OUCH! December 2023

The Power of the Passphrase

Are you tired of constantly creating complex passwords? Frustrated with having to remember and type all those characters, symbols and numbers? Well, we have a solution for you: the ever-powerful passphrase!

Passphrases

You may not realize it but passwords are one of the primary attack vectors for cyber attackers. Bad actors are targeting your passwords, and if they can guess correctly or hack the right one, they can easily access your email, bank accounts, or perhaps steal your entire identity. The weaker your passwords, the easier it is for them to get in. As such, strong passwords are one of the most effective ways to protect your accounts and online digital life. Traditionally, you were trained to use highly complex passwords. The idea was that the greater the complexity, the harder for cyber attackers and their automated programs to guess the password. But the problem with that is complex passwords are also hard to both remember and type accurately. An even better way to create a strong, secure password is something called a passphrase. Instead of complexity these are strong because of their length. Here's a couple examples:

Time for strong coffee!
lost-snail-crawl-beach

Passphrases are nothing more than a series of words and can contain over twenty characters if a site allows it. That may seem like a lot but both examples above contain more than twenty characters, and unlike passwords, passphrases are much easier to remember and simpler to type. The longer the passphrase, the more secure it is. In some situations, you may be asked to add some complexity to your passphrase — i.e., adding symbols, uppercase letters, or numbers. The easiest way to do this is to modify some of the letters in your passphrase with symbols or numbers. For example, by replacing the letter e with the number 3, the above examples become more complex, yet are still easy enough to remember and type:

Tim3 for strong coff33!
lost-snail-crawl-b3ach

Keep it Unique

In order for the passphrase to be truly secure, it also needs to be unique for every account. If you reuse the same passphrase, or one that contains an easily identifiable pattern, for multiple accounts, you are putting yourself in danger.

All a cyber attacker needs to do is hack one website you use frequently, steal the passphrase you use for that particular website, and if all your passwords/passphrases are the same they will then have access to all your other accounts. Can't remember all those long, unique passphrases for each of your accounts? We have a solution for you: password managers.

Password managers are special computer programs that securely store all your passwords in an encrypted vault protected by a primary password. To access the vault, you only need to remember the primary password. The password manager can automatically retrieve your passwords whenever you need them and will automatically log into websites for you. Password managers have evolved to contain other features, including storing answers to secret questions, warning you when you reuse passwords or end up on a spoofed website, using generators that will create strong passwords or passphrases for you, and many more. 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.

The Final Step – Multi-Factor Authentication

A final step to making your passphrases truly foolproof is adding a second layer of protection to them - something called Multi-Factor Authentication (MFA). MFA requires you to have two pieces of identification when you login to your accounts. This could be your password and a biometric like a fingerprint; or it could be your password and an auto-generated numerical code that is sent to a different device or email account. The code is unique every time and can be generated from a mobile phone or another trusted device. This process ensures that even if a cyber attacker gets your passphrase they still can't get into your accounts, as they don't have the second factor. MFA should be enabled whenever possible, especially for your most important accounts such as your banking, retirement, or personal email accounts. If you are using a password manager, it is highly recommended you protect it with a strong passphrase AND multi-factor authentication.

Passphrases are a great way to both simplify security and help secure your accounts. To make your online digital life even simpler and more secure, we suggest combining the power of password managers and MFA for your passphrases.

Guest Editor

Quintana Patterson is an IT Clinical and Compliance Manager for the University of Colorado Anschutz Medical Campus and chair of the WiCyS (Women in CyberSecurity) Equity Advocacy Committee. She is committed to ensuring women in this industry feel welcomed, supported, and valued.

Resources

Password Managers: https://www.sans.org/newsletters/ouch/power-password-managers/
Biometrics: https://www.sans.org/newsletters/ouch/biometrics-making-security-simple/
Multi-Factor Authentication: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/