Security Awareness

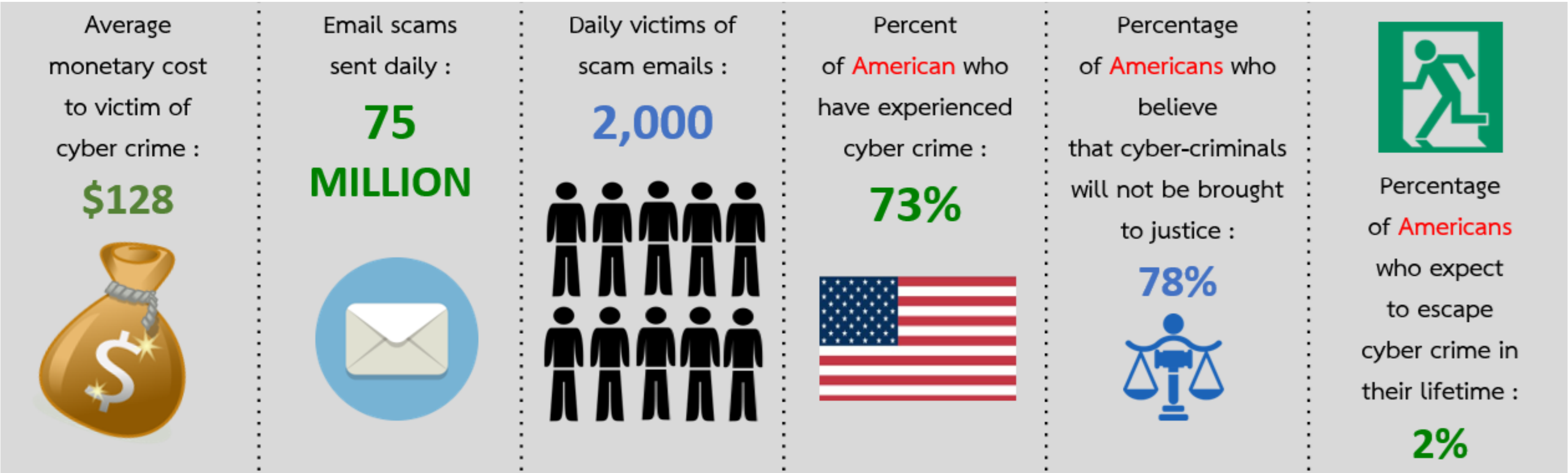
For General User

By Mahutthawat Raksakiettisak
System & Network Specialist

Topic for today

- Intro to Cyber threats
- You Are A Target
- Social Engineering
- System Security
- Basic Identification
- E-mail & Social login
- Enable 2fa
- 10 วิธีการ shopping online อย่างปลอดภัย

Cyber crime statistics



Average monetary cost to victim of cyber crime : $128

Email scams sent daily : 75 MILLION

Daily victims of scam emails : 2,000

Percent of American who have experienced cyber crime : 73%

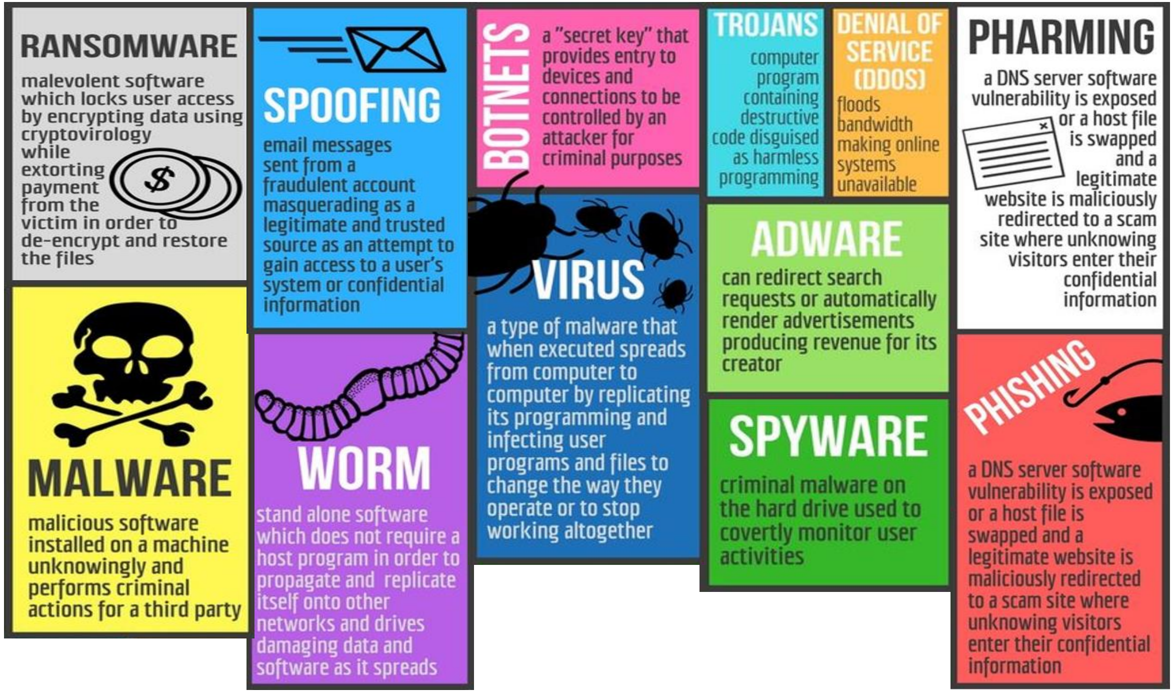
Percentage of Americans who believe that cyber-criminals will not be brought to justice : 78%

Percentage of Americans who expect to escape cyber crime in their lifetime : 2%

https://www.pinterest.com/pin/276197389633759142/

COMMON CYBER THREATS

Cyber threats are in the headlines and possibly in your network.
Here are some common forms of cyber threats to protect against



RANSOMWARE
malevolent software which locks user access by encrypting data using cryptovirology while extorting payment from the victim in order to de-encrypt and restore the files

MALWARE
malicious software installed on a machine unknowingly and performs criminal actions for a third party

SPOOFING
email messages sent from a fraudulent account masquerading as a legitimate and trusted source as an attempt to gain access to a user's system or confidential information

WORM
stand alone software which does not require a host program in order to propagate and replicate itself onto other networks and drives damaging data and software as it spreads

BOTNETS
a "secret key" that provides entry to devices and connections to be controlled by an attacker for criminal purposes

VIRUS
a type of malware that when executed spreads from computer to computer by replicating its programming and infecting user programs and files to change the way they operate or to stop working altogether

TROJANS
computer program containing destructive code disguised as harmless programming

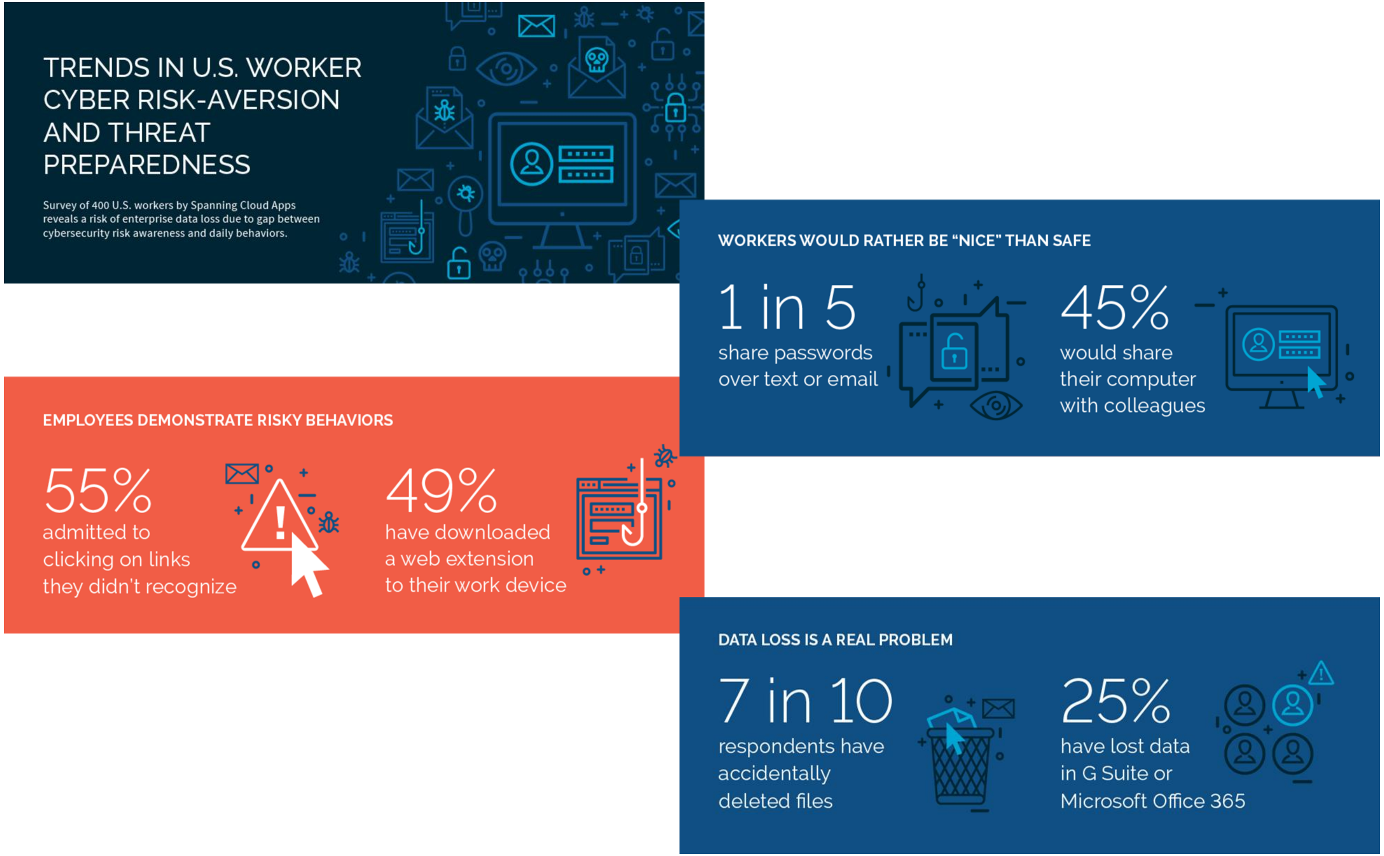
DENIAL OF SERVICE (DDOS)
floods bandwidth making online systems unavailable

ADWARE
can redirect search requests or automatically render advertisements producing revenue for its creator

SPYWARE
criminal malware on the hard drive used to covertly monitor user activities

PHARMING
a DNS server software vulnerability is exposed or a host file is swapped and a legitimate website is maliciously redirected to a scam site where unknowing visitors enter their confidential information

PHISHING
a DNS server software vulnerability is exposed or a host file is swapped and a legitimate website is maliciously redirected to a scam site where unknowing visitors enter their confidential information



TRENDS IN U.S. WORKER CYBER RISK-AVERSION AND THREAT PREPAREDNESS

Survey of 400 U.S. workers by Spanning Cloud Apps reveals a risk of enterprise data loss due to gap between cybersecurity risk awareness and daily behaviors.

EMPLOYEES DEMONSTRATE RISKY BEHAVIORS

55% admitted to clicking on links they didn't recognize

49% have downloaded a web extension to their work device

WORKERS WOULD RATHER BE "NICE" THAN SAFE

1 in 5 share passwords over text or email

45% would share their computer with colleagues

DATA LOSS IS A REAL PROBLEM

7 in 10 respondents have accidentally deleted files

25% have lost data in G Suite or Microsoft Office 365

https://www.business2community.com/infographics/employees-are-cyber-secure-in-theory-but-not-in-practice-infographic-02167513

You are a Target ‼

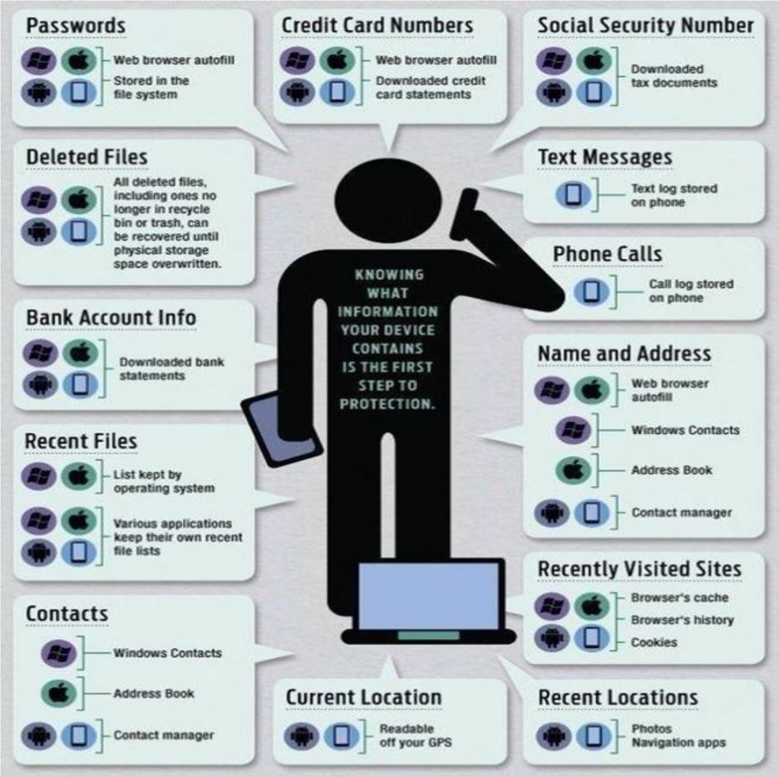
You are a target!!

- เรามีอะไร
- ทำไมต้องมา hack เรา
- เราไม่ได้มีเงินใน ธนาคารเยอะจะมา hack ไปทำอะไร
- เราไม่มีข้อมูลอะไร

What do your devices know about you?

Whether it's a computer on your desk or a phone in your pocket, your devices retain a lot of personal data. And all of that information may be vulnerable to cybercriminals.

- WINDOWS PCs
- MACS
- ANDROID TABLETS
- SMART PHONES



Passwords
Web browser autofill
Stored in the file system

Credit Card Numbers
Web browser autofill
Downloaded credit card statements

Social Security Number
Downloaded tax documents

Deleted Files
All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.

Text Messages
Text log stored on phone

Phone Calls
Call log stored on phone

Bank Account Info
Downloaded bank statements

KNOWING WHAT INFORMATION YOUR DEVICE CONTAINS IS THE FIRST STEP TO PROTECTION.

Name and Address
Web browser autofill
Windows Contacts
Address Book
Contact manager

Recent Files
List kept by operating system
Various applications keep their own recent file lists

Recently Visited Sites
Browser's cache
Browser's history
Cookies

Contacts
Windows Contacts
Address Book
Contact manager

Current Location
Readable off your GPS

Recent Locations
Photos
Navigation apps

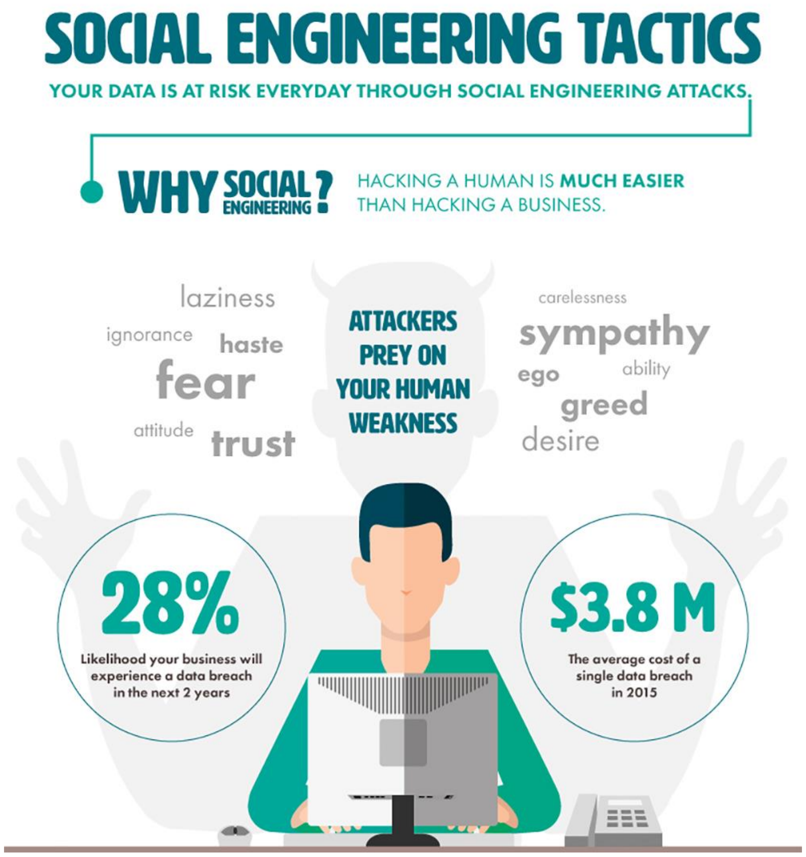
https://www.pinterest.com/pin/276197389633759142/

Social Engineering

Social Engineering

https://smejoinup.com/what-is-social-engineering-attacks-how-to-prevent-an-attack/

Social Engineering



SOCIAL ENGINEERING TACTICS

YOUR DATA IS AT RISK EVERYDAY THROUGH SOCIAL ENGINEERING ATTACKS.

WHY SOCIAL ENGINEERING? HACKING A HUMAN IS **MUCH EASIER** THAN HACKING A BUSINESS.

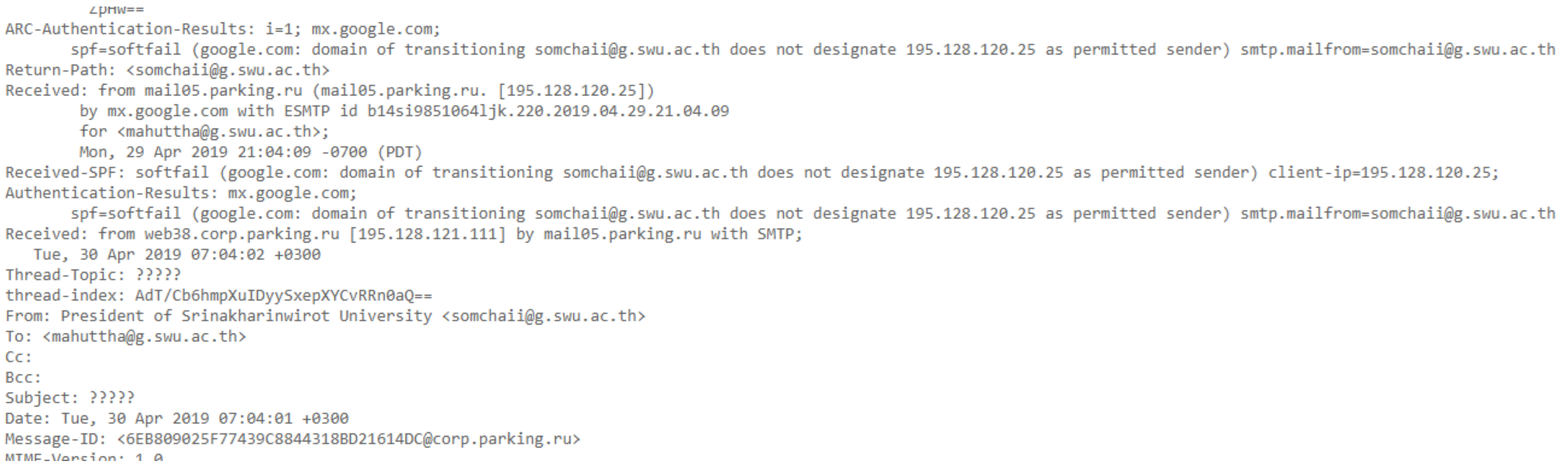
ATTACKERS PREY ON YOUR HUMAN WEAKNESS

28% Likelihood your business will experience a data breach in the next 2 years

$3.8 M The average cost of a single data breach in 2015

https://smejoinup.com/what-is-social-engineering-attacks-how-to-prevent-an-attack/

Social Engineering ในสถานการณ์ต่างๆ



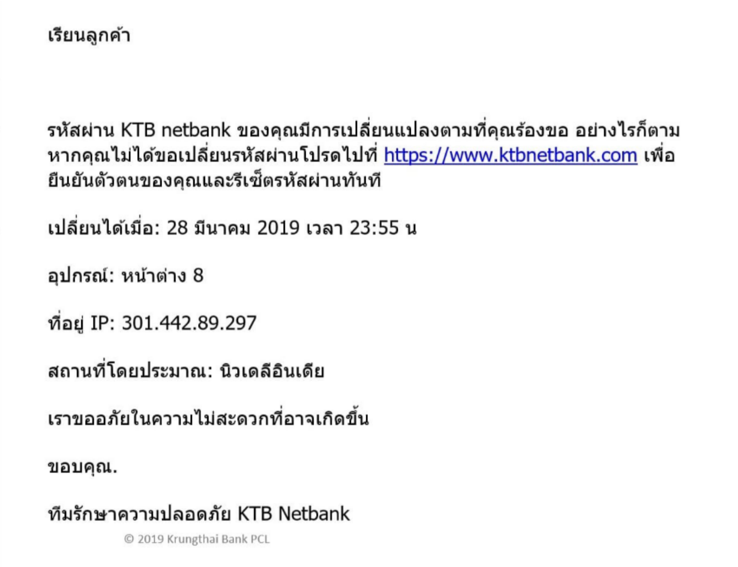
```
         ZpHw==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=softfail (google.com: domain of transitioning somchaii@g.swu.ac.th does not designate 195.128.120.25 as permitted sender) smtp.mailfrom=somchaii@g.swu.ac.th
Return-Path: <somchaii@g.swu.ac.th>
Received: from mail05.parking.ru (mail05.parking.ru. [195.128.120.25])
        by mx.google.com with ESMTP id b14si9851064ljk.220.2019.04.29.21.04.09
        for <mahuttha@g.swu.ac.th>;
        Mon, 29 Apr 2019 21:04:09 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning somchaii@g.swu.ac.th does not designate 195.128.120.25 as permitted sender) client-ip=195.128.120.25;
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning somchaii@g.swu.ac.th does not designate 195.128.120.25 as permitted sender) smtp.mailfrom=somchaii@g.swu.ac.th
Received: from web38.corp.parking.ru [195.128.121.111] by mail05.parking.ru with SMTP;
   Tue, 30 Apr 2019 07:04:02 +0300
Thread-Topic: ?????
thread-index: AdT/Cb6hmpXuIDyySxepXYCvRRn0aQ==
From: President of Srinakharinwirot University <somchaii@g.swu.ac.th>
To: <mahuttha@g.swu.ac.th>
Cc:
Bcc:
Subject: ?????
Date: Tue, 30 Apr 2019 07:04:01 +0300
Message-ID: <6EB809025F77439C8844318BD21614DC@corp.parking.ru>
MIME-Version: 1.0
```

Social Engineering ในสถานการณ์ต่างๆ

Download file document music from website with malicious virus attach it.

Contain some link from friend E-mail.

Phishing Scam



เรียนลูกค้า

รหัสผ่าน KTB netbank ของคุณมีการเปลี่ยนแปลงตามที่คุณร้องขอ อย่างไรก็ตาม หากคุณไม่ได้ขอเปลี่ยนรหัสผ่านโปรดไปที่ https://www.ktbnetbank.com เพื่อยืนยันตัวตนของคุณและรีเซ็ตรหัสผ่านทันที

เปลี่ยนได้เมื่อ: 28 มีนาคม 2019 เวลา 23:55 น

อุปกรณ์: หน้าต่าง 8

ที่อยู่ IP: 301.442.89.297

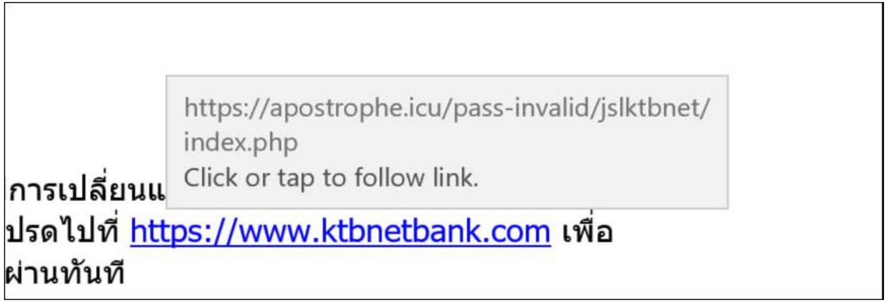
สถานที่โดยประมาณ: นิวเดลีอินเดีย

เราขออภัยในความไม่สะดวกที่อาจเกิดขึ้น

ขอบคุณ.

ทีมรักษาความปลอดภัย KTB Netbank

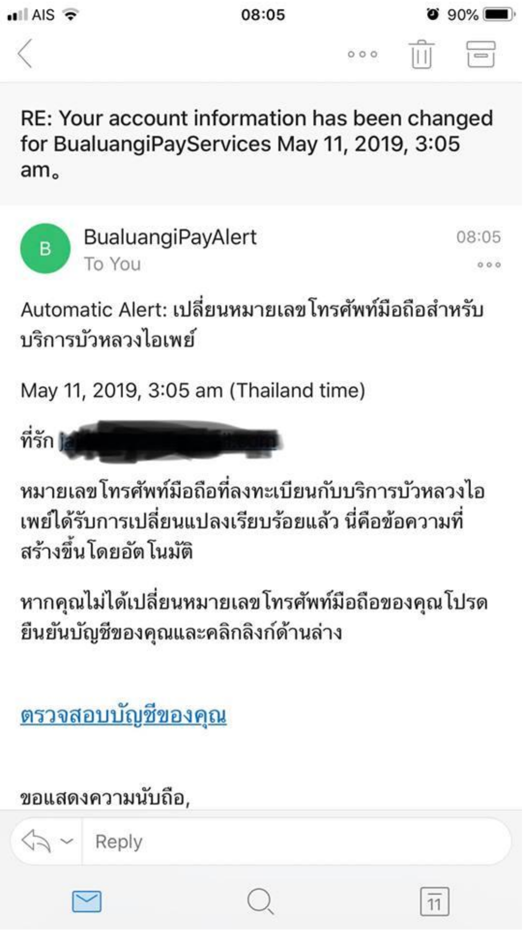
© 2019 Krungthai Bank PCL



https://apostrophe.icu/pass-invalid/jslktbnet/index.php
Click or tap to follow link.

การเปลี่ยนแ
ปรดไปที่ https://www.ktbnetbank.com เพื่อ
ผ่านทันที

Phishing Scam



RE: Your account information has been changed for BualuangiPayServices May 11, 2019, 3:05 am。

BualuangiPayAlert 08:05
To You

Automatic Alert: เปลี่ยนหมายเลขโทรศัพท์มือถือสำหรับบริการบัวหลวงไอเพย์

May 11, 2019, 3:05 am (Thailand time)

ที่รัก [redacted]

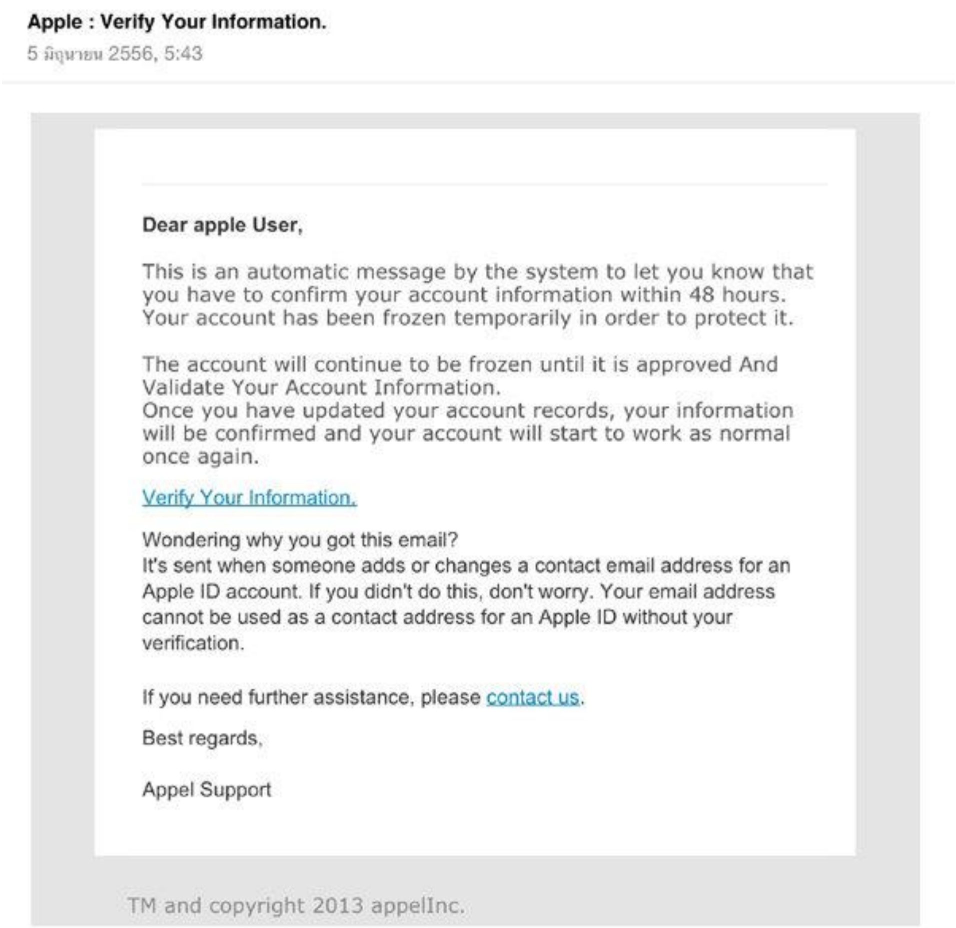
หมายเลขโทรศัพท์มือถือที่ลงทะเบียนกับบริการบัวหลวงไอเพย์ได้รับการเปลี่ยนแปลงเรียบร้อยแล้ว นี่คือข้อความที่สร้างขึ้นโดยอัตโนมัติ

หากคุณไม่ได้เปลี่ยนหมายเลขโทรศัพท์มือถือของคุณโปรดยืนยันบัญชีของคุณและคลิกลิงก์ด้านล่าง

ตรวจสอบบัญชีของคุณ

ขอแสดงความนับถือ,

Phishing Scam



Apple : Verify Your Information.

5 มิถุนายน 2556, 5:43

Dear apple User,

This is an automatic message by the system to let you know that you have to confirm your account information within 48 hours. Your account has been frozen temporarily in order to protect it.

The account will continue to be frozen until it is approved And Validate Your Account Information.
Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.

Verify Your Information.

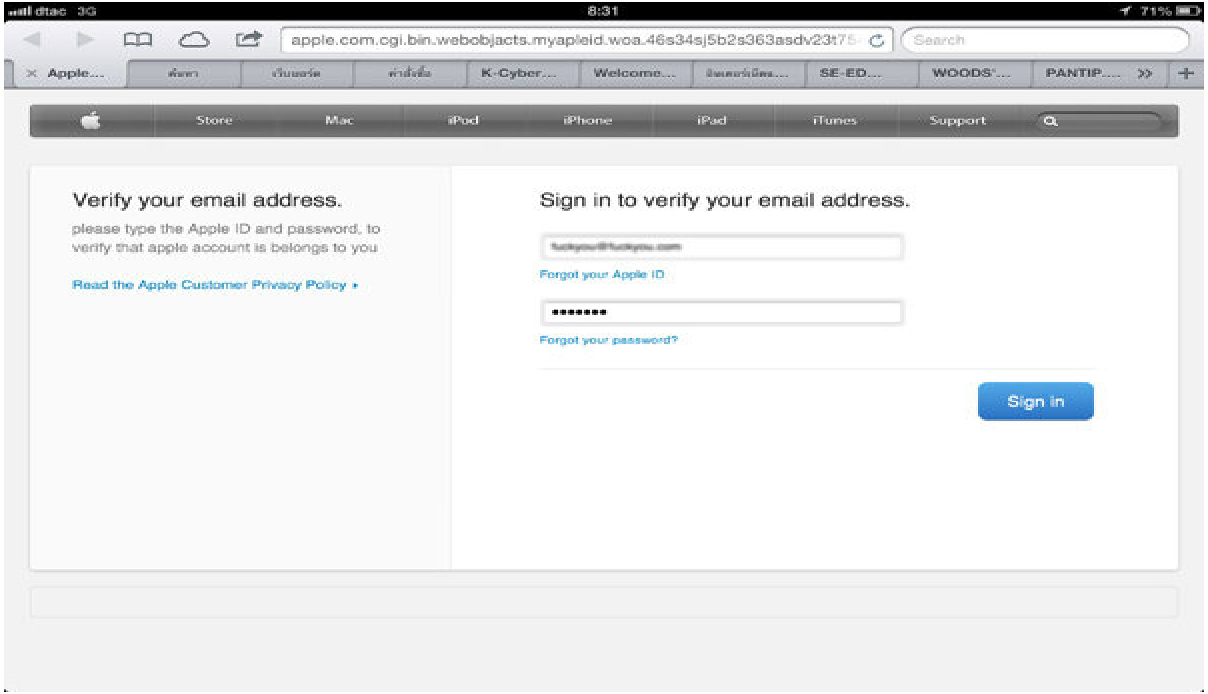
Wondering why you got this email?
It's sent when someone adds or changes a contact email address for an Apple ID account. If you didn't do this, don't worry. Your email address cannot be used as a contact address for an Apple ID without your verification.

If you need further assistance, please contact us.

Best regards,

Appel Support

TM and copyright 2013 appelInc.



apple.com.cgi.bin.webobjacts.myapleid.woa.46s34sj5b2s363asdv23t75

Verify your email address.

please type the Apple ID and password, to verify that apple account is belongs to you

Read the Apple Customer Privacy Policy ›

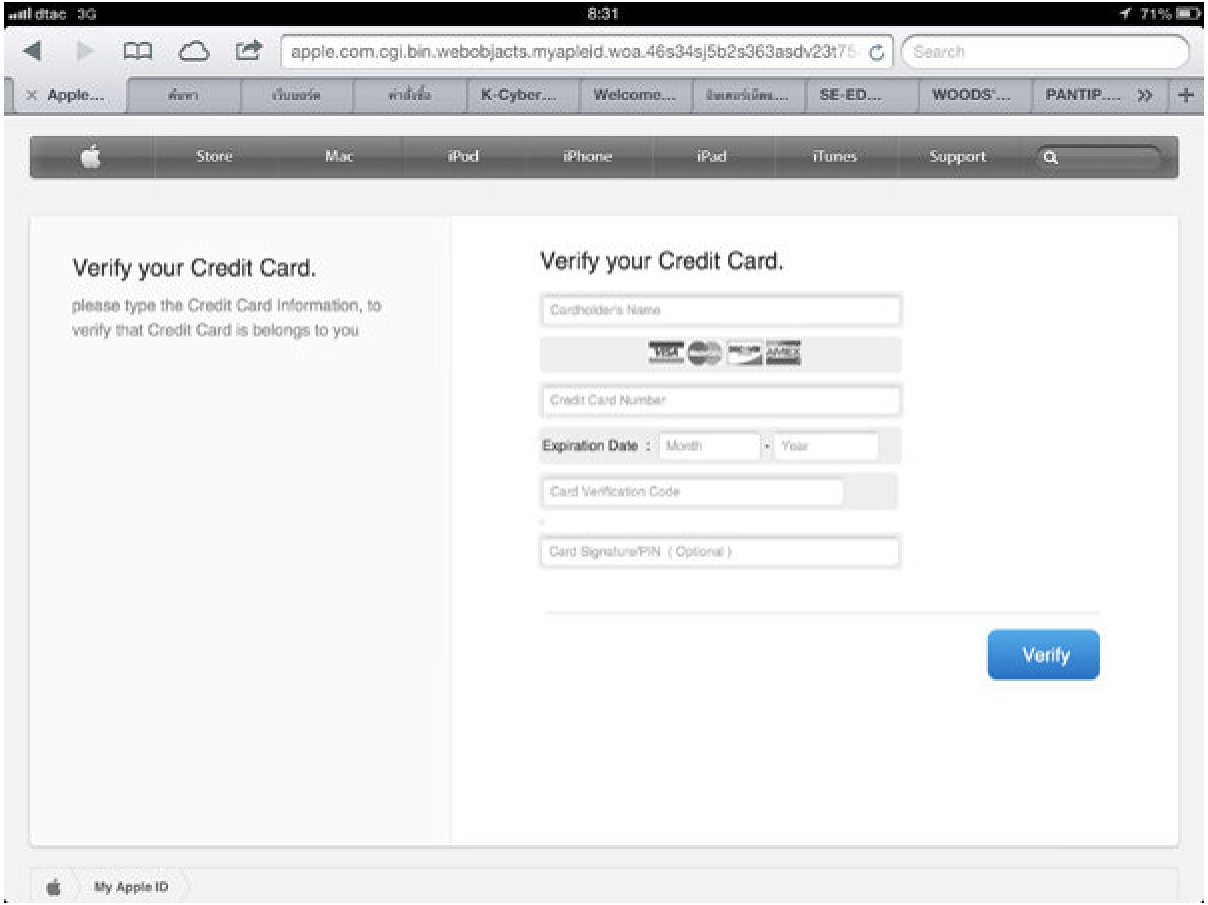
Sign in to verify your email address.

[redacted]

Forgot your Apple ID

••••••••

Forgot your password?



Verify your Credit Card.

please type the Credit Card Information, to verify that Credit Card is belongs to you

Verify your Credit Card.

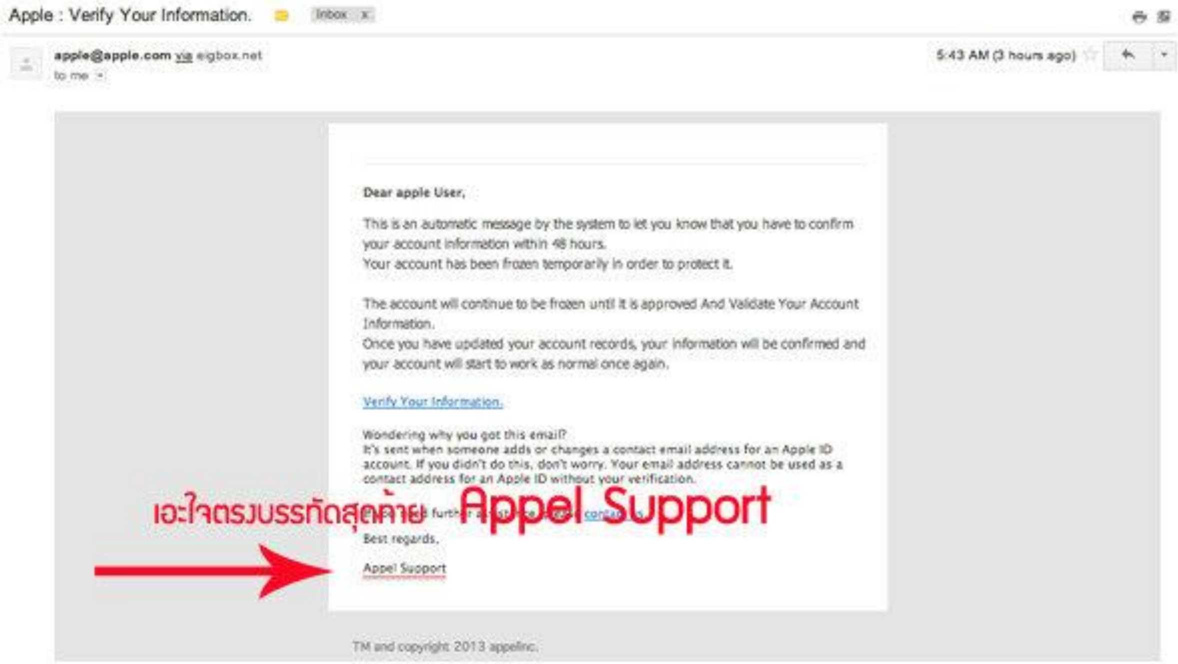
Cardholder's Name

Credit Card Number

Expiration Date : Month - Year

Card Verification Code

Card Signature/PIN (Optional)



Apple : Verify Your Information.

apple@apple.com via eigbox.net
to me

5:43 AM (3 hours ago)

Dear apple User,

This is an automatic message by the system to let you know that you have to confirm your account information within 48 hours.
Your account has been frozen temporarily in order to protect it.

The account will continue to be frozen until it is approved And Validate Your Account Information.
Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.

Verify Your Information.

Wondering why you got this email?
It's sent when someone adds or changes a contact email address for an Apple ID account. If you didn't do this, don't worry. Your email address cannot be used as a contact address for an Apple ID without your verification.

[illegible] further assistance, please contact us.

Best regards,

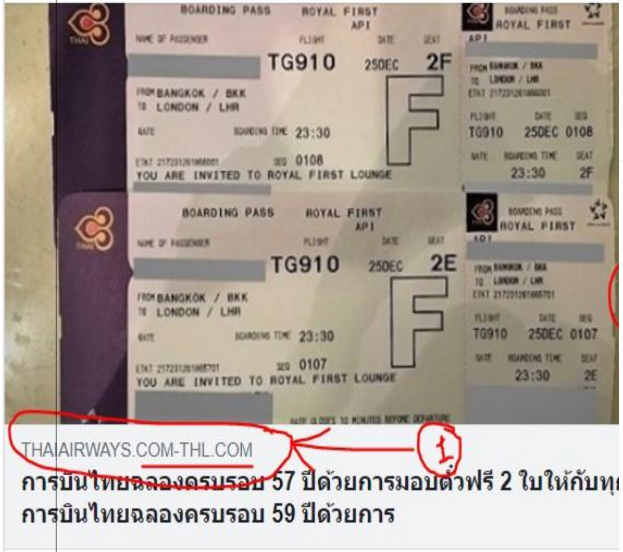
Appel Support

TM and copyright 2013 appelinc.

เอะใจตรงบรรทัดสุดท้าย Appel Support

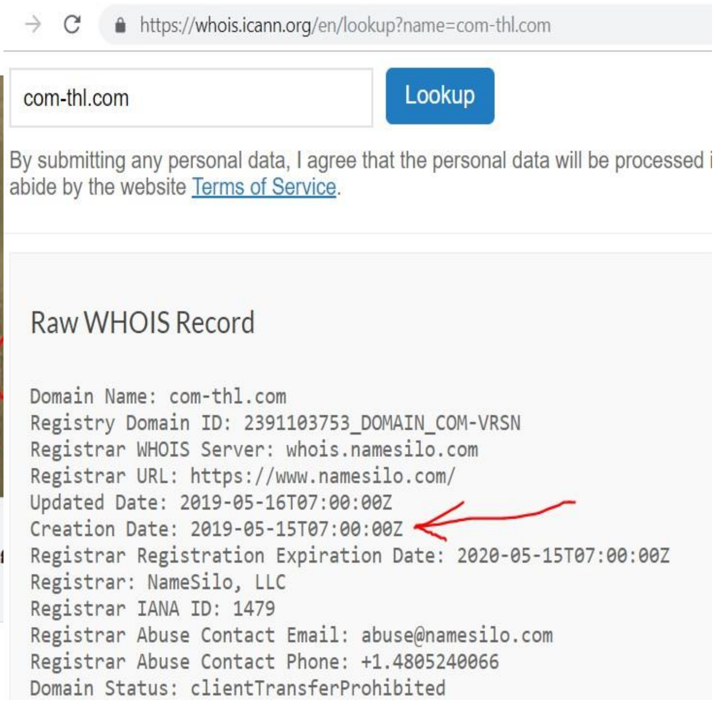
https://www.google.co.th/search?q=phishing+mail&tbm=isch&tbo=u&source=univ&sa=X&ei=5aOuUaDUAsPKrAfwyYCoBw&ved=0CEMQsAQ&biw=1196&bih=766

The picture can't be displayed.



THAIAIRWAYS.COM-THL.COM

การบินไทยฉลองครบรอบ 57 ปีด้วยการมอบตั๋วฟรี 2 ใบให้กับทุ
การบินไทยฉลองครบรอบ 59 ปีด้วยการ



com-thl.com

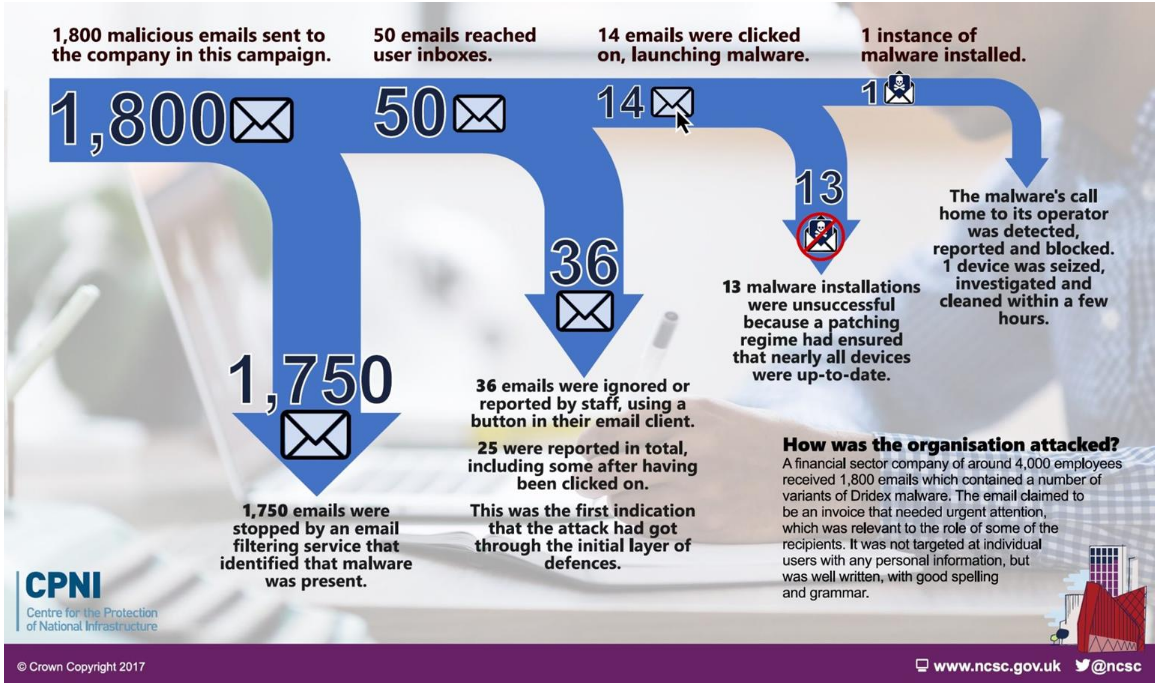
By submitting any personal data, I agree that the personal data will be processed i
abide by the website Terms of Service.

Raw WHOIS Record

```
Domain Name: com-thl.com
Registry Domain ID: 2391103753_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-05-16T07:00:00Z
Creation Date: 2019-05-15T07:00:00Z
Registrar Registration Expiration Date: 2020-05-15T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited
```

Multi-layered Phishing mitigations

The following real-world example shows how implementing layers of defences can help organisations (in this case a financial sector company of around 4,000 staff) defend themselves against phishing attacks. Reliance on any single layer would have missed some of the attacks, and cleaning infecting devices is costly and prohibitively time consuming.



1,800 malicious emails sent to the company in this campaign.

50 emails reached user inboxes.

14 emails were clicked on, launching malware.

1 instance of malware installed.

1,750 emails were stopped by an email filtering service that identified that malware was present.

36 emails were ignored or reported by staff, using a button in their email client.

25 were reported in total, including some after having been clicked on.

This was the first indication that the attack had got through the initial layer of defences.

13 malware installations were unsuccessful because a patching regime had ensured that nearly all devices were up-to-date.

The malware's call home to its operator was detected, reported and blocked. 1 device was seized, investigated and cleaned within a few hours.

How was the organisation attacked?
A financial sector company of around 4,000 employees received 1,800 emails which contained a number of variants of Dridex malware. The email claimed to be an invoice that needed urgent attention, which was relevant to the role of some of the recipients. It was not targeted at individual users with any personal information, but was well written, with good spelling and grammar.

CPNI
Centre for the Protection of National Infrastructure

www.ncsc.gov.uk @ncsc

https://safety4sea.com/the-need-of-multi-layered-phishing-mitigation-a-real-case-study/

Baiting Scenarios

Attack well known หลอกหล่อเหยื่อให้ติดเบ็ด

- เช่น บน website ที่ให้ download พวก porn site , crack

How To Prevent Social Engineering Attacks?

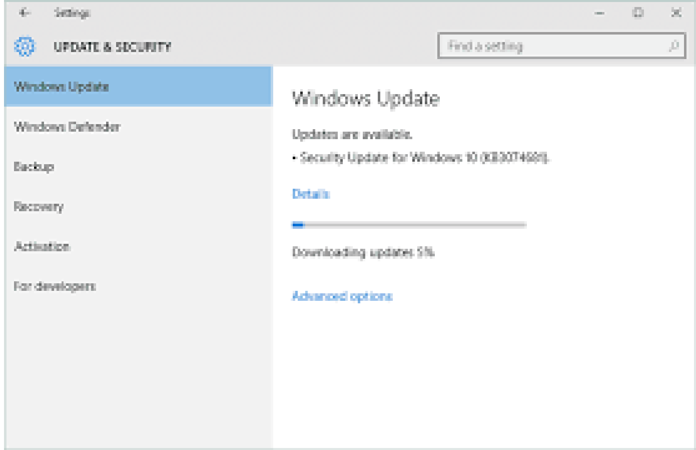
- DO NOT open emails in the spam folder or emails whose recipients you do not know
- DO NOT open attachments in the emails from unknown origin
- Use a reputable antivirus software
- Backup your data to disk offline or cloud
- Training security awareness
- Test social engineering attack in organization

Ref: https://www.transunion.com/article/how-to-protect-against-social-engineering

System Security

System Security

- Update antivirus and malware
- Update patch windows



Windows Update

Updates are available.

• Security Update for Windows 10 (KB3074681).

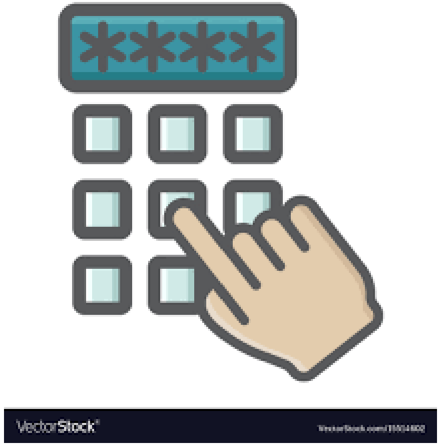
Downloading updates 5%

Password

Basic Identification

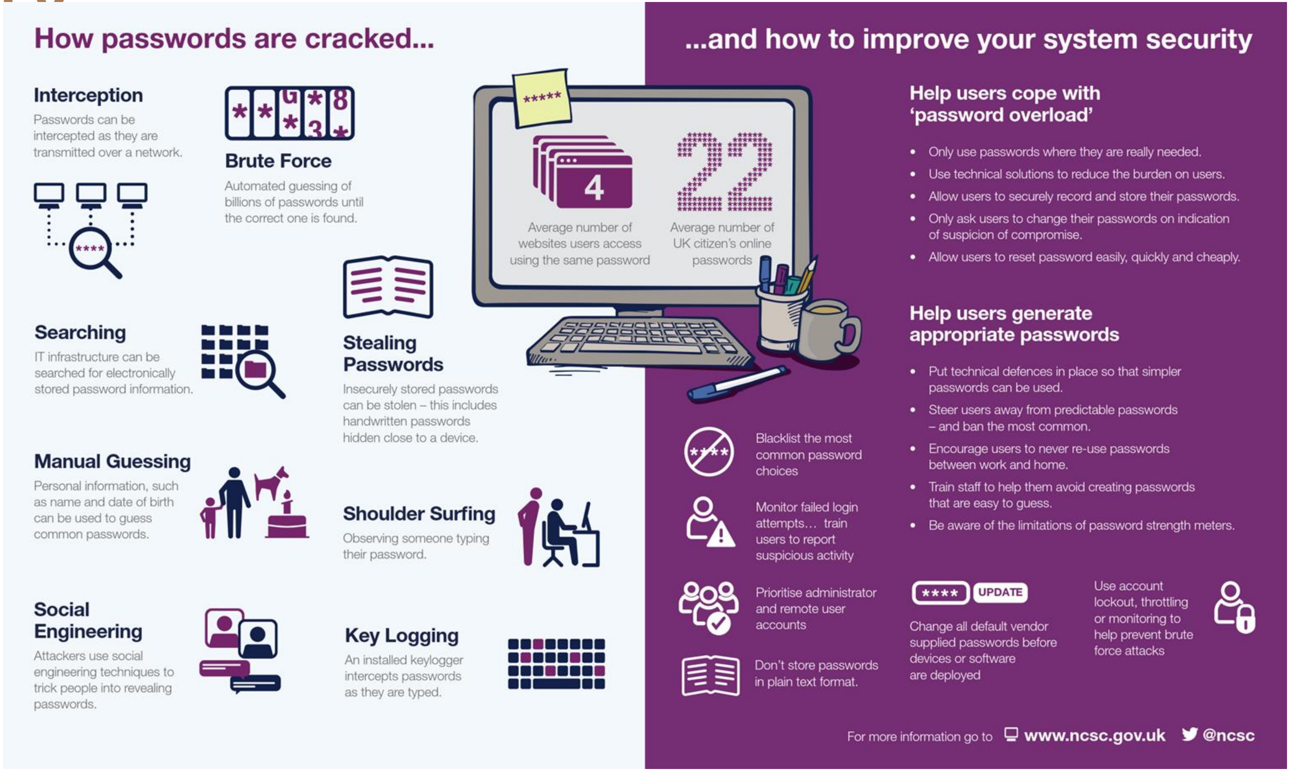
Something you know…

- Passwords, PINs, Secret or key
- Complex password



Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following device makes password security easier for your users – improving your system security as a result



How passwords are cracked...

Interception

Passwords can be intercepted as they are transmitted over a network.

Brute Force

Automated guessing of billions of passwords until the correct one is found.

Searching

IT infrastructure can be searched for electronically stored password information.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing

Observing someone typing their password.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging

An installed keylogger intercepts passwords as they are typed.

4

Average number of websites users access using the same password

22

Average number of UK citizen's online passwords

...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Blacklist the most common password choices

Monitor failed login attempts... train users to report suspicious activity

Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

**** UPDATE

Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks

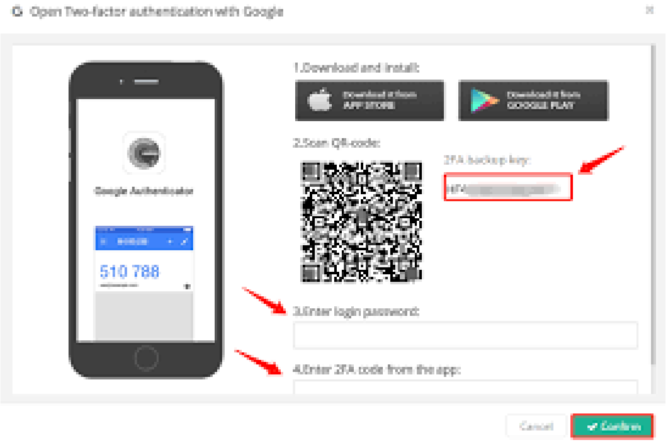
For more information go to www.ncsc.gov.uk @ncsc

https://www.ncsc.gov.uk/information/infographics-ncsc

Basic Identification (cont.)

Something you have

– Physical devices: magnetic cards, smart cards, tokens, bluetooth, password generators, cellphones…


Open Two-factor authentication with Google

1.Download and install:

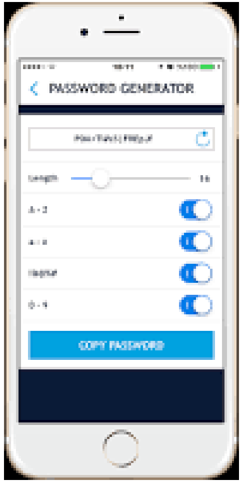
2.Scan QR-code:

2FA backup key:

[redacted]

3.Enter login password:

4.Enter 2FA code from the app:



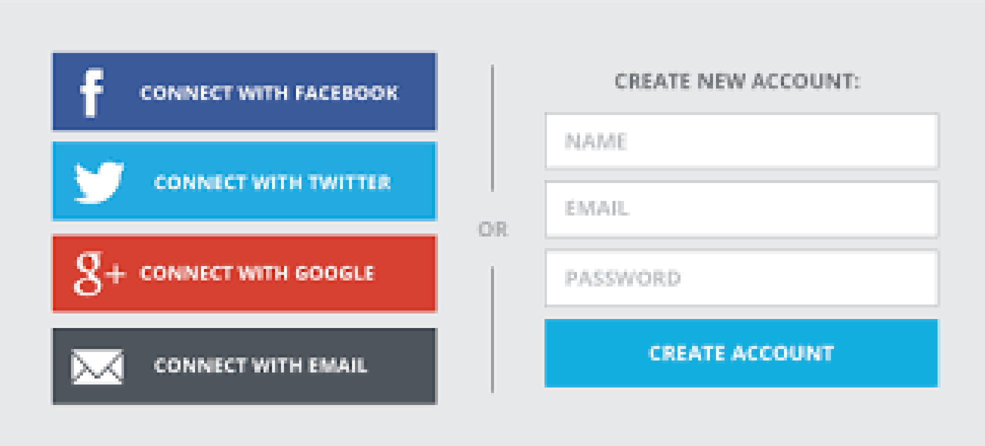
Basic Identification (cont.)

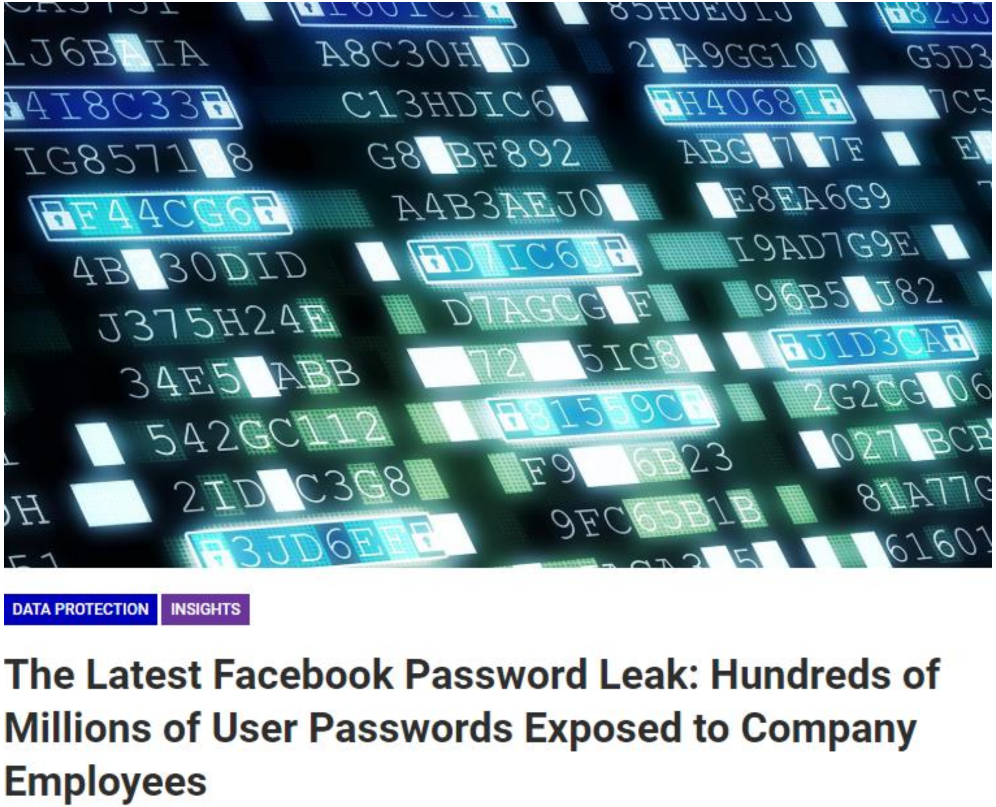
Something you are…

- Biometrics (fingerprints, iris recognition, voice, handwriting)

E-mail & Social login

E-mail & Social Login

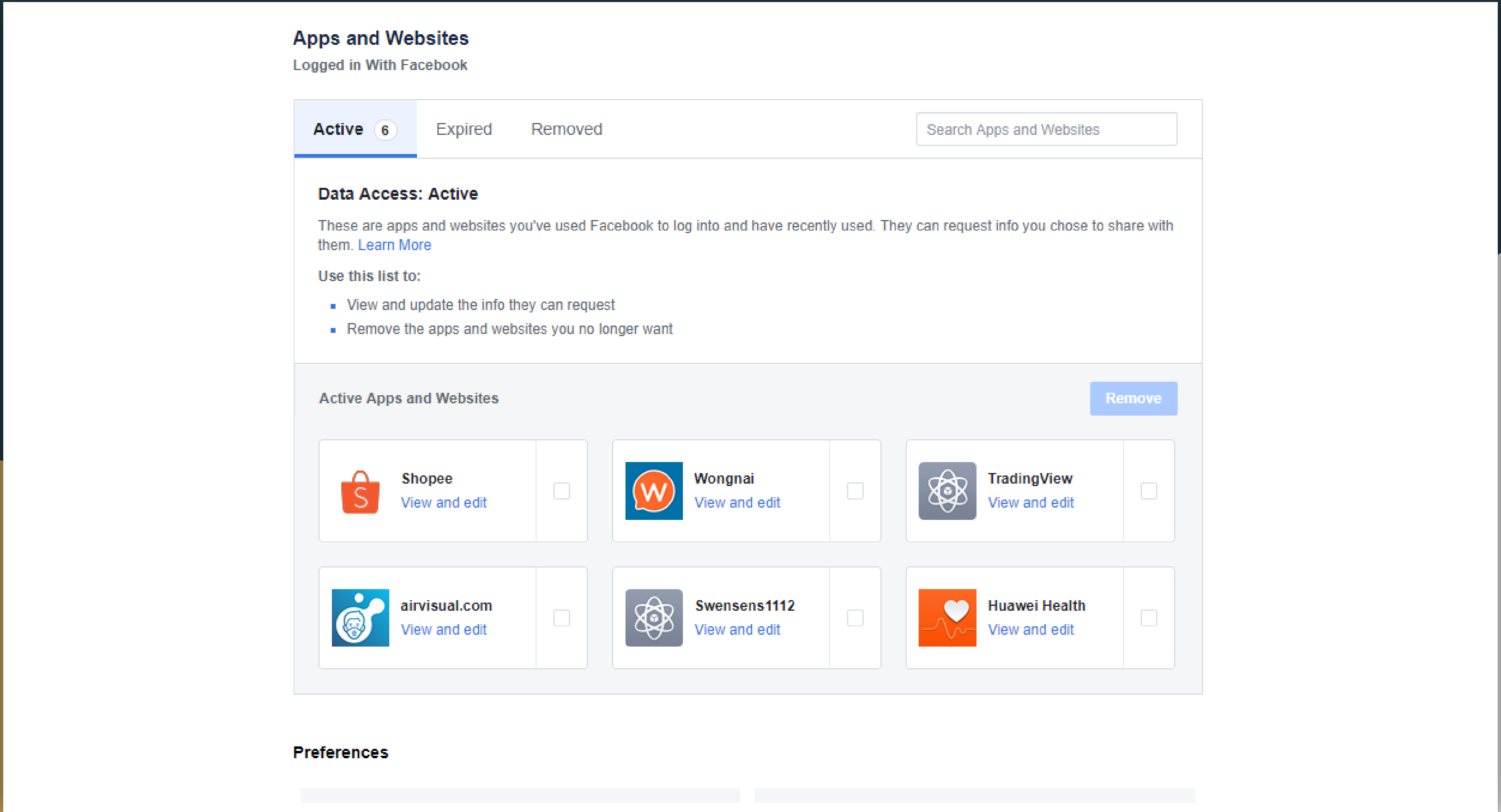




DATA PROTECTION INSIGHTS

The Latest Facebook Password Leak: Hundreds of Millions of User Passwords Exposed to Company Employees

https://www.cpomagazine.com/data-protection/the-latest-facebook-password-leak-hundreds-of-millions-of-user-passwords-exposed-to-company-employees/



Apps and Websites

Logged in With Facebook

Data Access: Active

These are apps and websites you've used Facebook to log into and have recently used. They can request info you chose to share with them. Learn More

Use this list to:

- View and update the info they can request
- Remove the apps and websites you no longer want

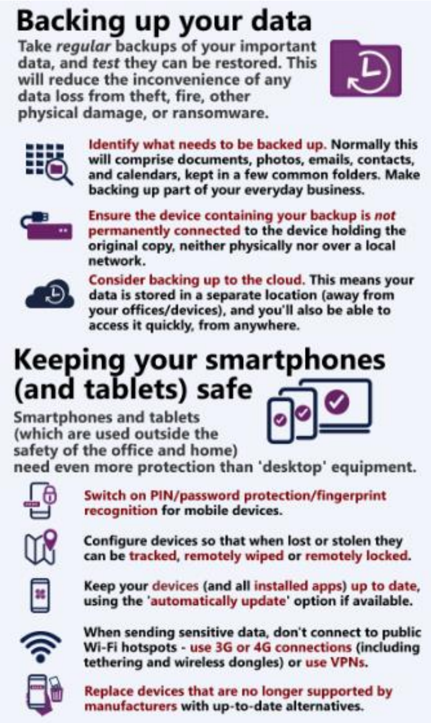
Active Apps and Websites

Shopee View and edit	□	Wongnai View and edit	□	TradingView View and edit	□
airvisual.com View and edit	□	Swensens1112 View and edit	□	Huawei Health View and edit	□

Preferences

Cyber Security
Small Business Guide

This advice has been produced to help small business protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below



Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.

Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

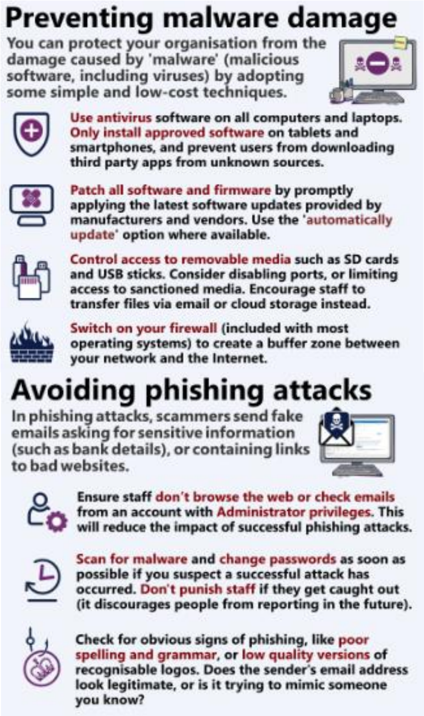
Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be tracked, remotely wiped or remotely locked.

Keep your devices (and all installed apps) up to date, using the 'automatically update' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - use 3G or 4G connections (including tethering and wireless dongles) or use VPNs.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.



Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. Only install approved software on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the 'automatically update' option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

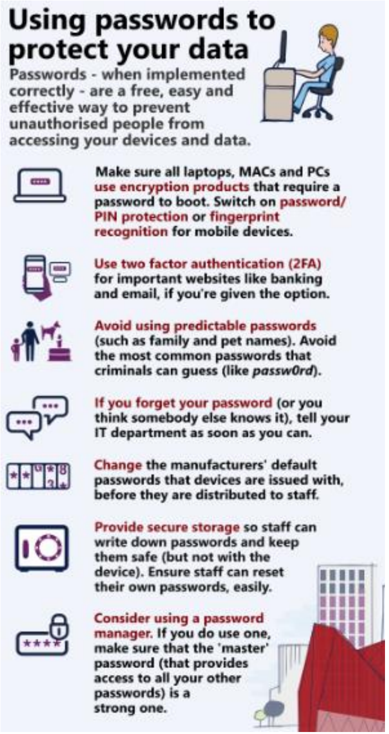
Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff don't browse the web or check emails from an account with Administrator privileges. This will reduce the impact of successful phishing attacks.

Scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred. Don't punish staff if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like poor spelling and grammar, or low quality versions of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?



Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, MACs and PCs use encryption products that require a password to boot. Switch on password/PIN protection or fingerprint recognition for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

If you forget your password (or you think somebody else knows it), tell your IT department as soon as you can.

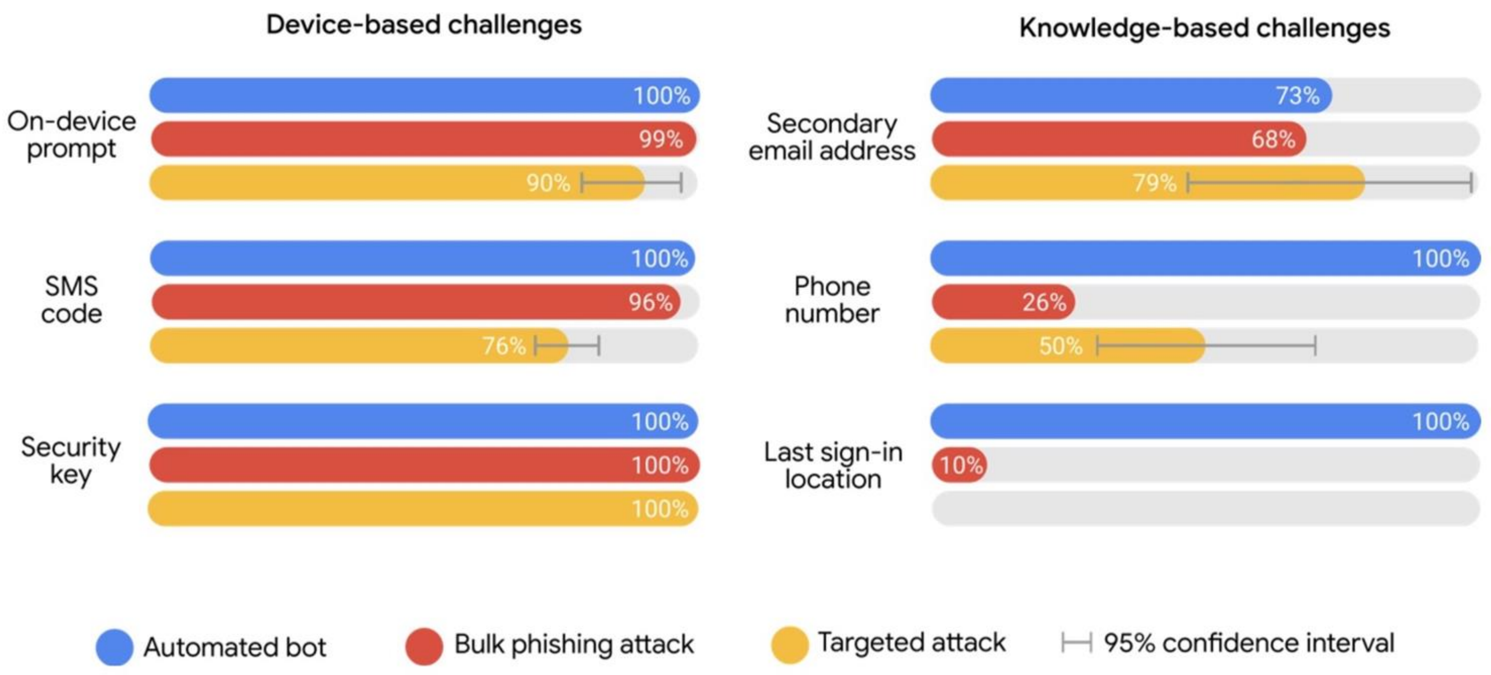
Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

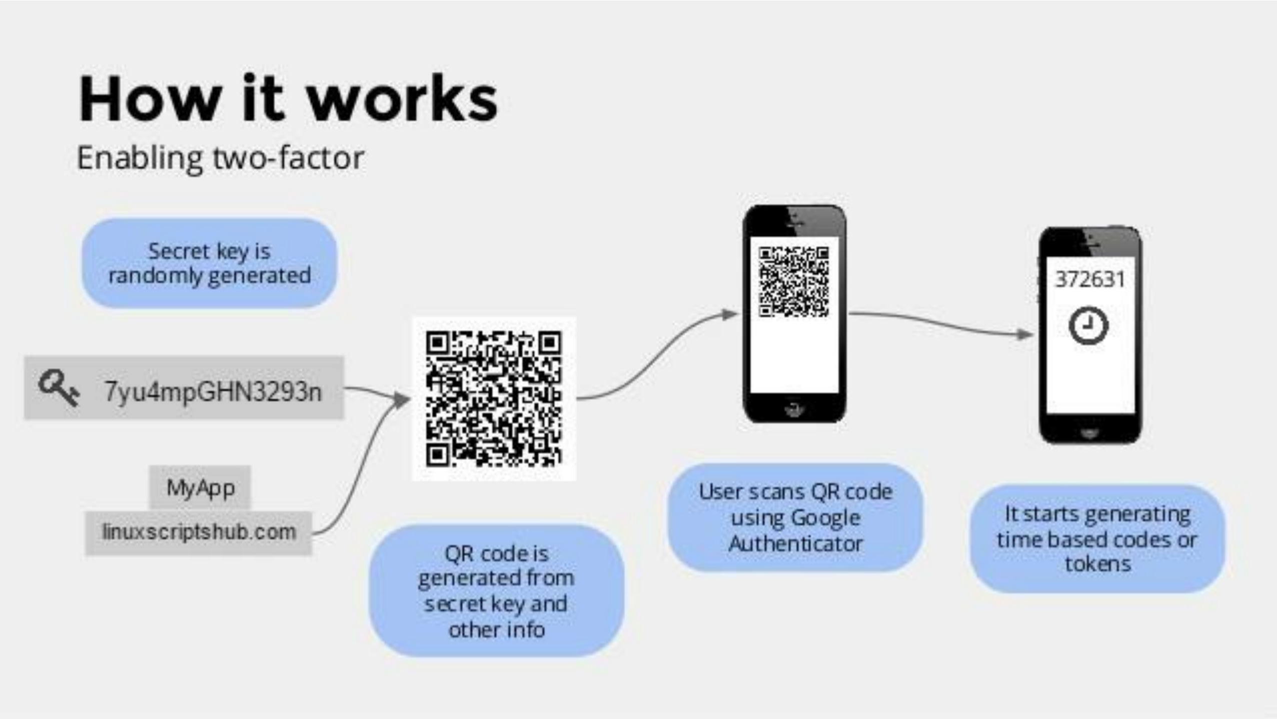
https://www.ncsc.gov.uk/information/infographics-ncsc

Google’s own data proves two-factor is the best defense against most account hacks



https://techcrunch.com/2019/05/20/google-data-two-factor-security/

Enable 2FA (2 Factor Authentication)



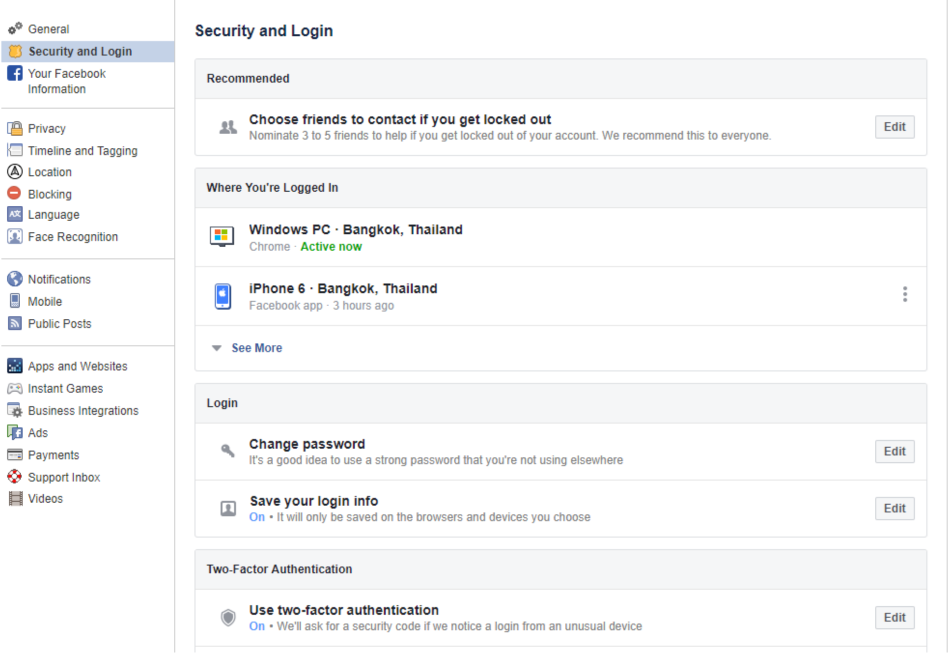
How it works
Enabling two-factor
Secret key is randomly generated
7yu4mpGHN3293n
MyApp
linuxscriptshub.com
QR code is generated from secret key and other info
User scans QR code using Google Authenticator
372631
It starts generating time based codes or tokens

https://myaccount.google.com/signinoptions/two-step-verification/enroll-welcome

Enable 2FA (2 Factor Authentication)

- Download google authentication application for (android , IOS)

Facebook -> setting -> security & login



Security and Login

Recommended

Choose friends to contact if you get locked out
Nominate 3 to 5 friends to help if you get locked out of your account. We recommend this to everyone. Edit

Where You're Logged In

Windows PC · Bangkok, Thailand
Chrome · Active now

iPhone 6 · Bangkok, Thailand
Facebook app · 3 hours ago

See More

Login

Change password
It's a good idea to use a strong password that you're not using elsewhere Edit

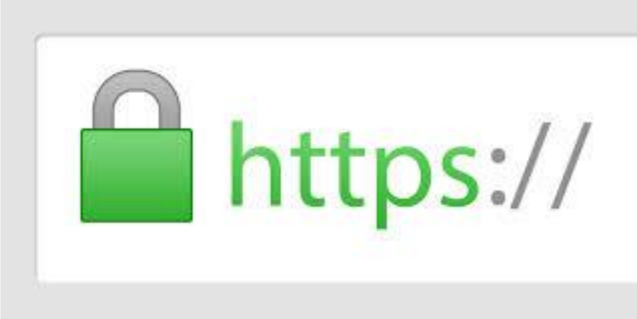
Save your login info
On • It will only be saved on the browsers and devices you choose Edit

Two-Factor Authentication

Use two-factor authentication
On • We'll ask for a security code if we notice a login from an unusual device Edit

10 วิธีในการ shopping online อย่างปลอดภัย

เลือก website ที่เป็น https



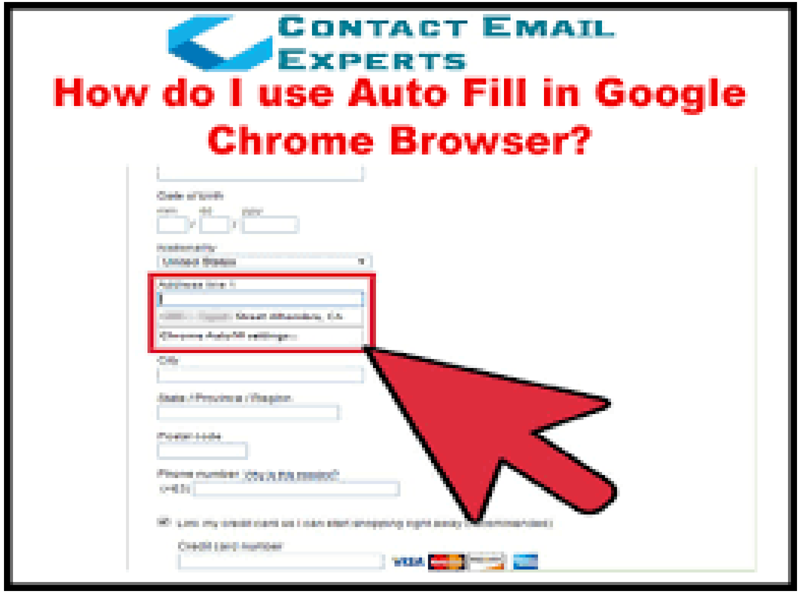
10 วิธีในการ shopping online อย่างปลอดภัย

ทำธุรกรรมผ่าน internet ส่วนตัว เช่น ที่บ้าน หรือเครื่องตัวเอง ไม่ควรใช้เครื่องสาธารณะ

10 วิธีในการ shopping online อย่างปลอดภัย

ใช้บัตรเครดิต หรือ E-wallet ไม่ควรใช้ เดบิต

ไม่บันทึกข้อมูลบัตรเครดิตบน browser



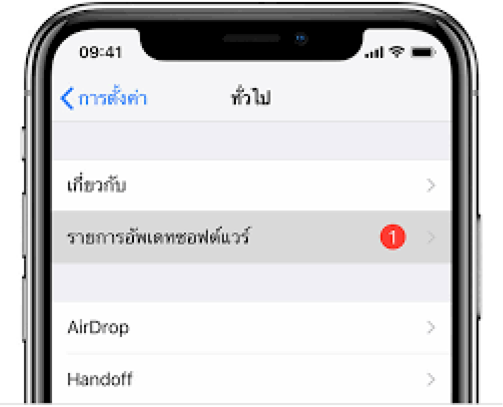
How do I use Auto Fill in Google Chrome Browser?

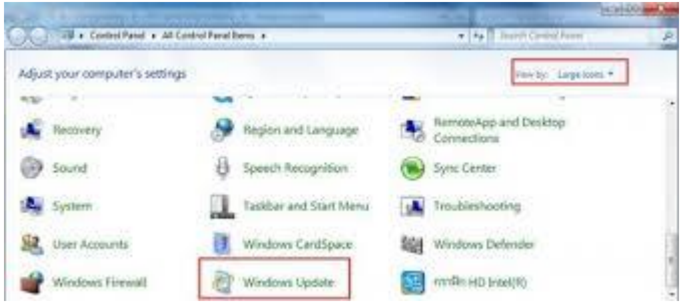
ซื้อจากร้านที่มีชื่อเสียงน่าเชื่อถือ โดยอาจดูจาก review หรือ rating

ไม่ควร click link ใน E-mail หรือ link แปลกๆ

ตั้ง password ในการ access เข้ามือถือ

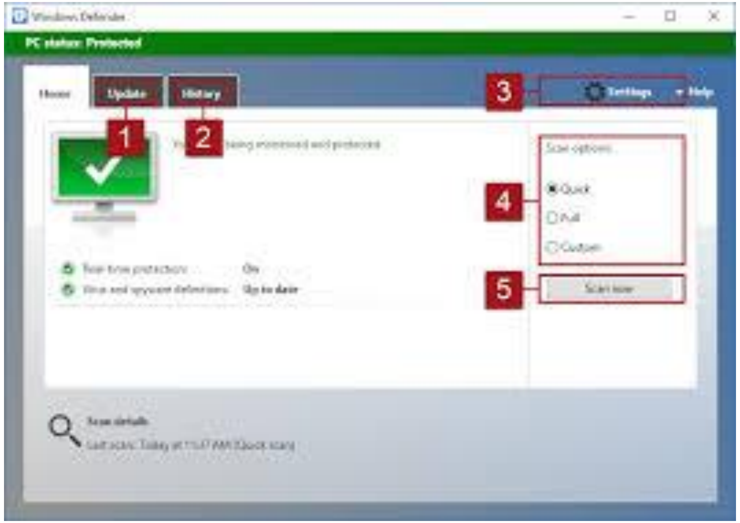
Update ระบบ application browser หรือซอฟต์แวร์บ่อยๆ





View by: Large icons ▾

ติดตั้ง antivirus



PC status: Protected

Yo… being monitored and protected

Real-time protection: On

Virus and spyware definitions: Up to date

Scan options:

● Quick

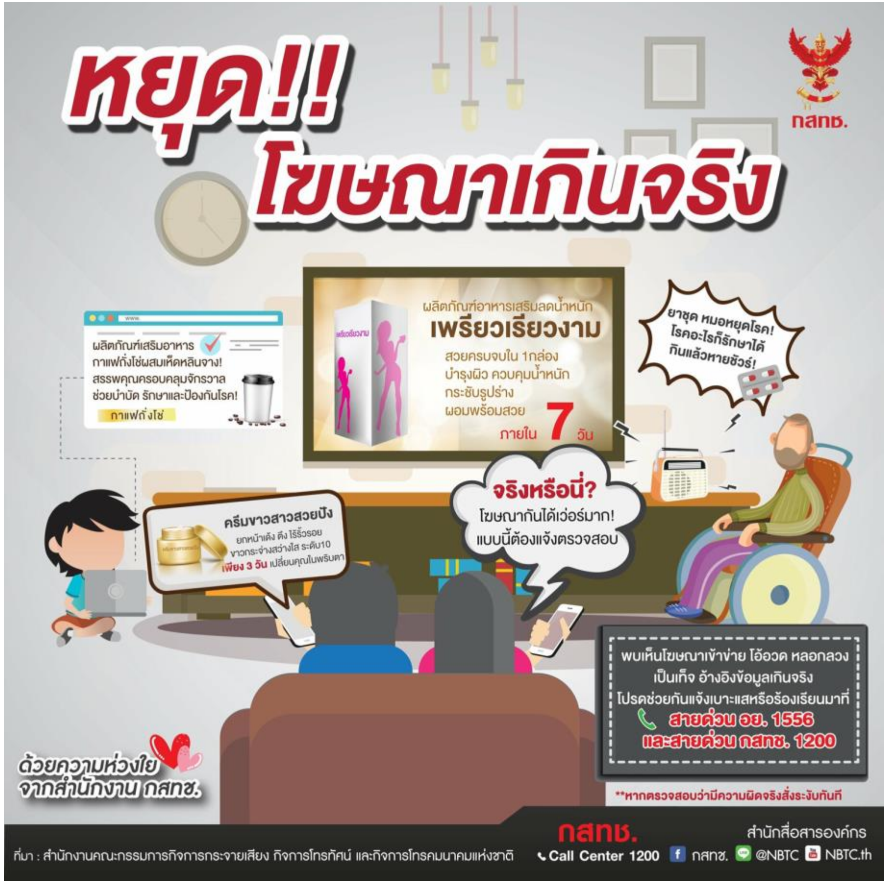
○ Full

○ Custom

Scan details

Last scan: Today at 11:47 AM (Quick scan)

อย่าหลงเชื่อข้อเสนอที่เกินจริง



พบเห็นโฆษณาเข้าข่าย โอ้อวด หลอกลวง
เป็นเท็จ อ้างอิงข้อมูลเกินจริง
โปรดช่วยกันแจ้งเบาะแสหรือร้องเรียนมาที่
☎ สายด่วน อย. 1556
และสายด่วน กสทช. 1200

**หากตรวจสอบว่ามีความผิดจริงสั่งระงับทันที

กสทช.
สำนักสื่อสารองค์กร

ที่มา : สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

☎ Call Center 1200 f กสทช. @NBTC NBTC.th

FAQ service in SWU

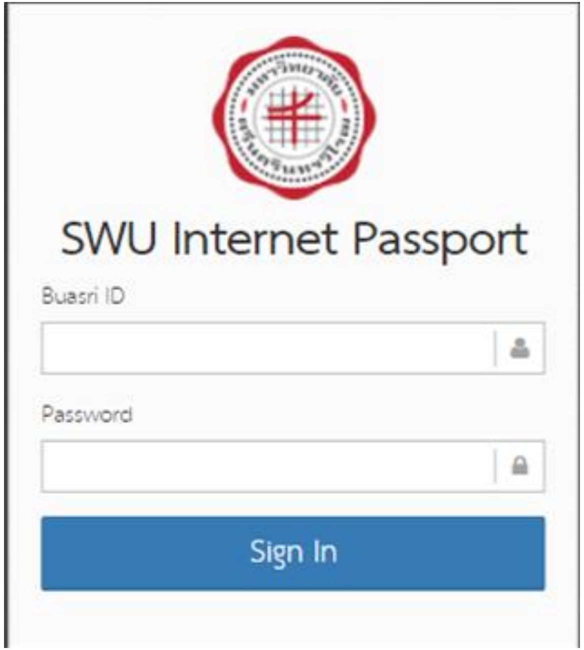
Just so you know

FAQ Service in University

I-Pass

- ทำไม I-Pass ต้องนับเวลา 2 ชั่วโมง
- ทำไม I-Pass ใช้ได้แค่ 2 เครื่องพร้อมกัน
- I-Pass สามารถดูได้ว่า Account เราไปใช้อยู่ที่ไหนบ้าง
- ถ้า Log-in เกิน 2 เครื่องจะทำอย่างไร
- ฉันไม่ได้ใช้งานเลยแต่ทำไมมีคนใช้ Account ฉันอยู่ (ตอบ รีบเปลี่ยนรหัสสิจ๊ะ)

สอนใช้งาน I-Pass



SWU Internet Passport

Buasri ID

Password