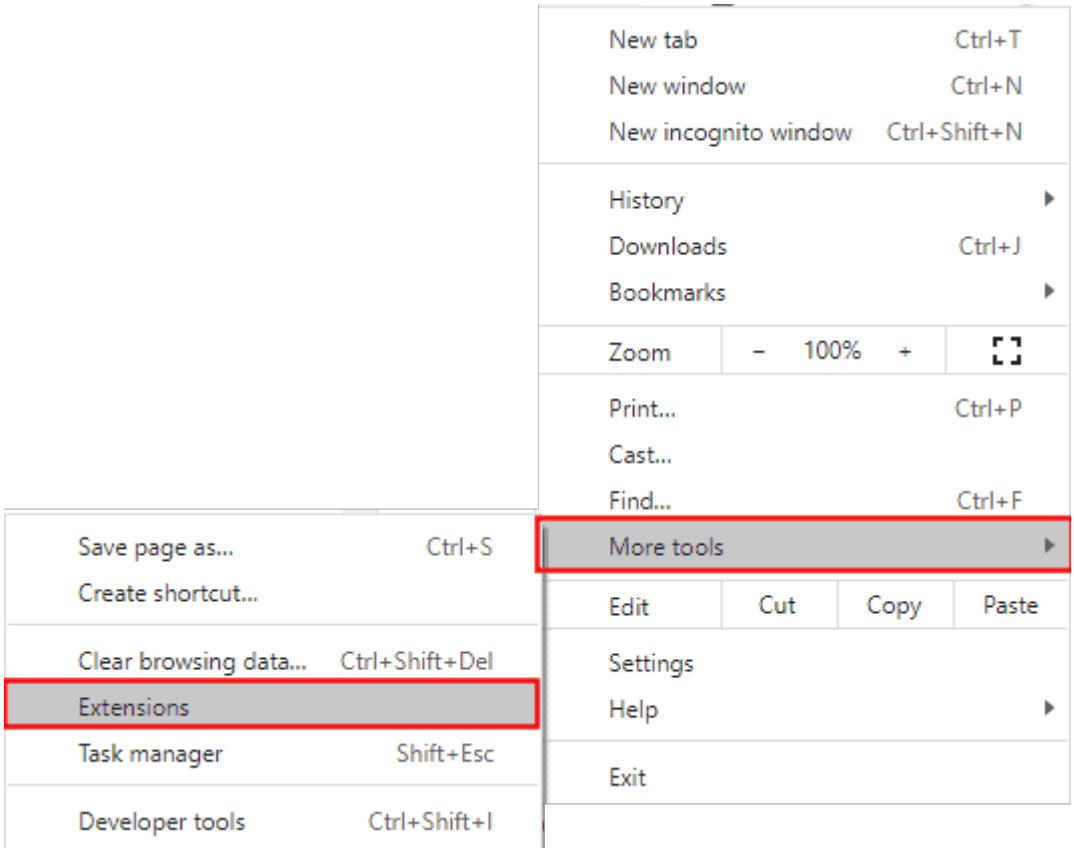
Nowadays, every site seems to require a login with passwords. How do you keep track of all those login credentials without getting lost? If you are a member of the Campus, you might also have an account in the Creation Cassel store, which has a different login. And furthermore, the store blog also has a different login (sorry, they are built on different platforms). It is so easy to get lost! So, here is one great tool you can you to keep everything straight: LastPass.

Get LastPass

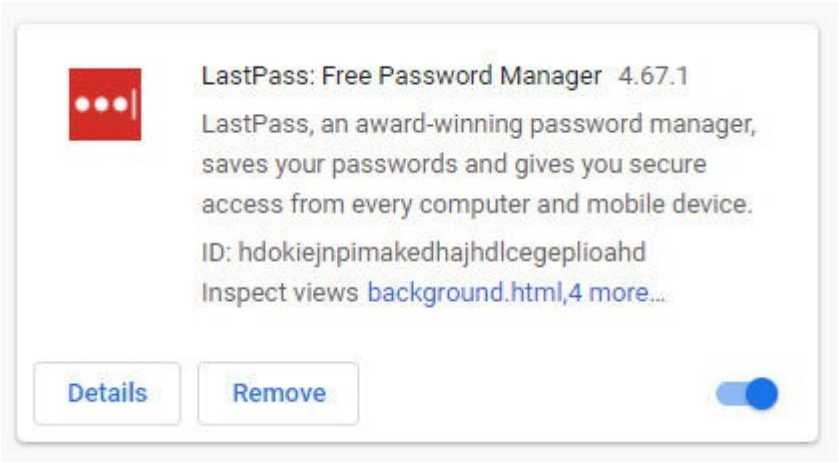
LastPass is available HERE. You can sign up and use it for free, and get all the necessary features you need. Once you sign up, and created an account, you would already be all set! Yes, it is that easy.

Chrome extension

One of the easiest ways to use **LastPass** is to add the extension in Chrome. So, if you are using that browser, click on the three dots, go to More tools and select Extensions.



Once you are in, type in LastPass and you should see this window (in my case, I have the option to Remove because I have already installed it):



If you are using Firefox, you can also add LastPass as an add-on to that browser.

Master Password

When using LastPass, since it is an online tool, you certainly want to keep it safe. LastPass will ask you for a MASTER password. That is the password you will need to access it, to log in, etc. It has to be a strong password and not one you use elsewhere. But not only it has to be strong, you have to be able to remember it easily. Here is a trick I found very useful to create a strong password while making it easy to remember.

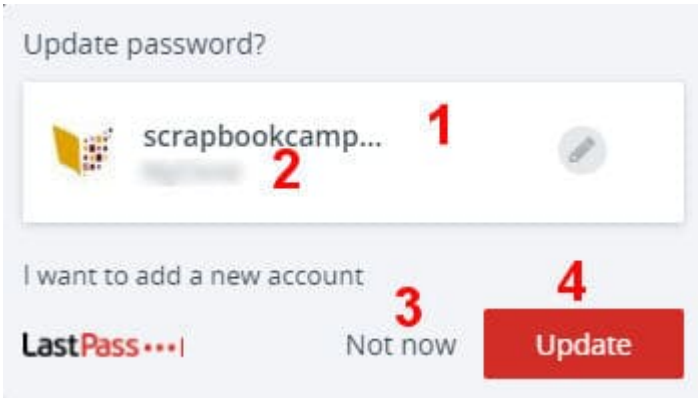
- Start with a phrase, a song or a poem that is very familiar to you. Let't think of "*Mary had a little lamb*" (of course, you should take something else!
- Consider the first letter of every word: *M*ary *H*ad *A* *L*ittle *L*amb, *L*ittle *L*amb, *L*ittle *L*amb. *M*ary *H*ad *A* *L*ittle *L*amb. *I*t's *F*leece *W*as *W*hite *A*s *S*now
- string those letters, in lowercase: *mhallllllmhallifwwas* . That is already something quite hard to guess. Even if someone glanced at it, they would not guess it.
- Now, let's add some uppercase. In this example, it is very simple to replace the "m" by "M", as it makes sense. If you don't have any name, you can just capitalize the very first letter, which is also common in writing a phrase. So our password now looks like *MhallllllMhallIfwwas*
- Can we add a digit? How about the fact that Mary has only ONE lamb? We can replace the article "a" by the digit "1". So we now have *Mh1llllllMh1llIfwwas*
- But we can do better, can't we? Let's add some non-alphanumerical characters. Let's add some punctuation! (that would be great to separate those "l".

Mh1ll,ll,ll.Mh1ll,Ifwwas (of course, you can choose a different symbol instead of commas)

Now, you can use THAT strong password as a Master Password for your LastPass.

Using LastPass

When you go to a site, and create a login or even enter your password on an existing login, you will automatically get a popup from LastPass asking you whether you want to save it or not.

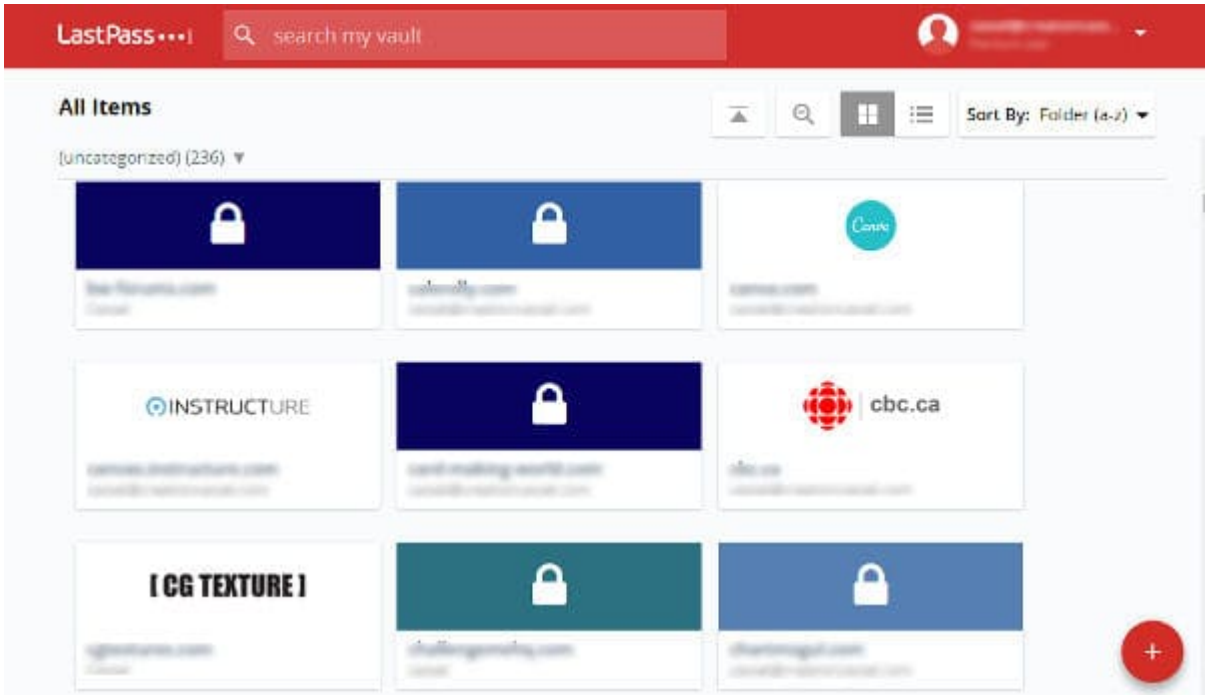


1. This will indicate the site you are on.
2. This is your username
3. If you don't want to save that password at this time, or if you entered something that is NOT a password (like a phone number, or an address), you can click Not now.
4. This will show Save or Update, depending on whether you have already saved this login information previously.

At his point, you will start to build your own password library. After visiting all the sites that you usually visit, and enter your credentials, LastPass will remember them, and the next time you want to log in one of them, it can fill in the information for you.

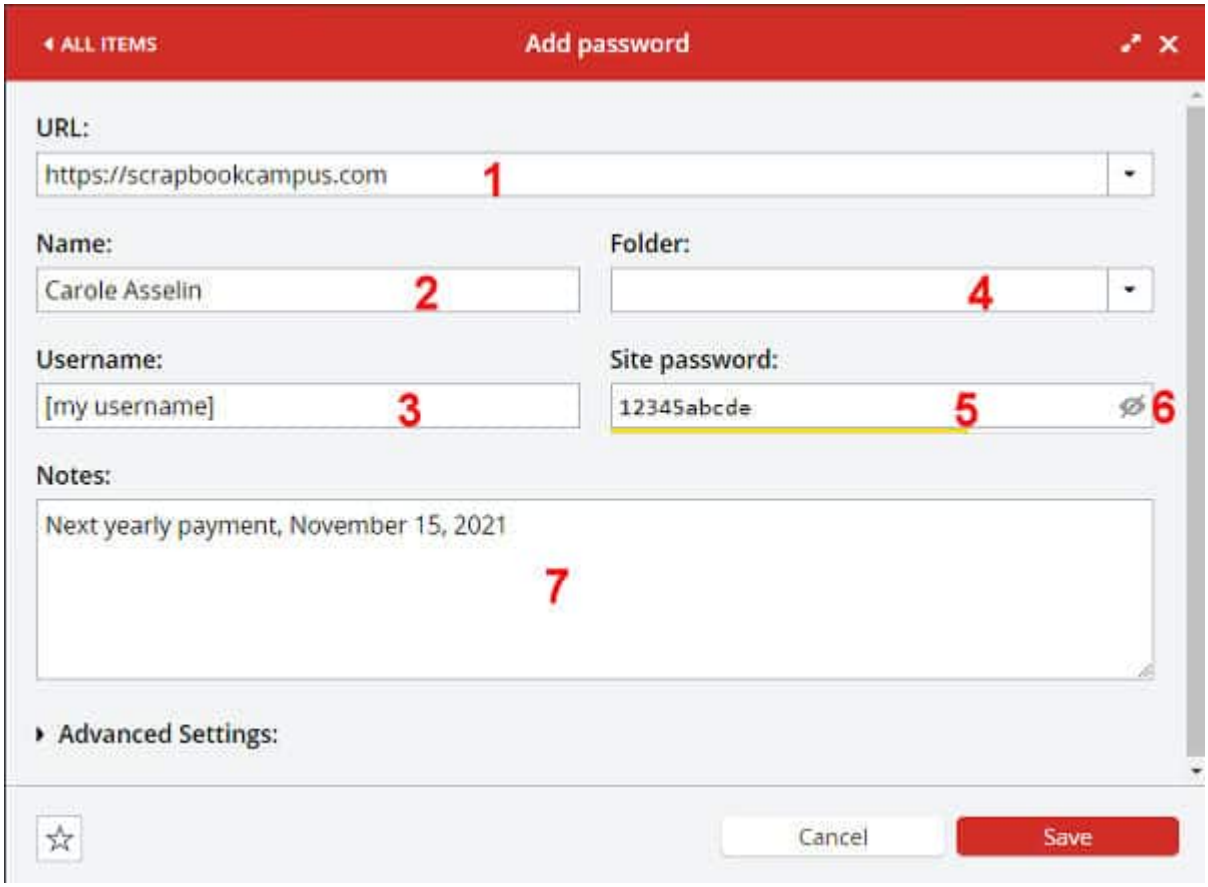
Inside LastPass

Although you might mostly use LastPass in the "front end" and let it fill in your credentials, you can also go inside and organize your passwords. Each site you have saved will have its own entry in the backend.



Even on the free plan, you have unlimited passwords you can save.

If you click on one of those entries, you will get a window like this:



Each entry inside of **LastPass** will include these fields:

1. the **URL** for the site where you are logging in
2. your **name**; this field is not automatically filled. It might or might not be necessary in most sites, so it might be empty.
3. the **username** that you are using for that particular site; this is entered automatically when you accept to save the password
4. the **Folder** is where you might have categorized this particular entry. It is not entered automatically.
5. the **password** is saved here.
6. you can choose to **view** the password (in case you need it somewhere else) or keep it hidden
7. in this box, you can add any information you might want to be associated with this site or password, or even your account. It could be the date of your last password change, for example.

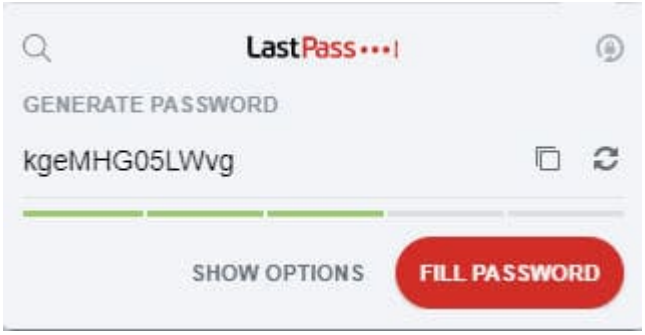
Adding safe notes

Although **LastPass** is thought of a great tool to keep your passwords, you can also use it to save other information, like some key details for online activity. You could save FTP information if you have a site to access or maybe your insurance or medicare number. Since LastPass can be accessed on your phone, you might find that useful.

Let LastPass choose your password

Although you are responsible to set a strong Master password, are you tempted to use a "regular" password on every site? This is a definite security issue. When you go to create an account on a new site, you can let LastPass choose a strong password for you. And since it remembers it, you don't have to!

When you are to choose a password for an account you are creating, you will see a little icon on the right, and when clicking on it, you will get this type of popup:



It will generate a password for you and you can accept it or click the double arrow circle to pick a different one. It is always random. Using a password generated by LastPass will allow you to ALWAYS have strong passwords, and ALWAYS different from one another, which is a safer process.

Now, if you use LastPass, you should no longer have to worry about having the correct credentials to log into the Campus, the store or the store blog!