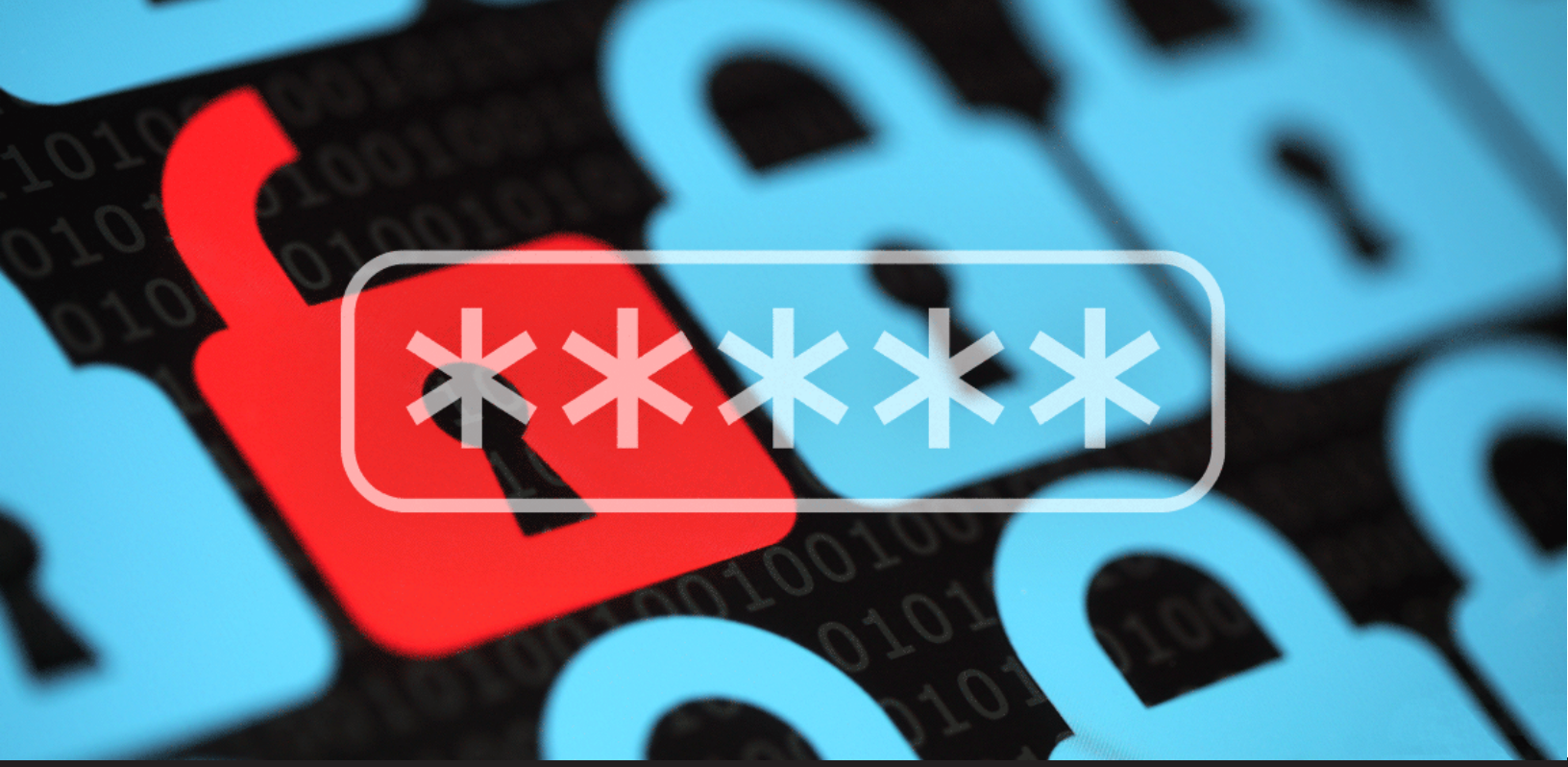

# [UPDATE] 10 Password Management Best Practices

Devolutions

## TECHNOLOGY ISN'T THE ONLY THING THAT NEEDS AN UPDATE EVERY ONCE IN A WHILE

Technology isn't the only thing that needs an update every once in a while. Password management best practices do as well, since the information security landscape — and unfortunately, the tactics and tools used by bad actors — is constantly changing.

The Devolutions Security Team has put together a list of 10 updated password management best practices based on various sources (including the Digital Identity Guidelines and Password Policy guidelines advocated by the NIST). We encourage all Sysadmins to adopt the following measures and policies ASAP:

## 1. Implement 2FA or MFA

Even the most diligent and careful end user can make a costly password-related mistake. For example, in a hurry, they could accidentally put their password in the wrong field. Or they could have no idea their computer has been compromised by a keylogger (short for keystroke logger).

In most cases, 2FA and MFA stop bad actors from accessing accounts, even if they have the correct login credentials. There are many good 2FA and MFA tools out there, including our Devolutions Authenticator, which is available for free, and also features push notifications.

## 2. Implement a Password Manager

With a password manager, users only need to remember two sets of login credentials instead of dozens, allowing them to become virtually passwordless. The first set of credentials is for their own system, and the second is to access the password manager. The password manager can also ensure that users choose very strong passwords or passphrases (see best practice #3) that are at least 16 characters in length.

In addition, if the password manager supports Microsoft's Single-Sign On (SSO), then users only need to create and remember one set of login credentials. Organizations that use SSO can even take things a step further and implement password-less authentication with solutions like Microsoft Hello (which uses biometrics) or Yubikey (which uses hardware). Click here for our updated comparison of popular password managers.

## 3. Use Passphrases

When users are obligated to remember passwords (i.e. when implementing passwordless authentication is not feasible), then length needs to be favored over complexity. This is because many users rely on patterns and tricks to help them remember passwords, such as "Password123!", or they use the practice of "Leetspeak" — the act of changing letters for similar characters such as "p@55w0rd" instead of "password"). These techniques are widely known and actively exploited by malicious actors.

Unfortunately, the vast majority of users cannot remember a 16+ character password without resorting to these patterns and tricks, which is why a passphrase makes sense. As we discussed a little while ago, a passphrase is much longer than a typical password (which makes it less vulnerable to a brute force attack), and it contains letters, symbols, spaces and numbers. For example: "My Purple Dog, Paul, Loves When I Play Frisbee With Him". As you can see, it is wiser to choose a passphrase that doesn't make logical sense and is not associated with the user (i.e. the user in this example does not have a dog, purple or otherwise ??). For even better security, users can mix languages.

## 4. Change Passwords After Evidence of a Compromise

In the past, organizations were advised to have end users regularly change passwords. These days, however, the guidance from NIST is very different: end users are better off NOT regularly changing passwords, because research has shown that they typically choose weaker, easier-to-crack credentials (see SP-800-63B Section 5.1.1.2 paragraph 9). Instead, users should only change passwords when there is evidence of a compromise.

To check for evidence, organizations can use services like the Have I Been Pwned? Domain Search, which finds all email addresses on a particular domain that have been caught up in a known data breaches. It is also possible to receive email notifications if email addresses appear in future breaches. This helps prevent bad actors from bypassing 2FA with social engineering, as the organization will know when to change passwords and on which services.

## 5. Compare Passwords Against a List of Known Weak and Compromised Passwords

Per NIST (see SP-800-63B Section 5.1.1.2 paragraph 5), before a new password is selected it should be compared against a list of known weak or compromised passwords. It's important for this list to include words related to a user's personal or work environment, such as the company name and the username. This is a good protection against a dictionary attack, which will try a list of known passwords. Common dictionary passwords include things like "qwerty1!" and "1122334455667788", and the most known password list would be rockyou.txt.

To streamline and standardize this process, organizations should deploy a password manager or remote connection tool that has built-in password checking functionality. For example, Remote Desktop Manager features "Pwned Password Check", which uses Troy Hunt's Pnwed Passwords Detection System and

automatically checks to see if a potential password has been compromised (i.e. "pwned") by hackers. Also, Azure AD offers a password protection feature. For their personal accounts, end users should be encouraged to use a tool like Have I Been Pwned? to see how many times a potential password has been breached.

## 6. Enforce Just-in-Time Access for Privileged Accounts

Hashes are often stored on a system when users or administrators connect on a machine. This can lead to a pass-the-hash attack, in which bad actors steal hashed credentials and reuse them to trick an authenticated system into creating a new authenticated session on the same network. Importantly, it is not necessary to crack the password — just to capture it, which means that it doesn't matter how long or complex the password/passphrase is.

To reduce this risk, organizations should implement just-in-time access for privileged accounts by using a robust Privileged Account Management solution. One option is Devolutions Password Hub, which features a PAM module that enables administrators to approve or reject access requests. It is also possible to enforce a mandatory password change after a credential has been used and/or at a scheduled time/date.

## 7. Enforce a Password History Policy

Organizations should enforce a password history policy to ensure that end users do not select old passwords. The Center for Internet Security (CIS) recommends setting this value to 24 or more (section 1.1.1). In addition, the policy should also enforce a minimum password age. Otherwise, end users could change their password multiple times within a few minutes in order to re-use the preferred password they started with.

## 8. Eliminate Password Re-Use

Speaking of password re-use: a surprisingly common practice is for users, and even some administrators, to re-use passwords all over the place. While this is convenient, it is also very risky and ill-advised. However, there are also scenarios where password re-use is not intentional. For example, a generic OS image is used to quickly set up systems, and it contains the same default local administrative account (a.k.a. backdoor accounts for administrators). Unfortunately, this means that compromising one machine unlocks all of them.

An excellent and practical solution to this problem is to implement Local Administrator Password Server (LAPS) for Windows domains, or rely on a third-party solution. This allows for different passwords to be used by all computers and servers, and it helps mitigate the risk and severity of large scales attacks.

## 9. Enable Copy/Paste Passwords

In theory, users should not be allowed to copy/paste passwords. But in reality, it is advised — because otherwise, users are likely to choose a password that is both easy to remember and simple to type.

And in case you think we've gone crazy, we aren't the only ones recommending this. Here is what NIST says (SP 800-63b paragraph section 5.1.1.2): "Verifiers SHOULD permit claimants to use 'paste' functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets."

## 10. Enroll End Users in a Cybersecurity Training Platform

While it is not strictly part of a password management process, in the bigger picture it is nevertheless vital for end users — who are and always will be the biggest part of the threat surface — to make sure they are part of the solution, instead of unintentionally part of the problem. To that end, organizations are urged to enroll their end users in a cybersecurity training platform that covers topics such as social engineering, email security, mobile device security, safe web browsing, safe social networking, protection of health information, etc. Managers can also track end user progress to identify knowledge gaps and training needs. To learn more, please read our article here.

## Looking Ahead

Creating a robust password management policy is important, but it's not the full picture. Organizations also need the right tools and technologies, and they must ensure consistency across all end users — especially non-technical business users who may put convenience ahead of security. A password manager, like Devolutions Password Hub, or a PAM solution, like Devolutions Password Server, is now a must for every organization. By using the appropriate tools, we can all work toward a safer future.

We hope that you find this updated information useful, and that it helps keep your organization, end users, data and reputations safe!