

Guide to securing your Google account

If technology is being used against you, use this website to secure your tech.

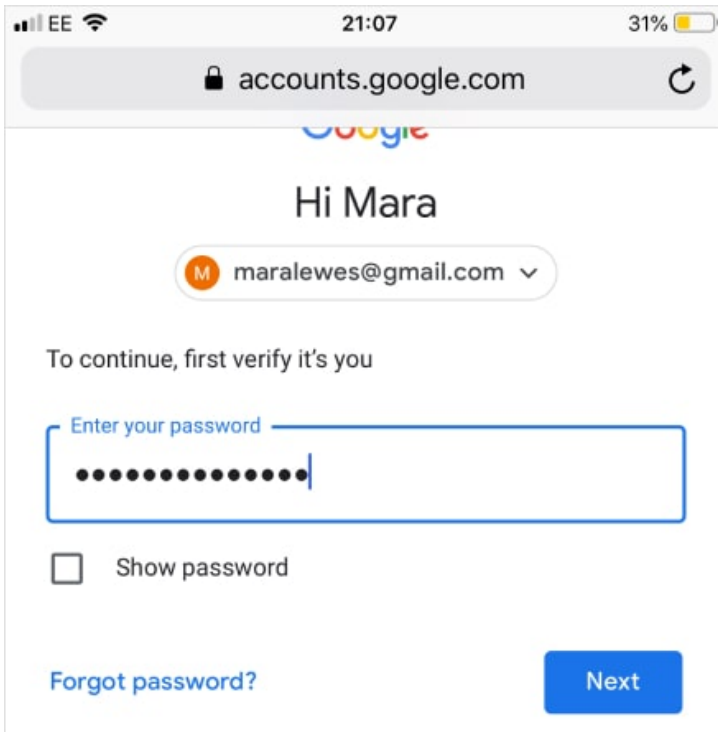
Note that depending on your [device/updates](#), the steps below may vary.

Caution: Remember, depending on whether or not you are living with the person who is harming you, you may choose to take different steps. Control and coercion make some of these steps impossible or not safe. Read these cautions before taking action.

Secure your tech

Step 1: Log into your Google account

1. Go to myaccount.google.com in your [browser](#).



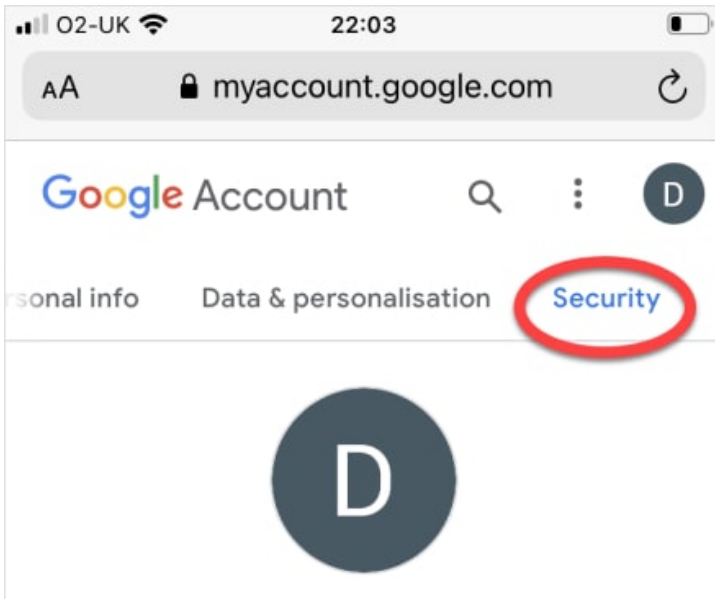
1. If asked, enter your Google **username and password**. Your [username](#) is the first part of your email before **@gmail.com**.

You can also log on through an android device. Open the [Settings app](#), then tap [Google](#), and manage your [Google account](#).

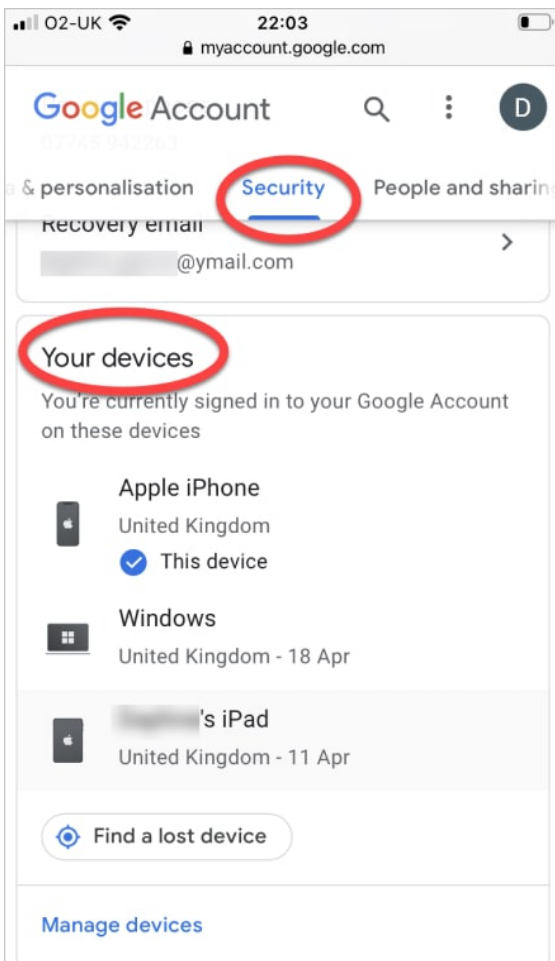
Step 2: Check devices signed in to the account

[Learn more about access logs.](#)

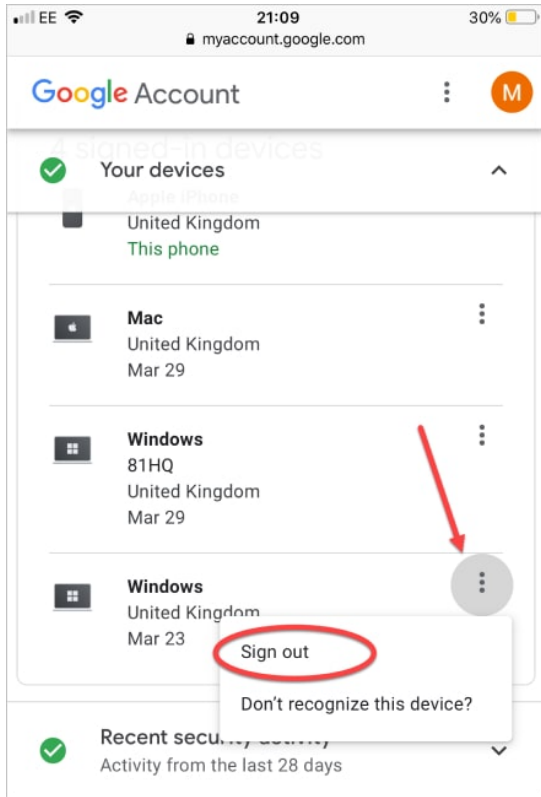
1. Choose **Security** from the menu.



2. Find **Your Devices** and review the devices logged into your account.



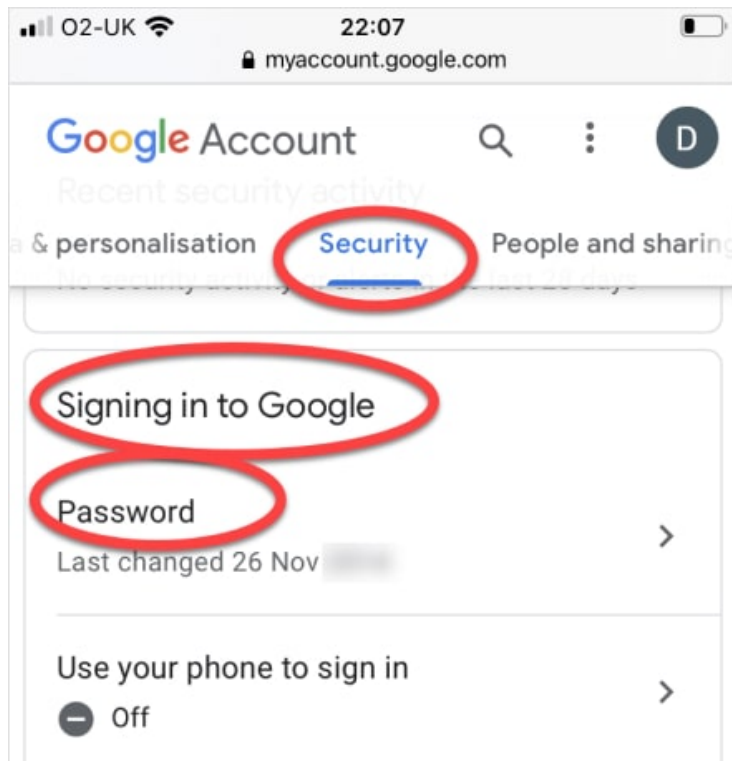
3. Remove any unwanted devices. **Caution:** A notification will be sent to other devices signed into the account. Some abusers may escalate their violence.



Step 3: Change your password

1. Choose **Security** from the menu.

2. In **Signing in to Google** choose **Password**.



3. Verify your old password, and then set a new password. **Caution:** No notification will be sent but someone would know that the access had been removed when they tried to regain access to the account. Some abusers may escalate their violence.

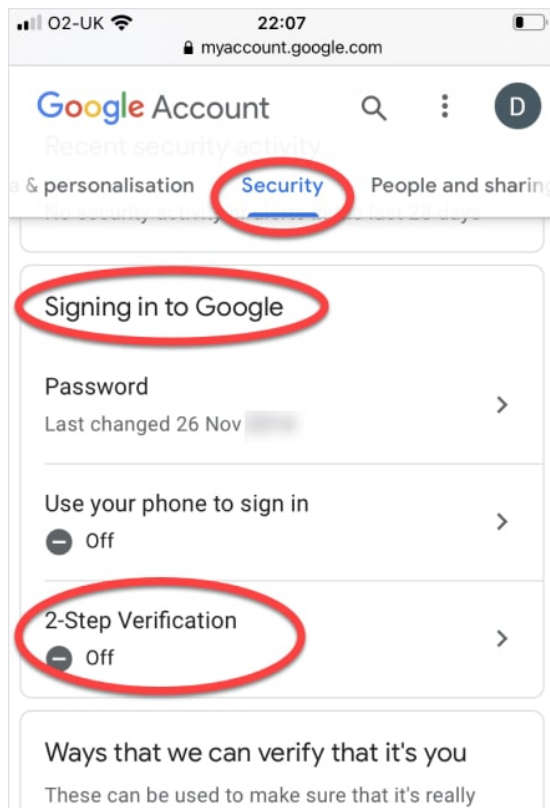
You can also use [Google's security checkup tool](#). This might also say "Critical security issues found" or "We keep your account protected."

Step 4: Set up Two-Factor Authentication

1. **Complete the previous step before** setting up 2-step verification, as other devices signed in to the account will receive

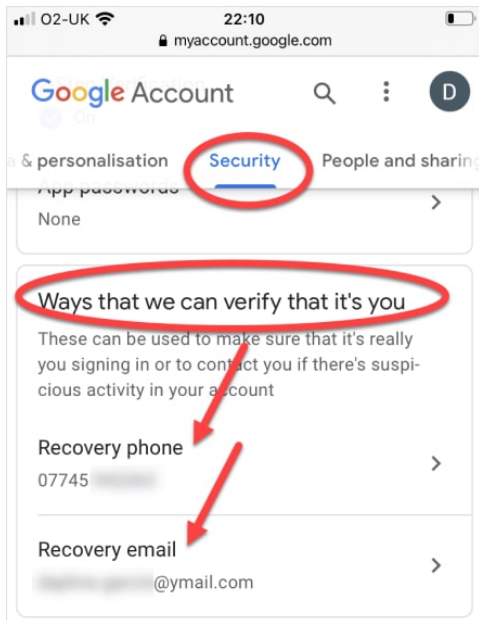
notifications each time you sign in. [Learn more about two-step verification.](#)

2. Choose **Security** from the menu.
3. In **Signing in to Google** choose **Two-Factor Authentication**.
4. Verify your password.
5. Choose how you want to set up 2-step. The most common choice is your phone, but you can also choose a text message or phone call, [or a security fob \(less common\).](#)
6. Choose a **backup option**. If you used your phone for 2-step, the backup would be a text message or phone call. You can also use **one-time backup codes** which you'll have to save somewhere safely.

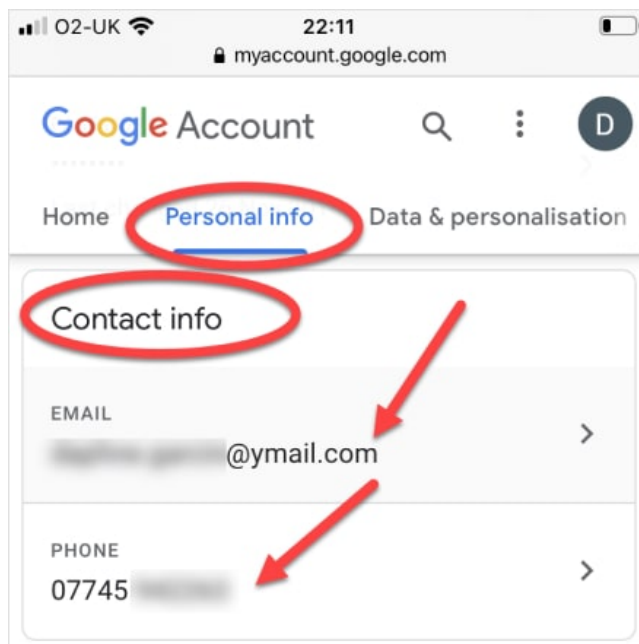


Step 5: Check recovery email and phone numbers

1. Choose **Security** from the menu.
2. Go to **Ways we can verify it's you**.



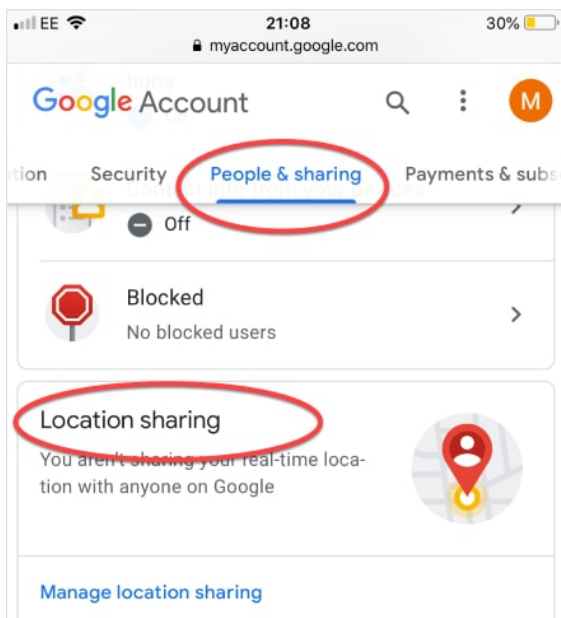
3. Review the recovery emails and phone numbers listed. Make sure the information is correct and remove any unwanted emails or phone numbers.
4. Next, choose **Personal Info** from the menu.



5. Review the emails and phone numbers listed in **Contact Info**. Make sure the information is correct and remove any unwanted emails or phone numbers.

Step 6: Check location sharing

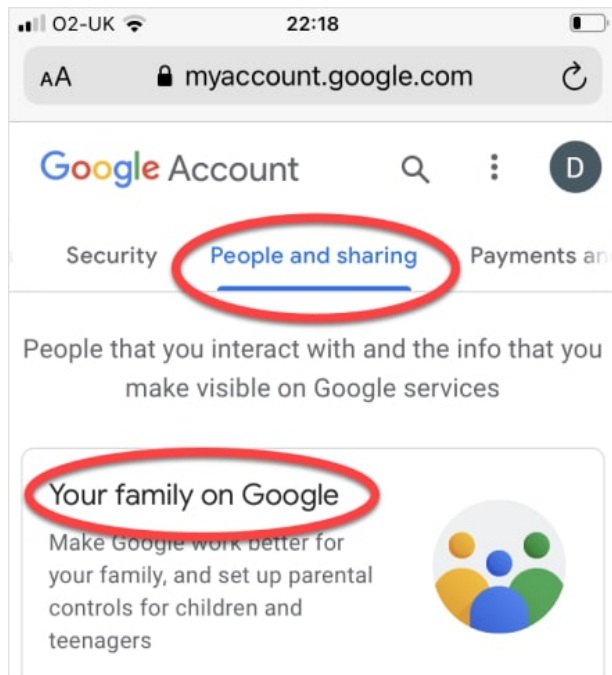
1. Go to **People and Sharing**.



2. Go to **Location Sharing** and review any contacts who can see your location. Remove any unwanted sharing. You can also temporarily pause sharing your location.
3. You may also want to turn off Find my phone. In your phone / device's **Settings** app, tap **Google** then tap **Security**, and then **Find my device**. Tap the slider until it is on the 'off' position. **Caution:** No notification will be sent, however the abuser may notice that they can no longer see your phone's location. Some abusers may escalate their violence.

Step 7: Check family link

1. Choose **People and Sharing** from the menu.
2. Go to **Your family on Google** and review who is in your family group.

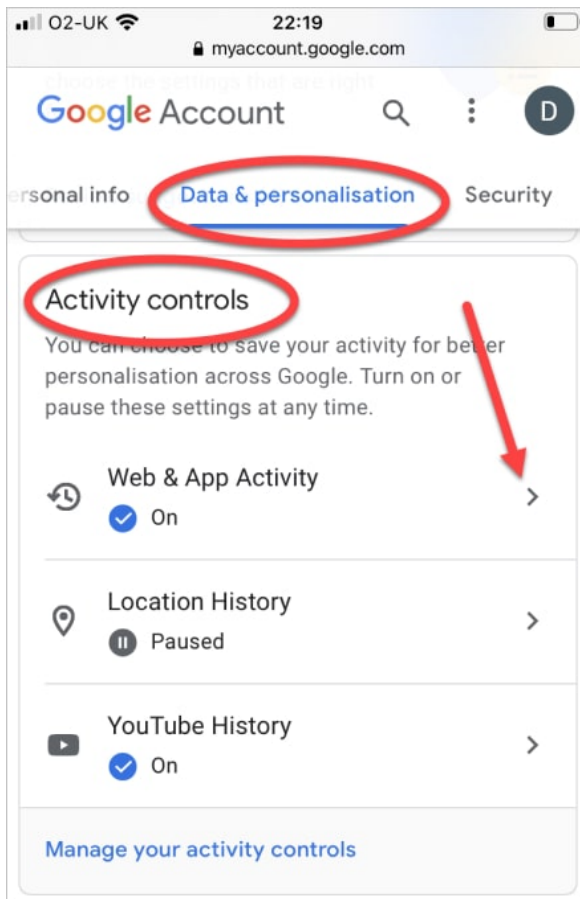


3. If you are the **Family Manager**, you can remove members. If you are the member of a family group, you can leave the group. **Caution:** A notification will be sent by email to those you remove. Some abusers may escalate their violence.

Family link allows someone set up as a “parent” to manage members who are set up as “children.” This includes resetting passwords, blocking emails, limiting websites, and more. It does not automatically give access to emails, location, and web or YouTube history. Anyone who has the password for the “child” account can access that information.

Step 8: Check Activity and timeline

1. Choose **Data and personalization** from the menu.
2. Go to **Activity controls** to review your history settings for location, web & app activity, and YouTube viewing history.

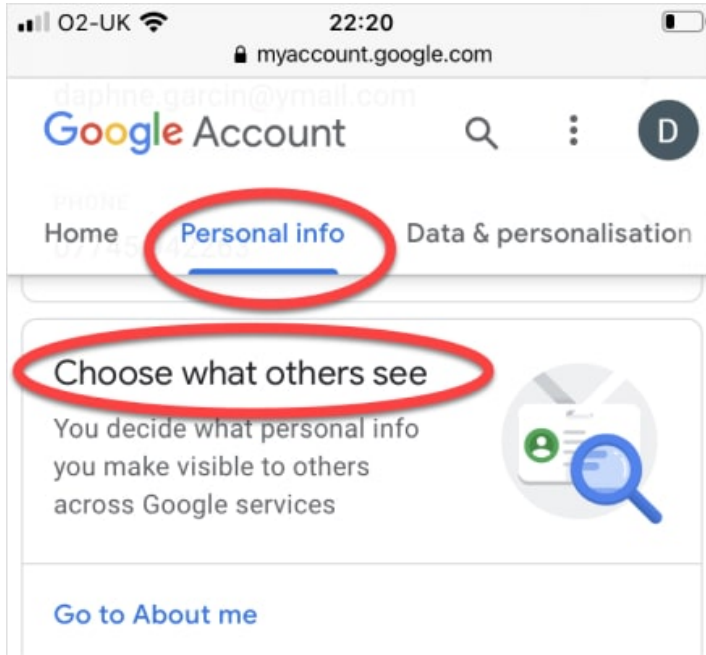


3. You can pause or turn each of these on or off, and you can review and delete selected items or set the history to automatically delete after a set time. **Caution:** If someone else is reviewing your history, it might seem suspicious if it has all been deleted. Some abusers may escalate their violence.

You can also use *Google's privacy checkup tool*, which might say "Privacy suggestions available."

Step 9: Check your personal information

1. Choose **Personal info** from the menu.



2. Go to **Choose what others see** and review what information is visible to anyone, or just to you. Adjust any items to increase your privacy.