

Best Practices: Creating a Secure Password

Even with advances being made in fingerprint and facial recognition, passwords are still the go-to when it comes to authentication credentials. However, password usage has recently become increasingly problematic. Weak or obvious passwords boost the risk to the user, and raise the chances that a hacker will be able to breach the device, account or network being protected.

DID YOU KNOW?

- The number of U.S. data breach incidents tracked in 2017 hit a new record high of 1,579 breaches, according to the 2017 Data Breach Year-End Review released by ITRC and CyberScout®. The Review indicates a drastic upturn of 44.7 percent increase over the record high figures reported for 2016.

SIMPLE TIPS

- To help you determine if your password is complex enough, try going to *HowSecureIsMyPassword.net*. It will estimate the time it would take a computer to hack your password.
- As best practice, change passwords every 60 to 90 days across all online accounts.
- Use strong credentials that include at least 12 characters with upper and lowercase letters, numbers and special characters.
- Use unique passwords for different accounts so that if a breach compromises one password your other accounts are not impacted.
- Don't use common passwords such as 123456, ABCDEFG, or simple phrases.
- Consider using an acronym to make the password easier to remember. For instance, the song lyric "I'm just a poor boy from a poor family," becomes the password IJAPBFAPF.
- Don't use obvious information for security questions such as a mother's maiden name, a hometown or pet's name.
- Don't store passwords in web browsers or other documents. In fact, passwords should not be stored on a user's personal computer at all unless they are within a password manager.
- If you have the option, try enabling two-factor authentication (2FA). This could come in the form of a text-based code sent to your phone that accompanies a password.

RESOURCES AVAILABLE TO YOU

- <http://blog.trendmicro.com/secure-entry-with-strong-passwords-improving-authentication-credentials/>
- <http://blog.trendmicro.com/yahoo-breach-time-keep-password-safe/>
- <https://howsecureismypassword.net/>