OUCH! | August 2020

OUCH!

SANS SECURITY AWARENESS

The Monthly Security Awareness Newsletter for You

Making Passwords Simple

Overview

You are often told your passwords are key to protecting your accounts (which is true!), but rarely are you given a simple way to securely create and manage all your passwords. Below we cover three simple steps to simplify your passwords, lock down your accounts, and protect your future.

Passphrases

The days of crazy, complex passwords are over. Those passwords are hard to remember, difficult to type, and with today's super-fast computers can be easy for a cyber attacker to crack. The key to passwords is to make them long; the more characters you have the better. These are called passphrases: a type of strong password that uses a short sentence or random words. Here are two examples:

Time for strong coffee!

lost-snail-crawl-beach

Both of these are strong, with over twenty characters, easy to remember, and simple to type but difficult to crack. You will run into websites or situations requiring you to add symbols, numbers, or uppercase letters to your password, which is fine. Remember though, it's length that is most important.

Password Managers

You need a unique password for every account. If you reuse the same password for multiple accounts, you are putting yourself in great danger. All a cyber attacker needs to do is hack a website you use, steal all the passwords including yours, then use your password to log in to all your other accounts as you. It happens far more often than you realize. Don't believe it? Check out the website www.haveibeenpwned.com to see what sites you use that have been hacked and your passwords potentially compromised. So what should you do? Use a password manager.

These are special computer programs that securely store all your passwords in an encrypted vault. You only need to remember one password: the one for your password manager. The password manager then automatically retrieves your passwords

whenever you need them and logs you in to websites for you. They also have other features such as storing your answers to secret questions, warning you when you reuse passwords, a password generator that ensures you use strong passwords, and many other features. Most password managers also securely sync across almost any computer or device, so regardless of what system you are using you have easy, secure access to all your passwords.

Finally, be sure to write down the password to your password manager and store that in a secure location at home. Some password managers even let you print out a password manager recovery kit. That way, if you forget the password to your password manager you have a backup. Or, if you get sick or find yourself in an emergency, your spouse or trusted family member can retrieve the information on your behalf.

Two-Step Verification

Two-step verification (often called two-factor authentication or multi-factor authentication) adds an additional layer of security. It requires you to have two things when you log in to your accounts: your password and a numerical code which is generated by your smartphone or sent to your phone. This process ensures that even if a cyber attacker gets your password, they still can't get into your accounts. Two-step verification is simple to set up and you usually only need to use it once when you log in from a new computer or device. Enable this whenever possible, especially for your most important accounts such as your bank or retirement accounts, or access to your email. If you are using a password manager, we highly recommend you protect it with a strong passphrase AND two-step verification.

It may sound silly, but these three simple steps go a long way in protecting your job, your reputation, and your financial future.

Subscribe to OUCH! and receive the latest security tips in your email every month - www.sans.org/security-awareness/ouch-newsletter.

Guest Editor

Justin Henderson *(@SecurityMapper) is co-founder of H & A Security Solutions, a Certified SANS Institute Instructor, and author for the SANS Cyber Defense and SIEM courses. He loves all things cyber defense and has been consulting for fifteen years.*

Resources

Have I Been Pwned:	https://haveibeenpwned.com/
Two-factor Authentication Site:	https://twofactorauth.org/
Long Live the Passphrase:	http://www.sans.org/u/OKJ
Time for Password Expiration to Die:	http://www.sans.org/u/OKO
NIST SP800-63B Digital Identity Guidelines:	https://pages.nist.gov/800-63-3/sp800-63b.html