

IT Security Awareness Talk
By NUS IT
Aug 2018 @ LKYSPP

Outline

1. Information Security Objective
2. Trending Cyber-attacks Techniques
3. Best Practices



Information Security Objectives



***Security is
lifestyle!***

***Think Safe.
Think Secure.***

What are the Information Security Objectives?

Preserve

Confidentiality

Integrity

Availability

C

Accessible by authorized personnel.

I

Accurate and complete.

A

Accessible when required.

Of Information and Information Systems

Source: IT Security Policy Chapter 1- Introduction to IT Security Policy, Section 2

Confidentiality Breach

Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack



Initial investigations showed that one SingHealth front-end workstation was infected with malware through which the hackers gained access to the data base. The data theft happened between June 27, 2018, and July 4, 2018.

<https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most>

Confidentiality Breach

Flaw in LinkedIn AutoFill Plugin Lets Third-Party Sites Steal Your Data

📅 Saturday, April 21, 2018 👤 Swati Khandelwal

 Share   Share  Tweet  Share



Not just Facebook, a new vulnerability discovered in LinkedIn's popular AutoFill functionality found leaking its users' sensitive information to third party websites without the user even knowing [...]

Source @ <https://thehackernews.com/>

Integrity Breach

Over 20 Million Users Installed Malicious Ad Blockers From Chrome Store

📅 Thursday, April 19, 2018 👤 Mohit Kumar

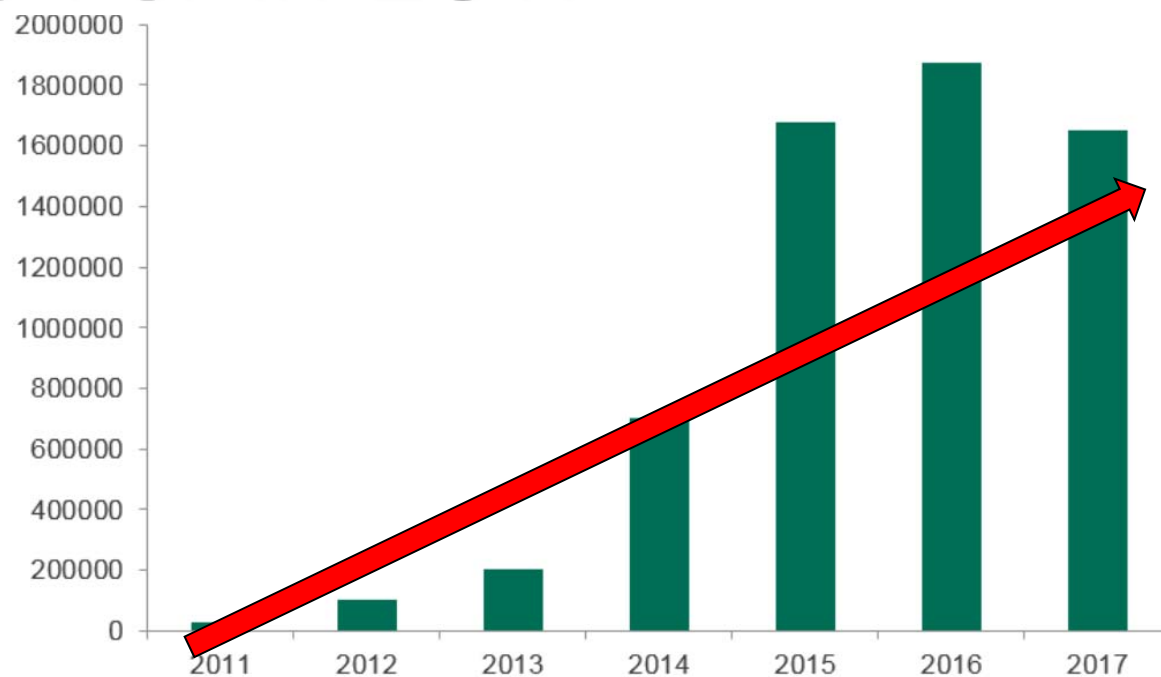


If you have installed any of the below-mentioned Ad blocker extension in your Chrome browser, you could have been hacked. A security researcher has spotted five malicious ad blockers extension in [...]

Source @ <https://thehackernews.com/>

Availability Breach

1.65M Users Victimized by Cryptocurrency Miner Threats So Far in 2017



Number of users Kaspersky Lab protected from malicious cryptocurrency miners from 2011 to 2017. (Source: Securelist)

Source: <https://www.tripwire.com/state-of-security/latest-security-news/1-65m-users-victimized-cryptocurrency-miner-threats-far-2017/>

Massive Brute-Force Attack Infects WordPress Sites with Monero Miners



Over the course of the current week, WordPress sites around the globe have been the targets of a massive brute-force campaign during which hackers attempted to guess admin account logins in order to install a Monero miner on compromised sites.

Source: <https://www.bleepingcomputer.com/news/security/massive-brute-force-attack-infects-wordpress-sites-with-monero-miners/>



What are the three security objectives?

Answer: Ensure the confidentiality, integrity and availability of information system and information.

Information Security Policies



Think Good practice
Implement Good practice
Protect our Data and System



Overview of Information Security Policies

IT Security

Acceptable Use (for NUS IT resources)

Guidelines for Acceptable Use (of NUS IT resources) ★

Software Terms of use

Software Management

Mobile Device

Guideline for personal computer and equipment


Data Management

Guideline to classification and protection of University data

Cloud

Legislation Acts

<http://statutes.agc.gov.sg/aol/search/display/view.w3p;ident=a0823194-a6f3-481d-898a-7854557b85e7;page=0;query=CapAct%3A88%20Type%3Auact,areved;rec=1;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fsearch%2Fsummary%2Fresults.w3p%3Bquery%3DCapAct%253A88%2520Type%253Auact,areved#legis>

Cap	Legislative Act	Brief Description
50A	Computer Misuse and Cybersecurity Act	Unauthorized access or modification of computer program/data
88	The Electronic Transaction Act	Preservation of the integrity and reliability of electronic record
311A	Spam Control Act https://www.ida.gov.sg/Policies-and-Regulations/Acts-and-Regulations/Spam-Control-Framework	Unsolicited communication in bulk either email or mobile
97	The Evidence (Computer Output) Regulations in Chapter 97 of the Evidence Act	Admissible evidence for court case (e.g. relevant facts not opinions)
2012	The Personal Data Protection Act https://www.pdpc.gov.sg/docs/default-source/publications-edu-materials/what-you-need-to-know-about-pdpa-v1-0.pdf?sfvrsn=4	Protection of personal data 
63	Copyright Act	Protection of intellectual work
221	Patent Act	Protection of invention
332	Trademark Act	Protection of branding
338	Undesirable Publications Act	Prohibited publication that may be obscene, objectionable, etc

[https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-key-concepts-in-the-pdpa-\(270717\).pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-key-concepts-in-the-pdpa-(270717).pdf)



Can I share my user account and password?

**Answer: No, you are liable for all actions performed
using the account**

ION Orchard fined S\$15,000 over customer data breach

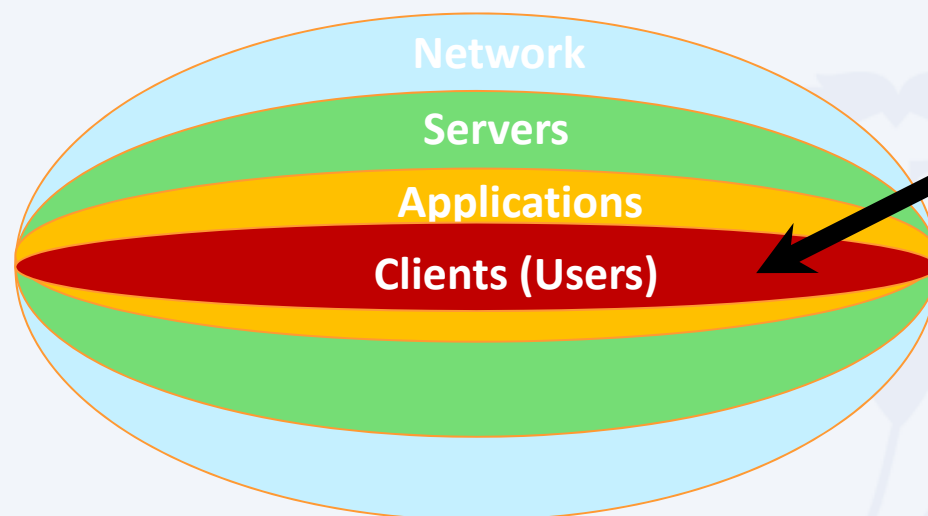


In the incident, which took place on Dec 26, 2015, an unknown perpetrator used valid admin account credentials to log in to a server that held personal customer data.

It found that Orchard Turn Developments did not have any policy to prohibit the sharing of admin account credentials, or to enforce the periodic expiry and renewal of these. Instead, it had only one admin account, which was shared among four authorised users.

Source: CNA @ Jul 2017

Trending Cyber Attacks Techniques: Phishing, Digital Currency Mining & Ransomware



“91% of Cyberattacks begins with Phishing Email “

– TrendMicro



Think Before You Click



Phishers use email to:

- Trick you into handing over your user information so that they can gain access to your system and network.
- Entice you to click on links that take you to web sites that will infect your computer with malware just by visiting it.
- Deliver file attachments that can infect your computer with malware.

Phishing email getting more sophisticated

DBS warns of phishing site targeting bank customers

-----Original Message-----

From : customerservice@posbbank.com.sg

Date : 03/03/2016 11:43 am GMT+8

To :

Subject : Security Update

This is not a DBS/POSB email
address



Dear Customer,

Kindly be informed that Singapore Banks has been under attack by hackers, and this has cost some customers to lose their money to this <https://virutallin.gq/secure/update/verification/posb/index.html> the Monetary Authority of Singapore to enact a new law mandating all customer verification/posb/index.html s to keep their money safe with banks. Click or tap to follow link.

Kindly click on www.posb.com.sg/secure/update to update your account with us and to keep your money safe, Failure to follow this instructions might result in the deactivation of your account, Please note that we will not be responsible for any account if you fail to update.

Link to phishing
website

Sorry For any inconvenience this may have caused you.

Thank you for using POSB Bank.

Kind regards,
Posb Bank Ltd.

Source: <https://www.todayonline.com/singapore/dbs-warns-phishing-site-targeting-bank-customers>

NUS Internal



Phishing via SMS

Fake SingHealth SMS messages are being sent out – here is how to verify that the one you received is authentic

If you are not affected by the cyberattack:



The image shows a screenshot of an SMS message from 'SingHealth'. The message text is: "www.singhealth.com.sg /cyberattack <Name>- you are not affected by the cyberattack. All your data is secure. No action needed. We apologise for any anxiety caused." To the right of the screenshot are three numbered steps: 1. Sender is SingHealth (with an arrow pointing to the sender name in the screenshot); 2. Check that the links are: www.singhealth.com.sg/cyberattack OR bit.ly/cyber-attack18 (with an arrow pointing to the link in the screenshot); 3. SingHealth will NOT ask for credit card or other financial information (with an arrow pointing to the text in the screenshot).

- 1 Sender is SingHealth
- 2 Check that the links are:
www.singhealth.com.sg/cyberattack
OR
bit.ly/cyber-attack18
- 3 SingHealth will NOT ask for credit card or other financial information

To verify the message, SingHealth said that its name will be reflected as the sender, and that it will not require credit card or other financial information:

“Check that the SMS is from ‘SingHealth’ and that when you ‘click’, it brings you to the SingHealth website.”



5 TIPS TO STAY SAFE ONLINE

following the SingHealth cyberattack

What patient data was taken:

- Name, NRIC number, address, gender, race and date of birth
- Outpatient dispensed medicines of about 160,000 patients

No other patient data were breached.

SingHealth has further tightened the security of its IT systems, and will contact its patients to inform if they are affected.

1 Beware fake messages

Authentic notifications will be sent by SingHealth. You can also check directly at datacheck.singhealth.com.sg.



2 Use strong passwords

Do not use personal information such as your NRIC or date of birth in your password or security questions. Visit www.csa.gov.sg/gosafeonline for tips to create strong passwords.



3 Enable Two-Factor Authentication (2FA)

When using e-Government and e-banking services, activate your 2FA for an added layer of protection.



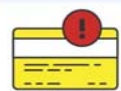
4 Watch out for scams

Beware of phone or online scams that ask for your PIN, password, SingPass or payment details. Government agencies will not ask for such details over email or phone. Never give your passwords to anyone else!



5 Check for fraudulent transactions

Regularly check your credit card and other transactions' history. Contact your bank immediately if you suspect fraudulent activities.



Adapted from CSA advisory:
www.csa.gov.sg/singcert/news/advisories-alerts/protecting-your-personal-data-2018



Source: <https://www.csa.gov.sg/singcert/news/advisories-alerts/protecting-your-personal-data-2018>

Phishing via Phone Calls with modified Caller ID

Singapore Airlines warns of phishing scams offering free air tickets

Beware of emails, **calls**, messages, surveys and contests that claim to be from Singapore Airlines (SIA) and which offer free air tickets or credits, said the flag carrier on Wednesday (Dec 20).



To appear more authentic, some **scammers modify their caller ID** to imitate SIA's official telephone numbers. ... The airline also advised customers to be on the alert for phishing websites that appear similar to the official SIA website, and to exercise caution in sharing their personal details online.

<https://www.channelnewsasia.com/news/singapore/singapore-airlines-warns-of-phishing-scams-offering-free-air-9513474>

Phishing via Email, SMS, whatsApp

Source: Straits Times 7 Sep 2017

AXA data breach affects 5,400 Singapore customers



The Singapore arm of AXA Insurance said that the personal data of 5,400 of its customers were stolen during a cyber attack. PHOTO: REUTERS

.. e-mail address, mobile number and date of birth were exposed

AXA made a police report, and advised customers to do the same if they had inadvertently disclosed personal data as a result of phishing attempts in the last few months as it could be connected to the AXA hacking incident

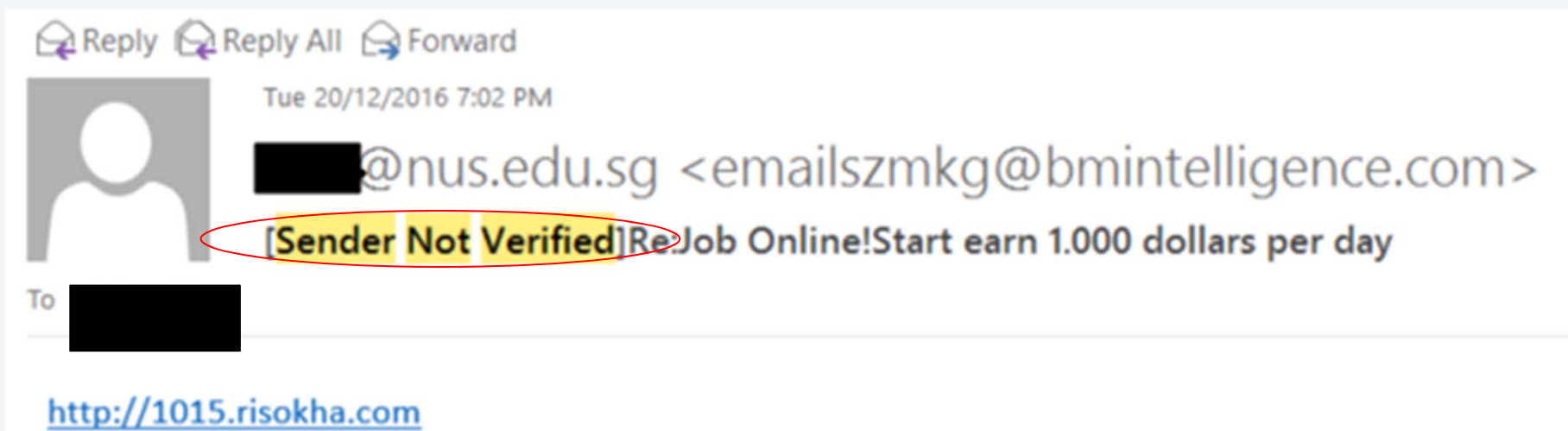
This method, known as phishing, can be executed via e-mail, SMS and WhatsApp - now that hackers have users' e-mail address and mobile number



How to identify a spoofed email address?



How to identify spoofed account?



How to identify spoofed account?



Digital Signature: Valid

Subject: Security Advisory on Phishing Email with Malicious Attach
 From: Computer Centre
 Signed By: computercentre@nus.edu.sg

The digital signature on this message is Valid and Trusted.
 For more information about the certificate used to digitally sign the message, click Details.

Warn me about errors in digitally signed e-mail before message open

Details...
Close

Message Security Properties

Subject: Security Advisory on Phishing Email with Malicious Attac

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

Security Layers
 Select a layer below to view its description.

- ✓ Subject: Security Advisory on Phishing Email with Malicious Attachm
- ✓ Digital Signature Layer
 - ✓ Signer: computercentre@nus.edu.sg

Description:
 OK: Signed message.

Click any of the following buttons to view more information about or make changes to the selected layer:

Edit Trust... View Details... Trust Certificate Authority...

Warn me about errors in digitally signed e-mail. Close

File Message Insert Options Format Text Review Developer Tell me what you want to do...

Cut Copy Paste Format Painter Clipboard

Basic Text: Bold, Italic, Underline, Text Color, Background Color, Bulleted List, Numbered List, Indent, Outdent, Paragraph, Undo, Redo

Names: Address Book, Check Names

Include: Attach File, Attach Item, Attach Signature

✉ We won't be able to deliver this message to itcare-sec@nus.edu.sg because the email address is no longer valid.

To... itcare-sec@nus.edu.sg

Cc...

Subject

Send

How to identify spoofed account?



- 1 Look out for "Sender Not Verified" in the subject
- 2 Look out for digital signature
- 3 Type the email address at the "to" field and click on check names





Can Phishing email be sent from legitimate account?

Answer:

Yes, the account could be compromised. Report any suspicious email using Phishing button.



**Phishing email
targeting NUS**

*This email is sent to all NUS Staff

Dear Colleagues,

Over the weekend, we detected a series of highly targeted phishing emails being sent to many NUS staff and students. Most of these were sent from compromised NUS accounts, and crafted using existing email subjects which the recipients were familiar with. By using these techniques, the phishing emails were made to appear more authentic, and resulted in more users falling prey.

Below is a sample of the phishing email for your reference. The link in green ("Click here to view message") would bring you to a website requesting you to enter your NUSNET credentials. DO NOT click on this link or any other links from suspicious emails. Please also report such phishing emails immediately by using the "Report Phishing" button. Alternatively, you may contact IT Care at 6516 2080 or itcare@nus.edu.sg.

Also, if you responded to any such email or clicked on any link in the email, please change your NUSNET password immediately.

From:
Sent: Sunday, July 15, 2018 9:07 AM
To:
Subject: Re: Re: Access Denied :

Unable to show this message

[Click here to view message](#)

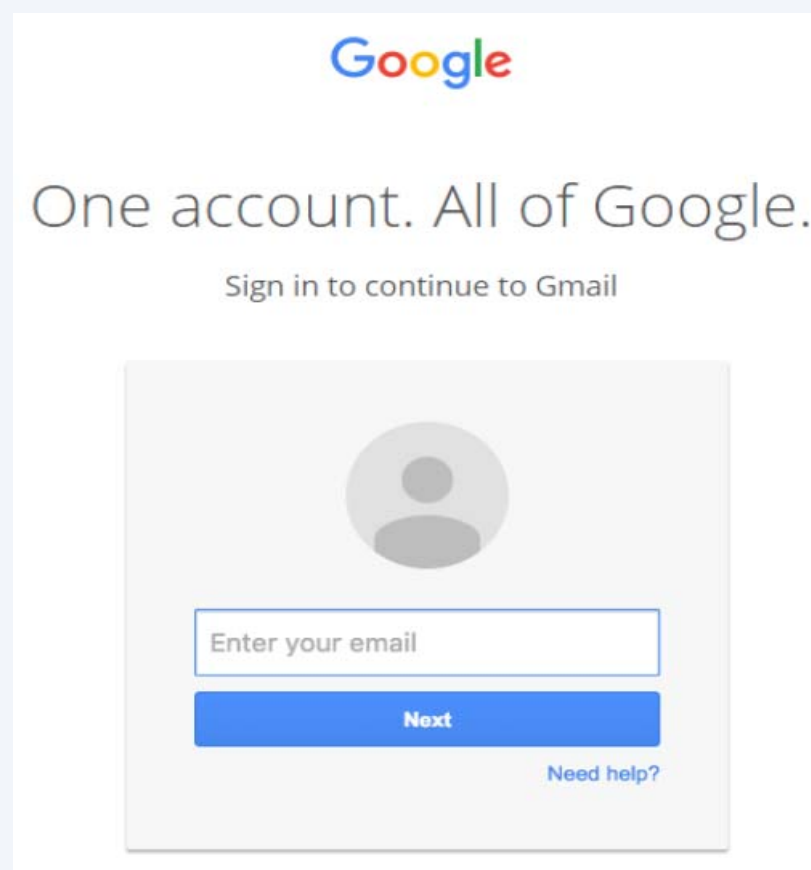
Pop3 message delayed: fibu - Date: 07/15/2018 1:06:48 (nus)

Evolving Phishing Email Techniques

Source: <https://www.wordfence.com/blog/2017/01/gmail-phishing-data-uri/>

Wide Impact: Highly Effective Gmail Phishing Technique Being Exploited

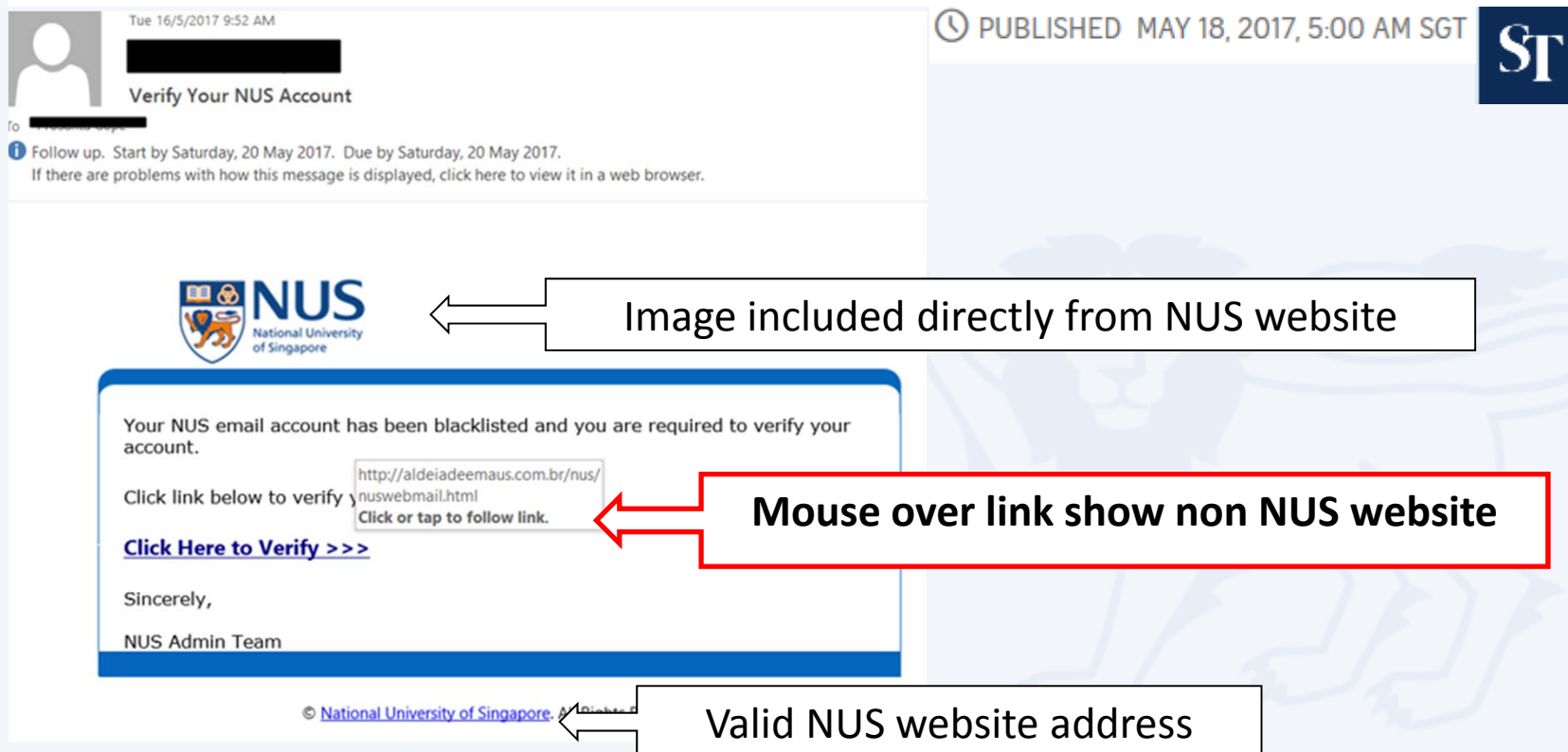
.... “The attackers log in to your account immediately once they get the credentials, and they use one of your actual attachments, along with one of your actual subject lines, and send it to people in your contact list



Phishing Email from Legitimate Account

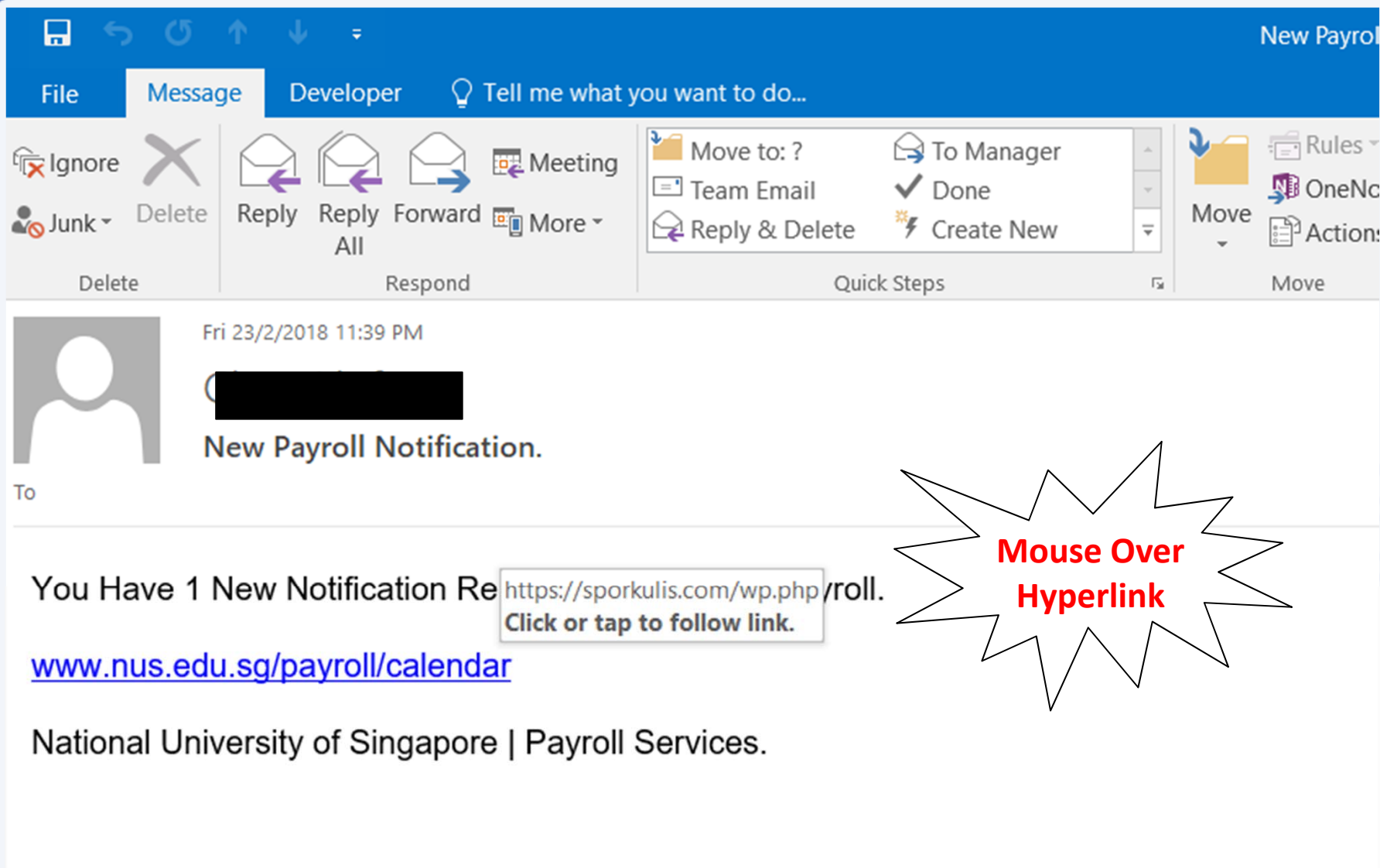
NUS staff hit by 'spear phishing' in new cyber attacks

....Spear phishing is the fraudulent practice of sending e-mail from trusted sender, to trick targeted individual to reveal information, click on malware infected link or attachment.



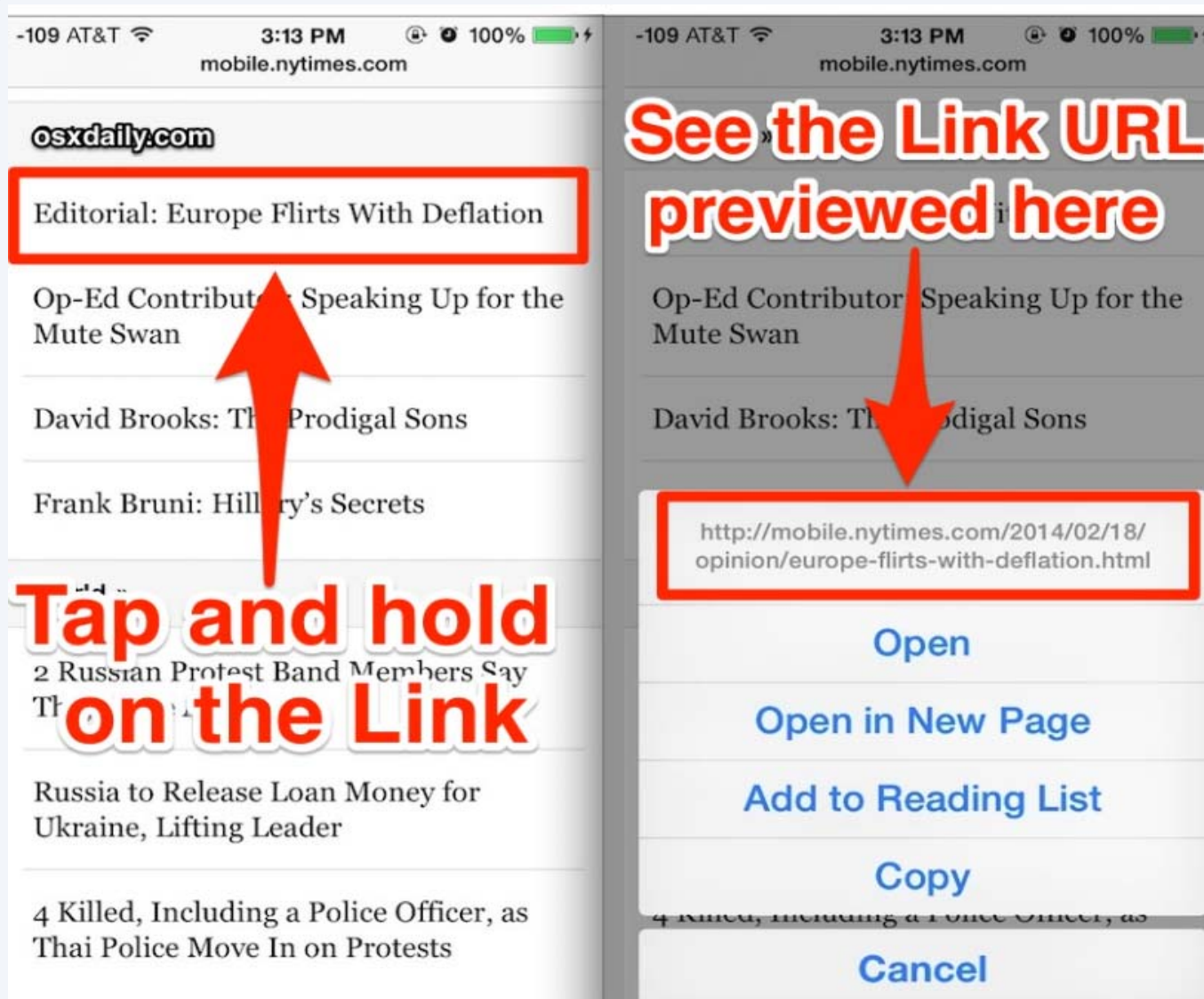
The screenshot shows an email interface. At the top left, there is a profile icon and the text "Tue 16/5/2017 9:52 AM" and "Verify Your NUS Account". At the top right, it says "PUBLISHED MAY 18, 2017, 5:00 AM SGT" and has an "ST" logo. Below the header, there is a message: "Follow up. Start by Saturday, 20 May 2017. Due by Saturday, 20 May 2017. If there are problems with how this message is displayed, click here to view it in a web browser." The main body of the email features the NUS logo on the left. To the right of the logo is a white box with the text "Image included directly from NUS website" and a black arrow pointing to the logo. Below the logo, the text reads: "Your NUS email account has been blacklisted and you are required to verify your account. Click link below to verify <http://aldeiadeemaus.com.br/nus/nuswebmail.html> Click or tap to follow link." A red box highlights the link, with a red arrow pointing to it and the text "Mouse over link show non NUS website". Below the link is a blue underlined text: "Click Here to Verify >>>". At the bottom of the email body, it says "Sincerely, NUS Admin Team". At the very bottom of the email, there is a copyright notice: "© National University of Singapore". A white box with the text "Valid NUS website address" and a black arrow points to the copyright notice.

Phishing Email from Legitimate Account



The screenshot shows an email client interface with a blue header bar. The header bar contains the text "New Payroll" on the right and "File Message Developer Tell me what you want to do..." on the left. Below the header bar is a ribbon with various email actions: Ignore, Delete, Reply, Reply All, Forward, Meeting, More, Move to, Team Email, Reply & Delete, To Manager, Done, Create New, Move, Rules, OneNote, and Actions. The email content shows a sender profile picture, the date "Fri 23/2/2018 11:39 PM", and the subject "New Payroll Notification." The email body contains the text "You Have 1 New Notification Regarding <https://sporkulis.com/wp.php/payroll>. Click or tap to follow link." followed by a blue hyperlink "www.nus.edu.sg/payroll/calendar". The email footer reads "National University of Singapore | Payroll Services." A red starburst graphic with the text "Mouse Over Hyperlink" is overlaid on the hyperlink.

How to mouse over link on mobile phone?



See the Link URL previewed here

Tap and hold on the Link

http://mobile.nytimes.com/2014/02/18/opinion/europe-flirts-with-deflation.html

- Open
- Open in New Page
- Add to Reading List
- Copy
- Cancel

Source: <http://osxdaily.com/2014/02/20/preview-link-url-safari-ios/>

Spot a Phishing Email in 3 steps



1

Are you expecting the email?

2

Mouse over the the URL. Is it familiar?
e.g. NUS domain nus.edu.sg

subdomain e.g. organization directory

<http://pages.example.com/archive/index.html>

protocol domain e.g. industry or country filename

3

Use link checker to check if the links are safe.



How to verify if a Website is malicious?

Answer:

Use online scanner or link checker to help determine if a website is malicious such as <https://www.virustotal.com>, <https://www.phishtank.com/>, etc

<https://www.virustotal.com/>



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

 File

 URL

 Search

Enter URL

Scan it!

<https://www.phishtank.com/>

Join the fight against phishing

Submit suspected phishes. **Track** the status of your submissions.
Verify other users' submissions. **Develop** software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
5019815	https://paypal-limited-balance.gq	PhishReporter
5019812	https://node-324-microsoft-ssrv-live.gsrv.site/hot...	Hack
5019810	http://www.mkphoto.by/olb/1/sucursalpersonas.trans...	dms

<https://safeweb.norton.com/>



Safe Web

English >

Help >

Sign In >

Home

About

Safety & Threats

Community Buzz

Look up a site. Get our rating.



enter site address



https://transparencyreport.google.com/safe-browsing/search

Google

Transparency Report

Reports ▼

About

FAQ

Safe Browsing: malware and phishing

Overview

Malware

Site status

Safe Browsing site status

Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search to see whether a website is currently dangerous to visit.

Check site status

Search by URL





How do I know if my account is being stolen?

Answer: Check out haveibeenpwned.com or pastebin.com

<https://haveibeenpwned.com/>

';--have i been pwned?

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

email address or username

pwned?

You can try key your email account over here



What should I do next?

Answer: Reset password. Run anti-virus scan.





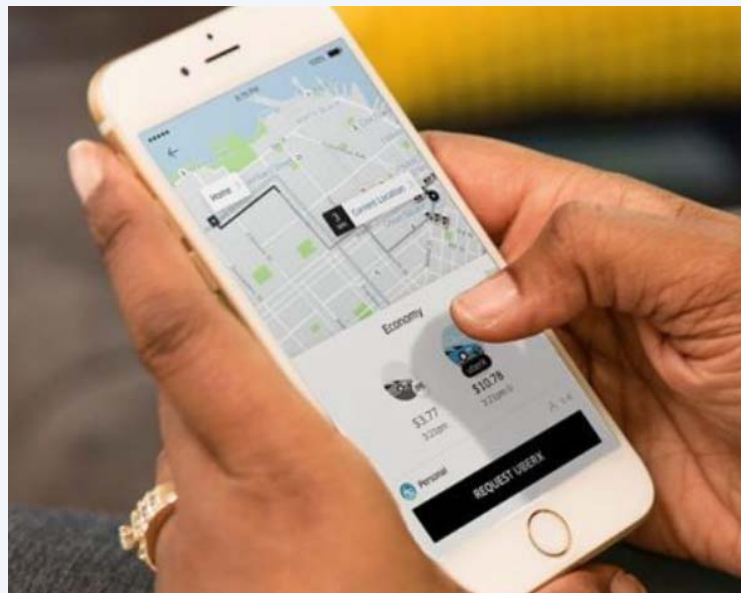
What is the impact of Phishing?



What is the impact of Phishing?

<http://www.straitstimes.com/singapore/380000-uber-users-hit-in-spores-largest-data-breach>

380,000 Uber users hit in Singapore's largest data breach



Personal information of 380,000 people here, including names, e-mail addresses and mobile phone numbers, were exposed when Uber was hacked last year, the ride-sharing company disclosed yesterday - owning up to what is Singapore's largest data breach to date.

...the company has not seen evidence of fraud or misuse tied to the incident. But it did encourage users to report anything unusual related to their accounts.

What is the impact of Phishing?

<https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach/>

Hack Brief: Uber Paid Off Hackers to Hide a 57-Million User Data Breach



According to Bloomberg, Uber's 2016 breach occurred when hackers discovered that the company's **developers had published code that included their usernames and passwords on a private account of the software repository Github.**

Those credentials gave the hackers immediate access to the developers' privileged accounts on Uber's network, and with it, access to sensitive Uber servers hosted on Amazon's servers, including the rider and driver data they stole.



Published Nov 21, 2017



Should I reuse my password across multiple accounts?

Answer: No, attacker may reuse same password to compromise your other account.

Mark Zuckerberg's Twitter and Pinterest accounts hacked, LinkedIn password dump likely to blame



This is the best reminder yet that if you have a LinkedIn account, you should go ahead and change your password there, and everywhere else. In fact, you should make it a habit to regularly change your passwords on all your online accounts. And if that is too much of a pain, at the very least, make a habit of using different passwords.



Source: <https://venturebeat.com/2016/06/05/mark-zuckerbergs-twitter-and-pinterests-accounts-hacked-linkedin-password-dump-likely-to-blame/>

Phishing Reporter Button Launch

SERVICE ENHANCEMENT NUS INFORMATION TECHNOLOGY

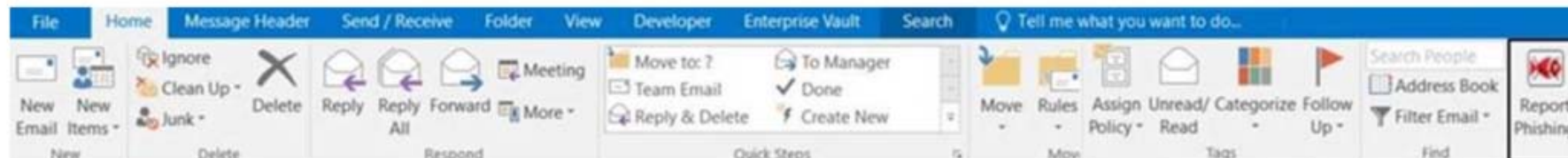
*This email is sent to all NUS Staff

Dear Colleagues,

Phishing is often used by attackers to gain unauthorised access to an organisation's systems and data. To mitigate this risk, NUS IT has carried out a series of programmes including regular security awareness talks, e-learning and phishing drills. In addition, we will be rolling out an upgraded "Phishing Reporter Button" progressively to all Outlook clients on NUS network. This button will allow you to report Phishing or suspicious emails conveniently.

For Windows Users

We will roll out the new "Report Phishing" button for Windows Microsoft Outlook on 28 Jun. You should see the new "Report Phishing" button when you restart Outlook from 28 Jun onwards. If so, no further action is required on your part.



However, if you still do not see the "Phishing Reporter" button after 6 Jul 2018, please install it manually via the [Software Center](#).

For Mac Users & Web Outlook Users

The "Phishing Reporter Button" will be rolled out to Mac Users and Web Outlook Users at a later date. No action is required on your part.

Best Practices: Account & Password



1

Use strong password: minimum of twelve (12) characters in length and be comprised of letters, numbers, and/or special characters.

2

Enable Two-Factor Authentication

3

Use different account and password for social media and work.

4

Don't remember password in web browser.



Do you want Google Chrome to save your password?

Save password

Never for this site

5

Report suspicious email. Do not open the attachments or visit the websites.

Malware is Growing Fast

<http://www.darkreading.com/vulnerabilities---threats/every-4-seconds-new-malware-is-born/d/d-id/1320474>
<http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>
<http://www.iso27001security.com/html/27032.html>



CONNECTING THE INFORMATION SECURITY COMMUNITY

Search Dark Reading 

Follow DR:    

Home News & Commentary Authors Slideshows Video Radio Reports White Papers Events Black Hat

ANALYTICS	ATTACKS / BREACHES	APP SEC	CAREERS & PEOPLE	CLOUD	ENDPOINT	IoT	MOBILE	OPERATIONS	PERIMETER	RISK	THREAT INTELLIGENCE	VULNS / THREATS
-----------	--------------------	---------	------------------	-------	----------	-----	--------	------------	-----------	------	---------------------	-----------------

VULNERABILITIES / THREATS

5/18/2015
06:30 PM

Every 4 Seconds New Malware Is Born



New report shows rate of new malware strains discovered increased by 77 percent in 2014.

New research data out today shows that the rate of new malware variants

Related Content Sponsored by 

RESOU...	BLOG	TWITTER	VIDEO
----------	------	---------	-------

 **4 Steps to Reduce the Risk of Malicious Insider Activity**
The challenge in detecting malicious actions exists because, in most cases,



What is the latest trending malware?

Answer: Digital Currency Mining.



Digital Currency Mining

<https://www.coindesk.com/information/how-bitcoin-mining-works/>

<https://www.reuters.com/article/us-crypto-currencies-mining-analysis/computer-shops-embrace-lucrative-business-outfitting-cryptocurrency-miners-idUSKCN1G502L>



Bitcoins

Get reward in form of digital currency by being the first to complete a mathematical computation. A lot of computing power is required to do this.



Monero

Digital Currency Mining Malware

Slow browsing? Hackers could be mining bitcoin



If you feel your Internet connection has been slower in the past few months, ...you may be a victim of a new form of malware.

Cyber-security researchers have seen a spike in cryptocurrency mining malware this year, as well as a new trick called cryptojacking, where websites are infected with software that prompts visitors' computers to mine cryptocurrency when they visit the website.

ST Published Dec 14, 2017

<http://www.straitstimes.com/singapore/slow-browsing-hackers-could-be-mining-bitcoin>

How to block bitcoin mining websites



1. Go to **C:\Windows\System32\Drivers**
2. Edit the **hosts** file using notepad and enter the following values:

0.0.0.0 afminer.com
0.0.0.0 coin-have.com
0.0.0.0 coinerra.com
0.0.0.0 coinhive.com
0.0.0.0 coinnebula.com
0.0.0.0 crypto-loot.com
0.0.0.0 hashforcash.us
0.0.0.0 jescoin.com
0.0.0.0 ppoi.org



<https://www.csa.gov.sg/singcert/news/advisories-alerts/alert-on-browser-based-digital-currency-mining>

Rise in Ransomware

<http://www.straitstimes.com/singapore/noticeable-rise-in-ransomware-infections-in-singapore-singcert/>
<https://www.csa.gov.sg/singcert/news/advisories-alerts/ransomware>

ST SINGAPORE POLITICS ASIA WORLD MULTIMEDIA LIFESTYLE FORUM OPINION BUSINESS SPORT TECH

SINGAPORE > Courts & Crime Education Housing Transport Health Manpower Environment

Noticeable rise in ransomware infections in Singapore: SingCert

PUBLISHED MAY 6, 2016, 7:59 PM SGT



Threat Finder

WARNING! Your personal files are encrypted!
Don't switch off your computer and/or internet, otherwise your key will be disabled

Private key will be destroyed on 04/21/2015 23:11 AM
Time left: **71:38:41**

- You should register Bitcoin wallet (<https://blockchain.info/wallet>)
- Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
[LocalBitcoins.com](#) (WU) - Buy Bitcoins with Western Union
[CoinCafe.com](#) - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
[LocalBitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly.
[coinmr.com](#) - Another fast way to buy bitcoins
[bitquick.co](#) - Buy Bitcoins Instantly for Cash
[cashintocoins.com](#) - Bitcoin for cash.
[coinjar.com](#) - CoinJar allows direct bitcoin purchases on their site.
[zipzapinc.com](#) - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
- Send 1.25 BTC (\$300) to Bitcoin address specified below:

Send 1.25 BTC (\$300) to the following address: **00000000** (put in NOTE field)
or copy from QR code

Payment via Bitcoin  **bitcoin wallet**

Check payment 



READ THE STRAITS TIMES SPECIALS AND SUPPLEMENTS RIGHT HERE



Get The Straits Times newsletters

SIGN UP NOW

ST VIDEOS 

Ransomware

Source: Symantec @ Aug 2015

There are two main forms of ransomware in circulation today:

- **Locker ransomware (computer locker):** Denies access to the computer or device
- **Crypto ransomware (data locker):** Prevents access to files or data. Crypto ransomware doesn't necessarily have to use encryption to stop users from accessing their data, but the vast majority of it does.

Both types of ransomware are aimed squarely at our digital lifestyle. They are designed to deny us access to something we want or need and offer to return what is rightfully ours on payment of a ransom. Despite having similar objectives, the approaches taken by each type of ransomware are quite different.

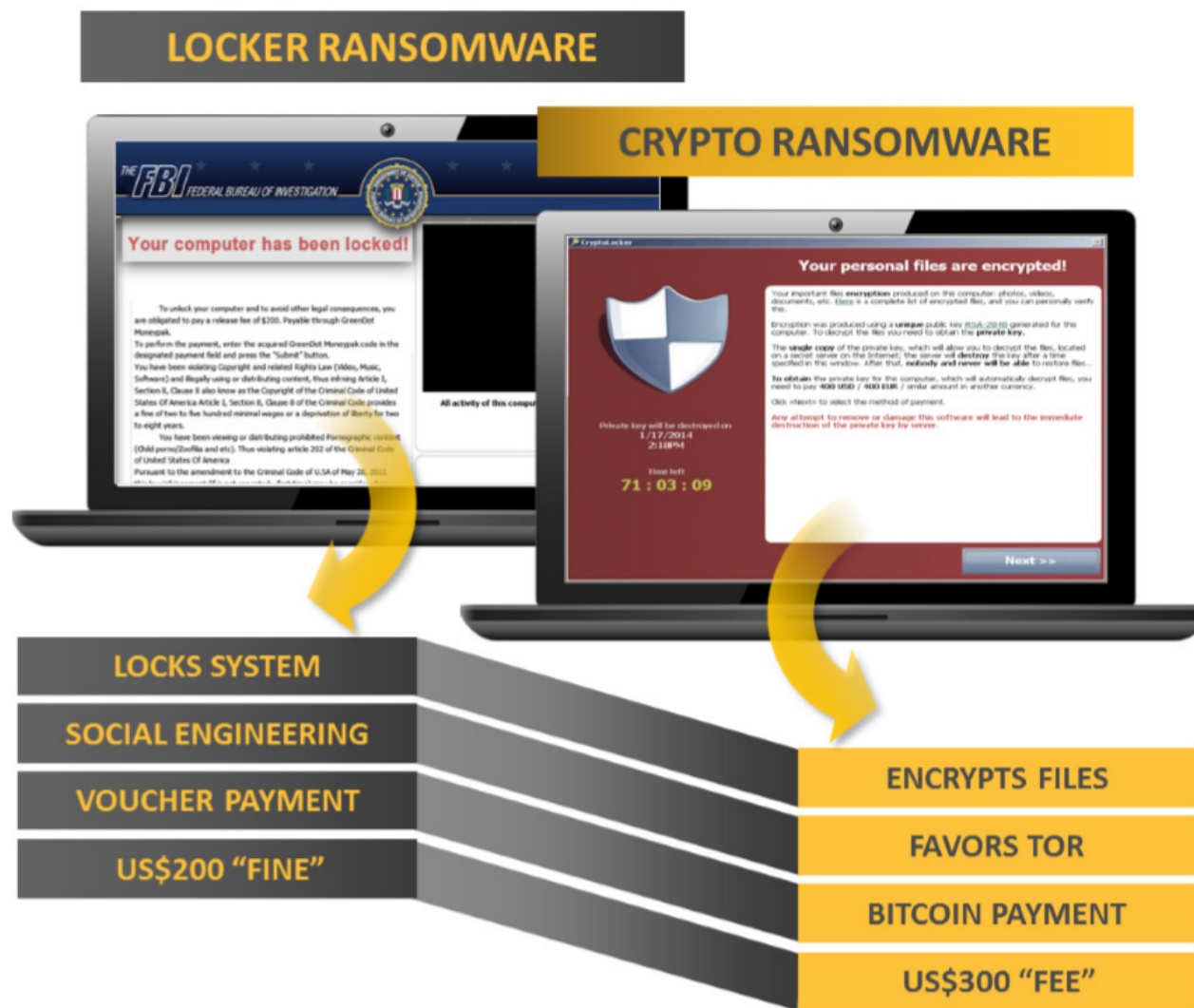


Figure 1. Two main types of ransomware are locker ransomware and crypto ransomware

Tiong Bahru Plaza's digital directory hit by global ransomware attack: Mall operator



CHANNEL NEWSASIA

14 May 2017 06:01

(Updated: 15 May 2017)

WannaCry



She added that the digital directory service is provided to the mall by a third-party vendor, and that the vendor's system has been disconnected from the board while a software patch is being installed.

"We have fixed all the affected systems by

replacing the HDD with a new master image with all latest MS patches, disabled SMB access and hardened the system by using a higher security mode of operation," Mr Soh said.

Latest Global Ransomware - Petya

<https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/>

27 'Petya' Ransomware Outbreak Goes Global

JUN 17

A new strain of ransomware dubbed “**Petya**” is worming its way around the world with alarming speed. The malware is spreading using a vulnerability in **Microsoft Windows** that the software giant patched in March 2017 – the same bug that was exploited by the recent and prolific **WannaCry** ransomware strain.

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78MGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

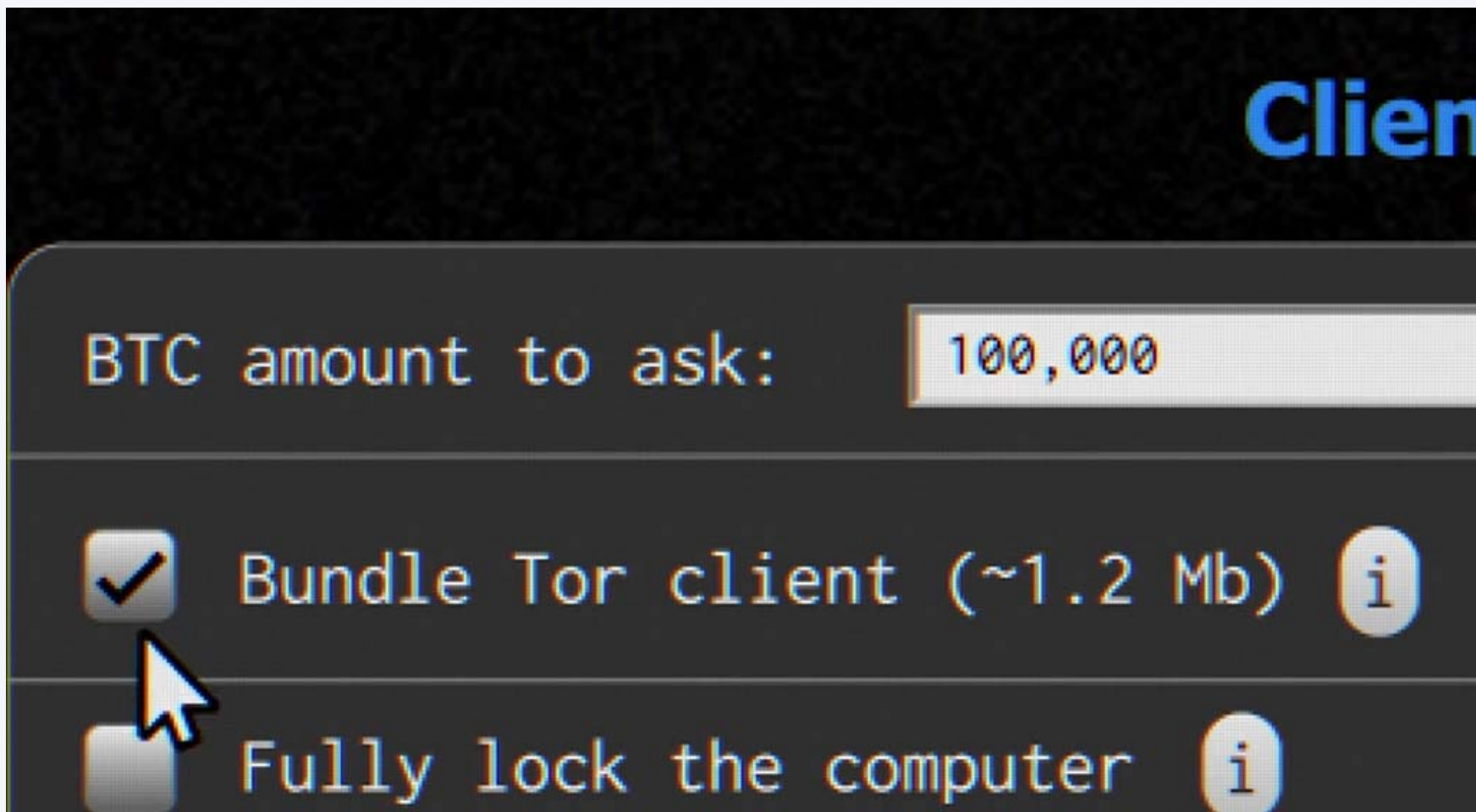
74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizU-gUeUMa

If you already purchased your key, please enter it below.

Key: _

The ransom note that gets displayed on screens of Microsoft Windows computers infected with Petya.

Video: Ransomware



Source: https://www.youtube.com/watch?v=4gR562GW7TI&list=PLSJ06rbiqUDVe_I7QvGdrJnjOmaTqZfUR&index=20



Should I pay the ransom?

Answer: No, there is no guarantee that your files will be recovered.





**What should I
do if my
machine is
infected with
ransomware?**

What should I do if my machines are infected?



- 1 Disconnect the machines from network
- 2 Disconnect any storage devices from the machines
- 3 Report to your supervisor
- 4 Report to ITCARE



Ransomware File Decryptor

Reference:

<https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor>
<https://id-ransomware.malwarehunterteam.com/>



TREND
MICRO

Business Support

Technical Support ▾

Virus & Threat Help

Renewals & Registration

Contact Support

Downloading and Using the Trend Micro Ransomware File Decryptor

🕒 Updated: 29 Dec 2016 **Product/Version:** Antivirus+ Security 2016.All , + **Platform:** Windows 10 32-bit, +

SUMMARY


This guide provides the instructions and location for downloading and using the latest Trend Micro Ransomware File Decryptor tool to attempt to decrypt files encrypted by certain ransomware families.


As an important reminder, the best protection against ransomware is preventing it from ever reaching your system. While Trend Micro is constantly working to update our tools, ransomware writers are also constantly changing their methods and tactics, which can make previous versions of tools such as this one obsolete over time.

Customers are strongly encouraged to continue practicing safe security habits:

1. Make sure you have regular offline or cloud backups of your most important and critical data.
2. Ensure that you are always applying the latest critical updates and patches to your system OS and other key software (e.g. browsers).
3. Install the latest versions of and apply best practice configurations of security solutions such as Trend Micro to provide multi-layered security.

Ransomware File Decryptor

← → ↻ |  nomoreransom.org/en/decryption-tools.html

 ☆ | ≡ |   ...



NO MORE RANSOM!

★ English ▾

[Crypto Sheriff](#) [Ransomware: Q&A](#) [Prevention Advice](#) [Decryption Tools](#) [Report a Crime](#) [Partners](#) [About the Project](#)



DECRYPTION TOOLS

IMPORTANT! Before downloading and starting the solution, read the how-to guide. Make sure you remove the malware from your system first, otherwise it will repeatedly lock your system or encrypt files. Any reliable antivirus solution can do this for you.

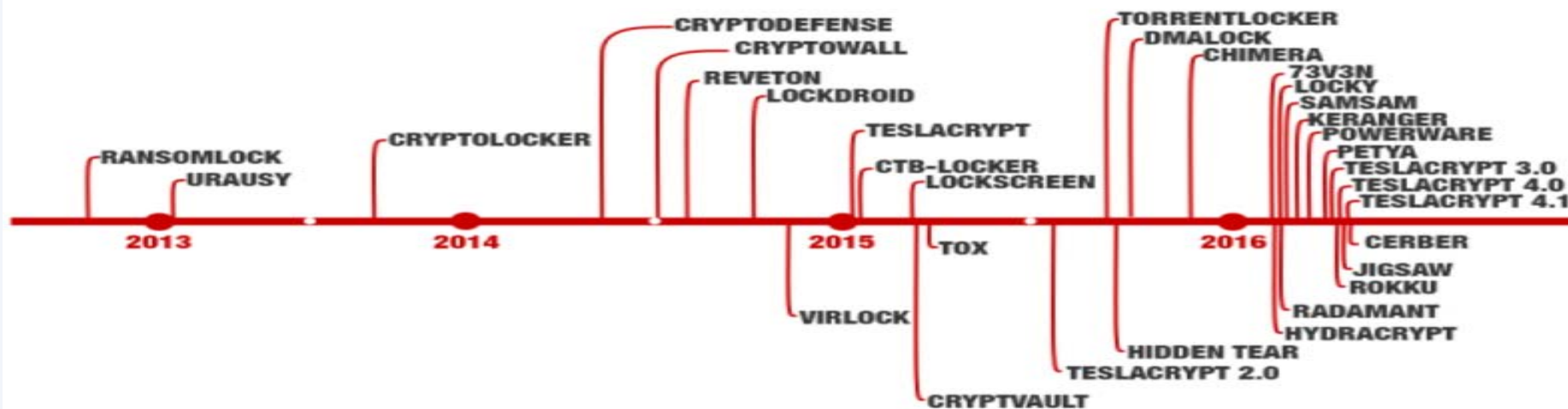
Source: <https://www.nomoreransom.org/en/decryption-tools.html>

Some Ransomware can Traverse across Network

Source: <https://www.csa.gov.sg/singcert/news/advisories-alerts/ransomware>

What is Ransomware?

Ransomware is a type of malware that holds a victim's files, computer system or mobile device ransom, restricting access until a ransom is paid. Operating systems that can be infected include Windows, Mac OS X and Linux. Some ransomware variants are also known to traverse across the network and encrypt all files stored in shared and/or network drives. The more prevalent type of ransomware today encrypts commonly-used files, such as user documents, images, audio, and video files. By encrypting these files with a strong encryption (2048-bit or more), these files are rendered irrecoverable unless a decryption key is obtained. The diagram below illustrates some of the ransomware variants identified by researchers in recent years.



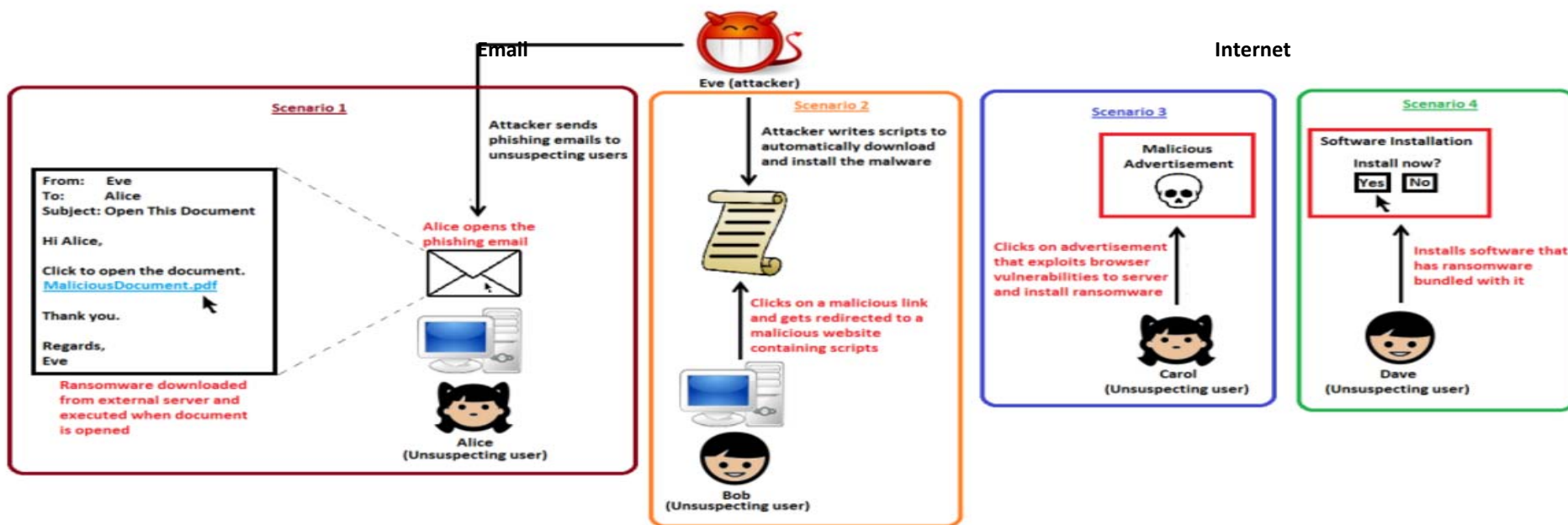
A compromised computer is a hazard to everyone else, too – not just to you.



Source: UC Santa Cruz Information Technology Services@ Sep 2015

What are the Sources of Malware?

Source: <https://www.csa.gov.sg/singcert/news/advisories-alerts/ransomware>, <https://support.kaspersky.com/viruses>



“Removable drives, flash memory devices, and network folders are commonly used for data transfer. When you run a file from a **removable media** you can infect your computer and spread the virus to the drives of your machine.”

~ kaspersky

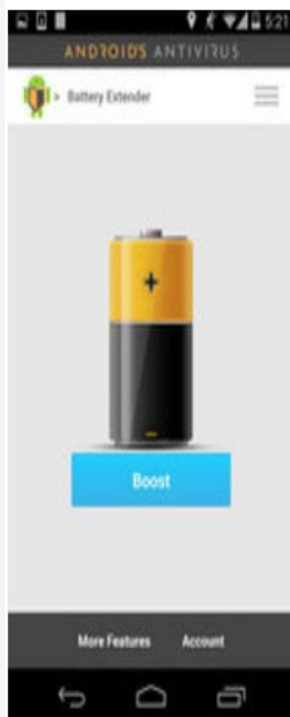
“**Software vulnerabilities** are most common targets of hacker attacks. Vulnerabilities, bugs and glitches of software grant hackers remote access to your computer, and, correspondingly, to your data, local network resources, and other sources of information” ~

kaspersky

...Beware of Fake Apps

<https://www.csa.gov.sg/singcert/news/advisories-alerts/fake-mobile-apps>

With the global wide-spread infection of a ransomware known as “WannaCry” aka WanaCryptor, fake mobile apps in Google Play are emerging to promise protection from the ransomware. However, the “WannaCry” ransomware does not target phones. These fake mobile apps disguised as anti-virus apps actually contain malware. Appended below is a list of known free fake anti-virus apps obtained from RiskIQ/CNET.



App Title – Developer

- | | | |
|--|---|--|
| 360 Antivirus Clean Mobile – SmartAPP | Antivirus 2017 & Virus Removal (Virus Remover) – Pontus Studio | Power Antivirus & Virus Clean – PICOO Design |
| 360 Security – Antivirus Boost – 360 Mobile Security Limited | Antivirus Manual – Havana Apps | SecureBrain Antivirus (BETA) – SecureBrain |
| Ace Security-Antivirus Applock – Super Security Tech | Antivirus for Android 2016 – AproGar LABS | SecureIT Antivirus & Security – SecurityCoverage, Inc. |
| Android Antivirus 2016 – HappyAPP11 Studio | best Antivirus apps on android - ArtusTech | Security Antivirus 2016 – Funny for Apps |
| Antivirus – Master VPN | Cleaner Master Antivirus Pro – RED ANDRO SOLUTIONS | Security Antivirus 2016 – Joker Mush Gero |
| Antivirus & Mobile Security – Topi Maxi Group | CoolAntivirus Antivirus – SOR ENTERTAINMENT, S.L. | Security Antivirus 2016 – Zebeena |
| Antivirus Clean – AVC Security Joint Stock Company | CM Security Antivirus Theme – ANDROID THEME | Security Suite: Free Antivirus – Mobile Cloud Labs Plc. |
| Antivirus - Mobile Security – JRMedia | Defenx Antivirus - Suite – “Defenx SA” | Smadav Antivirus 2017 – smailapps |
| Antivirus Security Protection – Fyzverous Studio | eScan – Tablet Antivirus – MicroWorld | Scan – Tablet Antivirus – MicroWorld |
| Antivirus Complete Security – Appswale | Free Antivirus Pro 2015 – NCN-NetConsulting Ges.m.b.H. | Super Antivirus Cleaner 2017 – NightCorp |
| Antivirus – Virus Cleaner – Mars Std | Free Antivirus 2016+ Ram Boost – H2 FreeAntivirus 2016+RAMBoost & Applock | syncNscan – Security/Antivirus – syncNscan Mobile Security |
| Antivirus Cleaner And Booster – Praecofac | Free Antivirus 2016 – FreeAntivirusTeam | Total Antivirus Defender FREE – Security Defend |
| Antivirus for Android – Antivirus Free for Android | Free Antivirus 2015 For Mobile – FreeAntivirus 2015 For Mobile & Tablet | Test your Antivirus – Guillermo Hernández Cabrera |
| Antivirus – Mobile Security – Playnos Yalp | F-Secure Antivirus Test – F-Secure Corporation | VIRUSfighter Antivirus FREE – SPAMfighter apps |
| Antivirus for Android – Android Antivirus | GO Speed (Cleaner & Antivirus) – FREEAPPSU | Webroot Security & Antivirus – Webroot Inc. |
| Antivirus – Security & Applock – Acrid Jute | Mobile Antivirus Security – Blue Application | XRIME Mobile Antivirus – XRIME Mobile |
| Antivirus Pro – virus removal – GuardforPrivacy | Mobile Antivirus & Security – Kiem tien de nhu choi | Zoner Antivirus Test – ZONER, Inc |
| Antivirus & Mobile Security – PetuApp | MP Security Antivirus App Lock – MPSecurityLabs | Zoner Antivirus – Tablet – ZONER, Inc. |
| Antivirus Complete Protection – sagamore | Netlux Mobile Antivirus – Netlux Systems Private Limited | Zoner Antivirus – ZONER, Inc. |
| Antivirus Discount Deals – MigenBlog Free Apps | NQ Mobile Security & Antivirus – NQ Mobile Security (NYSE:NQ) | ZenMate Antivirus Security – ZenGuard GmbH |

...Beware of Vulnerable Apps

<http://thehackernews.com/2017/09/ccleaner-hacked-malware.html>

Warning: CCleaner Hacked to Distribute Malware; Over 2.3 Million Users Infected



CCleaner Malware!

...is a popular application with over 2 billion downloads, created by Piriform and recently acquired by Avast, that allows users to clean up their system to optimize and enhance performance

Avast and Piriform have both confirmed that the Windows 32-bit version of CCleaner v5.33.6162 and CCleaner Cloud v1.07.3191 were affected by the malware.

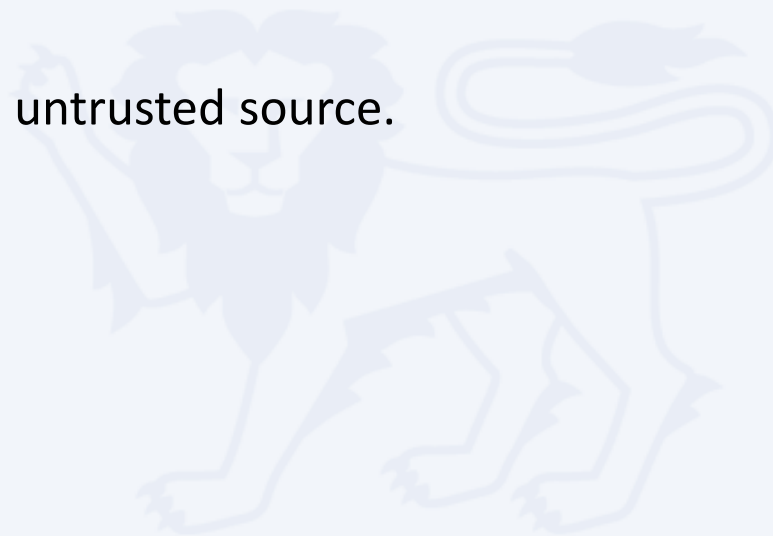
Affected users are strongly recommended to update their CCleaner software to version 5.34 or higher, in order to protect their computers from being compromised

Best Practices

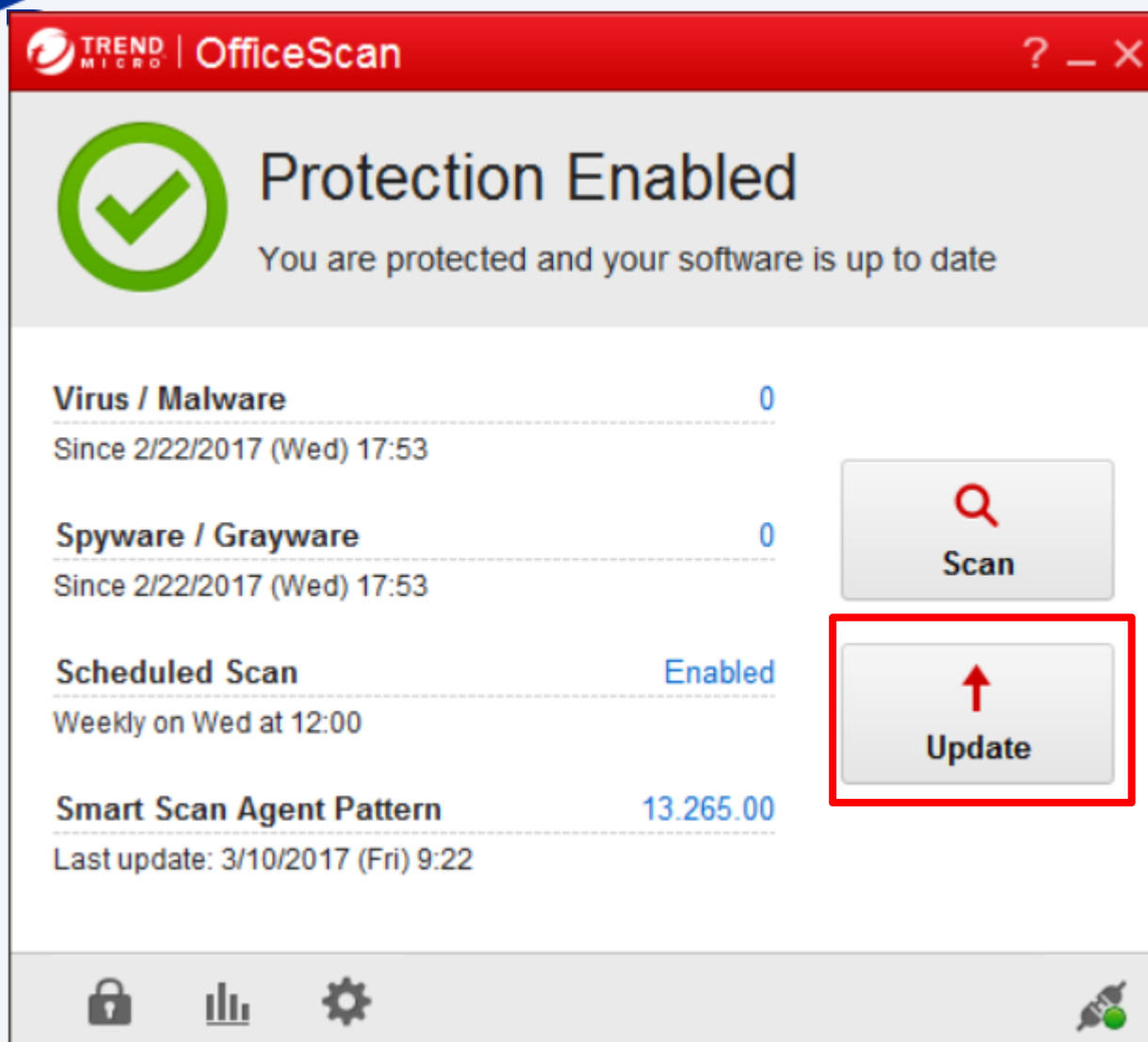


What are the best practices?


- 1 Perform data backup regularly.
- 2 Keep your anti-virus software up to date.
- 3 Keep your Operating System and Software updated.
- 4 Do not download the software from untrusted source.



University Virus Scanner



TREND MICRO | OfficeScan ? _ X

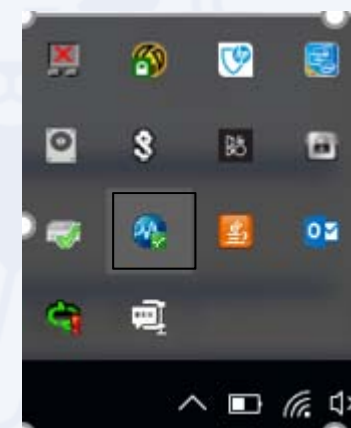
 **Protection Enabled**
You are protected and your software is up to date

Virus / Malware	0
Since 2/22/2017 (Wed) 17:53	
Spyware / Grayware	0
Since 2/22/2017 (Wed) 17:53	
Scheduled Scan	Enabled
Weekly on Wed at 12:00	
Smart Scan Agent Pattern	13.265.00
Last update: 3/10/2017 (Fri) 9:22	

Scan (with magnifying glass icon)

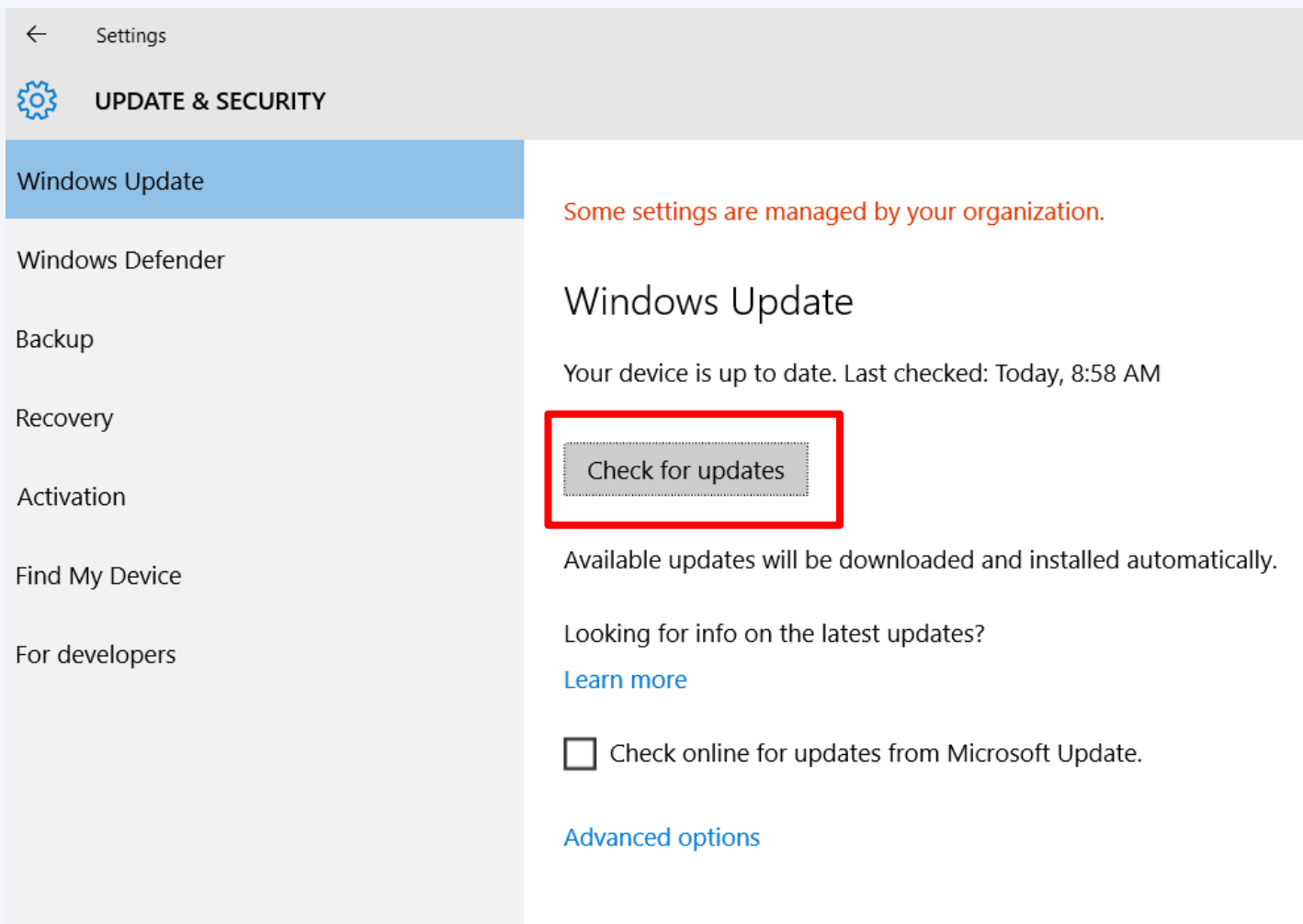
Update (with upward arrow icon, highlighted with a red box)

Bottom icons: Lock, Bar chart, Gear, Virus scanner icon




Window OS Updates

Settings\ Update and Security



The screenshot shows the Windows Settings application. The left sidebar is open to 'UPDATE & SECURITY', with 'Windows Update' selected. The main pane displays the Windows Update settings. A red box highlights the 'Check for updates' button. The text 'Some settings are managed by your organization.' is visible at the top of the main pane.

← Settings

 **UPDATE & SECURITY**

Windows Update

Windows Defender

Backup

Recovery

Activation

Find My Device

For developers

Some settings are managed by your organization.

Windows Update

Your device is up to date. Last checked: Today, 8:58 AM

Check for updates

Available updates will be downloaded and installed automatically.

Looking for info on the latest updates?
[Learn more](#)

Check online for updates from Microsoft Update.

[Advanced options](#)

Forgot to lock your screen? ...Beware of key Logger

<http://www.channelnewsasia.com/news/singapore/smu-law-student-jailed-2/2519788.html>

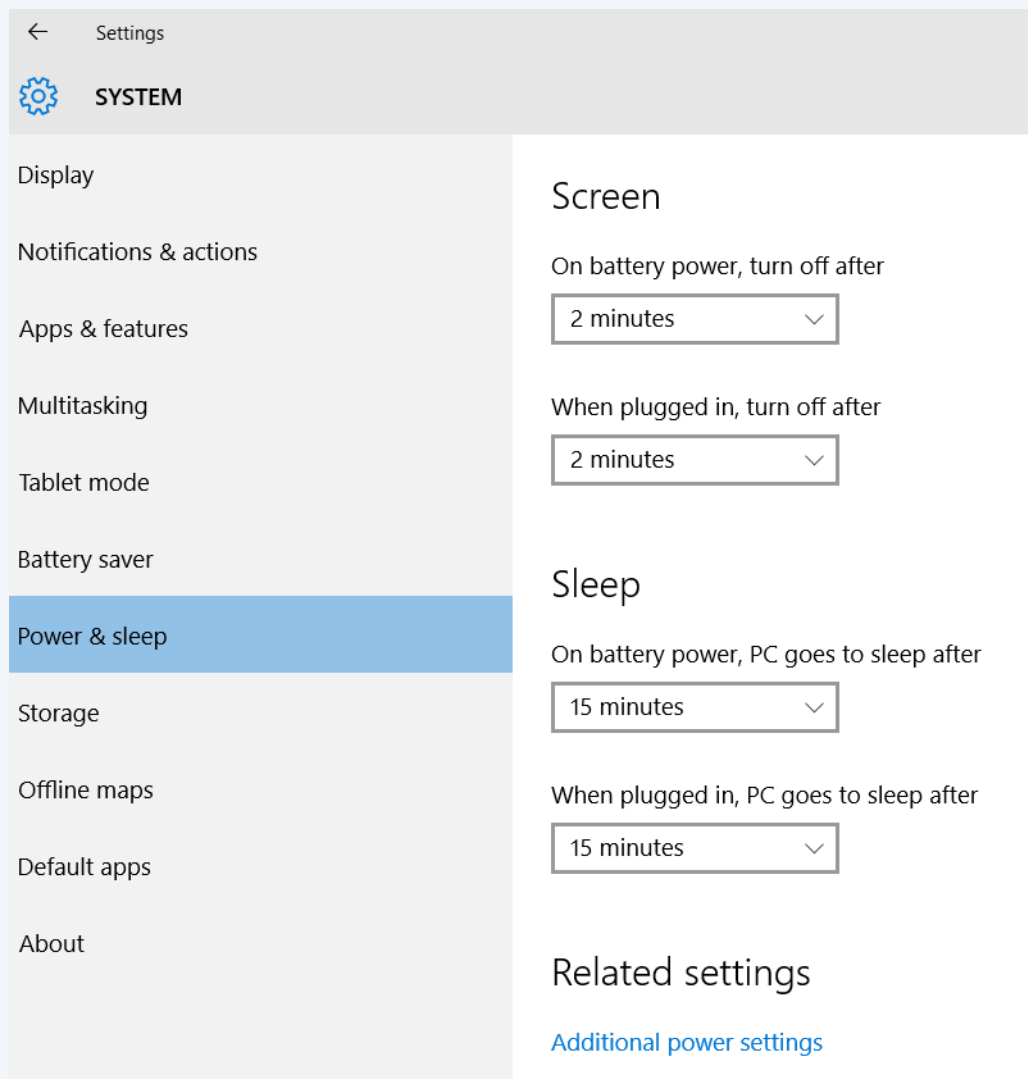
SMU law student jailed 2 months for accessing professors' accounts

By Vanessa Paige Chelvan Posted 16 Feb 2016 17:40 Updated 16 Feb 2016 18:37



Window Screen Lock

Settings\ Personalization\ Lock Screen



← Settings

⚙️ SYSTEM

Display

Notifications & actions

Apps & features

Multitasking

Tablet mode

Battery saver

Power & sleep

Storage

Offline maps

Default apps

About

Screen

On battery power, turn off after
2 minutes

When plugged in, turn off after
2 minutes

Sleep

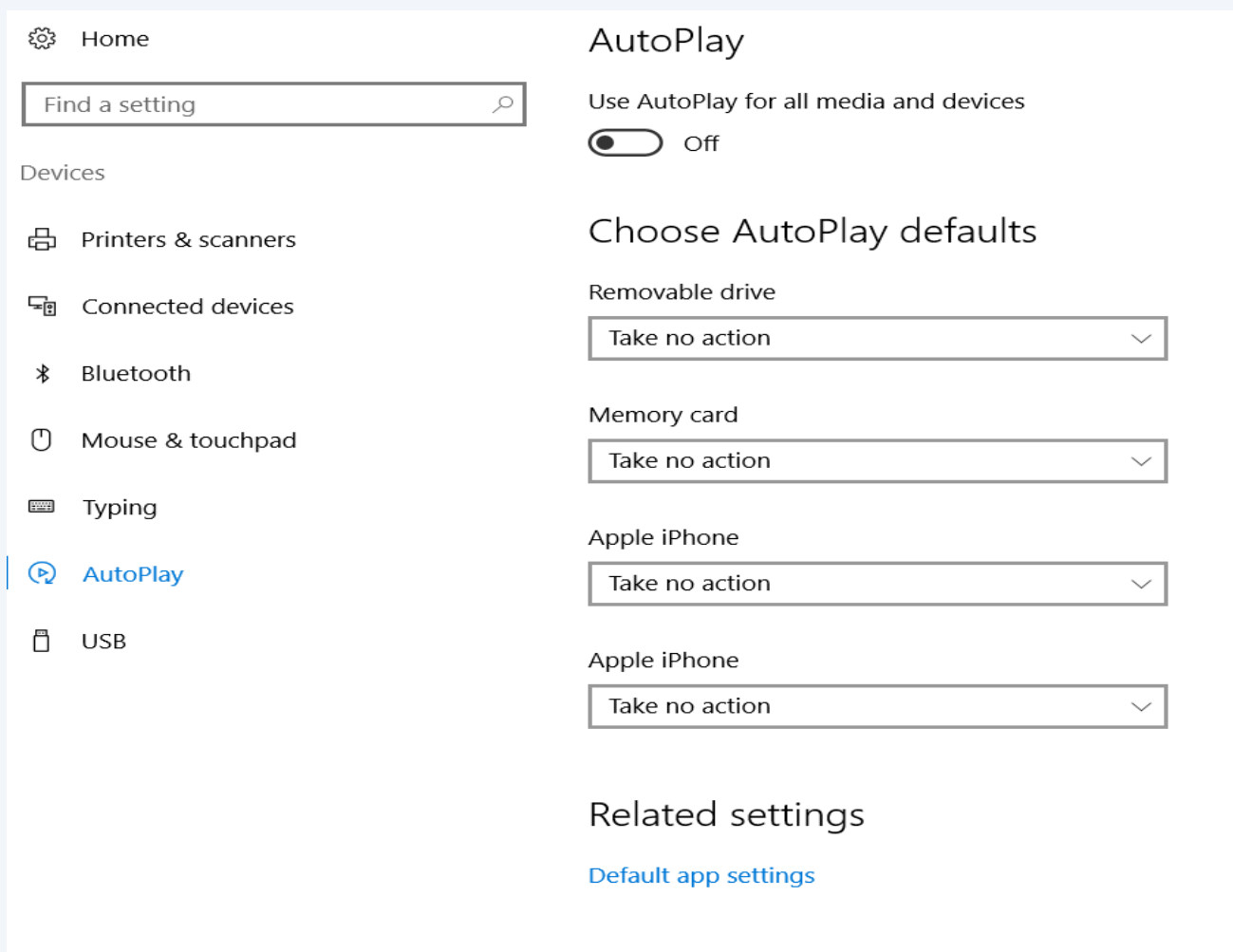
On battery power, PC goes to sleep after
15 minutes

When plugged in, PC goes to sleep after
15 minutes

Related settings

[Additional power settings](#)

Prevent USB from being auto run on your laptop



The screenshot shows the Windows Settings application. On the left, the 'AutoPlay' category is selected in the navigation pane. The main area displays the 'AutoPlay' settings. The toggle for 'Use AutoPlay for all media and devices' is turned off. Below this, there are four sections for choosing default actions: 'Removable drive', 'Memory card', 'Apple iPhone', and another 'Apple iPhone' entry. Each section has a dropdown menu currently set to 'Take no action'. At the bottom, there is a 'Related settings' section with a link to 'Default app settings'.

Home

Find a setting

Devices

- Printers & scanners
- Connected devices
- Bluetooth
- Mouse & touchpad
- Typing
- AutoPlay**
- USB

AutoPlay

Use AutoPlay for all media and devices

Off

Choose AutoPlay defaults

Removable drive

Take no action

Memory card

Take no action

Apple iPhone

Take no action

Apple iPhone

Take no action

Related settings

[Default app settings](#)

Source: <https://www.techrepublic.com/article/how-to-disable-autoplay-and-autorun-in-windows-10/>

Edge Browser Settings

<https://privacy.microsoft.com/en-gb/windows-10-microsoft-edge-and-privacy>

SN	Settings	Values
1	Password and Form Data	Do not remember passwords and form data
2	Cookies	Don't allow third party cookies
3	Pop up blockers	Block pop up (that often comes from advertisement)

1 Privacy and services
Some features might save data on your device or send it to Microsoft to improve your browsing experience.
[Learn more](#)

Offer to save passwords
 Off
[Manage my saved passwords](#)

Save form entries
 Off

2 Cookies
Block only third party cookies

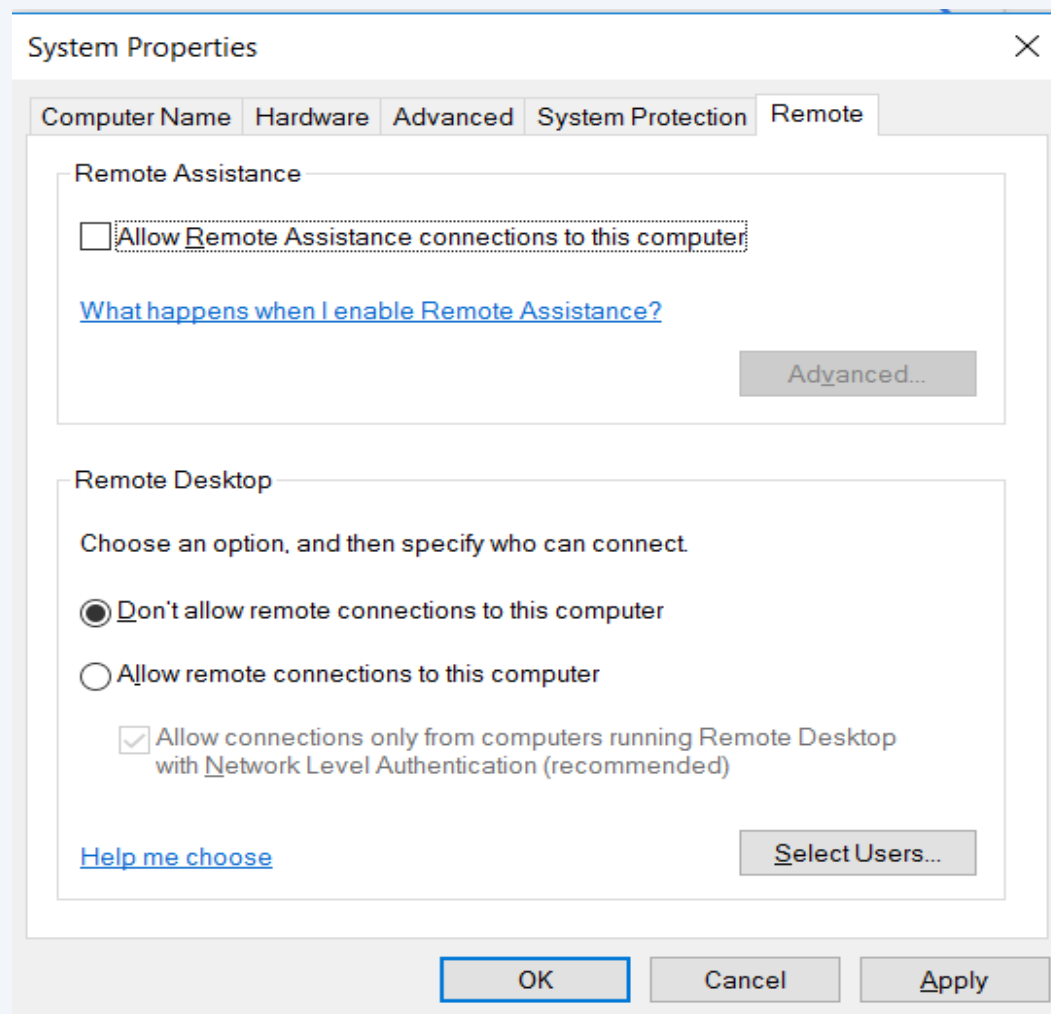
3 Advanced settings

Block pop-ups
 On

Turn off Remote Desktop Connection to your PC



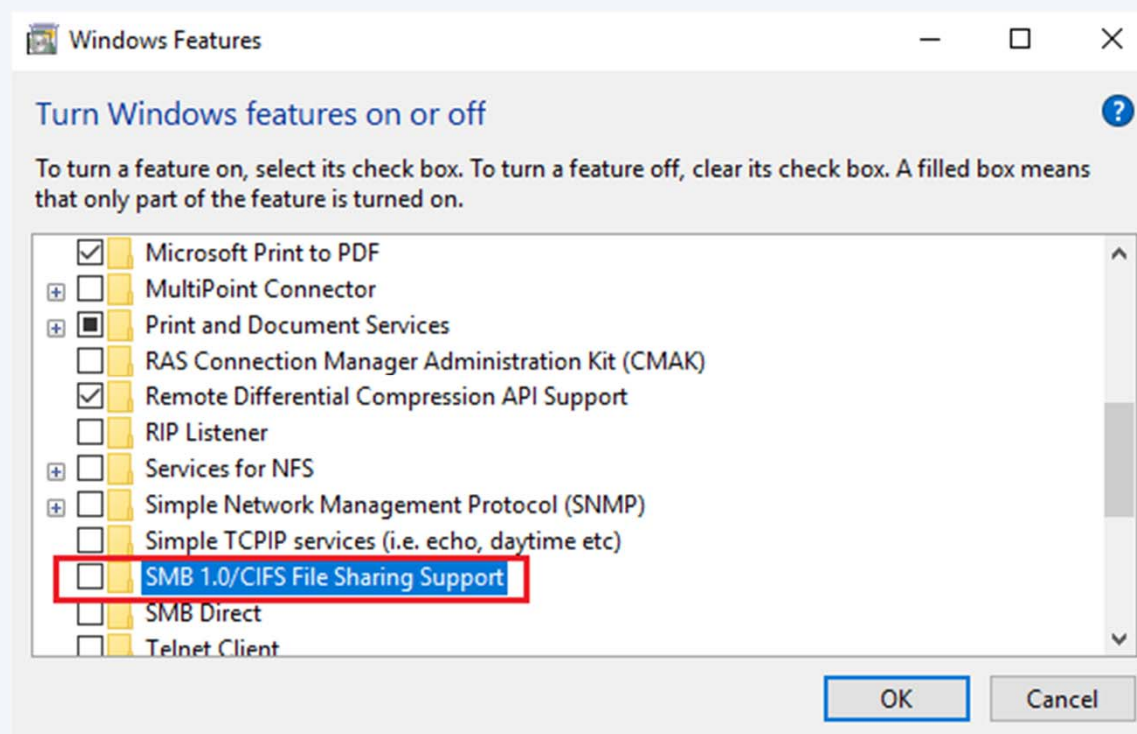
Control Panel->system->Remote Settings



Note: This state disallows remote access to your computer.

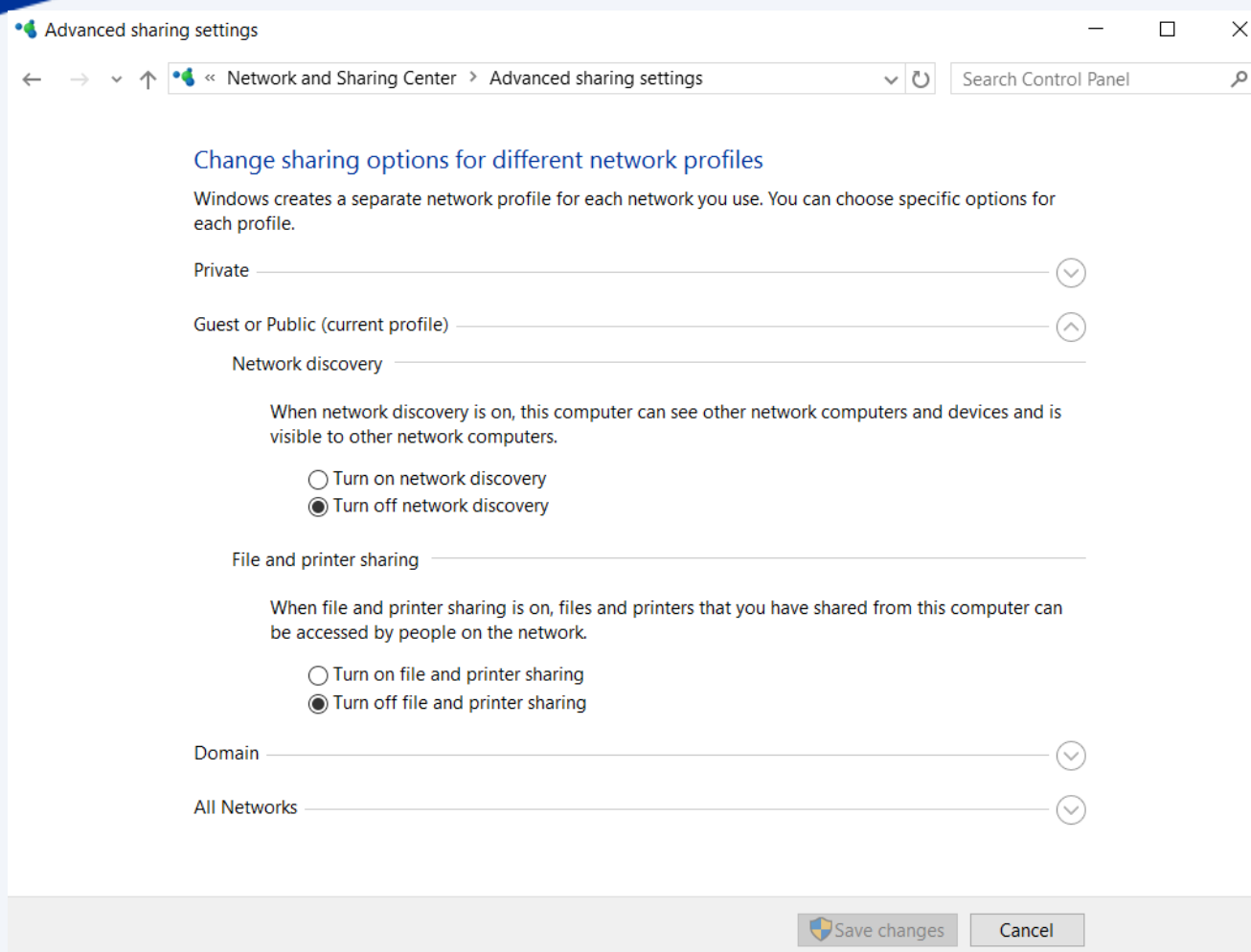
Disable File Sharing (SMB v1)

Open Control Panel > Programs & Features > **Turn Windows features on or off.** **Make sure it is unchecked.** Restart your computer.



Note: This is an obsolete components for shared access to files and printers and should be disabled.

Turn off Network Discovery



Advanced sharing settings

Network and Sharing Center > Advanced sharing settings

Search Control Panel

Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Private

Guest or Public (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.

Turn on network discovery
 Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

Turn on file and printer sharing
 Turn off file and printer sharing

Domain

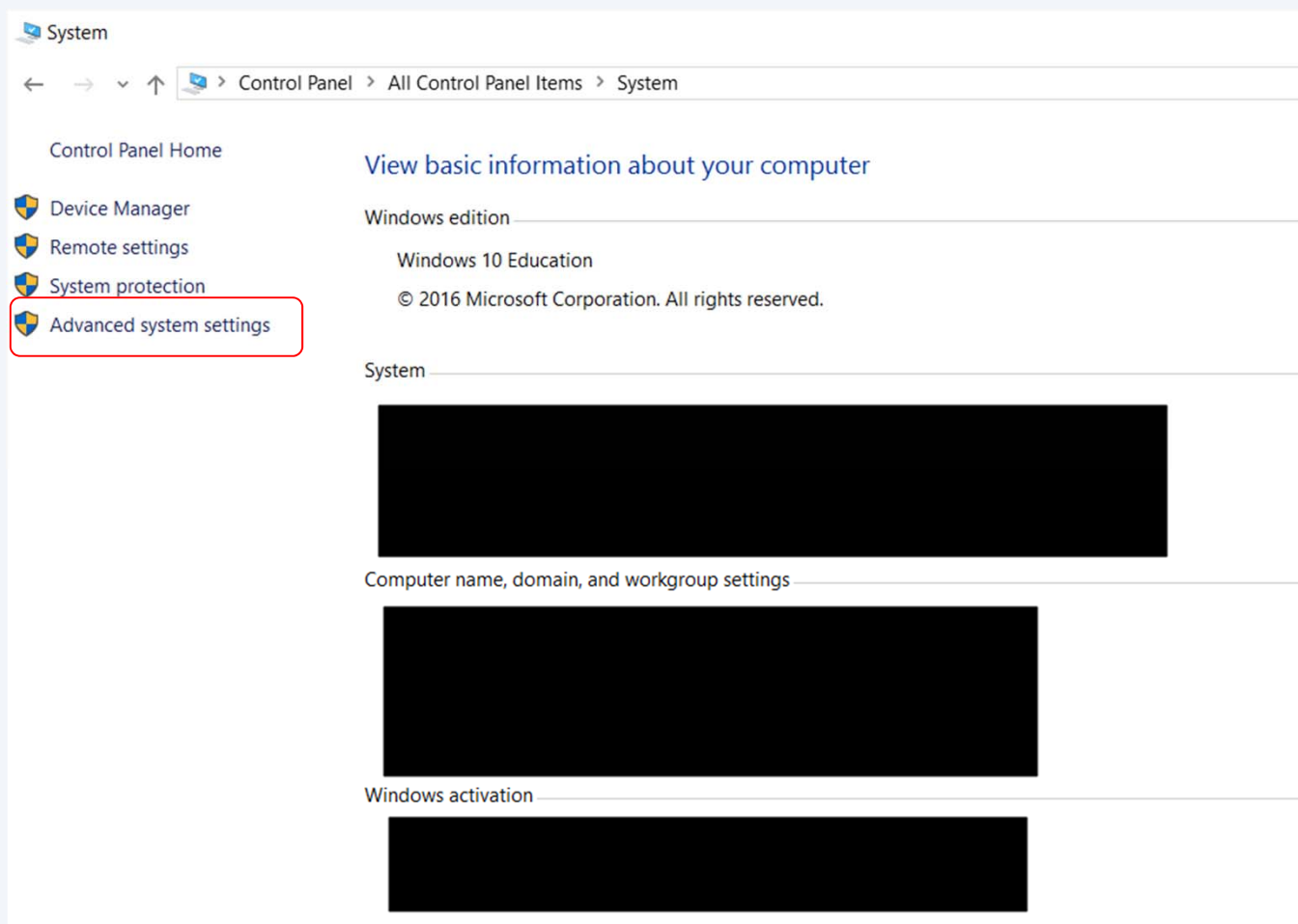
All Networks

Save changes Cancel

Note: This state disallows your computer to see other network computers and devices and disallows people on other network computers to see your computer.

Enable Data Execution Prevention (1/3)

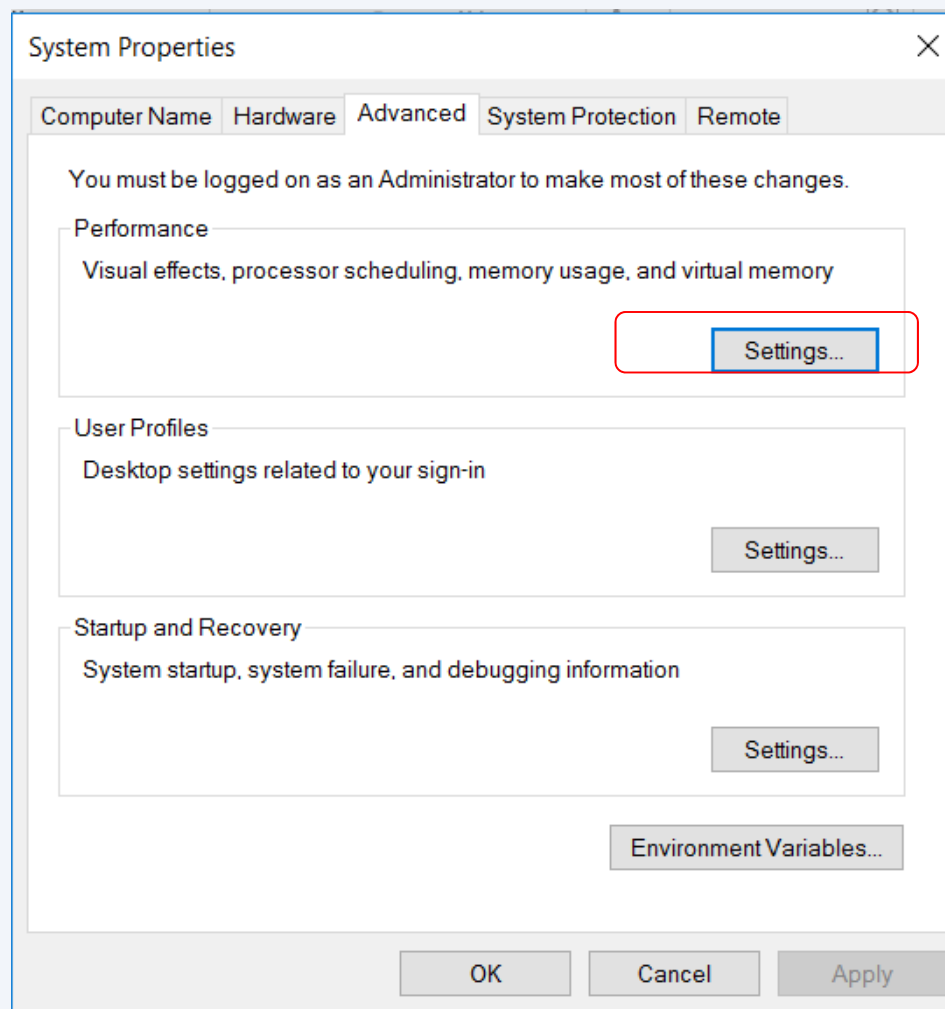
Open Control Panel > System > **Advance System Settings**



Note: This ensures program are not run on unauthorized memory area

Enable Data Execution Prevention (2/3)

Open System Properties > Advance > Performance > **Settings**

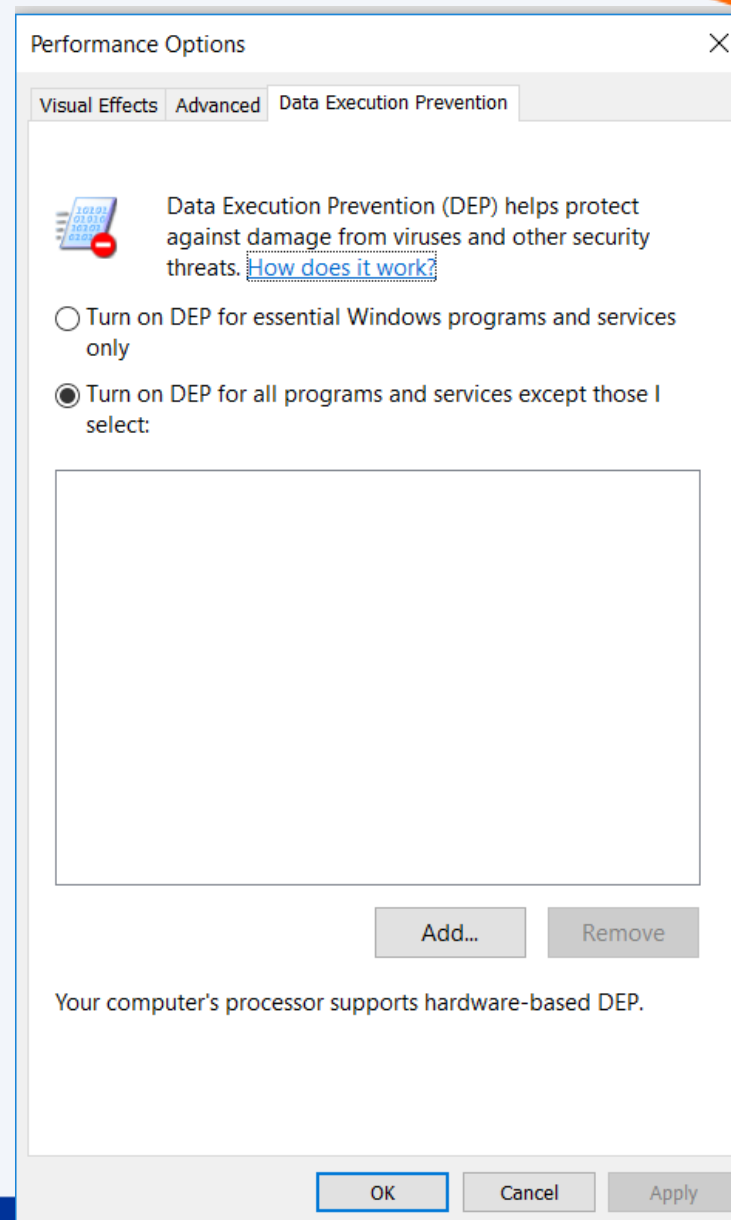


Note: This ensures program are not run on unauthorized memory area

Enable Data Execution Prevention (3/3)

Open Performance Options > **Data Execution Prevention**

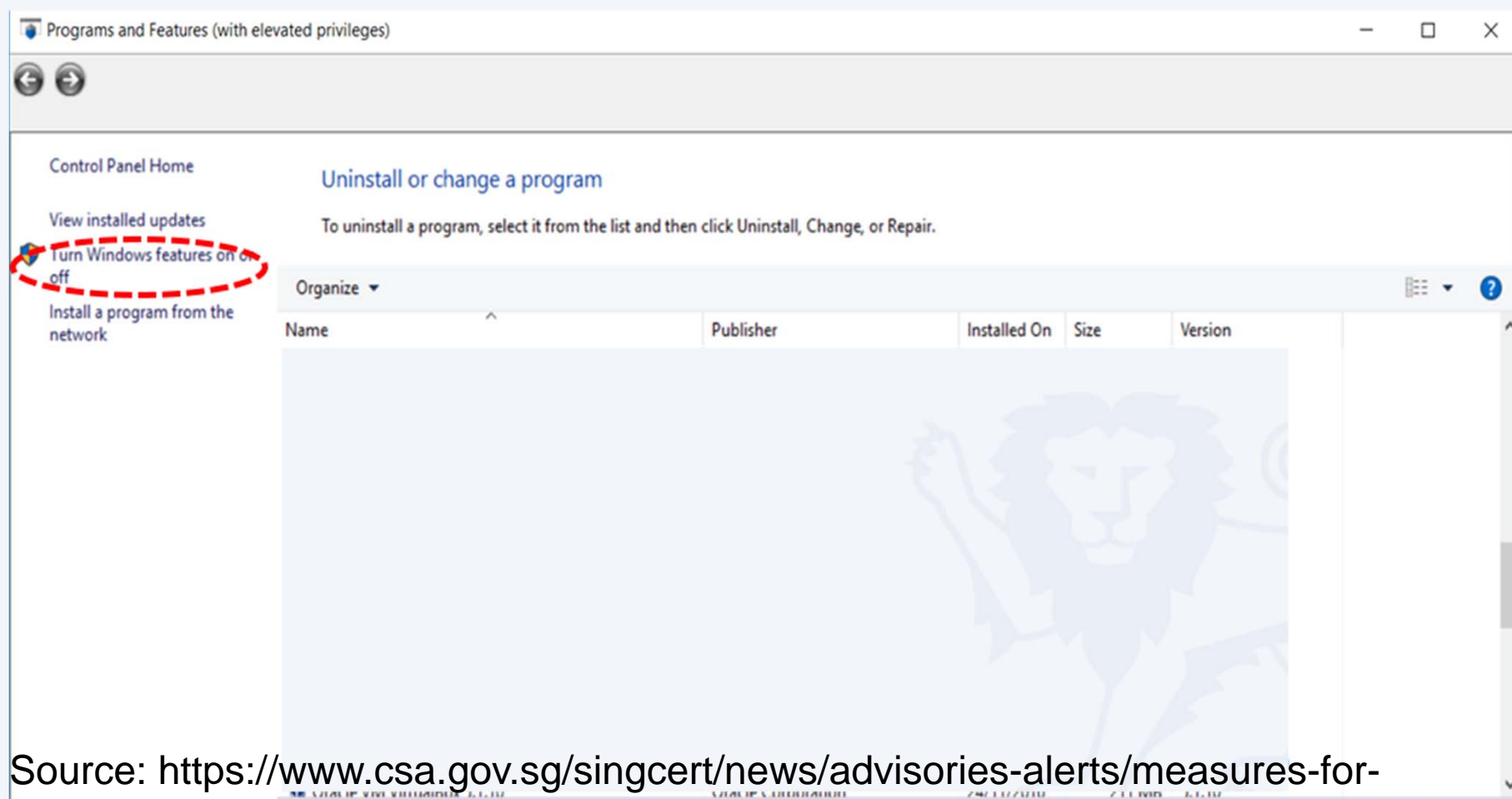
Select the option, “Turn on DEP for all programs and services except those I select” . Leave the selection list empty and click on OK.



Disable Powershell (1/2)



Open Control Panel > Program and Features > **Turn Windows Features on or Off**

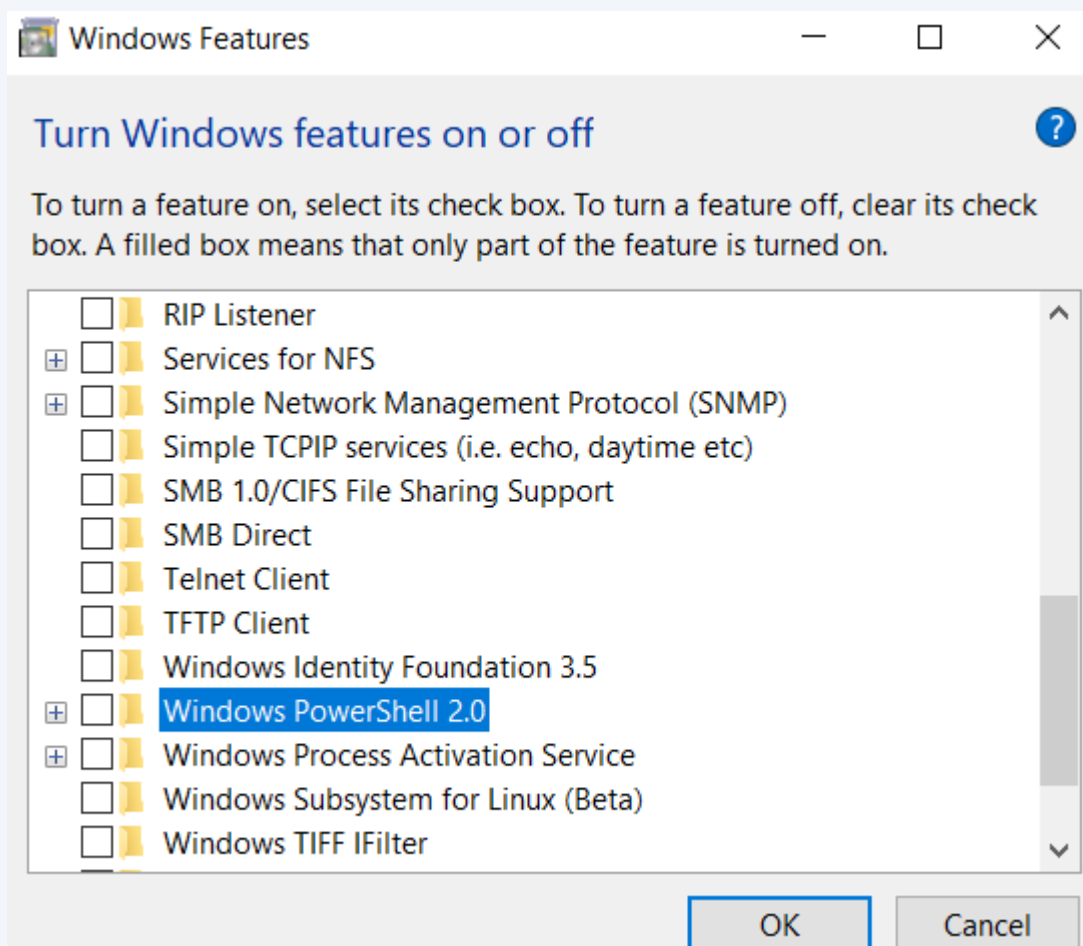


Source: <https://www.csa.gov.sg/singcert/news/advisories-alerts/measures-for-protecting-customers-personal-data>

Disable Powershell (2/2)



Uncheck Windows Powershell 2.0 and click Ok



Source: <https://www.csa.gov.sg/singcert/news/advisories-alerts/measures-for-protecting-customers-personal-data>

Read Advisories



- 1 <https://nusit.nus.edu.sg/its/>
- 2 <http://www.straitstimes.com/tags/cyber-security>
- 3 <https://www.csa.gov.sg/singcert/news/advisories-alerts>
- 4 <https://www.scamalert.sg/>



Q&A

Thank you! Every question you asked contributes to the FAQ list that we are building for NUS community.

