Creation of Passwords with Varying Complexity

Password	**Complexity**	**Length**	**Components Used**
123456	Very Weak	6	Numbers only
password	Very Weak	8	Lowercase only
hello123	Weak	8	Lowercase, numbers
Kolkata2025	Medium	11	Uppercase, lowercase, numbers
Sunshine_45	Medium-Strong	11	Mixed case, symbol, numbers
W!nt3r2025	Strong	9	Mixed case, numbers, symbol
K@nd0m_P@ss1	Strong	12	Mixed case, numbers, symbols
G!veM3$Access!	Strong	14	Mixed case, phrase, symbols
C0mpl3x#T0k3n!	Very Strong	13	Obfuscated characters
Zr@2&Jm1^T#9u0	Very Strong	14	Random characters
v7A$d92Lq!eZ#	Very Strong	12	High entropy, all character types
IL0ve!Cyber$ec2025	Very Strong	18	Passphrase, strong variation

Testing Passwords and Recording Results

Password strength tests were conducted using an online free password strength checker tool called ‘ **passwordmeter.com** ’. The detailed results for all tested passwords have been recorded and attached in the file named **‘ Password_test.pdf ’**. These include **individual scores**, **complexity evaluations**, **bonuses**, **deductions**, and **feedback** from the password checker tool.

For example, the password '**hello123**' scored 37%, was rated Weak, and lacked uppercase letters and symbols. It also contained common patterns such as repeated characters and numeric sequences.

Best Practices for Creating Strong Passwords

- Use a minimum of 12 characters.
- Include uppercase, lowercase, digits, and symbols.
- Avoid dictionary words and personal information.
- Never reuse passwords across different accounts.
- Use passphrases or randomized strings.
- Regularly update passwords.
- Use a password manager.
- Enable Multi-Factor Authentication (MFA).

Tips Learned from Evaluation

- Short passwords, even complex ones, are still weak.
- Symbols significantly increase password strength.
- Mixed-case letters and symbol positioning matter.
- Randomization increases cracking time dramatically.
- Memorable passphrases can be both strong and usable.

Common Password Attacks

🔹 1. Brute-Force Attack

A brute-force attack tries every possible combination of characters to guess the password. These attacks don't rely on any prior knowledge — just computational power. Simple or short passwords (like `abc123`) can be cracked in seconds. However, each additional character exponentially increases the difficulty. Advanced attackers use GPU clusters or botnets to perform high-speed attacks.

> **Defense:** Use passwords with high entropy (long, random, and mixed-type characters). Implement rate-limiting, CAPTCHA, and account lockout mechanisms to block automated attempts.

🔹 2. Dictionary Attack

In a dictionary attack, the attacker uses a list of commonly used passwords or dictionary words to guess the password. These lists often include real-world data from past breaches and popular variations (e.g., `summer2023`, `welcome@123`). This method is much faster than brute force because it focuses on likely passwords rather than all combinations.

> **Defense:** Avoid using words from dictionaries, names, or keyboard patterns. Instead, use random character combinations or unpredictable passphrases.

🔹 3. Credential Stuffing

This attack leverages stolen username-password pairs from previous breaches. Attackers try these credentials across other websites, hoping that the victim reused the same password on multiple accounts. Because people often reuse passwords, this method has a high success rate.

> **Defense:** Use a unique password for every service. Enable Multi-Factor Authentication (MFA) to block unauthorized access even if credentials are leaked.

◆ 4. Phishing

Phishing tricks users into giving up their passwords by mimicking trusted websites or services. This often happens via email or fake login pages. The attacker creates a site that looks legitimate and waits for the victim to enter their credentials, which are then stolen.

> **Defense:** Always check the URL of login pages, avoid clicking unknown links, and enable MFA. Security awareness training is also essential to detect phishing attempts.

◆ 5. Keylogging

Keylogging involves malicious software (or sometimes hardware) that secretly records every keystroke made by the user, including passwords. These logs are then sent to the attacker. Keyloggers can be installed via infected downloads or malicious email attachments.

> **Defense:** Use updated antivirus software, avoid untrusted downloads, and consider using on-screen keyboards or password managers that auto-fill credentials.

How Password Complexity Affects Security

Password complexity plays a pivotal role in safeguarding user accounts and digital assets against modern cyber threats. The more complex a password is — through longer length, inclusion of symbols, numbers, uppercase and lowercase characters, and unpredictability — the more resistant it becomes to brute-force and dictionary attacks. For instance, a password like **'123456'** can be cracked in under a second, whereas a password such as **'Zr@2&Jm1^T#9u0'** may take hundreds or thousands of years to breach using current computing power.

Complex passwords increase entropy, which is the level of randomness and unpredictability in a password. High entropy significantly expands the number of possible combinations, making it infeasible for attackers to guess or crack them in a realistic time frame. In addition, complexity disrupts patterns that are often exploited by automated tools in dictionary or credential-stuffing attacks.

However, complexity should not compromise memorability. Using strong but memorable passphrases like **'IL0ve!Cyber$ec2025'** can strike a balance between security and usability. Ultimately, password complexity, when combined with best practices such as regular updates and multi-factor authentication, forms the backbone of a strong identity protection strategy.