Password Strength Analysis

Passwords and Components

1. apple123 - Lowercase, numbers
2. Apple123 - Uppercase, lowercase, numbers
3. Apple123! - Uppercase, lowercase, numbers, symbol
4. Ap!2e7K@ - Uppercase, lowercase, numbers, symbols
5. aP9!r$Lz!w2q% - Uppercase, lowercase, numbers, symbols
6. CorrectHorseBatteryStaple - Long phrase, only words
7. C0mpl3x!tY@2025* - Complex, diverse character set

Password Strength Feedback

apple123 - 1/5 - Too common, lacks complexity

Apple123 - 2/5 - Slightly better, still predictable

Apple123! - 3/5 - Good mix, but short length

Ap!2e7K@ - 4/5 - Strong, random, but can be improved with length

aP9!r$Lz!w2q% - 5/5 - Excellent, very strong and hard to guess

CorrectHorseBatteryStaple - 4/5 - Good due to length, but predictable words

C0mpl3x!tY@2025* - 5/5 - Excellent, diverse, includes year, symbols, and complexity

Best Practices

- Use longer passwords (12+ characters).
- Include a mix of uppercase, lowercase, numbers, and special characters.
- Avoid personal information and dictionary words.
- Use password managers to store unique passwords.
- Regularly update passwords.

Password Attacks

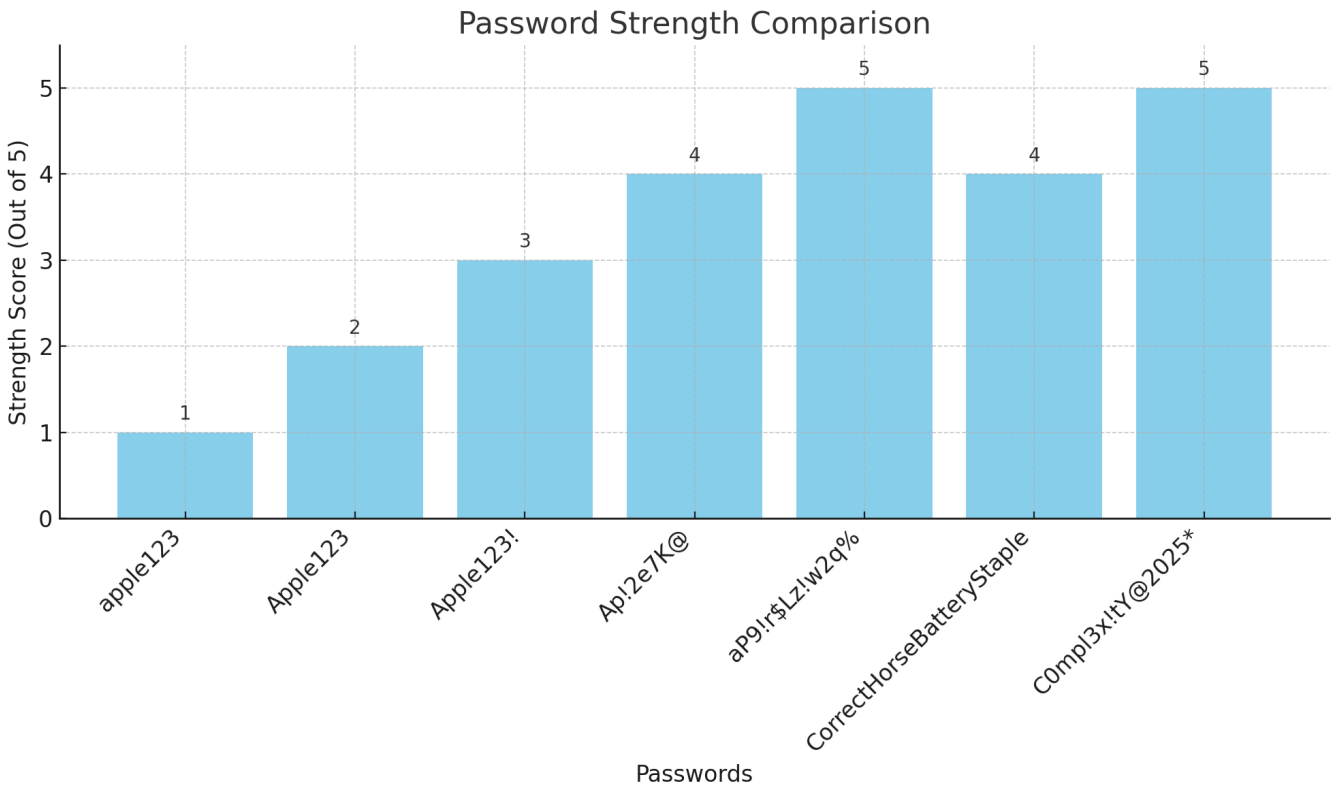
- Brute Force: Tries all combinations.
- Dictionary: Uses common wordlists.
- Credential Stuffing: Uses leaked credentials.
- Phishing: Tricks users into giving passwords.
- Keylogging: Captures keystrokes.

Password Complexity Summary

Complex passwords take longer to crack and resist attacks better.

Adding more characters and types (symbols, numbers) significantly increases security.

Unpredictability and diversity in characters are key.


Password Strength Comparison
Strength Score (Out of 5)
0
1
2
3
4
5
1
2
3
4
5
4
5
apple123
Apple123
Apple123!
Ap!2e7K@
aP9!r$LZ!w2q%
CorrectHorseBatteryStaple
C0mpl3x!tY@2025*
Passwords