

## Personalized privacy

# Customizing your Facebook settings



With more than 1.5 billion people logging in to their accounts on a daily basis, Facebook is the world's largest social network. The mobile app and website let users share comments, activities, photos, videos, links, news and more—creating a digital “town square” that’s informative, entertaining and engaging. But participation on any social media platform presents important privacy considerations. This publication explains how you can enjoy Facebook while preserving your personal privacy and staying safe online.

Facebook’s Data Policy (<https://www.facebook.com/policy.php>) explains in detail how the company collects and uses your information, how it’s shared and how long it’s retained. It also outlines your rights and how to exercise them.

## Facebook and privacy

Protecting your privacy is important whenever you’re online, whether you’re working, learning, banking, shopping or socializing. While it might be perfectly safe to share personal information, travel plans, children’s names, family photos and

other details of your life with family and close friends, making them public—intentionally or unintentionally—can open you up to unwelcome attention and a range of potential consequences.

Facebook settings allow users to customize their privacy preferences. The platform offers dozens of opportunities for controlling who can see what about you, what you see when you’re on the site or in the app, and what information Facebook has about you and how it’s used. Understanding what you can control in your Facebook account, and mastering the settings and options, can help you make the most of what Facebook offers.

## Privacy management tools

To help users customize their privacy settings, Facebook offers general resources—*Privacy Shortcuts* and *Privacy Checkup*—that walk you through the most important privacy considerations and centralize your options for making the privacy choices that are right for you.

**Privacy Shortcuts** is a one-stop-shop for account privacy and security information and settings. From this single page (accessible in the Facebook app under *Settings & Privacy*, and on the website under the “?” icon in the upper right-hand corner of the page) you can access many of the most widely used privacy settings along with information about what they do and how to adjust them.

**Privacy Checkup** (found by clicking *Review a few important privacy settings* near the top of the *Privacy Shortcuts* page in the app, or under the “?” icon on the website) guides you through important privacy settings on Facebook, helping you to strengthen your account security and control who can see what you share and how your information is used. Once you choose your settings in the four sections of the checkup, your preferences will apply to your future activity unless you change them again in *Privacy Checkup* or directly in *Settings*, or change your audience for individual posts.

Now that you know how to access your settings and where you can learn more about them, here’s what each one can do for you.

The most **basic Facebook privacy settings** allow you to control who sees what you share. Customizing just this handful of controls can go a long way toward achieving a privacy level you’re comfortable with.

Before discussing the specific settings, there are a few **key terms** you should be familiar with to understand the audience you’re sharing with on Facebook.

■ **Public:** When you share something with Public, that means that anyone, including people off of Facebook, can see it.

■ **Friends:** This option lets you post stuff to your friends on Facebook. If anyone else is tagged in a post, then the audience expands to also include the tagged person and their friends. If you don’t want your photo or post to be visible to the friends of the people you tag, you can adjust this setting.

■ **Custom:** When you choose Custom, you can

selectively share something with specific people, or hide it from specific people. You can also share with specific friend lists if you’ve set them up.

■ **Only Me:** This option allows you to post stuff to your timeline that is visible only to you. Posts with the audience of Only Me will appear in your News Feed but not your friends’ feeds. When you tag someone in your content and choose Only Me, the audience won’t expand to include the person you tagged.

**Your profile:** When you open a Facebook account, you set up a personal Facebook profile. Certain profile information will always be visible to the public, such as your name, profile picture and cover photo, gender pronoun, and username. You can add other details, like your relationship status, workplace or hometown, if you choose, and make them visible only to the audience you select (just yourself, your friends, friends of friends, a custom list you create, or the public). The dropdown audience selector menu next to each piece of information allows you to choose who can see it, and the default setting for these fields varies (for example, for language, it defaults to public, while for religious views, it defaults to friends of friends).

**Your friends list:** If you don’t want everyone to be able to see your list of friends, you can change the audience by selecting *Who can see your friends list?* (in the app, choose *Settings & Privacy > Settings > Privacy Settings* in the bottom right-hand corner menu, or on the website, choose *Settings > Privacy* in the top right corner menu). You have a handful of options, including creating a customized list. If you don’t want *anyone* else to see your friends list, you can choose “Only Me”; other people will see only mutual friends when they visit your profile, and you’ll still appear on the friends list of anyone you’re friends with. Facebook does not allow you to completely block all friend requests, but under *Who can send you friend requests?*, you can select “Friends of friends” instead of “Everyone.”

**Your timeline:** Only you and your friends can

post to your “timeline” (the part of your Facebook page where you share things). If you don’t want your friends to be able to post, select “Only Me” in the *Who can post on your timeline?* setting (in the app, *Settings & Privacy > Settings > Timeline and Tagging*, or on the website, *Settings > Timeline and Tagging*). What you share will be visible to the same audience as your last post unless you change it, which you can do by using the audience selector directly above or below the post (depending on if you’re in the app or the website). If you change your mind about the audience for an earlier post, you can change it, or even delete or hide the post from your timeline. Click on the “...” icon on the post to see your options. You can even change the audience for all past public and “Friends of friends” posts to just “Friends” in one step. Select the option to limit past posts in the app under *Settings & Privacy > Settings > Privacy Settings*, or on the website under *Settings > Privacy*.

If you decide there are past posts that you would like to hide or permanently remove, a feature called Manage Activity (*Settings > Your Facebook Information > Activity Log > Manage Activity*) enables you to choose multiple posts from your activity log and either delete them or archive them all at once. Archiving only hides them; you can restore them later if you choose. Deleting them will place them in the trash; any of the posts you don’t restore within 30 days will be automatically purged.

While you can always delete a post, it’s important to remember that you can’t do anything about who might have already seen it, so it’s best to be careful from the start. And remember, when you post to another person’s timeline, you have no control over who will see (or take a screenshot of) it. If you’ve hidden posts from your timeline (by clicking on the “...” icon at the top of a post and choosing *Hide from timeline*), no one can see them on your timeline, but they may still show up in search results and other places on Facebook.

**Your News Feed:** Everyone sees something different in their News Feed—a constantly

changing list of status updates, photos, videos, links, app activity, etc.—because the content is based on your Facebook activity. Facebook provides an explanation of how this works for a particular post under the “Why am I seeing this post?” option, where you can also take steps to manage what you see from that account in the future.

To manage what appears in your News Feed, you can make some adjustments. If you know you want to see posts from certain people, on the website, open the menu in the top right corner of the screen and choose *News Feed Preferences*; in the app, open the menu in the bottom right corner and choose *Settings & Privacy > Settings > News Feed Preferences*. From here, you can choose whose posts to see first. You can also “unfollow” people and groups so you won’t see their posts in your News Feed anymore, among other options. (They won’t know you unfollowed them, and you can start following them again at any time.)

**Tags:** Tagging in Facebook means identifying someone by name in a status update, photo, video, etc. Tagging will also add the post to that person’s timeline, unless you set the post audience to “Only me.” Anyone who is able to see a tag can click on it and go to that person’s profile, but what they see depends on the specific privacy settings that person has selected. In the *Timeline and Tagging* section of *Settings* on both the app and website, you can control a number of preferences for tags, including who can see posts you’re tagged in on your own timeline and whether you can review posts you’re tagged in before they appear on your timeline. You can also remove tags (of yourself, or that you placed on other people) from photos and posts. Edit your post or photo to remove your tag of others; or, to untag yourself, go to the post or photo and select “Remove tag” under the menu of options. While removed tags will no longer appear on the post or photo and the post or photo will no longer appear on your timeline, the item is still visible to the audience it’s shared with, and may be visible in places like News

Feed or search results. To remove it from Facebook completely, ask the person who posted it to take it down.

**Reactions and comments:** Anyone in the audience for your post also can react to it and comment on it, and see others' reactions and comments. Use the menu at the top or bottom of your post if you want to change the audience. You have the option to decide who can comment on your public posts. This is controlled in the *Public Posts* section in *Settings* for both the app and the website. In addition to the group you choose here (Public, Friends, or Friends of friends), anyone tagged in a post and their friends may be able to comment too. Also, be aware that if you commented on someone's post when the audience was set to, say, Friends, your comment would become public if the poster later changed the audience to Public.

## Advanced privacy settings

While the basic settings provide a great deal of control over who sees what, Facebook offers many additional options for fine-tuning your privacy level. Here are some of the other settings you can adjust to match your preferences.

**Face recognition:** Facebook uses facial recognition technology to identify people in photos and videos. This is done for convenience (lets you tag people quickly and easily), privacy (lets you know if you appear in an image but haven't been tagged/notified), safety (protects you from scammers using a photo of you as their profile picture), and accessibility (telling people with visual impairments who is in a photo). You can control the use of this technology under *Face Recognition* in *Settings* for both the app and website, where you can choose whether or not to allow Facebook to recognize you in photos and videos.

## Blocking, unfriending and unfollowing

■ **Blocking:** If you "block" someone, that person can no longer search for your profile, see things you post on your timeline, tag you, invite

you to events or groups, start a conversation with you, or add you as a friend. To block someone, go to *Blocking* under *Settings* for both the app and website and enter the person's name or email address. When you unblock someone, that person will be able to see your *public* posts, but won't automatically become your friend again.

■ **Unfriending:** "Unfriending" someone removes each of you from the other's friends list. But, unlike someone who's been blocked, an unfriended person can find you again on Facebook and try to restore the friendship. To unfriend someone, go to their profile and, in the app, click on the "Friends" icon below their profile image and select "Unfriend"; on the website, hover over "Friends" to the right of their profile photo and select "Unfriend."

■ **Unfollowing:** "Unfollowing" someone is the most subtle of the three options. It keeps your friend's posts from showing up in your News Feed, but you'll remain friends. Unfollow someone by clicking on the "..." icon on a post in your News Feed and choosing the desired option from the dropdown menu. You can also unfollow them directly by visiting their profile. On the app, click the icon indicating you are friends under their profile photo, click the "Following" button and select "Unfollow"; on the website, hover over the "Following" icon to the right of their profile photo and select the same.

**Search:** You can search for anything on Facebook—including people, posts, photos, videos, places, Pages, groups, apps, links and events. Whether your posts appear in someone's search results depends on the audience for that post. If you've made a post public, anyone may be able to see it when they search for something related to what's in your post. Depending on your privacy settings, people may be able to search for your Facebook profile using a phone number or email address. To control who can find you this way, click on *Who can look you up using the phone number you provided?* in the app, located under *Privacy & Settings* >



*Settings > Privacy Settings*; on the website, go to *Settings > Privacy* and then select “Everyone,” “Friends of friends,” “Friends” or “Only me.”

Do the same for *Who can look you up using the email address you provided?*

If you don’t want search engines outside of Facebook to link directly to your profile, you can make sure permission is denied in *Do you want search engines outside of Facebook to link to your profile?* (It can take some time for search engines to stop linking to your profile. Facebook does not have control over content that has already been indexed and cached in search engines, so you’d have to contact the search engine directly to request immediate removal.)

**Apps:** When you use Facebook Login to authenticate (or sign in to) third-party apps, you consent to sharing some information with the app. This information includes your name and profile picture, and other information you can choose to share, like age range, gender or a list of your friends who have also chosen to share their friend lists with the app.

When you log in for the first time, you will be presented with a list of what information the app is requesting permission to access and have the option to deny access to specific pieces of information.

To check which apps you’ve granted access to your Facebook data, find out which pieces of data they can access, and edit their permissions (what data they can access), go to *Apps and Websites* under *Settings* on both the app and website. By clicking through to *Logged in with Facebook*, you can edit active apps to change the data they can access; you can also select and remove the apps you no longer want connected to your Facebook account. (You’d have to contact the app developer directly to ask them to delete whatever data they’ve collected up to this point, and they’re probably under no obligation to do so.)

If you haven’t used an app or website for more than 90 days, the app may still have access to information you previously shared, but its ability

to make additional requests for private info has expired. You also can block certain apps completely by entering them in the *Manage Blocking* list (under *Privacy & Settings > Settings > Blocking* in the app, and *Settings > Blocking* on the Facebook website). Once you block an app, it can no longer contact you or get non-public information about you through Facebook.

## Ads

Facebook shows you ads based on your profile, your location, your activity on Facebook, and your activity elsewhere (websites, apps, some retailers, etc.) that can be matched to your Facebook profile. Likewise, you may see ads “served” by Facebook on other websites, apps and devices if they use Facebook’s advertising tools.

The “**Off-Facebook Activity**” tool allows you to view and manage the information other apps and websites share with Facebook about your interactions with them. You have the choice to disconnect the information from your account, and can also disconnect future off-Facebook activity. Visit *Your Facebook Information* under *Settings* on the website or in the app.

You also have control over the **types of ads** you see and how your information is used to personalize your ads experience. For any ad you see on Facebook, you can choose “Why am I seeing this ad?” to learn more about why that ad was shown, and you can also directly hide and report ads when you see them. For additional information and controls, visit *Ads* under *Settings* on the website or *Ad Preferences* under *Settings & Privacy > Settings* in the app. From there, you can hide ads from a particular advertiser, change whether advertisers can target you based on particular data, or change the things that influence which ads you see.

You’ll find a number of different options that provide transparency and control for users:

■ **Your Interests:** You can view and remove your “Interests” logged by Facebook used to personalize ads; these are based on the Facebook

Pages you interact with and the Facebook ads you click.

■ **Advertisers and Businesses:** You can view your relationship to other advertisers and businesses on Facebook, like whose ads you've clicked on. For example, you can see which advertisers ran an ad by uploading a list to Facebook containing your information (usually an email address or a phone number) and hide future ads from these advertisers.

■ **Your Information:** You can switch on and off whether advertisers can target ads to you based on your relationship status, employer, job title or education. You can also remove advertising categories Facebook has added you to based on your Facebook information and other activity. Advertisers use these categories to reach specific audiences.

■ **Ad Settings:** You can also turn off specific types of advertising.

■ You can choose to not see ads based on data that businesses send to Facebook about your activity off of the platform, like whether you purchased something on that partner's site.

■ You can stop advertising that's based on your Facebook activity from appearing on other websites, apps and devices that use Facebook's advertising services.

■ You can prevent your friends from being served ads that display your social actions. For example, this stops your "Likes" from being used to serve ads to your friends along with a message such as "Julie Jones likes this."

■ With "**Hide ad topics,**" you can tell Facebook you don't want to see ads about certain topics, like parenting, alcohol or pets, temporarily or permanently.

Clearing your interests and hiding certain types of advertising will not prevent you from being shown ads; the ads you see may be less personalized based on your activity. Learn more on Facebook's "Advertising" page (<https://www.facebook.com/ads/about>).



## Location tracking

Facebook uses your location for a variety of purposes, including to let you know about nearby friends (mobile app and opt-in only), events and businesses, deliver local ads and news, and detect suspicious activity on your account. Facebook offers a number of location settings. You can control whether your device shares precise location information with Facebook via *Location Services*, a setting on your mobile device.

If *Location Services* is off, Facebook may still understand your location using things like check-ins, events, and information about your internet connection. On Android, the *Background Location* setting in the Facebook app lets you control if Facebook can access your device's precise location through *Location Services* when you're not using the app. Similarly, on iOS, Facebook only collects your precise location when you're not using the app if you've set *Location Services* to "Always" on your device.

You can also control whether Facebook stores a history of your precise locations received through *Location Services* on your device via *Location History*, an opt-in setting within Facebook. You can

turn the feature on or off, and delete the history, if you choose, under *Settings > Location*. If Location History is on, you can view a timeline of specific places you have been, organized into days. The history reflects the location information received from your device through *Location Services*. Only you can see this information.

Learn more about the location data Facebook collects and how it uses it on the company's Data Policy page: <https://www.facebook.com/policy.php>.

## Your Facebook Information

The *Your Facebook Information* section, under *Settings* on the website or in the app, reveals what information has been collected about you, allows you to manage your data, and lets you delete your Facebook account and data. It includes these categories:

- **Access Your Information:** View your information by category (around two dozen of them).
- **Download Your Information:** Download a copy of your information.
- **Activity Log:** View your activity and audience for each, and, if desired, edit items.
- **Off-Facebook Activity:** View information businesses and organizations share with Facebook about your interactions with them, like visiting their apps or websites. You can disconnect that activity history from your Facebook account.
- **Managing Your Information:** This tool guides you through managing particular pieces of your Facebook and Instagram (owned by Facebook) data (located in *Account Ownership and Control* in the app).
- **Deactivation and Deletion:** From here, you can temporarily deactivate or permanently delete your Facebook account (located in *Account Ownership and Control* in the app). You have the option to download a copy of your information before deleting.

## Facebook best practices

There are some relatively simple but effective things you can do to protect your privacy while socializing on Facebook.

■ Take advantage of two-factor authentication (Facebook will send you a code by text message, or you will access a code via third-party authentication app that you'll need to input to log in from an unrecognized phone or computer). This will help prevent someone else from logging in to your account even if they do get ahold of your password. Choose to get an alert if there is an unrecognized login to your account. Set these up in *Security and Login*, under *Settings*.

■ Share optional profile details only with your closest friends, or don't share them at all. Paired with other information in your profile and timeline, some seemingly innocent facts—birthdate, employment history, places lived, etc.—could be used to compromise your identity or accounts.

■ Avoid "public" settings on your personal account. In most cases, "Only Me," "Friends" or customized lists are the best options (though "Friends of friends" might also be okay, depending on what you're sharing). Always check who you're posting to and change your audience as needed.

■ Don't announce your location in real time by clicking the "check in" pin when posting. Generally speaking, sharing your travels and activities is safer after they are over. If you do want to share your current location, be sure it's with a safe audience.

■ Don't accept "friend" requests from strangers, and edit your friends list regularly or create a Custom List to avoid sharing with a larger audience than necessary.

■ If you're already Facebook friends with someone and you get another request, it could be coming from a fake account. Check with your friend or family member to make sure it's really them asking to connect.

■ Review your settings regularly to make sure they still match your preferences. At the same time, review your *Activity Log* (under *Your Facebook Information* in *Settings*) to make sure old posts on your timeline still reflect your preferred audience (if not, you can change the audience, or hide or delete the post).

■ If you don't want your friends to be served ads displaying your social activity on Facebook, don't click "Share," "Like" or similar buttons associated with a page or post.

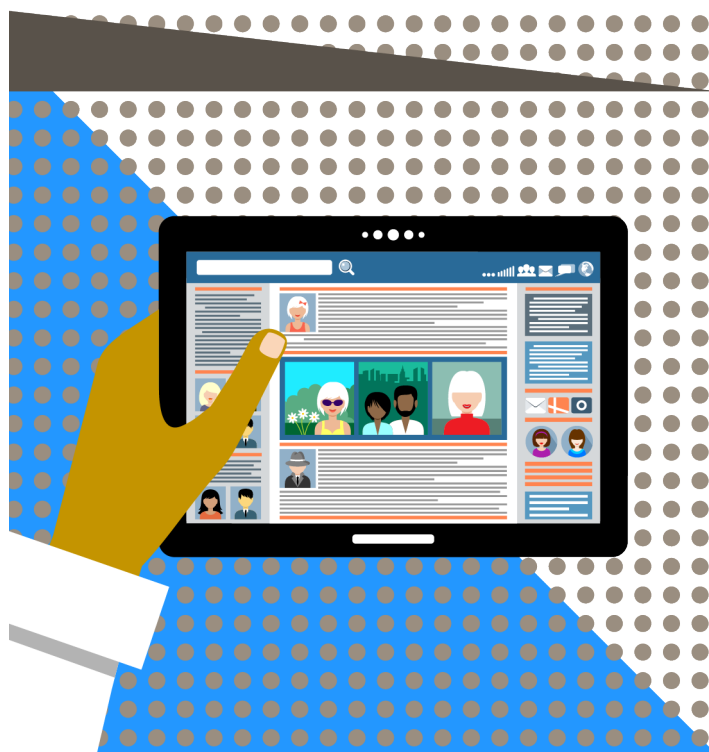
■ Many apps and websites allow you to log in using your Facebook username and password. Make sure to check what information the app is requesting permission to access, and remove any categories you don't want to share.

■ The best way to report abusive content or spam on Facebook is by using the *Report* link that appears near the content itself. Visit the "How to Report Things" page (<https://www.facebook.com/help/reportlinks>) for more detailed information.

## Learn more

**Facebook's Parents Portal** (<https://www.facebook.com/safety/parents>) offers links, tips and tricks to help parents guide their kids in using social media safely and responsibly.

**Facebook's Youth Portal** (<https://www.facebook.com/safety/youth>) provides general tips, insider tricks, privacy and safety information, and everything else that young people need to have a safe, responsible and enjoyable Facebook experience. (People under 13 may not establish Facebook profiles, even with parental approval.)



**Facebook's Online Well-being** page (<https://www.facebook.com/safety/wellbeing>) connects visitors to suicide prevention and social resolution resources.

**The Facebook Newsroom** (<https://newsroom.fb.com/news/>) posts the latest news stories about the company's activities and the issues of data privacy, online safety, social impact, and more.

**Facebook's Privacy Basics** (<https://www.facebook.com/about/basics>) makes it easier for people to find tools for controlling their information on Facebook, offering users tips on things like securing their account, understanding who can see their posts and knowing what their profile looks like to others.

Consumer Action's **Take control: Customizing your social media privacy settings** ([https://www.consumer-action.org/english/articles/social\\_media\\_privacy\\_controls](https://www.consumer-action.org/english/articles/social_media_privacy_controls)) explains how social media users can protect their privacy, offers specific tips for each of the eight most popular social networks, and links to resources where readers can learn more.

## About this guide

Consumer Action created this guide in partnership with Facebook.

© Consumer Action 2020

## About Consumer Action

[www.consumer-action.org](http://www.consumer-action.org)

Through education and advocacy, Consumer Action fights for strong consumer rights and policies that promote fairness and financial prosperity for underrepresented consumers nationwide.

**Consumer advice and assistance:** Submit consumer complaints to: <https://complaints.consumer-action.org/forms/english-form> or 415-777-9635. (Spanish-language complaints can be submitted to: <https://complaints.consumer-action.org/forms/spanish-form/>.)

Our hotline accepts calls in Chinese, English and Spanish.