The Power of the Passphrase: Why Longer Beats Smarter

A Simple Password, a Big Problem

Daniel had always considered himself "pretty good with computers." He shopped online, managed his finances digitally, and stayed in touch with friends through social media. Like many people, he protected his personal email account with a password he had used for years. It was short, easy to remember, and included his favorite sports team with a symbol and a number. He figured that was good enough.

One morning, Daniel woke up to dozens of notifications. Password reset emails, failed login alerts, and messages from friends asking why he was sending them strange links. His email account had been hacked into overnight. Once inside, the attacker reset passwords for his social media, shopping, and cloud storage accounts. Within hours, fake messages were sent to his contacts, purchases were made in his name, and private photos were downloaded.

The root cause wasn't sophisticated hacking or advanced malware. The most likely cause was a weak reused password that had either been exposed in a data breach at another website or simply guessed by the attacker's automated tools. A single weak password gave a cybercriminal the keys to Daniel's entire digital life.

Why Passwords Fail Us

Passwords are still the most common way we protect our online accounts, but they are also one of the weakest points in our security. Cybercriminals don't usually guess passwords one try at a time like in the movies. Instead, they use automated tools that can test millions or even billions of password combinations very quickly. They also rely heavily on stolen password lists from past breaches. If you reuse passwords or choose short and predictable ones, attackers already have a head start.

Strong passwords are one of the most fundamental ways to protect your accounts and online digital life. The problem with complex passwords, though, is they are hard to remember and hard to type. An even better way to create a strong, secure password is something called a "passphrase." A passphrase is simply a password made up of multiple words, sometimes combined into a short phrase. Instead of just complexity, these are strong because of their length. For example:

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

Longer passphrases are significantly harder for automated tools to crack, yet they remain easy to remember and type. In some situations, you may be asked to add some complexity to your passphrase, such as adding symbols, uppercase letters, or numbers.

Keep Your Passphrases Unique

Length alone is not enough. Your passphrase must also be unique for each account. If you reuse the same password or passphrase across multiple sites, a breach on just one account can expose all your other accounts. Attackers routinely test stolen credentials across email, banking, and social platforms in a process called credential stuffing.

Securely Storing all Those Passphrases

Can't remember all those long unique passphrases for each of your accounts? We have another solution for you: password managers. These 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 you 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.

Take it One Step Further

Even the strongest passphrase is not perfect. That's why you should enable multi-factor authentication (MFA) wherever possible. MFA adds an extra layer of protection by requiring something you have, such as a one-time code sent to another device, or something you are, such as a biometric check. This means that even if a passphrase is stolen, attackers are still blocked.

Simple Habits, Powerful Protection

Daniel's story could have ended very differently if he had used a long, unique passphrase and perhaps even enabled MFA. Weak or reused passwords are still very common, and allow cybercriminals to target you regardless of how otherwise careful or experienced you may be.

Guest Editor

Tarun Preetham Bulla is a cybersecurity educator and practitioner with industry experience in incident response, forensics, and threat detection. Tarun teaches undergraduate cybersecurity courses, manages cyber labs, mentors capstone projects, and focuses on preparing students for the workforce by integrating real-world industry expertise into education.

Resources

The Power of Password Managers: https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager
How Cybercriminals Steal Your Passwords: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/
Moving Beyond Passphrases: https://www.sans.org/newsletters/ouch/passkeys-simpler-safer-way-sign-in

You can find more Ouch! On the following link: https://www.sans.org/newsletters/ouch