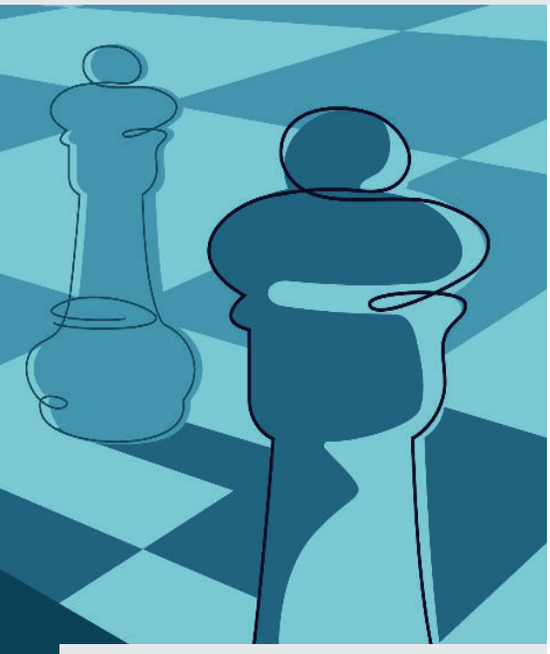
FIRSTLIGHT X cloud change

E-mail: inquiry@fcxnyc.com
Chat: via https://fcxnyc.com

10 tips for Choosing a Strong Digital Password



Checkmate: PASSWORD WINS

The first objective

is to ensure one's password is brute force-proof. A brute force attack is a trial-and-error method where hackers run through one combination of characters after another to gain unauthorized access to a system. The second objective is to create a password which is dictionary attack proof – if the password only contains one word or a predefined set of words it loses in strength. **Do not use the word "Password" in your password. Hackers have become very sophisticated. Fight back.**

1. 16 Characters Minimum

The longer the password, the better.

2. Mix It Up

Use multiple characters.

Use uppercase and lowercase letters at random in the middle of words. Use numbers. Use special symbols. Creating a password consisting of a set of mixed characters means the password is harder to crack.

3. Avoid Sequences

And avoid strings.

Repeated character use like "zzzzzz" or "888888" needs to be avoided. Sequences like "12345" or "abcde" are equally weak.

4. Avoid the Familiar

Never use personal information.

Avoid references to names of loved ones, birthdays, phone numbers and addresses.

5. Minimize Real Words

Or use uncommon terms: Mix in foreign language, archaic words and historic figures.

Hackers can use malicious programs which run every word in the dictionary. Remedy: break up common words with random characters.

6. Avoid Duplication

Never use a password twice. Create unique passwords for all of your accounts.

7. Increase disorder

Avoid common character substitution.

Unfortunately, swapping 1 for l and 5 for s is not as effective as it used to be. Hackers can now program their software for typical character swaps. Randomizing worls.

8.. Avoid Keyboard Paths

Using "Qwerty" is outdated. This because hackers can now program their software for memorable keyboard paths. In contrast however, using the muscle memory method where a user selects passwords they feel comfortable typing tends to work well.

9. Extra -long passphrases

Use words withou connection

Make sure works have no obvious connection to each other and use uncommon words like words in multiple languages or archaic words.

10. The ideal format: