

How to Report Compromised Facebook Account

TechRounder PDF Edition

Live article: <https://www.techrounder.com/social-media/how-to-report-compromised-facebook-account/>

By Vipin PG | Published February 7, 2023 | Updated October 7, 2026 | Format: Guide | 6 min read

Quick answer

If your Facebook account is compromised, these are the steps that matter: report it, secure the login, and get access back.

One of the most used social media platforms across the globe is Facebook, with over a billion users on the platform, making it one of the biggest targets for scammers and hackers. There are various ways to hack a Facebook profile; it can be through a phishing scam or can also be done by getting access to some of your most personal as well as sensitive information, eventually making you lose a lot.

So, if you've faced the same or someone you know has got their Facebook account hacked, you must go through this article to learn how to report a compromised Facebook account and how to secure one to keep it safe from hackers.

First and foremost, to report a Facebook hacked account, it is important to recognize that your account has been compromised.

How to recognize a hacked Facebook account?

There's no one way to tell you your account has been compromised. Firstly, you'll need to check whether or not there's unauthorized access in your account and to check this, follow these basic steps:

1. Tap on your profile picture and head to the settings & privacy menu; under this, tap on the settings option.
2. Scroll down, choose Security, and log in under the security menu.
3. You'll see all the devices that have your account logged in. You can remove any suspicious device by tapping on the logout option next to the device.

In case you don't find any suspicious device in the list, the other ways to check for a Facebook hacked account, such as:

- If your password or email address has been altered.
- Change in name or date of birth.
- Friend requests have been sent to strangers.
- The appearance of posts on the timeline which were not posted or created by you.

How to report a compromised Facebook account?

Once you've recognized a hacked account, you'll now want to report the compromised Facebook account. The social media platform allows you to report and recover Facebook hacked accounts or an account that has been misused. You need to follow these simple steps to redeem your account:

1. Go to [Facebook.com/hacked](https://www.facebook.com/hacked).
2. A list of reasons will appear on your screen, mentioning why you think your account was compromised. Tick the one you think is most appropriate about your account and click continue.
3. You'll be headed to a page to secure your account settings. Click on get started, and the tool will assess the application, passwords, email address, and more.

4. Once it is done analyzing, it will allow you to change your account's password and review your email ID.
5. After checking all the vital details, click on continue and follow the instructions on your screen to recover your Facebook hacked account.

You will need to recover your account even if the email address that was associated with your account has been changed. Also, always take note that Facebook does send a notification along with a link to your old mail ID whenever there's an update on the email address in your account, and by clicking on the given link, you can then and there reverse the change in email ID and secure your account.

Sometimes, your account has not been compromised, but someone is impersonating you or someone you know by creating a different profile by your name or their name. It is essential to report such accounts and stop them from performing a scam in your name. To report the account through a Facebook application or on the Facebook browser, follow these steps:

1. Visit the profile of the person that is impersonating someone.
2. Click on the three dots icon right under the profile's home page cover photo.
3. You'll see a pop-up menu if you're opening it on a browser or will be headed to a different page if you're opening it on the Facebook application.
4. Tap on a report or find the support or report option.
5. Now select a valid reason from the list for reporting the account and tap to submit to report the account successfully.

Once you report the account, Facebook will look into it, and if they find anything suspicious, they'll ask the person to verify the account. In case of failure of verification, the account gets closed.

How to secure your Facebook Account?

It is very important to keep your account safe; no matter if it has been hacked or not, precaution is necessary so that you don't compromise your Facebook account. So follow these tips to secure your account and keep it safe.

Use two-step verification: You may protect your Facebook account by using the two-step authentication tool that Facebook has introduced. When you access your Facebook account from a mobile device or a browser, the feature enables you to provide a unique login code to authenticate your login attempt each time. To activate this option, adhere to the following steps:

1. Go to the settings & privacy menu by tapping your profile image, then select the settings option.
2. Under the security option, scroll down and select Security and login.
3. Scroll down to two-factor authentication and tap on Use two-factor authentication.
4. You'll now see various options for the type of two-step authentication process you want to set.
5. If you tap on the Authentication app, Facebook will ask for your password to verify it's you. Then, if you select Text message, Facebook will ask for the contact number you want to receive the text message on, after which it'll send a code to the number provided to verify the number. It'll also ask for your password once you verify your phone number. There's also an option for a physical security key which you'll need to register once you select this option.
6. After the verification of each step, two-factor authentication will be activated on your account.

Receive alerts about unrecognized login: Facebook users can now configure alerts for unauthorized login attempts from their accounts. This security feature warns you when someone tries to log in using a different computer or web browser. In addition, the notifications will reveal further information about where the login attempt originated. Here's how to make it possible:

1. Go to the settings & privacy menu by tapping your profile image, then select the settings option.
2. Tap on 'Get alerts about unrecognized logins' under the Setting up extra security option.

3. You'll get two options, notification and email, and you can turn on both for better Security. You'll be asked to enter your password to verify and then tap on save to enable the notifications.

Some of the things to always keep in mind for better Security of your account:

- Always remember to log out from a device that is not yours. Also, ensure to log out if you're using an office laptop or system. This will surely prevent someone else from accessing your account.
- Always set a strong password. You should create a password that is easy to remember but difficult for others to crack. Never use your email address, phone number, date of birth, or other sensitive information when creating a password. Mixing letters, numbers, and special characters are typically advised to create a strong password. Using the strong password suggestion function in Google Chrome or Safari, you can create a password using random characters and store it in your Google or iCloud account.
- Do not share your login details with anyone. One of the most vital pieces of advice is never to divulge your login information to anyone. Scammers may create fake Facebook-like websites that ask you to sign in with your email address and password. Before you type in your login details, ensure you're on the correct website. Simply enter www.facebook.com into your browser to visit Facebook if you are unsure.
- Monitoring your computer for any potentially harmful malware is essential. To keep your sensitive information safe, regularly scan your computer for viruses, malware, and other threats and promptly remove them.

How to secure your Facebook account using the Facebook Security Checkup?

By running a Security Checkup on your account, Facebook also allows you to safeguard it. In essence, the function informs you whether your password is secure enough, whether two-factor authentication is enabled, and how to receive notifications if you log in using your Facebook account. The Facebook Security Checkup tool can be used in the following ways to safeguard your Facebook account.

1. Click this link to head to FB's security checkup tool.
2. It'll then give you the option to change your password and create a stronger one.
3. You will then be prompted to enable two-factor authentication. Click the Next button once you've turned it on.
4. Last but not least, each time you enter your Facebook account, you will be prompted to choose how you want to receive alerts. Select Turn On All by tapping it.

It is very important to follow these simple steps and keep your account secure. You must also ensure the same for the Facebook accounts of your family and friends to make sure they stay safe from their accounts being compromised.