

Facebook Compromise Cleanup

Compiled by the Clinic to End Tech Abuse

Last Updated: July 2, 2020

Who is this guide for?

Anyone who suspects or knows that someone else has gotten access to their Facebook account.

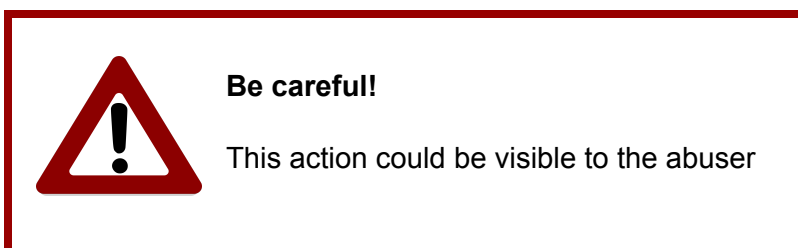
What does it cover?

- Checking whether someone else might have logged into your Facebook account recently
- Making sure the recovery email and phone number for your account belong to you
- Checking what information you are sharing publicly
- Making a Facebook account more secure

This guide does not cover Facebook Messenger.

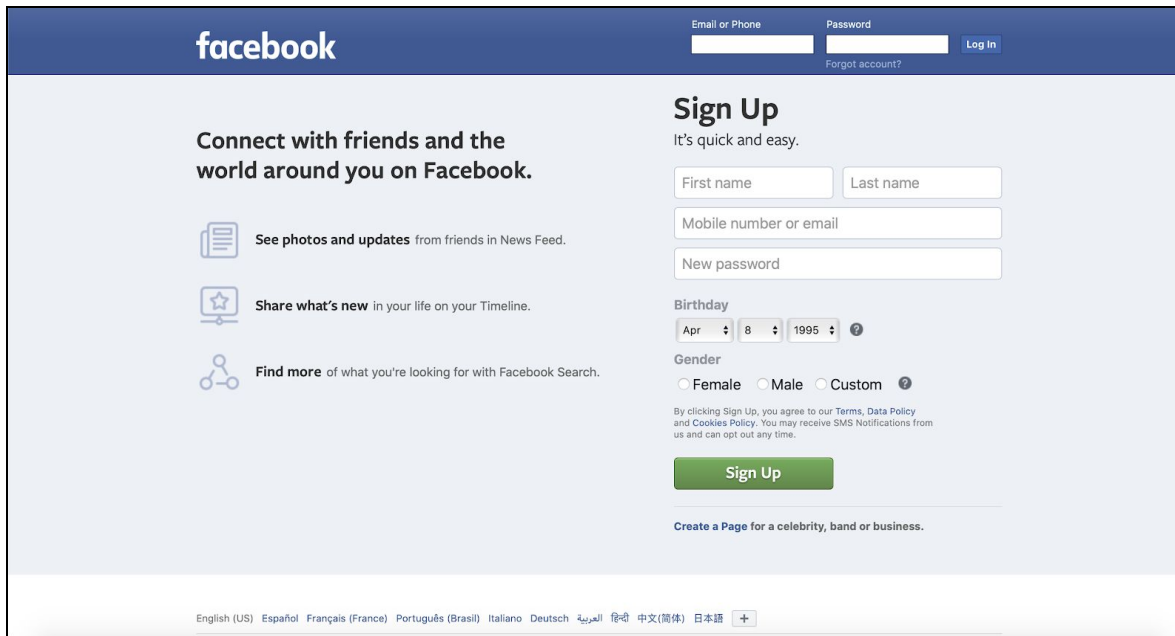
Before we start:

- If someone else is getting access to your account, they may know right away if you turn on two-factor authentication (extra security) or change other account settings. If the person is violent or threatening, losing access to your account may cause them to become more dangerous. We strongly recommend that you talk to a domestic violence or other appropriate organization to make plans for your safety before you make any changes to your account if you are worried about an increase in violence or other harm.
- We have marked changes that could be visible to an abuser with the following sign:



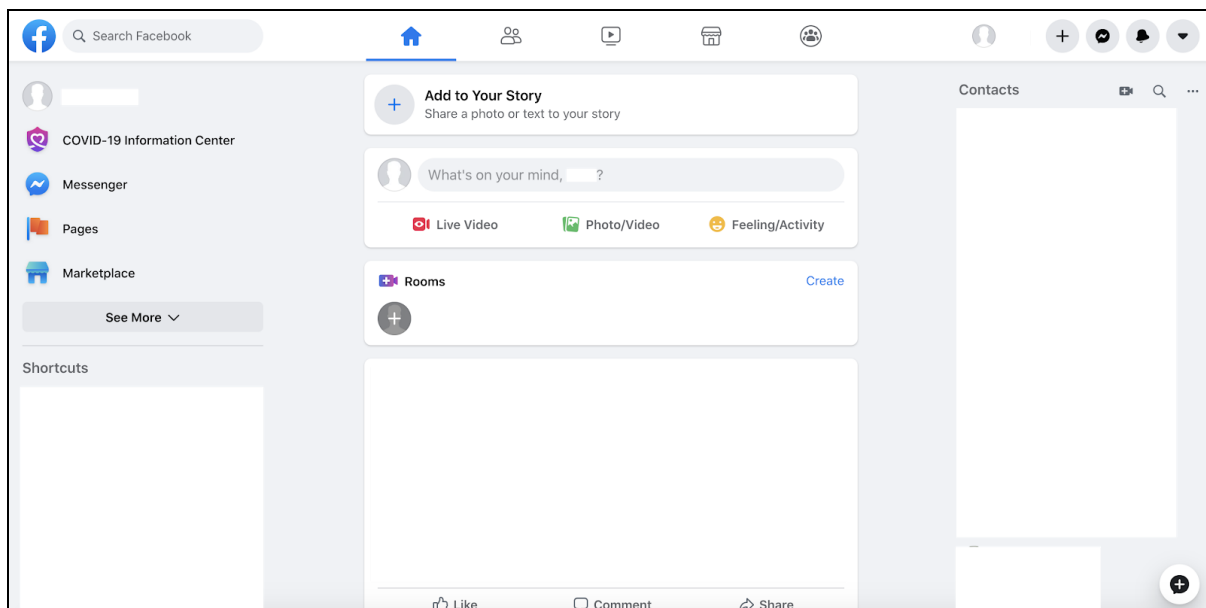
Step 1 - Log into your Facebook Account

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



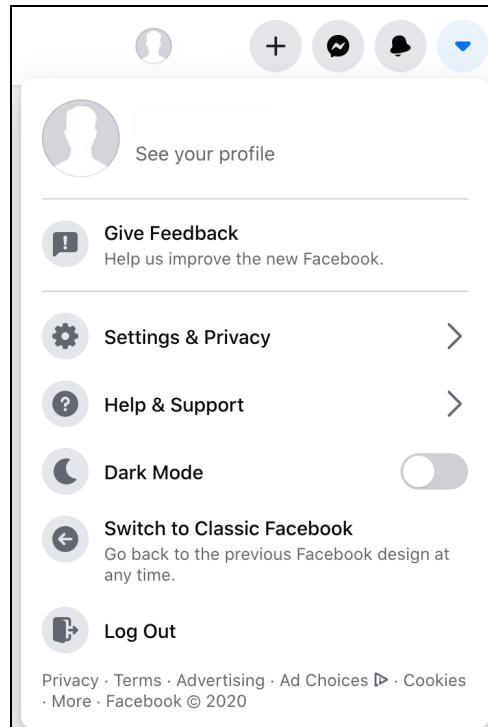
The image shows the Facebook Sign Up page. At the top, there is a blue header with the Facebook logo on the left and login fields on the right. The login fields include 'Email or Phone' and 'Password' with a 'Log In' button, and a link for 'Forgot account?'. Below the header, the main content area is divided into two sections. On the left, there is a section titled 'Connect with friends and the world around you on Facebook.' with three bullet points: 'See photos and updates from friends in News Feed.', 'Share what's new in your life on your Timeline.', and 'Find more of what you're looking for with Facebook Search.' On the right, there is a 'Sign Up' section with the text 'It's quick and easy.' Below this, there are input fields for 'First name', 'Last name', 'Mobile number or email', and 'New password'. There is also a 'Birthday' section with dropdown menus for month (Apr), day (8), and year (1995), and a 'Gender' section with radio buttons for 'Female', 'Male', and 'Custom'. A 'Sign Up' button is at the bottom of the sign up section. At the very bottom of the page, there is a language selection bar with options like 'English (US)', 'Español', 'Français (France)', etc.

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

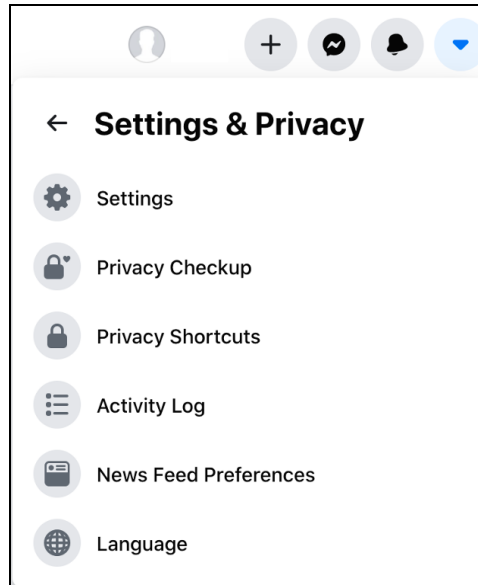


Step 2 - Go to Settings

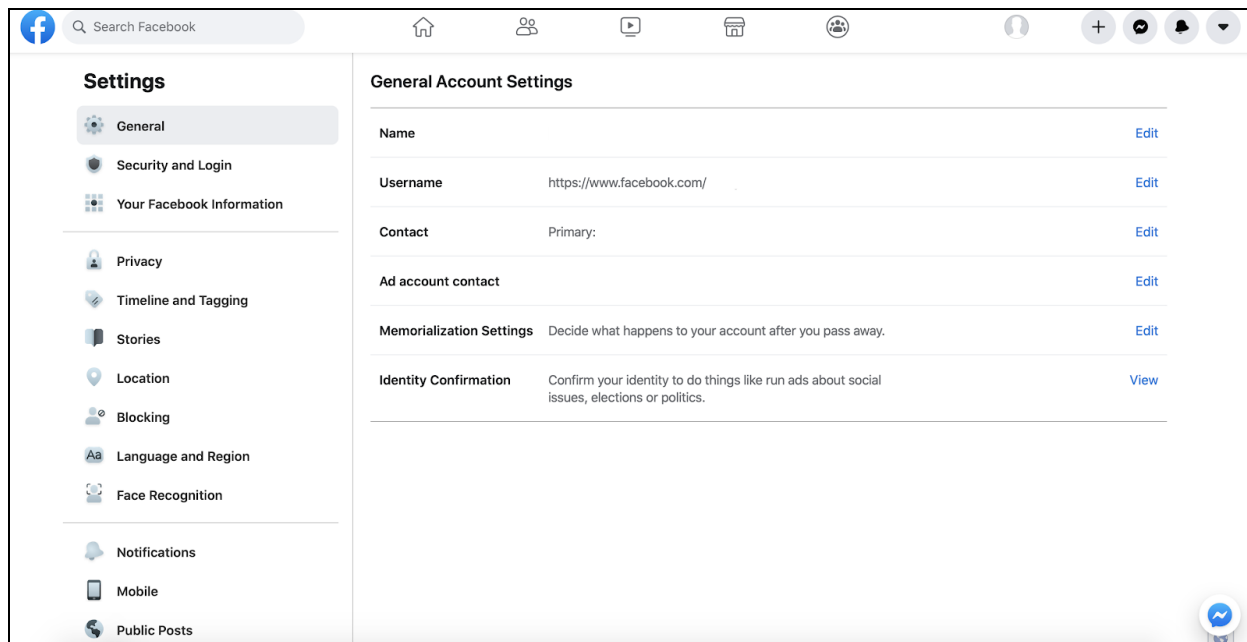
Click on the **downward triangle** at the top right corner of the screen, and you will see a menu that looks like this:



Then click on **Settings & Privacy**. You will see something like this:

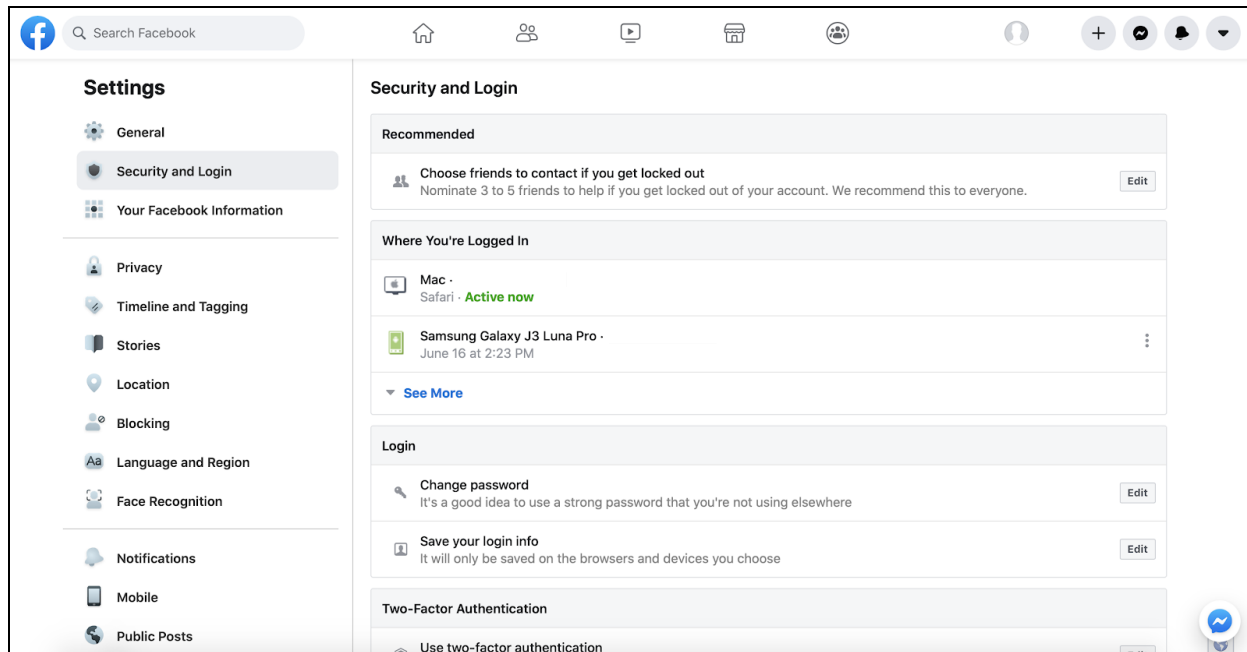


Now, click on **Settings**. You will see the following page:

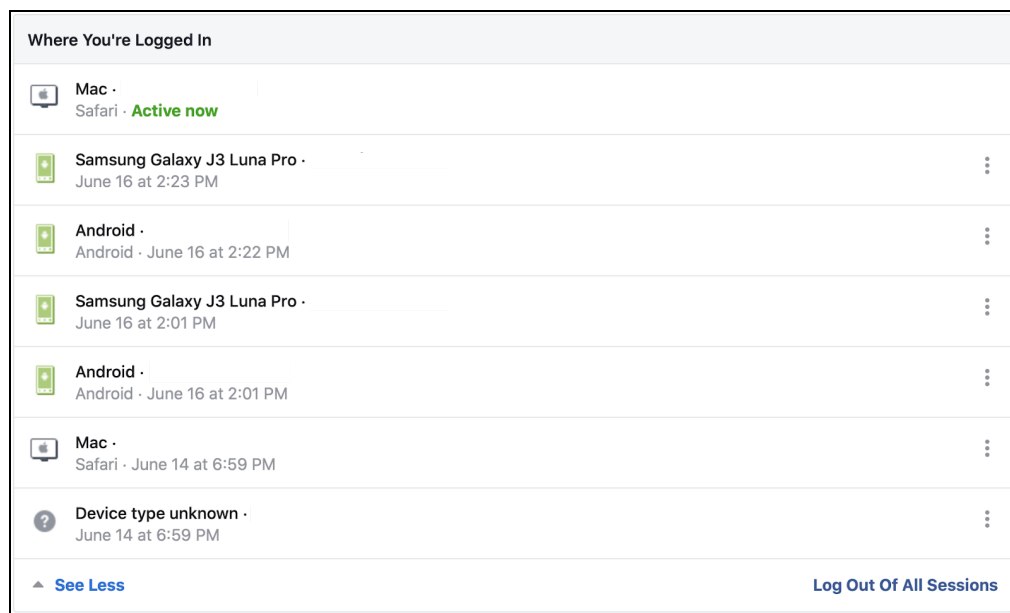


Step 3 - Check for Recent Logins

Click on **Security and Login** on the menu at the left hand side. You will be able to see a page like this:

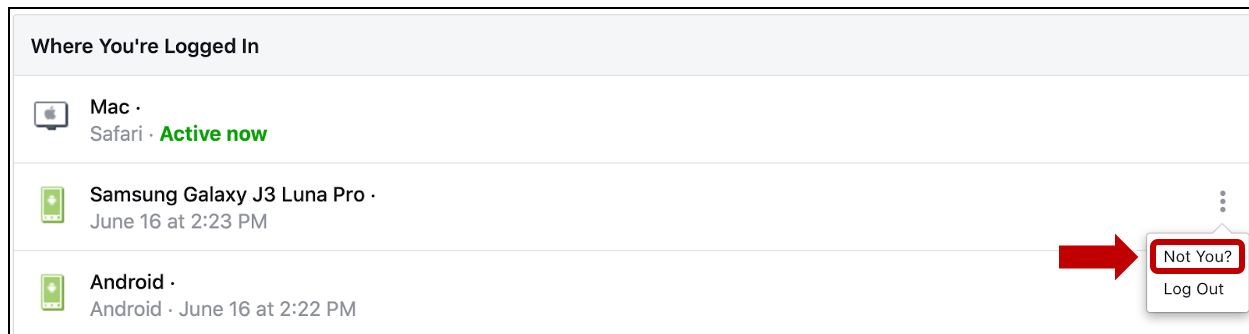


Look for the **Where You're Logged In** panel. In that panel, click on **See More** to see all the devices where someone is logged into your account.

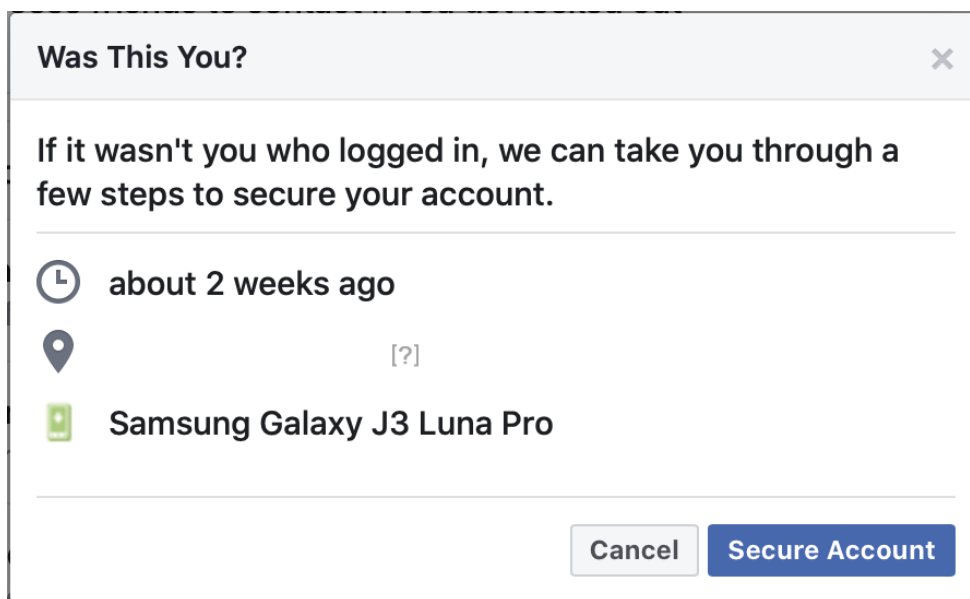


Each session you will see corresponds to a login to your account, and contains information about the device where someone signed into your Facebook account, the last time when that device logged in, and the browser or app that was used for the activity. (A browser is the program you use to visit websites. Examples include Chrome, Safari, Firefox, and Edge.)


In the **See More** window, you can check for more details about a specific login. To do this, click on the dots at the very right of the panel and click on **Not You?**



A popup window will appear:




If you want to log this device out of your Facebook account -- for example, if you think the device belongs to the abuser or someone else other than you --, you can do this by clicking on the **dots** at the very right of the panel and then clicking on **Log Out**:



Be careful!
This action could be visible to the abuser

Where You're Logged In

 Mac ·
Safari · **Active now**

 Samsung Galaxy J3 Luna Pro ·
June 16 at 2:23 PM


 Android ·
Android · June 16 at 2:22 PM

Not You?

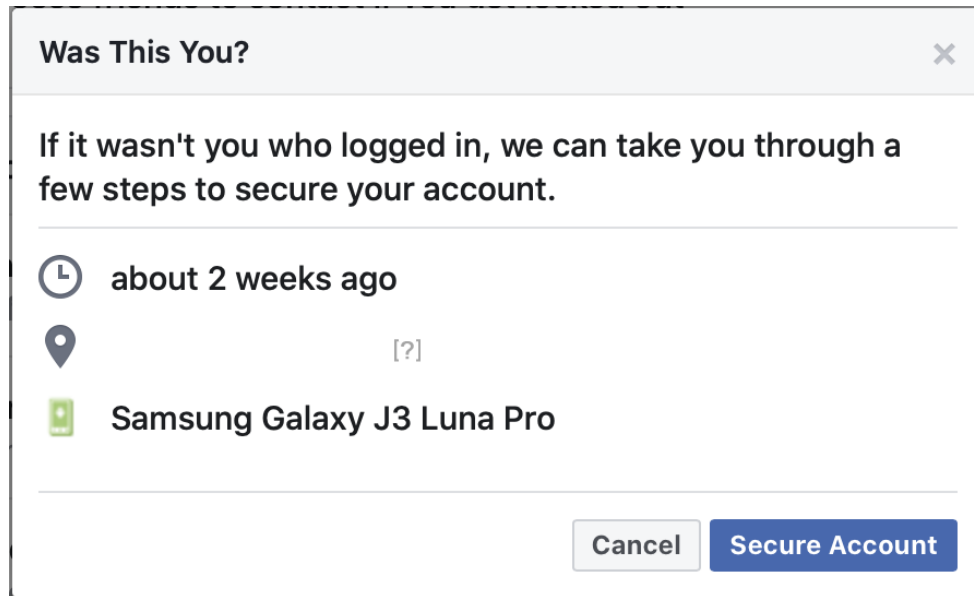
Log Out

If the abuser is logged into your account and you log them out, they could realize this immediately. You may want to talk to your caseworker or a domestic violence organization to make plans for your safety before taking this step.

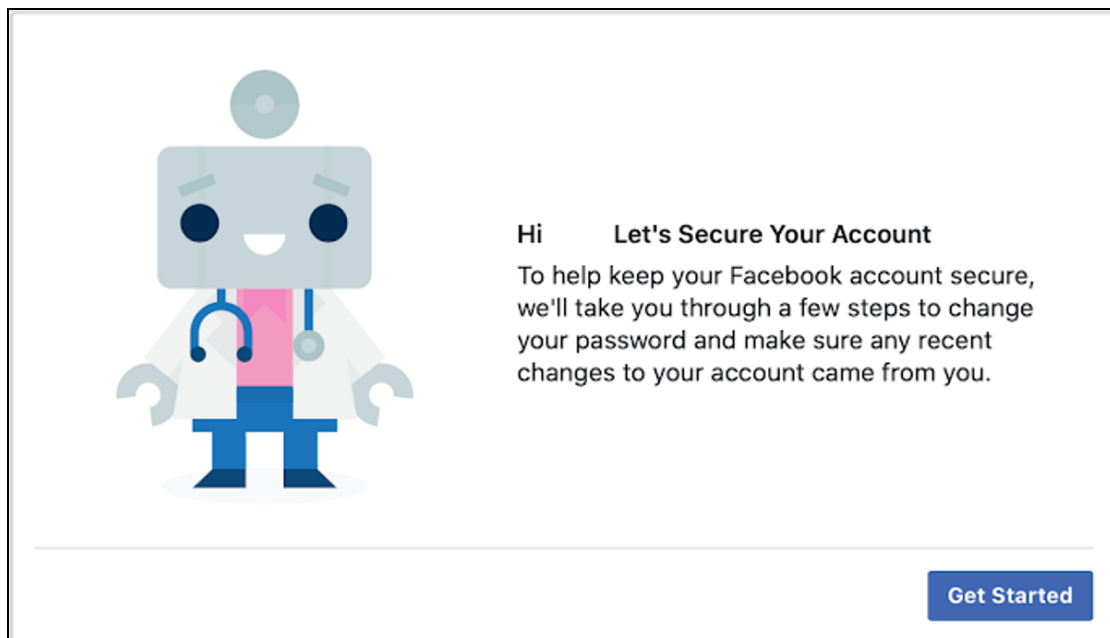
Step 4 - Secure Your Account



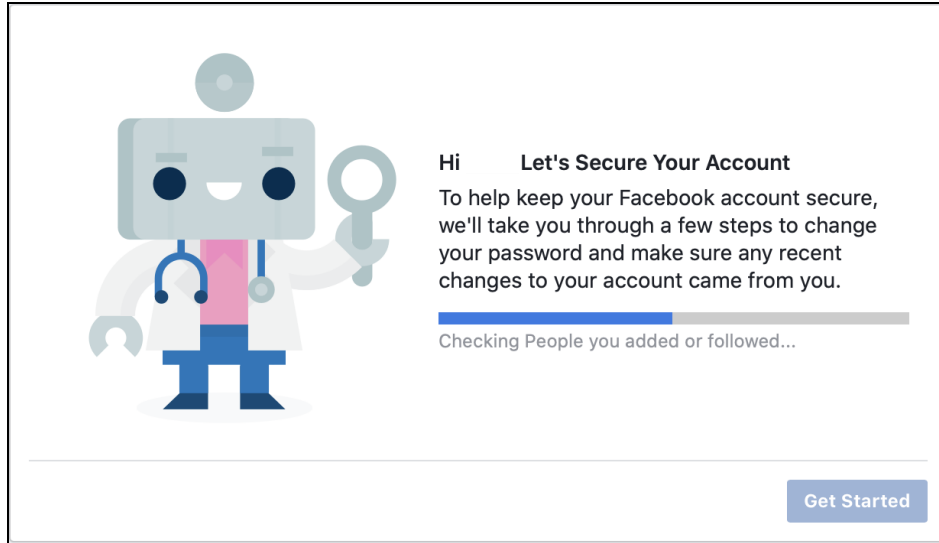
Be careful!
This action could be visible to the abuser



If you click on **Secure Account**, you will see something like this:



If you click on **Get Started**, Facebook will start a scan to detect any recent changes to your Facebook account:



After a few seconds, Facebook will recommend that you check some specific aspects of your Facebook account. You might see something like this:

Keep Your Account Secure

It looks like one change was made to your account. Now we'll help you change your password and look at the recent change to your account.

- 1 Password
- 2 Review your email address(es)

Continue

Click on **Continue**. In the next window, you can change your password:

Change Your Password

Please create a new one that you don't use anywhere else.

Current

New

Re-type New

Continue

After entering the information and clicking on **Continue**, you might see something like this:

Are there any email addresses here that you don't recognize?

These email addresses are all linked to your Facebook account.

☐ Added •

Skip

You will see all the email addresses that are linked to your Facebook account. The date when the email addresses were added to your Facebook account will also be shown. If there is an email address you do not recognize, you can select it using the **checkbox** and then click on the **Delete** button to remove it:

Are there any email addresses here that you don't recognize?

These email addresses are all linked to your Facebook account.

☒ Added •

Delete

Facebook might suggest other steps depending on the recent activity of your Facebook account. Here are some examples of what you might see:

Keep Your Account Secure

It looks like some changes were made to your account. Now we'll help you change your password, look at the recent changes to your account, and turn on extra security.

- 1 Password
- 2 Review your email address(es)
- 3 Select your username
- 4 Pages you liked or followed
- 5 People you added or followed
- 6 Posts

Continue

After you review all of the recommended aspects of your account, you will see something like this:

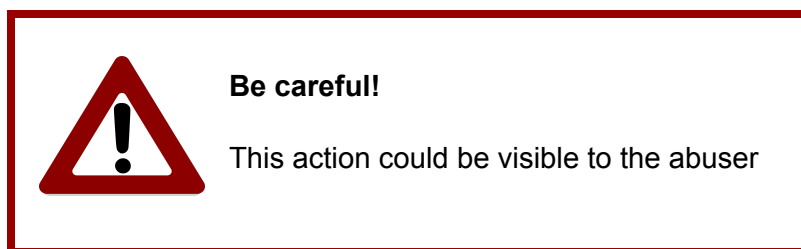
All Done!

Thanks for taking the time to secure your account.

- ✓ Password
- ✓ Review your email address(es)

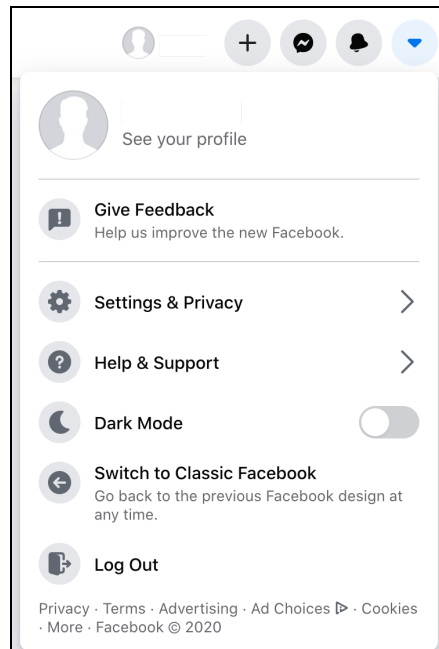
Go to News Feed

Step 5 - Check Recovery Email Address and Phone Number

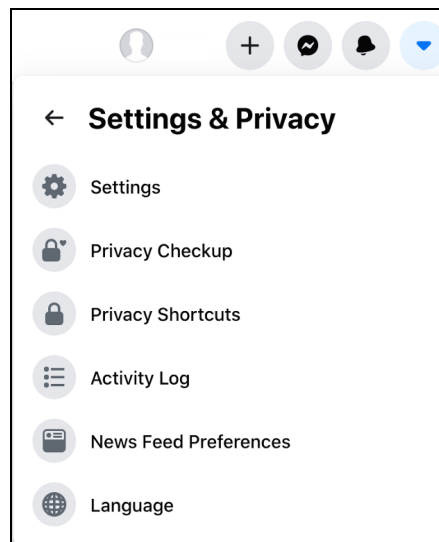


Often, abusers will change the recovery email address and/or phone number for your account to theirs, so they can keep access to the account.

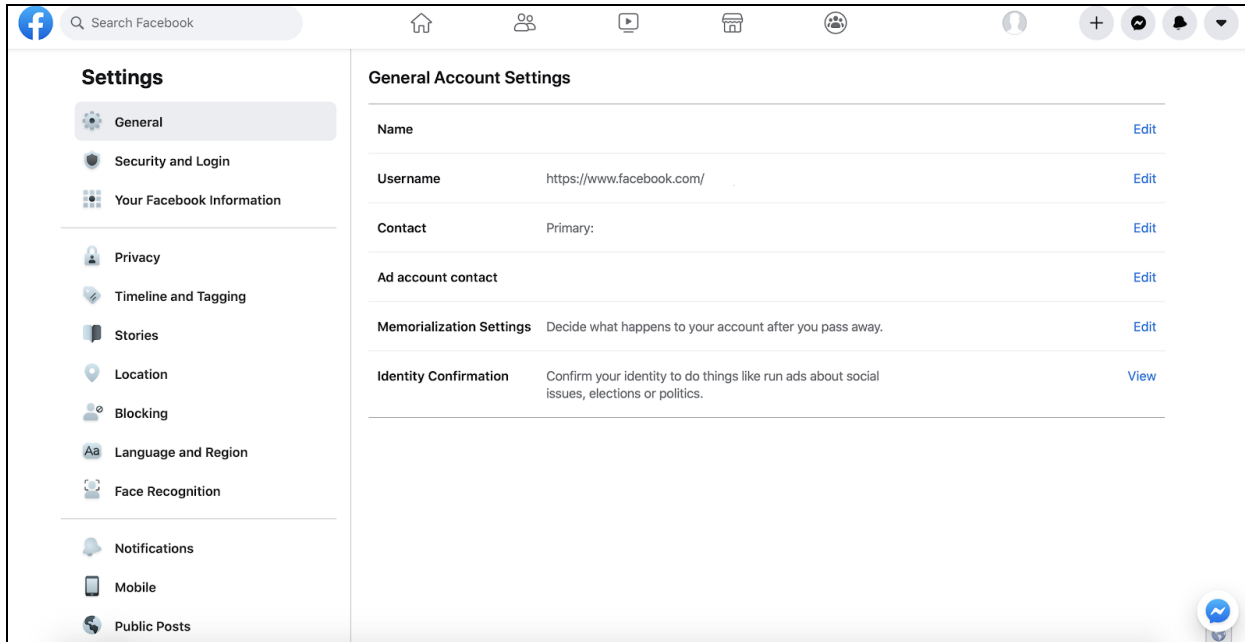
Click on the **downward triangle** at the top right corner of the screen:



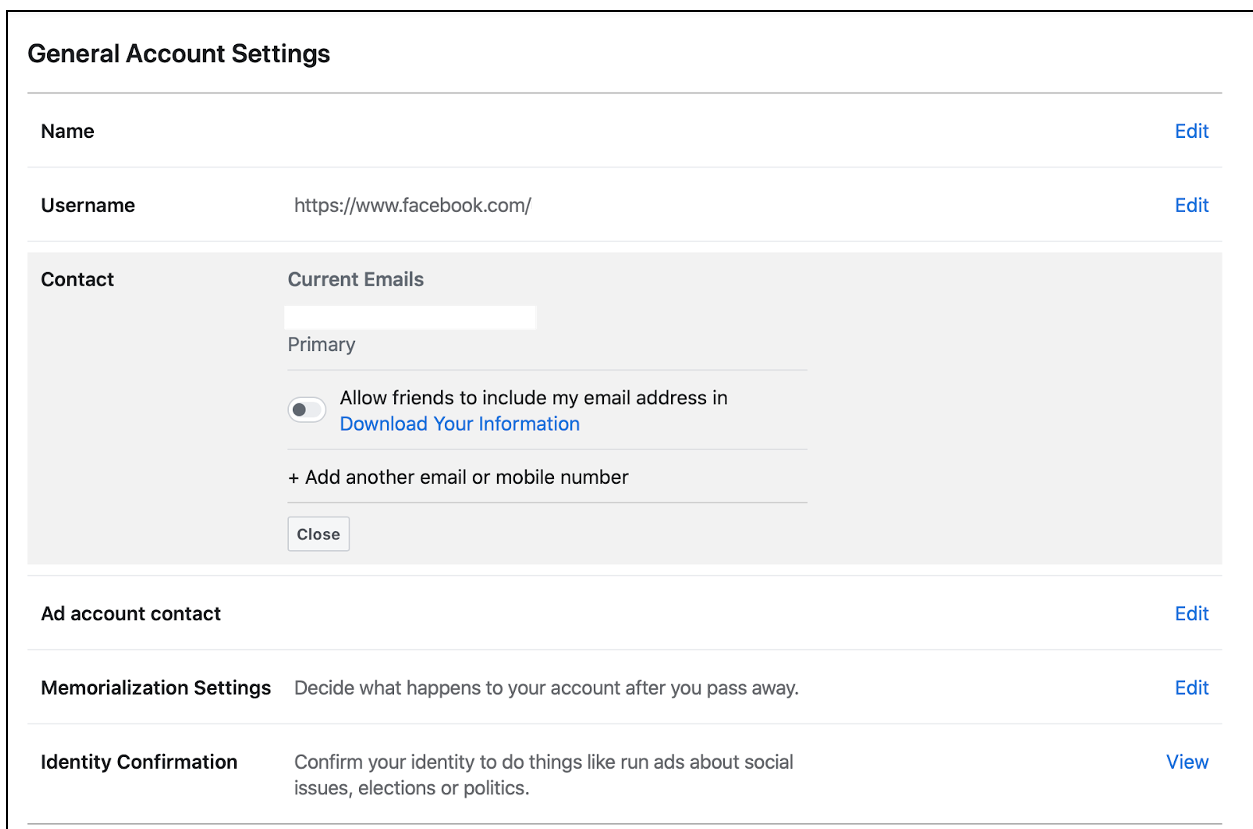
Then click on **Settings & Privacy**. You will see something like this:



Click on **Settings**. You will see the following page:



Now, click on **Contact** in the General Account Settings panel:

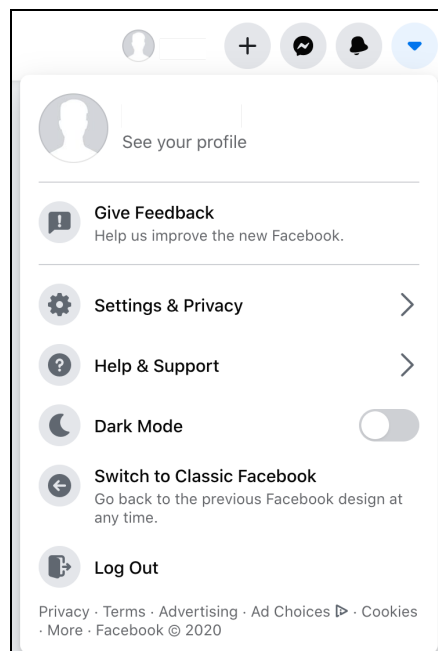


Check that the emails and phone numbers you see are safe ones. If any of these are controlled by your abuser, then that person could regain control over your Facebook account even if they do not know your password.

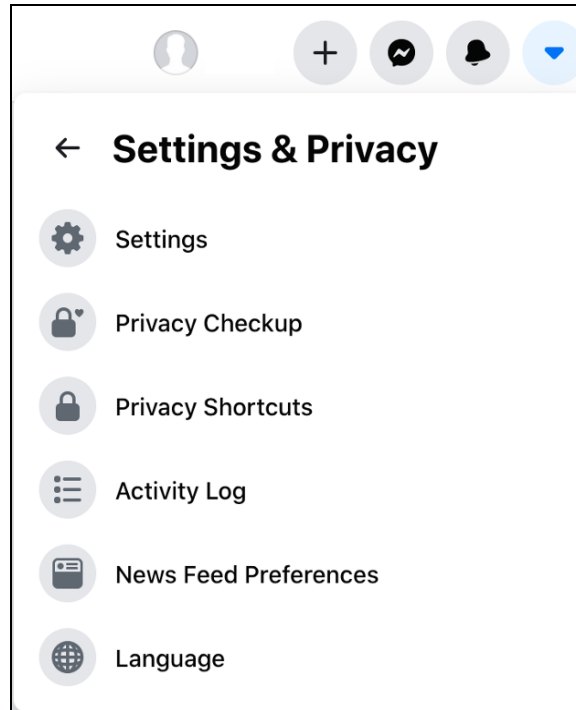
To fully recover your Facebook account, make sure you only use a safe email and/or safe phone number.

Step 6 - Do the Privacy Checkup

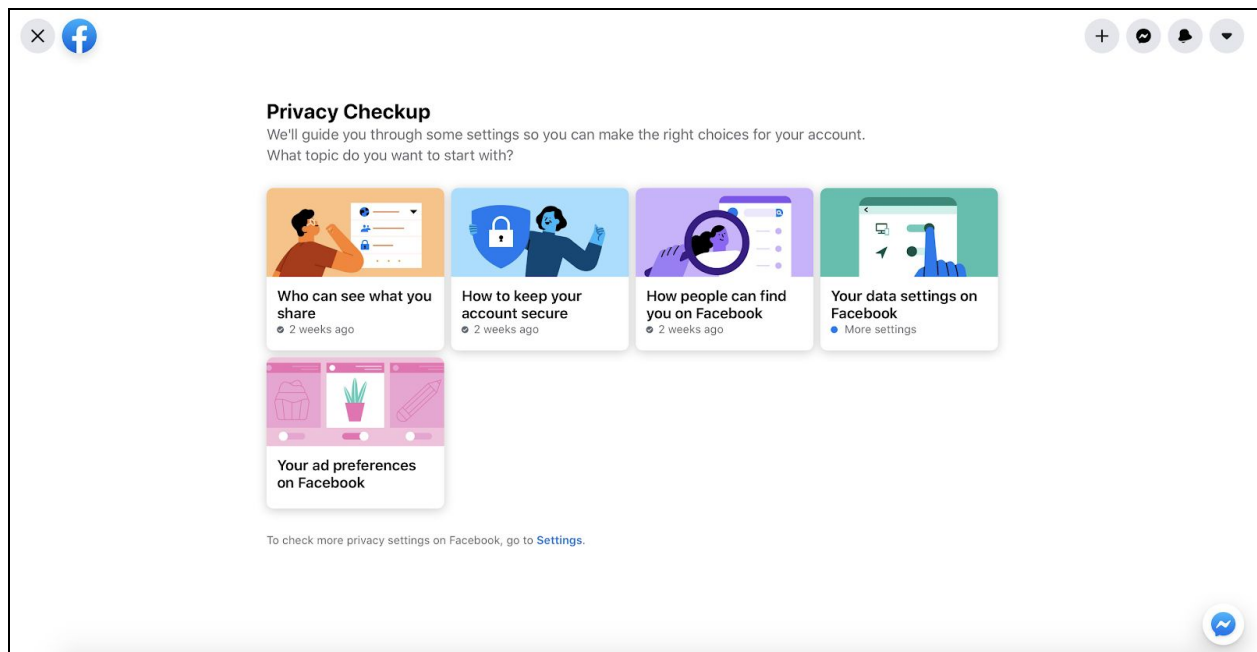
Click on the **downward triangle** at the top right corner of the screen:




Then click on **Settings & Privacy**. You will see something like this:



Click on **Privacy Checkup**. The following screen will appear:



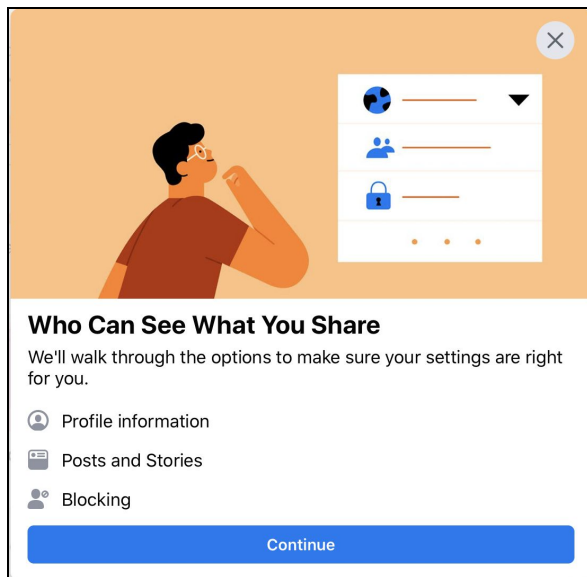
Facebook will show you some different ways to review your privacy and security settings. We recommend you to have a look at all of the options shown.




Be careful!

This action could be visible to the abuser


For example, if you click on **Who can see what you share**, the following will appear:



Click on **Continue**. The following box will appear:




Profile Information





Please review this info from your profile and decide who you're comfortable with seeing it. Your profile may have more than is listed here.


Email

 Only me

Birthday

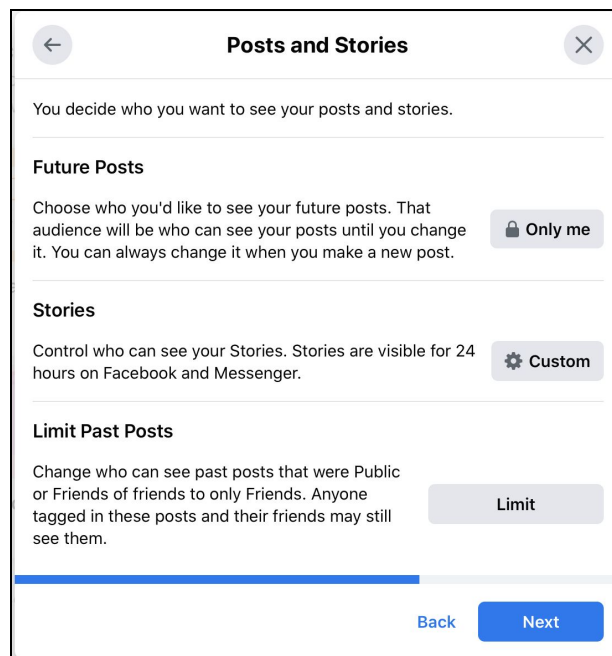
 Tip: Your friends might miss wishing you a happy birthday when is set to Only me. If you want them to be reminded, you could set to Friends.

 Only me

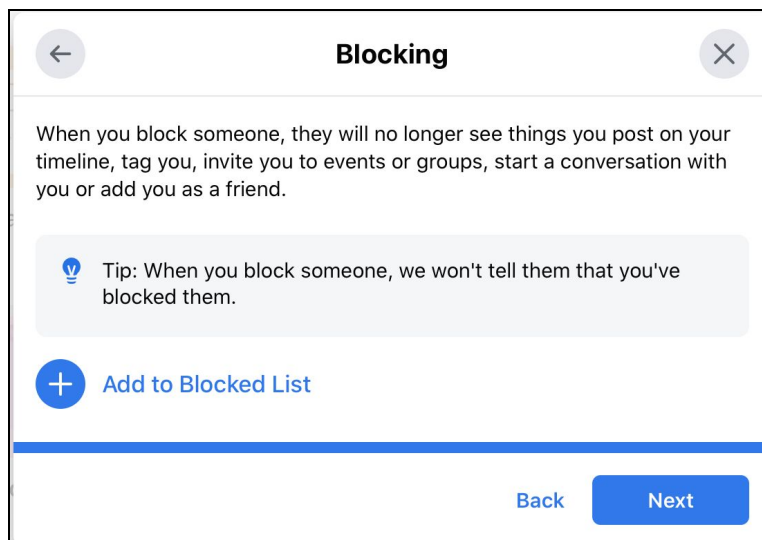
 Only me

[Back](#)[Next](#)

On this screen, you can change who can see your email and birthday. If you want to move on, click on **Next**. The following box will appear:

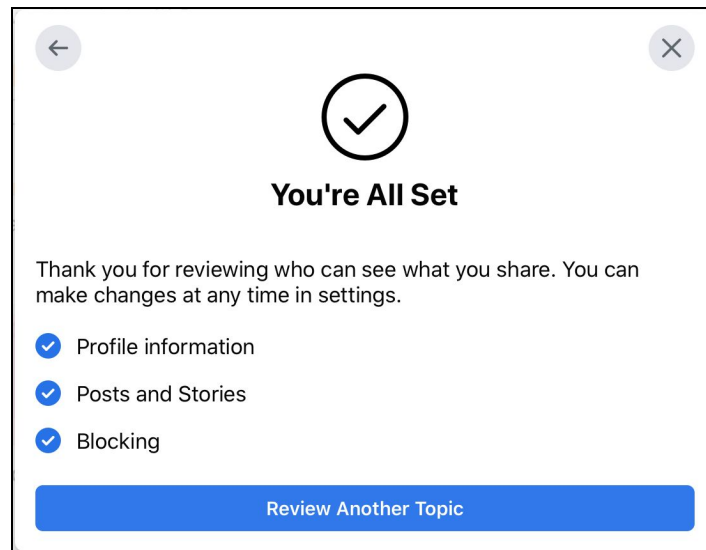


On this screen, you can change who can see your future posts and stories. Additionally, you can change who can see your past posts. When you want to move on, click on **Next**. The following box will appear:



On this screen, you can add someone to your "Blocked List." If you block someone, that person will not be able to see what you post, they will not be able to tag you, nor invite you to events and groups, start a conversation or add you to their friends list.

To move on, click on **Next**. The following box will appear:



If you click on **Review Another Topic**, you will be taken to the main page for Facebook's privacy checkup main page.

Finally, we also recommend you to turn on two-factor authentication to strengthen your account security. You can view our guide to turning on two-factor authentication for Facebook by clicking here:

https://82beb9a6-b7db-490a-88be-9f149baf221.filesusr.com/ugd/c4e6d5_01e4e6e33987443ea2244afcd7880706.pdf .

You can also find our guide by going to <https://www.ceta.tech.cornell.edu/resources>.

Two-factor authentication is an extra security step that can help keep your account safe and private even if somebody else knows or guesses your password.

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