What is a 'strong' password?

Definition

A strong password fits the following criteria:

- A password that is at least 12 characters long (But no longer than 19 characters, as some systems can't handle it)
- Contains at least two of the following:
  - A mixture of letters and numbers (IE: a8c3v4...)
  - A special character (IE: @$ _ ...)
  - A mixture of UPPER and lower case characters (IE: IuTyP)
- Generally does not contain words in the dictionary or names
- Does not contain something related to you that is public knowledge (School, address, birthdate)
- Is NOT your username
- Is NOT your name
- Is NOT your birthday
- Is NOT a keyboard pattern (IE: qwerty, 12345, asdf, abcde)

Examples of Strong Passwords

- ^731V620ut?71:e
- $6;9@B%5_1<C"f
- MWoFod8SA^xB6PZ

Some systems may also not like certain special characters, so be sure to validate the password or have alternatives on hand.

Some will say a password can be a passphrase, but one has to be careful about the phrase they use and not use the same one on multiple sites.

In either case, it is strongly recommended by ECI and UCSB's Office of Information Technology that any account on a machine have a strong password set to avoid being easily compromised by hackers and other malevolent users.

If you are having a hard time trying to keep track of said passwords, please refer to our recommendations on Password Managers for a means to keep your passwords, keeping in mind that your Master Password should be unique and not used anywhere else and one you can remember easily, while also adhering to the strong password definitions.

Related articles

- Securing Linux Computer
- I get 'Critical Security Alert' email from Google
- Digital Piracy
- Security Checklist
- Securing a computer on Campus