Password Strength Table

Password	Characteristics	Strength
password	All lowercase, common word	Extremely Weak
Password	Capitalized first letter, common word	Very Weak
P@ssw0rd	Common word with symbol and number substitutions	Weak
qwerty123	Keyboard pattern with numbers	Very Weak
Tr0ub4dour&3	Mixed case, numbers, symbol, moderate length	Moderate
CorrectHorseBatteryStaple	Long passphrase, no symbols or numbers	Strong
A1b2C3d4!@	Random-looking, mixed characters, short length	Moderate to Strong
xK8$q!L2*pZ	Fully random, 10 characters, mixed types	Strong
12345678	Only numbers, very common sequence	Extremely Weak
!@#$%^&*	Symbols only, common sequence	Very Weak

Best Practices for Strong Passwords

From the tests, you'll observe:

1. Length > Complexity: A long passphrase (CorrectHorseBatteryStaple) scores higher than short complex passwords (A1b2C3d4!@).

2. Mix Character Types: Uppercase, lowercase, numbers, symbols improve strength.

3. Avoid Patterns: qwerty123 or 123456 are easily cracked.

4. Randomness: Tools reward unpredictable sequences (xK8$q!L2*pZ).

5. Common Words: Even with substitutions (P@ssw0rd), dictionaries crack them.

Common Password Attacks

- **Brute Force**: Tries every possible combination. Long/complex passwords resist this.
- **Dictionary Attack**: Uses common words/passwords. Avoid predictable phrases.
- **Rainbow Tables**: Precomputed hashes. Mitigated by **salting** (added random data).

Example:

- password → Cracked instantly (in dictionaries).
- xK8$q!L2*pZ → Takes years to brute-force.

How Complexity Affects Security

- **Entropy Matters**: Higher entropy (randomness) = harder to crack.
  - password → 28 bits entropy → Cracked in seconds.
  - xK8$q!L2*pZ → 65+ bits entropy → Centuries to crack.
- **Length vs. Complexity**:
  - CorrectHorseBatteryStaple (25 chars, no symbols) → Secure due to length.
  - A1b2C3d4!@ (10 chars, complex) → Less secure than a long passphrase.

Tips Learned

- **Use 12+ characters**
- **Combine words unpredictably**
- **Avoid substitutions like** @ **for** a
- **Use a password manager**