How does a password manager work

Password managers have been around for a few years now, and amid growing cybersecurity concerns and data protection, they are seeing a consistently increasing usage around the world.

But why have they become a required element to a business? And how do they work to keep your data private, beyond just storing your passwords for you?

Password Vaults

The first and most obvious use of a password manager is the vaults. The place where the login data is stored. But how do they differ from using things such as Excel or Word?

Well, for one if you are using Excel or Word to store your passwords, we are going to be very clear with you; You are leaving your company at risk. A password manager is fully encrypted, meaning that only your master password on your registered devices can view them. They cannot be shared, displayed or distributed otherwise, even by your IT providers.

Services like Apple Keychain or Google Passwords is a step in the right direction, but they have a more limited encryption level and can be accessed using the same login you use for other services. While it may work well as a personal solution, it is by no means a secure way forward for your business.

LUCIDICA

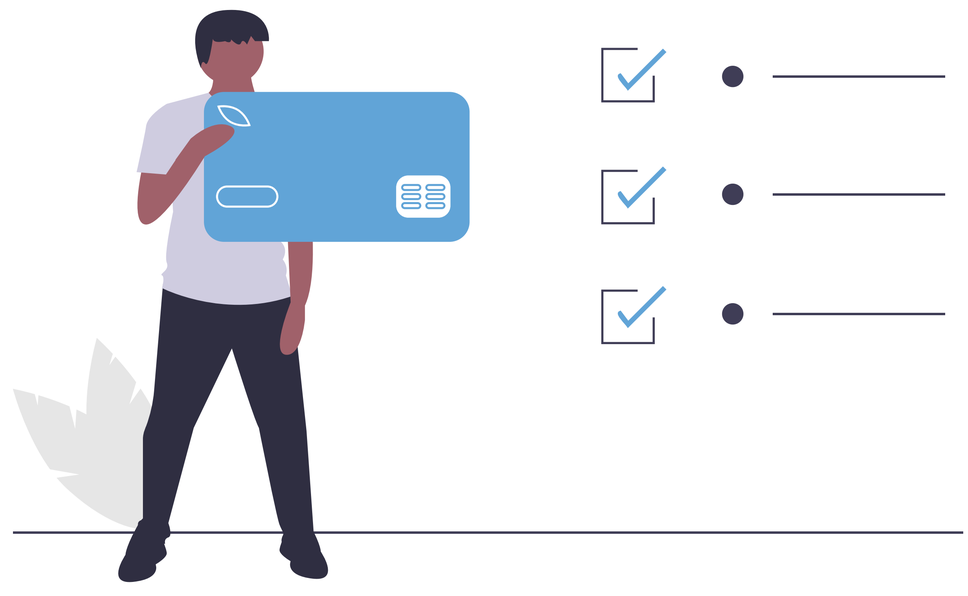
The IT team for your business

Password Generators

One of the most straightforward and most significant steps in password security is using their password generator features to create complex and unguessable passwords, and then remember them for you.

59% of consumers reuse passwords because they are too difficult to remember. Using the same password across multiple sites increases the chance of a breach. Using an individual password for each service means once one password is compromised, it is self-contained and doesn't comprise others.

As a business, it is required that you use individual passwords for different services as well as utilise the 2FA (Two-Factor-Authentication) wherever possible.



Share passwords & card information securely

When you need to share a password to give access to a site or need to share card information for someone internally to make a purchase, sending this outside of securely encrypted channels leaves them vulnerable.

Creating a record of this information on a chat system, email or otherwise is data that can be exploited.

Password managers allow you to securely transfer this information right to the other employees' vault. You can also set restrictions and time limits on this data share, having the data erase itself from their vault when they no longer need it.

Security Dashboard

The different password managers will come with various features on their security dashboards, but almost all will come with one.

These security dashboards allow you to monitor your overall password usage, score you on how well you are doing, show you any time duplicate passwords are utilised, alongside a few other bells and whistles.

One key feature of some of the more advanced managers is dark web scans. By utilising breach report data by companies across the world, you can identify which account has had personal information leaked, as what that data is.

If your password appears on this list, it will prompt you to change it, keeping you ahead of the curve.

This security dashboard also runs company-wide, allowing you as the administrator to see the overall company password health, and know where you can improve your measures.

Which password manager is best for you?

No cookie-cutter password manager fits you as a business as a lot of these services utilise different UX/UI designs to interact with you as an individual.

We here at Lucidcia use Password Boss, due to its depth and variety on the dashboard, as well as the different vaults that can be set-up with varying permission levels. We recommend doing some research and looking for what values you are after as a business.

LUCIDICA

The IT team for your business

If you are looking for a password manager yourself or thinking of changing, we can manage this service for you. So you know it is in safe hands and is supported correctly.

For more information, please reach out on 020 7042 6310 or to service@lucidica.com

LUCIDICA

The IT team for your business