Final Report: Creating and Evaluating Strong Passwords

This report explains the importance of creating and evaluating strong passwords. It provides key observations, best practices, and examples to show how different factors affect password strength. The purpose is to highlight practical methods for building secure digital identities and resisting cyber attacks.

Examples of Password Strength Levels

Example Type	Description	Strength Rating
Simple word	Single lowercase word (predictable, short)	Very Weak
Word + numbers	Common word with added numbers	Weak
Word + numbers + symbol	Word with numbers and a symbol	Good
Mixed case word + numbers	Upper/lowercase with numbers	Strong
Mixed case + numbers + symbol	Balanced mix of all character types	Very Strong
Random long string	Completely random characters, 16+ length	Very Strong (100%)

The table above shows how different approaches to creating passwords affect their strength. The more diverse and longer the password, the stronger it becomes.

Key Observations from Password Testing

- Short and simple words consistently ranked the lowest in strength.
- Adding numbers improved scores but still remained relatively weak.
- Symbols and uppercase letters provided a major boost to strength ratings.
- Length proved to be one of the most influential factors in making a password strong.
- Randomly generated long strings were always rated as the strongest.

Best Practices for Strong Passwords

- Include uppercase, lowercase, numbers, and symbols.
- Aim for 12–16 characters or more.
- Avoid dictionary words, names, or birthdates.
- Do not reuse passwords across accounts.
- Use passphrases for memorable but secure credentials.
- Enable MFA (Multi-Factor Authentication).
- Adopt password managers for secure storage.

Tools for Evaluating Password Strength

Online password strength checkers such as PasswordMeter were used to test password examples. These tools analyze character variety, length, and predictability to assign ratings from weak to very strong. They also give suggestions for improvement, such as adding special characters or increasing length.

Common Password Attacks

- Brute Force: Testing all combinations until the correct one is found. Prevented by long, complex passwords.
- Dictionary Attack: Using lists of common words. Prevented by avoiding predictable words and patterns.
- Phishing: Deceiving users into sharing credentials. Prevented by awareness and MFA.
- Credential Stuffing: Using stolen credentials from breaches. Prevented by using unique passwords per account.

Why Password Complexity Matters

Complexity greatly extends the time needed for an attacker to crack a password. For example, a simple 8-character password may be cracked in seconds, while a random 16-character string with mixed character types could take centuries. Thus, complexity and length are essential to strong security.

Additional Security Points

- Multi-factor authentication provides an additional safeguard even if a password is compromised.
- Password managers reduce the risk of reusing or simplifying passwords.
- Regular password updates can help mitigate risks from breaches.
- Cybersecurity awareness training is essential for reducing risks of phishing and social engineering attacks.
- Organizations should enforce strong password policies and periodic audits.

Conclusion

Through this evaluation, it became clear that password strength depends on a combination of character diversity, length, and unpredictability. Tools help assess password quality, but the ultimate responsibility lies in adopting best practices, staying informed about attacks, and using technologies like MFA and password managers. Strong passwords are a foundational step toward better cybersecurity.