Password Report Card

Most people are failing miserably when it comes to password length and complexity. The most common passwords (cleartext, alphanumeric) are all brute forcible in a matter of seconds. This is if they have not already been exposed (unencrypted) in a previous data breach.

So how does your password stand up when it comes to crack-ability?

Check your passwords against this grade sheet, to see whether you would "pass" or "fail" the test.

All numbers or lowercase characters (8 or fewer characters)

- Example: "123456"/ "soccer"
- Brute-forcible in the blink of an eye. Most people know not to do this. If you are still doing this, just stop it already!

F

Combination of numbers and lowercase characters (8 or fewer characters)

- Example: "ncc1701"/ "michael1"
- Slightly better, but still super easy to guess or crack!

F

Combination of numbers, upper and lowercase characters (8 or fewer characters)

- Example: "Drag0n!"/ "Cowboys#1"
- Where most people are at these days. Dictionary attacks will break both in a matter of minutes.
- Other considerations:
  - Often harder for an individual to remember.
  - When it comes time to change, most will just iterate; i.e., "Cowboys#1" becomes "Cowboys#2"

D

Long password phrases

- Example: "correcthorsebatterystaple"
- Better than those above. Easier to remember and the length of the password makes it harder to crack.

B-

Long password phrases with a "stop" character, symbol or number

- Example: "webutterthebre%adwithbutter"
- About the best you can do (other than increasing length).

B

Password Managers

- Randomly generated long passwords take the most exploitable element (the human element) out of password creation.

A+

KRANTZ
SECURE TECHNOLOGIES