CSC

MASTER THE PASSWORD.

A good password is free and an easy way to protect yourself from data breaches—and can be considered the last line of defense between company data and a cyber criminal. But even good passwords can be compromised. Find out how to reduce that threat.

✓ DO

Do lengthen
Make your password long. Using long passwords—at least 10-characters—makes it harder for cyber criminals to decode them.

Do use phrases
Use phrases that look random to anyone else, such as **TW2gsi2QT&bd** "The way to get started is to quit talking and begin doing." ~Walt Disney

Do use a manager
Use a master password and a password manager.

Do authenticate
Implement two-factor authentication to help restrict compromises.

⊘ DON'T

Don't be predictable
Don't use predictable patterns, or adjacent keys like "qwerty" and "asdf."

Don't use names
Don't use dictionary words in your password, or family or pets' names, confidential details like birth dates, phone, or identification numbers.

Don't repeat
Never use the same password for multiple sites.

Don't store
Never store your passwords in plain text on any computer.

DID YOU KNOW?

- The top three most popular—and hacked—passwords are *Password1*, *Welcome1*, and *P@ssword*.
- 8-character passwords are cracked within one day using brute-force techniques; 10-character passwords require about 591 days—close to 600 times more effort!
- The most common keywords used in passwords include baby, pet, and city names.
- Close to 30% of the top 10 character sequences are in this format: Uppercase letter (U) followed by a series of lowercase letters (l) appended by numbers (#) at the end, such as Ullllll##, for example *Hello11*.