FOCAL POINT
DATA RISK

# PASSWORD SECURITY

## ASK THE EXPERTS

## HOW LONG SHOULD MY PASSWORD BE?

It's simple. The longer your password, the more difficult it is to crack. When you choose a shorter password, it takes hackers less time and fewer computing resources to compromise your credentials. Many trusted industry organizations recommend a minimum of 8 characters, while others like the DoD advocate for at least 12 characters.

## HOW CAN I MAKE MY PASSWORD STRONGER?

Using simple, predictable words for your password makes it incredibly easy for hackers to compromise your credentials. Hackers have created massive databases of common words, phrases, and number combinations and will run your password through different algorithms until they get a match. But there are many ways to strengthen your password. By increasing the length and adding special characters, capital and lowercase letters, and numbers, you increase the "entropy" (or randomness) of your password, making it far more difficult to crack.

### WEAK PASSWORD TYPES

DICTIONARY WORDS
BIRTH DATE
PHONE NUMBER
COMPANY NAME
MOVIES, MUSIC, SPORTS TEAM NAMES
WORDS + NUMBERS ("CATFISH7")
SIMPLE OBFUSCATION ("P@S$W0RD")

## WHAT CAN AN ATTACKER DO WITH MY PASSWORD?

To many users, passwords can seem more like a roadblock than a critical security measure, and most people don't realize how valuable a password is to malicious attackers.

### PASSWORD REUSE

Many people use the same password for multiple applications and sites (Gmail, LinkedIn, Facebook, etc.), which compounds the potential damage of a single compromised password.

### USER ENUMERATION

Many companies use a single, enterprise-wide username format. Once an attacker figures out the credentials of one low-privilege user, the attacker can use that template to compromise the accounts of employees across all departments and levels.

### PASSWORD RECOGNITION

Often, corporate IT departments provide new users with initial passwords like ChangeMe123 and don't require users to change the password after the initial login. These easily cracked passwords allow attackers to identify password patterns and use them to compromise whole corporations.

## WHAT ELSE CAN I DO TO PROTECT MY PASSWORD?

There are a few additional steps you can take. First, change your passwords often. This can lock out cyber criminals who may be using your account. It also helps combat time-consuming brute force attacks. Second, make sure no one is watching as you enter passwords. And third, be cautious when downloading files from the Internet, as they may contain malware-like key loggers that will compromise your password.

focal-point.com 813-402-1208 info@focal-point.com