OUCH! | October 2015

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Overview
- How Password Managers Work
- Choosing a Password Manager

Password Managers

Overview

One of the most important steps you can take to protect yourself online is to use a unique, strong password for each of your accounts. Unfortunately, most of us have so many accounts that it's almost impossible to remember all of our passwords. A simple solution is to use a password manager, sometimes called a password vault. These applications are designed to securely store your login credentials. Moreover, they can make it much easier for you to log into websites, mobile apps and other applications.

Guest Editor

Lenny Zeltser focuses on safeguarding customers' IT operations at NCR Corp and trains security professionals at the SANS Institute. Lenny is active on Twitter as **@lennyzeltser** and publishes articles at **zeltser.com**.

How Password Managers Work

A password manager acts like a digital safe; it securely stores your usernames, passwords and other sensitive information. When a website requires you to login to your account, the password manager can automatically retrieve your password and securely log you into the website. This makes it simple to have hundreds of unique, strong passwords, since you do not have to remember them.

Password managers store your details 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 credentials, perhaps to log into your online bank or email accounts, you simply type your master password into your password manager to unlock the vault.

Some password managers store your vault on your local system or smartphone, while others store it on a remote website maintained by the company that built the password manager. In addition, most password managers include the ability to automatically synchronize the vault's contents across multiple devices that you authorize. This way, when you update a password on your laptop, those changes are synchronized to your smartphone, tablet or any other computers you are using. Regardless where the database is stored, you need to install the password manager application on your system or device to use it.

Password Managers

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 of your different passwords.

Password managers are designed to securely store your sensitive data. However, it's critical that the master password you use to protect the vault's contents is strong and very difficult for others to guess. In fact, we recommend you make your master password a passphrase, which is one of the strongest types of passwords possible. If your password manager supports two-step verification, use that for your master password. Finally, make sure that you do not use your master password for any other system or account. This way, even if a hacker manages to obtain a copy of your vault, they will be unable to guess the password and access its contents. 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 free and commercial password managers to choose from. When trying to find the one that's best for you, please keep the following in mind:

- Confirm that the password manager will work on all the systems and mobile devices where you might need to access your vault. The solution should also make it easy to keep the vault's contents synchronized across all of 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 to no community feedback. Just like fake anti-virus software, cyber criminals can create fake password managers to steal your information.
- Your password manager should be simple for you to use. If you find the solution too complex to understand, find an alternative that better fits your style and expertise.

- Make sure whatever solution you choose continues to be actively updated and patched, and be sure you are always using the latest version.
- The password manager should make it easy for you to select strong passwords for your various accounts, including the ability to automatically generate strong passwords 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.
- Be wary of password managers that employ proprietary or unknown encryption techniques, rather than encrypting your vault using industry-standard methods. If the vendor advertises how they developed their own encryption solution, stay away from them.
- 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 much more risk.

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

National Cyber Security Awareness Month

Come celebrate security awareness month with us as we provide numerous resources to help you, your family and your organization stay safe and secure online. http://www.securingthehuman.org/resources/ncsam

Resources

Passphrases:	http://www.securingthehuman.org/ouch/2015#april2015
Two-step Verification:	https://www.securingthehuman.org/ouch/2015#september2015
Top Five Password Managers:	http://lifehacker.com/5529133/five-best-password-managers
SANS Security Tip of the Day:	http://www.sans.org/tip_of_the_day.php

License

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus