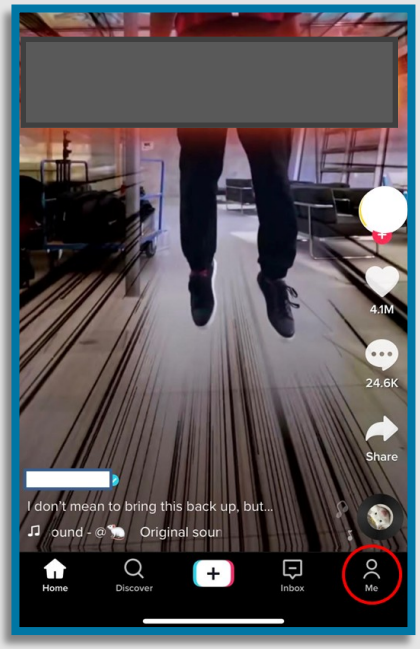
TikTok SMART CARD

Do's and Don'ts

- ***Do*** opt out of personalized data. TikTok is owned by a company based in China, opting out helps prevent your data from being gathered and redistributed without your knowledge.
- ***Do*** ensure family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.
- ***Do*** use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.
- Do ***not*** provide any identifiable information (e.g. name, hobbies, job title, etc.) on your profile or in your videos.
- Do ***not*** link your TikTok account to any third party applications such as Facebook, LinkedIn, Instagram or Twitter.
- Do ***not*** use default settings on TikTok. All default settings are set to allow "Everyone" to be able to view and comment on your videos.
- Do ***not*** use identifiable locations, backgrounds or relatable images, when posting videos. It is important to be aware of your surroundings when posting images.

TikTok can loosely be described as a social network for amateur videos, teenagers and young people are the primary users of the app. It is easy for random people to reach out to users, especially teens, for nefarious reason. Recently TikTok has attempted to fix this issue by updating it's privacy settings, as noted throughout this card. Understand that TikTok is owned by a Chinese-based company, and it is thus important to limit what personal information you include on your account, videos and posts.

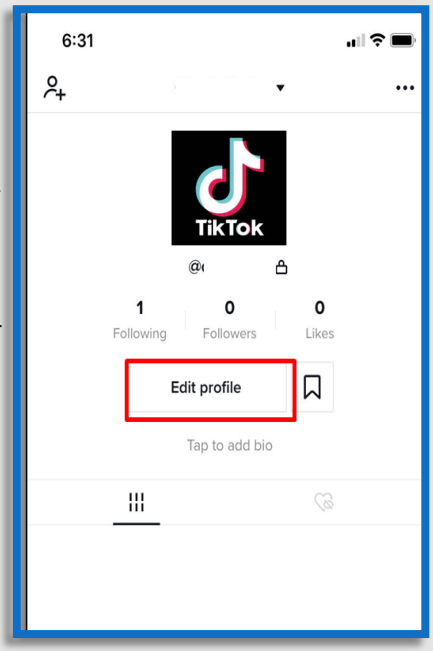
** This information describes how to make your TikTok account secure on Android and iPhone mobile devices. Most images provided are of Android screens. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal - when they are significant, such differences are noted specifically.



Edit Profile

When opening a new application, the first thing you want to do is set up your privacy settings in order to protect your personally identifiable information (PII). Default settings in Tik Tok are set to allow everyone to view, comment and access the information you post.

To begin locking down your account, look to the lower right hand corner and select "Me" to go to your profile settings (highlighted to the left in red). Click on the "Edit Profile" button. We recommend you do not use personal images or photos of yourself or your family. We also recommend you leave your "Bio" information blank or put as little personal information there as possible.

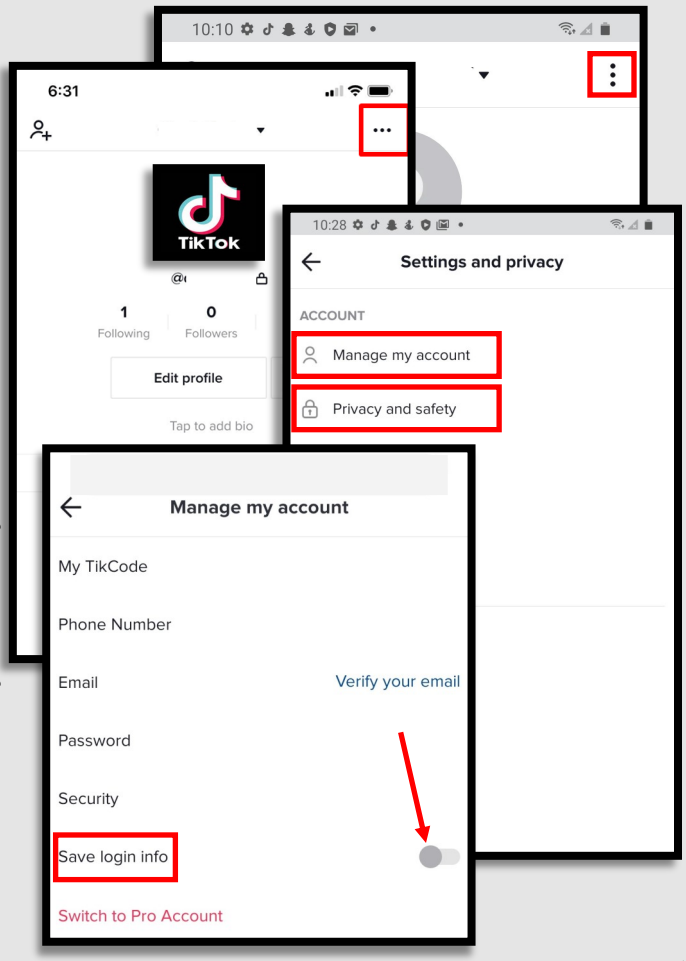


Shut Off Direct Messaging so that strangers cannot attempt to message you (or your children). Select the "Settings" icon, select "Privacy and safety", select "Who can send me messages", select either "Friends" or "Off".

We recommend you do ***not*** link your account to any other social media platform (e.g. Twitter, Instagram, Facebook), as TikTok will pull in your personally identifiable information and pictures from the other platforms. We also recommend you avoid using any Personally Identifiable Information (PII) anywhere on your profile. You are not required to put any personal or biographical information into your profile, and it is recommended you leave this section blank. PII is often used as a means to gain access to certain accounts (e.g. banks, credit cards, schools). Providing even just your birthday could help an identity thief steal your identity.

TikTok is a video-sharing social networking service owned by ByteDance, a Beijing-based company.

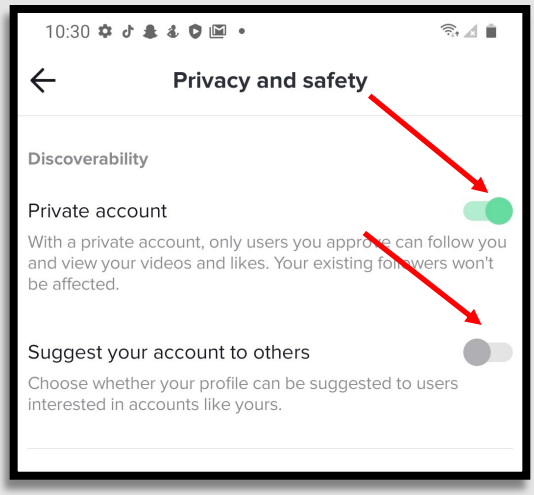
TikTok SMART CARD



Account Privacy & Login Information

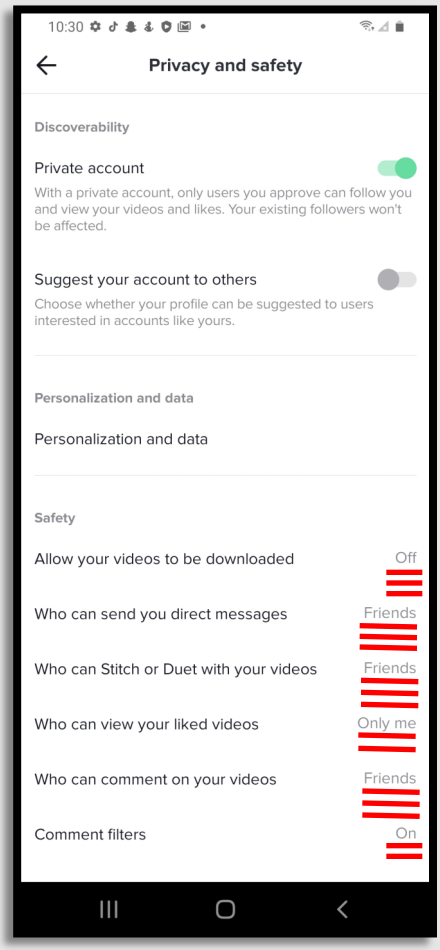
First, you will need to lock down your login information and set your account privacy. In order to access the "Settings and Privacy" tab go back to your "Profile" page and select the "Menu" button, (three horizontal lines on iPhone, 3 vertical lines on Android) in the upper right hand corner of your "Profile" screen (highlighted to the left). Under "Account", select "Manage my account". We recommend you set the "Save login info" toggle to "Off" in order to ensure that, should you lose your mobile device, no one has access to your TikTok account.

Next, let's look at how your posts appear to the cyber world. By default, all accounts are set to "Public", which means anyone can see what you post on Tik Tok. We recommend you set your account to "Private account", which will ensure that all videos can only be seen by the creator and no one else on the platform. With a "Private account" you can approve or deny users and limit incoming messages to "Friends" only. Note that even with a "Private account", your "Photo", Username" and "Bio" are still visible to all users of the platform. We recommend you set "Suggest your account to others" to "Off", which will allow you more agency in choosing and accepting your followers more proactively.



Go to "Privacy and safety", under "Settings and Privacy", then set "Private account" toggle to "On", and "Suggest your account to others" toggle to "Off" (see left).

Next, under "Safety", we recommend setting the toggles as they are seen to the right. It is most important that none of the options are set to "Everyone", as this allows all users to see your content.



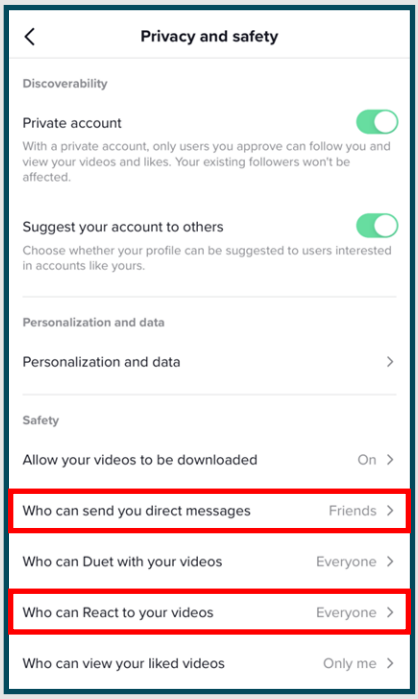
Parents: Keep in mind that children may be tempted to take risks to get more of a following or get "likes" on a video, so it's important to talk with them about what they share and with whom. Also, users can "like" or "react" to a video, follow an account, or send messages to each other. This means that there is a risk that strangers will be able to directly contact children on the app.

Talk with your children about what kinds of videos are okay to share, and with whom. Remember they are driven by "likes" and "reactions". #TikTokFamous

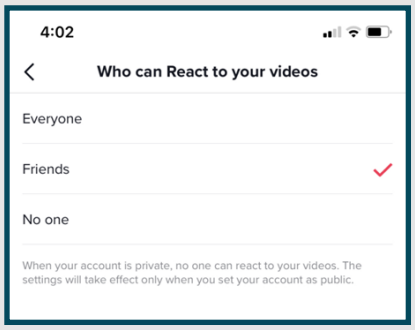
TikTok SMART CARD

Account Privacy, ctd.

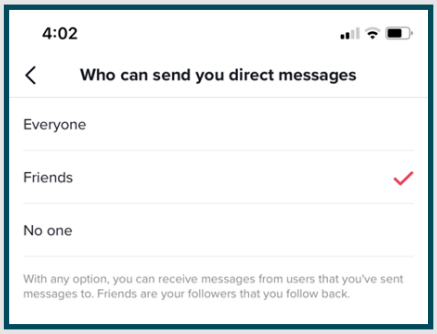
Following your child's TikTok account and paying close attention to your personal account is important not only for updates to policy and content, but to ensure account parameters. Help ensure your family is not vulnerable to anyone who can see what they are posting, liking and following.

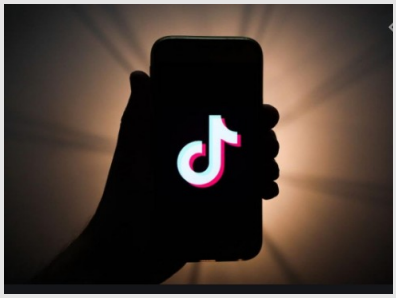


We recommend that you control who will be able to react to the videos you or you child post to TikTok. Again, under "Settings and privacy" and "Privacy and safety", you are able to set some of the security settings to filter and protect your account, but more importantly your data, privacy and information. Highlighted to the left you see how to limit who can react to videos you post to TikTok. It is highly recommended you limit those who can react to your videos, to only "Friends."

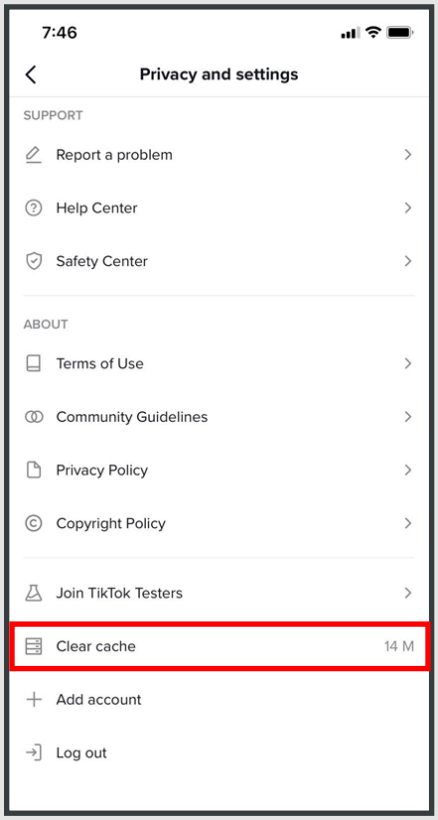


We also recommend you lock down "Who can send you direct messages", found in the same section. It is important you limit the people who can reach out and send a "Direct Message" to you (and your children). This will not only protect your safety, but also will protect you and your children from being "Messaged" by potential scammers or online predators.





Duets can be a fun way to create videos with another user, but you must be in control - Tik Tok gives you the option to **decide who can make duets with you** (everyone, no one, or just friends). We recommend you choose "Friends".



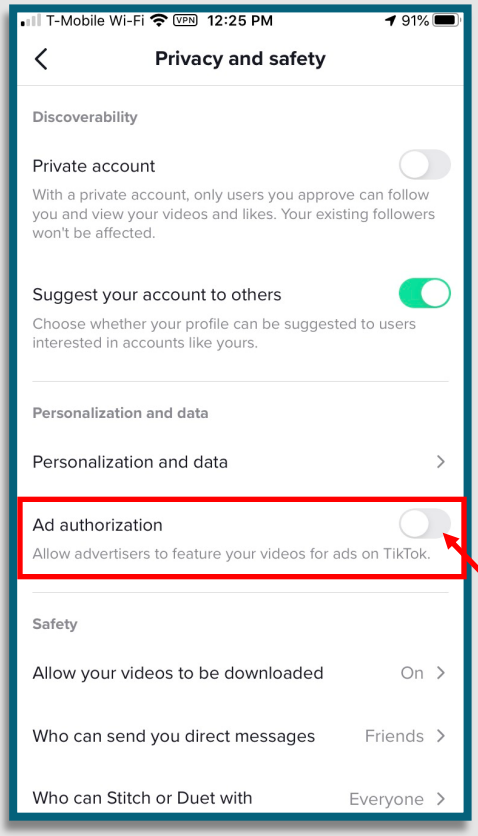
It is a good idea to clear your browser cache (highlighted to the right) because it will prevent you from using old forms, protect your personal information and help applications run better on your computer or phone. We recommend you clear your cache when you are done with every TikTok session in order to protect your information and remove potentially harmful data from your electronic device. In order to clear your TikTok cache, go to your "Profile" page, select the "Menu" icon in the top right of your profile screen. Select "Settings and Privacy, scroll to the bottom of the "Settings and Privacy" page and click on "Clear Cache."

With a "Private account", only users you've approved as followers can see your content, but you can also choose to **make a specific video private**. Private videos are visible only to you, and you can select this setting when you originally upload the video - or by later making an uploaded video private. If you've already uploaded the video, tap the "Share" icon, then "Who Can View This Video" > "Private". If you're about to post, tap "Who Can View This Video" > "Private".

If your account is locked down, you're doing GREAT! If you allow your videos to be downloaded, you run the risk of compromising personal information.

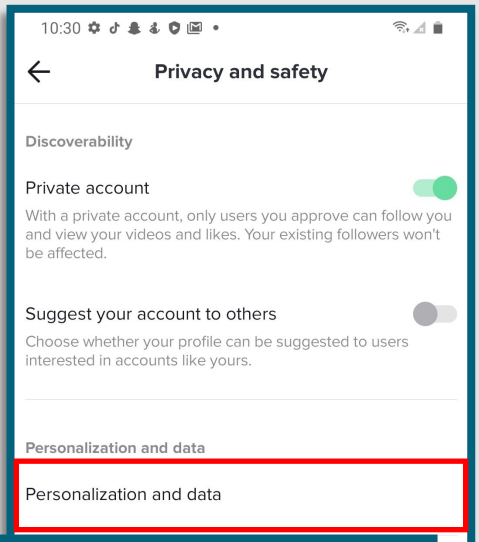
TikTok SMART CARD

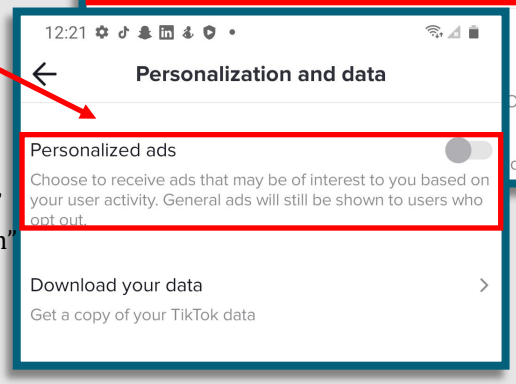
Personalized Advertising



Also in the "Settings and Privacy" section, you have the ability to control advertising data on your account. It is important to lock this kind of information down because, in order to personalize advertising for you, the app must access a lot of personal information and data on your device. It is best to disable this feature.

On your **Android**, under "Settings and privacy", then "Privacy and safety", in the second section select "Personalization and data", then ensure the "Personalized ads" toggle is set to "Off".

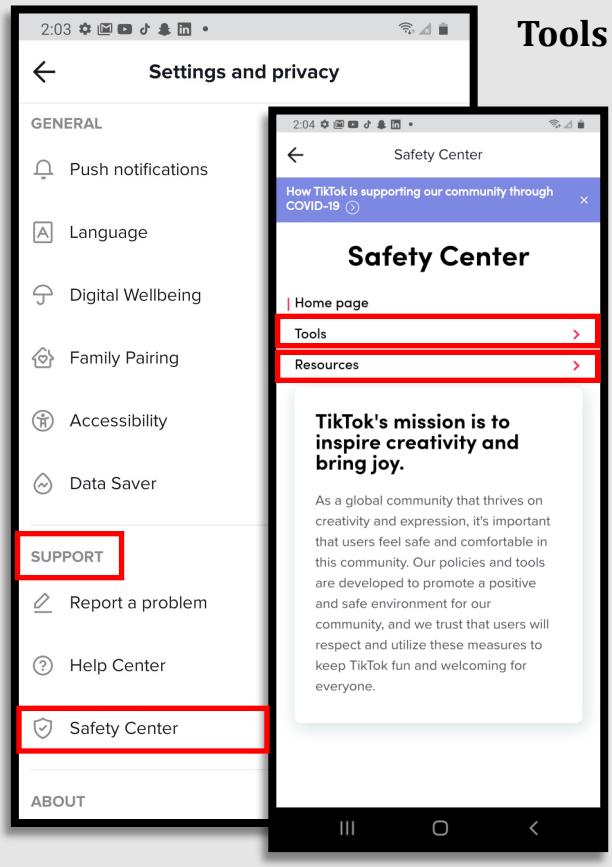




On your **iPhone**, select "Settings and Privacy", then "Privacy and safety", under the "Personalization and data" section. Ensure the "Ad authorization" option is toggled to "Off".

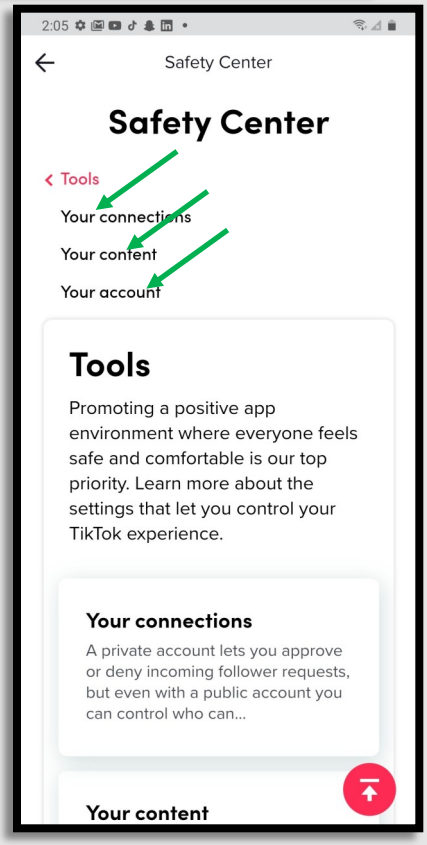
Safety Center:

Tools and Resources



Finally, let's visit Tik Tok's "Safety Center", which is a useful resource hub that will help you learn how to use Tik Tok in the most safe and enjoyable way. In this section, you will find "Tools" and "Resources" that will help you further navigate your content, security, and privacy options. First, find the "Safety Center" by going to "Settings and privacy", scroll to the middle of the menu and select "Safety Center" in the "Support" section.

Next, select "Tools", and you will be given options to explore how to maximize your control over your "Connections", your "Content", and your "Account".



Parents have expressed concern about the inappropriate language and content of some videos posted on TikTok, which may make it less suitable for younger children.

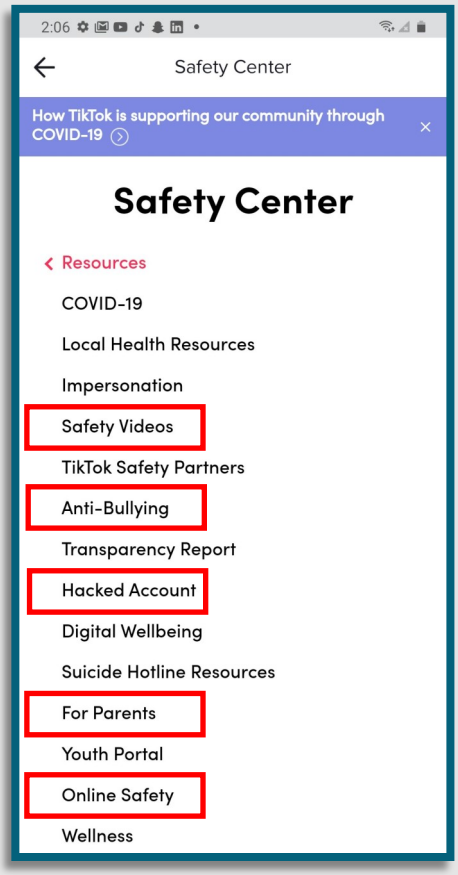
TikTok SMART CARD

Safety Center: Tools and Resources, ctd.

Back under "Safety Center", select "Resources" and see a list of various resources you will find useful. We recommend you check out "Safety Videos" (see right), and the "You're in Control" video series, which are short educational Tik Tok videos on topics, many of which are presented in this SmartCard, such as "Choosing who can duet with you", Reporting inappropriate behavior", etc.

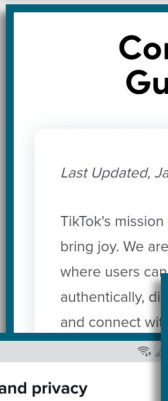
Also, check out the "Anti-Bullying" information, which explains what steps you can take to make sure you (or your child) are not receiving unwanted community interactions, as well as what you can do if you find yourself in a bullying situation.

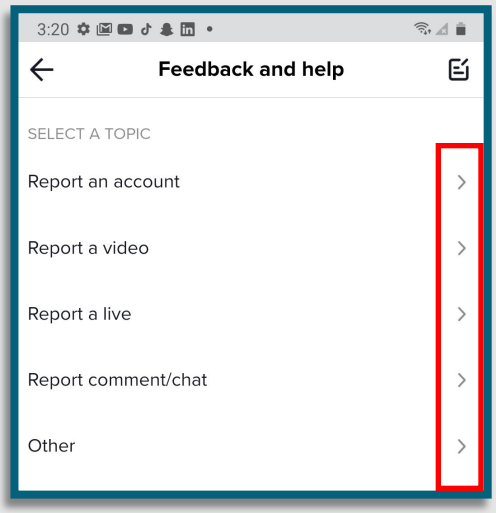
Next, if you are a parent, do check out the "For Parents" link, which offers more explanation about what Tik Tok is meant to be and how to keep your child safe on Tik Tok. For instance, this section explains that Tik Tok is for children 13 years and older, but that in the U.S. children under 13 may register for a "Child Account", which restricts posting and interactions on the platform. "Family pairing" and "Account Privacy" options are further explained as tools to help keep teens safe on Tik Tok. We recommend you visit the link and employ all recommendations suggested to keep you and your family safe.

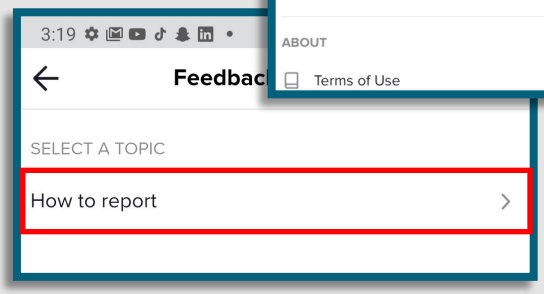


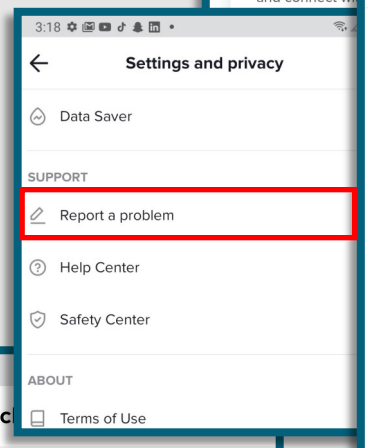
Report a Problem

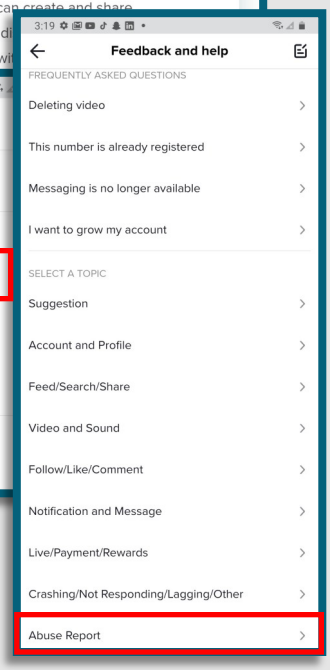
Tik Tok has "Community Guidelines" that outline the types of behavior it considers counter to its values. Content that violates these guidelines can be reported, removed, and reported to legal authorities. You can access the "Community Guidelines" via the "Safety Center" on Tik Tok. But if you see content you think should be reported, you can do the following: under "Settings and privacy", select "Report a problem", then scroll to the bottom of the "Feedback and help" page that appears, and select "Abuse Report". Select "How to report" and follow the rest of the prompts.











By changing all the safety settings for TikTok to "Friends" you are protecting your account from just anyone finding, commenting or contacting you or your child.

TikTok SMART CARD

Indicators of Possible Account Compromise:

Your TikTok account may have been hacked, if you experience following suspicious behavior:

- Change of your password, security email and associated phone number.
- Change of your username or nickname.
- Deleting / Posting videos without your permission.
- Sending messages you did not write.

If you suspect your account has been compromised, please follow the steps below to keep your account secure:

Change Password: In TikTok, a hacker will be automatically kicked out of your account after changing the password.

Check account information to determine if it is accurate: Select "Manage My Account" option under the TikTok settings, check if the associated account information is accurate. If you cannot change password by yourself, please contact TikTok via their In-app Feedback (App settings – Report a Problem). You may follow the steps shown below to change the password and verify account information.

- Tap on "…" for 'Privacy & Settings'
- Go to 'Manage My Account'
- Select password to change and other account information to verify

If you need to report **Spam/Fake Accounts/Harassment**: Go to https://support.tiktok.com/en

If your account was hacked: https://www.tiktok.com/safety/resources/hacked-account?lang=en&appLaunch=web and reach out to TikTok and notify them of your hacked account at https://www.tiktok.com/about/contact?lang=en

Also, if you find any bullying or inappropriate behavior TikTok has information at site https://www.tiktok.com/safety/resources/anti-bully?lang=en&appLaunch=web

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

Important Message from TikTok: If you have a public profile, anyone signed into TikTok can view your public videos. However, only approved followers can send you a message. Whether you choose to have a public or a private account, you can always: block another from contacting you at any time; save a video privately so content will not be viewable by any other user; filter comments; "manage" your duets.

Tips to keep your account safe:

1. Never trust 3rd-party websites that promise to give away free likes, fans, crowns, coins, or other incentives as they may be able to take your login info.

2. Select a secure password that contains at least one number and one special character.

Make sure your options for "Who can download my video" are set to "Nobody". Otherwise other users can download and share your videos. #lockitdown