Passphrases

Background

Passwords are something you use almost every day, from accessing your email or banking online to purchasing goods or accessing your smartphone. However, passwords are also one of your weakest points; if someone learns or guesses your password they can access your accounts as you, allowing them to transfer your money, read your emails, or steal your identity. That is why strong passwords are essential to protecting yourself. However, passwords have typically been confusing, hard to remember, and difficult to type. In this newsletter, you will learn how to create strong passwords, called passphrases, that are easy for you to remember and simple to type.

Passphrases

The challenge we all face is that cyber attackers have developed sophisticated and effective methods to brute force (automated guessing) passwords. This means bad guys can compromise your passwords if they are weak or easy to guess. An important step to protecting yourself is to use strong passwords. Typically, this is done by creating complex passwords; however, these can be hard to remember, confusing, and difficult to type. Instead, we recommend you use passphrases--a series of random words or a sentence. The more characters your passphrase has, the stronger it is. The advantage is these are much easier to remember and type, but still hard for cyber attackers to hack. Here are two different examples:

Sustain-Easily-Imprison
Time for tea at 1:23

What makes these passphrases so strong is not only are they long, but they use capital letters and symbols. (Remember, spaces and punctuation are symbols.) At the same time, these passphrases are also easy to remember and type.

You can make your passphrase even stronger if you want to by replacing letters with numbers or symbols, such as replacing the letter 'a' with the '@' symbol or the letter 'o' with the number zero. If a website or program limits the number of characters you can use in a password, use the maximum number of characters allowed.

Using Passphrases Securely

You must also be careful how you use passphrases. Using a passphrase won't help if bad guys can easily steal or copy it.

1. Use a different passphrase for every account or device you have. For example, never use the same passphrase for your work or bank account that you use for your personal accounts, such as Facebook, YouTube, or Twitter. This way, if one of your accounts is hacked, your other accounts are still safe. If you have too many passphrases to remember (which is very common), consider using a password manager. This is a special program that securely stores all your passphrases for you. That way, the only passphrases you need to remember are the ones to your computer or device and the password manager program.

2. Never share a passphrase or your strategy for creating them with anyone else, including coworkers or your supervisor. Remember, a passphrase is a secret; if anyone else knows your passphrase it is no longer secure. If you accidentally share a passphrase with someone else, or believe your passphrase may have been compromised or stolen, change it immediately. The only exception is if you want to share your key personal passphrases with a highly trusted family member in case of an emergency. One approach is to write down your key personal passphrases (make sure they are not work related), store them in a secure location, and share that location with a highly trusted family member. That way, if something happens to you and you need help, your loved ones can access your critical accounts.
3. Do not use public computers, such as those at hotels or Internet cafés, to log in to your accounts. Since anyone can use these computers, they may be infected and capture all your keystrokes. Only log in to your accounts on trusted computers or mobile devices.
4. Be careful of websites that require you to answer personal questions. These questions are used if you forget your passphrase and need to reset it. The problem is the answers to these questions can often be found on the Internet, or even on your Facebook page. Make sure that if you answer personal questions you use only information that is not publicly available or fictitious information you have made up. Can't remember all those answers to your security questions? Select a theme like a movie character and base your answers on that character. Another option is, once again, to use a password manager. Most of them also allow you to securely store this additional information.
5. Many online accounts offer something called two-factor authentication, also known as two-step verification. This is where you need more than just your passphrase to log in, such as a passcode sent to your smartphone. This option is much more secure than just a passphrase by itself. Whenever possible, always enable and 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. Many mobile devices allow you to change your PIN number to an actual passphrase or use a biometric, such as your fingerprint.
7. If you are no longer using an account, be sure to close, delete, or disable it.

Subscribe to OUCH! and receive a copy every month – www.sans.org/security-awareness/ouch-newsletter

Guest Editor

My-Ngoc Nguyen (@MenopN) is a Certified SANS instructor and CEO/Principal Consultant for Secured IT Solutions. She brings expertise with top certifications and 16+ years of developing, maturing, and managing cyber security programs for various industries and sectors.