

# WHAT IS YOUR NEW YEARS RESOLUTION FOR PROTECTING YOUR PASSWORDS?

## Password managers - Do I need one?

When it comes to creating and using passwords, there are a several tips to consider to ensure that your password remains safe and secure, including:

- using a strong password
- making it unique
- not reusing passwords
- using multi-factor authentication, otherwise known as MFA
- avoid using personal information
- using a memorable phrase
- not writing them down i.e. using a sticky note reminder on your PC.

Or you can simply use a **PASSWORD MANAGER**.

## Password managers – preventing password fatigue

Passwords are crucial for anyone who owns or uses a computer or smart device. They are the first line of defence in protecting your data. However, creating and remembering strong passwords for each account can be difficult. Password managers can help you to create, manage and store passwords securely for each of your accounts. They can come in a variety of forms, such as a phone application or website.

To access a password manager, you typically only need a single master password, a key or PIN. This means you only need to remember one items to login and access all of your stored passwords. Many password managers also check your current passwords and tell you which ones are weak or reused and need changing.

Password managers allow you to:

- create strong and unique passwords
- store passwords and other logins securely in one place from any device
- save time and effort by auto-filling your login details
- store your bank cards, PINs and identity details
- reduce the risk of someone intercepting your passwords.

To learn more, see Six reasons to use a password manager in 2025: <https://murrayphn.org.au/wp-content/uploads/2025/01/6-Reasons-to-Use-a-Password-Manager-in-2025.pdf>

# HOW TO SET UP A PASSWORD MANAGER

First, pick a password manager and set up an account; sites such as [Cybernews](#) and [CNET](#) list some of the top password managers and so are good places to start.

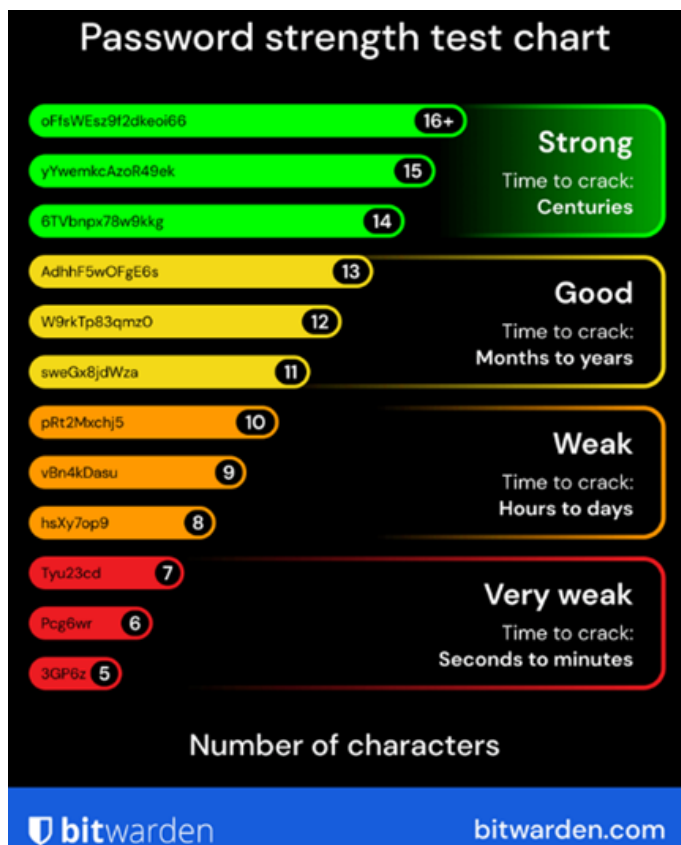
While password managers are great tools, like anything online, they can be attractive targets to cybercriminals. Therefore, it is advisable to check that you are using a reputable password manager and take good security measures by following the advice of the [Australian Cyber Security Centre](#).

Some password managers offer a free version with basic features, while paid plans often include extras like access on multiple devices, more file storage and options to share with family.

When setting up your account, you will need to create a master password; a robust password that ticks all rules for creating strong secure passwords. This is the one password you must remember, so make it memorable but hard for others to guess. Don't use a password you already use on other sites. Some password managers offer an "emergency kit" with your username and digital key.

You must not forget or lose your master password or emergency kit, as password managers usually don't have a way to recover it for security reasons and so if you get locked out, there is likely no way back in.

To check the strength of a password, visit the Victorian State Governments website:  
<https://service.vic.gov.au/find-services/personal/password-strength-tester>



## Contact

If you have any questions, feedback or require further information, contact Murray PHN's digital health team, e: [digitalhealth@murrayphn.org.au](mailto:digitalhealth@murrayphn.org.au).