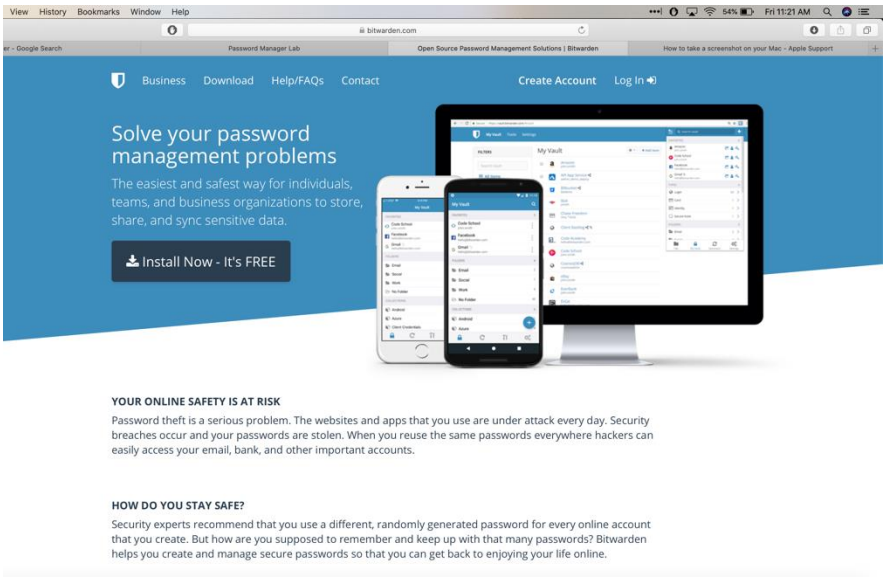
Mohanad Horani

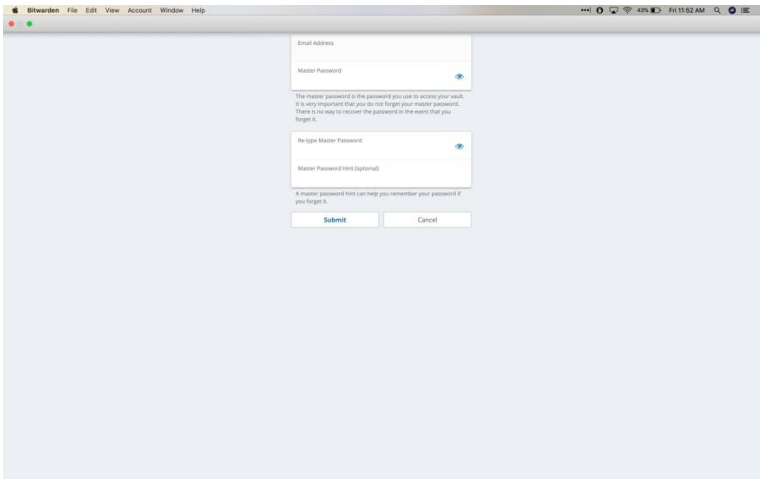
Password Manager Lab

UAT

Identity Protection and Personal Security

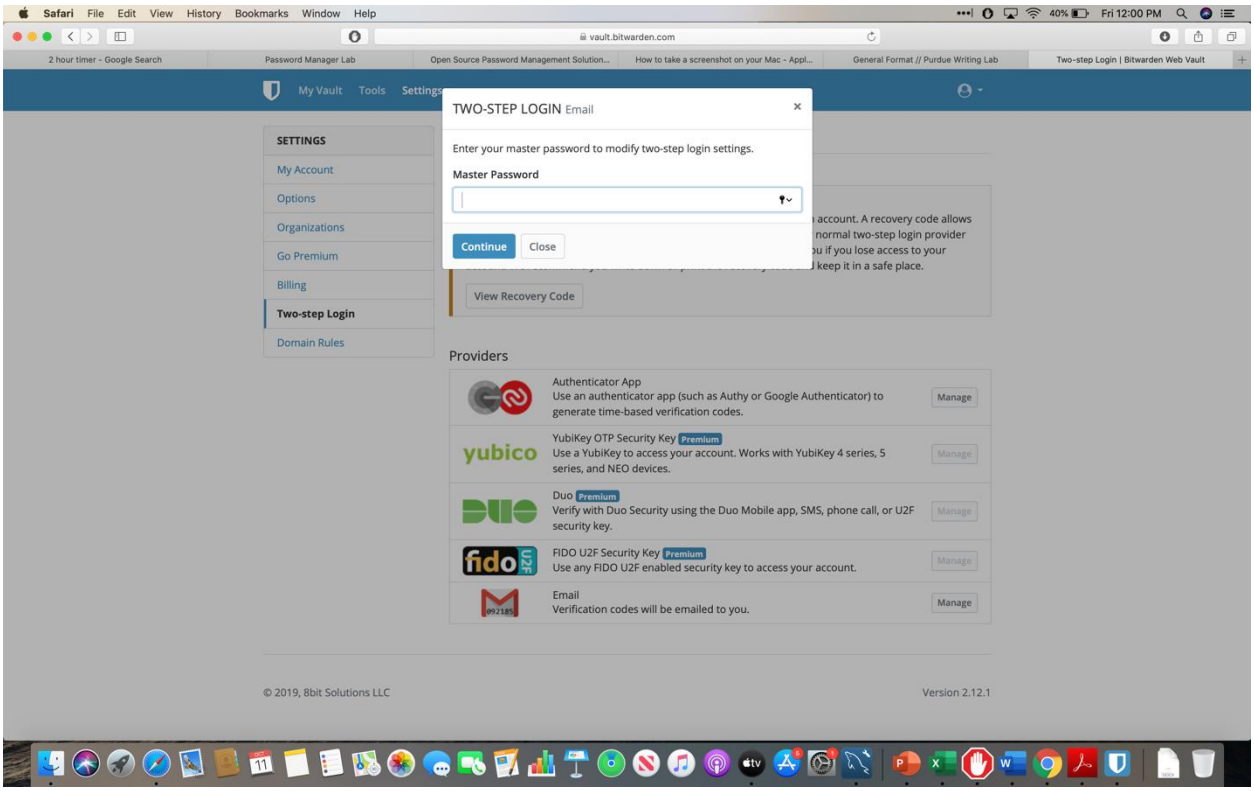


This is the website of my password manager which is called Bitwarden. I chose this particular password manager since it includes end to end AES-256 encryption. Not only that, the password manager that I chose has a secure cloud syncing feature that allows for use on a mobile device or any device that the password manager is compatible with.

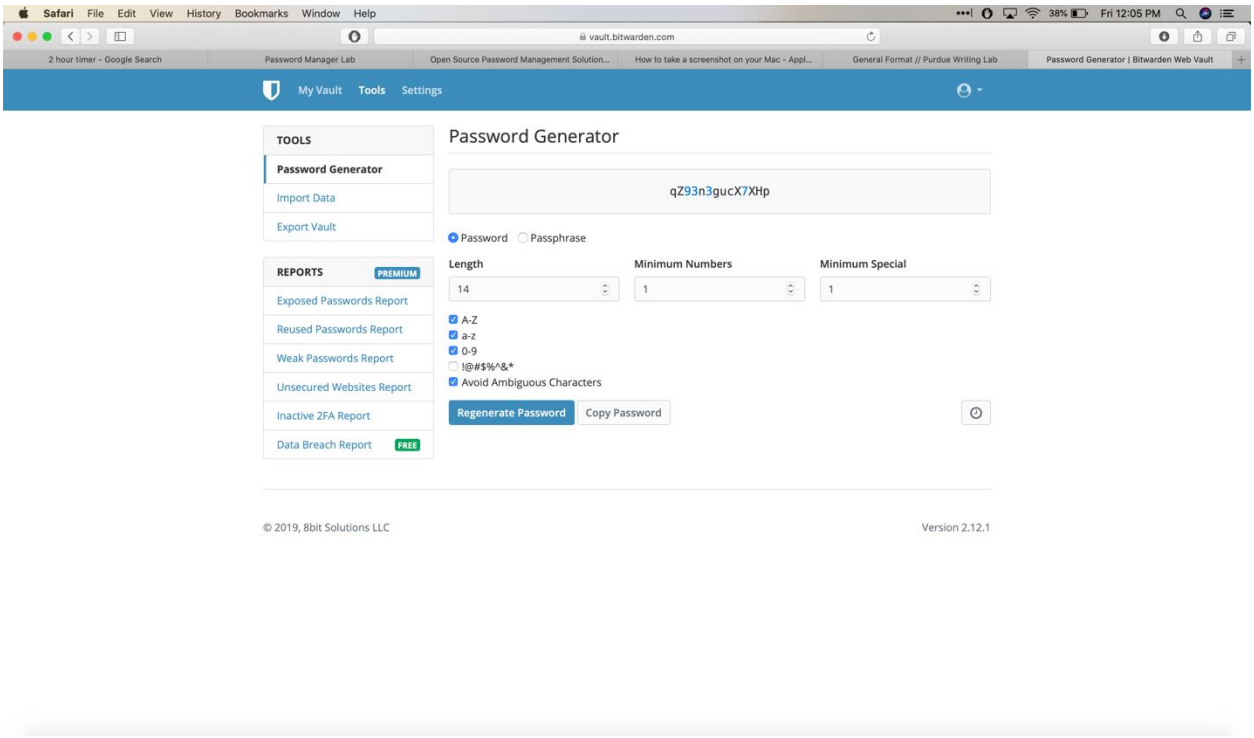


In the screen above, I was setting up an account with a strong and secure master password in order to access any other passwords that are stored in the password manager vault. The reason for that includes security and privacy. There is also an optional password hint option

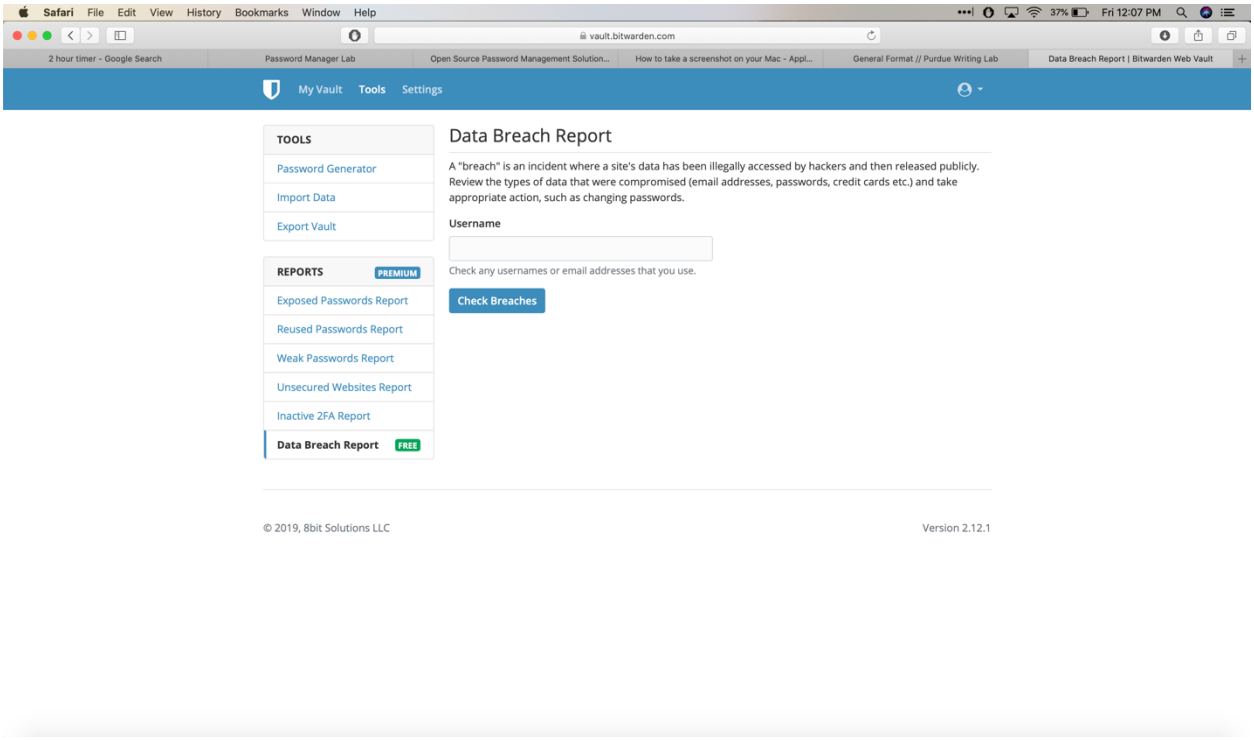
in case the user requires a reminder about their master password required to unlock the vault of passwords stored in the password manager.



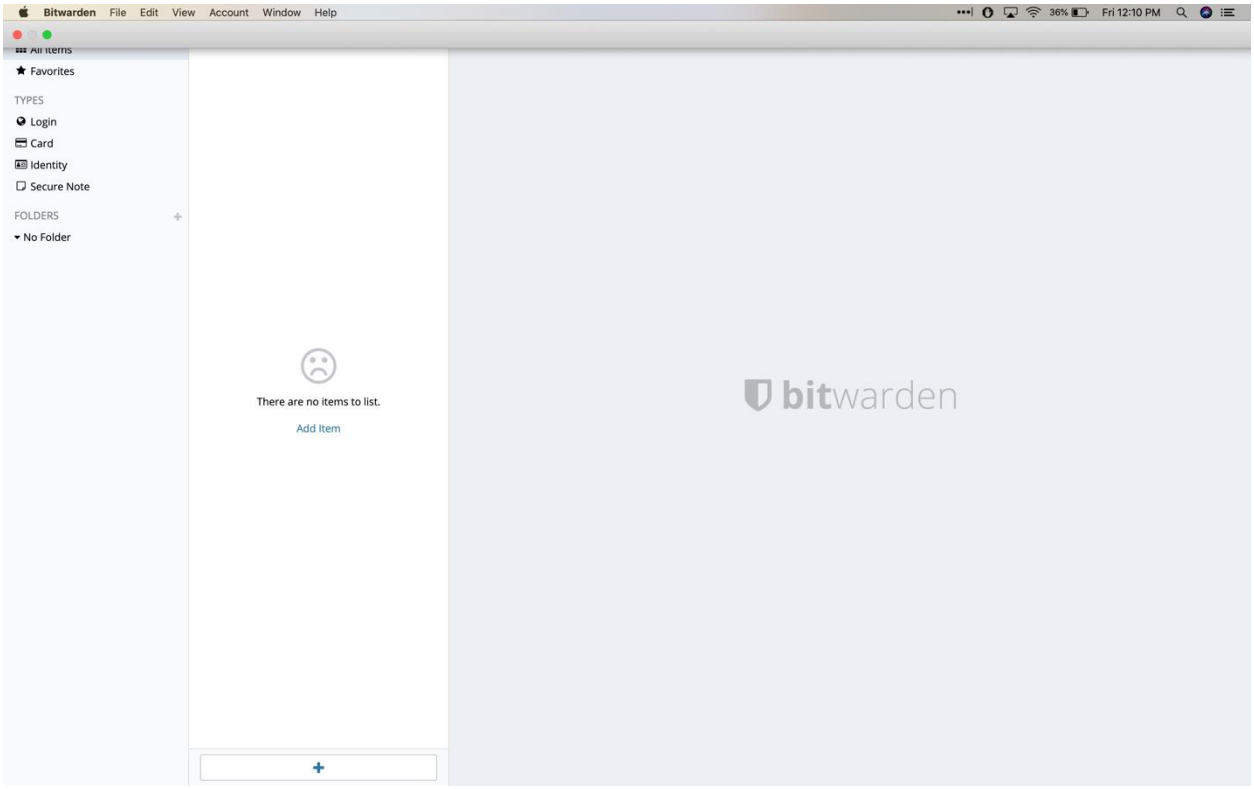
The feature being utilized in the picture above is two factor authentication. The purpose of this is to further prevent other users from accessing the password manager. In other words, there is an option to email verification codes in order to further protect the user's password manager account.



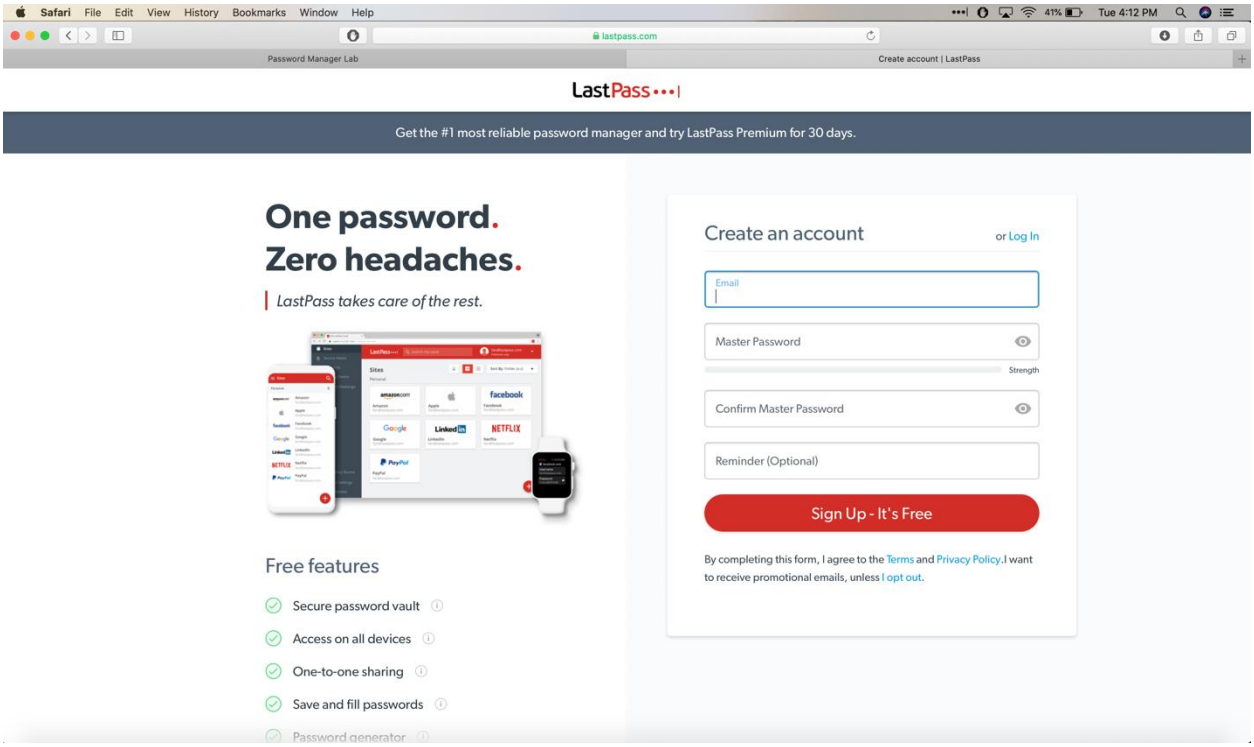
The tool being shown above is called a password generator. The reason behind a password generator is to help users think of passwords to utilize for their master passwords or any password for that matter.



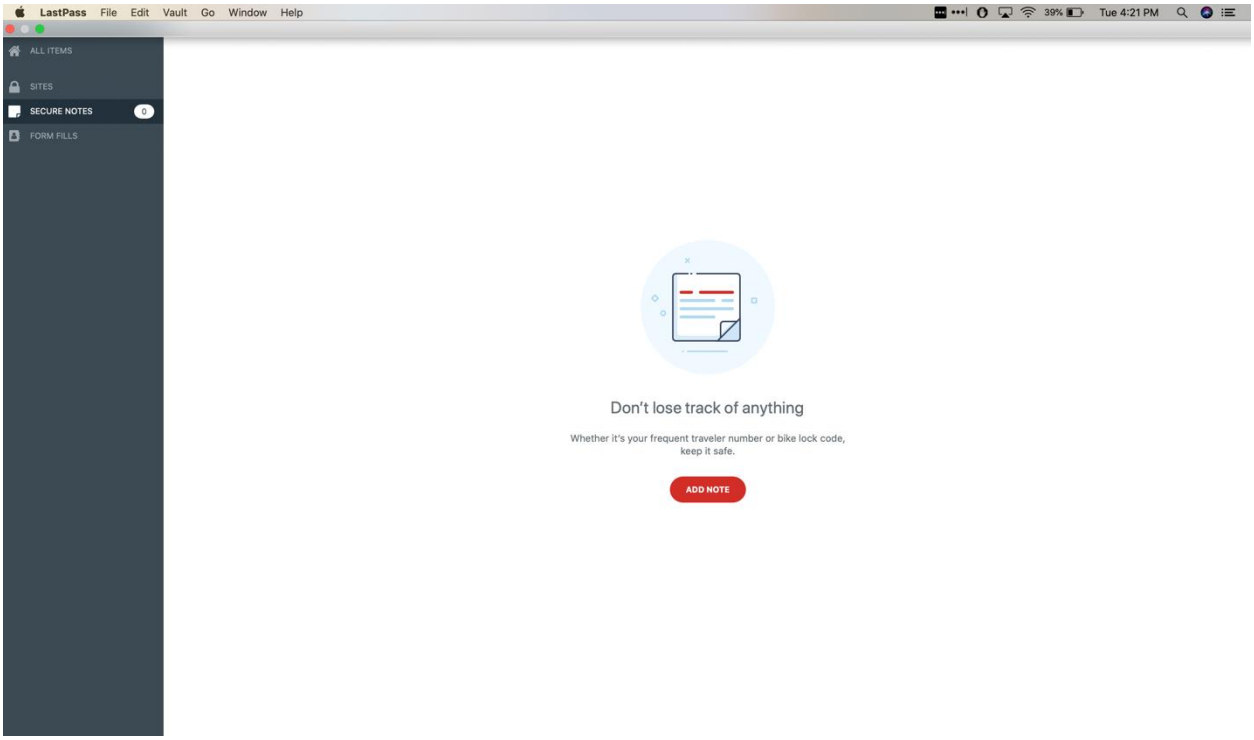
The reason for the picture being utilized above is to find out if the user has experienced any data breaches before by inputting their email address. The feature is called a Data Breach Report which finds lists of data breaches that the user has experienced.



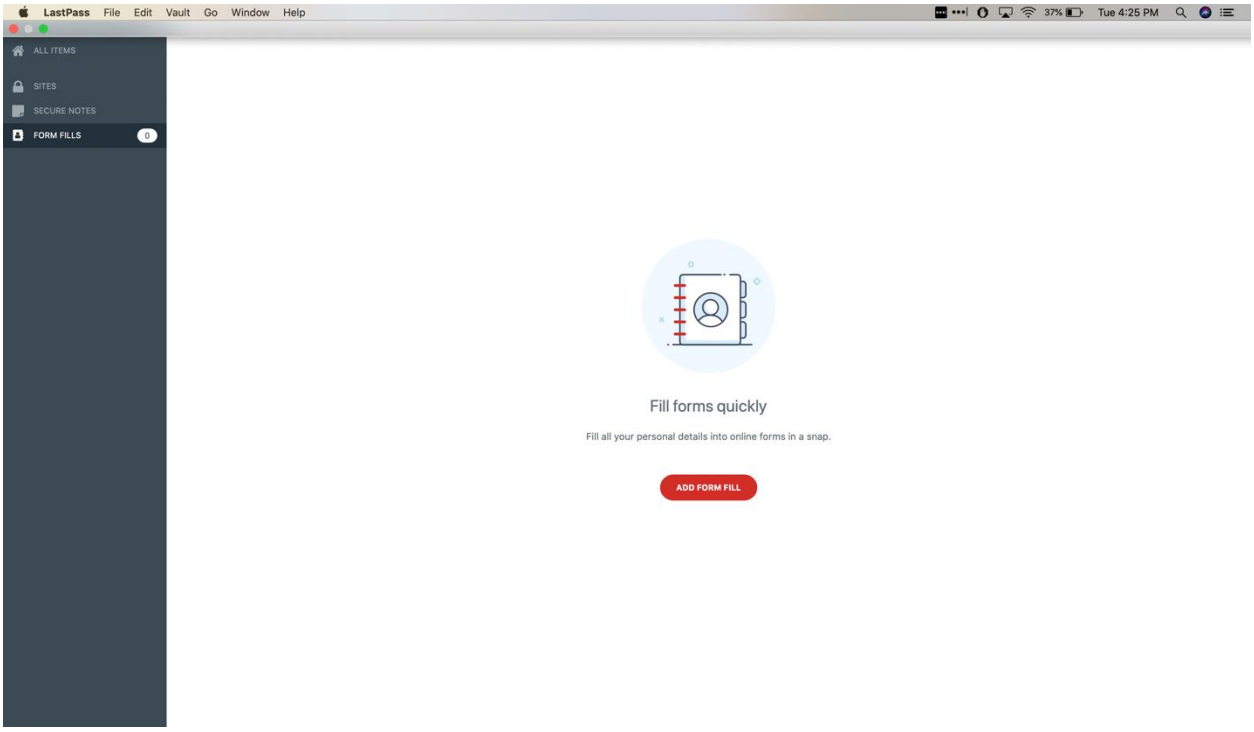
The feature being utilized above includes adding passwords to the vault such as passwords for identity and cards and login passwords. The purpose for that is to not only help the user store passwords all in one place, but also to secure them with a master password in order to make it extremely hard to access them.



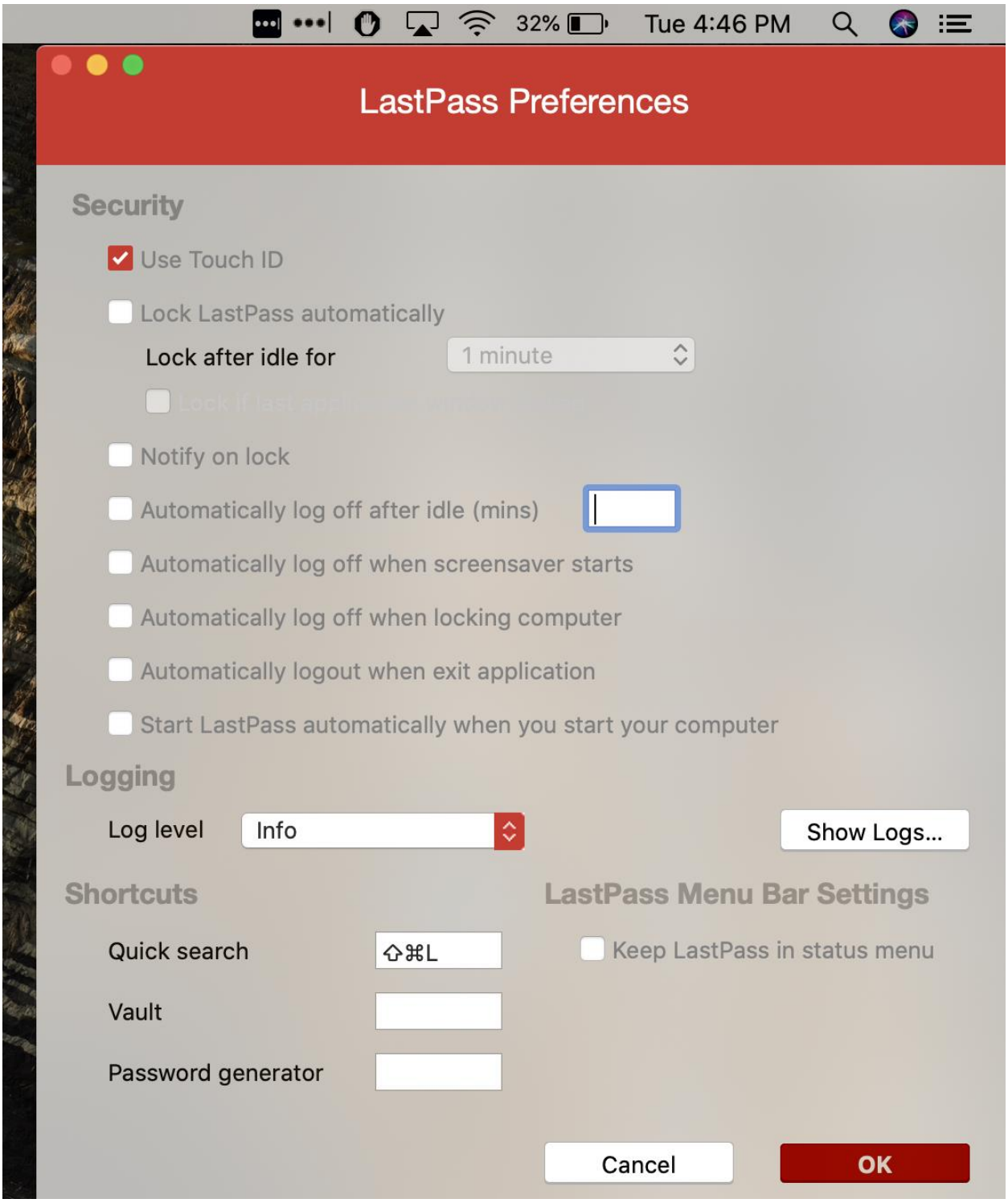
The screenshot above is an image of the screen utilized in order to sign up for and install the password manager called LastPass. LastPass also requires a master password up to 12 characters long unlike other password managers out there. Overall, this is the first step the user must take if installing a password manager such as LastPass.



The purpose of the screenshot above is to demonstrate how LastPass has a notes section in order to keep valuable notes such as a frequent flyer number or maybe even a bike lock code. The purpose of that is to be secure while at the same time remember all of the user's information that may be necessary.



The purpose of this screenshot is to demonstrate how a user can utilize a password manager such as LastPass in order to fill out forms in a much quicker and easier manner. This is sort of like the AutoFill feature for the iPhone, except it is more secure. Personal pieces of information for the user are kept in this section in order to make it easier for the user to fill out forms that they may be required to fill out.



One of my favorite features of LastPass that Bitwarden never had was the Touch ID capability in order to access the app and access all of the key pieces of information with only my

unique fingerprint. Although the hardware must support such a feature, this is essential for those users are in a time constraint and need access to their information but have forgotten it at the moment. Overall, this is sort of like 2 factor authentication (except it is a bit easier).

References:

Simplify your life. (n.d.). Retrieved October 15, 2019, from https://www.lastpass.com/.

Solve your password management problems. (n.d.). Retrieved October 15, 2019, from https://bitwarden.com/.