Password Strength Evaluation Report

Introduction

This report documents my findings from Task 6 of the Cyber Security Internship, which focused on understanding password strength and evaluating various passwords using online tools. The objective was to learn what makes a password strong and how different complexity factors contribute to security.

Methodology

1. Created multiple passwords with varying complexity levels
2. Tested each password on passwordmeter.com
3. Analyzed the scores and feedback provided by the tool
4. Researched common password attacks and best practices

Password Creation and Testing

Password Examples and Results

Password Example	Length	Contains (U,L,N,S)	Score	Feedback
Password123	10	U, L, N	65%	Medium strength - needs symbols
P@ssw0rd!2023	12	U, L, N, S	92%	Very strong
summer2023	9	L, N	40%	Weak - needs uppercase and symbols
Tr0ub4dour&3	11	U, L, N, S	88%	Strong
correcthorsebatterystaple	25	L	70%	Good length but needs complexity
A1!b2@c3#d4$	12	U, L, N, S	100%	Excellent strength

Observations

- Passwords combining uppercase, lowercase, numbers, and symbols scored highest
- Length significantly impacted strength (passwords >12 characters scored better)
- Passphrases (long combinations of words) showed good strength but benefited from added complexity

Creating and managing strong passwords is crucial for protecting online accounts from unauthorized access. Below is an in-depth explanation of the best practices for password security:

---

1. Use Long Passwords (12+ Characters)

- **Why?** Longer passwords exponentially increase the time required for brute-force attacks.
- **Example:**
    - Weak: P@ssw0rd (8 chars)
    - Strong: Winter$now2023! (15 chars)
- **Tip:** Aim for **at least 12 characters**, but **16+ is ideal** for high-security accounts (e.g., banking, email).

---

2. Include Multiple Character Types (Complexity)

- **Use a mix of:**
    - **Uppercase letters** (A-Z)
    - **Lowercase letters** (a-z)
    - **Numbers** (0-9)
    - **Symbols** (!@#$%^&*)
- **Why?** Complexity makes passwords harder to guess or crack.
- **Example:**
    - Weak: summer2023 (only lowercase + numbers)
    - Strong: Summ3r!@2023 (uppercase, lowercase, numbers, symbols)

3. Avoid Common Words & Predictable Patterns

- **Avoid:**
    - Dictionary words (password, admin)
    - Simple substitutions (P@ssword instead of Password)
    - Sequential patterns (123456, qwerty)
    - Personal info (John1985, PetName123)
- **Why?** Hackers use **dictionary attacks** and **pattern recognition** to crack weak passwords.
- **Better Alternative:** Use **random combinations** or **passphrases** (e.g., BlueCoffee$Mug42!).

4. Use Unique Passwords for Every Account

- **Why?** If one account gets hacked, attackers won't gain access to all your accounts.
- **Solution:**
    - Use a **password manager** (e.g., Bitwarden, LastPass, KeePass) to store and generate unique passwords.
    - Never reuse passwords across sites.

5. Enable Multi-Factor Authentication (MFA)

- **What is MFA?** An extra layer of security beyond just a password (e.g., SMS code, authenticator app, biometrics).
- **Why?** Even if a hacker gets your password, they can't log in without the second factor.
- **Best MFA Methods:**
    - **Authenticator apps** (Google Authenticator, Authy)
    - **Hardware keys** (YubiKey)
    - Avoid SMS-based 2FA if possible (SIM-swapping attacks).

6. Change Passwords Only When Necessary (But Keep Them Strong)

- **Old Myth:** "Change passwords every 90 days."

- **New Best Practice:**
    - Only change passwords if:
        - There's a **data breach** involving that account.
        - You suspect **unauthorized access**.
        - You previously used a **weak password**.
    - Otherwise, focus on **keeping a strong password long-term**.

---

7. Beware of Phishing & Social Engineering

- **Never enter passwords in:**
    - Suspicious emails or fake login pages.
    - Unverified websites (check for HTTPS and correct domain).
- **Use a password manager with autofill** to avoid typing passwords manually (reduces phishing risk).

---

8. Consider Using Passphrases

- **What is a passphrase?** A long, memorable sentence-like password.
- **Example:**
    - Weak: Iloveyou123
    - Strong: PurpleElephant$JumpsOver42Clouds!
- **Why?** Easier to remember, harder to crack than short complex passwords.

---

9. Avoid Storing Passwords in Plain Text

- **Never save passwords in:**
    - Notes apps, Excel files, or browsers without encryption.
- **Use a secure password manager** instead.

---

10. Regularly Check for Password Leaks

- Use **Have I Been Pwned?** (https://haveibeenpwned.com/) to see if your passwords were exposed in breaches.
- If a password is leaked, **change it immediately** and enable MFA.

Conclusion

This exercise demonstrated that password strength depends on multiple factors working together. While complexity is important, length is the most critical factor. The best passwords combine length, multiple character types, and avoid predictable patterns. Using a password manager and enabling multi-factor authentication provides the best protection for online accounts.