[redacted]

From: dig-comments@list.nist.gov on behalf of Anand Singh [redacted]
Sent: Monday, September 30, 2024 5:33 AM
To: dig-comments@nist.gov
Subject: [dig-comments] Re: NIST Recommends New Guidelines For Password Security

Hi,

Removing the need for special characters is a good initiative, along with other key changes mentioned above.

However, recovery of the password with some security questions is essential.
Recovery email or mobile can be hijacked ; but chances of having some personal information is rare.
Most answers to security questions are something which is not available in the public domain.

On Mon, Sep 30, 2024 at 4:04 PM The Cyber Security Hub™ via LinkedIn <newsletters-noreply@linkedin.com> wrote:

> **Cyber Security Hub Newsletter**
> The Latest Cyber Security Insights From Industry Leaders
>
> # NIST Recommends New Guidelines For Password Security
>
> **The Cyber Security Hub™**
>
> **Read this article on LinkedIn to join the conversation**
>
> **Read on LinkedIn**

[redacted]

The National Institute of Standards and Technology (NIST), the federal agency responsible for setting technology standards for government bodies, standards organizations, and private companies, has proposed eliminating some of the most confusing and counterproductive password policies. Among the key changes: ending mandatory password resets, restricting the use of certain characters, and discontinuing security questions.

Creating strong, secure passwords and managing them effectively is one of the most difficult aspects of cybersecurity. This task becomes even more complicated with the password rules enforced by employers, federal agencies, and online service providers. While these rules are meant to improve security, they often have the opposite effect. Despite this, such requirements are still widely imposed.

NIST published the second public draft of its updated Digital Identity Guidelines, known as **SP 800-63-4.** This 35,000-word document, dense with technical language and bureaucracy, outlines both the mandatory technical requirements and recommended best practices for authenticating digital identities. Any organization that deals with the federal government online must comply with these standards.

A section focusing on passwords introduces several much-needed, sensible changes to traditional policies. One notable update is the removal of the requirement for users to regularly change their passwords. This policy, which originated decades ago when password security was poorly understood, is outdated. Back then, people often used easily guessed names and dictionary words as passwords.

Currently, services typically require more robust, randomly generated passwords or passphrases. When such strong passwords are in use, forcing users to change them every few months can weaken security. The additional burden leads users to create simpler, easier-to-remember passwords.

Another problematic rule is the requirement to use specific characters, like numbers, special characters, and both uppercase and lowercase letters. When passwords are sufficiently long and random, these character requirements add no real security benefit. In fact, such rules can push users to choose weaker passwords.

NIST's updated guidelines now state:

- Verifiers and credential service providers (CSPs) **must not** impose specific character composition rules (like requiring a mix of character types).
- Verifiers and CSPs **must not** require periodic password changes, except in cases where there is evidence of a security compromise.

(For clarity, "verifiers" are entities that confirm a user's identity by validating their credentials, and CSPs are trusted entities that manage the registration and assignment of authenticators.)

In previous versions of the guidelines, the language suggested that organizations "should not" implement certain practices, indicating that they were discouraged but not prohibited. The new "shall not" language makes it clear that these practices must be eliminated to meet compliance standards.

The updated guidelines also include several other changes:

- Passwords must be at least eight characters long, with a recommendation of a minimum of 15 characters.
- Systems should allow passwords up to 64 characters in length.
- All printable ASCII characters, including spaces, should be allowed in passwords.
- Unicode characters should also be permitted, with each character counted as one unit for password length purposes.
- Password truncation should not be allowed, meaning the full password must be verified.
- Systems must not offer password hints accessible to unauthorized users.

- Knowledge-based authentication (like security questions) should no longer be used.

Reconsidering outdated practices

For years, critics have pointed out the flaws and risks of many widely used password policies, yet banks, online services, and government agencies have largely maintained them. If these new NIST guidelines are finalized, they may not be universally binding, but they could serve as a persuasive argument for abandoning outdated practices.

NIST is accepting public comments on the draft guidelines until 7th October. You can comment here: dig-comments@nist.gov.

Join the conversation