4.6. Security Toolkit: Password Management

What Everyone Needs to Know

Passwords are still the primary lock used to protect access to systems and data. This is why applications always prompt users to create more complex passwords and to change passwords often. You should always change your password when it is recommended and follow the password guidance when you do (e.g., do not reuse passwords across different accounts, do not share your passwords with other people, etc.). The difficulty has now become having too many passwords, all needing to be unique. The more challenging this becomes, the less inclined people are to create complex secure passwords. One way to mitigate this is to use a password manager for both work and personal accounts, which will store your passwords in a secure vault so that you don't need to memorize them.

What IT Needs to Know

Passwords present several challenges to IT staff. Organizations need to manage user access and permissions across multiple systems in their offices and in the cloud. As a result, users are responsible for multiple secure passwords and, potentially, multiple MFA solutions so users tend to make some password mistakes, e.g., they reuse passwords, choose an insecure password, neglect changing their passwords over time, share their passwords with other users. And when users leave the organization, the organization needs to retain access to its data on third-party systems.

There are a few ways that staff can address these challenges in password management. First, consider cybersecurity training for users to help them develop better password habits. You should also have policies on passwords (how often to change them, how to keep them secure, etc.).

Finally, consider a password manager. Password managers securely store multiple passwords, and they also help users create complex passwords that are harder to break. Password managers combined with single sign-on can greatly reduce the number of passwords users have to memorize, which will in turn lead to fewer passwords on post-it notes and fewer reused passwords. You can adopt an enterprise password-management solution and create accounts for all users, or you can add password managers to your user training and best-practice documents for staff. Be aware that some organizations also specifically tell users *not* to put work passwords into their personal password managers. Whichever you choose, be clear with users on what is expected of them.

Solutions to consider:

- keepersecurity: Website
- BeyondTrust: Website
- n-able passportal: Website

Resources:

- "Cybersecurity: What All Nonprofits Need to Know" (The Modern Nonprofit)
- "Creating and Managing Strong Passwords" (CISA)
- "NIST Password Guidelines" (n-able Passportal)

Last updated on December 15, 2023.

Print

Table of Contents

NEWS

News & publications

The news about recent activities for needed peoples.

More News

24 Mar 2023

Project Spotlight: UpToCode

Because everyone has a right to a safe home, Northeast Legal Aid (NLA) is...

Continue Reading

28 Feb 2023

Member Spotlight: Josh Lazar

We are heading south to Florida today to meet community member Josh Lazar, the...

Continue Reading

Our Partners

MAP | MICHIGAN ADVOCACY PROGRAM

LSC | America's Partner for Equal Justice

LEGAL SERVICES CORPORATION