

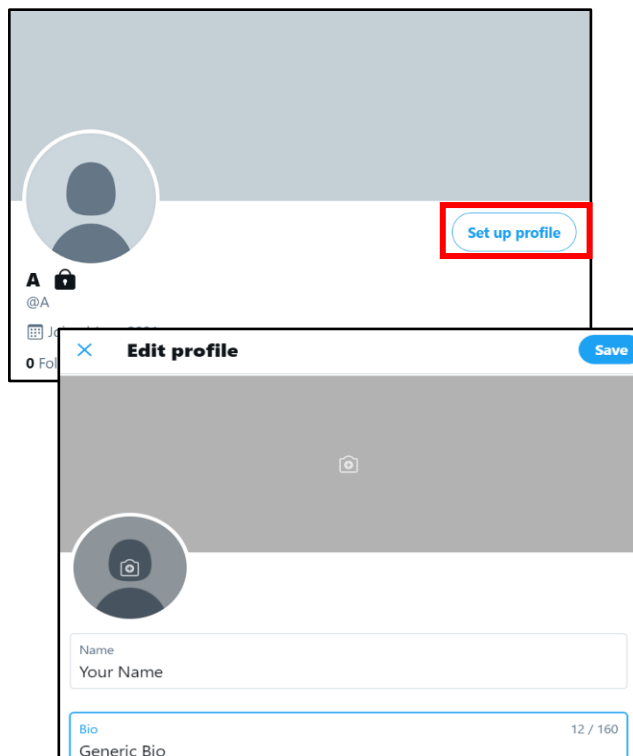
X (TWITTER)

- **Do** be careful when using #hashtags in posts as it allows users to index and associate your posts with a particular topic.
- **Do** use caution when posting images and videos of any kind. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.
- **Do** use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.
- **Do** ensure that family members take similar precautions with their accounts.
- **Don't** provide any identifiable information (e.g., name, hobbies, job title, etc.) on your profile or in your posts.
- **Don't** link your X account to any third-party applications such as Facebook, LinkedIn, or fitness apps.
- **Don't** allow X to access your location. Disable location services when posting images on whichever device you are using whether it be iOS, Android, or when uploading from your computer.
- **Don't** allow people you do not know in real life to follow you. Only maintain connections with people and pages you know and trust.

Your Profile

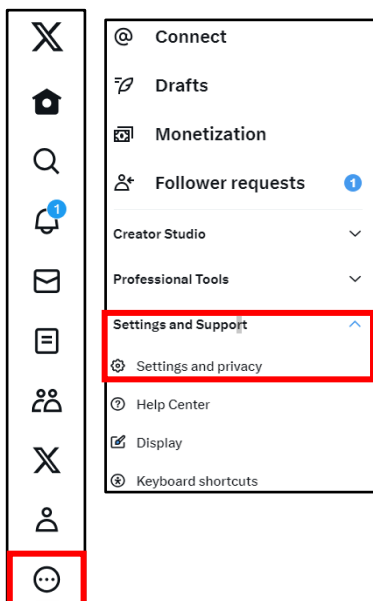
Let's start by locking down your account on your PC (web-based version) by first checking out what your "Profile" says about you. Click the "Profile" icon at the lower left of the screen - this is likely your profile picture. Click "Edit Profile" or "Set up Profile" as shown to the right.

Notice the "Profile Image" and "Header Image" sections. It is recommended you do not use photos of yourself for your profile and header photos. These are viewable to the public and present an unnecessary vulnerability.



Below the "Profile Image" section are the "Name," "Bio," "Location," "Website," and "Birthday" sections. Filling these in is not required, and it is recommended that you leave them blank or use generic information. Even if you use inaccurate location data, it is possible for someone to tie the data back to you by using data aggregator sites. Personally Identifiable Information (PII) is often used as a means to gain access to certain accounts (banks, credit cards, school etc.). Just providing your (correct) birthday could help someone steal your identity. Changing your birthday, even by just one day, during registration provides additional protection against identity theft.

X (TWITTER)



Settings and Privacy

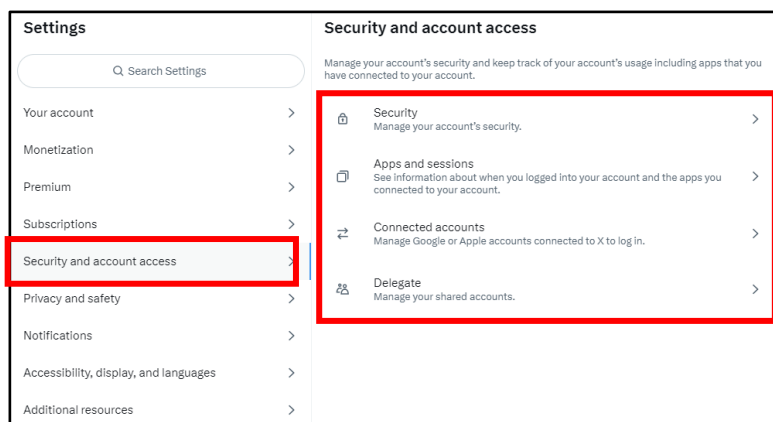
Now, let's move on to the "Settings and Privacy" tab under the "More" section on the same menu at the left-hand side of your screen.

Getting to the "Settings and Privacy" section on your smartphone varies slightly from the computer-based version. These settings need to be updated separately as X is programmed differently on each version. Settings may not automatically transfer between your devices.

From here, you will see your setting options and can review your account information, security, privacy and safety, notifications, etc.

Security and Account Access

Next, go to "Security and Account Access." Here it is recommended you activate "Two-factor authentication" and "Additional password protection" under the "Security" tab. You can also see the apps connected to your account, what accounts you use to login into X with, and manage any shared accounts you may have.



Security

Manage your account's security.

Two-factor authentication

Help protect your account from unauthorized access by requiring a second authentication method in addition to your Twitter password. You can choose a text message, authentication app, or security key. [Learn more](#)

Two-factor authentication >

Additional password protection

Enabling this setting adds extra security to your account by requiring additional information to reset your password. If enabled, you must provide either the phone number or email address associated with your account in order to reset your password.

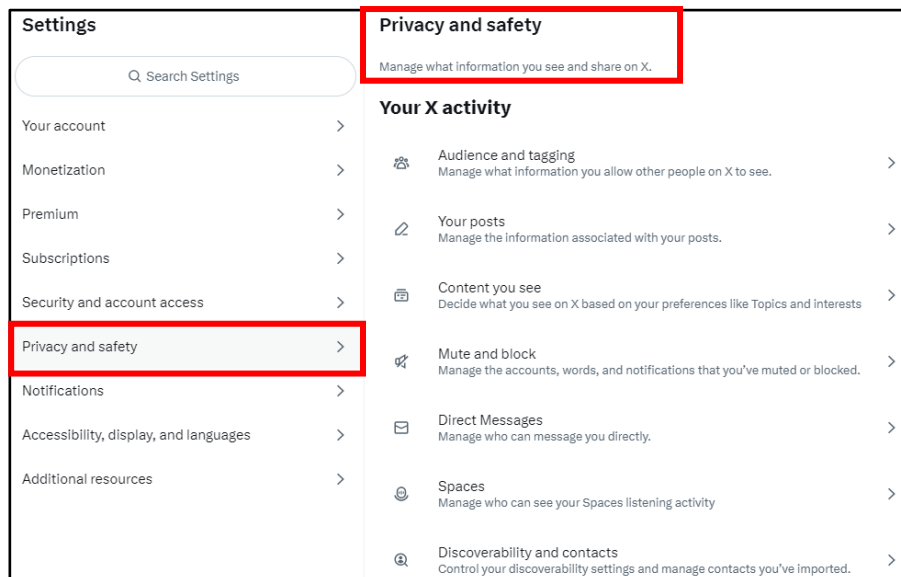
Password reset protect ☒

Changing an account's password does not automatically log the account out of X for iOS or X for Android applications. In order to log out of the account on these apps, sign in online and visit "Apps" in your settings. From there you can revoke access for the application, and the next time the app is launched a prompt will request that the new password be entered.

X (TWITTER)

Privacy and Safety Settings - Your X Activity

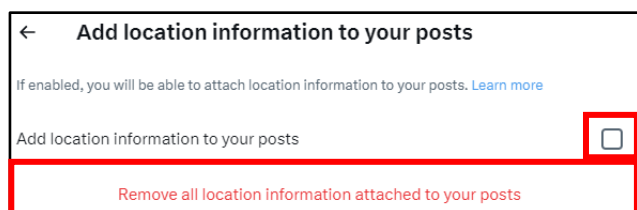
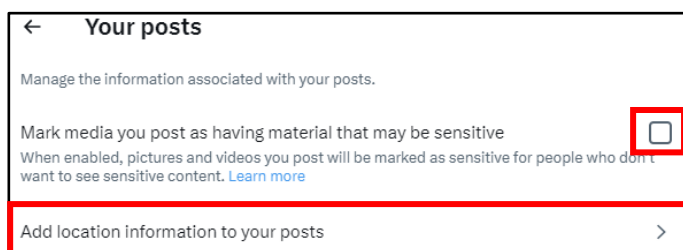
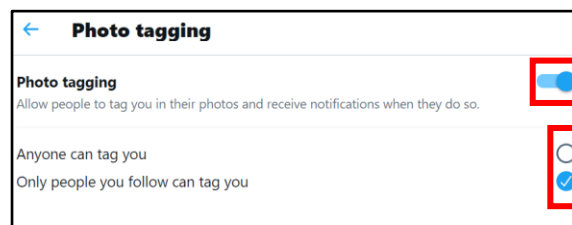
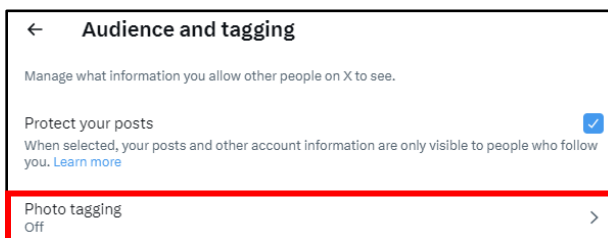
Next, go back to the left column, under “Settings” select “Privacy and safety” (see below).



Audience and Tagging

First, in the “Your X activity” section, go to “Audience and tagging.” Check the box to “Protect your posts” – this makes your account private.

Here you can turn off “Photo tagging” options or ensure only people you follow can tag you.



Location Information

Next, go to the “Your Posts” section. Here you can mark your posts as “sensitive,” which will prevent those who you do not want to see that type of content from viewing your posts.

It is also important to remove location data from your post. Make sure the box is unchecked in the “Add location information to your Posts.”

X (TWITTER)

Content You See

These next settings help control the content you see. This menu is especially helpful if you are locking down a child's account. This section also has a location setting in "Explore settings" that uses your location to show you content happening near you. It is best to leave this unchecked. You'll also want to ensure "Search settings" are hiding sensitive content and blocked/muted accounts from view.

Content you see

Decide what you see on X based on your preferences like Topics and interests

Display media that may contain sensitive content ☐

Topics >

Interests >

Explore settings >

Search settings >

Explore settings

Location

Show content in this location ☐

When this is on, you'll see what's happening around you right now.

Explore locations >

Search settings

Hide sensitive content ☒

This prevents posts with potentially sensitive content from displaying in your search results. [Learn more](#)

Remove blocked and muted accounts ☒

Use this to eliminate search results from accounts you've blocked or muted. [Learn more](#)

Direct Messages

Another setting to consider is how you're contacted on X. Go to the "Direct Messages" section. Uncheck the first box in this section in order to limit incoming messages from people you do not know. You can also check the "Filter low-quality messages" box which hides messages that are flagged as potential spam.

Direct Messages

Control who can message you

Depending on the setting you select, different people can send you a direct message. [Learn more](#)

Allow messages only from people you follow ☒

You won't receive any message requests

Allow message requests only from Verified users ☐

People you follow will still be able to message you

Allow message requests from everyone ☐

People you follow will still be able to message you

Other controls

Filter low-quality messages ☒

Hide message requests that have been detected as being potentially spam or low-quality. These will be sent to a separate inbox at the bottom of your message requests. You can still access them if you want. [Learn more](#)

Hashtags (#) are used to index key words and topics on X. Think of them as the topic of your "post." Understand that if your account is public, and you use a hashtag on a post, anyone who does a search on that hashtag may find your post. When you add a hashtag to a post, X adds the message to the hashtag group to allow more users see your post.

X (TWITTER)

← Discoverability and contacts

Control your discoverability settings and manage contacts you've imported.

Discoverability

Decide whether people who have your email address or phone number can find and connect with you on X.

Let people who have your email address find you on X ☐

Let people who have your email address find and connect with you on X. [Learn more](#)

Let people who have your phone number find you on X ☐

Let people who have your phone number find and connect with you on X. [Learn more](#)

Contacts

Manage contacts that you have imported from your mobile devices. [Learn more](#)

[Manage contacts](#)

[Remove all contacts](#)

These are the contacts that you have imported from your mobile devices. This information is used to personalize your experience on X, such as suggesting accounts to follow. You can remove any contacts you've previously uploaded and turn off syncing with X on all devices. Please be aware that this takes a little time. [Learn more](#)

Discoverability and Contacts

In the “Discoverability and contacts” section, ensure both boxes under “Discoverability” are unchecked. It is best to maintain as much control as possible over who is connecting with you.





In the “Contacts” section, you can review and remove any contacts X has collected. It is recommended that you not synchronize any of your accounts together or include any email accounts with contact information in them. Synchronizing your email accounts allows X to do more than just upload your contacts - X uses the information to learn more about you and your contacts.

“Remove all contacts,” if there are any in this section, and remember to keep your identifying information off your own X account, in case your contacts try to import your data to any of their accounts.

Privacy and Safety – Data Sharing and personalization

Now, go back to the “Privacy and safety” menu and scroll down. Here, you’ll see “Data Sharing and personalization.” This is where you can manage ad preferences and other location or data-based information from being used by the application.

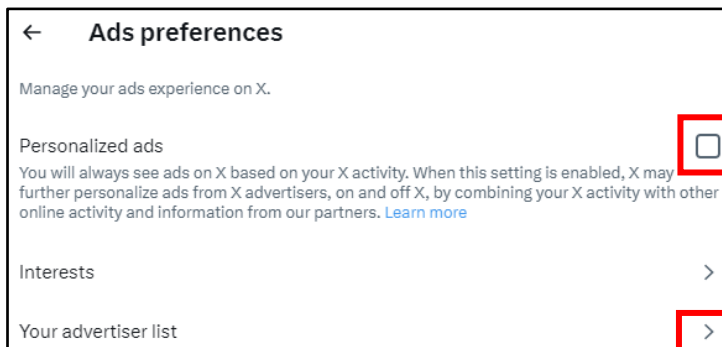
Data sharing and personalization

-  Ads preferences
Manage your ads experience on X. >
-  Inferred identity
Allow X to personalize your experience with your inferred activity, e.g. activity on devices you haven't used to log in to X. >
-  Data sharing with business partners
Allow sharing of additional information with X's business partners. >
-  Location information
Manage the location information X uses to personalize your experience. >

X (TWITTER)

Ad Preferences

In the “Ad Preferences” section, make sure you have unchecked the “Personalized ads” box. You can also see the interests X has mapped to you. Lastly, you can see if you are part of a tailored audience in the “Your advertiser lists.” Tailored audiences are often built from email lists or browsing behaviors. They help advertisers reach prospective customers or people who have already expressed interest in their business.



Inferred identity

Allow X to personalize your experience with your inferred activity, e.g. activity on devices you haven't used to log in to X.

Personalize based on your inferred identity

X will always personalize your experience based on information you've provided, as well as the devices you've used to log in. When this setting is enabled, X may also personalize based on other inferences about your identity, like devices and browsers you haven't used to log in to X or email addresses and phone numbers similar to those linked to your X account. [Learn more](#)



Inferred Identity

It is also recommended to deny X the ability to track your visits to other websites and your browser history, as well as turning off the personalization feature.

Data Sharing with Business Partners

X always shares information with business partners. It is recommended you leave, or ensure this setting is unchecked as well.

Data sharing with business partners

Allow sharing of additional information with X's business partners.

Allow additional information sharing with business partners

X always shares information with business partners as a way to run and improve its products. When enabled, this allows X to share additional information with those partners to help support running X's business, including making X's marketing activities on other sites and apps more relevant for you. [Learn more](#)



Location Information

Lastly, you can see (and clear) places you've been and turn off in-app preferences based on past locations.

Other location settings from the previous “Personalization” section are also listed here for you to review and edit as needed.

Location information

Manage the location information X uses to personalize your experience.

Personalize based on places you've been

X always uses some information, like where you signed up and your current location, to help show you more relevant content. When this setting is enabled, X may also personalize your experience based on other places you've been.



[See places you've been](#)



[Add location information to your posts](#)



[Explore settings](#)



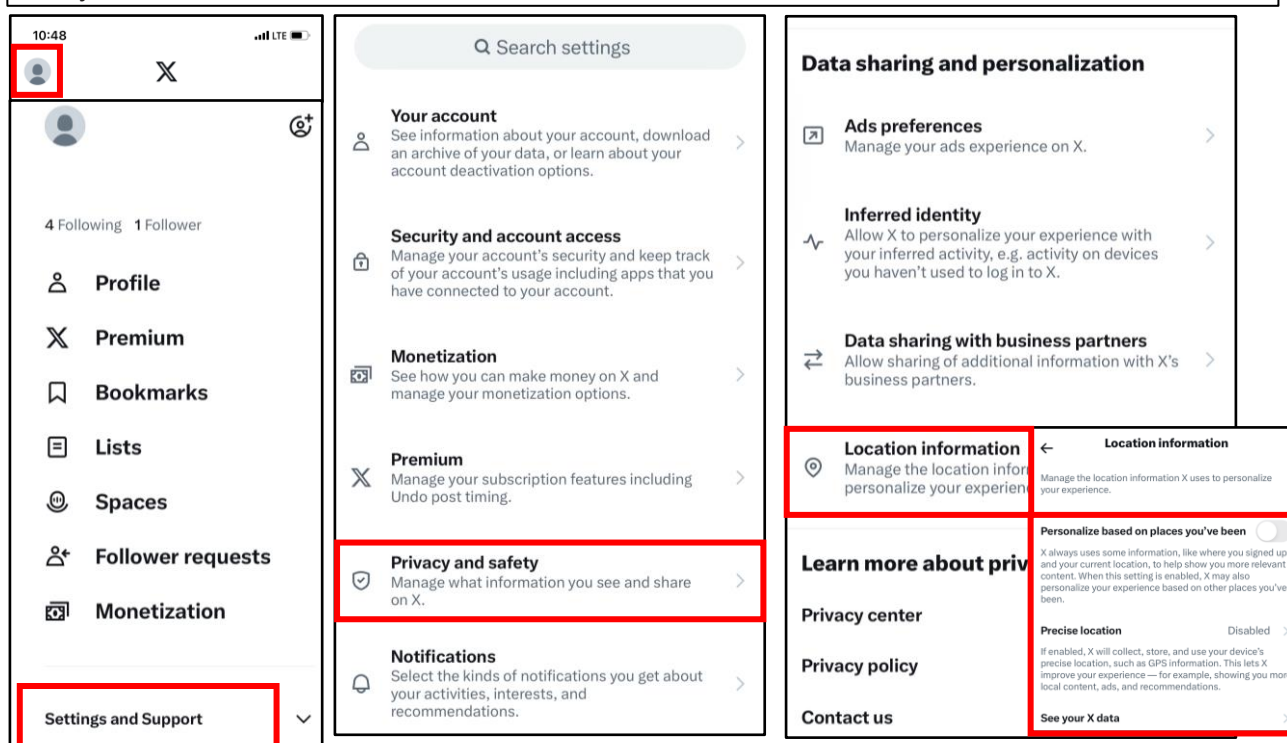
X (TWITTER)

Settings and Privacy

Getting to the “Settings” section on your smartphone is slightly different than the computer-based version. If you frequently access X on your mobile device, you will want to ensure all the previously discussed procedures are completed. Additionally, you will want to accomplish the one lockdown feature that is ONLY available on your smart device – the “Precise Location” feature.

It is important to turn this feature off because it allows X access to your location for advertisements and photo geo-tagging.

Set your “Location” to “Off” on ALL devices.



iPhone users: select the “Profile” icon at the top left of the screen, then select “Settings and Privacy” at the bottom of the menu. Next, select “Privacy and Safety,” scroll all the way down to “Location Information,” and “Precise Location” to ensure it is disabled. See images above.

Android users: getting to the “Settings and Privacy” section is similar to the computer-based version. Once you are in the “Settings and Privacy” link, select “Privacy and Safety” then scroll down to the bottom of the page and select “Precise Location.” It is recommended that you turn this function to “disable” and then select “done.” Images not provided, but similar to iPhone.

If you still need help or have questions, you can contact X using their Support handle @Support.