



IT Security Awareness Talk
By NUS IT
June 2018 @ Duke

Outline

1. Information Security Objectives and Policies
2. Data Protection Measures
3. Trending Cyber-attacks Techniques and 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

Flaw in LinkedIn AutoFill Plugin Lets Third-Party Sites Steal

Your Data

📅 Saturday, April 21, 2018 👤 Swati Khandelwal

 Share   Share  Tweet  Share



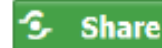
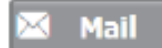
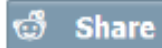
Not just Facebook, a new vulnerability discovered in LinkedIn's popular AutoFill functionality found leaking its users' sensitive information to third party websites without the user even knowing [...]

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

Integrity Breach

Over 20 Million Users Installed Malicious Ad Blockers From Chrome Store

📅 Thursday, April 19, 2018 👤 Mohit Kumar

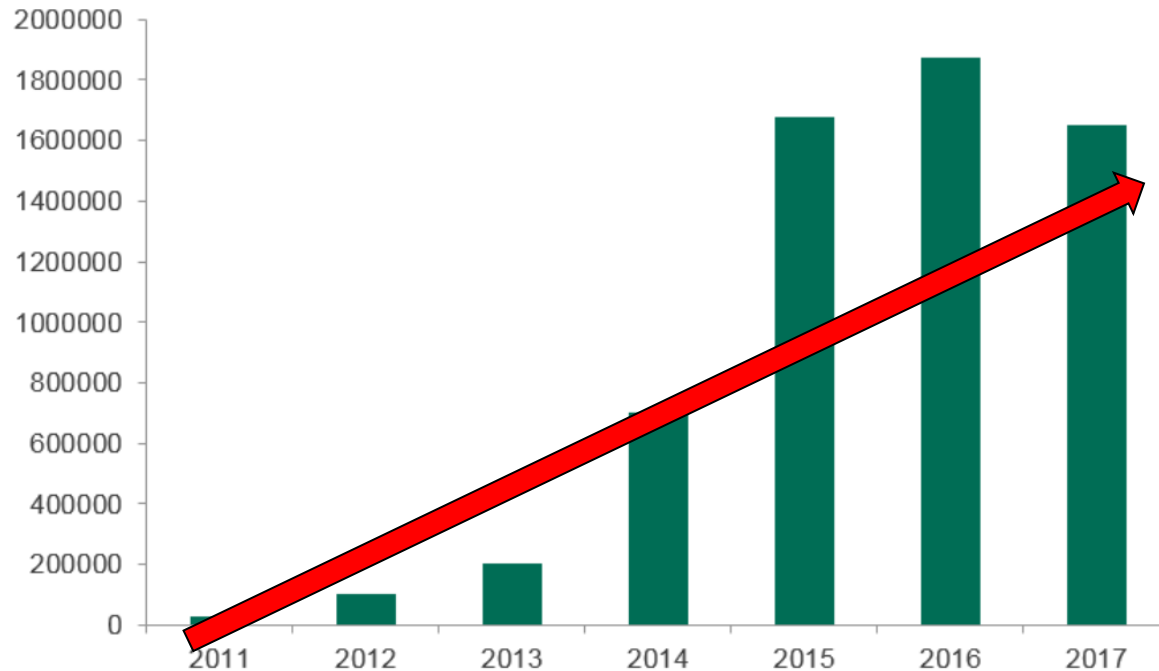


If you have installed any of the below-mentioned Ad blocker extension in your Chrome browser, you could have been hacked. A security researcher has spotted five malicious ad blockers extension in [...]

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/>

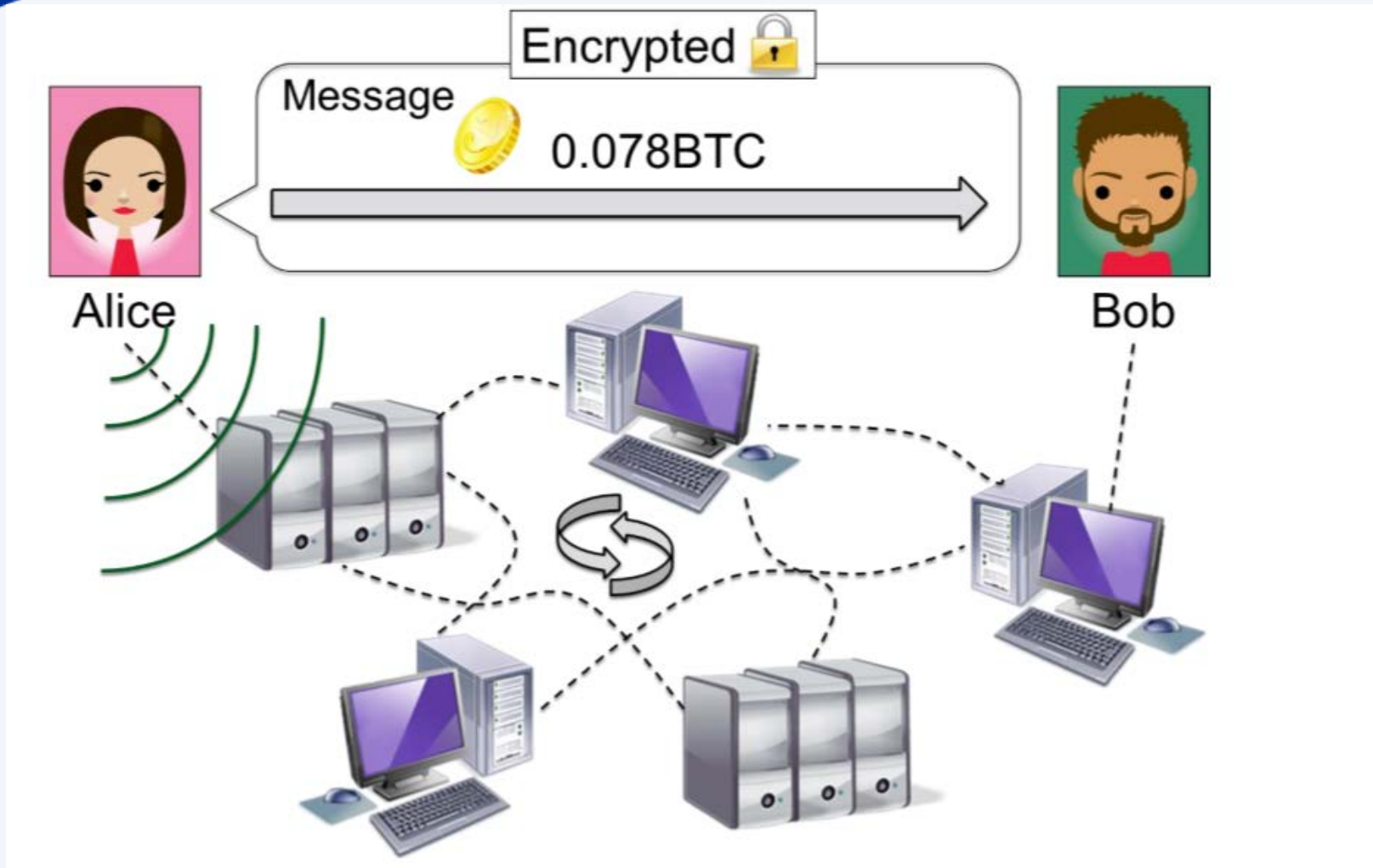
Massive Brute-Force Attack Infects WordPress Sites with Monero Miners



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/>

How cryptocurrencies work?



Source:
<https://skbi.smu.edu.sg/sites/default/files/skbife/HowDoCryptocurrenciesWorkErnieTeo.pdf>



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



Roles and Responsibilities in Information Security

System
Owner

Roles

User

IT Staff

Responsible to Comply to Policies, Circulars, Advisories

Overview of Information Security Policies

IT Security

Acceptable Use (for NUS IT resources)

Guidelines for Acceptable Use (for 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



**What is the latest
NUS IT guidelines
published this
year?**



SECURITY ANNOUNCEMENT

NUS INFORMATION TECHNOLOGY

Dear Colleagues,

Revisions to Acceptable Use Policy and Introduction of Guidelines for Acceptable Use

With the evolving IT landscape impacting current work practices, we note that there has been an increasing trend of NUS faculty and staff using personal devices at work, working remotely using public WiFi, and departments managing their email servers to meet specific needs.

To mitigate the risk of compromising confidentiality of University data, **all Academic Appointment Holders (e.g. Deans, Directors, Heads, etc.), Executive and Professional Staff and Non-academic Staff are required to use their university-assigned email accounts for all official correspondence with immediate effect.** Please refer to the revised [NUS IT Acceptable Use Policy \(AUP\)](#) for more details. The NUS IT **AUP** specifies the appropriate behaviour and use of IT resources by students, faculty, staff and authorised users in an effective, ethical and lawful manner. It is important to manage any potential risk while ensuring that the **AUP** stays relevant to support your IT needs.

We also wish to draw your attention to the [New Guidelines for Acceptable Use](#), which highlights the risks and best practices associated with the use of public WiFi, personal notebooks and departmental email servers.

If you need any information or clarification, please contact me (leongboon@nus.edu.sg) or Eileen Goh (ccegise@nus.edu.sg).



Can I use Goggle Email for Official correspondences?

Answer: No, with revised AUP (version 4.2 dated 1 Feb 2018), all Executive and Professional staff, Non-Academic staff and Senior Academic staff shall only use their University Assigned Email Accounts for official correspondence.

Applying Information Security Policies

	Policy	How does it apply to me?	
		Chapters /Clauses	Use Cases
1	IT Security	<ul style="list-style-type: none"> • Chp 4 - Access Control Security • Chp 10 – System Development and Maintenance • Chp 6 - Physical and Environmental Security 	<p>System Owner</p> <ul style="list-style-type: none"> • Review user accounts and access rights on Information System • Request for Security Assessment <p>User</p> <ul style="list-style-type: none"> • Lock screen when you walk away from your computer • Report security incident to ccecert@nus.edu.sg immediately
2	Acceptable Use for IT resources	<ul style="list-style-type: none"> • Computer Misuse and Cybersecurity Act • Spam Control Act • Copyright Act 	<ul style="list-style-type: none"> • No sharing of account or password • No spamming



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

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)

Applying Information Security Policies

	Policy	How does it apply to me?	
		Chapters /Clauses	Use Cases
3	Software Terms of use	<ul style="list-style-type: none"> Para 3 – Appropriate use of NUS Software 	<ul style="list-style-type: none"> Install licensed Software on NUS computers for use only during course of employment with NUS
4	Software Management	<ul style="list-style-type: none"> Para 3 (iii) - Policy 	<ul style="list-style-type: none"> Software used are appropriately licensed and inventoried
5	Guideline for personal computer and equipment	<ul style="list-style-type: none"> Para 1.1 Qualified Corporate Mobile Devices 	<ul style="list-style-type: none"> Use Qualified Corporate Devices <p>https://staffportal.nus.edu.sg/staffportal/it/equipmenttender</p>

Software Audit Circular dated 20th Oct 2016

1. Software License Records

Faculties and departments must keep an up-to-date **software inventory register** and documentary proof of software licenses purchased.

2. Use of Licensed Software in NUS-Owned Equipment

Faculties and departments are to ensure that only **software with licenses purchased are installed in NUS-owned equipment**. The actual installations must correspond with the licenses purchased. The [Software Inventory Reports](#) may be referenced to determine if additional licenses are required.

3. Acceptable Use of Shareware

Shareware is software that is freely available for download from the internet. In most cases, it is for non-commercial use only and **Institutes of Higher Learning (IHLs) are excluded**. Faculty and staff must check the shareware owner's End User License Agreement (EULA) if use by IHLs is free or requires the paid version.

4. Anti-Malware Software

The **University licenses TrendMicro OfficeScan** as the standard anti-malware software to protect University computers, allowing proper centralized management of the virus definitions and updates. Computers found without TrendMicro OfficeScan or with an outdated version **must have the software installed and updated** immediately. Faculty or staff responsible for the computers may install the software from [Software Center](#).

5. Use of Unauthorized Software

Faculty and staff must not use **unauthorized software** on NUS-owned equipment.



Can I use Shareware?

**Answer: Most shareware are free for personal use only.
Read the terms and conditions to verify.**

Applying Information Security Policies

SN	Policy	How does it apply to me?	
		Chapters /Clauses	Use Cases
7	Data Management	<ul style="list-style-type: none"> • Chp 3- Data Classification • Chp 4 – Data Administration (Data Collection, Sharing, Reporting Loss) 	<ul style="list-style-type: none"> • Classify the University Data handled (NUS Confidential, NUS Restricted, NUS Internal, Public) • Report data loss or leakage cases immediately to cceda@nus.edu.sg
8	Guideline to classification and protection of University data	<ul style="list-style-type: none"> • Section D – Measures to protect University Data 	<ul style="list-style-type: none"> • Sure data on laptop (using EFS), external USB storage (using Bitlocker) and email (e.g. password protect personal data file sent via email)
9	Cloud Policy	<ul style="list-style-type: none"> • Para 5.5 – Self Subscribed cloud service (for public or NUS Internal) • Para 6 – Enterprise Subscribed cloud service (NUS Confidential, NUS Restricted) 	<ul style="list-style-type: none"> • Subscribe to appropriate cloud services depending on the data classification and risk assessment (contact NUS IT Cloud Policy@nus.edu.sg for cloud assessment)

5. Self-Subscribed Cloud Service

- 5.1. This would include Cloud Services like DropBox, Facebook, Google Doc, Google Drive, Prezi and Piazza, etc. For corporate data, excluding teaching materials and research data, there shall be no Self-Subscribed Cloud Service involving NUS Confidential, NUS Restricted or personal data as the terms of Cloud Services agreement from Cloud Service Providers (CSPs) are often non-negotiable. User shall approach his/her department and consider Enterprise-Subscribed Cloud Service by conducting proper risk assessment and legal reviews. For corporate data that are classified as NUS Internal and meant for internal audience only, staff may consider Self-Subscribed Cloud Service but user access to Cloud shall be restricted and authenticated.



How do I know if I can use a cloud solution for conducting NUS business?

Answer:

Contact [NUS IT Cloud Policy@nus.edu.sg](mailto:NUS_IT_Cloud_Policy@nus.edu.sg).



Who must comply to IT Security Policy?

Answer: IT Security Policy Chap 1 Clause 3.4.1

3.4.1 Every staff, student and external party that has dealings with NUS information system resources is responsible for protecting and preserving the information in accordance with NUS IT Security Policy



Can I share IT Security Policy with my partners?

Answer: Yes, IT Security Policy Chap 1 Clause 3.6.3

3.6.3 Where access is required by Supplier to University Data and IT Resources, Supplier is required to sign NDA and comply with AUP, IT Security Policy, Data Management Policy and Guideline on Use, Classification and Protection of University Data where applicable.

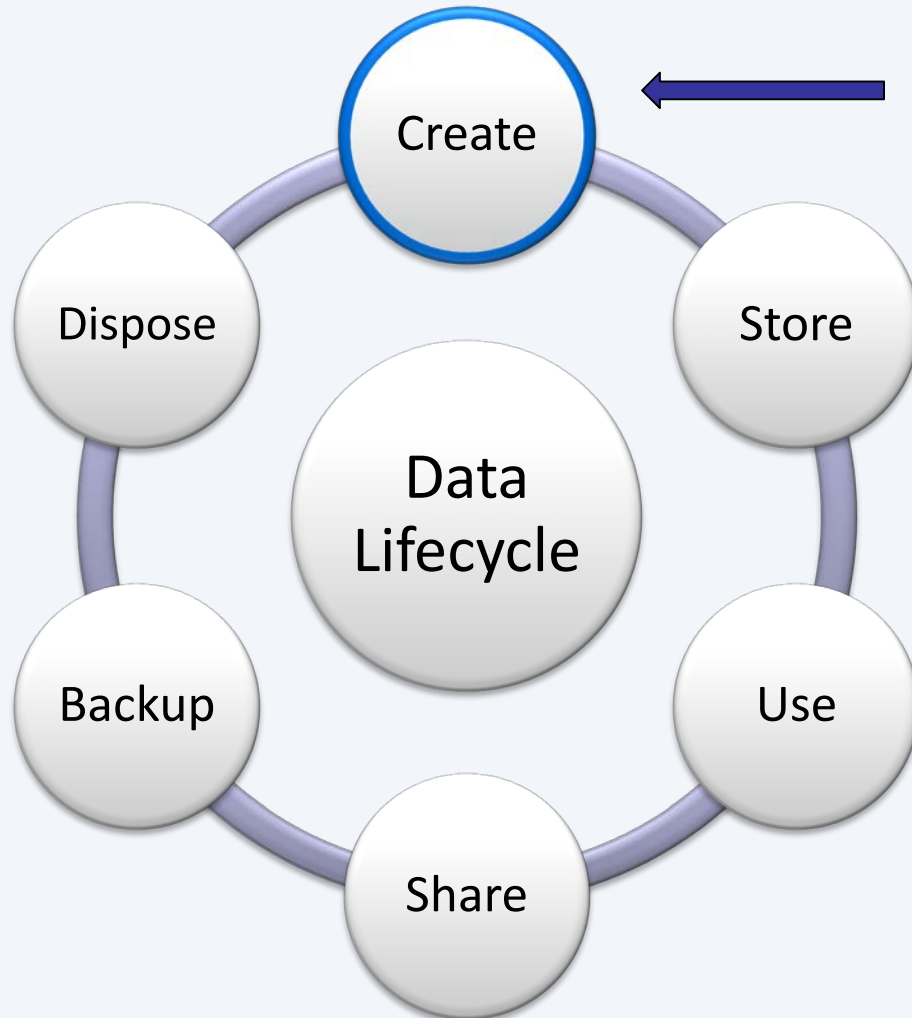
Data Protection Measures



***Security is
lifestyle!***

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

Data Lifecycle & Data Protection Best Practices



**Classify data as
NUS-Internal,
NUS-Restricted or
NUS-Confidential.**



NUS-Confidential Data

Documents, information, or materials which are sensitive or critical, including proprietary information, for use within NUS by authorised personnel on a need-to-know basis. Release of NUS Confidential data may result in financial loss, potential litigation and severe damage to the reputation and interests of NUS, or the individual or entity to which the documents, information or materials relate.

Examples:-

- Staff **salary**
- Staff **appraisal**
- Examination **marks/grades** (including CAP and SAP) and examination questions
- **Admission** data (results, admission points, criminal records)
- **Medical** records (including medical and case history, diagnosis, case note, etc)
- **Donor** records
- **Credit card/Bank account information** (including bank account number, name of payee, amount, etc. excluding staff number)
- **NRIC/FIN** (including unique identification number such as Singapore NRIC, FIN, employment pass no., work permit no., student pass no., etc)
- Information relating to significant **University initiatives or collaborations** which are **being negotiated**

NUS-Restricted Data

Documents, information, or materials other than those classified as NUS Confidential which are for use within NUS by authorised personnel on a need-to-know basis, including those which NUS has a contractual obligation to protect and all personal data as defined and classified in the DMP or any other applicable policy, procedure or guideline. Release of NUS Restricted data may involve damage to the reputation and interests of NUS, or the individual or entity to which the documents, information or materials relate.

Examples:-

- Student, current and ex-staff and alumni records (e.g. alumni **employment details**, including aggregated, banded and/or de-identified salary information of alumni and graduates), **research grant information and data**, certain **management information and reports**, and **information covered by confidentiality obligations**.
- Personal Data
 - a. **Identification numbers** (staff number, matriculation number)
 - b. **Personal contact information** (phone numbers, emails and addresses)
 - c. **Employment details** (including employer, designation, salary information of alumni and graduates, previous employment details of NUS staff)
 - d. **Information on spouse, children and next-of kin**



How do I classify data?

**Answer: Label document header and footer with NUS
Confidential, NUS Restricted and NUS Internal**

How do we classify data?

NUS-Confidential

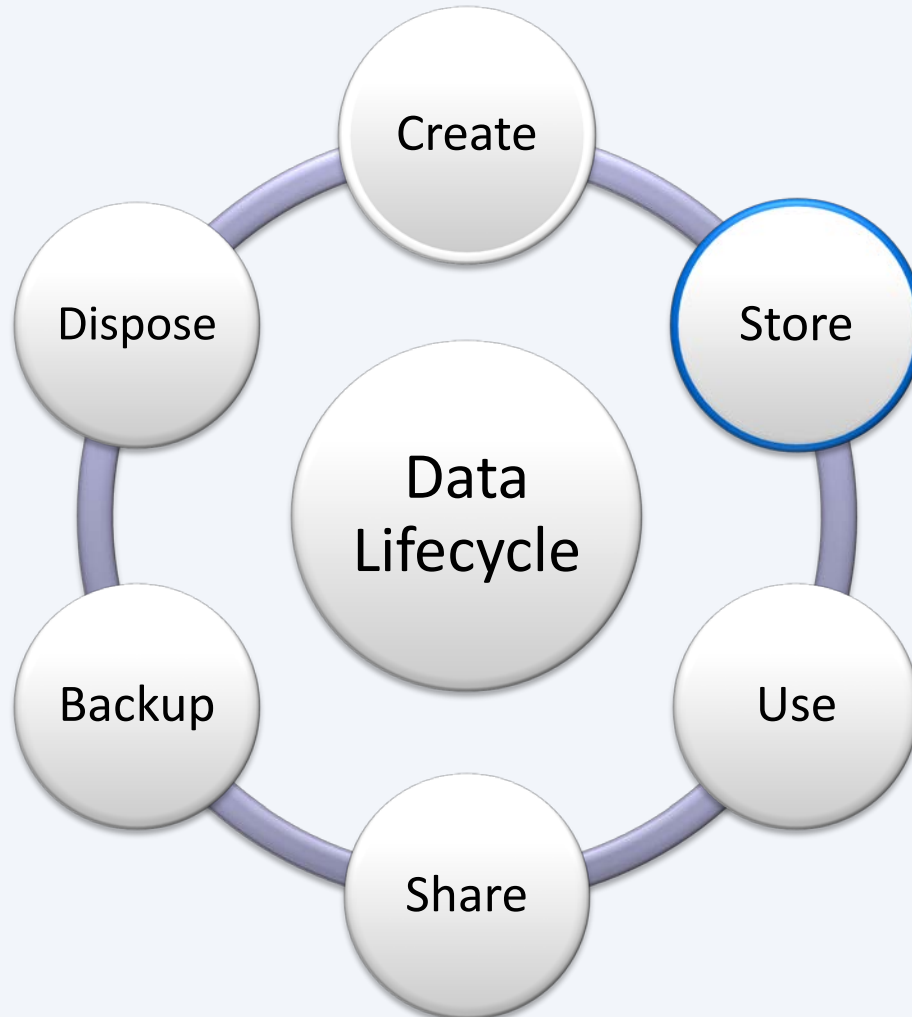
Classify data:
e.g. Label the document header and footer with appropriate data classification

e.g. Tan Ah Kou
S7712345B

NUS-Confidential



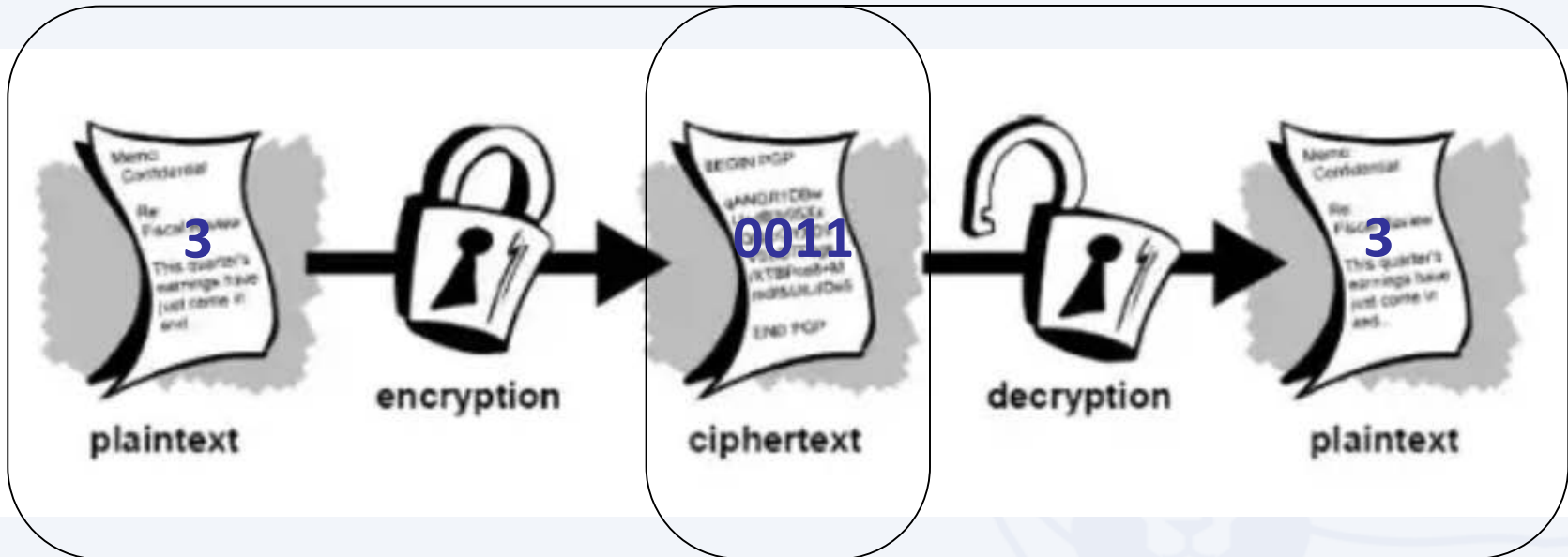
Data Lifecycle & Data Protection Best Practices



**Encrypt NUS-Confidential data
store on Laptop using
Encrypting File System (EFS)**



Data Encryption & Decryption



Source: <https://www.quora.com/What-are-encryption-and-decryption>

Sony's Data Leakage

First leaked data summary, some analysis *courtesy of IdentityFinder*:

- ✓ 26.4 GB in size, containing 33,880 files and 4,864 folders.
- ✓ Includes 47,426 unique Social Security Numbers (SSN)
- ✓ 15,232 SSN belonged to current or former Sony employees
- ✓ 3,253 SSN appeared more than 100 times
- ✓ 18 files contained between 10,860 and 22,533 SSN each.

Example of employee data found:

- ✓ One file (HR\Benefits\Mayo Health\Mayo XEROX assessment feed) contains 402 full Social Security numbers, internal emails, **plaintext passwords**, and employee names
- ✓ An additional 3000 or more Social Security numbers, names, contact details, contact phone numbers, dates of birth, email addresses, employment benefits, workers compensation details, retirement and termination plans, employees previous work history, *executive salaries*, medical plans, dental plans, genders, employee IDs, sales reports, copies of passport information and receipts for travel, as well as money order details to purchase movie tickets to resell back to the Sony staff. The leaked information also included documents, payment, and account information to order custom jewelry from Tiffany & CO via email.

Get This: Sony Hack Reveals Company Stored Passwords in Folder Labeled 'Password'



Source :

<https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/>
<https://www.entrepreneur.com/article/240517>

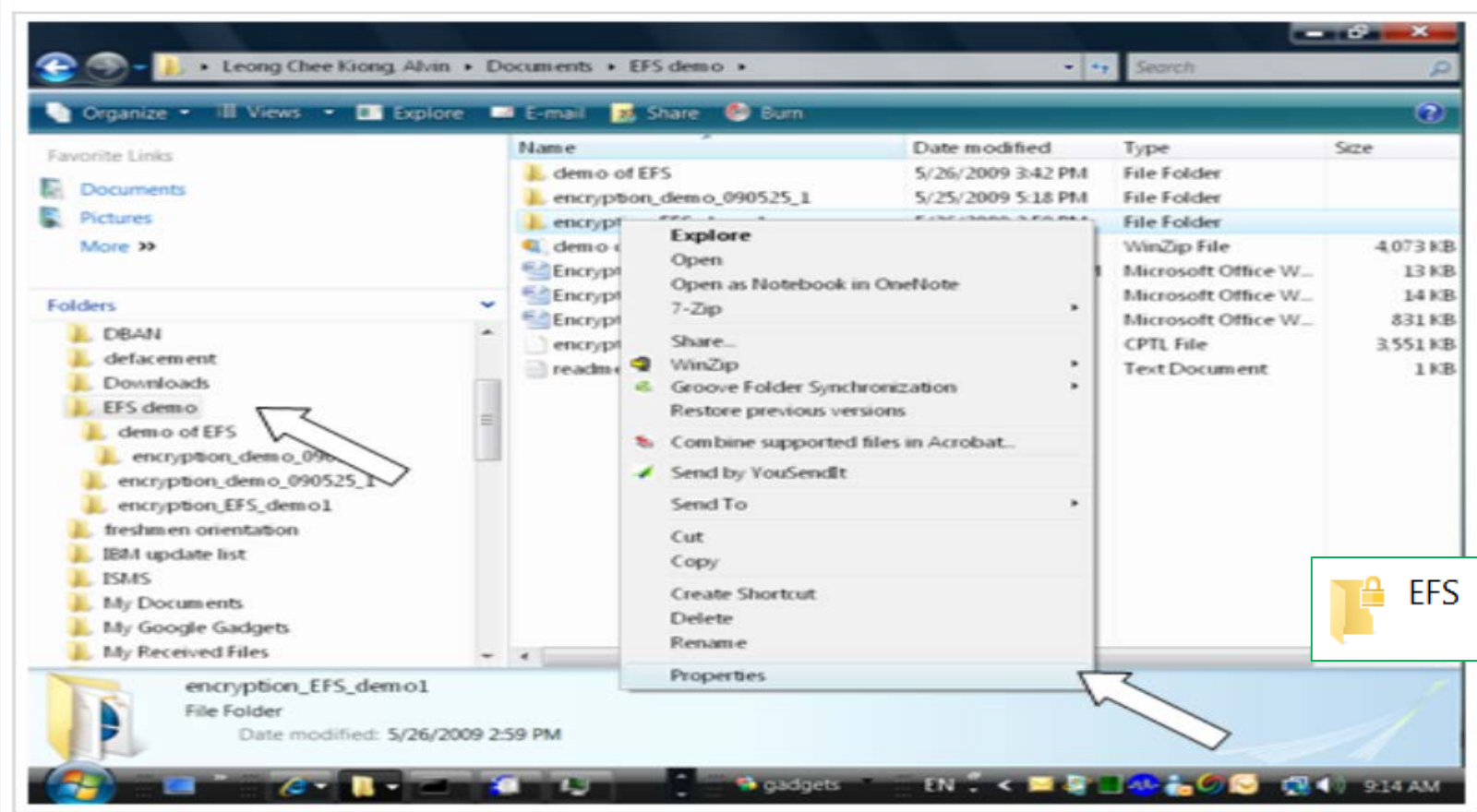


**How do we
prevent data
from being
accessed by
unauthorized
person?**

Answer: Encrypt the data

Encrypt Windows Folders (using EFS)

Right click on folder to encrypt. Select the option, “Properties”.

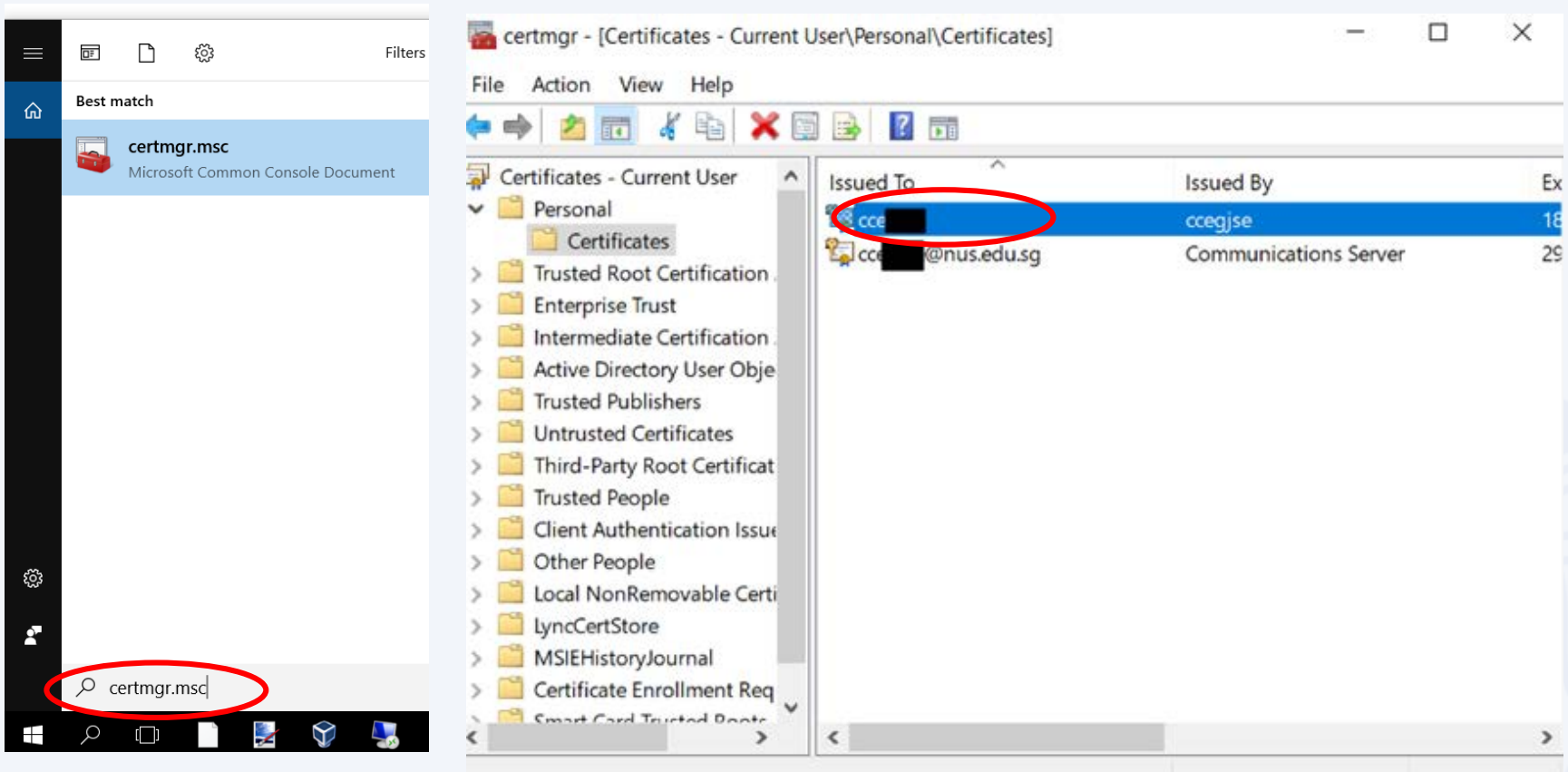


Picture: ZDNET

Note: EFS can encrypt the folders and files

Back up EFS Key

- Type certmgr.msc in the Search box and hit the ENTER key.
- Select Personal Folder and Click Certificates. Select userID.



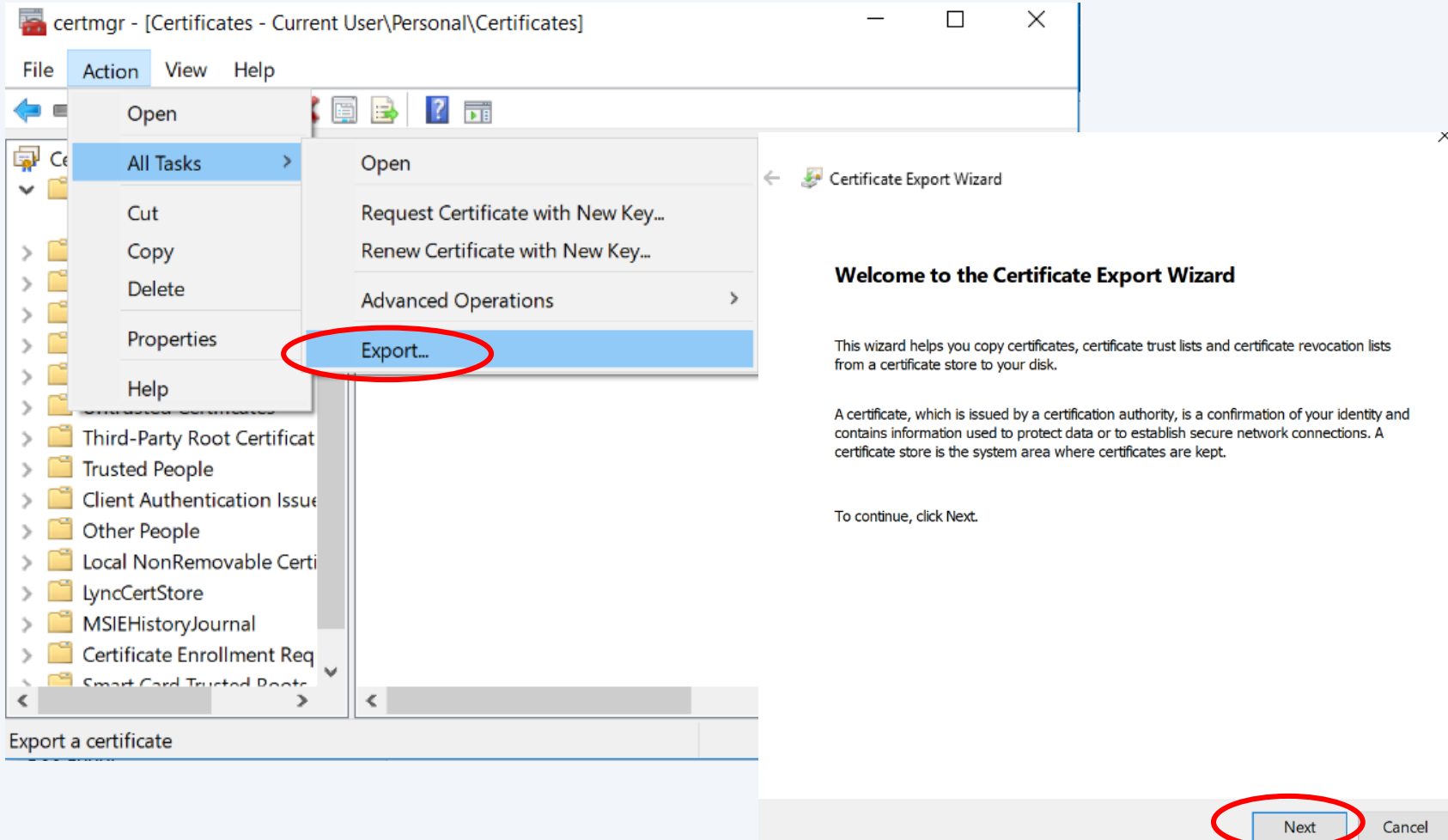
The screenshot shows the Windows search interface on the left and the certmgr.msc console on the right. In the search results, 'certmgr.msc' is listed as a Microsoft Common Console Document. In the console, the 'Personal' folder is expanded to show 'Certificates'. The 'Issued To' column of the certificate list is circled in red, showing a user ID that has been redacted with a black box.

Issued To	Issued By	Ex
cce [redacted]	ccegise	18
cce [redacted]@nus.edu.sg	Communications Server	29

Reference: <https://nusit.nus.edu.sg/its/resources/landing/>

Back up EFS Key

- Click Action -> All Tasks -> Export.
- Click Next on Certification Export Wizard



The screenshot shows the Windows Certificate Manager (certmgr) window with the 'Action' menu open. The 'All Tasks' option is selected, and the 'Export...' option is highlighted with a red circle. The Certificate Export Wizard is also open, showing the 'Welcome to the Certificate Export Wizard' screen. The 'Next' button is highlighted with a red circle.

certmgr - [Certificates - Current User\Personal\Certificates]

File Action View Help

Open

All Tasks >

Cut

Copy

Delete

Properties

Help

Open

Request Certificate with New Key...

Renew Certificate with New Key...

Advanced Operations >

Export...

Third-Party Root Certificat

Trusted People

Client Authentication Issue

Other People

Local NonRemovable Certi

LyncCertStore

MSIEHistoryJournal

Certificate Enrollment Req

Smart Card Trusted Root

Export a certificate

Certificate Export Wizard

Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

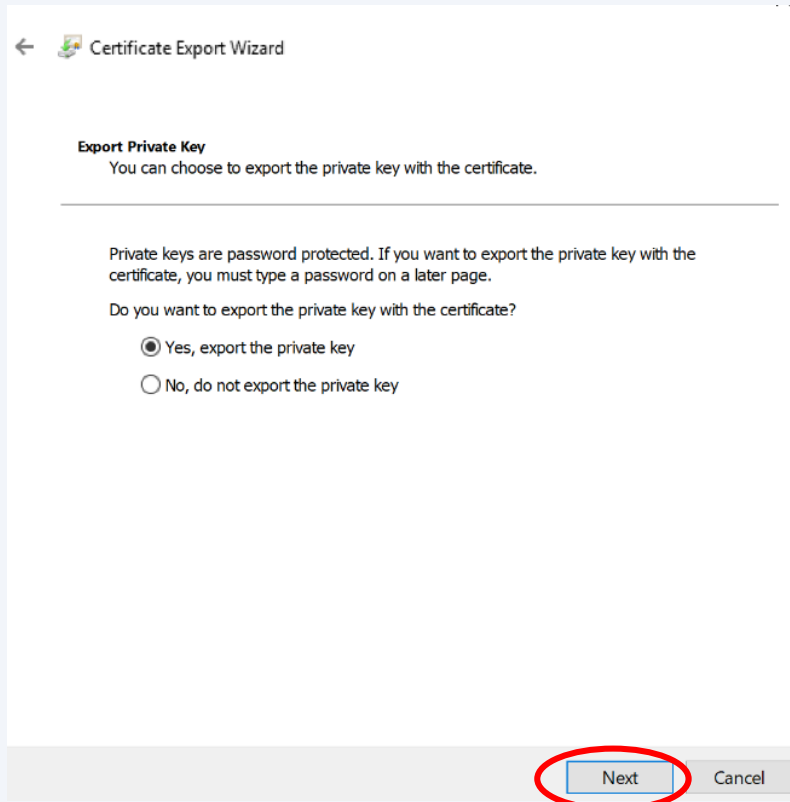
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Next Cancel

Back up EFS Key

- Select “Yes, export the private key”
- Click Next on Certification Export Wizard



← Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

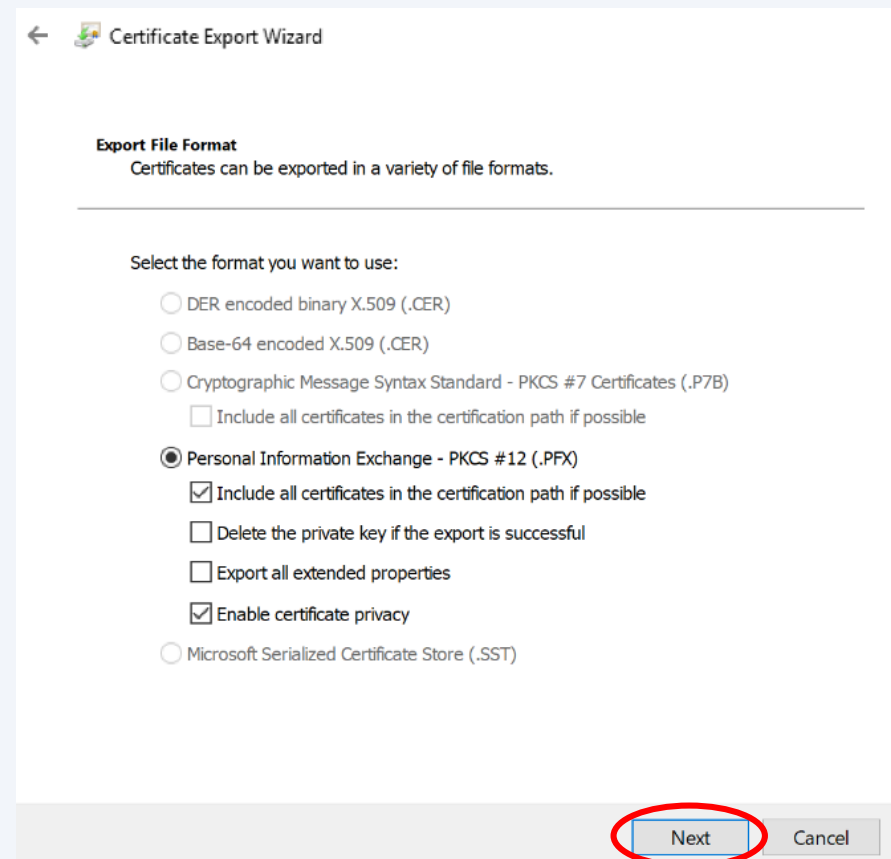
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

Yes, export the private key

No, do not export the private key

Next Cancel



← Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

DER encoded binary X.509 (.CER)

Base-64 encoded X.509 (.CER)

Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

Include all certificates in the certification path if possible

Personal Information Exchange - PKCS #12 (.PFX)

Include all certificates in the certification path if possible

Delete the private key if the export is successful

Export all extended properties

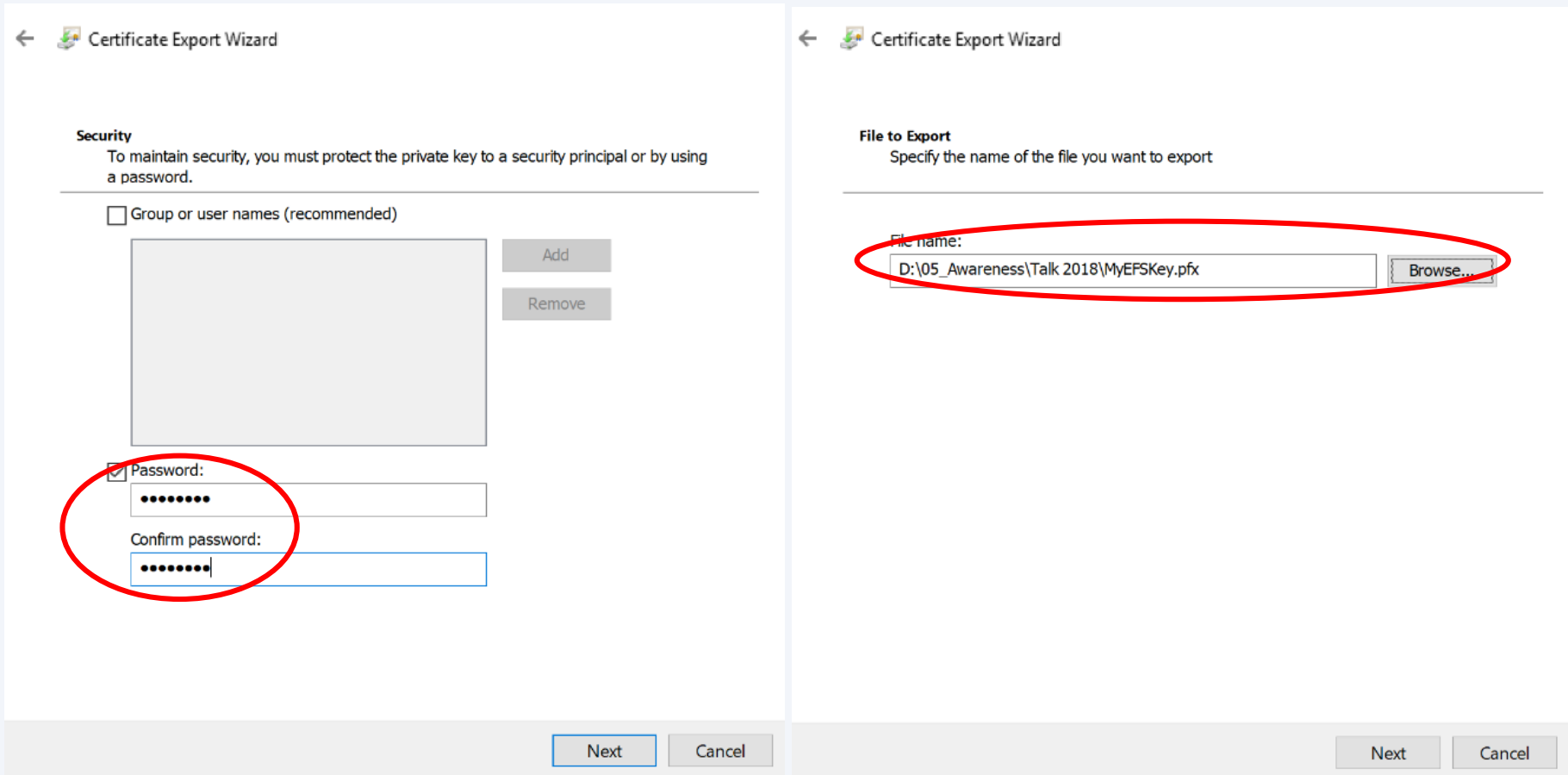
Enable certificate privacy

Microsoft Serialized Certificate Store (.SST)

Next Cancel

Back up EFS Key

- Select Password option and Enter Password. Click Next on Certification Export Wizard.
- Click on Browse button, select the folder and enter filename for the EFS Key.



← Certificate Export Wizard

Security
To maintain security, you must protect the private key to a security principal or by using a password.

Group or user names (recommended)

Password:

Confirm password:

Next Cancel

← Certificate Export Wizard

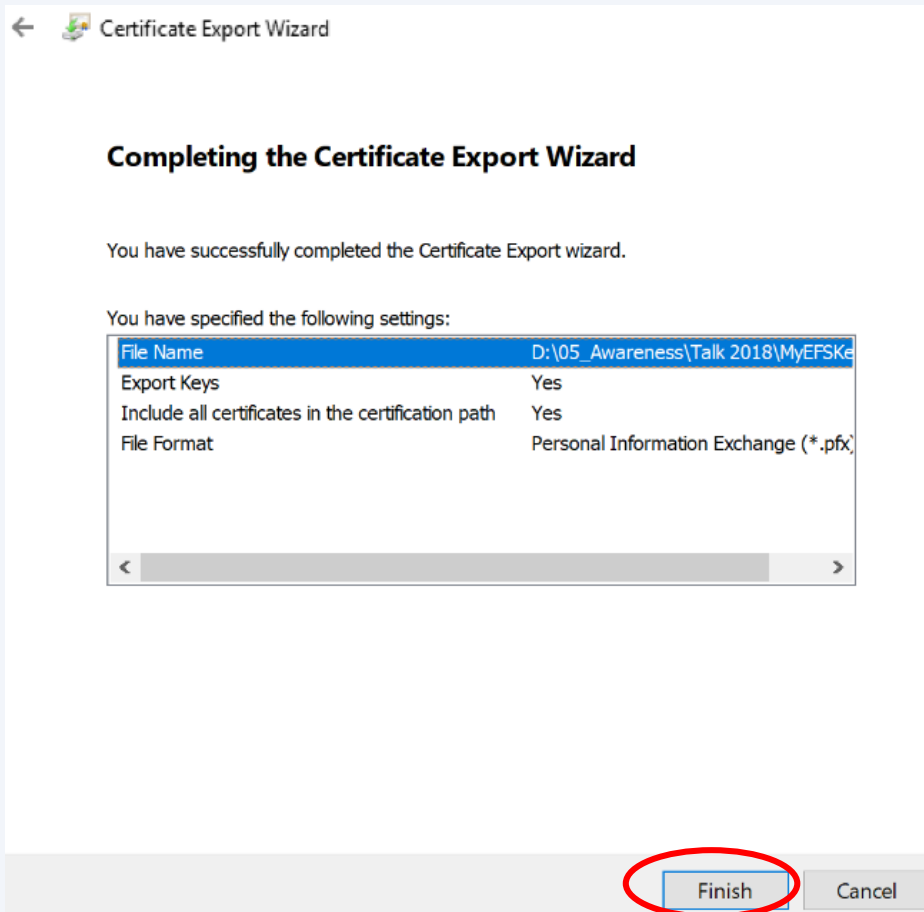
File to Export
Specify the name of the file you want to export

File name:
D:\05_Awareness\Talk 2018\MyEFSKey.pfx Browse...

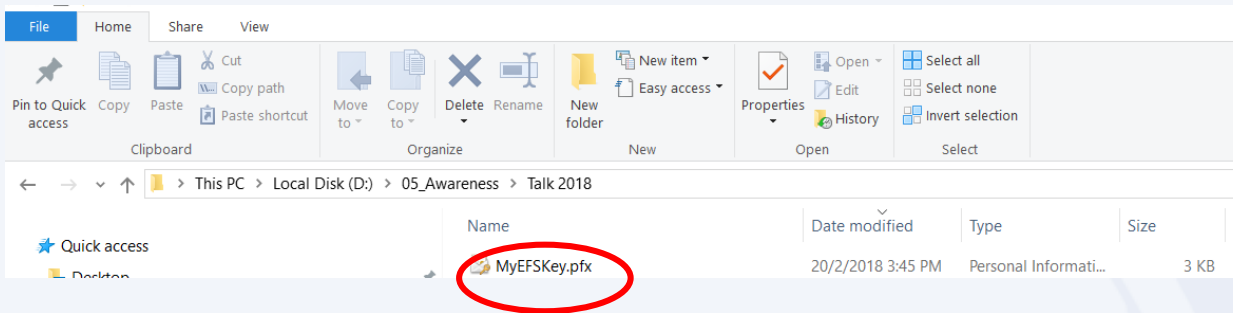
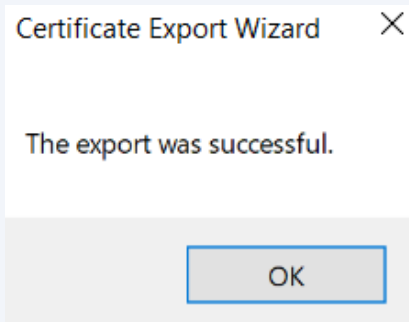
Next Cancel

Back up EFS Key

- Click Finish on Certification Export Wizard.



Back up EFS Key



- Always copy EFS key to another device such as USB.

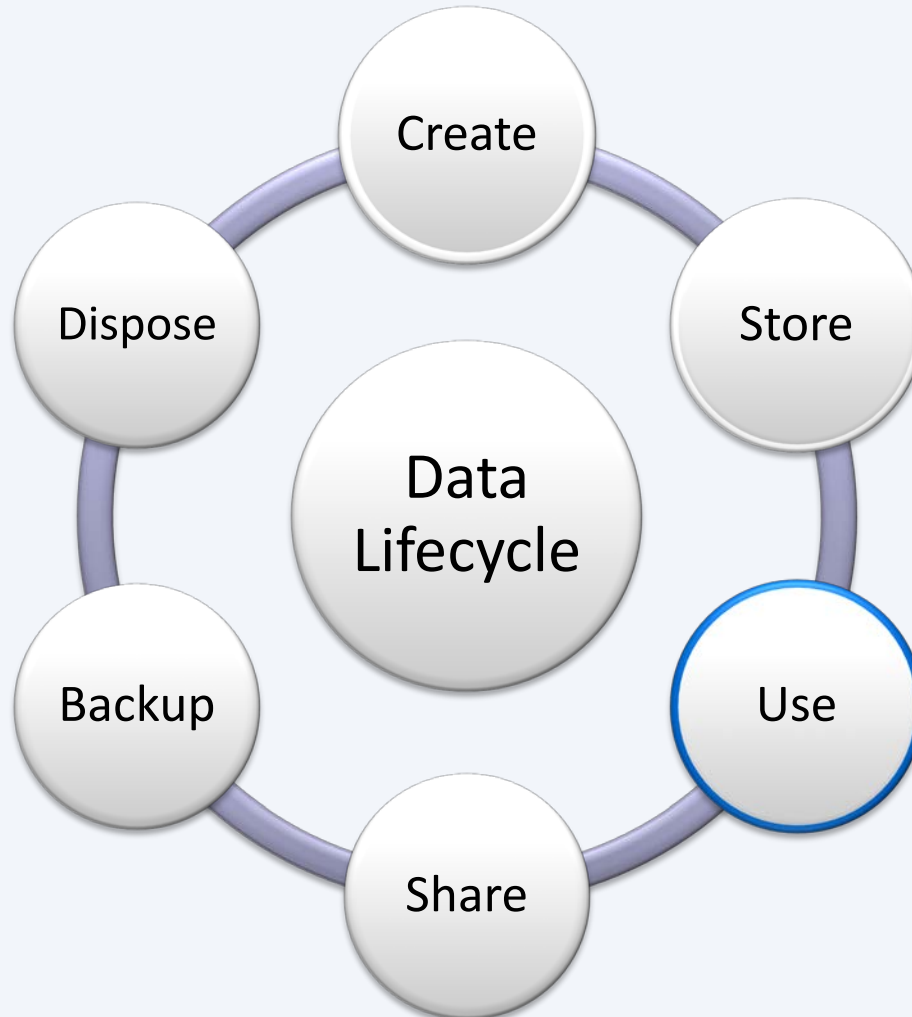


What happens if I lose my EFS key?

Answer: Data cannot be encrypted.



Data Lifecycle & Data Protection Best Practices



Access data securely:

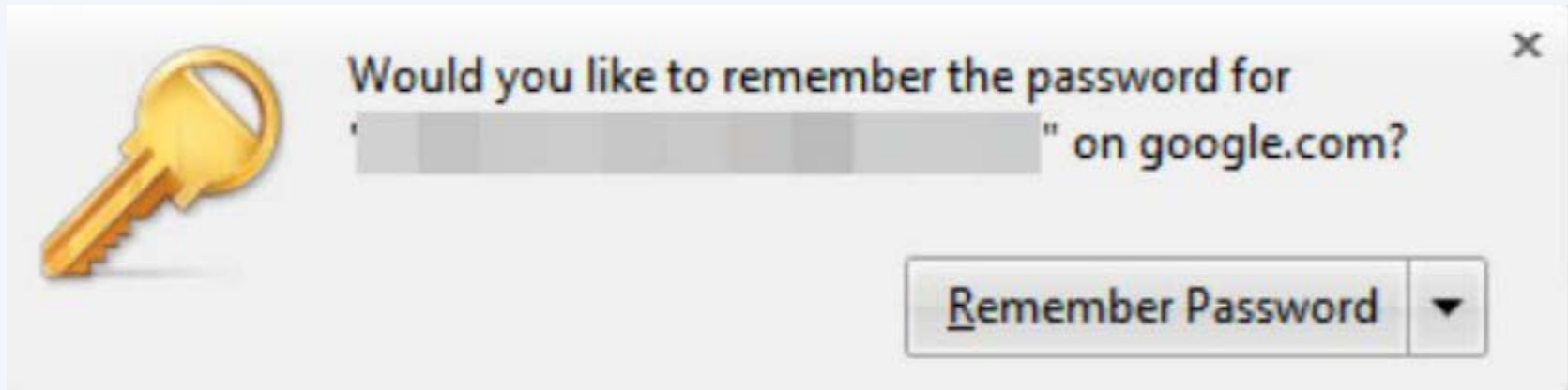
- Use VPN to access NUS system and data
- Use https website
- ...

Use https website



Source: <https://blog.easynews.com/http-vs-https-whats-the-difference/>

Do not store password in browser



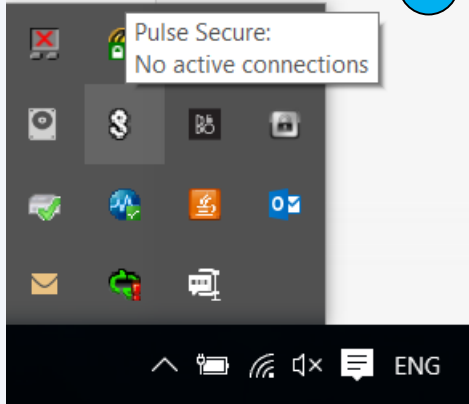
Source: <https://www.pandasecurity.com/mediacenter/security/browser-saves-password-secure/>



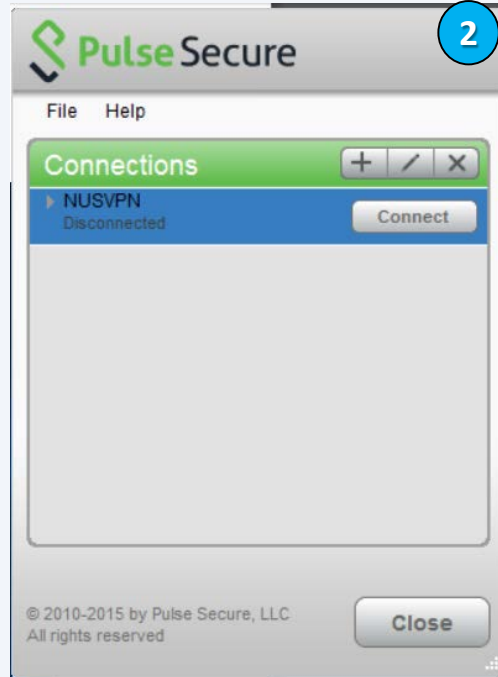
Use VPN to access NUS System & Data off Campus



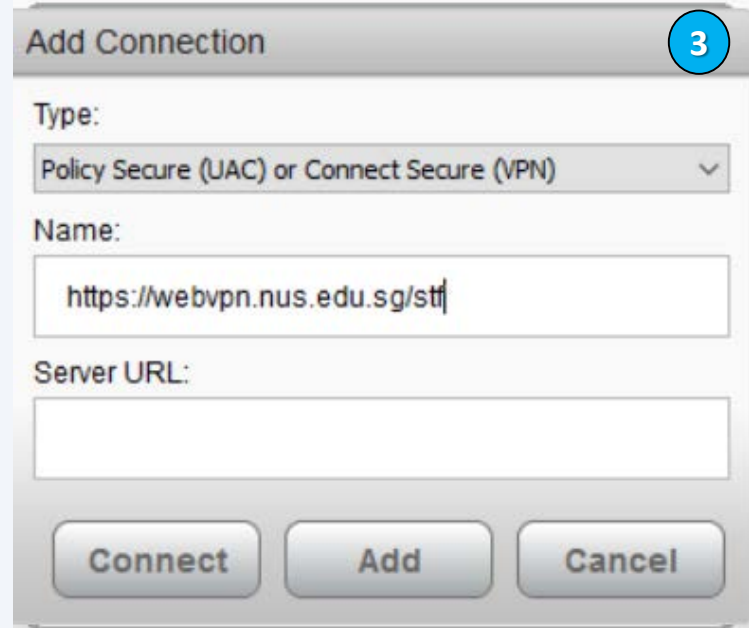
VPN - <https://comcen.nus.edu.sg/gat4/wp-content/uploads/downloads/nvpn/nVPN-config-guide-for-staff.pdf>



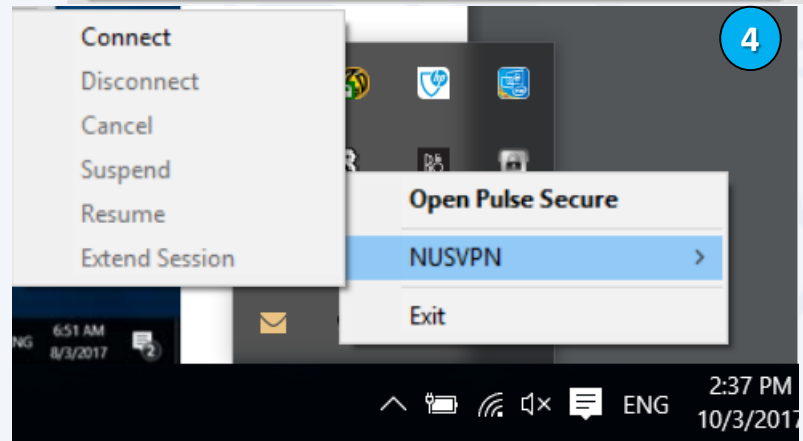
1



2



3



4



Should I use my NUS email address for registering with social media site?

Answer: No, you might received unsolicited emails from mailing group or unknown sender when you use NUS email account for subscribing to social media website.

What are the Data Protection Best Practices ?



1

Use VPN to access NUS System and data off campus.

2

Use https website for sensitive transactions (e.g. requires login)

3

Never remember password in browser.

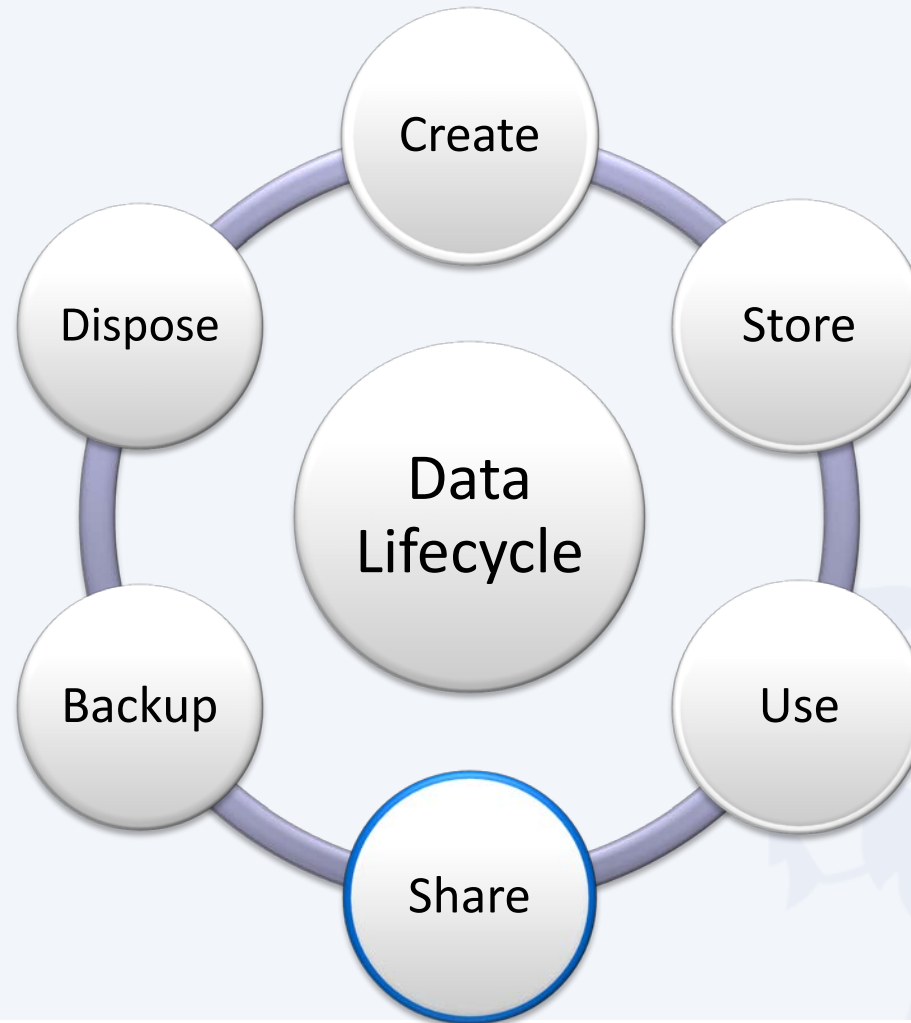
4

Log off from browser application after using it.

5

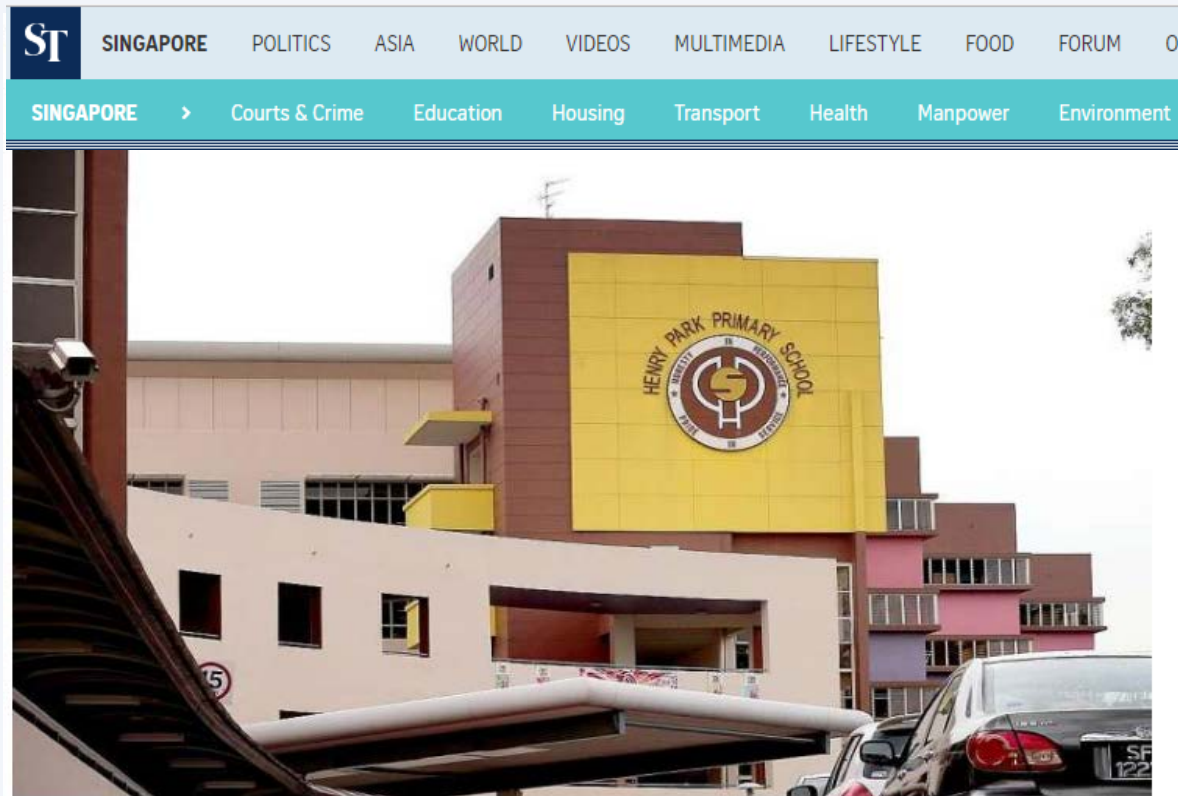
Keep work and personal email accounts separate.

Data Lifecycle & Data Protection Best Practices



Share data securely: Exchanging data over email, portable storage, shared folders

Sending Out Personal Data by Mistake



The personal data of more than 1,900 pupils from Henry Park Primary School was leaked when an Excel spreadsheet containing the children's particulars was mistakenly sent out to about 1,200 parents as part of an update about a school event. The file contained the names and birth certificate numbers of all 1,900 pupils in the school, and the names, telephone numbers and e-mail addresses of their parents.

Source (Mar 1, 2017): <http://www.straitstimes.com/singapore/take-steps-to-secure-online-accounts-experts-urge>

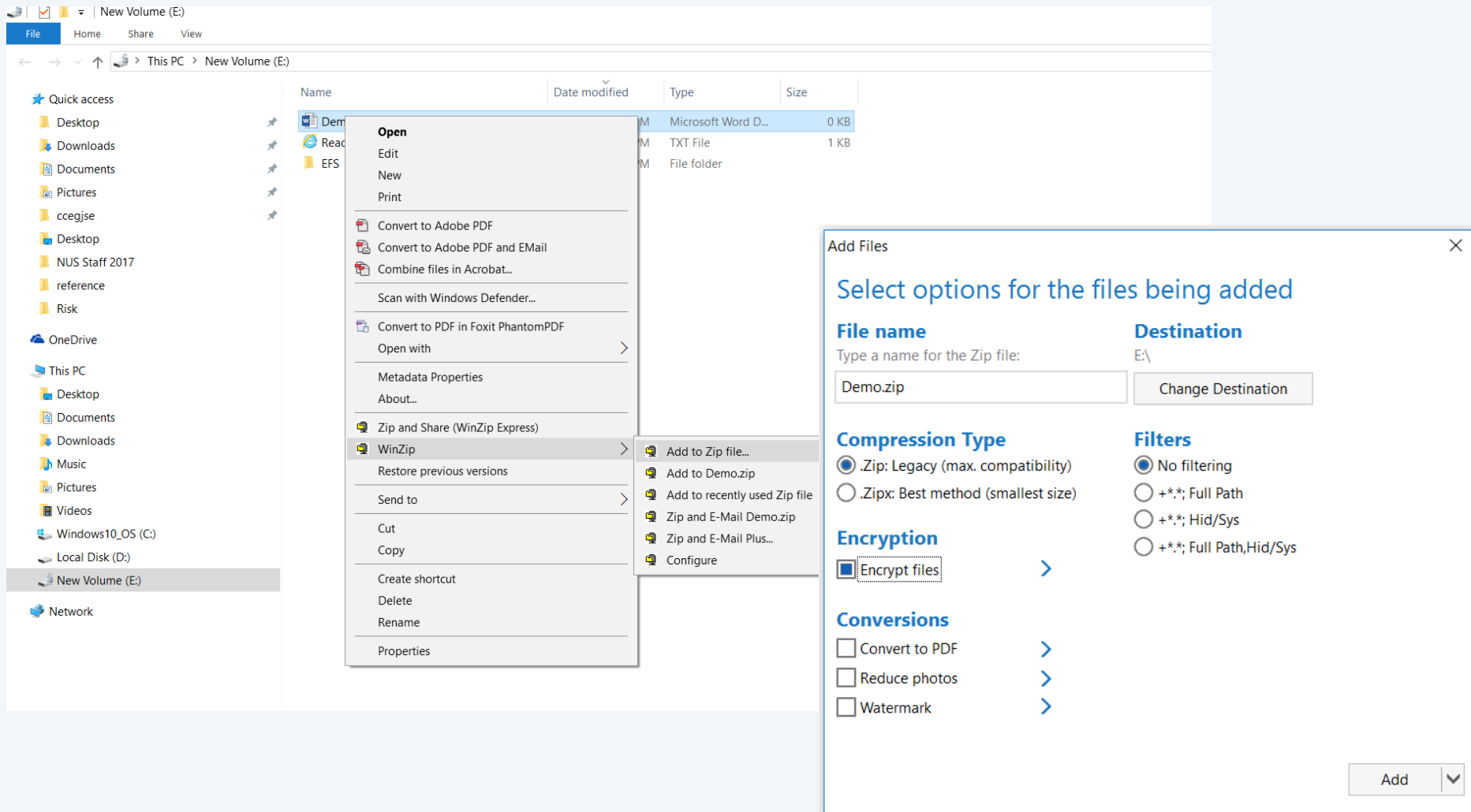
What are the protection measures?



- 1 Check that the recipient email address is correct
- 2 Encrypt the file with password using Winzip
- 3 Set delay email delivery



Encrypt Files with Password using Winzip



The screenshot shows a Windows File Explorer window for 'New Volume (E:)' with a context menu open over a file named 'Demo'. The 'WinZip' option is selected, opening a sub-menu with 'Add to Zip file...' highlighted. The 'Add Files' dialog box is open, showing options for file name, destination, compression type, encryption, and filters.

Name	Date modified	Type	Size
Demo		M	Microsoft Word D... 0 KB
Readme		M	TXT File 1 KB
EFS		M	File folder

Add Files

Select options for the files being added

File name
Type a name for the Zip file:
Demo.zip

Destination
E:\
Change Destination

Compression Type
 .Zip: Legacy (max. compatibility)
 .Zipx: Best method (smallest size)

Encryption
 Encrypt files

Filters
 No filtering
 .; Full Path
 .; Hid/Sys
 .; Full Path,Hid/Sys

Conversions
 Convert to PDF
 Reduce photos
 Watermark

Add



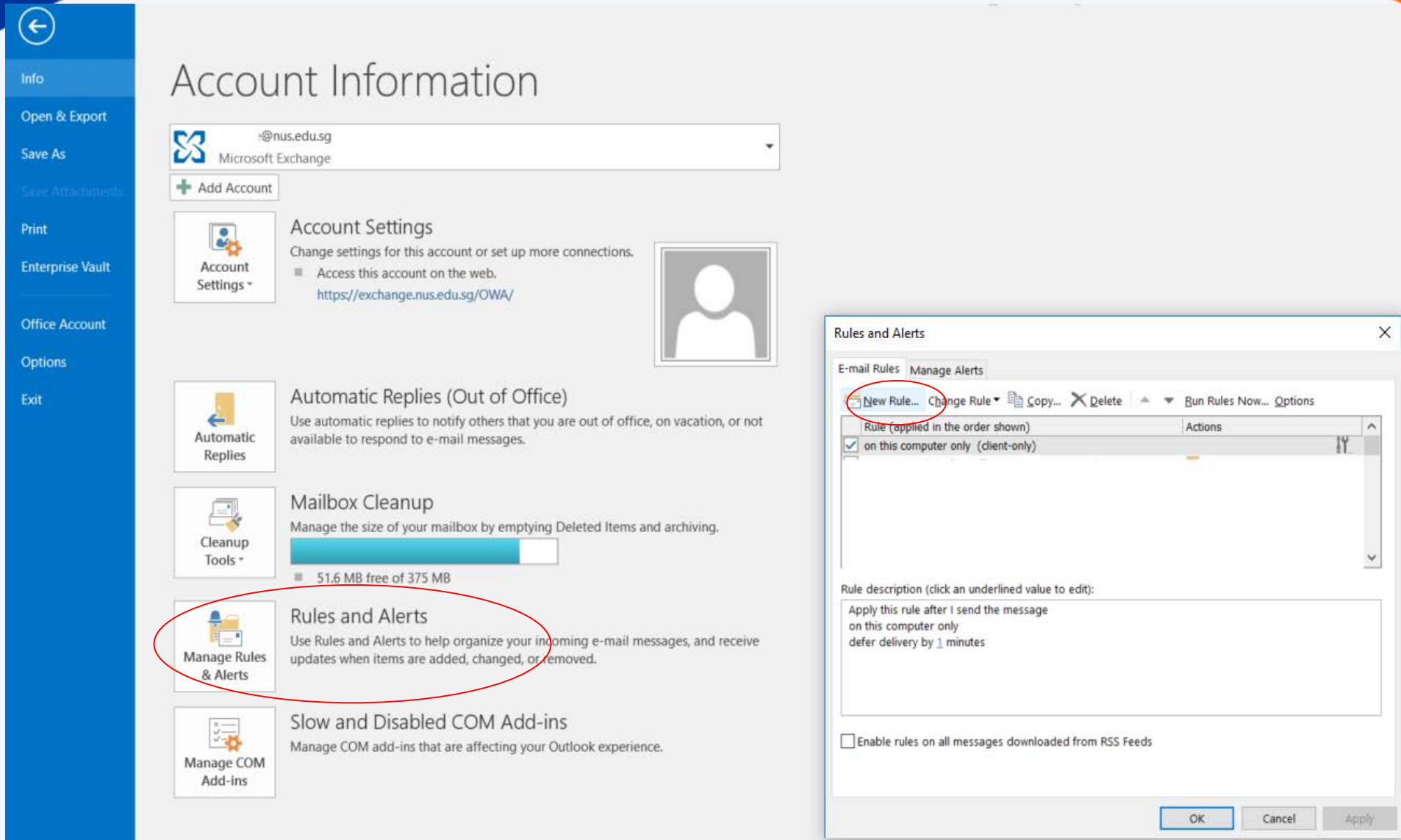
Encrypt Files with Password using Winzip

Configure your Winzip encryption settings to AES 256

The screenshot shows the WinZip application window with the 'Settings' menu open and the 'Encryption' option selected. A tooltip titled 'Encryption settings' explains that AES (128-bit and AES (256-bit) provide a stronger measure of security than Zip 2.0 (Legacy) which is known to be relatively weak but compatible with most Zip utilities. An 'Encryption Settings' dialog box is open in the foreground, displaying the following text: 'When enabled, the selected method is used to encrypt files added to a Zip file.' Under the heading 'Encryption Method', three radio buttons are visible: '256-bit AES' (selected), '128-bit AES', and 'Legacy (Zip 2.0)'. A link for 'More information about encryption and encryption methods' is also present. The background interface shows various settings like 'Encrypt', 'Reduce Photos', 'Convert to PDF', and 'Watermark' on the right side.

Deferment of Email Delivery

From outlook client, go to **File->Rules and Alerts->New Rule**



The screenshot shows the Outlook 'Account Information' page. The 'Rules and Alerts' option is circled in red. A 'Rules and Alerts' dialog box is open, showing a table of rules. The 'New Rule...' button is also circled in red. The dialog box shows a rule named 'on this computer only (client-only)' with a checkmark in the 'Rule (applied in the order shown)' column. The 'Rule description' section contains the text: 'Apply this rule after I send the message on this computer only defer delivery by 1 minutes'. The 'OK', 'Cancel', and 'Apply' buttons are visible at the bottom of the dialog box.

Account Information

Info

Open & Export

Save As

Save Attachments

Print

Enterprise Vault

Office Account

Options

Exit

Account Settings

Automatic Replies (Out of Office)

Mailbox Cleanup

Rules and Alerts

Slow and Disabled COM Add-ins

Rules and Alerts

Rule (applied in the order shown)	Actions
<input checked="" type="checkbox"/> on this computer only (client-only)	

Rule description (click an underlined value to edit):

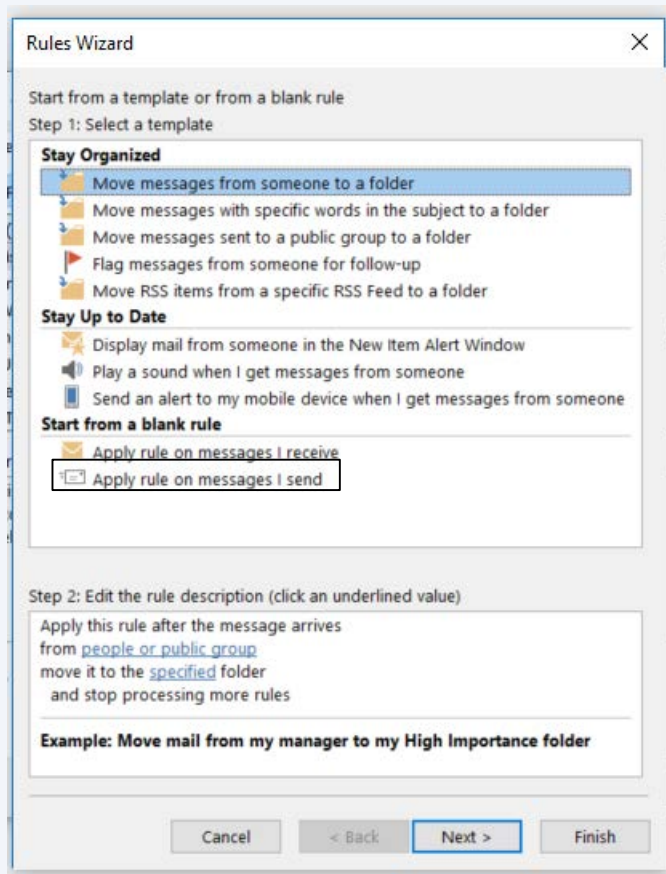
Apply this rule after I send the message
on this computer only
defer delivery by 1 minutes

Enable rules on all messages downloaded from RSS Feeds

OK Cancel Apply

Deferment of Email Delivery

Select the option, “**Apply rule on message I send**”. Click the button, “**Next**”



Rules Wizard

Start from a template or from a blank rule
 Step 1: Select a template

Stay Organized

- Move messages from someone to a folder
- Move messages with specific words in the subject to a folder
- Move messages sent to a public group to a folder
- Flag messages from someone for follow-up
- Move RSS items from a specific RSS Feed to a folder

Stay Up to Date

- Display mail from someone in the New Item Alert Window
- Play a sound when I get messages from someone
- Send an alert to my mobile device when I get messages from someone

Start from a blank rule

- Apply rule on messages I receive
- Apply rule on messages I send**

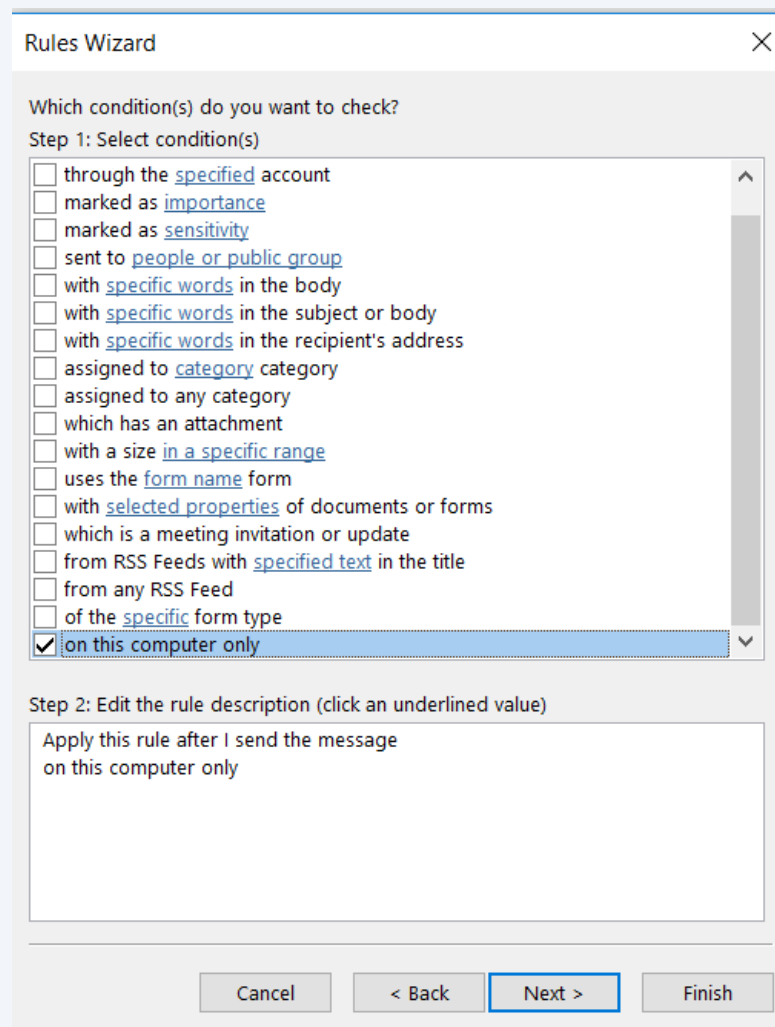
Step 2: Edit the rule description (click an underlined value)

Apply this rule after the message arrives from people or public group move it to the specified folder and stop processing more rules

Example: Move mail from my manager to my High Importance folder

Cancel < Back **Next >** Finish

Select the option, “**Apply on this computer only**”. Click the button, “**Next**”



Rules Wizard

Which condition(s) do you want to check?
 Step 1: Select condition(s)

- through the specified account
- marked as importance
- marked as sensitivity
- sent to people or public group
- with specific words in the body
- with specific words in the subject or body
- with specific words in the recipient's address
- assigned to category category
- assigned to any category
- which has an attachment
- with a size in a specific range
- uses the form name form
- with selected properties of documents or forms
- which is a meeting invitation or update
- from RSS Feeds with specified text in the title
- from any RSS Feed
- of the specific form type
- on this computer only**

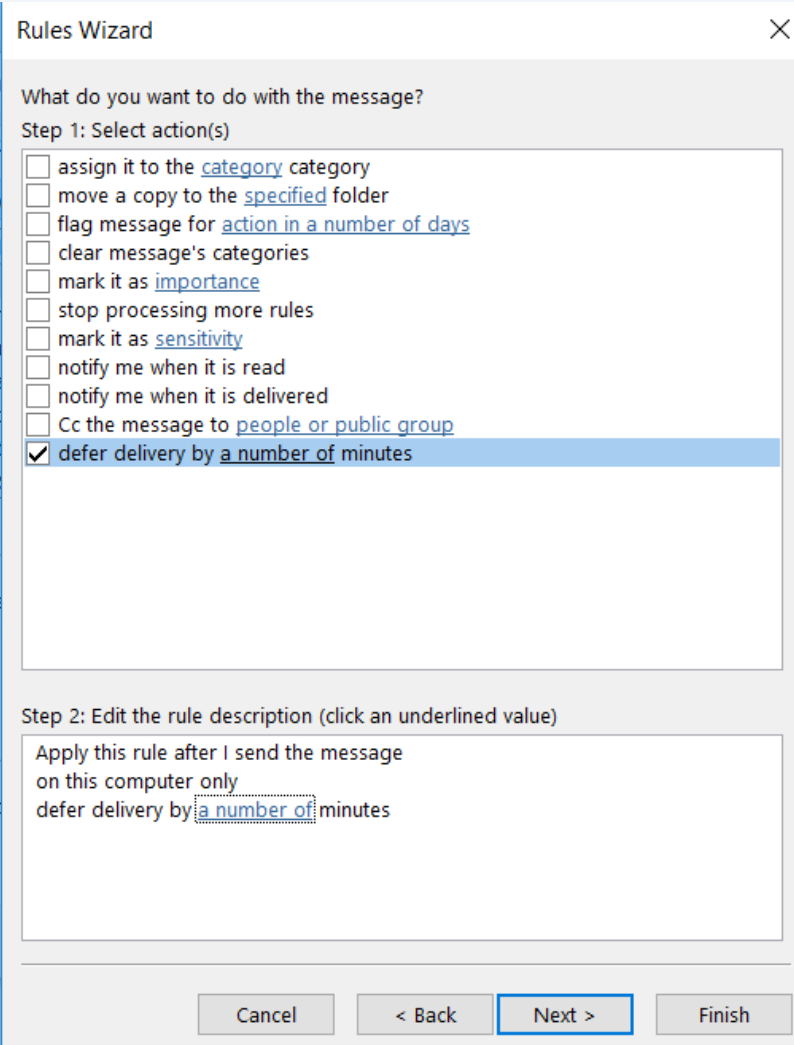
Step 2: Edit the rule description (click an underlined value)

Apply this rule after I send the message on this computer only

Cancel < Back **Next >** Finish

Deferment of Email Delivery

Select the option, “**Defer delivery by a number of minutes**”. Click on the hyperlink, “a number of” and specify the number of minutes to delay. Click the button, “**Finish**”



Rules Wizard

What do you want to do with the message?

Step 1: Select action(s)

- assign it to the [category](#) category
- move a copy to the [specified](#) folder
- flag message for [action in a number of days](#)
- clear message's categories
- mark it as [importance](#)
- stop processing more rules
- mark it as [sensitivity](#)
- notify me when it is read
- notify me when it is delivered
- Cc the message to [people or public group](#)
- defer delivery by [a number of minutes](#)

Step 2: Edit the rule description (click an underlined value)

Apply this rule after I send the message
on this computer only
defer delivery by [a number of](#) minutes

Cancel < Back Next > Finish

Sharing out Confidential Data Unknowingly

What is Open Shares

This a user misconfiguration where shared folder permission is set to allow EVERYONE to have full access. It provides a very easy and effective way for attackers to browse and steal the (sensitive) data without any hacking tool or skill.

What should I DO

You should do a self-check on your computer to discover if there is any Open Shares or folder that has been shared unintentionally, and remove it immediately.

SECURITY ADVISORY

NUS COMPUTER CENTRE

Dear Colleagues,

Sometimes we share files and folders on our Windows PC with colleagues for work purpose. However, if the security permissions are not set correctly, the (sensitive) data being shared will be exposed and accessible to anyone, including unauthorized personnel. Stealing data via insecure shared folders can be easily done by someone who is moderately IT savvy.

We suggest that you perform a self-check on your PC to find and remove any insecure shared folders. Please click [here](#) for the detailed steps.

Computer Centre will also perform regular scans on all staff PCs to check for insecure shared folders. The relevant department management will be notified if insecure shared folders are identified.

Regards,

Wu Wenlong
Head (IT Security)



Computer
Centre

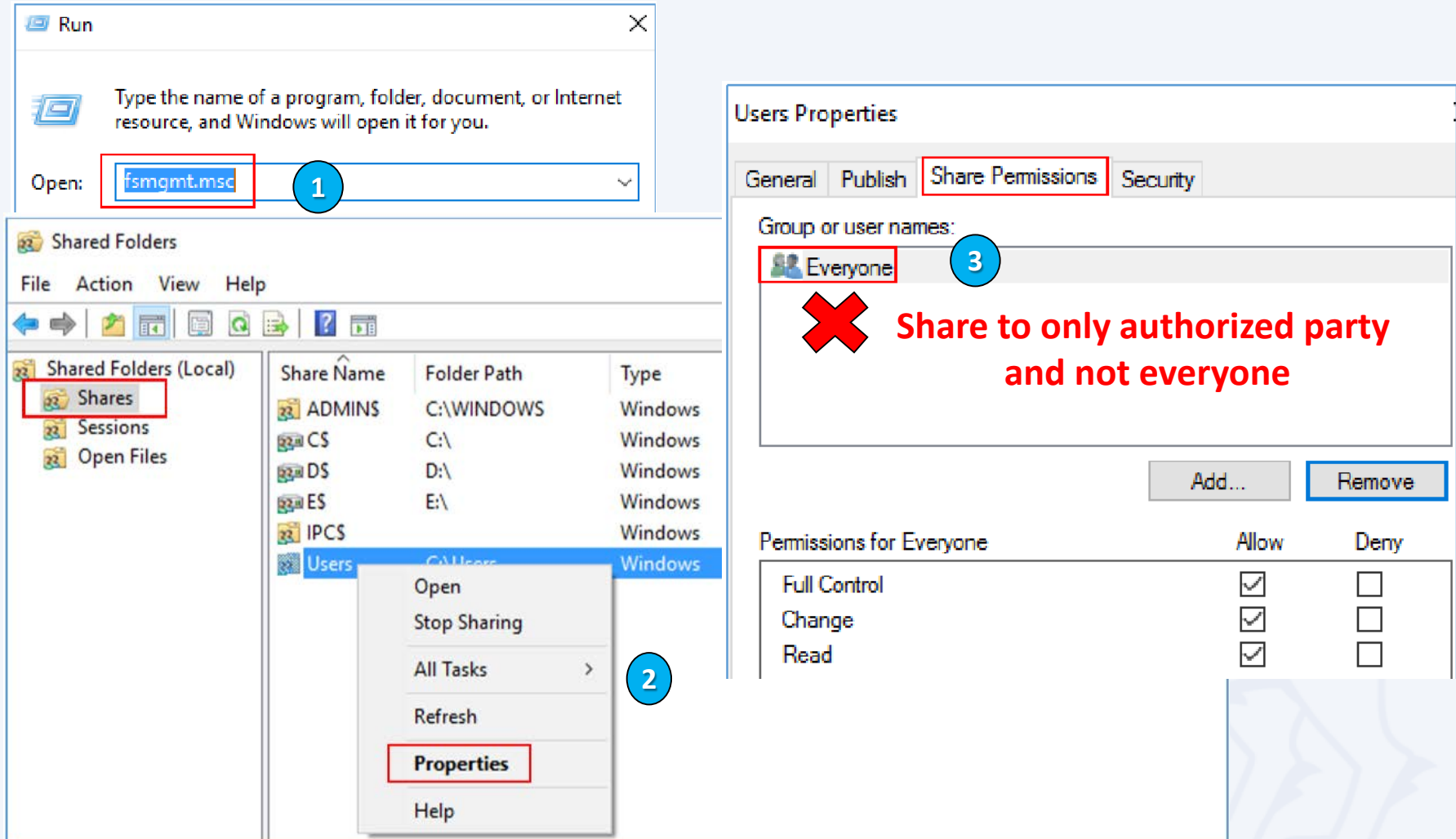


What is an Open Share folder?

Answer:

Content within folders can be read, update and delete by everyone.

Remove Insecure Share Folders



The image shows a Windows File Explorer window with the 'Shares' folder selected in the left pane. A context menu is open over the 'Shares' folder, with 'Properties' highlighted. A red box and a blue circle with the number '1' are around the 'fsmgmt.msc' text in the Run dialog box. A red box and a blue circle with the number '2' are around the 'Properties' option in the context menu. A red box and a blue circle with the number '3' are around the 'Everyone' user in the 'Users Properties' dialog box. A large red 'X' is placed over the 'Everyone' user, and a red text box says 'Share to only authorized party and not everyone'. The 'Share Permissions' tab is selected in the 'Users Properties' dialog, and the 'Remove' button is highlighted.

1 Run dialog box: `fsmgmt.msc`

2 File Explorer context menu: **Properties**

3 Users Properties dialog: **Share Permissions** tab, **Everyone** user selected.

Share to only authorized party and not everyone

Permissions for Everyone	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Change	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>

https://comcen.nus.edu.sg/services/it_security/data-security/check-and-remove-insecure-shared-folders/



How can I share large amount of data with other NUS colleagues?

Answer: Use Nbox, Sharepoint



Do I need to encrypt NUS data that are stored on portable storage?

Answer: Yes, use Bitlocker.

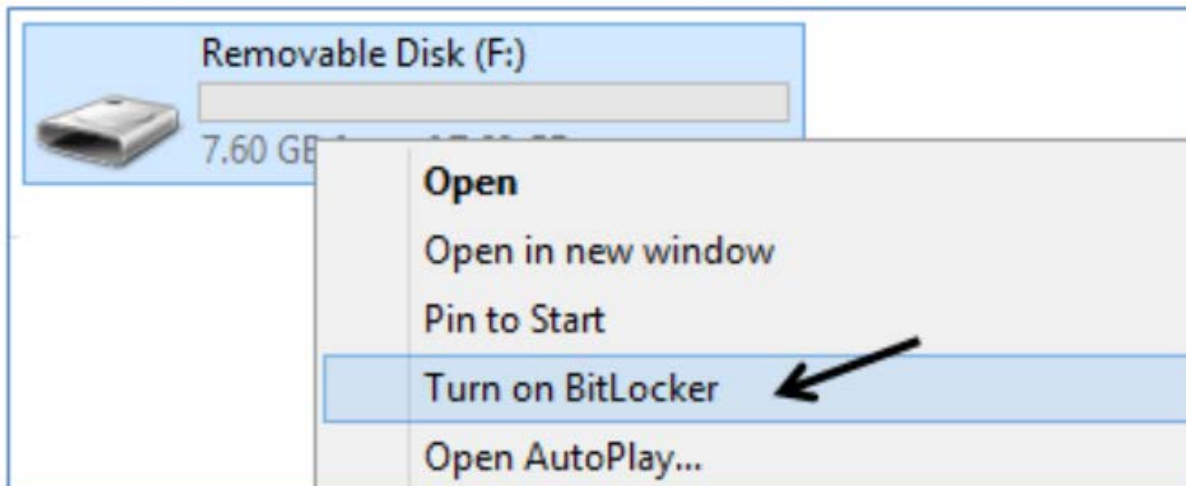
Refer to Guideline for Use, Classification and Protection of Data, Section D, Table 2.

Enable Bit Locker

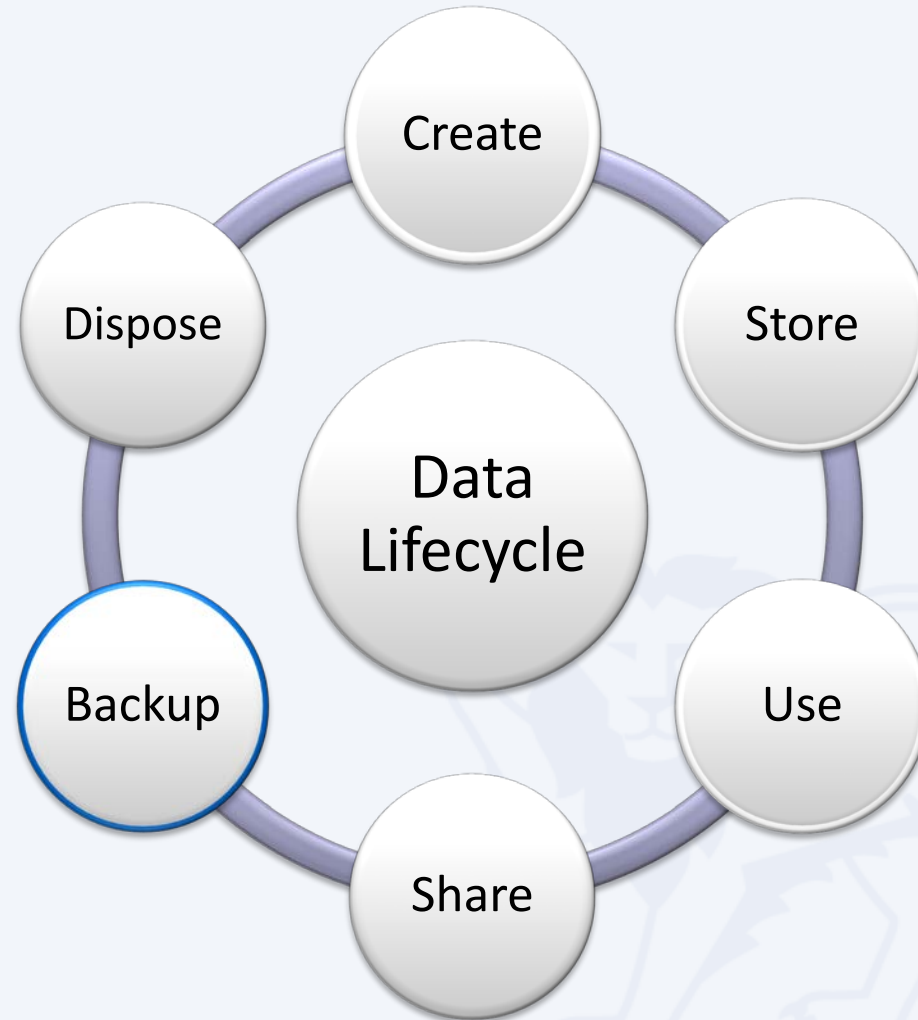
Source: <https://nusit.nus.edu.sg/its/resources/bitlocker/install-bitlocker/>

Window 10

1. Insert your thumbdrive into your computer.
2. Go to Computer and look for the drive letter assigned to your thumbdrive.
3. Right-click the drive and select Turn on BitLocker.



Data Lifecycle & Data Protection Best Practices



**Save important
data from your
computer to other
device**

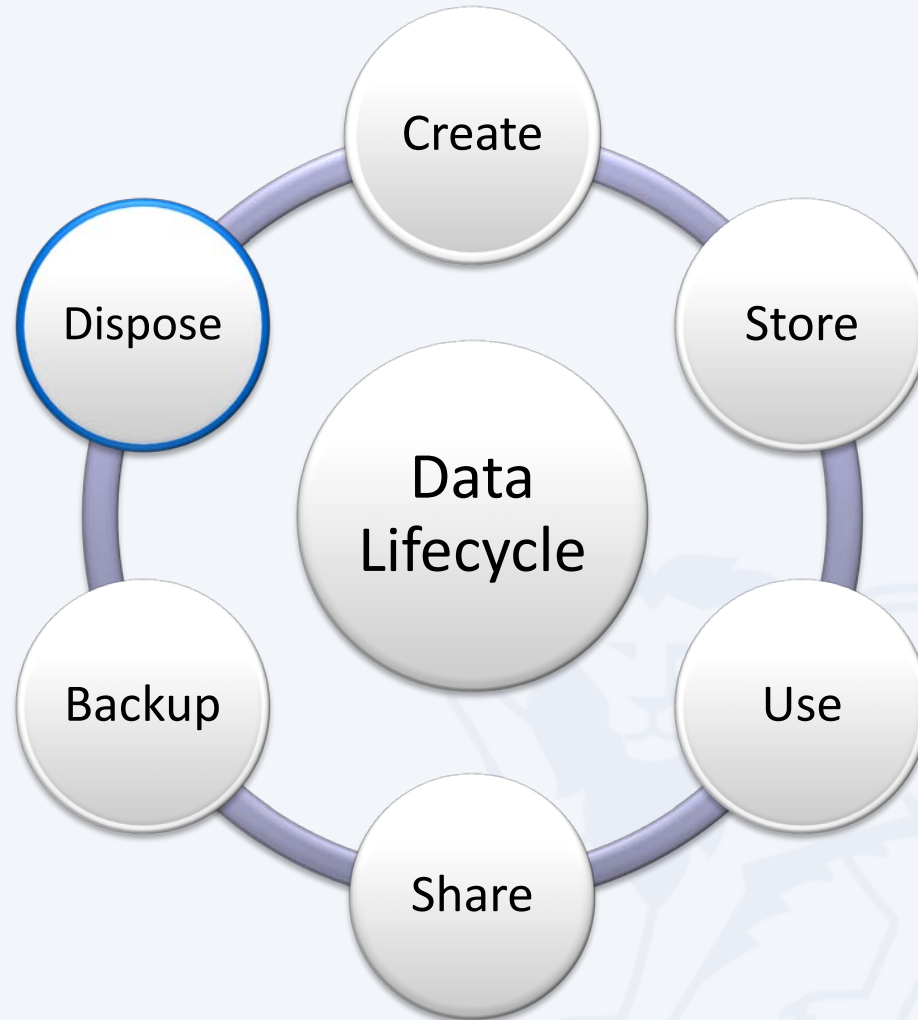
nBox at a Glance

	Personal	Team folder
Storage space	1TB (~1000GB)	20GB
Max. single file size	10GB	
Max. number of devices	5 per user	
File versioning	Yes (up to 10 versions per file)	
Retention of deleted files	Yes (up to 30 days)	
Available on	Windows, Mac, iOS, Android & web browsers	
Who can use nBox	NUS staff only	
Cost	Free	

https://nusit.nus.edu.sg/services/online_storage/nbox/

Data Lifecycle & Data Protection Best Practices

**Erase data
securely**



Secure Disposal of Hard Disk using Blancco Drive Eraser

<https://inetapps.nus.edu.sg/comcen/security/protect-data/secure-hard-disk-disposal-using-blancco.html>

It is mandatory to erase and destroy all University data stored in the storage media before disposal. For redeployment of hard disk, use Blancco for secure erasure. For disposal of any functional or non-functional hard disk that the data cannot be erased by Blancco, physical destruction would be required; shred/incinerate Solid State Drive (SSD) and degauss Hard Disk Drive (HDD).

NUS IT Co-op offers these services. You may contact them at 67792942 or email at coppc05@nus.edu.sg.

Dispose Data Securely

Dumping paper with personal info?
Shred it, says watchdog



A logo of the United Overseas Bank Limited seen in Singapore's central business district on January 7. PHOTO: REUTERS

Source: Straits Times 21 Jul 2016

Paper containing personal information must be shredded into small pieces and not dumped in unsecured bins.

Similarly, personal data stored on electronic media such as computer hard disks, USB drives or DVDs must be erased using specialised software to avoid accidental data leaks



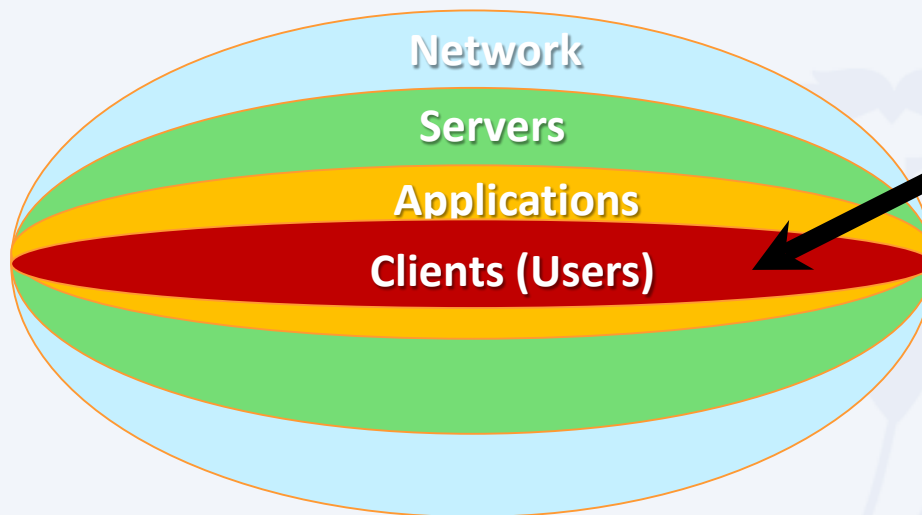
When and how do I report Data loss?

Answer:

Report immediately your supervisor and to cceda@nus.edu.sg



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



“91% of Cyberattacks begins with Phishing Email “

– TrendMicro



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 with attachment

Singtel warns of fake billing e-mail

PUBLISHED MAR 23, 2017, 5:00 AM SGT

Source: Straits Times



Singtel advises recipients of suspicious e-mails "not to respond to or click on any links in the message" and to delete such e-mails immediately.

ST understands that there were e-mails sent on Monday and Tuesday from noreply-
s2@singtel.com.sg with the header "Your Sigtel (sic) bill is now available for download".

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 WhatsApp

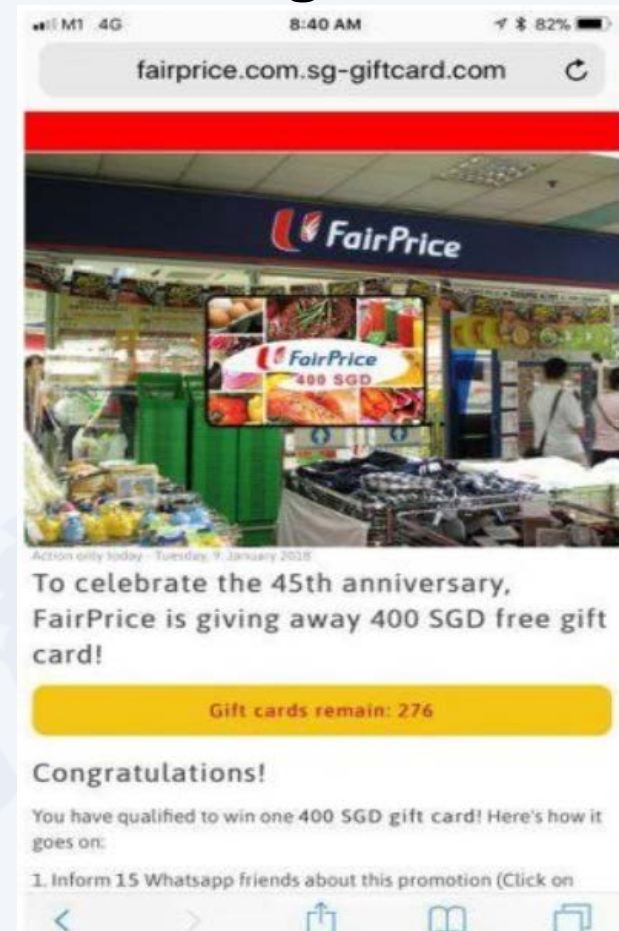
NTUC FairPrice 45th anniversary gift card message is a scam, supermarket chain warns

The new scam invites people to click on a link in a message claiming that FairPrice is giving away gift cards for its 45th anniversary.

A copy of the message that a Straits Times reader received via **WhatsApp** reads:

"Fairprice celebrates its 45th anniversary and gives each gift cards worth 400SGD each! I have just received one from here: [http:// fairprice. com /anniversary](http://fairprice.com/anniversary)".

<http://www.straitstimes.com/singapore/ntuc-fairprice-45th-anniversary-gift-card-message-is-a-scram-supermarket-chain-warns>



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

Commonly Spoofed Sector, Brand and Organizations

Source: Straits Times 16 Sep 2017

PHISHING



2,512 phishing URLs
with Singapore link

43% of security incidents reported
to SingCert by **individuals
and SMEs** occurred through
phishing attacks

Commonly spoofed
SECTOR



Banking
and
finance

Commonly spoofed
BRANDS

PayPal
Dropbox
Google

Commonly spoofed
**GOVERNMENT
ORGANISATIONS**

Ministry of Manpower
Immigration & Checkpoints
Authority

Source: CYBER SECURITY AGENCY OF SINGAPORE STRAITS TIMES GRAPHICS

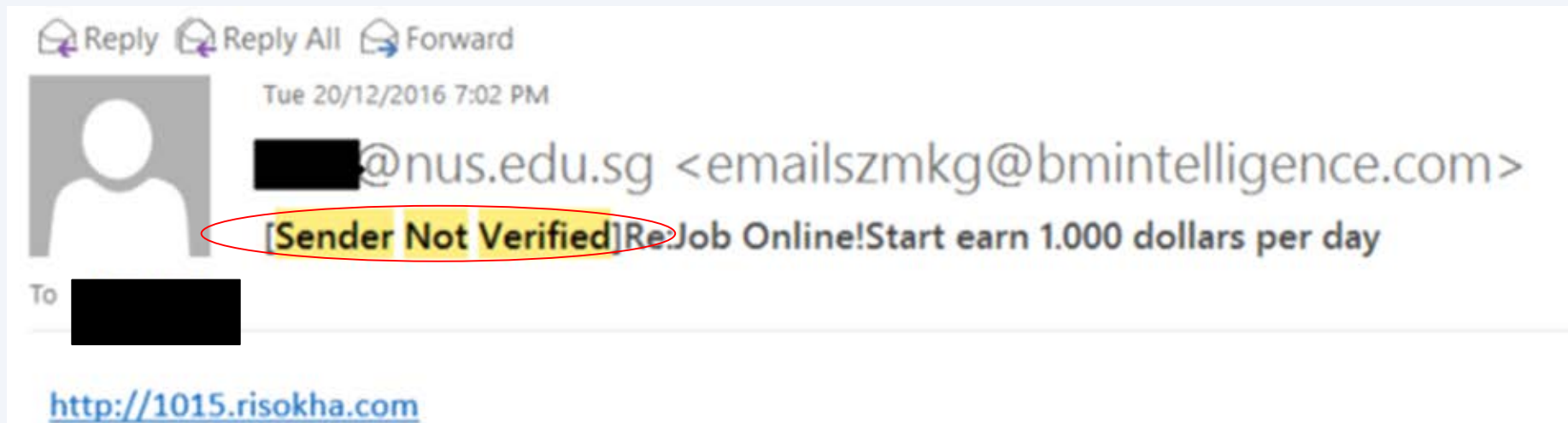
<http://www.straitstimes.com/tech/several-vital-sectors-subjected-to-cyber-attacks-report>



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

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 Attacm
- 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:

Warn me about errors in digitally signed e-mail.

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

Paste Copy Format Painter Clipboard

Basic Text

Names

Include

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

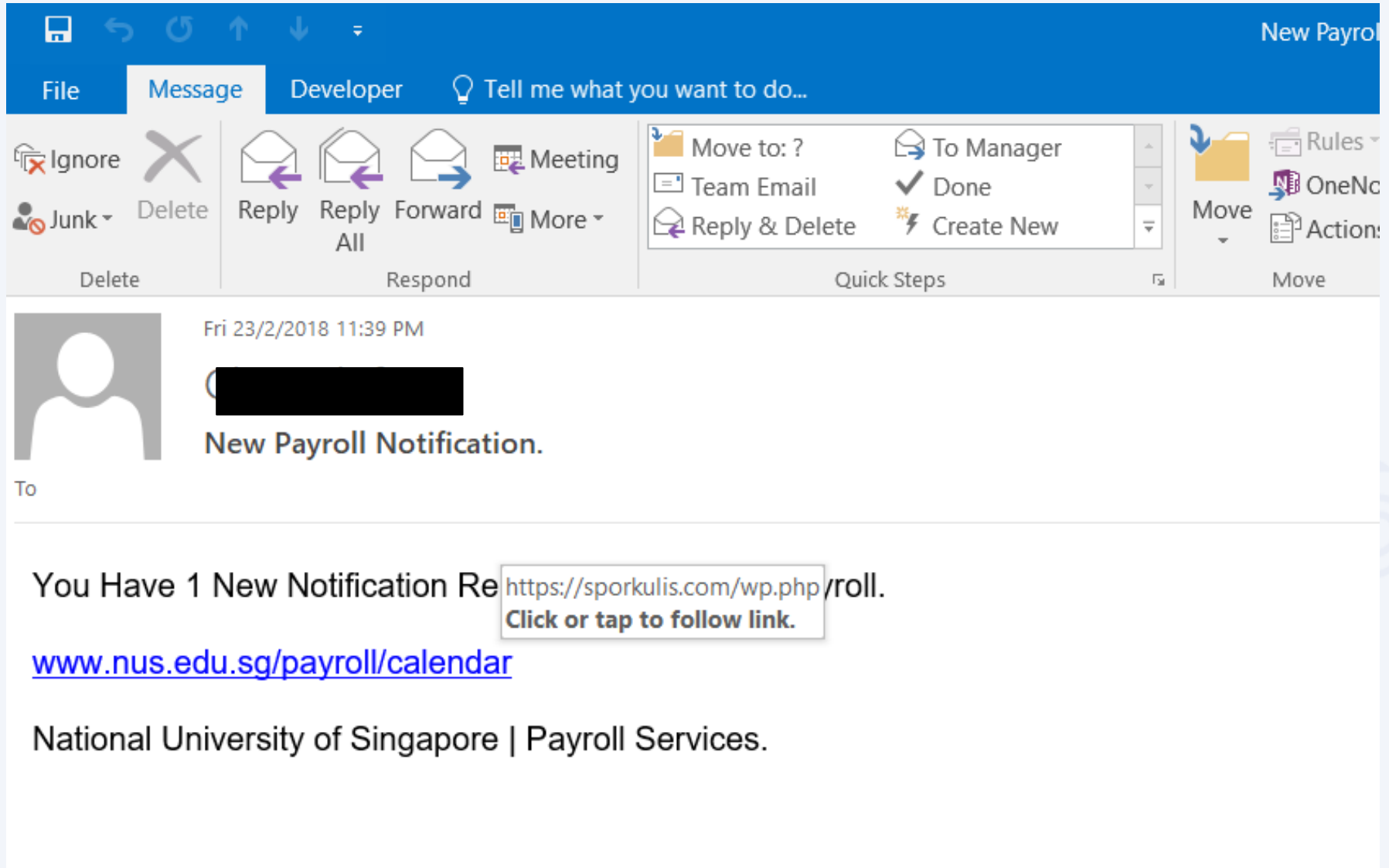
To... itcare-sec@nus.edu.sg

Cc...

Subject

Send

Phishing email targeting NUS



The screenshot shows an Outlook email interface. The top ribbon includes 'File', 'Message', and 'Developer' tabs. The 'Message' tab is active, showing various actions like 'Ignore', 'Delete', 'Reply', 'Reply All', 'Forward', and 'Meeting'. The email content area displays a notification from an unknown sender, dated 'Fri 23/2/2018 11:39 PM'. The subject is 'New Payroll Notification.' The body of the email contains the text: 'You Have 1 New Notification Regarding <https://sporkulis.com/wp.php/payroll>. Click or tap to follow link.' Below this is a blue hyperlink: 'www.nus.edu.sg/payroll/calendar'. The email concludes with 'National University of Singapore | Payroll Services.'



Can Phishing email be sent from legitimate account?

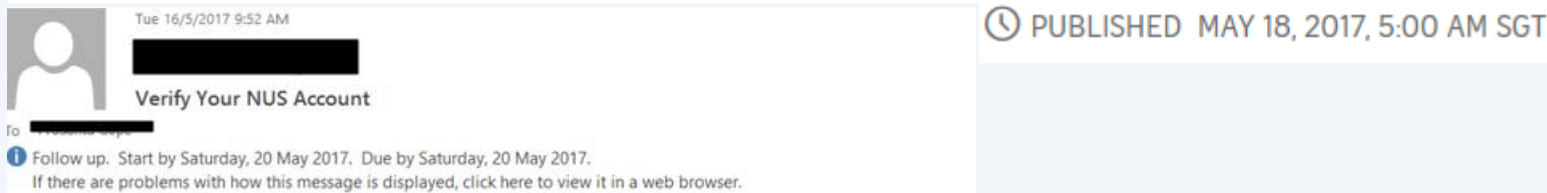
Answer:

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

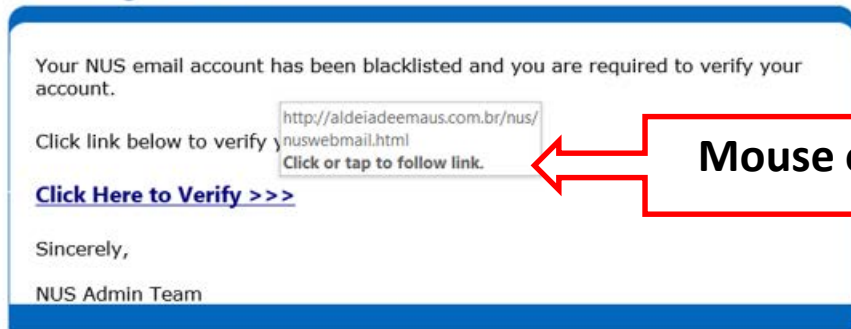
Phishing Email from Legitimate Account

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.



← Image included directly from NUS website



← Mouse over link show non NUS website

© National University of Singapore

← Valid NUS website address

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



Is this a Phishing email?



From: IT Care [mailto:it_care@nus.edu.sg]
Sent: Monday, 9 January 2017 9:13 AM
To: [REDACTED]
Subject: Your mailbox limit has exceeded
Importance: High

Dear Colleagues,

This is a gentle reminder to you from NUS Messaging Team. You and your colleagues have exceeded your mailbox limit. You are required to [login](#) to delete messages from your inbox, junk and deleted item folders. Failure to do so immediately will render your account deactivated.

Sincerely,
NUS Messaging Team

http://login.enterpriserewards.com.sg/be3428/?login_id=0ff8ece9-c297-493d-a1c4-771fe4868e96
Click or tap to follow link.

How to spot a Phishing Email?



- 1 Are you expecting the email? Is it the norm?
- 2 Examine the email address. Is it valid email address?
- 3 Examine the URL. Does it show NUS domain? i.e. nus.edu.sg


The diagram illustrates the components of a URL: `http://pages.example.com/archive/index.html`.
- `http://` is labeled as **protocol**.
- `pages` is labeled as **subdomain** (e.g. organization).
- `example.com` is labeled as **domain** (e.g. industry or country).
- `archive` is labeled as **directory**.
- `index.html` is labeled as **filename**.

- 4 Copy and paste URL into edge browser.



How to verify if a Website is malicious?

Answer:

Use online scanner to help determine if a website is malicious such as <https://www.virustotal.com>, or website that has been reported as Phishing site using <https://www.phishtank.com/>

<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:

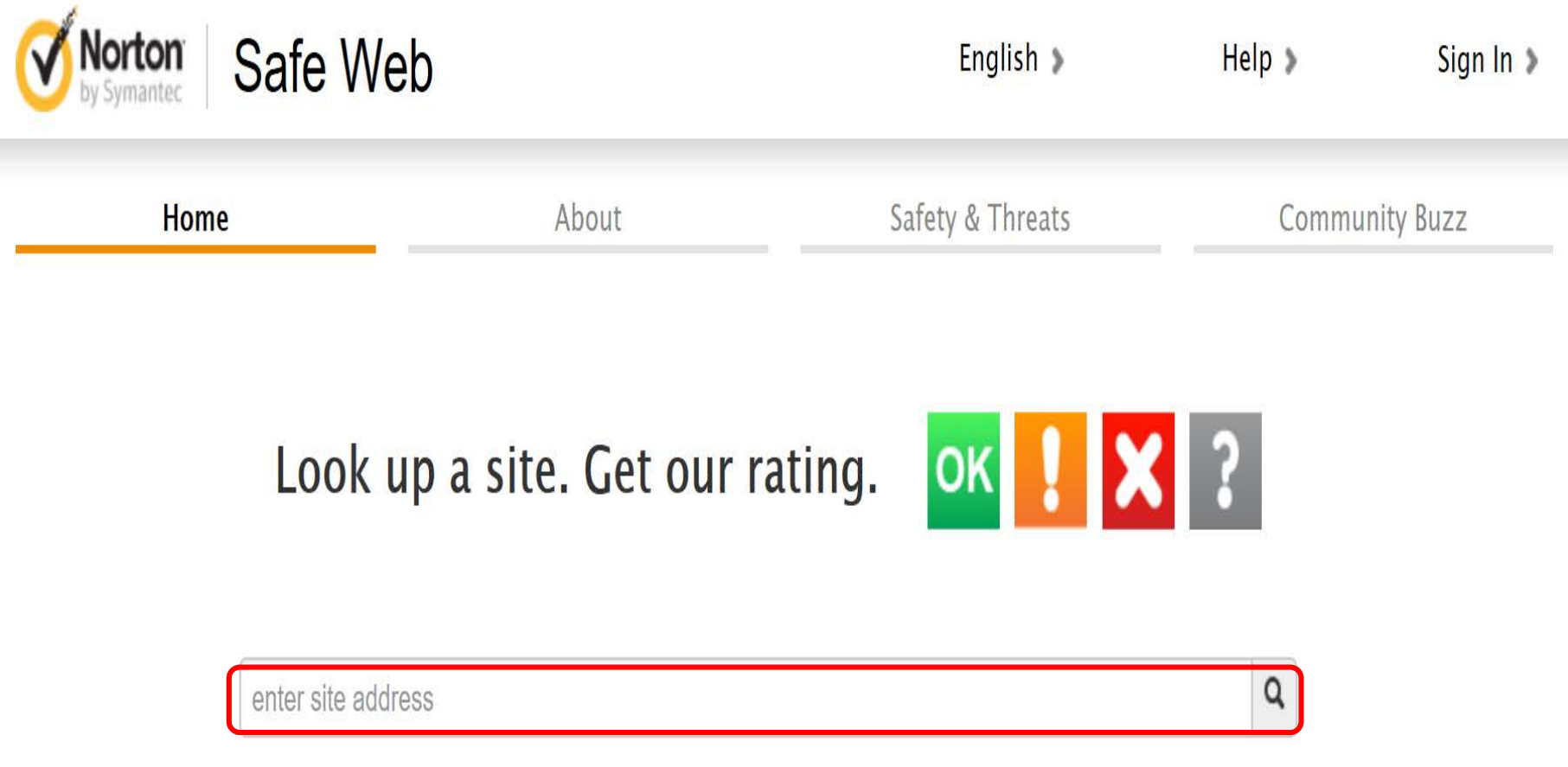
[Is it a phish?](#)

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/>



The screenshot shows the Norton Safe Web website. At the top left is the Norton by Symantec logo. To its right is the text "Safe Web". Further right are links for "English", "Help", and "Sign In". Below this is a navigation bar with four items: "Home" (highlighted with an orange underline), "About", "Safety & Threats", and "Community Buzz". The main content area features the text "Look up a site. Get our rating." followed by four colored icons: a green "OK" icon, an orange exclamation mark icon, a red "X" icon, and a grey question mark icon. Below this is a search input field with the placeholder text "enter site address" and a search icon on the right. The entire interface is set against a white background with a blue and orange curved header.

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



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





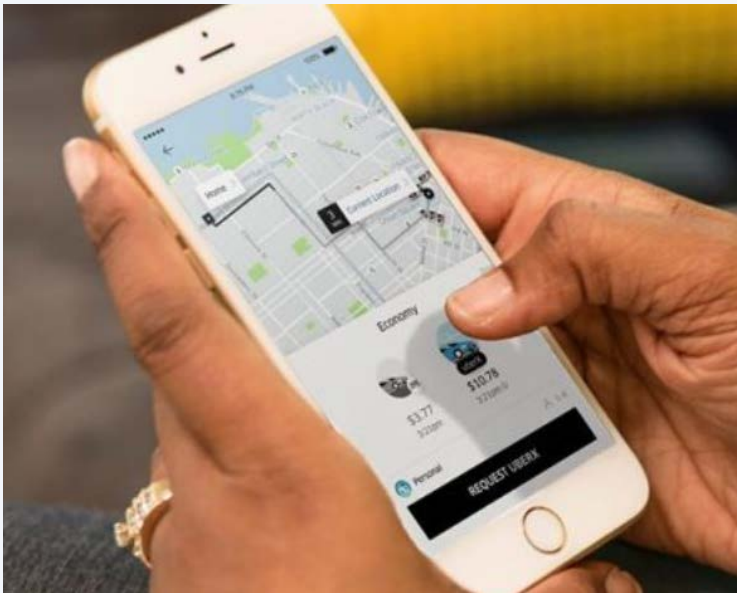
What is the impact of Phishing?



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

Think Before You Click



Phishing Reporter Button



Mon 9/1/2017 8:17 AM

Computer Centre

[New Service] Report Phishing with click of a button

To **NUS Staff**

Signed By computercentre@nus.edu.sg

SERVICE LAUNCH

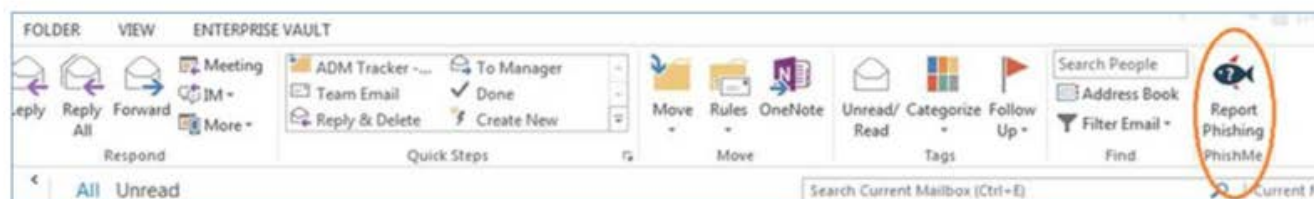
NUS COMPUTER CENTRE

Dear Colleagues,

Organizations suffer from data breaches when attackers gain unauthorised access to an organization's computers and network through phishing emails. To mitigate the risk from such threats, Computer Centre has made a concerted effort to increase security awareness and conduct regular phishing drills. From 9 Jan 2017, we will be rolling out a "Phishing Reporter" button progressively to all Outlook client of computers on NUS network. This will allow you to report Phishing or suspicious email conveniently.

For Windows Computer Users

From 9 Jan 2017, you may see the "Phishing Reporter" button installed on your Microsoft Outlook when you reopen it. No action is required on your part.



However, if you did not see the "Phishing Reporter" button after 19 Jan 2017, please install it via [Software Centre](#).

For MAC Users

Follow the instructions [here](#) to install the "Phishing Reporter" button.

How do I report Phishing or Suspicious Email?

Select the Phishing or suspicious email in the Outlook client and click on the "Phishing Reporter" button.

What happens after I clicked the "Phishing Reporter" button?

The reported email will be removed from your "Inbox" folder and forwarded to Computer Centre for investigation. A copy will remain in your "Sent Items" folder.

The information you provided will help to determine the source of attacks and prevent similar attacks on NUS.

If you have any query, please contact IT Care at 6516 2080 or ITCare@nus.edu.sg.



How do I report Suspicious or Phishing Email?

Answer:

Report suspicious email using Phishing Reporter Button

Email to ITCARE@nus.edu.sg



or



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

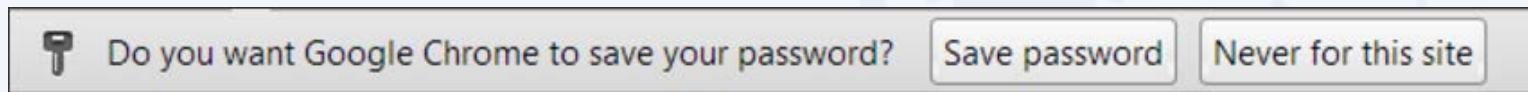
pwned?

You can try key your email account over here

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 Change password periodically.
- 3 Use different account and password for social media and work.
- 4 Don't remember password in web browser.





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>

InformationWeek
DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

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 Veriato

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.

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.
[coinjar.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: **or copy from QR code**

Your BOT ID: **00000000** (put in NOTE field)

During the payment of 300 USD please use your **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



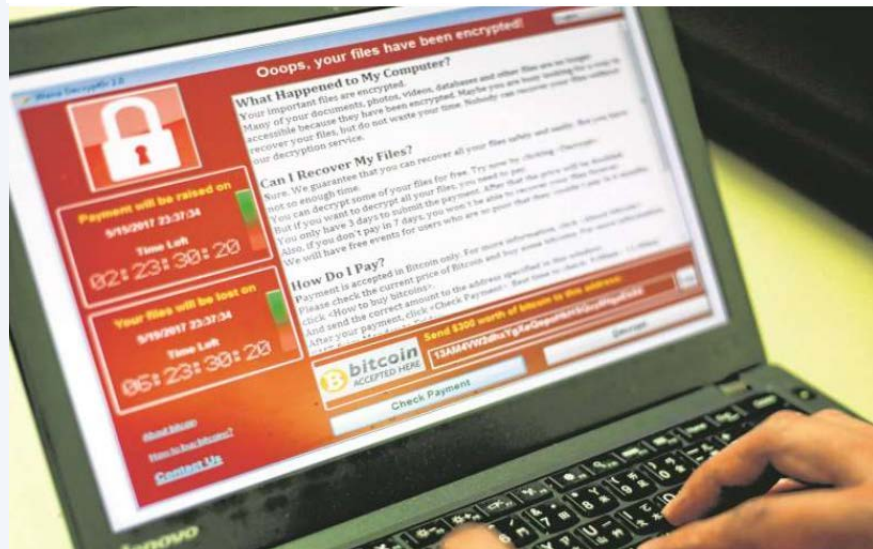
She added that the digital directory service is provided to the mall by a third-party vendor, and that the vendor's system has been disconnected from the board while a software patch is being installed.

“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.

WannaCry Ransomware

WannaCry ransomware: Critical sectors not affected at end of Monday



ST

PUBLISHED MAY 15, 2017, 6:49 PM SGT

Victims either did not apply a software patch, released in March (2017), to fix a known flaw in their Microsoft Windows systems, or were using old, unsupported systems such as Windows XP or Windows Server 2003.

Users might have initially been infected by clicking on a bogus link or attachment in the e-mail. Then the worm spreads to multiple machines over the intranet or Internet using a capability believed to have been developed by the United States National Security Agency - causing the attack to be unprecedented in scale by any ransomware

Advisory: WannaCry



Mon 15/5/2017 2:25 PM

Computer Centre

[Security Advisory] Widespread "WannaCry" Ransomware targeting unpatched Windows Systems

To  **NUS Staff**

Signed By computercentre@nus.edu.sg



Dear Colleagues,

As you know, there is a worldwide infection with a ransomware known as "WannaCry" aka "WanaCryptOr" discovered on 12th May 2017 that can infect any unpatched Windows device connected to the same network.

This ransomware can be blocked by a patch released by Microsoft in March 2017. Computer Centre deployed this patch within NUS in the same month as part our regular patch exercise. Since Friday, 12th May 2017, Computer Centre has taken additional measures to detect and block the intrusion and spread of this ransomware.

However, given the ease with which this ransomware infection can spread, it is very important that you double-check your desktop computer or laptop as soon as possible to confirm that your Windows software is up to date, using the following steps. If there are updates available, please install them.

For Windows 7 – Go to **Control Panel -> Windows Update -> Check for available updates**

For Windows 8 – Go to **Settings -> Change PC Settings -> Windows Update**

For Windows 10 – Go to **Settings -> Update & Security -> Windows Update**

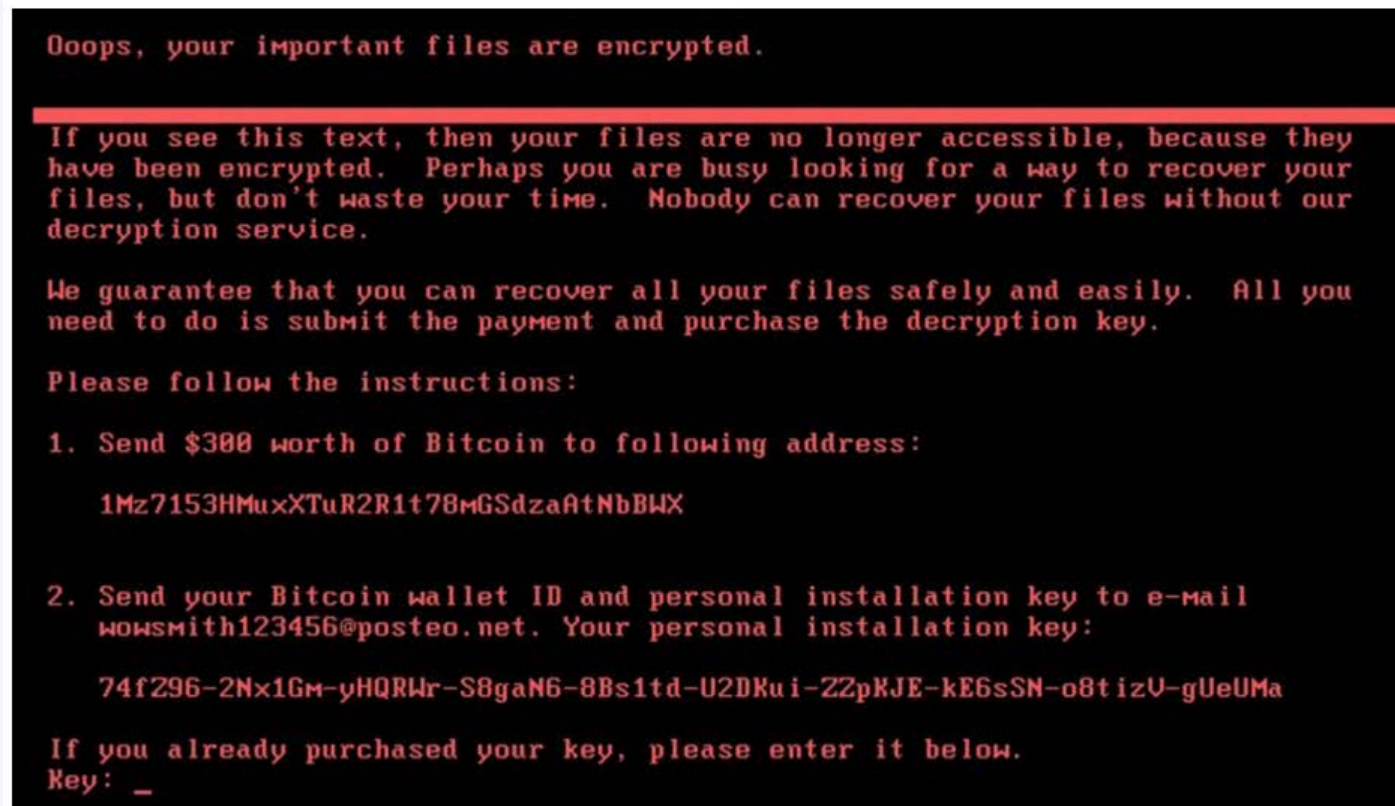
Latest Global Ransomware - Petya

<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.



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

Impact of Ransomware - Petya

<http://www.bbc.com/news/technology-40416611>



Global ransomware attack causes turmoil

The virus, the source of which is not yet known, freezes the user's computer until a ransom in untraceable Bitcoin is paid.

Ukrainian firms, including the state power company and Kiev's main airport, were among the first to report issues.

The Chernobyl nuclear power plant has also had to monitor radiation levels manually after its Windows-based sensors were shut down.

In a statement, the US National Security Council said government agencies were investigating the attack and that the US was "determined to hold those responsible accountable".

Petya Ransomware

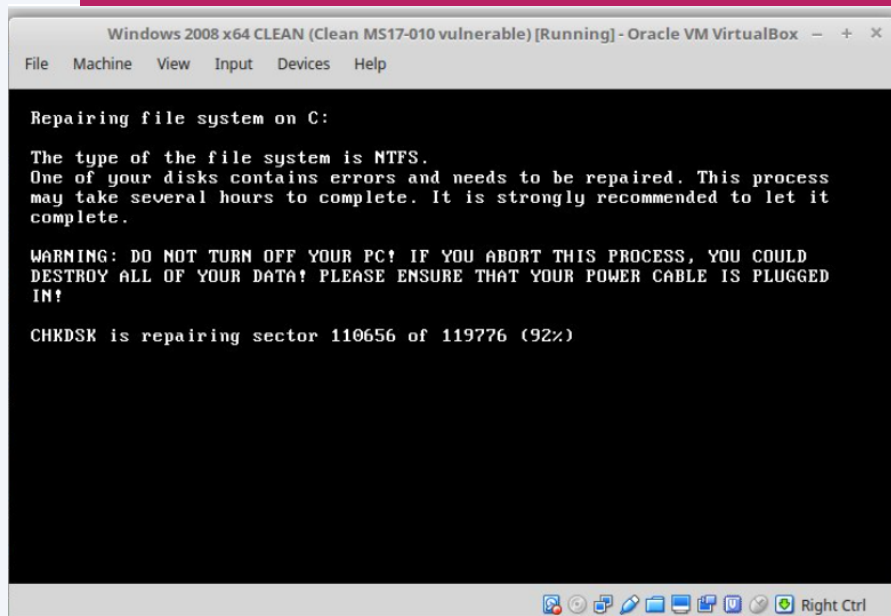
theguardian Wednesday 28 June 2017

What is the Petya ransomware attack, and how can it be stopped?

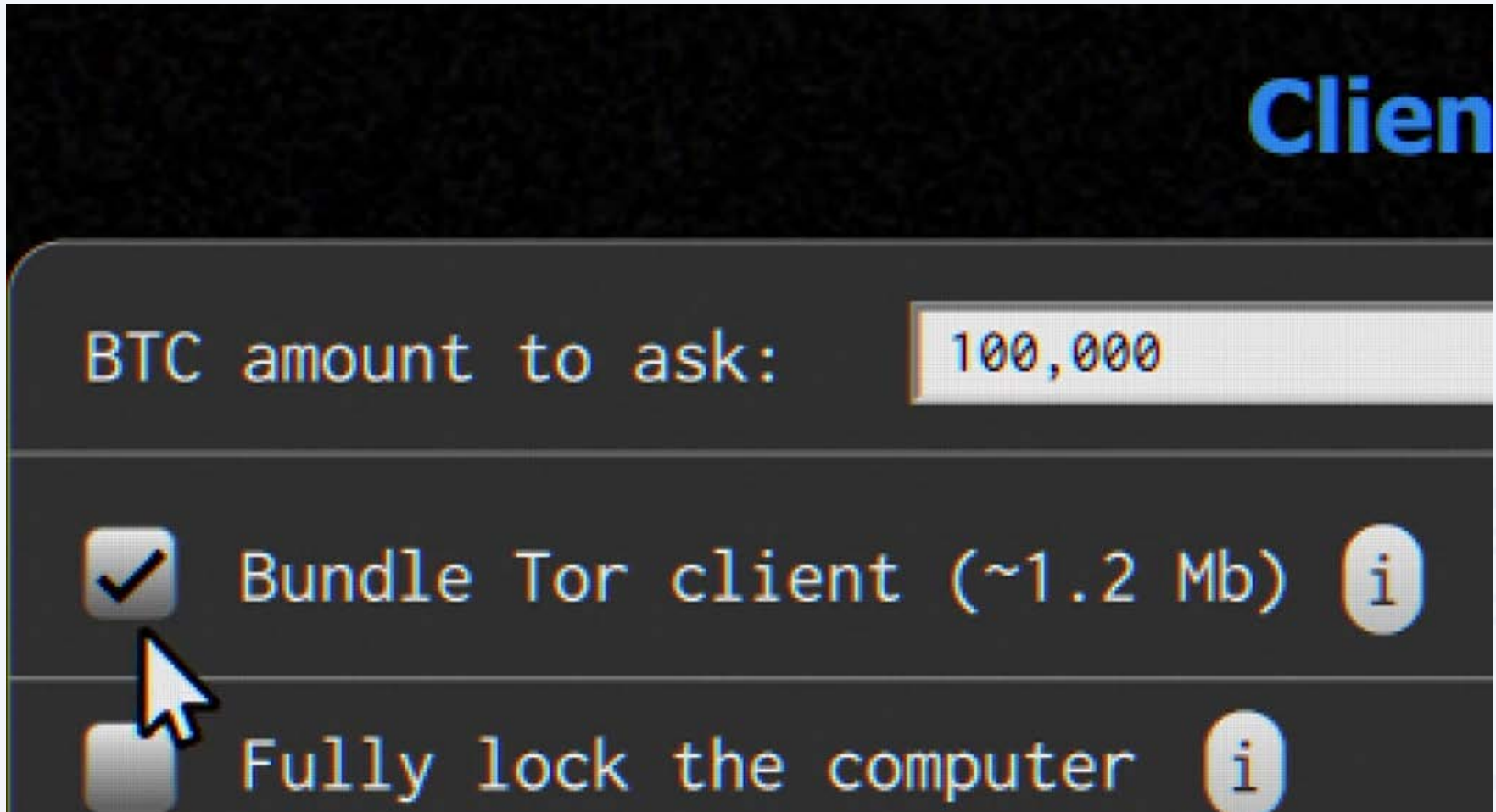
Companies have been crippled by an attack dubbed 'Petya', the second major ransomware crime in two months. **Olivia Solon** answers the key questions

The ransomware infects computers and then waits for about an hour before rebooting the machine. While the machine is rebooting, you can switch the computer off to prevent the files from being encrypted and try and rescue the files from the machine, as flagged by @HackerFantastic on Twitter.

If the system reboots with the ransom note, don't pay the ransom – the “customer service” email address has been shut down so there's no way to get the decryption key to unlock your files anyway. Disconnect your PC from the internet, reformat the hard drive and [reinstall your files from a backup](#). Back up your files regularly and keep your anti-virus software up to date.



Video: Ransomware



Source: https://www.youtube.com/watch?v=4gR562GW7TI&list=PLSJO6rbiqUDVe_I7QvGdrJnjOmaTqZfUR&index=20



**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





Should I pay the ransom?

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



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



The screenshot shows a web browser window with the URL [nomoreransom.org/en/decryption-tools.html](https://www.nomoreransom.org/en/decryption-tools.html). The page features a navigation menu with links: Crypto Sheriff, Ransomware: Q&A, Prevention Advice, Decryption Tools, Report a Crime, Partners, and About the Project. A prominent banner reads "NO MORE RANSOM!" in large, bold, black letters. Below this, a circular icon depicts a hand holding a key, with the text "DECIPHER" written vertically on the key. To the right of the icon, the text "DECRYPTION TOOLS" is displayed in a large, black, typewriter-style font. A red diagonal banner on the left side of the page reads "Winner SC Awards EDITOR'S CHOICE AWARD". A language dropdown menu is set to "English".

NO MORE RANSOM!

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.

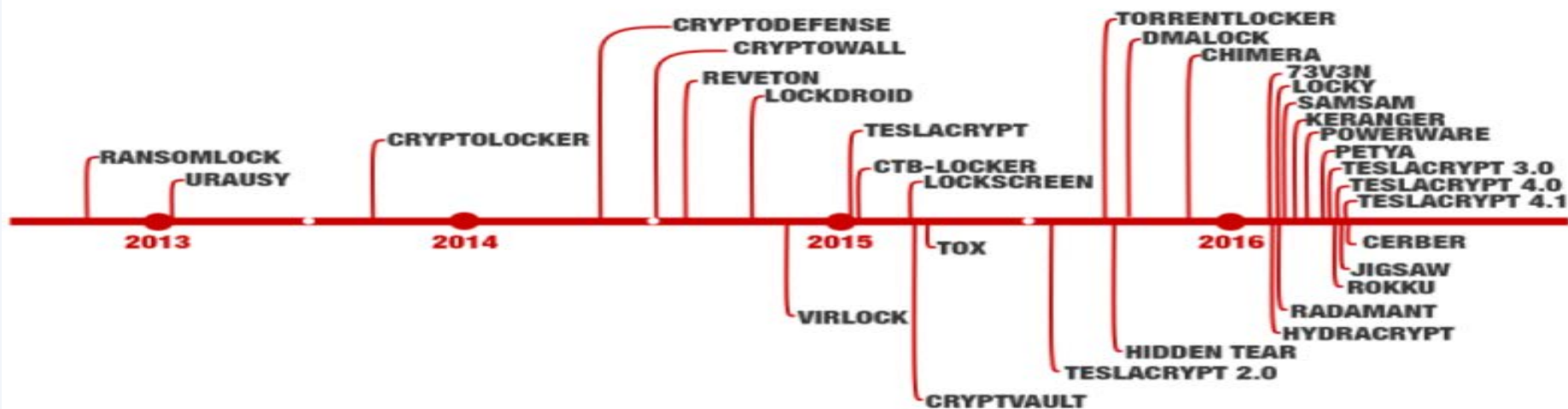
Source: <https://www.nomoreransom.org/en/decryption-tools.html>

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.



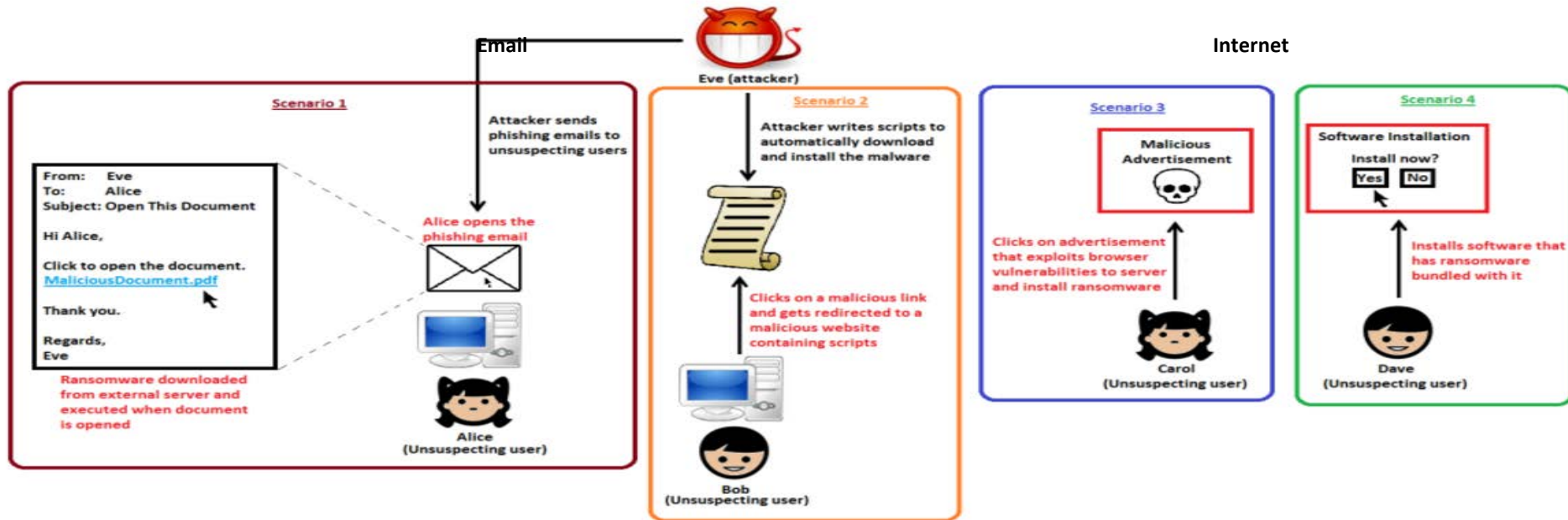
A compromised computer is a hazard to everyone else, too – not just to you.



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 Infected USB

Public servants barred from using unauthorised USB drives

 CHANNEL NEWSASIA

14 Jul 2017 02:48PM

(Updated: 14 Jul 2017 04:54PM)



The move comes after Internet access was cut from the work computers of all 143,000 public officers earlier this year, in a bid to prevent cyberattacks. Officers are still able to surf the Internet, but only on mobile devices or computers that are not connected to the office network.

“USB storage devices continue to be a means to introduce malware and exfiltrate data, especially as they have the potential to be easily misplaced,” it said.

...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 Aplock – 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 Free Antivirus 2016+RAM Boost & Aplock | 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 – Free Antivirus 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 & Aplock – 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.

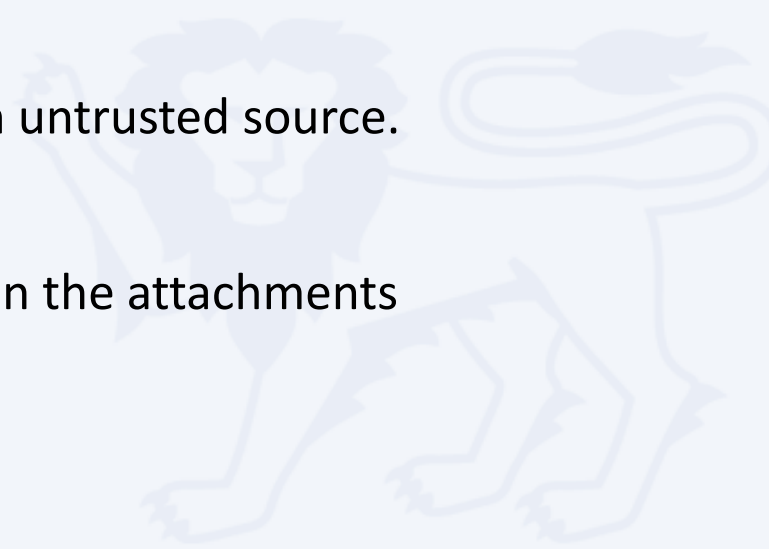
Affected users are strongly recommended to update their CCleaner software to version 5.34 or higher, in order to protect their computers from being compromised

Best Practices

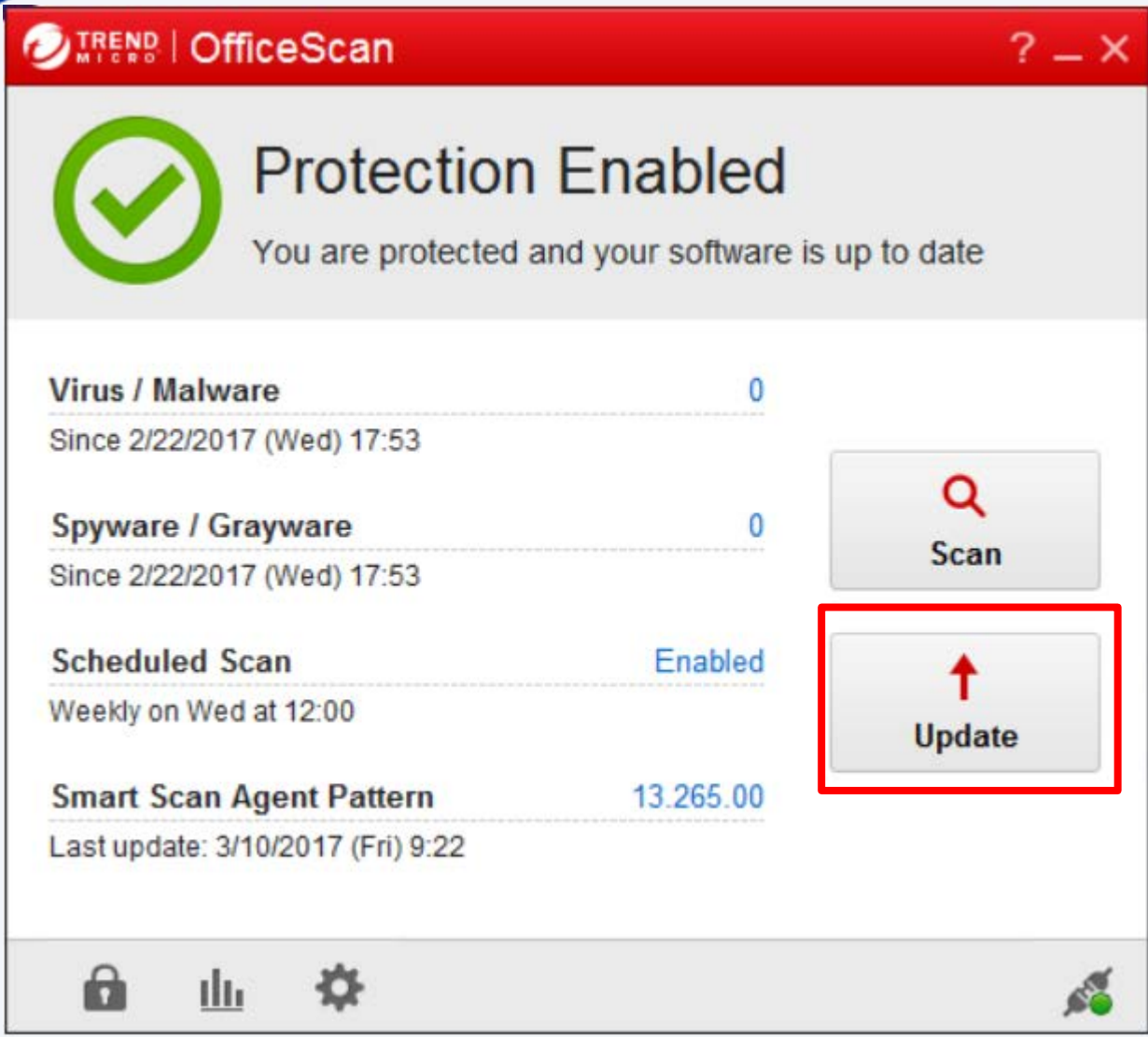


What are the protection measures?


- 1 Perform data backup regularly.
- 2 Keep your machines up to date with anti-virus software.
- 3 Keep your Operating System and Software updated.
- 4 Do not download the software from untrusted source.
- 5 Report suspicious email. Do not open the attachments or visit the websites.



University Virus Scanner



TREND MICRO | OfficeScan ? _ X

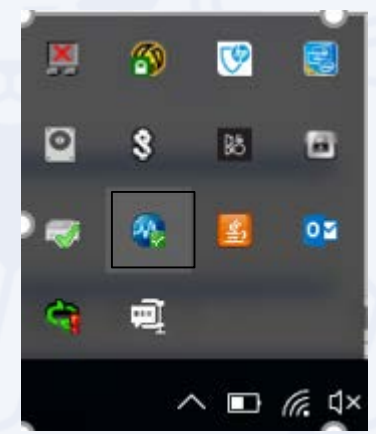
 **Protection Enabled**
You are protected and your software is up to date

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 (magnifying glass icon)

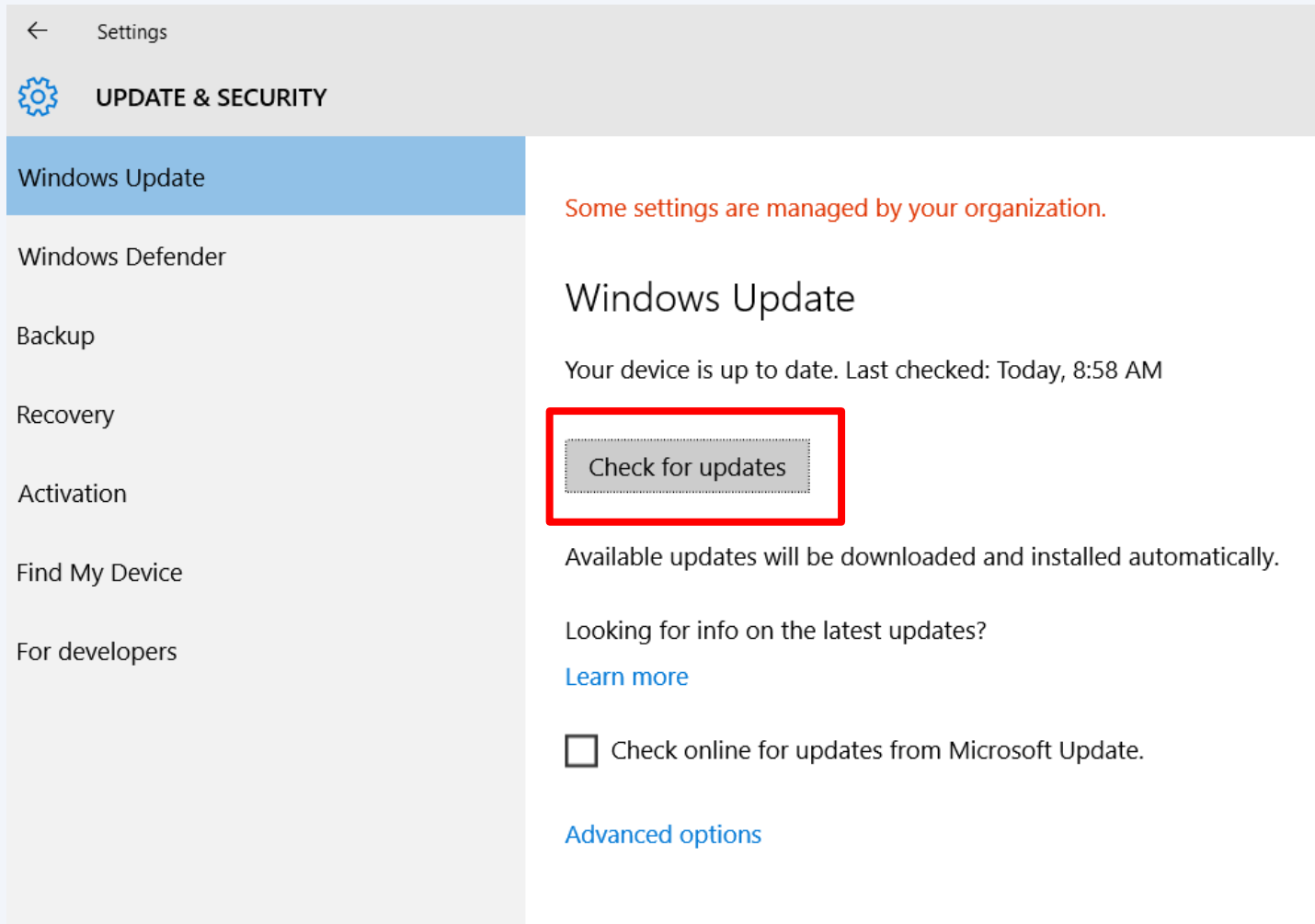
Update (upward arrow icon) - *Highlighted with a red box*

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




Window OS Updates

Settings\ Update and Security



The screenshot shows the Windows Settings application, specifically the 'UPDATE & SECURITY' section. The left-hand navigation pane lists various settings categories: Windows Update (highlighted in blue), Windows Defender, Backup, Recovery, Activation, Find My Device, and For developers. The main content area on the right is titled 'Windows Update' and displays the message 'Your device is up to date. Last checked: Today, 8:58 AM'. A red rectangular box highlights the 'Check for updates' button, which is a grey button with a dotted border. Below this, there is a message: 'Available updates will be downloaded and installed automatically.' followed by a link 'Learn more'. At the bottom, there is an unchecked checkbox labeled 'Check online for updates from Microsoft Update.' and another link 'Advanced options'.

← 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

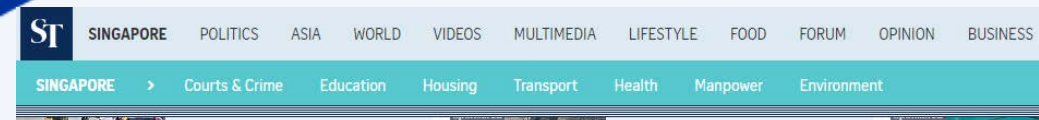
Available updates will be downloaded and installed automatically.

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

Check online for updates from Microsoft Update.

[Advanced options](#)

Confidentiality



Singapore privacy watchdog fines and warns 11 organisations for data breaches



Thursday, Apr 21, 2016

PDPC noted in a press release today (April 21) that 90,000 members' personal data were sent in an unencrypted email between K Box and its IT vendor, Finantech

The personal data of over 300,000 customers were exposed, with the firm possibly facing sanctions for lax security. Their names, addresses and mobile phone and identity card numbers were posted on several websites

Investigations by PDPC found that someone had extracted customers' information from K Box's computers and uploaded the data on file sharing website pastebin.com because the karaoke chain's security measures were lax. For instance, it did not update its computer software with the latest version, and computer account holders had weak passwords comprising only one letter in the alphabet.

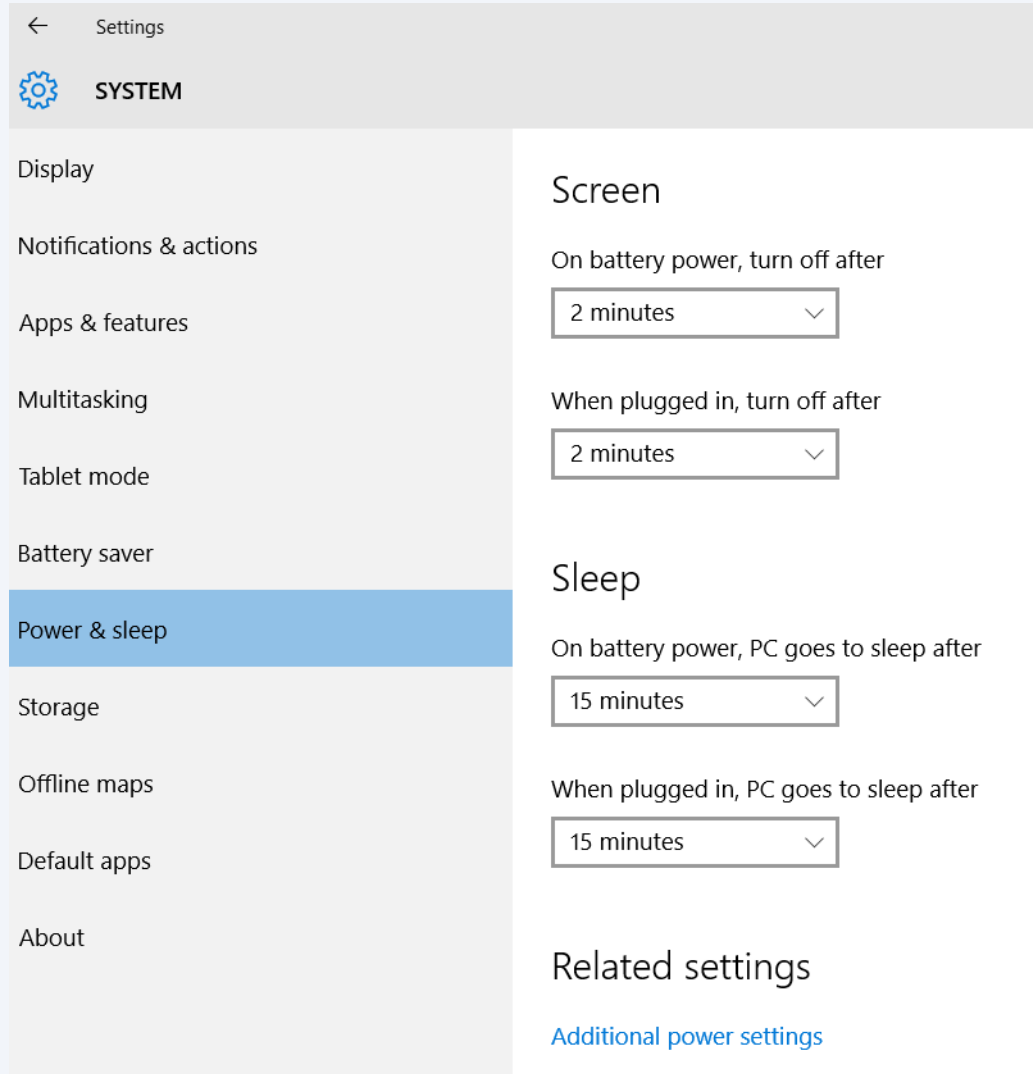


K Box was fined \$50,000 for not putting in place sufficient security measures to protect the pe
PHOTO: ST FILE

Source: Straits Times, Asia One @ Apr 2016


Window Screen Lock

Settings\ Personalization\ Lock Screen



The screenshot shows the Windows Settings application. At the top, there is a back arrow and the word 'Settings'. Below that is a gear icon and the word 'SYSTEM'. A list of settings categories is on the left, with 'Power & sleep' highlighted in blue. The main content area is divided into two sections: 'Screen' and 'Sleep'. The 'Screen' section has two settings: 'On battery power, turn off after' set to '2 minutes' and 'When plugged in, turn off after' set to '2 minutes'. The 'Sleep' section has two settings: 'On battery power, PC goes to sleep after' set to '15 minutes' and 'When plugged in, PC goes to sleep after' set to '15 minutes'. At the bottom, there is a 'Related settings' section with a link to 'Additional power settings'.

← 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](#)

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

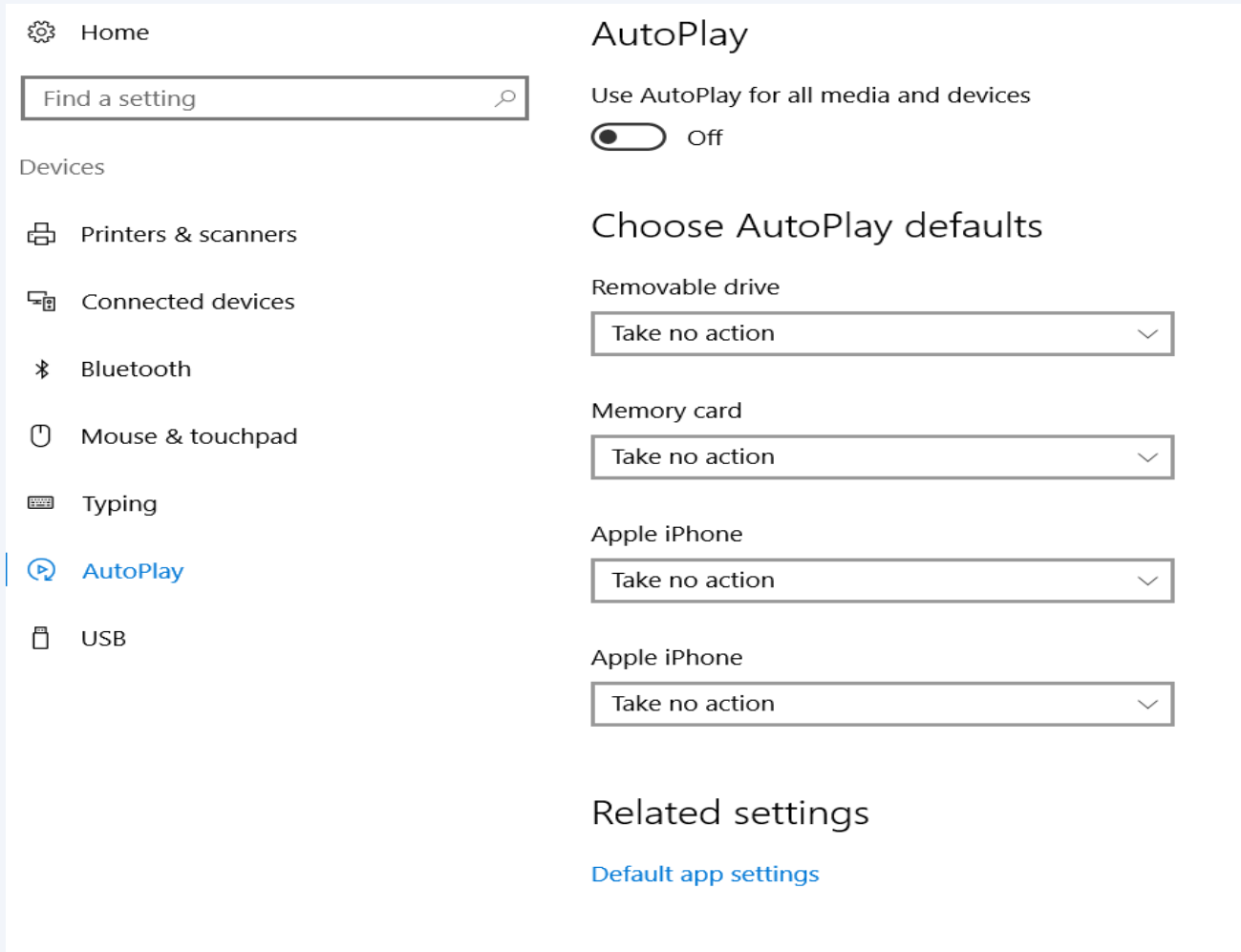
<http://www.channelnewsasia.com/news/singapore/smu-law-student-jailed-2/2519788.html>

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



Prevent USB from being auto run on your laptop



The screenshot shows the Windows Settings application. On the left, the 'AutoPlay' setting is selected and highlighted in blue. The main area displays the 'AutoPlay' settings. At the top, the 'AutoPlay' title is followed by the toggle 'Use AutoPlay for all media and devices', which is currently turned off. Below this, the 'Choose AutoPlay defaults' section contains three dropdown menus: 'Removable drive', 'Memory card', and 'Apple iPhone'. Each dropdown menu is currently set to 'Take no action'. At the bottom, the 'Related settings' section includes a link for '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

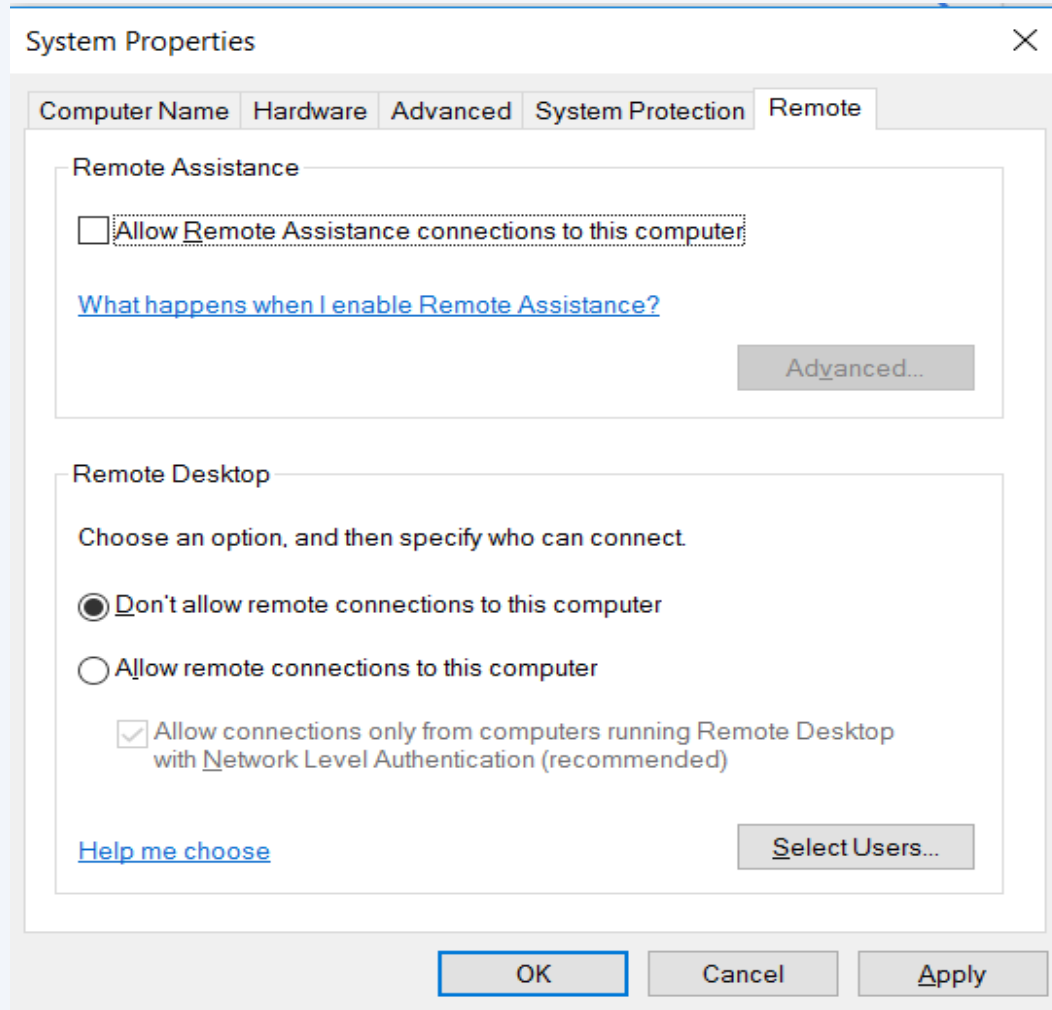
Take no action

Related settings

[Default app settings](#)

Turn off Remote Desktop Connection to your PC

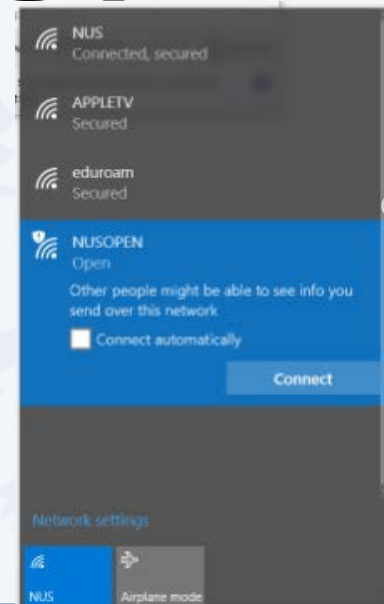
SystemPropertiesRemote.exe



Note: This state disallows remote access to your computer.

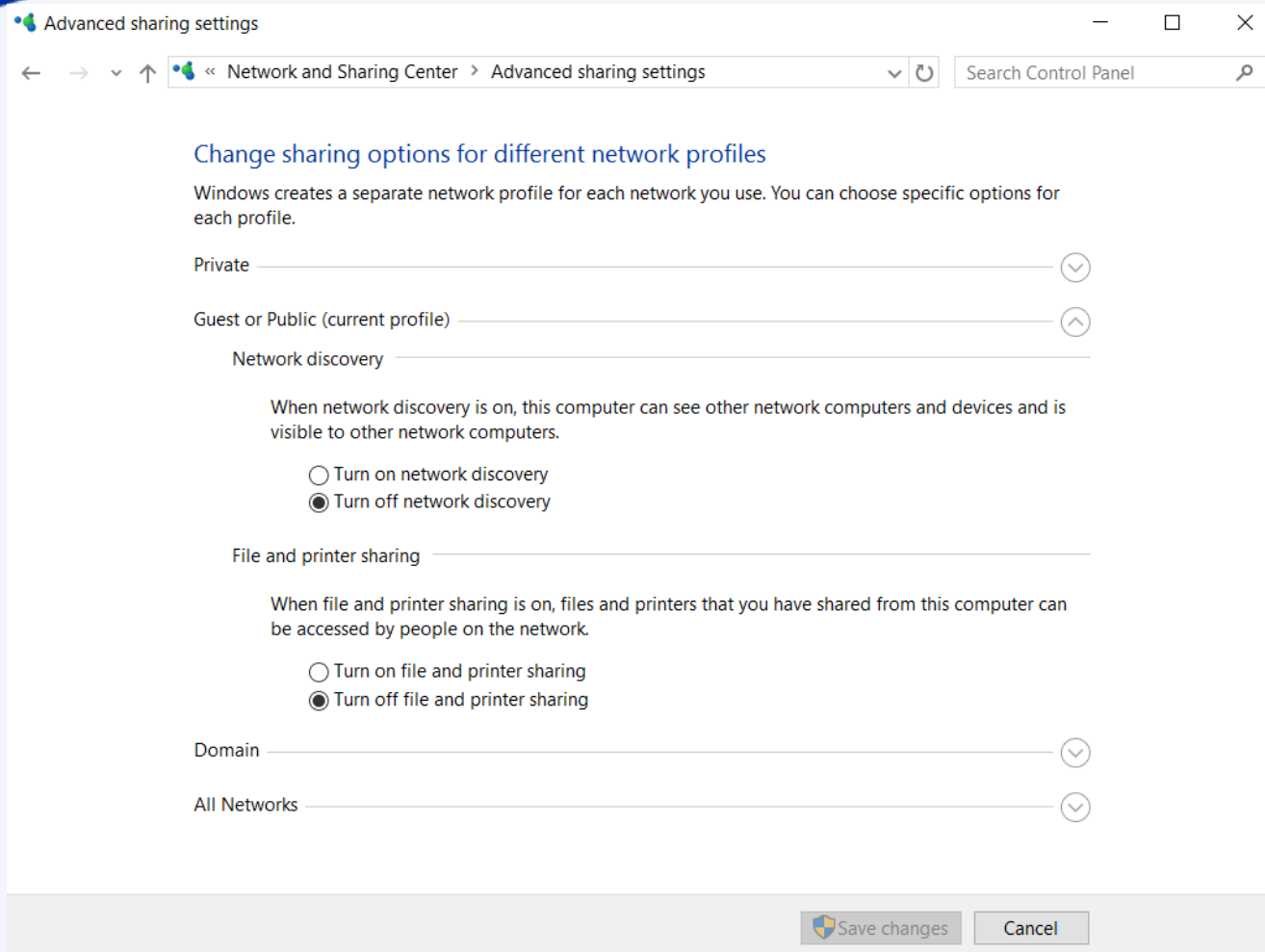


Which University WiFi should I use?



Answer: NUS

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

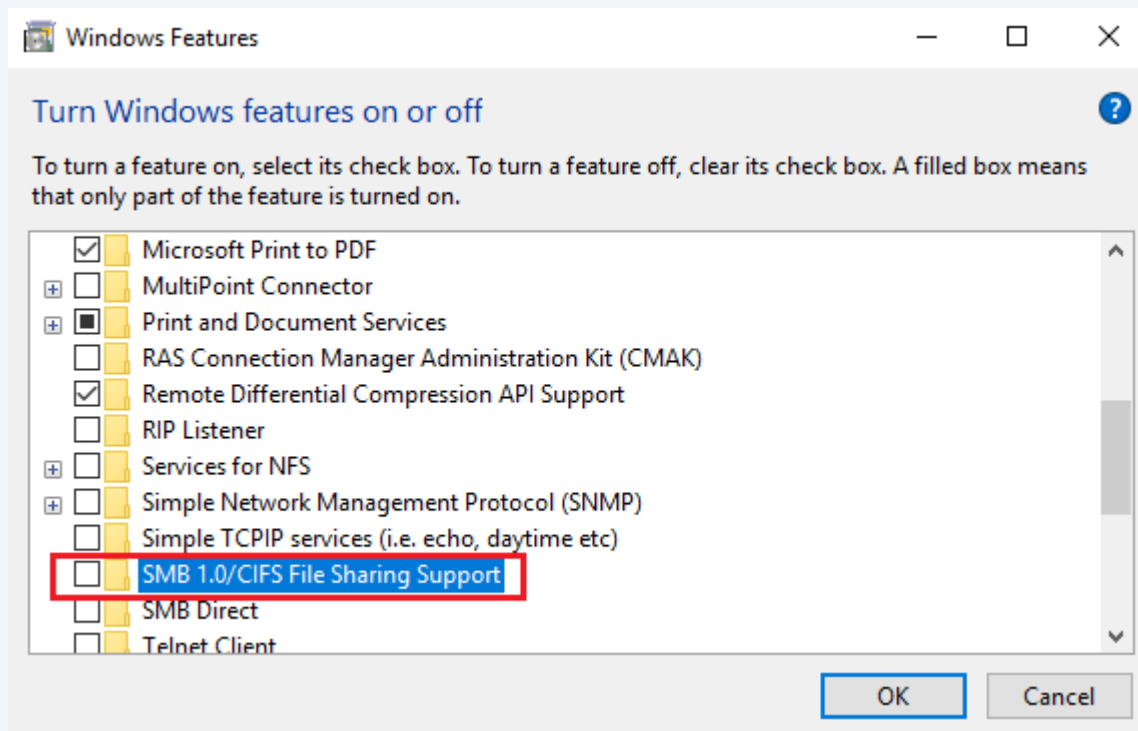
All Networks

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.

Disable File Sharing (SMB v1)

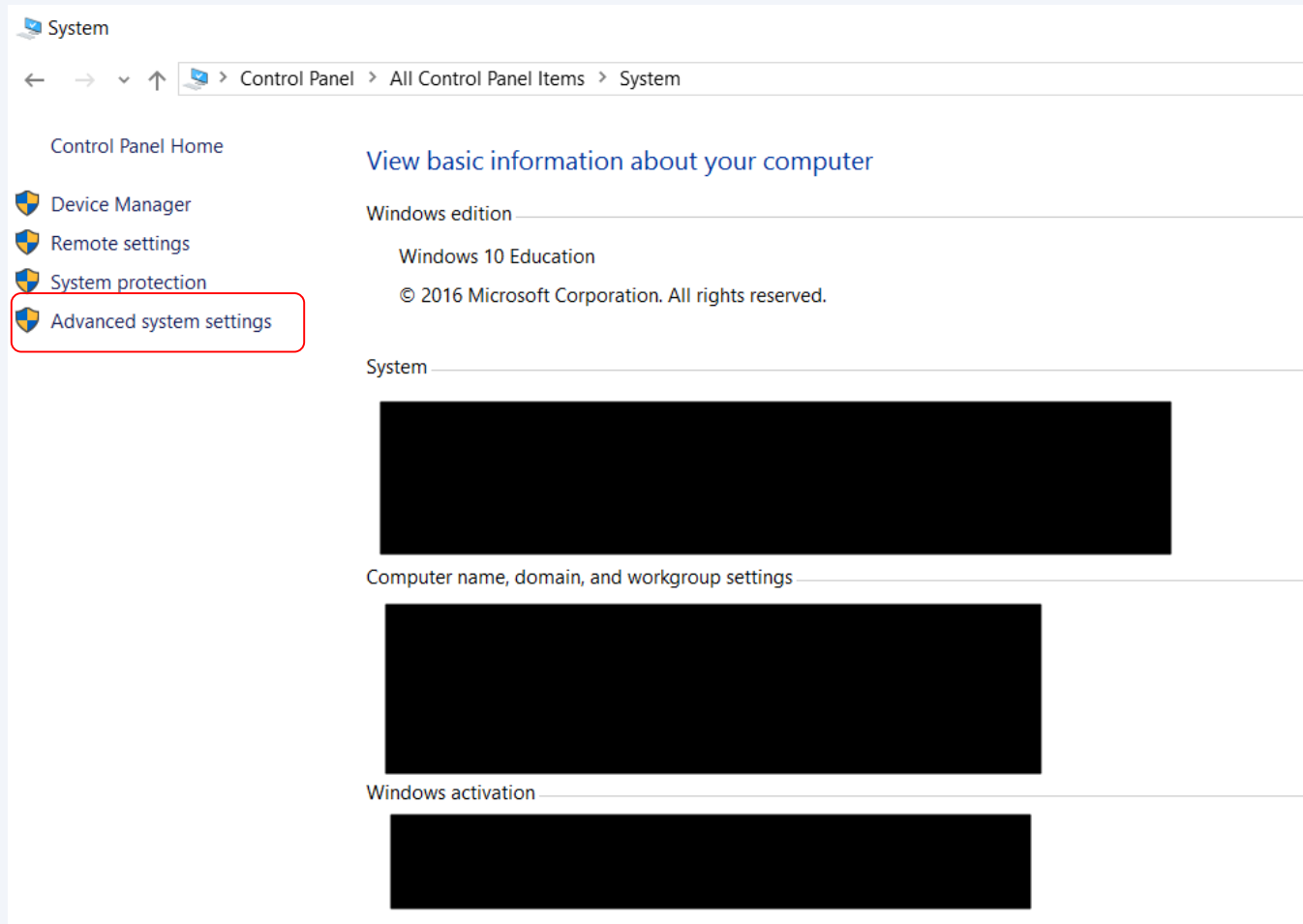
Open Control Panel > Programs & Features > **Turn Windows features on or off.** **Make sure it is unchecked.** Restart your computer.



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

Enable Data Execution Prevention (1/3)

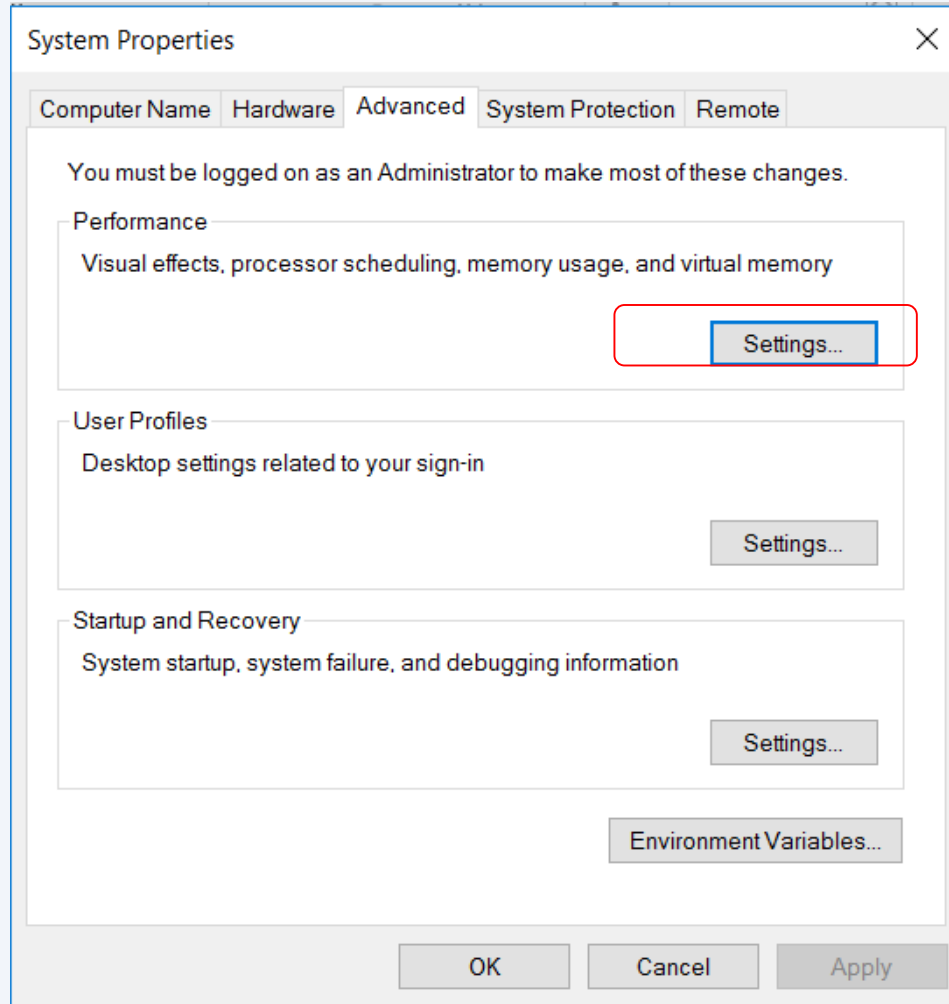
Open Control Panel > System > **Advance System Settings**



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

Enable Data Execution Prevention (2/3)

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

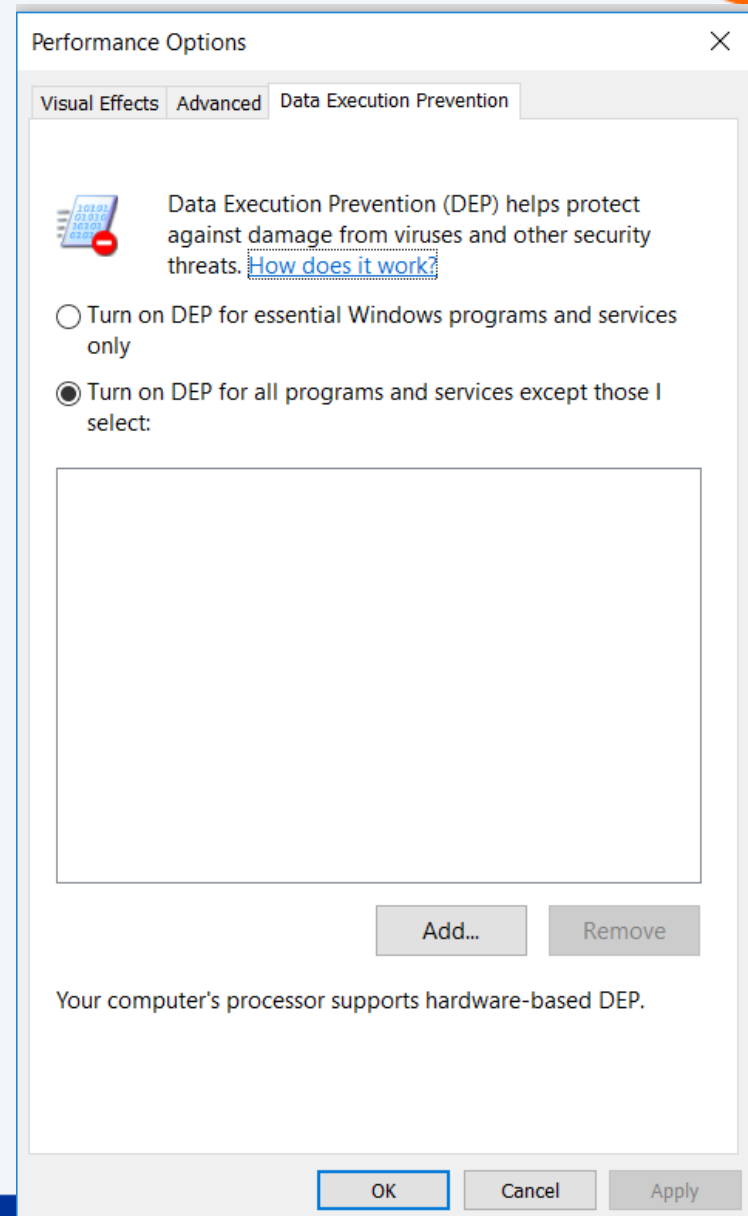


Note: This ensures program are not run on unauthorized memory area

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.



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

3 Advanced settings

Block pop-ups
 On

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.



Supplementary Slides





**How do I know
if my mobile
phone is
infected?**



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

Impact

The malware author can obtain sensitive information such as passwords and personal details from affected phones. Users may risk paying for a fake subscription to ensure the security of their mobile devices. Users with an infected phone will observe the following symptoms:

- Annoying ads pop up when data connection is available
- Sluggish phone performance
- Automatic downloading and installation of apps
- Existing apps function differently from usual
- Fake notifications or warnings on the mobile device
- Decrease in phone storage capacity

Prevention

- Do not download or install apps from non-official app stores
- Use a reputable anti-virus/anti-malware scanner to scan apps before installing
- Do not click on suspicious links, web pages or advertisements