Creating Strong Passwords

2022-04-29 - Eric Ruthenberg - Comments (0) - General

UNDER LOCK AND KEY

Creating strong passwords offers greater security for minimal effort

You can buy a small padlock for less than a dollar—but you shouldn't count on it to protect anything of value. A thief could probably pick a cheap lock without much effort, or simply break it. And yet, many people use similarly flimsy passwords to "lock up" their most valuable assets, including money and confidential information.

Fortunately, everyone can learn how to make and manage stronger passwords. It's an easy way to strengthen security both at work and at home.

What Makes a Password 'Strong'?

Let's say you need to create a new password that's at least 12 characters long, and includes numerals, symbols, and upper- and lowercase letters. You think of a word you can remember, capitalize the first letter, add a digit, and end with an exclamation point. The result: Strawberry1!

Unfortunately, hackers have sophisticated password-breaking tools that can easily defeat passwords based on dictionary words (like "strawberry") and common patterns, such as capitalizing the first letter.

Increasing a password's complexity, randomness, and length can make it more resistant to hackers' tools. For example, an eight-character password could be guessed by an attacker in less than a day, but a 12-character password would take two weeks. A 20-character password would take 21 centuries.

You can learn more about creating strong passwords in your organization's security awareness training. Your organization may also have guidelines or a password policy in place.

Why Uniqueness Matters

Many people reuse passwords across multiple accounts, and attackers take advantage of this risky behavior. If an attacker obtains one password—even a strong one—they can often use it to access other valuable accounts.

Here's a real-life example: Ten years ago, Alice joined an online gardening forum. She also created an online payment account and used the same password. She soon forgot about the gardening forum, but someone accessed

her payments account years later and stole a large sum of money.

Alice didn't realize the gardening forum had been hacked, and that users' login credentials had been leaked online. An attacker probably tried reusing Alice's leaked password on popular sites—and eventually got lucky.

Guarding Your Passwords

1. **Don't write them down** – Many make the mistake of writing passwords on post-it notes and leaving them in plain sight. Even if you hide your password, someone could still find it. Similarly, don't store your login information in a file on your computer, even if you encrypt that file.
2. **Don't share passwords** – You can't be sure someone else will keep your credentials safe. At work, you could be held responsible for anything that happens when someone is logged in as you.
3. **Don't save login details in your browser** – Some browsers store this information in unsafe ways, and another person could access your accounts if they get your device.

TIPS FOR FAMILY AND FRIENDS

Consider sharing what you've learned about passwords and ask family and friends about their cybersecurity knowledge or experiences.

1. **Never reuse passwords** – Create a unique, strong password for each account or device. This way, a single hacked account doesn't endanger other accounts.
2. **Create complex, long passwords** – Passwords based on dictionary words, pets' names, or other personal information can be guessed by attackers.
3. **Use a password manager** – These tools can securely store and manage your passwords and generate strong new passwords. Some can also alert you if a password may have been compromised.