**multiple passwords with varying complexity**

password → very simple, lowercase only

Password123 → adds uppercase & numbers

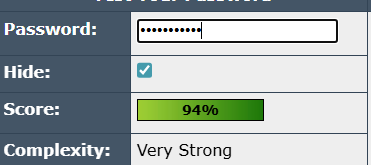
Passw0rd! → uppercase, numbers, symbol

My$ecureP@ss2025 → longer, mix of everything

q7!XrT9#vB2pL$ → random, strong, long

CorrectHorseBatteryStaple! → long passphrase, memorable & strong

**password strength checker**



**best practices for creating strong passwords**

longer and more random passwords score better.

Use **at least 12–16 characters**.

Mix **uppercase, lowercase, numbers, and symbols**.

Avoid common words or predictable patterns.

Consider **passphrases** that are long but easy to remember.

Use a **password manager** for unique passwords.

Short and simple passwords are weak.

Adding numbers, symbols, and uppercase improves strength.

Random strings or long passphrases are the most secure.

**common password attacks**

Reusing passwords is dangerous. Brute Force Attack → Trying all possible combinations until it works. Longer passwords make this much harder.

Dictionary Attack → Trying common words or phrases from a “dictionary” of passwords. Avoid common words.

Credential Stuffing → Using leaked passwords from other sites. Don’t reuse passwords.

**password complexity**

**Length matters**: Longer passwords take exponentially more time to crack.

**Character variety matters**: Using letters, numbers, and symbols increases possible combinations.

**Predictability matters**: Common words, dates, or sequences are weak.

**Randomness matters**: Random strings or unique passphrases drastically improve security.