SANS SECURITY AWARENESS

The Monthly Security Awareness Newsletter for You

Password Managers

Overview

One of the most important steps you can take to protect yourself is to use a unique, strong password for each of your accounts and apps. Unfortunately, it's almost impossible to remember all of the different passwords. In addition, we know it's time consuming to constantly have to type in your passwords at different sites, generate new passwords, track the answers to all your security questions, and numerous other factors. However, there is a solution that will make your life both much simpler and far more secure—password managers.

How Password Managers Work

Password managers work by storing all of your passwords in a database, which is sometimes called a vault. The password manager encrypts the vault's contents and protects it with a master password that only you know. When you need your passwords, such as to log in to your online bank or email account, you simply type your master password into your password manager to unlock the vault. The password manager will automatically retrieve the correct password and securely log you in to the website. You no longer have to remember your passwords or manually log in to your accounts.

In addition, most password managers include the ability to automatically synchronize across multiple devices. This way, when you update a password on your laptop, those changes are synchronized to all your other devices. Finally, most password managers detect when you're attempting to create a new online account or update the password for an existing account, and they automatically update the vault for you.

It's critical that the master password you use to protect the password manager is long and unique. In fact, we recommend you make your master password a passphrase—a long password made up of multiple words or phrases. If your password manager supports two-step verification, use that for your master password as well. Finally, be sure you remember your master passphrase. If you forget it, you will not be able to access any of your other passwords.

Choosing a Password Manager

There are many password managers to choose from. In the Resources section we provide a link to reviews of password managers. Meanwhile, when trying to find the one that's best for you, keep the following in mind:

Your password manager should be simple to use. If you find the solution too complex to understand, find a different one that better fits your style and expertise.

The password manager should work on all devices you need to use passwords on. It should also be easy to keep your passwords synchronized across all your devices.

Use only well-known and trusted password managers. Be wary of products that have not been around for a long time or have little or no community feedback. Cybercriminals can create fake password managers to steal your information. Also, be very suspicious of vendors that promote they developed their own encryption solution.

Avoid any password manager that claims to be able to recover your master password for you. This means they know your master password, which exposes you to too much risk.

Make sure whatever solution you choose, the vendor continues to actively update and patch the password manager, and be especially sure you are always using the most recent version.

The password manager should give you the option of storing other sensitive data, such as the answers to your secret security questions, credit card information, and frequent flier numbers.

Consider writing your master passphrase in a sealed envelope and storing it in a locked cabinet, physical safe, or lockbox.

Password managers are a great way to securely store all your passwords and other sensitive data, such as credit card numbers. However, make sure to use a unique, strong master passphrase and always use the latest version of whichever solution you choose.

Subscribe to OUCH! and receive the latest security tips in your email every month - sans.org/ouch.
Do you think you've got what it takes to get into the cybersecurity industry? Or are you looking to improve your existing skillset? Training with SANS helps you achieve your goals. Level Up with SANS today! sans.org/Level-Up-Ouch

Guest Editor

Russell Eubanks *is an information security leader based in Atlanta, with over 20 years of experience, and holds many security certifications. He is a Handler with the SANS Internet Storm Center and is a contributor to the Critical Security Controls. Russell can be reached at @russelleubanks and https://www.securityeverafter.com.*

Resources

Making Passwords Simple:	http://www.sans.org/u/10Uu
Digital Inheritance:	http://www.sans.org/u/10Uz
Wired Review of Best Password Managers:	https://www.wired.com/story/best-password-managers/