Beaming

Business guide to:
Password Managers

Using a password manager may be an appropriate way to support you with using the most secure password practices and ultimately protect your data from cyber attacks.

What is a password manager?

A password manager is an application that stores all of your passwords in one place, secured by a master password that's used to encrypt the rest of the database.

This enables you to generate many strong and unique passwords whilst only having to remember one.

Types of password manager

Cloud based

Cloud based password managers store passwords in an encrypted database on a server at a data centre.

- Access passwords from any location, in multiple services and devices.
- When selecting a provider carefully research how data will be secured during processing and storage.
- Likely to involve small regular payments.

On premise

On-premise password managers consist of an encrypted database held on a local network server/machine.

- Access database when you are connected to the local network.
- Retain full control over the database so you always know where your sensitive data is held and how it is secured.
- Likely to require one off set-up cost.

Advantages of using a password manager

When faced with remembering a separate complex password for every account, almost all of us will do one of two things:

1. Follow the advice we've been given by creating a strong, separate password for each account. But forget the password next time we log in, give up and have to create a new complex password.

Or

2. Skip trying to remember a complex password and go straight to using a familiar one we're able to remember.

One of the biggest pros of using a password manager is that you only have to remember one master password, which means you can make all your passwords as complex - and therefore hard to crack - as possible.

Speaking of complex passwords, most password managers will randomly generate strong passwords for you. That way you don't need to worry about whether you're meeting complexity requirements and can generate and save your new password with just a couple of clicks.

With the use of a browser plug in, they can also automatically pre-fill your details when logging onto websites, and can often be configured to do so across different devices.

Disadvantages of using a password manager

One of the objections to using a password manager is that if another person does gain access to your master, they will be able to access and potentially lock you out of all of your accounts.

Another problem is that if you were to forget your master password, you would not be able to access any of the information stored within the database and would likely have to individually reset the password on each of your accounts. Not impossible, but your time could certainly be better spent elsewhere!

Five top tips: using a password manager

We can understand why you may have some reservations about allowing all of your passwords to be stored in the same place, but overall and when used sensibly, a password manager will make having unique passwords for each of your online accounts a lot easier. This in turn reduces your risk of suffering a significant cyber attack. Follow our advice below to make sure you're following best practice.

1. Be careful about the master password you choose: it needs to be both secure and memorable. Put some thought into this one! It's a good idea to check your chosen password out on haveibeenpwned.com to make sure you're not using a phrase that's previously been uncovered in a data breach.

2. If you choose a cloud based password manager do some thorough research into the provider. What will they do to keep your information secure and does the loss of control (vs using a local password manager) weigh up against the convenience of being able to access your passwords from any location?

3. Enable two-factor authentication on your password manager to add an extra layer of security. This is particularly important if you do choose to use a cloud based password manager.

4. Even if you're not keen to entrust your very sensitive passwords – for your bank or email account, for example – to a password manager, you could still consider using one to store the details of your other accounts. This will free up more brain capacity for remembering those passwords you don't want to store in an app.

5. If you are using the auto-fill feature, make sure you have a "Timeout" set. This means that if you don't put your master password in every so often you will not be able to use the auto-fill.