Google/Gmail Account Safety Check

Compiled by the Clinic to End Tech Abuse (CETA)

Last Updated: December 1, 2022

Who is this guide for?
If you have a Google or Gmail account (they are the same) and suspect that your account and/or device has been compromised, this guide will help you review important settings that determine what information is collected, where it is saved, and with whom it is shared. It is particularly oriented towards intimate partner violence threats.

What does this guide cover?
● How to manually check important settings in myaccount.google.com
● How to check important Gmail setting
● Additional steps to take if you have an Android phone
● Additional steps to take if you use Google Chrome
● Other settings in myaccount.google.com

Aspects to take into account
● We strongly recommend that you talk to a domestic violence or other appropriate organization to make plans for your safety if you are worried about violence. Information about safety planning and/or local domestic violence agencies can be found https://thehotline.org.
● Some steps in these guides may, directly or indirectly, notify an abuser of your actions. For example, they may receive an alert that you have changed a password or notice that they can no longer read your messages.

We have marked changes that may notify an abuser with the following sign:

Be careful!
This action could be visible to the abuser

● All images included in this guide are for educational purposes only
Table of Contents

Introduction

Managing Account Access
  Checking Logged In Devices
  Checking Recovery Email and Phone
  Changing your password and turning on two-Step verification (2SV)
    Tips for creating a strong password
    Two-step verification

Checking Location Sharing

Checking Important Gmail Settings
  Checking Gmail forwarding
  Check for unrecognized Gmail filters
  Checking for linked Gmail Accounts
  Reviewing detailed Google login history

More Information for Android Users

More Information for Google Chrome Users

Other Settings in myaccount.google.com

Introduction

Many of the settings this guide will ask you to check are visible within the Google/Gmail general settings website. To access it, follow these steps:

1. Open a web browser and go to https://myaccount.google.com.
2. If you do not see a login form (or if you are not signed in), click on Go to Google Account on the top-right corner.
3. Sign in to your Google/Gmail account (enter your Google/Gmail address, hit enter, enter your password, and hit enter).

![Google Sign-in Screen]

4. After logging in, you will see something like this:

![Google Account Main Screen]

From now on, we will refer to the screen above as the **main Google Account screen**. There are various options on the left. In the following sections, you will be asked to click on some of those options.
Managing Account Access

Checking Logged In Devices

On the main Google Account screen click on **Security** in the left hand side panel:

![Google Account Security Panel](image)

You will see something like this:
Scroll down until you see a box titled **Your devices**:

Your devices
Where you’re signed in

5 sessions on Mac computer(s)

You’re signed in on more devices

Find a lost device

Manage all devices

Click on **Manage all devices**. You will see something like this:
The list will show you the devices in which your Google/Gmail account is currently being used or was used in the last 28 days.

Be careful!
This action could be visible to the abuser

If you see a device that you do not recognize or that you recognize but does not belong to you, you may click on it to see more information and, optionally, remove it. You may want to take a screenshot of any unfamiliar or strange activity before removing it.

### Checking Recovery Email and Phone

On the same screen that shows devices logged into your Google account, scroll up slightly until you see a box that says “Ways we can verify it's you” as in the image below.

![Ways we can verify it's you](image)

You can have multiple phone numbers and addresses registered; click on the arrow circled in red on the image below to see all phone numbers and emails associated with your account.

**Important:** removing an email address or phone number may send an alert notification to that phone or email. This action is highly visible.

Be careful!
This action could be visible to the abuser
Whoever controls the email addresses and phone numbers listed here can use them to reset the password to your account, even if they don't know the current password, so it is important to make sure that the information here belongs to you and to remove any phone numbers or email addresses that are not in your control.

**Changing your password and turning on two-Step verification (2SV)**

Scroll up from “Ways we can verify it's you” until you see a box titled **Signing in to Google**:  

Select **Password**. You may have to enter your current password.
Be careful!
This action could be visible to the abuser

Keep in mind that changing your password might log out all other devices that are currently logged into your Google account, even the ones that belong to you.

Tips for creating a strong password
- At least 8-12 characters long
- Includes capital and lowercase letters
- Includes random numbers
- Includes some symbols such as !, ?, @, and $
- Do not use words or numbers that could be easy for someone to guess, such as a child’s name, pet’s name, or birthday

Keep your passwords in a safe, secure location, either written down on paper, or in a password manager if you are the only one with physical access to your device.

Two-step verification
Two-step verification (2SV), also called Two-factor authentication, is a security feature to prevent other people from accessing your account, even if they know or guess your password. After someone enters their password to a Google account, 2SV will send a notification such as text message or a pop-up notification to a trusted phone or computer, alerting them that someone is trying to log in to the account, and ask them to approve or reject the log-in attempt.

Be careful!
This action could be visible to the abuser

In the same box labeled Signing into Google, click on 2-Step Verification (below Password). You may have to enter your Google account password again. After, you will see something like this:
Alternatively, Google will show you some information about 2-Step Verification and how to turn it on.

If you decide to turn on 2-step verification for your Google/Gmail account, you can choose how you would like Google to send you the extra information required for you to log in. There are various options. One of them is **Google prompt**:

<table>
<thead>
<tr>
<th>Google prompts (Default) ☑</th>
</tr>
</thead>
<tbody>
<tr>
<td>To receive Google prompts, just sign in to your Google Account on your phone.</td>
</tr>
<tr>
<td>After you enter your password on a new device, Google will send a prompt to every phone where you’re signed in. Tap any one of them to confirm.</td>
</tr>
<tr>
<td>You’re currently signed in on these devices that support prompts.</td>
</tr>
<tr>
<td>Your Google prompt devices</td>
</tr>
</tbody>
</table>

If you decide to use Google prompt, and you have a Google app (e.g, Gmail or YouTube) on your phone and are logged in, then every time you log into your Google/Gmail account Google will tell you to open a Google app on your phone and accept a prompt that will appear on the app as soon as you open it.
You can also choose to receive a security code required to log in via an app like Google Authenticator or via a voice or text message:

Moreover, Google allows you to generate backup codes that you can use to log in or set up a security key (e.g., a YubiKey):

Using a security key, Google prompt or an authenticator app like Google Authenticator is considered more secure than receiving 2-step verification codes via SMS.

At the bottom of the page, you will see this box:
Google will show you the devices you trust (i.e., devices in which 2-step verification is not needed). There is an option that allows you to revoke the trusted status from those devices.

**Checking Location Sharing**

On the main Google Account screen, click on **Data & privacy** from the left hand side menu:
You will see something like this:

![Google Account Data & Privacy](image)

Scroll down until you see a section titled **Info you can share with others**:

![Info you can share with others](image)

Click on **Location Sharing**. You will see something like this:
Anyone who is listed here may see your real-time location, especially if you use Google Maps to navigate or use Gmail on your mobile device. Review who, if anyone, can see your location.

Be careful!

This action could be visible to the abuser

You may remove someone from seeing your location on this screen by tapping "stop" next to their name.
Checking Important Gmail Settings

On the main Google Account screen click on the following icon near the top-right corner:

A menu will appear:

Click on Gmail. You will see something like this:
Click on the **gear icon** that appears near the top-right corner:

![Gear Icon](image)

A menu will appear:
Click on **See all settings**. You will see something like this:

### Settings

**Main menu:**
- New view - Use mail, Chat, Spaces, and Meet in their own streamlined view
- Original view - Use mail, Chat, Spaces, and Meet all in one view

**Language:**
- Gmail display language: English (US)
- Change language settings for other Google products
- Enable input tools - Use various text input tools to type in the language of your choice - Edit tools - Learn more
- Right-to-left editing support off
- Right-to-left editing support on

**Phone numbers:**
- Default country code:

**Maximum page size:**
- Show 90 conversations per page

**Undo Send:**
- Send cancellation period: 5 seconds

**Default reply behavior:**
- Reply
- Reply all

**Hover actions:**
- Enable hover actions - Quickly gain access to archive, delete, mark as read, and snooze controls on hover.
- Disable hover actions

**Send and Archive:**
- Show "Send & Archive" button in reply
- Hide "Send & Archive" button in reply

**Default text style:**

### Checking Gmail forwarding

Click on the **Forwarding and POP/IMAP** tab. You will see something like this:

### Settings

**Forwarding:**
- Add a forwarding address
- Tip: You can also forward only some of your mail by creating a filter!

**POP download:**
1. Status: **POP is enabled** for all mail that has arrived since 3/10/11
   - Enable POP for all mail (even mail that’s already been downloaded)
   - Enable POP for mail that arrives from now on
   - Disable POP
2. When messages are accessed with POP - keep Gmail's copy in the Inbox
3. Configure your email client (e.g. Outlook, Eudora, Netscape Mail)
   - Configuration instructions

Check that only recognized, approved accounts appear next to **Forwarding**.

16
Be careful!
This action could be visible to the abuser

If you don’t recognize an email address next to forwarding, then you can delete it on this page.

Check for unrecognized Gmail filters

Next, click on the Filters and Blocked Addresses tab at the top of the Settings screen. You will see something like this:

![Settings](image)

Filters set up without your knowledge can explain missing email or deleted emails. Check that there are only recognized and approved filters set up for your account.
Checking for linked Gmail Accounts

Now, click on the **Accounts and Import** tab. You will see something like this:

![Settings Page](image)

Check that only approved email accounts appear on this page. In particular, check the **Grant access to your account** section.

![Be careful!](image)

This action could be visible to the abuser

If you do not recognize an account that has been granted access to your account, you can remove it by clicking delete.

**Reviewing detailed Google login history**

Finally, on the current page scroll down until you see this:
Click on **Details**. A new window will appear:

This window will show you detailed information about recent logins on your Gmail account, including IP addresses. It is not uncommon to see many log-in entries on this page, even if you are the only person logged into your account. For example, if your phone refreshes your email to check if you received any new mail, then it also includes a “log-in” entry for each refresh. However, this information can be very useful if you do find unrecognized activity in your account.

---

**More Information for Android Users**

If you have an Android phone, we recommend that you visit [our Android Safety Guide](#) on our resources page.

**More Information for Google Chrome Users**

If you use Google Chrome, we recommend that you visit [our Google Chrome Safety Guide](#) on our resources page.
Other Settings in myaccount.google.com

Google has privacy and security checkups in myaccount.google.com. These checkups will show you some recommendations for your account. These check ups are geared towards general Internet safety, such as tracking by corporations from websites that you visit or advertisers; other than the settings reviewed in this guide, they are often not relevant to intimate partner violence threats.

On the main Google Account screen click on the search bar that appears at the top, type Security Checkup, and click on the first suggested option:

In order to access the Google Account Privacy Checkup on the main Google Account screen click on the search bar that appears at the top, type Privacy Checkup, and click on the first suggested option:

© Cornell Tech 2022. This guide is for nonprofit educational and research purposes only and is not intended for commercial use.