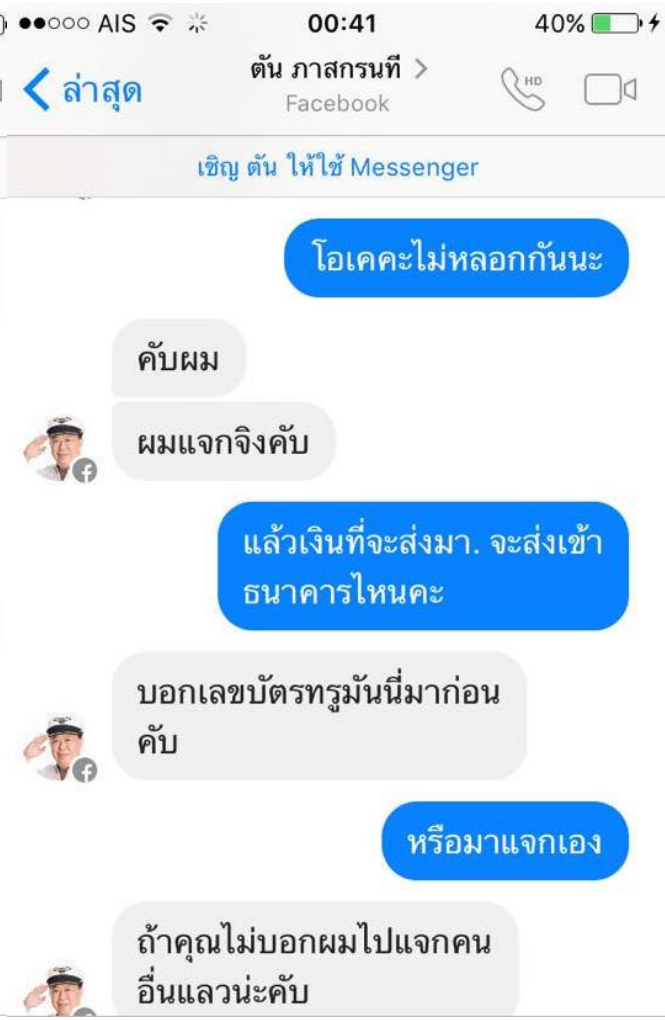




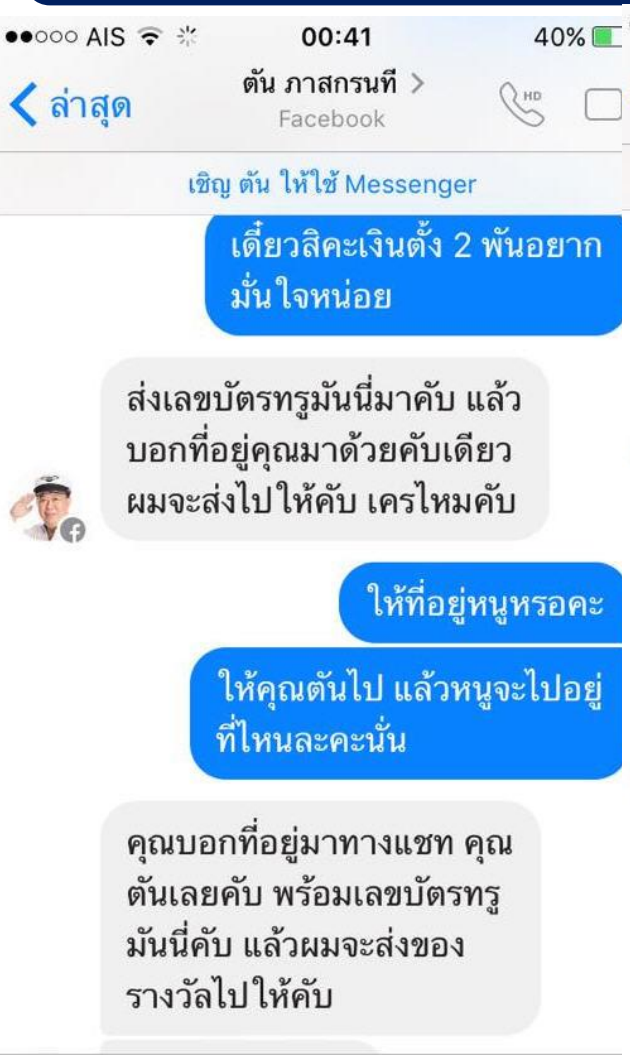
Profile ปลอมอ้างเป็น คุณตัน ภาสกรนที

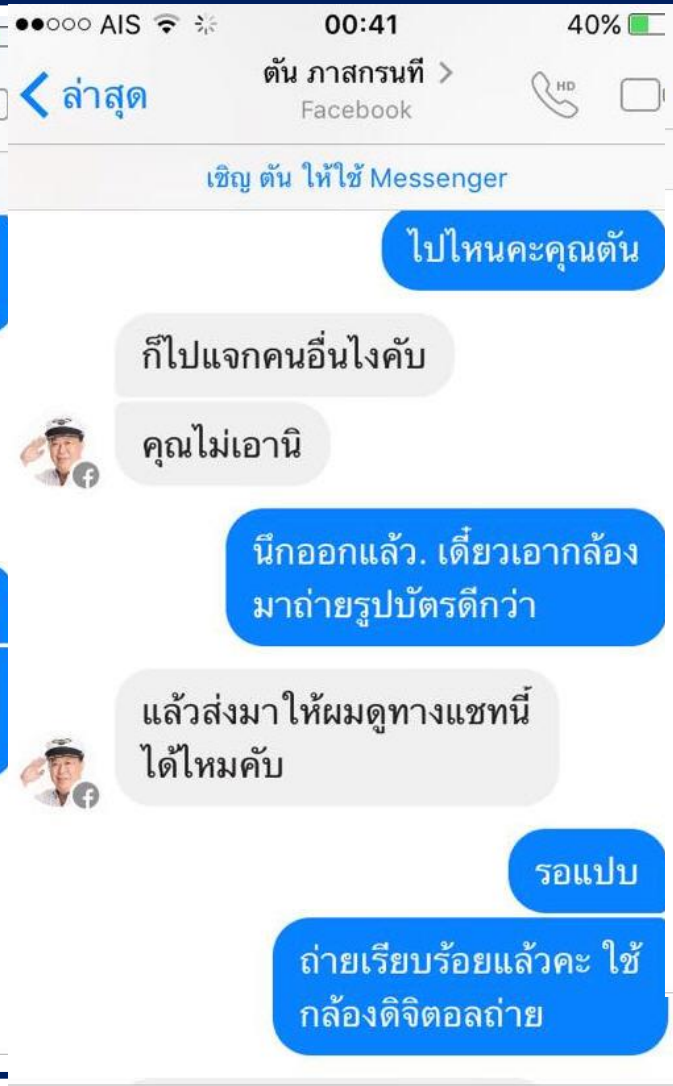


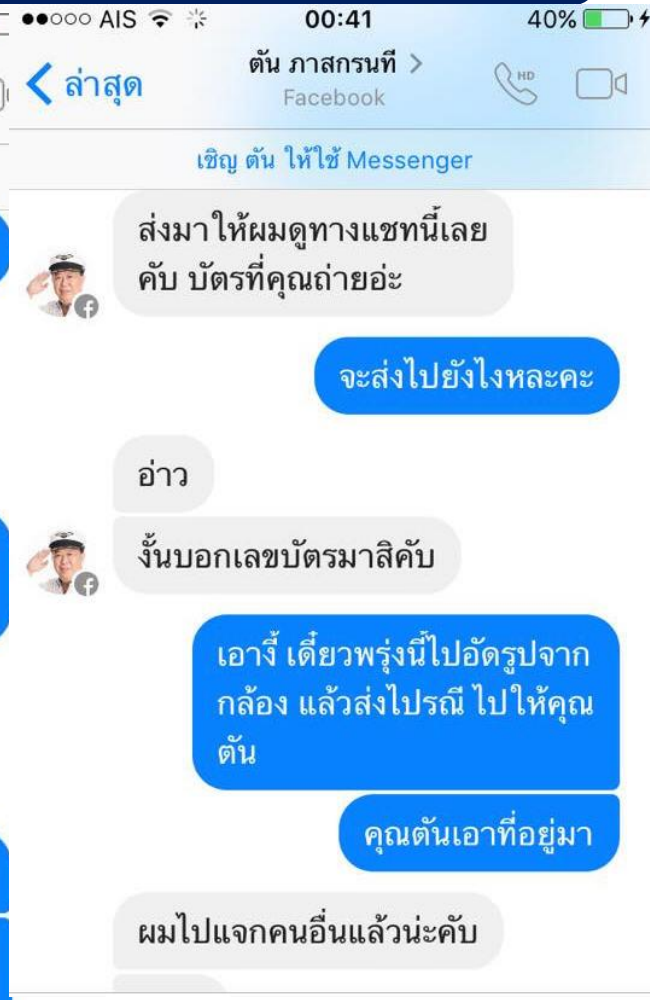




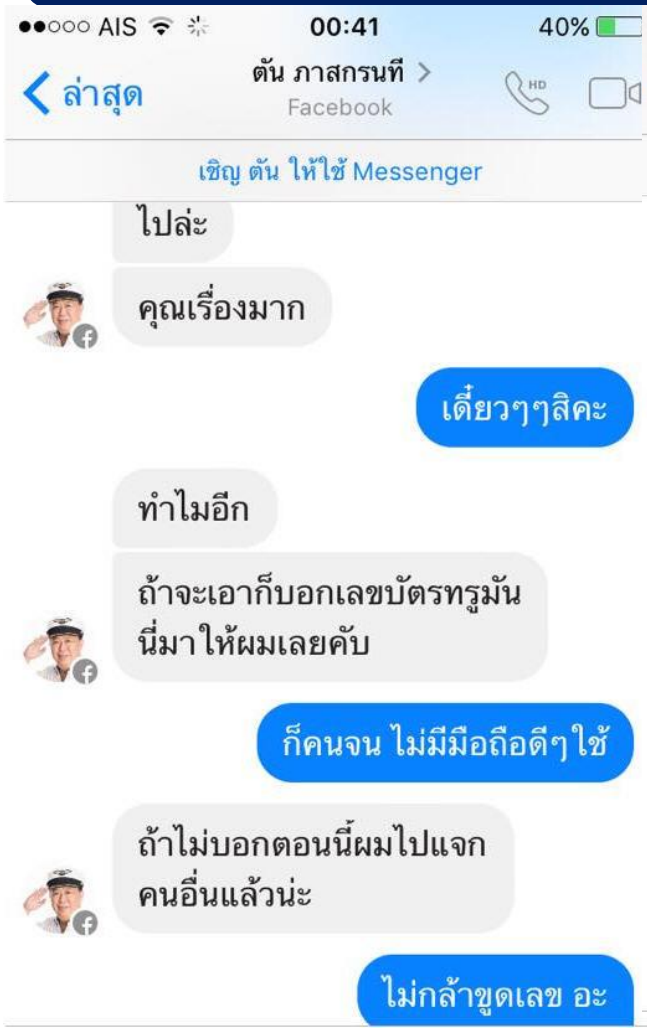
Profile ปลอมอ้างเป็น คุณตัน ภาสกรนที

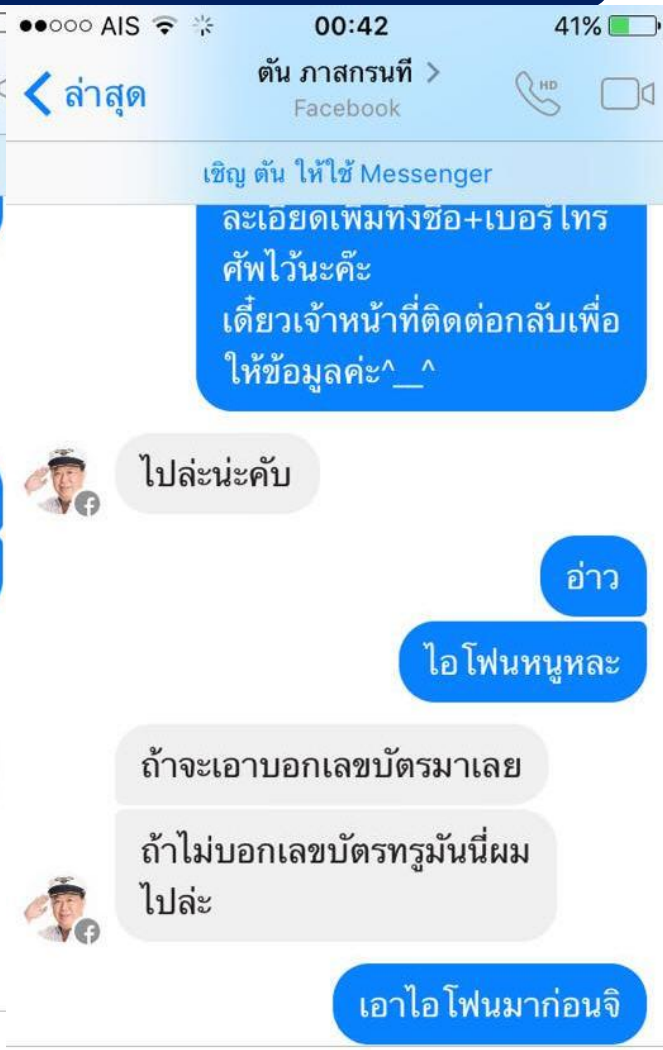






Profile ปลอมอ้างเป็น คุณตัน ภาสกรนที





Profile ปลอมอ้างเป็น คุณตัน ภาสกรนที

วิธีสังเกตเพจคุณตัน อิชิตันของแท้ (ป้องกันการโดนหลอกซื้อบัตรเติมเงินทรูมันนี่)
วิธีการหลอกลวงของมิจฉาชีพจากกรณี คุณตัน อิชิตัน

1. หลังจากที่มีแคมเปญแจกคอนโดและรถเบนซ์จากอิชิตัน ทำให้มิจฉาชีพใช้เป็นช่องทางในการหลอกลวงเอาทรัพย์สินจากผู้ที่หลงเชื่อ โดยวิธีการที่มิจฉาชีพใช้ก็คือ
2. สร้างเฟสบุ้คโดยใช้ชื่อ ตัน ภาสกรนที ที่มีรูปประจำตัวเป็น คุณตัน อิชิตัน เพิ่มเป็นเพื่อนใน Facebook ของเหยื่อ
3. ส่งข้อความแจ้งทางแชทในทำนองว่า เหยื่อเป็นผู้โชคดี เช่น “ยินดีด้วยนะครับ คุณคือผู้โชคดีได้รับเงิน 10 ล้านบาทและรถเบนซ์ 1 คัน ราคา 8 ล้านบาท แค่คุณไปซื้อบัตรทรูมันนี่ ที่เซเว่น 1,000 บาท จำนวน 2 ใบ แล้วถ่ายมาให้ผมแค่นี้คุณเป็นผู้โชคดีเลยครับ”
4. โดยเมื่อเหยื่อหลงเชื่อ จะให้เหยื่อขูดด้านหลังบัตรทรูมันนี่ แล้วถ่ายรูปหมายเลข 14 หลักหลังบัตร แล้วถ่ายรูปส่งไป
5. ซึ่งเมื่อเหยื่อหลงเชื่อ ก็จะไม่รับสายและบล็อกเฟซบุ๊คไปทันที และบัตรเติมเงินทั้ง 2 ใบถูกใช้ไปแทบจะในทันที

Profile ปลอมอ้างเป็น คุณตัน ภาสกรนที

ข้อสังเกตว่า เพจไหนคือเพจของแท้ของคุณตัน ภาสกรนที หลังจากที่มีเพจปลอมเป็นคุณตันออกมามากมาย ทำให้หลายคนเริ่มสงสัยและสับสนว่า อันไหนเป็นเพจคุณตัน อิชิตัน ของจริง ของปลอม วันนี้เราขอแนะนำวิธีการสังเกตง่ายๆ ดังนี้

1. ใช้เฟซบุ้คอันเดียวคือ www.facebook.com/tanichitan/
2. หลังชื่อบนเฟสบุ้ค จะมีเครื่องหมายถูกสีฟ้า ซึ่งเป็นการยืนยันว่าเป็นบุคคลที่มีตัวตนจริงจาก Facebook
3. มีคนถูกใจระดับสิบล้านขึ้นไป (ปัจจุบันที่ 13,106,470 คน เมื่อวันที่ 8 กันยายน 2559)
4. มีการเพิ่มข้อมูลเพิ่มเติมจากคุณตันว่า ทุกอย่างที่แจก ฟรี! และถ้ามีการขอบัตรเติมเงินทรูมันนี่ ให้โอนเงิน แสดงว่าของปลอม

Profile ปลอมอ้างเป็น คุณตัน ภาสกรนที

MTHAI หน้าแรก | ข่าวเด่น | ข่าวการเมือง | ข่าวเศรษฐกิจ | ข่าวทั่วไป | ข่าวต่างประเทศ | ข่าวสังคมออ

ตร. รวบผู้ต้องหาอ้างเป็น "คุณตัน ภาสกรนที" หลอกเงินชาวบ้าน ด้าน คุณตัน ยืนยัน ให้ดำเนินคดีให้ถึงที่สุด

นายศุภชัย สืบสุนทร อายุ 21 ปี ผู้ต้องหาตามหมายจับศาลจังหวัดตลิ่งชัน ฐานฉ้อโกงโดยแสดงตนเป็นคนอื่น และกระทำผิด พ.ร.บ.คอมพิวเตอร์ นำเข้าข้อมูลอันเป็นเท็จ ถูกตำรวจกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือ ปอท. จับกุมตัวได้ที่ห้องพักย่านบางกอกน้อย กรุงเทพมหานคร

โดย นายศุภชัย ผู้ต้องหามีพฤติการณ์ ปลอมแปลงสร้างเฟซบุ๊ก ชื่อ ตัน ภาสกรนที หลอกลวงผู้เสียหาย ผ่านทางข้อความเฟซบุ๊ก อ้างว่าผู้เสียหายเป็นผู้โชคดี ได้รับเงินจำนวน 10 ล้านบาท และรถยนต์ 1 คัน ราคากว่า 8 ล้านบาท จากการร่วมกิจกรรมชิงรางวัล แต่จะต้องซื้อบัตรเติมเงิน 1,000 บาท จำนวน 2 ใบ แล้วขูดเลขรหัสบัตรถ่ายภาพส่งกลับมาทางข้อความเฟซบุ๊ก จึงจะได้รับรางวัลดังกล่าว ผู้เสียหาย หลงเชื่อดำเนินการตามที่ผู้ต้องหากล่าวอ้าง แต่เมื่อส่งรหัสบัตรไปแล้วกลับไม่สามารถติดต่อ นายศุภชัย ได้ จึงเข้าแจ้งความดำเนินคดี

ทั้งนี้ จากการสอบสวน นายศุภชัย ให้การรับสารภาพอ้างว่าทำไปด้วยความคึกคะนอง เพิ่งทำเป็นครั้งแรก หลอกผู้เสียหายเพียง 3 ราย แต่ได้เงินมาเพียงรายเดียว จำนวน 2,000 บาท ด้าน นายตัน ภาสกรนที ยืนยันจะให้เจ้าหน้าที่ดำเนินคดีอย่างถึงที่สุดกับผู้ที่แอบอ้างชื่อตนเองเพื่อหาผลประโยชน์ พร้อมระบุ หากเป็นเพจจริงผู้โชคดีไม่จำเป็นต้องโอนเงินหรือเสียค่าใช้จ่ายใดๆ ในการรับรางวัลและขอให้ผู้เสียหายเข้าแจ้งความดำเนินคดีกับเจ้าหน้าที่เพื่อติดตามจับกุมตัวผู้กระทำผิดมาดำเนินคดี ต่อไป

อย่างไรก็ตาม สำหรับกรณีนี้ นายตัน ภาสกรนที หรือ ตัน อิชิตัน เจ้าของเครื่องดื่มชื่อดัง ได้เข้าแจ้งความกับพนักงานสอบสวน ปอท. เพื่อดำเนินคดีกับผู้ที่ปลอมแปลงและแสวงหาประโยชน์กับประชาชน จนทำให้ตนเองได้รับความเสียหายไปแล้ว ตั้งแต่ วันที่ 23 มีนาคม ที่ผ่านมา

7 วิธีตรวจสอบว่าเราตกเป็นเหยื่อ Romance Scam หรือไม่?

Romance Scam ก็คือการหลอกลวงผู้หญิง (ผู้ชายก็โดนได้ อย่าประมาท) ด้วยการพูดคุย การแชท หรือการส่งอีเมล ส่งข้อความเป็นการจีบ หรือทำให้เหยื่อเชื่อว่าเกิดความรัก หรือตกหลุมรัก ทำให้เชื่อใจ-ตายใจด้วยวิธีการต่างๆ (บางคนอดทนตามจีบ หยอดคำหวานใหแเป็นปีเลยนะคะ เพื่อสร้างความไว้เนื้อเชื่อใจ) และในที่สุดจะขอยืมเงิน หลอกให้ส่งยาเสพติด หรือช่วยเหลือด้วยวิธีการต่างๆ ที่เป็นอันตรายต่อเหยื่อเอง โดยเฉพาะชาวไนจีเรียผิวดำ ซึ่งเป็นชาติที่มีนักหลอกลวงมากที่สุดในโลก (Nigeria) กาน่า (Ghana) ไอเวอรี่โคล้สต์ (Ivory Coast) หรือประเทศแอฟริกาตะวันตกทั้งหลาย กลุ่มคนร้ายพวกนี้เค้าทำกันเป็นทีม

อันตรายที่จะเกิดขึ้นจากกลุ่มคนพวกนี้คือ

อาจถูกขอยืมเงิน ขอยืมสิ่งของ ขอให้แต่งงาน (เพื่อจะขอวีซ่าอยู่เมืองไทยถาวรหรือเปลี่ยนสัญชาติเป็นไทย) อาจถูกซ้อม ถูกข่มขืน ถูกฆ่าตาย ถูกขอให้ขนส่งยาเสพติด (สมรู้ร่วมคิด ติดคุกตลอดชีวิต) ถูกขอให้ออกใบทำงาน (Work permit) ในที่สุดอาจจะนำบริษัทของคุณมาใช้เป็นที่ฟอกเงิน ถ้าโอนเงินมาในชื่อเรา ตัวเราอาจจะโดนข้อหาหลอกลวงเงินจากผู้อื่น (ตัวอย่างเช่น นาย A ไปหลอกเงิน นส. B แล้วให้ส่งเงินมาในชื่อเราสมมติชื่อ นส. C หรือในบัญชีของเรา ....อาจจะโดนตำรวจสากลมาจับในฐานะฉ้อโกงคนอื่นๆ มานับไม่ถ้วน) เท่านี้ยังไม่พอ อาจจะต้องทำงานหาเงินเลี้ยงมัน .. คนร้ายพวกนี้ด้วย หากมีหลักฐาน เช่น พาสปอร์ต บัตรประชาชน (ID) หรือหลักฐานอื่นๆ เช่นใบเสร็จ บัตรเครดิต เบอร์บัญชี สามารถแจ้งเจ้าหน้าที่ตำรวจในบริเวณที่คุณอาศัยอยู่ก่อน เพื่อให้รับทราบ ลงบันทึก และชี้มูลความผิดก่อน แล้วหากเกี่ยวข้องกับต่างประเทศจริง ก็ต้องแจ้งตำรวจสากลอีกครั้ง

7 วิธีตรวจสอบว่าเราตกเป็นเหยื่อ Romance Scam หรือไม่?

7 คำถามว่าคุณตกเป็นเหยื่อ Romance Scam หรือไม่

1. **Have you been on a dating or social network site in the past 6 months?**
   คุณเคยเดท/จีบหรือพูดคุยกับกลุ่มหาเพื่อนทางเน็ตในช่วงเวลา 6 เดือนที่ผ่านมาหรือไม่?
2. **Has someone fallen in love with you quickly?**
   มีใครบางคนที่ตกหลุมรักคุณอย่างรวดเร็วหรือไม่?
3. **Do they immediately want to leave the dating site to use IM or email?**
   พวกเขาอยากจะย้ายจากคุยกันผ่านเว็บ ไปเป็นการส่งข้อความหรือส่งอีเมลอย่างรวดเร็วหรือไม่?
4. **Do they claim to be from the US but working overseas; Nigeria or UK?**
   พวกเขาอ้างว่า มาจากอเมริกา แต่ต้องไปทำงานต่างประเทศ เช่น ไนจีเรีย หรืออังกฤษ ใช่หรือไม่?
5. **Has someone asked you for money or to cash a check?**
   มีใครที่ขอร้องหยิบยืมเงิน หรือขอให้คุณเอาเช็คไปขึ้นเงินให้แล้วหรือยัง?
6. **Are they coming to visit you soon but a event prevents them from visiting?**
   พวกเขารีบบินมาพบคุณทันที แต่ดันเกิดเหตุการณ์ไม่คาดฝันทำให้มาหาไม่ได้หรือไม่?
7. **They have no close family or friend or business associates to turn to**
   พวกเขาไม่มีครอบครัว/ญาติที่ใกล้ชิด/เพื่อนสนิท/เพื่อนร่วมงาน ที่จะหันหน้าไปพึ่งได้เลย

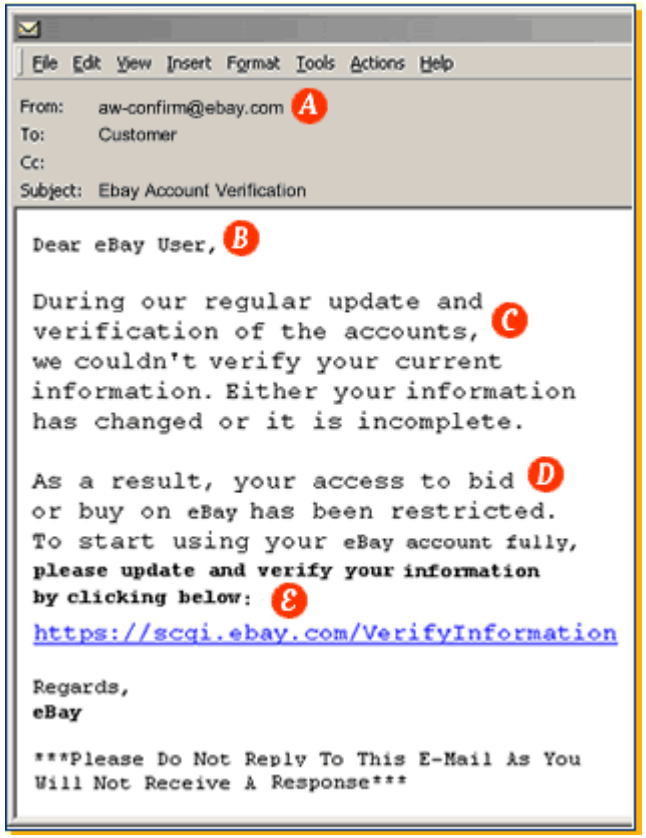
Spoof Email หรือ Phishing

อีเมล์ปลอมหรือที่เราเรียกกันว่า Spoof Email หรือ Phishing นั้นเป็นปัญหาสำคัญสำหรับผู้ใช้งานอินเทอร์เน็ต อีเมล์เหล่านี้มักจะเป็นการแอบอ้างว่าส่งมาจากบริษัทที่มีชื่อเสียง และจะขอให้ผู้ใช้ตอบกลับโดยใส่ข้อมูล เช่นบัตรเครดิต บัตรประชาชน หรือรหัสผ่านเข้าบัญชีผู้ใช้

ลักษณะทั่วไปของอีเมล์หลอกลวง

ข้อมูลต่อไปนี้จะช่วยไม่ให้คุณตกเป็นเหยื่อของ spoof อีเมล์เหล่านี้ และสามารถนำไปใช้ในการพิจารณาอีเมล์ที่ส่งมาจากบริษัทต่างๆ ไม่เฉพาะกับอีเบย์ แต่ทุกเมื่อที่คุณมีการทำธุรกรรมออนไลน์ ทางด้านขวามือ จะเป็นตัวอย่าง spoof mail ที่เห็นบ่อยๆ คือจะมีแบบฟอร์มให้คุณใส่ข้อมูลส่วนตัว อีเมล์แบบนี้เห็นได้ชัดว่าเป็นอีเมล์ปลอม และคุณไม่ควรให้ข้อมูลใดๆ ทั้งสิ้น

การตรวจสอบอย่างคร่าวๆ ว่าอีเมล์นั้นมาจากอีเบย์จริงหรือไม่


File Edit View Insert Format Tools Actions Help

From: aw-confirm@ebay.com (A)
To: Customer
Cc:
Subject: Ebay Account Verification

Dear eBay User, (B)

During our regular update and verification of the accounts, (C) we couldn't verify your current information. Either your information has changed or it is incomplete.

As a result, your access to bid (D) or buy on eBay has been restricted. To start using your eBay account fully, **please update and verify your information by clicking below:** (E)

https://scgi.ebay.com/VerifyInformation

Regards,
eBay

Please Do Not Reply To This E-Mail As You Will Not Receive A Response

Example Spoof Form

สัญญาณเตือนว่าอีเมล์ที่คุณได้รับเป็น อีเมล์ปลอม

A. Email address ของผู้ส่ง spoof email มักจะระบุอีเมล์ปลอมไว้ในช่อง From ด้วย และบางครั้งก็เป็นการปลอม ให้เหมือนอีเมล์ที่อีเบย์ใช้อยู่จริง. (From: billing@ebay.com; From: eBayAcctMaintenance@eBay.com; From: support@ebay.com).

B. คำขึ้นต้น Spoof Email จำนวนมาก จะขึ้นต้นด้วยคำทักทายทั่วๆไป เช่น "Welcome eBay User."

C. ความเร่งด่วน มีข้อความอ้างว่าอีเบย์กำลังอัพเดทข้อมูล หรือบัญชีผู้ใช้ อย่าเป็นกังวัลในข้อนี้ โอกาสที่อีเบย์จะทำข้อมูลของคุณหาย มีน้อยมาก

D. บอกว่าบัญชีของคุณกำลังมีปัญหา Spoof Email ส่วนใหญ่จะหลอกให้คุณเชื่อว่า กำลังมีเหตุการณ์ใดเกิดขึ้นกับบัญชีผู้ใช้ของคุณ และทำให้คุณไม่สามารถซื้อ หรือขายสินค้าบนอีเบย์ได้ หากไม่อัพเดทข้อมูลในทันที

E. ลิงค์ในอีเมล์
ถึงแม้ว่าในหลายอีเมล์จะมีลิงค์ใส่ เข้ามาด้วยแต่ลิงค์เหล่านี้ก็อาจ มีการปลอมแปลงได เช่นกัน

การตรวจสอบอย่างคร่าวๆ ว่าอีเมล์นั้นมาจากอีเบย์จริงหรือไม่

Example Spoof Form

สัญญาณเตือนว่าอีเมล์ที่คุณได้รับเป็น อีเมล์ปลอม

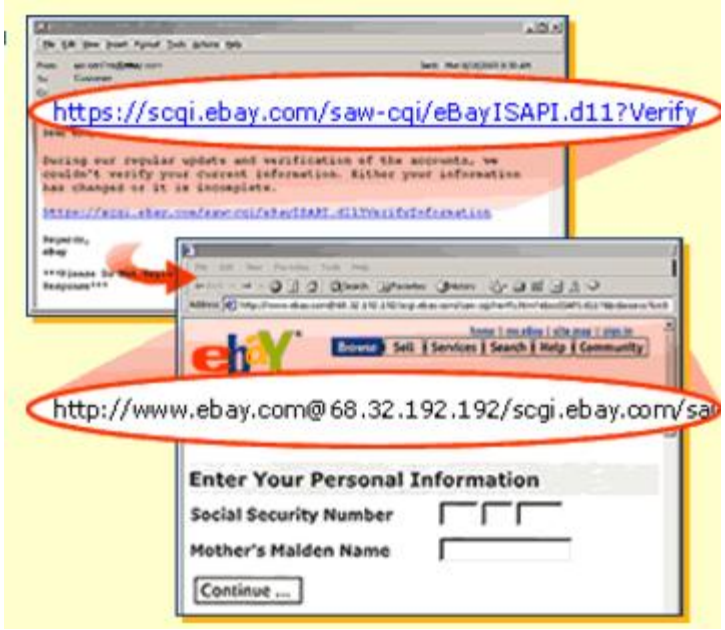
F. ขอข้อมูลส่วนตัว

การที่เนื้อความในอีเมล์มีการขอให้คุณ ใส่ข้อมูลส่วนตัว เช่น user ID, รหัสผ่าน หรือเลขบัญชีธนาคาร โดยคลิกลิงค์ หรือใส่ในฟอร์มที่ให้มาในอีเมล์ก็เป็น การบ่งชี้ว่าอีเมล์นั้นอาจเป็นอีเมล์หลอกลวงเช่นกัน

หากจะต้องมีการล็อกอินเข้าระบบใดๆของอีเบย์หรือเพย์พาล กรุณาเปิด browser และพิมพ์ url โดยตรง เช่น www.ebay.com หรือ www.paypal.com ไม่ควรคลิกจากลิงค์ในอีเมล์

แจ้งการได้รับอีเมล์ปลอมโดยส่งไปได้ที่ spoof@ebay.com

การตรวจสอบอย่างคร่าวๆ เว็ปไซด์ปลอม



Spoof Email มักจะใส่ลิงค์ไปที่เว็บไซต์ปลอม

จากตัวอย่างทางด้านขวา คุณจะเห็นว่าบางครั้งลิงค์ในอีเมล์ ไม่ได้ตรงกับ URL ที่เป็นลิงค์จริงๆ คุณจะรู้ได้อย่างไรว่า คุณอยู่ในเว็บไซต์อีเบย์จริงๆ

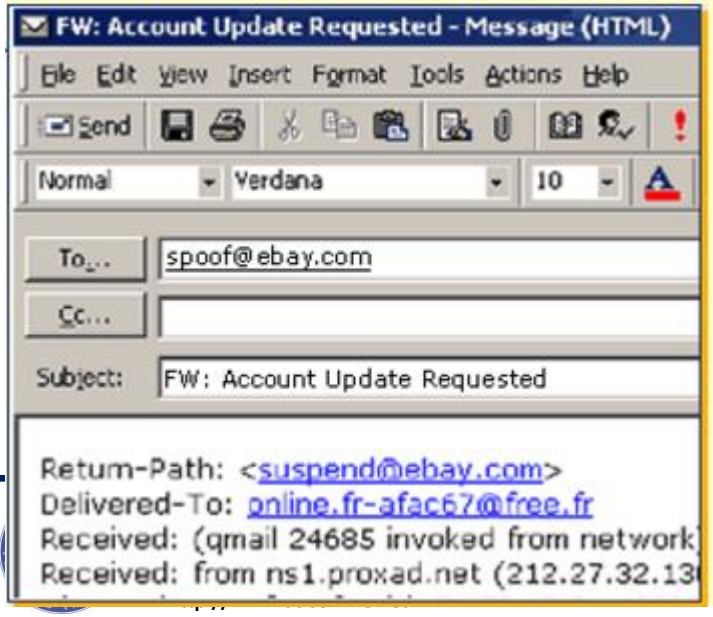
เว็บไซต์อีเบย์ที่ถูกต้อง
การระบุว่าเว็บอีเบย์ที่คุณเข้าอยู่ขณะนั้น เป็นเว็บไซต์อีเบย์จริงๆ ลองดูที่ .ebay.com ซึ่งจะต้องอยู่ก่อนเครื่องหมาย "/" แรก ในตัวอย่างล่าง โปรดสังเกตว่าจะต้องมี "." ก่อน eBay.com จึงจะรู้ได้ว่านั่นคือเว็บไซต์อีเบย์จริงๆ

ตัวอย่าง url ของเว็บไซต์ปลอม :
http://signin.ebay.com@10.19.32.4/
http://signin-ebay.com/

เว็บไซต์อีเบย์จริง:
https://signin.ebay.com/

อย่าคลิกลิงค์ในอีเมล์หากคุณไม่แน่ใจว่าเป็นลิงค์ของจริงหรือไม่ โดยเฉพาะเมื่ออีเมล์นั้นมีการขอให้คุณระบุข้อมูลทางการเงิน

ต้องทำอย่างไรหากได้อีเมล์ปลอม



คุณสามารถควบคุมอีเมล์ที่เป็น Spoof Mail เหล่านี้ได้ คุณสามารถป้องกันไม่ให้ข้อมูล ทางการเงินรั่วไหล โดยไม่หลงเชื่ออีเมล์ เหล่านี้ นอกจากนั้น คุณไม่ควรให้ข้อมูล ติดต่อ ข้อมูลสำหรับล็อกอิน หรือข้อมูลสำคัญอื่นๆ ในอีเมล์นั้น

คุณสามารถรายงาน Spoof Email เข้ามาได้ง่ายๆ
หากคุณไม่แน่ใจว่าอีเมล์นั้น มาจากอีเบย์จริงหรือไม่ คุณสามารถรายงานให้อีเบย์ทราบด้วยวิธีดังต่อไปนี้

1. ส่งอีเมล์นั้นไปให้ spoof@ebay.com
2. อย่าเปลี่ยนชื่ออีเมล์ (Subject Line) หรือส่งอีเมล์นั้นมาเป็น file แนบ (attachment) หากทำเช่นนั้นจะทำให้เราตรวจสอบ ได้ยากยิ่งขึ้น
3. เมื่อคุณได้ forward อีเมล์มาให้เราแล้ว คุณสามารถลบอีเมล์นั้นทิ้งไปได้

ทำให้บัญชีของคุณปลอดภัย

ข้อควรปฏิบัติเมื่อสงสัยว่าคุณอาจได้รับอีเมล์ที่หลอกลวง

- ดูอีเมล์ในส่วน My Message ส่วนใหญ่แล้วอีเมล์จากอีเบย์ที่เกี่ยวข้องกับสถานะผู้ขาย มักจะอยู่ใน My eBay ด้วย อย่างไรก็ตาม บางครั้งอีเมล์ที่ส่งจากทีมงานอีเบย์ภูมิภาค (เช่น จากอีเบย์ประเทศจีน หรืออีเบย์สิงคโปร์) อาจจะไม่อยู่ในส่วน My eBay ของคุณ ดังนั้น หากในอีเมล์ที่คุณได้รับ มีการขอให้คุณต้องล็อกอินเข้าไปให้ข้อมูลต่างๆ กรุณาเปิด browser ใหม่เท่านั้น ไม่ควรคลิกจากลิงค์ที่ให้มาในอีเมล์
- มีการระบุชื่อผู้ใช้ อีเมล์ที่เกี่ยวข้องกับสถานะบัญชีอีเบย์ จะต้องมีการระบุชื่อ และชื่อeBay ID ของคุณในวงเล็บ เอาไว้ที่หัวอีเมล์เสมอ
- สแกนไวรัส การสแกนไวรัสในเครื่องคอมพิวเตอร์ของคุณบ่อยๆ และตรวจสอบให้แน่ใจว่าซอฟท์แวร์ป้องกันไวรัสและระบบปฏิบัติการของคุณเป็นเวอร์ชั่นที่อัพเดทล่าสุดเสมอ
- หมั่นตรวจดูความผิดปกติของบัญชี. คุณควรตรวจสอบสถานะบัญชีของคุณเป็นระยะ เพื่อให้แน่ใจว่าไม่มีกิจกรรมใดผิดปกติ
- เปลี่ยนรหัสผ่านบ่อยๆ.หากคุณคิดว่าบัญชีของคุณกำลังไม่ปลอดภัย ควรเปลี่ยนรหัสผ่านในทันที

ทำให้บัญชีของคุณปลอดภัย

ข้อควรปฏิบัติเมื่อสงสัยว่าคุณอาจได้รับอีเมล์ที่หลอกลวง

- อย่าใช้รหัสผ่านซ้ำกัน เพื่อป้องกันไม่ให้ผู้ที่เข้าไปขโมยข้อมูลในบัญชีของคุณ สามารถเข้าไปดูข้อมูลอื่นได้อีก หากคุณมีบัญชีผู้ใช้มากกว่า 1 บัญชี แต่ละบัญชีควรมีรหัสผ่านที่แตกต่างกัน และในรหัสผ่าน ควรประกอบด้วยทั้งตัวหนังสือและตัวเลข เพื่อให้ผู้ไม่ประสงค์ดีคาดเดาได้ยากขึ้น
- ติดต่อธนาคารหรือผู้ให้บริการบัตรเครดิต หากคุณเผลอกรอกข้อมูลส่วนตัวลงในเว็บไซต์หรืออีเมล์ที่คาดว่าเป็นอีเมล์หลอกลวง กรุณาติดต่อเจ้าหน้าที่ธนาคารหรือบัตรเครดิตในทันที
- รายงานการขโมยข้อมูลบัญชีผู้ใช้ หากคุณคิดว่าบัญชีผู้ใช้ถูกขโมย กรุณารายงานไปที่ http://pages.ebay.com/help/confidence/isgw-account-theft-reporting.html
- รายงาน Spoof Email และเว็บไซต์หลอกลวง
- การรายงานอีเมล์และเว็บไซต์ที่หลอกลวงว่าส่งมาจากอีเบย์หรือเพยพาล ทำให้เราสามารถคุ้มครองผู้อื่นจากการหลอกลวงเดียวกันได้ และยังสามารถแจ้งผู้ให้บริการอินเทอร์เน็ต ให้บล็อคเว็บไซต์เหล่านั้น เพื่อไม่ให้สมาชิกท่านอื่นตกเป็นเหยื่อเพิ่มขึ้น

  ส่งอีเมล์ที่อ้างว่ามาจากอีเบย์มาที่ spoof@ebay.com และลบทิ้ง

  ส่งอีเมล์ที่อ้างว่ามาจากเพย์พาล ไปที่ spoof@paypal.com และลบทิ้ง

  ใช้เครื่องมือ Account Guard feature of eBay Toolbar เพื่อแจ้งเว็บไซต์ปลอม

เตือนภัยมิจฉาชีพ

พฤติกรรมที่น่าสงสัยและเข้าข่ายเป็นกลุ่มมิจฉาชีพ มีดังนี้

1. ขายสินค้าราคาถูกกว่าท้องตลาดมากเกินไป
2. หลอกล่อให้โอนเงินค่าสินค้าล่วงหน้าโดยไม่ให้หลักฐานเพื่อสร้างความน่าเชื่อถือแต่อย่างใด
3. เมื่อโอนเงินแล้ว ผู้ขายจะหายตัวไป ไม่รับโทรศัพท์ และปิดโทรศัพท์หนีในที่สุด
4. เปลี่ยนชื่อ และเบอร์โทรศัพท์ไม่ซ้ำกัน ทำให้ยากต่อการติดตาม
5. นัดเจอเพื่อดูสินค้า แล้วขอรับสินค้าก่อนโดยอ้างว่าจะโอนเงินให้ภายหลัง
6. ปลอม SMS จากทางธนาคาร เพื่อหลอกว่าโอนเงินให้แล้ว แต่แท้จริงยังไม่ได้โอนเงิน หรือหลอกว่าโอนเงินเกินให้ช่วยโอนเงินคืน
7. อ้างว่าดีลฟิชเป็นคนกลางในการชำระเงิน ให้ผู้ขายแจ้งขอรับเงินจากดีลฟิช
8. ปลอม SMS จากดีลฟิช อ้างว่าเป็น SMS การันตีว่าเป็นลูกค้าที่เชื่อถือได้ หรือ SMS ยืนยันว่าลูกค้ารายนี้ทำการโอนเงินแล้ว ซึ่งทางดีลฟิชไม่มีบริการ SMS ดังกล่าวแต่อย่างใด

เตือนภัยมิจฉาชีพเหลี่ยมโจรต่างชาติ

-------- Original Message --------
From:Ralph Nelly <ralphnelly1@hotmail.com>
Sent:Fri, 03 Oct 2014 13:11:22 +0700
To [redacted]
Subject:GET BACK TO ME NOW

Thanks for your reply....Am Ralph Nelly from LONDON....i will like to buy this item for my client in West Africa as a gift and i will offer you 20,000Baht for the item including the shipping cost via Thailand Post - EMS SPEED POST to my client in West Africa and i will transfer the money to your bank account immediately okay..so kindly get back to me with your bank details below so that i can transfer the money to your account immediately without any delay.and also send me more pics of the item Thanks

BANK NAME.....
FULL NAME.....
ACCOUNT NUMBER.....
SWIFT CODE.....
PHONE NUMBER.....

Below is my client shipping address below:

Name: OLUSEGUN LASISI
Address: NO 50 QUEEN CINEMA ADEOLA STREET
State: OYO STATE
City:IBADAN
Zip code: 23402
Tele: 2340855676213
COUNTRY...NIGERIA.

Awaiting for your quick response

เตือนภัยมิจฉาชีพเหลี่ยมโจรต่างชาติ

จาก: "banks jane" <banksjane2020@gmail.com>
วันที่: 22 ต.ค. 2014 12:14
หัวเรื่อง: About your Tag heuer carrera300slr1887
ถึง: [redacted]
สำเนา:

Hello Kie,

Thanks for the reply.I am perfectly okay with your price for the Tag heuer watch.I saw your watch on OLX in Thailand. Actually,i am a British and a member of the NGO's for health matters,but I am presently in Africa with my husband because of our Health Organization Program which will last for about a month.This program is to create awareness to people about various diseases,its causes and remedy.This is the reason why i am making the transfer to you from my bank in London as I am originally a British.

I want to buy the watch directly from you and you will send the item to me by FedEx.I am perfectly okay with the price for this item.

I will transfer the payment directly to you in your country from my international bank account in London.

So provide me with the Price for the Tag heuer watch + FedEx Shipping Cost.

Also send me your Full Bank Details for the payment transfer to you.

Below is my Address for the shipment as soon as the payment is made and approved by the bank in London.

Name: Mrs Jane S. Banks
Address: No. 5 Purple Street,
Ikotun,Lagos 23401
Country: Nigeria
Phone: +2348071099073

Waiting for your reply with the total cost for the payment including your full bank details for the payment.Also,i want you to devalue the item when preparing the FedEx courier Invoice for the shipment so as to reduce the custom duties to be paid by me when receiving the item okay.I hope you understand.

Thanks Mrs Jane.

เตือนภัยมิจฉาชีพเหลี่ยมโจรต่างชาติ

เตือนภัยมิจฉาชีพ

ต้องแจ้งกับเจ้าหน้าที่ว่า “ขอให้เจ้าหน้าที่ดำเนินคดีจนกว่าคดีจะถึงที่สุด” อย่าแจ้งเพียงว่า แจ้งความไว้เป็นหลักฐาน (ถ้าแจ้งความไว้เป็นหลักฐานเฉยๆ เจ้าหน้าที่ตำรวจอาจเพิกเฉย เพราะถือว่าการแจ้งแบบนี้แปลว่าเจ้าทุกข์จะดำเนินการทางศาลด้วยตนเอง)

ทำอย่างไรเมื่อถูกโกง

1. บันทึกรายละเอียดของประกาศนั้น ไว้เป็นหลักฐาน โดยเซฟหน้าประกาศนั้นและ print ออกมาเป็นเอกสาร
2. เตรียมหลักฐานการโอนเงิน , เลขที่บัญชีธนาคาร , หลักฐานการติดต่อระหว่างคุณกับมิจฉาชีพ เช่น e-mail , เบอร์โทรศัพท์ หรือหมายเลขพัสดุ
3. แจ้งความกับเจ้าหน้าที่ตำรวจที่ สน.ท้องที่ที่คุณไปโอนเงิน ว่า “ถูกฉ้อโกง” เพื่อลงบันทึกประจำวัน และออกใบแจ้งความเพื่อดำเนินคดี
4. นำใบแจ้งความ ส่งให้ผู้ดูแลเว็บไซต์ เพื่อขอหมายเลข IP ของมิจฉาชีพ (หมายเลข IP สามารถใช้แกะร่องรอยและขยายผลในการจับกุมได้)
5. นำเอกสารข้อ 1-4 ส่งให้เจ้าหน้าที่ตำรวจ สน.ท้องที่ที่แจ้งความ เพื่อออกหมายจับ และพาไปจับกุมตัว หรือ ส่งให้กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (http://www.tcsd.in.th)

เตือนภัยมิจฉาชีพ

1. ก่อนทำการซื้อ-ขาย ควรขอข้อมูลจากผู้ขาย เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ อีเมล์ เลขที่บัตรประชาชน และเลขที่บัญชี พร้อมทั้ง ชื่อบัญชี ภาษาไทย + ภาษาอังกฤษ ให้ชัดเจน เพื่อนำข้อมูลเหล่านี้ไปค้นหาใน Google ดูว่ามีฟีดแบ็คจากผู้อื่นแจ้งเตือนไว้หรือไม่หากเคยมีการโกงไว้ในเว็บอื่นๆ จะเห็นผู้ซื้อคนอื่นๆ โพสต์เตือนเอาไว้ เป็นข้อมูลเล็กน้อยที่เราจะสามารถตรวจสอบได้ก่อนโอนเงิน
2. ถ้าต้องโอนเงินให้ก่อน ควรขอเบอร์โทรศัพท์บ้านของผู้ขาย และโทรเช็คว่ามีตัวตนอยู่จริง
3. กรณีอ้างว่าเป็นร้านค้า ให้ขอหลักฐาน เบอร์โทรศัพท์ของร้าน ทะเบียนการค้า หรือข้อมูลอื่นๆ ที่เป็นการยืนยันว่าเป็นร้านค้าจริง ๆ
4. ถ้าชื่อบัญชีไม่ตรงควรระวังและตรวจสอบข้อมูลจากผู้ขายโดยละเอียด ให้ขอเบอร์โทรบ้าน และโทรเช็คก่อนทุกครั้ง

*** ข้อมูลข้างต้นเป็นคำแนะนำเพื่อลดความเสี่ยงถูกโกงเท่านั้น เพราะไม่มีวิธีการใดๆ ที่จะรับรองได้ 100% ***

เตือนภัยมิจฉาชีพ

โดยแก๊งค์มิจฉาชีพอาจมีพฤติกรรมดังนี้

1. มิจฉาชีพที่ติดต่อเข้ามาจะเป็นชาวต่างชาติ (อาจอ้างว่าทำอาชีพนักธุรกิจ/ตำรวจ) ส่ง e-mail ถึงท่านเป็นภาษาอังกฤษ หรือภาษาไทยที่แปลกๆ เนื่องจากแปลจากเว็บแปลภาษา
2. หลอกสั่งสินค้าท่านในปริมาณมาก และ/หรือ จะเสนอราคาซื้อที่สูงกว่าปกติ เพื่อดึงดูดใจผู้ขาย และอาจจะอ้างว่าจะรับผิดชอบค่าส่งของเอง โดยไม่สนใจว่าค่าใช้จ่ายจะสูงแค่ไหน
3. หากเป็นสินค้าไอที หรือสินค้าชิ้นเล็ก ที่ท่านสามารถส่งได้ มิจฉาชีพจะอ้างว่าตัวเองอยู่อเมริกา อังกฤษ หรือประเทศอื่นๆ แล้วขอให้ท่านส่งสินค้าไปให้เพื่อนหรือลูกที่อยู่ประเทศไนจีเรียเป็นของขวัญ
4. หากเป็นการติดต่อซื้อขายรถยนต์ มิจฉาชีพจะอ้างว่าตัวเองอยู่ต่างประเทศ แต่จะให้ตัวแทนมาดู หรือลองขับรถ แทน หรืออาจจะอ้างว่าให้บริษัทขนส่งสินค้ามาทำการรับรถที่บ้านท่าน
5. มิจฉาชีพจะอ้างว่า จะจ่ายเงินทาง Paypal โดยใช้บัตรเครดิตที่ขโมยมา เมื่อ Paypal ตรวจสอบพบว่าเป็นบัตรที่ขโมยมา ก็จะดึงเงินท่านคืนเจ้าของบัตรตัวจริง
6. หรือมิจฉาชีพอาจจะขอเลขบัญชีธนาคารของท่าน แล้วบอกว่าจะโอนเงินมาให้ผ่านทางธนาคารต่างประเทศ จากนั้นมิจฉาชีพจะทำการส่ง e-mail ปลอมของธนาคารต่างประเทศ (ซึ่งอาจจะมีโลโก้ทำให้ท่านเชื่อถือ) เพื่อยืนยันว่าตัวเองได้ทำการโอนเงินมาให้ท่านเรียบร้อยแล้ว แต่มิจฉาชีพจะอ้างว่า ท่านต้องทำการส่งของมาก่อน เพื่อนำ Tracking Number รายละเอียดการส่งของไปยืนยันกับธนาคาร ธนาคารจึงจะโอนเงินเข้าบัญชีให้ท่าน
7. หากท่านบอกรายละเอียดเลขที่บัญชีแก่มิจฉาชีพไปแล้ว แต่ยังไม่ได้ส่งของ มิจฉาชีพจะอ้างว่าได้ทำการแจ้งตำรวจ หรือ FBI หรือหน่วยงานอื่นๆ เพื่อทำการขู่ให้ท่านส่งของไปให้
8. ดังนั้น เพื่อความปลอดภัย ท่านไม่ควรบอกเลขที่บัญชีหรือข้อมูลส่วนตัวใดๆทั้งสิ้น

เตือนภัยมิจฉาชีพ

ระวังหลักฐานโอนเงินปลอม

สำหรับผู้ลงขายสินค้าอย่าชะล่าใจเมื่อได้เห็นสลิปการโอนเงินที่ผู้ซื้อส่งมาเป็นหลักฐาน เพราะกลโกงใหม่ล่าสุดของมิจฉาชีพคือการปลอมหลักฐานการโอนเงิน หรือสลิปการโอนนั่นเอง โดยมิจฉาชีพมักจะเลือกผู้ขายที่ขายสินค้าหลายชนิด หรือมีช่องทางการขายหลากหลายช่องทาง จากนั้นจะใช้โปรแกรมด้านกราฟฟิกตัดต่อภาพให้ออกมาเสมือนว่าเป็นสลิปจริงๆ แต่ไม่มีการโอนเงินเข้าบัญชีผู้ขายจริง

หากผู้ขายตรวจสอบเพียงสลิปการโอนเงิน แล้วจัดส่งของไปให้ ท่านก็จะเสียทรัพย์ไปฟรีๆ

ปัญหานี้ป้องกันได้!

ไม่ว่าท่านจะเป็นผู้ขายรายใหญ่ หรือรายย่อย เมื่อผู้ซื้อแจ้งว่าชำระเงินแล้ว ท่านควรตรวจสอบบัญชีธนาคารของท่านว่ามีเงินจำนวนดังกล่าวเข้ามาจริง ตรงตามที่ผู้ซื้อแจ้งมาหรือไม่ เสียเวลานิดหน่อย แต่ไม่เสียรู้ และไม่เสียทรัพย์ให้เจ็บใจด้วย

ในการป้องกันบัญชี Gmail, Outlook และ Yahoo จากการถูกแฮกด้วยวิธีง่าย ๆ

1. ตั้งค่าให้มีการยืนยันแบบ 2 ขั้นตอน (2-step verification) การยืนยันแบบ 2 ขั้นตอนเป็นวิธีการ พิสูจน์ตัวตนที่ต้องใช้ข้อมูล 2 ส่วน ร่วมกัน เพื่อเพิ่มความมั่นคงปลอดภัยให้กับการเข้า สู่ระบบหรือบริการ โดยหลัก ๆ แล้วจะใช้ ข้อมูลจาก 2 ใน 3 ส่วนนี้คือ

1. สิ่งที่รู้ (Something you know) เช่น รหัสผ่าน
2. สิ่งที่มี (Something you have) เช่น โทรศัพท์มือถือ, รหัสบัตร เติมเงิน
3. สิ่งที่เป็น (Something you are) เช่น ลายนิ้วมือ, ม่านตา

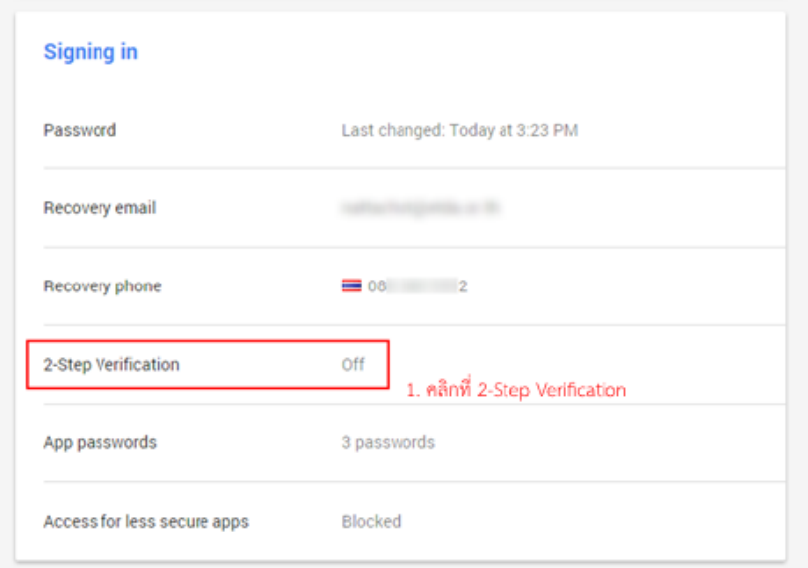
การยืนยันแบบ 2 ขั้นตอนช่วยลดโอกาสในการถูกขโมยข้อมูลส่วนตัวในบัญชีอีเมลของเราลงได้

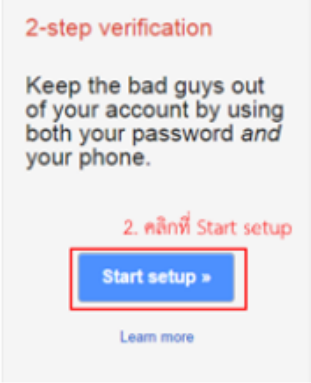
2. การตรวจสอบประวัติ การใช้งานหรือการตั้งค่าที่น่าสงสัยอย่างสม่ำเสมอ ผู้ใช้งานควรตรวจสอบว่ามีผู้ไม่หวังดี แอบเข้ามาล็อกอินใช้บัญชีของเราหรือไม่ จากประวัติการใช้งาน โดยอาจสังเกตความ ผิดปกติจากช่วงเวลาหรือประเทศที่พบการใช้งาน เช่น พบการล็อกอิน ณ เวลาเที่ยง คืน จากต่างประเทศ นอกจากนี้ก็ควรตรวจสอบว่าผู้ไม่ หวังดีเปลี่ยนค่าต่าง ๆ อาจเพิ่มอีเมลหรือหมายเลขโทรศัพท์ที่ใช้ในการยืนยันตัวตน เพื่อแอบล็อกอินเข้ามาขโมยข้อมูล หากผู้ใช้ งานพบความผิดปกติ ควรเปลี่ยนช่องทางในการเข้าถึงบัญชี เช่น รหัสผ่าน หมายเลข โทรศัพท์ อีเมลสำหรับกู้คืนบัญชี รวมถึง เพิกถอนรหัสเฉพาะสำหรับแอปพลิเคชัน สิทธิการเข้าถึงข้อมูลของแอปพลิเคชัน ต่าง ๆ และอุปกรณ์ที่อยู่ในรายการ Trusted Device ซึ่งเป็นรายการอุปกรณ์ ที่ผู้ใช้ไว้ใจ ไม่จำเป็นต้องใส่รหัสผ่านที่ 2 ในการล็อกอิน สำหรับรายละเอียดใน การตรวจสอบประวัติการใช้งานและการตั้งค่าที่น่าสงสัยนั้น

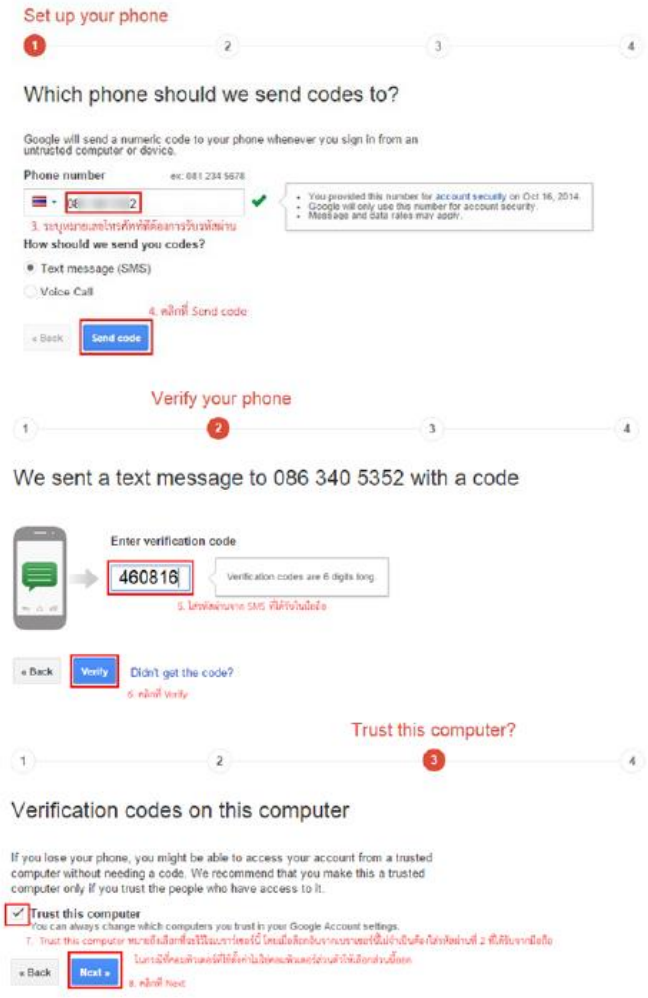
3. ข้อควรระวังในการเข้าใช้งานจากเครื่องคอมพิวเตอร์สาธารณะ

4. การตั้งรหัสผ่านที่ทำให้คาดเดาได้ยาก

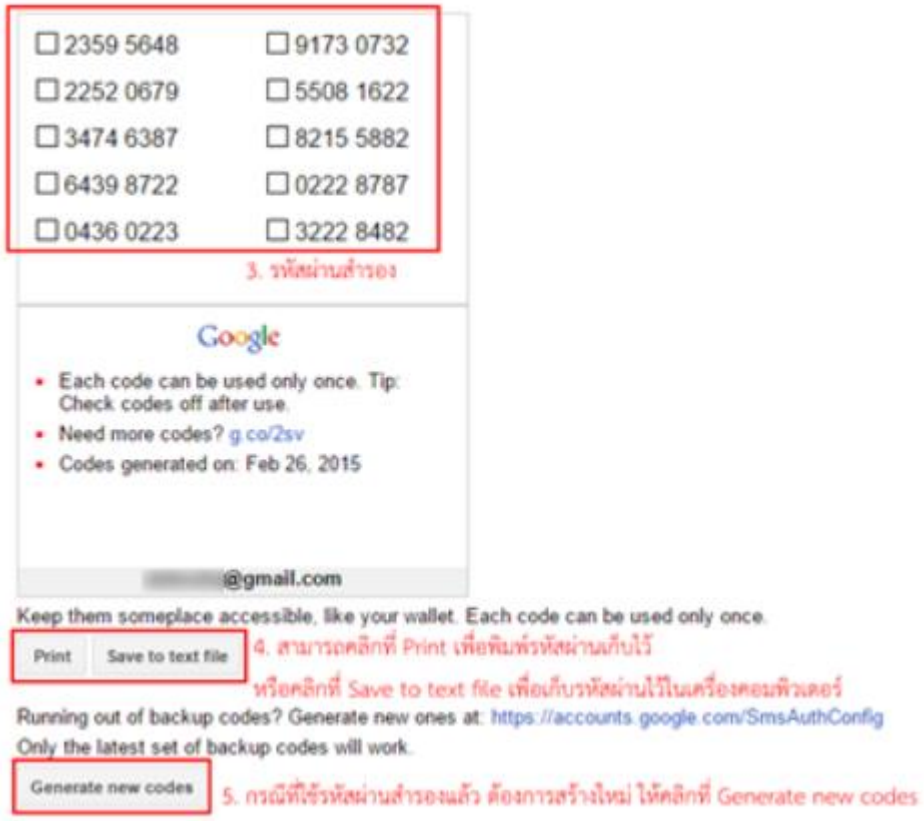
ในการป้องกันบัญชี Gmail, Outlook และ Yahoo จากการถูกแฮกด้วยวิธีง่าย ๆ







ในการป้องกันบัญชี Gmail, Outlook และ Yahoo จากการถูกแฮกด้วยวิธีง่าย ๆ



เตือนภัยอีเมลหลอกลวงสำหรับผู้ซื้อขายออนไลน์

เตือนภัยอีเมลหลอกลวงสำหรับผู้ซื้อขายออนไลน์

อีเมลที่ใช้ติดต่อธุรกิจถือเป็นทรัพย์สินสำคัญที่ต้องมีมาตรการรักษาความมั่นคงปลอดภัย เพราะถ้าถูกผู้ไม่หวังดีเข้าถึงหรือยึดอีเมลได้ ก็จะใช้แอบอ้างเพื่อทำธุรกรรมต่างๆ แทนเรา สร้างความเสียหายทั้งเงินและชื่อเสียงอีกด้วย

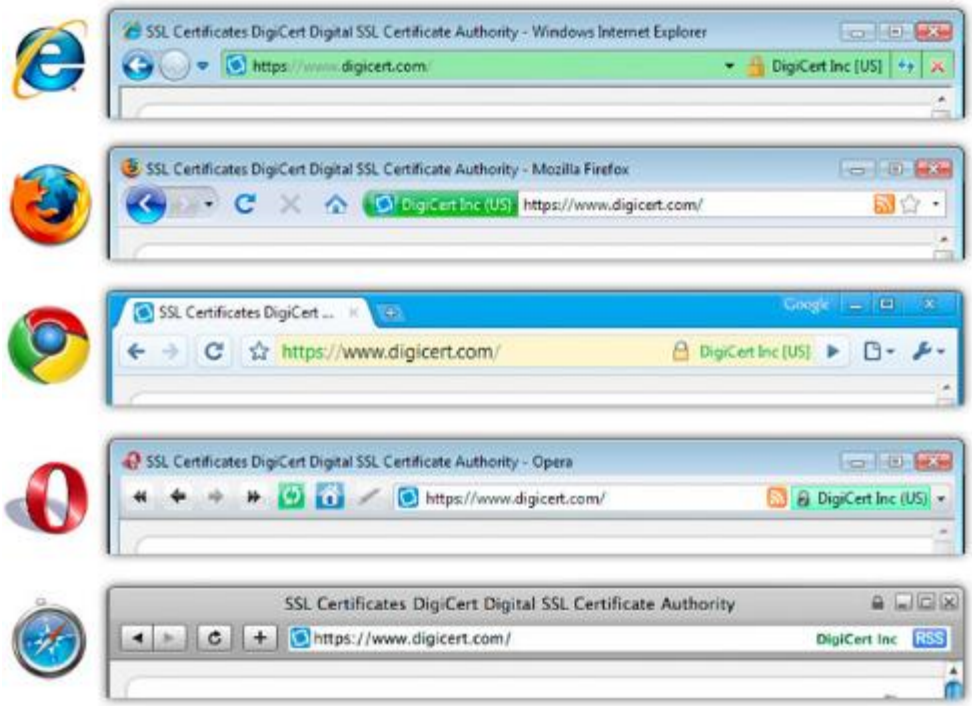
ชำระเงินออนไลน์อุ่นใจ ต้องรู้จักคำว่า “PHISHING”

ชำระเงินออนไลน์อุ่นใจ ต้องรู้จักคำว่า “PHISHING”

ทุกวันนี้ ธนาคารส่วนใหญ่ได้ให้บริการการทำธุรกรรมผ่านอินเทอร์เน็ต หรือที่เรียกว่า “Internet Banking” ที่ทำให้ผู้ซื้อสามารถโอนเงินหรือจ่ายเงินอย่างง่ายดาย โดยไม่จำเป็นต้องไปที่ธนาคารจริงๆ

ชำระเงินออนไลน์อุ่นใจ ต้องรู้จักคำว่า “PHISHING”

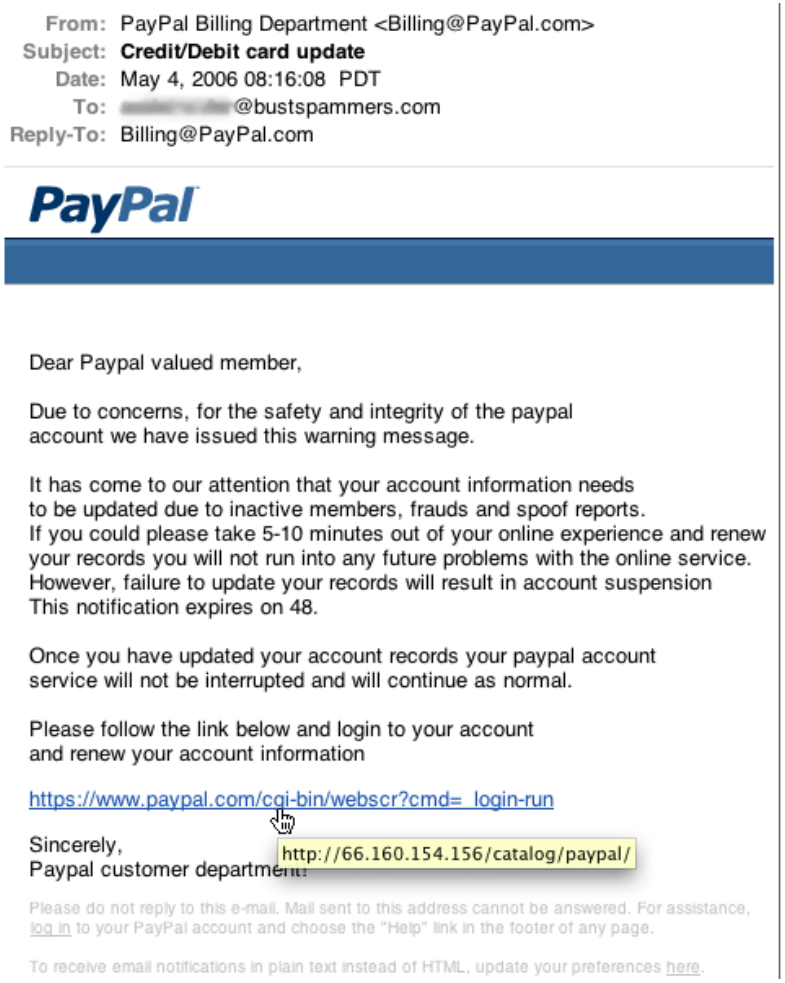
1. พิจารณาว่าเว็บไซต์ที่ใช้บริการนั้นมีการเข้ารหัส เช่น รหัส Secure Sockets Layer หรือ SSL ซึ่งนำข้อมูลมาเข้ารหัสพิเศษ
2. จำกัดวงเงินการโอนหรือการจ่ายค่าสินค้า
3. ระวังเว็บไซต์ประเภทฟิชชิ่ง (Phishing) ซึ่งเป็นกลวิธีในการหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลส่วนตัว อันจะนำไปสู่การแสวงหาผลประโยชน์ที่อาจก่อให้เกิดความเดือดร้อนแก่ผู้ที่ถูกล่อลวง ข้อมูลส่วนตัวนั้นมักจะเป็นรหัสประจำตัวต่างๆ Password เลขที่บัตรเครดิต เลขที่บัญชี หรือเลขที่บัตรประชาชน



ชำระเงินออนไลน์อุ่นใจ ต้องรู้จักคำว่า “PHISHING”

3. ระวังเว็บไซต์ประเภทฟิชชิ่ง (Phishing) ปลอมแปลงลักษณะของอีเมล

เหมือนส่งมาโดยธนาคาร สถาบันการเงิน หรือบริษัทห้างร้านที่มีชื่อเสียง ซึ่งมักมีเครื่องหมายการค้า สี และรูปแบบอีเมลเหมือนส่งมาจากบริษัทดังกล่าว โดยเนื้อหาของอีเมล จะเป็นการบอกให้ผู้ใช้บริการดำเนินการอย่างใดอย่างหนึ่ง ซึ่งที่พบได้มากคือการหลอกให้คลิกลิงก์ที่อยู่ในอีเมล เพื่อทำการกรอกข้อมูลต่างๆ ผู้ใช้บริการอาจได้รับข้อความในเชิงเตือน หรือข่มขู่ เช่น “หากไม่ดำเนินการภายใน 15 วัน ทางบริษัทมีความจำเป็นต้องปิดบริการของท่าน”



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

PayPal

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

http://66.160.154.156/catalog/paypal/

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.

To receive email notifications in plain text instead of HTML, update your preferences here.

ชำระเงินออนไลน์อุ่นใจ ต้องรู้จักคำว่า “PHISHING”

3. ระวังเว็บไซต์ประเภทฟิชชิ่ง (Phishing)

สร้างเว็บไซต์เลียนแบบ

ผู้ทำการ Phishing ได้ทราบข้อมูลรหัสประจำตัว และ Password ครบแล้ว ก็จะนำข้อมูลดังกล่าวไปทำธุรกรรมทางการเงิน เช่น โอนเงินไปยังบัญชีปลายทาง ซึ่งเปิดขึ้นเพื่อรอรับเงินที่ได้มาด้วยวิธีการทุจริตนี้ จากนั้นคนร้ายจะไปถอนเงินออกจากบัญชี หรือนำไปซื้อสิ่งของจนหมด

แอบอ้างเป็นพนักงาน หรือเจ้าหน้าที่ในหน่วยงานราชการ ธนาคาร หรือบริษัทต่างๆ ทางโทรศัพท์ โดยแจ้งให้ลูกค้าทำการโอนเงินทาง ATM ไปยังบัญชีปลายทางซึ่งเปิดเอาไว้โดยกลุ่มบุคคลทุจริตนั่นเอง หรือบางครั้งอาจใช้วิธีหลอกถามข้อมูลส่วนตัว ซึ่งสามารถนำไปใช้ในภายหลัง เพื่อย้อนกลับมาโจมตีบัญชีของลูกค้าเองอีกครั้ง ในประเทศไทยนั้น การ Phishing ทางโทรศัพท์เป็นวิธีที่พบบ่อยที่สุด เนื่องจากคนบางส่วนยังไม่มีความรู้ในการใช้ธนาคารออนไลน์ ทำให้เป็นเป้าหมายที่โดนโจมตีแล้วได้ผล

วิธีหลีกเลี่ยงไม่ให้ตกเป็นเหยื่อของ Phishing

1. **ระมัดระวังไม่หลงเชื่อข้อความใดๆ ในอีเมล หรือโทรศัพท์ที่ได้รับ** หากมีการอ้างว่าส่งอีเมลหรือติดต่อมาจากสถาบันหรือบริษัทใดก็ตาม ควรค้นหาหมายเลขโทรศัพท์ของสถาบัน หรือบริษัทนั้น หรือติดต่อไปยัง Call Center ของบริษัทนั้นๆ โดยไม่ต้องติดต่อไปตามหมายเลขโทรศัพท์ที่มีอยู่ในอีเมลต้องสงสัยฉบับนั้น เพื่อตรวจสอบว่ามีการส่งอีเมลลักษณะดังกล่าวจริงหรือไม่
2. **ไม่คลิกลิงก์ในอีเมลเพื่อการเข้าสู่หน้าเว็บไซต์ ให้ใช้วิธีพิมพ์ URL เข้าสู่เว็บไซต์ของบริษัทดังกล่าวด้วยตัวเอง** เพื่อป้องกันไม่ให้เผลอคลิกเข้าสู่เว็บไซต์ปลอมที่กลุ่มผู้ร้ายได้เตรียมไว้
3. **ไม่เปิดเผยข้อมูลส่วนบุคคล** เช่น หมายเลขบัตรประชาชน บัตรเครดิต เลขที่บัญชี รหัส ATM แก่คนอื่นผ่านทางอีเมล โดยหมั่นตรวจสอบข้อมูลการทำรายการธุรกรรมของตนเองอย่างสม่ำเสมอ โดยไม่จำเป็นต้องรอให้ครบ 1 เดือน ตรวจสอบใบแจ้งรายการใช้บัตรเครดิตทุกครั้งที่ได้รับ และตรวจสอบให้แน่ใจว่าไม่มีรายการธุรกรรมแปลกปลอม หากพบรายการที่น่าสงสัยให้ติดต่อธนาคารหรือบริษัทผู้ออกบัตรทันที
4. **กำหนด Password ที่มีความมั่นคงปลอดภัย** ธนาคารพาณิชย์ชั้นนำที่ให้บริการธนาคารออนไลน์ต่างตระหนักถึงความมั่นคงปลอดภัยโดยการเพิ่มมาตรการความมั่นคงปลอดภัย ไม่ว่าจะเป็นการติดตั้งระบบตรวจจับการเจาะข้อมูล และติดตั้งระบบความมั่นคงปลอดภัย 2 ชั้นแล้วก็ตาม ก็ยังมีปัจจัยภายนอกที่ธนาคารไม่สามารถควบคุมได้ นั่นก็คือความมั่นคงปลอดภัยในส่วนที่ขึ้นอยู่กับตัวผู้ใช้บริการ ที่บ้านหรือที่ทำงาน เนื่องจากผู้ใช้จำนวนไม่น้อยยังไม่ได้ให้ความสำคัญในการเรียนรู้เกี่ยวกับการใช้ประโยชน์ของ Password , ไม่ควรเลือกฟังก์ชั่นจำ Password อัตโนมัติ , หมั่นเปลี่ยน Password, ไม่เขียน Password ไว้บนกระดาษและแปะไว้ตามที่ต่างๆ, ไม่ควรใช้ Password เดียว ทั้งการเข้าอีเมล การใช้บริการธนาคารออนไลน์ และอื่นๆ

เล่น **Social Network** ให้ปลอดภัย “รู้” ไว้เลี่ยงอันตราย

ผู้ใช้งาน Social Network มีโอกาสเผยแพร่ข้อมูลได้ง่าย รวมทั้งทุกคนสามารถใช้งานได้ ก็ทำให้ข้อมูลใน Social Network อาจจะเป็นข้อมูลที่ไม่ถูกต้อง อีกทั้งมีโอกาสที่จะสูญเสียความเป็นส่วนตัวไปได้

SME มือใหม่ ระวังภัยออนไลน์

1. ทรัพย์สินออนไลน์ ต้องรักษาไม่ต่างกับทรัพย์สินในโลกจริง
2. การติดต่อกับคนแปลกหน้า ถือเป็นเรื่องใหญ่ที่สุด
3. ระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนที่จะส่งให้ และโปรดระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรม Internet Messaging หรือช่องทาง Social Media ทั้งนี้เพื่อหลีกเลี่ยงการติดมัลแวร์ เนื่องจากหลายครั้งพบว่ามัลแวร์มักจะถูกส่งมากับไฟล์แนบหรือจากเว็บไซต์ที่ไม่เหมาะสม
4. ตั้งรหัสตามมาตรฐาน และจัดเก็บมิดชิด และตั้ง Pin Code / Passcode อุปกรณ์มือถือ
5. ติดตั้งโปรแกรมป้องกันอันตรายจาก Malware ย่อมาจาก Malicious Software เป็นคำรวมๆ ที่ใช้เรียกโปรแกรมที่มีจุดประสงค์ร้าย มุ่งโจมตีหรือก่อกวนการทำงานของผู้ใช้อื่นหรือระบบอื่น Malware ได้แก่ ไวรัส (Virus), หนอน (Worm), โทรจัน (Trojan), สปายแวร์ (Spyware) ฯลฯ
6. ระมัดระวังการเปิดอีเมล์หรือไฟล์จากสื่อบันทึกข้อมูลต่างๆ โดยเฉพาะที่มาจากคนที่ไม่รู้จัก
7. ระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนที่จะส่งให้ และโปรดระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรม Internet Messaging หรือช่องทาง Social Media ทั้งนี้เพื่อหลีกเลี่ยงการติดมัลแวร์ เนื่องจากหลายครั้งพบว่ามัลแวร์มักจะถูกส่งมากับไฟล์แนบหรือจากเว็บไซต์ที่ไม่เหมาะสม
8. หลีกเลี่ยงการใช้แผ่นดิสก์ ซีดี ทรัมบ์ไดรว์ จากแหล่งไม่น่าเชื่อถือ หรือไม่ใช้ร่วมกับบุคคลอื่น ควรมีการตรวจเช็คไวรัสและโปรแกรมอันตรายก่อนใช้งานทุกครั้ง
9. ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และพิจารณาข้อมูลก่อนการแชร์ต่อ ตลอดจนไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง
10. ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป็อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดย

SME มือใหม่ ระวังภัยออนไลน์

11. ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสม หรือผิดกฎหมาย
12. เก็บล็อก ต้องทำตามกฎหมาย
13. สำรองข้อมูลเป็นประจำ
14. Wi-Fi ต้องเข้ารหัสเท่านั้น
15. ป้องกันข้อมูลสูญหาย
16. ช่องโหว่ซอฟต์แวร์ ภัยที่ต้องการการดูแลอย่างต่อเนื่อง ต้องอัพเดทแพต
17. ตรวจสอบซอฟต์แวร์และฮาร์ดแวร์ที่ติดตั้งในเครื่อง
18. ระบบให้สิทธิเข้าถึง
19. ระบบสำรอง
20. นโยบายความปลอดภัยและความตระหนักของพนักงาน

SME มือใหม่ ระวังภัยออนไลน์

อาการที่แสดงว่าเครื่องอาจโดนโปรแกรมอันตราย

1. ใช้เวลานานผิดปกติในการเปิดเครื่อง หรือเรียกโปรแกรมขึ้นมาทำงาน
2. ขนาดของโปรแกรม หรือ วันเวลาของโปรแกรมเปลี่ยนไป
3. ข้อความที่ปกติไม่ค่อยได้เห็นกลับถูกแสดงขึ้นมาบ่อย ๆ
4. เกิดอักษรหรือข้อความประหลาดบนหน้าจอ
5. เครื่องส่งเสียงออกทางลำโพงโดยไม่ได้เกิดจากโปรแกรมที่ใช้งานอยู่
6. แป้นพิมพ์ทำงานผิดปกติหรือไม่ทำงานเลย
7. ไฟแสดงสถานะการทำงานของดิสก์ติดค้างนานกว่าที่เคยเป็น
8. ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้งานสูญหายไป
9. เครื่องบูทตัวเองโดยไม่ได้สั่ง หรือ หยุดทำงานโดยไม่ทราบสาเหตุ
10. มีหน้าต่างปรากฏขึ้นมาบ่อยครั้งที่เปิดดูเว็บไซต์
11. ทูลบาร์ (tools bar)แถบปุ่มเครื่องมือเพิ่มขึ้น
12. หน้าจอมีไอคอน (icon) ประหลาดๆ เพิ่มขึ้น
13. เมื่อเปิดเว็บเบราเซอร์ หน้าเว็บแรกที่ปรากฏจะเป็นเว็บที่ไม่เคยเห็นมาก่อน
14. สร้างความรำคาญ โดยการเปิดหน้าเว็บโฆษณาอยู่ตลอดเวลา

สำหรับหน่วยงานราชการ

ปฏิบัติตามนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด โดยมีรายการดังต่อไปนี้เป็นอย่างน้อย ดังนี้

- นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
- พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
- พ.ร.บ. ลิขสิทธิ์


ประกอบธุรกิจอย่างไรไม่ให้ถูกหลอกลวงจากอาชญากรรมทางคอมพิวเตอร์
กรณีอาชญากรรมทางคอมพิวเตอร์ในรูปแบบ fake e-mail
วันพฤหัสบดีที่ 8 กันยายน 2559 เวลา 08.30-16.00 น.
ณ โรงแรมอมารี ดอนเมือง แอร์พอร์ต ถนนวิภาวดีรังสิต กรุงเทพมหานคร
FAKE

ขอบคุณครับ