



Be aware

How do I know if an email is a scam?

- ✓ **Urgency or threats**
Look for signs of threatening language that calls for immediate action (ie. update personal details now, pay now, etc).
- ✓ **Hyperlinks and attachments:**
Look at the links and attachments - but **DO NOT** click or open.
- ✓ **The envelope-sender email address ("From" field)**
Check for unusual or unknown senders. Always review who the email is coming from and addressed to.
- ✓ **Dramatic statements**
Lucrative offers or eye-catching statements (ie. won a prize, congratulations, etc).
- ✓ **Any attempts to gain your Personally Identifiable information (PII)**
Legitimate companies are unlikely to ask for your PII in an email.
- ✓ **Spelling mistakes**
Attackers are less concerned than a normal sender would be, about spelling or being grammatically correct.
- ✓ **Check the email signature**
Most legitimate senders will include a full signature block at the bottom of their emails.
- ✓ **What should I do if I receive a suspicious email?**
Please forward suspicious emails as an attachment to spam@curtin.edu.au and delete the email promptly. If you are concerned that you may have clicked on a scam email or link by mistake, please contact IT Support immediately on +61 8 9266 9000 (ext #9000).