



**NANYANG
TECHNOLOGICAL
UNIVERSITY**
SINGAPORE

Module 03: Managing Cybersecurity



Learning Objectives

By the end of this lesson, you will be able to:

- Explain how we can detect phishing to prevent its negative consequences
- Identify what makes a password strong to avoid hacking
- Illustrate what is data security and the four levels of data classification
- Adopt safe practices as an IT user, especially when sending emails and in public Wi-Fi networks

How is Cybersecurity important to us?

- From the recent world economy forum risk report 2021, cyber risk continue to be ranked among the global risk like pandemic and climate changes. The COVID 19 pandemic has accelerated technology adoption but at the same time exposing us to more cyber threats.
- We live in an era there has been an unprecedented amount of data that being collected, processed and stored on device or clouds services. As such, cybersecurity plays an important role in securing that works or any other digital infrastructure that we use from unauthorised access or even malicious attacks.
- With cybercrime damages projected to reach 10.5 trillion USD by year 2025, Government agencies organisation across the world are investing in Cybersecurity infrastructure to protect their business and millions of users trust them with their data.
- Not only donations and businesses face threat from the action and intension of hackers, individual personal sensitive information such as intellectual property, financial data can be stolen as well. This can be sold for profit compromising personal safety of an individual or his or her family. For example, there has been incidence of hackers attacking household cameras, devices invading people's privacy.
- In this module we will touch on topic on what individual can do to protect our data and how organisation including NTU have step up to prevent cyber-attack.



Do these headlines ring a bell?

Such headlines have become common place as cyber security incidents spike.



NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE

Phishing



Phishing

The internet is an ideal place for hackers to lurk and target unsuspecting victims

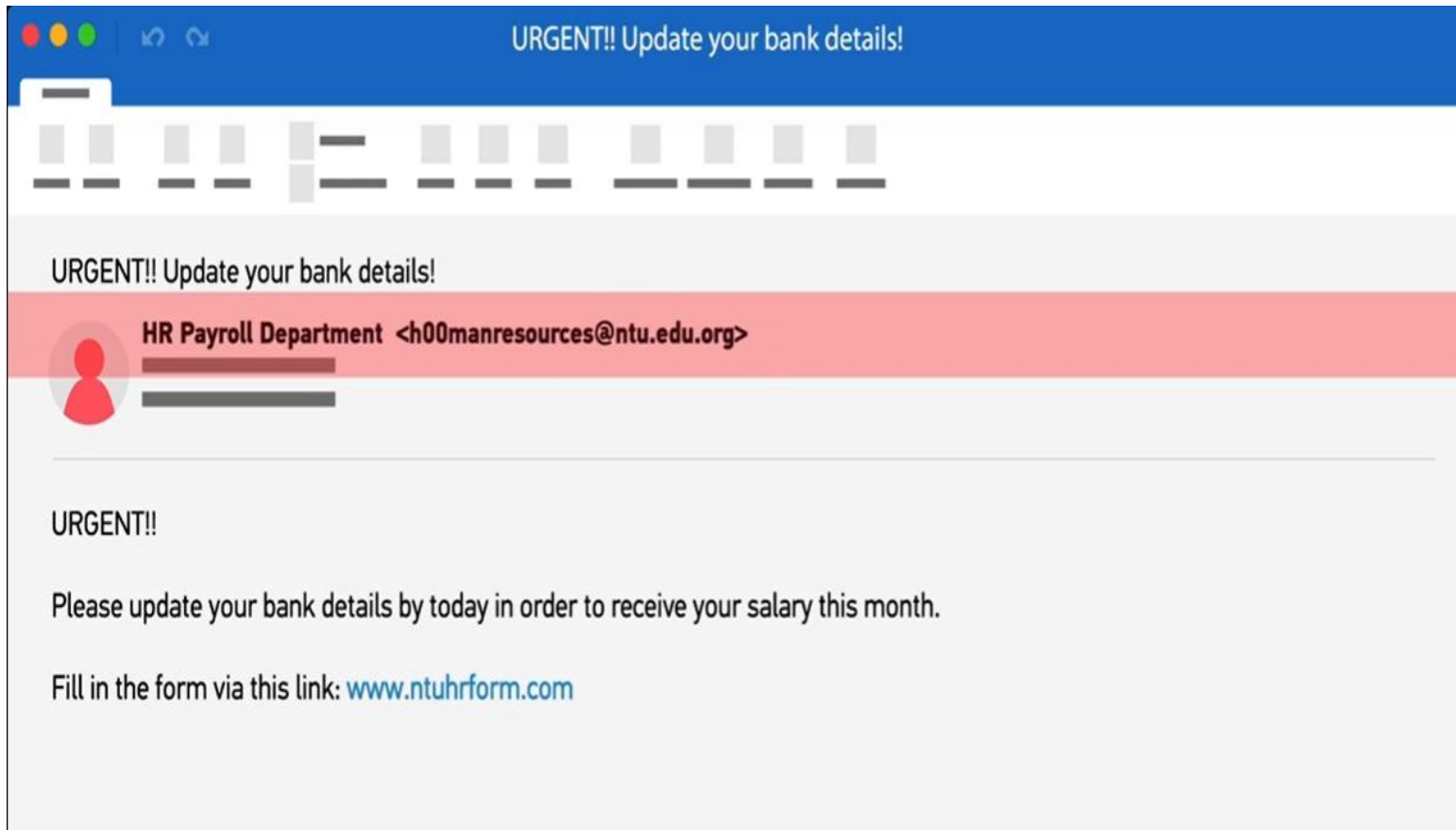


In 2018 alone, more than 16,100 phishing cases occurred

16,099
PHISHING LINKS IN 2018

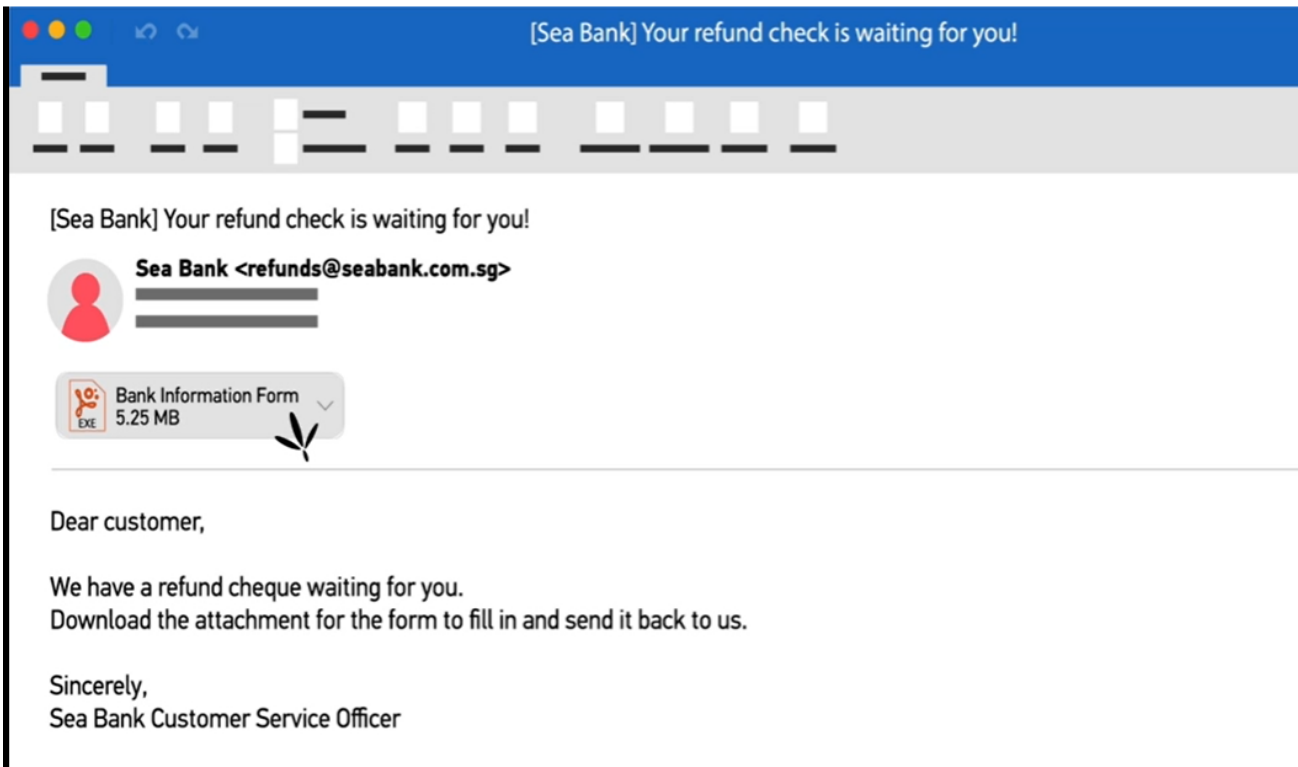
Cyber Security Agency of Singapore. (2019). Singapore Cyber Landscape 2018.
Retrieved from <https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2018>

Phishing: How you can detect and prevent phishing attacks

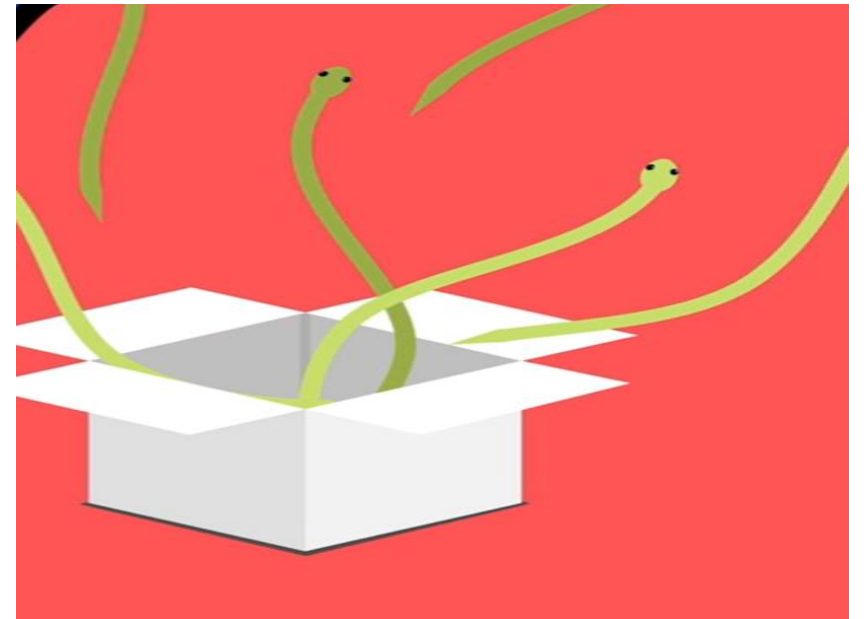


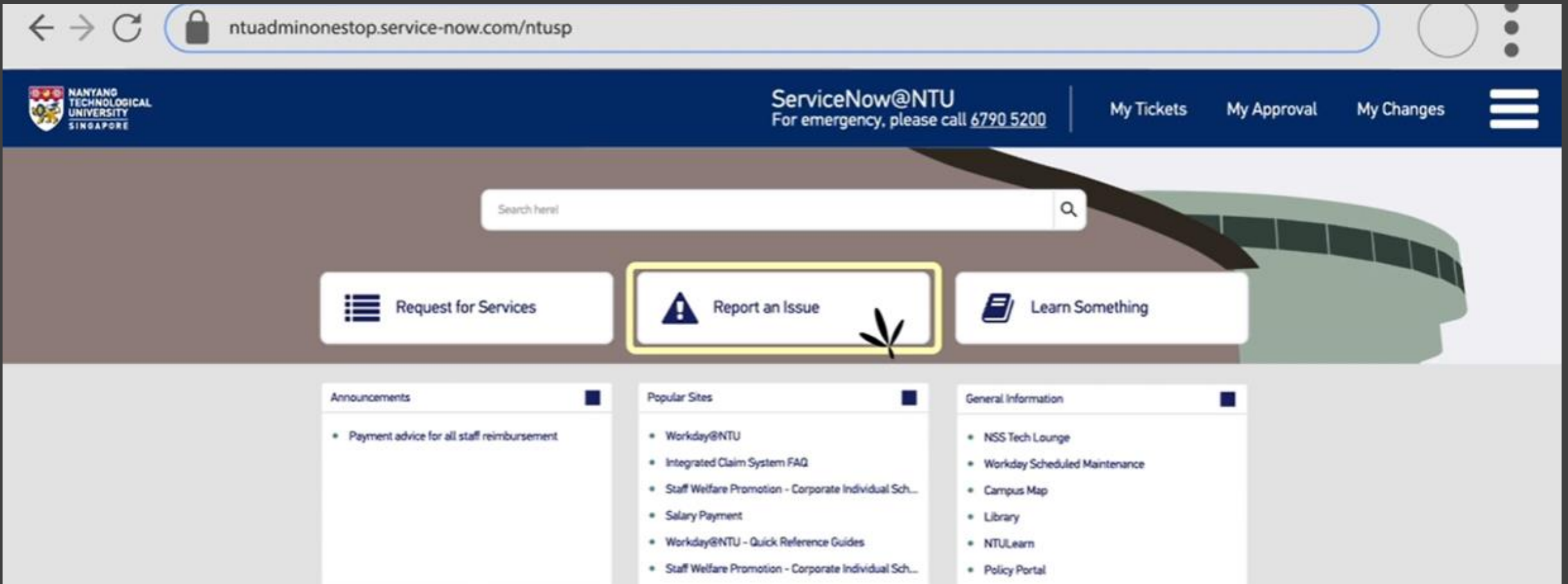
- When receiving an email, always be cautious and check who the sender is. There might be predators who are on the hunt for your precious personal information.
- Be cautious before you click on any hyperlinks in your emails, they can be dangerous.

Phishing: How you can detect and prevent phishing attacks



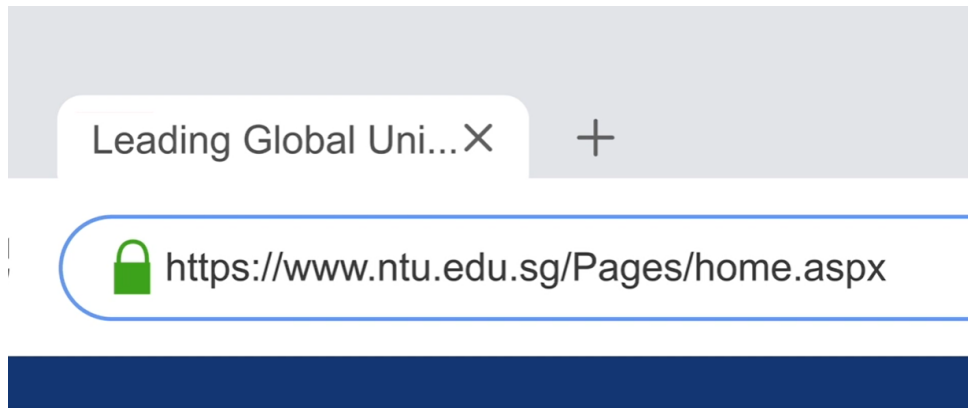
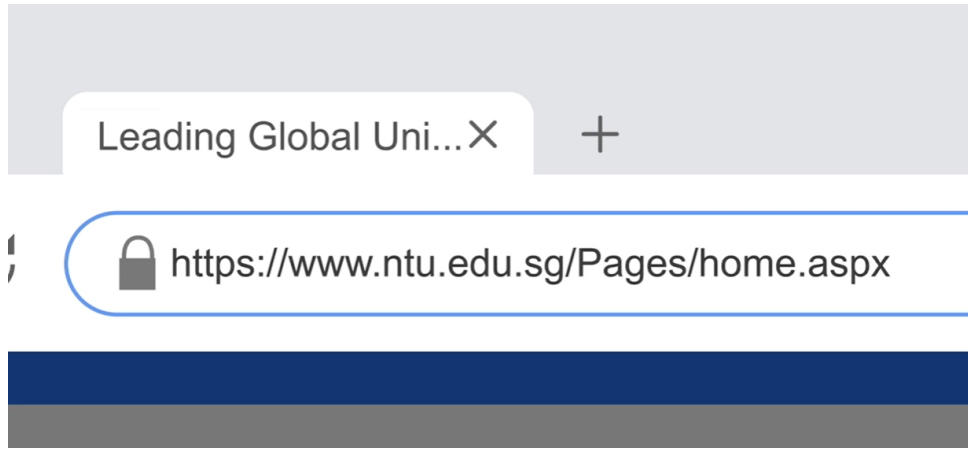
- Receiving unknown email attachments are like receiving suspicious packages.
- They might contain malware.





Phishing: How you can detect and prevent phishing attacks

- When everyone is vigilant, we can minimise the threats.
- If you receive a suspicious email, you should report it to ServiceNow@NTU.
- It's also wise to delete the email and do not forward it to your friends or colleagues.



Phishing: How you can detect and prevent phishing attacks

- Hackers gather your personal information to use them with bad intentions.
- It is prudent to type in the correct address yourself to make sure that you are viewing the actual website.
- As a precaution, look out for the lock icon in the address bar and ensure that the web address starts with “https”.

Phishing: How you can detect and prevent phishing attacks

- Learning to protect ourselves in the cyber space may seem daunting. An additional way to keep ourselves cyber safe is to understand the concept of C.I.A.

C I A

Phishing: How you can detect and prevent phishing attacks

- “C” is for confidentiality – protect your personal information and share only what is necessary.
- “I” is for Integrity – Practise good cyber hygiene and beware of fake sources of information.
- “a” is for availability – Prevent getting locked out of your devices and your actions can affect others.

The letters 'C', 'I', and 'A' are displayed in a large, bold, sans-serif font, spaced out horizontally. They are dark gray and set against a white rectangular background.

Remember

Cyber security is everyone's responsibility.






**NANYANG
TECHNOLOGICAL
UNIVERSITY**
SINGAPORE

Strong Passwords





Complex
password...

Easy to
remember ?

Strong Password

- Life is a little easier when we practise good password habits and consciously set up strong passwords for all our accounts.

Strong Password

Here're some suggestions on how to do this

- Ensure your passwords are at least eight characters long.
- Make your password a little bit more complex by including a mixture of numbers, symbols, upper- and lower-case letters.

Password

wG9e\$1P!

AT LEAST EIGHT CHARACTERS ✓

CONSISTS OF A MIXTURE OF NUMBERS,
SYMBOLS, UPPER AND LOWER-CASE LETTERS ✓

Password

AT LEAST EIGHT CHARACTERS ✓



Strong Password



Password

Password123

USE UNCOMMON WORDS



Password

Beartrick

DO NOT USE PERSONAL INFORMATION



Password

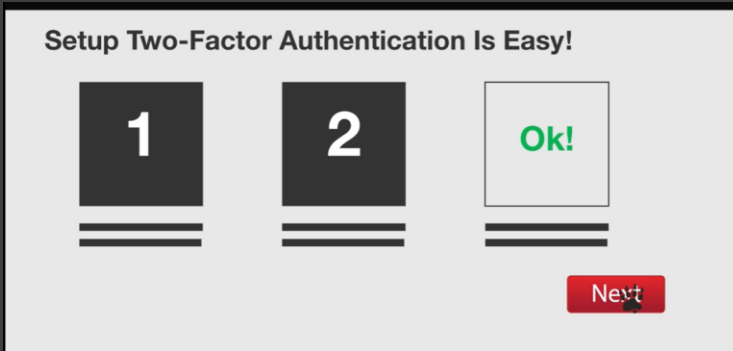
Monkey

USE UNCOMMON WORDS



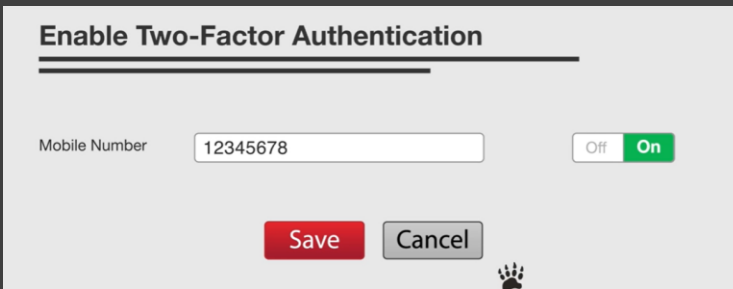
Here're some suggestions on how to do this

- Use uncommon or non-standard words in your passwords, or you could also create a password from a sentence that makes sense to you.
- It is not a good idea to use personal information that people who know you can guess.



Strong Password

- Where possible, always activate the Two-Factor Authentication.
- This could be done by enrolling your mobile number or email address to receive a one-time password, or through an authentication app





Strong Password

- It is also important to realise that despite our best efforts, hackers are still capable of hacking every password through the “brute-force” technique, when given sufficient time.
- Let’s make it harder for hackers by using a different password for each account and be sure to change them regularly.



**USE STRONG
PASSWORDS**

Take care and remember that cyber security is everyone's responsibility!



NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE

Data Security





What is Data?

- Data can be in both physical and digital formats. It can belong to an individual or an organisation.
- Organisation data – for example University's data
This includes all the information and records in the University's possession that is generated from its operations, and covers data and information disclosed by third parties working with the University.



**NANYANG
TECHNOLOGICAL
UNIVERSITY**
SINGAPORE

Classifications of Data Security





Levels of Data Security

Data is classified into four levels of security.

Levels of Data Security

Level 1 – Open

- This applies to data that can be distributed to the public or published on the internet.

Level 2 – Restrict

- Applies to any data that is generally made accessible to members of the university community but not to the public.
- Examples are internal meeting minutes, presentation files and project reports.

Level 3 – Confidential

- It applies to any data that is contractually defined as confidential or is by nature confidential.
- Such data include personal identifiable information, staff performance reports and audit reports.
- If confidential data is disclosed, the target may be subject to statutory penalties, and this causes damage to the University.

Level 4 – Classified

- Applies to any information that is covered under the Official Secrets Act. Unauthorised disclosure of such information may result in damage to national security.



BE VIGILANT

Take care and stay vigilant.

Some tips on securing data better

Pay attention to these measures

- Lock your workstation when leaving your desk
- Adopt a clean-desk policy and keep your desk clear
- Send and store work information through organisational accounts
- Keep your data storage devices securely



NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE

Acceptable IT Usage



Some of the good practices for acceptable IT usage

- Always choose to use trusted Wi-Fi networks and avoid doing sensitive transactions like internet banking or emailing confidential information.
- Always choose to use “BCC” instead of “CC” –when sending a mass-email, it is always a good practice to place your recipients’ email addresses under “BCC” instead of “CC” to keep their identities confidential.
- Be mindful when connecting an external device to your computer as you would not know if it has been compromised by a virus or malware. Do remember to install an anti-virus software on your devices and always ensure that it is up to date.
- For more information about the Acceptable IT Usage Policy, refer to the AIUP document in our policy portal.



No part of this video shall be filmed, recorded, downloaded, reproduced, distributed, republished or transmitted in any form or by any means without written approval from the University.