RESEARCH
@ SINGHEALTH DUKE-NUS ACADEMIC MEDICAL CENTRE

Academic Medicine Research Institute
Duke-NUS SingHealth

IT SECURITY AWARENESS

Corporate Email Accounts

- Corporate emails should only be used for official work mails and communication
- Take precaution against emails from external sources

Email is from external source.
Do not click on links or open files if unsure of sender.

Social Engineering

- Be aware of deception to manipulate you into divulging info or get access to your machine e.g. fake emails (phishing), fake phone calls and tailgating

How to protect yourself:

- Check the legitimacy of the email domain
- Do not click on any links listed in a suspicious email message
- Do not open any attachments contained in a suspicious email
- Examine email message closely – look for obvious signs of fraud such as poor spelling, unprofessional imagery and bad grammar
- Never allow remote access to your computer from somebody claiming to work in a specific well-known company
- Never give personal information over the phone

Report Suspicious Events

- Think someone have stolen data from your PC?
- Suspect malware in your PC?
- Loss, theft or damage of IT resources?
- Think your laptop is compromised?

Contact IT Helpdesk!

Contact : **1800 666 7777**
Email : ***it.helpdesk@singhealth.com.sg***

All staff must be aware of the current IT policies in both Infopedia and Docupedia

Look out for email communications and keep yourself updated.