FORTRA

How to Create a Strong Password in 7 Easy Steps

Cybercriminals know that most people create passwords that are easy to remember and will often reuse the same password across multiple accounts. Because of this, all it takes is hacking into one account to easily access the rest of the accounts. Please take a few minutes to review these seven strong password best practices and to create new passwords for any accounts that do not follow these password guidelines:

1

DO NOT USE SEQUENTIAL NUMBERS OR LETTERS
For example, do not use 1234, qwerty, jklm, 6789, etc.

USE A COMBINATION OF AT LEAST EIGHT LETTERS, NUMBERS AND SYMBOLS
The longer your password and the more character variety it uses, the harder it is to guess. For example, M0l#eb9Qv? uses a unique combination of upper- and lowercase letters, numbers and symbols.

2

3

DO NOT INCLUDE YOUR BIRTH YEAR OR BIRTH MONTH/DAY IN YOUR PASSWORD
Remember that cybercriminals can easily find this information by snooping into your social media accounts.

COMBINE DIFFERENT UNRELATED WORDS IN YOUR PASSWORD OR PASSPHRASE
This makes it difficult for cybercriminals to guess at your password. Do not use phrases from popular songs, movies or television shows. Use three or four longer words to create your passphrase. For example, 9SpidErscalKetobogGaN.

4

5

DO NOT USE NAMES OR WORDS FOUND IN THE DICTIONARY
Substitute letters with numbers or symbols to make it difficult to guess the password. Or deliberately use spelling errors in the password or passphrase. For example, P8tty0G#5dn for “patio garden.”

USE A PASSWORD MANAGER TO STORE YOUR PASSWORDS
Do not store your passwords in a document on your computer. Make sure you’re using the password manager tool provided to you by the IT/support team to store all professional and personal passwords.

6

7

DO NOT REUSE YOUR PASSWORDS
Every device, application, website and piece of software requires a unique and strong password or PIN. Remember, if a cybercriminal does guess one of your passwords, they will use this to attempt to hack into all of your personal and professional accounts.

Remember

Never share your passwords with anyone. This includes your colleagues, the IT/support team, customer service/helpdesk personnel, family members and friends.