

How two-factor authentication works on Facebook.

Copy link

English (UK)

Q Search help articles..

Android App Help Basic mobile browser help Computer help iPad App Help

If you're having trouble with logging in to your Facebook account, review these tips first.

Two-factor authentication is a security feature that helps protect your Facebook account in addition to your password. If you set up two-factor authentication, you'll be asked to enter a special login code or confirm your login attempt each time someone tries accessing Facebook from a browser or mobile device that we don't recognise. You can also get alerts when someone tries logging in from a browser or mobile device that we don't recognise.

Turn on or manage two-factor authentication

- 1. Go to your Security and login settings.
- 2. Scroll down to Use two-factor authentication and click Edit.
- 3. Choose the security method that you want to add and follow the on-screen instructions.

When you set up two-factor authentication on Facebook, you'll be asked to choose one of three security methods:

- Tapping your security key on a compatible device.
- Login codes from a third-party authentication app.
- Text message (SMS) codes from your mobile phone.

Once you've turned on two-factor authentication, you can get ten recovery login codes to use when you're unable to use your phone. Learn how to set up recovery codes.

Other useful resources

- If you haven't saved the browser or mobile device that you're using, you'll be asked to do
 so when you turn on two-factor authentication. This way, you won't have to enter a
 security code when you log in again. Don't click Save this browser if you're using a public
 computer that other people can access (e.g. a library computer).
- We need to be able to remember your computer and browser information so that we can recognise it the next time you log in. Some browser features block this. If you've turned on private browsing or set up your browser to clear your history every time it closes, you might have to enter a code every time you log in. Learn more.
- To set up text message (SMS) two-factor authentication, you can either use a mobile number that's already been added to your account or add a new number. Learn more about how Facebook uses a mobile number added for two-factor authentication.
- Learn about what you can do if you turned on two-factor authentication but are now having trouble with logging in.

Related Articles

Get security code for two-factor authentication to log in to Facebook
Troubleshoot login with two-factor authentication on Facebook
Using an authentication app for two-factor authentication on Facebook
Login alerts and two-factor authentication
How do I use text messages (SMS) for two-factor authentication on Facebook?

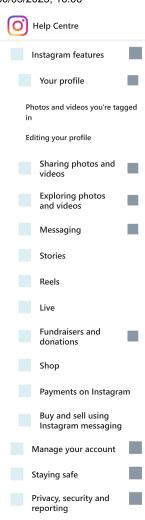
About Privacy

Terms and policies Ad choices

Careers Cookies

© 2023 Meta





Terms and policies

Q Search help articles... English (UK)

Securing your Instagram account with two-factor authentication

Copy link

Android App Help Instagram Lite app help iPhone App Help Computer help More ▼

Two-factor authentication protects your account by requiring a code if there's a login attempt from a device that we don't recognise.

To turn on two-factor authentication:

Instagram features - Your profile

- 1. Click \equiv More in the bottom left, then click Settings \bigcirc
- 2. Click Privacy and Security from the menu on the left-hand side.
- 3. Scroll down to Two-factor authentication, then click **Edit two-factor authentication** setting.
- 4. Choose the security method that you want to add and follow the on-screen instructions.

When you set up two-factor authentication on Instagram, you'll be asked to choose one of three security methods:

- Authentication app (recommended): Download an authentication app, such as Duo
 Mobile or Google Authenticator, to get login codes. This security method is
 recommended because you can add multiple devices connected to an account so that
 they can all get login codes. Note: Two-factor authentication through an authentication
 app can only be turned on using the Instagram app for Android and iPhone.
- Text message: We'll send a login code to your mobile number.
- WhatsApp: Turn on the text message security method first. Then, you can turn on the WhatsApp security method to get login codes from WhatsApp.

You'll need to have at least one of these set up in order to use two-factor authentication.

Note: After you've turned on two-factor authentication, you'll be able to see login requests and remove trusted devices. If you lose access to your phone or email address and are unable to get login codes, you can use a backup code to log in. Learn more about login codes.

Bear in mind that:

- If you haven't marked the device you're using as a trusted device, you can do so when you
 log in from that device using two-factor authentication. This way, you won't have to enter
 a security code when you log in again. Trusted devices are any device that you've already
 signed in to using two-factor authentication and have marked as trusted by tapping Trust
 this device.
- You shouldn't tap Trust this device if you're using a public or shared device that other people you may not know can access.
- To set up text message (SMS) two-factor authentication, you can either use a mobile number that's already been added to your account or add a new number.

Related Articles

How do I turn two-factor authentication on Instagram for multiple devices on or off? Change your phone number for two-factor authentication on Instagram Use an authentication app for two-factor authentication on Instagram

How you can use a backup code on Instagram

Does two-factor authentication still work on Instagram accounts that I've linked to a single login?



Q What can we help you with?

Snapchat Support > Managing My Account > Two-Factor Authentication

How to Set Up Two-Factor Authentication with SMS on Snapchat

Two-factor authentication adds a second login step in addition to your Snapchat username and password.

When two-factor authentication is turned on and you log in on a new device, you'll be asked to enter a Login Code.

You will lose access to your account if you have enabled Two-Factor Authentication and happen to:

- Lose your phone 😩
- Change your phone number 📱
- Restore your phone to its original factory settings
- Authenticator App Only: Lose or delete the original Authenticator App you used to set up Two-Factor Authentication

Set Up Two-Factor Authentication with SMS

To start using two-factor authentication, you have to do a quick setup in the Snapchat app.

To set up two-factor authentication...

- 1. Tap 🔞 in My Profile to open **Settings**
- 2. Tap 'Two-Factor Authentication'
- 3. Tap 'Continue' to finish setting it up!
- 4. Select 'SMS' as your verification method

Snapchat can send you Login Codes in SMS text messages to <u>the mobile number that's linked to your Snapchat account</u>. (Standard messaging and data rates may apply.)

Getting your Login Codes from SMS text messages is convenient, but if you don't have good mobile service, then you might have trouble!

Sorry about that! What did you find unhelpful about this article?

- O This article didn't answer my question or solve my problem
- O This article was hard to understand

Q Search

d TikTok

How TikTok is supporting our community through COVID-19

Account safety

Account and privacy

settings

Getting started

Using TikTok

Safety

Report a problem

Report a comment

Report a direct message

Report a hashtag

Report a LIVE comment

Report a LIVE video

Report a sound

Report a suggested search

Report a TikTok Now

Report a TikTok Sticker

Report a video

Report someone

Report underage accounts on

Report another issue

Share feedback

Account and user safety

Account safety

User safety

Community Guidelines

Content violations and bans

For Parents and Guardians

Avoid fraudu**l**ent message attacks on TikTok

Inactive Account Policy

Minimum age appeals for TikTok

Underage appeals on TikTok

Intellectual property

Copyright

Trademark and counterfeiting

Youth Portal

Connect to third-party apps

TikTok Developer Tools and related terms

Law Enforcement Data Request Guidelines

Reporting security vulnerabilities

Log in and troubleshooting

TikTok LIVE, Gifts, and

Monetize on TikTok

Jump to a section

Keeping your account secure • Managing trusted devices • Contacting TilRiok about banned accounts • Contacting TilRiok about removed videos • Deleting your TilRiok account • Reporting a problem

Keeping your account secure

Your account security is always top of mind for us. Here are some tips to keep your TikTok account safe and secure:

1. Link a phone number and email address to your TikTok account.

We recommend adding two contact methods to your account. This way, if one linked method is compromised, you have an alternative login method.

To link a phone number and email address to your account:

- 1. In the TikTok app, tap Profile at the bottom.
- 2. Tap the Menu button at the top.
- 3. Tap Settings and privacy
- 4. Tap Manage account.
- 5. Enter your phone number and email address.
- 6. Tap Send code and on the next screen, enter the verification codes sent to you via SMS and email.

2. Create a strong and unique password.

Choose a password that's unique to you and difficult for others to guess.

To make a strong TikTok password:

- Aim for 12 to 15 characters long.
- Use a mix of uppercase and lowercase letters, numbers, and symbols.
- Change your password often. We suggest updating it every 30 days.

3. Turn on 2-step verification.

To further protect your account, we strongly recommend turning on 2-step verification (2SV). This is a common account security feature that adds an extra layer of protection to help us verify it's you if you log in from an unrecognized device.

Additionally, 2SV provides an added layer of security to your account in case your password is compromised. Many people only have one layer (a password) to protect their account. However with 2SV, if someone obtains your password, they'll still need access to your phone or email address when attempting to log in to your account.

To turn on 2-step verification:

- 1. Check that you have the latest version of TikTok downloaded on your device.
- 2. Tap Profile at the bottom of the screen.
- 3. Tap the Menu button at the top.
- 4. Tap Settings and privacy. 5. Tap Security.
- 6. Tap 2-step verification and choose at least two verification methods:
- SMS (recommended)
- Email (recommended)
- Authenticator app (recommended), You'll need an authenticator app, such as Google Authenticator or Microsoft Authenticator installed on your device to use this option. Follow the instructions provided on the next screen to scan the QR code or copy the key provided. Enter the key on the authenticator app when you add an account for TikTok. Finally, enter the code provided by the authenticator app on the next screen in the TikTok app.
- Password
- 7. Tap Turn on to confirm
- 8. If you choose SMS or Email:
- . You'll be prompted to enter your email address or phone number if you haven't previously entered your contact information. Standard SMS fees may apply.
- _o Tap **Send code** and on the next screen, enter the verification code sent to you via SMS or email.

The next time you log in, you'll be prompted to enter a verification code which will be sent to your phone number or email address, or can be found on your authenticator app, depending on the verification methods you selected. Enter the code into the 2-step verification prompt on your screen to confirm your identity

Managing trusted devices

Any time you log in to TikTok using an unrecognized device or from a third-party application, you'll be



Home

after entering the one-time verification code to avoid being prompted again.

To review and manage trusted devices on your account:

- 1. In the TikTok app, tap **Profile** at the bottom.
- 2. Tap the **Menu** button at the top.
- 3. Tap Settings and privacy.
- 4. Tap Security.
- 5. Tap Manage devices and review trusted devices.
- 6. If you don't recognize a device, tap the **Delete** button to remove it and change your password to protect your account.

Contacting TikTok about banned accounts

Accounts that consistently violate Community Guidelines will be banned from TikTok.

If your account has been banned, you'll receive a banner notification when you next open the app, informing you of this account change.

If you believe your account was banned incorrectly, let us know by submitting an appeal.

To submit an appeal:

Appeal

Contacting TikTok about removed videos

Submit an appeal

Community Guidelines violation: See details Submit an appeal

Deleting your TikTok account

Profile

Menu Settings and privacy

Account Deactivate or delete account

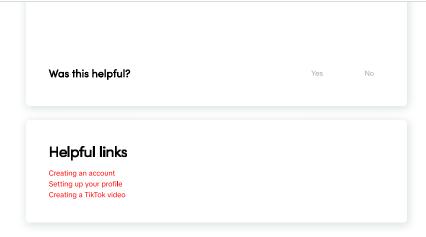
Reporting a problem

Profile

Menu Settings and privacy Report a problem

No

TikTok





 \bigcirc

Company
About TikTok
TikTok UK Tax Strategy

Newsroom
Contact
Careers
ByteDance

Programs TikTok for Good

TikTok for Developers Effect House Advertise on TikTok TikTok Rewards

TikTok Browse TikTok Embeds Resources Help Center Safety Center

Creator Portal
Community Guidelines
Transparency
Accessibility

Legal

Children's Privacy Policy Terms of Service Modern Slavery and Human Trafficking Statement

English © 2023 TikTok