

Introduction

Password Managers store your passwords, along with the usernames and web addresses they are for, as well as generating new, random passwords. By storing the official websites into your Password Manager, you can access them directly from the manager, rather than clicking on links or risking navigating to a phishing website.

Where do I get a Password Manager?

Password Managers are available on App Stores and can attract a cost. Some also have a free version, but with certain limitations, or others are always free without limitations. Always do your own research. Read reviews to see what others are saying about various Password Managers to help you decide which one may be the best for your situation.

Are Password Managers Safe to Use?

Password Managers are as safe as you are with your online activities. IDCARE recommends Password Managers that have multi-factor authentication (username, password and code) and can limit specific device usage. This means limiting access to a specific device or devices. The benefits of using a Password Manager include ensuring that you have variable passwords and complex ones that you do not have to remember. Remembering passwords is one of the main reasons people use the same password for several online accounts. Using the same password is also one of the main reasons why online accounts are vulnerable to being hacked. Password Managers help ensure this doesn't happen.

Be careful about where you store and how you store recovery keys and codes to your Password Manager. It is really important to store the key safely and not share it with anyone. If you lose the key and forget your master password, it is often impossible to access your Password Manager again.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

How do I choose a Password Manager?

- ☐ Choose a Password Manager that you find easy to use.
- ☐ Make sure that you login and download the software from the legitimate site.
- ☐ Look at all the services that the Password Manager provides, and choose the one that best suits your needs.
- ☐ Take advantage of the free trial period, so that you can make sure that you are comfortable using the product and to give yourself time to get used to it. If you don't think you have chosen the right Password Manager, export the data you have saved there so that you can put it into the next Password Manager you trial.

Starting with a Password Manager

- ☐ Try before you buy – most Password Managers will allow you to export your saved data and import data from other Password Managers. If the Password Manager you are considering using doesn't allow this, then you may find it difficult to change to another Password Manager down the track.
- ☐ When you first choose a Password Manager, you will need to create a master password to access your account manager. This is **your most important password**, so make it something easy for you to remember, but hard for anyone else to guess.
- ☐ Make sure you also set up multi-factor authentication, so you need both your password and that extra level of protection to access your password manager. This could be using facial recognition on your phone, SMS verification codes, or codes sent to an authenticator app.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

I've chosen a Password Manager to trial. Now what?

- ☐ Start putting your passwords into it. You can do this by manually entering them into the Password Manager, or as you log in to each website your Password Manager will ask if you would like to add that site and login details to the Password Manager.
- ☐ As you enter more and more passwords, you might see a warning come up telling you that you have used that password somewhere else, or that it is not a strong password. In either case, that is the time to update that password, so it is both unique and strong.
- ☐ Some Password Managers will also alert you if there is a two-factor or multi-factor authentication option for each of your stored services and remind you to set this up.
- ☐ Password Managers may also let you know if your username or password has been involved in a data breach. If so, change your password, just to be safe.
- ☐ Check out your Password Manager's autofill options. Sometimes this is only for auto filling the login credentials (so you don't have to click "copy" to enter that auto-generated password). Or it may also have autofill options for online forms, so that you don't have to fill in your personal information every time.

Remember, whatever Password Manager you choose, it is only as safe as your online activities. Never share your master password, master key, or verification codes, no matter how legitimate the request seems. Always make sure you are using legitimate websites or apps before entering your username, password, verification code or other personal information.

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 160 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.