How Strong is Your Password?

When an attacker wants to get into your online account or device, they'll usually attack the password since it's often the only thing securing it, unless you have two-factor authentication (2FA) switched on. Since many people don't bother with 2FA, this turns passwords into what's called a single point of failure.

We all know the annoyance of creating a new account online: you enter the password you want, and then the service bugs you about minimum length and using special characters. There's a reason you're being pushed to do this.

Password entropy is a measure of how unpredictable and random your Password is.

Entropy is a scientific concept that is most commonly associated with a state of disorder, randomness, or uncertainty. Password entropy is measured in bits, the basic unit for measuring information in computing.

How many bits of entropy for a good password?

For non-vital accounts, 25-30 bits of entropy are enough. For more important accounts, aim for 60-80 bits of entropy, up to 100 for crucial ones.

Greater entropy creates better passwords, but what exactly makes for better entropy? Factors to take into consideration:

- Use of lowercase characters
- Use of uppercase characters
- Use of numbers
- Use of special characters
- Length of the password

How to calculate password entropy?

Calculation can been done using a complicated formula and we will not go into that here. There are on-line calculators for that job (listed below).

When using a regular US keyboard layout, you have 26 letters. If you were to create a password using only lowercase letters, your pool size is 26. If we use an entropy calculator assuming a length of eight characters, that gives us an entropy of 37.60 bits, which is terrible.

Uppercase letters + Lowercase letters the pool size is 52.

If we add the digits 0-9 we increase the pool to 62, and then once we add the 33 symbol keys, our pool is increased to 95. Using just 8 characters, that gives us an entropy score of 52.56 bits, still well below the cutoff of 64 bits. The only other way to further increase your entropy is to make the password longer.

Increasing length to 10 using all printable characters gives us 65.70 bits.

Increasing length to 12 using all printable characters gives us 78.84 bits.

So Exactly what does the number of bits mean?
We use the number of bits to calculate the maximum number of guesses a computer would need to break your password.

How effective is your password against adversaries who try to guess it or use a brute-force attack?

A brute force attack means that someone sets up a script to try all possible combinations of characters to find the password.

So your only chance is to use a password that would take a very long time to guess (optimally, several millions of years).

To check your Password:

Brute Force Calculator

Password Entropy Calculator

Has My Password been hacked/pwned?

Password Strength Testing Tool

Password entropy is NOT all that matters!

Never rely solely on entropy to decide whether to use a particular password!

Password entropy is just one aspect of deciding which type of password would be considered secure. It may happen that two passwords have the same entropy, and one of them is reasonably strong while the other is extremely weak.

This is because of password dictionaries, which are lists of leaked passwords that are available online. Using such lists is known as a dictionary attack, and any attacker attempting to unlock your account would try it before moving on to a brute force attack. So, if you use a password that is in a dictionary of common passwords, it doesn't matter how many bits of entropy this password contains - it will get broken very quickly!