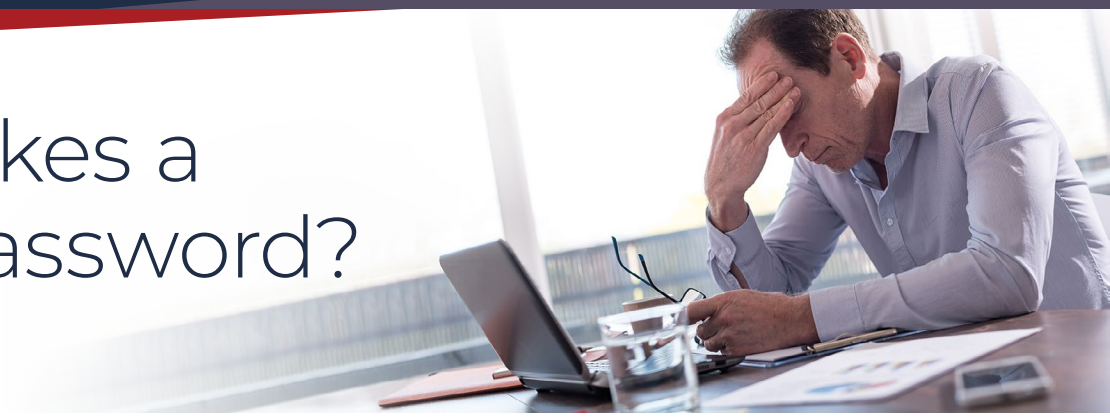
MILNER

What Makes a Strong Password?



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 — F

123456 / soccer

Brute-forcible in the blink of an eye.
If you are still doing this, just stop it already!

Combination of numbers and lowercase characters — F

ncc1701 / michael1

Slightly better, but still super easy to guess or crack!

Combination of numbers, upper and lowercase characters — D

DragOn! / Cowboys#1

Commonly used, but dictionary attacks will break these in minutes. Harder to remember and thus tend to be iterative (Cowboys#2, Cowboys#3)

Long password phrases — B-

correcthorsebatterystaple

Better than those above. Easier to remember and the length of the password makes it harder to crack.

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

webutterthebre%adwithbutter

About the best you can do
(other than increasing length).

Password Managers — A+

5gyh%epP&j9sd3pf#dH

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

Talk to an expert!

milner.com