

Phishing email checklist

Pause and verify if any answer is yes.

Check before you click

- ☐ Is the message trying to rush or scare me into acting quickly?
- ☐ Does the sender name look right while the email address looks wrong?
- ☐ Am I being asked to sign in or approve something I did not initiate?
- ☐ Is the email asking for a password, MFA code or recovery information?
- ☐ Does the link destination differ from what the message claims?
- ☐ Is the attachment unexpected or unusual for this task?
- ☐ Does the request break our normal payment or approval process?
- ☐ Is someone asking for secrecy or telling me to bypass checks?
- ☐ Does the message push me to use a different contact method?
- ☐ Would I hesitate to forward this message to IT for review?

If you clicked or approved a prompt

- 1 Stop. Close the page and do not approve any further prompts.
- 2 Report it to IT immediately and say what happened and when.
- 3 Use the official app or portal if you need to change a password.
- 4 If an attachment behaved strangely, disconnect the device from the network.

Keep this checklist near your desk or share it with your team.

Email security and phishing support

milnsbridge.com.au/cyber-security-services/email-security/

1300 300 293 | info@milnsbridge.com.au