OUCH! | September, 2017

The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

- Overview
- How Password Managers Work
- Choosing Password Managers

Password Managers

Overview

One of the most important steps you can take to protect yourself online is to use a unique, strong password for every one of your accounts and apps. Unfortunately, it is most likely impossible for you to remember all your different passwords for all your different accounts. This is why so many people reuse the same password. Unfortunately, reusing the same password for different accounts is dangerous, because once someone compromises your password, they can access all your accounts that use the same password. A simple solution is to use a password manager, sometimes called a password vault. These are programs that securely store all your passwords, making it easy to have a different password for each account. Password managers make this simple, because instead of having to remember all your passwords, you only have to remember the master password to your password manager.

Guest Editor

Chris Christianson is an Information Security Consultant based in California, with 20 years of experience and numerous technical certifications. He has spoken at a variety of conferences and is a contributor to many industry articles. Chris can be reached at **@cchristianson** and **https://ismellpackets.com**.

How Password Managers Work

Password managers work by storing all 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 to retrieve your passwords, such as to log in to your online bank or email, you simply type your master password into your password manager to unlock the vault. In many cases, the password manager will automatically retrieve your password and securely log in for you. This makes it simple to have hundreds of unique, strong passwords, since you do not have to remember them.

Some password managers store your vault on your computer or mobile device, while others store it in the Cloud. In addition, most password managers include the ability to automatically synchronize your password vault's contents across multiple devices that you authorize. This way, when you update a password on your laptop, those changes are

Password Managers

synchronized to all your other devices. Regardless where the database is stored, you need to install the password manager application on your system or device to use it.

When you first set up a password manager, you need to manually enter or import your logins and passwords. Afterwards, the password manager can detect when you're attempting to register for a new online account or update the password for an existing account, automatically updating the vault accordingly. This is possible because most password managers work hand-in-hand with your web browser. This integration also allows them to automatically log you into websites.

Password managers are a simple way to securely store and use all your different passwords.

It's critical that the master password you use to protect the password manager's contents is strong and very difficult for others to guess. In fact, we recommend you make your master password a passphrase, one of the strongest types of passwords possible. If your password manager supports two-step verification, use that for your master password. Finally, be sure you remember your master password. 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 for you 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. Cyber criminals can create fake password managers to steal your information. Also, be very suspicious of any vendors that developed their own encryption solution.

Password Managers

- 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 sure you are always using the latest version.
- The password manager should include the ability to automatically generate strong passwords for you and show you the strength of the passwords you've chosen.
- The password manager should give you the option of storing other sensitive data, such as the answers to your secret security questions, credit cards, or frequent flier numbers.

Password managers are a great way to securely store all your passwords and other sensitive data. However, since they safeguard such important information, make sure you use a unique, strong master password that is not only hard for an attacker to guess, but easy for you to remember.

Subscribe to OUCH!

Get the OUCH! security awareness newsletter every month for free, in the language of your choice. Simply subscribe at https://securingthehuman.sans.org/ouch.

Resources

Top Password Managers of 2017:	https://www.pcmag.com/article2/0,2817,2407168,00.asp
Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Two-step Verification:	https://www.securingthehuman.org/ouch/2015#september2015
Lock Down Your Login:	https://www.lockdownyourlogin.org/
SANS Security Tip of the Day:	https://www.sans.org/tip-of-the-day

License