Passwords and passphrases

Protect yourself online by keeping your passwords safe

If you use the same password across your accounts, change them now to reduce the risk of one breached password compromising the rest of your accounts.

What should you do?

Don’t reuse passwords.

Create unique, strong passwords for each individual account.

Use a passphrase

Use four to five random words, something you can remember but is hard to guess, e.g. BlueSkyTr1angleTr0ut! Do not use predictable word or number combinations.

Use a reputable password manager.

A password manager only requires you to remember one master passphrase and can generate and securely store all your passwords.

Use multi-factor authentication (MFA).

Adds an extra layer of security in case your password is compromised. Use MFA for both work and personal devices.

Never write down or share passwords.

Do not reveal your passwords or passphrases to others and do not write them down for people to see.

Lock your devices.

Always lock your devices when you walk away from them. Use a password, passcode or biometrics (e.g. fingerprint).

Where to find more info

In the workplace, it is important that you adhere to the password policy set by your IT team. For more information on passphrases and password managers, visit: **https://www.cyber.gov.au/protect-yourself/securing-your-accounts/passphrases**