LastPass: Managing Passwords (and more) at Penn

Last Modified on 03/27/2024 1:27 pm EDT

To help you keep track of your passwords, the University of Pennsylvania has partnered with LastPass to make this password management software available to all members of the Penn community.

Before You Start

You'll need the following to use the University's version of LastPass:

- A standard Internet Browser
- An active PennKey account
- Your current login credentials to any site you want to add to LastPass

NOTE: Choose a strong but memorable Master Password! If you forget your password, **account recovery can be very difficult**. If you are unable to go through account recovery, your account will need to be reset (and you may lose all your data)! See LastPass' help site for more details.

Sign up for LastPass

Instructions for signing up for LastPass Premium:

- https://www.isc.upenn.edu/how-to/lastpass.

LastPass Tips

- **Strong Password:** When setting up the account, make sure to choose a strong, unique password that isn't used for anything else.
- **Add Secure Notes:** LastPass is a useful website that can be utilized to keep track of many things, not just passwords. The "Add Secure Note" feature allows you to keep track of information that you need secure and accessible, whether it's a WiFi network login, social security number, or a PIN code.
- **Password Recovery:** Add a recovery phone # by going to **Account Settings -> General -> SMS Account Recovery**. This is recommended in case you need to recover the account.
- **Extra Security:** Add an extra layer of security: Go to **Settings** and choose **Multi-Factor** options to add an extra layer of security.
- **Chrome Tip**: If you use Chrome, we recommend that you **do not use Chrome's autofill** password option for the LastPass website. If anyone has access to the computer, then they'll automatically have access to LastPass, which will then give access to everything on your LastPass account.

- Take a look at our Google Security & Privacy Checkups article for more information regarding Google Chrome's password security and privacy settings.

For more information, consult the Last Pass FAQ.

Student Note: Students will not lose any data stored in their LastPass Premium account when the subscription expires, but Multi-Factor options will no longer be available.

LastPass Security Breach Recommendation

Although the University's Information Security team has determined the risk of hackers accessing secure information is low for most LastPass users, it is critical to stay prepared in case a security breach does occur.

We recommend taking the following steps **as soon as you are made aware of a breach:**

- Change your LastPass **master password** as soon as possible. Make it a complex password, as recommended in the PennKey Password Rules.
- Change any passwords stored in LastPass that have **access to potentially sensitive data**, including:
    - Your PennKey password
    - Your Wharton Account password
    - Banking and other financial account passwords (e.g. Ben Financials)
- Enable Two-factor authentication for LastPass and any other accounts that support it.
- Change credentials that are stored with links to login pages.
- Change or remove additional sensitive information stored in LastPass, such as addresses or other identifying information.

Recommendations

In addition to the Action Items listed above, we recommend that you:

- Change all passwords stored in your vault, starting with your most important ones first.
- If you have sensitive data stored in other fields, change that data if applicable.
- Update the LastPass default iteration setting of 100100. Directions for changing that are here -- 310,000 is now recommended.
- Remove LastPass entries for services you are no longer using.
- Be on the lookout for suspicious spam/phishing messages from attackers pretending to be LastPass

Because your email address and the sites LastPass stores passwords for may have been accessed, there is an increased risk of phishing attacks impersonating LastPass itself or targeting LastPass users. Please remain alert for these types of attacks. If you are unsure of the legitimacy of any email, please reach out to your support team.

Questions?

Faculty & PhD Students: Academic Distributed Representatives

Staff: Administrative Support

Students: Wharton Computing Student Support

For more information regarding LastPass password management, you can also reach the Wharton Information Security Office at security@wharton.upenn.edu.