

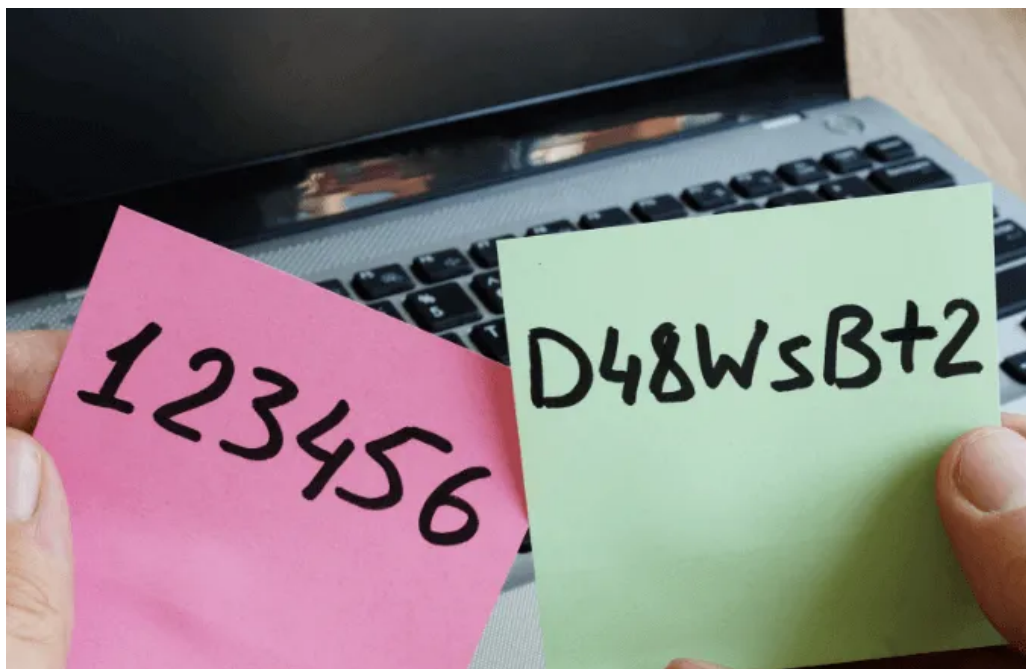
www.online-tech-tips.com/computer-tips/what-is-a-password-manager-why-are-they-useful/

What Is a Password Manager & Why Are They Useful?

7-8 minutes

What is a password manager? A password manager is an [encrypted piece of software](#) that stores and manages all the passwords and login information you use to access online sites, apps, and other services.

Not only does it keep your sensitive data and credentials safe, it also [generates unique and strong passwords](#) for you so you don't have to keep reusing the same ones across your devices and platforms.



Think of it as a notebook where you store your most valuable login credentials, locked by a master key known only to you.

How a Password Manager Works

A password manager stores your passwords in an encrypted form to protect them from prying eyes and improper access. It also displays your selection of login credentials so you don't have to remember hundreds of passwords on your own except the master password or in some cases the PIN you use to sign into the app.

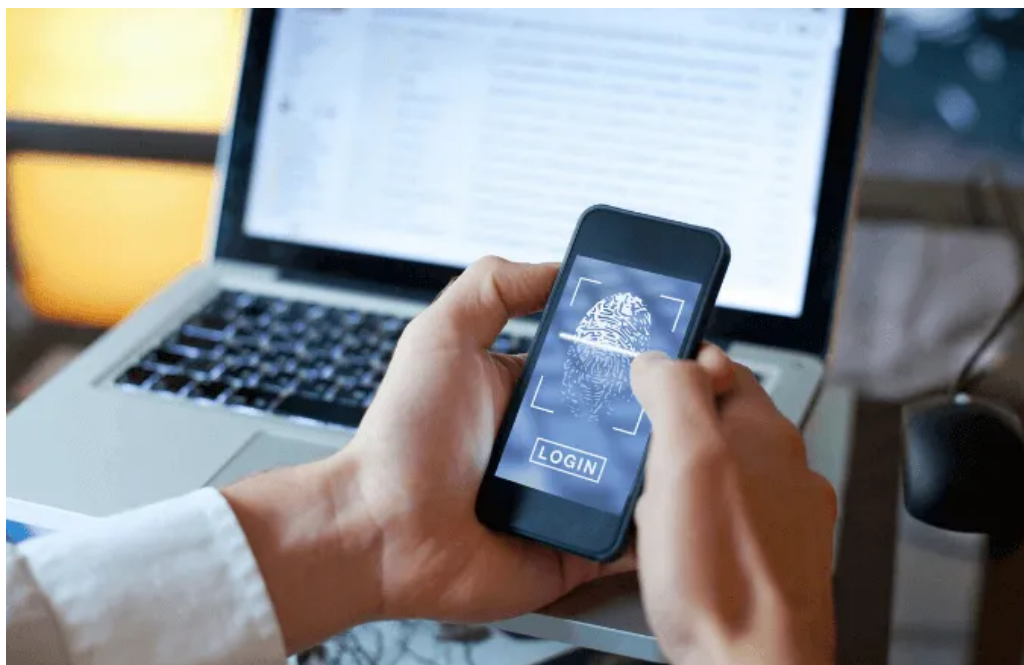
Some even let you authenticate your device using facial or fingerprint recognition instead of entering your master password as you can read in our [best password manager](#) guide. For even better security, some include the two-factor authentication in different forms such as Google Authenticator, biometrics, or SMS-based, depending on the app you pick.



Most password manager apps come with [browser extensions](#) that automatically fill in passwords for you, plus an encrypted sync feature that allows you to carry your passwords with you wherever you go and use it across all your Windows, Mac, Android and iOS devices.

Once you [install and set up the password manager](#), pull up the app, copy and paste your password into the login field, and access the service you need.

When you log into a secure site, the password manager will install a browser plugin that captures and replays your password and saves your login credentials. The next time you visit the same site, the app offers to fill in your logins for you automatically. Not all password managers have this feature though.

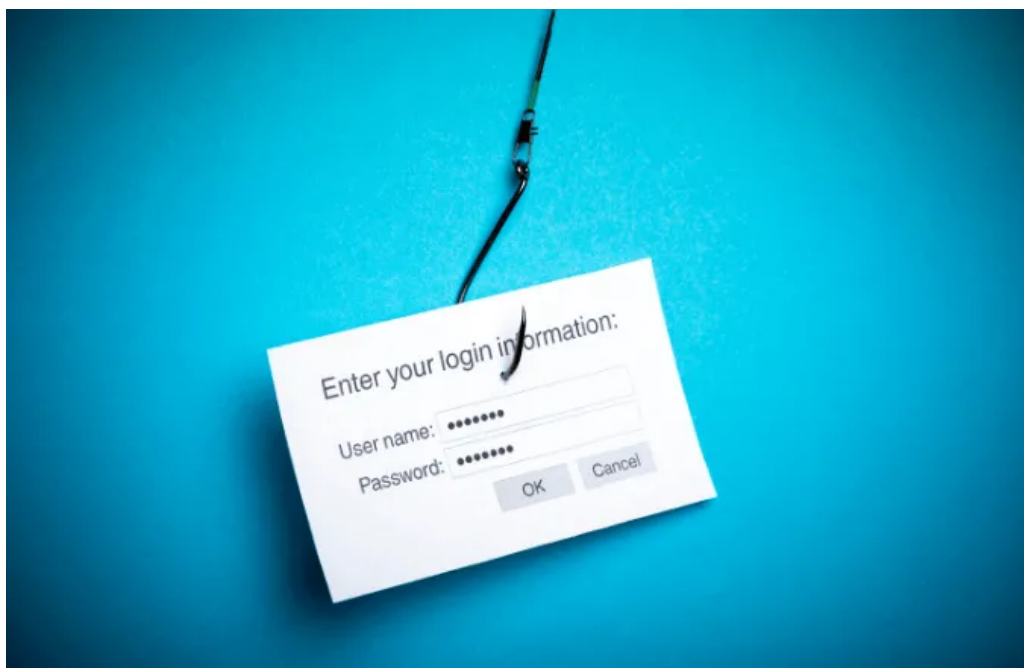


However, if you've saved multiple logins for the same site, the app will offer you multiple login options for your account. Depending on the password manager app you choose, you can find one with a browser toolbar menu with your saved logins so you can visit the saved site directly and get logged in automatically.

Some password managers can import your saved data from or export it to other products, making it easier when you want to switch to a new password manager. Others go further to provide secure online storage for your documents, and let you share your credentials with trusted people.

Most of them can flag your duplicate and weak passwords, offer help with updating them, and if you pick an advanced one, it can automate the process of changing passwords for you.

Are Password Managers Really Safe?



With all the recent cases of [identity theft and security breaches](#) happening around us, one would wonder whether using a password manager is more secure than keeping your sensitive login credentials to yourself.

You probably even heard of the [LastPass hacking attack](#) that happened in July 2015, which put their systems to the test. The goal was to access its password vaults, and though the hackers managed to get into the LastPass servers, they couldn't get through to steal user passwords.

Their attempt was unsuccessful because LastPass can't access each user's password vault, neither does it have their master passwords, meaning the passwords [stay encrypted](#) and locked down in your vault. This is why it's important to have a strong and unique password for all the apps, websites and services you log into.

Many of us use weak passwords or reuse the ones we already have on multiple accounts, which dispose us to identity theft and other crimes.

With a password manager, you'll get a better combination of convenience and security than you would without one, but that doesn't mean it's a magic pill.



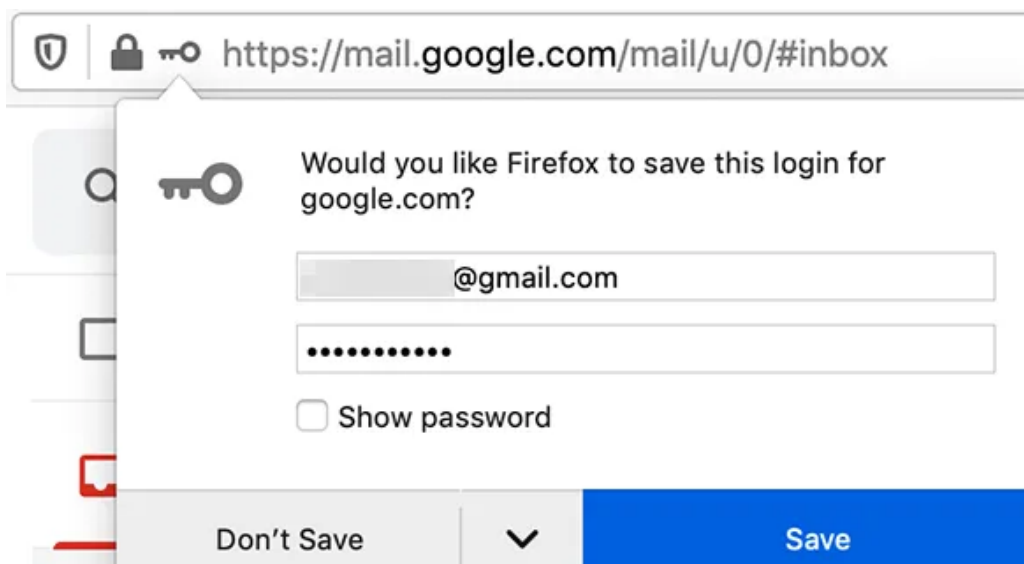
You should take [other security measures](#) to ensure your login data is kept under tight security like using two-factor authentication for your valued accounts, setting lock screens on all devices, and using [devices that you trust](#).

When you want to change to a different password manager app, simply export your data (if the app has this feature), delete your account, and you're good to go.

Note: Most password managers store your master password locally or on a server, but they can't read the password because it's encrypted. This keeps your data safe against breaches, but if you forget the password, you can't recover your account through the company.

Thankfully though, some password managers can help you recover your account by offering DIY kits, but if that doesn't work, then you have to create a new account and reset all your passwords manually for each app, website or online service and start over. Make sure to read our [comparison of LastPass, 1Password and Dashlane](#).

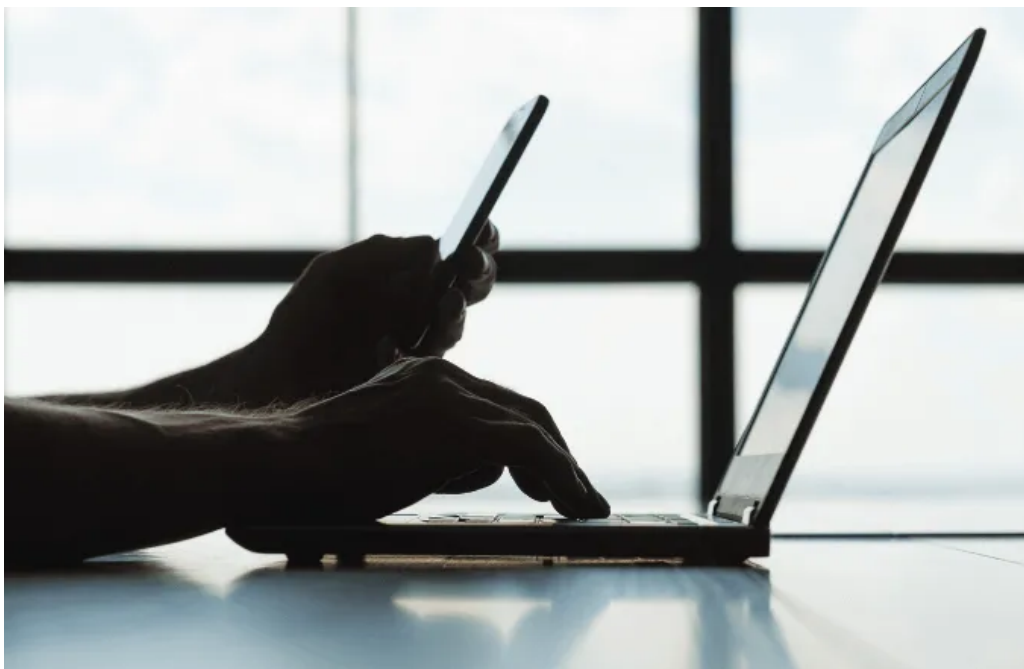
A Word About Using a Browser Password Manager



Your web browser probably has a built-in password manager though it's rudimentary, and nothing compared to what a dedicated password manager can do for you.

For example, the Chrome password manager can store your passwords on your computer, but they're not in encrypted form. This means that the password files on your computer are easily accessible to others, unless your device's hard drive is encrypted.

Users of Mozilla Firefox get to enjoy the Master Password feature that password manager apps offer, so you can encrypt and store your passwords on your computer. However, it doesn't generate passwords for you and it doesn't have the encrypted sync feature that lets you sync and use your login data across all your Windows, Mac, Android and iOS devices.



The same goes for iCloud Keychain, which is great if you're using Apple devices only, but it comes up short once you get a Windows or Android device that uses Chrome or Firefox browsers.

A dedicated password manager's singular goal is to protect your passwords, which is why you'll get more helpful features by using one. Your browser has other priorities so there's hardly any time to improve its password management functions.

Secure Your Digital Life

It's hard enough trying to memorize or remember a 30-character password full of text, numbers, and symbols, but forgetting it is a nightmare. Instead of saving your passwords on your phone, tablet, computer, in documents, sticky notes or autofill, get a password manager. It's a much better and more secure way of keeping your logins under lock and key, and your first defense against getting hacked.