5 ways to detect a phishing e-mail

1. Is the e-mail from a Business E-Mail Address?

- **Watch for …**

The message is sent from a public e-mail domain.

2. Is the domain name is misspelled

- **Watch for letter substitutions and deletions.**

Are there 1's instead of i's?

Are there letters missing?

Are there 0's instead of O's?

Right	Wrong
unitec.ac.nz	unitec.acnz
	unitex.ac.nz
	unitec.zc.nz
	Unitec.com
	unitec.com
	unltec.ac.nz
	un1tec.ac.nz
datacom.co.nz	daacom.co.nz
	datcom.co.nz
	dataom.co.nz
	datacm.co.nz
revera.co.nz	revira.co.nz
	reera.co.nz
	revra.co.nz
	revea.co.nz

3. The e-mail is poorly written

- **Is the e-mail written in correct English?**

Look for:

- Spelling mistakes.
- Grammatical Mistakes

Spelling mistakes are less common due to spell checkers.

Grammatical errors that a native speaker wouldn't make:

"We detected something unusual to use an application"

A string of missed words, such as:

"a malicious user might trying to access"

or

"Please contact Security Communication Center".

4. Suspicious attachments or links

- **Does the e-mail includes suspicious attachments or links?**

Look for:

- Is there an infected attachment?

Never open an attachment unless you are completely confident that the message is from a legitimate party.

Moreover, you should look out for anything suspicious in ALL attachment.

- Suspicious links

One way to spot a suspicious link is if the destination address doesn't match the context of the rest of the e-mail.

For example, if you receive an e-mail from SKY , you would expect the link to direct you towards an address that begins 'sky.co.nz'.

5. The message creates a sense of urgency

- **The manufactured sense of urgency is effective in workplace scams.**

Look for:

- Is the e-mail really from whom it proports to be from?

Criminals know that most people will drop everything when ‘the boss’ e-mails with an important request.

- If in doubt, check!

Phishing scams of this nature are especially risky since, even if the recipient is suspicious, they maybe afraid to question their boss.

If they were wrong, they have:

- failed to meet their boss’ urgent request
- implied that there was something unprofessional in the way the e-mail was written.

Unitec values cyber security and accepts that it is *better to be safe than sorry* and would congratulate the employee for their cautiousness.

- Remain Vigilant