Managing passwords with LastPass 1.50

In this article, I will show you a password management tool LastPass 1.50, which is a tool that provides all the features available to any competitor.

Network administration - Imagine having to remember the passwords for stores on the main streets! What a very difficult thing. This is similar to what happens on the Internet today. However, the difference is that on the Internet you can choose one of the available tools to manage a large number of these passwords. Some tools only manage passwords, some can fill out web forms, some can be used on USB and some can print selected passwords. Among many of these tools, we have chosen LastPass 1.50, which is a tool that provides all the features available to any competitor but has an attractive price - for free!

A big difference between LastPass and the rest is that it stores the password data and populates the information online with your form. RoboForm Pro 6.3 also has the same feature but the software is still in beta. On the positive side, this online storage means that you can access your data from the web browser. However, the negative aspect, it means your sensitive data is stored in someone's server. In this regard LastPass has a unique way to explain why it is safe: when your data is stored and transmitted on the web, it is always protected by AES 256-bit encryption. The data will be decrypted only on your internal system using a master password that only you know. But what if this hosting company doesn't exist? What if a popularity overloads their servers and so

you can't connect to your data? No worries about this issue. If the servers are offline, you will be able to add or edit login data, because an internal copy of LastPass will keep one copy stored separately on encrypted data.

If you forget your master password, LastPass will not be able to recover your data. All you can do when you forget your master password is to delete your account and start with a new account. In case if the bad guys break in and steal LastPass servers, they can't use encrypted data because they don't have a password. We checked the description of how the company protects your data and concluded that this method is no more risky than using an online backup system. Make sure your master password is a strong password that no one can guess.

Let's start

Once you install, LastPass will work immediately. If you don't have an account, LastPass will set up a new account for you. The account creation screen will include a section to define your master password, along with a password strength checker and a link to assist you in creating a strong password. You must also check the box indicating that you understand your login data will be saved online by LastPass.

During the installation process, LastPass will import any password that can be from Internet Explorer and Firefox. The archive of these passwords is obviously not safe: If LastPass can get them, malicious programs can. Therefore, LastPass will save them in its secured 'vaults' and delete unsecured original password protected browsers. Large Software Password Manager 1.0 also imports these insecure passwords, but the latest version of Identity Safe (a feature of Norton 360 version 3.0 and Norton Internet Security 2009) only imports from IE and says no to Firefox.

LastPass will then invite you to enter personal data for one or several profiles. These data include physical address, phone number, email, credit card information, and . You can fill in as many preferences and you can come back to edit this data at any time. Choose a simple pair of options like logging out of LastPass when you close your browser, or set the LastPass Vault to the home page. In Internet Explorer and Firefox, LastPass appears as a button on the menu bar. Just click on this button to log in to LastPass and wake up its other features.

Save Password

Like most modern password managers, LastPass automatically captures usernames and passwords when they log into websites. Like ID Vault 4.0 and Identity Safe, LastPass can also capture passwords entered using other Windows password dialogs. After you log in, LastPass will display a green banner in your browser to suggest saving your login information or setting the site to the exclusion list to never save its password.

If you choose to save the login data, you can edit the name for the saved item, as you can do in Identity Safe and RoboForm. 1-Click SIgnupShield Suite 5 always uses the URL as the item name. You can assign the site a certain category at this time; This category becomes a submenu when you select sites from LastPass's menu. UPEK Eikon To Go Digital Privacy Manager, DigitalPersona Personal 4.0, and the Identity Safe feature of Norton 360 also allow you to assign items but only RoboForm and LastPass can save the log in sub-categories (and become mini menu). However Large Software, ID Vault, and 1-Click do not provide items, which means that their list of logins and menus cannot be strong. This way you can group all of your financial passwords in a submenu, and all the shopping passwords are placed in another submenu for convenient use.

Some websites use login techniques, like nonstandard fields or multipage logins that can create a loop for password managers. 1-Click best manage this issue, it will watch the whole process and record it for *replay* . ID Vault has a complex log database used by financial sites but has problems with new sites. LastPass, on the other

hand, manages this issue by allowing you to save all data fields on each page - in this respect, it is similar to Eikon and DigitalPersona. LastPass's method worked well on sites we tested.

Users tend to stick with a password manager when they have used it because they may have a lot of trouble saving the entire collection of passwords in a new program. LastPass has an impressive ability to import existing password data from 1Password, KeePass, MSI PasswordKeeper, MyPasswordSafe, PassPack, Password Keeper, Password Safe, RoboForm and TurboPasswords. If your existing password manager is not on that list, LastPass can still import your old application data, as long as it can export to a CSV file.

This import capability is unique. Large Software also claims it can import data from RoboForm and KeePass, but when tested, the ability to import from RoboForm is not very good, losing nearly half of them. In contrast, LastPass successfully completed the job, successfully importing the entire list of over 200 existing RoboForm logins.

Capture new registrations

LastPass also notifies you when you register a new account on a secure site. When you work, the application will generate a random strong password and save your brand-new login information. When you return to the site, LastPass will log you in automatically. 1-Click and RoboForm also have similar capabilities to automatically capture new registrations.

You can specify the desired length for random passwords and can also configure it to be able to use specific character sets: uppercase characters, lower case characters, numbers and Period. With Large Software's password generator, there is no guarantee that random passwords will include characters from all selected volumes. RoboForm's password generator is secured by displaying character sets. You can see them by checking all 4 types and creating a 4-character password. 1-Click can also be better controlled, you can allow or require the type of each character.

One of the few features that LastPass lacks is the ability to evaluate the strength of your existing website passwords, while DigitalPersona and Identity safe can assess the strength of each saved password, while DigitalPersona also can display both the overall safety level.

Replay password

When you visit a site where LastPass has a set of certificates, then the application will automatically fill in the username and password, add the LastPass icon and a red border to show you what it has done. All you need to do now is click to submit. For imported logins or situations where the page does not detect correspondence, a yellow banner will appear and ask if you like the certificate. And when you have saved multiple logins, LastPass will fill most of the most recently used logins but still display a banner to allow you to choose other logins.

Why do you have to navigate to the site manually while you can visit that site directly from LastPass? Click the LastPass button in your browser, select Sites from the menu, and pick up the site you want to visit. LastPass will navigate to that site and log in automatically. Or click the LastPass button and open LastPass Vault to get a list of logins, a list sorted by category, but with the option to collapse the categories you don't care about. If you don't see what you want, type in the search box and the list will be narrowed down with the items you type, as in the 1-Click login list. LastPass has a great length to make it easy to visit your secure sites again.
From the storage area, you can launch, edit or delete any saved items. There is also an option to share items by email with 50 friends, though they have to install LastPass to be able to do something with the share.

Fill out the form

Not only does each password have something you have to enter on web forms, but there are also a lot of personal information items you need to type. What credit card would you use to buy a new computer? Where is it released? Like Identity Safe, 1-Click and RoboForm, LastPass can save personal data and automatically fill out web forms for you.

In LastPass, you can create one or more profiles to save personal information. Each profile can hold the address, personal information like birth date, e-mail information about phone numbers, credit cards and bank accounts as well as any number in the user-defined fields. means.

When LastPass detects a web form, the application fills in the data fields corresponding to the saved information by using whatever profile you choose. You can use multiple profiles sequentially - for example, use a profile that contains address and other profile information containing a credit card. And if you mark a subset of profiles, LastPass will automatically fill in those fields.

Mobility

One problem with saving all the passwords in the password manager is that you always don't use the same computer. You may want to log into Facebook on your work computer (during a break). Or you may need to create an online transaction from a certain café. Fortunately for you, LastPass has the ability to move in many ways that you can imagine.

First, because your data is stored online, you can log in to it from any computer connected to the Internet. This way the keyloggers will not be able to steal the password you didn't type while you can use the included virtual keyboard to enter the master password. You can even print a required password before moving. Each of those passwords can open your LastPass Vault once (and only once). If some bad guy knows your password, he will not be able to use this password again.

Like Large Software, LastPass also offers a portable version so you can copy the program to a USB and use it anywhere. The company's website provides a link to download Portable Firefox: Add the LastPass plug-in and you're ready to go. You can export a copy of your encrypted data to USB and work from there. 1-Click and RoboForm also have portable versions, but users need to purchase them separately.

If you think you need to access your login data while off-line, you can download LastPass Pocket. With this utility and an exported copy of the log in USB, you can access all the data (once you have entered your master password and email). Similar applications are available for iPhone and BlackBerry, but increasing access to data requires you to upgrade to LastPass Premium for $ 1 per month. RoboForm also provides an application (view only) similar to Windows Mobile, Palm, Symbian and BlackBerry, all of which are free.

Most password managers work with Internet Explorer and Firefox; however, ID Vault is an exception, supporting Internet Explorer only. Large Software has special support for about 20 browsers, which is an impressive number. However, you can use LastPass on any browser that supports JavaScript and bookmarklet. Help will explain in detail how to use the bookmarklet to enter passwords or web forms in Safari, Chrome, Konquerer and Opera.