Password Managers

Why use a password manager?

One password to remember, forever

Use a password manager to generate unique, strong passwords for different websites and store them in a secure “vault”. To access that vault, **all you need to remember is one single, very strong, unique password.**

Password reuse? Break the habit

We’ve all likely used the same logins for different websites in the past, but this puts important data at risk: **hackers can use leaked passwords to gather sensitive information** about you and your family. **HaveIBeenPwned** (**https://haveibeenpwned.com/**) can show you when website data breaches have leaked your passwords. Luckily, **password managers make it simple to create strong, unique passwords.** When there’s a security breach in the future, you’ll have peace of mind knowing your data on other websites is not at risk.

Secure and accessible with features you need

We’ve all likely used the same logins for different websites in the past, but this puts important data at risk: **hackers can use leaked passwords to gather sensitive information** about you and your family. **HaveIBeenPwned** can show you when website data breaches have leaked your passwords. Luckily, **password managers make it simple to create strong, unique passwords.** When there’s a security breach in the future, you’ll have peace of mind knowing your data on other websites is not at risk.

Why use a password manager?

There are many reputable password manager solutions, each with its own pros and cons. Three of the most popular are highlighted below. Each is available on all major platforms and offers similar functionality but has its own design and unique features.

https://lastpass.com

https://dashlane.com

https://keepersecurity.com

Each solution offers a basic free version with a robust feature set as well as paid versions with additional functionality. If you choose to upgrade to one of the paid versions, you are responsible for the associated cost.

See the drop-down below for a comparison of these three solutions.

Accenture's Guidance on password managers

Use of a password manager is recommended.

We do encourage a password manager as an Information Security best practice for your personal information. If used properly, a password manager will be easier to use and more secure than needing to remember multiple strong passwords.

If you use a password manager to store personal credentials, it should be protected with Multi-Factor Authentication.

We recommend this extra layer of security, especially if you choose to store personal logins and passwords.

You are responsible for the protection of your personal credentials.

While we recommend the use of a password manager, like any other commercially available product that you chose to use at home, we cannot guarantee that it will never be compromised. We believe it is still the safest approach, and our security leaders use password managers every day. Because you could be impacted personally, the choice of whether to use a password manager and which one to use is solely up to you.

Detailed password manager comparison table

	LastPass	dashlane	KEEPER
	https://lastpass.com	**https://dashlane.com**	**https://keepersecurity.com**
STANDOUT FEATURES	• Feature rich free version • Extensive two factor authentication options • Solid and consistent design across	• Can change almost all passwords instantly • Intuitive interface across all platforms	• Particularly strong security features (Breach watch, Zero knowledge, SOC2) • Intuitive design across platforms
CONSIDERATIONS	• Stand-alone desktop app limitations in Mac	• Premium version is more expensive than other password managers	• Less robust form-filling capabilities • No PIN for mobile app • No bulk password change
NOTABLE LIMITATIONS OF FREE VERSION	• Limited password sharing • Limited Two Factor Authentication (2FA)	• Single device only • Maximum of 50 stored passwords	• Single device only
ADDITIONAL INFORMATION	• Ease of use, excellent support for all major platforms, wide range of features and variety of configurations • The free version of LastPass syncs across an unlimited number of devices • Paid version's price has tripled in the past few years, going from $12 per year to $36 per year.	• Bulk password changer, which can reset hundreds of your passwords at once • Can scan email to find old accounts • Premium plan is costly at $60 per year; Premium Plus plan is $120 per year • Free plan was downgraded to 50 sets of credentials	• Cheaper than premium versions of both Dashlane and LastPass • Has excellent "Zero Knowledge" security, but does not have a bulk password changer • Won't let you create a PIN to quickly access the mobile app

Please visit each respective solution's website for a more complete and up-to-date list of features.