Task 6: Create a Strong Password and Evaluate Its Strength

Objective:

This task aims to explore the characteristics of strong passwords by creating multiple examples and analyzing their strength using trusted online tools. The outcome is to understand how different password patterns resist various forms of cyberattacks.

Tools and Methodology

The following tools were used to assess password strength:

- PasswordMeter.com
- Security.org Password Strength Checker
- NordPass Password Checker

Passwords were created with varying lengths and character combinations. Each password was then tested using the above tools, and the results were recorded.

Evaluation and Results

The following table presents an analysis of selected passwords, highlighting their complexity, scores, and estimated time to crack. This comparative approach reveals the direct correlation between password structure and resistance to attacks:

Password | Length | Complexity | Score | Crack Time | Feedback

---

abc123 | 6 | Basic digits and letters | 25% | <1 second | Highly insecure

Avi@1234 | 8 | Includes symbol and caps | 63% | 5 hours | Moderate but guessable

AviM@nd@l2025 | 13 | Mixed, long | 88% | 3M years | Good, but still has patterns

Qz!rT7#pLx$9Wd2 | 15 | Fully random, complex | 100% | 1T years | Excellent security

Key Insights and Best Practices

- Use 12+ characters to resist brute force.

- Mix character types: upper, lower, digits, and symbols.

- Avoid names, birthdays, or reused sequences.

- Random placement of characters enhances security.

- Never reuse passwords across services.

Overview of Common Password Attacks

1. Brute Force: Exhausts all combinations.

2. Dictionary Attack: Uses a list of known weak passwords.

3. Credential Stuffing: Leverages leaked passwords from other platforms.

4. Phishing: Tricks users into submitting passwords on fake sites.

Conclusion

Stronger passwords greatly enhance defense against cyberattacks. Tools like password checkers help assess and improve password quality. Following strong password practices is essential in maintaining account security in today's threat landscape.