How-To Geek

Why You Should Use a Password Manager and How to Get Started

The majority of people use very weak passwords and reuse them on different websites. How are you supposed to use strong, unique passwords on all the websites you use? The solution is a password manager.

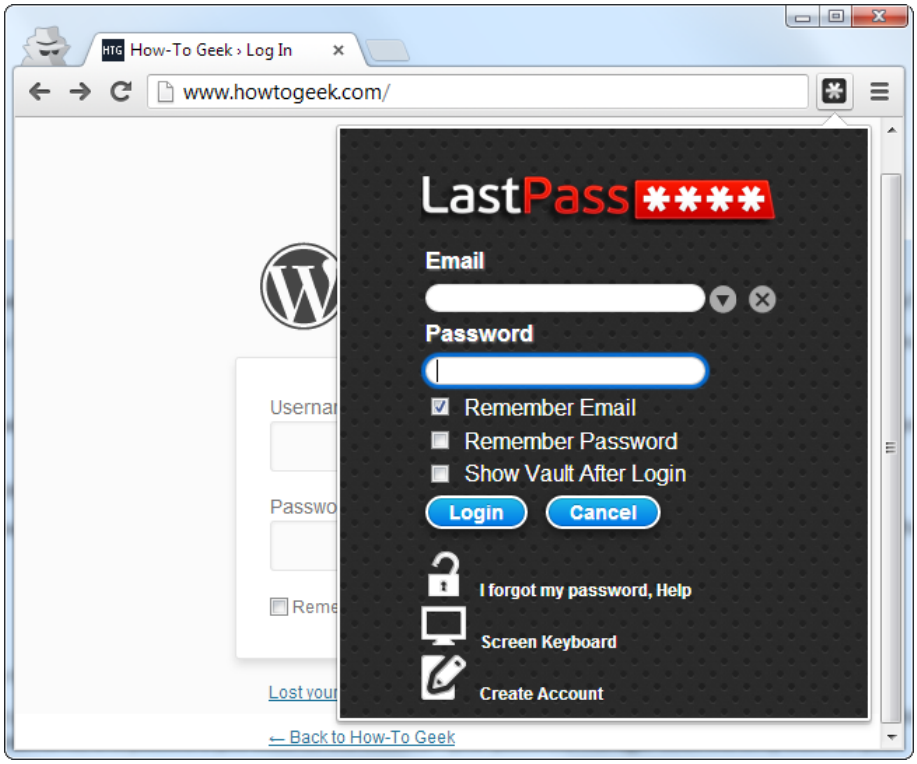
Password managers store your login information for all the websites you use and help you log into them automatically. They encrypt your password database with a master password – the master password is the only one you have to remember.

Don't Reuse Passwords!

Password reuse is a serious problem because of the many password leaks that occur each year, even on large websites. When your password leaks, malicious individuals have an email address, username, and password combination they can try on other websites. If you use the same login information everywhere, a leak at one website could give people access to all your accounts. If someone gains access to your email account in this way, they could use password-reset links to access other websites, like your online banking or PayPal account.

To prevent password leaks from being so damaging, you need to use unique passwords on every website. These should also be strong passwords – long, unpredictable passwords that contain numbers and symbols.

Web geeks have hundreds of accounts to keep track of, while even the average person likely has tens of different passwords. Remembering such strong passwords is nearly impossible without resorting to some sort of trick. The ideal trick is a password manager that generates secure, random passwords for you and remembers them so you don't have to.

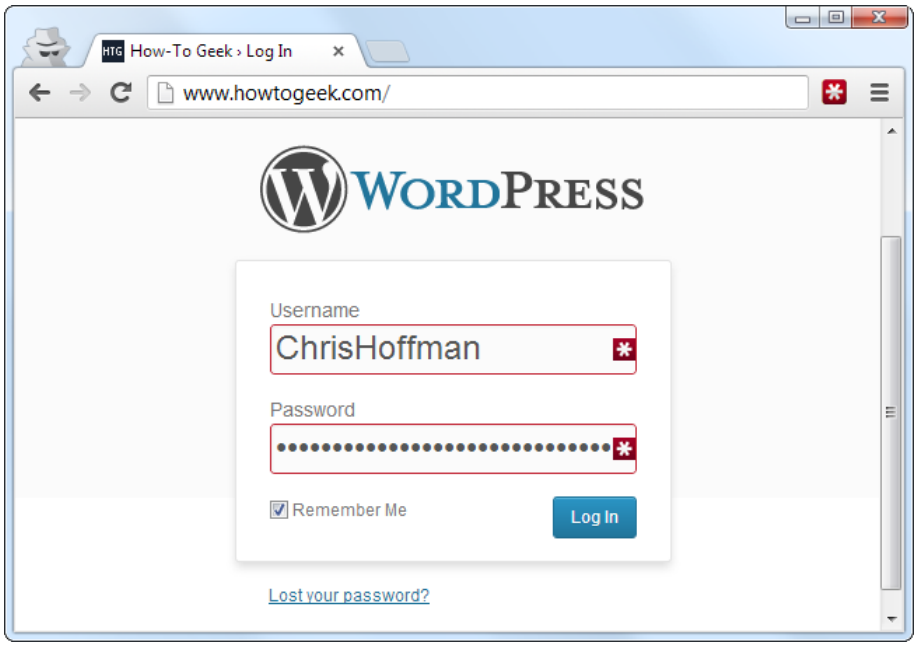


What Using a Password Manager is Like

A password manager will take a load off your mind, freeing up brain power for doing productive things rather than remembering a long list of passwords.

When you use a password manager and need to log into a website, you will first visit that website normally. Instead of typing your password into the website, you type your master password into the password manager, which automatically fills the appropriate login information into the website. (If you're already logged into your password manager, it will automatically fill the data for you). You don't have to think about what email address, username, and password you used for the website – your password manager does the dirty work for you.

If you're creating a new account, your password manager will offer to generate a secure random password for you, so you don't have to think about that, either. It can also be configured to automatically fill information like your address, name, and email address into web forms.



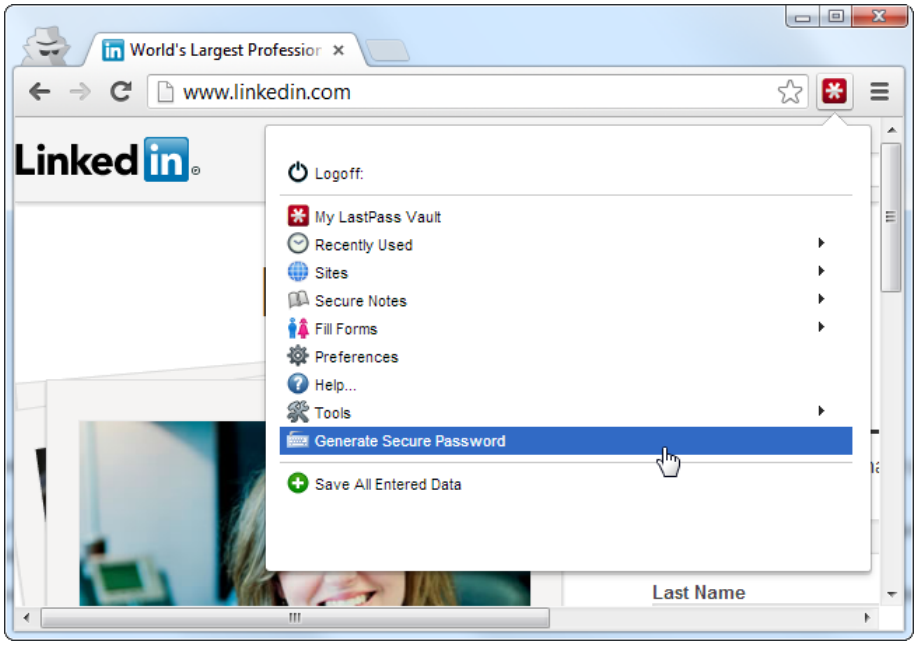
Why Browser-Based Password Managers Aren't Ideal

Web browsers – Chrome, Firefox, Internet Explorer, and others – all have integrated password managers. Each browser's built-in password manager can't compete with dedicated password managers. For one thing, Chrome and Internet Explorer store your

passwords on your computer in an unencrypted form. People could access the password files on your computer and view them, unless you encrypt your computer's hard drive.

Mozilla Firefox has a "master password" feature that allows you to encrypt your saved passwords with a single "master" password, storing them on your computer in an encrypted format. However, Firefox's password manager isn't the ideal solution, either. The interface doesn't help you generate random passwords and it lacks various features, such as cross-platform syncing (Firefox can't sync to iOS devices).

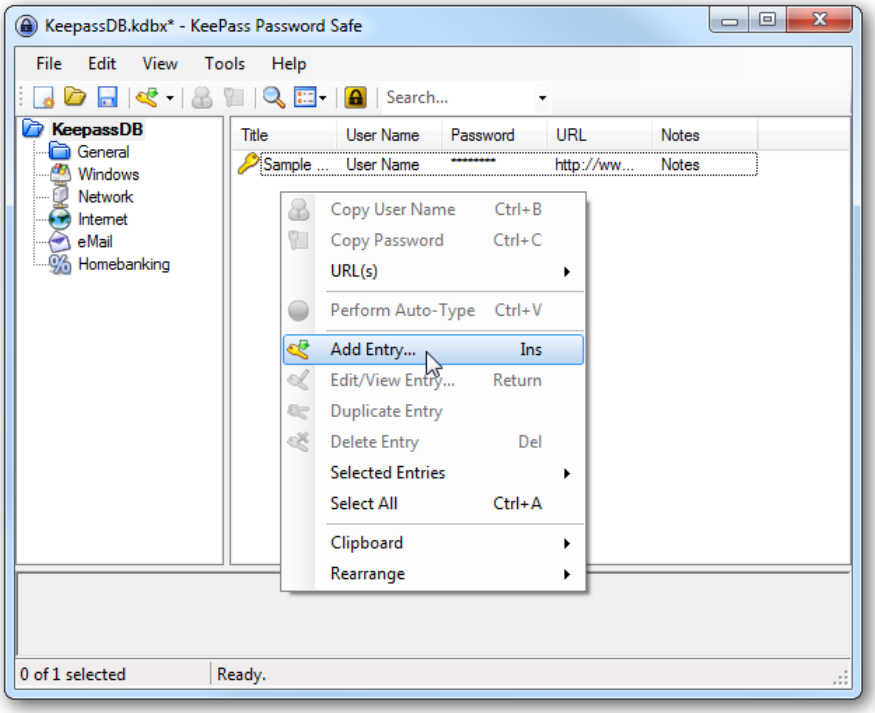
A dedicated password manager will store your passwords in an encrypted form, help you generate secure random passwords, offer a more powerful interface, and allow you to easily access your passwords across all the different computers, smartphones, and tablets you use.



Password Managers to Use

A variety of password managers are available, but two stand out as the best options. Each is a solid option, and which you prefer will depend on what's more important to you:

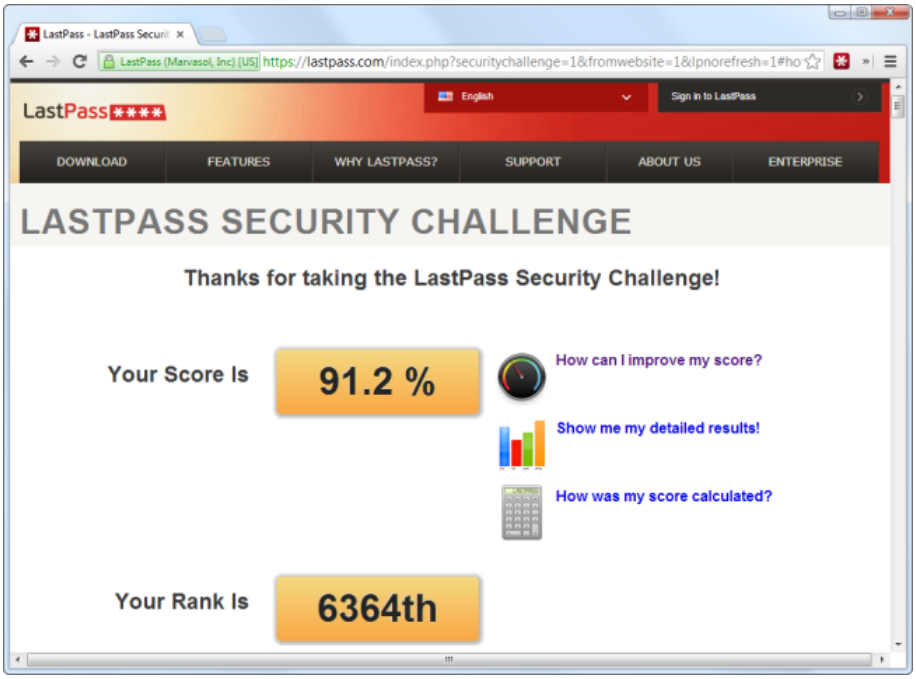
- LastPass: We love LastPass here at How-To Geek. It's a cloud-based password manager with extensions, mobile apps, and even desktop apps for all the browsers and operating systems you could want. It's extremely powerful and even offers a variety of two-factor authentication options so you can ensure no one else can log into your password vault. We've covered LastPass's many security options in great detail. LastPass stores your passwords on LastPass's servers in an encrypted form – the LastPass extension or app locally decrypts and encrypts them when you log in, so LastPass couldn't see your passwords if they wanted to. For more information about LastPass, read our guide to getting started with LastPass.
- KeePass: LastPass isn't for everyone. Some people just aren't comfortable with a cloud-based password manager, and that's fine. KeePass is a popular desktop application for managing your passwords, but there are also browser extensions and mobile apps for KeePass. KeePass stores your passwords on your computer so you remain in control of them — it's even open-source, so you could audit its code if you wanted to. The downside is that you're responsible for your passwords, and you'll have to sync them between your devices manually. Some people use a syncing solution like Dropbox to sync the KeePass database between their devices. For more information, check out our introduction to KeePass.



Getting Started with Your Password Manager

The first big decision you will need to make with a password manager is choosing your master password. This master password controls access to your entire password manager database, so you should make it particularly strong – it's the only password you'll need to remember, after all. You may want to write down the password and store it somewhere safe after choosing it, just in case – for example, if you're really serious, you could store your master password in a vault at the bank. You can change this password later, but only if you remember it – if you lose your master password, you won't be able to view your saved passwords. This is essential, as it ensures no one else can view your secure password database without the master password.

After installing a password manager, you will likely want to start changing your website passwords to more secure ones. LastPass offers the LastPass Security Challenge, which identifies the weak and duplicate passwords you should focus on changing.



Password managers also allow you to store other types of data in a secure form – everything from credit card numbers to secure notes. All data you store in a password manager is encrypted with your master password.

Password managers can even help against phishing, as they fill account information into websites based on their web address (URL). if you think you're on your bank's website and your password manager doesn't automatically fill your login information, it's possible that you're on a phishing website with a different URL.