



Digital safety guide

Instagram privacy & security



The settings that keep your account, photos, and whereabouts to yourself. Go one section at a time — no need to do it all at once.

Before you start

Find Settings	Tap your profile picture (bottom right), then the menu button (three lines, top right) to open Settings and activity . On a computer: instagram.com › More › Settings .
Accounts Center	Home to your password, two-factor authentication, and ad settings. Meta is renaming it Meta Account during 2026–27.
Can't find it?	Menus move. Use the search bar at the top of Settings.

✓ Do

Check the background before you post: house numbers, street signs, license plates.

Use a long, unique password and turn on two-factor authentication (page 5).

Keep personal details off your profile. A first name or nickname is fine.

Ask family to do the same. Their settings can expose you, too.

✗ Don't

Tag your location while you're still there. Post it after you leave.

Accept follow requests from strangers. Fake accounts use stolen photos.

Send private details by message. Since May 2026, Instagram messages aren't end-to-end encrypted. Use Signal or WhatsApp.

Store a card in Instagram. Check Accounts Center › Payments.



01 Make your account private

The single most important setting. Once it's on, only followers you approve can see your posts, stories, and reels.

Settings and activity › Account privacy › Private account › Turn on

Going private doesn't remove anyone who already follows you. On your profile, tap **Followers** and remove anyone you don't know.

🎯 *Good to know*

- Meta uses public posts from adults to help train its AI. It says it doesn't use posts from private accounts.
- Business and creator accounts can't be private, and since July 2025 their public posts can show up in Google and Bing. To limit that, turn off **Allow public photos and videos to appear in search engine results** under Account privacy.

02 Choose who can reach you

Comments

Settings and activity › Comments

Under **Allow comments from**, pick a smaller group than Everyone. Add anyone you'd rather not hear from to **Block comments from**.

Hidden Words

Settings and activity › Hidden Words

Turn on **Hide comments**, **Advanced comment filtering**, and **Hide message requests**. Add your own words to hide, too. "Crypto" and "giveaway" are scam favorites.

Messages

Settings and activity › Messages and story replies

Under message requests, limit who can message you so strangers can't reach your inbox.



03 Control what others see and share

Online status

Settings and activity › Messages and story replies

Turn off **Show activity status** to hide when you're online. (You won't see when others are online, either.)

Resharing

Settings and activity › Sharing and reuse

Turn off the options that let people send your stories in messages or add your posts and reels to their own stories.

Facebook

Accounts Center › Sharing across profiles

Pick your Instagram account, then turn off automatic sharing of your story, posts, and reels to Facebook.

Who can tag you

Settings and activity › Tags and mentions

Under **Who can tag you**, choose **Don't allow tags** (most private) or **Allow tags from people you follow**. Then turn on **Manually approve tags**, so no tag reaches your profile until you say yes.

Remove a tag

Open the post › ⋮ › Tag options › Remove me from post

Prefer to stay tagged but out of sight? Choose **Hide from my profile** instead.

Suggestions

On a computer: instagram.com › Profile › Edit profile

Turn off **Show account suggestions on profiles**, so Instagram stops recommending your account to people browsing other profiles.

🕒 *Good to know*

A private account protects your own posts only. A comment you leave on someone else's public post, or a photo of you on a public account, can be seen by anyone.



04 Guard your location and photos

Instagram strips the hidden location data out of photos when you upload them. A location tag, a recognizable background, or Instagram Map can still give you away.

Instagram Map

Messages › Map › Settings (gear) › No one

Shares your location with friends on a map. It's off unless you turned it on, but check anyway. Location-tagged posts still appear there.

Then check your phone's own settings, which decide what Instagram can reach at all.

iPhone

Settings › Privacy & Security

Location Services › Instagram › **Never**.
Or pick While Using the App and turn off
Precise Location.

Photos › Instagram › **Limited Access**, so it
only sees the photos you pick.

Contacts › turn off Instagram.

Tracking › turn off Instagram.

Android

Settings › Apps › Instagram › Permissions

Location › **Don't allow**.

Photos and videos › the most limited choice
offered. Names vary by phone.

Contacts › **Don't allow**.

Ads: search Settings for "Ads" and choose
Delete advertising ID.

To stop contact uploads: **Accounts Center** › **Your information and permissions** › **Upload contacts**, then turn off **Connect contacts**. Contacts already uploaded can be deleted under Manage contacts on [instagram.com](https://www.instagram.com).

Why it matters

In 2022, artist Dries Depoorter recorded publicly viewable webcams for weeks, gathered public Instagram photos tagged at the same spots, and used AI to match them, pinpointing when each photo was taken. Only public posts with a location tag could be matched.



05 Lock the front door

Everything in this section lives in one place:

Settings and activity › Accounts Center › Password and security

Two-factor authentication	A second check after your password, so a stolen password alone isn't enough. Use an authentication app if you can; a text message is a fine fallback. Keep the backup codes on paper somewhere safe.
Passkey	If you see Passkeys , set one up. You'll sign in with your face, fingerprint, or screen lock, and fake login pages can't steal it.
Where you're logged in	Log out of any phone or computer you don't recognize, then change your password.
Login alerts	Turn them on so you hear about new sign-ins right away. While you're here, run Security Checkup once.
Saved login	If your phone or computer is shared, or has no passcode, turn this off so Instagram asks for your password each time.
Password	Make it long and used nowhere else. Change it right away if someone else might know it; there's no need to change a strong one on a schedule.

🔒 *Shared phones and teens*

- Instagram lets several accounts sign in on one phone and switch between them, sometimes without a password. Add accounts only to your own phone, and always log out of a borrowed one.
- Everyone under 18 gets a Teen Account that starts out private; under-16s need a parent's permission to loosen settings. Parents can supervise through **Family Center**. Remind kids never to share passwords with friends.



06 Clean up old connections

Apps and websites

Settings and activity › Website permissions › Apps and websites

Remove any app or website you don't recognize or no longer use. Ideally, the Active list is empty.

07 If something goes wrong

A post or account bothers you

Tap ⋮ on the post or profile to **Report**, **Mute**, **Restrict**, or **Block**. Restrict hides their comments from everyone but them.

Someone is pretending to be you

On the fake profile, tap ⋮ › **Report**, then the option for pretending to be you. Or search "impersonation" at help.instagram.com.

You can't get in

Visit instagram.com/hacked from any device. Once you're back in, change your password.

Words to know

Authentication app: an app that shows a new sign-in code every 30 seconds.

End-to-end encryption: only you and the other person can read the message.

Passkey: sign in with your face, fingerprint, or screen lock. No password.

Location tag: a place name added to a post, seen by anyone who sees the post.

Want a hand with this?

We'll walk through every setting in this guide with you, at your pace.

watchstander.tech hello@watchstander.tech

Instagram, Facebook, and Meta are trademarks of Meta Platforms, Inc. Watchstander Tech is not affiliated with or endorsed by Meta. Steps checked October 2026; apps change often, so your screens may look different. © 2026 Watchstander Tech, LLC.