What do I need to know about using LastPass at MIT?

Q: What do I need to know about using LastPass at MIT?

Answer

Many members of the MIT community are making use of LastPass for storing passwords and other credentials. While IS&T makes no official recommendation on whether or not LastPass is suitable for a specific purpose, we have created this page to address many common questions from the community.

What is LastPass?

LastPass is a password manager, which allows users to store website credentials and other secure data. These credentials can be accessed through the LastPass website, or via a browser plugin. The browser plugin enables features such as automatically logging you in to certain websites, or automatically filling in a form on a web page with credit card data.

Many web browsers also offer the ability to store passwords and other commonly-used data. The key difference between LastPass and the built-in functionality of your web browser is that LastPass stores your data in an encrypted form in the cloud. This makes it easy to access your credentials, even when you're using a different computer.

LastPass is free for basic user, and offers a premium option for a nominal fee, which provides mobile access to your password vault via iOS and Android applications.

Are there other password manager services?

Similar services include Password Genie, Splash ID, Dashlane, and the open-source KeePass. Additionally, as noted above, all the major web browsers (Safari, Firefox, Chrome, and Internet Explorer) offer the ability to store usernames and passwords for websites. Additional third-party extensions may add a cloud synchronization feature to this functionality.

While LastPass is currently the most popular option among MIT community members, another program may better suit your needs.

What are the pros and cons of using a password manager?

At the most basic level, a password manager makes it easy to use Strong Passwords for all online services. With more and more services requiring credentials of some sort, there is a tendency to make the passwords as simple as possible so that they can be easily memorized, or to use the same password for multiple services. A password manager allows you easily use a unique password for every service, and often will also generate secure passwords for you. When using a password manager, you must still remember your "master password", which should be as strong as possible, but it's still only a single password to remember.

Some password managers (such as LastPass), also allow the sharing of credentials between multiple LastPass users. This can be used, for example, to securely store a password for an online resource (e.g. a Twitter account) shared by a department or lab group. There are pros and cons to using this sharing feature, and you should consult the LastPass documentation prior to use.

One consequence of using a password manager is that if you forget your master password (or lose your hardware token, in the case of some password managers), you will lose access to all stored data, and will have to reset the passwords for each of the services that you stored in your password manager. To mitigate this, LastPass (and other password managers) may provide the ability to recover or reset your master password.

Is my data in LastPass secure?

According to the LastPass website, your data is only ever decrypted on your computer, when you enter your master password. (This is one of the reasons LastPass cannot "reset" your master password if you lose it). As of this writing, your data on the LastPass servers is encrypted with AES-256, which is one of the more secure encryption algorithms available. Your encrypted data is also transferred between your computer and LastPass using standard SSL encryption.

The LastPass extensions can be configured to keep your password vault "open" for a period of time, thus minimizing the number of times you have to provide your master password to unlock the vault. The LastPass mobile applications can also keep your vault unlocked, while instead requiring a 4-digit PIN to access your data. You should configure the LastPass browser extensions and/or mobile apps to best suit your security needs.

Once your password vault has been "opened", your data is as vulnerable as any other information stored on your computer. As always, you should ensure that your anti-virus software is up to date, that your operating system is configured to take automatic updates, and that you are

using Strong Passwords to prevent unauthorized access to your computer.

Should I store my Kerberos password or other MIT credentials in LastPass?

IS&T does not prohibit the storage of your Kerberos password in a secure storage location. Provided you select a strong password for your LastPass master password, your Kerberos password or other MIT credentials are no more at risk than any other data stored in LastPass. However, as many community members use their password on a daily basis, it may not be necessary to store it in LastPass.

For credentials issued for other MIT services (e.g. CSAIL, Media Lab, MIT Medical), you should consult with the service maintainer regarding any policies that may exist concerning the use or storage of such credentials.

See Also

- LastPass Landing Page