Lawcover®

CYBER SECURITY SNAPSHOT

PROTECT YOUR PASSWORDS

Update your passwords regularly

Use a password manager to generate and store your passwords securely

Never use the same password twice

Establish clear and consistent procedures when creating and updating passwords

Do not use personal information when creating a password

STEP BY STEP

CREATE STRONG PASSWORDS

Passwords are the first line of defence against unauthorised access to your computer and information. The stronger your password, the more protected you are from cybercriminals. You should maintain strong passwords for all accounts on your computer.

DO	DON'T
Use a combination of at least 8 – 12 letters, numbers, and symbols The longer your password and the more character variety it uses, the harder it is to guess. For example, M0l#eb9Qv? uses a unique combination of upper- and lowercase letters, numbers, and symbols.	**Don't use sequential numbers or letters** e.g. 1234, qwerty, jklm, 6789, etc.
Combine different unrelated words in your password e.g. 9SpidErscalKetobogGaN This makes it difficult for cybercriminals to guess your password. Use three or four longer words to create your password.	**Do not use passwords that include personal information. E.g. pet's name, your birthday or that of family members, any words related to your hobby, job, or interests etc.** Cybercriminals can easily find this information on social media accounts or websites.
Use a password manager to store your passwords securely Password managers have inbuilt, specialised security to guard against cybercriminals.	**Do not use names or words found in the dictionary** Substitute letters with numbers or symbols to make it difficult to guess the password, or deliberately use spelling errors in the password or passphrase (e.g. P8tty0G#5dn for "patio garden").
Establish clear and consistent procedures for creating and updating passwords e.g. specific password conventions that must be followed.	**Do not store your passwords in a document on your computer or in a notebook** This can be easily infiltrated by a cyber criminal, stolen or lost.
	Do not reuse your passwords

STEP BY STEP

USE A PASSWORD MANAGER

USE A PASSWORD MANAGER

A password manager is a more secure way to store and keep track of all of your passwords. It can also be used to generate unique and strong passwords according to a set criteria, can be accessed across multiple devices and can provide reports and activity logs to help track usage.

There are many password manager programs and apps available. Research your options to ensure the best fit for your needs.

PASSPHRASES

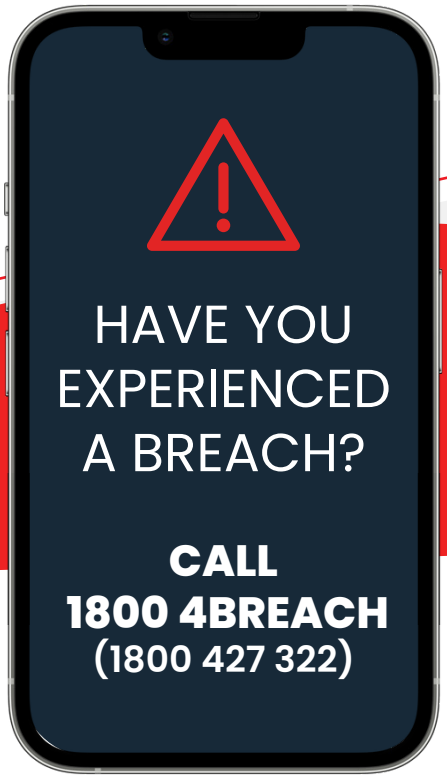
As complex passwords can be difficult to remember, passphrases that are 4 or more random words combined can be used (e.g. correcthorsebatterystaple). Refrain from using common, well known phrases or song lyrics.

PASSWORDLESS LOGIN

Passwords remain one of the weakest links in authentication, as users often struggle to create unique and secure passwords. As a result, the same password (or slight variations of it) is frequently reused across multiple sites, making it easier for hackers to compromise accounts.

As an alternative, passwordless authentication can be implemented, using methods such as biometrics, hardware tokens, or one-time passwords. This approach can help eliminate the risks associated with repeated password use.

> If the passwords securing your data aren't strong, then your information is at risk.



Lawcover®

Lawcover Insurance Pty Ltd | ABN 15 095 082 509
Phone (02) 9286 8877 | practicesupportservices@lawcover.com.au | lawcover.com.au