|  |  |  |  |
| --- | --- | --- | --- |
| **Password** | **Strength Rating** | **Estimated Crack Time** | **Feedback** |
| A1pL3#sTr0ng! | Very strong | 2 Million years | Excellent |
| apples | Weak | Instantly | Needs numbers, caps, symbols |
| Apple@123 | Strong | 3 weeks | Good complexity |
| apple123 | Weak | Instantly | Too common |

**What Makes a Good Password?**

* A password should be at least 12 characters long (ideally 16 characters or more); our password-related research has found that 45 percent of Americans use passwords of eight characters or less, which are not as secure as longer passwords.
* A password should include a combination of letters (both uppercase and lowercase), numbers, and characters.
* You must have a unique password for each online account.
* A password shouldn’t include any of your personal information like your birthday or address, as identity theft and data breaches can compromise such information. It’s also best not to include any information that can be accessed on social media like kids’ or pets’ names.
* A password shouldn’t contain any consecutive letters or numbers (i.e. ABCD, 1234, etc.)
* A password shouldn’t be the word “password” or the same letter or number repeated.

**Best Practices for Creating Strong Passwords**

To create secure passwords, follow these:

Use at least 12 characters.

Combine uppercase + lowercase letters.

Include numbers and symbols.

Avoid using:

* Names
* Common words (e.g., "password", "qwerty")
* Personal info (birthdays, phone numbers)
* Use passphrases (e.g., Blue!Sky9$RunsFast) – they’re easier to remember, but hard to crack.
* Never reuse passwords across sites.
* Use a password manager to store strong, unique passwords.

**Tips Learned from the Evaluation Tools**

From the feedback given by password strength checkers:

Length matters most — longer passwords are exponentially harder to crack.

Symbols and numbers make passwords much stronger.

Common passwords (even if long) are still very weak.

Patterned substitutions (e.g., @ for a, 0 for o) aren't always secure if predictable.

**Common Password Attacks:**

Attack Type & Description

1. Brute Force: Tries every possible combination. Very time-consuming for strong passwords.
2. Dictionary Attack: Uses a list of common passwords or words (e.g., password123, admin) to guess.
3. Credential Stuffing: Reuses stolen usernames/passwords from previous data breaches.
4. Phishing: Tricks users into revealing their passwords.

**Summary: Why Password Complexity Matters**

Complex passwords resist brute-force and dictionary attacks.

Long + unpredictable = strong.

A simple 6-character password like admin12 can be cracked in seconds.

A 14-character password with symbols like B!ackC0ffee2024# could take centuries to break.

Complexity protects your data even if an attacker gains access to hashed/stored credentials.

|  |  |  |
| --- | --- | --- |