

Gmail and Google - Compromise Cleanup

Improving Your Security If You Think Someone Else Has Gotten In

Compiled by the Clinic to End Tech Abuse

Last Updated: July 24, 2020

Who is this guide for?

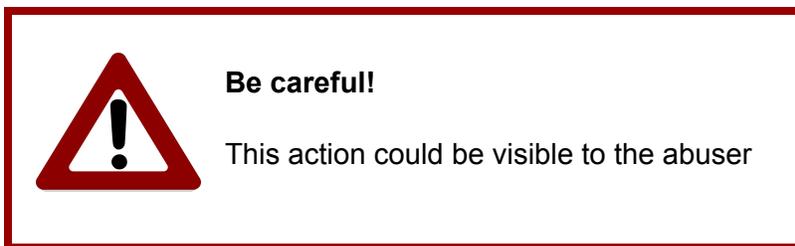
Anyone who suspects or knows that an abusive partner or someone else may have gotten into their Google or Gmail account.

What does it cover?

- Checking for recent logins by others
- Checking the recovery email and phone number
- Securing the account so that it is safer
- Changing your password and setting up a stronger one
- Checking if your emails are being forwarded to another account

Before we start:

- Make sure you can log into the account.
- Is it safe for you to make changes to your account? If anyone else has access to your account, they may learn quickly about any changes you make, such as if you change your password. Some abusers may become more violent if they get locked out of your account. If this is a concern for you, we strongly recommend that you carry out safety planning with a domestic violence or other support professional before making any changes to your account.
- Google provides detailed instructions on how to secure a hacked or compromised account. If you like, you can follow their instructions here:
<https://support.google.com/accounts/answer/6294825>
- We have marked steps that an abuser could find out about with the following warning:

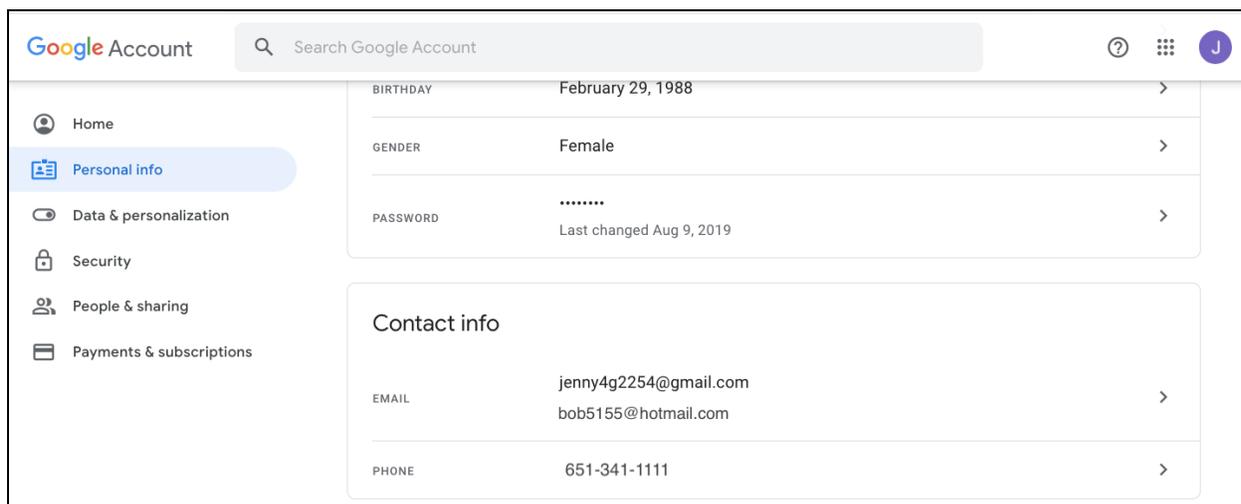


Step 1: Check recovery email and phone number

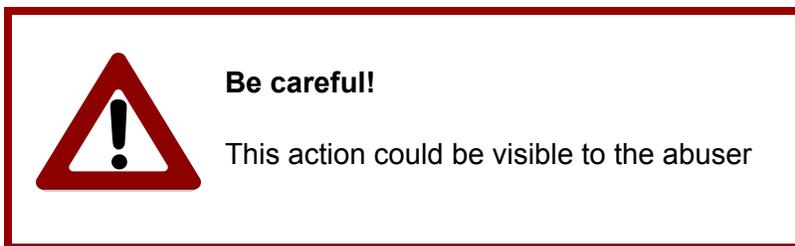
If someone else has gotten into your account, they may have changed the recovery email address and/or phone number to theirs. This can help them get access back into the account even if you do something like change the password.

To check the recovery email and phone number, click on **Personal info** (on the left menu) and scroll down to *Contact info*.

Do you recognize all the email addresses and phone numbers that are shown?



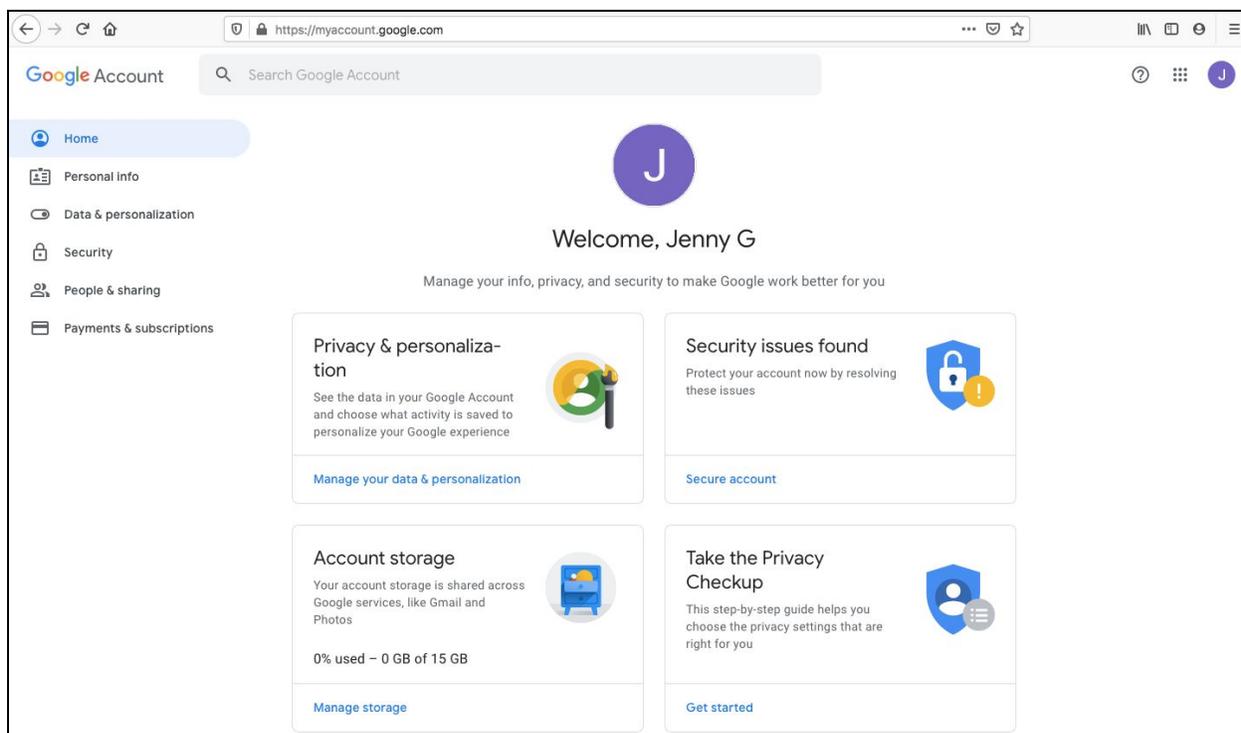
Important: To fully recover the account, we suggest changing the recovery email and phone number to ones that belong to you. Please know that if your recovering email or phone number belongs to someone else, and you change that information, the other person could realize this immediately.



If you are unable to get access to your email account or phone number in order to set them as your “recovery” information, you can try carrying out a Google account recovery: <https://accounts.google.com/signin/recovery>.

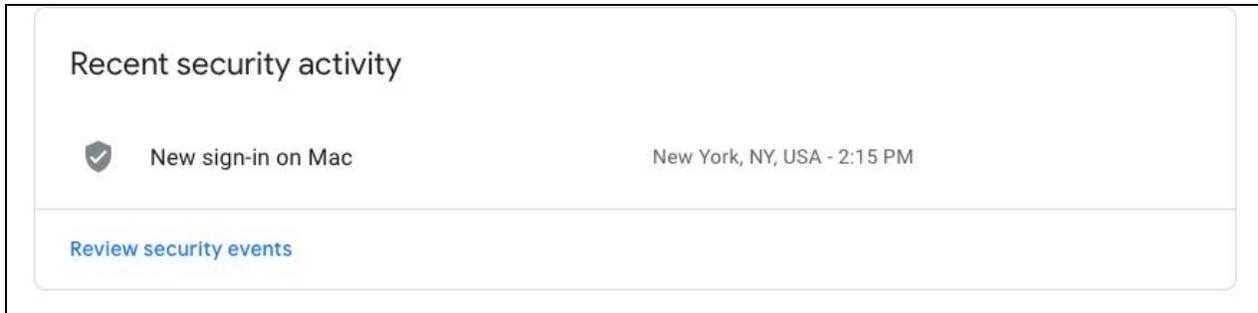
Step 2: Check for recent logins

Login to your Google account by going to <https://myaccount.google.com>. You should see a webpage that looks like the following:



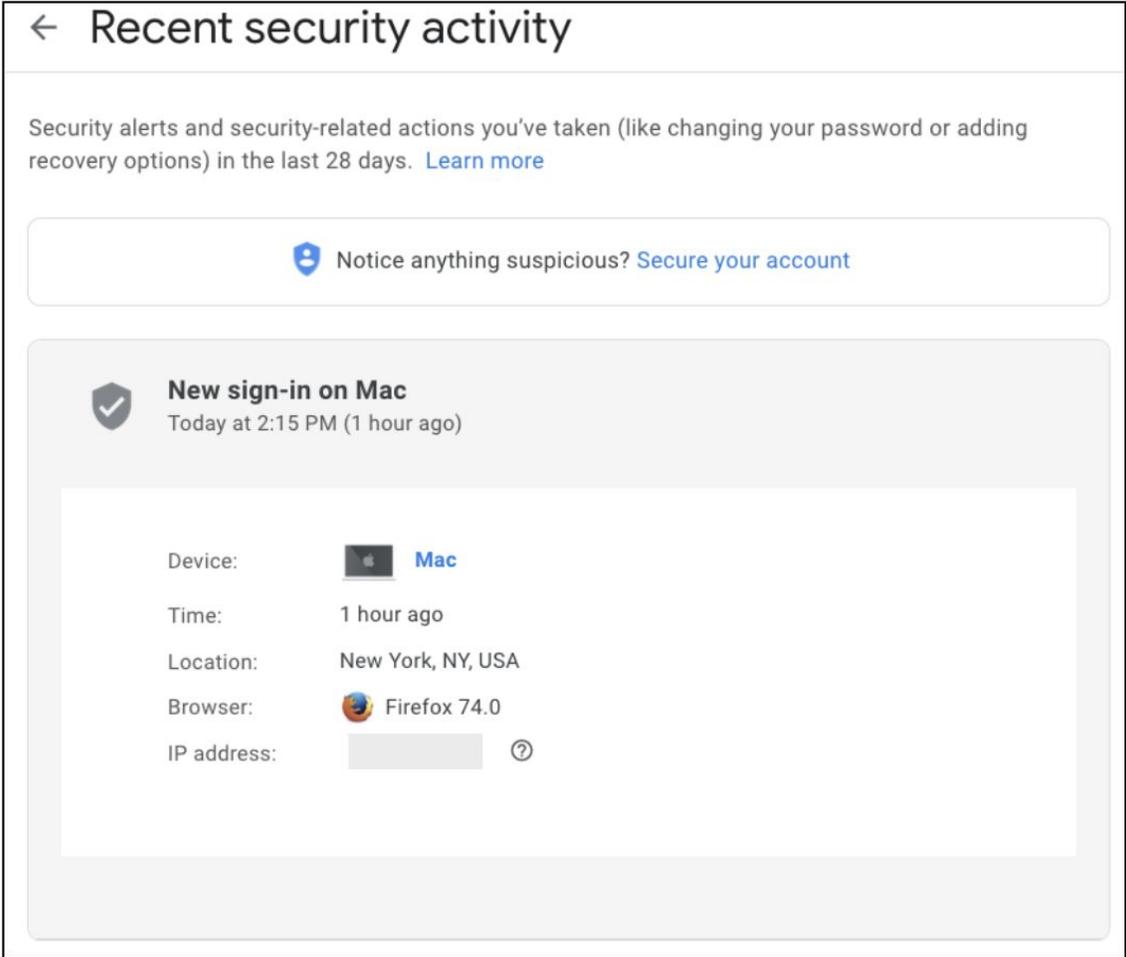
Click on **Security** in the left-hand menu, or just click on this link: <https://myaccount.google.com/security>.

If you scroll down, you should see a section called *Recent security activity*.

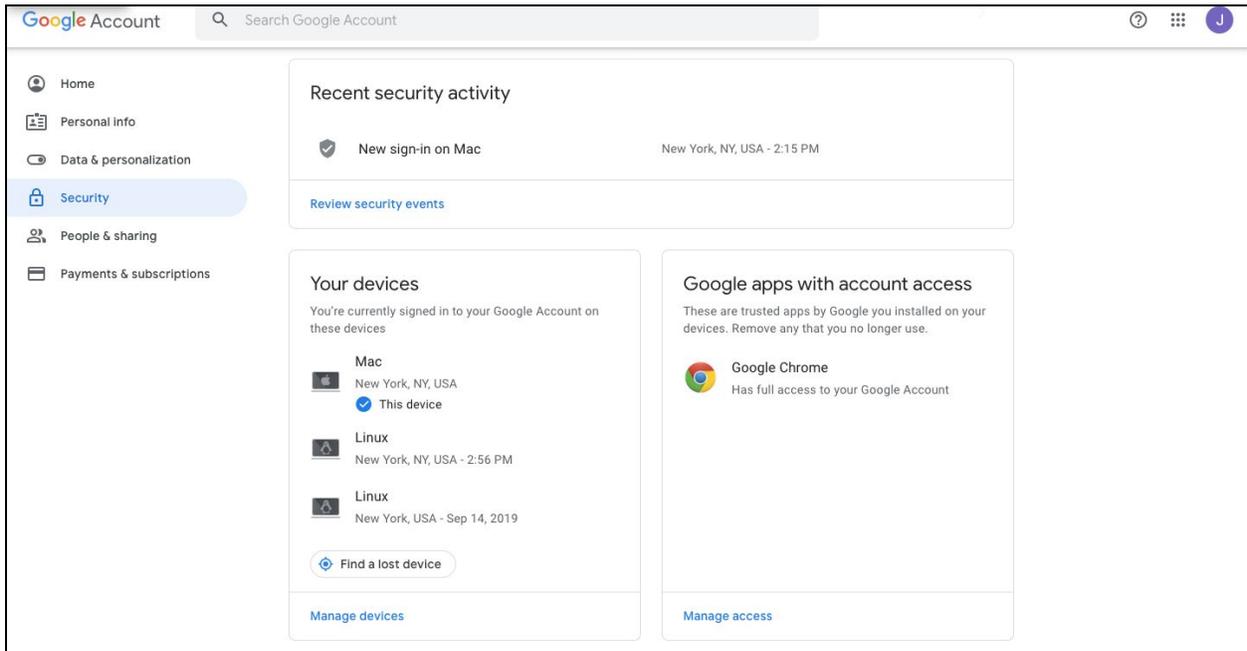


Clicking on **Review security events** will give a screen that should look something like what you see below. Each entry is for a device that has recently logged into the account, and includes information about the device (Google’s best guess about what kind of computer or phone was being used), the time the device logged in, the location, the web browser used, and the IP address. (An IP address is an online identifier that can show approximately where the device was when it logged in.)

Google only shows information about logins during the past 28 days.



Just below *Recent security activity*, you will find a box called *Your devices*:



Check to make sure you recognize all of the devices that are logged in. If you don't recognize one of them or think it belongs to someone else, you can log the device out.

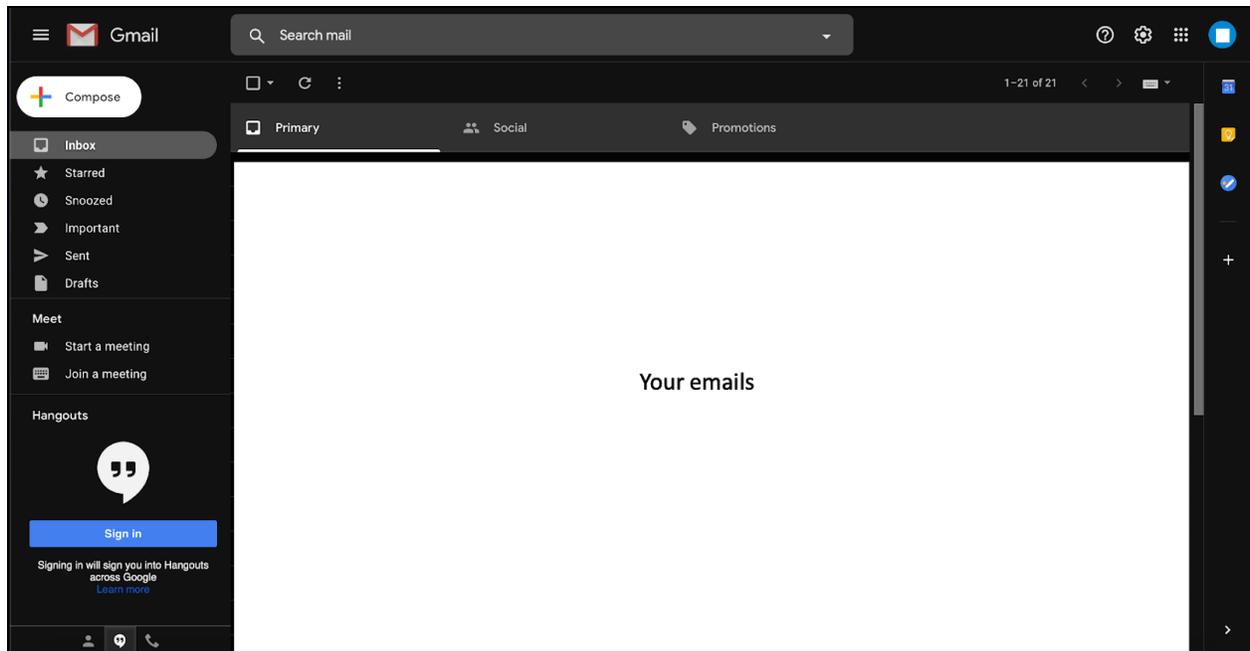


Be careful -- if you log a device out of your account this way, the person who was logged in could realize this immediately.

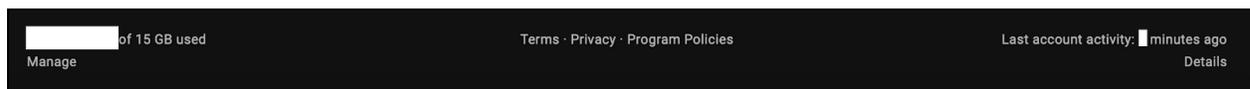
In order to log a device out of your account, click on **Manage devices** inside the *Your devices* box. Then, select the device you want to log out and click **Sign out**.

Another way to check for recent logins is by going to <https://www.google.com/gmail/>

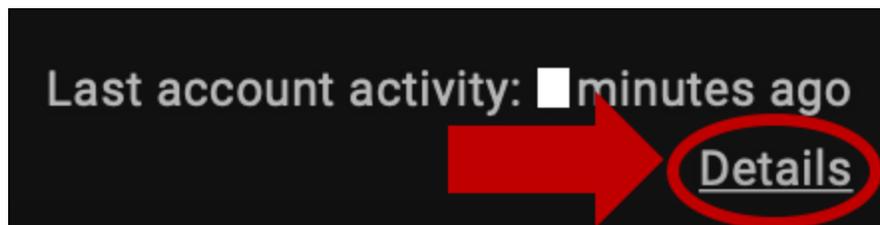
Enter your email address and password. When you log in, you will see something like this:



Scroll down until you see something like this:



Click on **Details** (it appears on the left below *Last account activity*):



A new window will appear:

Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. [Learn more](#)

This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

Visit [Security Checkup](#) for more details

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	Location (IP address) [?]	Date/Time (Displayed in your time zone)
Browser (Safari) Show details	*	3:24 pm (7 hours ago)
Browser (Safari) Show details	*	2:30 pm (8 hours ago)
Mobile		2:29 pm (8 hours ago)
Browser (Safari) Show details		11:01 am (11 hours ago)
Mobile		10:57 am (11 hours ago)
Mobile		10:20 am (12 hours ago)
Mobile		Jul 23 (1 day ago)
Browser (Safari) Show details		Jul 23 (1 day ago)
Browser (Safari) Show details		Jul 23 (1 day ago)
Browser (Safari) Show details		Jul 23 (1 day ago)

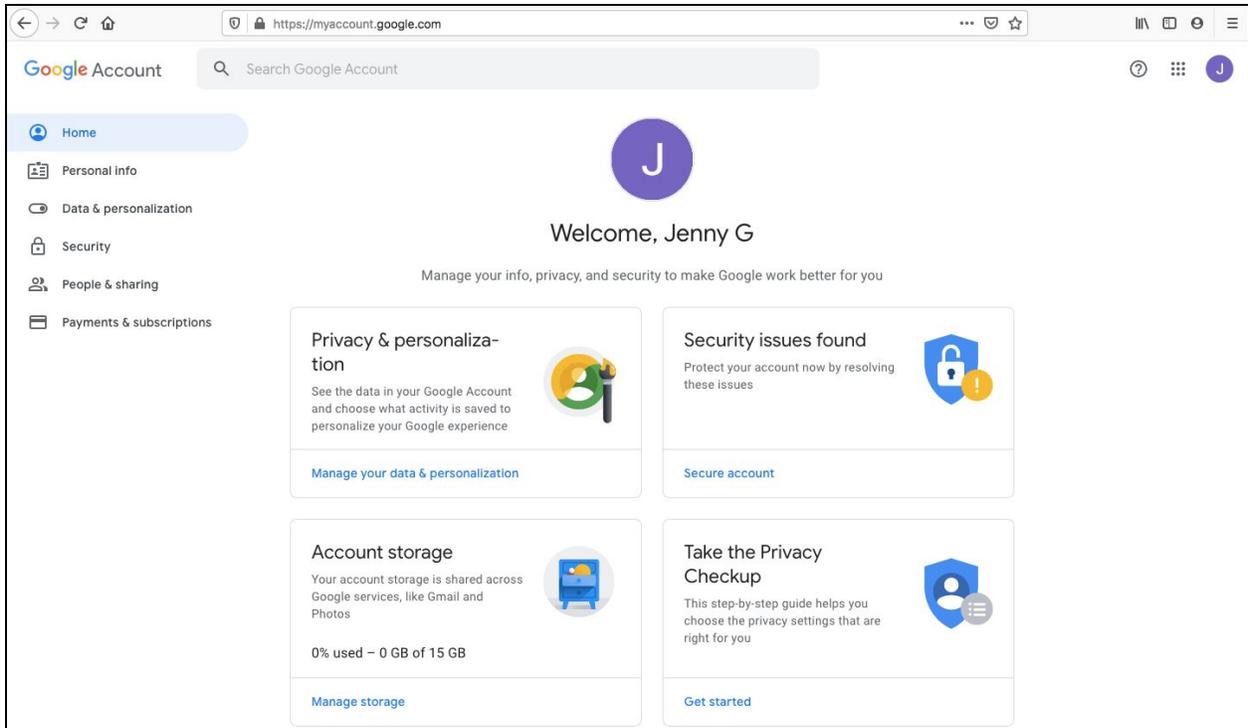
* indicates activity from the current session.

This computer is using IP address

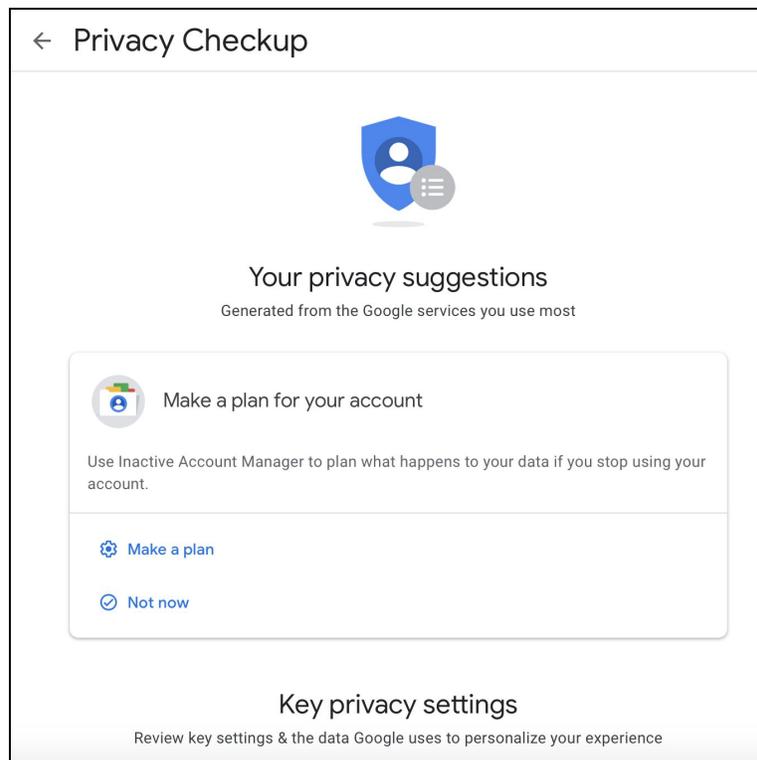
The window will show you recent login information about your Gmail account. The information shown includes: access type (browser or mobile), IP address and country, and date/time.

Step 3: Securing the account

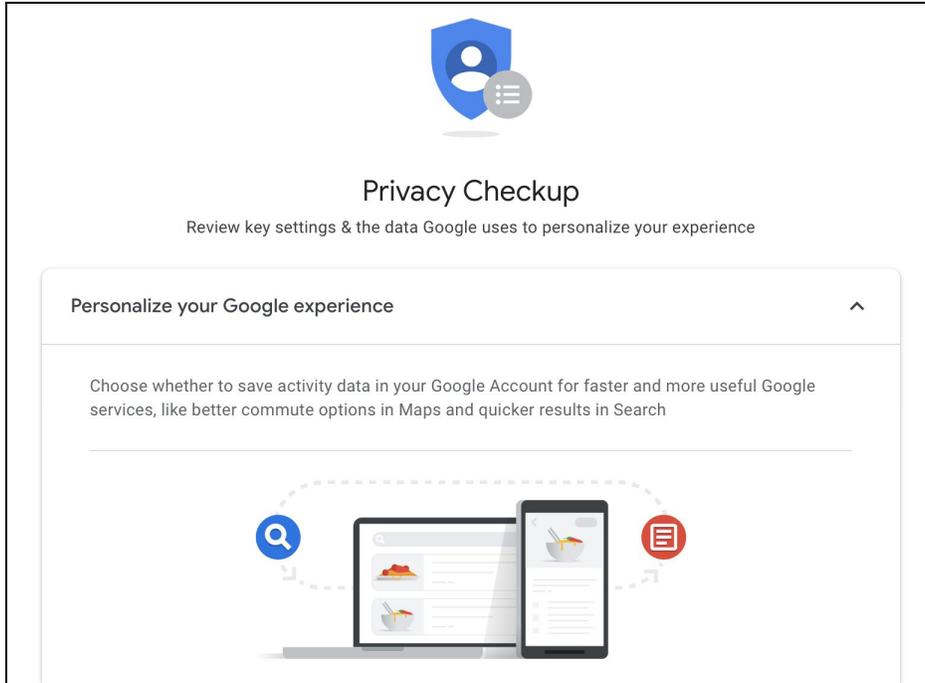
We recommend you to do the **Privacy Checkup** Google offers. In order to access this feature, make sure you are on the following webpage (myaccount.google.com):



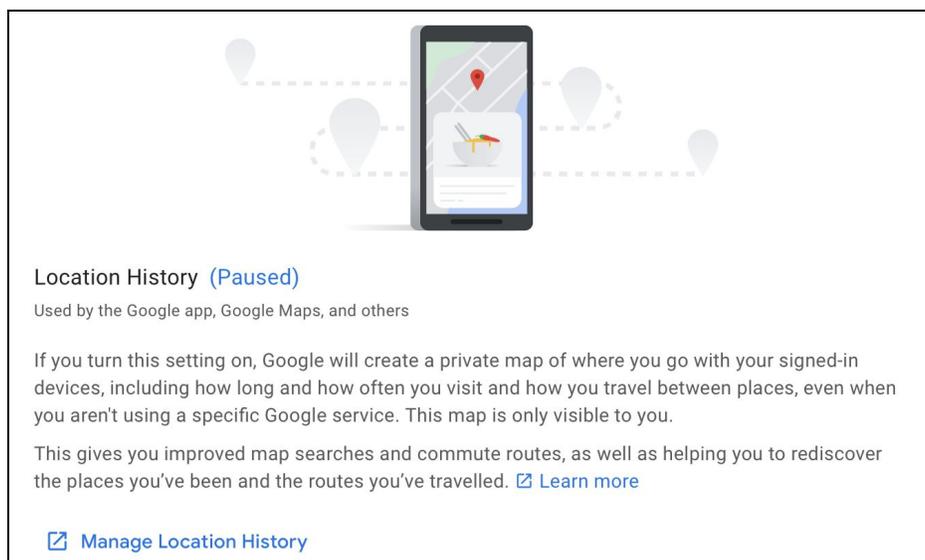
In the *Take the Privacy Checkup* box that appears near the center of the screen, click on **Get started**. You might see something like this:



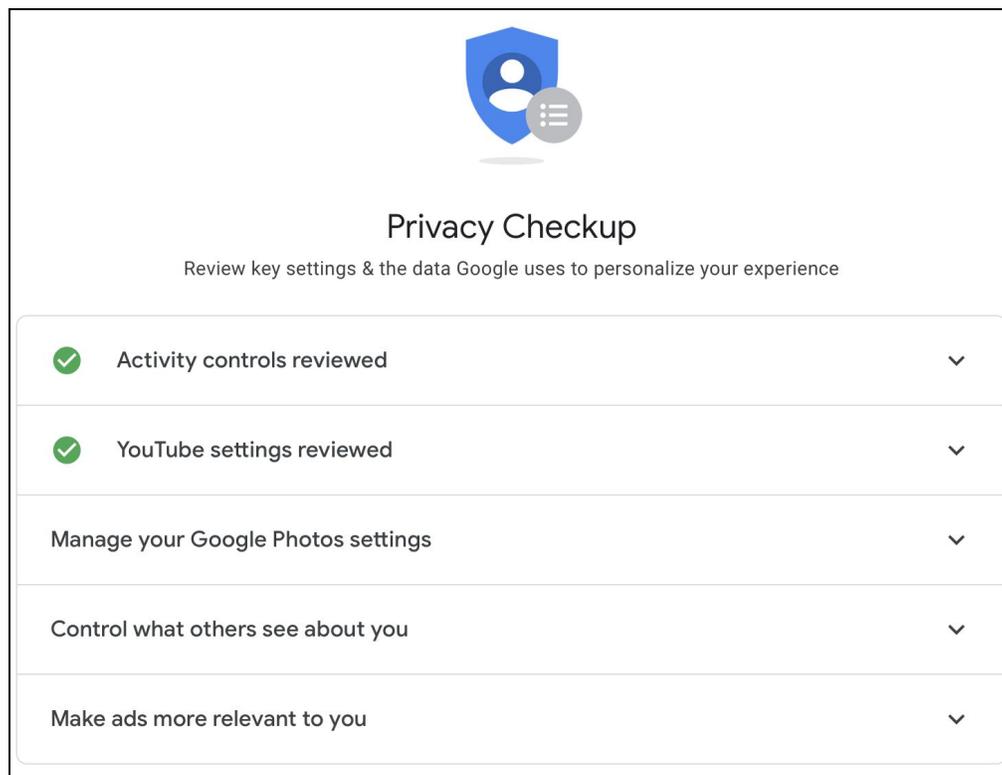
In this page, Google will show you important privacy and security settings you might want to review. For example, in the **Key privacy settings** section, you can stop Google from storing your activity when you browse the Internet (if you use Google Chrome as your web browser) or use Google apps (such as Google Maps):



Inside the step 1 of the Privacy Checkup (Personalize your Google experience), make sure location history is paused if you are concerned about someone else getting access to it (as shown in the next image):



The Google Privacy Checkup will consist of more steps, such as reviewing YouTube and Google Photos settings:

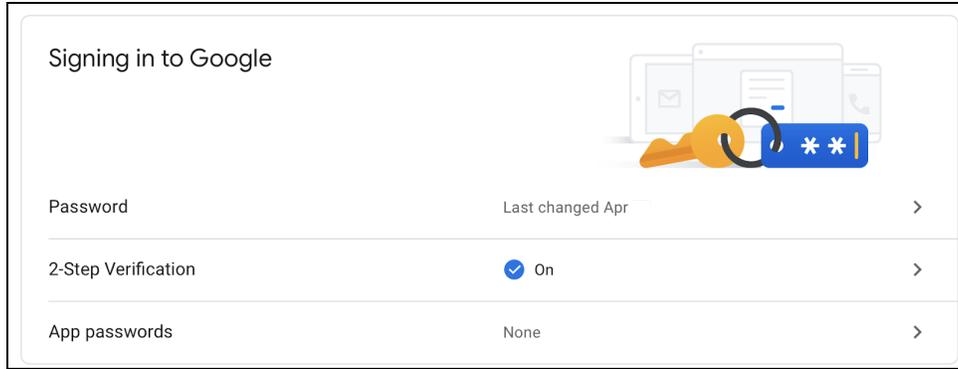


We also recommend turning on two-step verification. Doing this can help keep someone else from signing into your account and seeing your information even if they guess your password. Please see the **Gmail and Google Apps - Turning on Extra Security** guide located at <https://www.ceta.tech.cornell.edu/resources>).

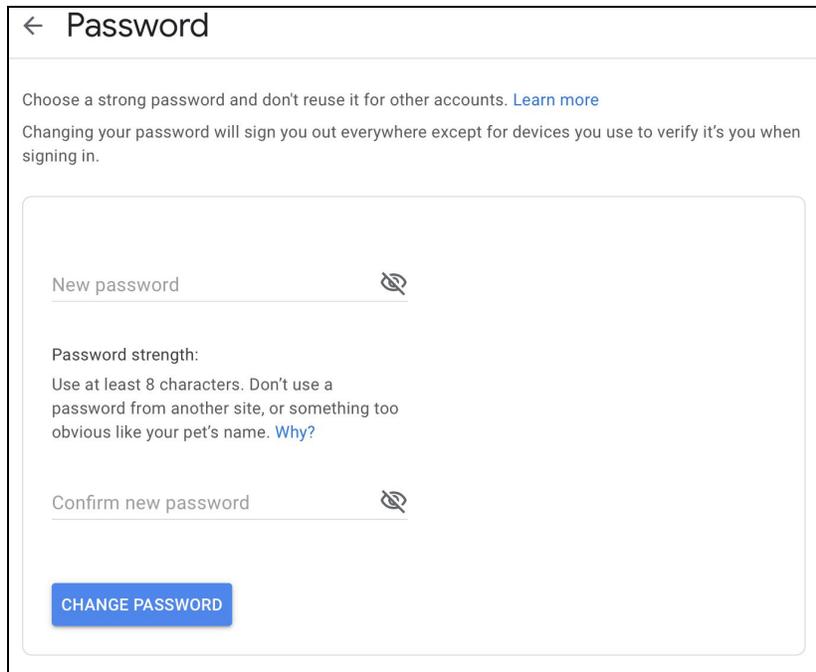
Step 4: Changing your password

In order to change your password, click on this link: <https://myaccount.google.com/security>

You will see something like this:



Click on **Password**. You will be required to enter your current account password to proceed. Then, you will see something like this:



Enter a new password. We recommend choosing a strong password that other people will be unlikely to guess. In particular, we suggest you use:

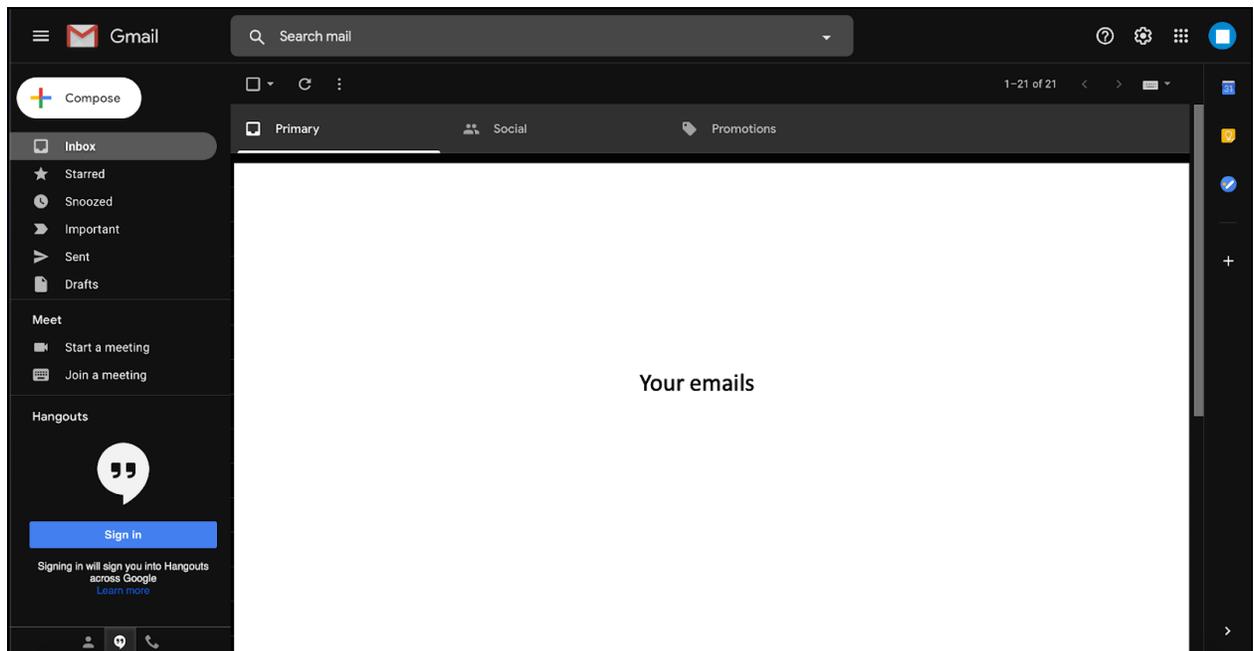
- A mix of capital and lowercase letters,
- Some numbers and symbols (such as &, ?, @, or #),
- A password that is at least 8-12 characters long, and
- A password that doesn't include any words that someone could easily guess, such as your name, children's or pets' names, or birthdays.

Enter your new password again in the **Confirm new password field**. Finally, click on **CHANGE PASSWORD**.

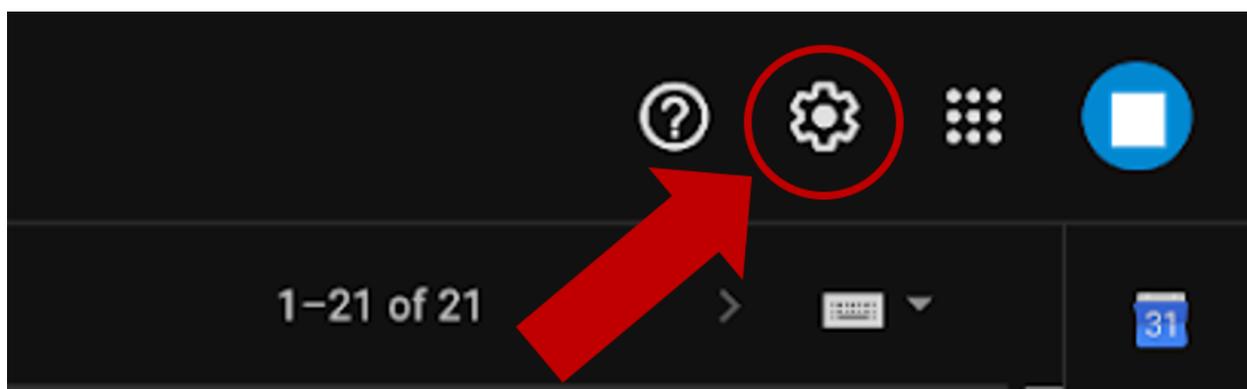
Step 5: Checking if your emails are being forwarded

Go to <https://www.google.com/gmail/>

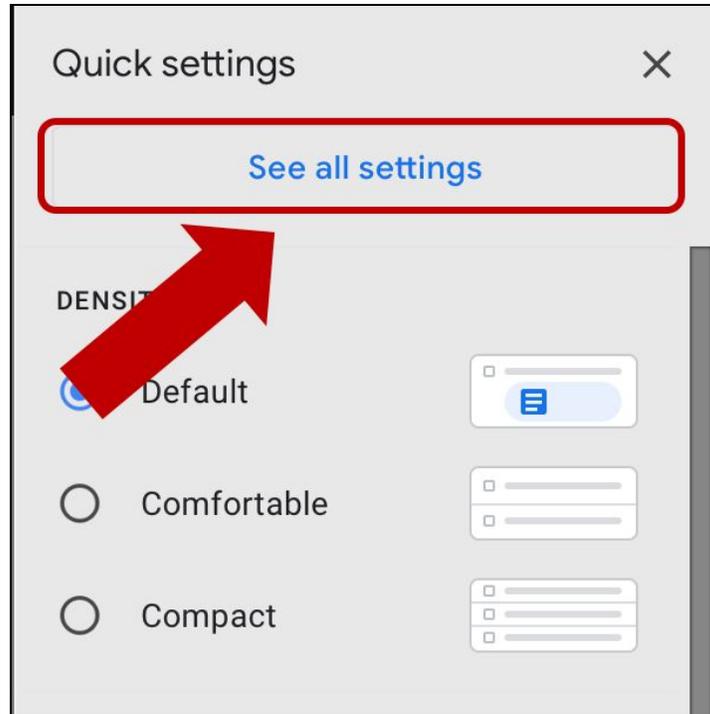
Enter your email address and password. When you log in, you will see something like this:



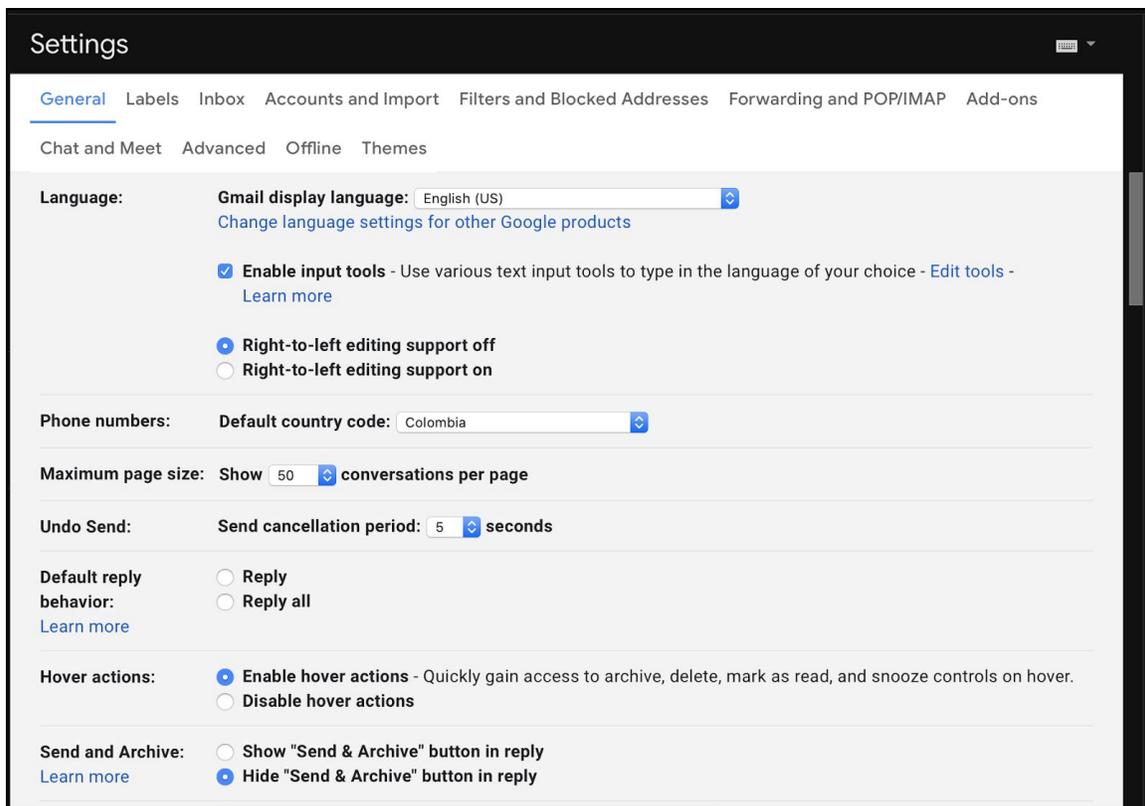
Click on the gear symbol at the top right corner:



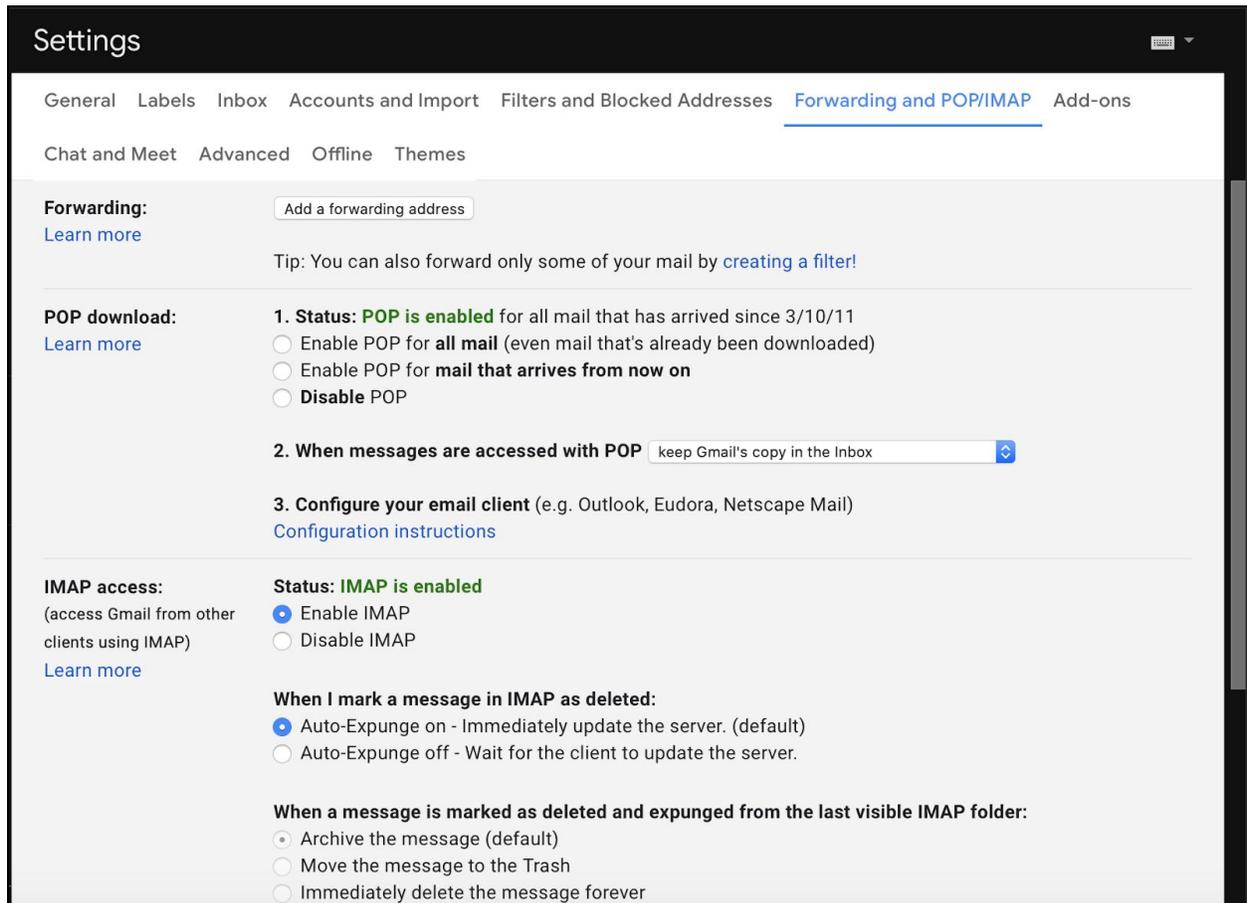
A menu will appear. Click on **See all settings**:



You will see something like this:



At the top, click on **Forwarding and POP/IMAP**. You will see something like this:



Check the **Forwarding** section. Are there any forwarding addresses?

© Cornell Tech 2020. This guide is for nonprofit educational and research purposes only and is not intended for commercial use. Images from Google are included selectively pursuant to the “fair use” provisions of United States copyright law, 17 U.S.C. § 107.