Tips for Better Password Management

blog.netwrix.com/2023/01/27/tips-for-better-password-management

Joe Dibley

Even as more advanced forms of authentication, such as biometrics, are developed and implemented, passwords continue to be a commonly used form of authentication. This is partly due to the fact that they are relatively simple to implement and require little infrastructure to support. However, the fact that they are so widely used also means that they are a common target for hackers, which is why it's so important to use strong, unique passwords and manage them properly.

However, it's hard for people to remember many strong passwords, so they often write them down or store them in unsecured locations, which is a huge security risk. Accordingly, it's important to educate all users about best practices for password management.

In short, the problem with passwords is that it's a trade-off between security and convenience. The use of passwords will never be 100% foolproof, but with education and proper tools, you can make it more difficult for hackers to gain access to your sensitive information and systems.

Handpicked related content:

Password Policy Best Practices for Strong Security in AD

What should be considered in a good password management approach?

- **Create and** enforce a policy **requiring the use of strong passwords.** According to latest NIST best practices, password length contributes to far more to password security than complexity, so there is no need to require a combination of uppercase and lowercase letters, numbers, and special characters for passwords; in fact, a short password, even a complex one, will take a hacker less time to crack than a long one with less complexity, and it will harder for the user to remember. It is still recommended to avoid using easily guessable information and to test new passwords against a dictionary of compromised passwords.
- Implementing **two-factor authentication** (2FA) or **multi-factor authentication** (MFA) is a very good idea as it adds an extra layer of security by requiring a second form of identification, such as a fingerprint or a code sent to the user's phone, in addition to a password.
- It's important for users to **avoid using a single password** for multiple accounts and sites. If a hacker gains access to a username and password combination, then they will often try to reuse those digital credentials against different services to further their access.

- **Change your passwords** if you suspect a breach. While it is no longer recommended to force users to change their password frequently, changing passwords that might have been compromised reduces the risk of accounts being taken over by someone who has obtained the current passwords.
- **Educate users**. To protect your data and maintain the integrity of systems and services, it's important for users to be regularly trained on managing their passwords and on how to spot and respond to phishing and other attack techniques.
- Avoid accessing sensitive information or other IT resources on public networks. **Using a virtual private network** (VPN) can also help encrypt your internet connection and protect your data from being intercepted by hackers.
- It's also important to **keep your software and devices updated and patched** to ensure that you have the latest security features and that known vulnerabilities, especially those that are being actively exploited, are promptly mitigated.
- Consider investing in a good **password management solution**. These tools provide an easy way to create, store and manage passwords and other sensitive information, and some can even integrate with browsers and other systems for added convenience. This enables your users to use strong, unique passwords for each of their accounts without having to remember them all.

While following these tips on how to manage passwords cannot guarantee that your accounts will never be hacked, they will significantly reduce the risk of a successful attack.

Handpicked related content:
NIST Password Guidelines

Choosing an effective password management solution

When selecting a password manager, it's important to find a solution that is easy to use and provides good protection. Ultimately, the best password management solution for you will depend on your specific needs and preferences, so it's better to evaluate several and choose the one that best meets your requirements. Here are the key criteria to evaluate:

- **Security.** The most important consideration when assessing a password management solution is security. It should use strong encryption to protect your password data and should have been independently audited for security vulnerabilities. Also research whether (and how often) the vendor has been breached and how it responded.
- **User-friendliness.** The solution should be easy to use, with a clear and intuitive user interface that makes it easy to create, store and manage passwords.
- **Compatibility.** The password manager should work on a variety of devices and operating systems and support all of the browsers you use.
- **Auto-fill during login.** This feature saves time and effort by automatically filling in your credentials on websites and apps.

- **Multifactor authentication.** The password manager should support MFA as an added layer of security to protect your data.
- **Backup and recovery.** The password manager should include a way to back up and restore your password data in case of data loss.
- **Secure sharing options.** The solution should provide secure options for sharing passwords with team (or family) members, if necessary.
- **Reporting and analytics.** This feature can be beneficial in providing insight into how passwords are being used, including who's accessing them and when, and for detecting and alerting you about potential security breaches.
- **Customer support and price.** The price of the solution should be reasonable for the budget you have reserved. In addition, the software vendor should have a reputation for providing good customer support to assist you in case you need help getting started or run into any issues later.
- **Regular updates.** It's important to choose a solution that is frequently updated to include new features and address security vulnerabilities.

Password Security and Management Made Easy with Netwrix

Secure management of user credentials is essential for enterprise security and a fundamental requirement for compliance with many standards and regulations. Netwrix Password Secure is an enterprise password management solution that enables you to eliminate weak passwords, implement password policies for specific teams and pass compliance audits more easily — all while simplifying password management for both business users and IT teams. Users can even securely share passwords, keys, profiles and other secrets with their teammates.

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.