# LastPass Security Breach

Last Modified on 01/09/2023 3:03 pm EST

LastPass recently released a statement with more details about a compromise earlier this year in which unknown acts obtained customer cloud storage vaults. University InfoSec has determined the risk of hackers gaining access to that encrypted data is low for most LastPass users.

*As we learn more about how this breach affects the Wharton Community we will update this page.*

## Impact

Following the notice on 12/22/22 from LastPass regarding its recent security compromise, the University's Information Security team (InfoSec) has determined the risk of hackers gaining access to that encrypted data is low for most LastPass users. Out of an abundance of caution, we are reaching out to LastPass users with the recommendations listed below. These recommendations reflect current best practice.

## Actions Needed

We recommend taking the following steps **as soon as possible**:

- 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?

If you have questions or comments, please reach out to your Wharton Computing Support Representative.