

LastPass Advice: Updated 2023

Last year, I presented and recommended LastPass. In December 2022, they announced a [breach](#). The data was encrypted, which helps, but there are some vulnerabilities you should know about.

Based on what I consider an inadequate response, and the recommendations of security experts I trust, I no longer recommend LastPass.

What is the nature of vulnerabilities?

- Metadata such as the URLs of websites you visit and your username are unencrypted.
 - The metadata be used in phishing emails you get, so be careful.
- In the breached data, your passwords are encrypted, but...
 - If your master password is weak, it's easier for them get past the encryption.
 - If your password iterations number is low, this increases your risk.

How vulnerable is MY data?

If you were using LastPass before December 2022...

- If you have a good LastPass master password, AND used the recommended [100100 password iterations](#), you don't have much of a current problem.
- If you have a **weak master password**, you are **especially vulnerable**.
- If your **password iterations was set low** at the time of the breach, you are **especially vulnerable**.

To Check password iterations:

- > Open your vault
 - > Go to Account Settings (bottom left)
 - > Show Advanced Settings (at bottom)
 - > Scroll down to Security

Password iterations is likely set at 100,100 and that is OK. Rarely, it is set much lower, like 5,000 or even 1, for a very old, non-updated, account. Current recommendation is 600,000. I use over 1,000,000.

What do to next, if you determine your breached data is especially vulnerable:

- Change all your passwords now, starting with email and banking.
- As always, also enable Multifactor authentication where possible.
 - Even if a hacker obtains your password, they likely won't get past your multi-factor authentication, such as your phone.
- Make yourself safer going forward
 - Change your master password to a new, unique, strong password.
 - Increase your password iterations to 1 million.

If you're thinking of leaving LastPass

- Any password manager is better than not having one at all, including LastPass
- 1 Password and Bitwarden are the replacements I am considering for myself.

Paul Herrick
JPHerrick@gmail.com

