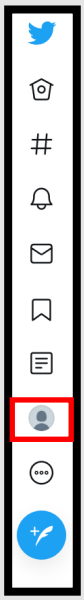
TWITTER SMART CARD

Do's and Don'ts

- Don't provide any identifiable information (e.g. name, hobbies, job title, etc.) on your profile or in your Tweets.
- Don't link your Twitter account to any third party applications such as Facebook, LinkedIn, or fitness apps.
- Don't allow Twitter to access your location. Disable location services when posting images on whichever device you are using whether it be iOS, Android or uploading them 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.
- Do be careful when using hashtags # in Tweets as it allows users to index and associate your Tweet with a particular topic.
- Do ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.
- Do use caution when posting images and videos of you or your family. 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.



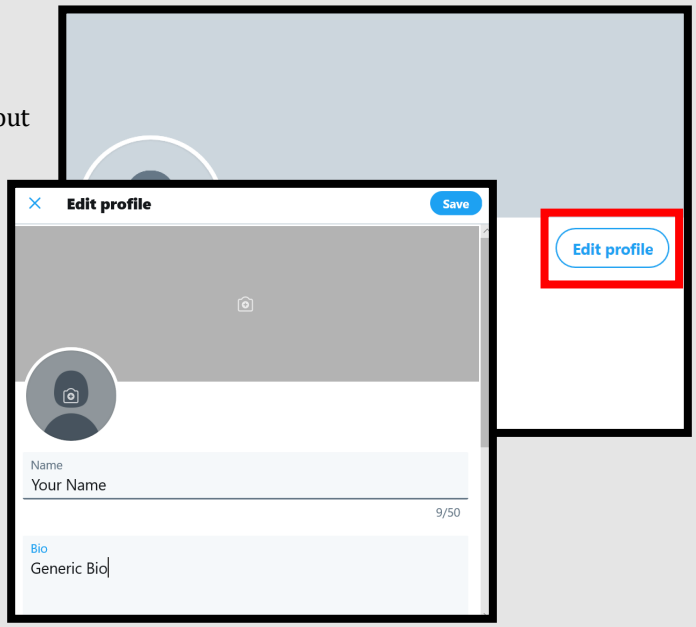
Personal Computer (PC) Version

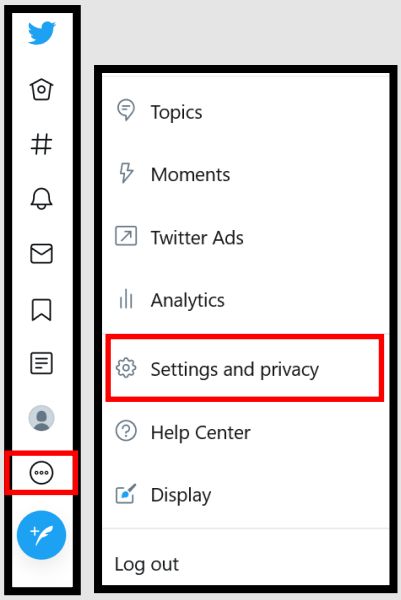
Let's start to lock down your account by first checking out what your "Profile" says about you.

Click the "Profile" icon at the lower left of the screen — this is likely your profile picture.

Click "Edit Profile" as shown to the right.

First, notice the "Profile Image" and "Header Image" sections. It is recommended that you do ***not*** use photos of yourself for your profile and header photos. These are viewable to the public and present an unnecessary vulnerability. Alternative options include avatars and landscape or other types of photos that are not personal and do not contain identifying information within them.





Below the "Profile Image" section are the "Name", "Bio", "Location", "Website" and "Birthday" sections. These are ***not*** required to be filled in, and it is recommended that you leave them blank or generic. 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.). Thus, providing even your birthday could help an identity thief. steal your identity.

Now, let's move on to the "Settings and Privacy" tab on the same menu at the left hand side of your screen. (see left)

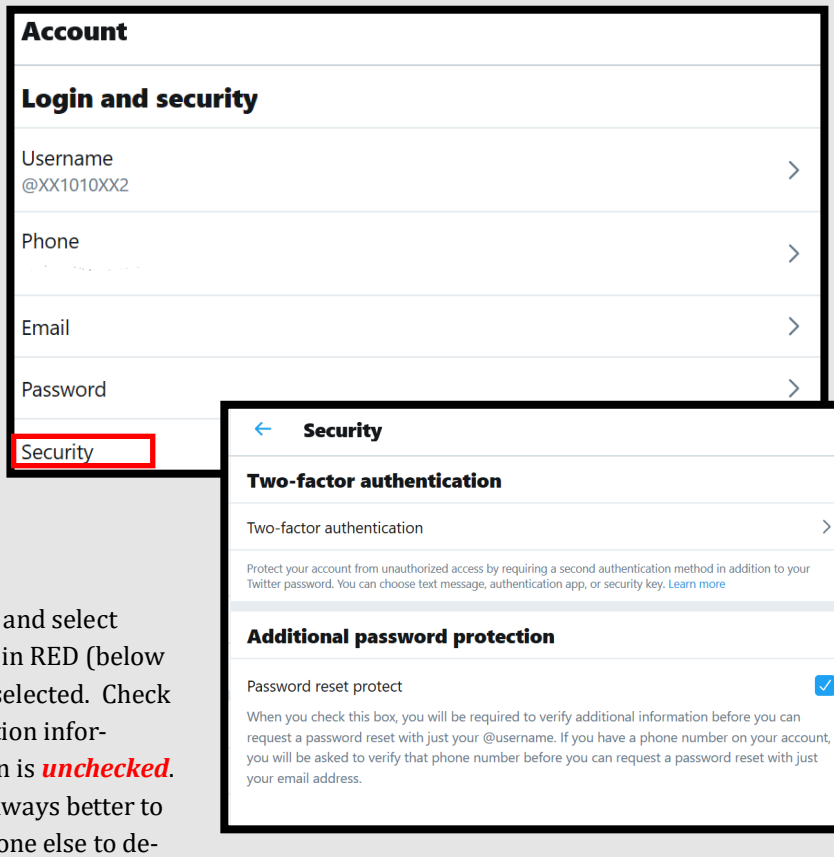
All of these settings need to be separately updated on all the various devices you use to access Twitter, including Android phone, iPhone, and home computers. Twitter is programmed differently on each of these devices, and the settings will not automatically transfer among them. Also, set your "Location" to "Off" on ALL devices.

Twitter accounts are hacked all the time. Make sure to use a strong password that is changed periodically as well as 2FA #safetyfirst

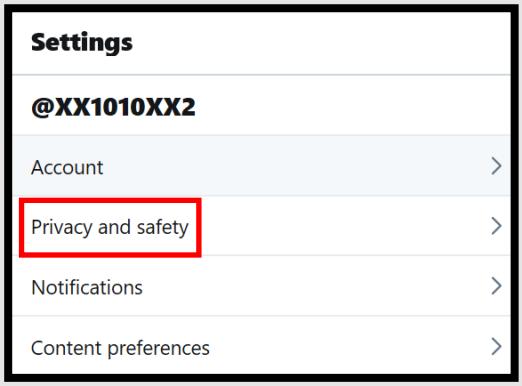
TWITTER SMART CARD

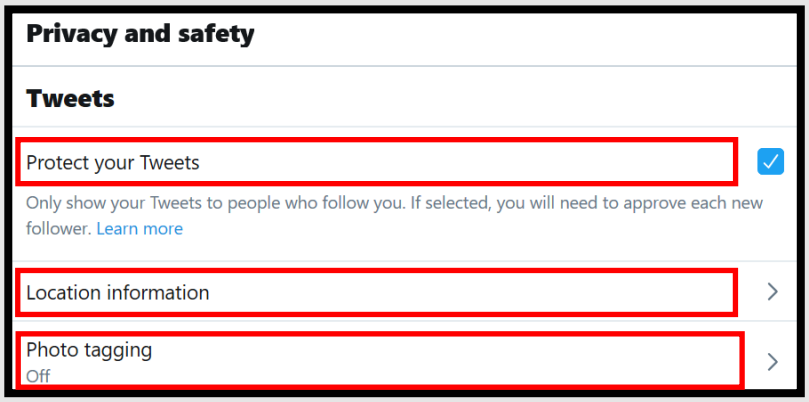
Personal Computer (PC) Version

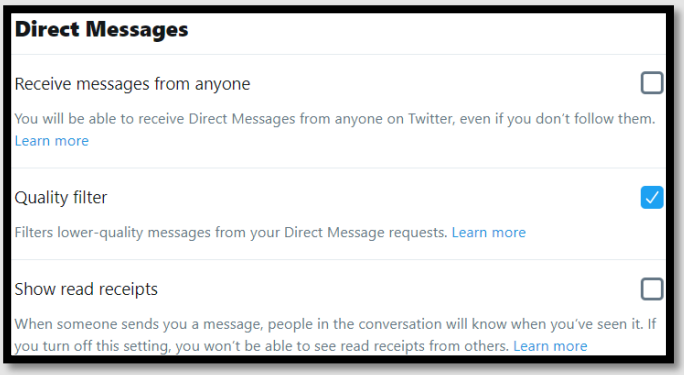
Once in “”Settings and Privacy” you can review your “Account” information, including “Security” settings and how data, such as your “Username” is displayed. Remember to stop and think about what your “Username” says about you, what is it giving away? In the “Account” section, select “Security”. “Two-factor authentication” is the most secure option, and is recommended for your account. Choose your preferred “Two-factor authentication” option, most likely “Text Message”. Also ensure “Password reset protect” is checked. These settings add layers of protection to prevent your account from being hacked.



Next, go back to the left column, under “Settings” and select “Privacy and Safety” (see below). All the sections in RED (below right) are recommended settings that should be selected. Check the box for “Protect your Tweets”, click on “Location information” and make sure the box on the next screen is ***unchecked***. Ensure “Photo tagging” is “Off”. Remember it is always better to control your information than it is to allow someone else to decide for you.







Let’s scroll to the middle of the page and locate the “Direct Messages” section. Uncheck the first and last boxes in this section in order to limit incoming messages from people you do not know.

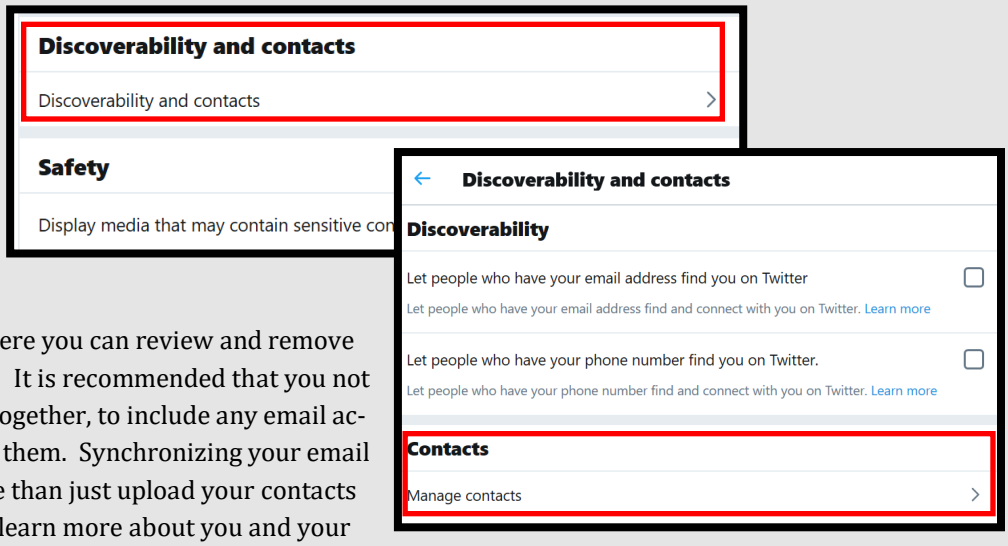
Note: In addition to the information you share with it, Twitter will use your Tweets, content you’ve read, Liked, or Retweeted, and other information to determine what topics you’re interested in, your age, the languages you speak, and other signals. The purpose is generally to show you more relevant content.

Parents! Following your child’s school is important for updates, but if your account isn’t locked down, anyone can see which school your child attends. #lockitdown

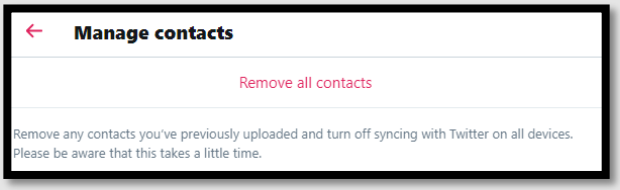
TWITTER SMART CARD

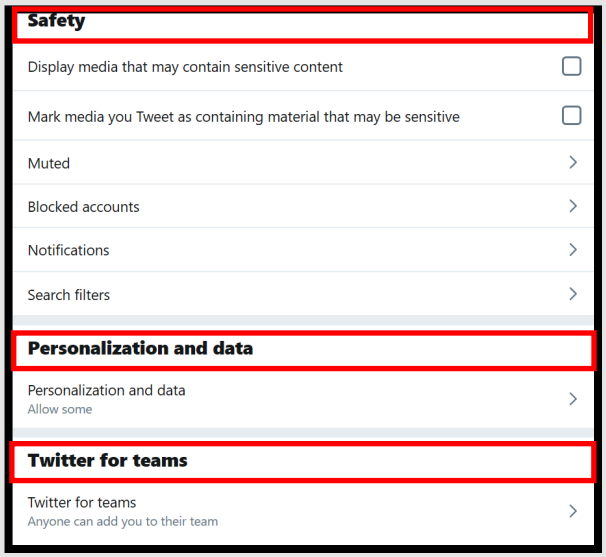
Personal Computer (PC) Version

Next is the "Discoverability and contacts section" (see right). Ensure both boxes under "Discoverability" are unchecked. It is best to maintain as much control as possible of who is connecting with you.

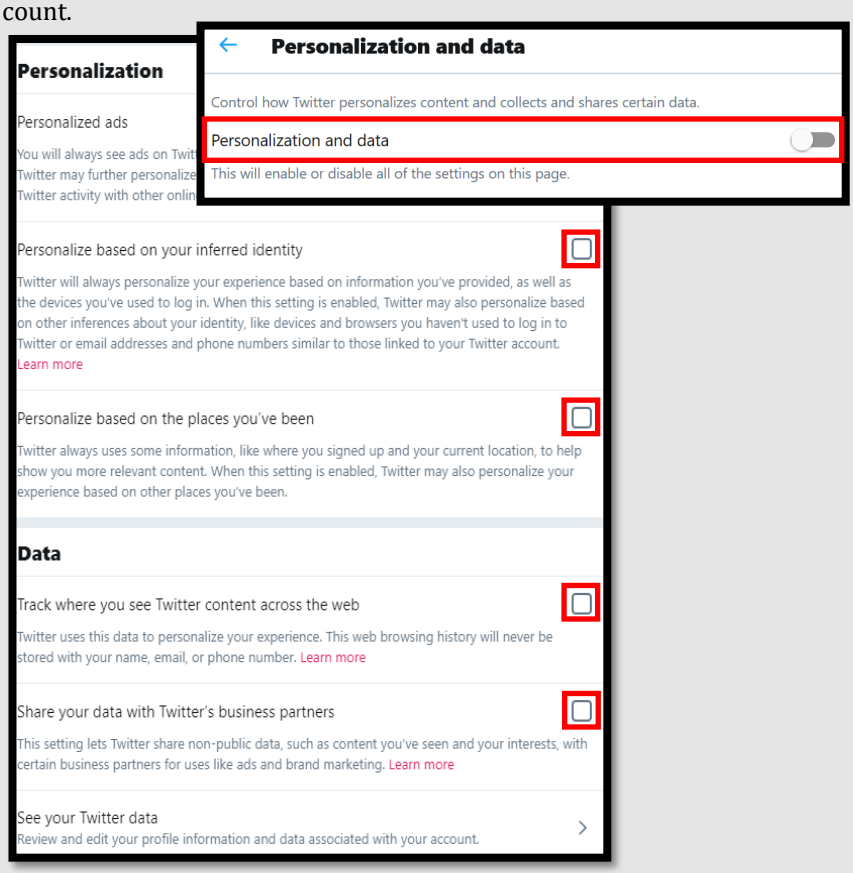


Now click the "Contacts" section. Here you can review and remove any contacts Twitter has collected. It is recommended that you not synchronize any of your accounts together, to include any email accounts with contact information in them. Synchronizing your email accounts allows Twitter to do more than just upload your contacts — Twitter uses the information to learn more about you and your contacts. You should not synch accounts, "Remove all contacts," if there are any in this section, and remember to keep your identifying information off your own Twitter account, in case your contacts try to import your data to any of their accounts.





Below the "Discoverability and contacts "section is the "Safety" section (left). You may want to review this section in order to better control the types of content you see, and more importantly to control what is displayed on your ***child's Twitter*** account.



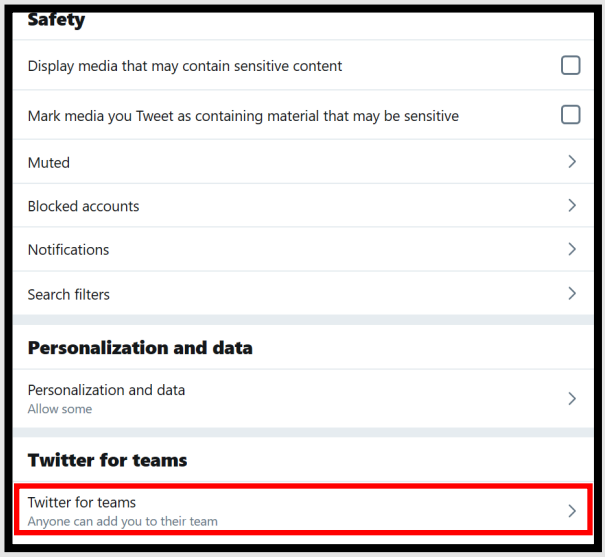
Next, go to the "Personalization and data" section and disable the "Personalization and data" switch, as shown to the right. This will stop Twitter from collecting data regarding your preferences, locations, behaviors and activities. It is recommended that you fully disable this function. Twitter will always collect some data on you from your account, for instance based on your Tweets, comments, and engagements within the app. But where you can limit such collection, it is advised that you do, in order to control as much as possible, the extent to which your information is passed around the Internet.

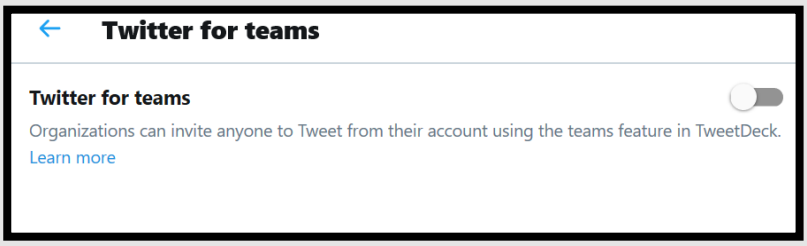
Parents! Following your child's school is important for updates but if your account isn't locked down anyone can see which school your child attends. #lockitdown

TWITTER SMART CARD

Personal Computer (PC) Version

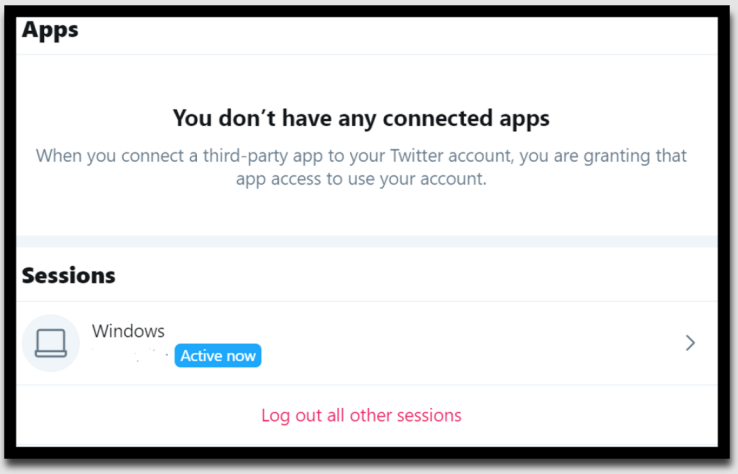
Finally, identify the "Twitter for teams" section. It is important to stay in control of who has access to your profile. We recommend you turn the "Twitter for teams" switch off. This will make it so no one can add you to a team without your permission.

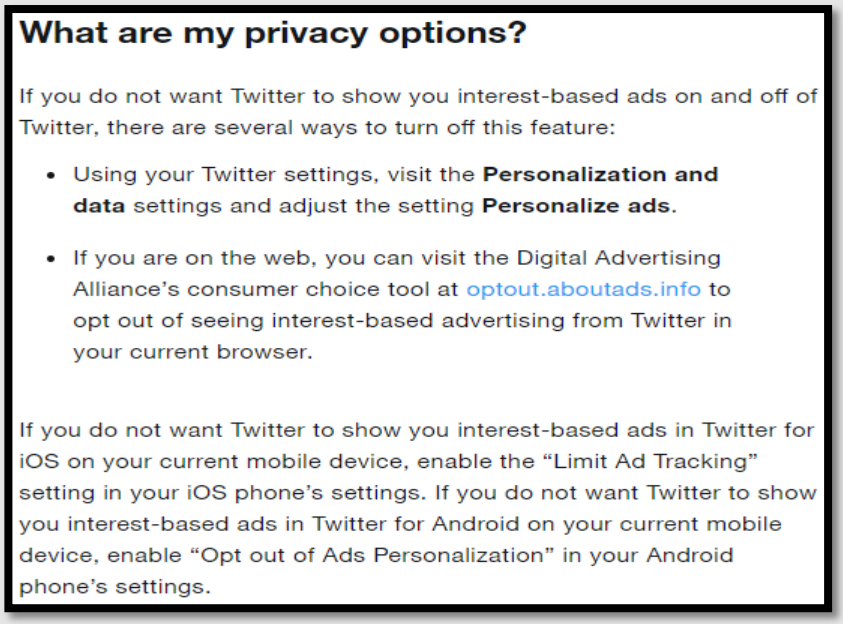




In order to manage your Apps and/or sessions go to "Account" and on the right hand column select "Apps and Sessions". Here you can go through any apps you may have granted access to your Twitter account and revoke access. Limit which apps have access to your account and your personal information.

App Permissions: Third-party apps may request access to perform different actions using your Twitter account. Apps with "read access" can view your profile info, Tweets, and account settings. Apps with "read and write" access can view the above information, as wells as update and manage your profile and account settings, and post, delete, and engage Tweets on your behalf. Always keep an eye on your "Connected Apps", especially what permissions they have.





What are my privacy options?

If you do not want Twitter to show you interest-based ads on and off of Twitter, there are several ways to turn off this feature:

- Using your Twitter settings, visit the **Personalization and data** settings and adjust the setting **Personalize ads**.
- If you are on the web, you can visit the Digital Advertising Alliance's consumer choice tool at optout.aboutads.info to opt out of seeing interest-based advertising from Twitter in your current browser.

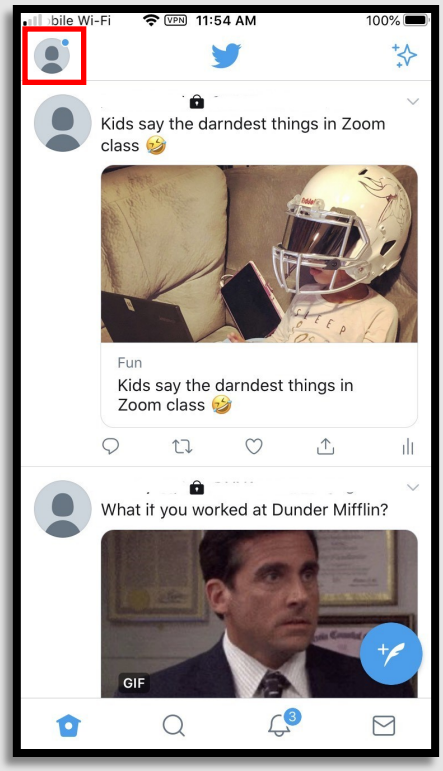
If you do not want Twitter to show you interest-based ads in Twitter for iOS on your current mobile device, enable the "Limit Ad Tracking" setting in your iOS phone's settings. If you do not want Twitter to show you interest-based ads in Twitter for Android on your current mobile device, enable "Opt out of Ads Personalization" in your Android phone's settings.

If you prefer to opt out of Twitter's interest-based ads, follow these instructions: go to **optout.aboutads.info** which will then take you outside of Twitter to the Digital Advertising Alliance page where you can not only opt out of ads from Twitter but other ads that might be using your "cookies" to track you. You do need to be logged into Twitter in order to remove the interest-based ads from your account. Additionally, if you are blocking your cookies, you may have to allow access to them prior to beginning the removal process.

Parents! Following your child's school is important for updates but if your account isn't locked down anyone can see which school your child attends. #lockitdown

TWITTER SMART CARD

Mobile Device Version

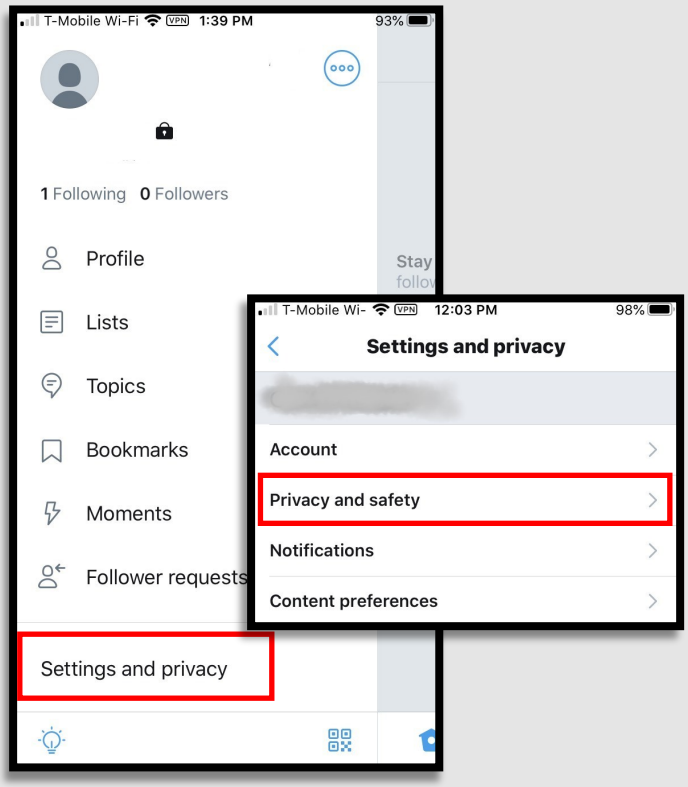


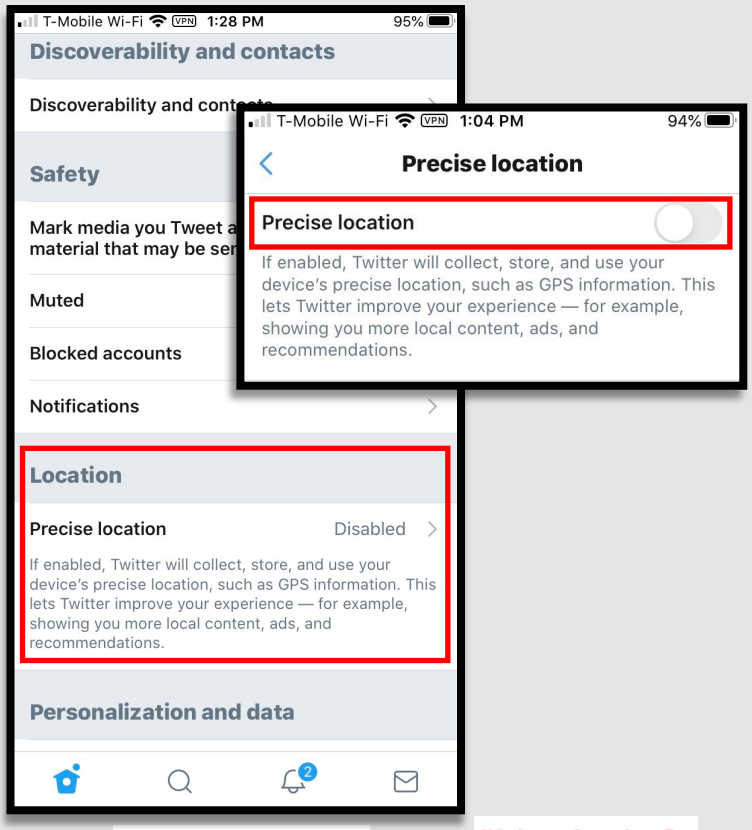
* Images are of iPhone Operating System (iOS), but the steps apply equally to Android Operating System (aOS), as differences between the two are negligible.

If you frequently access Twitter on your mobile device, you will want to ensure all of the above procedures are completed. Additionally, you will want to accomplish 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 Twitter access to your location for advertisements and photo geo-tagging. Getting to the "Settings" section on your smart phone is one of the biggest differences between the computer-based and phone-based accounts and is shown in the screenshots displayed on this page.

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", and "Precise Location" to ensure it is disabled. (see images)

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)





#TheMoreYouKnow #DataSecurity #dataprivacy #identitytheft

Hashtags # are used to index key words and topics on Twitter, think of them as the topic of your "tweet" or "post". Understand that if your account is public and you use a hashtag on a tweet, anyone who does a search on that hashtag may find your tweet. People use hashtags as a way to improve crowdsourcing requests. When you add a hashtag to a tweet, Twitter adds the message to the hashtag group so more users see your "tweet". Even if your Twitter account is private and your tweets are protected, be cautious of what you post online. Accounts can be compromised and settings can mistakenly be disabled.

Always check to make sure your location settings are locked down on Twitter. This means both on your smart device in the "Settings" section, and via the App.

TWITTER SMART CARD

Indicators of Possible Account Compromise:

Do you think your account may have been compromised or hacked? Have you noticed any of the following:

* Unexpected Tweets posted by your account
* Direct Messages sent from your account that you did not initiate
* Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
* A notification from Twitter stating that your account may be compromised
* A notification from Twitter stating that your account information (bio, name, etc.) has changed
* Your password is no longer working or you are being prompted to reset it. *If this occurs it is highly recommended that you sign-in online and change your password immediately.

If you said "Yes" to any of the above , Twitter advises you take the following actions:

- Delete any unwanted Tweets that were posted while your account was compromised
- Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be posted after you've changed your password
- Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess
- Consider using login verification (if you haven't done so already), instead of relying on just a password. Login verification introduces a second check to make sure that you and only you can access your Twitter account
- Be sure to check that your email is secure. It may be worth changing the password to both your Twitter account and the email associated with your Twitter account.

If you need to report **Spam/Fake Accounts/Harassment**: Go to https://help.twitter.com/en/contact-us

If your account was hacked: https://help.twitter.com/en/safety-and-security/twitter-account-hacked

Also, if you find that your account has been hacked, it is best to let Twitter know by filling out the "Hacked Account" form located on the forms site at: https://help.twitter.com/forms

If you cannot log in to your email account, Twitter has provided links to each email accounts "having trouble signing in" page for your convenience. https://help.twitter.com/en/managing-your-account/cant-access-my-accounts-email-address

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

A six character password can be cracked in one second

Password Length	Possible Combinations	Time To Crack (S = Seconds, M = Minutes, H = Hours, Y = Years)
4	45697	<1 s
5	11881376	<1 s
6	308915776	<1 s
7	8031810176	~4 s
8	208827064576	~1.5 M
9	5429503678976	~45 M
10	141167709565337 6	~19 H
11	3670344486987780	~.1 Y
*12	95428956661682200	~1.5 Y
13	2481152873203 74E4	~39.3 Y
14	64509974703297 2E5	~1,022.8 Y
15	1677259342285 73E7	~26,592.8 Y
16	4360874289942 89E8	~691,412.1 Y
17	113382731538515E10	~17,976,714 Y
18	2947951020001390E10	~467,394,568 Y

Important Message from Twitter: Changing an account's password does not automatically log the account out of Twitter for iOS or Twitter for Android applications. In order to log the account out of 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.

If you frequently receive password reset messages that you did not request, you can require that your email address and/or phone number must be entered in order to initiate a password reset. Find instructions and information about resetting your password.