

Your Facebook Account Was Hacked? 4 Things to Do Immediately

makeuseof.com/tag/4-immediately-facebook-account-hacked

December 11, 2019

By Tina Sieber Updated Mar 04, 2022

Suspect your Facebook account was hacked? Learn how to find out for sure, and steps you should follow to fix it.



The silent struggle of thousands of Facebook users whose accounts have been hacked outside of major breaches rarely makes headlines. Facebook itself doesn't offer much but a wall of silence. Are you sure your account hasn't been compromised?

If you suspect that your Facebook password was leaked or that your account was breached, act fast! Facebook hackers could lock you out of your account and hassle your friends and family. Secure your Facebook account now and get it back before it's too late. We'll show you how.

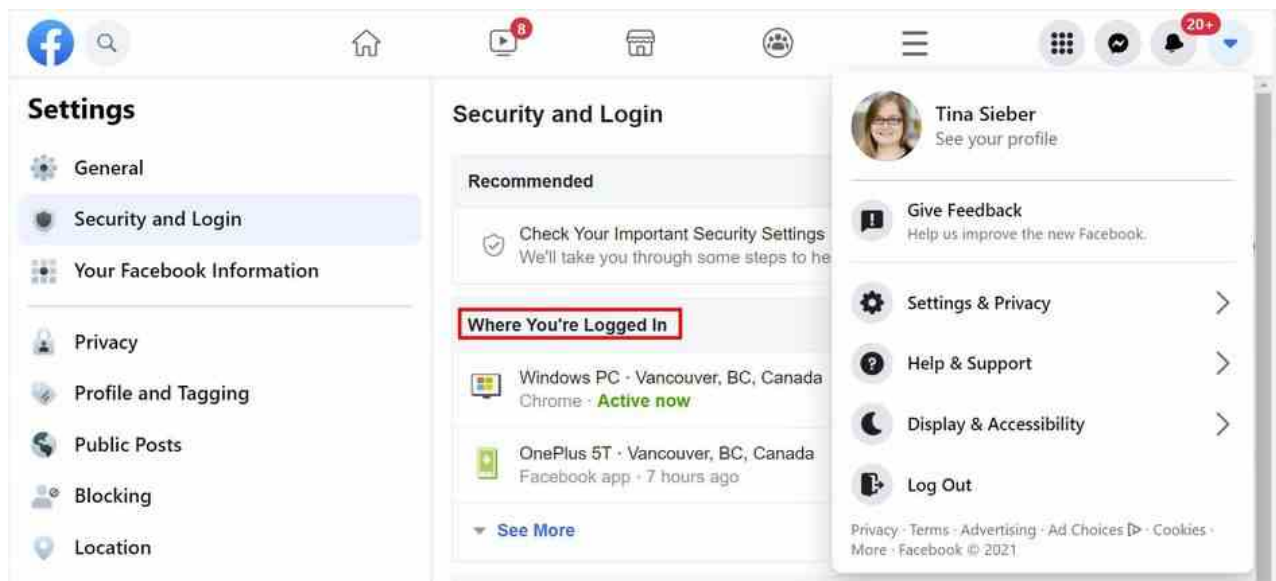
How to Know Whether Your Facebook Account Was Hacked

So, how do you know if your Facebook account was hacked? If a Facebook hacker manages to get into your account, they will leave a trace.

To check for traces, log into your Facebook account and click the **arrowhead** in the top right to expand the Account menu. From that menu, pick **Settings & privacy > Settings** and go to **Security and Login**.

Related: [How to Recover Your Facebook Account When You Can't Log In](#)

At the very top, you'll see a list of devices from which you've most recently logged into your Facebook account and when they were active.



Other signs that your account may have been hacked include:

- Your personal data, including your password, email address, phone number, or name were changed by a third party. Within **Settings > General**, check your full **Contact** information, i.e. click the respective field to expand it. You can see all phone numbers associated with your account under **Settings > Mobile**.
- Friend requests and private messages were sent from your account without you doing. Within **Settings**, go to **Your Facebook Information > Access Your Information** and look over the various details there.
- Your timeline contains posts you didn't add or permit. To see your timeline, click your profile picture in the top right or, if you can't see it there, click the hamburger menu icon, then you should see your picture in the top left.

If you're using Facebook to log into other applications, like Spotify or Instagram, we strongly recommend changing the respective logins or tightening your Facebook security to secure these third-party accounts.

If you spot any suspicious activity in your logins or have seen one or more of these other signs, you'll find what you need to do below...

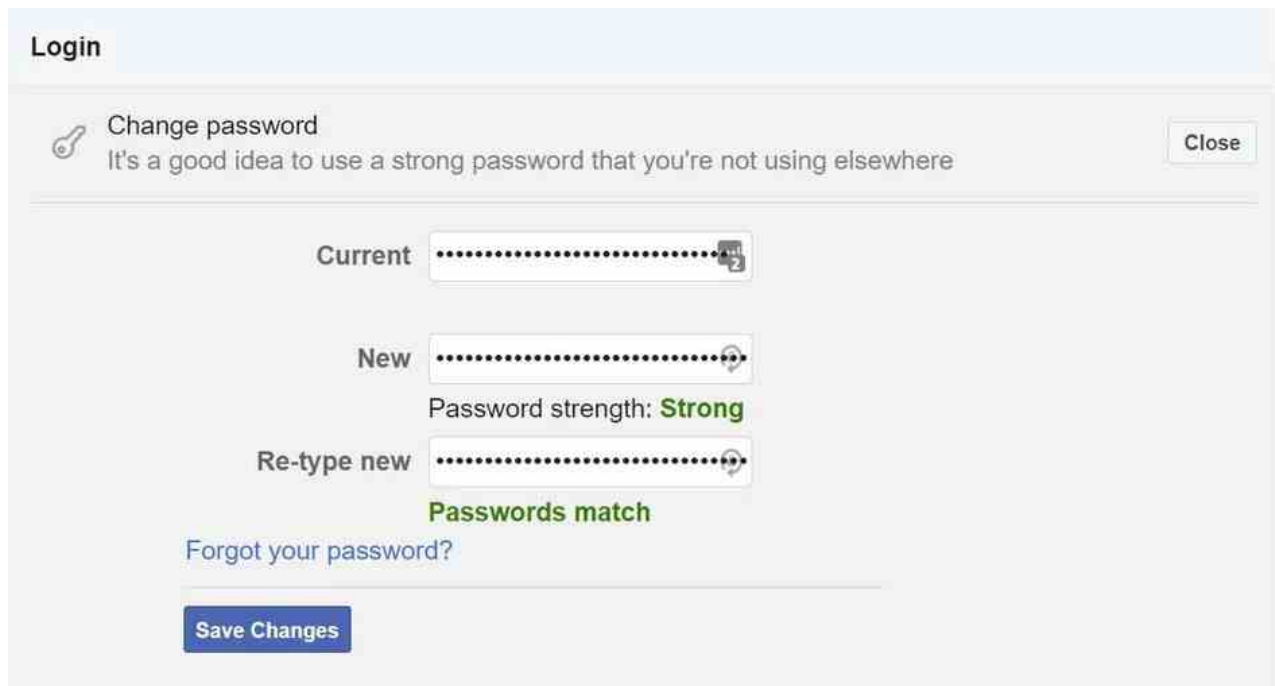
What to Do If Your Facebook Account Was Hacked

If you have confirmed that your account has been compromised, here are the steps you should follow...

1a. Change Your Facebook Password

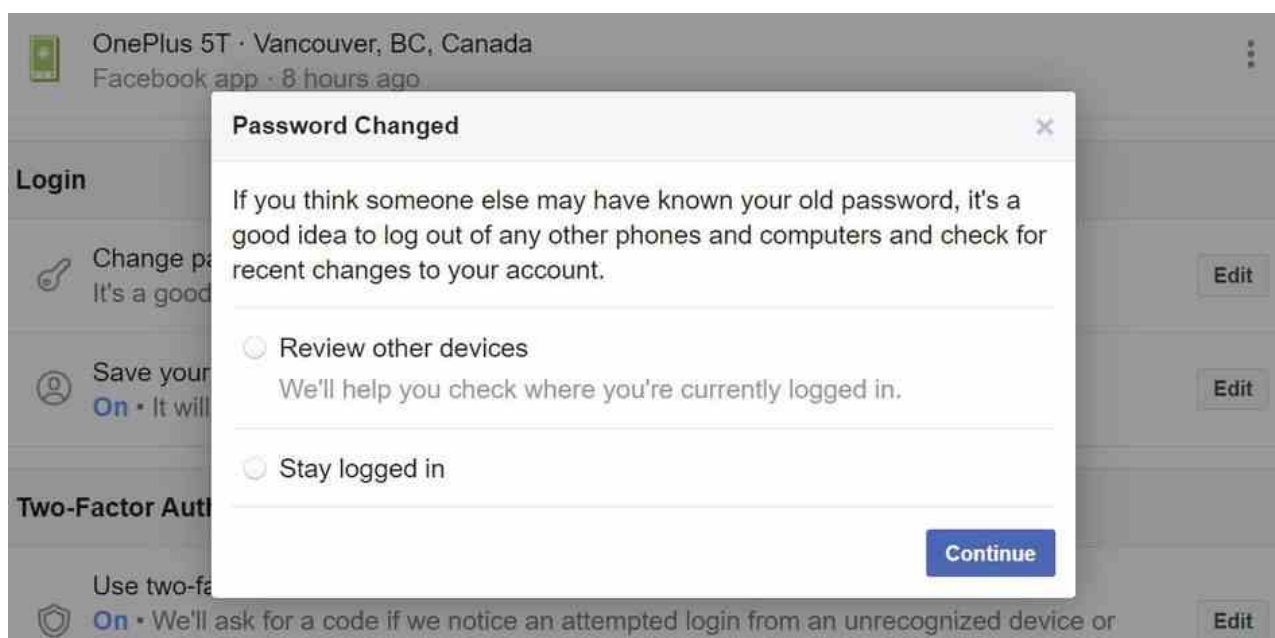
In case your Facebook hacker hasn't changed your password, you got lucky! Immediately update your password **before** you log out of suspicious sessions (you don't want to alert the hacker). If it's too late, head to step 1b.

Under **Settings > Security and Login**, scroll down to **Login** and click **Change password**. Enter your current password, set a strong new password, and click **Save Changes**.



The screenshot shows the 'Login' section of the Facebook settings. At the top, there is a 'Change password' option with a key icon and a 'Close' button. Below this, a message states: 'It's a good idea to use a strong password that you're not using elsewhere'. The form contains three password input fields: 'Current', 'New', and 'Re-type new'. The 'New' field has a strength indicator showing 'Strong' in green. Below the 'Re-type new' field, it says 'Passwords match' in green. There is a link for 'Forgot your password?' and a blue 'Save Changes' button at the bottom.

Next, you should see a **Password Changed** confirmation window that lets you **Review other devices** or Stay logged in. Choose the former and click **Continue**. In my case, this actually didn't do much, but it's nice to see this reminder.



The screenshot shows a 'Password Changed' dialog box overlaid on the Facebook settings page. The dialog has a title bar with a close button (X). The main text reads: 'If you think someone else may have known your old password, it's a good idea to log out of any other phones and computers and check for recent changes to your account.' Below this, there are two radio button options: 'Review other devices' and 'Stay logged in'. The 'Review other devices' option is selected. A blue 'Continue' button is at the bottom right of the dialog. The background shows the 'Login' settings page with the 'Change password' option and a 'Save your session' option.

Log Out of Facebook Sessions

After changing your password, scroll back up to **Where You're Logged In**. Either **Log Out** of individual sessions by clicking the three vertical dots or click the **Log Out Of All Sessions** option in the bottom-right after expanding the list.

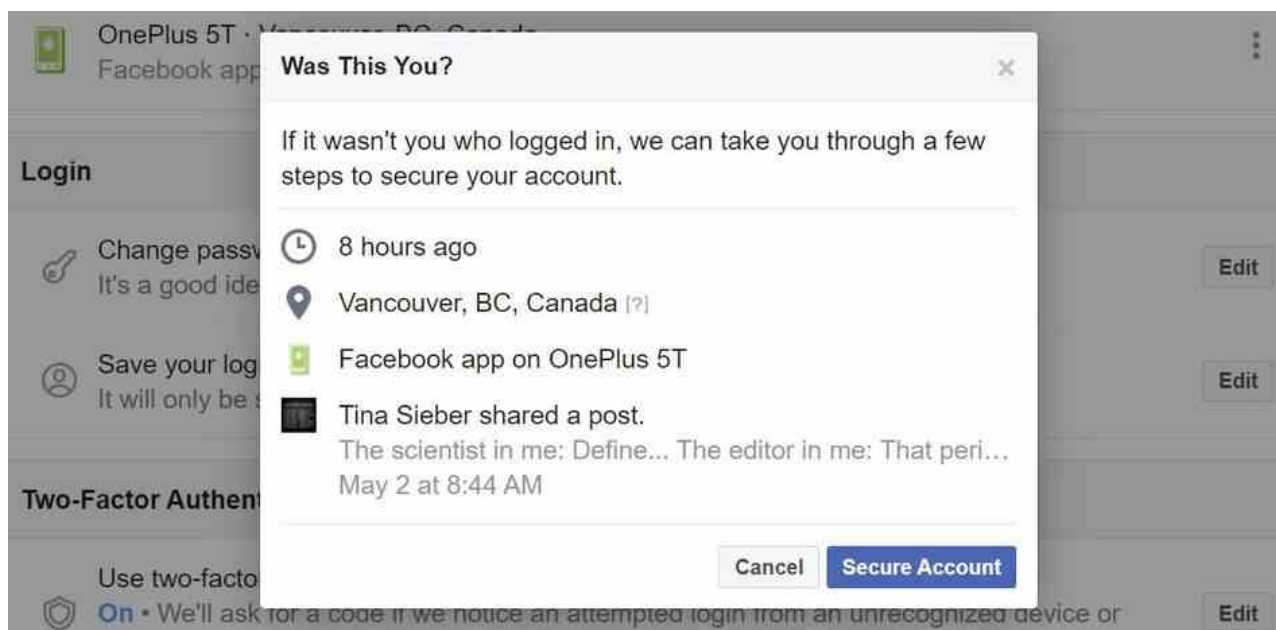
Do this only if you're sure you can log back in.



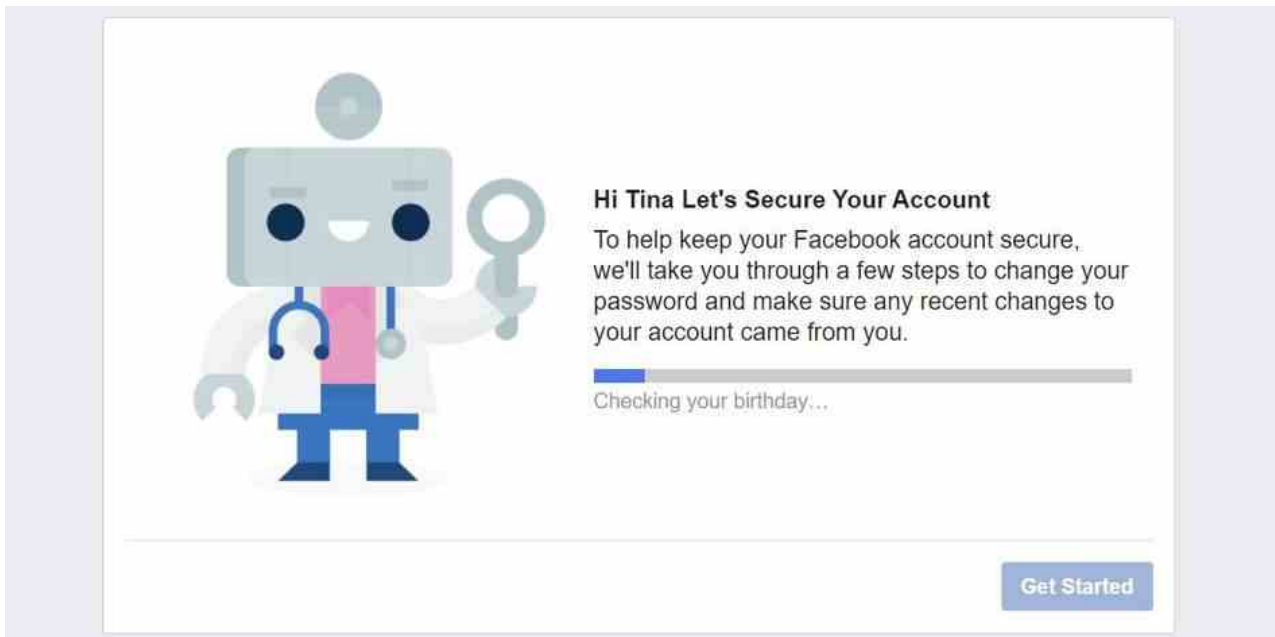
We recommend logging out completely, provided your contact details and security settings are up to date. You don't want to jeopardize your means of logging back in. If you're unsure, manually log out of all recent sessions that seem suspicious.

Secure Your Account

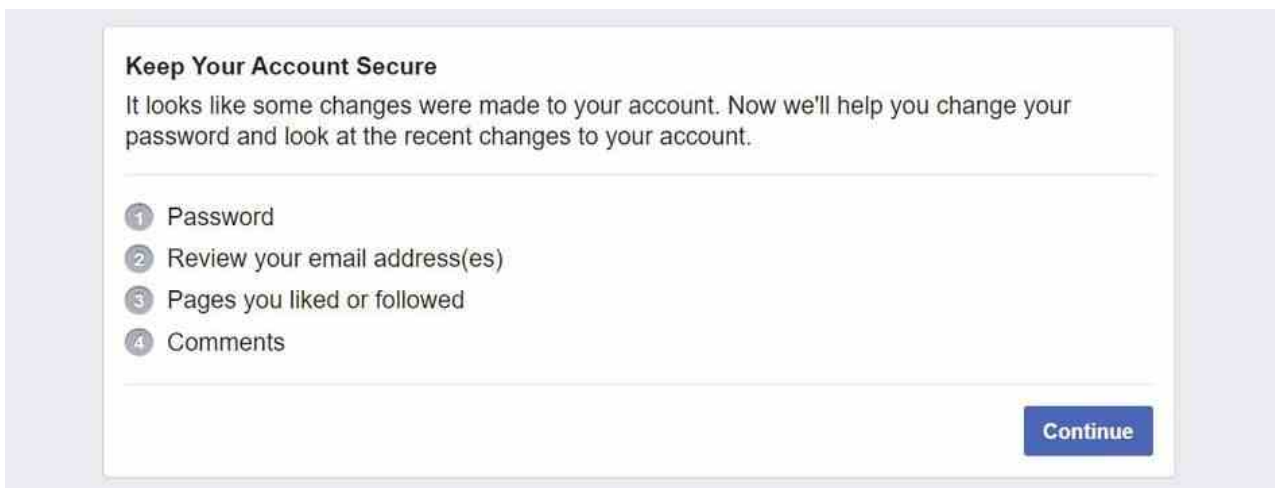
You also have the option to earmark individual sessions as **Not You**. This will bring up a pop-up showing details of that session.



Click **Secure Account** if you don't recognize the location, device, and last activity. Click **Get Started** to trigger an automated step-by-step process of securing your account.



The next screen summarizes the steps of the process. Click **Continue**.



When you're done, you'll be sent back to your feed. If you still think your account has been compromised, proceed to Step 3.

1b. Reset Your Facebook Password

If the hacker did change your password, and you need to recover your Facebook account, act quickly. Try to regain access. There is a **Forgot your password?** link underneath the Facebook login:



This will let you retrieve your password in several ways. First, you'll have to **Find Your Account**. You can either enter the email address you used to register with Facebook or any other secondary email address you added, as well as your phone number.

Find Your Account

Please enter your email or phone number to search for your account.

Email or phone

Search Cancel

If Facebook can find your account, you can choose how to **Reset Your Password**.

If the hacker changed your email address, you should have received a message to the original address. Find this message because it contains a special link that will let you reverse the change and secure your account.

In my case, Facebook offered to send a recovery code to any of the email addresses I added to my account. We highly recommend that you specify multiple backup email addresses. Remember that you must keep those accounts equally secure, at least by using a strong password and ideally by enabling two-factor authentication on your email accounts.

Reset Your Password

How do you want to get the code to reset your password?

Send code via email

Send code via text message

Tina Sieber
Facebook User

No longer have access to these? Continue Not You?

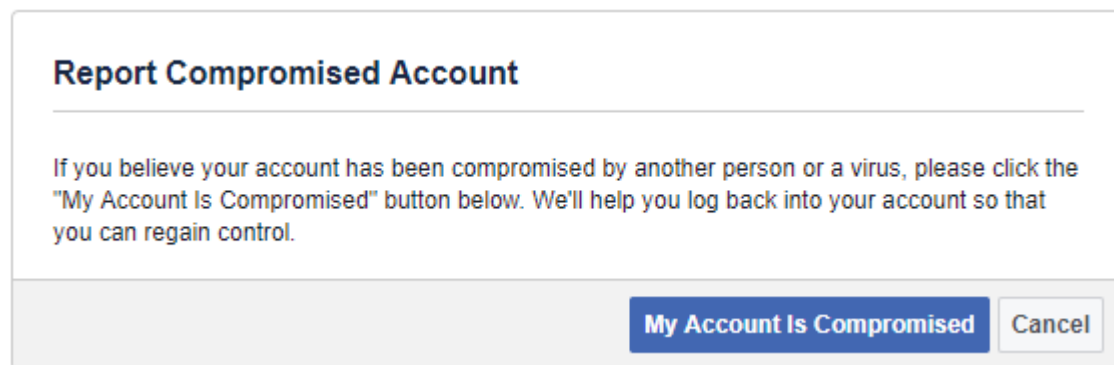
You can see your name and profile picture because you're using a computer network you've logged in on before.

Use the **No longer have access to these?** link if that's the case. Facebook will ask how they can reach you to verify your identity. This can take a while.

If you believe that the Facebook hacker who has access to your account has been abusing it, proceed to step 2.

2. Report the Facebook Hack

If your account wasn't simply hacked, but is sending out ads and spam to your friends, you must report it as compromised to Facebook using [Facebook.com/hacked/](https://www.facebook.com/hacked/).



You can also use this in case you have lost access to your account by means of a phishing attack. Facebook will help you recover access to your account.

3. Remove Suspicious Applications

Oftentimes, it's not an evil person that randomly hacked your account. You may just have granted access to a malicious Facebook application that subsequently hijacked your account.

To remove suspicious applications, go to **Settings > Apps and Websites** and go through the list. Click **See More** to expand the list of **Active** apps and websites, set a checkmark on apps or websites you'd like to remove, click the **Remove** button in the top-right, and confirm whether you'd also like to "delete posts, photos or events posted on your timeline" from these sources.

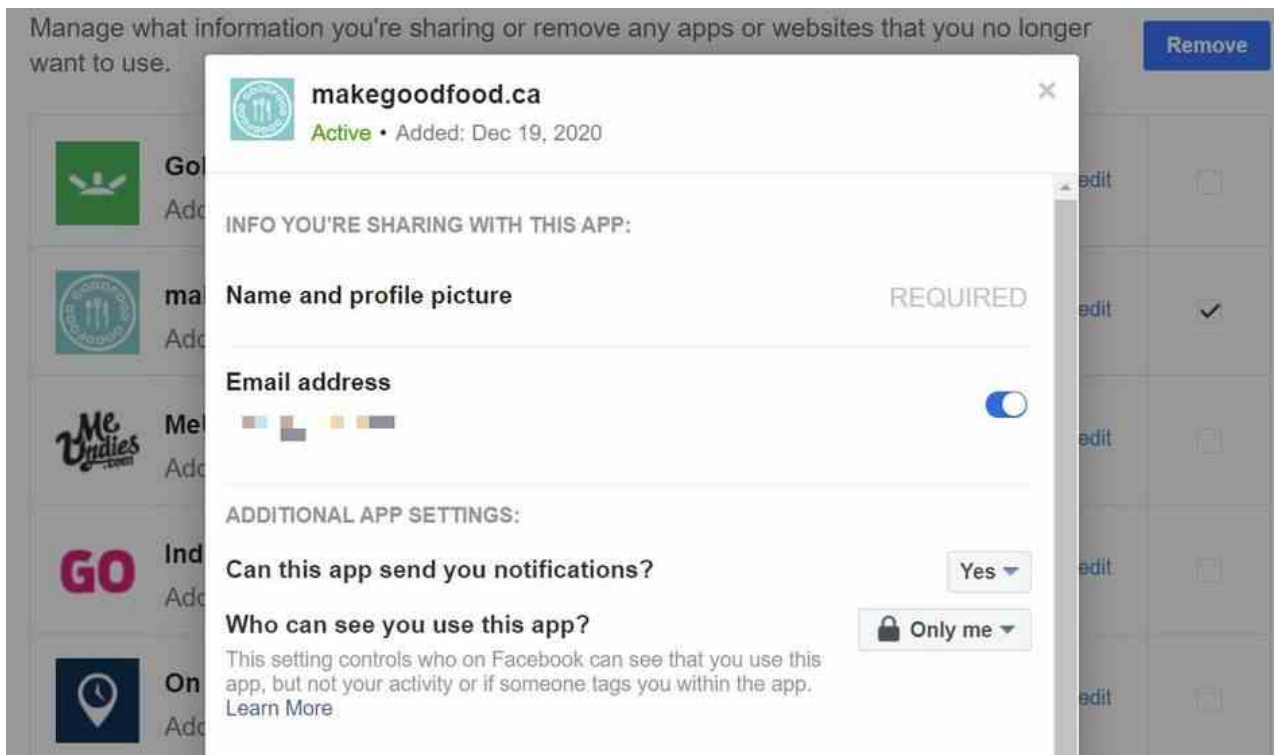
Apps and Websites

These are apps and websites you've used Facebook to log into. They can receive information you chose to share with them. Expired and removed apps may still have access to information that was previously shared with them, but can't receive additional non-public information. [Learn More](#)

A screenshot of the Facebook "Apps and Websites" settings page. At the top, there are three tabs: "Active" (with a count of 13 and a red box around it), "Expired", and "Removed". To the right is a search bar labeled "Search Apps and Websites" with a magnifying glass icon. Below the tabs is a blue "Remove" button. The main content area shows a list of two items: "GoFundMe" (added on Apr 11, 2021) and "makegoodfood.ca" (added on Dec 19, 2020). Each item has a "View and edit" link and a checkbox. The checkbox for "makegoodfood.ca" is checked and has a red box around it.

We also recommend removing all **Expired** apps and websites.

Alternatively, click the **View and Edit** link and change the app's permissions, which includes options like app visibility, access to your personal information, and actions it can take.



4. Do Damage Control

After doing everything you can to regain control over your hacked Facebook account and preventing further damage, inform your friends and family about what is going on.

This is a precautionary step in case the hacker has used your account to reach out to people. If you presently can't access your account, contact your Facebook friends through other social networks, by email, or have a mutual friend inform them via Facebook.

Improving Facebook's Privacy and Security Settings

Once you're back in control, we highly recommend that you review your Facebook settings.

- Under **Settings > General**, update your contact details, and add additional email addresses or mobile phone numbers that you have access to. Likewise, remove those you no longer have access to.
- Head to **Settings > Security and Login** to set up extra security measures, including alerts about unrecognized logins, two-factor authentication, and choose three to five trusted friends who can help you to recover your account should you get locked out.
- Under **Settings > Privacy**, choose the privacy settings you're comfortable with. We recommend letting only friends see your future posts and retroactively limiting the visibility of past posts.

Note that the single most important security feature you can enable on any of your accounts is two-factor authentication. We strongly recommend that you set up two-factor authentication on your social accounts that offer this feature. You can use Microsoft

Authenticator and Google Authenticator with Facebook.

How Do You Keep Your Facebook Account Safe?

Once you get hacked, you're forced to learn about all the mistakes you made. And hopefully, you'll never make them again.

This is the time to learn how hackers can attack your privacy and how to protect yourself against them. Hackers never stop evolving, so your knowledge of their tactics needs to keep up.

About The Author

Tina Sieber (840 Articles Published)

While completing a PhD, Tina started writing about consumer technology in 2006 and never stopped. Now also an editor and SEO, you can find her on Twitter or hiking a nearby trail.

