Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

QUICK WINS FOR YOUR PASSWORD MANAGER

cyber.gov.au

Passwords protect so many parts of our lives, from our money to our businesses and even the appliances in our smart homes. Remembering all these passwords can be a real challenge, particularly when every account has different password requirements. That's where password managers can help.

A password manager is an application that securely stores, generates and manages passwords for all of your accounts. With a password manager, you only need to remember one master password, the password manager takes care of the rest. Think of a password manager as a safe for your passwords and the master password as the key to the safe. You can use password managers on computers and mobile devices.

Password Manager Wins

Win #1

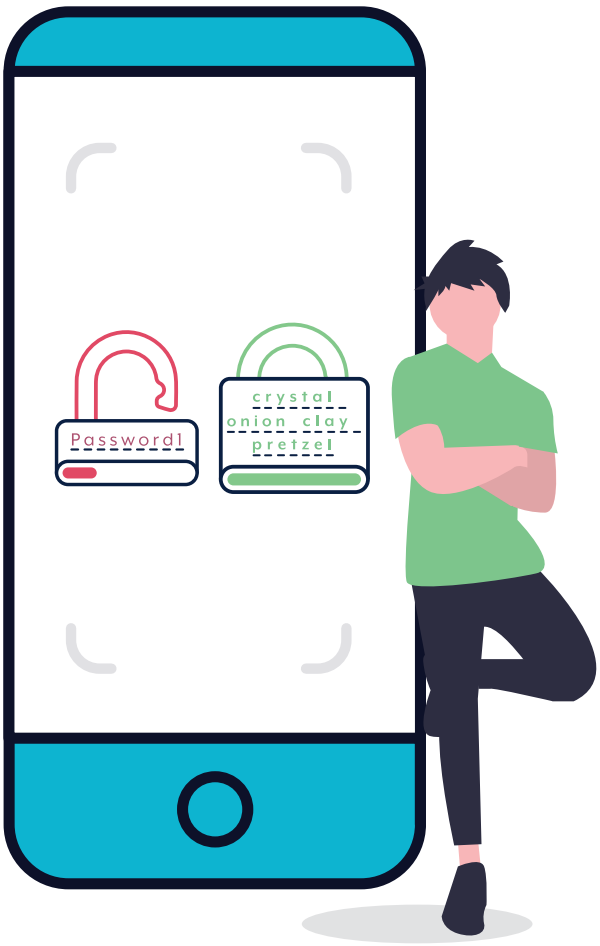
Make your master password your strongest

Your master password is the key to your safe. If someone guesses your master password, they may be able to access all your passwords. Make sure your master password is unique and your strongest password.

The strongest type of password is a passphrase which is easy to remember. Passphrases are a combination of random words, for example, 'crystal onion clay pretzel'. The best passphrases:

- are at least 14 characters long
- use a random mix of four or more words
- do not use popular phrases, for example, song lyrics or famous quotes.
- are not re-used across multiple accounts

Passphrases are easy for you to remember and hard for machines to crack.



Do not reuse passwords

It is not secure to use the same password for all of your accounts. With a password manager, you can have different passwords for all of your accounts while only having to remember your master password.

Win #2

Enable multi-factor authentication (MFA)

MFA is a method of increasing the security of a password manager.

MFA requires you to prove your identity in two or more ways before you can access sensitive features of your password manager. It typically requires a combination of at least two of:

- something you know (e.g. a passphrase or PIN)
- something you have (e.g. an authenticator app or physical token) or
- something you are (e.g. your fingerprint or face scan).

Enabling MFA on your password manager adds an additional layer of security. It means that even if a cybercriminal learns your master password, they will not be able to access your other passwords as your other authentication methods keep your password manager secure.

Don't lose access to your password manager

Forgetting your master password or losing access to your multi-factor authentication method is like losing the key to a physical safe. It may mean you lose access to all the passwords stored in your password manager.

Win #3

Choose the right password manager for you

There are many different types of password managers but their quality and security may vary. When choosing a password manager, do your research to ensure that the vendor has a good reputation and that their product has strong security features, strong privacy features and is maintained with regular security updates.

Different password managers have different features. Consider what features are important to you. You may want to check if your password manager:

- has a plan that covers family members
- can manage your passwords across multiple devices
- supports all the different devices you use
- ensures only you can see your saved passwords, even the company that makes the password manager cannot see them.

Many password managers are free and some are included with certain devices and programs.

Be careful when using the 'remember me' feature

Some password mangers have a 'remember me' feature. If you select 'remember me' the password manager will trust the device you are using and ask you for your master password less frequently.

Do not use the 'remember me' feature for your password manager if you are on a public computer or if you share the device with other users.

If you do, other people that use the device could access your accounts.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre