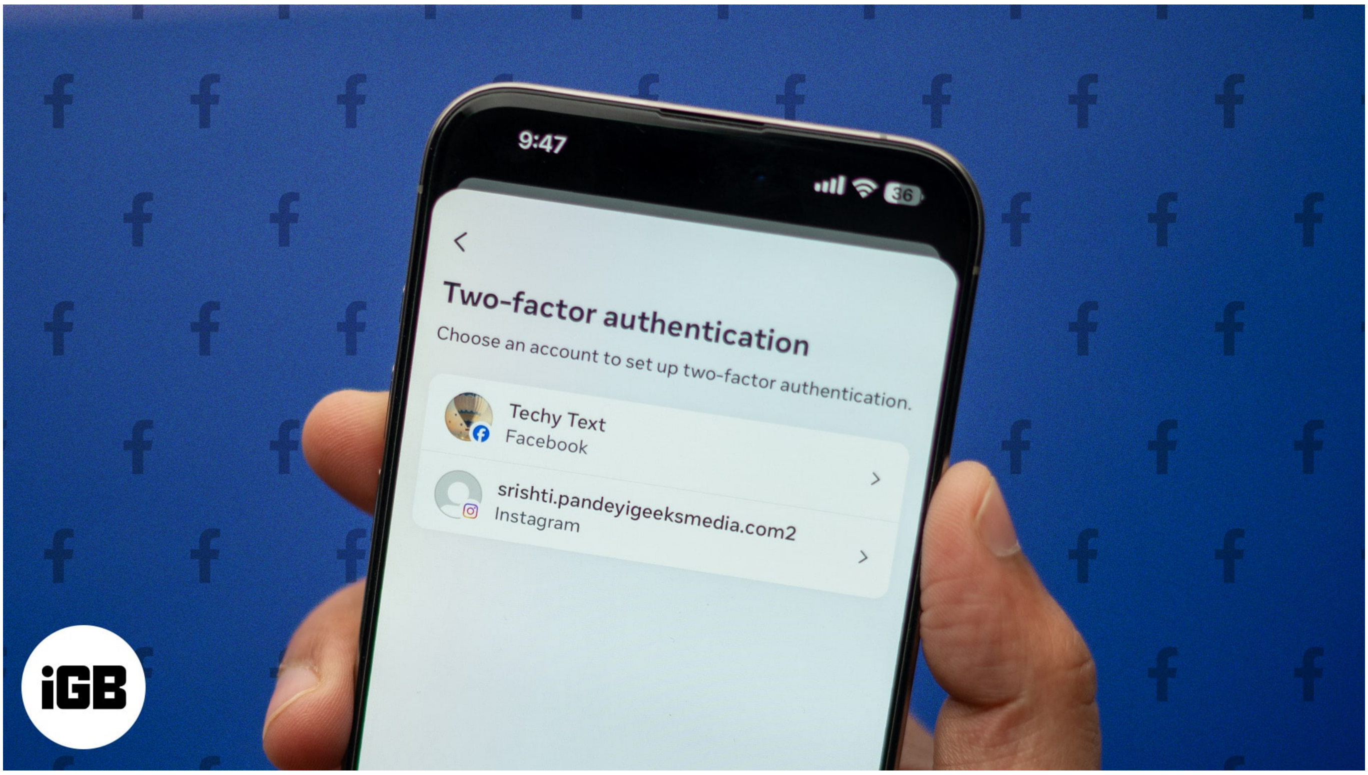
Key Takeaways

- Two-factor authentication (2FA) adds an extra layer of security to your Facebook account by requiring a second form of verification beyond just your password.
- To set up two-factor authentication Facebook, Open the Facebook app on your iPhone, go to the **menu**, select **Settings & Privacy** > **Settings**, navigate to Accounts Center > **Password and Security**, then tap **Use Two-Factor Authentication**.
- On Mac or PC, Log into Facebook on a web browser, click your **profile picture**, go to **Settings & Privacy** > **Settings** > Accounts Center, then select **Password & Security** and click **Two-Factor Authentication**.
- In case you lose your phone or method of authentication, Facebook allows generating recovery codes.

With the increase in online threats, protecting our personal data on social media platforms is crucial. This is why Facebook has incorporated two-factor authentication to keep away trespassers. When enabled, you must enter a special security code in addition to your password; for those who may wonder what it means and how to do that, they are on the right blog.



Two-factor authentication

Choose an account to set up two-factor authentication.

Techy Text
Facebook

srishti.pandeyigeeksmedia.com2
Instagram

#image_title

In this blog post, I will show you how to set up two-factor authentication on Facebook using an iPhone, iPad, and Mac or PC. I will also walk you through everything you need to know about this crucial security feature.

Table of Contents

What is two-factor authentication (2FA) on Facebook?

Two-factor authentication is a security feature that requires you to provide two different forms of verification when logging into your Facebook account from an unrecognized browser or mobile device.

The first factor is typically your password, while the second factor can be a one-time code sent to you via SMS, a security key, or a code generated by an authentication app. Unless you confirm your login attempt, no one can access your account.

Thus, it ensures that only you can access your Facebook account, even if someone else has your password. This extra step makes it much harder for hackers to break into your account. Let’s understand in brief.

Why should you enable 2FA for your Facebook account?

Since Facebook contains private information like messages from friends, your images and phone number, setting up 2-factor authentication must be performed to protect your digital identity. It offers several advantages:

- **Enhanced security:** Two-factor authentication significantly improves the overall security of your Facebook account, as you need to perform an extra step when logging into your account from an unrecognized device.

- **Protection against unauthorized access:** Even if someone manages to obtain your password, they won't be able to access your account without the second factor of authentication.
- **Mitigation of phishing attacks:** Attackers will find it more difficult to access your profile via phishing since many of these codes are location-specific or time-sensitive.

Now that you understand how essential it is, let's proceed to the steps.

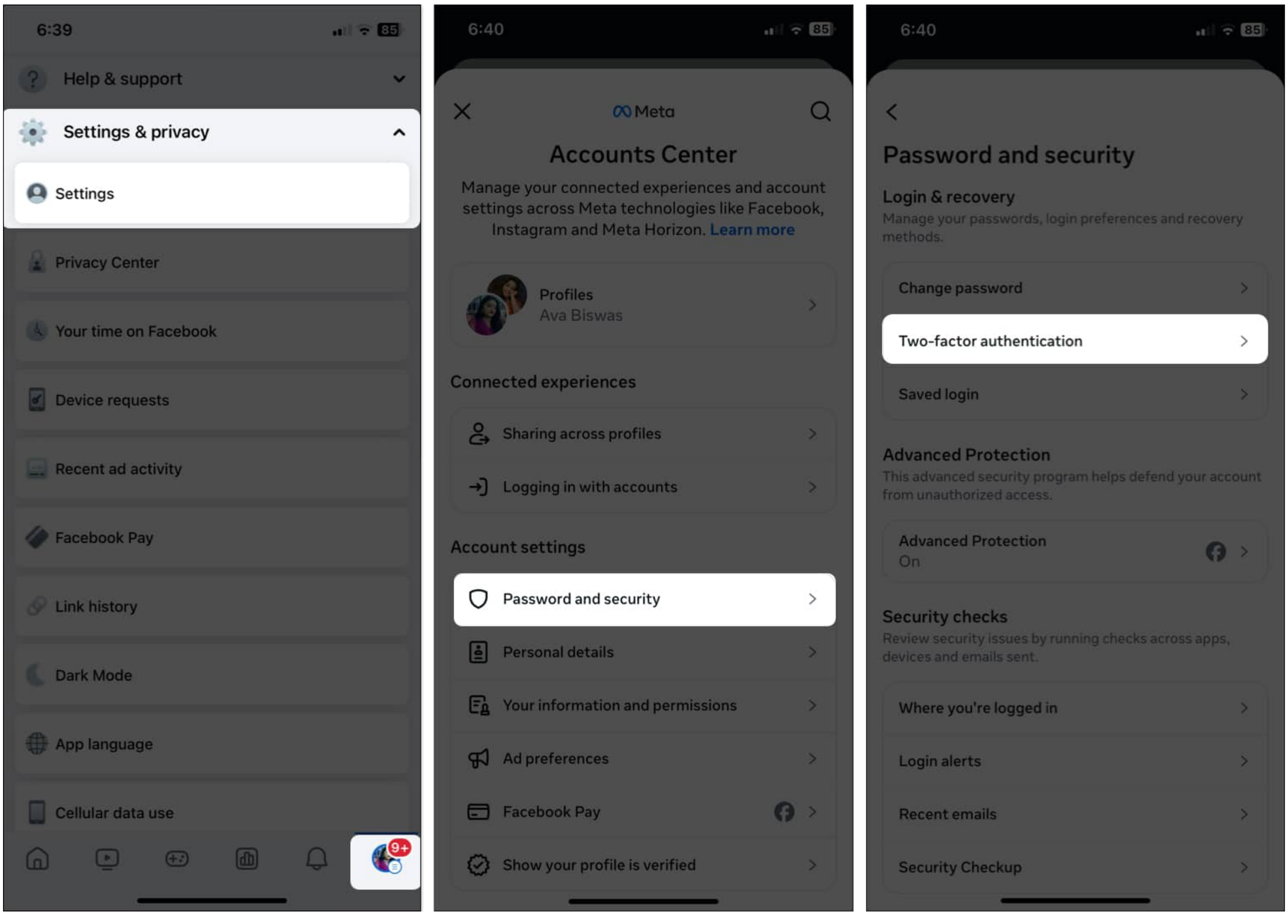
Pro Tip
If you want to protect your personal information on Facebook, you may also lock your Facebook account. It will restrict strangers from accessing your profile details and your social media posts and content. Only your friends on Facebook can interact with you after your profile is locked.

How to set up two-factor authentication on your Facebook account

Setting up 2FA on Facebook is easy; you can do it from your iPhone, iPad, Mac, or PC. Below are step-by-step guides for each device.

Turn on 2FA for Facebook on your iPhone or iPad

1. Launch the **Facebook** app.
2. Tap the **menu icon** (three lines) at the bottom right corner.
3. Scroll down and tap on **Settings & privacy**. Select **Settings** from the context menu.
4. Now, go to the **Accounts Center**.
5. For iPhone, tap on **Password and security**. On iPad, select **Security and login**.
6. Next, tap **Use two-factor authentication**.



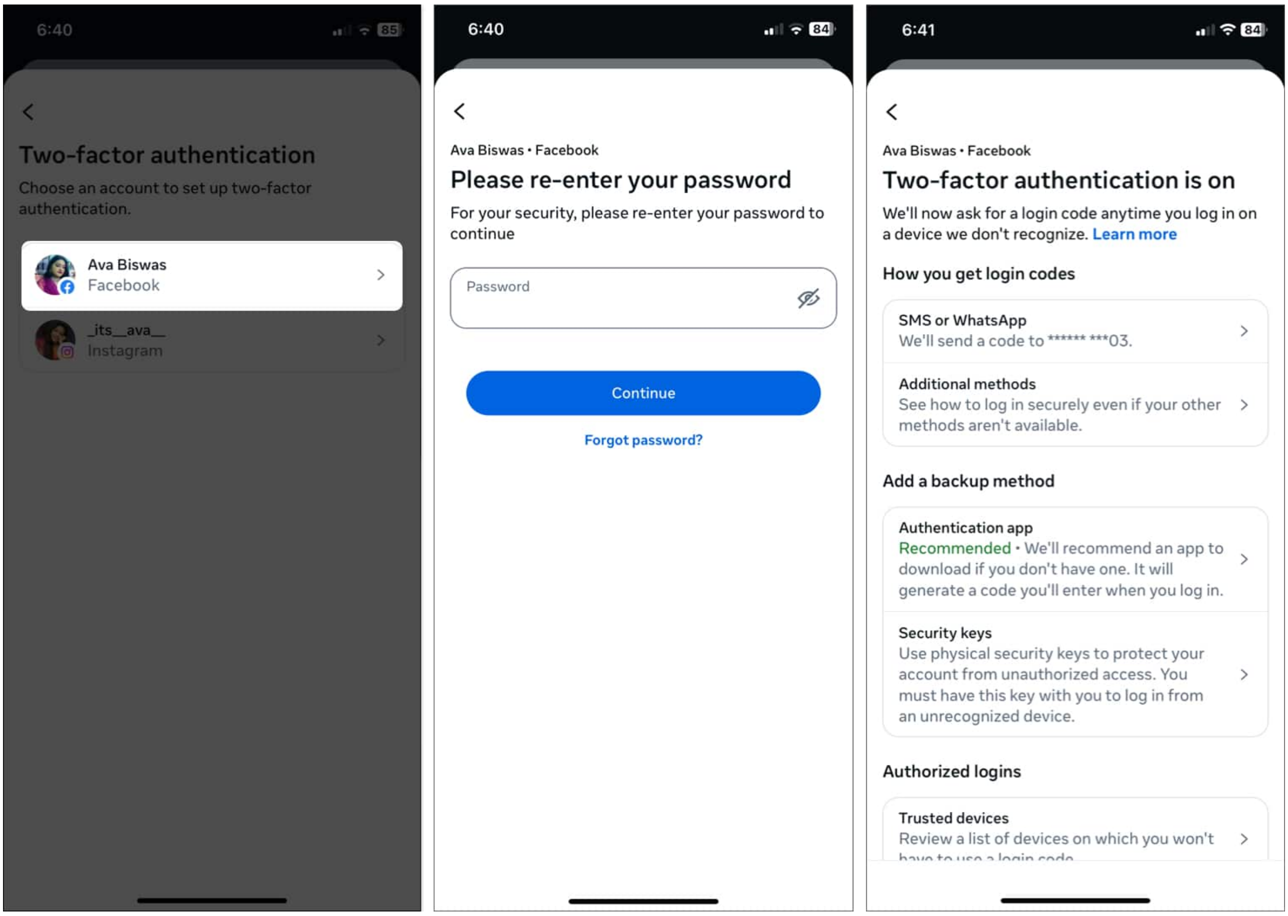
Manage your connected experiences and account settings across Meta technologies like Facebook, Instagram and Meta Horizon. Learn more

Manage your passwords, login preferences and recovery methods.

This advanced security program helps defend your account from unauthorized access.

Review security issues by running checks across apps, devices and emails sent.

7. If your Facebook and Instagram account are connected, select your **Facebook account**.
8. Enter your Facebook account password if prompted and tap **Submit**.
9. Select the preferred 2FA method (Text message SMS code, third-party two-factor authentication app, or Security Key).



6:40

Two-factor authentication

Choose an account to set up two-factor authentication.

Ava Biswas
Facebook

_its__ava__
Instagram

6:40

Ava Biswas • Facebook

Please re-enter your password

For your security, please re-enter your password to continue

Password

Continue

Forgot password?

6:41

Ava Biswas • Facebook

Two-factor authentication is on

We'll now ask for a login code anytime you log in on a device we don't recognize. Learn more

How you get login codes

SMS or WhatsApp
We'll send a code to ****** ***03.

Additional methods
See how to log in securely even if your other methods aren't available.

Add a backup method

Authentication app
Recommended • We'll recommend an app to download if you don't have one. It will generate a code you'll enter when you log in.

Security keys
Use physical security keys to protect your account from unauthorized access. You must have this key with you to log in from an unrecognized device.

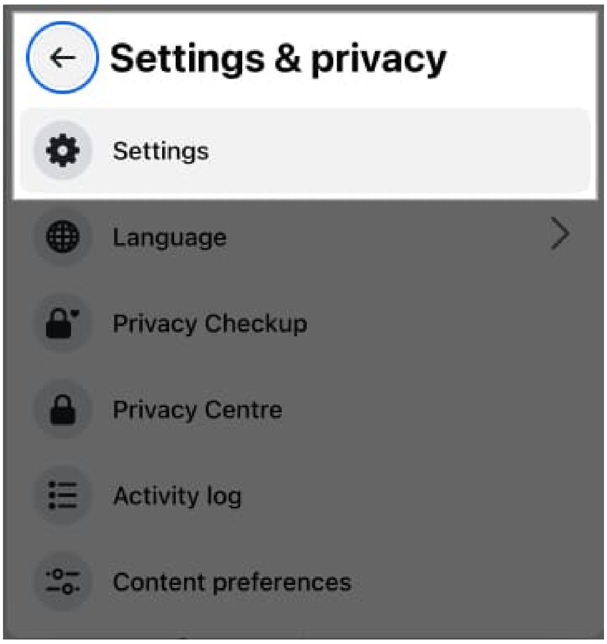
Authorized logins

Trusted devices
Review a list of devices on which you won't have to use a login code

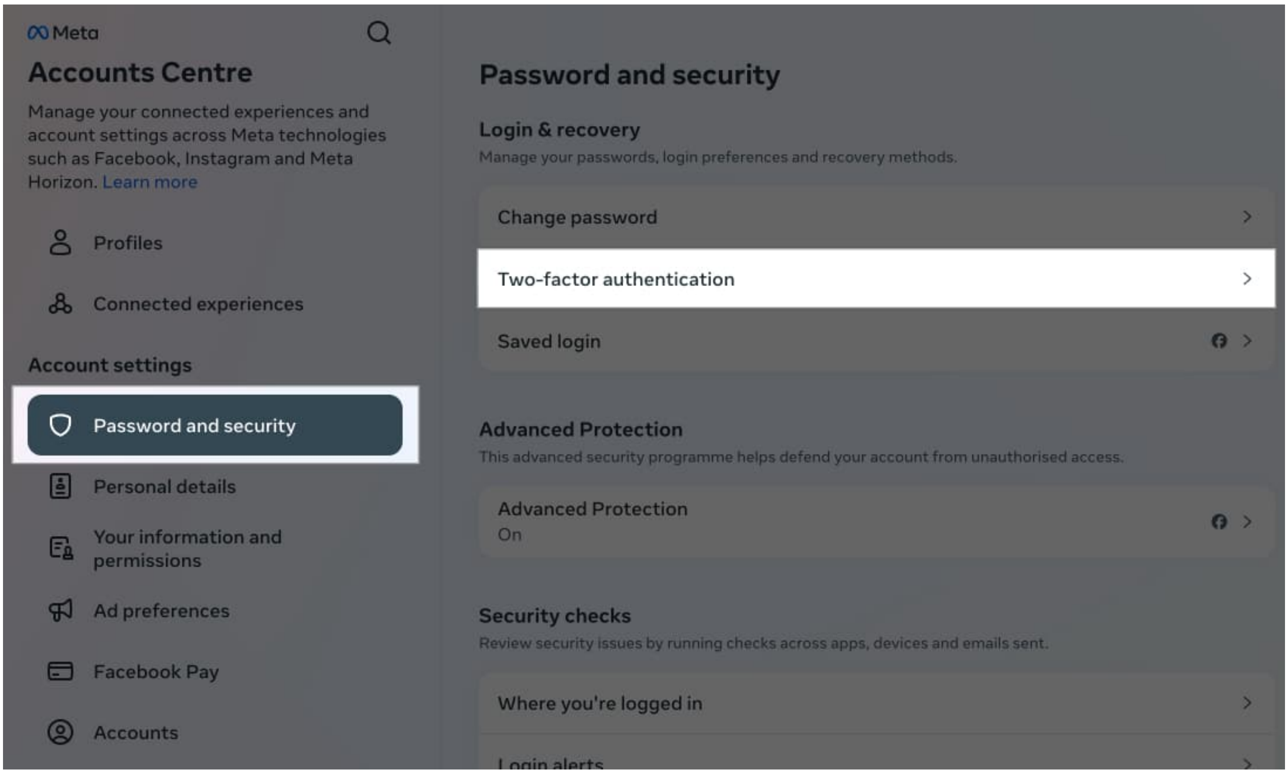
10. Follow the on-screen instructions to complete the setup.

Turn on 2FA for Facebook on your Mac or PC:

1. Open **Facebook** in a web browser and log into your account.
2. Click on your **profile picture** at the top right of the page.
3. Now, select **Settings & privacy** and click **Settings**.



4. In the left menu, click **Accounts Center**.
5. Here, select **Password & security** from the sidebar.
6. Click on **Two-factor authentication** on the right.



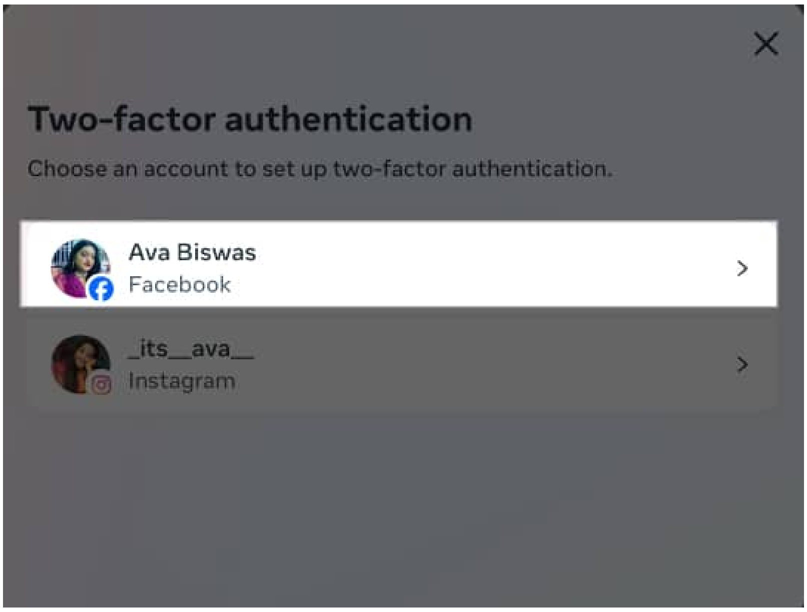
Manage your connected experiences and account settings across Meta technologies such as Facebook, Instagram and Meta Horizon. Learn more

Manage your passwords, login preferences and recovery methods.

This advanced security programme helps defend your account from unauthorised access.

Review security issues by running checks across apps, devices and emails sent.

7. Choose your **Facebook account**.



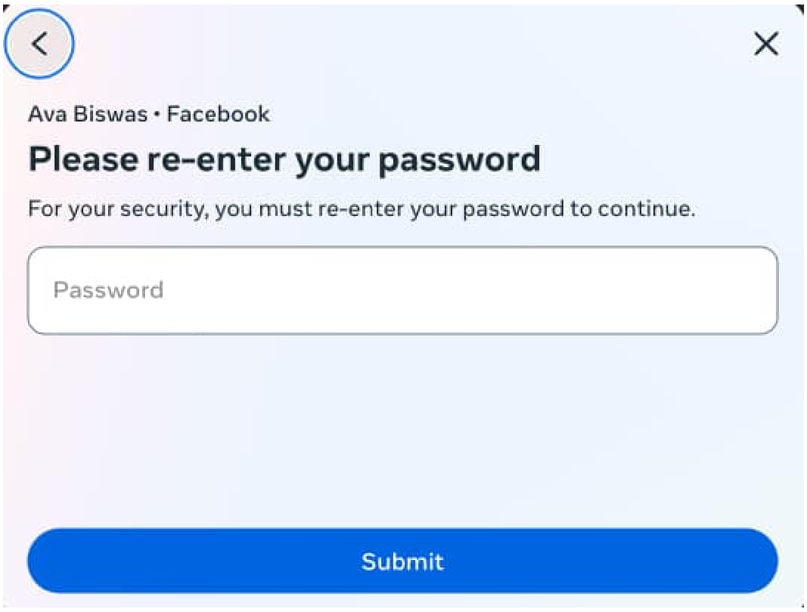
Two-factor authentication

Choose an account to set up two-factor authentication.

Ava Biswas
Facebook

_its__ava__
Instagram

8. Type in your password, and click **Submit**.



Ava Biswas • Facebook

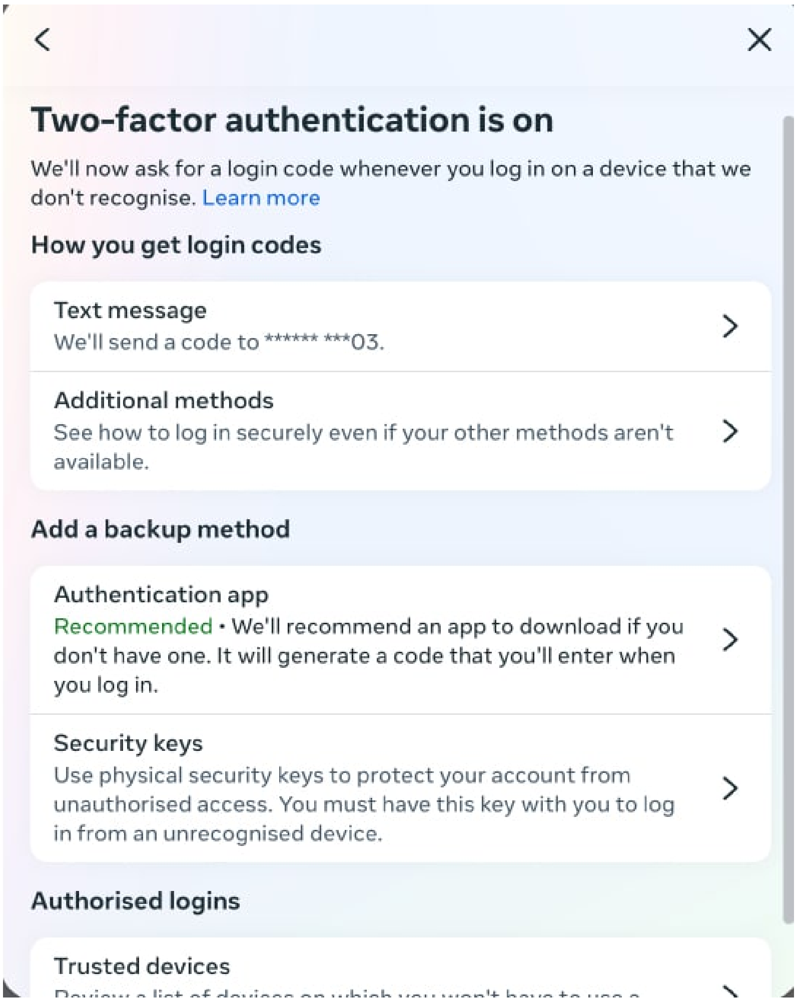
Please re-enter your password

For your security, you must re-enter your password to continue.

Password

Submit

9. Choose your preferred authentication method and follow the on-screen prompts to finish the setup.



Two-factor authentication is on

We'll now ask for a login code whenever you log in on a device that we don't recognise. Learn more

How you get login codes

Text message
We'll send a code to ****** ***03. ›

Additional methods
See how to log in securely even if your other methods aren't available. ›

Add a backup method

Authentication app
Recommended • We'll recommend an app to download if you don't have one. It will generate a code that you'll enter when you log in. ›

Security keys
Use physical security keys to protect your account from unauthorised access. You must have this key with you to log in from an unrecognised device. ›

Authorised logins

Trusted devices
Review a list of devices on which you won't have to use a

If you want to know how authentication methods secure your account, keep on reading.

How two-factor authentication works on Facebook

I have already explained the basic working principle of Facebook's two-factor authentication feature. Whenever someone tries to log into your account, they must provide an additional verification code. Facebook offers three main methods to authenticate your login attempts:

- **Text message (SMS or WhatsApp):** While logging onto Facebook, you receive a unique six-digit security code via SMS or WhatsApp to your registered phone number. This code is valid for a limited time, such as 30 or 60 seconds. If you don't have a number set on your account, you can add it while enabling the feature.
- **Security key:** You can use a physical security key that plugs into your device's charging port or connects via Bluetooth/NFC for authentication. As the security key is

present with you, it becomes impossible to break into your account. Select Security keys as your authentication method and register your security key.
- **Two-factor authentication apps:** Apps like Google Authenticator generate time-sensitive codes that you enter when logging into Facebook. You may download any third-party authenticator app on your device where you mostly use Facebook and scan the barcode Facebook provided to set it up.

You may choose any of the methods to enable two-factor authentication for your Facebook account that's most convenient and secure for you. After that, you can add another backup authentication method or get Facebook recovery codes to ensure you never lose access to your account. We will discuss this later in the post.

Once the setup is done, you must enter the verification code each time you try to log in from an unrecognized device or browser. You may save the browser when prompted to ensure a smooth login from your primary devices. This way, Facebook will not ask for 2FA codes from that device again.

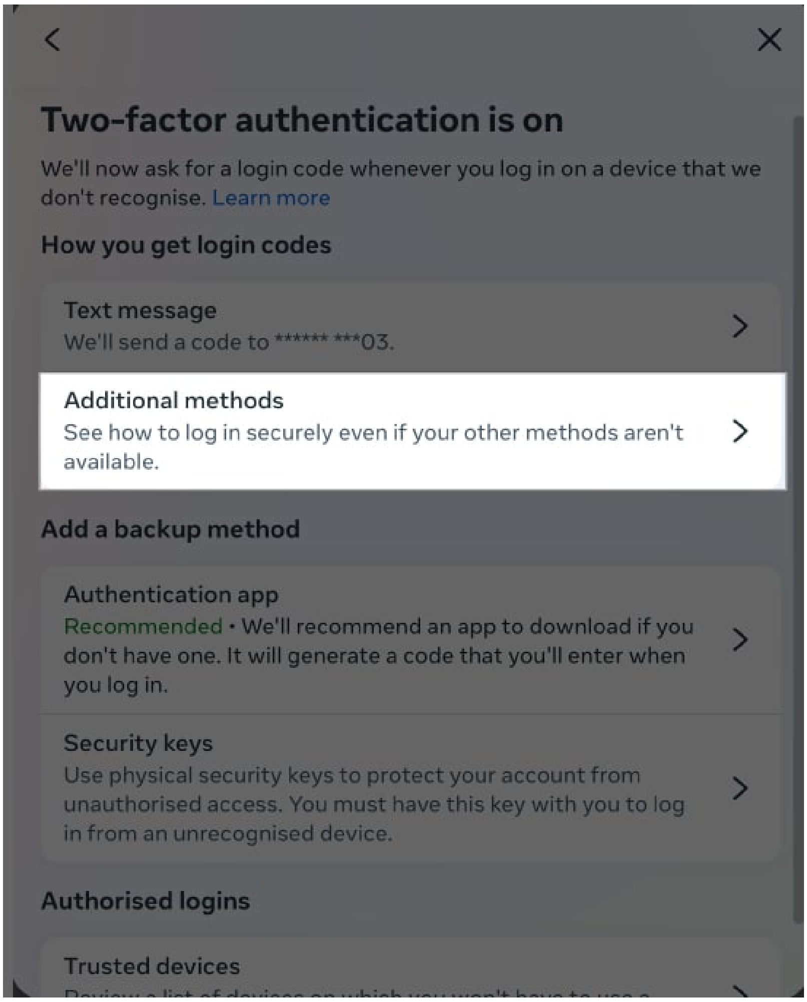
Also, you can get alerts and approve your next login attempts from recognized devices. However, you must always verify your login attempt if you access Facebook from an incognito browser.

Note
You can review your authorized devices and remove the ones you don't use anymore to increase security. Access the **Use two-factor authentication** settings and select **Trusted devices** at the bottom. Here you can see a device list you have approved. Select the **device** and hit **Remove device**.

How to set up recovery codes on Facebook

Facebook provides ten recovery codes that you can use to access your account in case you lose access to your phone or security key. Moreover, if you face trouble using the two-factor authentication method you set up, you can use it to log into your Facebook. To set up recovery codes:

1. Go to your Facebook account **settings** and navigate to the **Use two-factor authentication** section.
2. Select **Additional methods**.



Two-factor authentication is on

We'll now ask for a login code whenever you log in on a device that we don't recognise. Learn more

How you get login codes

Text message
We'll send a code to ****** ***03.

Additional methods
See how to log in securely even if your other methods aren't available.

Add a backup method

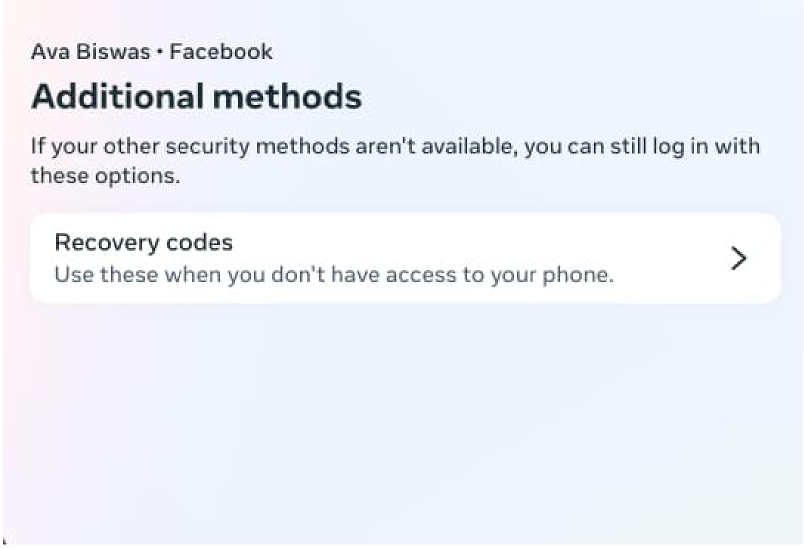
Authentication app
Recommended • We'll recommend an app to download if you don't have one. It will generate a code that you'll enter when you log in.

Security keys
Use physical security keys to protect your account from unauthorised access. You must have this key with you to log in from an unrecognised device.

Authorised logins

Trusted devices

3. And choose **Recovery codes**.



Ava Biswas • Facebook

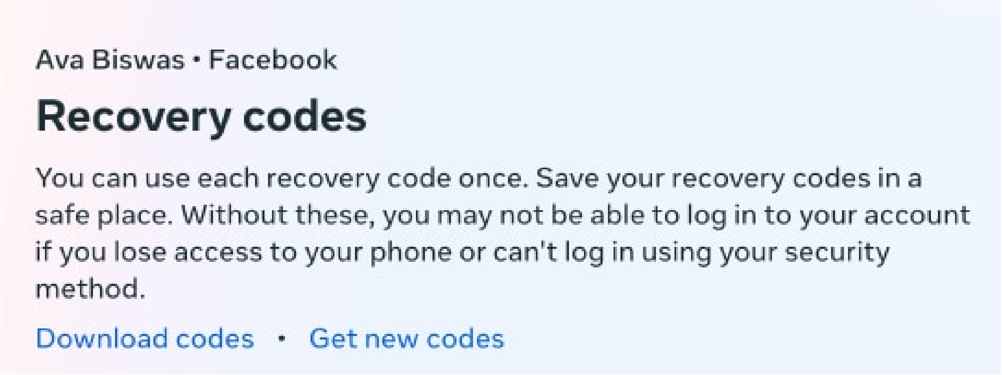
Additional methods

If your other security methods aren't available, you can still log in with these options.

Recovery codes
Use these when you don't have access to your phone.

4. Facebook will generate ten recovery codes of four digits. You can use each code for

one time only.
5. Copy-paste the code or tap on **Download codes**.



Ava Biswas • Facebook

Recovery codes

You can use each recovery code once. Save your recovery codes in a safe place. Without these, you may not be able to log in to your account if you lose access to your phone or can't log in using your security method.

Put down your recovery codes in a secure place. If anyone has access to them, they can log into your account. Setting up multiple other ways, like a backup phone number or email address, might also be advisable in case you lose access to your primary authentication method.

Bonus: Set up alerts about unrecognized logins on Facebook

You can create alerts for unrecognized logins, increasing the security of your Facebook account. This will notify you of any login to your account from unrecognized devices or locations.

To enable unrecognized login alerts:

1. Go to your Facebook Accounts Center settings and navigate to the **Password and security** section.
2. Select **Login alerts**.
3. Now, choose your **Facebook account**.
4. Checkmark where you want to receive the alerts (email or Facebook notifications).
5. Get back to save your choice.

By receiving these alerts, you can quickly act if someone tries to access your account without permission. If you get a suspicious login alert, select **This was me**. After that, Facebook will assist you in securing your account.

Signing off…

Two-factor authentication on Facebook is essential to protect your personal information from prying eyes. Follow the guidelines provided to set up Facebook two-factor authentication on your iPhone, iPad, Mac, or PC, ensuring the safety of your account even if someone else knows the password. Remember to also set up recovery codes and alerts for unrecognized logins to further strengthen your account's security.

FAQs

Why am I not getting my authentication code from Facebook?

Sometimes, it takes a while to receive an SMS code. Therefore, always check back constantly. If you do not receive your verification code from Facebook at all, ensure that you have set the correct phone number in your profile settings. Go to the Use two-factor authentication section, select SMS or WhatsApp, and check the last two digits of your phone number. If you can't recognize it, select Change phone number, enter your number, and verify it. You can also try requesting a new code or using a backup method, such as an authentication app or recovery codes.

What should I do if two-factor authentication isn't working?

If 2FA isn't working, ensure you're entering the correct code within the specific time limit. To log in, you must connect to an active internet connection. If your device is acting up, restart it and try again. You may also use a recovery code if saved before. To contact Facebook Support, select Need another way to authenticate? On the **login page**, then choose **Other Options** and hit **Get more help**.

Can I turn off two-factor authentication on Facebook?

Yes, you can turn off Facebook two-factor authentication at any time if you no longer want to use this security feature. Navigate to **Settings & privacy**, select **Settings**, and access **Accounts Center**. Now, select **Password and security** and choose **Use two-factor authentication**. Select your **account** and enter your **password**. Next, choose the **authentication** method and **toggle it off**. However, you can't turn off two-factor authentication if you have enabled Advanced Protection for Facebook.