LastPass Security Breach in June 2015

Q: LastPass Security Breach in June 2015

LastPass Enterprise is a password management system that will be rolled out to the MIT community this summer. LastPass Enterprise encompasses access to data and passwords via Windows, Mac OS X and mobile native clients, as well as via any web browser. It is a convenient solution for the password problem of teams and unlocks features such as shared password folders and secure notes.

You can find articles about LastPass Enterprise via the MIT LastPass FAQ. Note that LastPass Enterprise for MIT includes two-factor authentication using Duo.

On June 15, 2015, LastPass sent out a notice to its customers regarding suspicious activity on its network. The notice is posted here.

Below are answers to questions you may have about the LastPass security breach.

What was compromised due to the breach of the LastPass network?

No encrypted vault data or master passwords were compromised. The data that was stolen was email addresses, which are often used as usernames, and password reminders.

Are there any actions we should take in response to the breach of the LastPass network?

Master passwords are encrypted and LastPass uses “per user salts” which means that an attacker would have to crack each master password individually. However, the data that was stolen may be used to attempt to crack passwords. To be on the safe side, it is a good idea to change your master password. A master password should be a unique password, not used anywhere else and using the password strength test provided by LastPass. LastPass users should also be aware that the stolen email addresses may be used in targeted phishing campaigns.

My LastPass account is Duo-enabled, but what if my username was captured and my password was cracked? Could someone still access my account?

No. Assuming someone had your username and password for an MIT LastPass account and tried to get in from a remote device, they would see the Multi-factor Authentication pop-up window. If they check “This computer is trusted, do not require a second form of authentication” box, they would still need to complete Multi-factor Authentication at least once prior to checking that box. It would be impossible for someone to access your account unless they also had your mobile device or hardware token.

It isn’t recommended to check the “this computer is trusted” box unless your computer is further protected (e.g. full disk encryption, password-protected, physically restricted in a locked office, etc).

If you believe your LastPass account has been compromised, IS&T LastPass administrators can “disable” your account, which would keep your data intact, but prevent anyone from signing in.

Can someone disable multi-factor authentication on my LastPass Enterprise account if they have my username and click on the “If you lost your device, click here to disable multi-factor authentication” link?

No. For Enterprise users, that link does not disable multi-factor authentication but rather sends an email to the administrators letting them know you have requested that multi-factor be disabled. It would not be sent unless an administrator approved the request.

For personal LastPass users, that link sends an email to the address on file with the account, with a link you’d have to click on to approve the request. A malicious person could not disable multi-factor unless they also have access to your email account.