SIX REASONS TO USE A PASSWORD MANAGER IN 2025

1. Password attacks are on the rise

Cybercriminals made more than $1 billion in ransom payments last year. Ransomware, malware and password-based attacks are increasing. According to Verizon's 2023 Data Breach Investigations Report, 74 per cent of breaches involve stolen credentials. If you use the same password across multiple sites, one breach can compromise all of your accounts. A password manager helps you create strong, unique passwords and alerts you if your credentials are found on the dark web.

2. Reduces password fatigue

The average person has about 100 online accounts. Remembering that many passwords is hard and leads people to reuse passwords. Password managers generate and store strong, unique passwords for you, so you only need to remember one master password.

3. Creates strong, unique passwords

Password managers have built-in generators to create strong passwords instantly. With autofill, you don't have to come up with passwords yourself, ensuring each account is secure.

4. Protects you from phishing scams

Phishing emails and texts can trick you into giving away your login details. Password managers can spot phishing sites because they only autofill credentials if the URL matches what's stored. If it doesn't autofill, it's a red flag.

5. Securely shares passwords and more

Sharing sensitive info via email or text is risky. Password managers like 'Keeper' let you share data securely. You can control access and revoke it anytime. Features like one-time share allow you to share records temporarily, even with non-users.

6. Works across multiple browsers and devices

Built-in password managers like 'iCloud Keychain' and browsers like 'Chrome' have limitations. Standalone managers i.e. 'Keeper' work across all devices and browsers, giving you access anywhere.

Risks of not using a password manager

- **Password reuse**: Using the same password for multiple accounts means one breach can compromise all.
- **Weak passwords**: Strong passwords are hard to create and remember. Weak passwords are easy to crack.
- **Multiple resets**: Frequent password resets can lead to weak or reused passwords.
- **Insecure sharing**: Sharing passwords via text or email is risky and unencrypted

For further information, contact digitalhealth@murrayphn.org.au

Source: Should You Use a Password Manager in 2024?