Windows 10 Password Security

ODDS ARE THAT YOUR PASSWORD IS WEAK

Most people don't have good password habits. They either don't know how to easily create and manage them, or assume a strong one needs to be an arbitrary combination of letters, numbers, and symbols. Here are two ways to dramatically increase your level of password protection, without sacrificing convenience:

MNEMONIC OVER NUMERIC

1. Start with a memorable phrase.

For example, the first six words of Abraham Lincoln's famous Gettysburg Address, "Four score and 7 years ago" is a simple passphrase. The quote meets the majority of password standards: 8-32 characters in length and includes capital and lowercase letters, at least one number, and one special character (the spaces—or underscores if spaces are not allowed).

2. Maximize the weirdness.

Increase the quantity of numbers and special characters used. For example, modify the letters in our previous example to read "4 $core @nd 7 Ye@rs ago."

3. Customize, don't copy.

By simply combining attaching a simple suffix to the end of each passphrase, you can reuse your master password easily without the dangers of duplicate uses. For a Facebook account, try adding "FB" to the end of passphrase, or "IG" for Instagram.

USE A PASSWORD MANAGER

An arbitrary collection of words, numbers, and symbols does make for a safe password, but not a memorable one. Enter the password manager. These services act as a multi-platform, take-me-anywhere keychain that not only stores passwords, but generates them for you every time you need a new one.

Setting one up can be time intensive, as you normally will want to manually change your old passwords for each of your accounts and allow the manager to generate a new one. However, the result is a secure password for every service that you control with just a single master login. Through a desktop app, browser extensions, and a mobile app, a good manager takes the work—and risk—out of creating and storing a bevy of unique and secure passwords.

ENABLE MULTI-FACTOR AUTHENTICATION

Many secure environments offer two-factor authentication at login, including web services (Google, Microsoft, iCloud), security-minded portals (banks and bill paying), and Windows 10. By combining two types of "passwords," the strength of protection is exponentially increased, without asking the user to do much more. Many web services use a smartphone app, or a code texted to a verified number during a login attempt. Windows Hello on Windows 10 can take advantage of hardware-based features like a facial recognition or fingerprint.

Passwords are nothing new, and though biometrics are becoming increasingly more common, the reality is that passwords are still your first line of protection for nearly every part of your digital identity — and securing them is solely in your hands.

Be more secure from power on to power off.