Task 6: Create a Strong Password and Evaluate Its Strength

## Objective

To create passwords of varying complexity, evaluate their strength using online tools, and understand how complexity impacts password security.

## Tools Used

• PasswordMeter.com (<https://www.passwordmeter.com>)

(or)

• Security.org Password Strength Test (https://www.security.org/how-secure-is-my-password/)

## Passwords Created & Evaluation Results

### 1. Medium Strength (Better, but Still Predictable)

|  |  |  |  |
| --- | --- | --- | --- |
| Password | Score (PasswordMeter) | Crack Time Estimate | Feedback Summary |
| Jo@hua2004 | 62% | A few hours | Better than basic, but still includes name clearly |
| Joshua\_420 | 58% | A few minutes | Use of symbol helps, but still predictable |
| 20Joshua04 | 60% | A few hours | Slight pattern variation, still name-based |
| Jo@h@a420 | 65% | Several hours | Improved with substitutions, but still recognizable |

Medium Security Insight: These passwords show moderate improvement by adding symbols and mixing numbers but are still vulnerable due to the presence of a recognizable name (Prakanth).

### 2. Strong Passwords (High Security)

|  |  |  |  |
| --- | --- | --- | --- |
| Password | Score (PasswordMeter) | Crack Time Estimate | Feedback Summary |
| Jo@h#20ua!420 | 82% | Hundreds of years | Good complexity, special characters, shuffled structure |
| 420\_JosH@uA#2004! | 92% | > 100,000 years | Strong mix of symbols, upper/lowercase, numbers |
| !J@oh20#u22a420$ | 95% | 3 billion years | High randomness and entropy |
| 20JoSh!ua\_4@20 | 88% | Hundreds of thousands of years | Good character variety and moderate memorability |

High Security Insight: Strong passwords hide recognizable patterns and names, include multiple character types, and exceed 12 characters.

## Password Strength Best Practices

✅ Use at least 12 characters

✅ Mix uppercase, lowercase, numbers, and special characters

✅ Avoid using real names, dictionary words, or common patterns

✅ Prefer randomized structures or passphrases

✅ Consider password managers to store and generate strong passwords

## Common Password Attacks:

|  |  |
| --- | --- |
| Attack Type | Description |
| Brute Force | Tries all possible combinations — long, complex passwords reduce risk |
| Dictionary Attack | Uses a list of common or leaked passwords — avoid common names or word-based combos |
| Credential Stuffing | Reuses leaked usernames/passwords from other sites — never reuse passwords |
| Phishing/Social Engineering | Tricks user into giving passwords — complexity helps if leaked |

## How Password Complexity Affects Security

• Password complexity increases the number of guesses required, exponentially boosting resistance to brute-force attacks.  
• Length and diversity (e.g., symbols, case changes) greatly increase entropy (randomness).  
• Predictable or personal passwords, even if long, are still at risk from dictionary or targeted attacks.  
• Passwords like 420\_JosH@uA#2004! take millions to billions of years to crack, while Joshua20 can be cracked instantly.

## Conclusion

Using online tools, it's clear that name-based and short passwords are easily broken, while longer, randomized combinations provide strong security. Best practices like mixing character types and avoiding common patterns help create secure credentials suitable for sensitive accounts.