Compromised Account Resources

At Meta, we take account integrity seriously. We have teams dedicated to safety and security, and helping users whose accounts are compromised regain access to their accounts. Below are some tips on how users can recover compromised accounts and keep their accounts safe.

Steps We Take to Protect Users

Security is built into Meta's apps and we offer several security features, such as login alerts and two-factor authentication, to help users protect their accounts. For example, when the email address associated with a user's Facebook account has changed, we send a message to the previous email account with a special link. Users can click this link to reverse the change and secure their account if the user did not authorize the change. We also have teams dedicated to helping legitimate account owners regain access to and secure their accounts, while at the same time, blocking access to bad actors.

Recovering a Compromised Account

Our Account recovery tools are designed to (1) help legitimate account owners regain access to their accounts, and (2) try to prevent bad actors who may try to abuse our account recovery systems from gaining access to other users' accounts. Like many other platforms, we authenticate users through the contact points (such as emails and phone numbers) they've added to their account to ensure they are who they say they are.

A user who thinks their account has been compromised, but whose account is still active, should first visit the Report Compromised Account page to secure their account: https://www.facebook.com/hacked.

- Users who are still able to log into their accounts can use this link to tell us if they found content they didn't create, such as a post, message, or event, or if someone logged into their account without their permission, among other things. We'll ask the user to change their password and review recent login activity to confirm whether recent logins were made by the user or by a bad actor.

- Users who are unable to log into their account should click the "My Account Is Compromised" button and follow the instructions to recover their account. We'll ask the user to provide the email or mobile number associated with their account. In some cases, we may ask for additional information that only the rightful account owner would possess in order to restore access and prevent abuse, such as a picture of their government-issued identification card (e.g., driver's license).

A user whose account was disabled after being compromised—which may happen if a compromised account posts content that violates our Community Standards—should visit the My Personal Account Was Disabled page to request a review of their account.

- Users should only use this form if their account has been disabled for violating our Community Standards. Please report hacked accounts that are still active to the Report Compromised Accounts page: https://www.facebook.com/hacked.

- Users should be prepared to provide: (1) their full name; (2) the email address or mobile number they use to log into their account; and (3) a form of ID that proves the user's identity.

    - If we ask for information to verify the user’s identity, they can send us a photo of a government-issued ID, such as a driver’s license, passport, birth certificate, or national identity card. The ID should contain either (1) the user’s full name and date of birth, or (2) the user’s full name and a photo of the user.

    - If a user has lost access to their account, they may be asked to provide a copy of something that shows a photo of the user or their date of birth as these details are shown on their Facebook account. This extra precaution helps us ensure that only verified users have access to the account.

    - Please visit our website for additional information on acceptable forms of ID.

    - We use trusted service providers to help review the user’s information. The user’s ID will be stored securely and will not be visible to anyone on Facebook. We may encrypt and store a user’s ID for up to one year to improve our automated systems for detecting fake IDs. Please visit our website for additional information on what happens to IDs after users send them to us.

Protecting Your Account

Here are some recommendations to all users to help keep their accounts secure:

- Pick a strong and unique password and don't share it with anyone else.

- Review and update your email accounts and phone number associated with your Facebook account and remove any that you don't use or have access to anymore.

- Use different passwords for each account you have, particularly for your email account and your Facebook account. If someone has access to your email account, they may be able to use it to gain access to your Facebook account.

- Take advantage of our extra security features, including two-factor authentication.

- Review our other security tips.