Best Practices for Creating Strong Passwords

To help ensure your passwords are both secure and difficult to crack, follow these best practices:

1. Use a Minimum of 12-16 Characters

- The longer the password, the harder it is to crack. Aim for at least 12 characters; 16 characters or more is ideal. This makes brute-force attacks significantly harder.

2. Avoid Common Words and Phrases

- Don’t use easily guessable words like "password," "123456," or your name.
- Avoid common phrases or personal information such as birthdays, pet names, or addresses.
- Instead, use random combinations or a passphrase (e.g., Tr@n5p0rt!C$tle).

3. Mix Uppercase, Lowercase, Numbers, and Symbols

- Include uppercase and lowercase letters, numbers, and special characters like @, #, $, etc.
- This increases the complexity and makes it harder to crack using brute force.

4. Avoid Sequences and Repeated Characters

- Don’t use predictable sequences like "1234", "abcd", or "qwerty".
- Avoid repeated characters like "aaa", "111", or "!!!".

- Randomness is key! For example, a password like S!lverR3tr@iv3#2 is far stronger than Silver123.

5. Use Passphrases or Random Word Combinations

- **Passphrases**: Use multiple random words combined in a string (e.g., "Coffee!Mountain@2023"), but with numbers and symbols included to add complexity.
- **Random Word Combination**: Pick random words and mix them with symbols (e.g., K@ng@roo$1P!zza).
- Passphrases are easy to remember but can be highly secure if made long enough and mixed well.

6. Use a Password Manager

- If remembering complex passwords is difficult, consider using a password manager to store them securely.
- A password manager can generate and store unique passwords for each of your accounts, which will be nearly impossible to crack.

7. Enable Multi-Factor Authentication (MFA)

- Whenever possible, enable multi-factor authentication (MFA) on your accounts.
- Even if someone guesses or cracks your password, they will still need access to the second factor (e.g., an SMS code or authentication app).

8. Avoid Using the Same Password Across Multiple Sites

- Using the same password on multiple accounts increases the risk if one account is compromised.
- Always use unique passwords for different sites and services.

9. Regularly Update Your Passwords

- Change passwords regularly, especially for sensitive accounts (e.g., banking, email, etc.).
- Consider rotating passwords every 3-6 months for critical accounts.

10. Use Non-Dictionary Words and Avoid Substitutions

- Avoid using dictionary words even with substitutions (e.g., @ instead of “a” or 1 instead of “I”). These substitutions are well-known and often included in attack lists.
- Use a random mix of characters or consider using a password generator for truly random strings.

11. Test Your Password’s Strength

- Always check the strength of your password using a reliable password strength checker (e.g., HowSecureIsMyPassword, PasswordMeter, etc.).
- Ideally, aim for 80/100 or higher in strength checkers.