GUIDE

STRENGTHEN YOUR PASSWORD SECURITY

A Best Practices Guide to Implementing NIST Standards

Included Inside:

How SpyCloud Active Directory Guardian helps you meet NIST password standards automatically.

SpyCloud

PASSWORDS CONTINUE TO BE A WEAK LINK IN SECURITY DEFENSES

It's no surprise that passwords remain a favorite target for cybercriminals. After all, juggling complicated password requirements and countless accounts is a recipe for predictable patterns. Due to the continuously expanding scope of a person's digital exhaust, many users fall into traps like recycling old passwords, tweaking them slightly to meet complexity rules, or opting for simple, easy-to-guess passwords.

According to our research, 70% of users reuse passwords.

These behaviors make life easier for attackers. Armed with automated tools, they carry out credential stuffing and password spraying attacks on a massive scale. The impact? **53% of security professionals** report that poor password practices hinder their ability to prevent account takeover (ATO), while ATO attacks themselves increased by **24%** year-over-year.

Without strong password policies and enforcement, it only takes one weak or compromised password to threaten your authentication processes and increase the risk of data breaches, financial losses, and operational chaos – even if you're running MFA and SSO.

To help organizations tackle these challenges, **the National Institute of Standards and Technology (NIST) revamped its password guidelines** in SP 800-63-4 in 2024 to focus on usability and security. The updated recommendations account for real-world user behavior while promoting modern authentication strategies that strengthen defenses against today's identity threats, including preventing the use of passwords exposed on the dark web. And for those of you running Active Directory, SpyCloud Active Directory Guardian can make NIST guideline implementation easy with an automated approach.

WHAT'S IN THIS GUIDE

This guide lays out the risks of password exposure, breaks down the key updates to NIST's latest password guidelines, and explains how SpyCloud Active Directory Guardian implements many of the recommendations for you by:

- Automatically blocking weak or banned passwords before they become a problem
- Continuously monitoring for exposed user passwords within your workforce
- Automatically remediating compromised passwords within five minutes of discovery

THE RISKS OF PASSWORD EXPOSURE

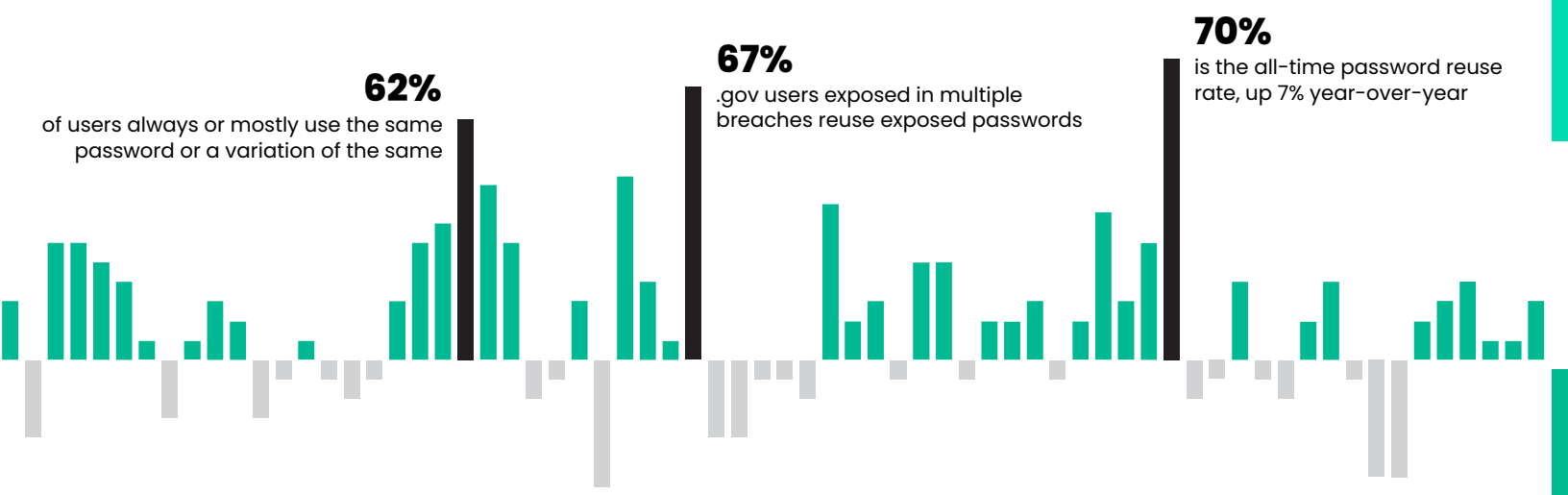
Password exposure is a gateway for cybercriminals to exploit accounts and gain unauthorized access to organizational systems — and the threat is growing. In the last year alone, SpyCloud **recaptured over 3.1 billion passwords from breaches** from the dark web. These exposed passwords often come from:

- **DATA BREACHES |** where attackers infiltrate databases to steal large volumes of credentials
- **MALWARE INFECTIONS |** that silently siphon login data from devices and browsers (both managed and unmanaged)
- **PHISHING ATTACKS |** that trick individuals into handing over authentication information, further fueling the pool of exposed credentials available

▸ *Password Protection Pitfalls*

3.1+ BILLION

passwords were recaptured from the dark web last year...



In a recent study by **LastPass**, only 12% of respondents said they use different passwords for different accounts, and 62% stick to the same password or slight variations. In our analysis, we saw a similar trend, with the **all-time password reuse rate climbing from 61% to 70%** in 2025.

Exposed passwords open the door for attackers to infiltrate not just one account or application but to move laterally across multiple systems. Successful account takeovers give actors a foothold that can escalate into data theft, reputational harm, and financial loss. Business email compromise (BEC), a form of ATO, remains one of the attacks with the largest financial implications, with global losses of **approximately $2.9 billion in 2023**.

To reduce risk, organizations need to improve password hygiene and take proactive steps to minimize identity exposure.

For security and identity teams, the scale can be overwhelming and you can't be expected to manually identify and remediate every exposed password that violates NIST standards. Following NIST's guidelines provides a framework for strengthening password security, but implementation requires automated tools to help businesses get ahead of password risks, and protect your assets and reputation.

SpyCloud Active Directory Guardian helps organizations align with the latest NIST guidelines by preventing employees from selecting bad passwords and detecting and automatically remediating any exposed employee credentials, eliminating manual work and preventing follow-on attacks.

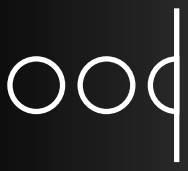
OVERVIEW OF NIST'S UPDATED PASSWORD GUIDELINES

NIST, a federal agency under the Department of Commerce, plays a key role in shaping cybersecurity practices by creating information security standards and guidelines. While its recommendations are mandatory for federal systems, they're also widely adopted as best practices across the private sector.

NIST's latest recommendations, outlined in **Special Publication 800-63B** as part of the Digital Identity Guidelines series, focus on authentication and identity lifecycle management. One of the most notable updates? It ditches the outdated belief that passwords must be long and overly complex. Instead, the guidelines now advocate for passwords that are "easy to remember" but "hard to guess."

This shift underscores NIST's philosophy that usability and security aren't at odds – they work best when aligned. In addition to relaxing password requirements, the guidance includes standards for multifactor authentication (MFA) as well as caveats on the use of biometrics ("something you are") as factors, supporting only their "limited use" in conjunction with something other than a password ("something you know"), namely a specific kind of second factor: "something you have," like a hard or soft token.

THREE COMMON FACTORS FOR AUTHENTICATION



PASSWORD
something you know

TOKEN
something you have

FINGERPRINT
something you are

NIST UPDATED PASSWORD RECOMMENDATIONS

PASSWORD LENGTH & COMPLEXITY

NIST's current password recommendations prioritize:

- **Password length over complexity:** Require passwords to be a minimum of eight characters, with a recommended minimum of 15 characters for stronger security. Passwords up to 64 characters should be allowed to accommodate passphrases and other user-friendly options.
- **No unnecessary constraints:** Allow all special characters but avoid mandating their use, reducing frustration and helping users to create passwords they can remember.

SECURITY ENHANCEMENTS

To further strengthen authentication systems, SP 800-63B introduces these critical measures:

- **Multi-factor authentication (MFA):** Organizations should combine passwords with additional factors such as biometrics or hardware tokens to add a crucial layer of protection.
- **Password screening:** Organizations must screen user passwords against blocklists of commonly used, expected, or compromised passwords to mitigate the risk of credential-based attacks.
- **No mixing of characters requirement:** Along the lines of simplifying user experience, requirements of mixing character sets are forbidden.

PROHIBITED PRACTICES

The guidelines take a firm stance against outdated and ineffective practices that do little to enhance security:

- **Password hints and knowledge-based authentication:** These methods are discouraged due to their susceptibility to social engineering and data breaches.
- **Routine password expiration:** Forcing users to change passwords regularly often leads to predictable changes or unsafe practices like password reuse, undermining security goals.

NIST's updated guidelines reflect an understanding of both human behavior and technological challenges, encouraging organizations to adopt security measures that are effective, practical, and adaptable to today's cyber threats.

SIMPLIFY NIST PASSWORD GUIDELINES WITH SPYCLOUD

Keeping your organization aligned with NIST password guidelines is critical, but let's be honest – it's not always easy. While tools like Microsoft Active Directory offer built-in controls, the real challenge lies in keeping up with the constant flood of exposed passwords. With new breaches surfacing every day – and the growing threat of infostealer malware extracting valuable data like credentials, PII, and more – identity and security teams often find themselves struggling to keep up. That's where SpyCloud steps in.

SpyCloud Active Directory Guardian takes the guesswork out of password security by continuously scanning credentials against the largest repository of originated recaptured darknet data – including **over 30 billion exposed passwords** and counting. If SpyCloud detects exposed passwords, Active Directory Guardian automatically remediates them ***in as little as five minutes*** from time of discovery. SpyCloud Active Directory Guardian offers enhanced enterprise protection with a variety of scanning options to detect exposed credentials tied to your **employees' holistic identities** - their past or present, professional or personal identities - often hidden from typical security methods

By integrating with your Active Directory environment, SpyCloud helps you catch exposed passwords early, shutting attackers out before they can infiltrate your systems and steal corporate data and critical IP.

Here's how SpyCloud Active Directory Guardian enables your team to support NIST guidelines and better password security:

- **NIST Password Policy Enforcement |** Prevent employees from using weak, exposed, or commonly used passwords
- **Continuous Monitoring |** Detect exposures around the clock, looking for exposed passwords in-use by employees
- **Automated Protection |** Automatically reset exposed passwords within five minutes of discovery, or notify and flag employees
- **Recurring Password Audits |** Schedule regular scans to identify and remediate password reuse among employees
- **Executive Reporting |** Provide clear, actionable reports on password security, and the impact of your proactive remediation efforts

By continuously scanning billions of exposed credentials from breaches, malware infections, and successful phishing attacks, SpyCloud Active Directory Guardian detects and remediates any exposed AD credentials to prevent identity-based attacks ***before*** criminals can act.

CASE STUDY

University of Oklahoma Remediates 1,000 Exposed Email Accounts in Less than 24 Hours

The University of Oklahoma (OU) faced challenges common to higher education: students and staff frequently reused passwords across platforms, leaving the university's 80,000 active accounts vulnerable. However, OU didn't have an effective way to monitor these accounts and discover all of the exposures. It was relying on third parties and open source resources such as Pastebin sites and HaveIBeenPwned.

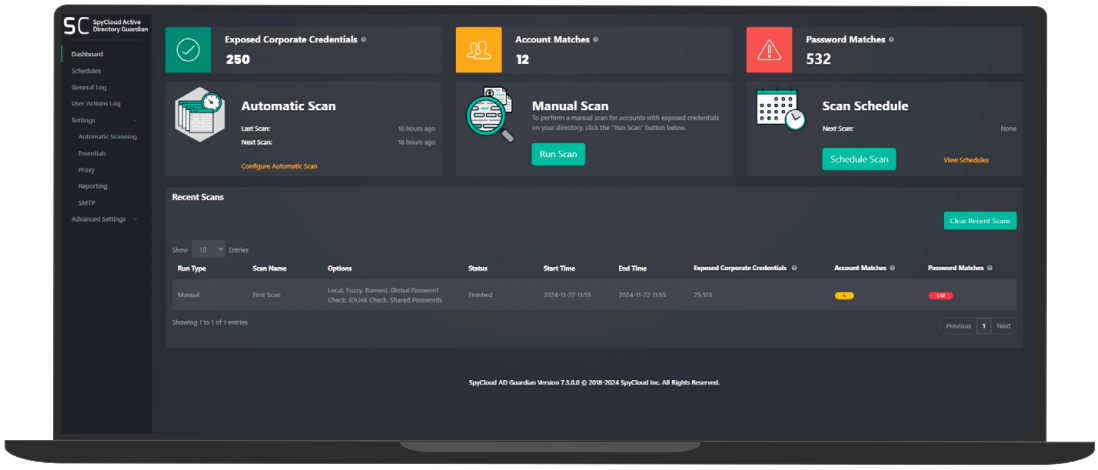
OU decided to integrate **SpyCloud Enterprise Protection, including Active Directory Guardian,** with their preferred SOAR to ingest SpyCloud's recaptured darknet data into their platform – continuously monitoring for and detecting new exposures.

Using SpyCloud Active Directory Guardian, OU was able to take a list of more than 7,000 exposed emails, and discover over 1,000 compromised Active Directory accounts with matching passwords. OU was able to automatically remediate and secure all 1,000 accounts in less than 24 hours.

"Before SpyCloud, if we were alerted to 7,000 exposed passwords to manually check, we would most likely have had to ignore them due to a lack of resources. With SpyCloud, we can get that information in less than 30 minutes, and in a matter of hours, thousands of accounts were secured. "

AARON BAILLIO

Deputy CISO | University of Oklahoma



HOW SPYCLOUD ACTIVE DIRECTORY GUARDIAN WORKS

Active Directory Guardian helps you align with NIST guidelines from the moment your employees create a password – continuously detecting newly compromised passwords that could be in the hands of criminals.

Active Directory Guardian works behind the scenes to automatically flag and reset passwords that NIST classifies as "commonly used, expected, or compromised." That includes everything from passwords found in breaches to those on a pre-populated banned password list.

You can check Active Directory passwords as they are created, customize ongoing password scans to fit your workforce's behavior, and automatically reject weak or exposed passwords.

Whenever a user chooses a new Active Directory password, SpyCloud Active Directory Guardian checks the password for:

- Repeated characters
- Sequential characters
- Banned passwords
- Previously-exposed passwords
- Required length
- Containing a user login
- Matching the minimum threshold

If Active Directory Guardian detects a match, the risky password is blocked and the user is prompted to make a new selection.

By continually detecting and scanning passwords against SpyCloud's extensive database, Active Directory Guardian effectively prevents the use of banned, stolen, or weak passwords, automatically prompting resets for compromised accounts. **A Gartner Peer Insights review hailed Active Directory Guardian for protecting user accounts with "nearly zero effort."**

SpyCloud Active Directory Guardian goes further, automating the remediation of stolen credentials and offering a variety of scanning options to detect exposed identities, including:

- **EXACT-MATCH SCANS |** Automatically scan, around the clock, detecting any recaptured credentials that match an in-use pair
- **HOLISTIC IDENTITY SCANS |** Conduct deeper scans with SpyCloud's proprietary IDLink identity analytics to expose the overlap of your employee's personal and professional identity, scanning for hidden credentials in the hands of criminals, **finding up to 14x more passwords per user**
- **FUZZY VARIATION SCANS |** Dynamically generate and **test 1,000 common variations** of exposed credentials using "fuzzy matching" - similar to how criminals automate stuffing attacks – to detect compromised credentials even if they've been slightly modified. If criminals can guess it, they can use it.

Quickly and automatically scan SpyCloud's database looking for any exact matches with exposed credentials, detecting and resetting exposed passwords within five minutes of discovery. For even stronger protection, you can run daily Active Directory scans with both IDLink analytics and fuzzy matching to catch hidden threats to your organization.

1
Password

Corporate Credential

UP TO
14x
Passwords

Found with IDLink Advanced Analytics

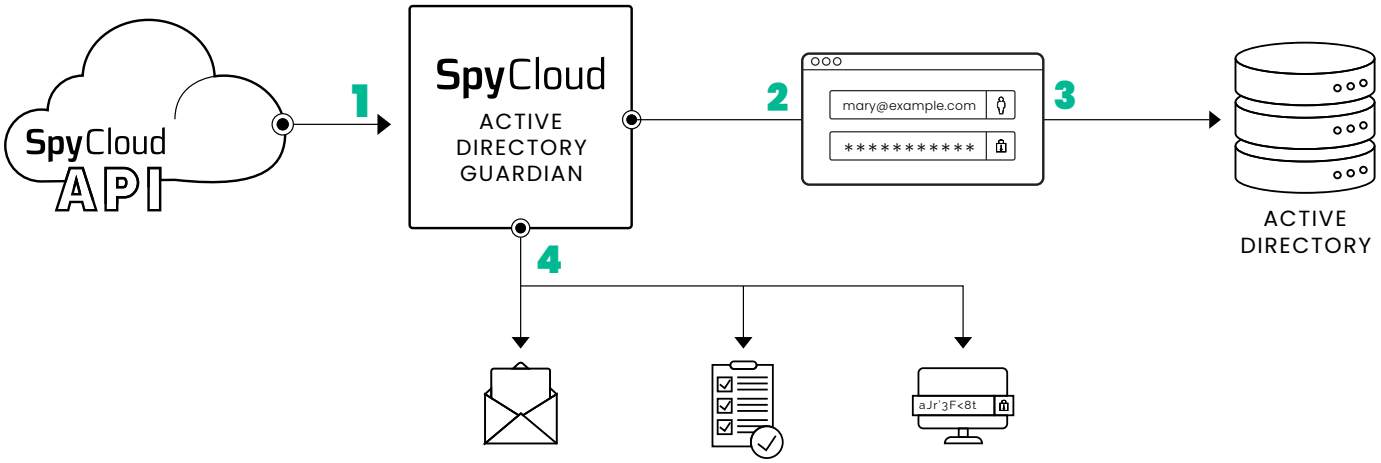
UP TO
14,000
Variations

Found with SpyCloud Fuzzy Matching

Automated Remediation

With SpyCloud's Active Directory Guardian

Here's a brief overview of how it works:



1 Active Directory Guardian continuously detects exposed credentials that match your watchlist domains

▼

2 All **AD** users are checked for matches against exposed credentials in SpyCloud's database

▼

3 Active Directory Guardian can check AD users to ensure passwords have never been exposed

▼

4 Active Directory Guardian notifies you of any matches, or automatically resets the password

▶ ***Organizations like EBSCO have already seen the benefits of Active Directory Guardian. By using SpyCloud, they eliminated over 1,000 hours of manual credential checks and remediation. As their team put it: "It has significantly lowered the amount of time multiple teams had to spend searching the dark web to confirm compromise – let alone remediate it."***

NEXT STEPS FOR ALIGNING WITH NIST GUIDELINES

Adhering to the NIST password guidelines is a must in the face of relentless cyber threats. Weak and compromised passwords are often exploited by criminals to initiate account takeovers, but organizations can protect themselves by implementing strong password policies aligned with NIST's recommendations.

It doesn't have to be a heavy lift. SpyCloud Active Directory Guardian eliminates the scale of the problem – designed to make adherence to the latest guidelines simple and effective while also boosting your overall security.

To bring your password policies up to NIST standards:

CONTINUOUSLY DETECT AND REMEDIATE PASSWORD EXPOSURES

Effective password security takes more than good policies – it requires constant vigilance. With SpyCloud Active Directory Guardian, you can continuously scan for compromised credentials across billions of recaptured identity data points and act immediately. Automatically resetting exposed passwords stops attackers before they can do damage.

ADOPT A HOLISTIC IDENTITY THREAT PROTECTION APPROACH

Instead of relying only on corporate account-level identities, a holistic identity lens incorporates unseen risks tied to your employees' broader digital identity, including past and personal exposures that can make your business a target. Correlate commonly exposed identity data to give identity and security teams the most valuable perspective in defending against identity threats, but also the tools to immediately take action.

PROMOTE USER EDUCATION AND STREAMLINE GOVERNANCE

Even the best tools and policies rely on user behavior. Foster a culture of security by teaching employees about best practices for creating and managing passwords. Encourage the use of passphrases, teach users to recognize phishing attempts, and provide guidance on avoiding password reuse. When users know better, they do better, helping strengthen your defenses.

STAY UPDATED WITH NIST PUBLICATIONS

Keeping pace with NIST's latest recommendations is essential for maintaining a strong security posture in today's evolving threat landscape. Beyond the well-known SP 800-63B guidelines on authentication, NIST offers a suite of complementary resources that provide deeper insights into digital identity and security.

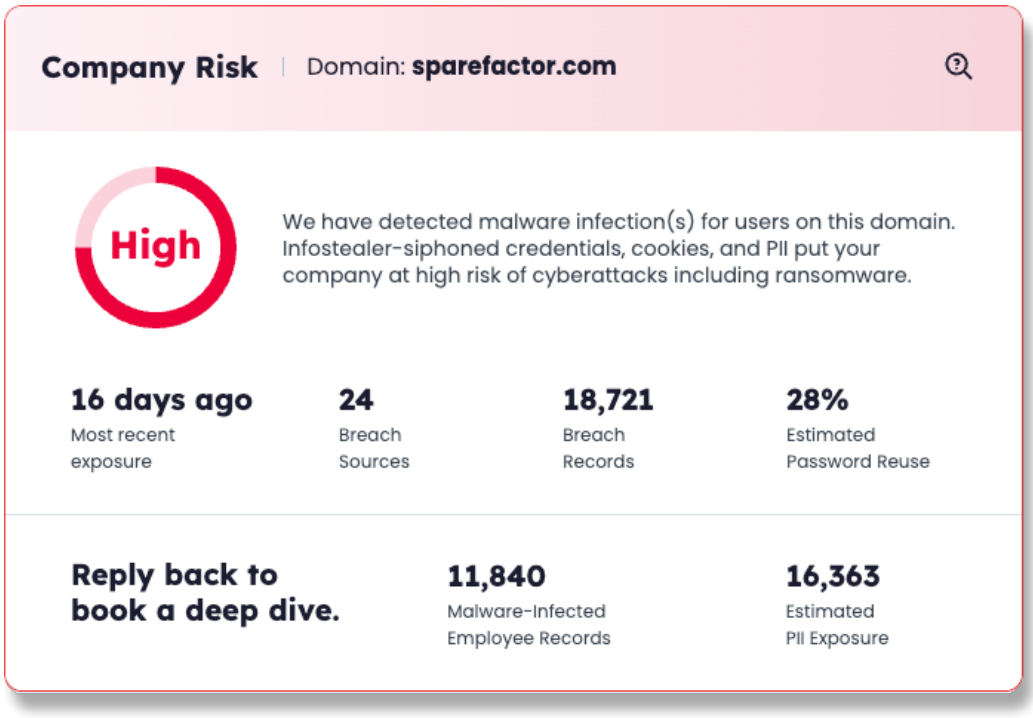
Here are key NIST resources to incorporate into your cybersecurity strategy:

- NIST Digital Identity Guidelines
- SP 800-63A: Digital Identity Guidelines – Enrollment and Identity Proofing
- NIST SP 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management
- SP 800-63C: Digital Identity Guidelines – Federation and Assertion

Regularly revisiting these materials is important for compliance, and gives you a leg up to fortify your defenses. Establish a routine for policy reviews and updates in line with NIST's evolving recommendations to maintain alignment with best practices and stay prepared for emerging threats.

TRY SPYCLOUD'S FREE ENTERPRISE EXPOSURE TOOL

Understanding your organization's dark web exposure is the first step in defending against identity-based threats. **SpyCloud's free Check Your Exposure Tool** provides an immediate view of recent dark web exposures, password reuse rates, and your company's overall darknet risk.



STRENGTHEN YOUR PASSWORD SECURITY AND NIST ALIGNMENT TODAY

By adopting a proactive approach with SpyCloud, your organization can build resilience against evolving threats, safeguard accounts, and maintain a strong security posture.

"When you need a tool that can give you comfort that you're using your time and security resources wisely, SpyCloud is the answer."

ANTHONY BRUNSON

Security Operations Manager | LendingTree

See SpyCloud Active Directory Guardian in Action

Discover how SpyCloud can streamline your adherence to NIST guidelines, protect against account takeover, and strengthen your organization's cybersecurity defenses.

GET A DEMO ▸