Password Security Evaluation Report

# 1. Created Passwords with Varying Complexity

|  |  |
| --- | --- |
| Password | Complexity Description |
| apple123 | Simple, lowercase + numbers |
| Apple123 | Moderate, capital + lowercase + numbers |
| Apple@123 | Stronger, adds symbol |
| App@2025!Secure | Very strong, mixed case, symbols, longer |
| X9!$mQwL#2!b | High entropy, randomized characters |
| 123456 | Very weak, only digits |
| Qwerty!@# | Common pattern, weak to dictionary attacks |
| T1m3$R0ck5! | Strong, passphrase-like |

# 2. Password Strength Checker Results

Based on tools like Kaspersky, LastPass, and Security.org

|  |  |  |  |
| --- | --- | --- | --- |
| Password | Strength | Time to Crack | Feedback |
| apple123 | Weak | Seconds | Too common |
| Apple123 | Moderate | Minutes | Add symbols |
| Apple@123 | Strong | Hours to days | Good, add more length |
| App@2025!Secure | Very Strong | Centuries | Excellent |
| X9!$mQwL#2!b | Very Strong | Centuries | Excellent |
| 123456 | Very Weak | Instant | Avoid common numbers |
| Qwerty!@# | Weak | Seconds to minutes | Too common pattern |
| T1m3$R0ck5! | Strong | Decades | Good structure |

# 3. Feedback Patterns Observed

* - Short passwords (<8 characters) are always weak.
* - Symbols and mixed case improve strength significantly.
* - Randomness and length >12 are crucial.
* - Avoid dictionary words, patterns, or dates.

# 4. Best Practices for Strong Passwords

* - Use at least 12–16 characters.
* - Combine uppercase, lowercase, numbers, and symbols.
* - Avoid using personal information.
* - Prefer random strings or passphrases.
* - Never reuse passwords across websites.

# 5. Tips Learned from Evaluation

* - Longer passwords are stronger than shorter complex ones.
* - Use passphrases with symbols (e.g., MyDog@8EatsFish!).
* - Randomly generated passwords are best for critical accounts.
* - Use a password manager for secure storage.
* - Avoid patterns and predictable substitutions.

# 6. Common Password Attacks

* Brute Force: Tries all combinations. Slower with longer passwords.
* Dictionary Attack: Uses common word lists. Weak against short/simple passwords.
* Credential Stuffing: Tries leaked credentials on other sites.
* Phishing: Tricks users into revealing passwords.

# 7. Summary: How Password Complexity Affects Security

Password complexity significantly increases resistance to attacks. A short password like 'apple123' can be cracked in seconds, while a complex password such as 'App@2025!Secure' might take centuries. Length, randomness, and a mix of character types are key to strong password security.