

Password Strength Survey

Aymen MSADDAK
Moona SAADAOU
Husin KHLIF
Aya ARFAOUI

April 27, 2025

1 Introduction

This survey is conducted on real-world implementations of password strength testers to examine how companies and organizations integrate these tools into their systems.

2 Corporate/Enterprise Implementations

Large organizations enforce password policies to protect sensitive data, comply with regulations, and mitigate breaches.

2.1 Microsoft Active Directory (AD)

AD's Group Policy Object (GPO) lets admins enforce rules such as:

- Minimum length (e.g., 12+ characters).
- Complexity requirements (uppercase, numbers, special chars).
- Block lists for common passwords (e.g., "Password123").
- Regular password expiration (though NIST now discourages this).

The implementation integrates with Azure AD for hybrid cloud environments, adding breach detection (screens passwords against leaked databases).

AD is used by 90 percent of Fortune 500 companies as it shows how legacy systems adapt to modern threats (e.g., phishing-resistant MFA).

Sources:

- [Password policy recommendations - Microsoft 365 admin](#) published on 04/02/202
- [Eliminate bad passwords using Microsoft Entra Password Protection](#) published on 03/04/2025

2.2 Google Workspace

Google Workspace implements specific password guidelines and rules that include:

- Length over complexity: Encourages long passphrases (e.g., "correct-horse-battery-staple").
- Breach detection: Flags passwords exposed in third-party breaches (via Google's 'Password Checkup' tool).
- MFA enforcement: Requires 2FA for admin accounts.

How it Works:

- Demonstrate the shift from rigid rules to user-friendly, risk-based policies.
- Use machine learning to detect suspicious log-ins.

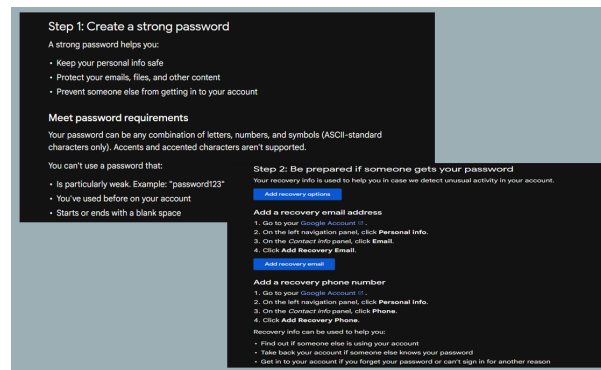


Figure 1: Create a strong password and a more secure account

Sources: [Google's Password Recommendations](#)

2.3 Financial Institutions

Major financial institutions such as JPMorgan Chase and HSBC implement stern regulation when it comes to passwords:

- Strict complexity: 12+ characters, mandatory special characters, no reuse, etc.
- MFA everywhere: applications require biometrics or hardware tokens after password entry.

These organizations also execute behavioral analysis by detecting brute-force attempts in real time. How it works:

- Complies with PCI-DSS and FFIEC regulations.
- High-security sectors prioritize "defense in depth."



Figure 2: Password time to crack

Sources:

- [It's time to change your password](#) published on January 2014
- [Authentication and Access to Financial Institution Services and Systems](#) published on August 2021

2.4 Tech Companies

Cisco's Identity Services Engine (ISE):

- Rates passwords in real time using entropy checks.
- Integrates with threat intelligence feeds to block compromised passwords.

IBM's Security Verify uses AI to detect weak passwords (e.g., keyboard patterns like 'qwerty'). These regulations show enterprise-grade tools that combine password testers with broader IAM (Identity Access Management).



Figure 3: Know and control devices and users on your network

Sources:

- [Cisco Identity Services Engine \(ISE\)](#)
- [IBM Products](#)

2.5 Common Challenges in Enterprises

- User Pushback: Employees bypass rules by incrementing passwords (e.g., 'Summer2023' → 'Summer2024').
 - Solution: Training + nudges (e.g., showing password strength in real time).
- Legacy Systems: Older software may not support modern standards (e.g., 256-character passwords).
 - Solution: Middleware like 'Thycotic Secret Server' to bridge gaps.

3 Web Applications and E-Commerce

Different platforms implement and enforce password security measures and regulations in different ways.

3.1 Dropbox: Advanced Password Strength Estimation with zxcvbn

Dropbox developed zxcvbn, an open-source password strength estimator that evaluates passwords based on their resistance to guessing attacks, rather than simplistic criteria such as length or character variety.

Key Features:

- Analyzes passwords against a large dataset of common passwords, names, and patterns.
- Recognizes and penalizes predictable patterns such as dates, repeated characters, and keyboard sequences.

- Provides real-time feedback without enforcing rigid composition rules, promoting user-friendly passphrases.

Security1!

password:	Security1!	
guesses_log10:	5.29842	
score:	1 / 4	
function runtime (ms):	2	
guess times:		
100 / hour:	3 months	(throttled online attack)
10 / second:	6 hours	(unthrottled online attack)
10k / second:	20 seconds	(offline attack, slow hash, many
10B / second:	less than a second	(offline attack, fast hash, many
warning:	This is similar to a commonly used password	
suggestions:	- Add another word or two. Uncommon words are better - Capitalization doesn't help very much	
match sequence:		
	'Security'	'1!'
pattern:	dictionary	pattern: bruteforce
guesses_log10:	2.97497	guesses_log10: 2
dictionary_name:	passwords	
rank:	472	
reversed:	false	
base-guesses:	472	
uppercase-variations:	2	
l33t-variations:	1	

Figure 4: Password Strength Estimation Interface

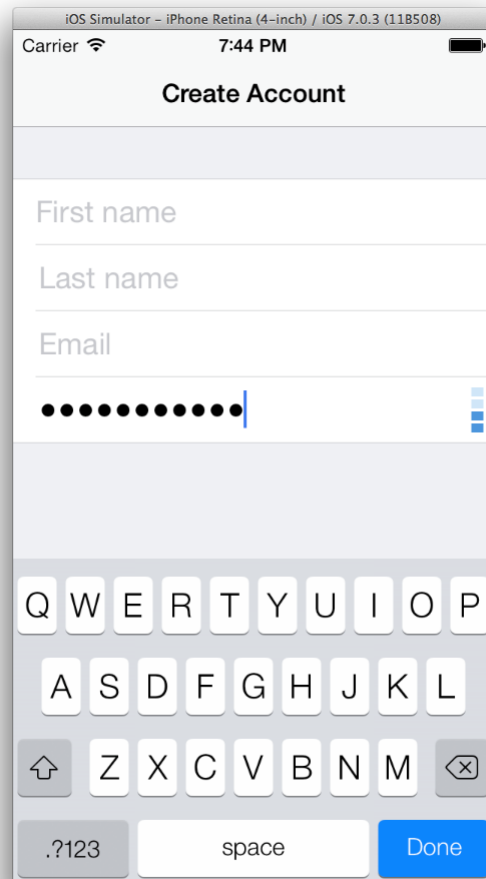


Figure 5: Implementation in iOS Applications

Sources: [Dropbox Tech Blog on zxcvbn](#)

3.2 WordPress: Enforcing Strong Passwords via Plugins

WordPress, a widely used content management system, improves password security through plugins such as Force Strong Passwords and Password Policy Manager. These tools enforce robust password policies, especially for administrator accounts.

Key Features:

- Mandates minimum password lengths and complexity requirements.
- Prevents the use of common or previously compromised passwords.
- Integrates seamlessly into the WordPress admin interface for ease of use.

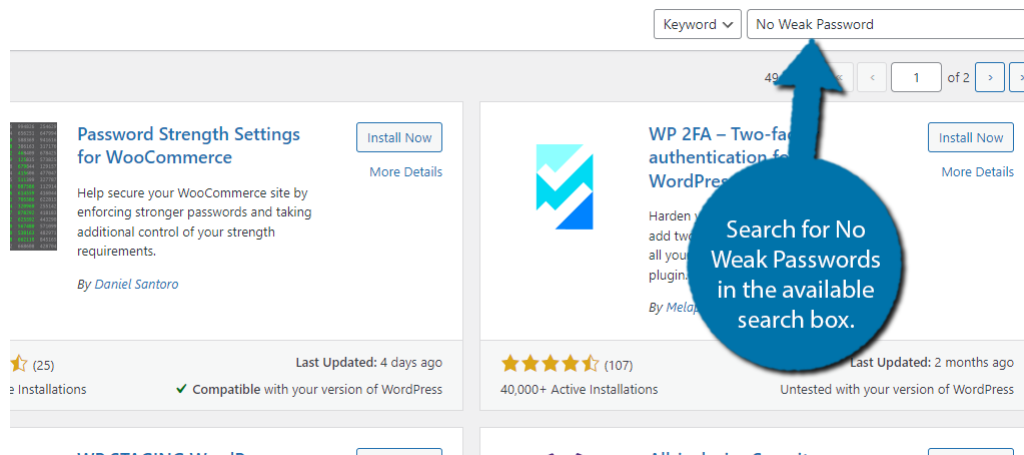


Figure 6: Force Strong Passwords Plugin Interface

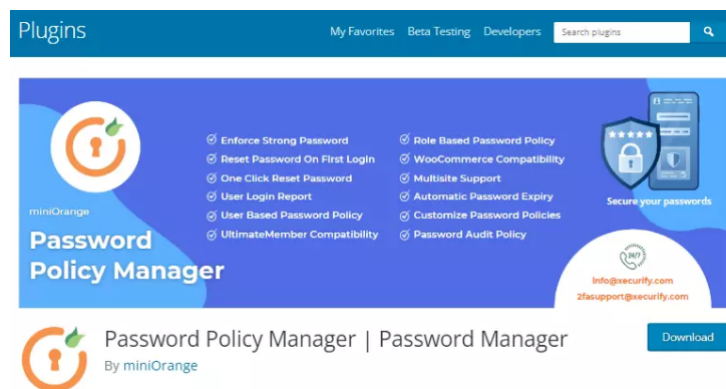


Figure 7: Password Policy Manager Settings

Sources:

- [WPBeginner Guide on Forcing Strong Passwords](#)
- [ServerGuy on Password Policy Manager](#)

3.3 Amazon: Balancing Security and Usability

Amazon implements password policies that encourage strong passwords while maintaining user convenience. Their guidelines focus on balancing security and user experience.

Key Features:

- Recommends passwords with a minimum length and a mix of character types.
- Discourages the use of easily guessable information, such as names or common words.
- Has introduced passkey support, allowing users to authenticate using biometric data for enhanced security and ease of access.



The image shows the Amazon 'Create new password' interface. At the top is the Amazon logo. Below it, the heading 'Create new password' is followed by the text 'We'll ask for this password whenever you Sign-In.' There are two input fields: 'New password' and 'Re-enter password', both containing ten black dots. A blue information icon and text state 'Passwords must be at least 6 characters.' At the bottom is a large yellow button labeled 'Save changes and Sign-In'.

Figure 8: Amazon Password Update Interface

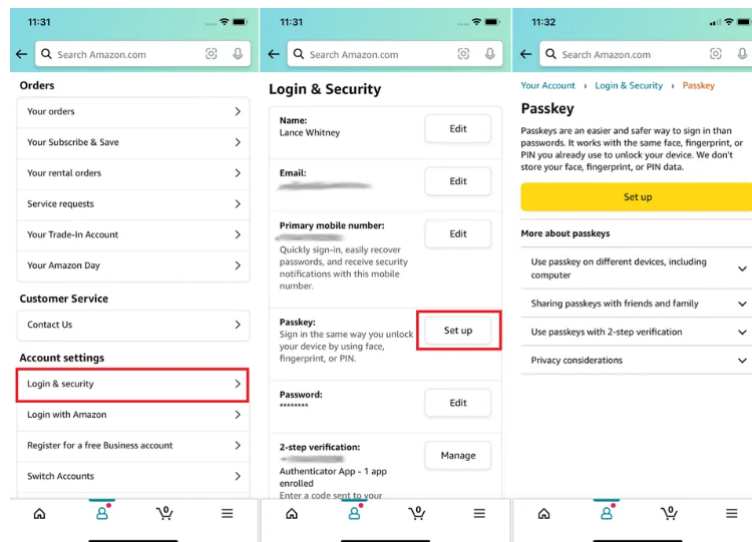


Figure 9: Passkey Authentication Overview

Sources:


- [Amazon WorkMail Password Best Practices](#)
- [Amazon Help on Passkeys](#)

4 Government and Healthcare

U.S. Federal Systems follow NIST SP 800-63B, which discourages frequent password resets, but mandates screening against breach databases.

4.1 Government Sector: NIST Guidelines and Implementations

- NIST SP 800-63B: Digital Identity Guidelines:
 - Password Composition: Discourages the use of complexity requirements and periodic password changes, as these can lead to predictable patterns.
 - Password Strength Meters: Encourages the use of password strength meters to provide real-time feedback during password creation, helping users choose stronger passwords.
 - Blacklist Common Passwords: Recommends checking passwords against a list of commonly used or compromised passwords to prevent their use.
 - Throttling Authentication Attempts: Advises implementing throttling mechanisms to mitigate online password-guessing attacks.
- NIST SP 800-118: Guide to Enterprise Password Management:
 - Policy Development: Guide for creating effective password policies that balance security and user convenience.
 - User Education: Emphasizes the importance of educating users about password best practices.
 - Password Management Tools: Recommends the use of password managers and strength meters to assist users in creating and maintaining strong passwords.

% of Passwords Found to be Compromised but Otherwise Compliant				
	Minimum Password Length	Maximum Password Length	Password Complexity	Recommended actions to prevent compromised passwords
NIST 78% Compliant	At least 8 characters	—	Disallow context-specific words as passwords Prevent the use of repetitive or incremental passwords	Check passwords against breached password lists
PCI 59% Compliant	At least 7 characters	—	At least 1 number and one alpha character	—
HITRUST/HIPAA 57% Compliant	At least 8 characters	—	At least 1 upper or lower or number or symbol Not too many consecutive identical characters	—
ICO/GDPR 43% Compliant	At least 10 characters	Do not set maximum password length	Don't mandate the use of special characters	Block the use of common and weak passwords. Screen passwords against a password list of the most commonly used passwords, leaked passwords from breaches and guessable words related to the organization. Update the leaked password list regularly and explain to users why their passwords have been rejected.
NCSC 83% Compliant	At least 8 characters	Do not set maximum password length	—	Change passwords promptly when suspected they have been compromised

*Over 800 million known compromised passwords analyzed SOURCE: specopssoft.com/blog/83-percent-known-compromised-passwords-satisfy-regulatory-requirements

Figure 10: Percentage of Passwords to be Compromised but Otherwise Compliant

Sources:

- [NIST Special Publication 800-63B](#)
- [Office of Inspector General](#)
- [NIST Pages](#)

4.2 Healthcare Sector: HIPAA Technical Safeguards

- HIPAA Security Rule: Technical Safeguards:
 - Access Control: Implements unique user identifications and emergency access procedures.
 - Audit Controls: Record and examine access and activity in systems containing e-PHI.
 - Integrity Controls: Ensure that e-PHI is not altered or destroyed improperly.
 - Authentication: Verify that a person or entity seeking access to e-PHI is who they claim to be.
- Integration of Password Strength Testers:
 - Real-Time Feedback: Providing users with immediate feedback on password strength during creation.
 - Enforcing Strong Passwords: Preventing the use of weak or commonly used passwords.
 - User Training: Educating staff about the importance of strong passwords and how to create them.

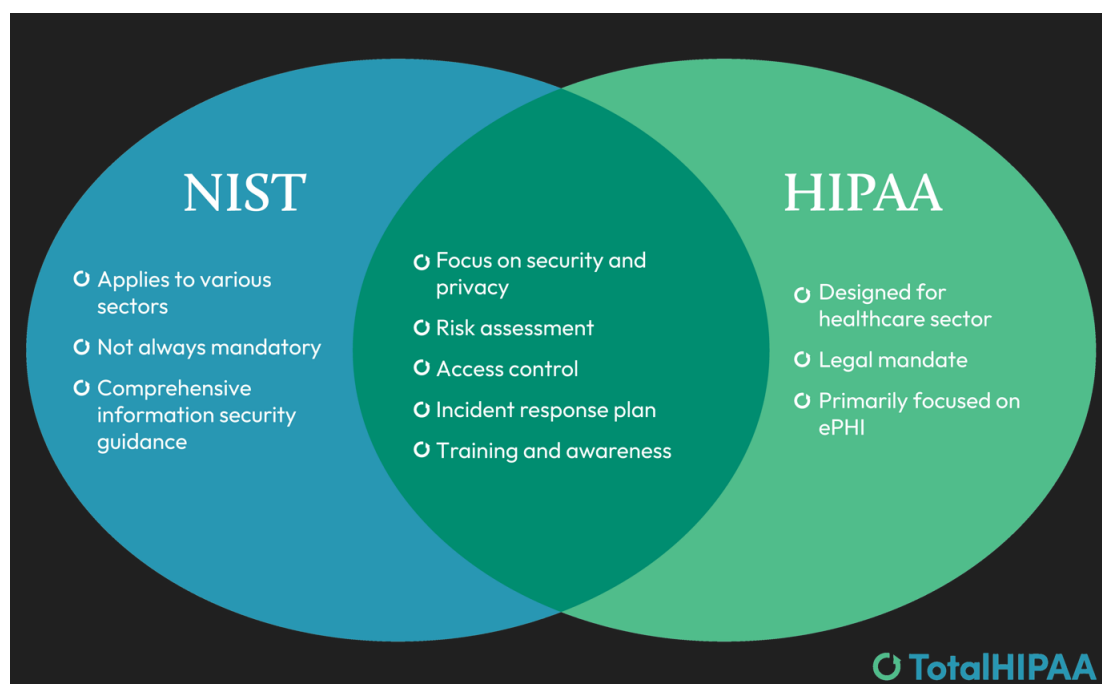


Figure 11: NIST / HIPAA

Sources:

- [Guidance on Risk Analysis Requirements under the HIPAA Security Rule](#)
- [HIPAA Security Series 4 - Technical Safeguards](#)

5 Open-Source Tools and Libraries

5.1 Famous Tools:

- [KeePass](#): uses entropy-based strength meters, providing feedback after password entry.
- [Bitwarden](#): offers real-time strength feedback during password creation, powered by zxcvbn.
- [LastPass](#): provides basic strength feedback using zxcvbn, though not as dynamic as others.
- [1Password](#): offers custom feedback combined with zxcvbn, giving real-time suggestions as you type.

5.2 GitHub Repositories for Password Strength Estimation:

- [Low-Budget Password Strength Estimation](#): a password strength estimator inspired by password cracking techniques, developed by Dropbox.

- [passowrd-sheriff](#): enforces password policies, including length, character sets, and strength.
- [owasp-password-strength-test](#): an OWASP project that tests password strength based on patterns and entropy.

5.3 Feature Comparison: Password Manager Strength Feedback

Feature	LastPass	1Password	Bitwarden	KeePass
Password Strenght Meter	Yes (zxcvbn-based)	Yes (custom + zxcvbn integration)	Yes (real-time, zxcvbn)	Yes (entropy-based)
Real-Time feedback	Limited	Yes	Yes	No (post-entry)
Open Source	No	No	Yes	Yes
Custom Policy Supprt	Yes	Yes	Yes	Yes
Cross-Platform Sync	Yes	Yes	Yes	via plugins / sync tools

Table 1: Feature Comparison