BUSINESS IN THE COMMUNITY
The Prince's Responsible Business Network

FACTSHEET

PASSWORD MANAGERS – A BUYERS' GUIDE

What are Password Managers?

Password Managers are affordable and easily usable tools that create and store passwords for you and are accessible via a 'master' password. This means you only need to remember one password to gain access to all your securely stored passwords.

They offer a range of advantages. For example:

1. They make it easy for you to use long, complex, unique passwords across different sites and services, with no human memory burden
2. They are better than humans at spotting fake websites, so they can help prevent you falling for phishing attacks
3. They can generate new passwords when you need them and automatically paste them into the right places
4. They can sync your passwords across all your devices, so you'll have them with you whether you're on your laptop, phone or tablet

Why are Password Managers so popular?

Your laptops, computers, tablets and smartphones contain a lot of business-critical data, the personal information of your customers, and details of the online accounts that you access, making it very important that you protect access to them.

A free, easy and effective way to prevent unauthorised access is by using passwords. However, between your work and home life, you will have a lot of passwords to remember. This burden leads to less secure practices like: using easily guessable passwords, reusing the same password across multiple accounts, or writing passwords down and not keeping them safe.

Password managers help alleviate this burden and offer other security benefits too.

Which Password Managers should I choose?

There are two key criteria to consider. How does it fit around how I work and how secure is it?

Looking at usability: it is important to look at the features of any tool and understand how you can implement it within your businesses with the least amount of disruption. There are three main types of password managers:

1. **on-device managers** – which store password data locally on a single device.
2. **browser-based third party or built in managers** – which are fully integrated with web browsers and can sync data across all devices where that web browser is used and know when you're on a website that needs a password, popping up to fill in the password.
3. **cloud-synced managers** – which store password data on a remote server and allow you to access it from any of your devices via an app or through browser plug-ins.

Looking at security: Business in the Community's (BITC) Business Emergency Resilience Group consider that for small businesses and individual users, there is generally no significant security differentiators between the leading products on the market. This makes it hard to recommend a specific product but those listed below are currently viewed as the market leaders and have been subject to

HRH THE PRINCE OF WALES
ROYAL FOUNDING PATRON

the scrutiny of consumers and security researchers alike:

- 1password
- Chrome
- KeePass
- Keychain
- LastPass

* This is a representative list of market leaders and does not imply that those products not on the list are any less secure.

Ultimately your choice will be down to the circumstances in which you will be using the password manager, the technologies you are using and the features you need.

What are the downsides?

Like any security product, password managers have pros & cons, but BITC advises that the pros typically outweigh the cons making them a sensible solution for small businesses looking to reduce their risk profile without spending large amounts of money or introducing 'security friction'. For more information on this discussion, the National Cyber Security Centre (NCSC) have published an article going in to more depth.

The main downsides are:

1. If you forget the master password for your password manager you will not be able to get back in. You will have to carry out password resets on all your accounts. This could be time consuming and disruptive to your business.
2. Browser-based password managers may not automatically sync between all your devices if the devices use different operating systems. Also, if more than one person uses a device on the same user profile, they would have access to your passwords and therefore all the things they protect and you may not want that.
3. You can't use them for everything. Some service providers (such as certain banks) mandate against the use of password managers. If you tell them you've put your banking passwords into one (or written them down in any way at all) they might not give you your money back if you are the victim of cybercrime.

The most important thing to remember when using a password manager is that since the master password is protecting all your other passwords, make sure it's a strong one. The NCSC offers the following advice on creating good passwords.

In summary

The number of passwords we need to remember is only going to increase. Password managers offer you an affordable way to significantly improve your risk profile without adding friction to your business.

While there are some downsides to using them the positives vastly outweigh the negatives and it is deemed 'good practice' to use password managers to protect your business and employees.

Your choice of password manager will be down to the circumstances in which you will be using the password manager, the technologies you are using and the features you need.

More information and further guidance and context on password managers can be found on the NCSC's website – https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-passwordmanagers

ENJOYED THIS CONTENT?

You might also like to:

- find out more about responsible business
- find out more about our advisory services
- join us at one of our upcoming events

Talk to one of our expert team today to learn how membership of BITC can help you take your responsible business journey further, and drive lasting global change.