How do I identify a suspicious email / phishing attempt?

helpdesk@nmit.ac.nz - 2019-08-20 - Stay Safe Online

Stop & Think before you Click!

A phishing email is a fake entity, normally criminal, masquerading as a genuine one attempting to hook you into divulging your identity or other key information.

Apply these tests – the more triggered, the more likely it's bad, bad, bad….

Are you expecting it? This content, from this person, at this time? Bear in mind:

- The sender's email account might have been compromised
- Does the tone/language/request fit the sender?
- Why are they sending it to you? Does the context make sense?

Sense of urgency/importance/threat to act now? Does it involve money or your identity? Criminals are literally banking on time-poor, overcrowded inboxes pressuring you into acting before thinking about why, so…..

Read it. Carefully. Twice.

- **Poor English/grammar/spelling** is often a big giveaway. Professional companies have professional communications writers, using consistent language.
- **Inconsistent design/fonts** – scammers always seem to have poor graphics skills and not spend their ill-gotten gains on professional design – be very afraid when they do
- **Does it mention you by name?** Just because it does doesn't mean all OK, but if it doesn't and generic, it adds weight to a likely scam.

Where does that link actually go to? ***Hover*** carefully over the link to reveal the web address it'll actually send you to. Dodgy ones:

Don't/tend not to	Do/tend to/can
Include the phrase 'safelinks'	Include a genuine company name but with some odd extras or scrambled in some way
Exactly match the genuine Googled web address for a company	Have a slight typo on a genuine company name
Match what the email tends to be referring to	

Finally does it 'feel' right? If something doesn't sit quite right, it probably isn't.

If in doubt, validate by another route

- Phone the sender
- Search for the named website on Google and log in there.

If you're reasonably sure it is a scam

- **Report it** – flag as SPAM/Phishing within your email service so it learns for next time, and if masquerading as a large company, forward it to their anti – phishing / SPAM services
- **Delete it** – so you don't fall for it when searching your inbox 6 months later, or accidentally forward to others