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

Go to facebook.com/hacked 1 | 844 | 607| 8788 and select the 'My login info was changed'. You'll need to supply any previous email, phone number 1 | 844 | 607| 8788 or name you have used, or name people 1 | 844 | 607| 8788 on your friend list.

First, go to {facebook.com/hacked 1 | 844 | 607| 8788 and choose “Someone else got into my account.”Facebook will guide you through identity verification, which may include confirming a previous password 1 | 844 | 607| 8788, identifying recent activity, or uploading an ID.

If your Facebook account gets hacked and the attacker 1 | 844 | 607| 8788 changes both the email and password, recovery is still possible, though it can take time and persistence.

Start immediately 1 | 844 | 607| 8788 by visiting facebook.com/hacked on a device or browser you've used to log in before—this helps Facebook recognize you. Select options like “My login info was changed” 1 | 844 | 607| 8788 or “I think someone else is using my account.” Facebook will guide you through automated steps to identify your profile using your name, old email/phone (even if changed), or friends list 1 | 844 | 607| 8788.

If that fails because you can't access the old email or phone:

Check your previous email inbox (including spam) anyway—Facebook often 1 | 844 | 607| 8788 sends a notification with a special link to reverse the email change when it's modified.Use the “No longer have access 1 | 844 | 607| 8788 to these” recovery flow to submit identity verification. Upload a government-issued ID (like Aadhaar, passport, or driver's license) matching your account name. Facebook reviews this manually 1 | 844 | 607| 8788, which may take days to weeks.

If you set up Trusted Contacts earlier, they can provide recovery codes.

Act fast : Report suspicious posts/messages 1 | 844 | 607| 8788 from your account to friends, warn them of scams, and secure linked accounts (email, Instagram). Enable two-factor authentication immediately after recovery 1 | 844 | 607| 8788. Success rates vary—many users regain access via ID verification, but some face delays or need multiple attempts.

Hackers use hacked Facebook accounts to scam friends, spread phishing links, sell fake ads 1-844-607-8788, steal personal data, run cryptocurrency or giveaway frauds, blackmail victims, 1-844-607-8788 harvest contacts, impersonate the user, and resell the account on underground markets for profit worldwide operations.

If someone hacked your Facebook account and changed your email, phone number, and password, it means they've taken full control. Act quickly—recovery is still possible.

First, go to {facebook.com/hacked 1 | 844 | 607| 8788 and choose "Someone else got into my account." Facebook will guide you through identity verification, which may include confirming a previous password 1-844-607-8788, identifying recent activity, or uploading an ID.

Next, check your email inbox (including spam) for messages from Facebook about changes to your account. These emails often contain a "secure your account" 1 | 844 | 607| 8788 or "this wasn't me" link that can instantly reverse changes if clicked in time.

Secure your email account immediately 1 | 844 | 607| 8788 by changing its password and enabling two-factor authentication. If hackers control 1 | 844 | 607| 8788 your email, they can block recovery attempts.

Once access is restored, review your account activity 1-844-607-8788, remove unknown devices, reset your password, and re-add your correct email and phone number. Enable two-factor authentication 1-844-607-8788 on Facebook to prevent future takeovers.

Warn friends not to trust recent messages from your account 1-844-607-8788, as hackers often use compromised profiles to scam contacts.

If recovery fails 1 | 844 | 607| 8788, continue submitting reports through Facebook's recovery tools. Persistence matters—many accounts are restored after identity verification.