



IT Security Awareness Briefing

By NUS IT

Aug 2018 @ MD1

Outline

1. Personal Data Protection Act
2. Cyber Attack - Phishing Techniques
3. Best Practices



Personal Data Protection Act



AUP & 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

Personal Data Protection Act

The Personal Data Protection Act 2012 (the “PDPA”) establishes a general data protection law in Singapore which governs the collection, use and disclosure of individuals’ personal data by organisations.

Examples of Personal Data: NRIC, Name, Address, Contact Number, Medical records, Financial records

<https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/finaladvisoryguidelinesonpdpaforselectedtopics28march2017.pdf>

[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)



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

| APR 28, 2017, 2:55 PM

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 authorisation.

The spreadsheet was created for the college's freshmen orientation camp in 2016, which was led by student leaders.

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 tasked to help run the camp.

It was found that an unknown party had changed the setting on the spreadsheet to "share using a link".

As a result, any user with the URL link will have access to the spreadsheet and the personal data in it, possibly exposing such information to those beyond the university, wrote PDPC deputy commissioner Yeong Zee Kin



How does PDPA applies to me?

Answer: I need to handle personal data provided by NUS with care.





How do I protect data on my thumb drive?

Answer: Encrypt the data on thumb drive using Bitlocker.

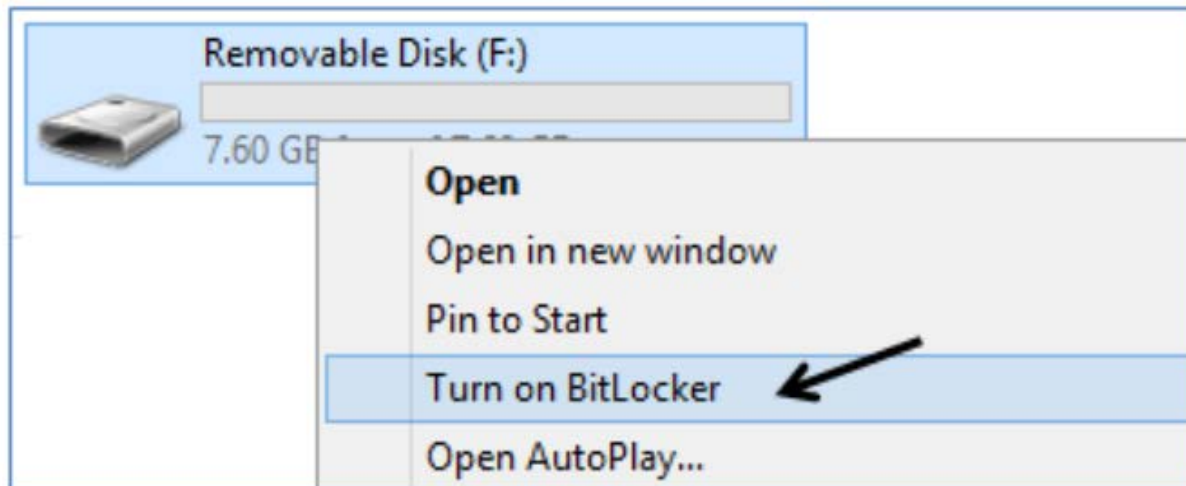


Enable Bit Locker

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

Window 10

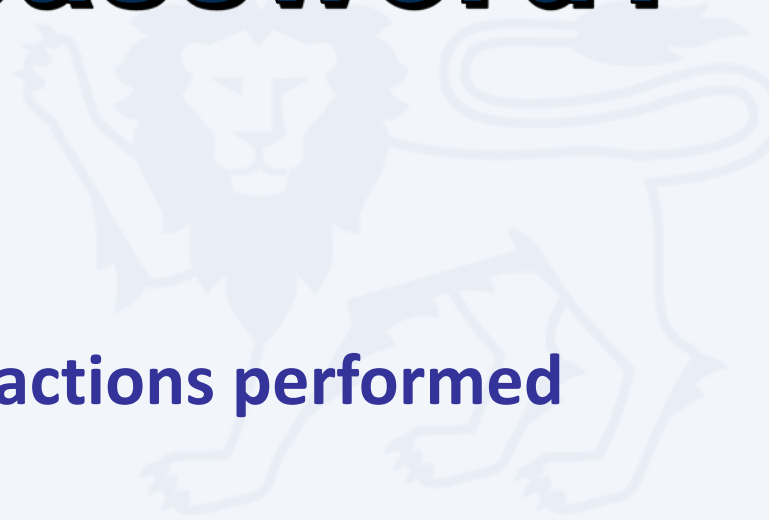
1. Insert your thumbdrive into your computer.
2. Go to Computer and look for the drive letter assigned to your thumbdrive.
3. Right-click the drive and select Turn on BitLocker.





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

Phishing Threats



“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 getting more sophisticated

DBS warns of phishing site targeting bank customers

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

From: customerservice@posbbank.com.sg

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

To:

Subject: Security Update

This is not a DBS/POSB email
address



Dear Customer,

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

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

Link to phishing
website

Sorry For any inconvenience this may have caused you.

Thank you for using POSB Bank.

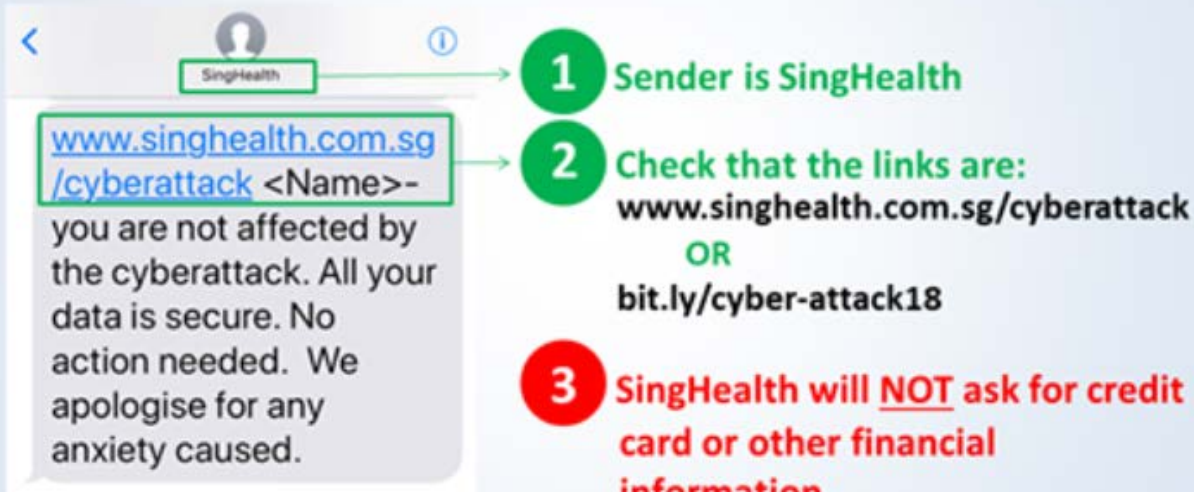
Kind regards,
Posb Bank Ltd.

T

Phishing via SMS

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

If you are not affected by the cyberattack:



The image shows a screenshot of an SMS message from SingHealth. The message text is: "you are not affected by the cyberattack. All your data is secure. No action needed. We apologise for any anxiety caused." A link is provided: www.singhealth.com.sg/cyberattack <Name>. To the right of the screenshot, three numbered steps are listed:

- 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.”

How to verify if a website is malicious?

<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!



Can Phishing email be sent from familiar email account?

Answer:

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

Phishing Reporter Button Launch

SERVICE ENHANCEMENT

NUS INFORMATION TECHNOLOGY

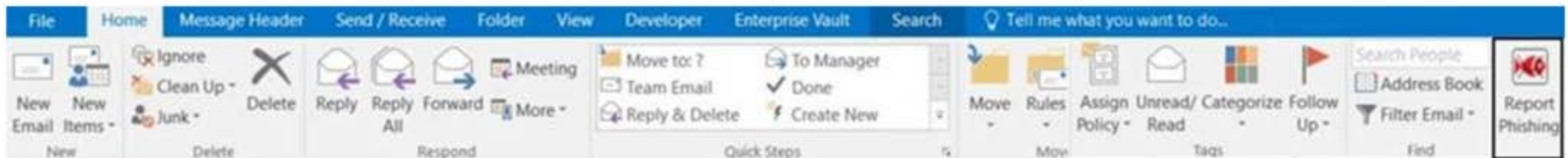
*This email is sent to all NUS Staff

Dear Colleagues,

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

For Windows Users

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



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

For Mac Users & Web Outlook Users

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

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.

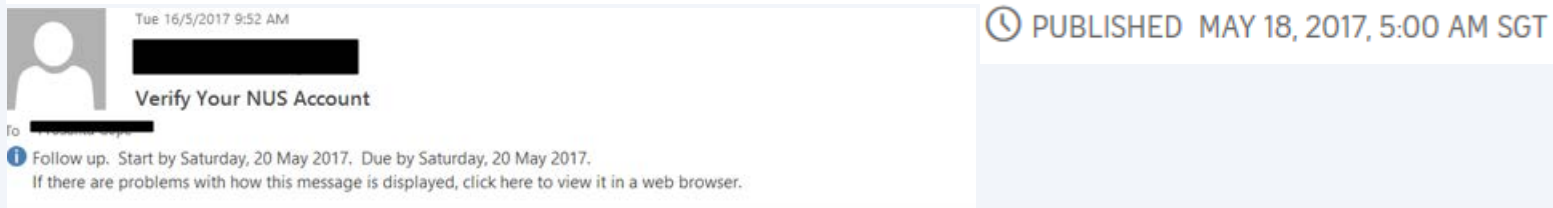


Image included directly from NUS website

Your NUS email account has been blacklisted and you are required to verify your account.

Click link below to verify

<http://aldeiadeemaus.com.br/nus/nuswebmail.html>
Click or tap to follow link.

Mouse over link show non NUS website

[Click Here to Verify >>>](#)

Sincerely,

NUS Admin Team

© National University of Singapore

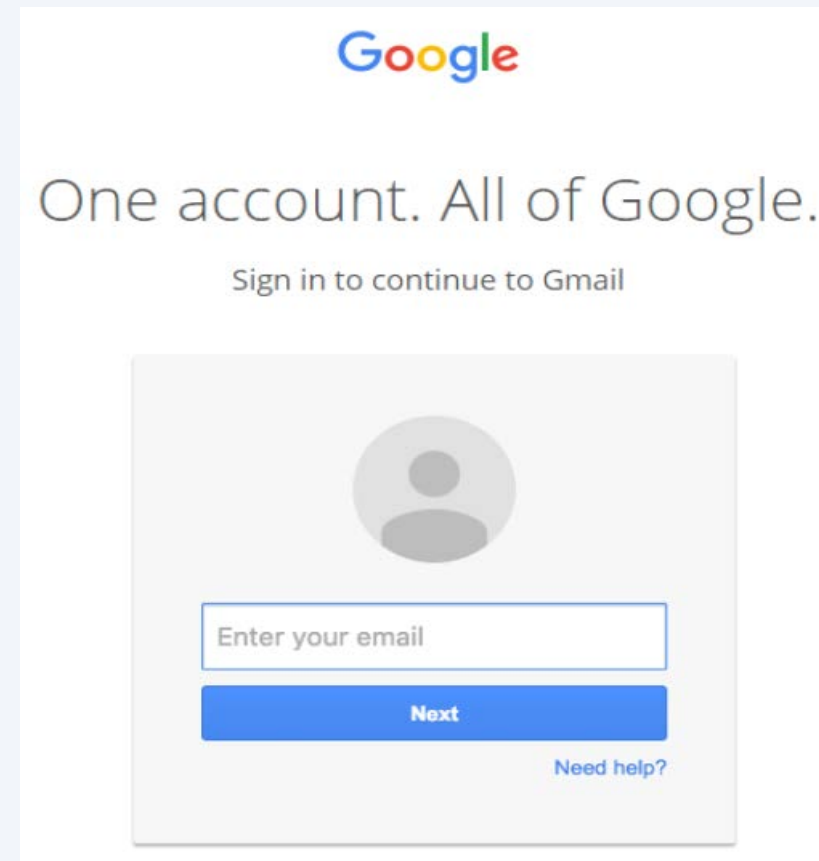
Valid NUS website address

Evolving Phishing Email Techniques

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

Wide Impact: Highly Effective Gmail Phishing Technique Being Exploited

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



**Phishing email
targeting NUS**

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

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

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

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

Unable to show this message

[Click here to view message](#)

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



Spot a Phishing Email in 3 steps



1

Are you expecting the email?

2

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

subdomain e.g. organization directory

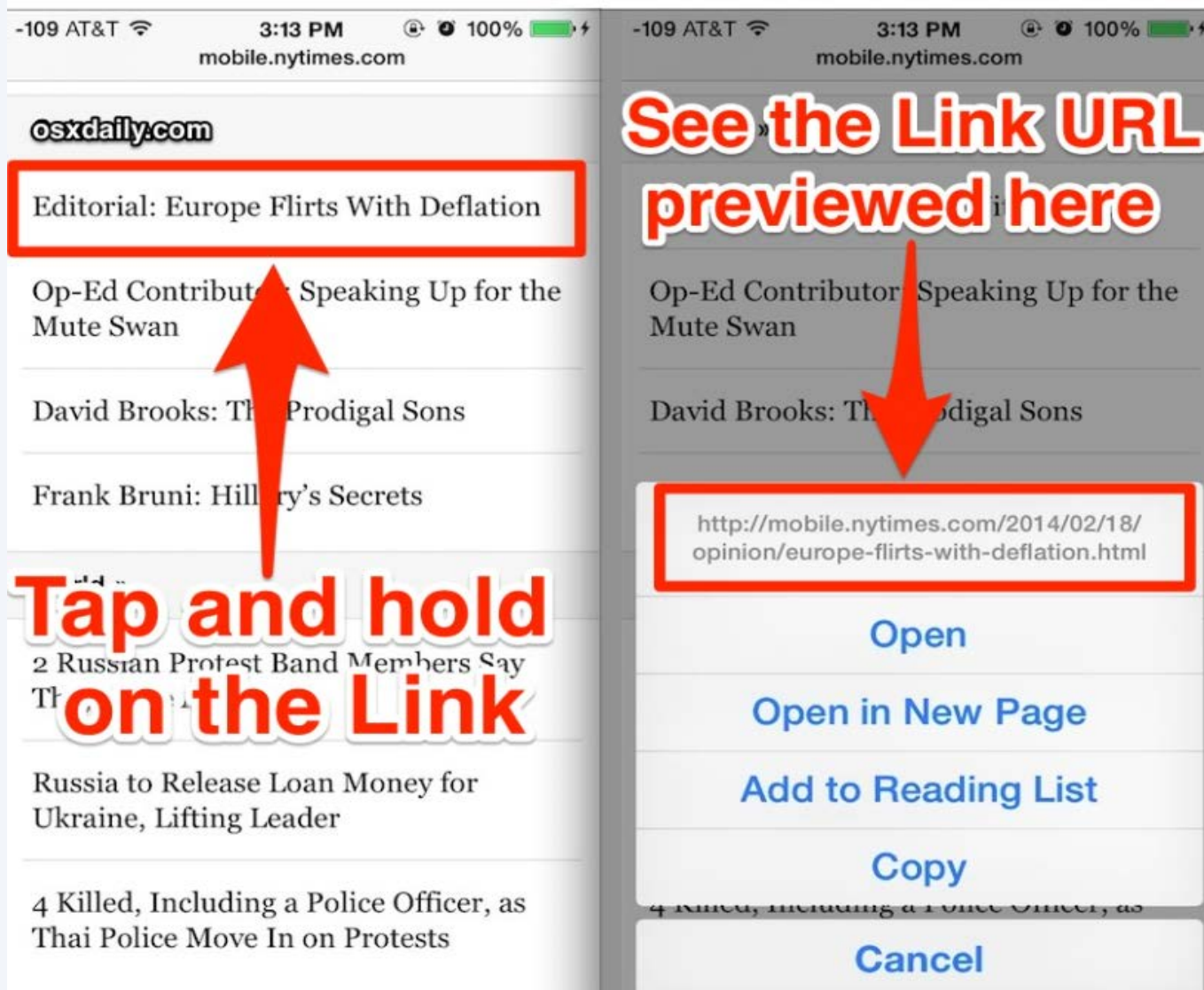
<http://pages.example.com/archive/index.html>

protocol domain e.g. industry or country filename

3

Use link checker to check if the links are safe.

How to mouse over link on mobile phone?



osxdaily.com

Editorial: Europe Flirts With Deflation

Op-Ed Contributor Speaking Up for the Mute Swan

David Brooks: The Prodigal Sons

Frank Bruni: Hillary's Secrets

Tap and hold on the Link

See the Link URL previewed here

Op-Ed Contributor Speaking Up for the Mute Swan

David Brooks: The Prodigal Sons

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

Open

Open in New Page

Add to Reading List

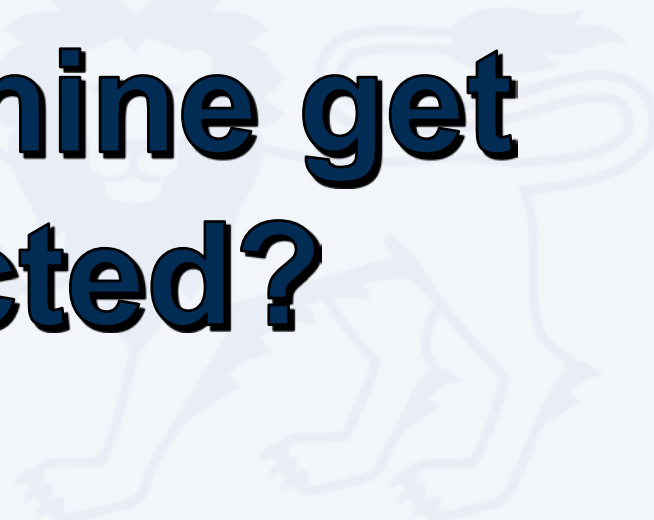
Copy

Cancel

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

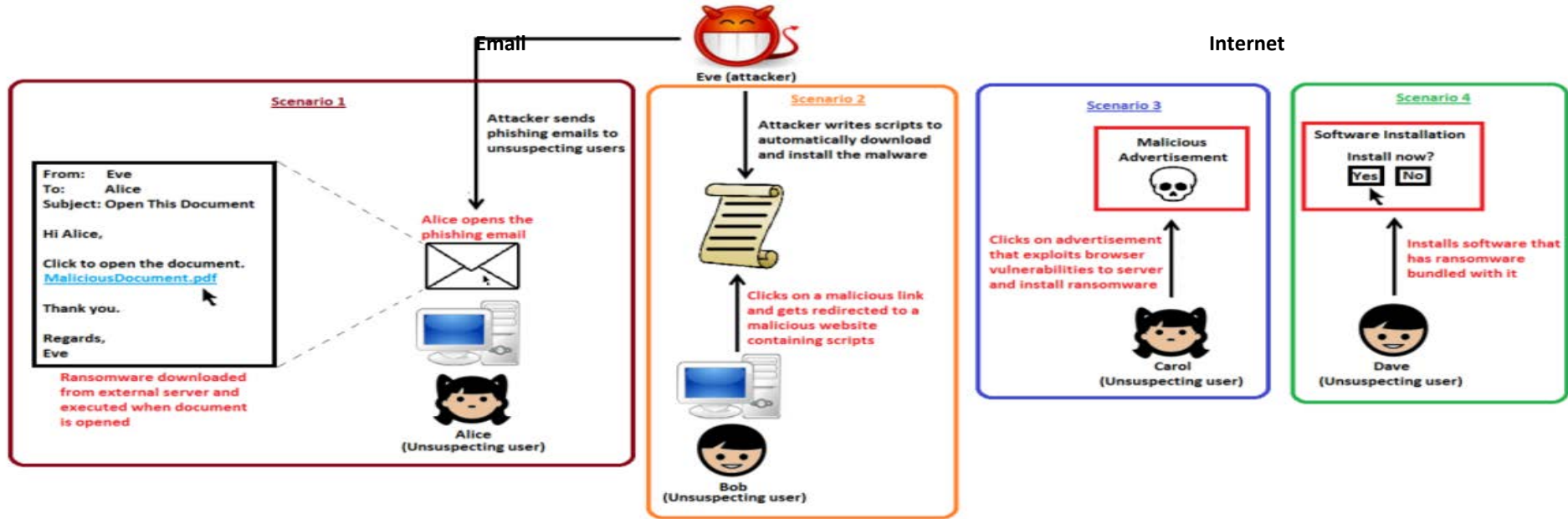


**How did my
account get
compromised
or machine get
infected?**



Sources of Malicious Software

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



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

~ kaspersky

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

kaspersky

...Beware of Fake Apps

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

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



App Title – Developer

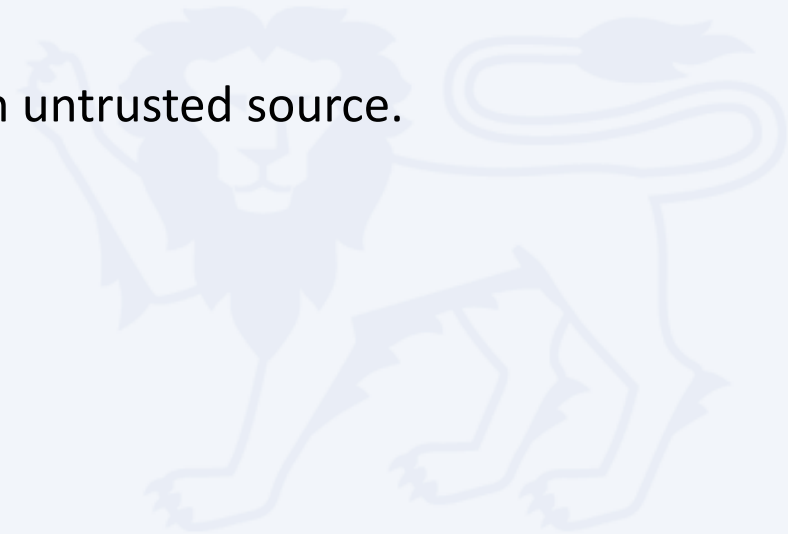
- 360 Antivirus Clean Mobile – SmartAPP
- 360 Security – Antivirus Boost – 360 Mobile Security Limited
- Ace Security-Antivirus Aplock – Super Security Tech
- Android Antivirus 2016 – HappyAPP11 Studio
- Antivirus – Master VPN
- Antivirus & Mobile Security – Topi Maxi Group
- Antivirus Clean – AVC Security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

Protection Measures

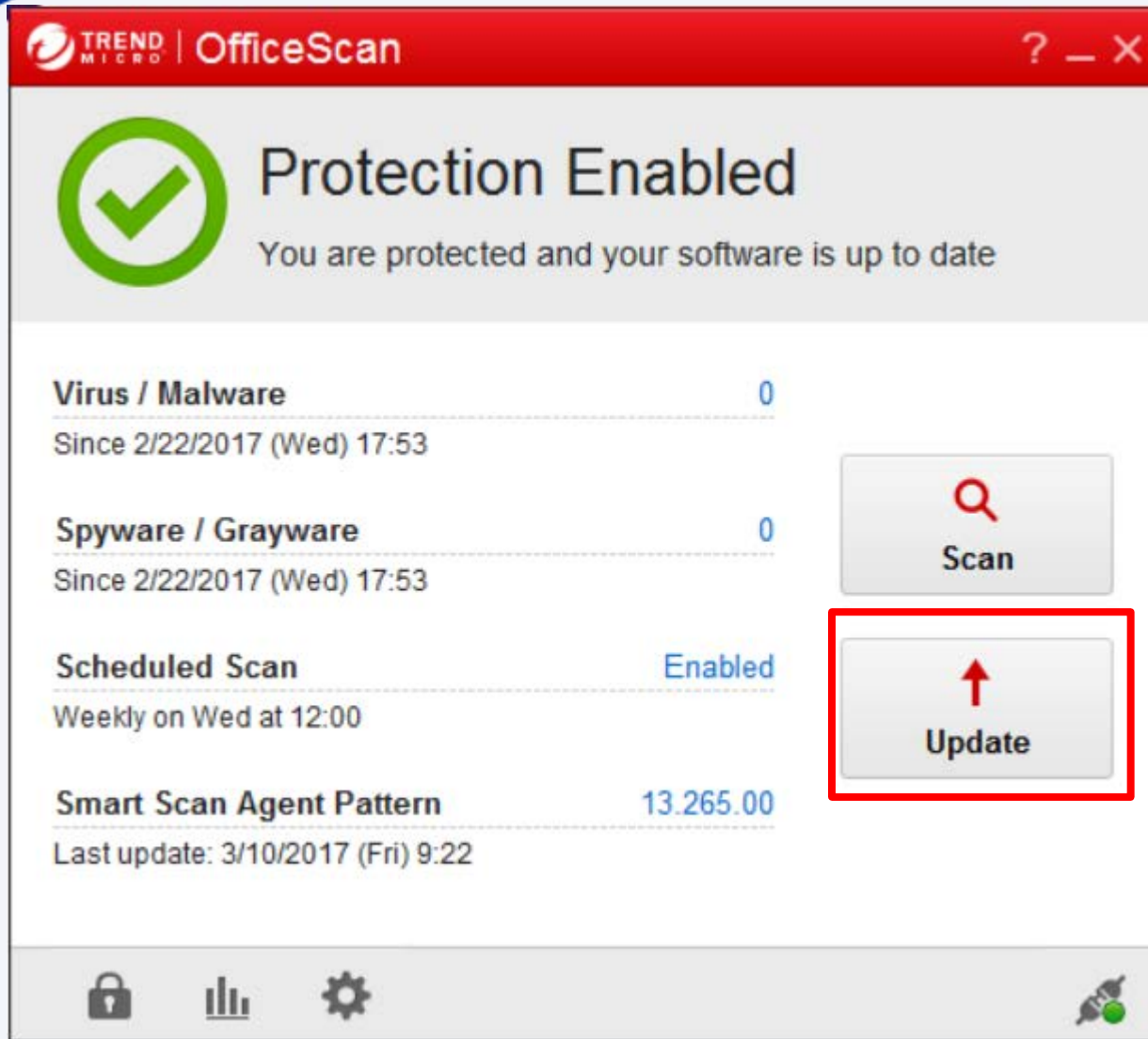


What are the best practices?


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



University Virus Scanner



TREND MICRO | OfficeScan ? _ X

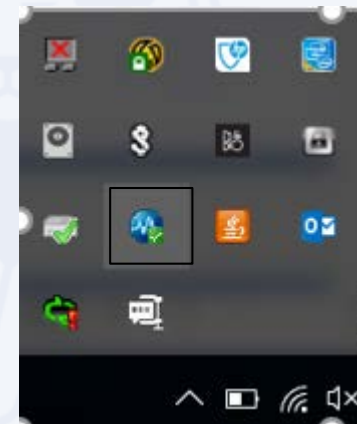
 **Protection Enabled**
You are protected and your software is up to date

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

Scan (magnifying glass icon)

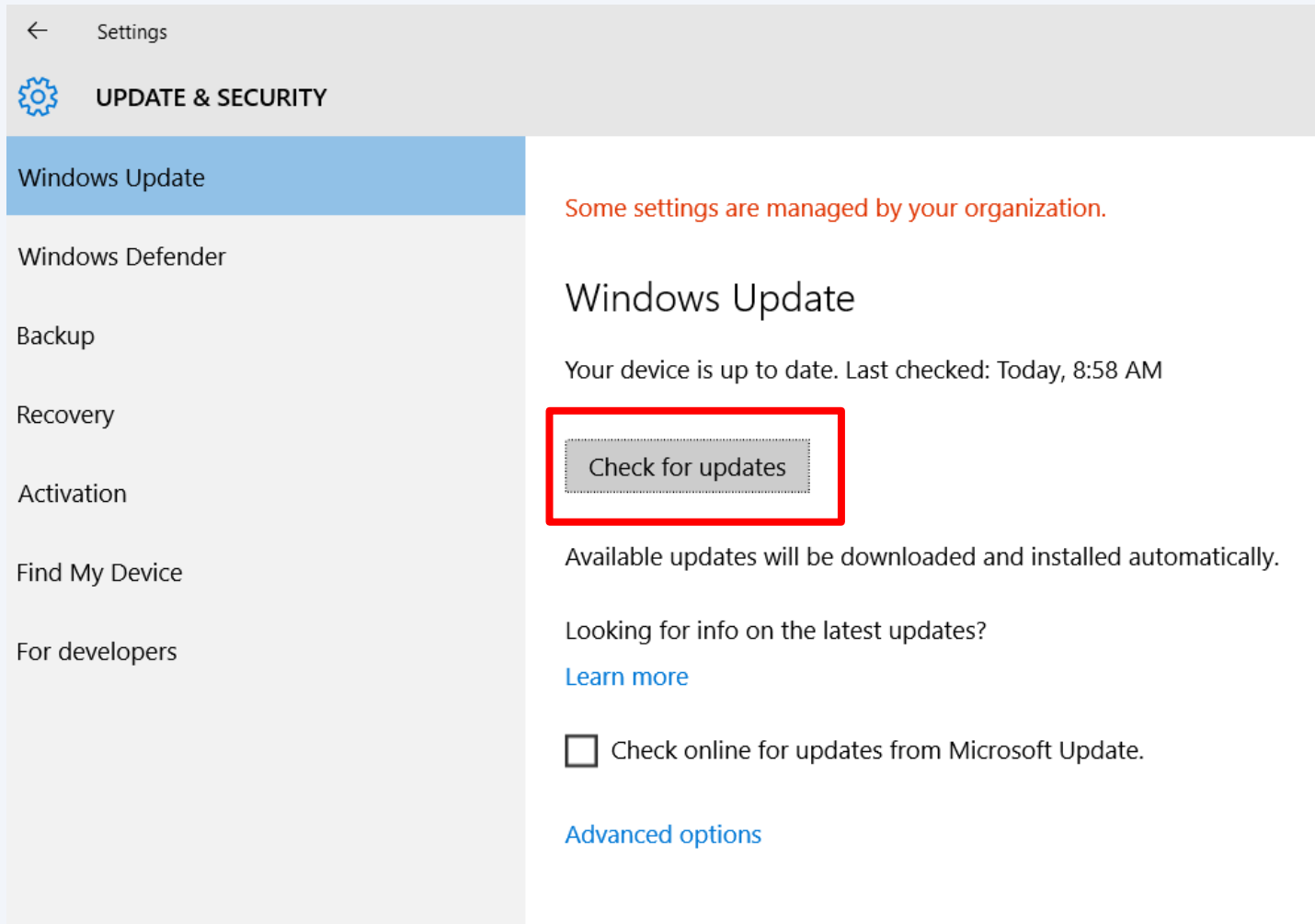
Update (upward arrow icon)

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



Window OS Updates

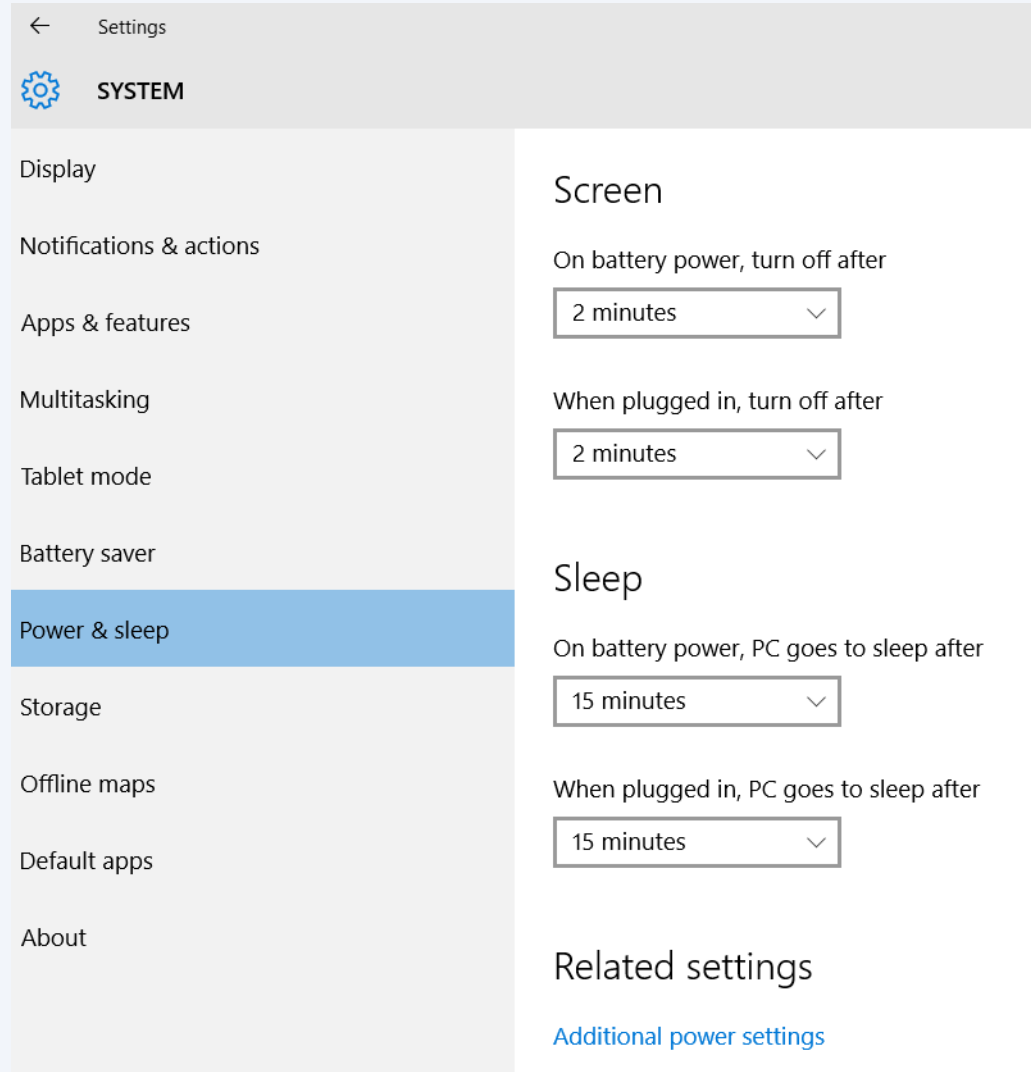
Settings\ Update and Security



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 displays the 'Windows Update' settings. At the top, a message states 'Some settings are managed by your organization.' Below this, the title 'Windows Update' is shown, followed by the status 'Your device is up to date. Last checked: Today, 8:58 AM'. A 'Check for updates' button is prominently displayed and highlighted with a red rectangular border. Below the button, it says 'Available updates will be downloaded and installed automatically.' There is a link for 'Learn more' and an unchecked checkbox for 'Check online for updates from Microsoft Update.' At the bottom, there is a link for 'Advanced options'.

Window Screen Lock

Settings\ Personalization\ Lock Screen



The screenshot shows the Windows Settings application. The left sidebar contains the following categories: Settings, SYSTEM, Display, Notifications & actions, Apps & features, Multitasking, Tablet mode, Battery saver, Power & sleep (highlighted), Storage, Offline maps, Default apps, and About. The main content area is titled 'Screen' and contains 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 for '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

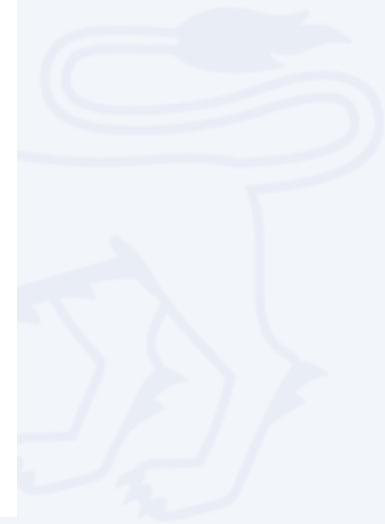
15 minutes

When plugged in, PC goes to sleep after

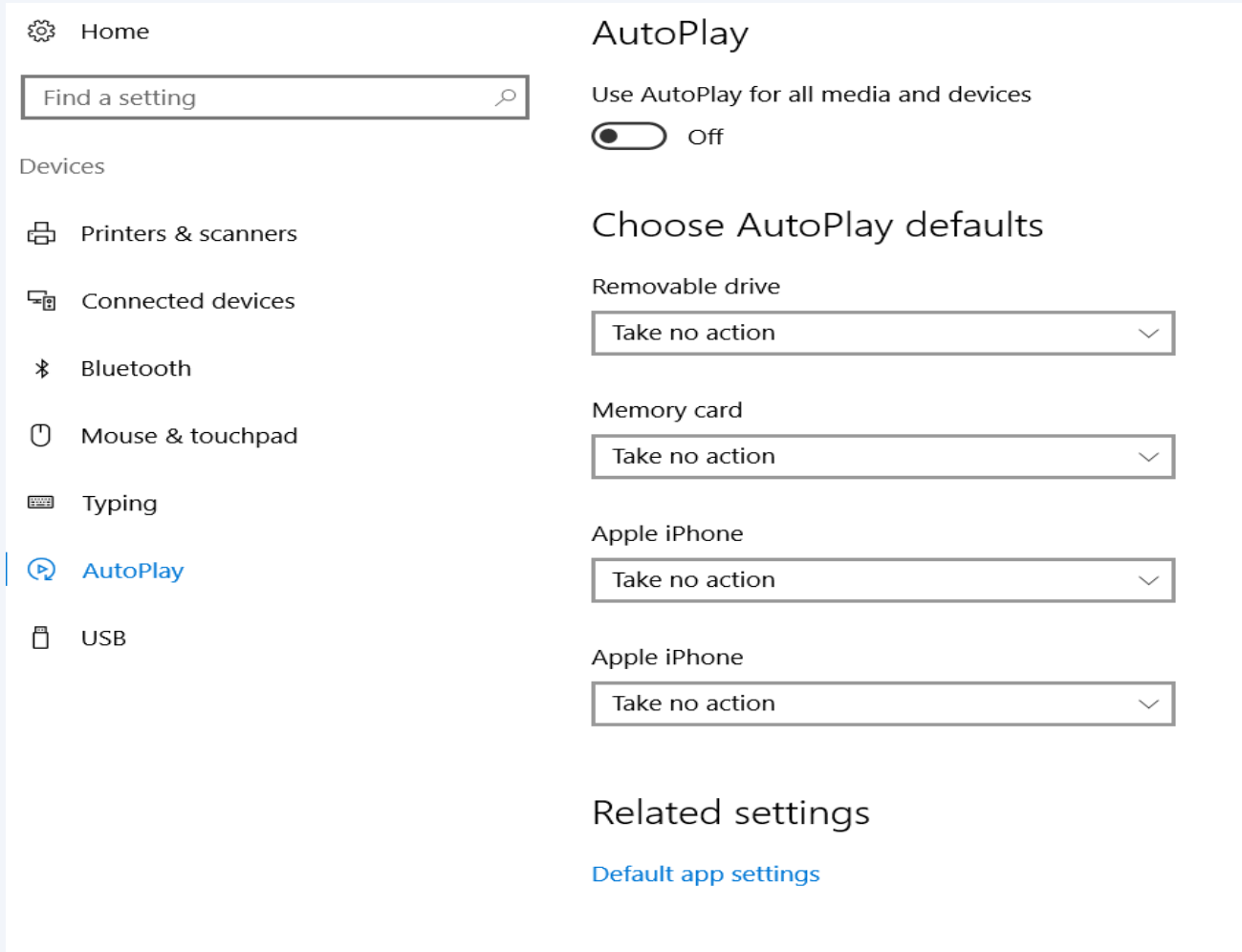
15 minutes

Related settings

[Additional power settings](#)



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 on the right is titled 'AutoPlay' and contains the following elements:

- A search bar at the top with the placeholder text 'Find a setting'.
- A section titled 'Devices' with a list of categories: Printers & scanners, Connected devices, Bluetooth, Mouse & touchpad, Typing, **AutoPlay** (selected), and USB.
- The 'AutoPlay' settings section, which includes:
 - A toggle switch for 'Use AutoPlay for all media and devices', currently set to 'Off'.
 - A section titled 'Choose AutoPlay defaults' with three dropdown menus:
 - 'Removable drive' set to 'Take no action'.
 - 'Memory card' set to 'Take no action'.
 - 'Apple iPhone' set to 'Take no action'.
 - A second 'Apple iPhone' dropdown menu, also set to 'Take no action'.
- A 'Related settings' section with a link to 'Default app settings'.

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

Edge Browser Settings

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

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

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

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

Save form entries
 Off

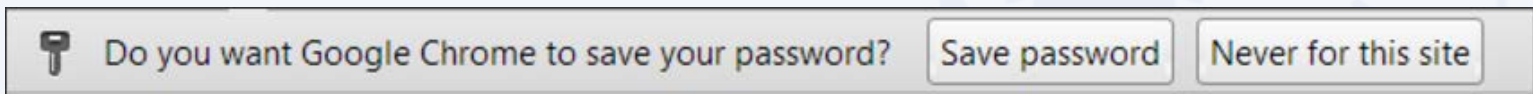
2 Cookies
Block only third party cookies

3 Advanced settings

Block pop-ups
 On

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.



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

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.

