Password Managers

A Higher Education Information Security Council (HEISC) Resource

July 2015

HIGHER EDUCATION INFORMATION SECURITY COUNCIL

EDUCAUSE

What Is a Password Manager Tool?

A password manager tool is software that helps users encrypt, store, and manage passwords. The tool also helps users create secure passwords and automatically log in to websites.

Who Might Use a Password Manager Tool, and Why?

Users should employ unique passwords for each website or system to help minimize the impact from the breach of one website or system; however, most users cannot remember a separate password for many sites and tend to use the same password or write them on a sticky note attached to their computer. Additionally, organizations may have passwords that need to be shared across teams and want a secure method to do so. Password manager tools allow users to more securely manage many distinct passwords and automatically log them in to websites.

The Benefits of Using a Password Manager Tool

Password manager tools enable users to create and securely maintain unique passwords for websites and other systems without having to memorize or write them down.

Risks to Consider When Using a Password Manager Tool

Special care should be taken to secure the password tool, as it will grant access to all passwords. The "master" password that grants access to the tool should be very strong and unique, and multifactor authentication should be used if possible. Additional considerations include whether you want your password management tool to store the passwords locally or in the cloud.

List of Technologies and Tools That a User Might Consider

Below are three popular password manager tools that an end user might consider for use. In addition, some vendors provide enterprise versions, which allow centralized control of all accounts within the organization. Users should evaluate which tool works best for their own unique purposes. Neither EDUCAUSE nor HEISC recommends a particular tool; users employ these tools at their own risk.

LastPass is easy to use, supports most popular browsers and mobile devices, offers multifactor authentication options for the master password and notifications for hacked sites, does not share the encryption key with LastPass, provides a password strength indicator, and performs additional password tests such as ensuring you're not using the same password across multiple sites. However, the ease of use requires that the password database be stored in the cloud. Additionally, as a web-based tool, your password database is available to anyone with an Internet connection and your master password. For this reason, it is strongly recommended that you use multifactor authentication.

KeePass/KeePassX does not share encryption keys with KeePass, but it provides a password strength indicator. The password database is not stored in the cloud. Use across multiple devices is a little more complex, as the user needs to maintain access to the private password database manually.

1Password does not share encryption keys with 1Password, but it provides a password strength indicator. The password database can be stored in Apple's iCloud, through Dropbox, or locally on personal devices. Use across multiple devices is simple if stored in the cloud but more secure if stored locally. The iOS version can be configured to support Touch ID on compatible devices.

Higher Education Reference Pages

- Boston University
- Indiana University
- Pepperdine University
- Purdue University
- University of Illinois at Urbana-Champaign
- InCommon webinar: Security Awareness for User Authentication: Passwords and Beyond (October 9, 2013)

Sustain and Improve Your Information Security Program

The Higher Education Information Security Council (HEISC) supports higher education institutions as they improve information security governance, compliance, data protection, and privacy programs. The HEISC *Information Security Guide*, created *by* practitioners *for* practitioners, features toolkits, case studies, effective practices, and recommendations to help jumpstart campus information security initiatives. Don't reinvent the wheel—get the guide at **educause.edu/security**.