# Password Strength Evaluation Report

## Step 1: Created Passwords with Varying Complexity

|  |  |
| --- | --- |
| Password | Complexity & Notes |
| password123 | Weak (common, easy to guess) |
| IloveIndia2025 | Weak (common, but longer) |
| Qwerty@123 | Medium (predictable, but improved) |
| Pa$$w0rd | Weak (pattern-based) |
| Mys@f3B@nk!2025 | Medium (uses symbols & caps) |
| !&X4g!8#Tf2ZbPq | Very Strong (random, long) |

## Step 2: Character Type & Length Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Password | Uppercase | Lowercase | Numbers | Symbols | Length |
| password123 | ✗ | ✓ | ✓ | ✗ | Short |
| IloveIndia2025 | ✓ | ✓ | ✓ | ✗ | Medium |
| Qwerty@123 | ✓ | ✓ | ✓ | ✓ | Medium |
| Pa$$w0rd | ✓ | ✓ | ✓ | ✓ | Short |
| Mys@f3B@nk!2025 | ✓ | ✓ | ✓ | ✓ | Medium |
| !&X4g!8#Tf2ZbPq | ✓ | ✓ | ✓ | ✓ | Long |

## Step 3: Password Testing

Tested each password on Security.org and putted screenshots.

## Step 4: Scores and Feedbacks

Scored time to crack and feedback put these.

password123  
Scores: Time to crack - 1 month  
Feedback: Too common, weak.

IloveIndia2025  
Scores: Time to crack - 9 million years  
Feedback: Technically strong due to length (13 characters) and mix of uppercase, lowercase, and numbers. Adding symbols and using uncommon words can improve it.

Qwerty@123  
Scores: Time to crack - 5 years  
Feedback: Pros: Uses uppercase and lowercase letters, includes a number and a special character (@). Cons: Based on a common pattern (Qwerty123), predictable.

Pa$$w0rd  
Scores: Time to crack - 1 week  
Feedback: Common word + leet + too short. Extend length. Weak due to guessable format.

Mys@f3B@nk!2025  
Scores: Time to crack - 41 trillion years  
Feedback: Long, random, strong use of symbols, mixed case, and digits.

!&X4g!8#Tf2ZbPq  
Scores: Time to crack - 41 trillion years  
Feedback: Highly secure, random, long, complex format.

## Step 5: Identify Best Practices for Creating Strong Passwords

- Use long passwords (12+ characters).  
- Mix uppercase, lowercase, digits, and symbols.  
- Avoid common words and predictable patterns.  
- Don't reuse passwords across sites.

## Step 6: Tips Learned from the Evaluation

- Passwords using leetspeak (e.g., Pa$$w0rd) are still weak if predictable.  
- Length plays a major role in cracking time.  
- Random combinations with symbols are much stronger.

## Step 7: Research Common Password Attacks

- Brute Force: Trying all combinations until success.  
- Dictionary Attack: Using a list of common passwords.  
- Phishing and keylogging are also indirect password threats.

## Step 8: Summary of Password Complexity and Security

Password complexity significantly affects security. Longer passwords with mixed characters and randomness are exponentially harder to crack. Avoiding predictable patterns and using unique passwords for different accounts is essential for maintaining cybersecurity.