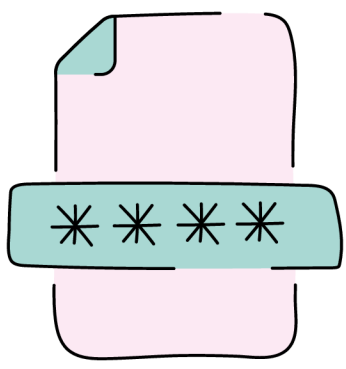
ACSC PRACTICES FOR SECURE PASSWORDS

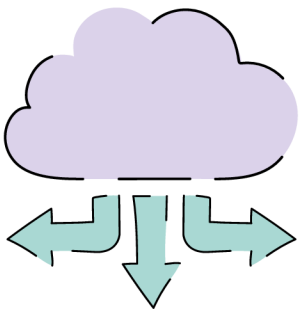
1 USE A PASSPHRASE, NOT A PASSWORD

Passphrases are longer and typically easier to remember than random character strings. A passphrase is a sequence of words or a sentence that is both long and complex enough to be secure.

2 USE LONG & COMPLEX PASSPHRASES

A passphrase should be at least 14 characters long. Use a mix of uppercase, lowercase letters, numbers and symbols. And avoid common and predictable passphrases.



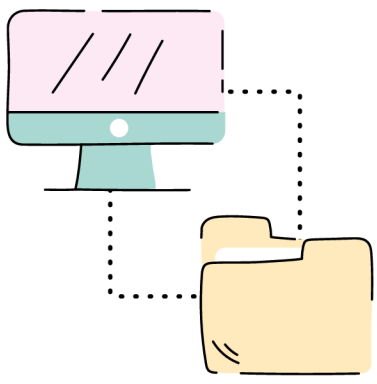


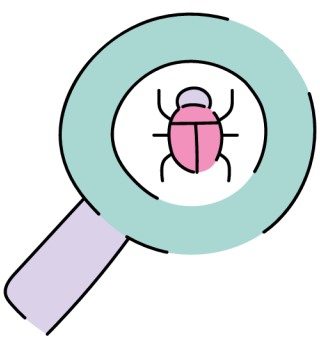
3 DO NOT REUSE PASSPHRASES

Use unique passwords or passphrases for each account, especially for critical services like email, banking, and social media.

4 USE A PASSWORD MANAGER

To manage multiple complex passwords, use a password manager. This tool can securely store and generate strong, unique passwords for each of your accounts.





5 ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Wherever possible, enable multi-factor authentication (MFA) in addition to your password. This adds an extra layer of security by requiring a second factor of authentication.

Follow the Australian Cyber Security Center on their website to stay up to date on the latest digital security news and developments.