**Password Strength Evaluation Report**

# Objective

To understand characteristics of a strong password, evaluate different passwords using an online checker, and summarize best practices.

**Tools Used**

Website: https://www.passwordmeter.com

# Passwords Evaluated & Scores

1. pass123-> Score: 32% (Weak) - Too short, lacks complexity

A screenshot of a computer

AI-generated content may be incorrect.

1. Pass1234 -> Score: 54% (Moderate) - No symbols, predictable

A screenshot of a computer

AI-generated content may be incorrect.

1. Pa$$1234 -> Score: 75% (Strong) - Good but short

A screenshot of a computer

AI-generated content may be incorrect.

1. T9^g!Qm#z@Lp -> Score: 100% (Very Strong) - Excellent strength

A screenshot of a computer

AI-generated content may be incorrect.

# Best Practices

* Use 12+ characters.
* Mix uppercase, lowercase, numbers, symbols.
* Avoid real words, names, or patterns.
* Dont reuse passwords across sites.
* Use a password manager and enable MFA.

# Common Password Attacks

* Brute Force: Tries every possible combo.
* Dictionary Attack: Uses common words/passwords.
* Credential Stuffing: Reuses stolen credentials.
* Phishing: Tricks users into revealing passwords.

# Impact of Complexity on Security

* Longer & more complex = harder to crack.
* Random characters increase password entropy.
* Avoiding patterns protects from automated attacks.

# Conclusion

Strong passwords combine length, complexity, and randomness. MFA and password managers are essential for added protection.