Password Strength Evaluation Report

1. Introduction

The purpose of this report is to evaluate the strength of different passwords using online password strength checkers and to understand what makes a password secure. By testing passwords of varying complexity, we identify best practices for password creation and examine how complexity affects protection against common cyberattacks.

---

2. Tools Used

- **Passwordmeter.com** (primary online password strength checker)
- Comparable free password strength checkers (for cross-verification of results)

---

3. Methodology

1. Created a set of test passwords with varying levels of complexity.
2. Assessed each password using online strength checkers.
3. Recorded scores, feedback, and observed patterns.
4. Researched password attack methods to contextualize results.
5. Summarized findings into best practices.

---

4. Password Strength Evaluation

Password Example	**Features**	**Strength Score / Feedback**	**Observations**
password	Lowercase only, 8 characters	Very Weak (0–10%)	Common dictionary word; trivial to guess.
Password1	Upper + lower + number, 9 characters	Weak (30–40%)	Slightly stronger, but predictable pattern.
P@ssw0rd!	Mixed case + symbols + numbers, 9 chars	Moderate (50–60%)	Better, but still based on a common pattern.

Tr33$Un!v3rse	Mixed case + numbers + symbol, 12 chars	Strong (70–80%)	Good balance of length and complexity.
9#kT!vS1mZpL8@xQ	Random mix, 16 characters	Very Strong (90–100%)	Highly resistant to brute force and dictionary attacks.

---

5. Real-World Scenarios

Scenario 1: Weak Password Breach

An employee at a financial services firm used the password **Password1** for both their email and company portal. Attackers used a **dictionary attack** and cracked the account within seconds. Because the same password was reused across platforms, both personal and corporate accounts were compromised, leading to data theft.

Lesson: Even slight modifications to common words (e.g., Password1) are easily cracked.

Scenario 2: Brute Force on Short Passwords

A social media account with the password **summer22** was brute-forced in under an hour. Attackers then used the compromised account to send phishing messages to all contacts.

Lesson: Short, predictable patterns (word + year) are highly vulnerable.

Scenario 3: Strong Password Protection

A university student used the password **Tr33$Un!v3rse** (12 characters, mixed case, numbers, and symbols). An attacker attempted brute force, but calculations showed it would take **decades** with current computing power. The account remained secure.

Lesson: Strong, complex, and lengthy passwords provide real protection against automated attacks.

Scenario 4: Randomly Generated Password

A cloud storage account protected by **9#kT!vS1mZpL8@xQ** remained safe even after multiple credential-stuffing attempts. The attacker had access to leaked data from other sites, but because this password was **unique and random**, the account was not compromised.

Lesson: Random, unique passwords combined with good security practices (like MFA) offer the highest protection.

---

6. Best Practices for Strong Passwords

- **Prioritize Length:** Use 12–16 characters or more.
- **Mix Character Types:** Combine uppercase, lowercase, numbers, and symbols.
- **Avoid Predictability:** Do not rely on dictionary words or common substitutions.
- **Increase Randomness:** Random sequences are harder to crack.
- **Use Passphrases:** A sequence of unrelated words (e.g., BlueCar$Monkey!47) can be both strong and memorable.
- **Ensure Uniqueness:** Each account should have a different password.
- **Leverage Password Managers:** These tools generate and store strong, unique passwords.

---

7. Common Password Attacks

- **Brute Force Attack:** Systematically tries all possible combinations. Countered by long, complex passwords.
- **Dictionary Attack:** Uses precompiled lists of common words and patterns. Avoiding dictionary words and predictable substitutions prevents success.
- **Credential Stuffing:** Attackers reuse stolen credentials across platforms. Unique passwords for every account mitigate this threat.

---

8. Conclusion

The analysis confirms that **password complexity and length directly enhance security**. Weak, predictable passwords are vulnerable to real-world attacks, while long, random, and unique passwords provide strong defense against brute force and dictionary attacks.

Recommendations:

- Use passwords of at least 12–16 characters.

- Adopt password managers to maintain strong and unique credentials.
- Enable **multi-factor authentication (MFA)** wherever possible.

Final Outcome: This evaluation demonstrates how password complexity impacts real-world security. By applying best practices, individuals and organizations can significantly reduce the risk of compromise.