Password Strength Evaluation Report

1. Password Strength Analysis

The following passwords were tested against an online password strength checker. Below are their results:

Password	Score	Complexity	Strength Level
1234567890	7%	Very Weak	Poor security, easily guessable
123@	31%	Weak	Not secure, vulnerable to brute-force attacks
blue@123	45%	Good	Moderate security but could be improved
Campus@34	78%	Strong	Good security, but can be enhanced
secret@SAFE#45	100%	Very Strong	Excellent security, highly resistant to attacks

2. Best Practices for Strong Passwords

Through our evaluation, we identified key best practices for password security:

- **Use a combination of characters**: Incorporate uppercase, lowercase letters, numbers, and special symbols.
- **Increase length**: Passwords should ideally be **14+ characters** for enhanced security.
- **Avoid predictable patterns**: Avoid dictionary words, common phrases, and personal details.
- **Ensure uniqueness**: Use different passwords for different accounts to mitigate risk.
- **Use a password manager**: Helps in securely storing complex passwords without memorization.

3. Common Password Attack Methods

Passwords can be compromised through various attack techniques:

- **Brute Force Attacks**: Hackers systematically try all possible combinations until they succeed.
- **Dictionary Attacks**: Uses common words and phrases to crack predictable passwords.
- **Credential Stuffing**: Attempts previously leaked passwords on multiple accounts.
- **Keylogging & Phishing**: Tricks users into revealing credentials.

4. Impact of Password Complexity on Security

The evaluation highlights that complexity directly correlates with resistance to hacking attempts. Stronger passwords with **unique patterns, increased length, and randomness** drastically reduce susceptibility to attacks.