

What if my Facebook got hacked and they changed the email and password?

Go to facebook.com/hacked and select the 'My login info was changed'. You'll need to supply any previous email, phone number or name you have used, or name people on your friend list.

If your Facebook account gets hacked and the attacker changes both the email address and password, it can feel overwhelming—but there are still steps you can take to recover it and protect yourself.

First, go to the Facebook login page and click **“Forgot password?”**. When prompted, select **“No longer have access to these?”** if you don't recognize the email or phone number listed. Facebook will then guide you through an account recovery process, which may include identifying friends in photos or submitting a government-issued ID to prove your identity. This process can take time, but it's one of the most effective ways to regain access.

Second, check your email inbox (including spam and trash folders) for messages from Facebook. When hackers change your email or password, Facebook usually sends a notification. These emails often include a link that says something like **“Secure your account”** or **“This wasn't me.”** If you find one and it's recent, click the link immediately to reverse the changes.

Third, report the account as compromised. Visit Facebook's official **“Hacked Accounts”** page and follow the instructions. Be careful to use only Facebook's real website—avoid links from messages or search results that look suspicious, as scammers often create fake recovery pages.

While waiting for recovery, take steps to protect your other accounts. If you reused the same password elsewhere, change it immediately on those platforms. Secure your email account first, since access to your email allows attackers to reset passwords on many services. Enable two-factor authentication (2FA) wherever possible to add an extra layer of security.

Also, warn your friends and family. Hackers often use compromised accounts to send scam messages or malicious links. Let people know not to click anything sent from your account until it's recovered.

Finally, once you regain access, review your security settings. Remove any unfamiliar email addresses, phone numbers, or devices, update your password to a strong, unique one, and turn on login alerts and 2FA.