expert.services /blog/managing-your-website/security/password-managers

# The Pros and Cons of Password Management

3-4 minutes

---

You may remember our blog - Top 5 most common passwords – do yours appear in the list? - which outlined some big no nos when choosing a new password (if you haven't read it yet, we recommend that you do). As some of our clients use password managers (PM), we thought we would build on that by providing you with the pros and cons of using one.

**Pros:**

- Humans can be unreliable as they can come up with bad passwords, forget their password, or are genuinely disinterested in security. With a PM there is no need to worry about remembering all your different passwords.
- Using the same credentials for each account is dangerous as it creates one point of failure.
- Good password managers encrypt all your personal data in case someone hacks the PM software directly; the hacker might get your passwords but they won't know who the passwords belong to.
- PMs can keep you up to date with the latest breaches and advise you if any accounts may have been affected/hacked.
- Can use offline password manager (not stored on the web/not a web browser plugin).

**Cons:**

- Single point of failure - if someone gets hold of your master password, they have all your passwords.
- Password manager programs are a target for hackers.
- It's not easy to login using multiple devices.
- If the main password is used/typed/saved on a computer with malware, your main password can compromise all your other passwords controlled by the PM - all your passwords are only as secure as your master password.
- Not all PM's are adequately encrypted which can render the whole process of setting one up useless.

Perhaps the simplest advice we can give, is to have two factor authentication when possible. Two factor authentication is a two step verification that along with your password and username, requires another level of authentication. Hence, if someone gets hold of your password, they won't be able to proceed without entering the next level of authentication. e.g. Google Authenticator.

Also, always make sure that your email password is secure and changed often. Computers are always at risk of malware and at the end of the day, all password recoveries go to your email. If your email is compromised, a hacker can get access to all your accounts by doing a simple password recovery. The only place you should have it written down, if at all, is on a piece of paper kept at a safe location.

Another good idea we've come across is to have two notebooks. In one notebook, put your account data and a corresponding serial number. In the second notebook next to the serial number, write down the corresponding password. Always make sure the second notebook is kept in a safe place, in case you forget one of your passwords.

It's important to mention that **there are no silver bullets**. No password is ever 100% secure but there are definitely ways that you can make it harder for hackers to get hold of your password. Common sense goes a long way. Not opening any suspicious links or emails from people you don't know is always a good start, and making sure your operating system is always up to date with the latest security updates is crucial in many cases.