**Create a Strong Password and Evaluate Its Strength**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Password | Length | Score | Complexity | Feedback Summary |
| 1 | 11 | 30% | Weak | Missing uppercase, symbols, and other character variety. Heavy deduction due to repeated and consecutive lowercase letters. |
| 2 | 11 | 76% | Strong | Good mix of character types, but impacted by predictable and repetitive patterns. |
| 3 | 14 | 91% | Very Strong | Solid password with all types included. Deductions due to lowercase character patterns and repeated characters. |
| 4 | 16 | 100% | Very Strong | Excellent password: long, diverse, no patterns, and no weaknesses detected. |

**Tips learned from the evaluation:**

* Aim for 12+ characters.
* Include uppercase, lowercase, numbers, and symbols.
* Avoid repeating characters and sequential patterns.
* Spread out symbols and numbers (not just at the beginning or end).
* Mix cases and avoid long runs of the same character type.

**Best practices for creating strong passwords:**

1. Use a Long Password

* Aim for at least 12–16 characters.
* Longer passwords are exponentially harder to crack.

2. Mix Character Types

Include at least three of the following:

* Uppercase letters (A–Z)
* Lowercase letters (a–z)
* Numbers (0–9)
* Symbols (!@#$%^&\*() etc.)

3. Avoid Predictable Patterns

* Don’t use sequential characters (abc, 123, qwerty).
* Avoid repeated characters (aaa, 111).
* Mix your characters unpredictably.

4. Avoid Common Passwords and Personal Info

* Don’t use names, birthdays, pet names, or common passwords like password123.
* Hackers use these in dictionary and brute-force attacks.

5. Use Passphrases (Strong & Memorable)

* Combine random words or a sentence:  
  Blue!Elephant\_Runs7Fast
* Easier to remember and still secure.

6. Use a Password Manager

* Let it generate and store strong, unique passwords for each account.
* Avoid reusing passwords across sites.

7. Change Passwords When Necessary

* Change immediately if you suspect compromise.
* No need to rotate frequently *unless required* (frequent changes can reduce security if they cause weaker choices).

8. Don’t Write It Down (Unless Secured)

* Never store passwords in plain text (e.g., sticky notes or Word documents).
* If written, keep in a secure physical or digital location.

**Common Password Attacks:**

1. Brute Force Attack

How it works:

* Attacker tries all possible combinations of characters until the correct password is found.
* Time-consuming but guaranteed to succeed eventually, especially on weak or short passwords.

Defense:

* Use long passwords (12+ characters).
* Include symbols, numbers, and mixed cases.
* Implement account lockouts or rate-limiting after failed attempts.

2. Dictionary Attack

How it works:

* Uses a precompiled list (dictionary) of common passwords and words.
* Much faster than brute force because it avoids unrealistic combinations.

Defense:

* Avoid using real words, common phrases, or predictable passwords.
* Include randomness and complexity (e.g., Tr33!F0x^Zebra9).

Password complexity plays a critical role in protecting against cyberattacks

1. Increases Resistance to Attacks

* Complex passwords are harder to crack using brute force and dictionary attacks.
* Adding length, uppercase/lowercase letters, numbers, and symbols increases the number of possible combinations exponentially.

2. Prevents Common Guessing Techniques

* Simple or common passwords like password123 or qwerty are easily guessed or found in attacker dictionaries.
* Complexity ensures your password isn’t among the top used or easily predicted ones.

3. Slows Down Attackers

* Complex passwords take longer to crack, giving defenders more time to detect and respond to threats.
* Some complex passwords are virtually uncrackable within a human-relevant timeframe.

4. Reduces Risk from Reused Passwords

* Using complex and unique passwords for each account helps prevent credential stuffing (when attackers reuse stolen passwords).

Best Practices:

* Use at least 12–16 characters.
* Combine letters (upper & lower), numbers, and symbols.
* Avoid dictionary words, repeated characters, and predictable patterns.
* Use a password manager to generate and store complex passwords.