SpyCloud

Understanding the Latest NIST Password Guidelines:

Security Meets Usability

THREE COMMON FACTORS FOR AUTHENTICATION

Referenced throughout this paper

1 Password

Something you know

2 Token

Something you have

3 Fingerprint

Something you are

Executive Summary

In June 2017, the National Institute of Standards and Technology (NIST) released its 74-page updated *Special Publication 800-63B* on Digital Identity Guidelines. The non-regulatory federal agency, which operates under the Department of Commerce, is tasked with "developing information security standards and guidelines, including minimum requirements for federal systems." However, the guidance also serves as a set of best practices across private sector industries as well.

The updated guidance abandons the long-held philosophy that passwords must be long and complex. In contrast, the new guidelines recommend that passwords should be "easy to remember" but "hard to guess." According to NIST, usability and security go hand-in-hand.

In addition to relaxing password requirements, the guidance includes standards for multi-factor authentication as well as caveats on the use of biometrics as factors, supporting only their "limited use" in authentication. In fact, NIST views the biometric factor with such skepticism that it prescribes its use as a factor only 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.

In short, the new NIST guidance recommends the following for passwords:

- **A minimum of eight characters and a maximum length of at least 64 characters**
- **The ability to use all special characters (with no special requirement to use them)**
- **A method of prohibiting "commonly-used, expected, or compromised" passwords, including dictionary words and passwords exposed in previous breaches**

NIST advises against the following:

- **Knowledge-based authentication**
- **Hints and reminders for forgotten passwords**
- **Composition rules**
- **Routine password expiration**

Now let's take a deep dive into the updated guidance from NIST.

"If you can picture it in your head, and no one else could, ***that's a good password."***

Passwords: easy to remember, hard to guess

- **Previous breach exposures**
- **Less than 8 characters**
- **Context-specific words**
- **Dictionary words**
- **Repetitive characters**
- **Password hints**

In an interview with NPR, NIST's senior standards and technology adviser Paul Grassi, who oversaw the revision, claimed that the traditional guidance was "producing passwords that are easy to guess for bad guys and hard to guess for legitimate users." The frustration of keeping track of passwords that are just as hard to remember as they are to guess was duly noted by the agency. It even nixed suggested use of special characters, uppercase and lowercase characters, and allowed spaces. In addition, passwords need not be replaced after a set expiration period.

"If you can picture it in your head, and no one else could," said Grassi, "that's a good password."

Needless to say, this is good news for us mere mortals who can't memorize long and complex passwords or stubbornly refuse to use password managers due to multiple vulnerabilities in the most popular services.

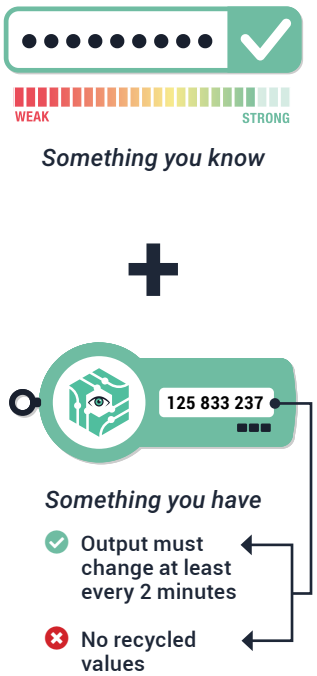
So with guidance around longer passwords of 8-64++ characters, and nixing the ***requirement*** for special characters, it's clear that the philosophy around these changes stems from an appreciation for "usability for security's sake." Certain common passwords may no longer be used, and all Unicode and printing ASCII characters may now be used, including spaces (though, to repeat, they are no longer required). Specifically, the guidance explains that some special characters were forbidden by particular services to prevent upload of payloads written to leverage SQL injection (SQLi) vulnerabilities[1] in the authentication fields of some web forms, so it makes sense to simply remove the requirement altogether for security's sake.

The guidance also prohibits the use of hints for recovery passwords. NIST's position is that they substantially weaken authentication.

---

[1] This is especially true for characters like the single quote (') (used in SQL as a string terminator) or semicolon (;) (used to end a SQL statement), and often used in various conjunctions (admin' or 1=1, for example) to test for SQLi vulnerabilities. If a web form has not been tested for SQLi, web applications could theoretically be vulnerable to itSQLi when authentication credentials are checked against databases that contain usernames, passwords, or even their hashes. But according to Jim Fenton at the NIST Information Technology Lab, this shouldn't be a problem under the new guidance. "Verifier SHALL hash the entry anyway," he wrote in his presentation. "So SQL injection shouldn't be a concern."

NIST RECOMMENDS



Authenticators: it's not all about what you know

The social media and industry chatter around the latest NIST requirements seem to focus on the fact that they are indeed "user friendlier" when it comes to password selection. These changes are enclosed specifically in section 5 under ***Authenticator and Verifier Requirements***, which provides new guidance specific to authenticators. Thanks to the myriad of services that offer or suggest two-factor authentication (2FA), almost everyone has, at some point, used a second factor to authenticate.

This section's updated guidance is not just specific to passwords (which the guidelines refer to as "memorized secrets"). New language is also introduced around authenticators beyond just "something you know" to include "something you have"—stressing the importance of a combination of two single-factor authenticators: as NIST puts it, a "memorized secret" (password) and a "look-up secret" (token). So-called "soft tokens," like third-party authentication apps such as Google Authenticator, and "hard tokens" such as a physical encryption key or fob, are discussed throughout Section 5 of the guidelines.

NIST provides clarity on how specifically multi-factor authentication should be implemented, whether that means using a multi-factor "one time password" (OTP) device, multi-factor cryptographic software, or a multi-factor cryptographic device. New technical guidance specifies even bit length requirements for secret keys and their algorithms (112 bits) for multi-factor OTP authenticators, as well as requirements for passwords used by the authenticators (randomly-chosen numeric secret at least 6 decimal digits in length or of comparable complexity, as described in Section 5.1.1.2).

Time requirements for how often an authenticator's output must be changed in real-time (at least every two minutes) are also included, and the values given must be given only once (not recycled). By comparison, Google Authenticator generates one-time codes between six and eight digits in length whose software tokens change every 30 seconds.

NIST RECOMMENDS

Something you are

+

Something you know

+

Something you have

Biometrics are no secret

With the advent of convenience-oriented services like Touch ID on MacBook Pro, "something you are" is now used as an authentication factor both outside and inside of the workplace. A recent study suggested that 90% of businesses will use biometric authentication by 2020. Given this, biometric authentication was not lost NIST. It differentiates biometric authentication as probabilistic versus other factors, which are described as deterministic. And NIST's interpretation is not limited only to fingerprints, facial recognition, and the iris as characteristics for identification; the document also considers behavioral characteristics such as typing cadence as "something you are."

NIST provides a caveat to its guidance on biometrics, even going so far as to recommend only their "limited" use. Moreover, NIST cautioned that "biometrics do not constitute secrets" and warned that they may be obtained without a victim's knowledge, such as by taking a picture of them or by acquiring that information through other means without their permission or through subversion.

Given these limitations, NIST explains in Section 5.2.3 that biometrics may only be used "as part of multi-factor authentication with a physical authenticator (***something you have***)." In other words, ***biometrics and your password are not enough***. NIST compliance now demands the addition of a third factor besides a biometric, such as a soft or hard token. "When biometric authentication meets the requirements in Section 5.2.3," reads the guidance, "the device has to be authenticated in addition to the biometric — a biometric is recognized as a factor, but not recognized as an authenticator by itself." Therefore, when conducting authentication with a biometric, it is unnecessary to use two authenticators because the associated device serves as "something you have," while the biometric serves as "something you are."

Security guidance for the rest of us

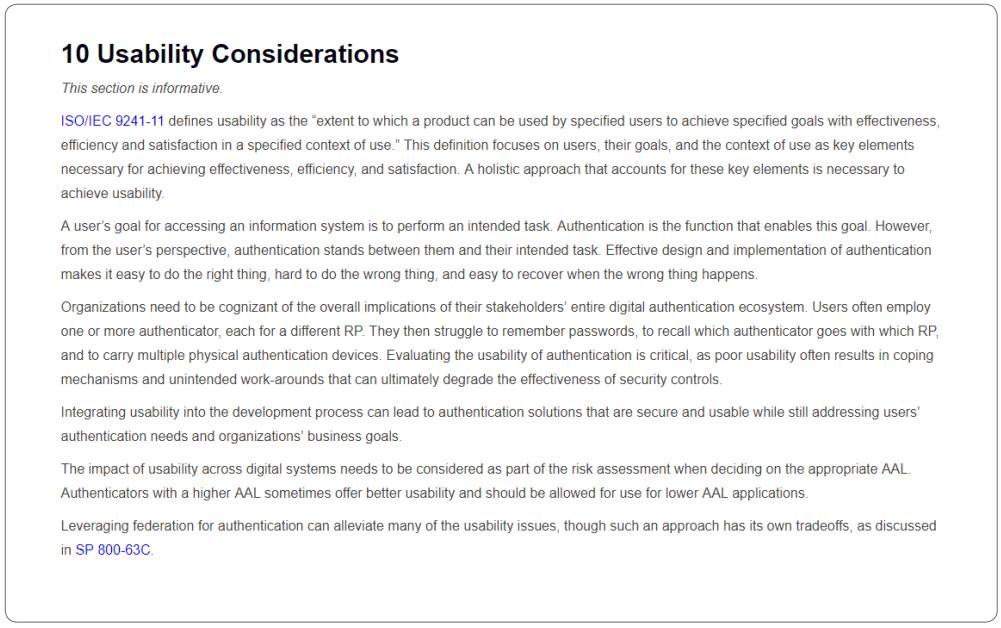
Those of us who are looking to interpret the guidance for our own personal use will likely relate to the recommendations pertaining to OTP apps like Google authenticator ("something you have") along with a password ("something you know") to log into popular apps and services. Many of us aren't even using biometrics to log in yet.

The inclusion of new guidance specific to multi factors (including new limited guidance on biometric factors), provides more context to the importance of how we manage our passwords (what we "know") in conjunction with these other factors.

The common wisdom of choosing passwords that are both easy to remember and hard to guess remains, and the use of multi-factor authentication does not reduce the importance of choosing a good "memorized secret." Rather, the new "relaxed" guidance on password length and complexity simply acknowledges human behavior.

"If it's not user friendly, ***users cheat."***

The addition of the "easy to remember, hard to guess" language is essentially what everyone has taken away from the updated guidelines. Within it, NIST considers the human factor in federal and industry guidance and not only includes language on the risk it adds, but ***recommends*** that organizations consider usability as part of their entire risk assessment, given that people "struggle to remember" passwords and carry around multiple devices.



10 Usability Considerations

This section is informative.

ISO/IEC 9241-11 defines usability as the "extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." This definition focuses on users, their goals, and the context of use as key elements necessary for achieving effectiveness, efficiency, and satisfaction. A holistic approach that accounts for these key elements is necessary to achieve usability.

A user's goal for accessing an information system is to perform an intended task. Authentication is the function that enables this goal. However, from the user's perspective, authentication stands between them and their intended task. Effective design and implementation of authentication makes it easy to do the right thing, hard to do the wrong thing, and easy to recover when the wrong thing happens.

Organizations need to be cognizant of the overall implications of their stakeholders' entire digital authentication ecosystem. Users often employ one or more authenticator, each for a different RP. They then struggle to remember passwords, to recall which authenticator goes with which RP, and to carry multiple physical authentication devices. Evaluating the usability of authentication is critical, as poor usability often results in coping mechanisms and unintended work-arounds that can ultimately degrade the effectiveness of security controls.

Integrating usability into the development process can lead to authentication solutions that are secure and usable while still addressing users' authentication needs and organizations' business goals.

The impact of usability across digital systems needs to be considered as part of the risk assessment when deciding on the appropriate AAL. Authenticators with a higher AAL sometimes offer better usability and should be allowed for use for lower AAL applications.

Leveraging federation for authentication can alleviate many of the usability issues, though such an approach has its own tradeoffs, as discussed in SP 800-63C.

Figure 1: NIST's guidance on usability considerations and their impact on an organization's overall security posture.

NIST consultant Jim Fenton presented a talk called "Toward Better Password Requirements" at BSides. He included "Guiding Principles," which included such sentiments as "strong user experience," "put burdens on the verifier rather than user whenever possible," "don't ask the user to do things that don't significantly improve security," and even "if it's not user friendly, users cheat."

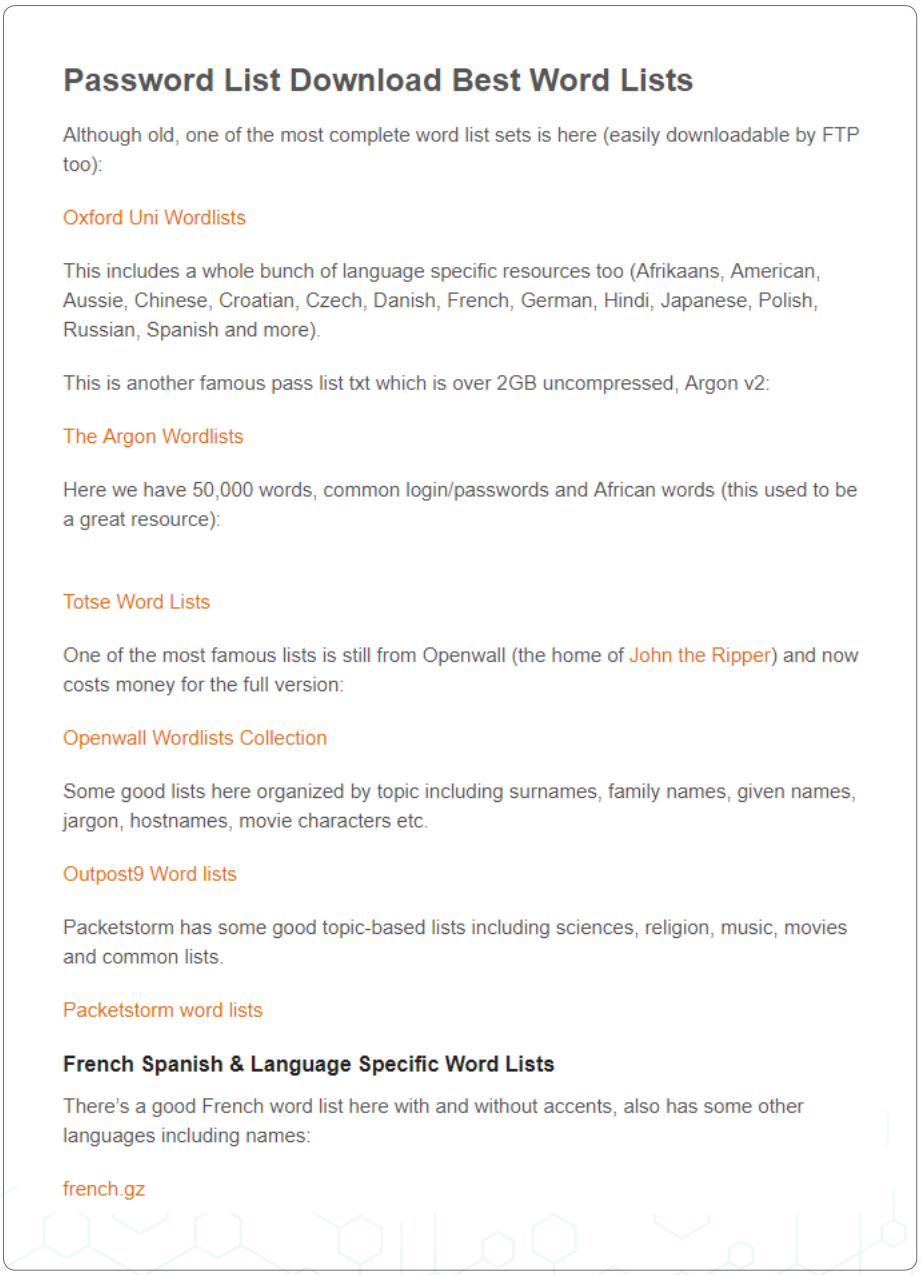
NIST ends its guidance by concluding that length and complexity requirements beyond those they've recommended only "increase the difficulty of memorized secrets" as they "increase user frustration."

But there's a method to the madness. Not unlike Fenton's comment that "users cheat" when restrictions work against them, NIST laments that, as a result, "users often work around these restrictions in a way that is counterproductive." NIST also offers that "other mitigations such as blacklists, secure hashed storage, and rate limiting are more effective at preventing modern brute-force attacks. Therefore, no additional complexity requirements are imposed." In other words, human behavior is predictable. And this makes it easier for criminals to exploit humans.

*NIST calls for organizations to reject passwords that are "**commonly used, expected, or compromised.**"*

Protect your organization

Threat actors are already well aware of what the most commonly-used passwords are. The screenshot below comes from a site that hosts combo lists. These are often sold on underground markets or traded on online "cracking" communities. Threat actors load these lists into automated credential stuffing tools and, with the help of botnets, test the stolen credentials against many sites at once (such as banking sites or streaming content services). These lists are often uploaded into cracking tools such as Sentry MBA or Vertex.
As shown, many of these dictionaries available for download contain oft-used passwords in several languages.



Password List Download Best Word Lists

Although old, one of the most complete word list sets is here (easily downloadable by FTP too):

Oxford Uni Wordlists

This includes a whole bunch of language specific resources too (Afrikaans, American, Aussie, Chinese, Croatian, Czech, Danish, French, German, Hindi, Japanese, Polish, Russian, Spanish and more).

This is another famous pass list txt which is over 2GB uncompressed, Argon v2:

The Argon Wordlists

Here we have 50,000 words, common login/passwords and African words (this used to be a great resource):

Totse Word Lists

One of the most famous lists is still from Openwall (the home of John the Ripper) and now costs money for the full version:

Openwall Wordlists Collection

Some good lists here organized by topic including surnames, family names, given names, jargon, hostnames, movie characters etc.

Outpost9 Word lists

Packetstorm has some good topic-based lists including sciences, religion, music, movies and common lists.

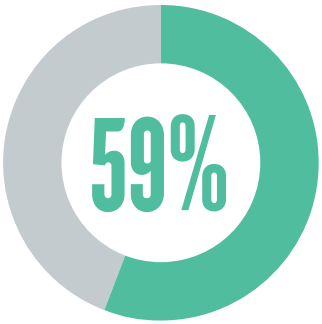
Packetstorm word lists

French Spanish & Language Specific Word Lists

There's a good French word list here with and without accents, also has some other languages including names:

french.gz

Figure 2: Screenshot of dictionaries used by threat actors in their combo lists.



of all internet users ***use the same password*** *across all of their accounts.*

These are the types of situations that the NIST guidelines hope to alleviate. The trick is to choose passwords that ***only you know***, so that they don't end up on lists like these.

But even NIST realizes it cannot control human behavior. With the average internet user managing over 200 accounts, it is difficult to blame the 59% of users who reuse the same password across every one of those accounts. When a password is compromised in a third party breach from one service, perhaps ending up on a combo list, criminals will attempt to reuse that password on multiple services.

Acknowledging that users will engage in this kind of behavior, NIST recommends that organizations mitigate risk by rejecting passwords that are "commonly-used, expected, or compromised," including but not limited to dictionary words, previously-breached passwords, and repeated characters.

Simplify NIST Password Guidelines with SpyCloud

Most NIST guidelines can be enforced using the built-in controls in directory services like Microsoft Active Directory. However, the list of exposed passwords evolves constantly as new breaches emerge. For busy security teams, keeping up with the latest breach data and applying it to user credentials poses a major challenge.

This is exactly where a solution like SpyCloud can help. SpyCloud helps enterprises align with NIST password guidelines by checking user passwords against the largest database of stolen credentials in the world. With over 77 billion recovered breach assets to date, and 1 billion more added every month, enterprises can integrate SpyCloud's breach data into their SIEM, Active Directory, and internal custom applications with fast, high-volume access. SpyCloud enables immediate remediation when it really counts — before criminals have illegitimately accessed corporate systems and data or siphoned off cash & loyalty points from consumer accounts.

With SpyCloud Active Directory Guardian, enterprises can easily operationalize SpyCloud's data to automatically detect and reset Active Directory passwords NIST would classify as "commonly-used, expected, or compromised," including passwords exposed in breaches and a pre-populated "banned password" list. For added assurance, Active Directory Guardian makes it possible to check Active Directory passwords against every password in SpyCloud's database using k-anonymity, independent of username.

Given the NIST guidelines, a solution like SpyCloud is key to an enterprise's efforts to prevent account takeover.

SpyCloud