

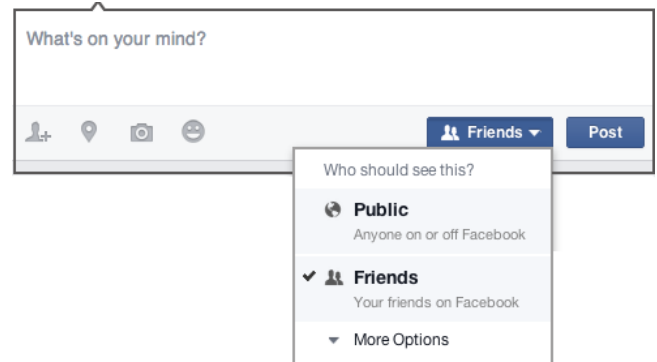
# SOCIAL MEDIA PRIVACY AND SECURITY

## >> FACEBOOK

### When I post something, how do I choose who can see it?

You'll find an audience selector tool most places you share status updates, photos and other things you post. Click the tool and select who you want to share something with.

The tool remembers the audience you shared with the last time you posted something and uses the same audience when you share again unless you change it. For example, if you choose Public for a post, your next post will also be Public unless you change the audience when you post. This one tool appears in multiple places, such as your privacy shortcuts (<https://www.facebook.com/privacy>) and privacy settings. When you make a change to the audience selector tool in one place, the change updates the tool everywhere it appears.



### How do I control who can see what's on my profile and timeline?

- To edit things like places you've lived or your family and relationships, click About below your cover photo, then hover over the info you'd like to change and click Edit. Use the audience selector next to this info to choose who you're sharing it with.
- Anyone can see your public information, which includes your name, profile picture, cover photo, gender, username and networks.
- Only you and your friends can post to your timeline. When you post something, you can control who sees it by using the audience selector. When other people post on your timeline, you can control who sees it by choosing the audience of the Who can see what others post on your timeline setting. (See above)

### What can I do to keep my account secure?

- **Protect your password.** Don't use your Facebook password anywhere else online, and never share it with other people. Your password should be difficult to guess. Avoid including your name or common words.
- **Never share your login information.** Scammers may create fake websites that look like Facebook and ask you to login with your email and password. Always check the website's URL before you enter your login information. When in doubt, type [www.facebook.com](http://www.facebook.com) into your browser to get to Facebook.
- **Log out of Facebook when you use a computer you share with other people.** If you forget, you can log out remotely.
- **Don't accept friend requests from people you don't know.** Scammers may create fake accounts to friend people. Becoming friends with scammers might allow them to spam your timeline, tag you in posts and send you malicious messages.
- **Watch out for malicious software.** Keep your web browser up to date and remove suspicious applications or browser add-ons.
- **Never click suspicious links, even if they appear to come from a friend or a company you know.** This includes links on Facebook (example: on posts) or in emails. Keep in mind that Facebook will never ask you for your password in an email. If you see a suspicious link on Facebook, report it.
- **Use extra security features.** For example, you can get alerts about unrecognized logins, set up two-factor authentication or choose friends to be your trusted contacts.

# SOCIAL MEDIA PRIVACY AND SECURITY

## >> TWITTER

### How do I control who can see my profile and tweets?

In contrast to Facebook, Twitter tends to be a far more public platform. When you sign up for Twitter, all of your tweets are public by default. Users can search for tweets by keyword or topic, and it is common for users to read and respond to tweets written by people they don't know in real life.

When you follow other users, their tweets will show up on your timeline. You don't need to request permission to follow anyone unless the user's tweets are protected.

If you wish to prevent people you don't know from reading your tweets, you can always protect your tweets. This option, which is available under Settings, allows you to approve or deny access to every user who requests to follow you. However, it is important to remember that there is always the possibility that anything on the internet may become public.

Tweet privacy  Protect your Tweets

If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. [Learn more.](#)

### How can I keep my account secure?

- Use a strong password that you don't reuse on other websites.
- Use login verification. (*See below*)
- Require your email and phone number to request a reset password link or code.
- Be cautious of suspicious links and always make sure you're on [Twitter.com](#) before you enter your login information
- Never give your username and password to third parties, especially those promising to get you followers, make you money or verify your account.
- Make sure your computer software, including your browser, is up-to-date with the most recent upgrades and anti-virus software.

**Login alerts:** When you log in to your Twitter account from a new device for the first time, you will receive a notification via email as an extra layer of security for your account. If you did not log in from the device, you should follow the steps in the notification email to secure your account, starting by changing your Twitter password immediately.

**Login verification:** Login verification is an extra layer of security for your Twitter account. Instead of only entering a password to log in, you'll also enter a code which is sent to your mobile phone. This verification helps make sure that you, and only you, can access your account.

After you enable this feature, you will need both your password and your mobile phone, or a security key (via [twitter.com](#)) to log in to your account. When you log in to [twitter.com](#), [Twitter for iOS](#), [Twitter for Android](#) or [mobile.twitter.com](#), you will receive a six-digit login code to enter.


# SOCIAL MEDIA PRIVACY AND SECURITY

## >> INSTAGRAM

### How do I control who can see my profile and posts?

By default, anyone can view your profile and posts on Instagram. You can make your posts private so that only followers you approve can see them. If your posts are set to private, only your approved followers will see them on hashtag or location pages.

### To set your posts to private from the Instagram app:

- Tap  to go to your profile, then tap .
- Tap  Settings.
- Tap Privacy and Security, then Account Privacy, and turn on Private Account.

### Things to keep in mind about private posts:

- Private posts you share to social networks may be visible to the public depending on your privacy settings for those networks. For example, a post you share to Twitter that was set to private on Instagram may be visible to the people who can see your tweets.
- Once you make your posts private, people will have to send you a follow request to see your posts, your followers list or your following list.
- Follow requests appear in Activity, where you can approve or ignore them.
- If someone was already following before you set your posts to private and you don't want them to see your posts, you can block them.
- People can send a photo or video directly to you even if they're not following you.

### How can I keep my account secure?

- Pick a strong password. Use a combination of at least six numbers, letters and punctuation marks (like ! and &). It should be different from other passwords you use elsewhere on the internet.
- Change your password regularly, especially if you see a message from Instagram asking you to do so. During automated security checks, Instagram sometimes recovers login information that was stolen from other sites. If Instagram detects that your password may have been stolen, changing your password on Instagram and other sites helps to keep your account secure and prevent you from being hacked in the future.
- Never give your password to someone you don't know and trust.
- Turn on two-factor authentication for additional account security.
- Make sure your email account is secure. Anyone who can read your email can probably also access your Instagram account. Change the passwords for all of your email accounts and make sure that none are the same.
- Log out of Instagram when you use a computer or phone you share with other people.
- Don't check the "Remember Me" box when logging in from a public computer; as this will keep you logged in even after you close the browser window.
- Think before you authorize any third-party app.