Gmail - Turning On 2-Step Verification (Extra Security)

Compiled by the Clinic to End Tech Abuse

Last Updated: April 17, 2020

What is 2-step verification and what does it do?
It is an extra security step that provides more protection for an online account. By turning it on, every time you try to log into your account, you will be required to provide a password as well as a second piece of information such as a code that only you should know.

Who is this guide for?
Anyone who would like to strengthen their security and privacy on Gmail. It is especially for anyone who is concerned that an abusive person may be secretly getting access to their account.

You can also look at Google's own guide here: https://support.google.com/accounts/answer/185839?co=GENIE.Platform%3DDesktop&hl=en.

What does this guide cover?

- How to turn on 2-step verification, an extra layer of security for your Gmail account.
- How to choose among different 2-step verification methods to protect your account.

Before we start:

- If the abuser has access to your account, they may know right away if you turn on 2-step verification. Turning on 2-step verification will lock other people out of your account even if they know the password.
- We strongly recommend that you talk to a domestic violence or other appropriate organization to make plans for your safety before you turn on 2-step verification if you are worried about violence or threats.
- We have marked changes that could be visible to an abuser with the following sign:

Be careful!

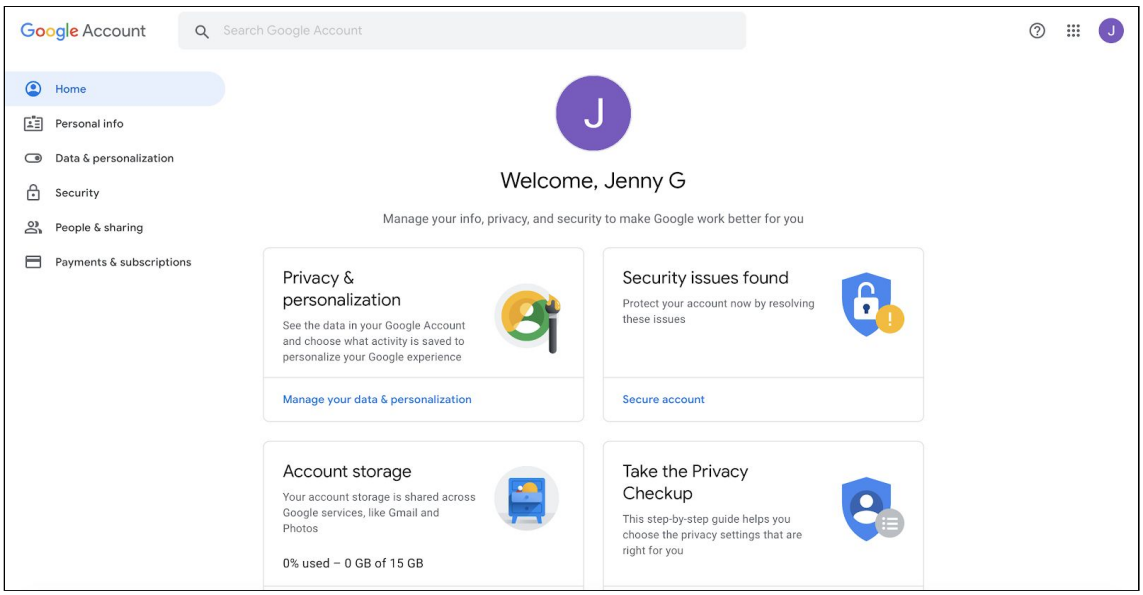
This action could be visible to abuser

- You will need to be able to log into your Gmail account.
- It will help if you know whether you have already turned on 2-step verification. For example, after you enter your password, do you also have to enter a code?

Images of the Google Account website are included below for educational and research purposes only.

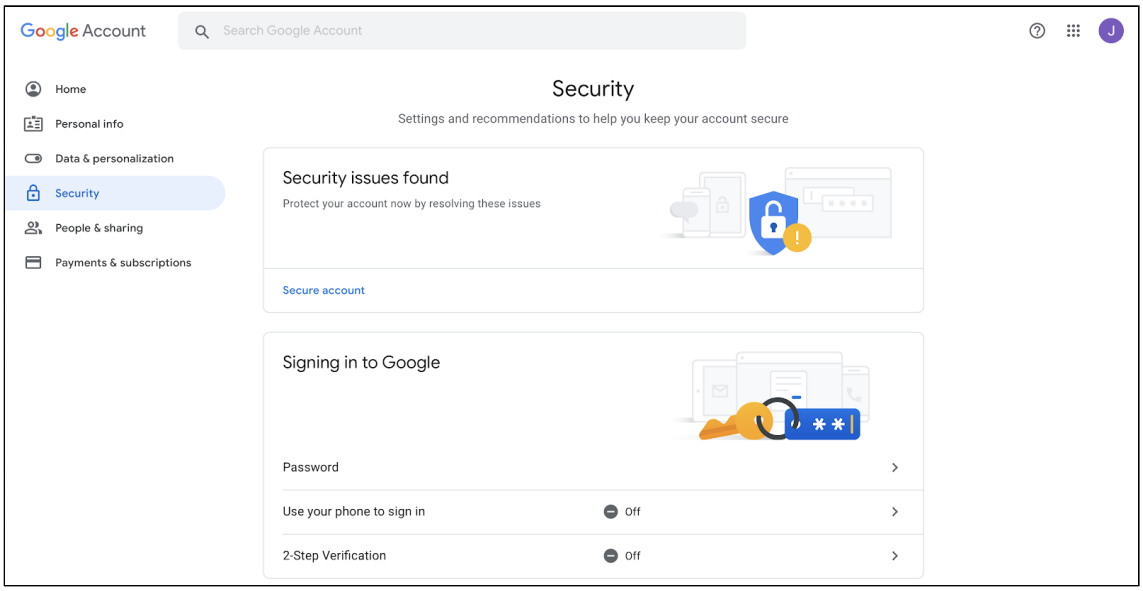
Step 1 - Log into your Google Account

Log into your Google account at https://myaccount.google.com. You should see a webpage that looks like the following:



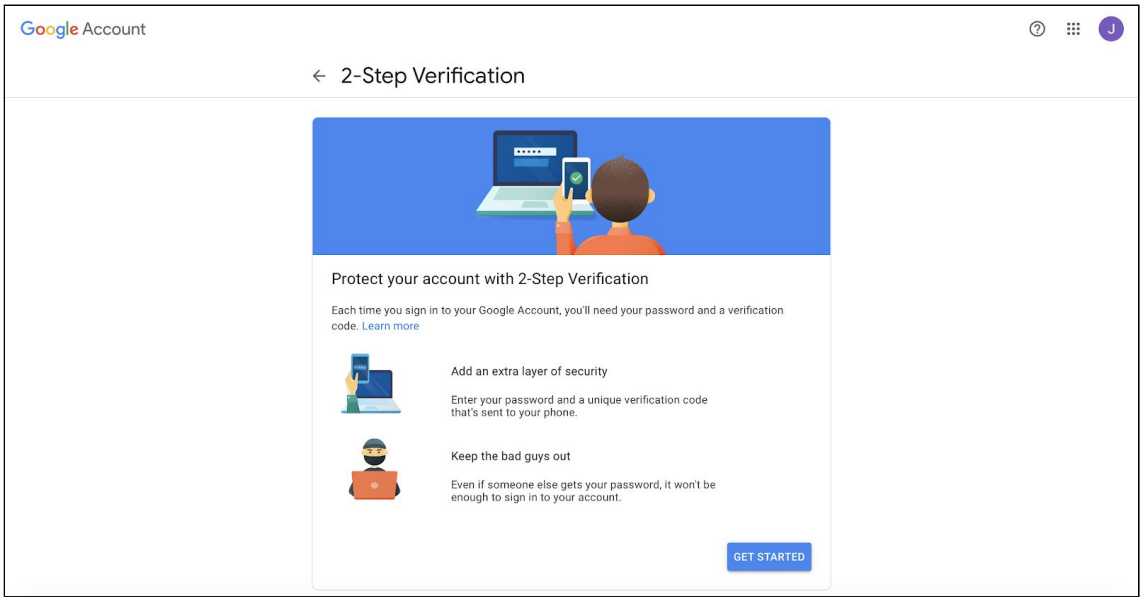
Step 2 - Go to *Security*

Click on **Security** from the left menu. You should see a webpage like the following:



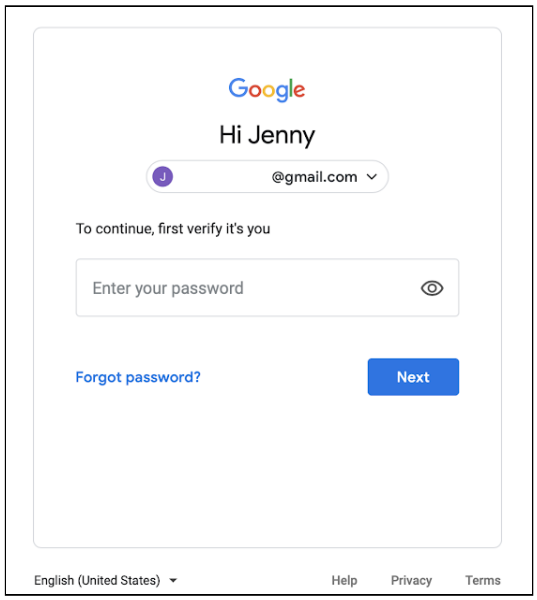
Step 3 - Enter the *2-Step Verification* section

Inside the **Signing in to Google** section, you will find a row titled **2-Step Verification**. Click on that row. You should see a website like the following:



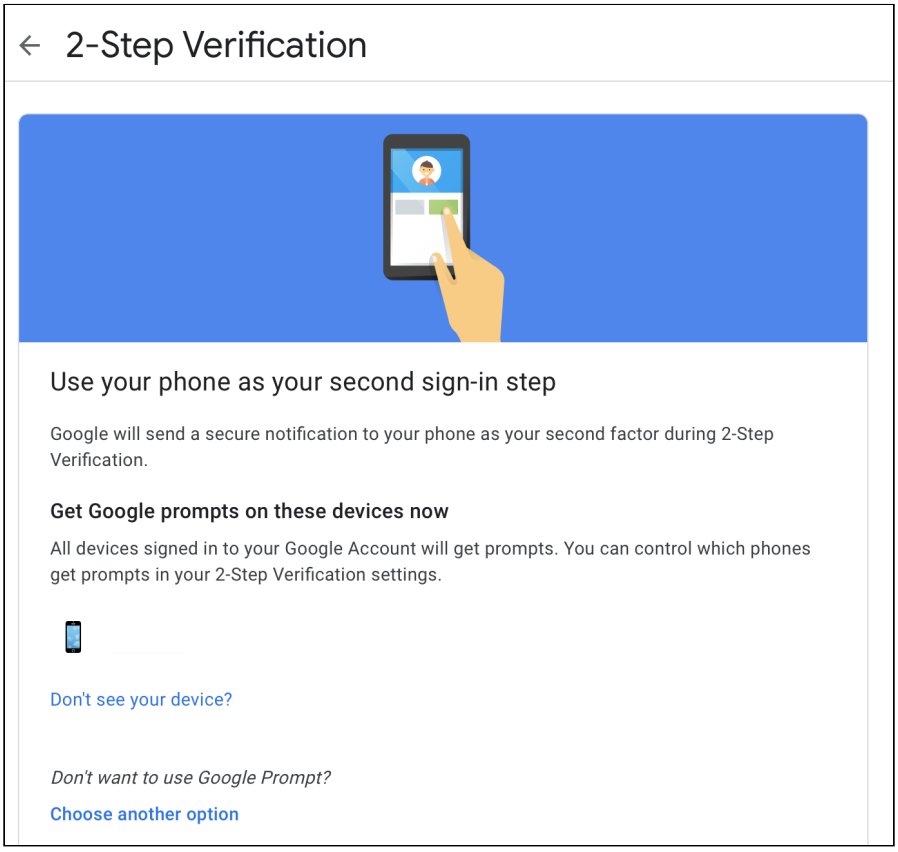
Click on the blue **GET STARTED** button near the bottom.

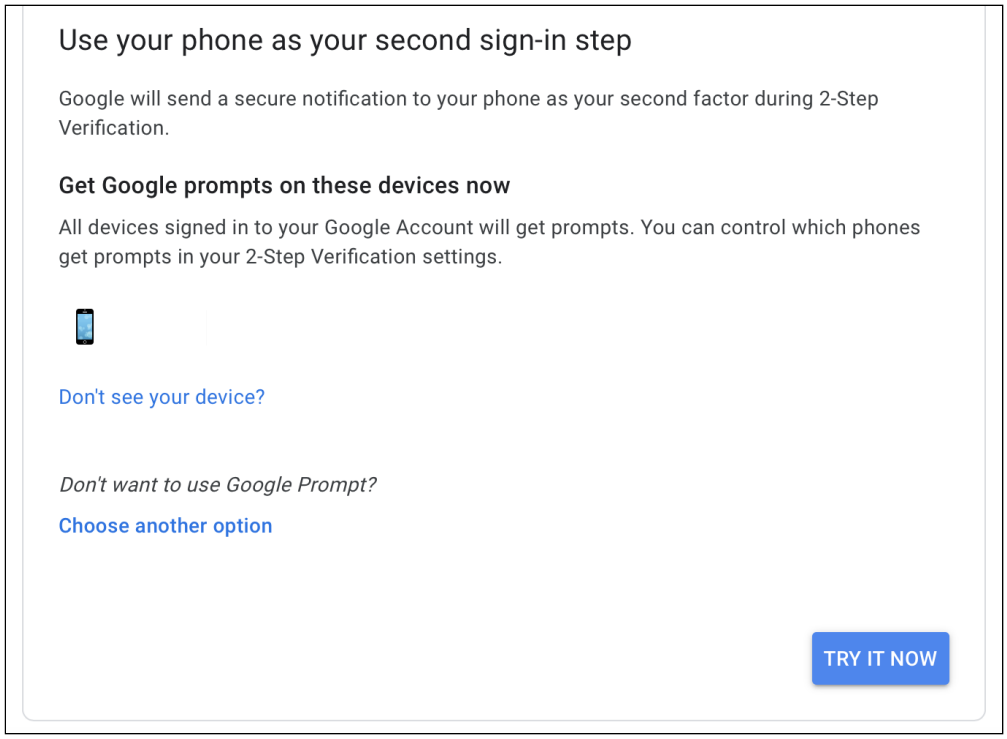
Then, you will be taken to a webpage in which you have to enter your Google account password:



Step 4 - Enable 2-Step Verification

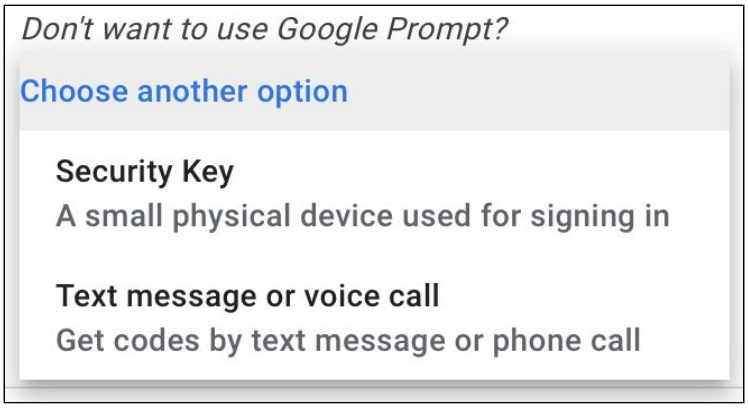
After entering your Google account password and clicking on **Next**, you should see a webpage like the following:





This website suggests that you use **Google Prompt** as the second factor to sign in to Google services like Gmail. If you select this option by clicking on the **TRY IT NOW** button, Google will send your registered devices a prompt you have to accept to have access to your account. To see your registered devices, check the list of devices that appears on this page.

Alternatively, you could click on **Choose another option**:



Be careful!

This action could be visible to abuser

In the following pages (after the **Staying safe** section), you will find 3 paths, one for each of the options shown above (**Google Prompt**, **Text message or voice call**, and **Security Key**) to configure 2-step verification.

Staying safe

Using 2-step verification can help keep the abuser from getting access to your private Gmail or Google information. Even if they know your password, they will not be able to get in unless they also know the extra code, which will change every time you log in.

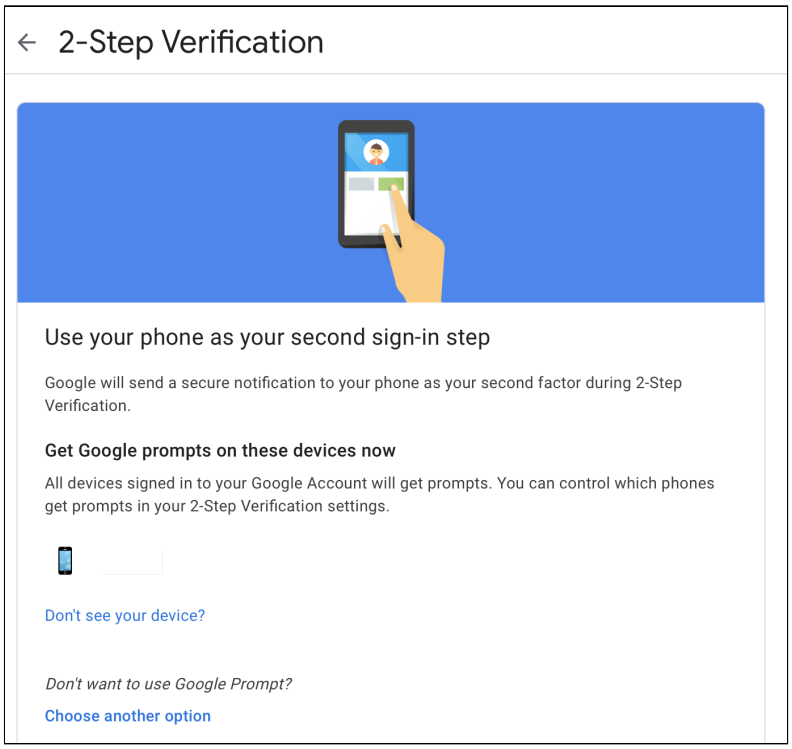
But if the abuser has been going into your Gmail or Google account, they might realize right away that they can no longer get in. If you think this could make them become more dangerous, we urge you to contact an organization that helps abuse survivors first.

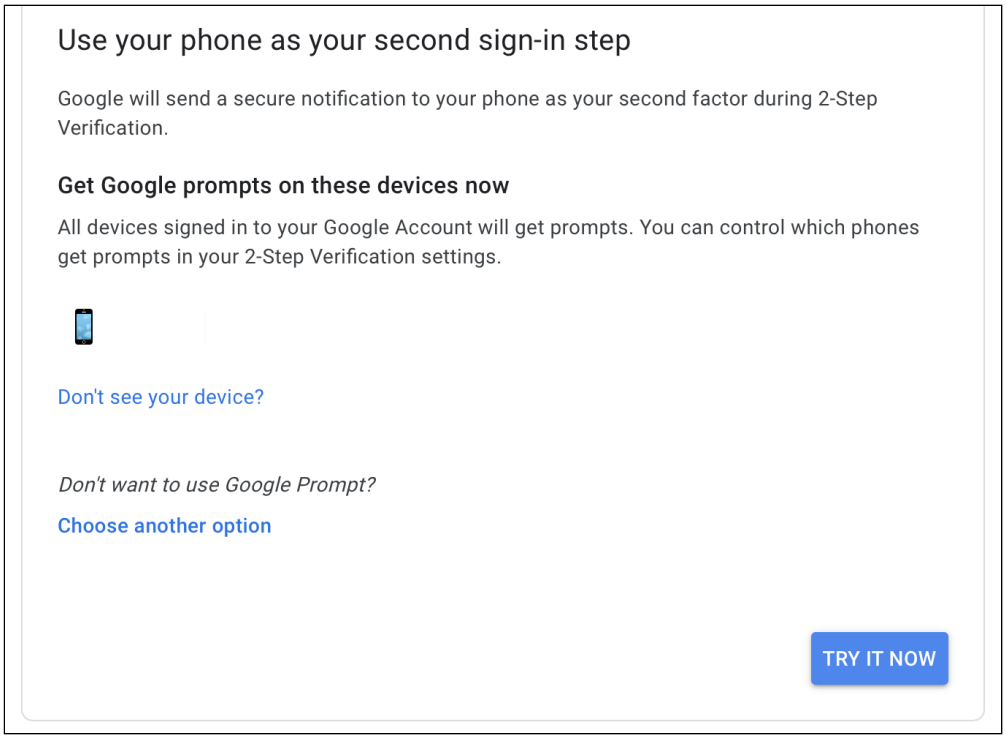
Additionally, regardless of the 2-step verification option you choose, after you select it and set it up, you will receive an email to your registered accounts telling you that 2-step verification has been turned on. If the abuser has access to your email, they might see this message.

If you are concerned about this, please talk to the professional who is helping you make plans for your safety.

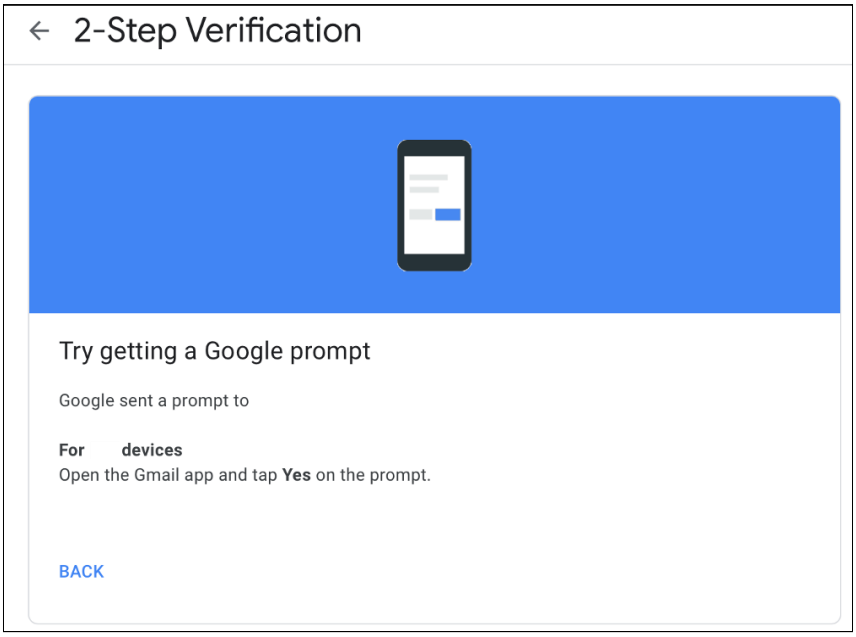
Path 1 - You decided to use the *Google Prompt* method

This is the **2-Step Verification** page:



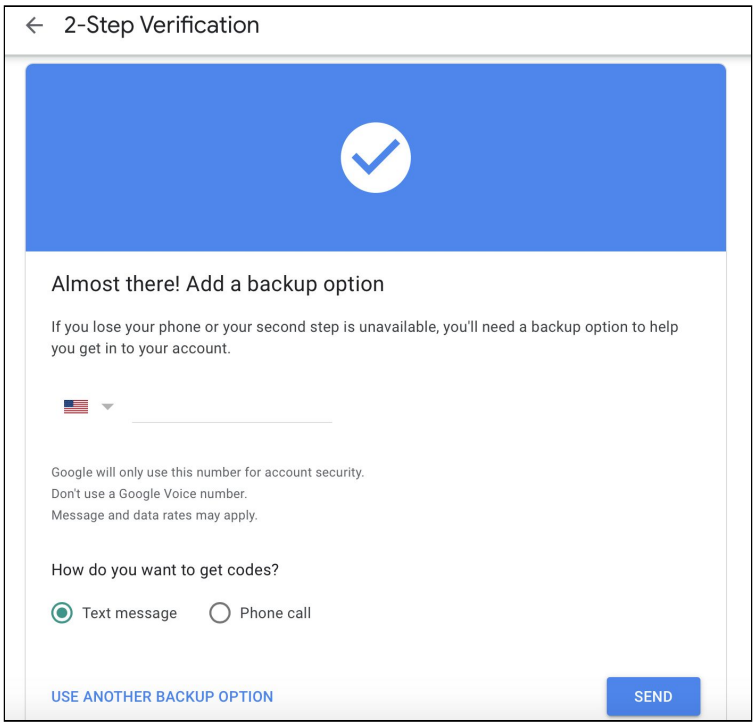


Click on the **TRY IT NOW** button. You will see the next page:



Instructions based on your registered devices (generally a mobile phone) will be shown. Follow them to accept a prompt Google sent to your phone. You will receive a prompt that looks similar to this:

Tap on **YES** and check your computer again. The next web page will appear:



In order to finish the process of enabling 2-step verification, you have to set up a **backup option** that will allow you to access your Gmail and Google accounts even if your selected 2-step verification method is not available (for example, because you lost your phone).

You have two choices. (1) You can register a phone number and receive a backup code as a text message or phone call when you need it. (2) Or, you can request that Google create 10 backup codes now and copy them down. (You can use any of these codes to get access to your account if you cannot use your usual 2-step verification method.) You can choose the backup option you feel most comfortable with.

Be careful!

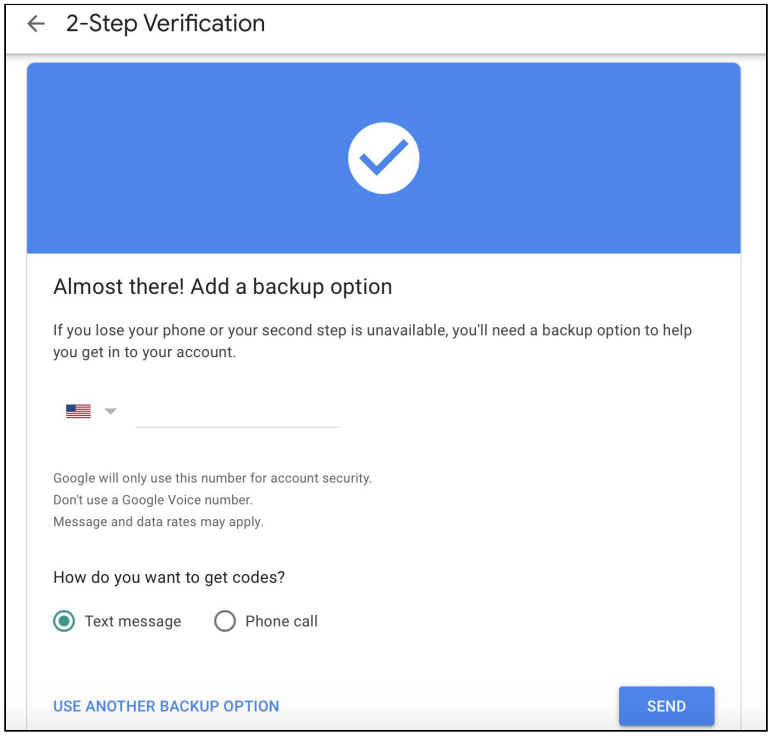
This action could be visible to abuser

Be careful if you decide to request that Google create 10 backup codes, because you would have to store them safely. For some people, the safest option will be to write down the codes on a piece of paper and keep them in a safe place. If you store the codes on your phone or computer, such as by taking a picture, then the abuser

could get access to the codes if they also have access to your device or the account where you are storing the information.

Path 1, Backup Option 1 - USE YOUR PHONE NUMBER

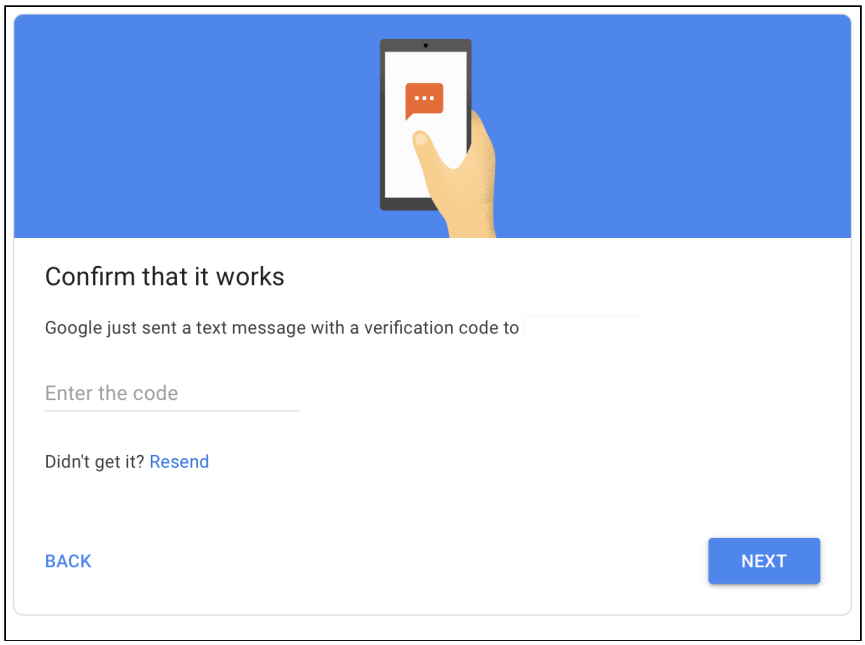
This is the page where you will set up a **backup option**:



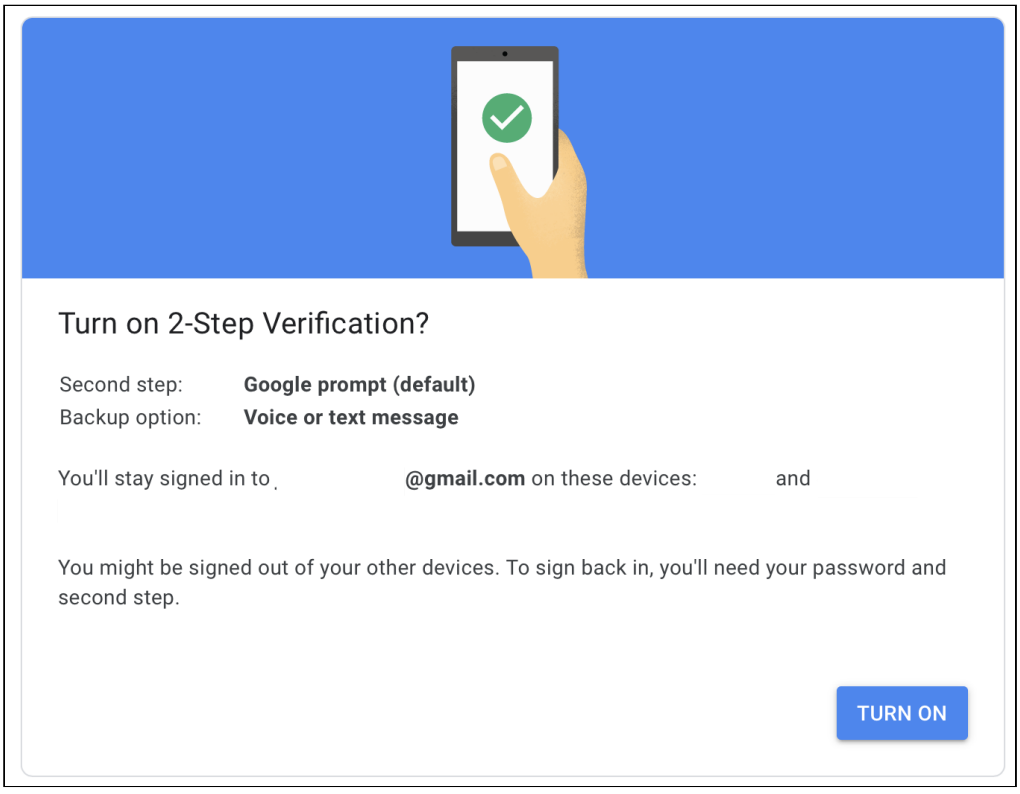
To use your phone number, enter it into the blank next to the country flag (make sure the flag matches the country where your phone number is registered).

Then, you have to select the way you want to get a backup code when you need it. You have two options: receiving the code as an SMS (text) or as a phone call. You might consider to use the phone call option if you are worried the abuser could see your SMS texts.

Finally, click on **SEND**. The following will appear:



Google will send you an SMS (text) or will call you to provide you with a verification code. Enter it in the **Enter the code** text field and click on **NEXT**. The following screen will appear:



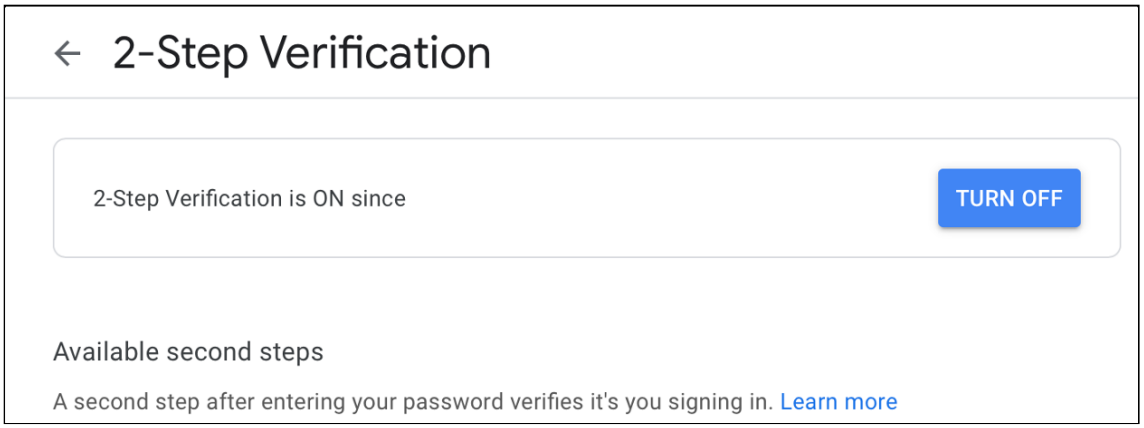
Be careful!

This action could be visible to abuser

Turning on 2-step verification could lock the abuser out of the account, which they might realize right away. Additionally, be aware that if the abuser has access to an email account where you receive emails from Google, that other person may see the message from Google saying that you have turned on 2-step verification. This means they may realize quickly that they have lost access to your Gmail or other Google account.

If you are concerned about this, please talk to the professional who is helping you make plans for your safety.

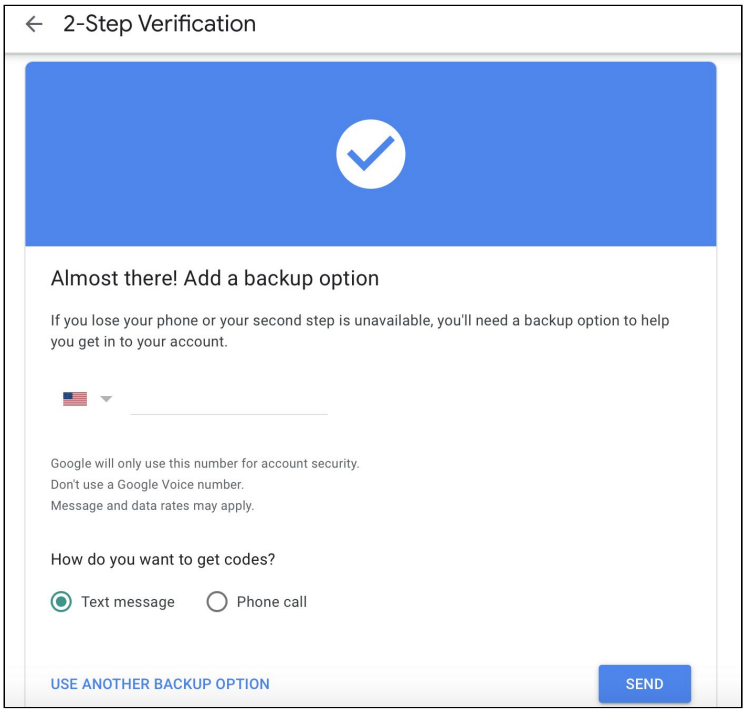
If you click on **TURN ON**, you will be taken to the following webpage:



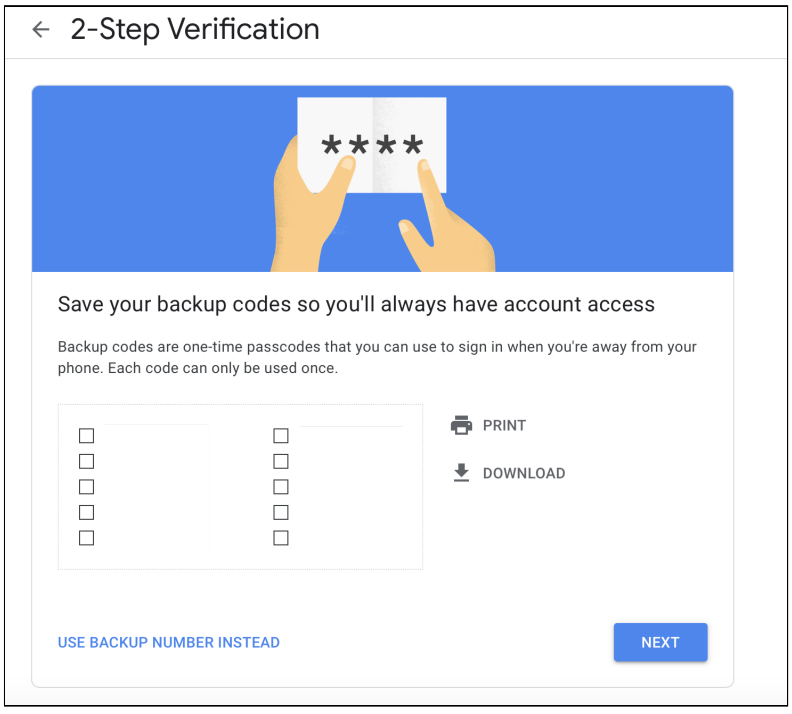
Congratulations!
You have enabled 2-Step Verification for your Gmail account and thus, for all Google services you might be using!

Path 1, Backup Option 2 - USE ANOTHER BACKUP OPTION

This is the page where you set up a **backup option**:



If you click on **USE ANOTHER BACKUP OPTION**, you will see something like this:



These are 10 backup codes you can use to log into your account if you cannot use your selected 2-step verification method.

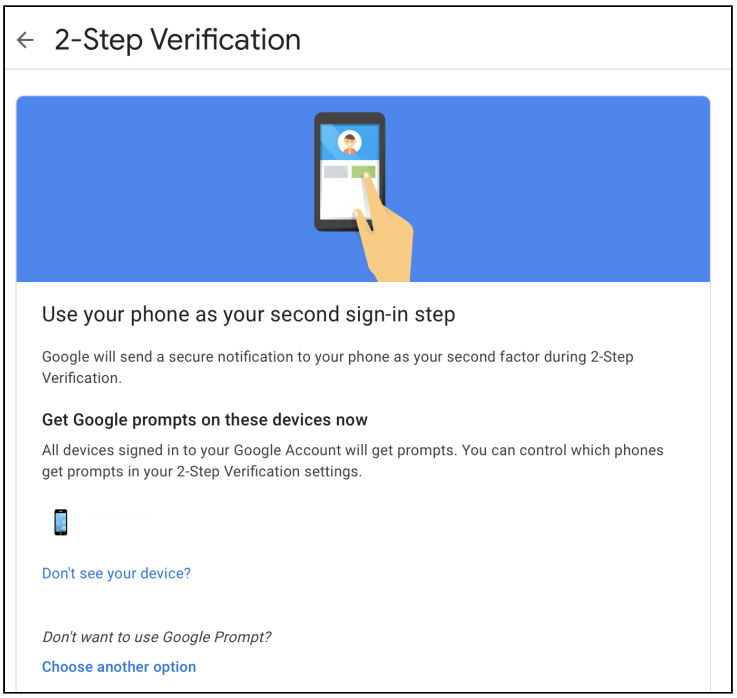
Be careful!

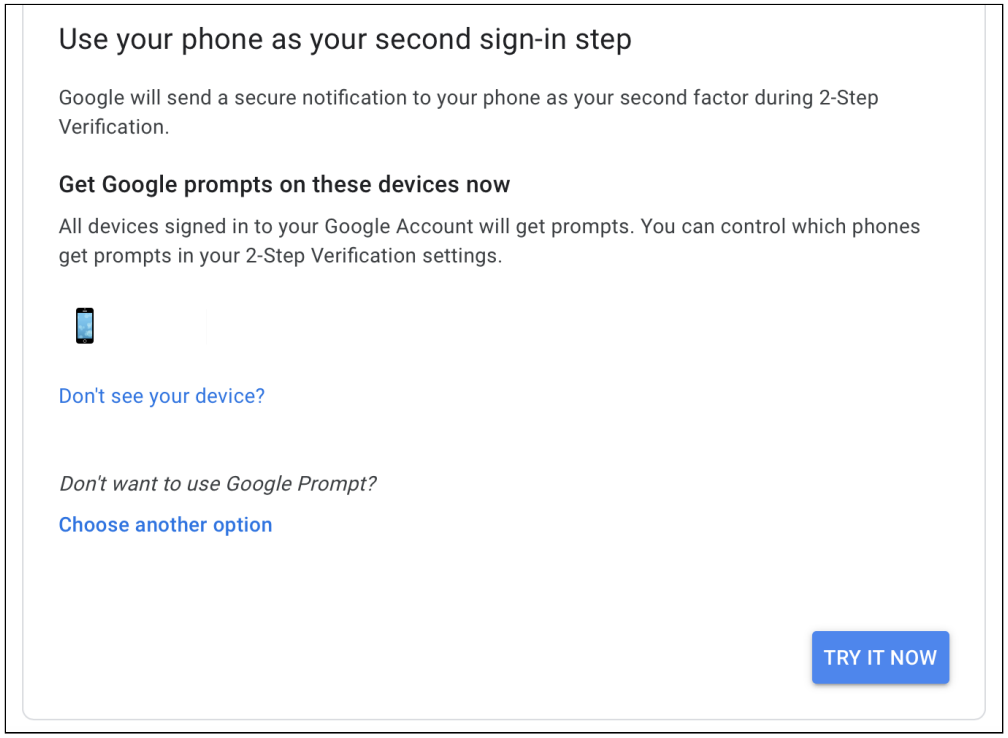
This action could be visible to abuser

You need to store the backup codes safely. It is recommended that you write them down and keep them away from the abuser. On the other hand, if you take a picture or store the codes inside a notes app, the abuser could find and use them to get into your Google account if they have access to your phone, or the app where you are storing the codes.

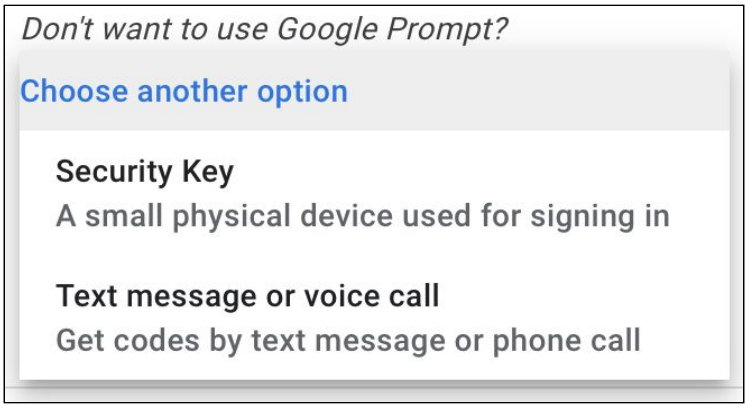
Path 2 - You decided to use the *Text message or voice call* method

This is the **2-Step Verification** page:

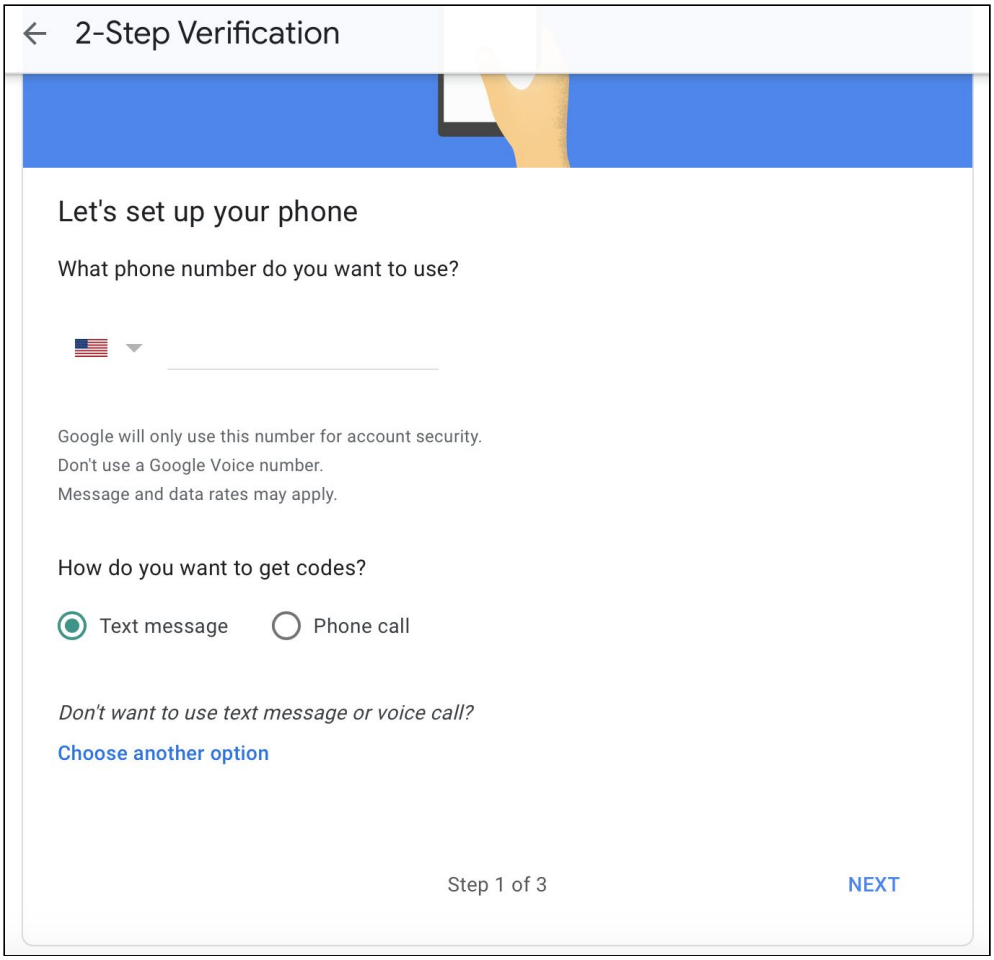




Click on **Choose another option**. The following will appear:



Click on **Text message or voice call**. The following will appear:



You'll enter your phone number, pick the way you want to receive the codes needed to log into your account (text message or phone call), and click on **NEXT**. Then,

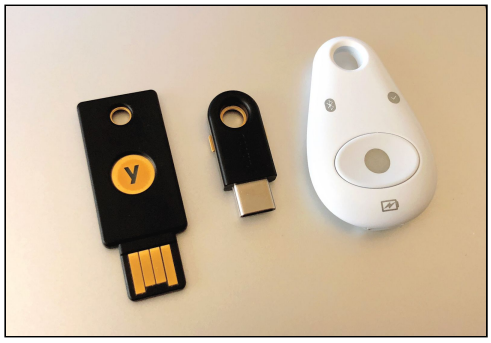
Google will send you a code by SMS (text), and you'll enter it. Or, Google will communicate with you through a phone call.

Finally, you will be taken to a confirmation screen. If you click on **TURN ON**, 2-Step Verification will be turned on.

Congratulations!
You have enabled 2-Step Verification for your Gmail account and thus, for all the Google services you might be using! From now on, when you try to log into your Gmail account (and your Google account in general), Google will send you a code via SMS or call you by phone, and that's how you'll get access to your account.

Path 3 - You decided to use the method in which a *Security Key* needs to be inserted to your PC to access your account

Before continuing, please bear in mind that you can only use this option if you have a physical security key similar to the ones shown in the next image:

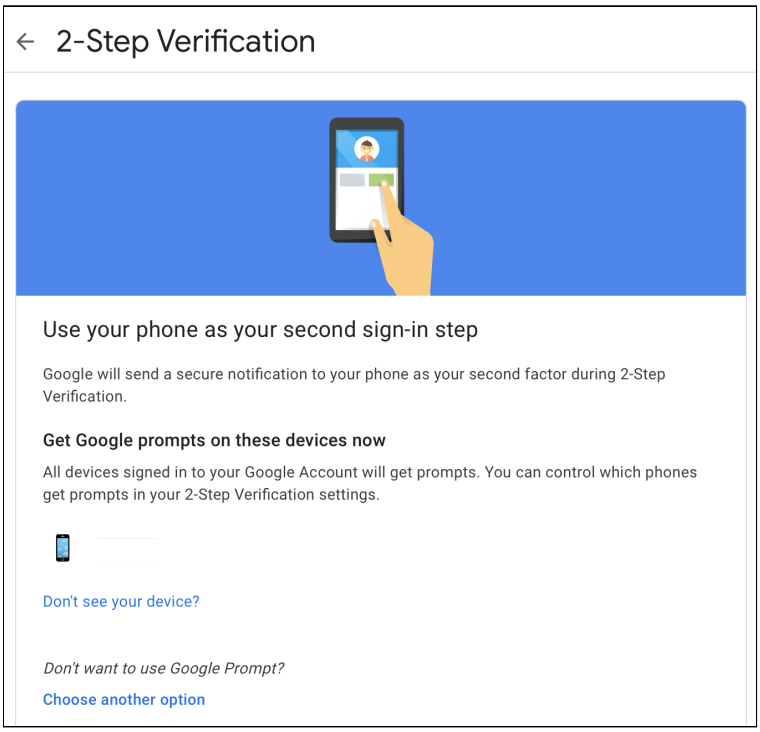


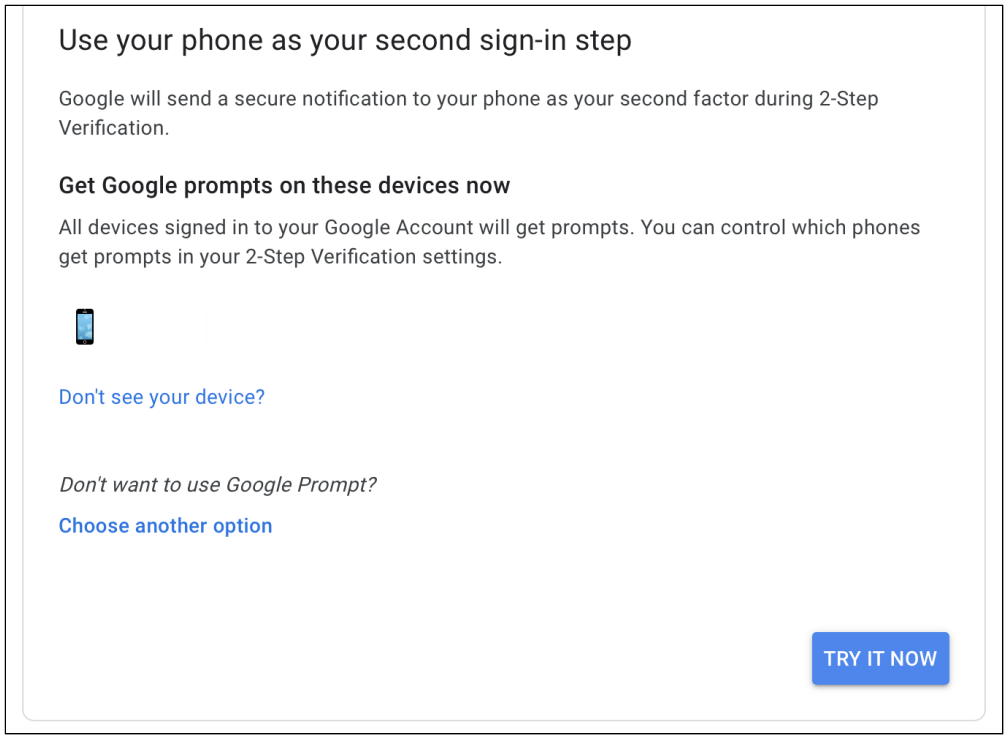
The security keys shown in the image above **are not** ordinary USB thumb drives. They have a chip inside that's specially designed for two-factor authentication.

Where can I buy a security key? - Examples	
Amazon	https://www.amazon.com/slp/security-keys/w9xxs8zvdyob687
Yubico Store	https://www.yubico.com/store/

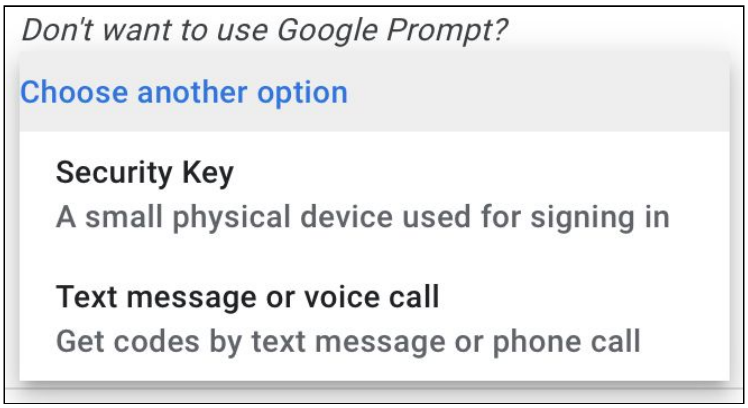
There is a comparison between different security keys in the following article: https://www.theverge.com/2019/2/22/18235173/the-best-hardware-security-keys-yubico-titan-key-u2f

This is the **2-Step Verification** page on Google:

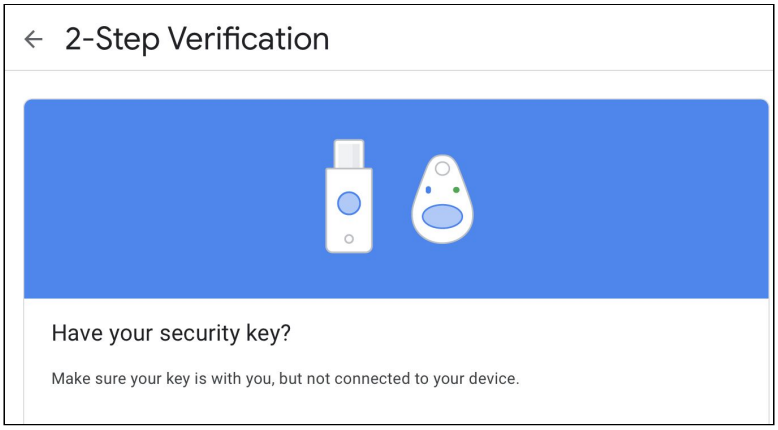


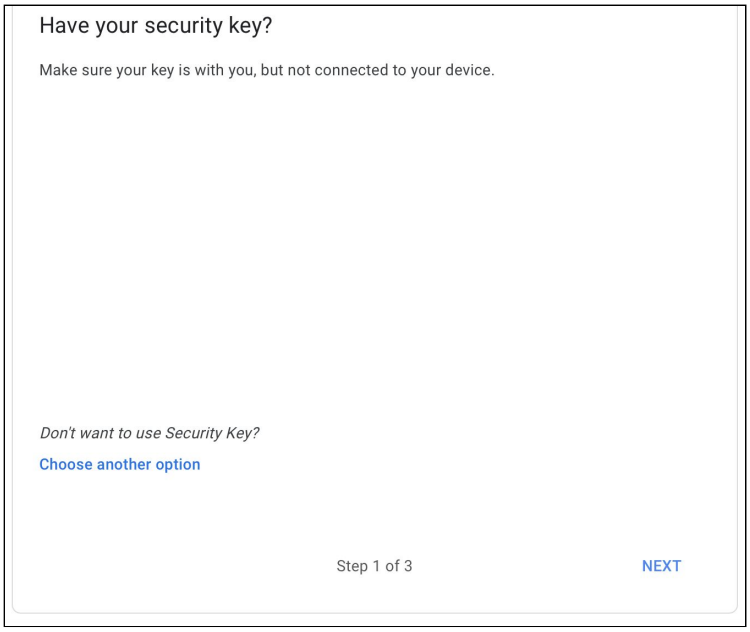


Click on **Choose another option**. The following will appear:

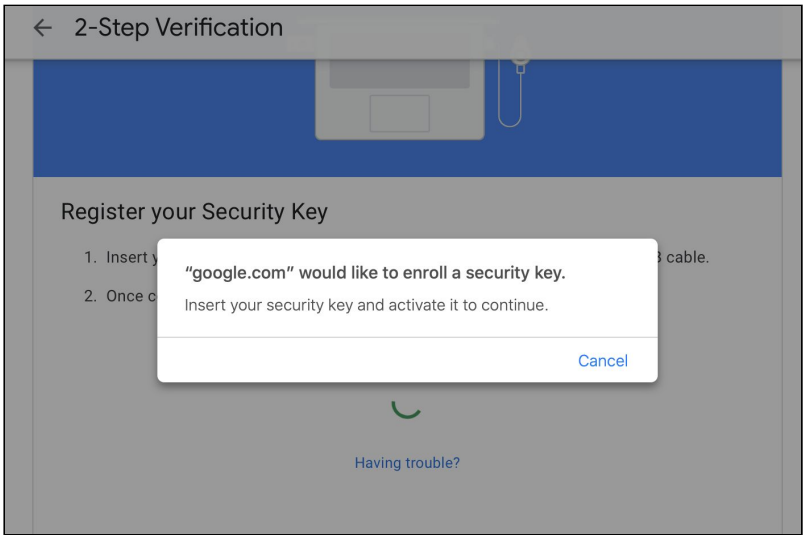


Click on **Security Key**. The following will appear:





Click on **NEXT** to continue. Then, a message like the following will appear:



You have to insert your security key into your computer and activate it. Then, follow the instructions that appear on the screen.

Congratulations!
You have enabled 2-Step Verification for your Gmail and other Google accounts! From now on, every time you want to get access to your Gmail account (and your Google account in general), you will be asked to insert your physical security key to your computer.

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