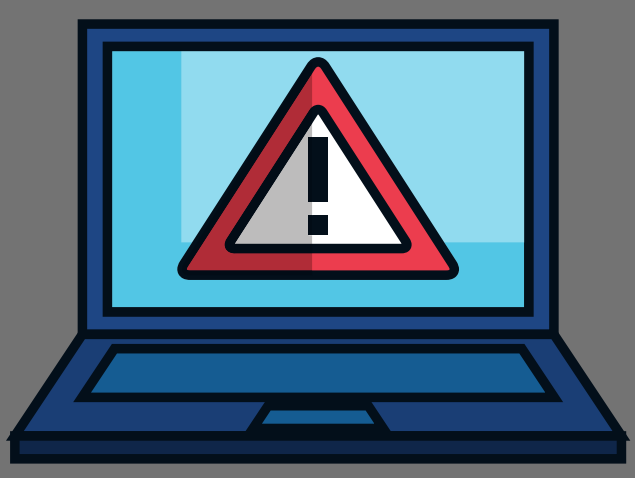
University of Nottingham
UK | CHINA | MALAYSIA

# CYBERSECURITY AWARENESS

## IT Services Department

## BEWARE OF RANSOMWARE



A sophisticated piece of malware that blocks the victim's access to his/her files by encryption and extort payment to restore the access. Unfortunately, it is almost impossible to decrypt files encrypted by ransomwares and never pay the ransom as it does not guarantee the restoration of your access to your files.

The university is closely monitoring services in an effort to detect and remove any threat before it reaches our user community

If you receive any suspicious emails, please follow the steps below:

·Do not click on any links

·Do not reply to the message, do not open any attachments.

·Forward a copy of the email to the IT Service Desk at itservicedesk@nottingham.edu.my.

·Delete the email from your inbox, deleted items, and sent items.

These messages may appear to come from friends or colleagues, particularly if you use a University device to view your personal email accounts.

## DATA SECURITY WHILE WORKING REMOTELY

If you are working remotely on any type of device, you are responsible for making sure that any University personal or sensitive information remains safe and secure. We recommend that you only use your UNM's Office365 account, including OneDrive and do not save the data anywhere else

Guidance for Data Security While Working Remotely

# HOW TO SPOT AND DEAL WITH SPOOF/PHISHING EMAILS:

One of the ways your computer can be compromised is through emails. Here are some useful tips to help you spot and deal with these spoof/phishing emails.

- Never reply to any email asking for your passwords, PINs or other account details.
- Make sure you know how to spot suspicious links and websites.
- Don't open attachments unless you completely trust where they have come from.
- If in doubt, always check with the IT Service Desk or your service provider (e.g. your bank) before responding to anything that looks suspicious.
- If you have clicked on the link and keyed in your password, please immediately go to

  https://itaccounts.nottingham.ac.uk

  to change to a new password. Otherwise, please ignore and delete it.

# PROTECT YOUR DATA BY SETTING STRONG PASSWORDS.

- Ensure that your password is 12 characters or longer
- Use upper case, lower case, numbers and special characters
- Don't use personal information or information that other people may find easy to guess.
- Ensure that your password is unique from all other passwords you use

Once you've created a strong password you must protect it:

- Don't share it with anyone
- Don't write it down, instead use a password manager
- Use different passwords for your University and personal accounts. If someone is able to figure out one of your passwords, they won't be able to access everything.
- Cover your fingers and keyboard when typing your password in public
- Do not reply to or click on links in emails that ask you for your password

# BACKING UP YOUR FILES REGULARLY:

Failing to back up may result in loss of important files due to accidental deletion, data corruption, hardware failures, virus or ransomware attacks, theft etc..

It is the responsibility of individual staff to back up your own working files on your computer regularly.

You are advised to back up/store your working documents in OneDrive while shared departmental files should be stored on SharePoint for ease of collaboration.