OUCH! | May 2013

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- Strong Passwords: Passphrases
- Using Passwords Securely
- Resources

Passwords

Background

Passwords are one of the primary ways we prove who we are. It is how you access your email, bank online, purchase goods and access devices such as your laptop or smartphone. In many ways, passwords are the keys to your kingdom. As a result, if someone has your password, they can steal your identity, transfer your money or access all of your personal information. Strong passwords are essential to protecting your identity and information. Let's learn what makes a strong password and how to use them securely.

Guest Editor

Raul Siles is the guest editor for this issue of OUCH! Raul is the founder of and a senior security analyst at Taddong, and also a SANS author, instructor and security passionate. You can follow Raul on Twitter at @taddong and on his blog at blog.taddong.com.

Strong Passwords: Passphrases

The problem is cyber criminals have developed sophisticated programs that can guess, or "brute force," your passwords, and they are constantly getting better at it. This means they can steal your passwords if they are weak or easy to guess. Never use common information for your passwords, such as your birth date, your pet's name or anything else that can be easily determined from your social networking posts or Google. Instead, the best way to create a strong password is to use a long password, and the more characters you have, the better. In fact, instead of using a single word, use multiple words -- or even a complete sentence. This type of password is called a passphrase, and it is one of the strongest you can use. Here is an example of one:

time for my coffee

That is it; that is all you need. If required, you can make your password even stronger by adding symbols, capital letters or numbers, such as those you see in the example below. This is especially important if you are using a website that does not allow multiple words or a complete sentence for your password:

Time f0r my coffee!

Passwords

Notice how this example uses a capital letter. You can also replace letters with numbers or symbols, such as replacing the letter 'a' with the '@' symbol and the letter 'o' with the number zero, or use common punctuation marks such as a question mark, period or even spaces. If a website or program limits the number of characters you can use in a password, use the maximum number of characters allowed.

Use strong passwords, preferably passphrases made up of multiple words, and be sure to use them securely.

Using Passwords Securely

In addition to using strong passwords, you must be careful how you use them. Having a strong password is no good if bad guys can easily steal or copy it.

1. Be sure to use different passwords for different accounts. For example, never use the passwords for your work or bank accounts as the passwords for your personal accounts, such as Facebook, YouTube or Twitter. This way, if one of your passwords is hacked, the other accounts are still safe. If you have too many passwords to remember, consider using a password manager. This is a special program you run on your computer or mobile device that securely stores all of your passwords for you. The only passwords you need to remember are the ones to your computer and the password manager program. If your passwords are for work, then check with your supervisor or your help desk to see if using a password manager is permitted in your organization.

2. Never share your password with anyone else, including co-workers. Remember, your password is a secret; if anyone else knows your password it is no longer secure. If you accidently share your password with someone else or believe it may have been compromised or stolen, be sure to change it immediately.

3. Do not use public computers, such as those at hotels or libraries, to log into a work or bank account. Since anyone can use these computers, they may be infected with malicious code that captures all of your keystrokes. Only log in to your work or bank accounts on trusted computers or mobile devices you control.

Passwords

4. Be careful of websites that require you to answer personal questions. These questions are used if you forget your password and need to reset it. The problem is the answers to these questions can often be found on the Internet, or even your Facebook page. Make sure that if you answer personal questions you only use information that is not publicly available or fictitious information you have made up. Password managers can help with this, as many allow you to store this additional information.

5. Many online accounts offer something called two-factor authentication, or two-step verification. This is where you need more than just your password to log in, such as codes sent to your smartphone. This option is much more secure than just a password by itself. Whenever possible, always use these stronger methods of authentication.

6. Mobile devices often require a PIN to protect access to them. Remember that a PIN is nothing more than another password. The longer your PIN is, the more secure it is. In fact, many mobile devices will allow you to change your PIN number to an actual password.

7. Finally, if you are no longer using an account, be sure to close, delete or disable it.

Become a Security Professional

Become a certified security professional from the largest and most trusted security training organization in the world at SANSFIRE. Over 40 security classes taught by the world's leading experts. 14-23 June in Washington DC. http://www.sans.org/event/sansfire-2013

Resources

Two-Step Verification:	http://www.google.com/landing/2step
Password Managers:	http://www.freepasswordmanager.com
Password Strength:	https://xkcd.com/936
Common Security Terms:	http://www.securingthehuman.org/resources/security-terms
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis