new Pass
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
passw 1234
F9
F10
F11
F12
Del
delete
enter
return

NIST Changes Course and Advises Against Regularly Changing Passwords

THE U.S. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) HAS UPDATED ITS RECOMMENDATIONS FOR USER PASSWORD MANAGEMENT

The U.S. National Institute of Standards and Technology (NIST) has updated its recommendations for user password management, and some of the advice is causing quite a stir across the InfoSec world.

Out with the Old

In the past, NIST, along with many other compliance organizations, urged companies to enforce two longstanding password management policies: one required users to choose highly complex passwords, and the other required users to change those passwords on a regular basis.

In with the New

However, in a somewhat surprising move, NIST has reversed its position on these two password management pillars. Now, it is advising companies to let users choose relatively simple passwords (although not ridiculously simple ones like "password" and "1234567') and to end the practice of requiring users to regularly reset their passwords with something unique.

The Gap Between Theory and Reality

The simplest way to understand NIST's significant advisory changes is to highlight the unfortunate gap that many IT security professionals have been struggling with for decades: the gap between what users are supposed to do in theory, and what many of them do in reality.

In theory, users — regardless of their department, division, team, or job title — are supposed to fully understand the critical importance of password management, even if they don't know (or care) about the technical details behind malware, threat vectors, APT campaigns, and so on. Indeed, most people don't understand how a car works, but we are still able to drive and follow the rules of the road because we all understand the safety concerns of being on the road.

In light of this understanding, users — again, in theory — are supposed to actively and willingly choose highly complex passwords for each account, and periodically change them. Not because they are being prodded and poked by "the IT folks" to do it, but because it is the smart and necessary thing to do.

However, in practice, too many users — certainly not all of them, but enough — fail to realize that if they are not part of the security solution, then they are part of the security problem. As a result of this lack of understanding (or lack of interest), such users often use the same complex passwords for multiple accounts. To make matters worse, when they are obligated to change their passwords, they tend to choose passwords that are simpler and easier to remember — and therefore easier to hack than what they had been using.

Security Fatigue

The root cause of this problem — and the bane of existence for many IT professionals — is a condition dubbed "security fatigue". As we have written about previously, security fatigue sets in when users are overwhelmed and exhausted by the need to remember multiple passwords, practices, and rules related to information security. And instead of leveling up to meet this obligation, they cut corners and push the envelope to see what they can get away with while still avoiding the wrath of IT. Unfortunately, with so many users to manage — each of which may have dozens of unique accounts — expecting IT to enforce 100% compliance is unfair and unrealistic. There is only so much they can do. As mentioned, users must play an active role in being part of the security solution.

Mitigating the Damage

Given this reality, NIST's reversal is essentially about mitigating the risk that users — unintentionally but inevitably — represent. By recommending that users choose complex passwords rather than highly complex passwords, and that they don't regularly change those passwords (since they tend to choose easier passwords), NIST is trying to make companies safer by closing the gap between theory and reality.

Best Practices

To adjust to this new normal on the password management landscape, we recommend adopting the following best practices:

1. Screen New Passwords Against Lists of Commonly Used or Compromised Passwords

In Remote Desktop Manager v14, we introduced the new "Pwned Password Check" feature, which analyzes new passwords against a list of more than 500,000,000 passwords that are known to have been exposed in data breaches. More information about this feature, including simple setup instructions, is available here.

2. Use Passphrases Instead of Passwords

A passphrase is much longer than a typical password — which takes it well out of the brute force attack vulnerability zone — and contains spaces in between words such as this: "The more complex your password is the better!" A passphrase can contain symbols and numbers, and it doesn't have to be a proper sentence or grammatically correct. Jenny, our Marketing Product Specialist, wrote a great article on the benefits of using passphrases and the shortcomings of using passwords. Stay tuned as our article will be published later this week.

3. Implement 2FA

While it's not bulletproof, implementing two-factor authentication (2FA) adds another layer of defense against unauthorized access. For a comparison of popular 2FA tools (now updated to include FreeOTP, Authenticator Plus and SoundLogin), please click here.

Additional Updates

There are several more updates in NIST's Special Publication 800-63, which, in addition to password management, also provides guidance on identify proofing, authentication and federated identity. The publication (which is comprised of multiple documents) is available for download on the NIST website at: https://pages.nist.gov/800-63-3.