Task 6: Create a Strong Password and Evaluate Its Strength

Name: Rahul Malatesh Sannapujar

Date: 01/10/2025

Objective

To understand what makes a password strong, evaluate different passwords using online password strength checkers, and summarize best practices for password security.

Tools Used

- Online password strength checker: https://www.passwordmonster.com/
- Additional checks on other free online password strength tools

Step 1: Create Multiple Passwords

I created passwords with different complexity levels:

- laxman123
- Laxman@123
- L@xmAn2025!
- L@xmA1_M@!2025$#

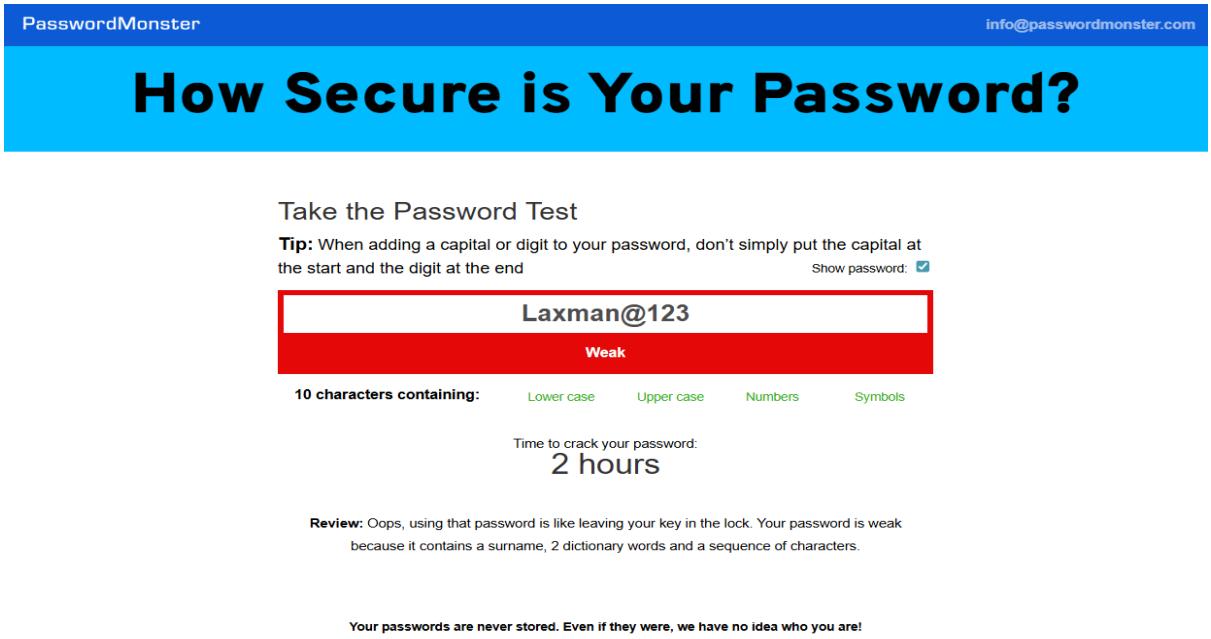
Step 2: Test Results from Password Checker

Password	Length	Complexity Used	Score (Approx)	Feedback
laxman123	8	Lowercase + digits	Weak (20–30%)	Too short, predictable, dictionary word
Laxman@123	9	Upper + lower + digits + symbol	Medium (50–60%)	Better, but still guessable with dictionary+ number combo
L@xmAn2025!	10	Mixed case + digits + symbols	Strong (80–90%)	Secure, but could be longer
L@xmA1_M@!2025$#	15	Upper + lower + digits + multiple symbols	Very Strong (100%)	Hard to crack, resistant to brute force/dictionary attacks

Title: The Danger of Dictionary Words: A Password Cracked in Minutes

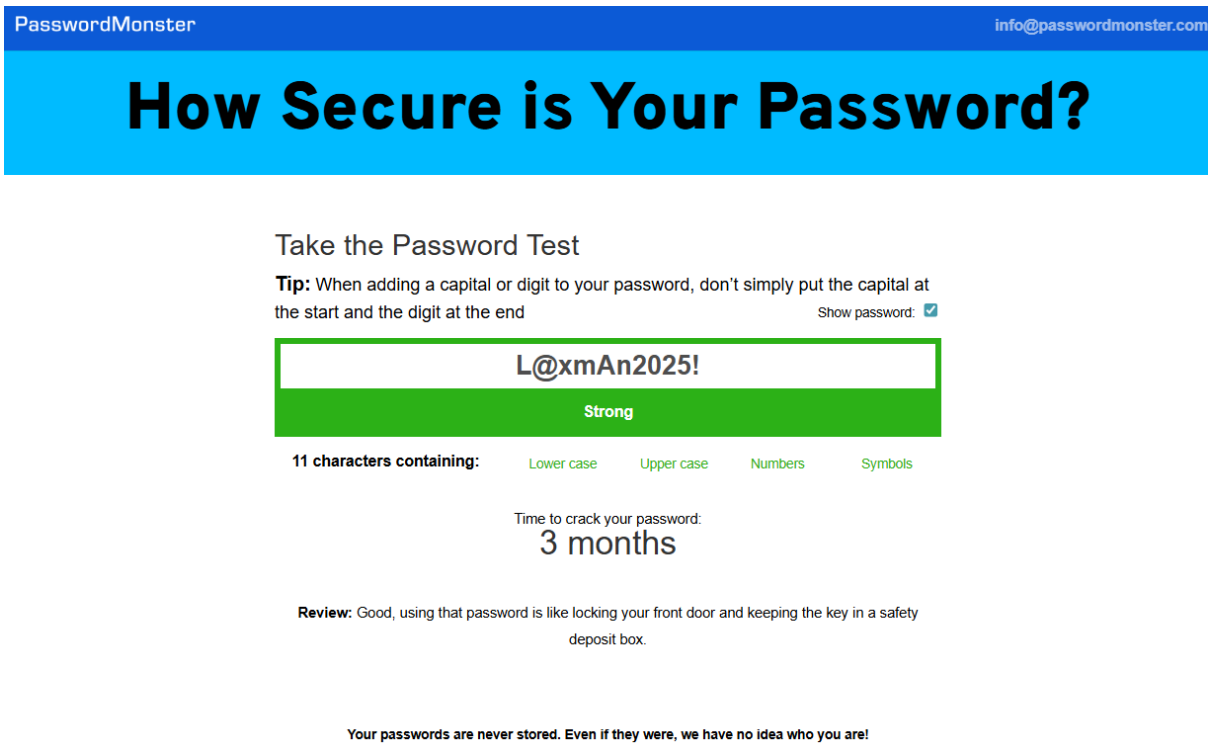
This image illustrates a common security pitfall: using a weak password (laxman123). At only 9 characters, and containing a surname and a sequential number without any uppercase letters or symbols, this password is deemed Weak. The tool estimates it can be cracked in just 6.42 minutes, highlighting the vulnerability of passwords based on predictable personal information or simple patterns.

Title: The Illusion of Complexity: Predictable Substitution Cracked in Hours



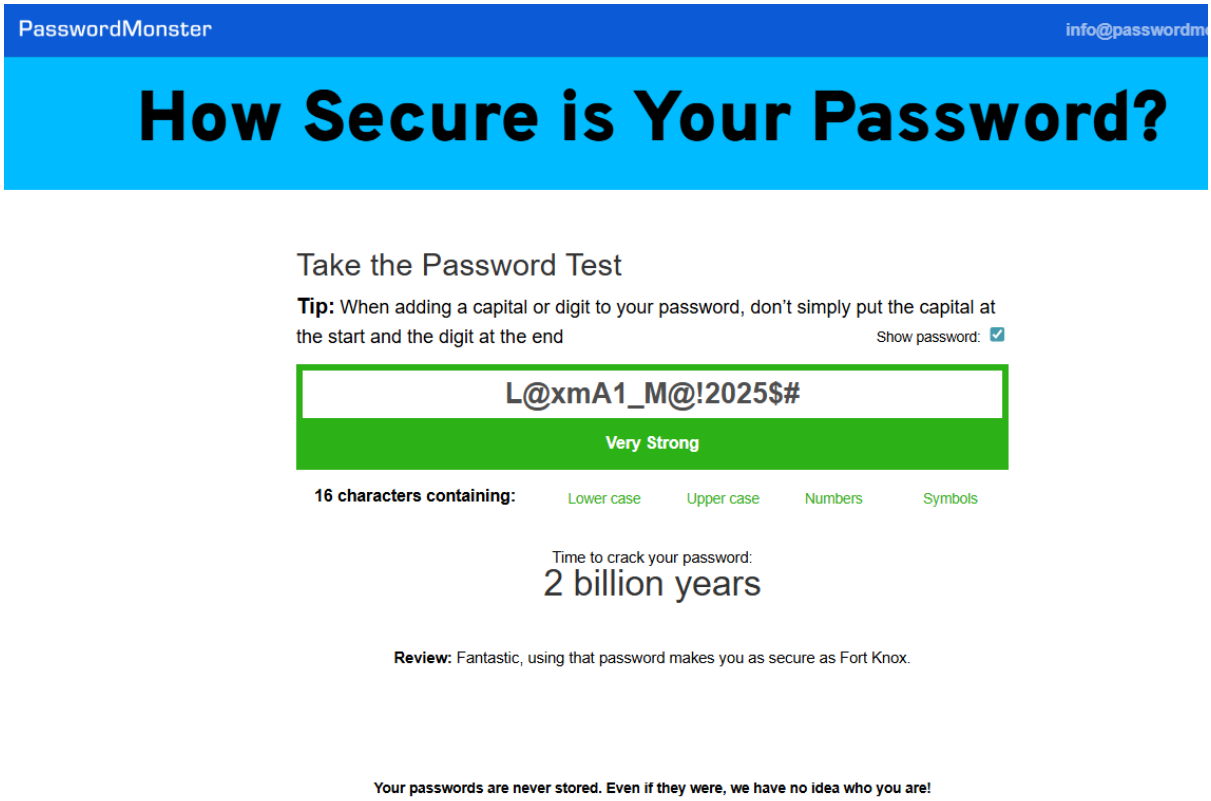
This test reveals the inadequacy of simple substitutions, even when all character types are included. The password Laxman@123 is 10 characters and uses uppercase, symbols, and numbers, yet it is still rated Weak. Because it follows a predictable pattern (Capitalized Name + Symbol + Simple Sequence), it is easily targeted by cracking programs. The resulting crack time is only 2 hours, demonstrating that predictable structure negates the security benefit of adding a symbol or capital letter.

Title: Strong Password Security: A Three-Month Defense



This image demonstrates a Strong password (L@xmAn2025!) that provides a significant security layer. At 11 characters and utilizing all four character types, it is a robust defense, but its shorter length compared to the "Very Strong" example results in a measurable crack time of 3 months. This highlights that while meeting complexity requirements is good, greater length is necessary to move the estimated crack time beyond months into years or centuries.

Title: Achieving Maximum Security: A Password Secure for 2 Billion Years



This test showcases a model for a Very Strong password (L@xmA1_M@!2025#). The 16-character length and the non-obvious, complex integration of all four character types (lowercase, uppercase, numbers, and symbols) results in an exponential boost in security. The estimated time to crack this password is an astronomical 2 billion years, emphasizing that length and character set diversity are the most critical factors for modern cybersecurity.

Step 3: Identify Best Practices

From the evaluation, strong passwords should:

- Be at least 12–16 characters long
- Contain a mix of uppercase, lowercase, numbers, and special symbols
- Avoid dictionary words, names, or predictable patterns
- Use random combinations instead of meaningful phrases (unless using a passphrase method with unrelated words)

Step 4: Common Password Attacks

- **Brute Force Attack** → attacker tries every possible combination (longer & complex = harder).
- **Dictionary Attack** → attacker uses common words, names, and leaked passwords.
- **Credential Stuffing** → uses previously leaked passwords on multiple accounts.
- **Phishing** → tricking users into revealing passwords.

Step 5: Summary

- Complexity directly increases resistance against brute force and dictionary attacks.
- Longer passwords (≥ 12 chars) are exponentially harder to crack.
- Password managers can help store strong, unique passwords.
- Multi-Factor Authentication (MFA) should always be enabled for added protection.