



THE
EASTERN
CYBER
RESILIENCE
CENTRE

Little Steps to Becoming Cyber Resilient

Password storage – how do you manage 100 unique passwords?



We should all be aware that compromised and default passwords must be changed and that we should ensure we set a strong, complex password for each login. The issue is how do you remember a different password for each account you utilise?

Some stats for you:

Most people have *over 100 accounts* which require username and password.

The average number of passwords has *increased 25%* in the last year, compared to a similar poll in 2019, which placed the average number of passwords at 70 to

80. One reason for this could be the global pandemic, which has forced many people to use more services online, introducing the necessity to generate new accounts.

This might explain why people use easy-to-guess passwords — they simply have too many to remember. So, it is hardly surprising that people use either very simple passwords or have a few and reuse them for all accounts.



What should I do?

Decide the best method for you and your employees to remember those passwords. You can:

- **use a password manager** - either as part of the browser or as a separate solution
- **write them down** (keeping them away from prying eyes and safe - maybe locked away in a cabinet and written in a code that only you can understand). Do not store them electronically on a word document named

"passwords" as this will be an obvious place for an attacker in your system to look

If you want to get rid of insecure, re-used passwords, then this should be a priority action for you to implement

What is a password manager?

A password manager is an app on your phone, tablet or computer that stores your passwords securely, so you do not need to remember them all.

Some password managers can synchronise your passwords across your different devices, making it easier to log on, wherever you are which can either be a separate programme or a browser plug-in.

Whatever the case, you only have to remember one "master password".

It is worth finding online reviews of the password managers you're considering, deciding on the features you need (and the support the vendor provides) before choosing one that's right for you.

Web browsers can also remember passwords for you.

Using the browser means you must keep your devices secure, and never leave it in a state where someone else can access it without entering a password. If your device is lost or stolen, then potentially none of your passwords are safe.

Some password managers will also keep an eye out for your data and notify you if any of the accounts you have been used have been compromised.