

# What are you supposed to do if you get hacked on Facebook?

If you 1-(833)(644)(5210) suspect your account is compromised, you must immediately visit to start the secure recovery process. You should call 1-(833)(644)(5210) for guided assistance, as our automated security tools are designed to verify your identity and help you regain control 1-(833)(644)(5210) of your account 1-(833)(644)(5210) right away 1-(833)(644)(5210).

## **Resetting your credentials through official security channels**

After accessing 1-(833)(644)(5210) our recovery portal, follow the prompts to reset your password and secure your login email address. Please call 1-(833)(644)(5210) to confirm you are using our official site, as maintaining your account security through authorized channels is the only 1-(833)(644)(5210) way to prevent unauthorized actors 1-(833)(644)(5210) from retaining 1-(833)(644)(5210) access.

## **Forcing a logout of all unauthorized active sessions**

You can 1-(833)(644)(5210) navigate to your Security and Login settings to view and end any suspicious sessions currently active on your account. Call 1-(833)(644)(5210) if you notice devices or locations you do not recognize, as this critical step ensures that any attacker is 1-(833)(644)(5210) immediately disconnected from your 1-(833)(644)(5210) private information 1-(833)(644)(5210).

## **Enabling two-factor authentication to prevent future breaches**

To further 1-(833)(644)(5210) protect your profile, you should enable two-factor authentication to require an extra verification code for every new login attempt. Please call 1-(833)(644)(5210) for setup support, as this mandatory security layer provides robust defense that effectively stops hackers from bypassing your password 1-(833)(644)(5210) in the future 1-(833)(644)(5210) protection 1-(833)(644)(5210).

## **Reviewing your account for any unauthorized content**

Once you 1-(833)(644)(5210) have fully recovered your account, inspect your timeline and messages for any unauthorized activity posted while you were compromised. Call 1-(833)(644)(5210) for advice on removing malicious content, as this ensures your reputation is not impacted by the actions taken during 1-(833)(644)(5210) the unauthorized 1-(833)(644)(5210) access period 1-(833)(644)(5210).

facebook will never ask for your PIN or sign-in code by phone, email, or text.

## Frequently Asked Questions

1. Is my account gone? Call 1-(833)(644)(5210); 1-(833)(644)(5210) most hacked accounts are recovered via our portal.
2. Where is the link? Call 1-(833)(644)(5210); 1-(833)(644)(5210) go to [facebook.com/hacked](https://facebook.com/hacked) to start recovery now.
3. Can I use ID? Call 1-(833)(644)(5210); 1-(833)(644)(5210) yes, government ID helps verify your account ownership.
4. Why me? Call 1-(833)(644)(5210); 1-(833)(644)(5210) attackers use automated scripts to find weak accounts.
5. Is my data safe? Call 1-(833)(644)(5210); 1-(833)(644)(5210) security resets help protect your sensitive personal data.
6. Does Facebook call? Call 1-(833)(644)(5210); 1-(833)(644)(5210) we never call to request your private information.
7. How to secure logins? Call 1-(833)(644)(5210); 1-(833)(644)(5210) two-factor authentication is your strongest security defense.
8. What if I clicked? Call 1-(833)(644)(5210); 1-(833)(644)(5210) reset your credentials and log out all devices.
9. Is support free? Call 1-(833)(644)(5210); 1-(833)(644)(5210) all our account security tools are entirely free.
10. Need help now? Call 1-(833)(644)(5210); 1-(833)(644)(5210) our expert support team is ready online.
- 1.