Password Management

Table of Contents

Introduction

Managing passwords on computers is a major problem for many computer users. Many web pages require that you enter a user name and password to use the page.

There are many approaches that people use for this problem:

Solution	Pros	Cons
Write down passwords on paper(s)	Very simple	Not very secure Easy to lose paper Easy to mistype password
Save passwords in an encrypted file or note	Relatively simple Reasonably secure	Need to open file Need to copy / paste Need file on all devices
Have browser save the passwords for you	Simple Easy to use Very Secure	Works well if you use one browser on all devices
Use a password manager	Simple Easy to use Multiple browsers Very secure	Must absolutely remember the master password

For most people, if they use one browser on all of their devices, the simplest and easiest solution is to have the browser remember the passwords and fill them in automatically when you open a web page with a password entry form.

The browser or password manager can also automatically create and save complex passwords when you need to create one for a website.

Password Rules

There are a few simple rules to keep in mind about passwords:

1. Never use simple passwords. Always use a long sequence of upper and lower case characters, numbers and special characters. Longer passwords are much safer than shorter ones.

2. Never use the same password on multiple sites

3. Let your browser create complex passwords for you and save them so you don't need to type them in on websites. This is much easier and safer than writing down passwords on paper. If you use multiple browsers on various devices, you can use a password manager to create and save passwords for you.

4. Make sure the password you use to access your email is long and complex. The reason is that if someone can access your email account, they can change all of your passwords by requesting that a website send you a password reset email which, of course, they can access. The first one they will change is your email account.

5. Make sure your passwords to access Internet storage ("**cloud accounts**") are long and complex. Examples are Apple iCloud, Google Drive, Dropbox, etc. These companies keep your data encrypted on the "cloud" but if someone can guess your password they can get access to this data.

6. Make sure your passwords to access financial websites and to log into your browser are long and complex.

7. Use **two factor authentication** on sensitive websites (e.g. financial and email). The website will send you a code on your phone that you must enter to log into the site.

You normally don't need to change your passwords if you follow these steps. If you hear about a data breach at a company where you have a password, you should definitely change that password immediately.

Basic Approach

The basic approach to using your browser or a password manager to save your passwords is to let it save passwords when it asks via a popup window. You should not try to add passwords to your browser or password manager manually. This is error prone, unnecessary, and a waste of your time.

After you have manually entered a password into a website you will know if the password is correct because you will then be logged into the site. This is when the browser or password manager will popup a window to ask if you want to save the password. Simply click the Yes or Save button.

If the password you entered is different from the one you have saved, the browser or password manager will popup a window to ask if you would like to update the saved password. Simply click the Yes or Update button.

When you go to a website with a saved password, the browser or password manager will fill in the saved user ID and password for you. You sometimes have to click in the password field to get the browser to fill in the saved password. This depends on the browser and device.

When you want to create a new password for a website, let the browser or password manager generate the new password. This happens the first time you create an account for a website or decide to change your password.

Manually Creating Passwords

You should always use a long password with mixed upper and lower case letters, numbers and symbols. Some websites have specific requirements that you have to use when creating a password manually.

Normally you would let the browser or password manager create a password for you but if it is a password that you will need to enter frequently you will probably want a password that you can remember and type without mistakes.

You should **NOT** use names of your family, pets, numbers from your address or phone number and other items that are easy to guess.

One good approach is to choose a phrase, like: "I love Senior Planet"

Start by taking out the spaces and changing to lower case characters:

iloveseniorplanet

You can then capitalize some of the letters, e.g. the last one in each word.

ilovEsenioRplaneT

You can then change some of the letters to numbers and symbols, e.g. "L" to "1", "o" to 0, "a" to "@":

i10vEseni0Rp1@neT

This is a reasonable password. It is 17 letters long, has upper and lower case letters and some symbols.

Using Browsers to Save Passwords

All of the major browsers support generating and saving passwords. The first step is to set the browser setting to make sure it does this.
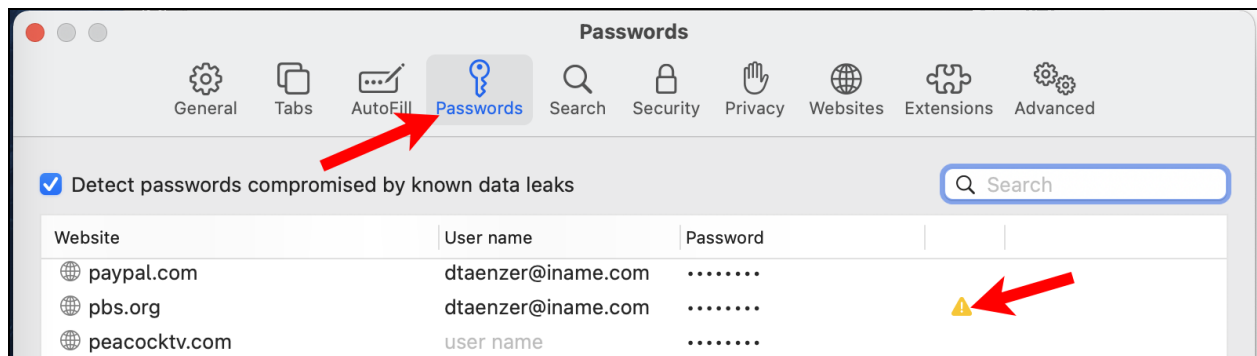
Safari

In the Safari browser, click the Safari menu next to the apple icon in the upper right part of the screen and choose Preferences:

Then click the Autofill button near the top of the Preferences window and make sure the "User names and passwords" box is checked:
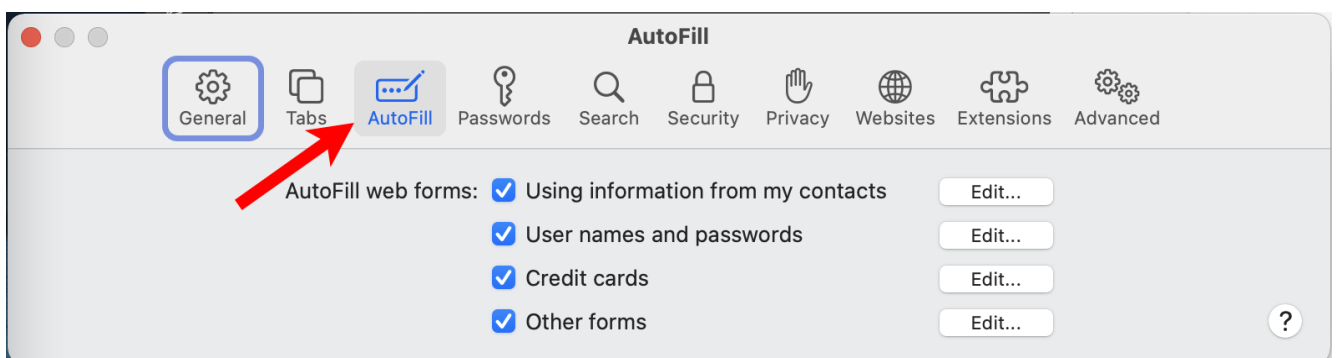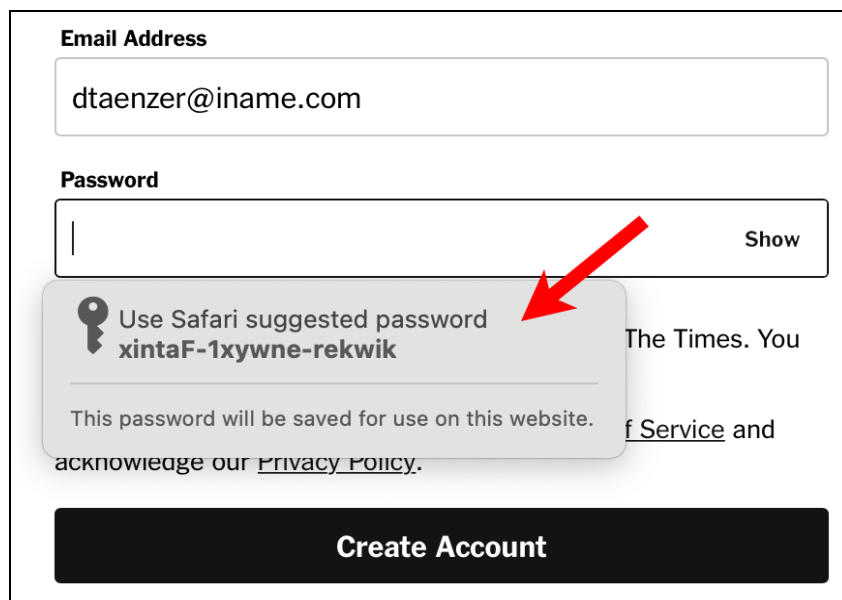
You can click the Passwords button to view your saved passwords. You will need to enter your login password to use this part of the preferences.

Safari will display a yellow warning mark if your password is too simple or has been reused in another website.
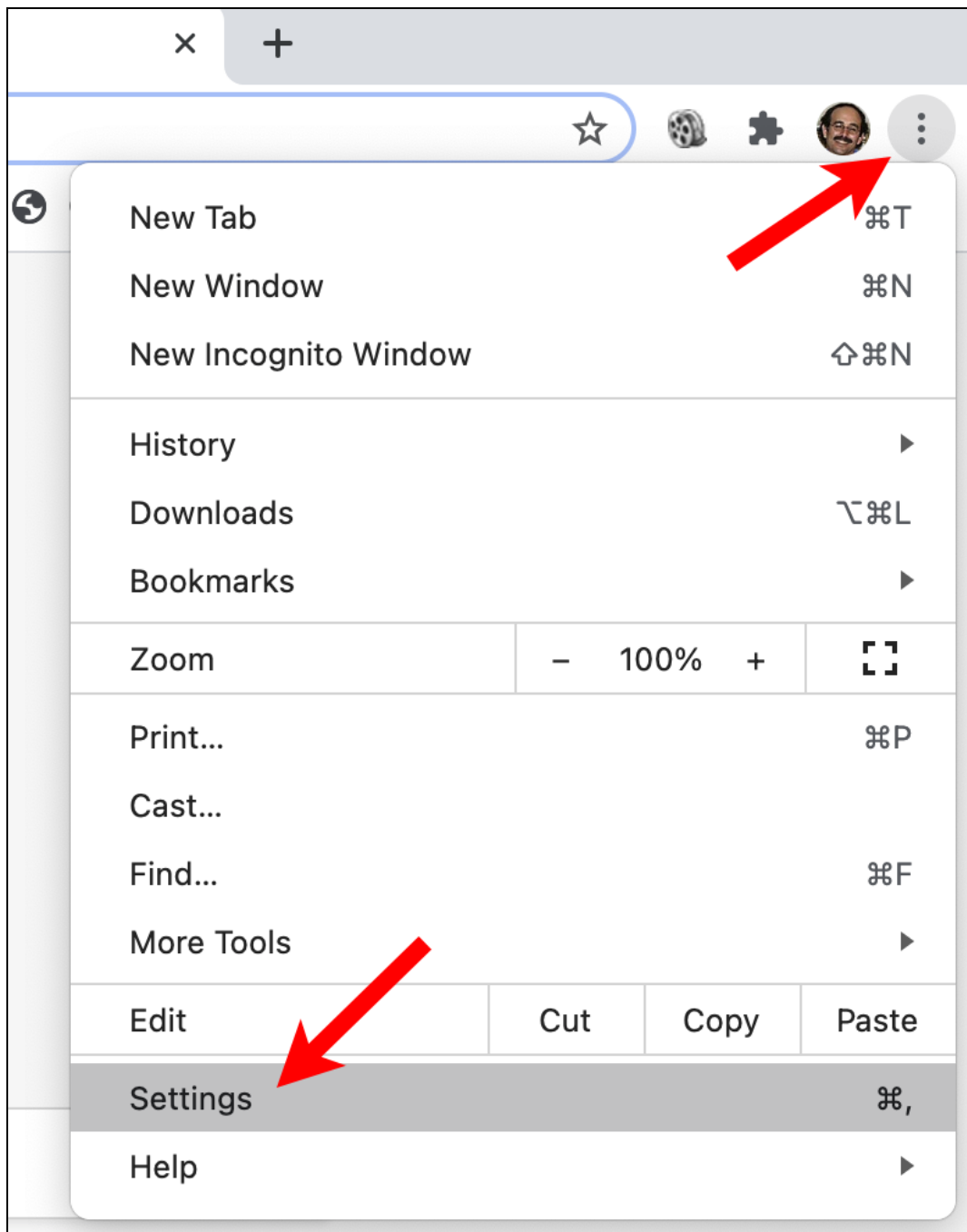
When you need to create a password or replace one, Safari will offer to use a complex generated password, e.g.:
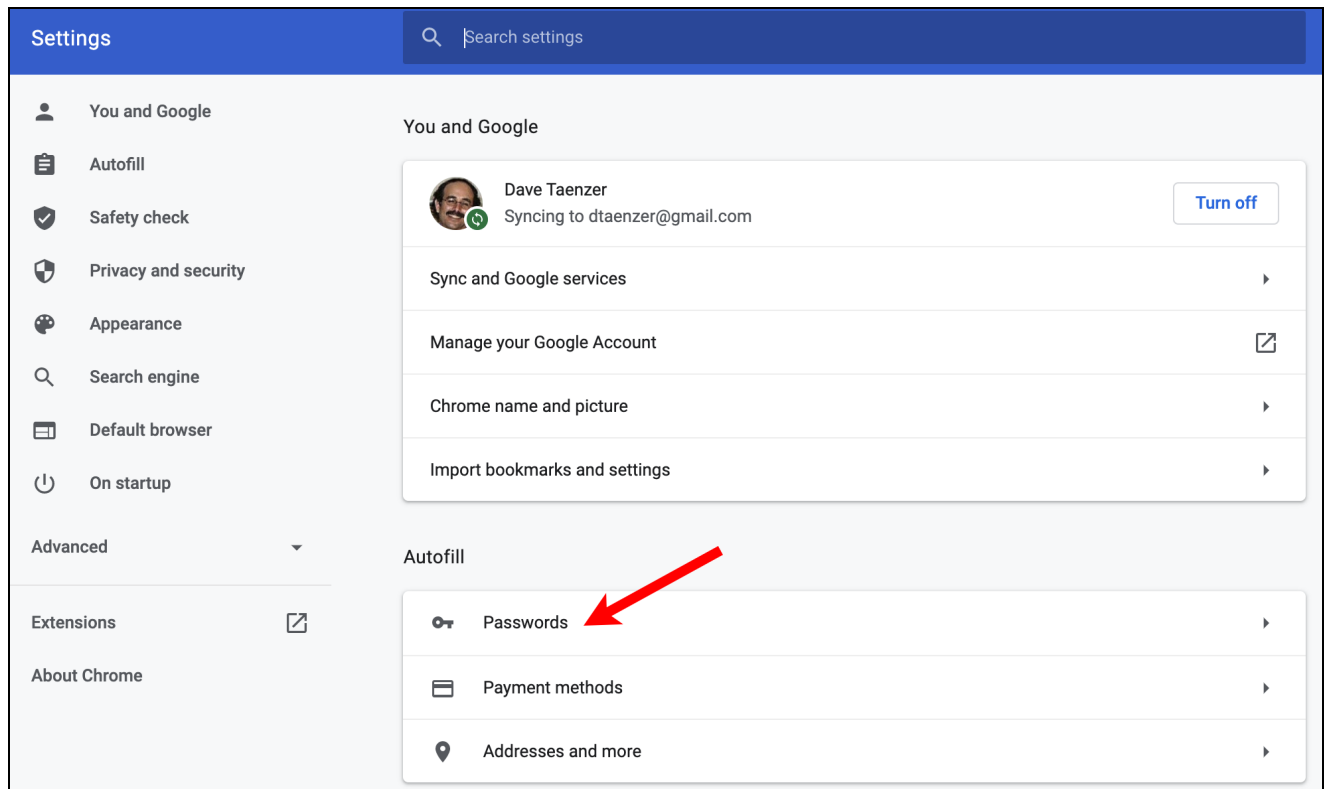

You click on the "Use Safari suggested password" button to fill in the password and save it for this website.
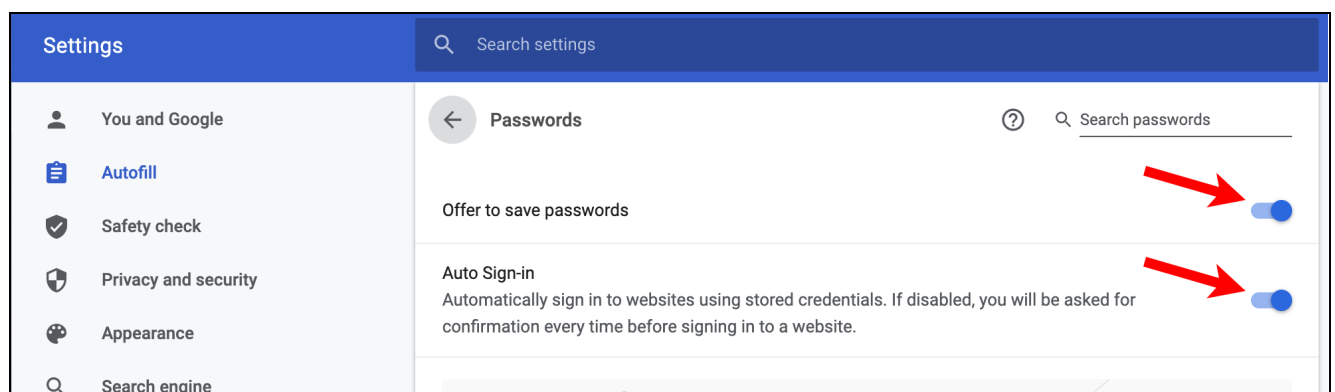
Chrome

In the Chrome browser, you click on the More menu in the upper right corner of the window (three vertical dots) and select Settings:

You then click on Passwords in the Autofill section:

And then click the top two switches to enable password saving and autofill:

When you need to create a password or replace one, Chrome will offer to use a complex generated password, e.g.:

Email Address

dtaenzer@iname.com

Password

| Show

Use suggested password   Y*78&rJ{ia?%^BT   es. You

Chrome will save this password in your Google
Account. You won't have to remember it.   e and

Create Account

You click on the "Use suggested password" button to use the complex password and save it for the website.

FireFox

In the FireFox browser, you click on the More menu in the upper right part of the window (three horizontal lines) and click on Preferences:
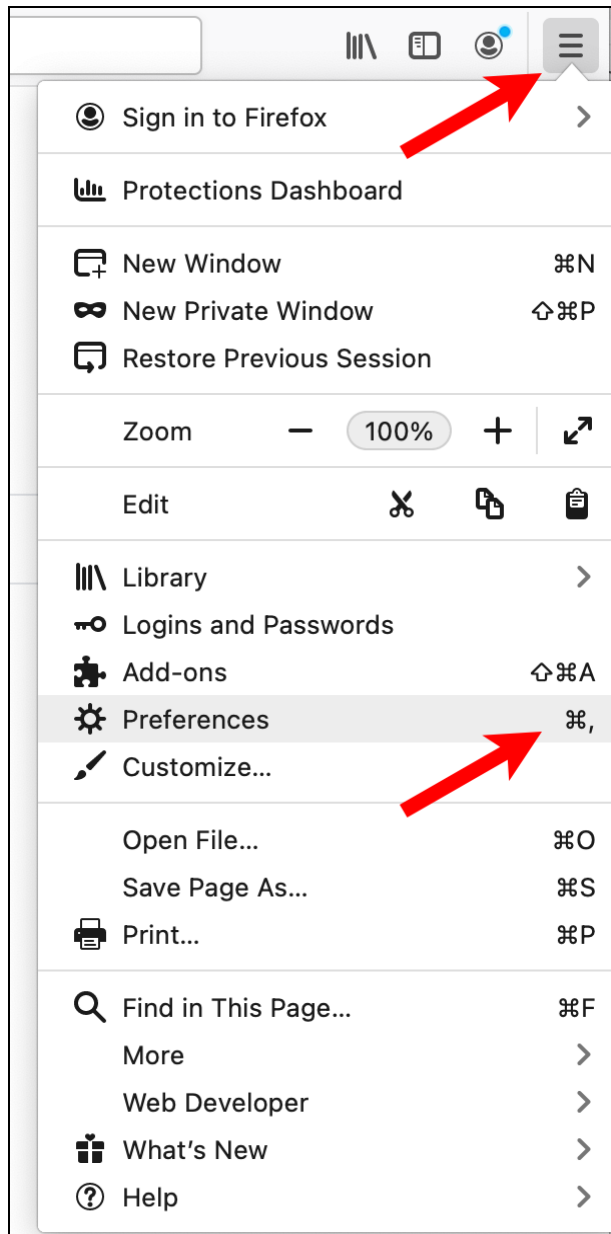
Click on "Privacy and Security" on the left and then scroll down to the "Logins and Password" section:
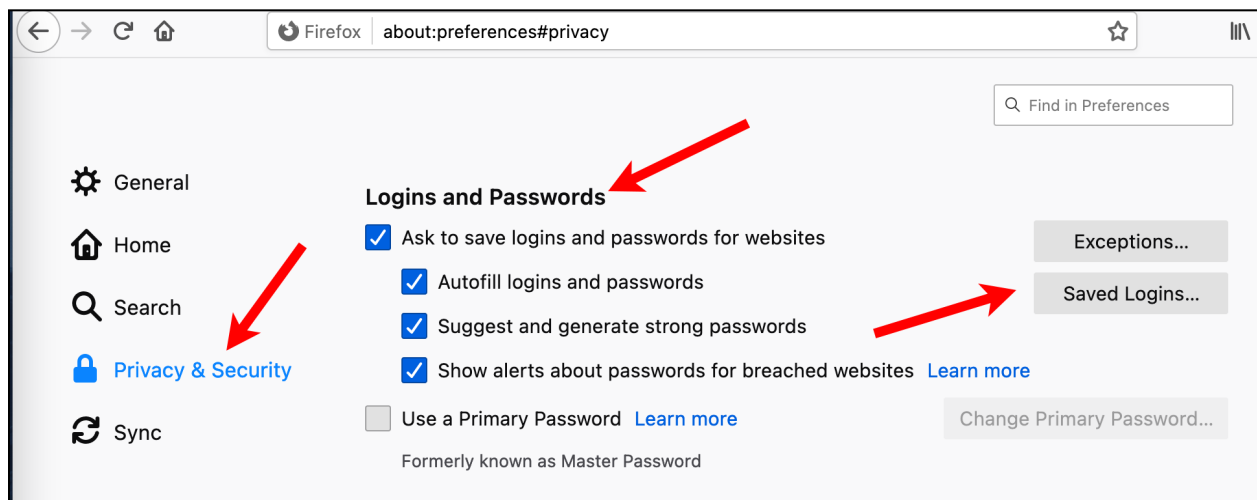
You can click on the "Saved Logins…" button to view your saved passwords.

When you need to create a password, Firefox will create on for you:

Using LastPass Password Manager

If you often use multiple browsers and you want all your browsers to automatically fill in your saved passwords, you should consider using a password manager. There are many of these available. One popular one is LastPass which offers a free option but you will need to buy a subscription to use it on multiple devices. This is currently $3 per month.

> **https://www.lastpass.com/pricing**

This works using a master password that you create. All of your passwords are encrypted and decrypted on your machine with your master password. It should be long and hard to guess.

The LastPass company does not keep your master password and if you lose it, you lose access to all of your passwords. You should make this password long but easy for you to remember.
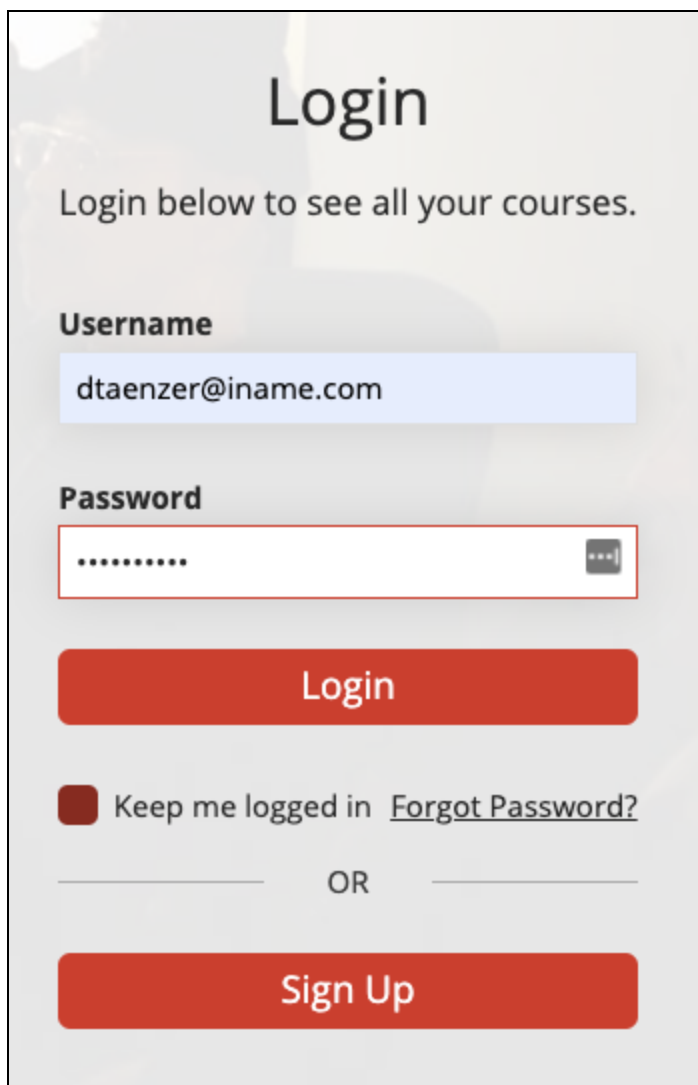
To use a password manager, you download the program to your computer or the app to your portable device and create a master password.

You should not try to add passwords directly into the system, but should let it capture them as you use them on the web.

Adding an Existing Password to LastPass

After you add LastPass to your browser, it is very easy to add your existing passwords to LastPass.

- ● Go to web site that requires a password, e.g. seniorplanetu.org and enter your password

Login

Login below to see all your courses.

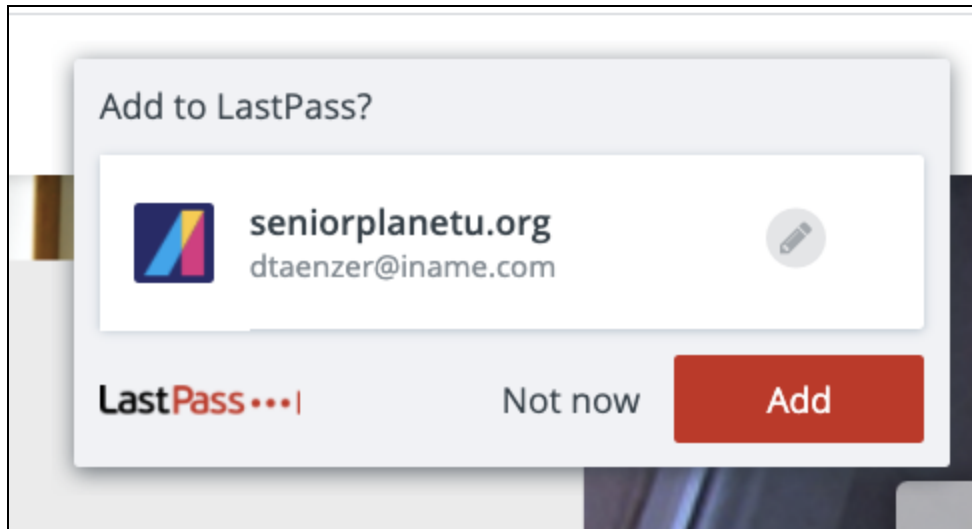**Username**

dtaenzer@iname.com

Password

··········

Login

■ Keep me logged in Forgot Password?
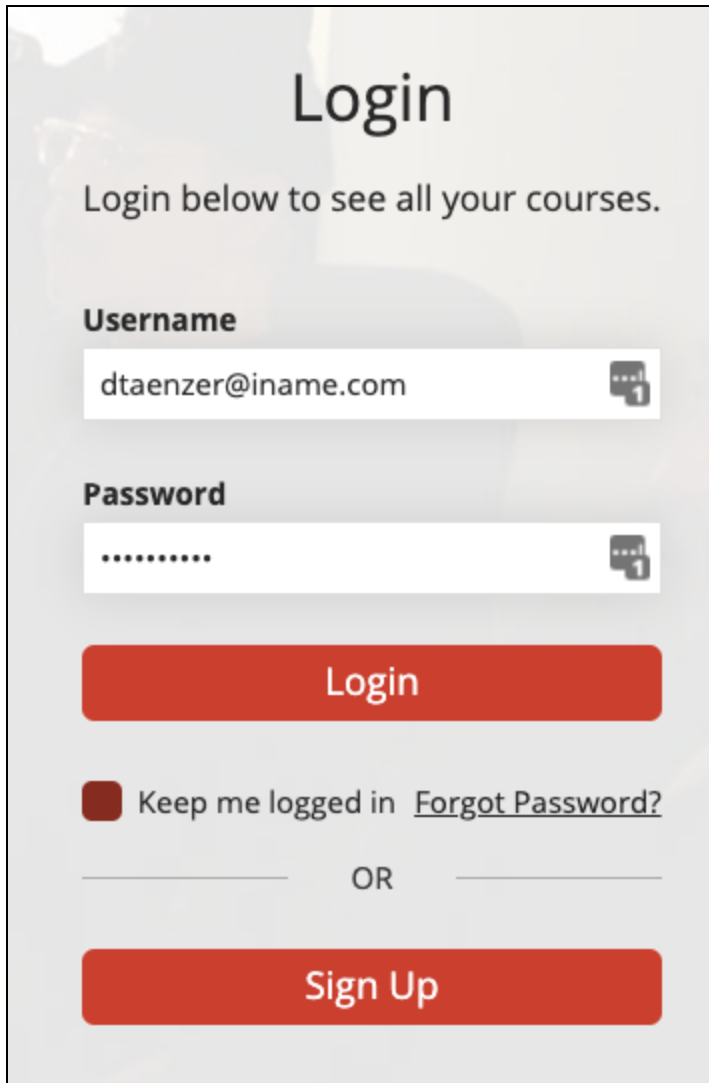
—————— OR ——————

Sign Up

- A LastPass popup window will ask you if you want to add this password to your vault

- Click the Add button to add this password to LastPass

The next time you go to that site, the password will be filled in for you:

Login

Login below to see all your courses.
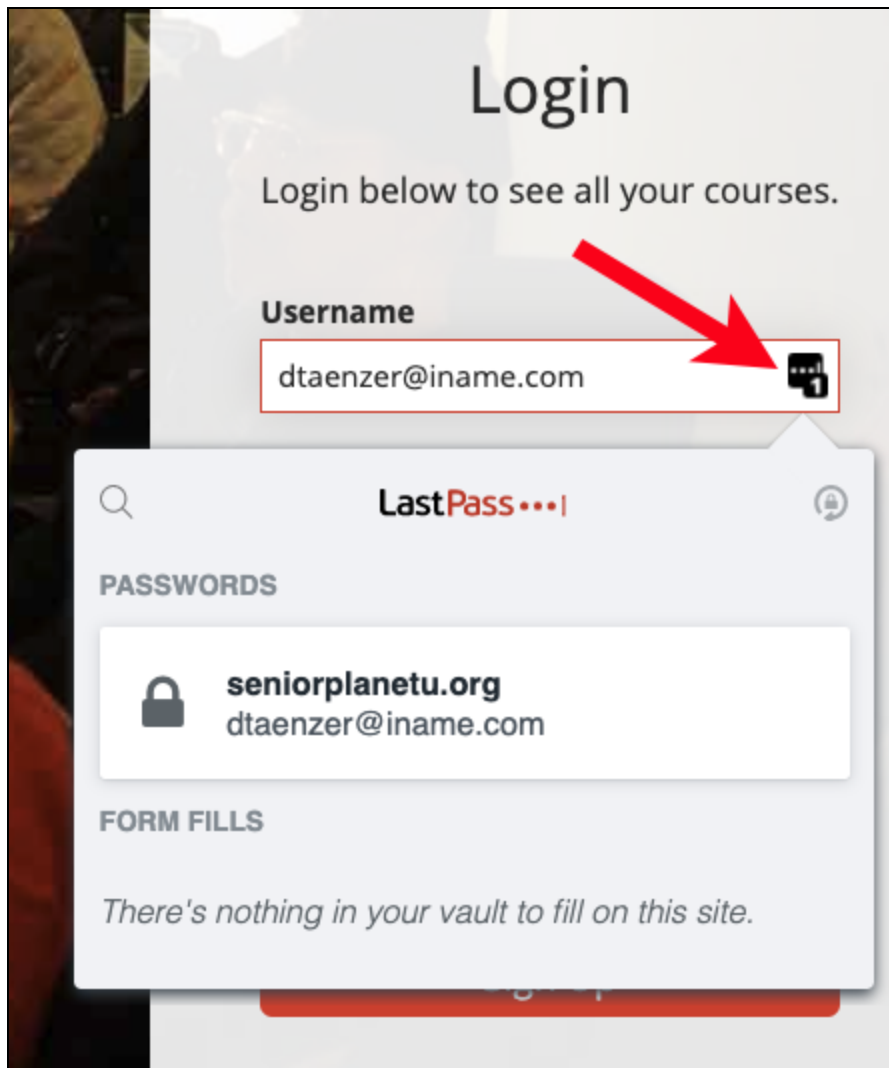
Username

dtaenzer@iname.com

Password

··········

Login

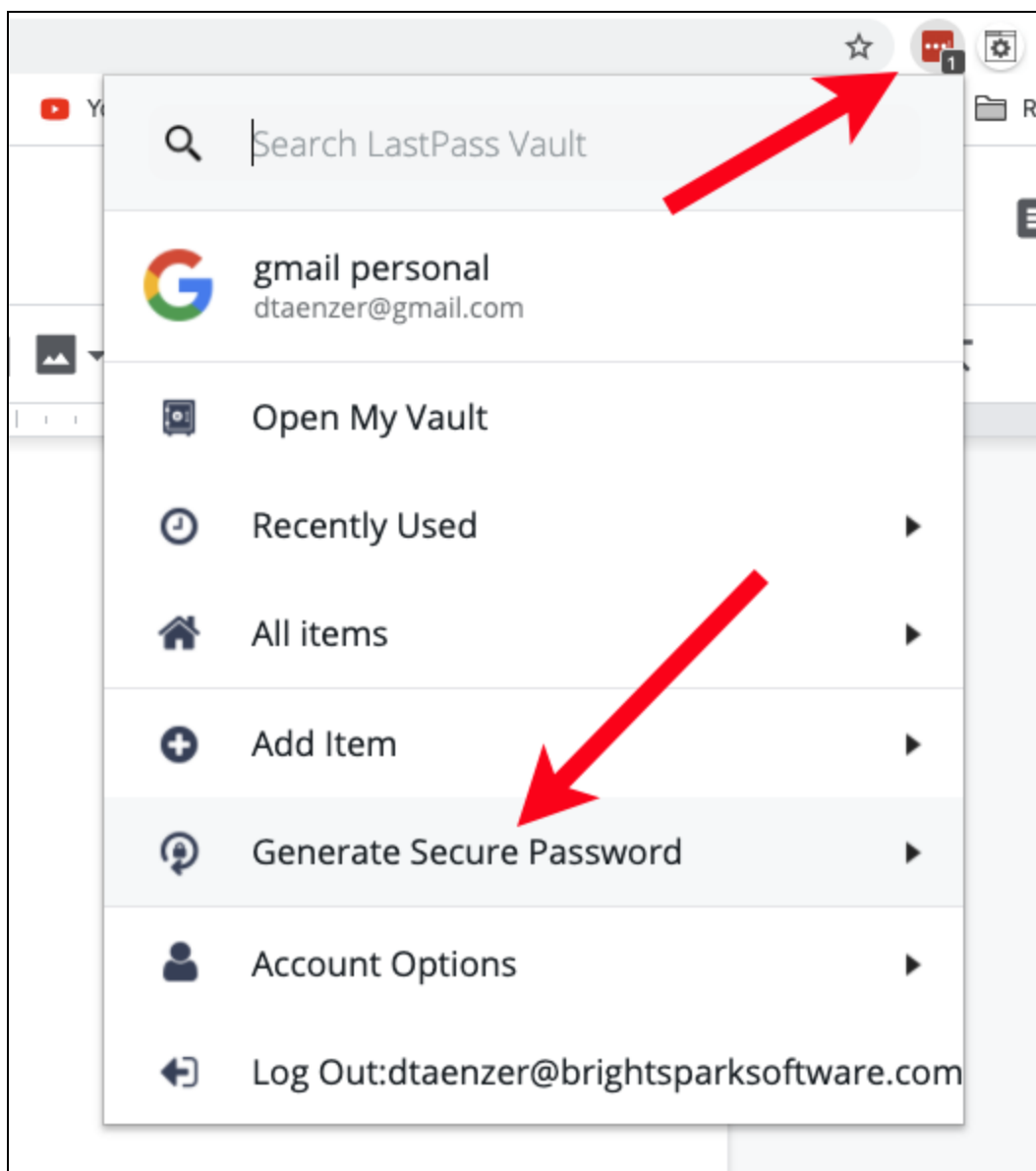☐ Keep me logged in Forgot Password?

—————— OR ——————

Sign Up

If your password does not appear, click the dark Icon in the field and it will be filled in for you:
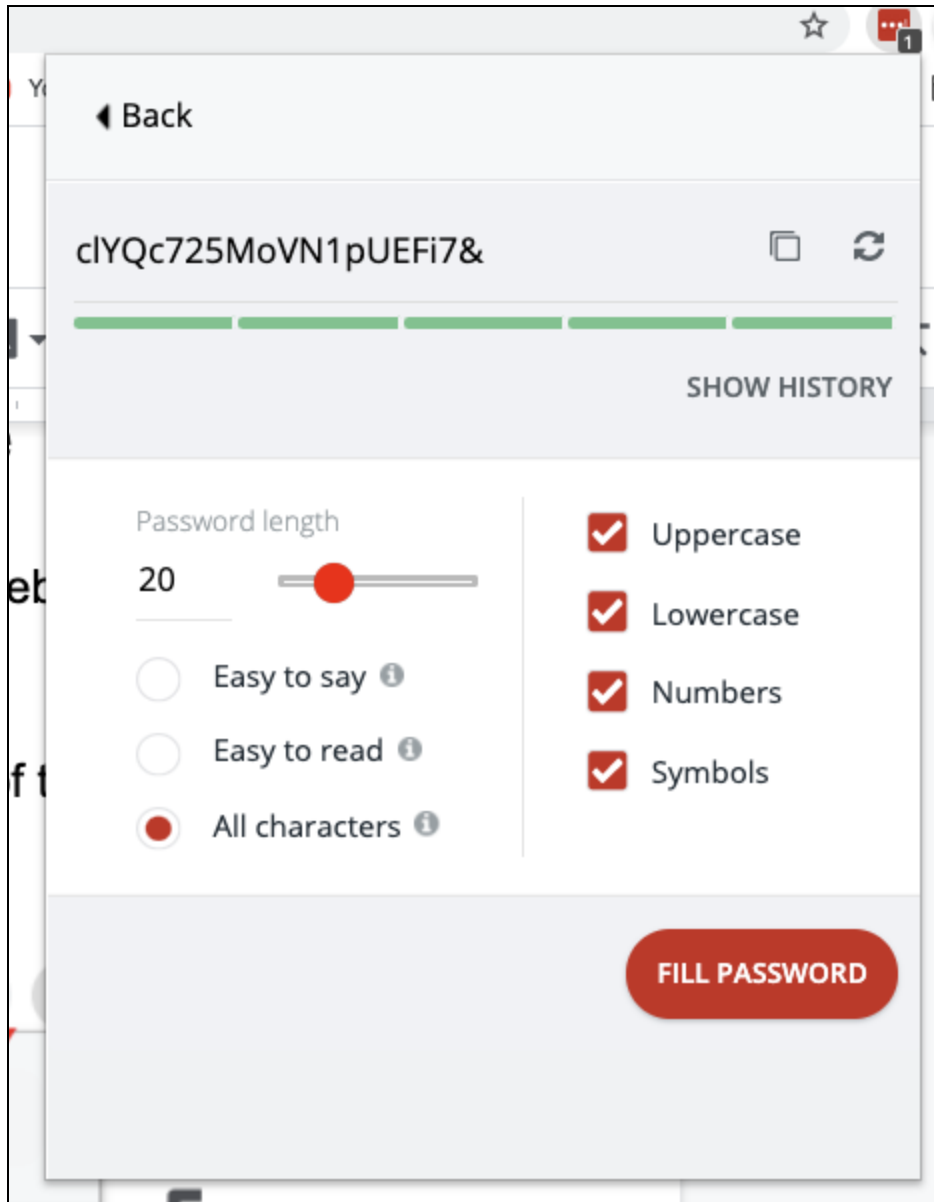
Generating a New Password for a Site

When you are asked to create a new password for a web site, you can let LastPass generate one for you.

You click on the LastPass Helper Icon at the top right of the browser or right click in the password field, then click on Generate Secure Password:

This window pops up:

It lets you customize the length of the new password and some other characteristics and then you click the Fill Password button to put it into the password field on the web page.

For example, let's say you are at a form to create a new account:

Create Account

By creating an account, you agree to Kohl's Security & Privacy Policy and Legal Notices.

First Name   Last Name

Email Address   Password   Show password

name@mail.com

At Least 8 Characters Long   · · · · · · · ·

Numbers and Letters   ABC123

Upper and Lower case   Aa

It says that it needs to be 8 characters long with numbers and letters. You click the LastPass Icon in the upper right of the browser window and generate one to use.

You don't need to remember it. That is what LastPass is for.

Suggested Next Steps

If you are currently using paper to write down your passwords or saving them in a file on your computer:

- Start by making sure your device, email, Cloud and financial passwords are strong. If not, update them to a better password.

- If you are able to use one browser on all your devices, just try turning on the option to save passwords and autofill them for you.

- If you cannot use the same browser everywhere or want to use multiple browsers and be easily able to access your passwords from other computers, you can install a free version of a password manager to try it out.

- As you use websites going forward, let the browser save the passwords for you and next time you go there you won't need to type the password in again.

- If you have any unsafe passwords or are reusing the same password on multiple sites, log into the website and change to a new password that the browser or password manager creates for you. Then let the browser or password manager update the saved password for you.

- After a while, you hopefully will like this approach much more than paper (or a file on your computer) and can eventually get rid of your slips of paper and let the computer handle this problem for you.

Some people find it useful to save the most critical passwords on a single piece of paper and let the browser create and save all the rest. You should then make sure this piece of paper is stored safely.

The single sheet of paper should contain the following types of passwords:

- **Device passwords** (e.g. Mac or PC login password, passcodes for your phone and/or tablet(s)

- **Cloud account passwords**, e.g. Apple, Google, Dropbox

  APPLE

      ID: XXXXX
      Password: PPPPPP

  GOOGLE

      ID: XXXXX
      Password: PPPPPP

- **Email Passwords**, e.g. Google, Yahoo, AOL, etc.

      Email ID: XXXXX
      Password: PPPPPP

- **Financial Institutions**

  Bank 1

      ID: XXXXX
      Password: PPPPPP

- **Password Manager Master Password**

References

Here are some articles about password managers. You will notice that they all mention the same password managers but order them differently.

PC Magazine: Best Password Managers 2022

https://www.pcmag.com/picks/the-best-password-managers

CNET: Best Password Managers 2022

https://www.cnet.com/how-to/best-password-manager/

Wired: 5 Best Password Managers

https://www.wired.com/story/best-password-managers/

Consumer Reports: Best Password Managers

https://www.consumerreports.org/password-managers/best-password-managers-review-digital-security-privacy-ease-of-use/

Macworld: How to take control of your passwords using iCloud Keychain on your iPhone, iPad, and Mac

https://www.macworld.com/article/3607709/icloud-keychain-passwords-safari-chrome-iphone-ipad-mac.html

Use iCloud Passwords in Chrome on your Windows computer

https://support.apple.com/guide/icloud/use-icloud-passwords-on-your-windows-computer-mmfeee20145e/icloud

How to install Apple's iCloud password manager on Google Chrome

https://www.trustedreviews.com/how-to/how-to-install-apples-icloud-password-manager-on-google-chrome-4120981