

# IT Security Awareness Talk

## By NUS IT

Apr 2019

## Outline

1. Lesson Learnt From SingHealth Data Breach & Best Practices
2. Identify and Report Security Incident
3. Trending Cyber-attacks Techniques & Best Practices
4. Data Protection Measures



# Lesson Learnt From SingHealth Data Breach



## How did the data breach occur?

### WHAT DATA WAS TAKEN?

**NAME, NRIC NUMBER,  
ADDRESS, GENDER, RACE  
AND DATE OF BIRTH OF  
1.5 MILLION PATIENTS  
RECORDS OF OUTPATIENT  
MEDICINE DISPENSED TO  
ABOUT 160,000 PATIENTS**

# TODAY

05 OCTOBER, 2018

The hackers behind the SingHealth cyber attack snuck in...nearly a year before stealing the data of **1.5 million patients...**

The attacker gained a foothold through an unpatched **front-end computer** at Singapore General Hospital, likely through a **phishing email**.

<https://www.todayonline.com/singapore/malware-used-singhealth-cyber-attackers-uniquely-tailored-had-not-been-observed-elsewhere>

## How did the data breach occur?

**SINGHEALTH CYBERATTACK**

21 SEPTEMBER, 2018 

May - Jun 2018

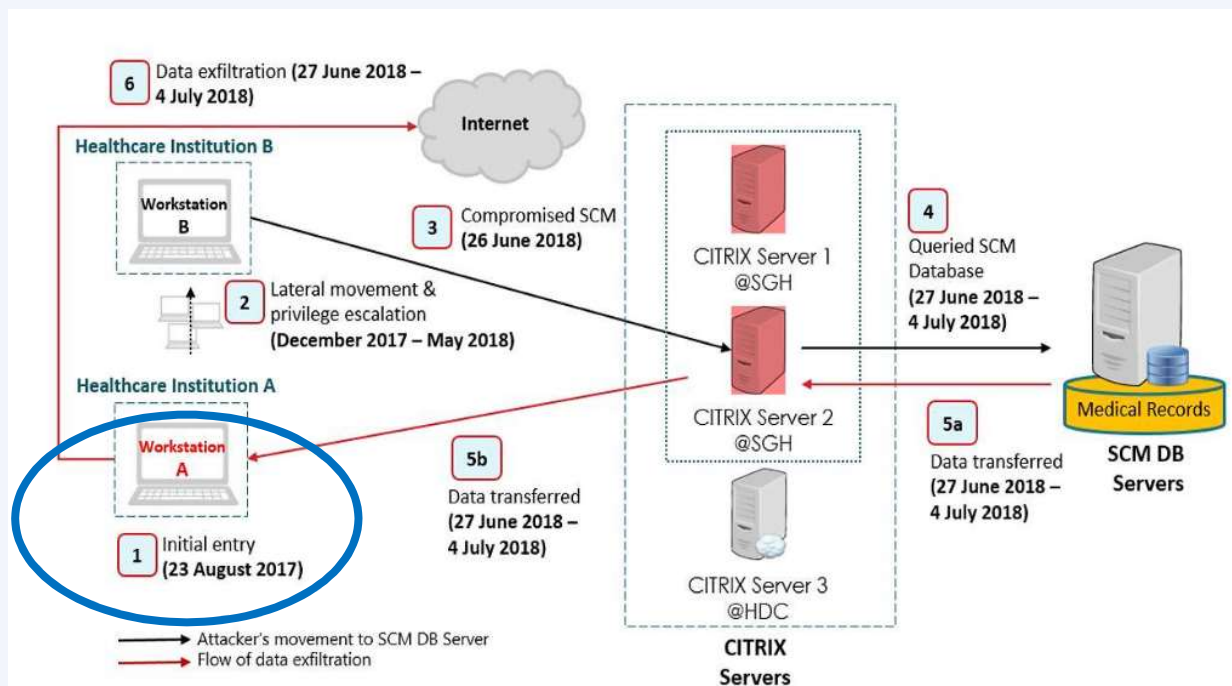


“The attacker was able to gain access to an end-user workstation via a publicly available hacking tool because the workstation was running on a version of **Microsoft Outlook** that was not patched to address the use of that hacking tool,” ...

<https://www.channelnewsasia.com/news/singapore/singhealth-cyberattack-committee-inquiry-staff-hack-10744182>

## Factors Leading to the Data Breach @ Front End Computer

- 1 User fall prey to Phishing email
- 2 Front end workstation was running vulnerable version of Outlook



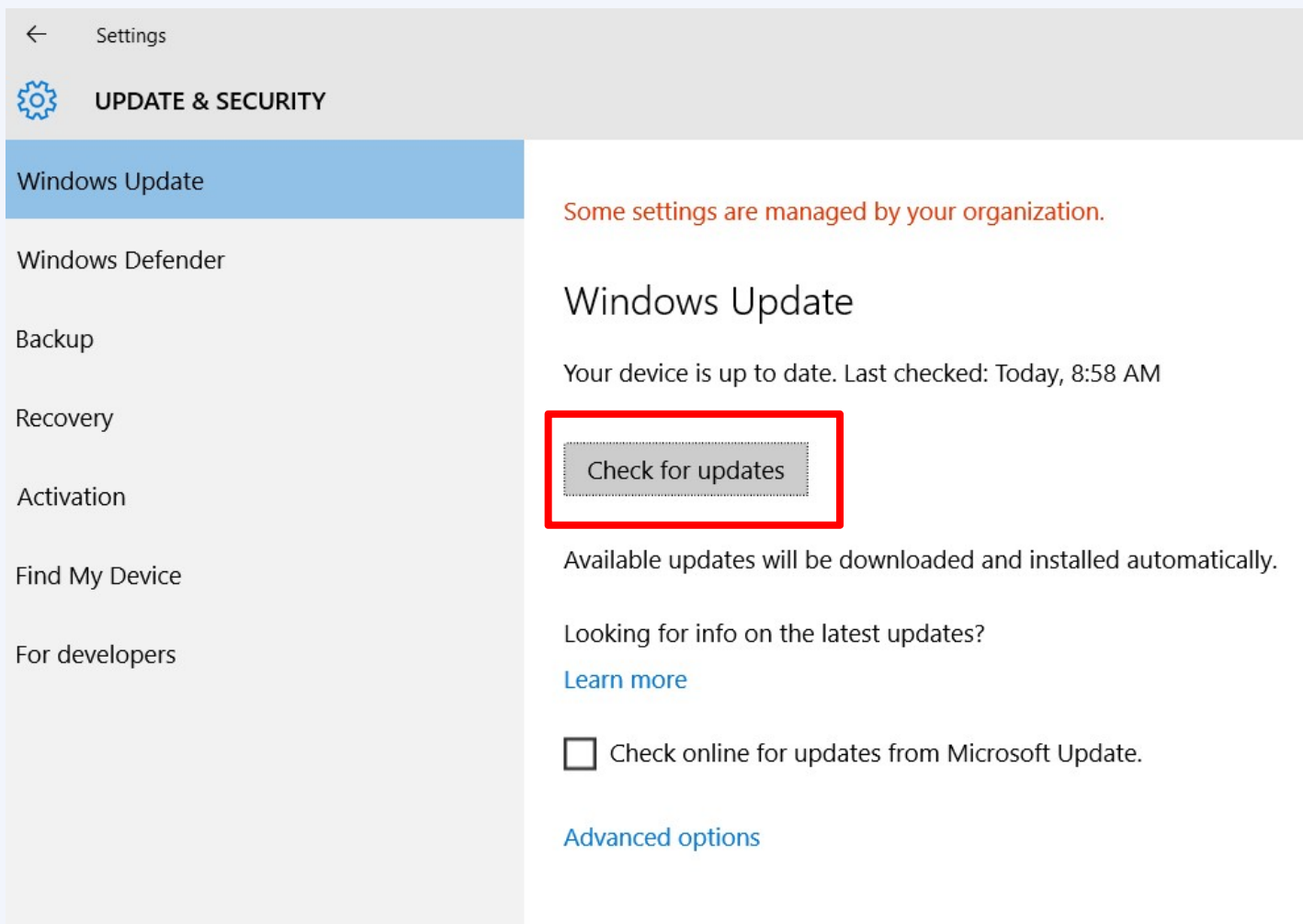
<https://www.channelnewsasia.com/news/singapore/customised-uniquely-tailored-malware-singhealth-cyberattack-10794852>

## Averting the Data Breach - Apply Security Best Practices

- 1 Keep operating system updated
- 2 Keep software updated
- 3 Disable Windows PowerShell (tool for system administrator)
- 4 Stay vigilant, don't click on suspicious email and report it

# Keep Window OS Updated

Settings-> Update and Security->Check for updates



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 status, indicating the device is up to date. A red box highlights the 'Check for updates' button. Below this, there is a checkbox for 'Check online for updates from Microsoft Update' which is currently unchecked, and a link for '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.

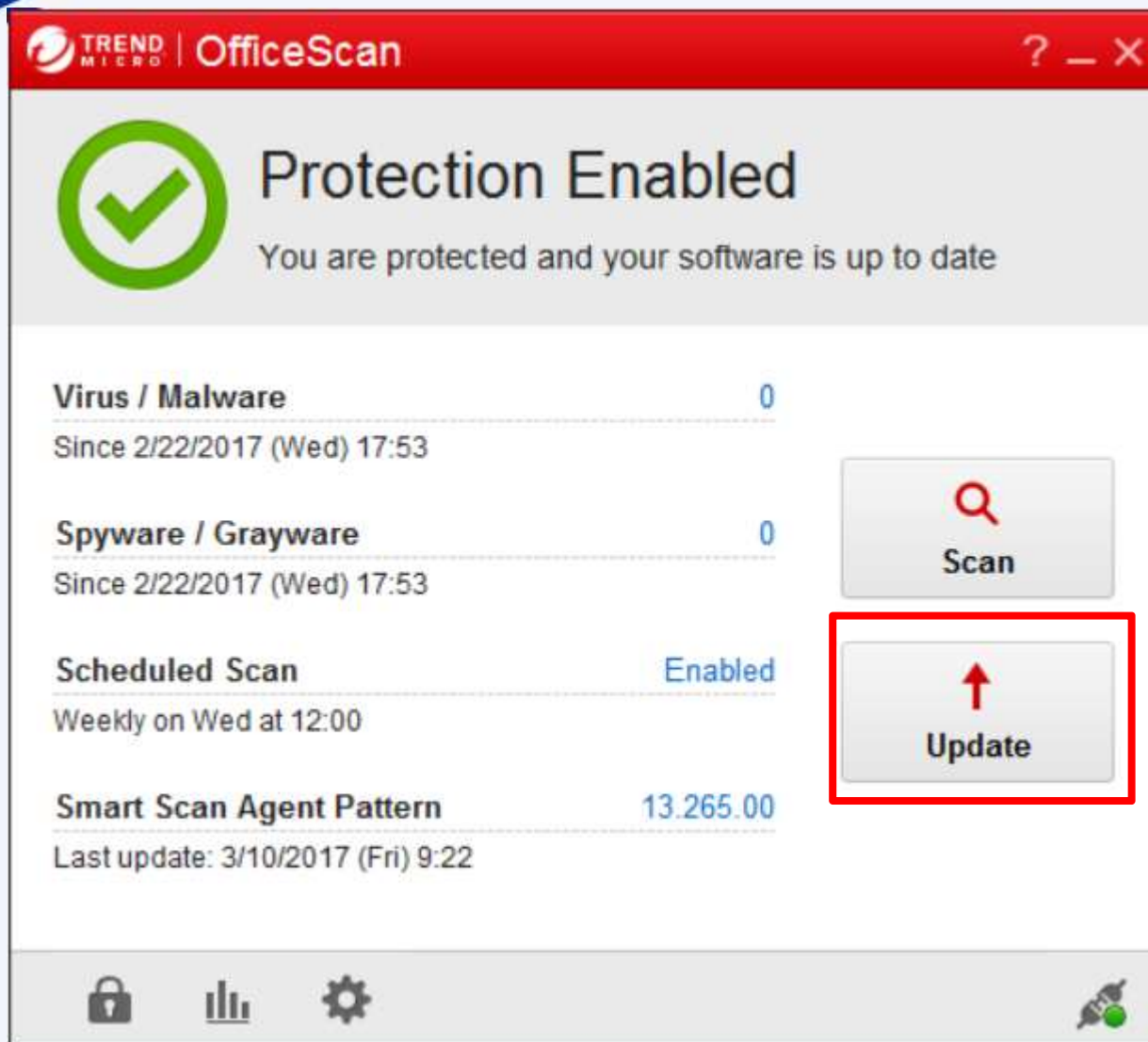
Looking for info on the latest updates?  
[Learn more](#)

Check online for updates from Microsoft Update.


[Advanced options](#)



## Install University Anti Virus Software from Software Centre



**TREND MICRO | OfficeScan** ? \_ X

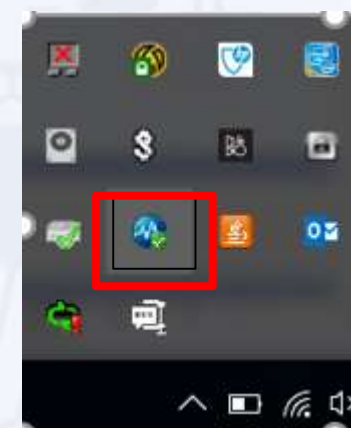
 **Protection Enabled**  
You are protected and your software is up to date

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



**Scan**

**Update**

Navigation icons: Lock, Bar chart, Gear, Refresh



## Trend Micro Office Scan Client Status

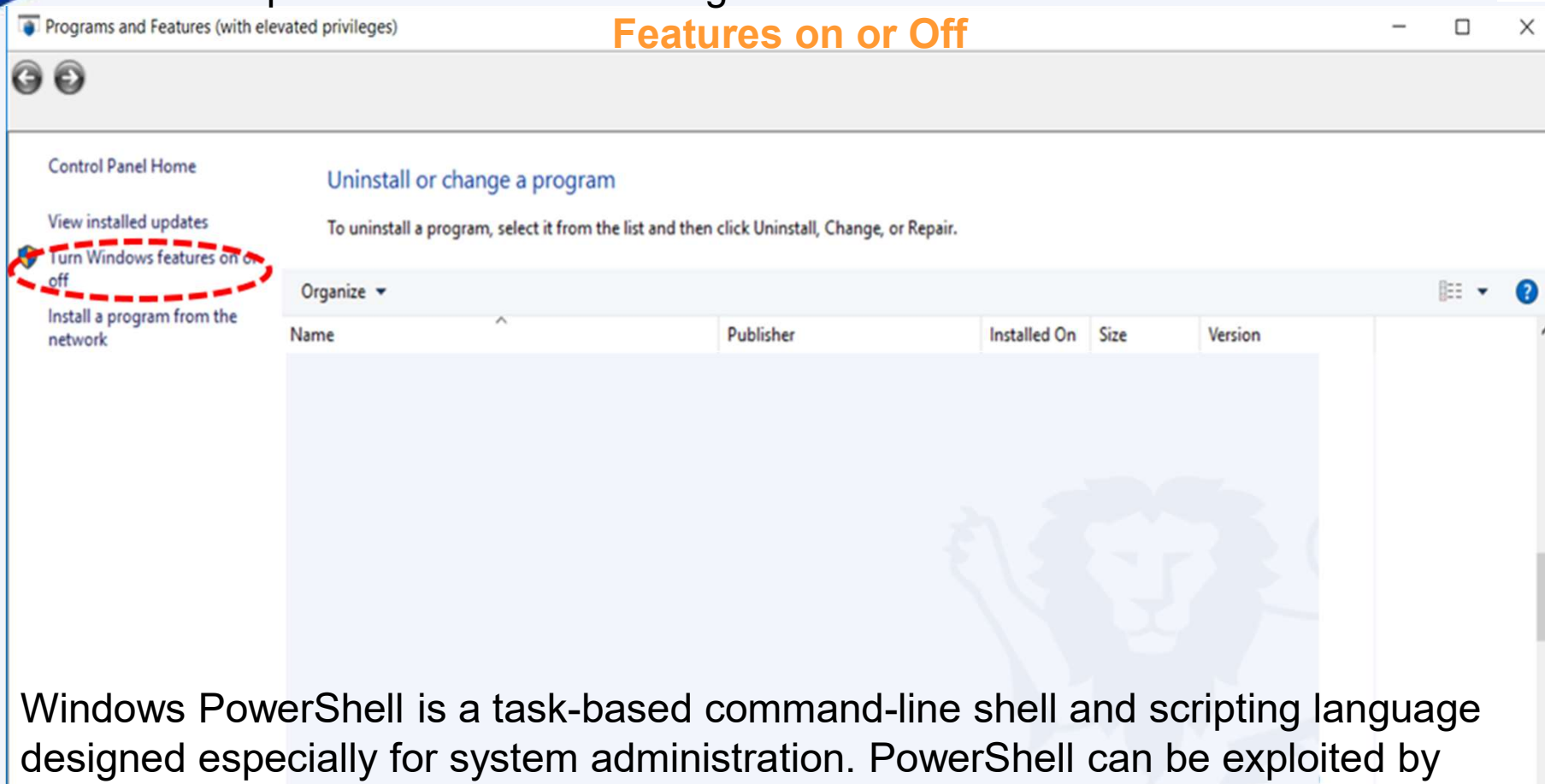
Client Status	Description	Visual Hint
Client connection with the OfficeScan server	Online clients are connected to the OfficeScan server. The server can initiate tasks and deploy settings to these clients	<p>The icon contains a symbol resembling a heartbeat.</p>  <p style="text-align: center;">✓      ✗</p> <p>The background color is a shade of blue or red, depending on the status of the Real-time Scan Service.</p>
	Offline clients are disconnected from the OfficeScan server. The server cannot manage these clients.	<p>The icon contains a symbol resembling the loss of a heartbeat.</p>  <p>The background color is a shade of blue or red, depending on the status of the Real-time Scan Service.</p> <p>It is possible for a client to become offline even if it is connected to the network. For details about this issue, see <a href="#">An OfficeScan Client is Connected to the Network but Appears Offline.</a></p>

[https://docs.trendmicro.com/all/ent/officescan/v10.6/en-us/osce\\_10.6\\_sp1\\_olh/c\\_s\\_connect\\_icons.html](https://docs.trendmicro.com/all/ent/officescan/v10.6/en-us/osce_10.6_sp1_olh/c_s_connect_icons.html)

## Disable PowerShell (1/2)



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



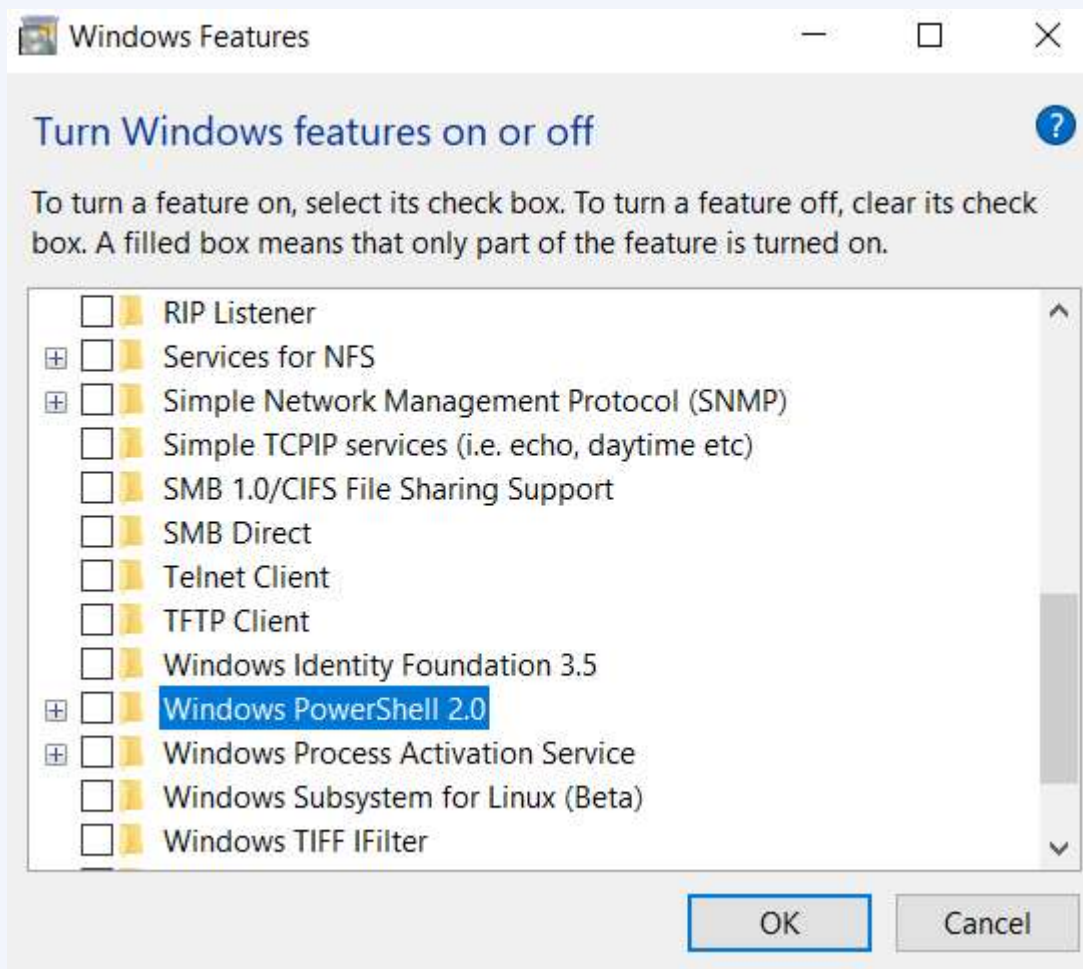
Windows PowerShell is a task-based command-line shell and scripting language designed especially for system administration. PowerShell can be exploited by attackers to execute malicious commands and scripts. Consider disabling PowerShell if it is not required by standard user workstations.

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

## Disable PowerShell (2/2)



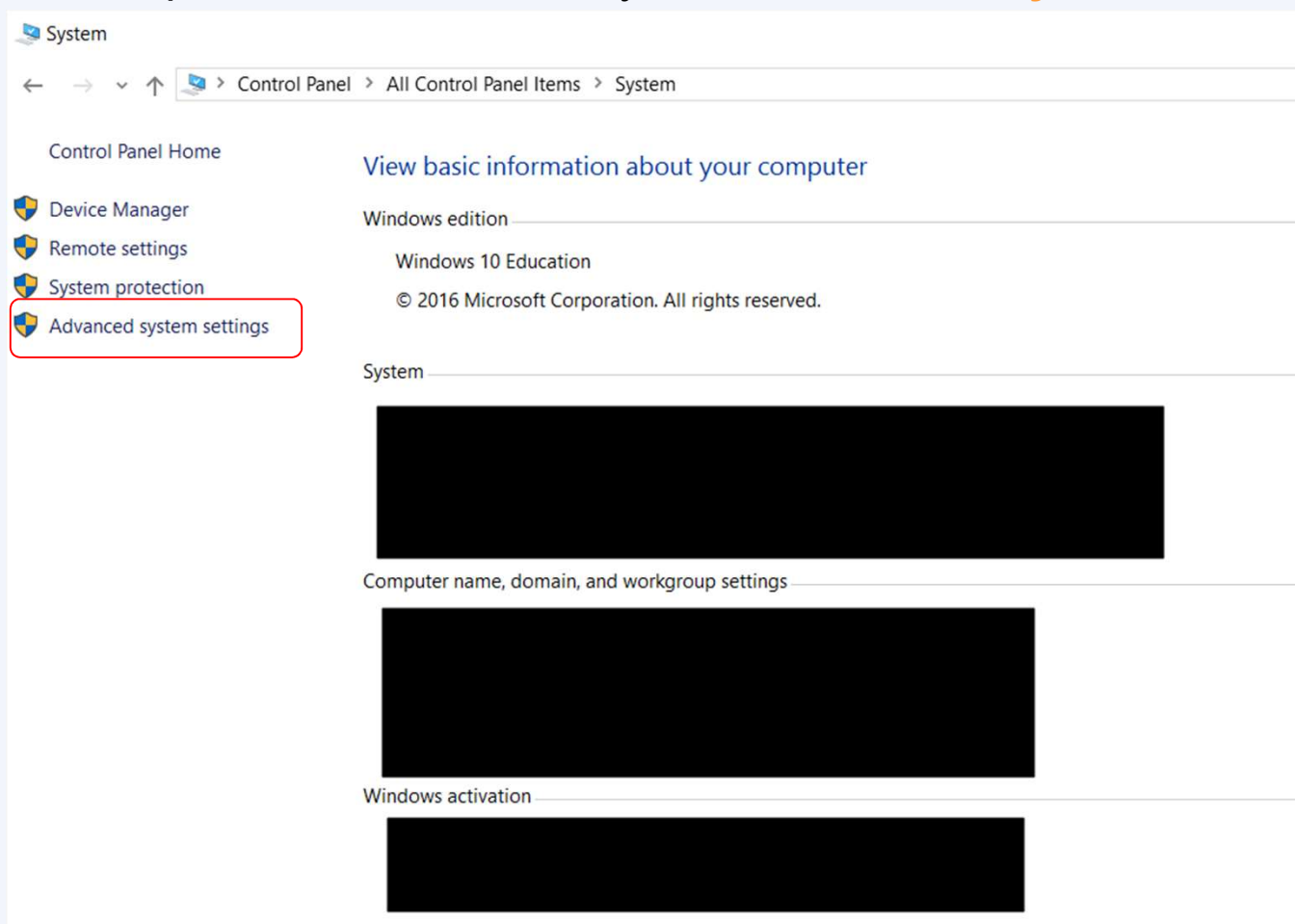
Uncheck Windows PowerShell 2.0 and click Ok



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

# Enable Data Execution Prevention (1/3)

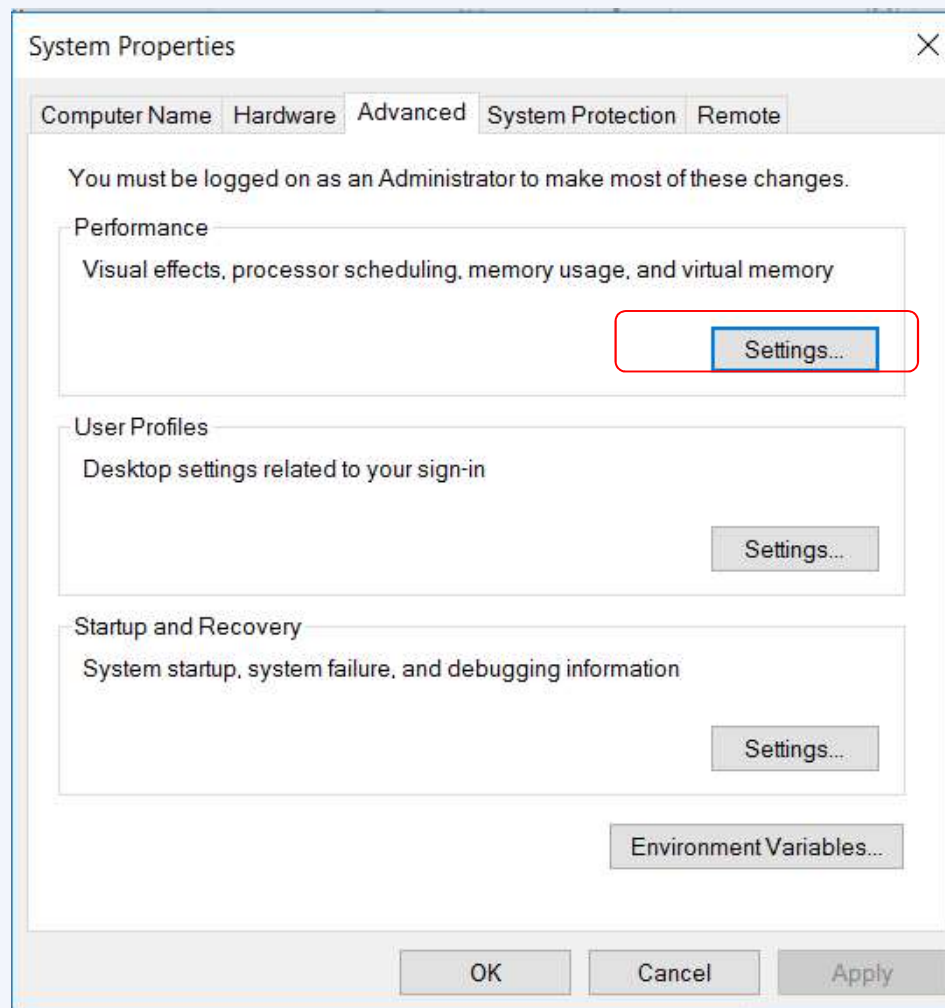
Open Control Panel > System > **Advance System Settings**



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

## Enable Data Execution Prevention (2/3)

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

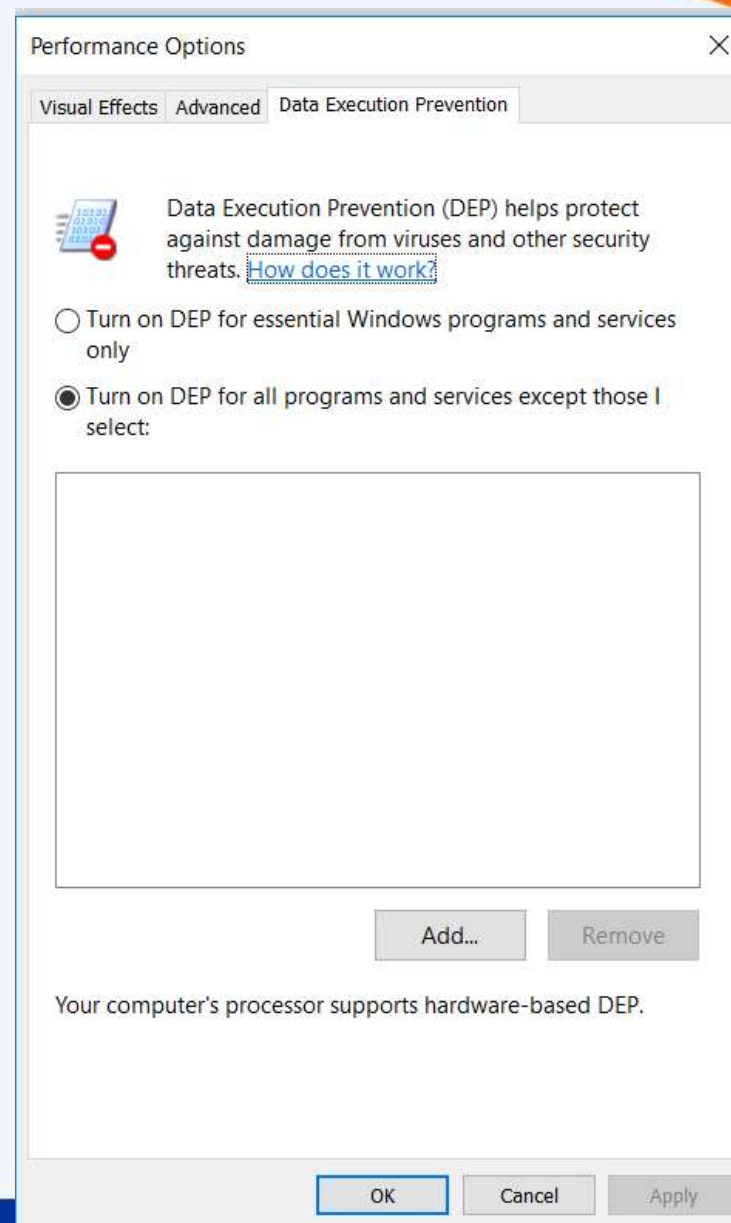


Note: This ensures program are not run on unauthorized memory area

## 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.





# How do I report Suspicious or Phishing Email?

**Answer:**

Report suspicious email using Phishing Reporter Button

Email to [ITCARE@nus.edu.sg](mailto:ITCARE@nus.edu.sg)



or





# What should I do if I fall prey to Phishing email?

## Answer:

- Report phishing using Phishing reporter button
- Inform ITCARE if your account has access to sensitive information or system
- Change password from another machine
- Scan machine with university licensed anti-virus
- Format the machine maybe required in some cases



# How do I know if my machine is compromised?

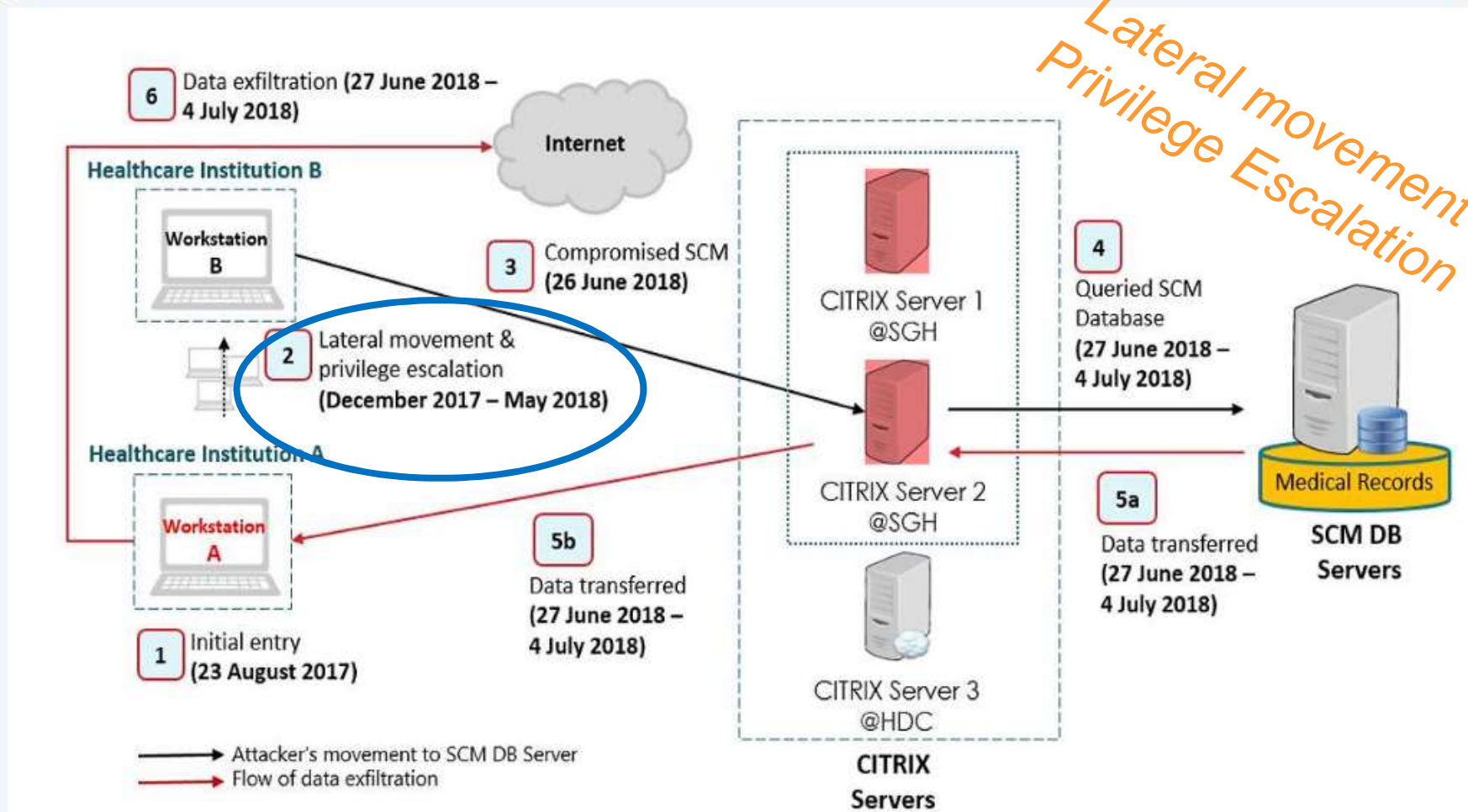
**Answer:**

**For example:**

- **Your computer's local account passwords have been changed**
- **You see new User Accounts added (lusrmgr.msc)**
- **Your friends are reporting strange or spam emails from you**
- **You find new programs or toolbars installed on your computer**
- **Your security or anti-virus software has been disabled**
- **Your Internet searches or home page are redirected**

<https://www.thewindowsclub.com/how-do-i-know-if-computer-hacked/>

# How did the data breach occur?



<https://www.channelnewsasia.com/news/singapore/customised-uniquely-tailored-malware-singhealth-cyberattack-10794852>

## Factors leading to the data breach @ Front End Computer

1

Lateral movement to other machines.

E.g.

- Share Folders
- Remote Desktop Protocol (e.g. RDP)
- Remote Services (e.g. VNC, Telnet, SSH)

2

Privilege Escalation from standard to system/admin account.

E.g.

- Missing patches
- Weak folder permissions settings



## Averting the Data Breach - Apply Security Best Practices

1

Remove open share folders.

<https://nusit.nus.edu.sg/its/resources/tips-to-check-and-remove-insecure-shared-folder-in-windows-pc/>

2

Disable Remote Desktop Connections

<https://www.lifewire.com/disable-windows-remote-desktop-153337/>

3

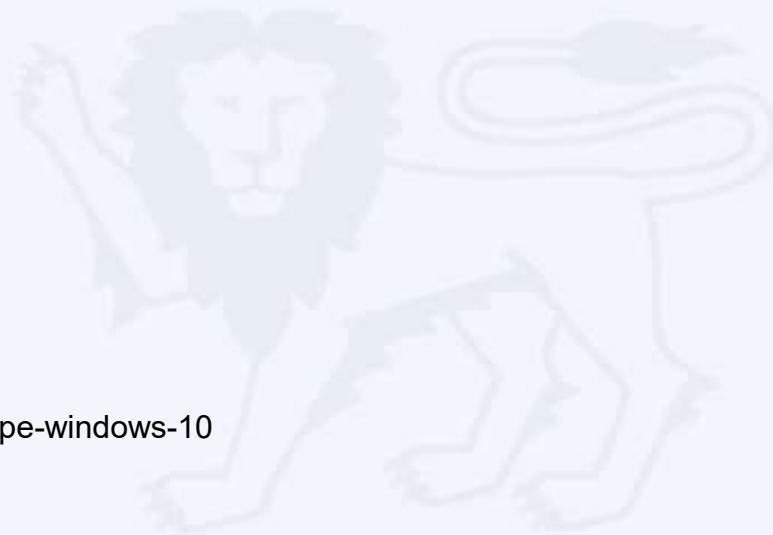
Disable Remote Assistance

<https://www.ricksdailytips.com/disable-remote-assistance/>

4

Use standard account

<https://www.windowcentral.com/how-change-user-account-type-windows-10>





# What is an Open Share folder?

**Answer:**

**Folders with content can be read, update and delete by everyone.**

## What is Open Share Folder?

<https://nusit.nus.edu.sg/its/resources/tips-to-check-and-remove-insecure-shared-folder-in-windows-pc/>

### 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.

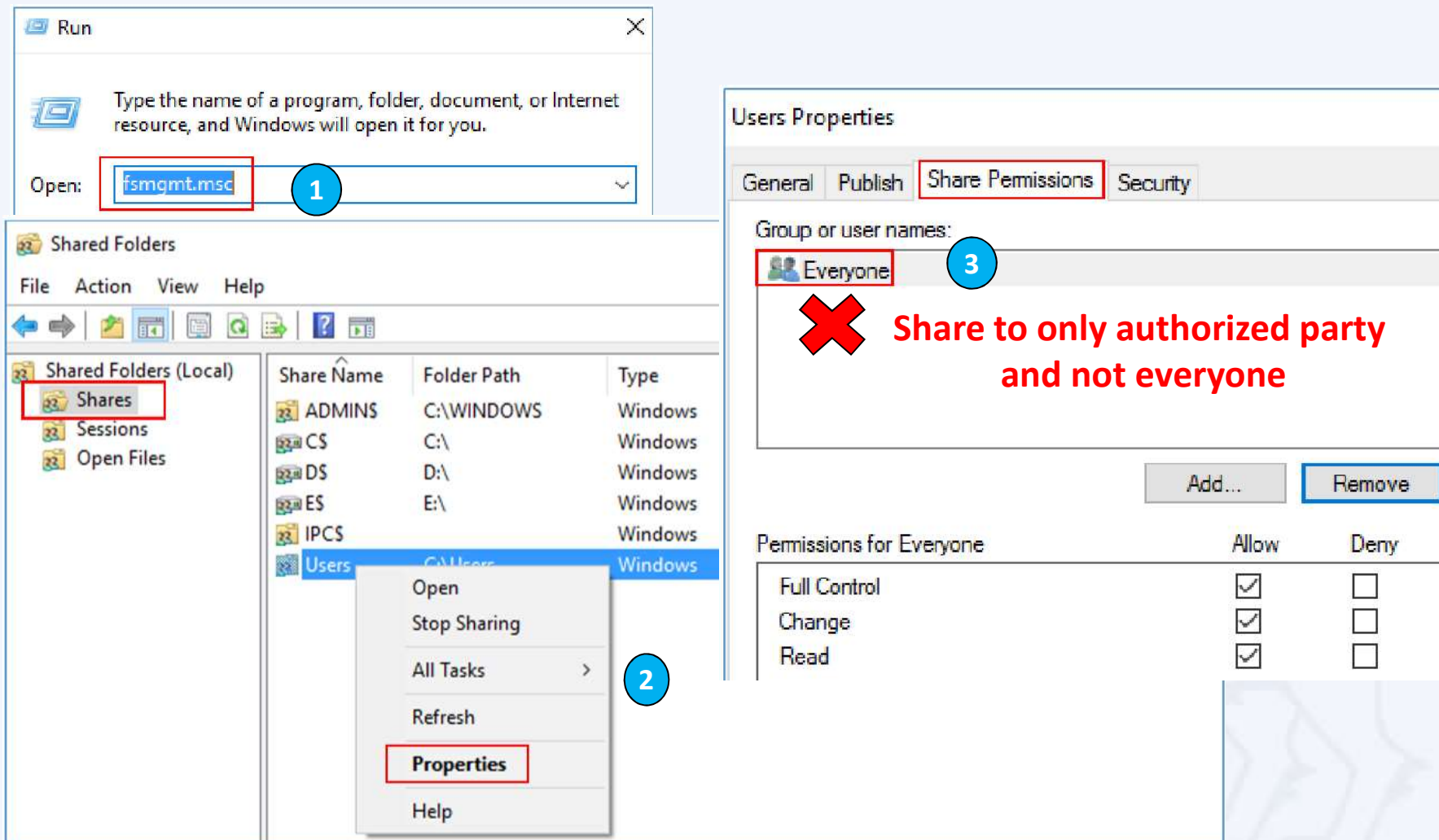
### What is Open Shares

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.

# 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 'Users' share, 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' group in the 'Users Properties' dialog box. A red 'X' is placed over the 'Everyone' group, 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 'Permissions for Everyone' table is visible.

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://nusit.nus.edu.sg/its/resources/tips-to-check-and-remove-insecure-shared-folder-in-windows-pc//>



# 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



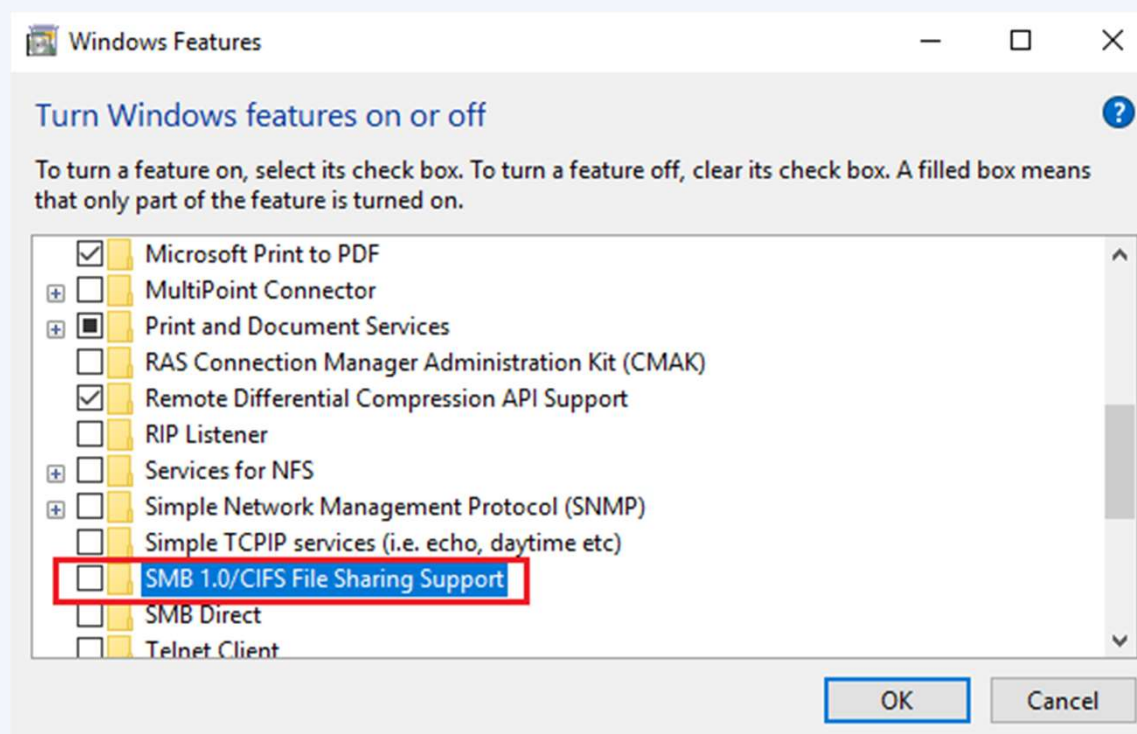
She added that the digital directory service is provided to the mall by a third-party vendor, and that the vendor's system has been disconnected from the board while a software patch is being installed.

"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.

## Disable Deprecated File Sharing Protocol (SMB v1)

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

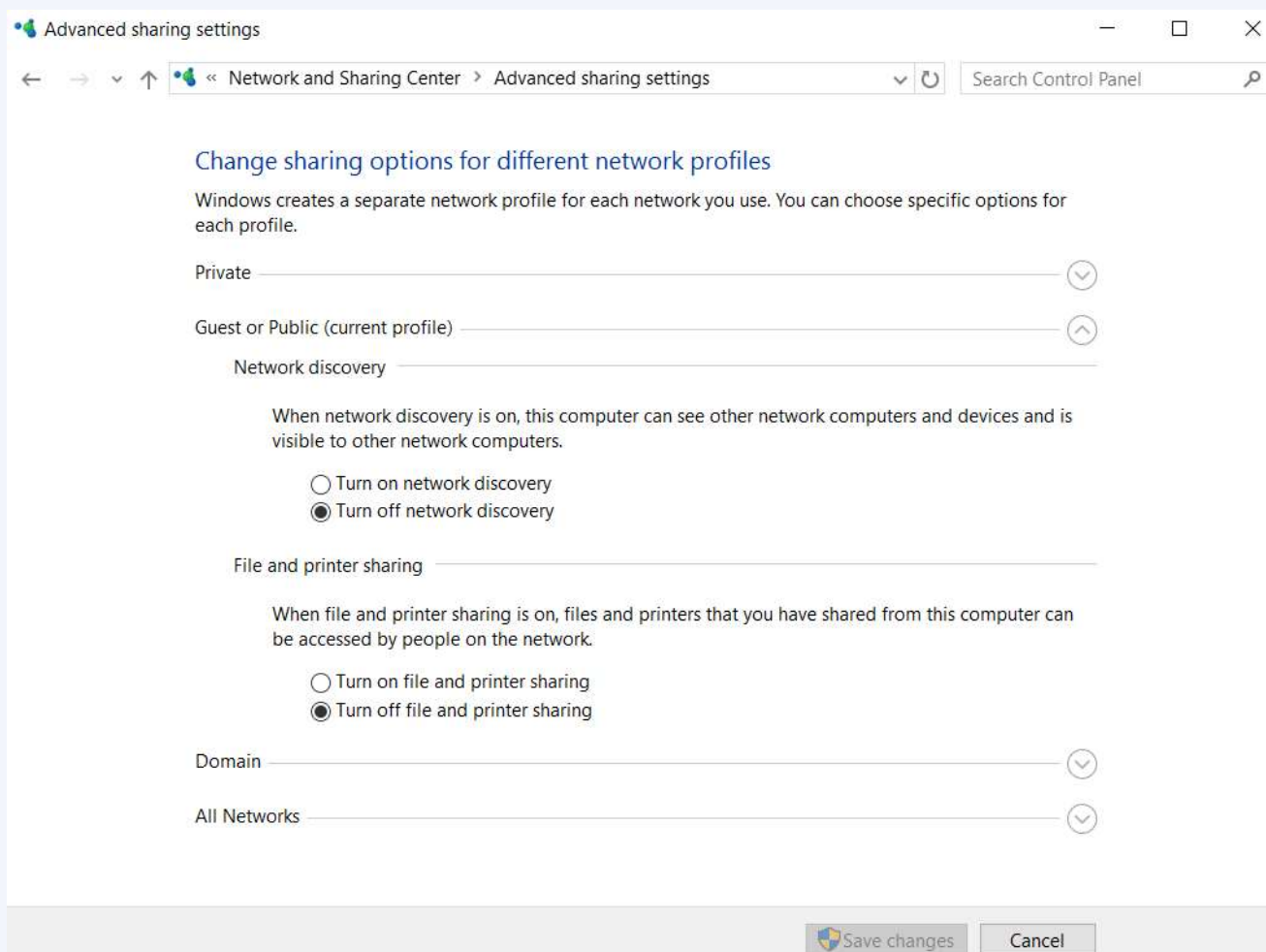


Note: This is an obsolete components for enabling shared access to files and printers and should be disabled.

# Turn off Network Discovery, File and Printer Sharing



Open Control Panel > Network and Internet > **Network and Sharing Centre**



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

## Remote Access Scam (Attack Techniques)

Scammers initiate contact by displaying fake error messages on websites you visit, displaying support numbers and enticing you to call.

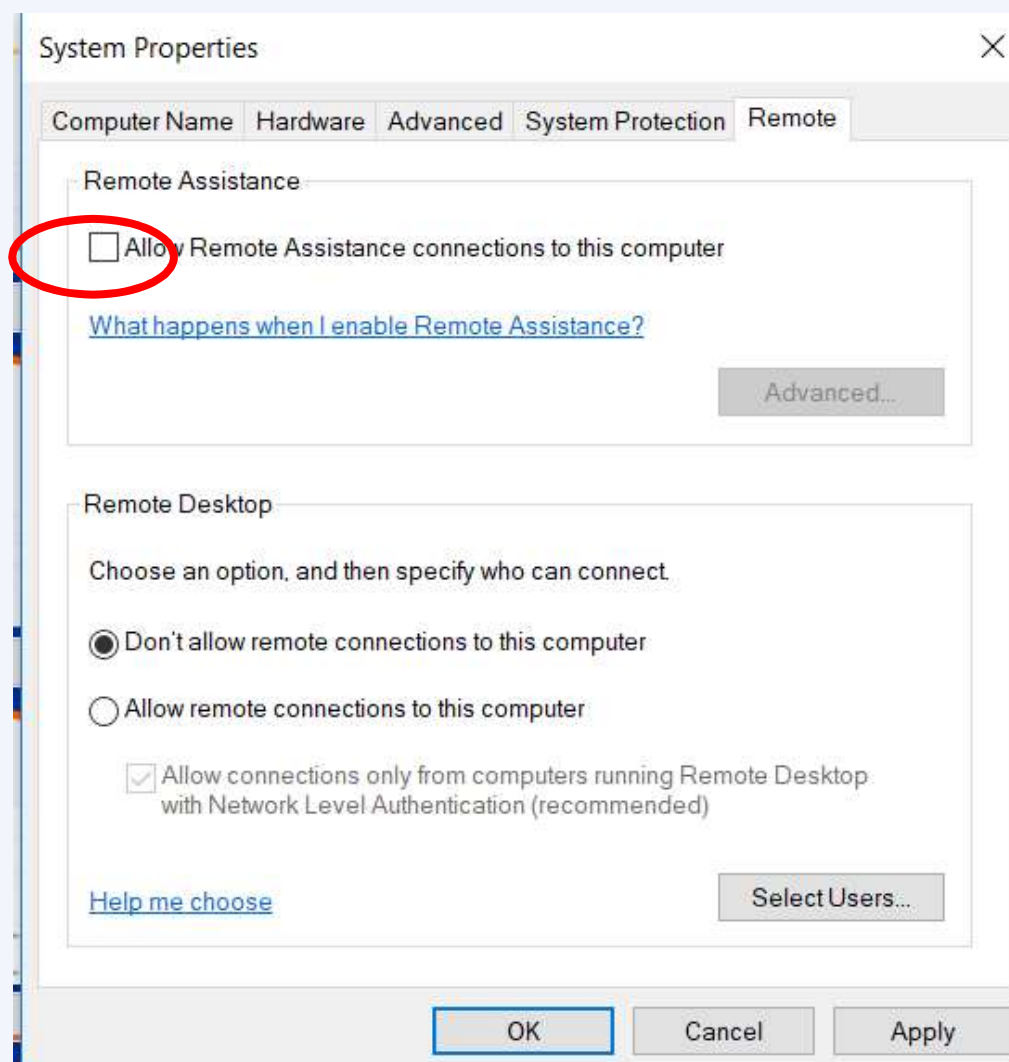
Remote access scams prey on peoples' fear, greed or lack of technological understanding to impair their judgement, making them more likely to commit the grave error of giving a scammer access to their device.



<https://support.microsoft.com/en-sg/help/4013405/windows-protect-from-tech-support-scams>  
<https://www.nextadvisor.com/blog/how-to-avoid-and-recover-from-remote-access-scams/>

## Disable Remote Assistance

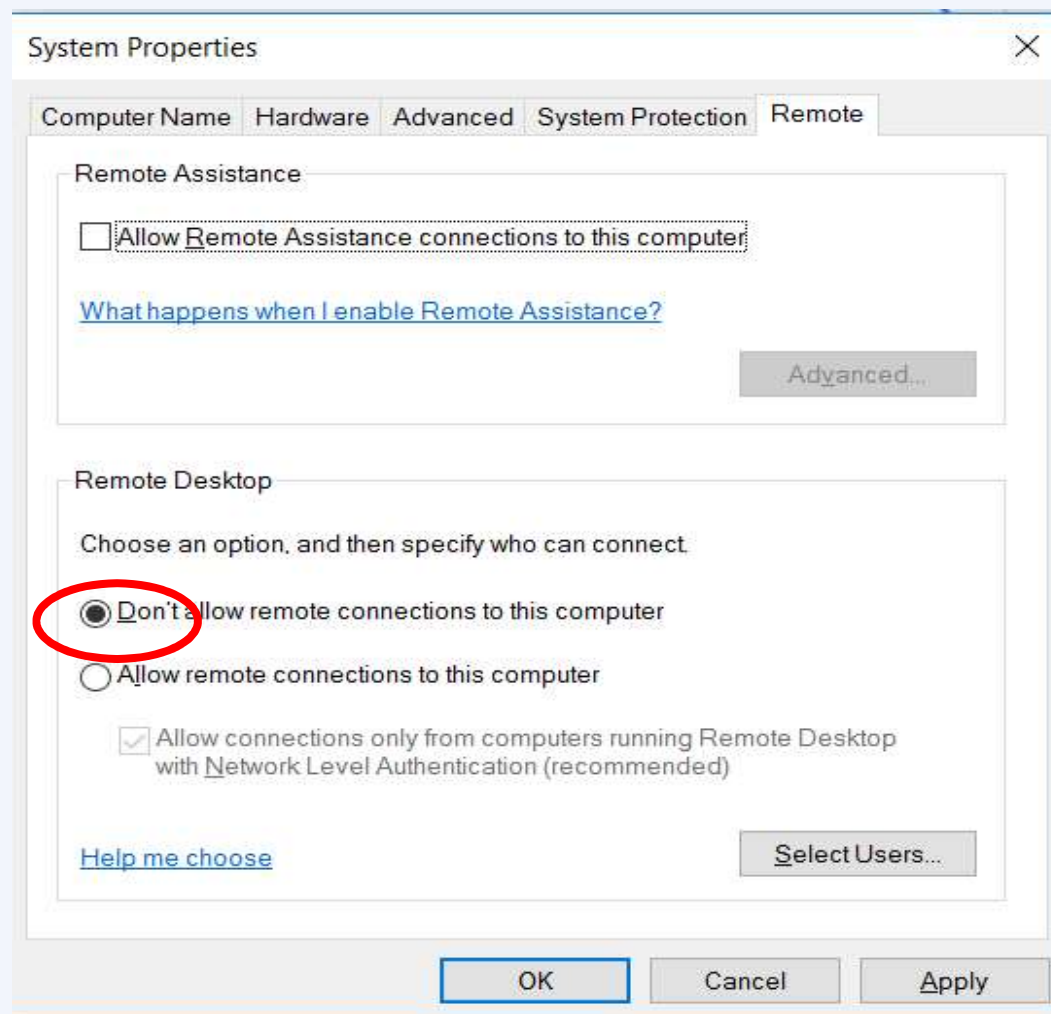
Control Panel->system->Remote Settings



Note: This state disallows someone else to temporarily take control of your PC over the Internet in order to fix a problem for you.

## Turn off Remote Desktop Connection to your PC

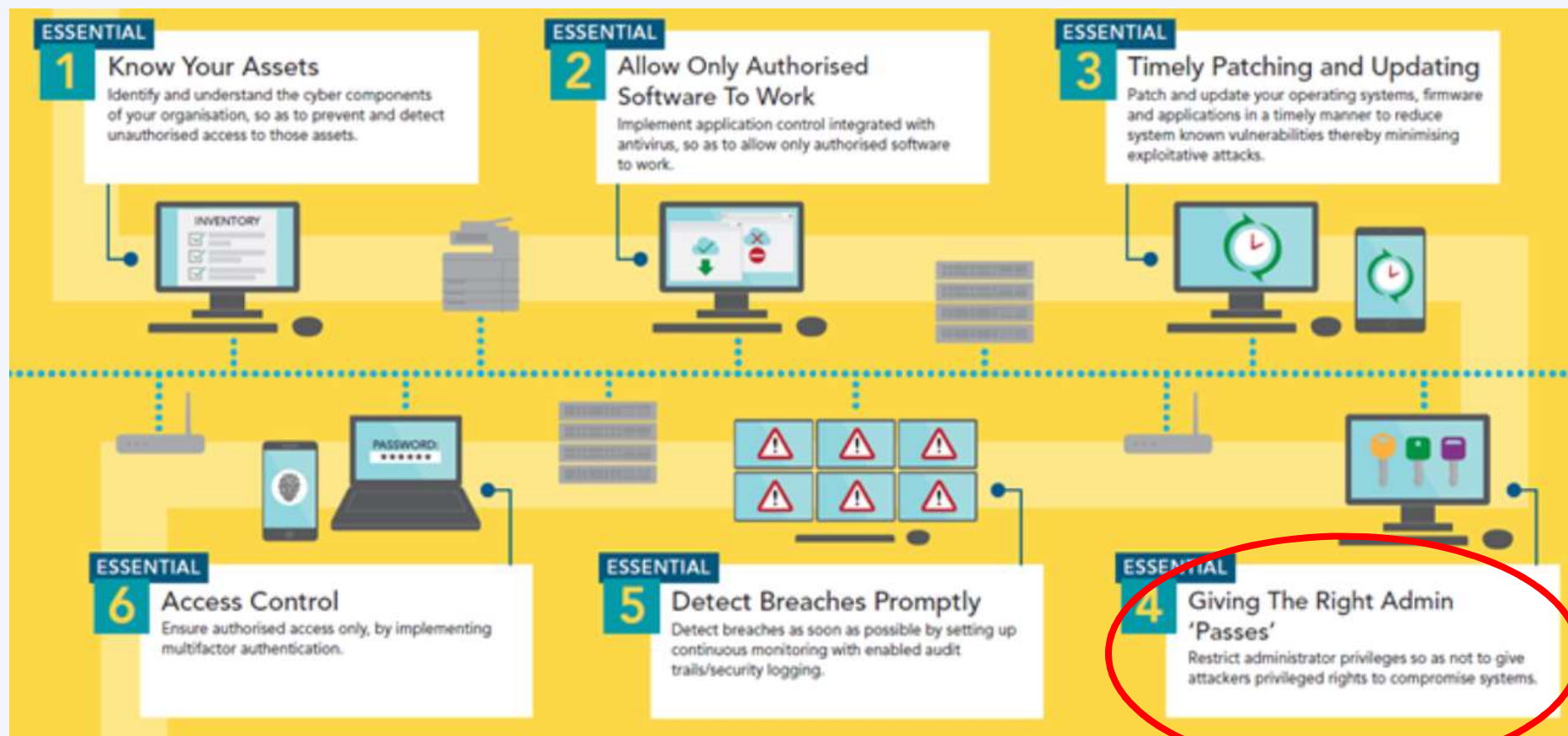
Control Panel->System and Security->System->Remote Settings



Note: This state disallows remote access to your computer.

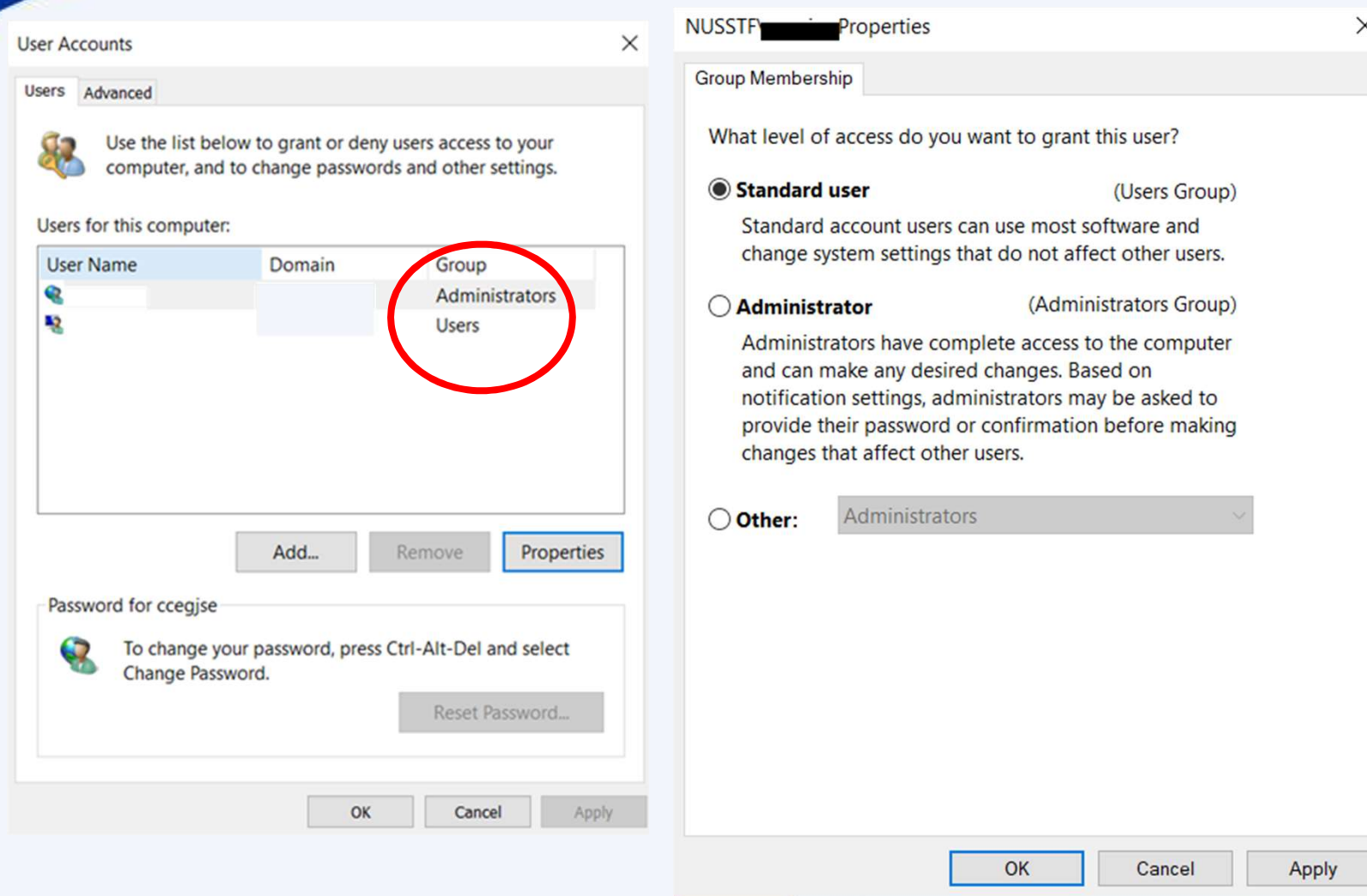
# Six Essential Cyber Defence Measures by CSA

Administrator privileges allow user to do many things such as install software and add new user. Restrict administrator privileges to authorised individuals.



## Use Standard Account

Control Panel->Change Account Type->Properties



The image shows two overlapping Windows dialog boxes. The background window is 'User Accounts' with the 'Advanced' tab selected. It displays a table of users for the computer. The 'Group' column for the selected user is circled in red, showing 'Administrators' and 'Users'. The foreground window is 'NUSSTF Properties' with the 'Group Membership' tab selected. It asks 'What level of access do you want to grant this user?' and has three radio button options: 'Standard user (Users Group)', 'Administrator (Administrators Group)', and 'Other: Administrators'. The 'Standard user' option is selected.

User Name	Domain	Group
		Administrators
		Users

What level of access do you want to grant this user?

- Standard user** (Users Group)  
Standard account users can use most software and change system settings that do not affect other users.
- Administrator** (Administrators Group)  
Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users.
- Other:** Administrators

Note: Users with this type of account can run applications, but they can't install new programs. If a task requires elevations an username and password for an administrator will be needed



## How did the data breach occur?



### THE STRAITS TIMES

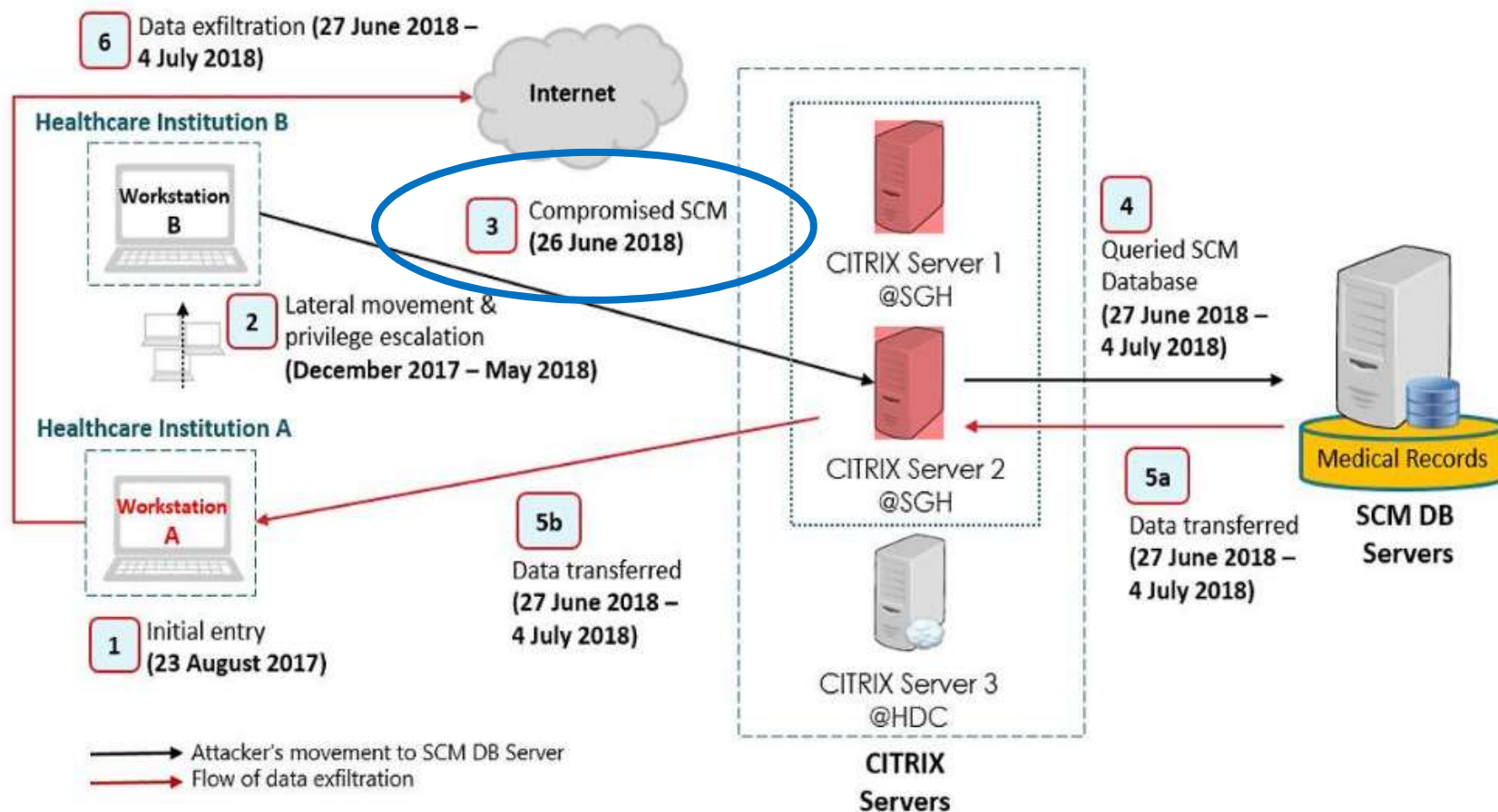
SEP 22, 2018

Solicitor-General cites **weak password**, lack of awareness of how critical the situation was

...one administrator account for the **healthcare group's server** ...had the password, **P@ssw0rd**, and was breached easily, ...

<https://www.straitstimes.com/singapore/tardy-responses-security-failings-led-to-singhealth-breach>

# How did the data breach occur?



<https://www.channelnewsasia.com/news/singapore/customised-uniquely-tailored-malware-singhealth-cyberattack-10794852>

## How did the data breach occur?

# Exploited server had not been updated for more than a year

...the server did in fact have an **older version of an antivirus software installed**

He added that he was **not proficient** in managing the security aspects of servers...

Mr Tan had been **given the password** for the server's local administrator account, **in case his help was needed.**



## How did the data breach occur?

...the attacker exploited an **inactive administrator account** to remotely log into a server containing the EMR records. The **server should have been decommissioned** but was not.

**THE BUSINESS TIMES**

SEP 21, 2018

<https://www.businesstimes.com.sg/government-economy/attack-on-singhealth-network-traced-back-to-aug-2017-coi-hearing>



## Factors leading to the data breach @ Servers

1 Local Administrator account has weak Password (P@ssw0rd)

2 Server had outdated window patches (~14 months)

3 Server had outdated anti-virus (older version)

4 System administrator was not trained

5 System administrator account was no longer required

6 Server should have been decommissioned but was not

## Averting the Data Breach - Apply Security Best Practices

1

Use strong password and 2FA for administrator account

Email to [ITCARE@nus.edu.sg](mailto:ITCARE@nus.edu.sg) for more information. Refer IT Security Policy Chp. 4 Clause 6.3.2.

2

Engage NUS IT to manage your server (includes patch mgmt svc)

Email to [ITCARE@nus.edu.sg](mailto:ITCARE@nus.edu.sg) for more information

3

Get NUS IT anti-virus agent install on your server

Email to [ITCARE@nus.edu.sg](mailto:ITCARE@nus.edu.sg) for more information

4

Refer NUS IT hardening guidelines for securing your server

[https://nusit.nus.edu.sg/its/wp-login.php?redirect\\_to=/its/policies/nus-it-security-policy](https://nusit.nus.edu.sg/its/wp-login.php?redirect_to=/its/policies/nus-it-security-policy)

5

Monitor administrator or privileges account activities. Remove account that is no longer required

Refer IT Security Policy Chp. 4 Clause 4.3.4.

6

Decommission system that is no longer required.



# What is a strong password?

**Answer: Minimum of twelve (12) characters in length; and  
comprised of letters, numbers, and special characters**



# How to decommission a system?



## Decommission System Checklist

<https://ntouch.nus.edu.sg/ux/myitapp/#/catalog/home>

1

### Decommission your server

Select Virtual Machine - Delete

2

### Decommission your IP address

Firewall request – Modify/Delete

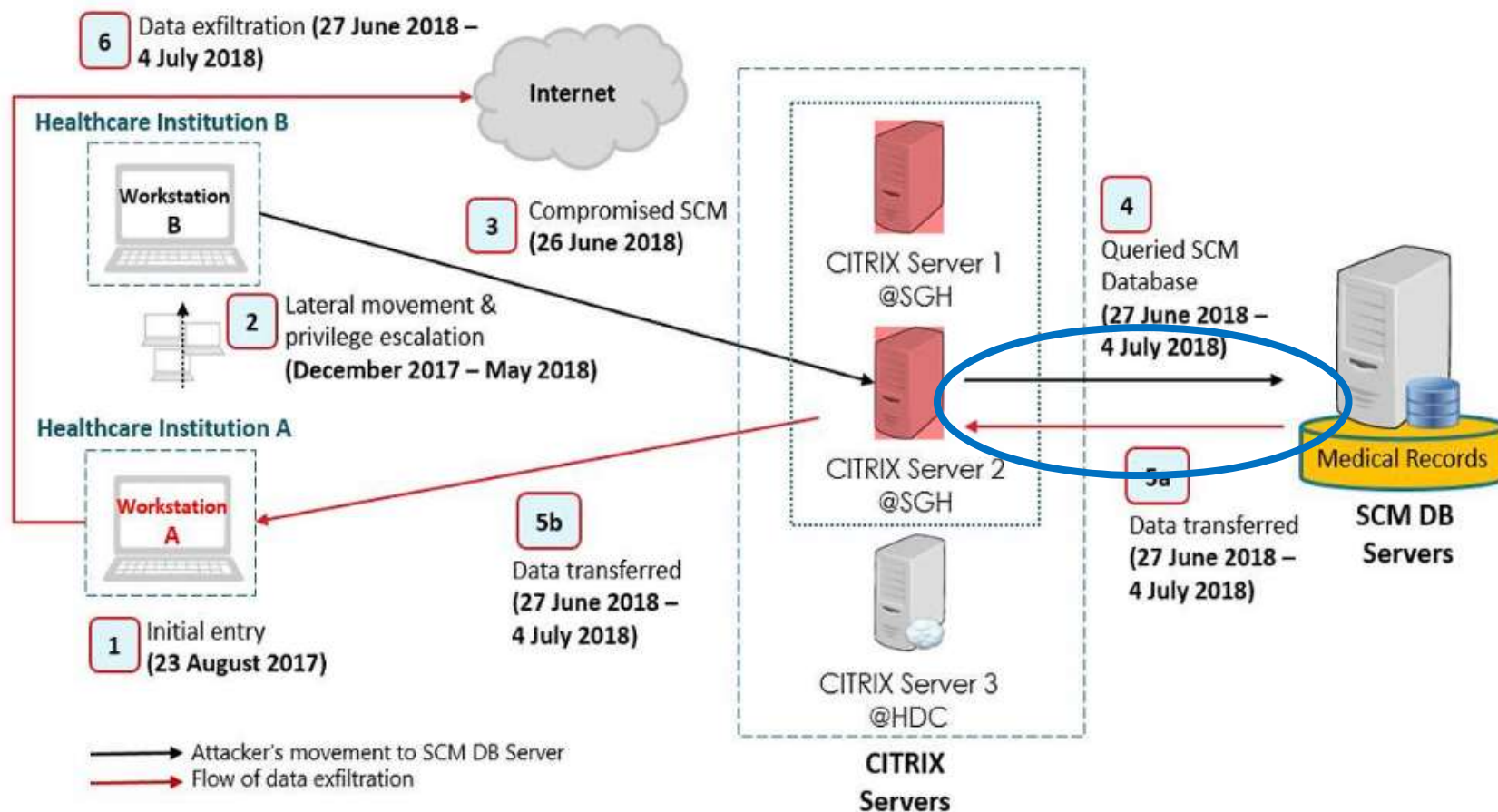
3

### Decommission your domain name

Hostname registration



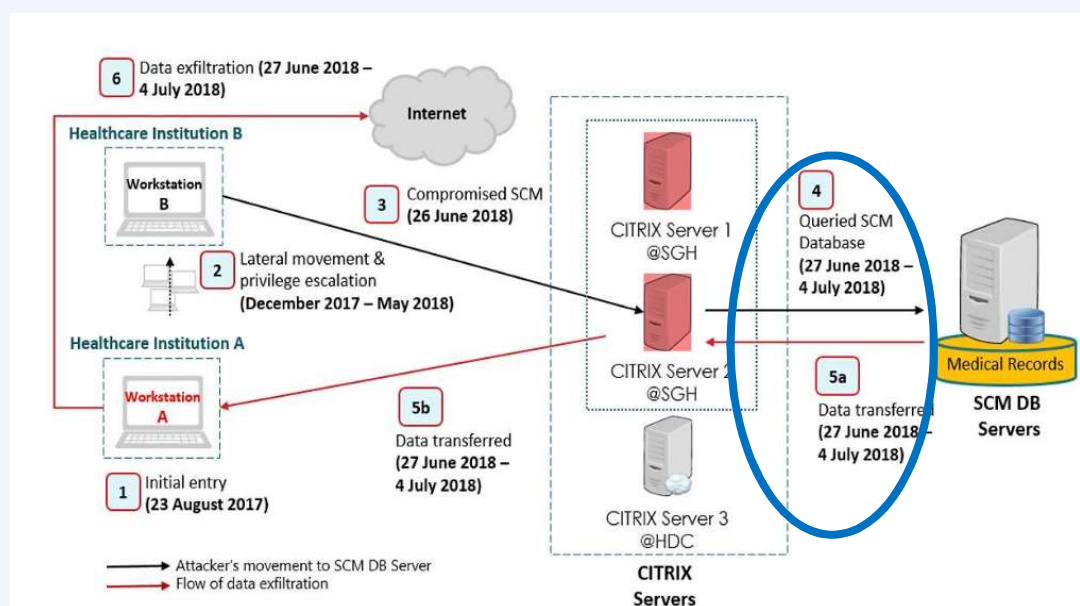
# How did the data breach occur?



<https://www.channelnewsasia.com/news/singapore/customised-uniquely-tailored-malware-singhealth-cyberattack-10794852>

## How did the data breach occur?

The Allscripts SCM software was mentioned as there is evidence there was **“insecure coding vulnerability”** in it and it is **“highly probable”** the vulnerability allowed the attacker to **easily retrieve SCM database credentials** from the Citrix server on H-Cloud, which can then be used to log in to the database.



## Averting the Data Breach - Apply Security Best Practices

1

Get your website application scan for vulnerability before and upon commission or when there are major changes

Email to CCECERT [@nus.edu.sg](mailto:CCECERT@nus.edu.sg) for more information

2

Fix these website application vulnerability on timely basis



## How did the data breach occur?



### THE STRAITSTIMES

SEP 22, 2018

Solicitor-General cites weak password, **lack of awareness of how critical the situation was**

Although IHiS staff detected unauthorised failed attempts to access SingHealth's critical systems as early as June 11 this year, they **did not alert IHiS senior management** until the night of July 9.

**No training or briefing** was provided to me or my team on the IHiS Sirf (Security Incident Reporting Framework)

<https://www.straitstimes.com/singapore/tardy-responses-security-failings-led-to-singhealth-breach>

## How did the data breach occur?

# Team would have 'no day, no night' if I raised alert: Exec

It was his job to sound the alarm on suspicious cyber activities in Singapore's biggest health network - but ...**decided not to, even though the warning signs were there.**

The reason for his reluctance: It would lead to more work for him and his team and pressure from his bosses, ...claim that he and his team members would have "**no day, no night**".

<https://www.straitstimes.com/singapore/team-would-have-no-day-no-night-if-i-raised-alert-exec>

**THE STRAITSTIMES** NOV 1, 2018

## Averting the Data Breach - Apply Security Best Practices

1

Report suspicious activities or incidents immediately

Email to CECERT [@nus.edu.sg](mailto:CCECERT@nus.edu.sg) for more information

2

Keep management inform on security events and incidents

Email to CECERT [@nus.edu.sg](mailto:CCECERT@nus.edu.sg) for more information

3

Be aware of what is an incident and how to report one

Email to CECERT [@nus.edu.sg](mailto:CCECERT@nus.edu.sg) for more information



# Identify and Report Security Incidents



***Security is  
lifestyle!***

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



## Examples of Security Incidents Relating to Staff/Students

- 1 Unauthorized use of your accounts (e.g. emails access or sent without your knowledge).
- 2 Receive or Fell prey to Phishing or suspicious emails (e.g. you received or responded to email requesting for your account information).
- 3 Lost or stolen mobile devices or portable storage containing University data (especially if it contains personal data)



# Will my emails get downloaded when I access email from my mobile?

**Answer: Yes**

<https://www.howtogeek.com/99423/email-whats-the-difference-in-pop3-imap-and-exchange/>

## Examples of Security Incidents Relating to Staff/Students

- 4 Incorrectly sent email which contains NUS confidential or personal data.
- 5 NUS confidential or personal data exposed on public website.
- 6 Knowledge or discovery of any vulnerabilities in NUS systems or applications

# 143 NUS student volunteers' data breached; school directed to provide mandatory training



The commission found that a URL link for a Google Sheets spreadsheet, started by students from NUS College of Alice and Peter Tan, had disclosed personal data of students without authorization.

It contained the full names, mobile numbers, matriculation numbers, shirt sizes, dietary preferences, dates of birth, dormitory room numbers and email addresses of the student volunteers ...

<https://www.straitstimes.com/singapore/143-nus-student-volunteers-data-breached-school-directed-to-provide-mandatory-training>

**THE STRAITSTIMES** APR 28, 2017

# Singapore Airlines data breach affects 285 accounts, exposes travel details



The "software bug" surfaced after changes were made to the Singapore carrier's website on January 4 and enabled some of its [Krisflyer members to view information belonging to other travellers](#), SIA told ZDNet in an email.

<https://www.zdnet.com/article/singapore-airlines-data-breach-affects-284-accounts-exposes-travel-details/>



JAN 5, 2019

## Examples of Security Incidents Relating to System Administrators

1

Unauthorized logins to system, including successful and persistent failed logins.

2

Unauthorized use of system for processing or storing of data (e.g. upload unintended files to website).

3

Changes to system without instruction, or consent, say evident changes on system hardware, firmware, or software functionality, configuration, logs or data (e.g. web page defacement).

4

Unwanted disruption of service (e.g. unusually high volume of request for e-services).

## How to Report Security Incident?

1

How and When did the incident occur?

2

Who reported the incident?

3

How was the incident discovered?

4

What were the targeted systems or accounts details?  
e.g. userID, ip address, MAC address, URL

5

Was there any data loss or leakage? If so, please elaborate the data classification and description.

6

Was there any follow up actions taken and possible impacts to the university?

## How to Report Security Incident?

For unauthorized used of email and phishing related incidents

- 1 Email to NUS IT CARE at [itcare@nus.edu.sg](mailto:itcare@nus.edu.sg)
- 2 Contact NUS IT CARE at 6516-2080.

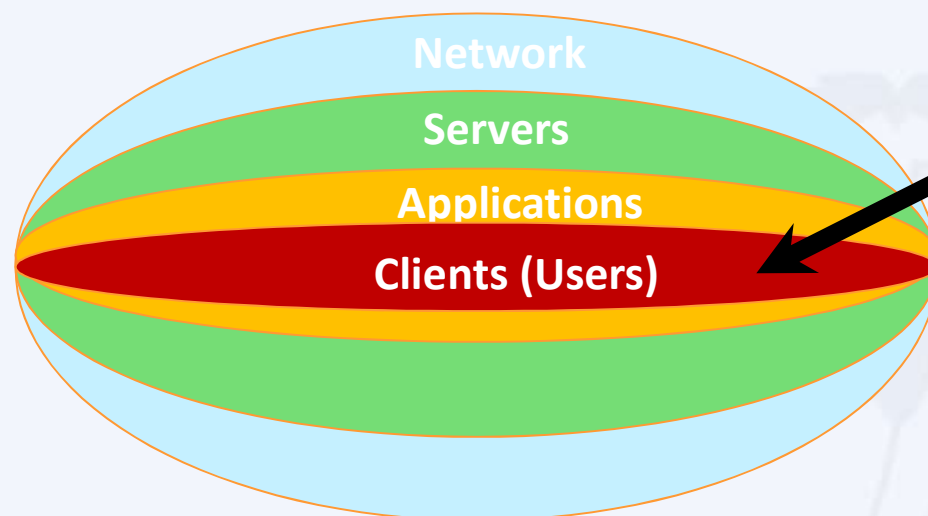
For any other system related incidents

- 3 Use online security incident reporting form  
<https://nusit.nus.edu.sg/its/cceforms/i-want-to/report-an-incident/>
- 4 Email to [CCECERT@nus.edu.sg](mailto:CCECERT@nus.edu.sg)

NUS Restricted



# Cyber Attacks Techniques: Phishing, Smishing, Vishing, USB Drop Attack & Malware



## What is Phishing Email?

Email sent by attackers, often using spoofed email account,

Or pretending to be someone you know with aim to:

- **Steal your user credentials** so that they can gain access to your device 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.
- **Open attachments** that can infect your computer with malware.

## Sample Phishing Email Reported By Staff



Fri 23/2/2018 11:39 PM

**New Payroll Notification.**

To



You forwarded this message on 26/2/2018 2:29 PM.

You Have 1 New Notification Re <https://sporkulis.com/wp.php/roll>.

**Click or tap to follow link.**

[www.nus.edu.sg/payroll/calendar](http://www.nus.edu.sg/payroll/calendar)

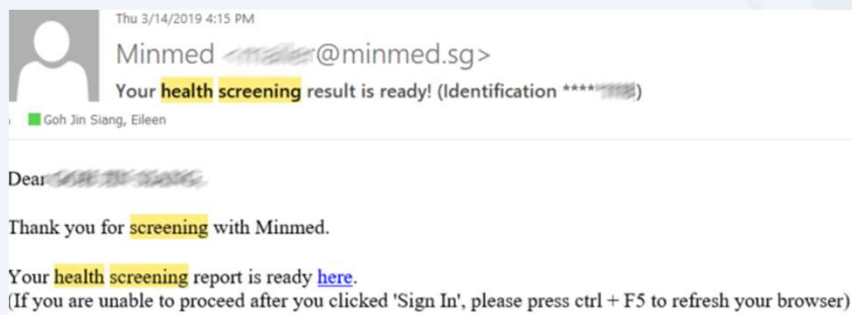
National University of Singapore | Payroll Services.

<https://nusit.nus.edu.sg/its/resources/scenariophishing-drill/phish-bowl/>



# Can official email have non-NUS URL?

**Answer: Yes**



## Sample Phishing Email Reported By Staff


Mon 4/6/2018 9:15 AM



Annette Gruber <info@sabai-sabai-sukhumvit.com>

Fwd: Doc-2018-0604

To

 We removed extra line breaks from this message.



We have received your letter headed authorization to process pending payment to another bank....



Hello,

We received your letter headed authorization to process your pending payments to another bank account as shown in the attached excel file; all bearing your details. Kindly confirm if this request was made by you so we can proceed accordingly.

Sincerely,  
Annette Gruber  
Accounting Department

---  
SABAI-SABAI-SUKHUMVIT  
984/22-27 Soi Pridi Banomyong 40, Sukhumvit 71 Rd., Prakanong, Wattana, Bangkok 10110 Thailand.  
tel: +66-89-2102320  
fax: +66-89-21949408  
mail: [info@sabai-sabai-sukhumvit.com](mailto:info@sabai-sabai-sukhumvit.com)  
web: [www.sabai-sabai-sukhumvit.com](http://www.sabai-sabai-sukhumvit.com)

<https://nusit.nus.edu.sg/its/resources/scenariophishing-drill/phish-bowl/>

## Cyber Attackers Vectors

Attackers can utilize

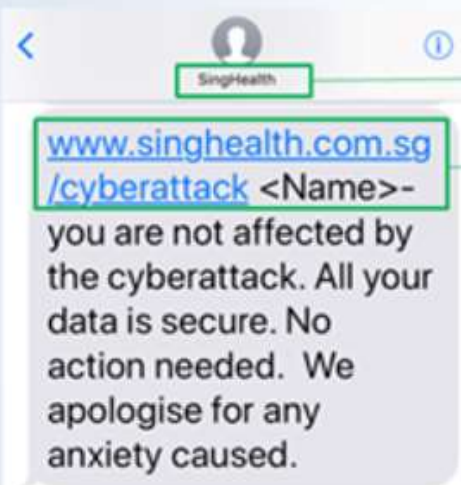
- **Phishing:** Email
- **Smishing:** SMS, WhatsApp, Social Media
- **Vishing:** Phone Calls
- **Others:** USB



## “Phishing” via SMS (Smishing)

# 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:



- 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.”

## “Phishing” via Phone Calls (Vishing) 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.

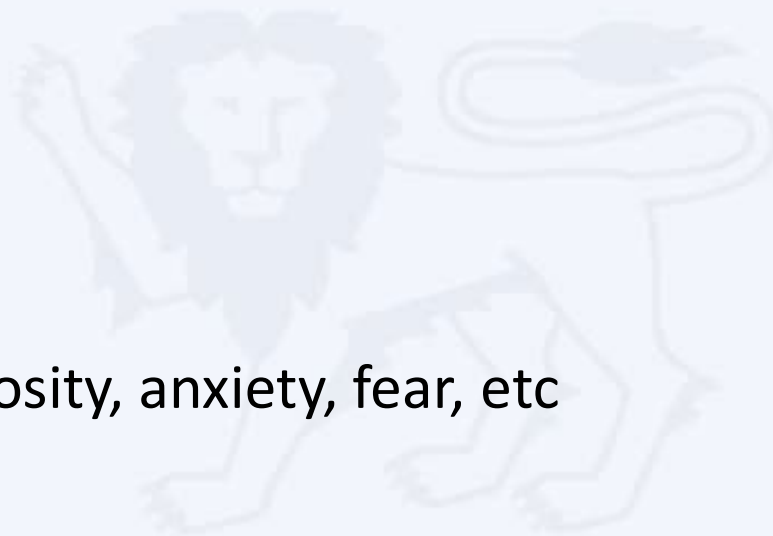
<https://www.channelnewsasia.com/news/singapore/singapore-airlines-warns-of-phishing-scams-offering-free-air-9513474>



## Attackers Techniques

Attackers can:

- Spoof Email and Phone Numbers
- Fake News and Website.
- Use Familiar Email Subject
- Adopt Emotive such as greed, curiosity, anxiety, fear, etc



## Phishing email getting more sophisticated

# DBS warns of phishing site targeting bank customers

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

From : [customerservice@posbbank.com.sg](mailto: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 <https://virutallin.gq/secure/update/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](http://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 [www.posb.com.sg/secure/update](http://www.posb.com.sg/secure/update) 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.

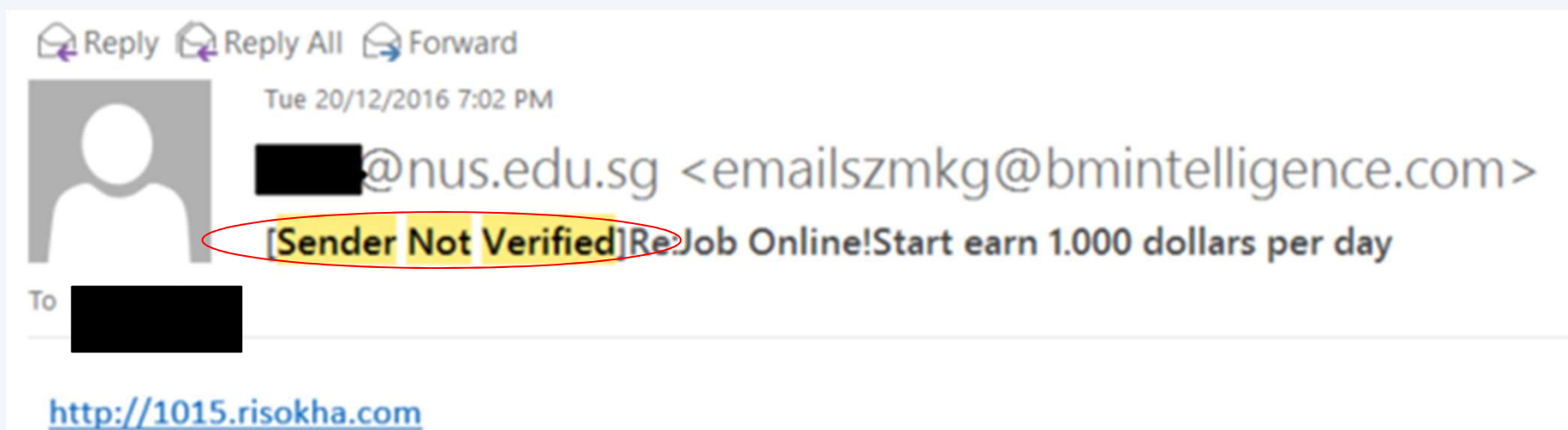




# How to identify a spoofed email address?



## How to Identify Spoofed Email?



# How to Identify Spoofed Email?

Mon 16/11/2017 8:07 AM  
 Computer Centre  
 Security Advisory on Phishing Email with Malicious Attachment  
 To: NUS staff  
 Signed By: computercentre@nus.edu.sg

## SECURITY ADVISORY NUS COMPUTER CENTRE

Dear Colleagues,

### Phishing Email with Malicious Attachment

Millions of people use email every day to send files from computer to computer. Opening unverified file attachments can be dangerous. Phishers used email to send malicious file attachment disguised as spreadsheet, document or even funny pictures.

**What risk does the attachment posed?**

The attachments contain malicious code that runs on your computer and do undesirable things such as stealing your information and installing ransomware.

**How do I identify malicious attachments?**

These attachments are typically from unknown or suspicious sender. The email body often contain statements to induce recipients to open the



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.

[Details...](#)

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

[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...

Paste   Copy   Cut   Format Painter   Clipboard

**B I U**   **A**   Address Book   Check Names   Attach File   Attach Signature Item

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

To:

Cc:

Subject:

Send

## How to Identify Spoofed Email?

- 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 email account & subject?

**Answer:**

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

\*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](mailto: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)



## Phishing Email from Legitimate Account & Familiar Subject

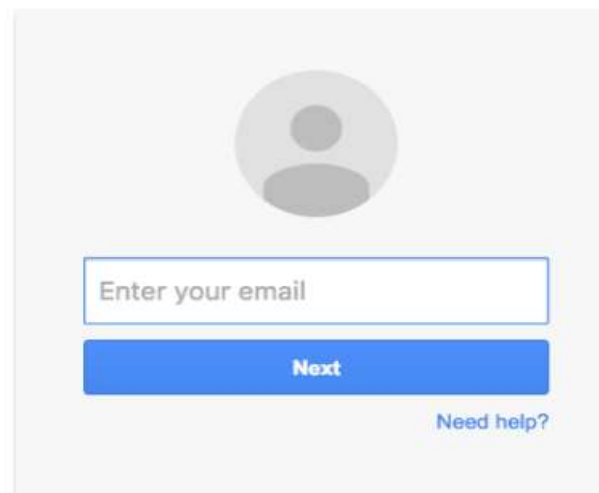
<https://www.wordfence.com/blog/2017/01/gmail-phishing-data-uri/>

# 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

One account. All of Google.

Sign in to continue to Gmail



A screenshot of a Gmail sign-in page. At the top, it says "One account. All of Google." followed by "Sign in to continue to Gmail". Below this is a grey box containing a circular profile picture placeholder, a text input field with the placeholder text "Enter your email", a blue "Next" button, and a "Need help?" link.

## Look Out for Scam Emails

**From:** [REDACTED]@gmail.com>  
**Sent:** 09 January 2019 13:11  
**To:** [REDACTED]  
**Subject:** Re:

Ok, The amount i want is \$100 each in three (3) piece so that will make it a total of \$300 I'll be reimbursing back to you. i need physical cards which you are going to get from the store. When you get them, just scratch it and take a picture of them and attach it to the email then send it to me here ok

On Wednesday, January 9, 2019, [REDACTED]@nus.edu.sg> wrote:

Dear [REDACTED]  
I am in office.

**From:** [REDACTED]@gmail.com>  
**Sent:** Wednesday, 9 January 2019 1:25 PM  
**To:** [REDACTED]@nus.edu.sg>  
**Subject:**

Are you available?



# How to verify if a Website is malicious?



## How to identify fake or malicious website?

<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!

## How to identify fake or malicious website?

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



[Home](#) [Add A Phish](#) [Verify A Phish](#) [Phish Search](#) [Stats](#) [FAQ](#) [Developers](#) [Mailing Lists](#) [My Account](#)

### 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
<a href="#">5019815</a>	<a href="https://paypal-limited-balance.gq">https://paypal-limited-balance.gq</a>	<a href="#">PhishReporter</a>
<a href="#">5019812</a>	<a href="https://node-324-microsoft-ssrv-live.gsrv.site/hot...">https://node-324-microsoft-ssrv-live.gsrv.site/hot...</a>	<a href="#">Hack</a>
<a href="#">5019810</a>	<a href="http://www.mkphoto.by/olb/1/sucursalpersonas.trans...">http://www.mkphoto.by/olb/1/sucursalpersonas.trans...</a>	<a href="#">dms</a>

## How to identify fake or malicious website?

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



Safe Web

English >

Help >

Sign In >

Home

About

Safety & Threats

Community Buzz

Look up a site. Get our rating.



## How to identify fake or malicious website?

<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 to Identify Fake or Malicious Website?



- 1 Enter the known website directly from your browser
- 2 Mouse over the the URL. Is it familiar? e.g. NUS domain (nus.edu.sg)

subdomain e.g. organization      directory

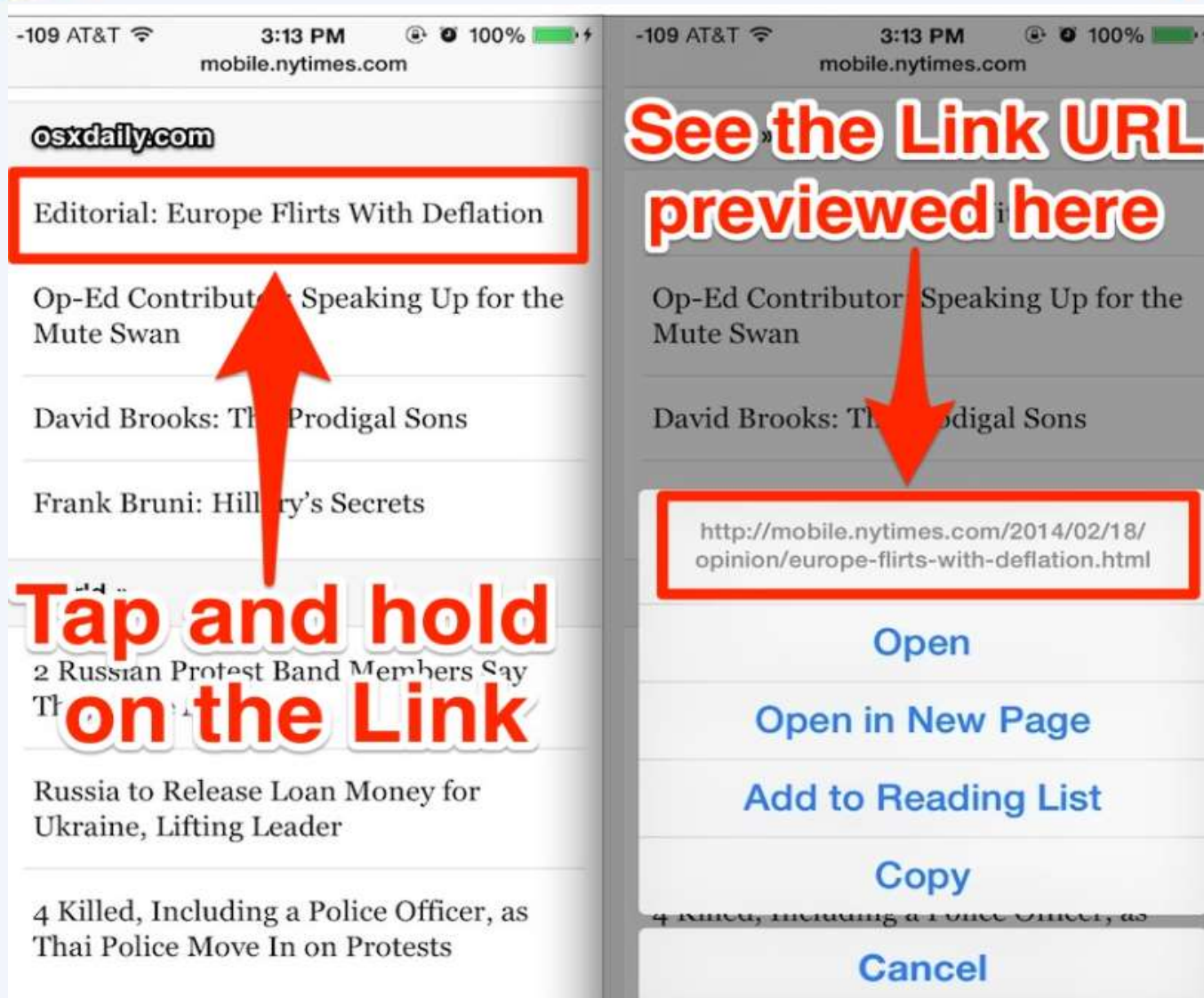
http://pages.example.com/archive/index.html

protocol      domain e.g. industry or country      filename

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



## How to identify fake or malicious website?



**See the Link URL previewed here**

**Tap and hold on the Link**

Editorial: Europe Flirts With Deflation

Op-Ed Contributor Speaking Up for the Mute Swan

David Brooks: The Prodigal Sons

Frank Bruni: Hillary's Secrets

2 Russian Protest Band Members Say They...

Russia to Release Loan Money for Ukraine, Lifting Leader

4 Killed, Including a Police Officer, as Thai Police Move In on Protests

<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/>



# How do I know if my account is being stolen?

Answer: Check out [haveibeenpwned.com](http://haveibeenpwned.com) or [pastebin.com](http://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.**





# 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



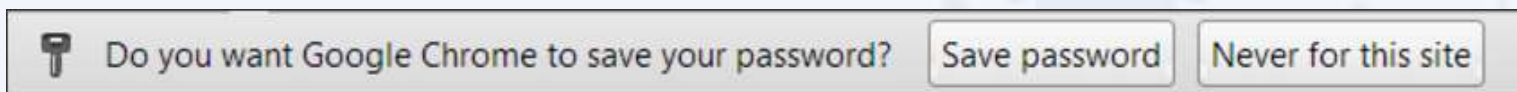
This is the best reminder yet that if you have a LinkedIn account, you should go ahead and change your password there, and everywhere else. In fact, you should make it a habit to regularly change your passwords on all your online accounts. And if that is too much of a pain, at the very least, make a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

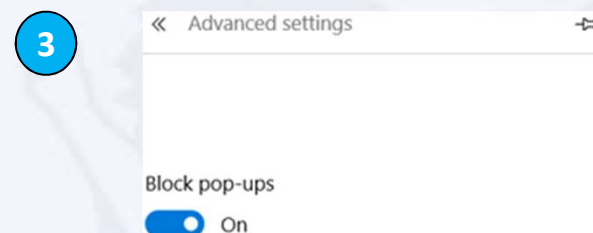
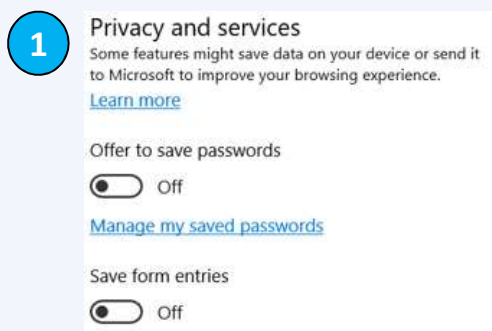
## Best Practices: Account & Password

- 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.



# Edge Browser Settings

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)



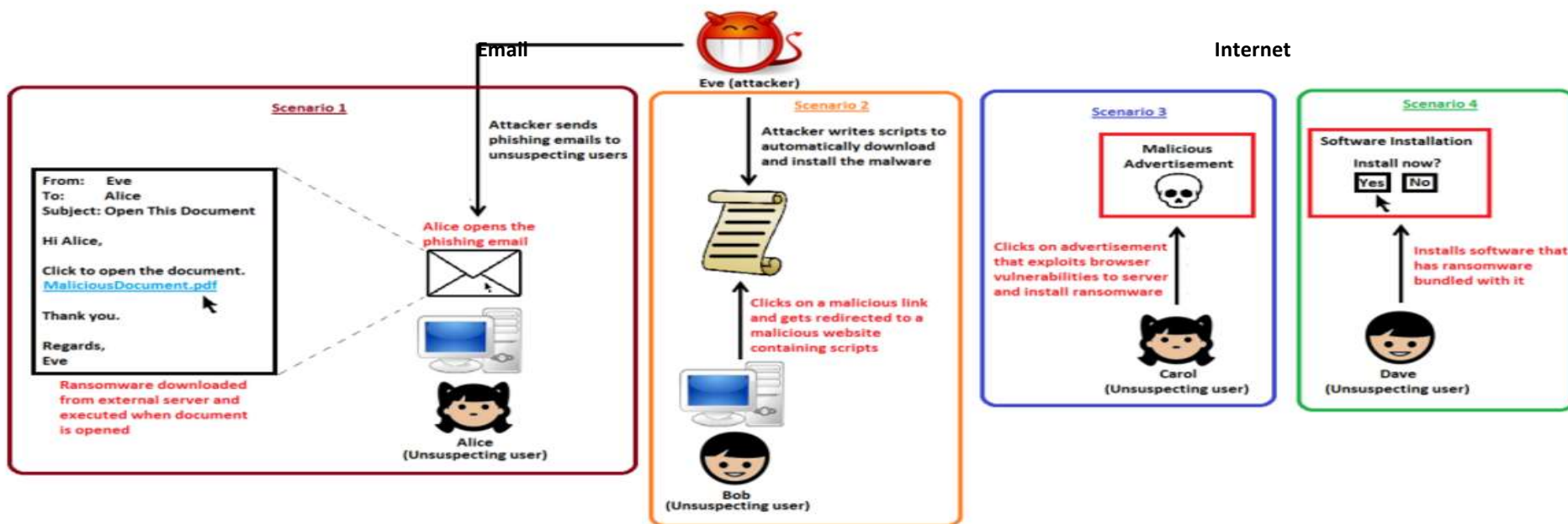
<https://privacy.microsoft.com/en-gb/windows-10-microsoft-edge-and-privacy>

<https://www.macworld.com/article/3106793/security/disable-third-party-cookies-as-a-hedge-against-a-new-browser-based-attack.html>



# 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” ~

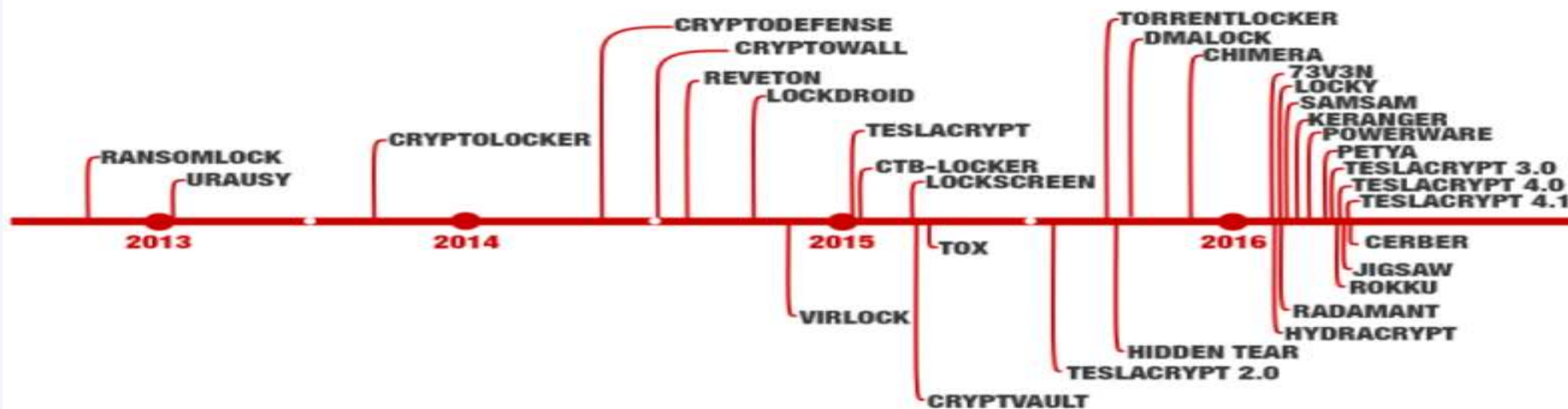
kaspersky

## Some Malware 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

...Beware of Infected USB

# Public servants barred from using unauthorised USB drives

 CHANNEL NEWSASIA

14 Jul 2017 02:48PM

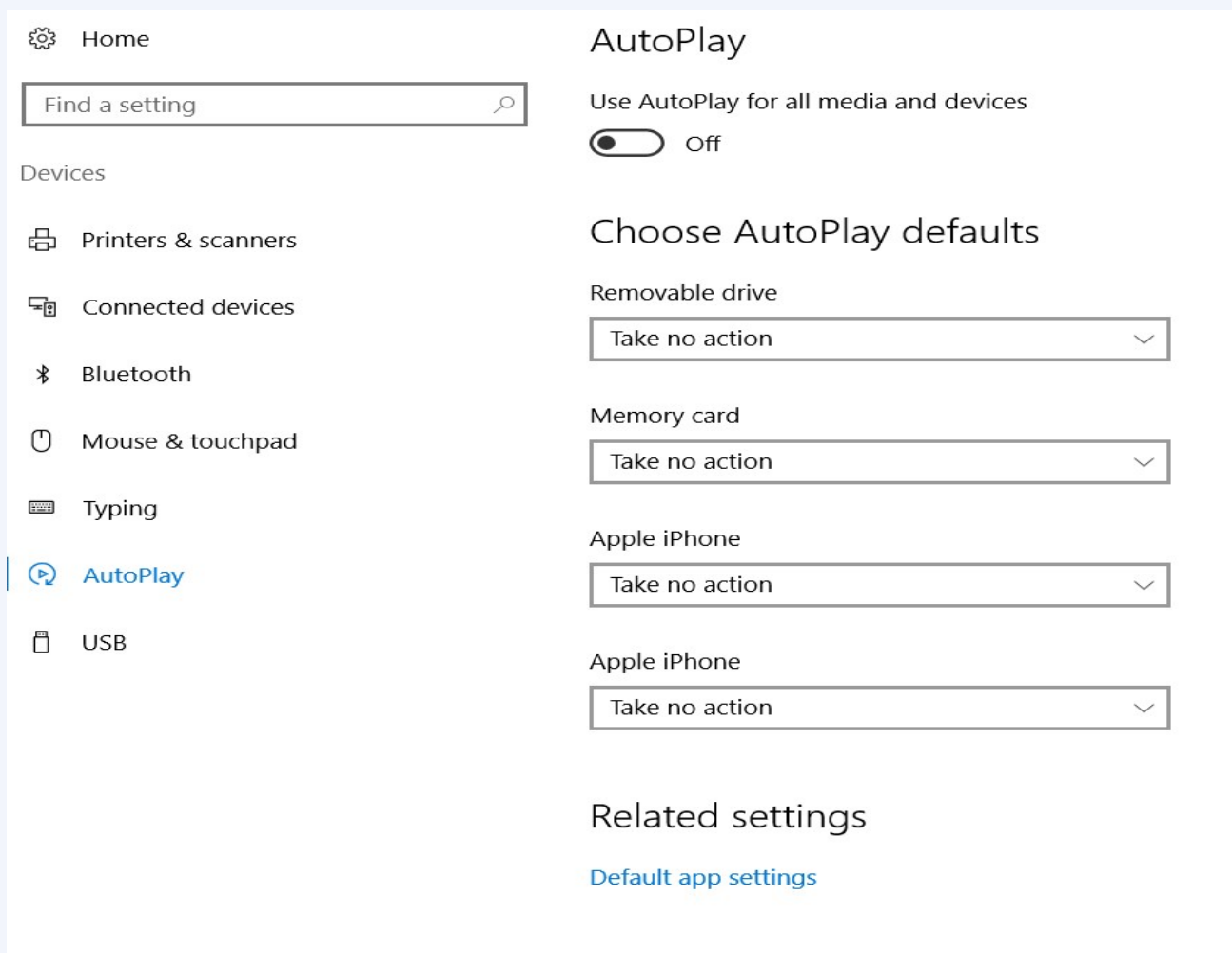
(Updated: 14 Jul 2017 04:54PM)



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.

## Prevent USB from being auto run on your laptop



The screenshot shows the Windows Settings application with the 'AutoPlay' settings page open. On the left, a navigation pane lists various settings categories, with 'AutoPlay' selected and highlighted in blue. The main content area is titled 'AutoPlay' and contains the following settings:

- AutoPlay**
  - Use AutoPlay for all media and devices:  Off
- Choose AutoPlay defaults**
  - Removable drive: Take no action (dropdown menu)
  - Memory card: Take no action (dropdown menu)
  - Apple iPhone: Take no action (dropdown menu)
  - Apple iPhone: Take no action (dropdown menu)
- Related settings**
  - [Default app settings](#)

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

## ...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 Free Antivirus 2016+RAM Boost & 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 – 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 & 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 – MPSEAPPYLABS                               | 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

## 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/>





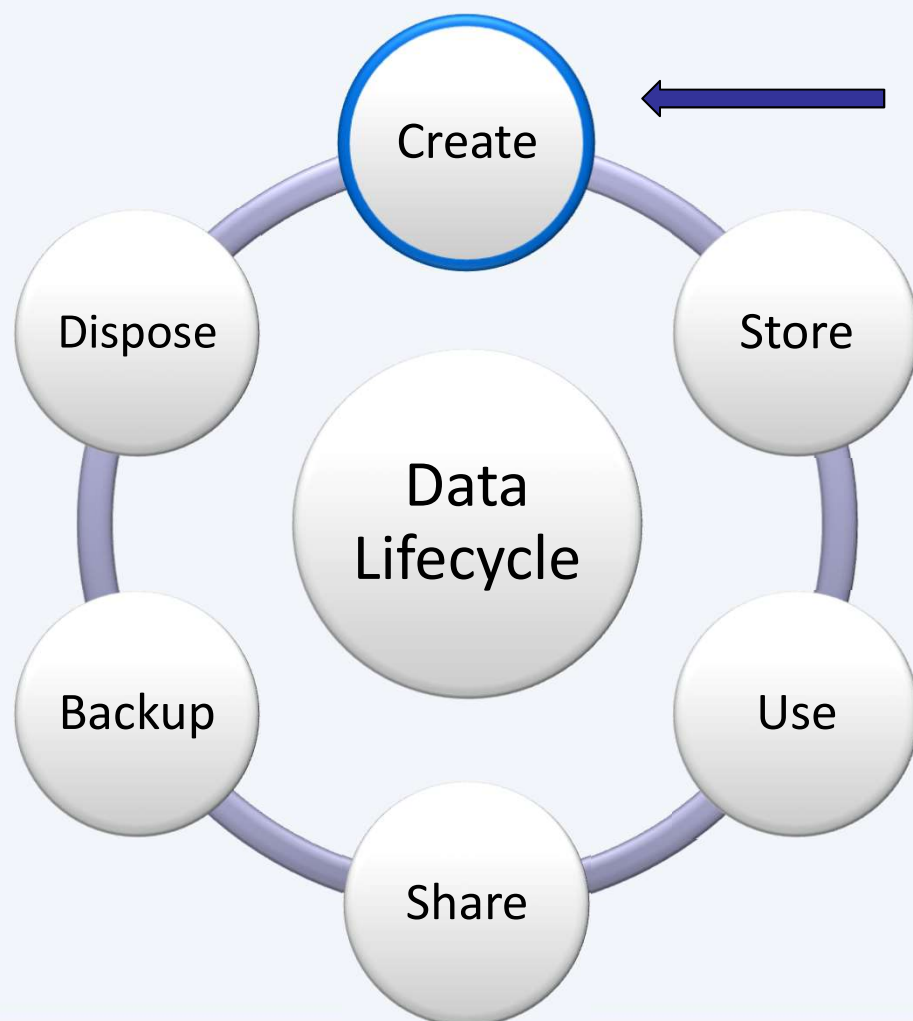
# Data Protection Measures



***Security is  
lifestyle!***

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

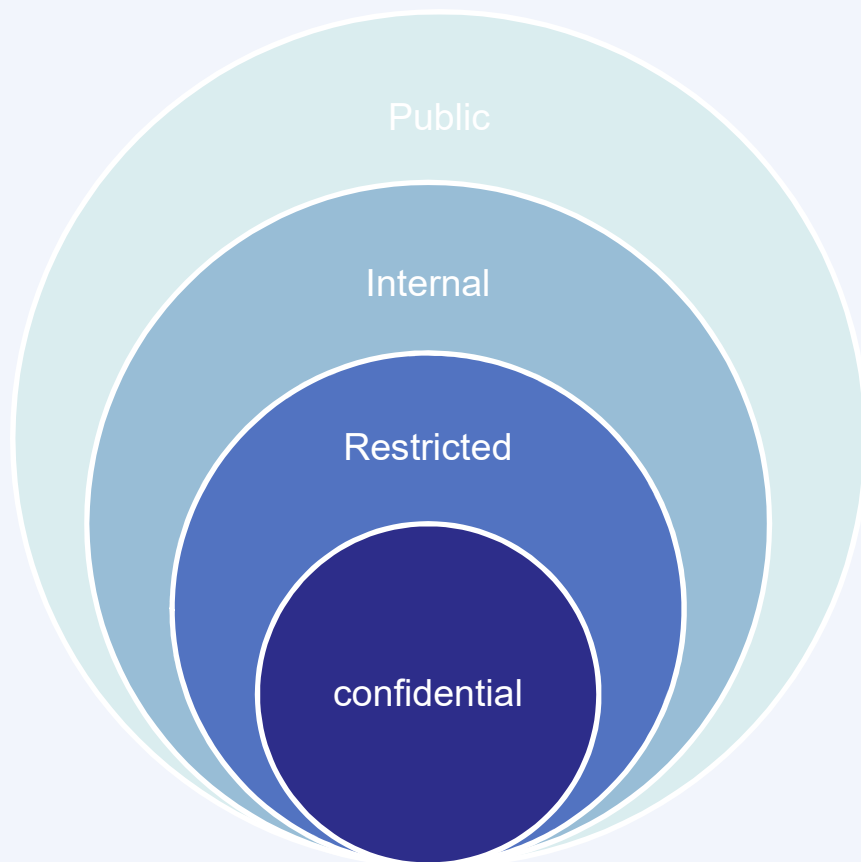
## Data Lifecycle & Data Protection Best Practices



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







## How Do I Classify Data?



***“Classify university data based on its **sensitivity and impact** to the university in terms of **reputation, finance and operation** should there be data breach”***

## Data Classification Examples

Data Classification	Examples
 <b>NUS Confidential</b>	<ul style="list-style-type: none"> <li>• Personal Data (i.e. Name, NRIC/FIN, DOB, Contact Details)</li> <li>• Staff salary, staff appraisal</li> <li>• Examination marks/grades &amp; examination questions</li> <li>• Financial data (e.g. Credit card / bank account numbers)</li> <li>• Admission data (e.g. race, religion)</li> <li>• Medical records</li> <li>• Donor records</li> </ul>
 <b>NUS Restricted</b>	<ul style="list-style-type: none"> <li>• Academic details of student (e.g. course info)</li> <li>• Employment details (e.g. position hired for)</li> <li>• Management reports</li> <li>• Information covered by confidentiality obligation (e.g. contracts)</li> </ul>
 <b>NUS Internal</b>	<ul style="list-style-type: none"> <li>• Staff circulars</li> <li>• Internal policies</li> <li>• Operating procedures</li> </ul>
 <b>Public</b>	<ul style="list-style-type: none"> <li>• Publicly posted press releases/statistics</li> <li>• University maps</li> <li>• Newsletters, newspapers, magazines</li> </ul>

## Data Management Policy Sep 2018

***“All university data shall be classified ...” – Data Management Policy version 2.4 Sep 2018, Clause 3.1.1***



**NUS Confidential Data includes personal data** such as name, NRIC/Passport/FIN number, personal email and contact number, photograph, fingerprint, video/voice recording, medical record, etc



# How do I classify data?

**Answer: For example, Label document header and/or footer with  
NUS Confidential, NUS Restricted and NUS Internal**

## How do we classify data?

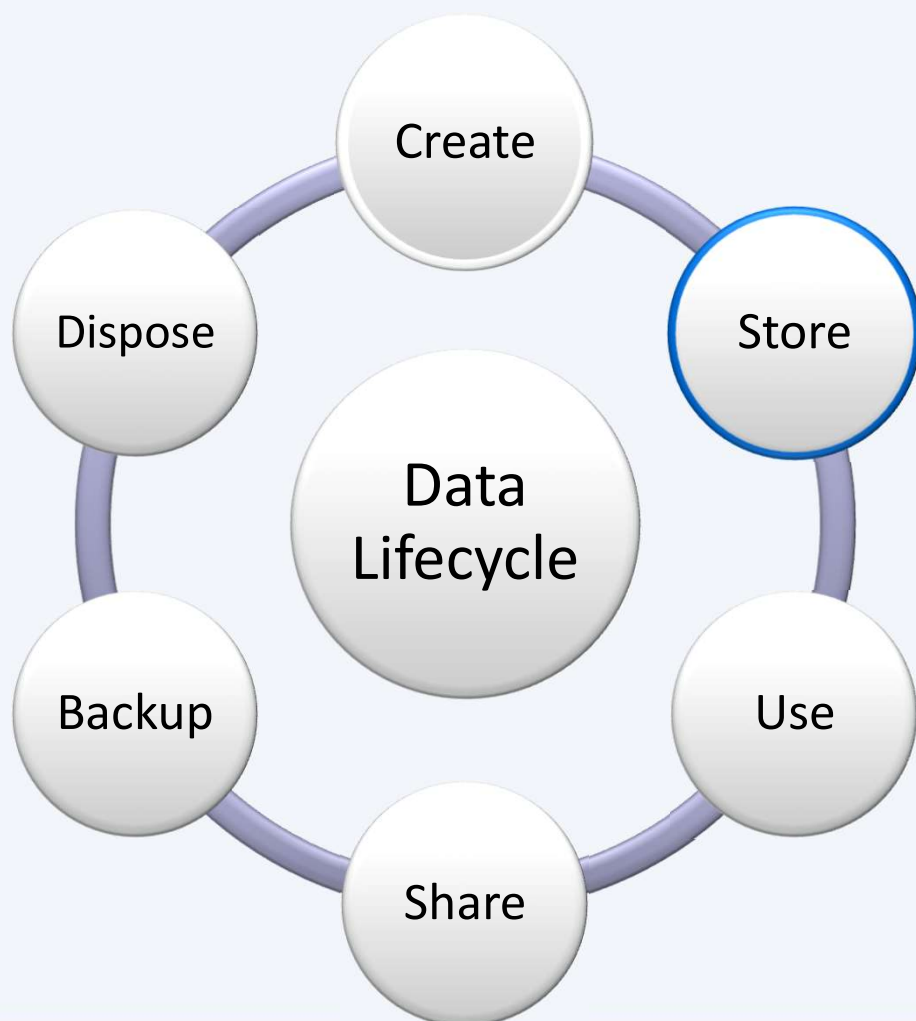
**Classify data:**  
e.g. Label the  
document  
header and  
footer with  
appropriate  
data  
classification

**NUS Confidential**

**e.g. Tan Ah Kou**  
**S7712345B**

**NUS Confidential**

## Data Lifecycle & Data Protection Best Practices

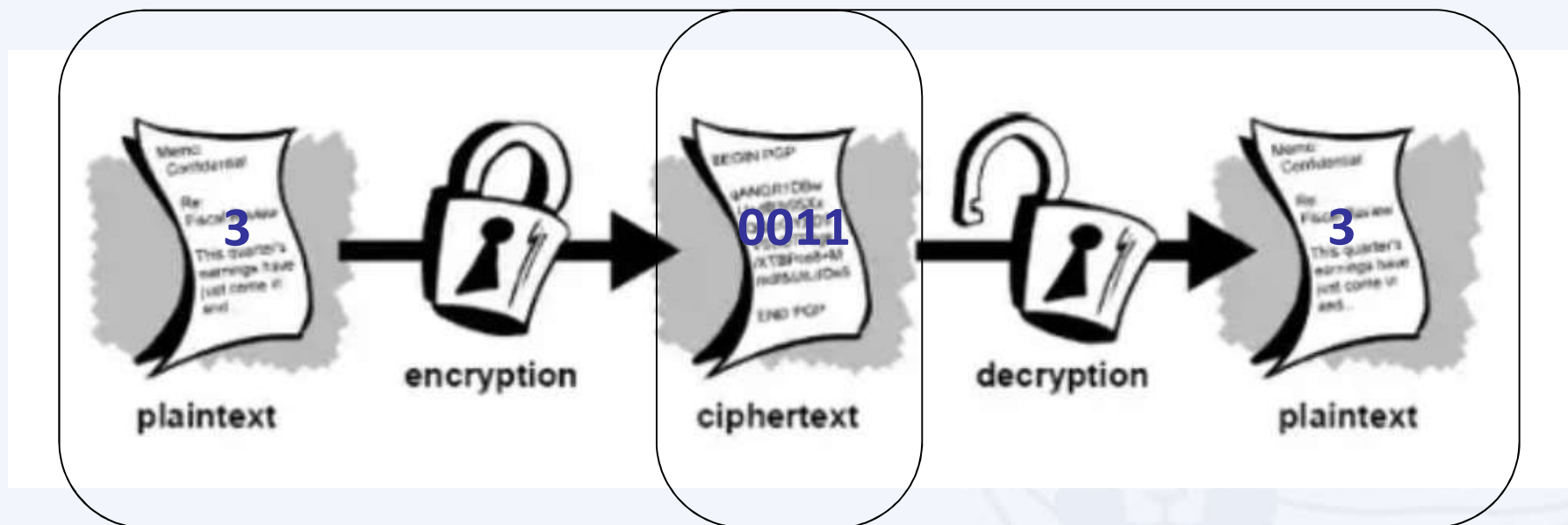


**Encrypt NUS-Confidential data  
store on Laptop using  
Encrypting File System (EFS)**





## 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.

**Source :**

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

<https://www.entrepreneur.com/article/240517>

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





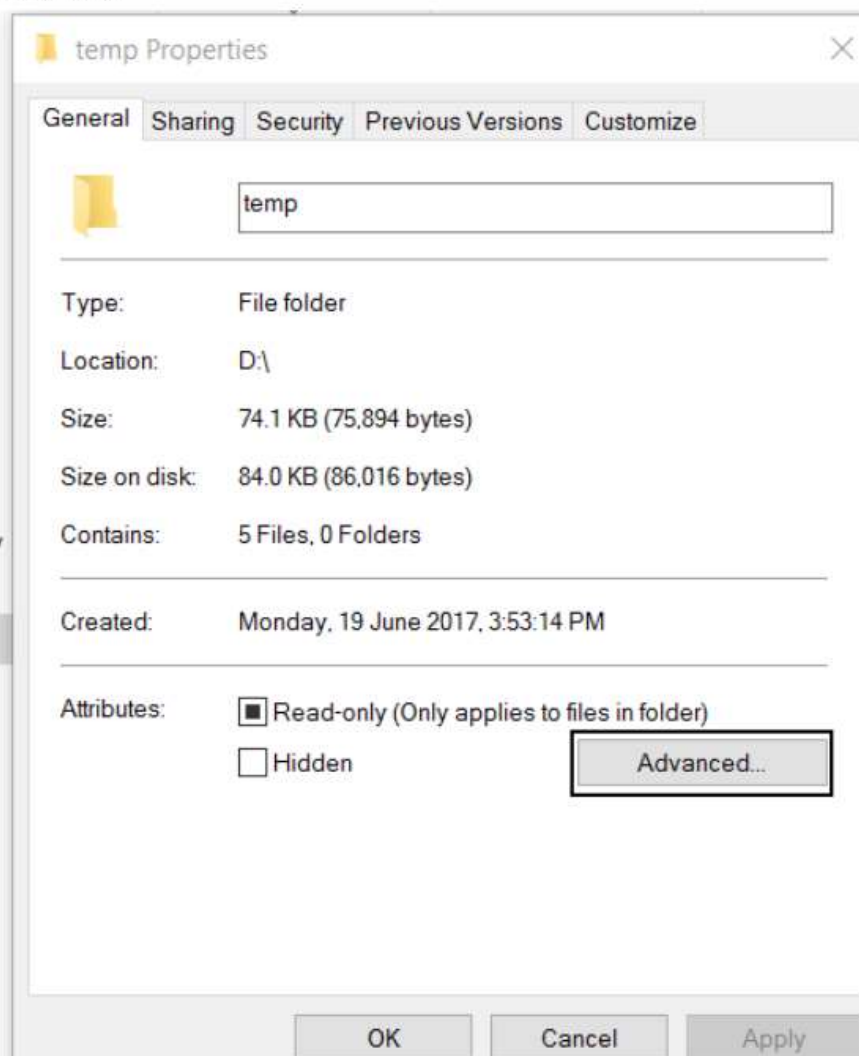
**How do we  
prevent data  
from being  
accessed by  
unauthorized  
person?**

**Answer: Encrypt the data**

## Enable EFS

### Windows 10

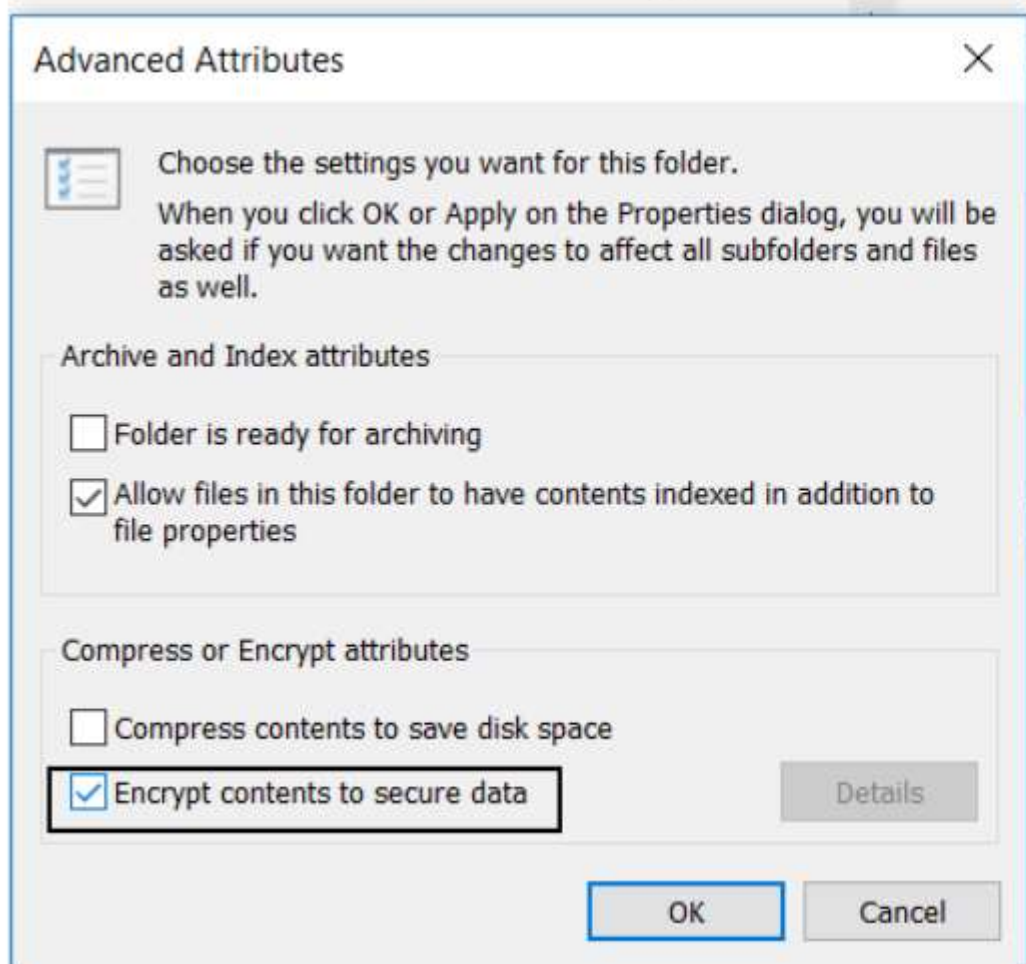
1. Right-click the folder that you want to encrypt and click Properties. In the Properties dialog box, click Advanced.



<https://nusit.nus.edu.sg/its/resources/encrypt-windows-folders/encrypt-windows-folders-and-contents/>

## Enable EFS

- From Advance Attributes box, Tick the “Encrypt contents to secure data” check box and click OK.



<https://nusit.nus.edu.sg/its/resources/encrypt-windows-folders/encrypt-windows-folders-and-contents/>

## Enable EFS

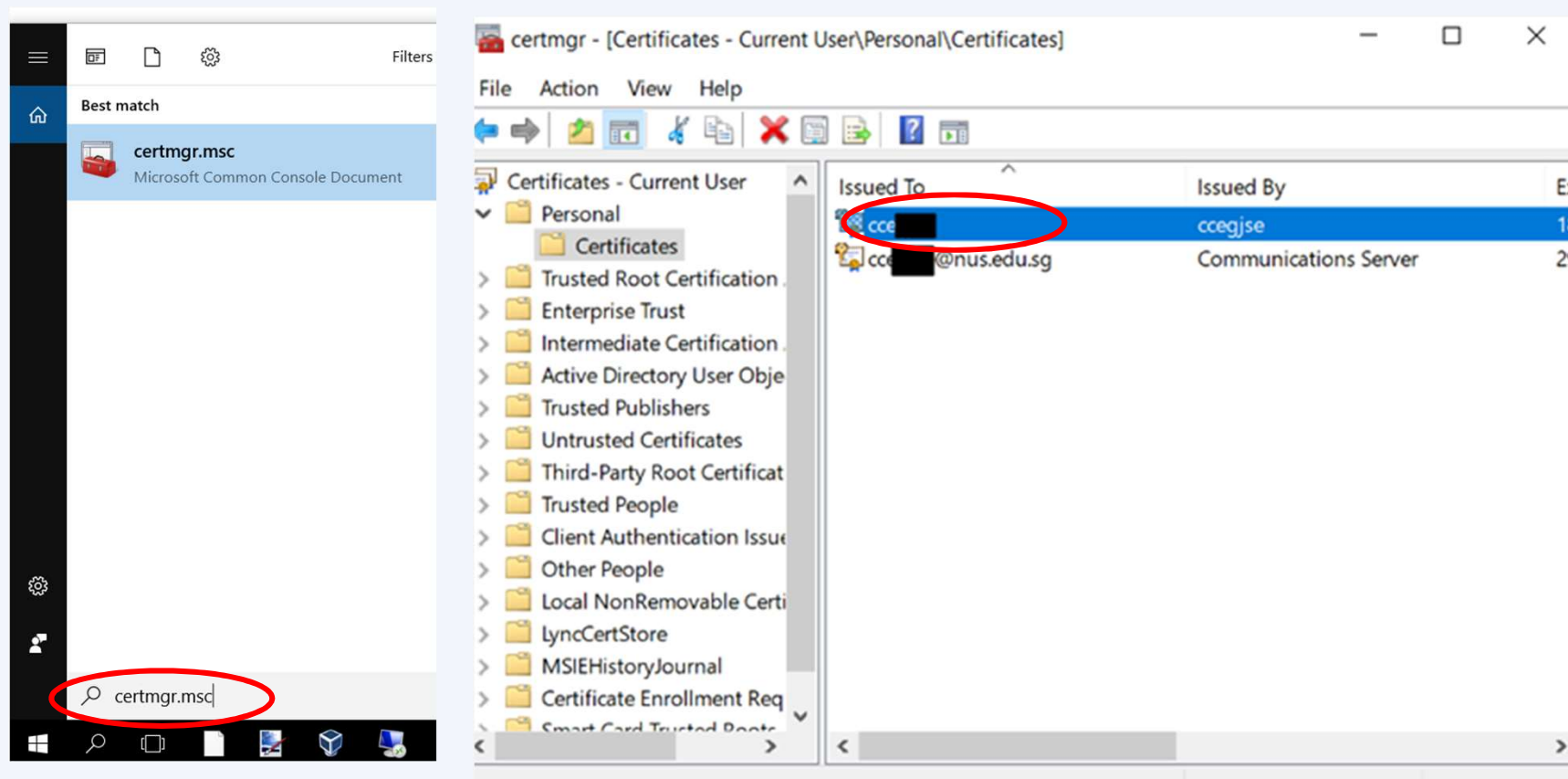
3. From Confirm Attribute Changes box, select Apply changes to the folder, subfolders and files, click Ok.



<https://nusit.nus.edu.sg/its/resources/encrypt-windows-folders/encrypt-windows-folders-and-contents/>

## Back up EFS Key

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



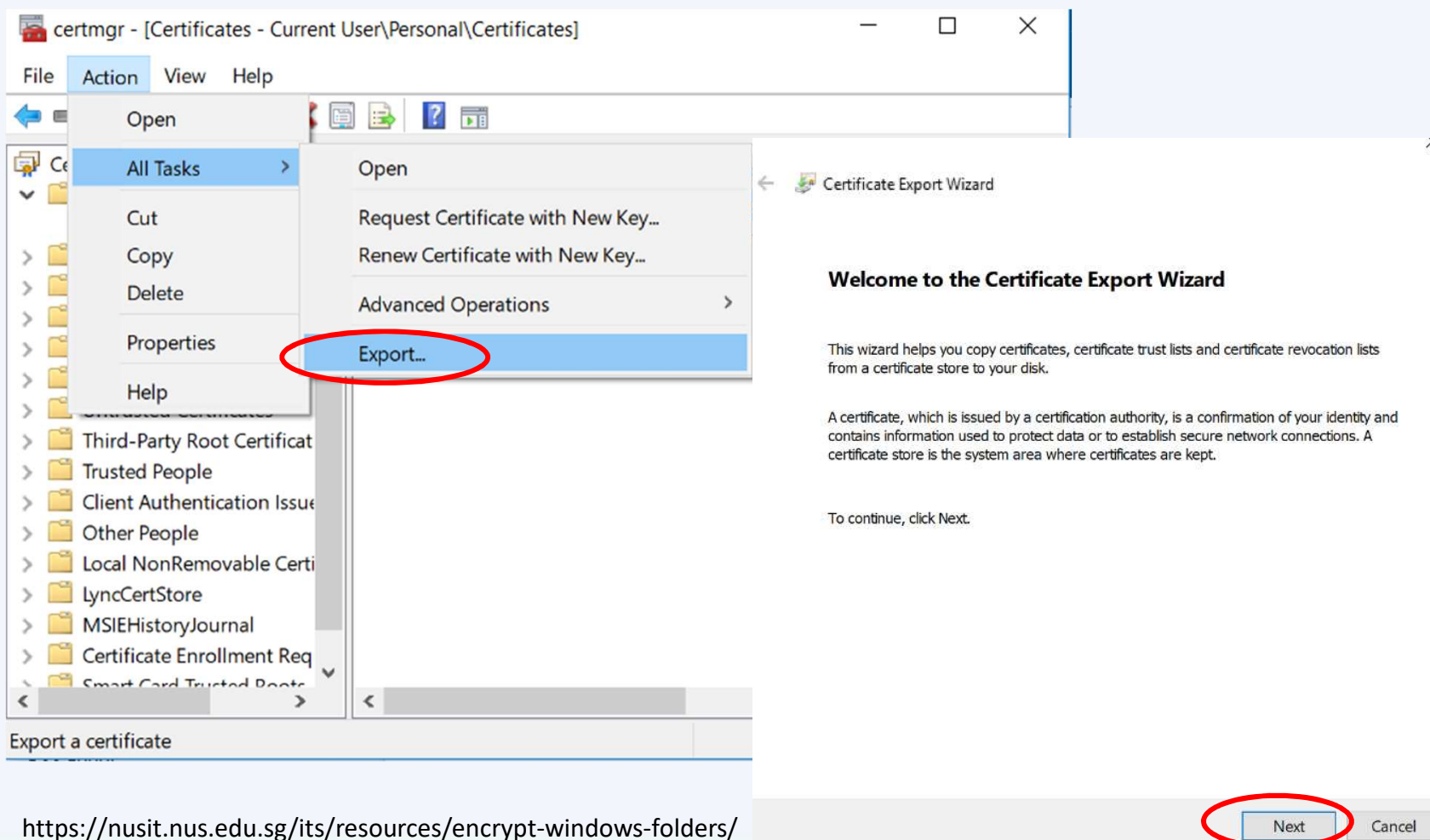
The screenshot shows the Windows search interface on the left and the certmgr console on the right. In the search box, 'certmgr.msc' is entered and circled in red. The search results show 'certmgr.msc' as a Microsoft Common Console Document. The certmgr console window is open to the 'Certificates - Current User' folder, with the 'Certificates' subfolder selected. The 'Issued To' column is expanded, and the entry 'ccejse@nus.edu.sg' is highlighted with a red circle. The 'Issued By' column shows 'ccejse' and 'Communications Server'.

Issued To	Issued By	Expiration Date
ccejse	ccejse	18/01/2018
ccejse@nus.edu.sg	Communications Server	29/01/2018

<https://nusit.nus.edu.sg/its/resources/encrypt-windows-folders/>

## Back up EFS Key

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



The screenshot shows the Windows Certificate Manager window (certmgr) with the 'Action' menu open. The 'All Tasks' sub-menu is expanded, and the 'Export...' option is highlighted with a red circle. In the foreground, the 'Certificate Export Wizard' dialog box is open, displaying the 'Welcome to the Certificate Export Wizard' screen. The 'Next' button at the bottom right of the wizard is also 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 Issu

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.

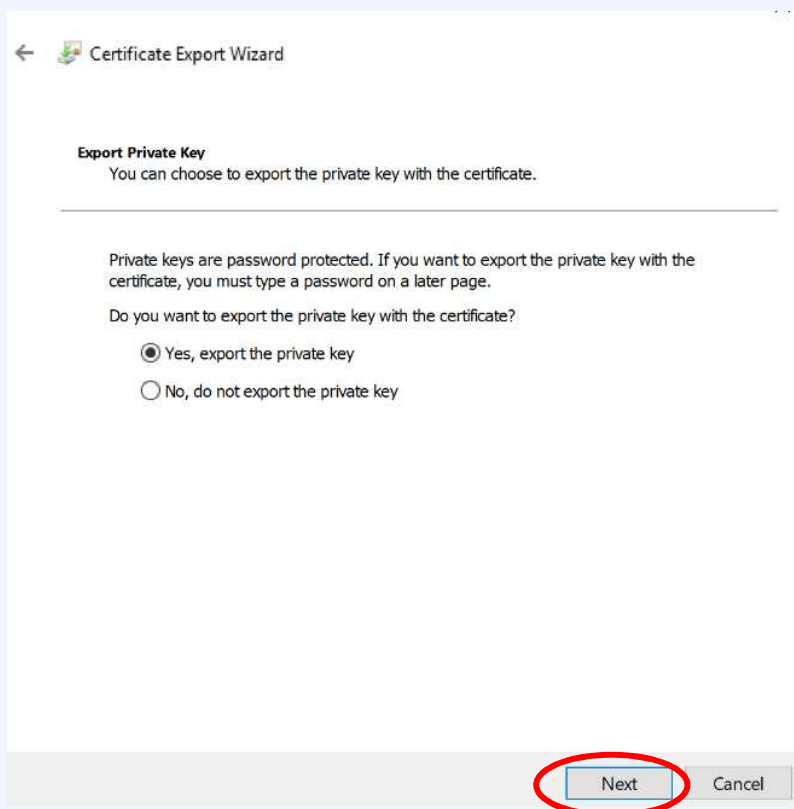
Next Cancel

<https://nusit.nus.edu.sg/its/resources/encrypt-windows-folders/>



## 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.

---

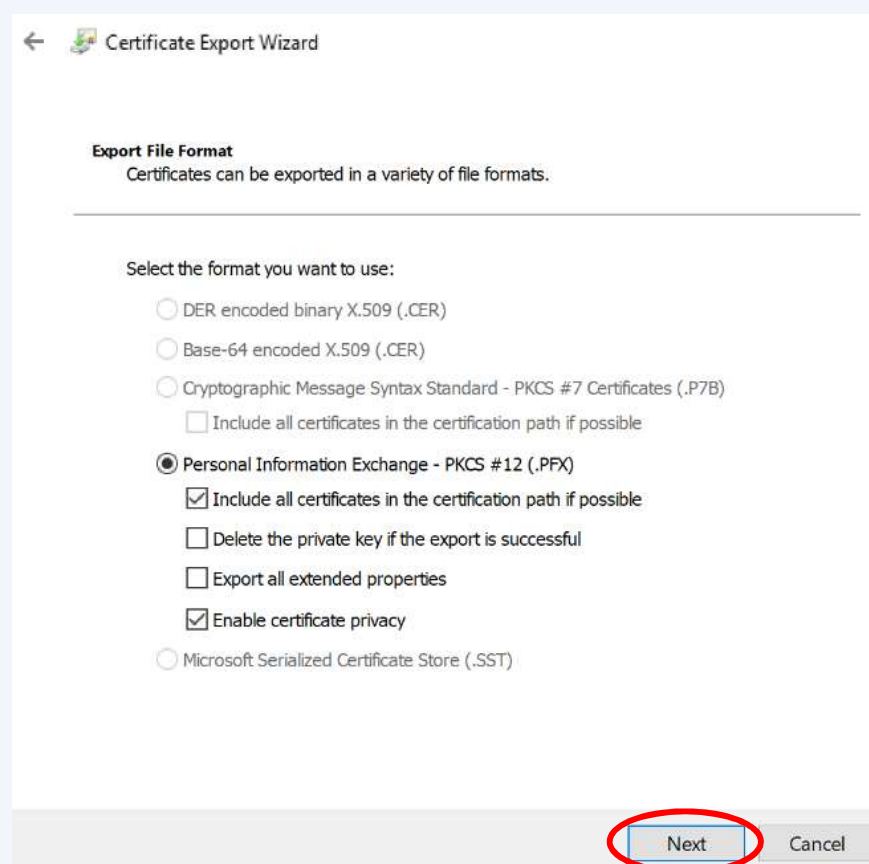
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

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

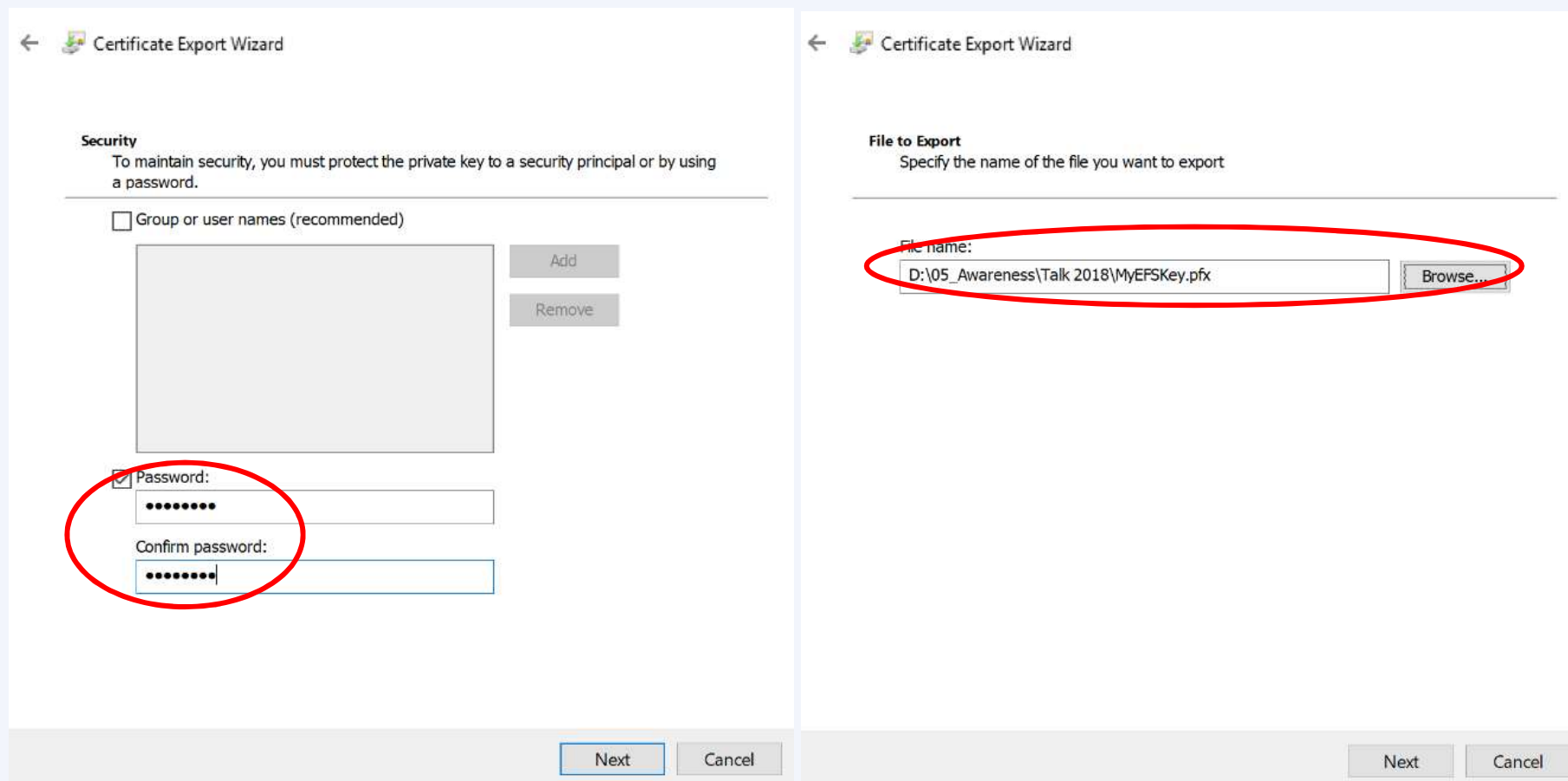
Microsoft Serialized Certificate Store (.SST)

Next Cancel

<https://nusit.nus.edu.sg/its/resources/encrypt-windows-folders/>

## 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

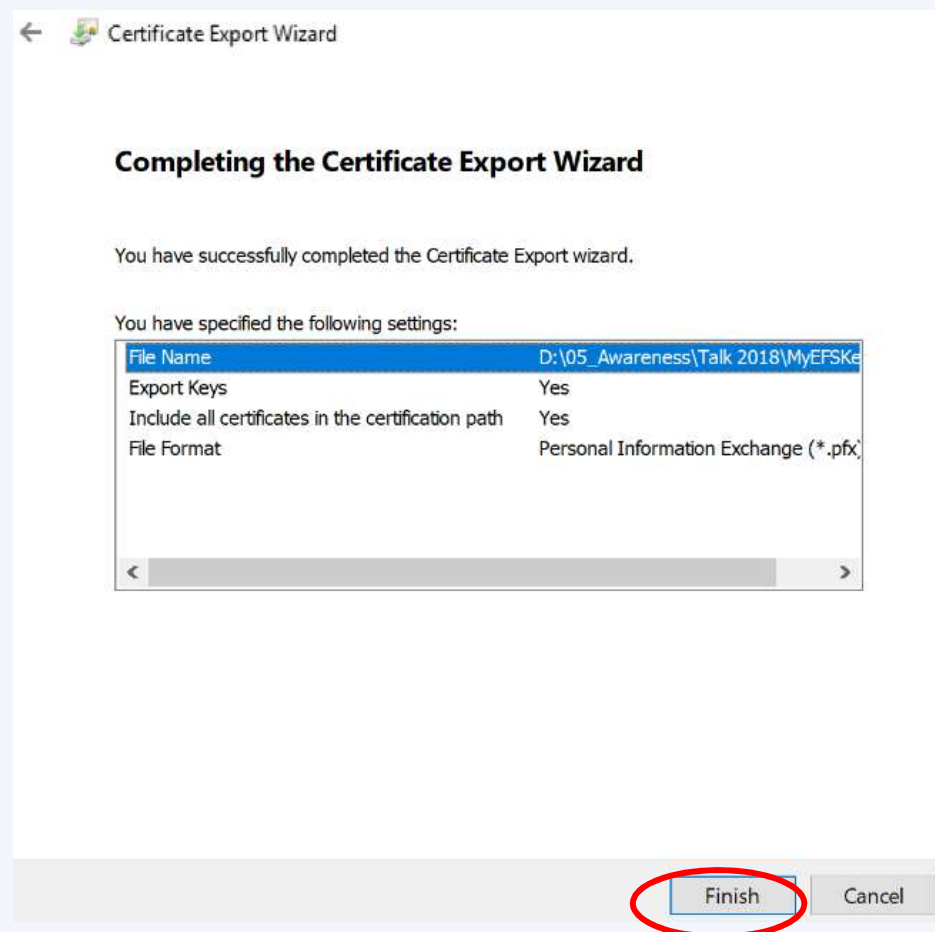
File name:  
D:\05\_Awareness\Talk 2018\MyEFSKey.pfx Browse...

Next Cancel

<https://nusit.nus.edu.sg/its/resources/encrypt-windows-folders/>

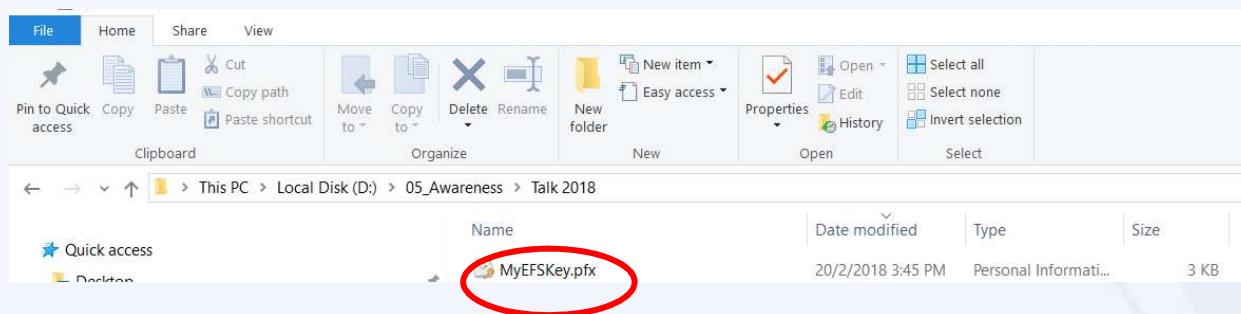
## Back up EFS Key

- Click Finish on Certification Export Wizard.



<https://nusit.nus.edu.sg/its/resources/encrypt-windows-folders/backup-of-encryption-certificate-and-private-keys-for-windows-vista-7/>

## Back up EFS Key



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

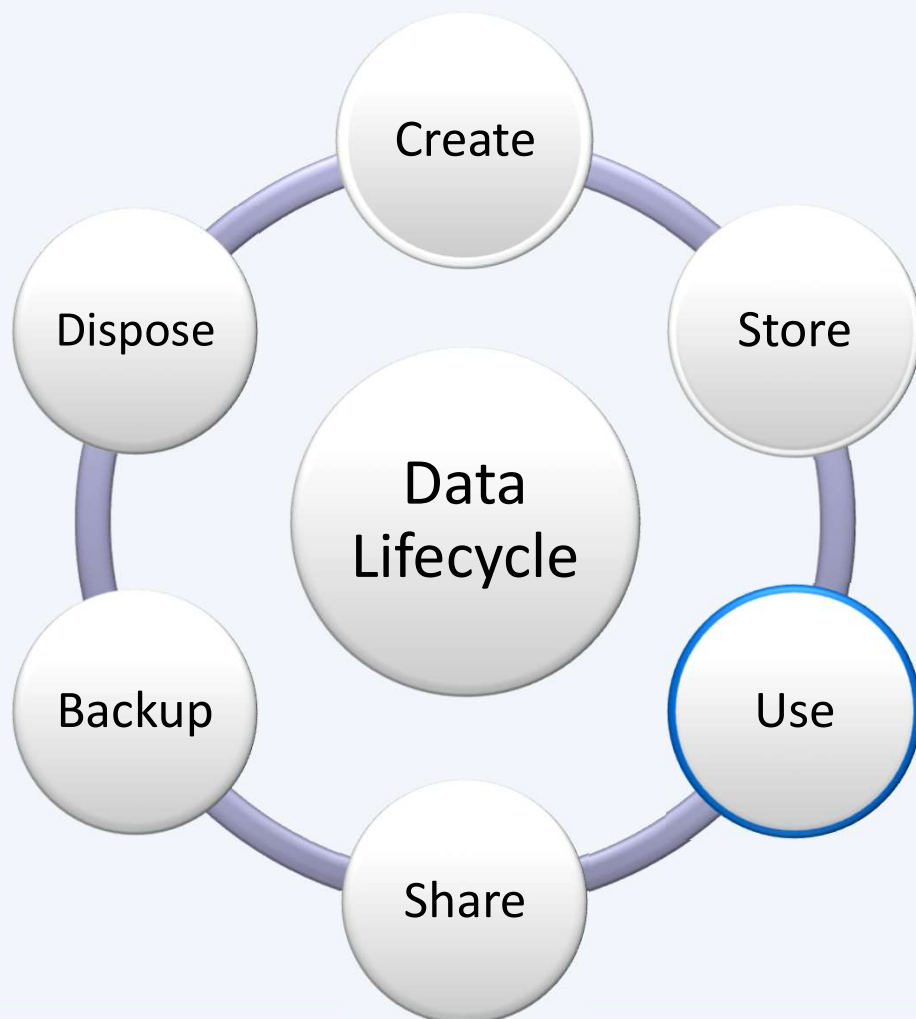


# What happens if I lose my EFS key?

**Answer: Data cannot be decrypted.**



## Data Lifecycle & Data Protection Best Practices

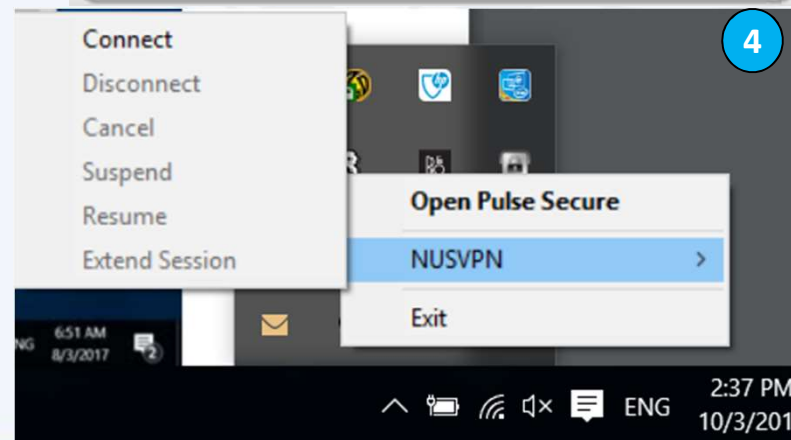
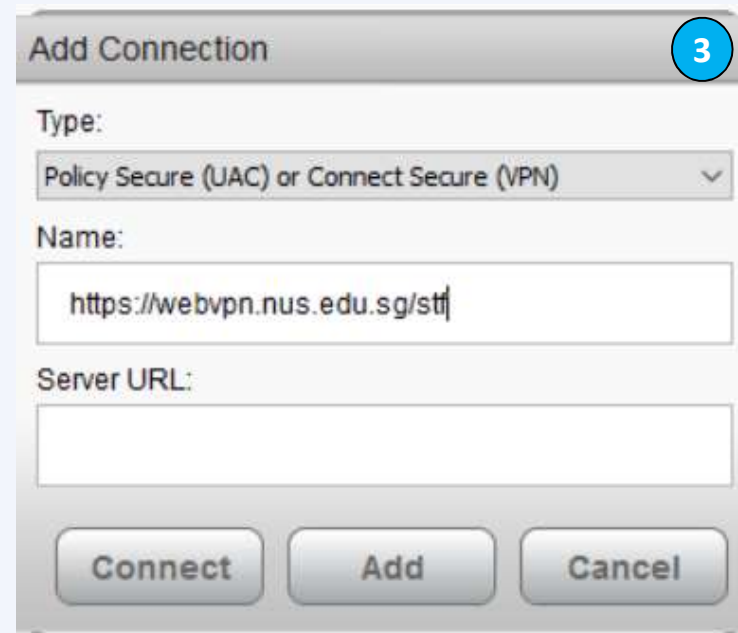
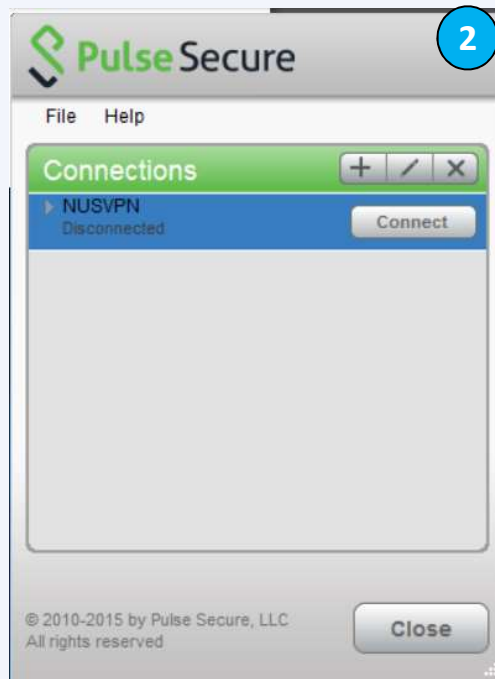
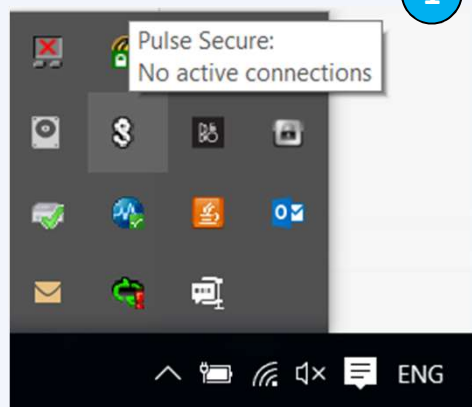


### Access data securely:

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

# 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>



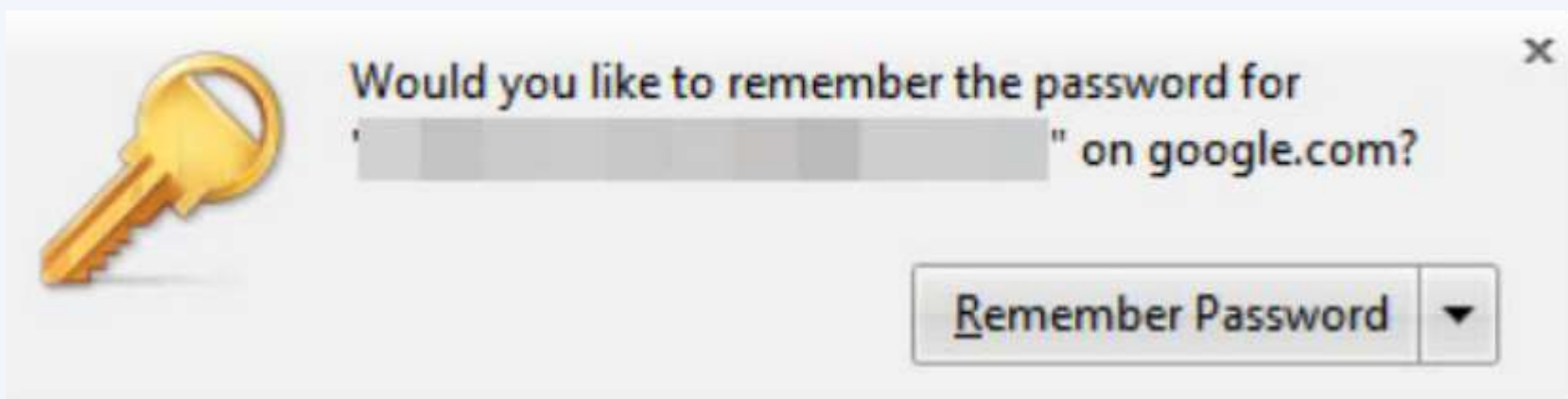
## Use https website



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/>



# 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 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

Log off from browser application after using it.

# 'Data monger' fined \$6k by privacy watchdog for selling personal data without notification or consent

A data monger is someone who makes money from dealing in other people's personal data such as phone and NRIC numbers.

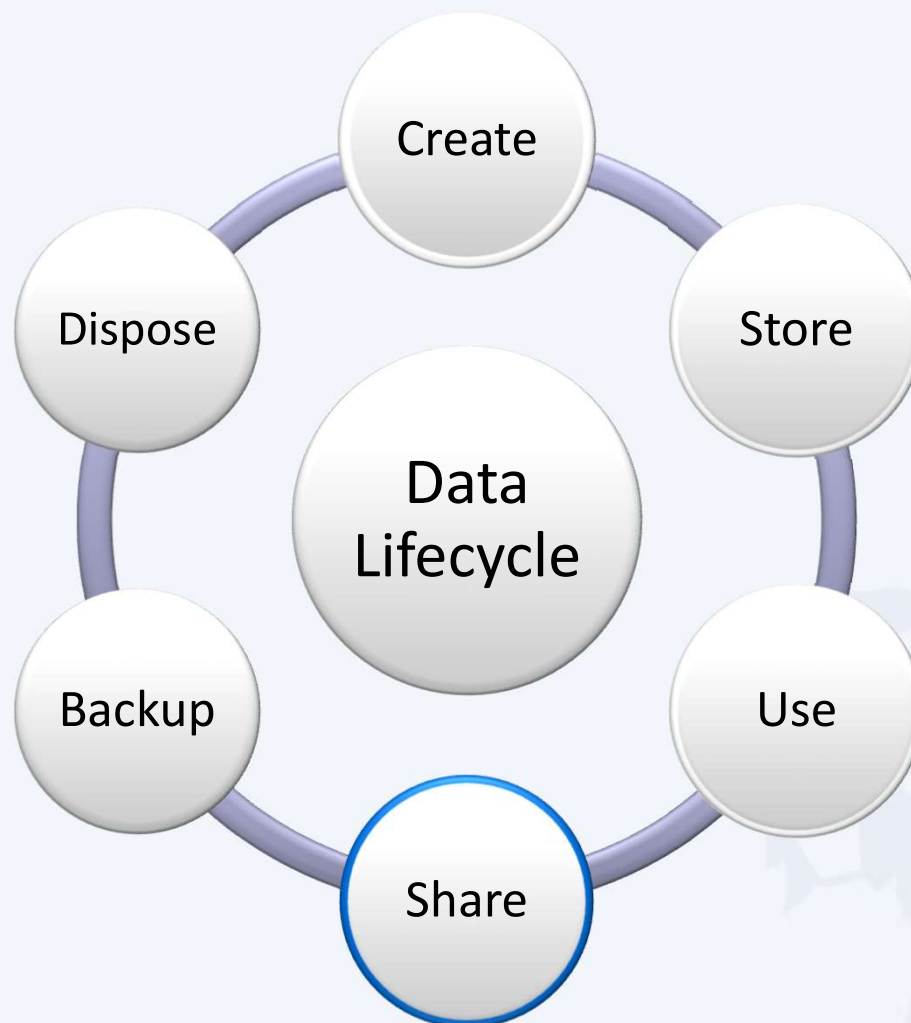
The Personal Data Protection Commission (PDPC) fined former telemarketer Sharon Assya Qadriyah Tang \$6,000 on Jan 11 for selling personal data without notifying the individuals involved or obtaining their consent.

A data monger is someone who makes money from dealing in other people's personal data such as phone and NRIC numbers.

The Personal Data Protection Commission (PDPC) fined former telemarketer Sharon Assya Qadriyah Tang \$6,000 on Jan 11 for selling personal data without notifying the individuals involved or obtaining their consent.

**Source: Straits Times, @ Jan 2018**

## Data Lifecycle & Data Protection Best Practices



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

## Sending Out Personal Data by Mistake

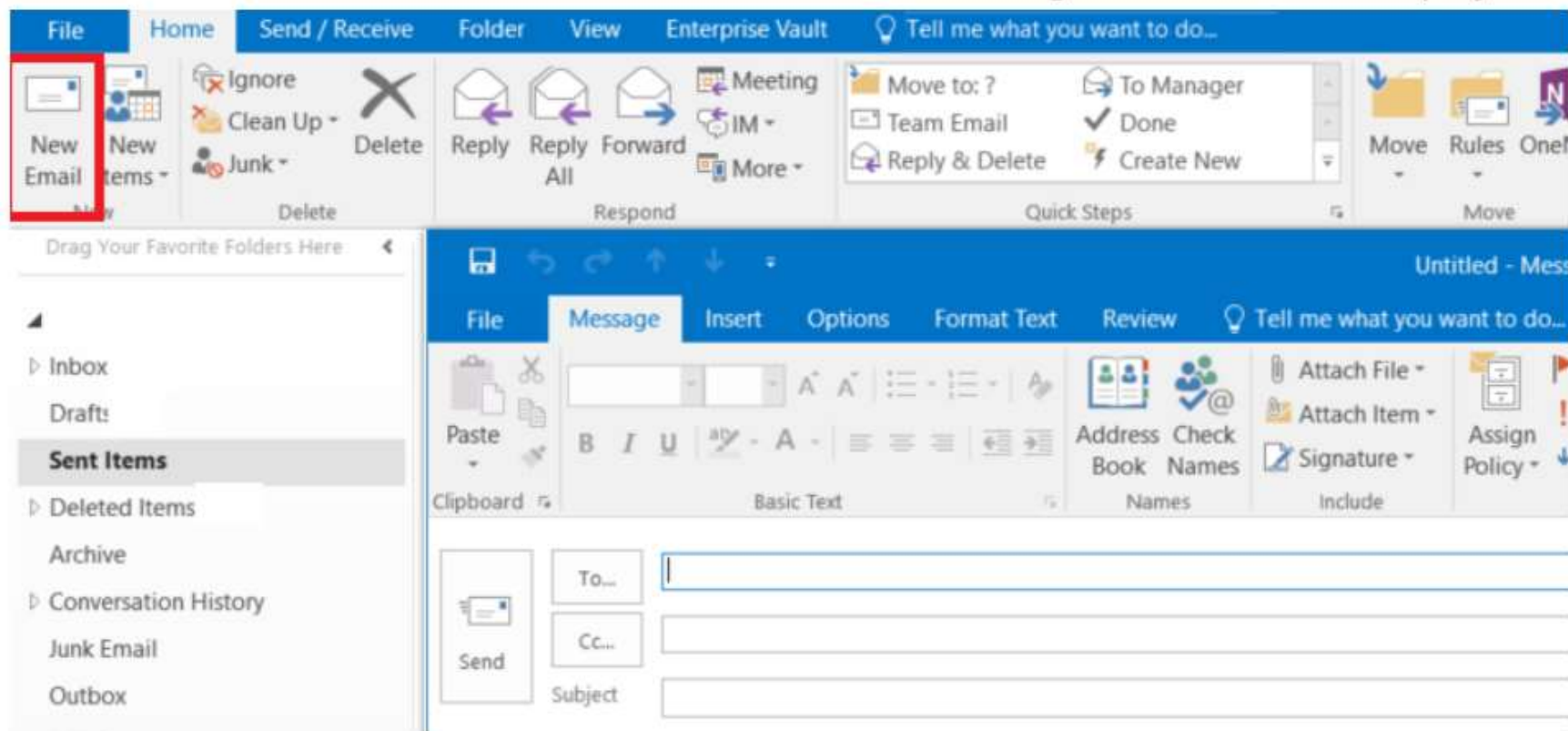


The personal data of more than 1,900 pupils from Henry Park Primary School was leaked when an Excel spreadsheet containing the children's particulars was mistakenly sent out to about 1,200 parents as part of an update about a school event. The file contained the names and birth certificate numbers of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

## Encrypt Email with RMS (Internal Users)

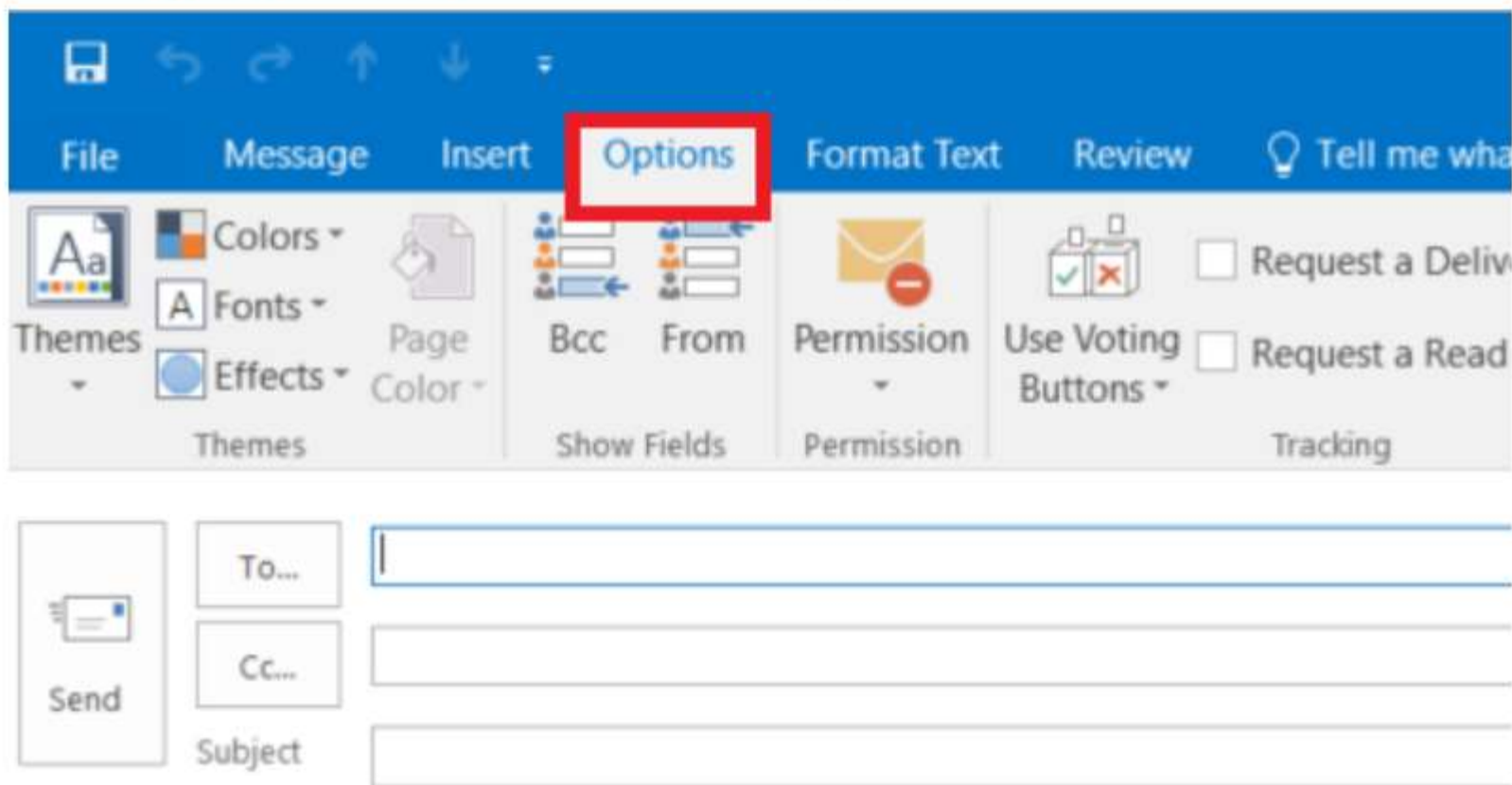
1. Select **New Email** from Outlook menu. The Outlook message window will be displayed.



<https://nusit.nus.edu.sg/its/resources/encrypt-email-without-attachments/>

## Encrypt Files with RMS (Internal Users)

2. Select **Options** from the Outlook message window.

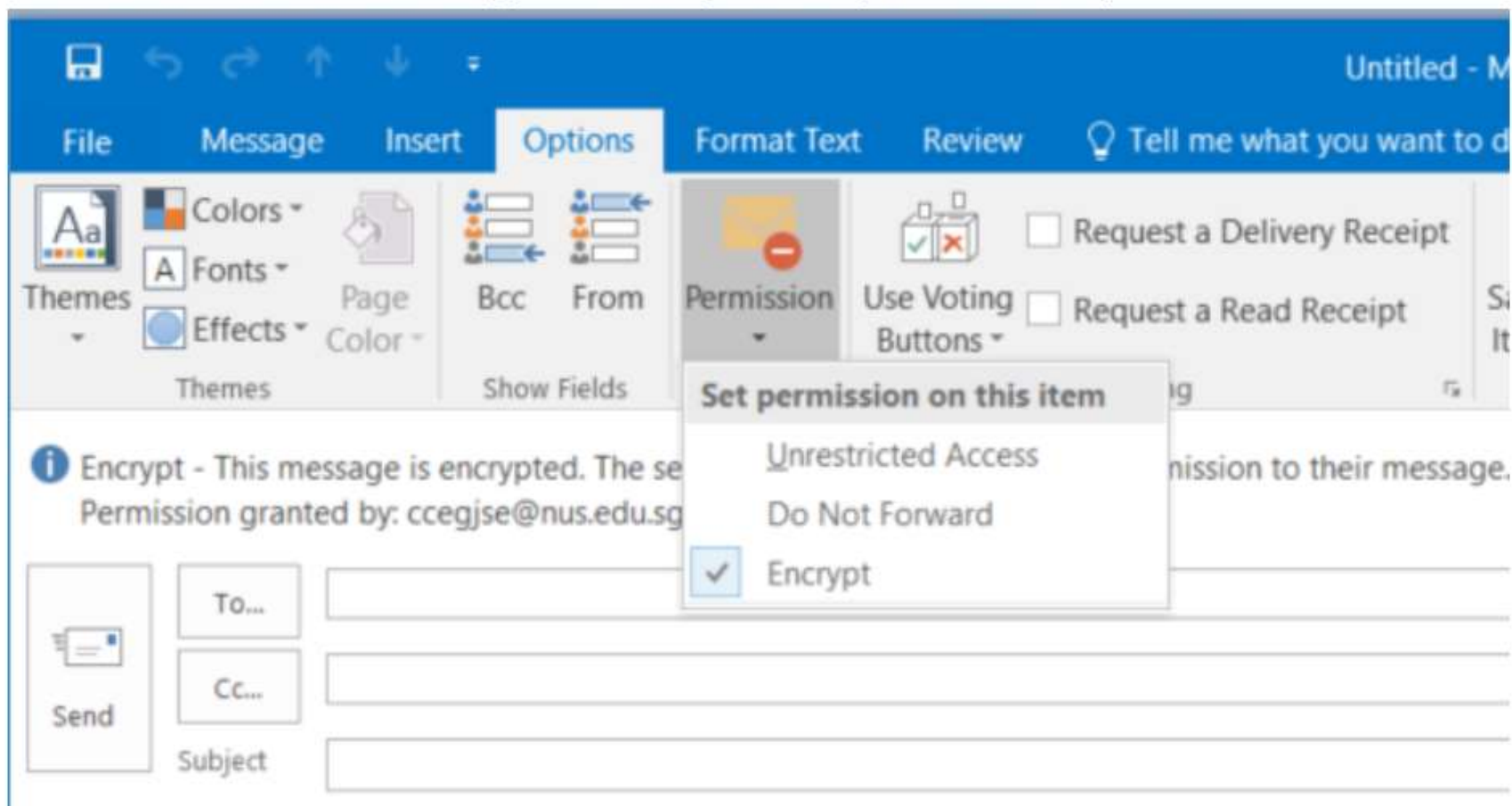


<https://nusit.nus.edu.sg/its/resources/encrypt-email-withwithout-attachments/>



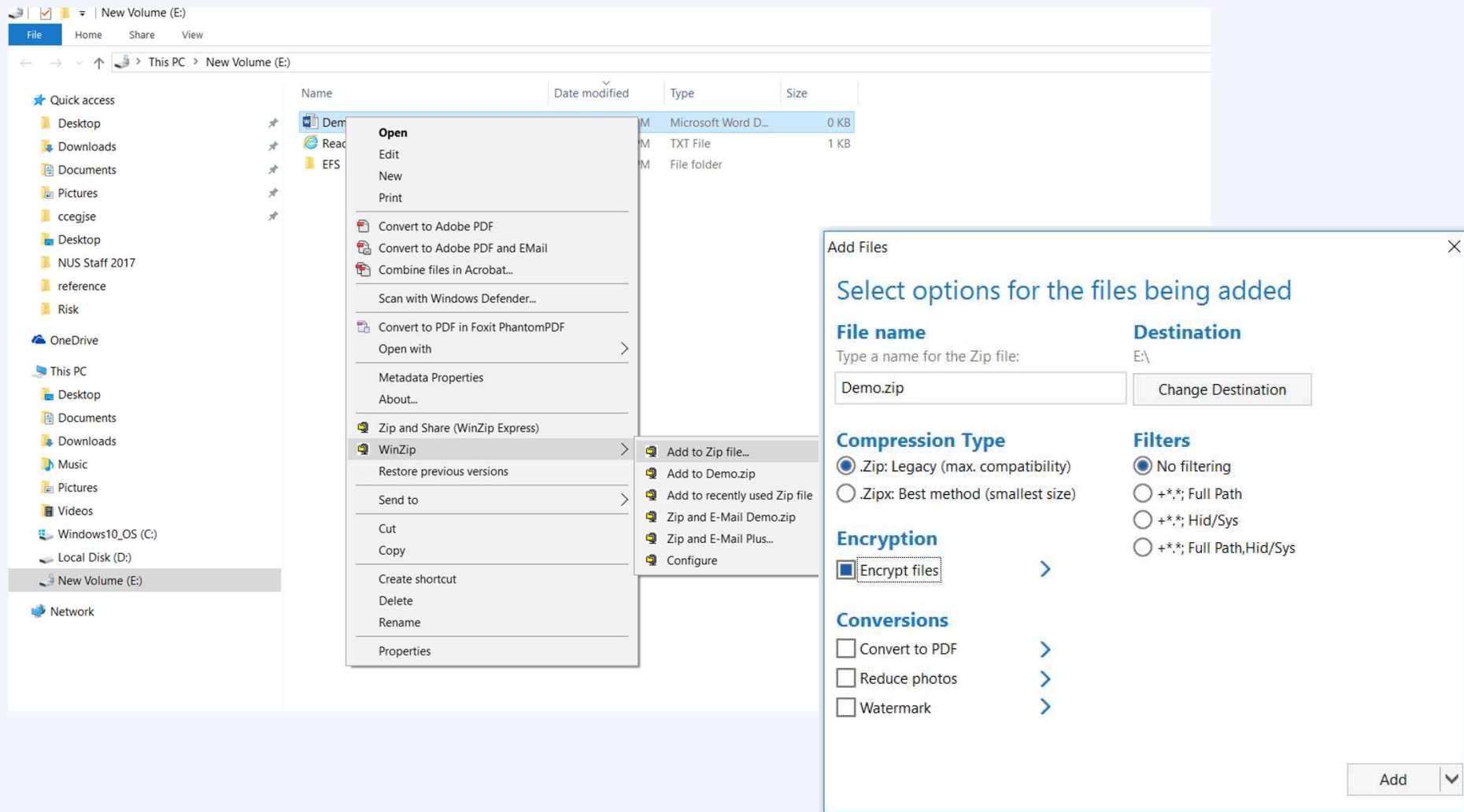
## Encrypt Files with RMS (Internal Users)

3. Select **Permission->Encrypt** from the Outlook message window. Your email including its attachment are now encrypted when you completed this step.



<https://nusit.nus.edu.sg/its/resources/encrypt-email-withwithout-attachments/>

# Encrypt Files with Password using Winzip



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

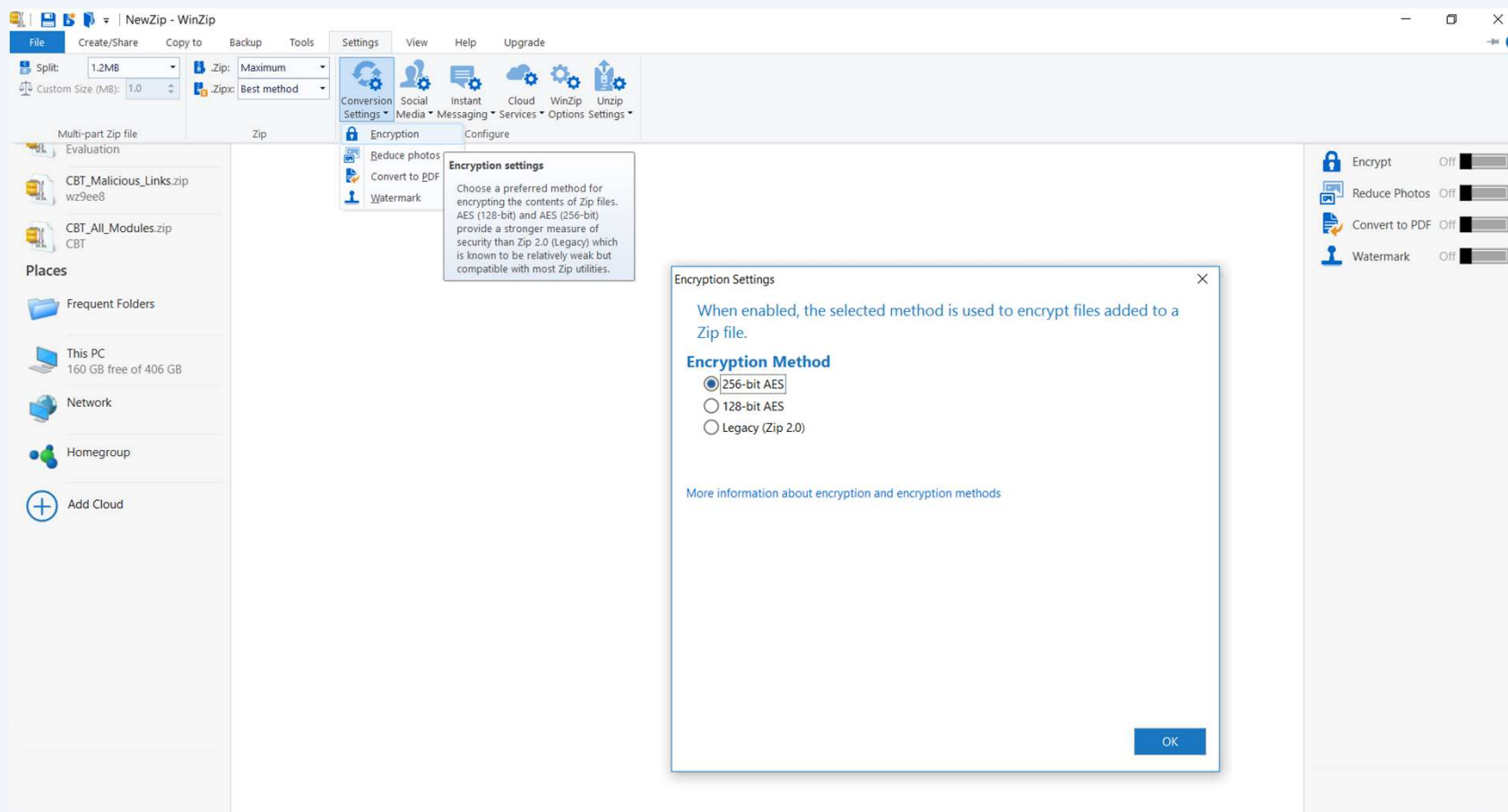
Name	Date modified	Type	Size
Demo.docx		Microsoft Word Document	0 KB
Readme.txt		Text File	1 KB
EFS		File folder	

**Add Files Dialog Options:**

- File name:** Demo.zip
- Destination:** E:\
- 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

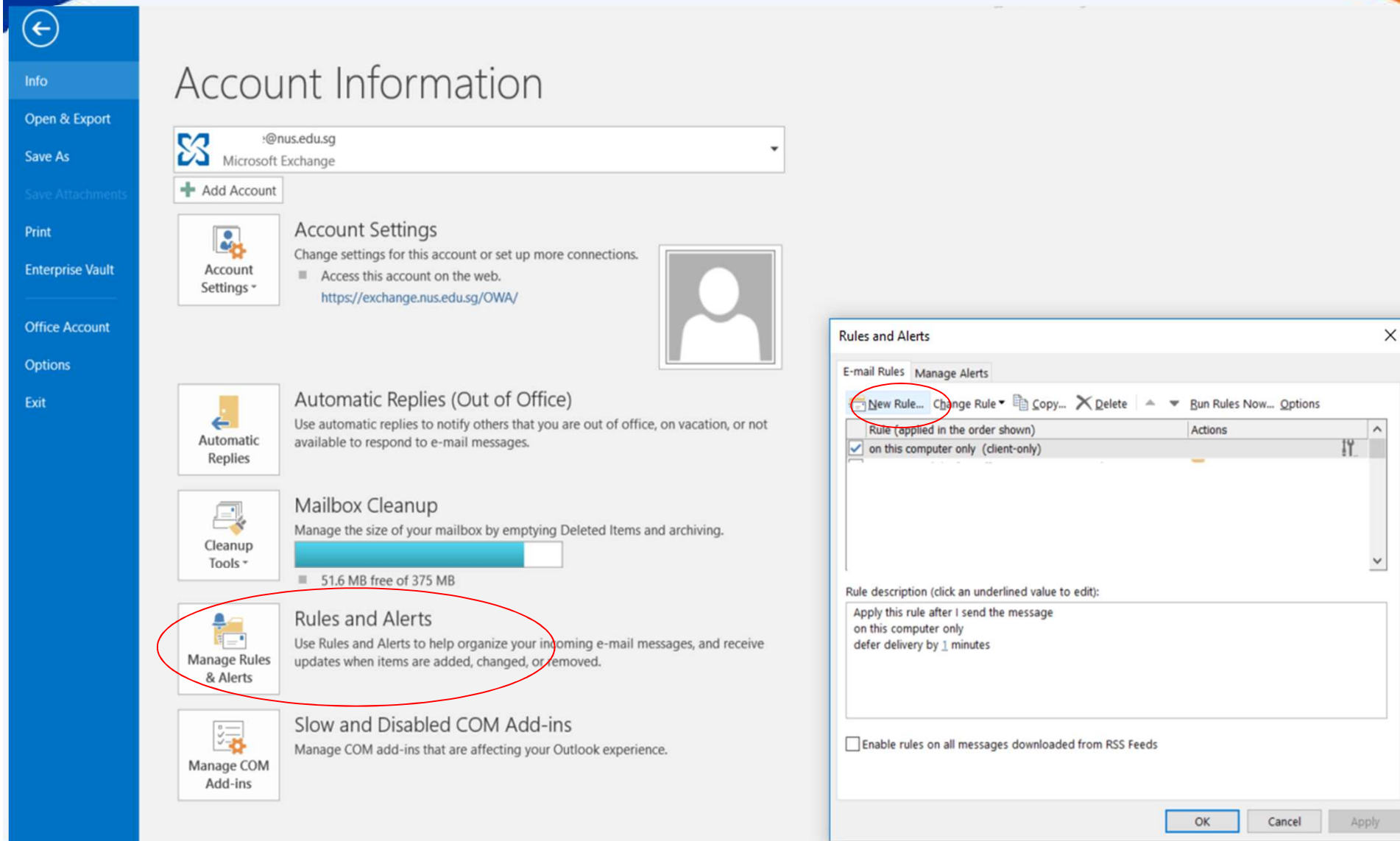
# Encrypt Files with Password using Winzip

Configure your Winzip encryption settings to AES 256



# Deferment of Email Delivery

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



The screenshot shows the Outlook 'Account Information' pane. The 'Rules and Alerts' option is circled in red. A 'Rules and Alerts' dialog box is open, showing a list of rules. The rule 'on this computer only (client-only)' is selected, and its description is visible below. The 'New Rule...' button in the dialog is also circled in red.

**Account Information**

Info  
Open & Export  
Save As  
Save Attachments  
Print  
Enterprise Vault  
Office Account  
Options  
Exit

Account Information

Microsoft Exchange

Account Settings

Automatic Replies (Out of Office)

Mailbox Cleanup

**Rules and Alerts**

Slow and Disabled COM Add-ins

**Rules and Alerts** dialog box:

E-mail Rules Manage Alerts

New Rule... Change Rule... Copy... Delete... Run Rules Now... Options

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):

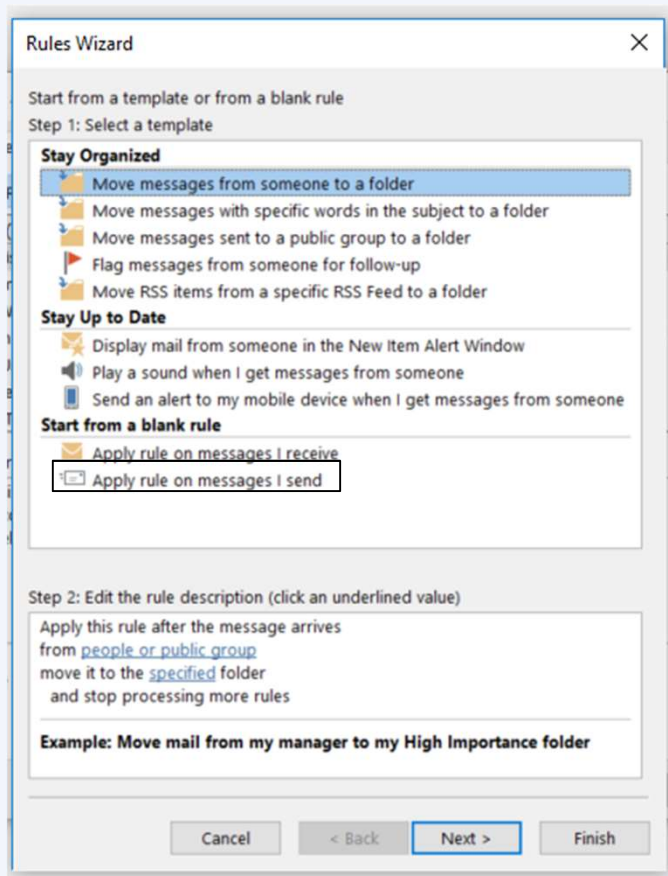
Apply this rule after I send the message  
on this computer only  
defer delivery by 1 minutes

Enable rules on all messages downloaded from RSS Feeds

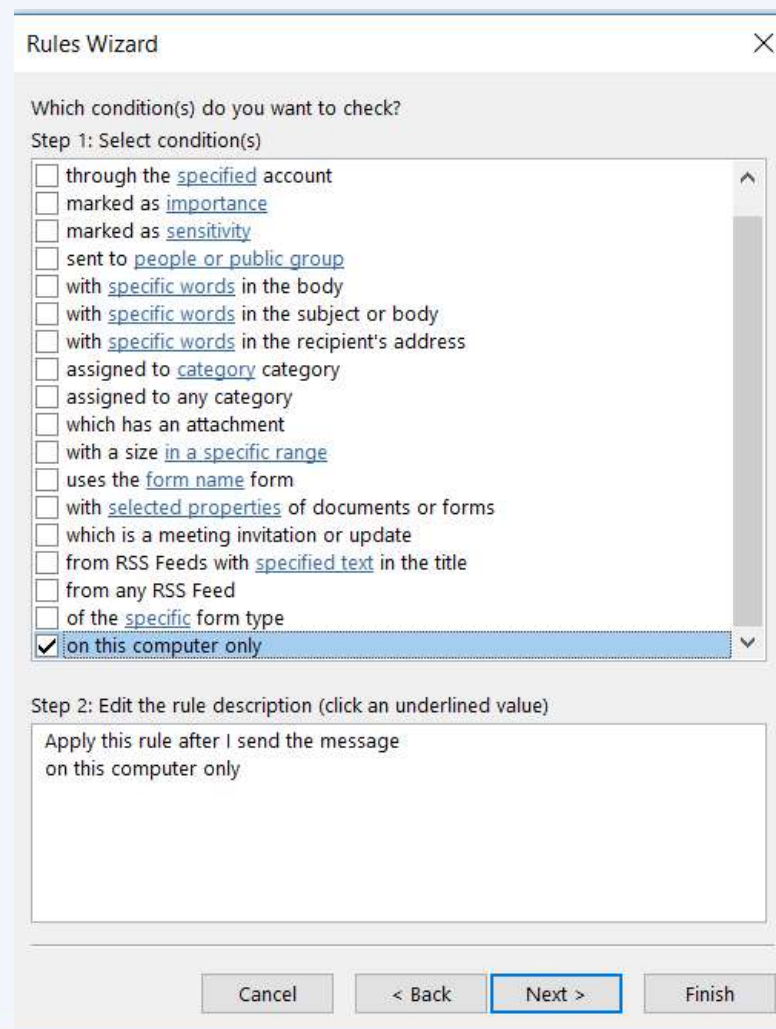
OK Cancel Apply

# Deferment of Email Delivery

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

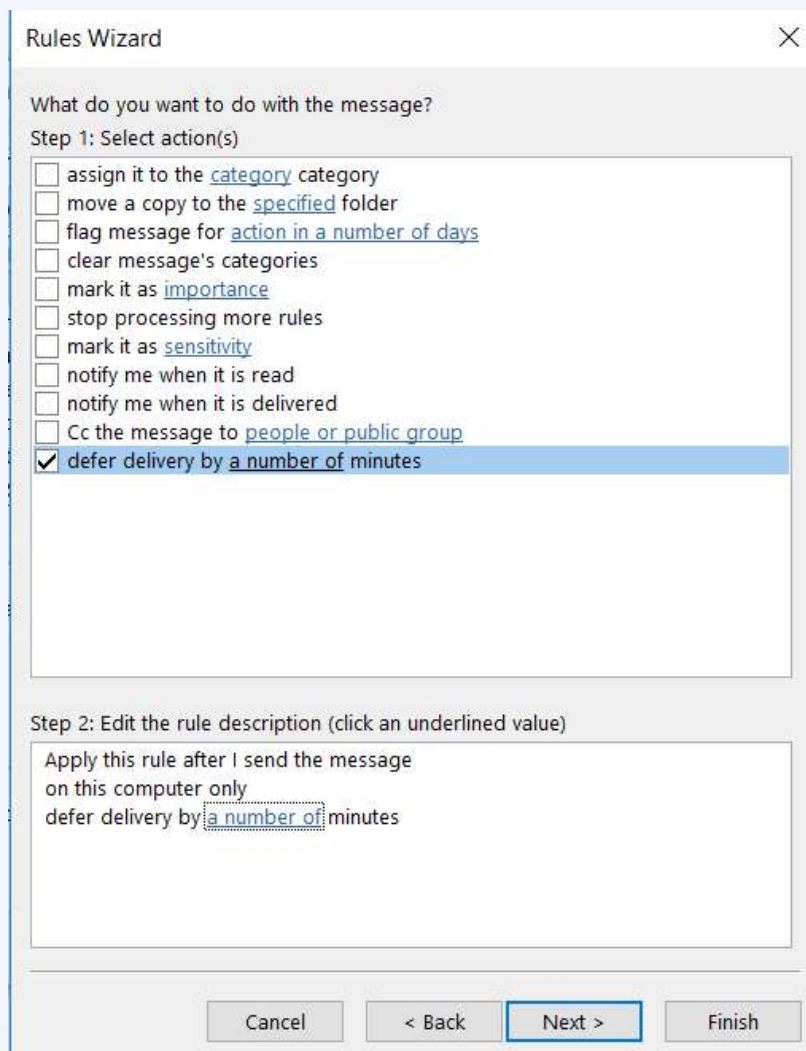


Select the option, “**Apply on this computer only**”. Click the button, “**Next**”



## 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



# 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

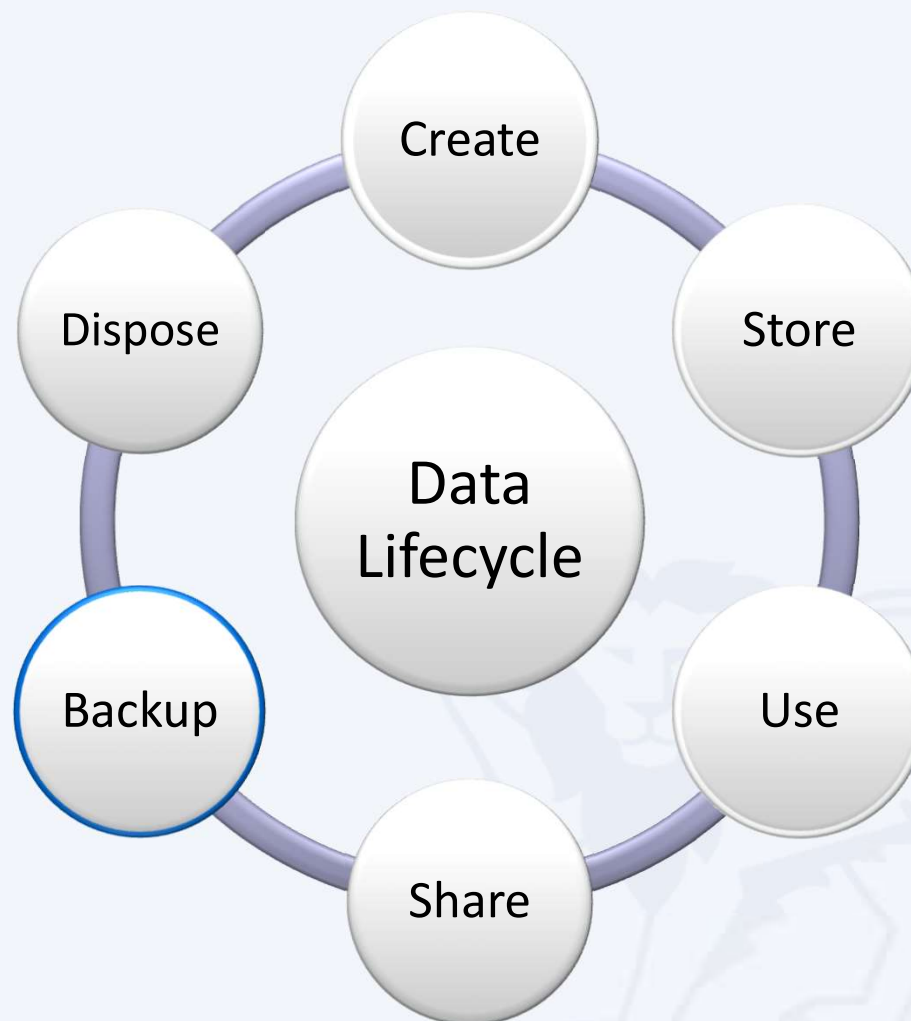
Source: <https://nusit.nus.edu.sg/its/resources/bitlocker/install-bitlocker/>

### 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**

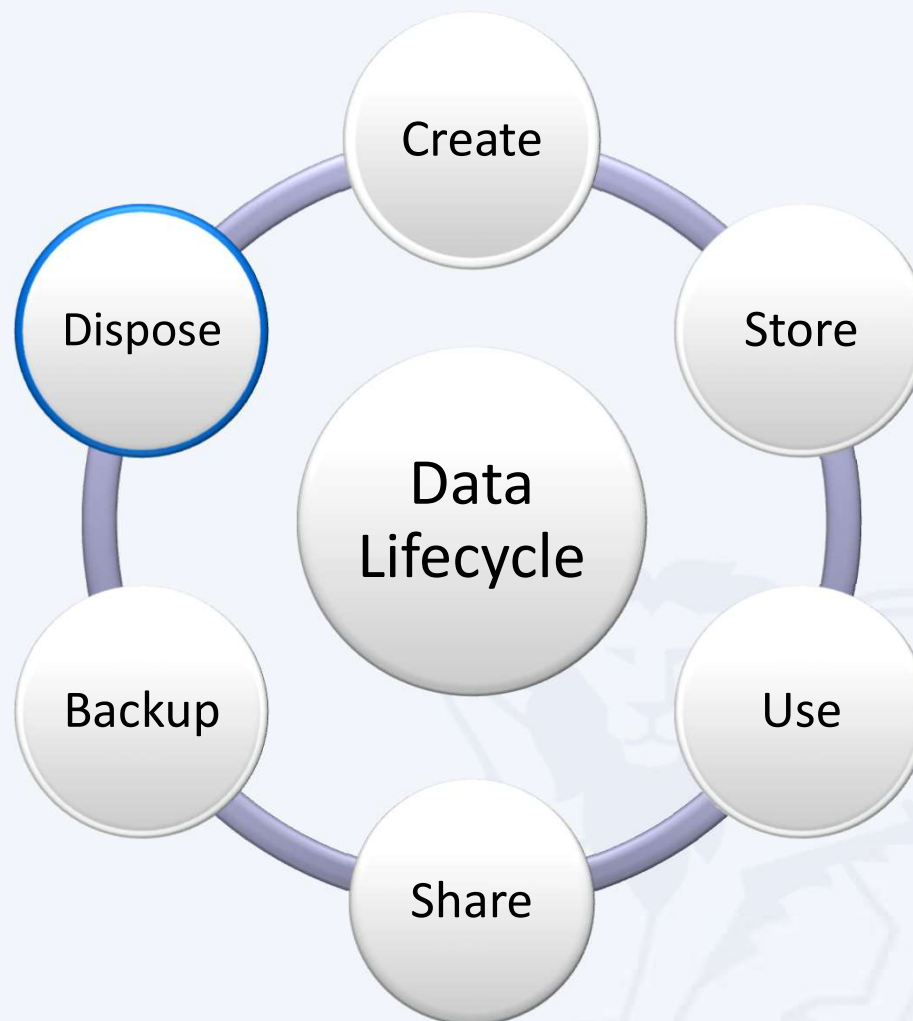
## nBox at a Glance

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

[https://nusit.nus.edu.sg/services/online\\_storage/nbox/](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](mailto: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](mailto:cceda@nus.edu.sg)**

# Q&A

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





# Supplementary Slides



# Information Security Policies FAQ



Think Good practice  
Implement Good practice  
Protect our Data and System





# Can I use Google Email for Official correspondences?

**Answer: No, with 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.**



# Can I share my user account and password?

**Answer: No, you are liable for all actions performed using the account. AUP Clause 5.1.**

## **5. Specific Uses Of IT Resources**

### **5.1 Personal Responsibility**

(i) Users shall not reveal their login, passwords and NUS Smartcard PIN to anyone.

# 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



# Can I use Shareware?

**Answer: Most shareware are free for personal use and not for commercial use. For example, malwarebyte and Ccleaner. Read the terms and conditions to verify.**

## Software Audit Circular dated 20<sup>th</sup>Oct2016

### 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.

## Department Software License Report

<https://staffportal.nus.edu.sg/staffportal/it/software/software.html#5>

### Department Report

The department report shows a complete list of software installed in all computers tagged to the users in a department. Department/faculty will be able to review and ensure that software license installations comply with the number of software licenses purchased. The report is available for Head of Department (HOD) and designated staff to access. The designated staff refers to the previously nominated staff in Altiris system. If your department requires additional access, please obtain HOD's approval and email to [Software Administrator](#).

Follow the steps below to generate department report:

1. Go to <https://www.nus.edu.sg/swr/login.aspx>
2. If you are using Internet Explorer, click **Login**. Otherwise, sign in using your NUSNET ID in nusstf\userid format and click **Login**.
3. Click **Report** -> **Department** tab on navigation bar



Clause 3.1 Faculty Deans and Heads of Departments (HODs) are responsible for ensuring that all software used within the faculty or department and stored on computers in the faculty or department have been properly obtained and are being used within the terms of the software license.





# 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).

## 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.



# 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.