■ Task 6 — Password Strength Evaluation

Objective: To analyze and evaluate the strength of different passwords using an online password checker, calculate entropy, and understand how password complexity affects security.

■ Passwords Tested

Password: password123

Length: 11 | **Contains:** Lowercase, Numbers

Rating: ■ Very Weak | **Estimated Crack Time:** 0 seconds

Summary: Common and predictable; easily cracked instantly.

Password: P@ssw0rd!

Length: 9 | **Contains:** Lowercase, Uppercase, Numbers, Symbol

Rating: ■ Very Weak | **Estimated Crack Time:** 0 seconds

Summary: Common dictionary pattern with substitutions.

Password: 7clouds9Song

Length: 12 | **Contains:** Lowercase, Uppercase, Numbers

Rating: ■■ Strong | **Estimated Crack Time:** 1 month

Summary: Strong but could be improved by adding symbols.

Password: Taco$Blue8Tree#

Length: 15 | **Contains:** Lowercase, Uppercase, Numbers, Symbols

Rating: ■ Very Strong | **Estimated Crack Time:** 338 years

Summary: Excellent strength; meets modern security standards.

Password: correct horse battery staple

Length: 28 | **Contains:** Lowercase only

Rating: ■ Very Strong | **Estimated Crack Time:** 13 million years

Summary: Extremely strong due to long length and randomness.

■ Observations

1. Short or common passwords are instantly cracked by brute-force or dictionary attacks.
2. Length and randomness are key — long passphrases outperform short complex passwords.
3. Mixed character types drastically increase entropy.
4. Passwords ≥15 characters are generally resistant to brute-force attacks.

■ Recommendations

- Use at least 12–16 characters per password.
- Combine uppercase, lowercase, digits, and symbols.
- Prefer random passphrases (4–6 unrelated words).
- Store credentials securely with a password manager (e.g., Bitwarden, KeePass).
- Enable Multi-Factor Authentication (MFA).
- Avoid personal info or predictable substitutions.

■ Conclusion

Long, random passwords or multi-word passphrases are nearly impossible to brute-force. The best balance between security and memorability is a random passphrase (≥6 words) or a 15+ character mixed password stored in a manager with MFA.

■■ Five Common Password Attacks

1. Brute-force attack

What: Try every possible password until one works (offline or online).

Indicators: Repeated failed login attempts; many auth attempts in logs.

Defenses: Enforce long passwords, rate-limit logins, account lockouts, require MFA.

2. Dictionary attack

What: Try common words, phrases and predictable variants instead of all combinations.

Indicators: Rapid successful guesses for weak accounts using common words.

Defenses: Ban common passwords, use strength checks, require minimum entropy/length.

3. Password spraying

What: Try a small set of very common passwords across many accounts to avoid lockouts.

Indicators: Low-volume failed attempts across many accounts.

Defenses: Per-account and per-IP rate limits, MFA, anomaly detection.

4. Credential stuffing

What: Use leaked username/password pairs from other breaches to try logins elsewhere.

Indicators: Login attempts using known emails from breach lists; successful logins after breach disclosures.

Defenses: Detect reused passwords, use breach-checking (k-anonymity), enforce MFA and unique passwords.

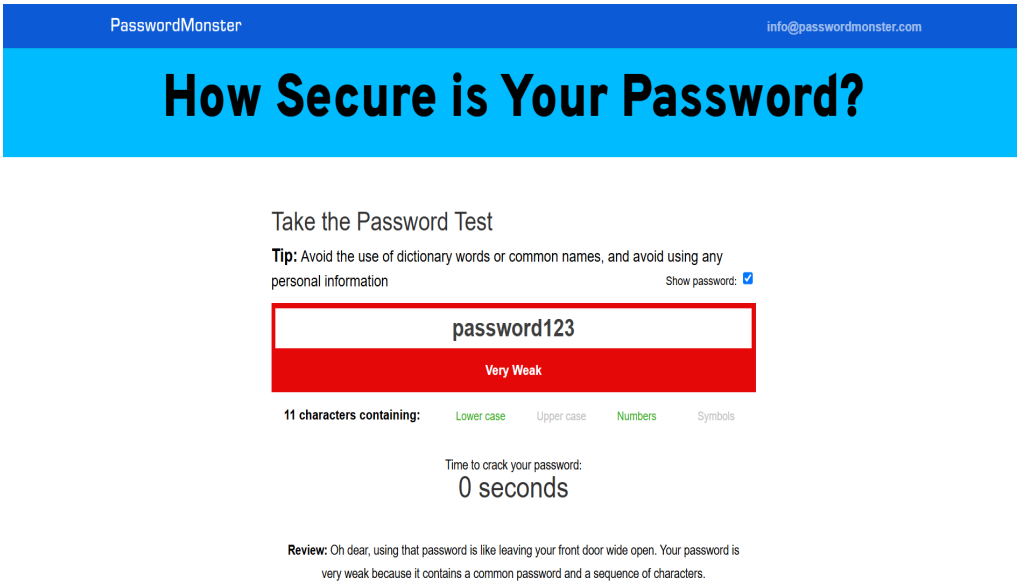
5. Phishing (credential harvesting)

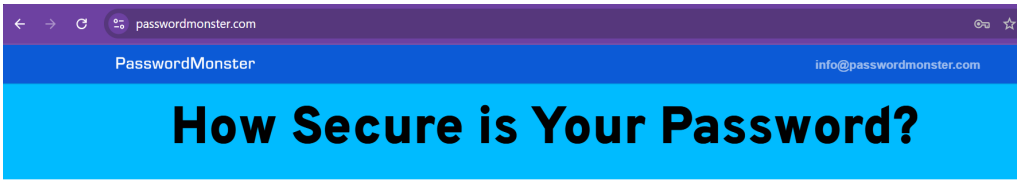
What: Trick users into submitting credentials to fake sites or via social engineering.

Indicators: Users report suspicious emails; unexpected password resets or logins from new devices.

Defenses: Phishing awareness training, email protections (SPF/DKIM/DMARC), phishing-resistant MFA.

■ Screenshot Evidence





Take the Password Test

Tip: Avoid the use of dictionary words or common names, and avoid using any personal information

Show password: ☑

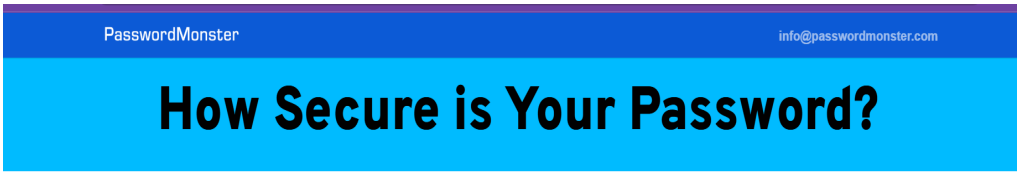
P@ssw0rd!

Very Weak

9 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
0 seconds

Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it contains a common password and a dictionary word.



Take the Password Test

Tip: Stronger passwords use different types of characters

Show password: ☑

Taco$Blue8Tree#

Very Strong

15 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
338 years

Review: Fantastic, using that password makes you as secure as Fort Knox.

Take the Password Test

Tip: Avoid the use of dictionary words or common names, and avoid using any personal information

Show password:

7clouds9Song

Strong

12 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
1 months

Review: Good, using that password is like locking your front door and keeping the key in a safety deposit box.

Take the Password Test

Tip: Stronger passwords use different types of characters

Show password:

correct horse battery staple

Very Strong

28 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
13 million years

Review: Fantastic, using that password makes you as secure as Fort Knox.