# Password Complexity and Security Report

**Author:** DHARUNYA  
**Date:** Tuesday, September 30, 2025

## Executive Summary

This report provides an in-depth evaluation of password strength and security practices by creating, testing, and analyzing multiple passwords of varying complexity. It highlights best practices, common attack methods, the impact of password complexity on security, and recommendations for robust password management.

## Methodology

* **Passwords Created:** Multiple passwords with different lengths and combinations of uppercase, lowercase, numbers, and symbols.
* **Tools Used:** Online password strength checkers (Password Monster, Bitwarden, Kaspersky Password Checker).
* **Evaluation:** Each password was tested for strength, and feedback was recorded. Scores, crack times, and tool recommendations were noted for each password.

## Findings

## Password Strength Results

* **Short/simple passwords** (e.g., "abcd1234"): Rated very weak; can be cracked in seconds. These often use only lowercase letters and numbers, making them highly vulnerable.
* **Medium complexity passwords** (e.g., "Abc12345"): Rated medium; crack time is hours to days. These may include mixed case and numbers but often use dictionary words or predictable patterns.
* **Long, complex passwords** (e.g., "Q$8r2!uP9x@Lw3s"): Rated very strong; crack time is centuries. These use a mix of cases, numbers, symbols, and avoid common words or patterns.
* **Feedback:** Password checkers consistently recommend longer passwords with a mix of character types and avoiding dictionary words or keyboard patterns.

## Best Practices for Strong Passwords

* Use at least **12–16 characters** for each password.
* Include **uppercase, lowercase, numbers, and symbols**.
* Avoid dictionary words, names, or predictable patterns (like "qwerty" or "asdfghjkl").
* Never reuse passwords across accounts.
* Change passwords regularly, especially for sensitive accounts (every 90 days is recommended).
* Use password managers to generate and store strong, unique passwords securely. Tips Learned
* Password length is the most important factor for strength.
* Adding symbols and mixing character types increases security.
* Avoid keyboard walks and common patterns, as attackers include these in their cracking tools.
* Password managers or log templates can help organize and store strong, unique passwords safely.

## Common Password Attacks

* **Brute Force:** Attackers try every possible combination; short/simple passwords are easily cracked.
* **Dictionary Attack:** Uses lists of common words and patterns; passwords with dictionary words or keyboard walks are vulnerable.
* **Credential Stuffing:** Attackers use leaked username/password pairs from previous breaches; password reuse increases risk.
* **Phishing:** Tricks users into revealing passwords via fake websites or emails.
* **Rainbow Table Attack:** Uses precomputed tables to reverse password hashes; weak or unsalted hashes are at risk.
* **Password Spraying:** Tries a few common passwords across many accounts to avoid detection.
* **Keylogging:** Malware records keystrokes, capturing passwords as users type them.

## In-Depth Analysis: Password Trends and Risks

Recent research shows that even long passwords can be compromised if they use predictable patterns or have been exposed in breaches. For example, "Qwerty" and other keyboard walks are among the most commonly breached passwords. The average compromised password length in recent studies was 8-12 characters, but millions of breached passwords were over 16 characters. This highlights the need for not just length, but true randomness and uniqueness.

Organizations should audit their password policies and scan for compromised passwords regularly. Weak or reused passwords, blank passwords, and passwords that never expire are major vulnerabilities. Implementing policies that block known breached passwords and enforce complexity requirements is critical for reducing risk.

## How Password Complexity Affects Security

* **Complex passwords** (long, random, mixed characters) are much harder to crack, making brute force and dictionary attacks impractical.
* **Simple or reused passwords** are easily guessed or compromised, especially in credential stuffing attacks.
* **Regular updates and unique passwords** for each account reduce the risk of widespread compromise.
* **Predictable patterns** (like keyboard walks) are targeted by attackers and should be avoided.

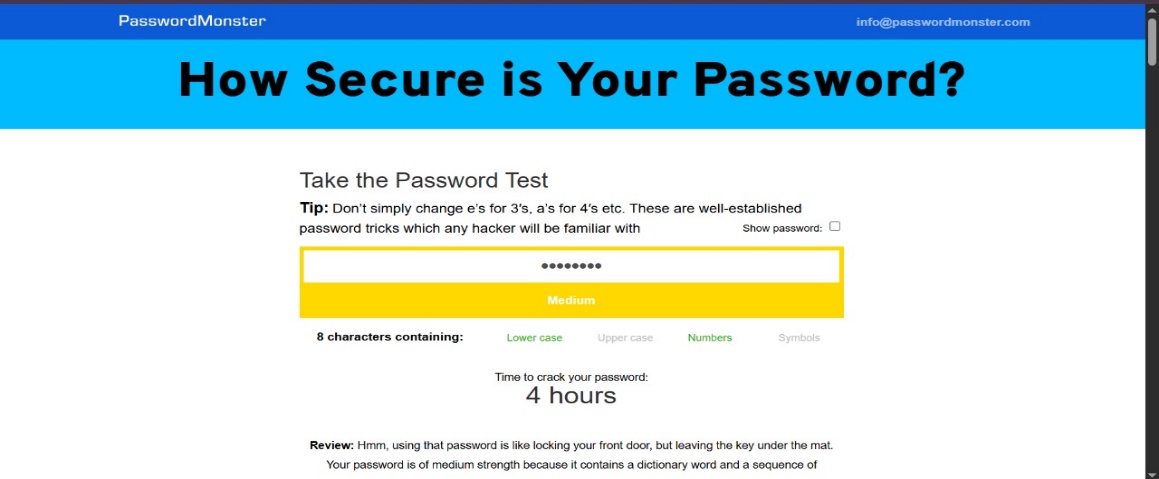
## Recommendations

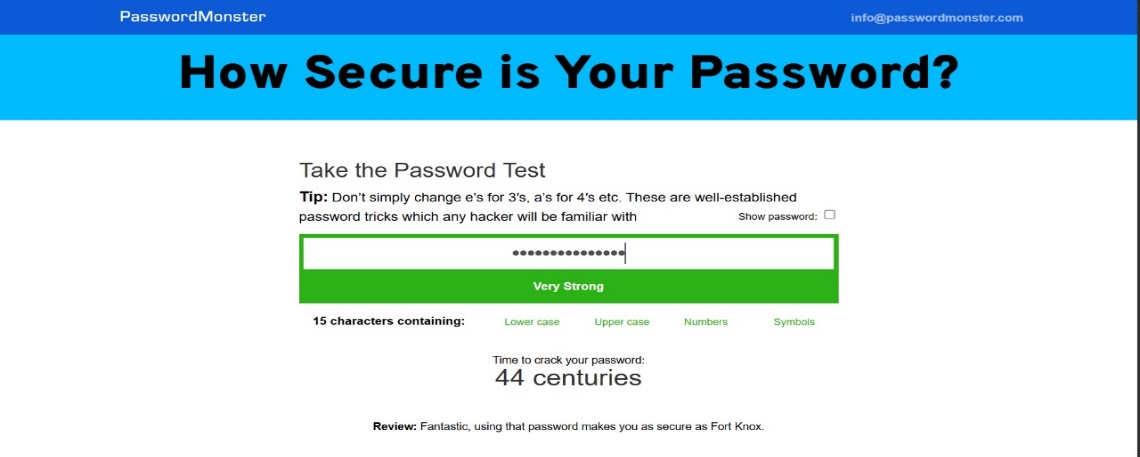
* Enforce a minimum password length of 13 characters for all accounts.
* Block the use of known breached passwords and common patterns.
* Require password changes for sensitive accounts at least every 90 days.
* Educate users about phishing and social engineering risks.
* Use password managers to help users create and store strong, unique passwords.
* Regularly audit password policies and scan for compromised credentials.

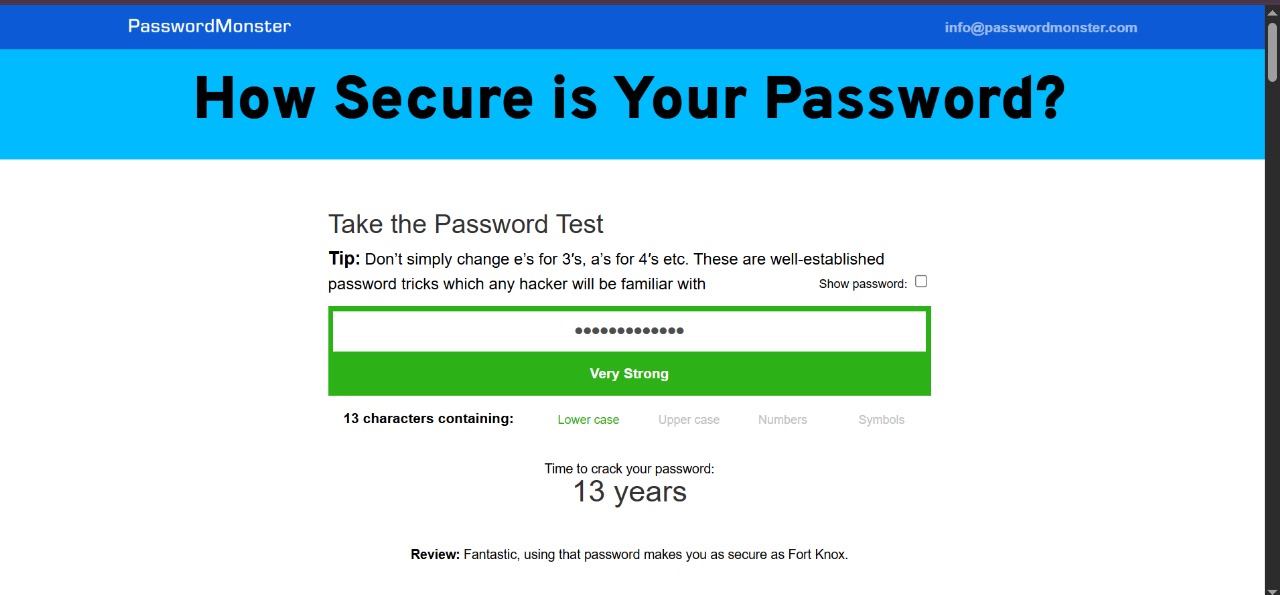
## Conclusion

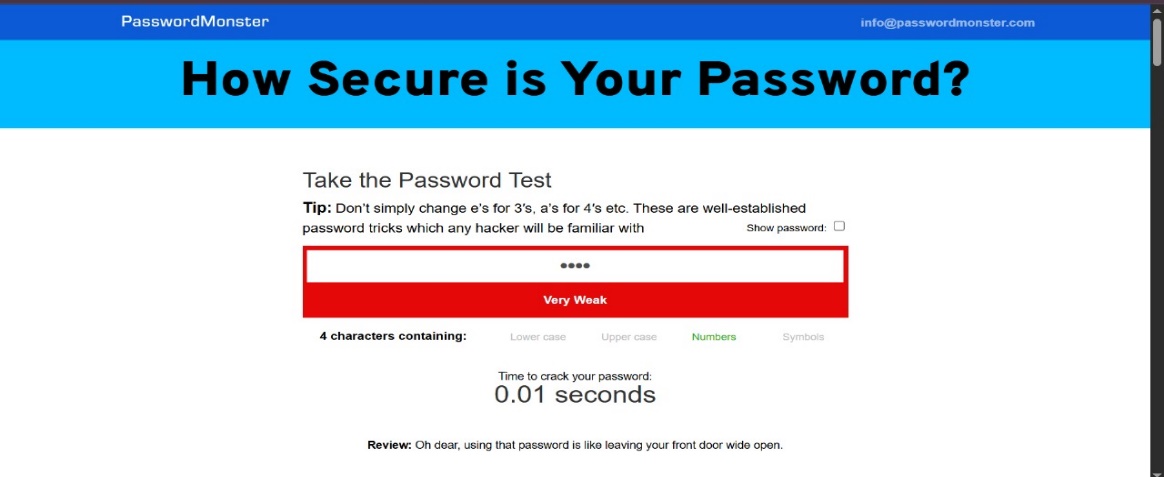
Strong password practices - using long, complex, and unique passwords - are essential for protecting accounts and data. Understanding common attack methods and following best practices significantly improves security and reduces the risk of compromise. Organizations and individuals must stay vigilant, update policies, and use modern tools to defend against evolving password threats.

**Photos**

****

****

****

****