Facebook - Turning On Two-Factor Authentication (Extra Security)

Compiled by the Clinic to End Tech Abuse

Last Updated: April 17, 2020

What is two-factor authentication 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 that only you should know.

Who is this guide for?
Anyone who would like to strengthen their security and privacy on Facebook. 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 Facebook's own guide here: https://www.facebook.com/help/148233965247823.

What does this guide cover?

- How to turn on two-factor authentication, an extra layer of security for your Facebook account.
- How to choose among different two-factor authentication 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 two-factor authentication. Turning on two-factor authentication 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 two-factor authentication 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!

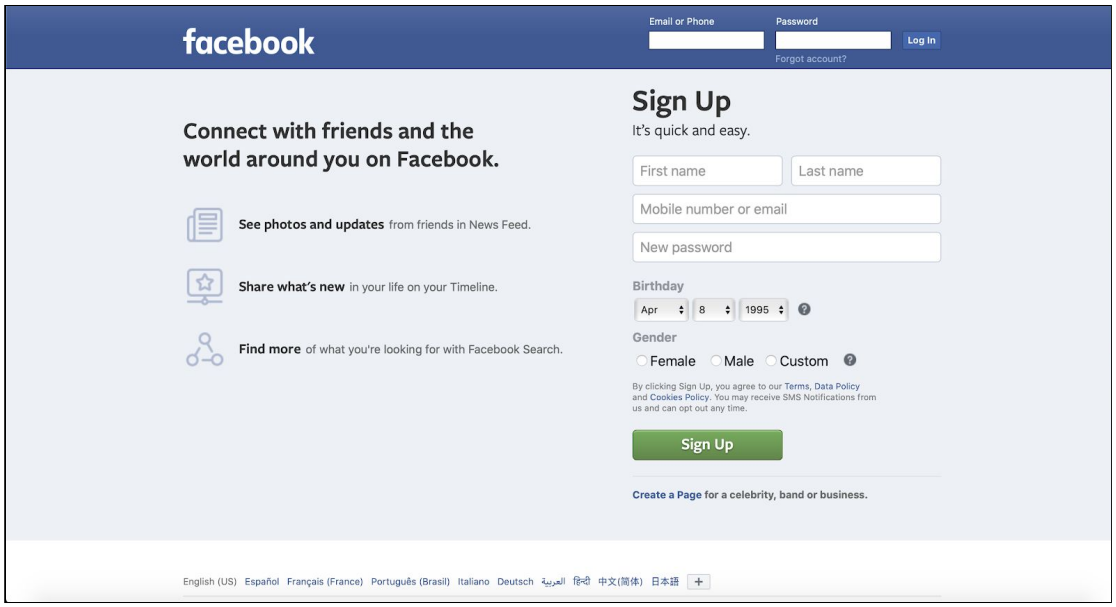
This action could be visible to abuser

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

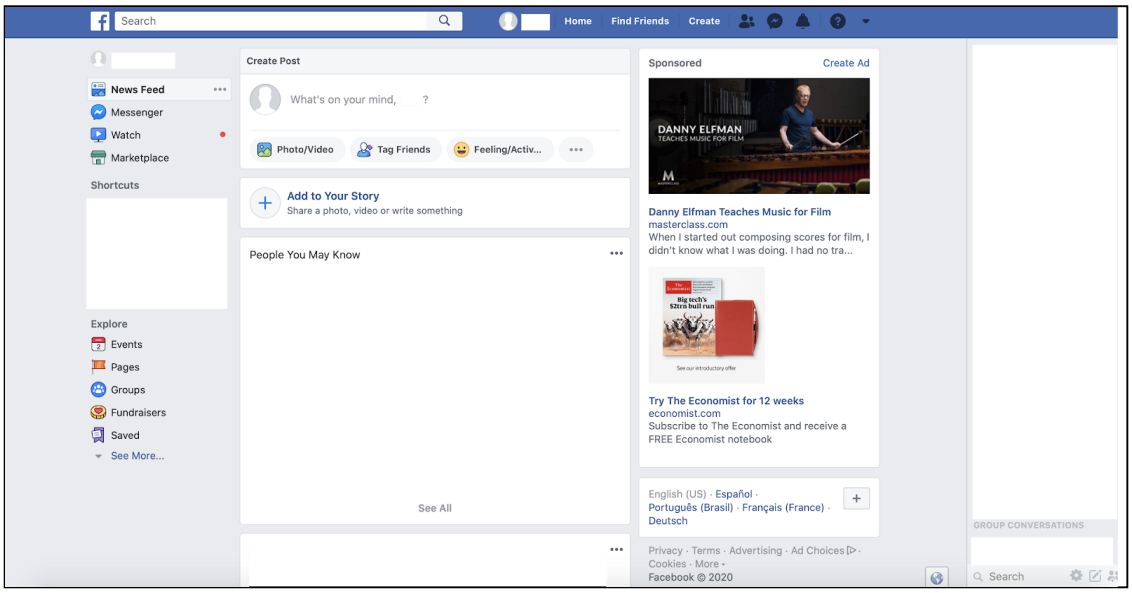
Images of the Facebook website are included below for educational and research purposes only.

Step 1 - Logging into your Facebook Account

Log into your Facebook account at https://www.facebook.com:

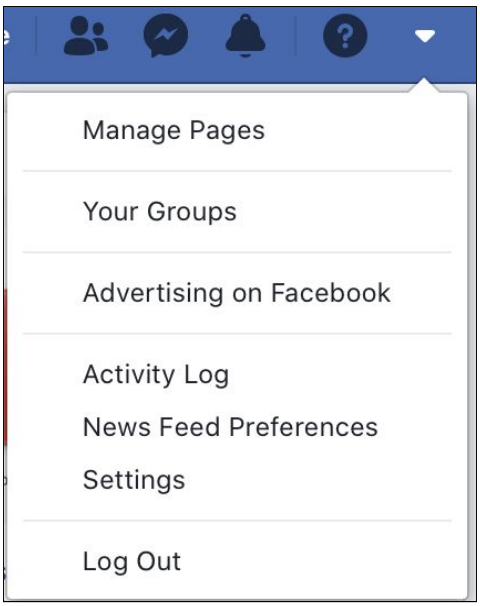


After logging in, you should see a webpage that looks like the following:

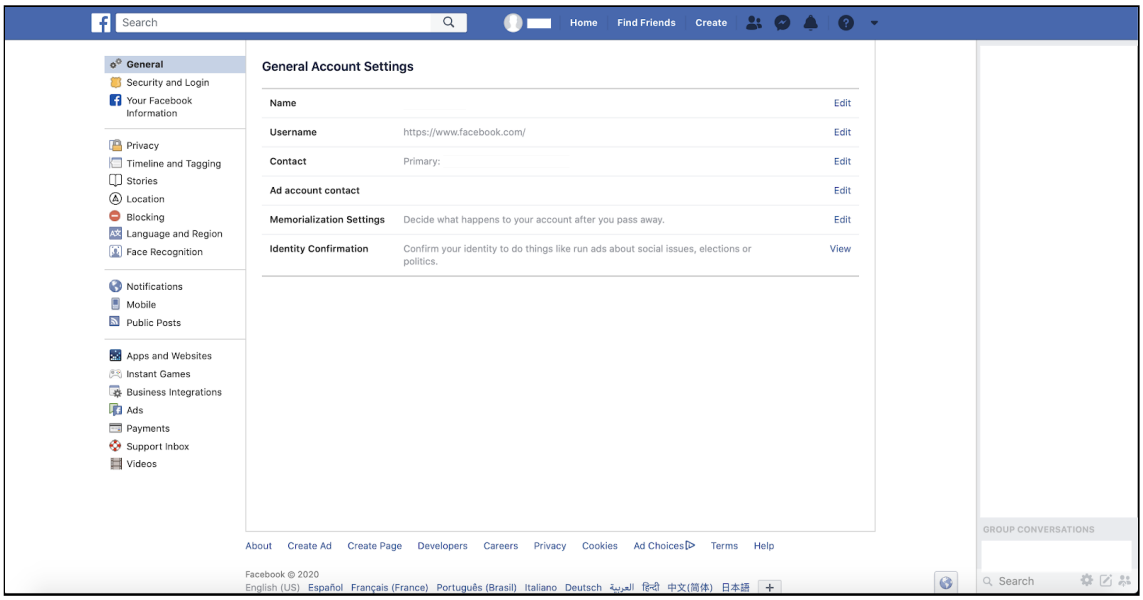


Step 2 - Going to *Security and Login*

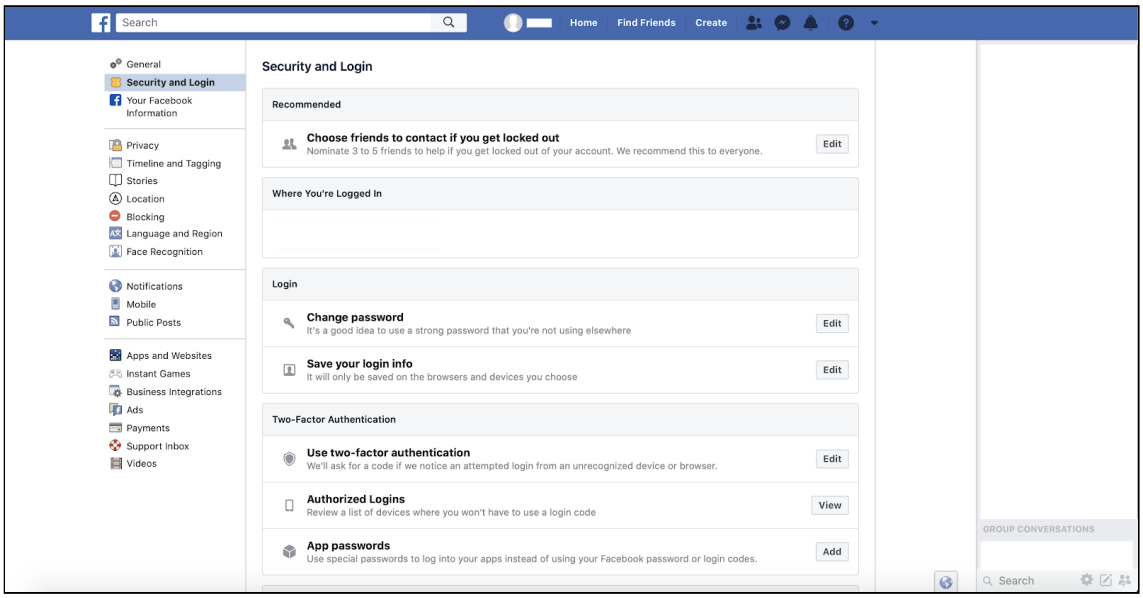
Click on the **downward triangle** at the top right corner of the screen:



Then click on **Settings**. A page like the following one will appear:

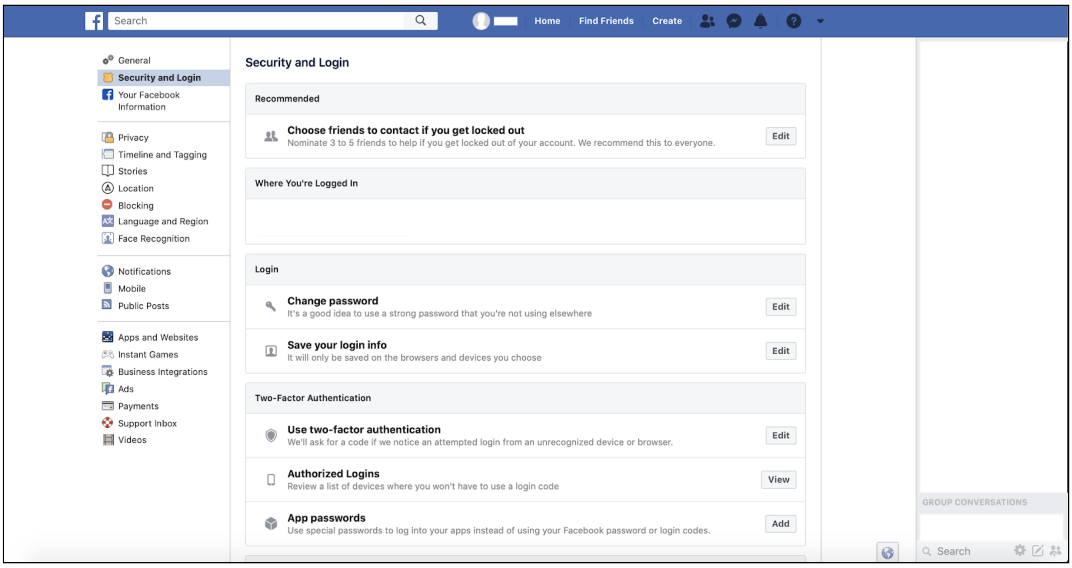


Click on **Security and Login** from the menu on the left. A page like the following will appear:

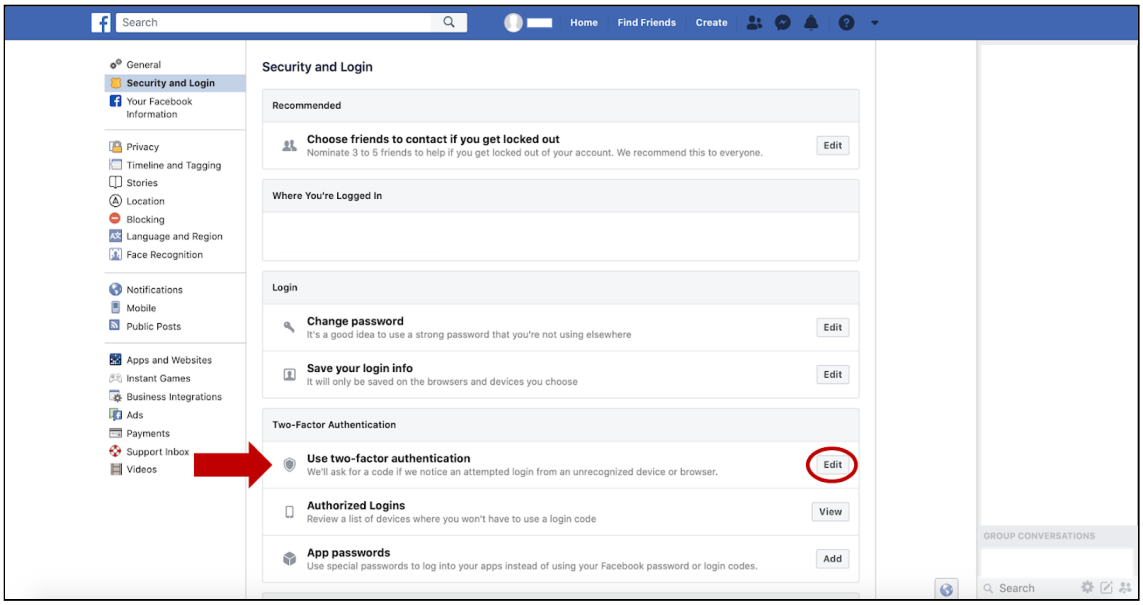


Step 3 - Turning on Two-Factor Authentication

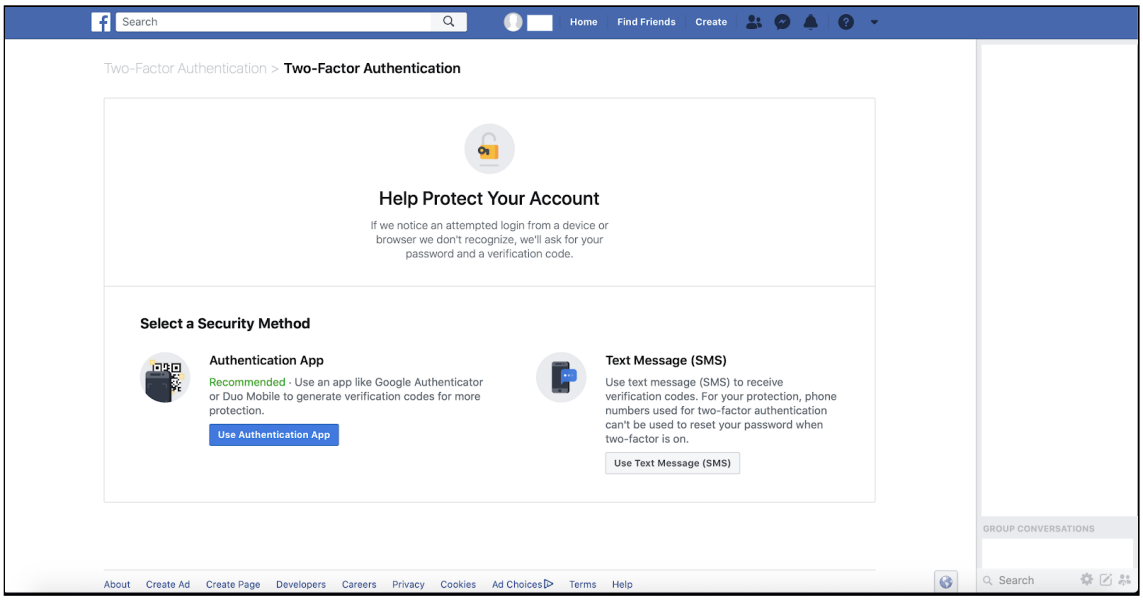
You should now see the following screen:



There is a box titled **Use two-factor authentication** near the bottom. Inside that box, there is an **Edit** button on the right:



Click on the **Edit** button. A page like the following will appear:



Facebook will ask you two select between two security methods (**Authentication App** and **Text Message**) that will provide you with a second piece of information you will require to log into your account.
Choose the method you feel most comfortable with:

- **Authentication app:** This is a mobile app that will give you a code (also called a One-Time Password) whenever you try to log into your account. This option may be more secure for you than the text message option if you are worried that the abuser can see your texts.

  However, you will need to install an app on your device, and you may want to think about whether the abuser could see this new app on your phone.

  Examples of authentication apps are: Microsoft Authenticator, Google Authenticator, and Duo Mobile.

- **Text message (SMS):** if you choose this option, then every time you try to log into your account, an SMS (text) message with a code will be sent to your mobile phone. You will then enter the code into Facebook to log into your account. You will not have to install any new apps.

  Remember that if the abuser can unlock your phone or see its screen, they may be able to see the code you get by text. In general, if you are worried that the abuser may be reading your text messages, it may be better to use an authenticator app instead (see above).

Be careful!

This action could be visible to abuser

In the following pages (after the **Staying safe** section), you will find two paths, one for each of the two security measures Facebook asks you to choose from (**Authentication App** or **Text Message**) to enable two-factor authentication.

Staying safe

Using two-factor authentication can help keep the abuser from getting access to your private Facebook 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.

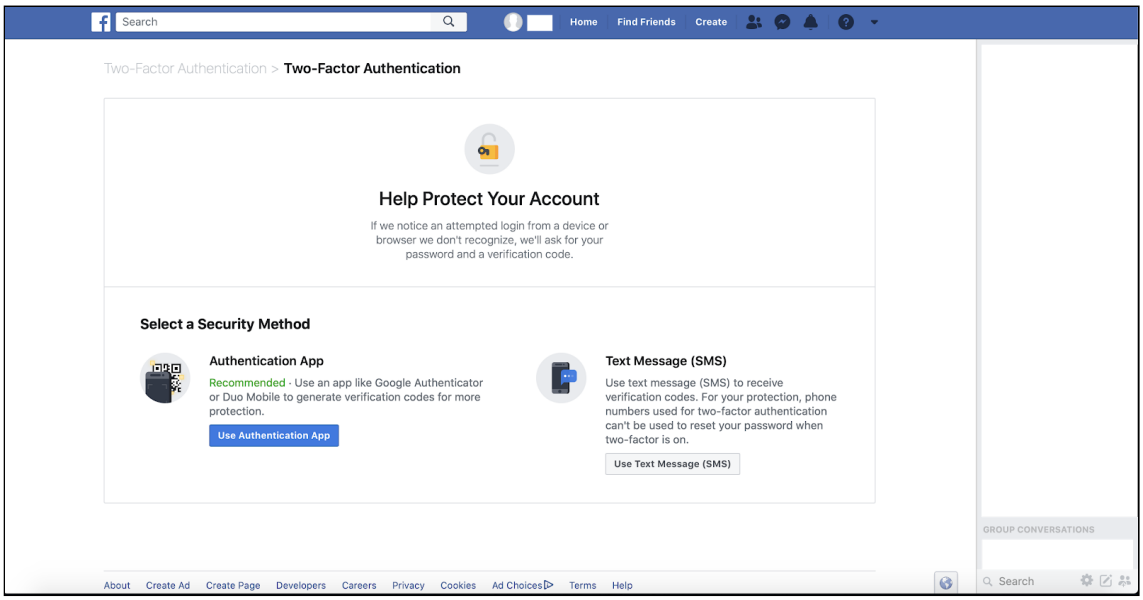
But if the abuser has been going into your Facebook account, they might realize right away that they can no longer get in. If you think this could make them become more dangerous, we urge you to contact an organization that helps abuse survivors first.

Additionally, depending on your Facebook notification settings, you might get an email from Facebook telling you that two-factor authentication has been turned on. If the abuser has access to your email, they might see this message. You can check your Facebook notification settings by clicking on the **downward triangle** at the top right corner of the screen, then clicking on **Settings**, and in the new page, clicking on **Notifications**.

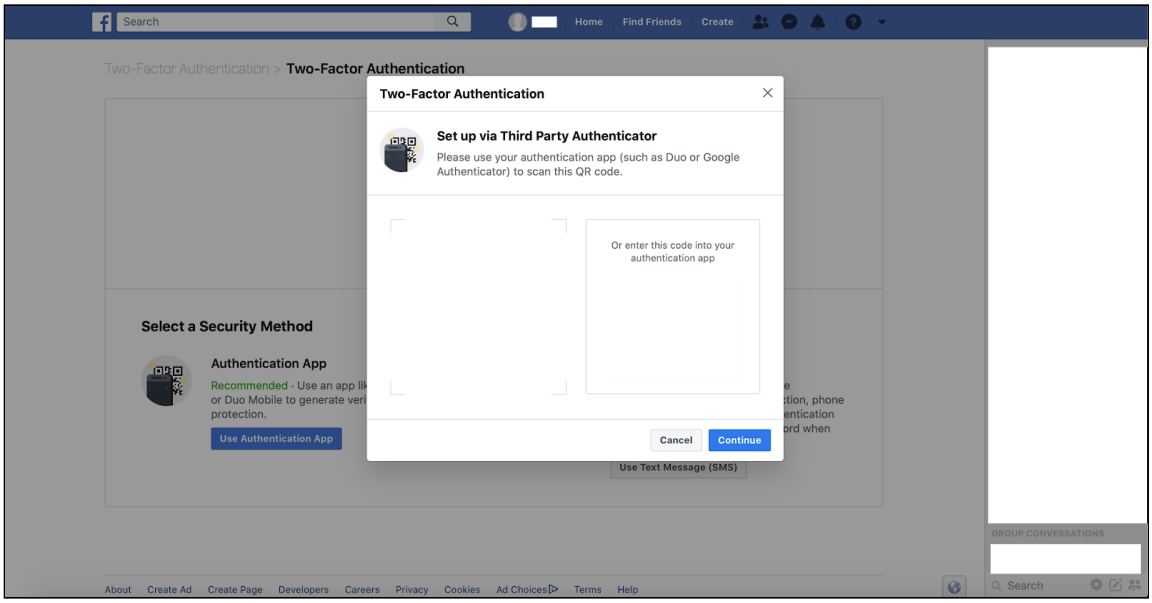
If you are concerned about this, please talk to the professional who is helping you make plans for your safety.

Path 1 - You decided to use the *Authentication App* method

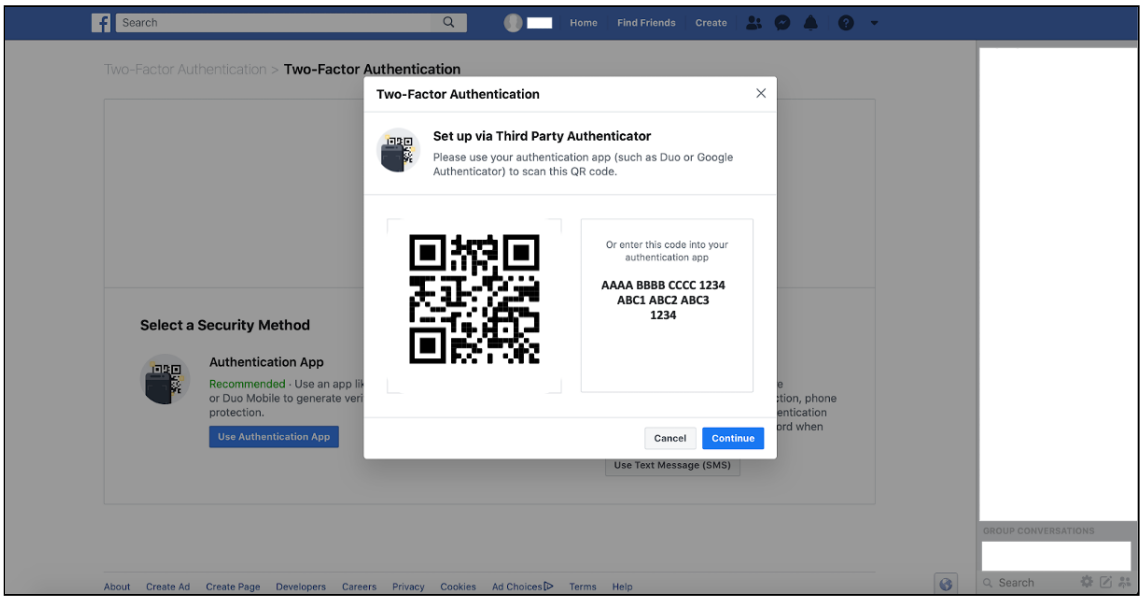
This is the **Select a Security Method** page:



Click on the **Use Authentication App** button. The following popup will appear:



The popup will display a QR code on the left and a code on the right. You will see something like the following:



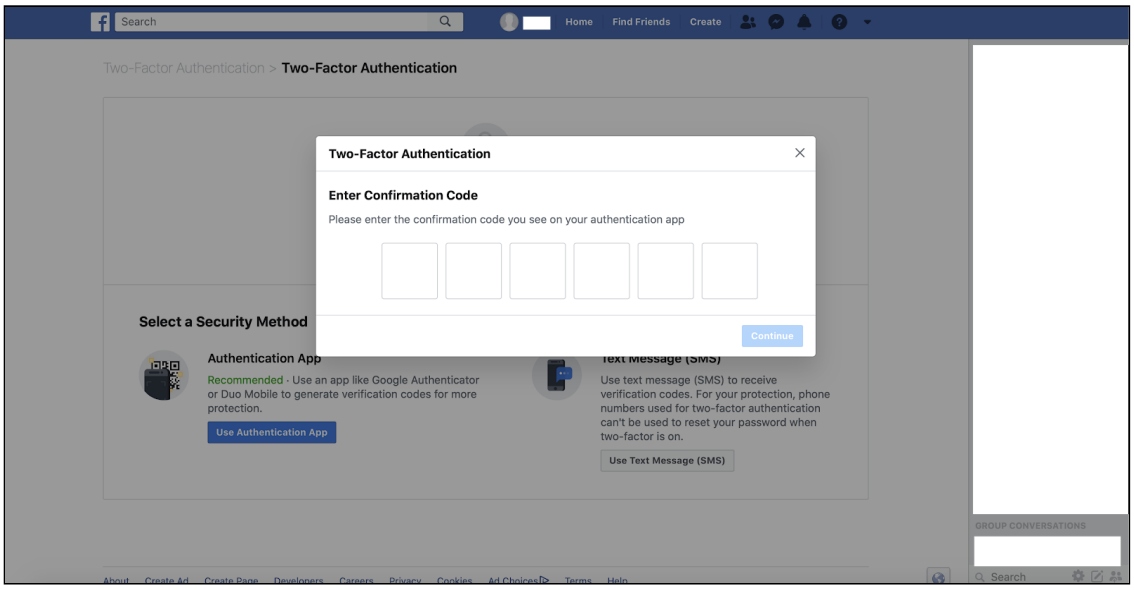
To move forward, you will need to install an **authentication app** (like Microsoft Authenticator, Google Authenticator, or Duo Mobile) on your phone. You can do this by going to the Apple App Store if you have an iPhone, or the Google Play Store if you have an Android phone such as a Samsung, LG, or Motorola.

Then, open the app. Regardless of the authentication app you installed, the main thing to do now is scan the QR code shown in the popup, or enter the code in it. The app should tell you what to do.

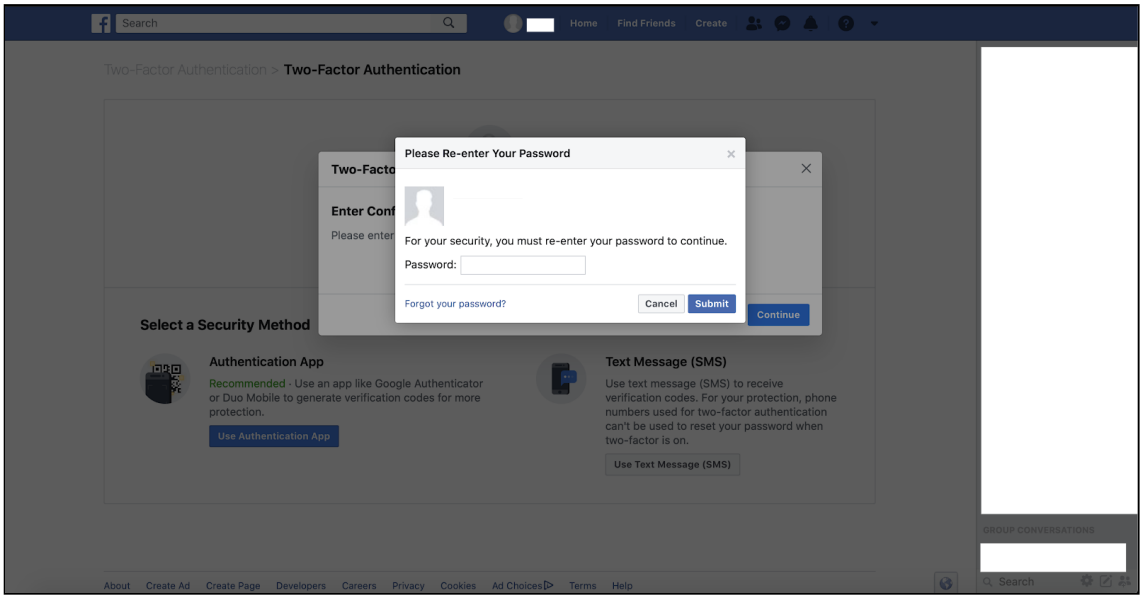
Doing this will register your Facebook account in the app, allowing it to create codes you can use as a second factor to log into your account.

If you installed **Google Authenticator**, tap on the **+** button at the top right corner. A menu will appear at the bottom of the screen. Tap on **Scan barcode**. Then use your phone to scan the shown QR code (on the page shown above), which will look like a box with black and white patterns. You will now see a row titled “Facebook” with a number in your Google Authenticator app. Click **Continue** in Facebook’s pop-up window (on the page shown above).

A new Facebook popup window should appear. Enter the Facebook-generated code you see into the Google Authenticator app.



You will need to enter your Facebook login information again.



Finally, click on **Submit**.

Be careful!

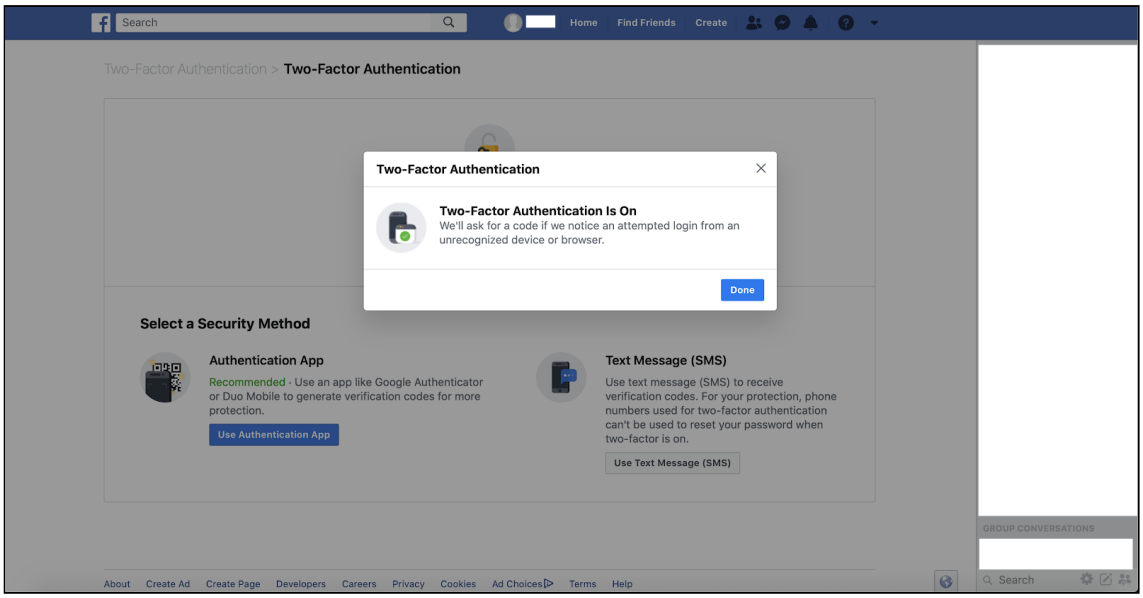
This action could be visible to abuser

You might receive a notification to your registered Facebook email account telling you that two-factor authentication has been turned on. This depends on your Facebook notification settings (to check them, click on the **downward triangle** at the top right corner of the screen, then go to **Settings**, then **Notifications**).

Be aware that if the abuser has access to an email account where you receive emails from Facebook, he may see the message from Facebook saying that you have turned on two-factor authentication. This means they may realize quickly that they have lost access to your Facebook account.

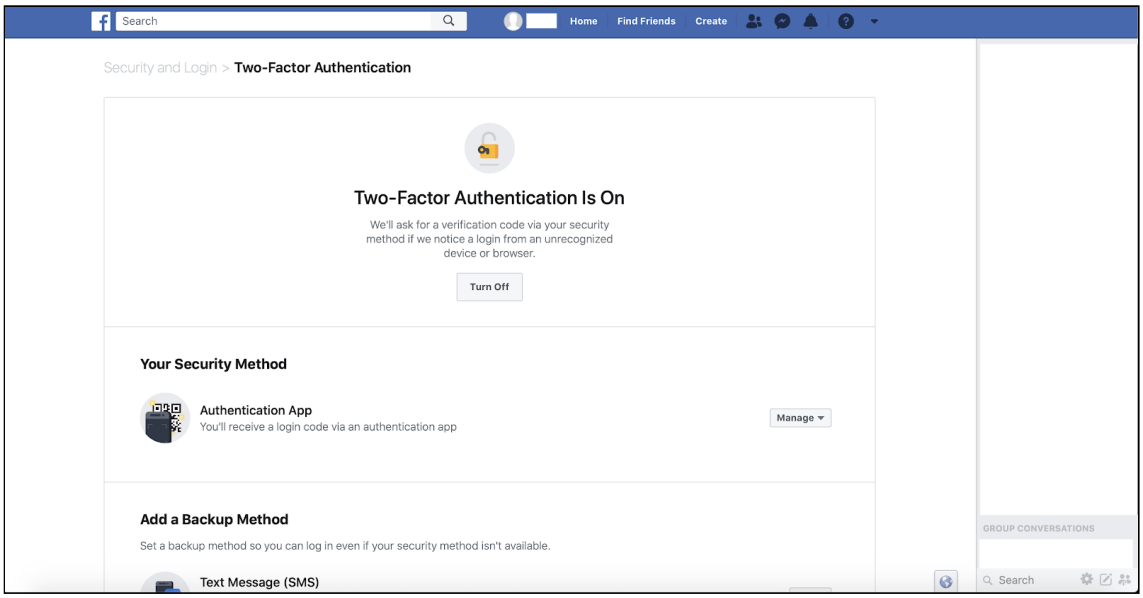
If you are concerned about this, please talk to the professional who is helping you make plans for your safety.

After clicking on **Submit** button, you will see a pop-up like the following one:



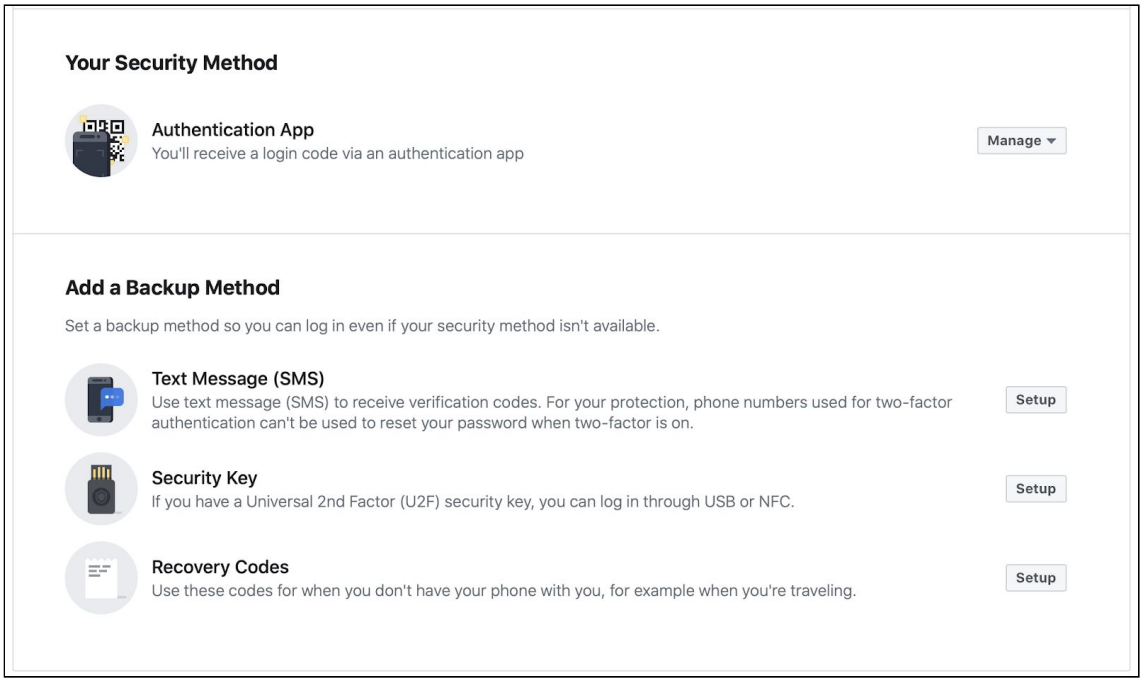
Congratulations!
You have turned on two-factor Authentication for your Facebook account!

Finally, click on **Done**. The following website will appear:



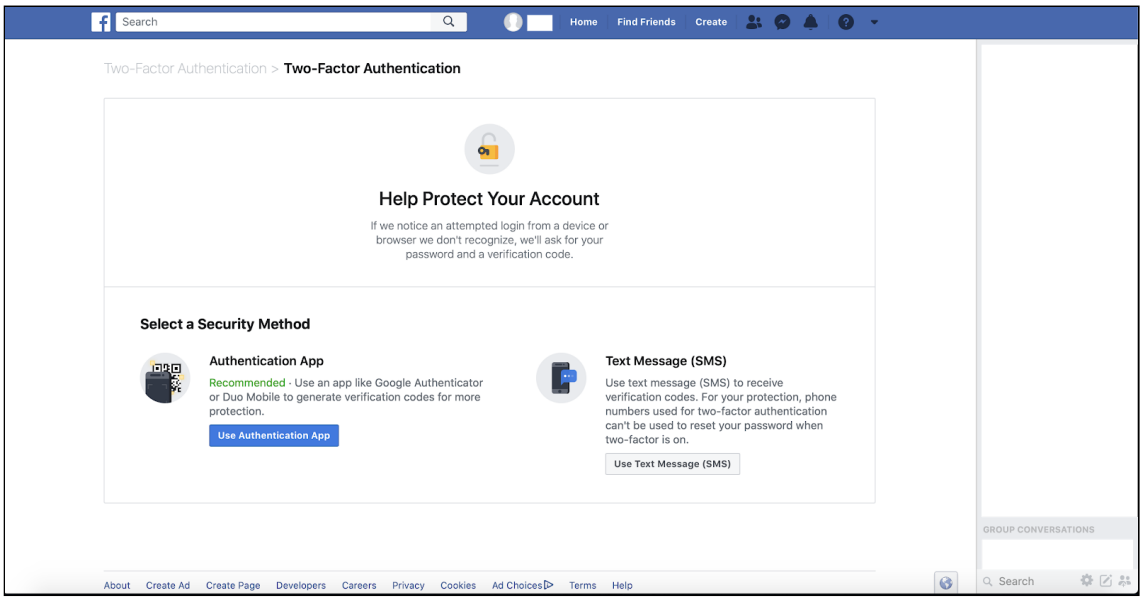
If you scroll down, you will see the **security method** you have just chosen and more information.

Now, you could set up a **backup method** that will allow you to access your Facebook account even if your selected security method is not available (for example, because you lost your phone that has the Google Authenticator app on it).

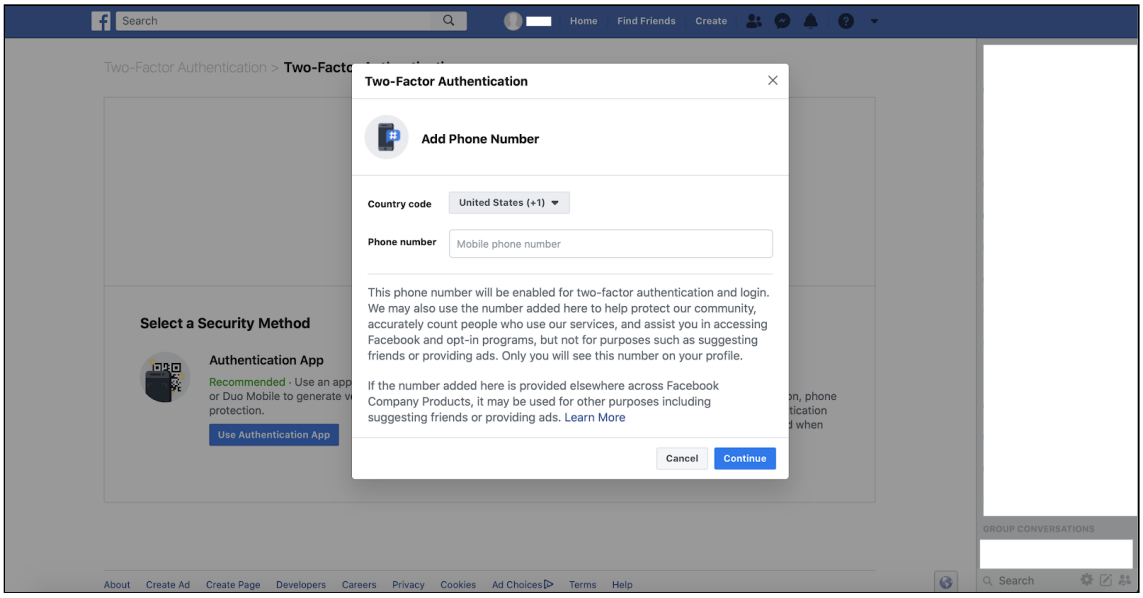


Path 2 - You decided to use the *Text Message (SMS)* method

This is the **Select a Security Method** page:



Click on the **Use Text Message (SMS)** button. The following popup will appear:



First, we suggest thinking about whether the abuser has physical access to your phone -- that is, whether they can regularly look at the screen or unlock the phone. If this is true, or if you have other reasons for thinking they can see your text messages, then this may affect whether getting codes by text message is the best choice for you.

If you have decided to choose this option, enter your phone number and click on **Continue**. An SMS text will be sent to your phone with a code. Enter the code in the field you see in the pop-up window on Facebook and follow the instructions.

Congratulations!
You have enabled Two-Factor Authentication for your Facebook account!