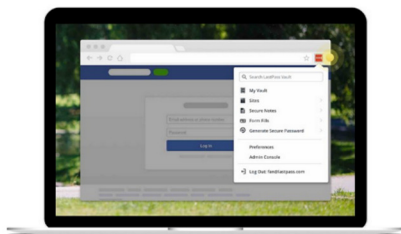


The image shows the top half of the LastPass website. At the very top is a dark navigation bar with links: 'How It Works', 'Go Premium', 'Families', 'For Business', 'Pricing', 'Get LastPass Free', and 'Log In'. Below this is a dark banner with the text 'NEW! LastPass Enterprise has some exciting new features! See the Details >'. The main content area has a white background. It features the headline 'Simplify your life.' in a large, red, sans-serif font. Below the headline is the text 'LastPass remembers all your passwords, so you don't have to.' in a smaller, dark grey font. Underneath this is a red button with the text 'Get LastPass Free'. Below the button is a link that says 'Upgrade to Premium for just \$2/Month >'. At the bottom of this section are three overlapping screenshots of mobile app interfaces for Facebook, Amazon, and Yahoo! The Facebook app shows a login screen with a 'Log in as' dropdown. The Amazon app shows a shipping address and a 'Fill form with' dropdown. The Yahoo! app shows a 'New Password' screen with a strength indicator.

### 1. Get the LastPass browser extension.

Install the extension in your browser for saving & accessing your passwords.

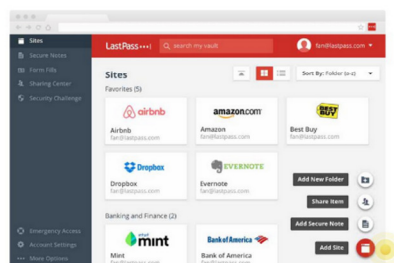


LastPass  
 Set your vault's Master Password  
 Master Password  
 Make it a good one  
 Confirm Master Password  
 Repeat your master password  
 Remember Me  
 Click here to learn why. Design  
 Unlock my vault

Our minimum requirements  
 At least 8 characters long  
 Not your email  
 Not easily guessable  
 Our advice  
 Use a strong unique key to you  
 #Hackingpasswords  
 What makes a password strong?

Check out our blog for tips on [How to Make a Strong Master Password](#).

Where you can add, view and manage items that you've saved to LastPass.

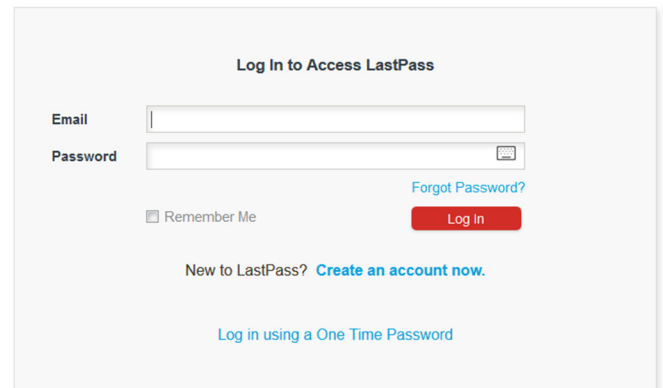


Forgetting passwords is a thing of the past. Start by filling your vault. We have many ways for you to add sites: let LastPass save sites as you login, import sites from your email, import/upload from another password manager, and more.

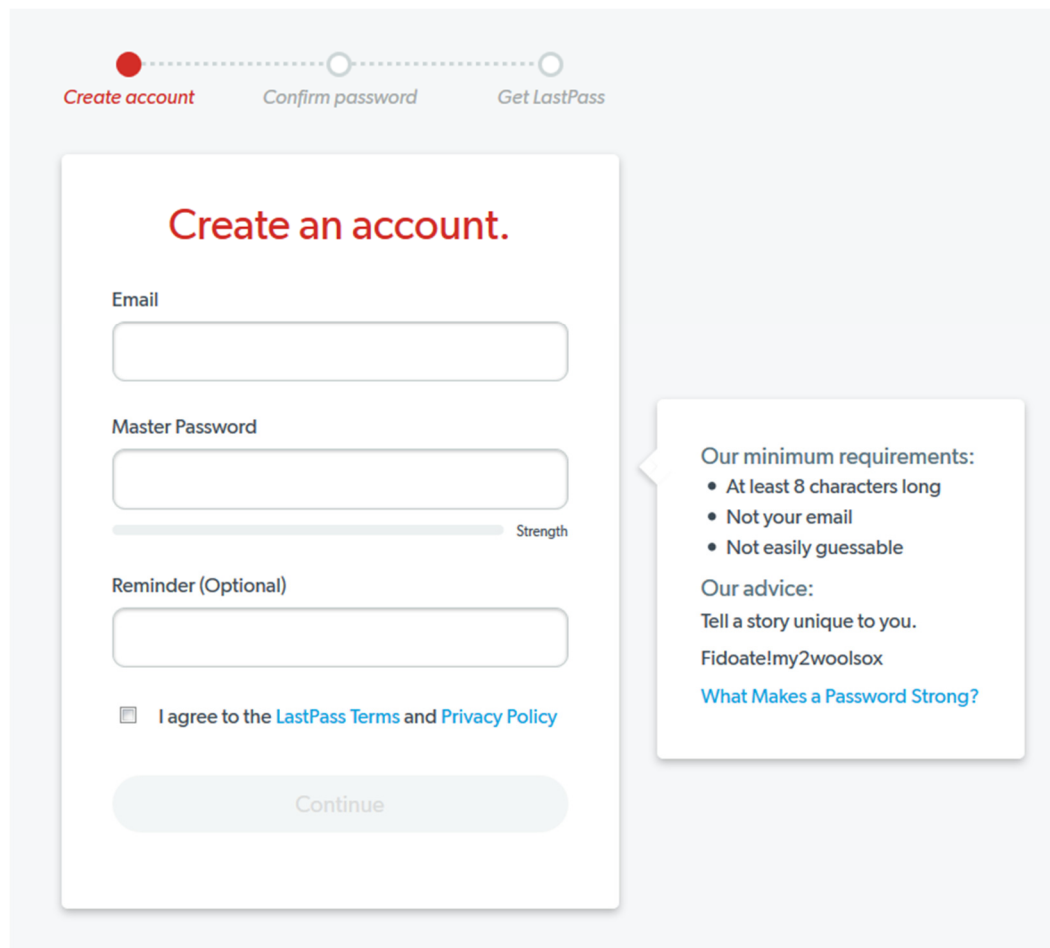
## Setting up your account

To create an account with LastPass you'll need to have an email account, which will act as your "username" for LastPass. You will also need to create a secure password - remember this will (hopefully) be the last password you need to remember.

For LastPass your password needs to be at least 8 characters long. If you are having trouble coming up with something, LastPass suggests your password can be a short story unique to you. For more information you can click on their "What Makes a Password Strong?" link shown below:

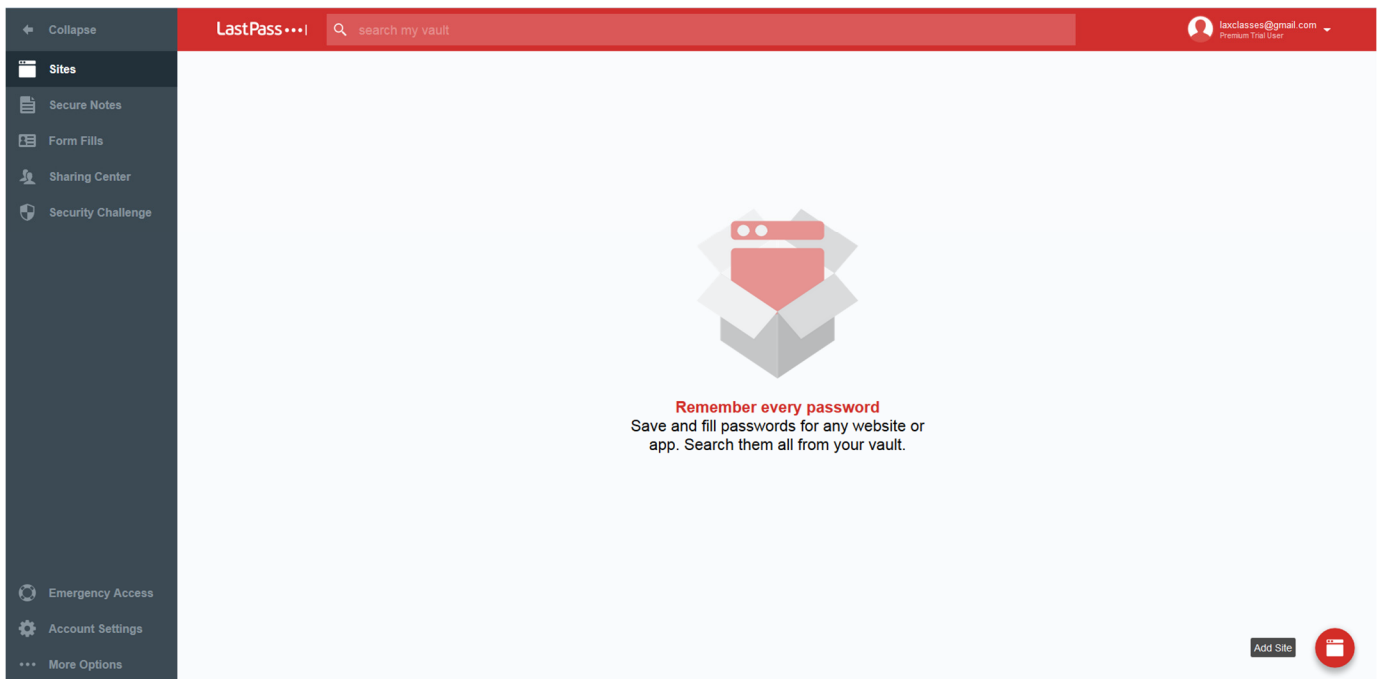


The image shows the LastPass login interface. At the top, it says "Log In to Access LastPass". Below this are two input fields: "Email" and "Password". To the right of the "Password" field is a "Forgot Password?" link. Below the input fields is a checkbox labeled "Remember Me" and a red "Log In" button. At the bottom, there is a link "New to LastPass? Create an account now." and another link "Log in using a One Time Password".



The image shows the LastPass account creation interface. At the top, there is a progress bar with three steps: "Create account" (highlighted with a red dot), "Confirm password", and "Get LastPass". Below the progress bar is a white box with the heading "Create an account." in red. Inside this box are three input fields: "Email", "Master Password", and "Reminder (Optional)". Below the "Master Password" field is a "Strength" indicator. Below the "Reminder (Optional)" field is a checkbox labeled "I agree to the LastPass Terms and Privacy Policy". At the bottom of the white box is a "Continue" button. To the right of the white box is a callout box with the heading "Our minimum requirements:" followed by a list of requirements: "At least 8 characters long", "Not your email", and "Not easily guessable". Below this is the heading "Our advice:" followed by the text "Tell a story unique to you." and the example password "Fidoate!my2woolsox". At the bottom of the callout box is a link "What Makes a Password Strong?".

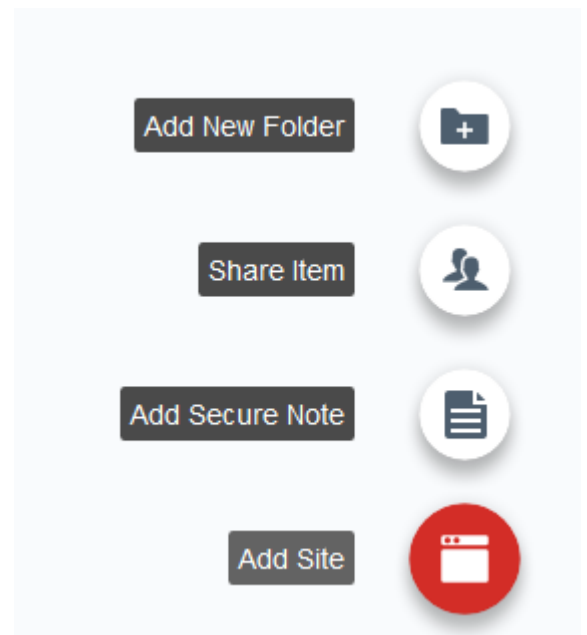
## Adding passwords



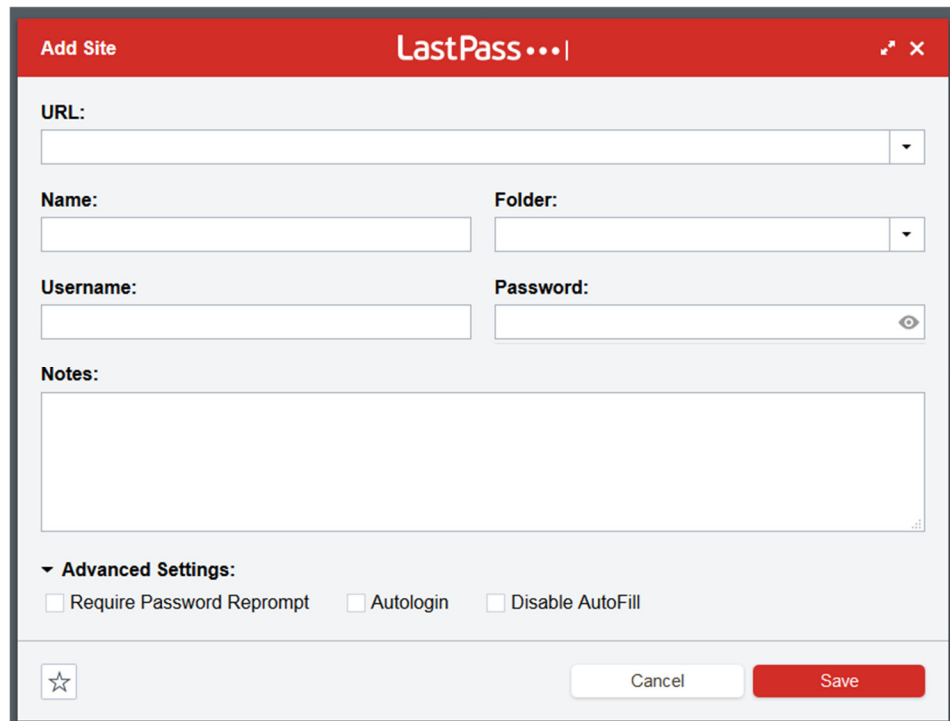
Once you have created your account you will be able to access your password “vault.” This is where you will find your passwords in the future. Using our earlier example, the vault is the pages in a notebook where you record your login information.

To create a new entry, click the red button in the bottom left that reads “Add Site.” Here you can also add a secure note\*, share one of your saved items, or create a folder to organize your passwords.

\*Secure notes allow you to store private information and work like a basic text file. They’re encrypted and stored in your vault. Examples of information you might keep in secure notes include: bank account numbers, password numbers, combinations to safes or other information you’d like to have access to wherever you are but that you’d like to keep safe from hackers.



Once you have clicked “Add site” the following window will pop up for you to fill out, similar to a rolodex card:



The URL field is where you will put in the website address that the account belongs to. Examples: gmail.com, amazon.com, bestbuy.com.

Name is the name of the website. Examples: Gmail, Amazon, BestBuy.

Folder is a drop down where you can select folders you’ve created to store the password in, these help you organize like passwords. Examples might be: Online Stores, Streaming Websites, Banking.

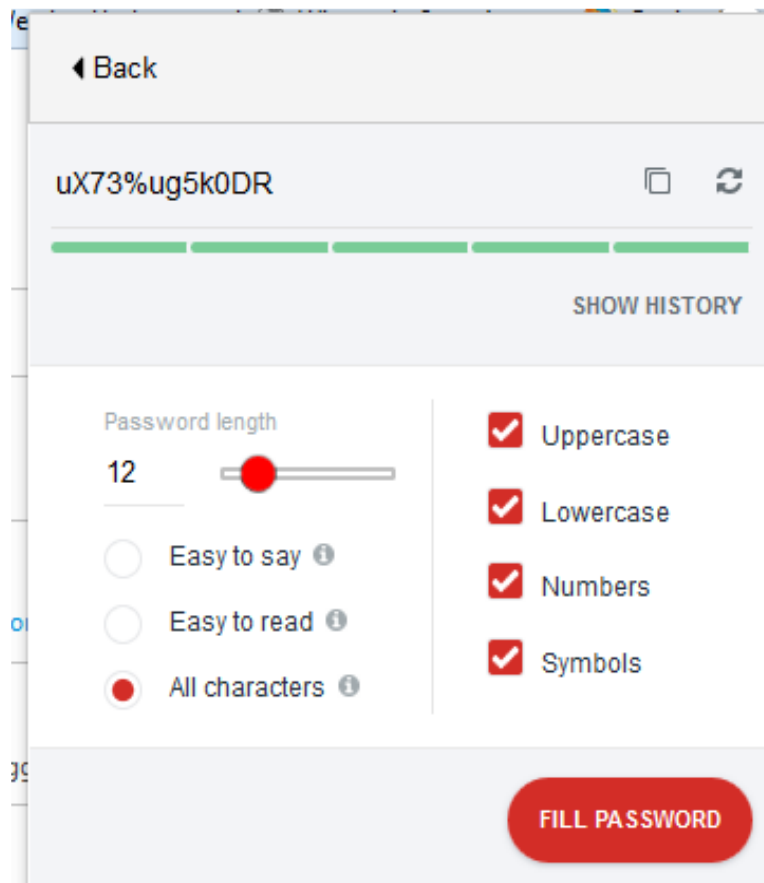
Username is the username used for your login on the site. This may be your name, a created name you use online, or perhaps your email address.

Password field is where you record your password. If you would like you can have LastPass generate a random password for you. The generated passwords are long strings of letters, numbers, and special characters; you can set how many characters total and whether you want to avoid hard-to-read characters such as the number 0 and capital letter O. These passwords are hard to hack and can’t be socially engineered because you won’t need to remember them, you can simply access them from LastPass as needed.

The notes field is good for storing extra information such as answers to security questions if a site requires them.

Under advanced settings you can tell LastPass to automatically log you in on store websites or turn off LastPass auto filling your username and password.

## Generating a safe password

The image shows a screenshot of the LastPass password generator interface. At the top, there is a 'Back' button. Below it, a generated password 'uX73%ug5k0DR' is displayed next to copy and refresh icons. A green progress bar is shown below the password. A 'SHOW HISTORY' link is located to the right of the progress bar. The main section contains settings for password generation. On the left, 'Password length' is set to 12 with a slider. Below this are three radio button options: 'Easy to say', 'Easy to read', and 'All characters', with 'All characters' being selected. On the right, there are four checked checkboxes for 'Uppercase', 'Lowercase', 'Numbers', and 'Symbols'. At the bottom right, there is a red button labeled 'FILL PASSWORD'.

As mentioned on the last page you can use LastPass to create randomly generated passwords. Unlike the suggested method of creating a unique story about yourself that we discussed when creating your LastPass password, the goal here is to create a long string of characters that are both impossible to guess and difficult for computers to crack.

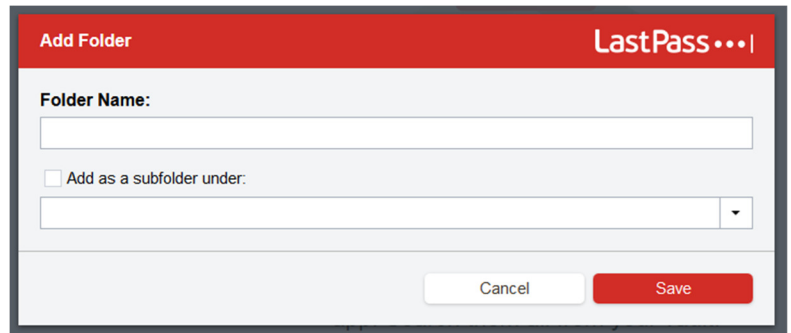
Because these passwords are stored in LastPass, the idea is that you do not have to remember them as you can simply access them at any time when needed; the password being random isn't something to worry about. However, LastPass offers options to make these random passwords easy to say and read, if you'd like. You are able to select which type of characters are used (to help match the requirements of whatever site you are on). For password length, LastPass will generate passwords from 4-100 characters long.

LastPass also offers an auto change password feature that routinely updates your password for websites that allow this feature. The number of websites that allow this option is growing.

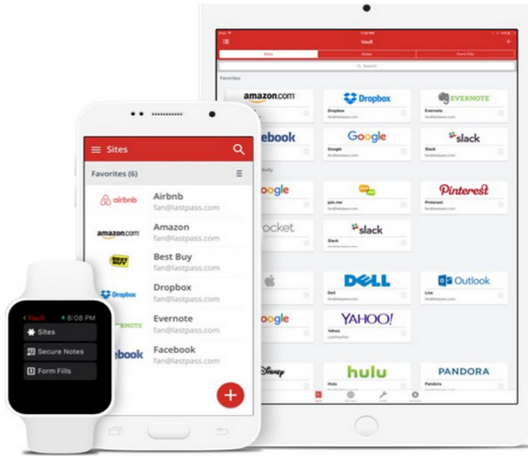
If you would prefer to come up with your own passwords, you are also able to do that as well. The main thing to remember is that it is best to create a unique password for each website that requires a login.

## Organize your vault

After you have amassed a large collection of saved passwords it may be a good idea to organize your vault. You can do this either by using the “Add Folder” option from the button in the bottom right of your vault or editing one of your saved passwords. You are also able to make subfolders if you would like to further separate out your passwords. Grouping similar websites together makes it easier to locate the passwords you need.

A screenshot of the LastPass 'Add Folder' dialog box. It has a red header with 'Add Folder' on the left and 'LastPass' on the right. Below the header, there is a 'Folder Name:' label followed by a text input field. Underneath that is a checkbox labeled 'Add as a subfolder under:' followed by another text input field and a dropdown arrow. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

## Access your passwords anywhere



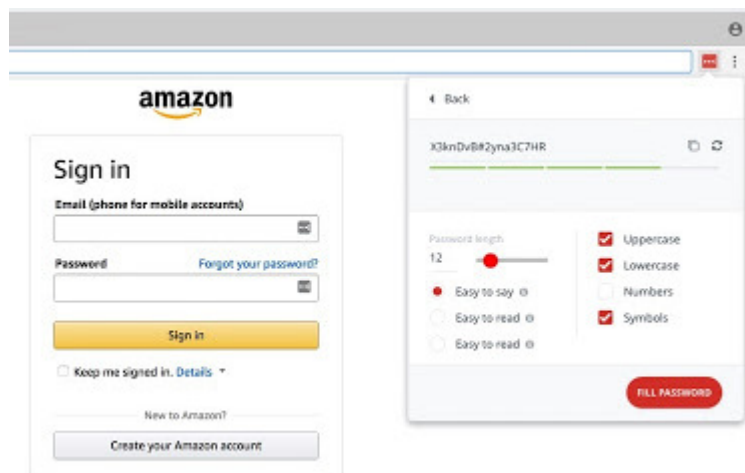
## Access, granted.

Your LastPass account is backed up and synced across all devices for access to your passwords no matter where you are.

Get the app on all your favorite devices.



LastPass offers you many ways to access your passwords on a variety of platforms. Besides visiting Lastpass.com to access your vault, you can download a Lastpass app for your mobile phone that allows you to access your vault offline. You can also install Lastpass add-ons to your browser of choice, allowing you to generate and retrieve passwords no matter where you are on the internet by simply clicking on the Lastpass extension button (as shown to the right).



## Account settings

Account settings are divided between a few categories. General is where you'll find your options to change your account email, master password, language, time zone, and recovery phone number. The other tabs are Multifactor Options (LastPass has partnered with other businesses to allow multifactor authentication, you can enable them here), Trusted Devices (when you have multifactor authentication on you can choose to trust a device for up to 30 days, they are listed here), Mobile Devices (shows a list of mobile devices linked to your account), Never URLs (turn off LastPass on specific URLs), Equivalent Domains (indicates when websites have multiple URLs and links them together), and URL Rules (set specific rules for LastPass on specific URLs). Some of these features are locked to premium accounts.

## Premium Options

LastPass offers two types of premium accounts. One is for individuals and the other is for families (up to 6 users). The features you unlock by upgrading to premium are: Emergency Access, one-to-many sharing, advanced multi-factor options, priority tech support, LastPass for applications (on Windows), and 1 GB of encrypted file storage.

<p><b>Premium</b></p> <p><b>\$ 2 /month</b></p> <p>1 user</p> <p>Secure your online backup plan and enjoy flexible sharing.</p> <p><b>Go Premium</b></p> <p><i>Billed \$24 annually</i></p>	<p><b>Families</b></p> <p><b>\$ 4 /month</b></p> <p>6 users</p> <p>All of your family's passwords organized, secure, and at your fingertips.</p> <p><b>Try Now</b> <b>Buy Now</b></p> <p><i>Billed \$48 annually</i></p>
---	--

### Leading in security.

As a password manager, our first priority is safeguarding your data. We've built LastPass so that we never have the key to your account.

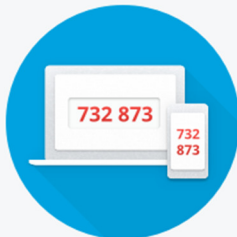


#### Strong encryption algorithms.

We've implemented AES-256 bit encryption with PBKDF2 SHA-256 and salted hashes to ensure complete security in the cloud. You'll create an account with an email address and a strong master password to locally-generate a unique encryption key.

#### Local-only encryption.

Your data is encrypted and decrypted at the device level. Data stored in your vault is kept secret, even from LastPass. Your master password, and the keys used to encrypt and decrypt data, are never sent to LastPass' servers, and are never accessible by LastPass.



#### Two-factor authentication.

Two-factor authentication (sometimes referred to as multifactor or 2FA) adds extra security to your LastPass account by requiring a second login step before authorizing access to your vault. [Learn More](#)

In the words of LastPass:

"Security is our highest priority at LastPass, including quickly responding to and fixing reports of material bugs or vulnerabilities. LastPass is in part able to achieve a high level of security for our users by looking to our community to challenge our technology. We appreciate the important work that the security research community provides and appreciate responsible disclosure of issues. Further, we believe that when the security process works as designed, we all benefit."