

Social Media Security & Privacy Handbook

(Name of Organization)

(Date of Last Update)

[A. Privacy Requirements:](#)

[B. Social Media Conduct:](#)

[C. Step-by-Step Guides](#)

[1. Meta Platforms](#)

[1.1 Meta Business](#)

[1.2 Facebook](#)

[1.3 Instagram](#)

[1.4 Threads](#)

[1.5 WhatsApp](#)

[2. TikTok](#)

[3. LinkedIn](#)

[4. Bluesky](#)

[5. X formerly Twitter](#)

[For more information on securing your social media profiles check out these sources below:](#)

Sections A-B: Organizational Policy

Sections 0-5: Step-by-step Guides any Individual can Follow

A. Privacy Requirements:

Employees must review and adjust the privacy settings on their social media and public profiles to limit the exposure of personal information. Professional profiles (e.g., LinkedIn) should be kept up-to-date with a focus on career-related content, if employees consent to do so and it is safe for them to disclose that information online. These requirements exist to protect both the organization and working individuals, ensuring that certain privacy standards are in place to reduce risk.

- [Insert organization-specific privacy policy here. Decide the degree of privacy required, with consent from each employee.]

B. Social Media Conduct:

Employees are advised to exercise caution when sharing personal or professional information on social media. Posts should not disclose confidential organizational information or personal details that could be exploited by malicious actors.

- **Consent Form:** [Insert link to organizational social media consent form here.]
 - Sample Template available on ODLAN's website.
- **Avoid Linking Accounts:** Employees should avoid linking personal accounts (e.g., personal email, personal social media) with work-related accounts to minimize the risk of cross-platform breaches. Linking personal and organizational accounts creates a bridge between private life and the workplace. When these accounts are linked, a compromise on one side can impact the other. A breach on a personal account can expose organizational systems, and a breach on an organizational account can expose personal information. Keeping them separate protects both the organization and the individual.

C. Step-by-Step Guides

Platforms Covered:

Below are privacy setting recommendations for Meta Platforms (Meta Business, Facebook, Instagram, Threads, and WhatsApp), TikTok, LinkedIn, Bluesky, and X (formerly Twitter). Screenshots of instructions were taken as of May 2026 via mobile app.

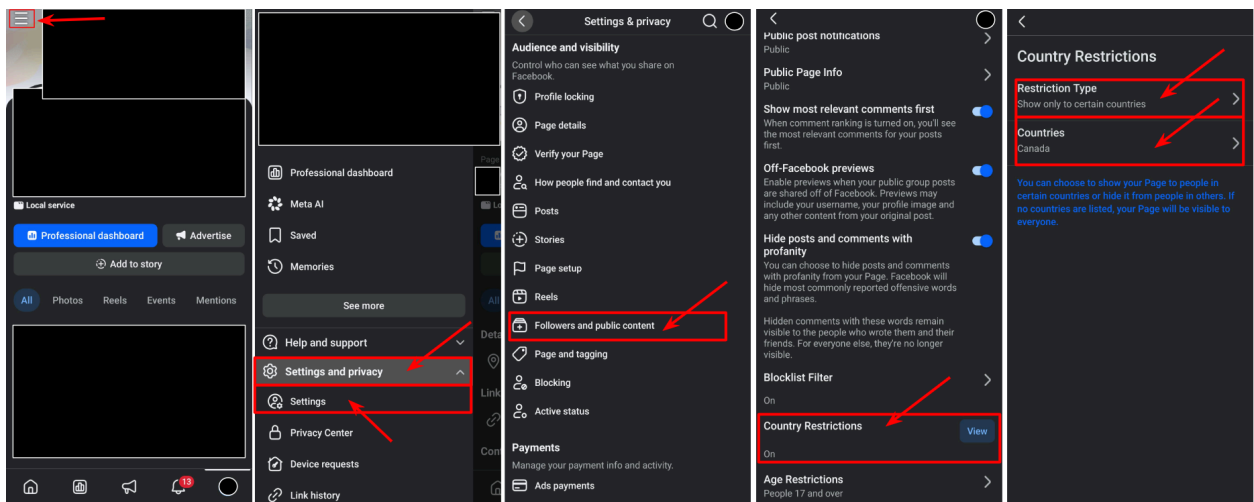
1. Meta Platforms

1.1 Meta Business

⚠ Note: These settings apply only to Meta Business accounts on Facebook. They do not apply to personal Facebook accounts. For personal Facebook account settings, see section 1.2.

Location Restriction:

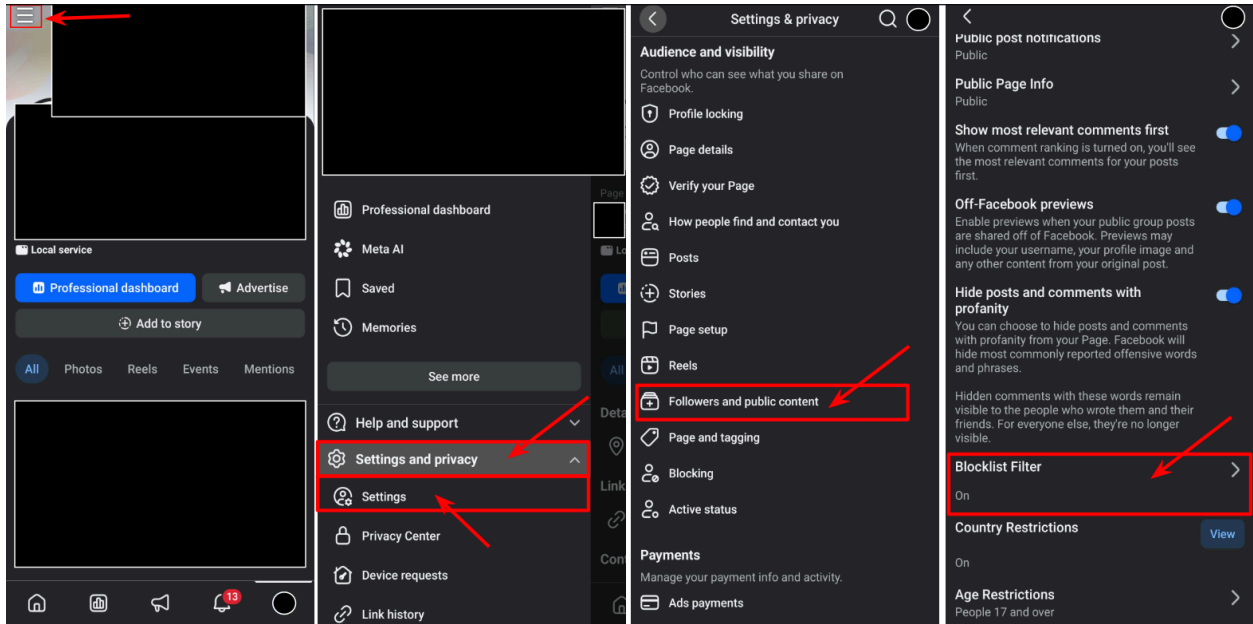
1. From Your Business Account page, tap the **Menu** Icon (≡) in the top left.
2. Select **Settings and privacy** (⚙) then **Settings**
3. Scroll down to the *Audience and visibility* section and select **Followers and public content** > **Country Restrictions**
4. Toggle **ON** and select countries to restrict or allow view access



Word Filters:

1. From Your Business Account page, tap the **Menu** Icon (≡) in the top left.
2. Select **Settings and privacy** (⚙) then **Settings**
3. Scroll down to the *Audience and visibility* section and select **Followers and public content** > **Blocklist Filters**
4. Add specific words, phrases, or emojis you don't want to see
 - **⚠ Content Warning** for the sample list below: The example list of “bad words” contains profanity, slurs, and sexually explicit terms that may be offensive or disturbing. Please review the list only if you're comfortable doing so.
 - Check here for a sample list of bad words to filter out.

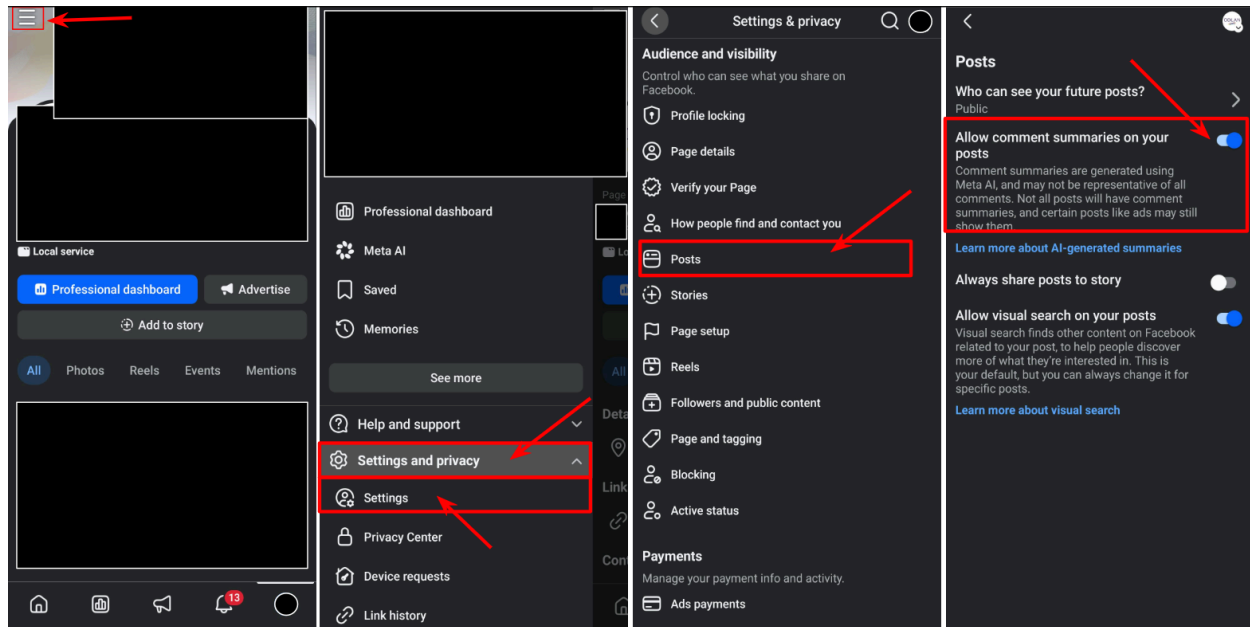
- <https://docs.google.com/document/d/10irgql6yCVPEqYHRqRe72SGMeBcENAH5CeebHylpL6A/edit?tab=t.0>



Turn off AI Summary on Posts:

Facebook's Meta AI automatically summarizes your posts/comments. AI is not always accurate and you could be held accountable for the information it displays on your page. Opt out of AI so your content is not being processed through an AI tool, being shared with unknown vendors, or training AI to directly harm your community.

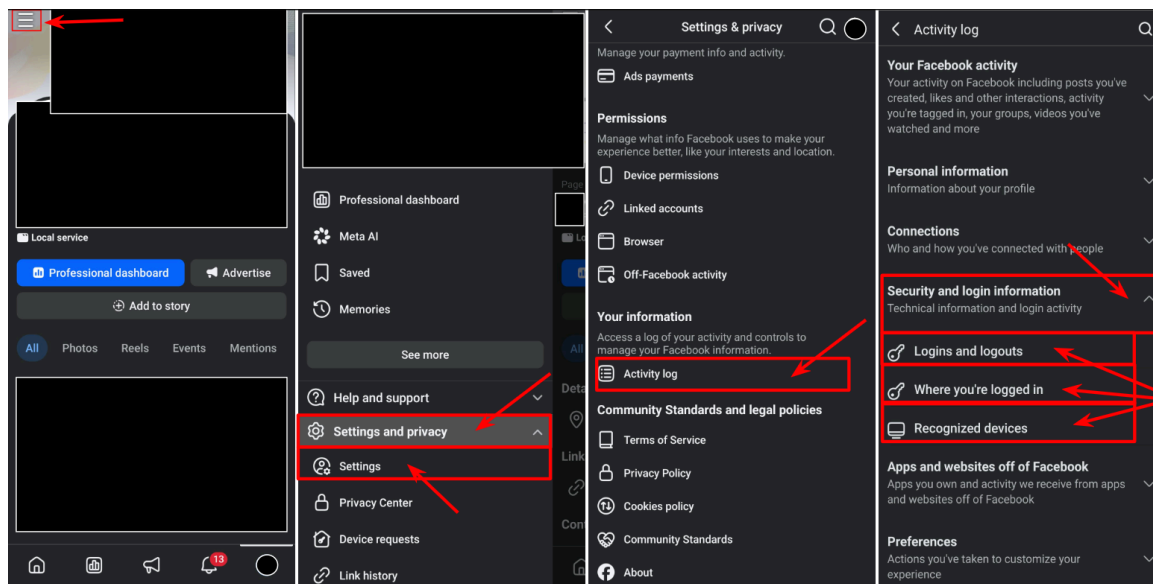
1. From Your Business Account page, tap the **Menu** Icon (≡) in the top left.
2. Select **Settings and privacy** (⚙️) then **Settings**
3. Scroll down to the *Audience and visibility* section and select **Posts**
4. Toggle **OFF** *Allow comment summaries on your posts*



Review Login Activity & Sign Out of Unrecognized Devices:

Regularly check where your account is logged in to ensure no unauthorized access.

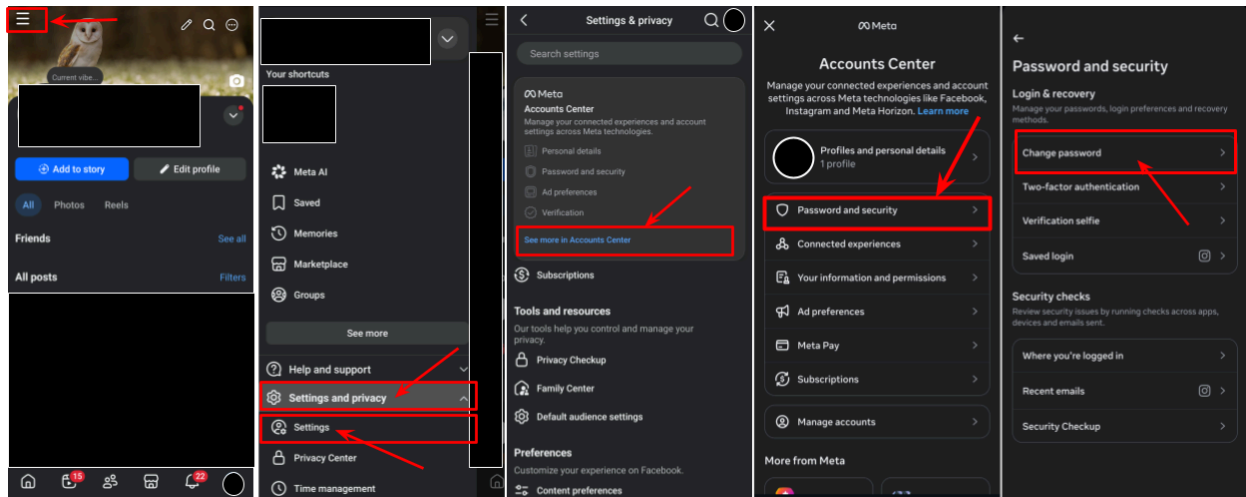
1. From Your Business Account page, tap the **Menu** Icon (≡) in the top left.
2. Select **Settings and privacy** (⚙️) then **Settings**
3. Scroll down under *Your Information* and select **Activity Log > Security and login information**
4. Review **Logins and logouts**, **Where you're logged in & Recognized devices**
5. Remove access from any devices or accounts that are unfamiliar



1.2 Facebook

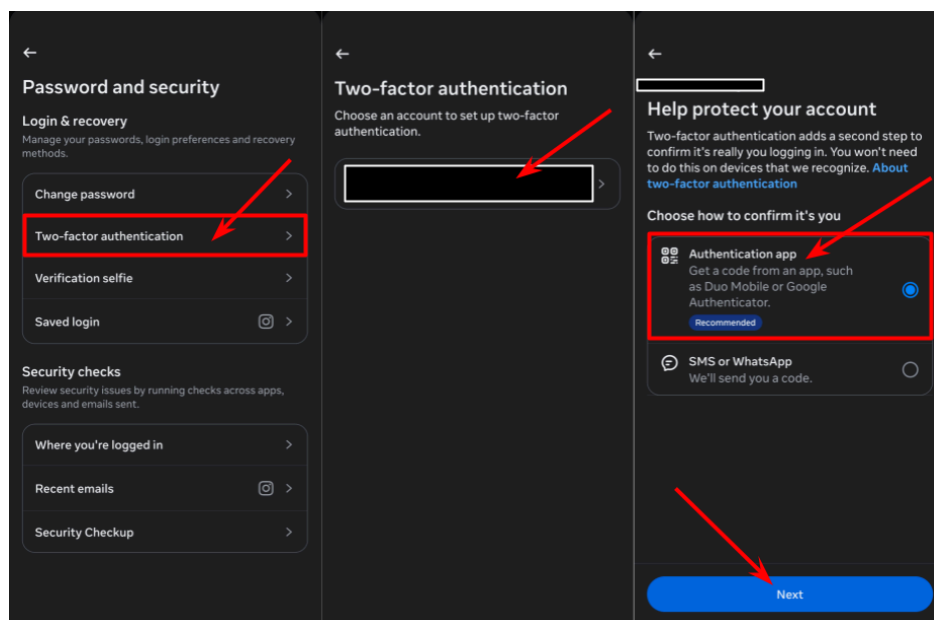
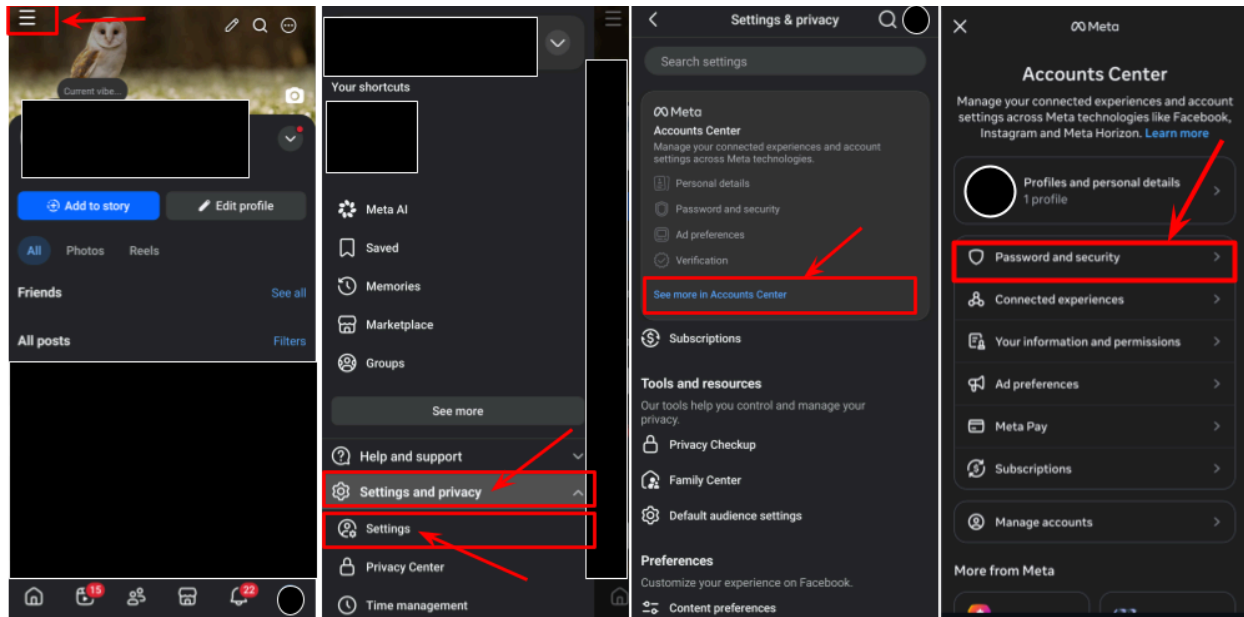
Updating Your Password to a Strong and Unique One:

1. From Your Profile page, tap the **Menu Icon** (≡) in the top left.
2. Select **Settings and privacy** (⚙️) then **Settings**
3. Tap **See more in Account Center** > **Password and security** > **Change password**
4. Then Select the account you want to update and Enter a new, strong password



Setting Up Two-Factor Authentication (2FA):

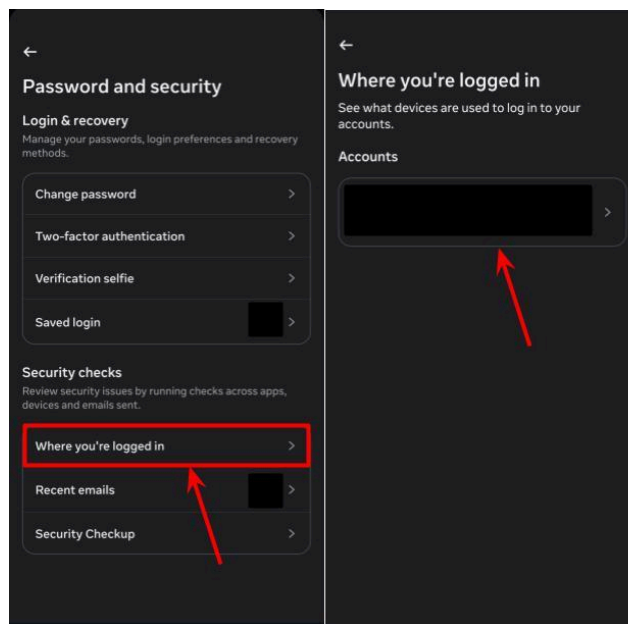
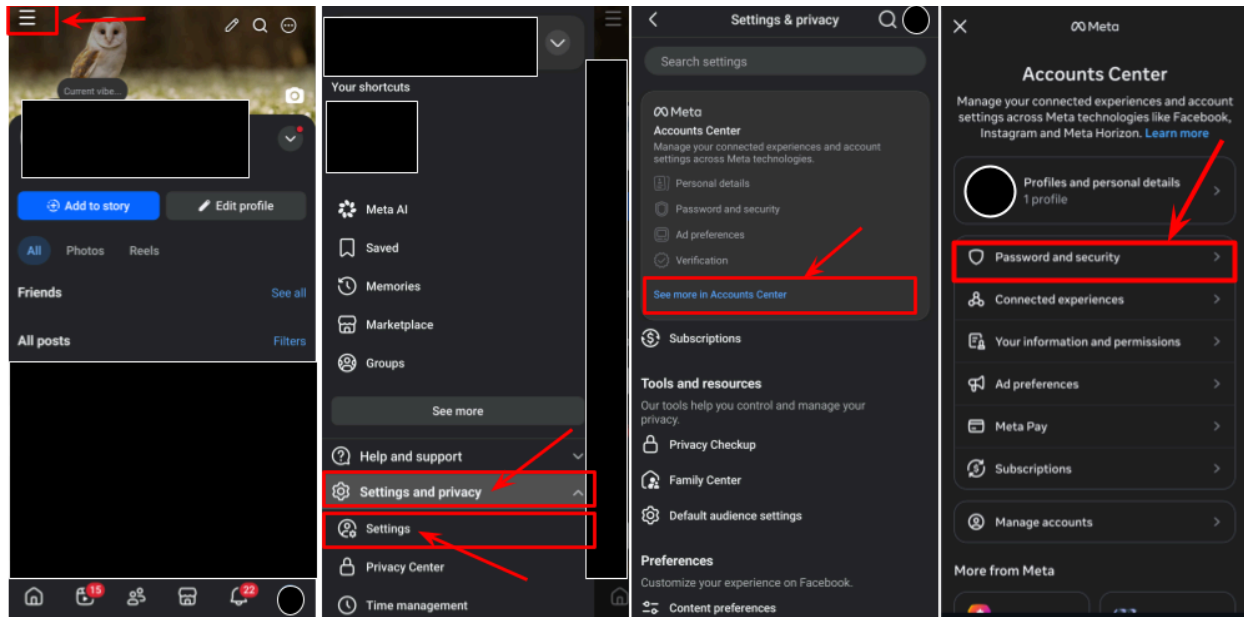
1. From Your Profile page, tap the **Menu Icon** (≡) in the top left.
2. Select **Settings and privacy** (⚙️) then **Settings**
3. Tap **See more in Account Center** > **Password & Security** > **Two-factor authentication**.
4. Choose the account you want to secure.
5. Select **Authentication App** as the security method and follow the on-screen instructions.



Review Login Activity & Sign Out of Unrecognized Devices:

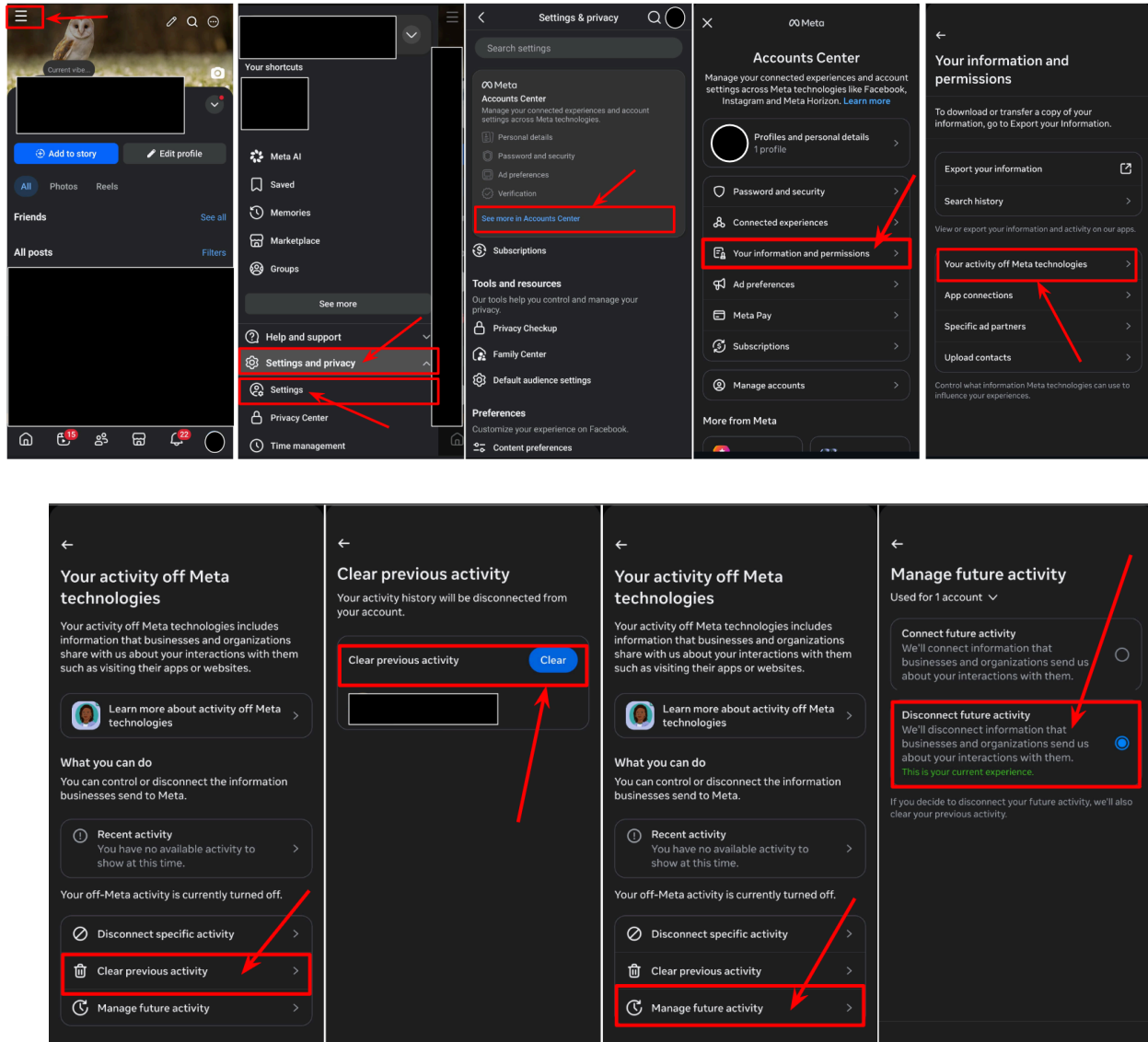
Regularly check where your account is logged in to ensure no unauthorized access.

6. From Your Profile page, tap the **Menu Icon** (≡) in the top left.
7. Select **Settings and privacy** (⚙️) then **Settings**
8. Tap **See more in Account Center** > **Password & Security** > **Where You're Logged In**.
9. Select the account to check and review the list of active sessions.
10. If you see any unfamiliar locations or devices, remove its access immediately



Manage Activity Outside of Meta:

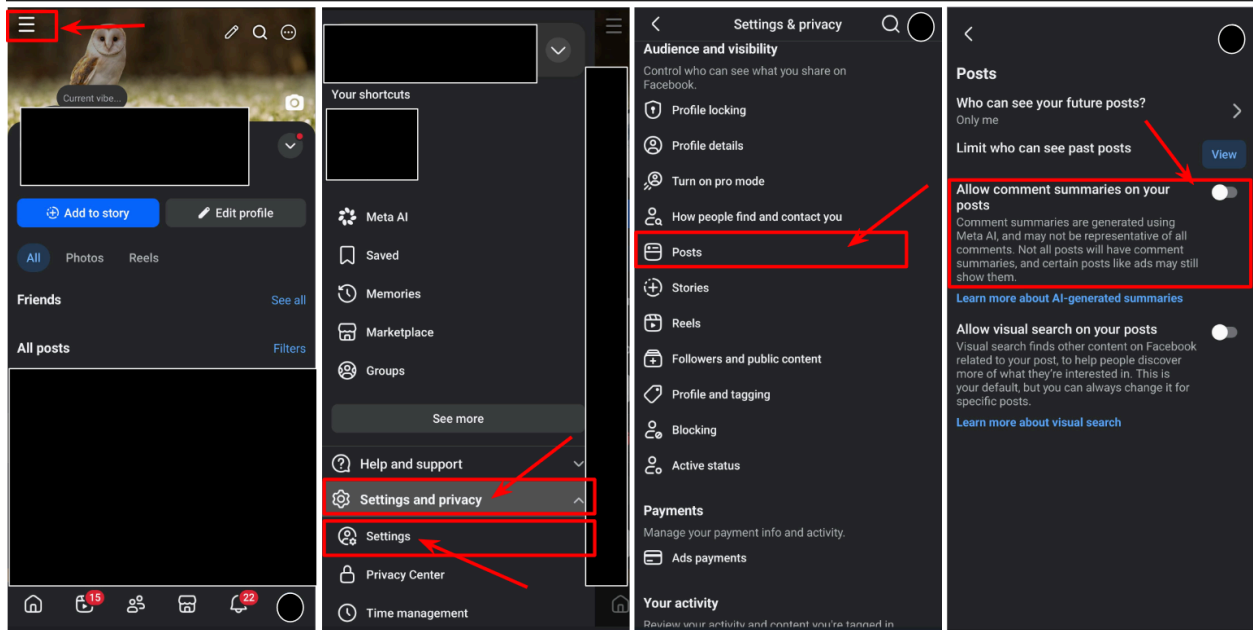
1. From Your Profile page, tap the **Menu Icon** (≡) in the top left.
2. Select **Settings and privacy** (⚙️) then **Settings**
3. Tap **See more in Account Center** > **Your Information & Permissions** > **Your Activity Off Meta Technologies**.
4. **Clear Previous Activity:** Remove data linked to external sites and apps.
5. **Manage Future Activity:** Select **Disconnect Future Activity** to prevent tracking from external sources.



Turn off AI Summary on Posts:

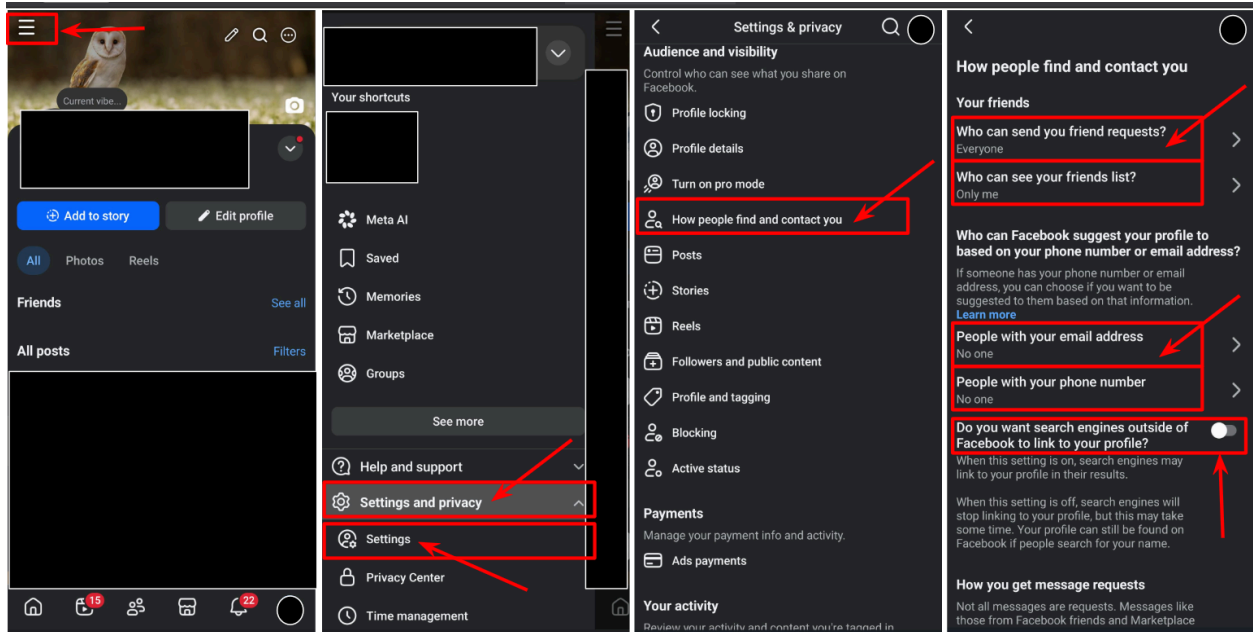
Facebook's Meta AI automatically summarizes your posts/comments. AI is not always accurate and you could be held accountable for the information it displays on your page. Opt out of AI so your content is not being processed through an AI tool, being shared with unknown vendors, or training AI to directly harm your community.

1. From Your Account page, tap the **Menu** Icon (≡) in the top left.
2. Select **Settings and privacy** (⚙️) then **Settings**
3. Scroll down to the *Audience and visibility* section and select **Posts**
4. Toggle **OFF** *Allow comment summaries on your posts*



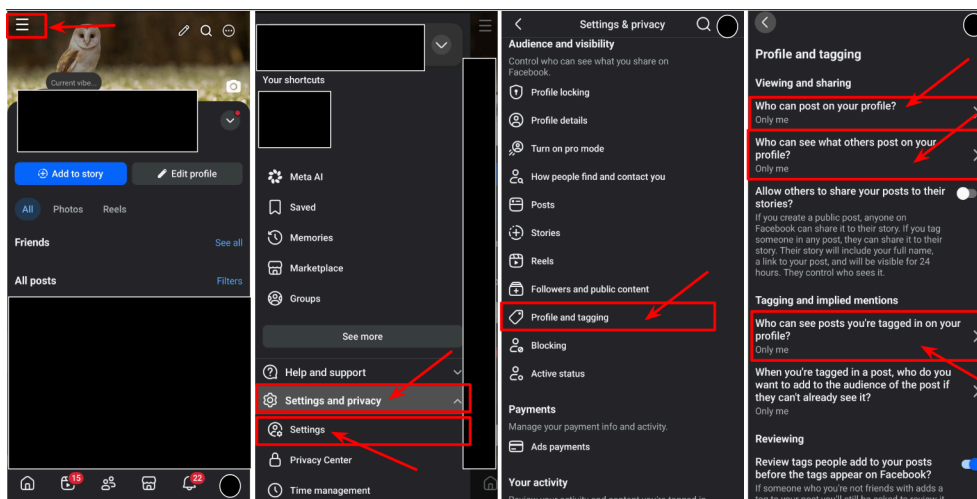
Managing How People Find and Contact You:

1. From Your Profile page, tap the **Menu Icon** (≡) in the top left.
2. Select **Settings and privacy** (⚙️) then **Settings**
3. Scroll down under *Audience and Visibility* and choose **How People Find and Contact You**
4. Adjust settings for **Who can find you using your phone number or email**, **Whether search engines outside Facebook can link to your profile**, & **Who can see your friends list or send friend requests**
 - Customize these options based on your privacy preferences.



Manage Profile Visibility and Tags:

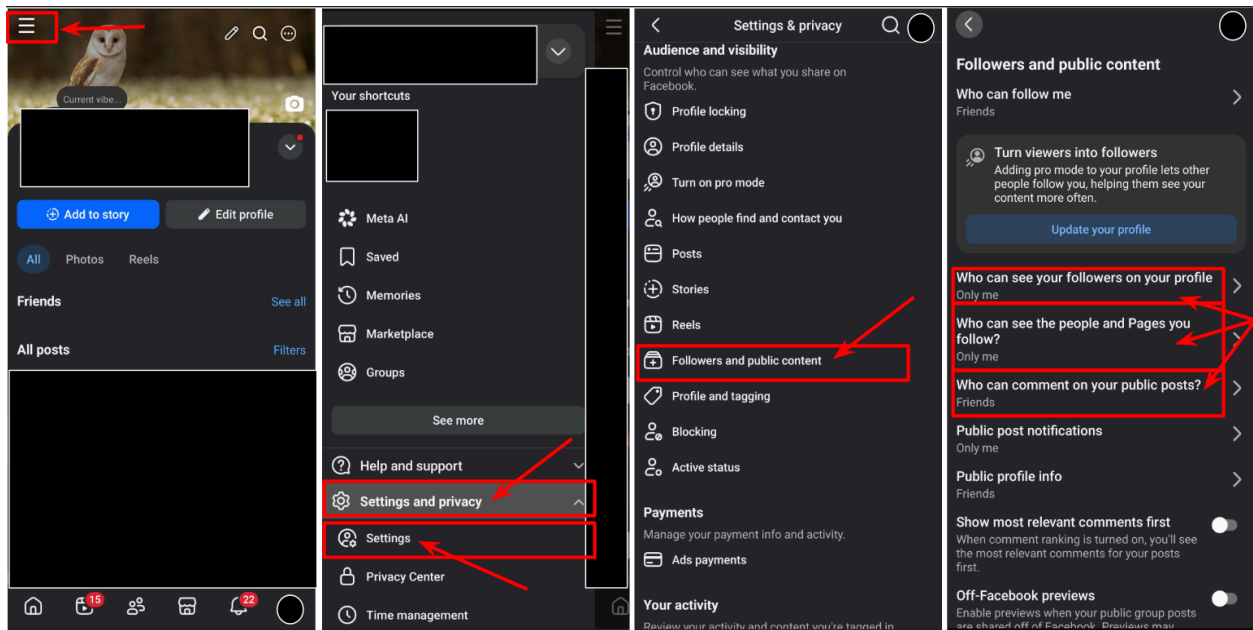
1. From Your Profile page, tap the **Menu Icon** (≡) in the top left.
2. Select **Settings and privacy** (⚙️) then **Settings**
3. Scroll down under *Audience and Visibility* and choose **Profile and tagging**
4. Adjust settings for **Who can post on your profile**, **Who can see what others post on your profile** & **Who can see posts you're tagged in**
 - o Customize these options based on your privacy preferences.



Manage Public Content Your Followers See:

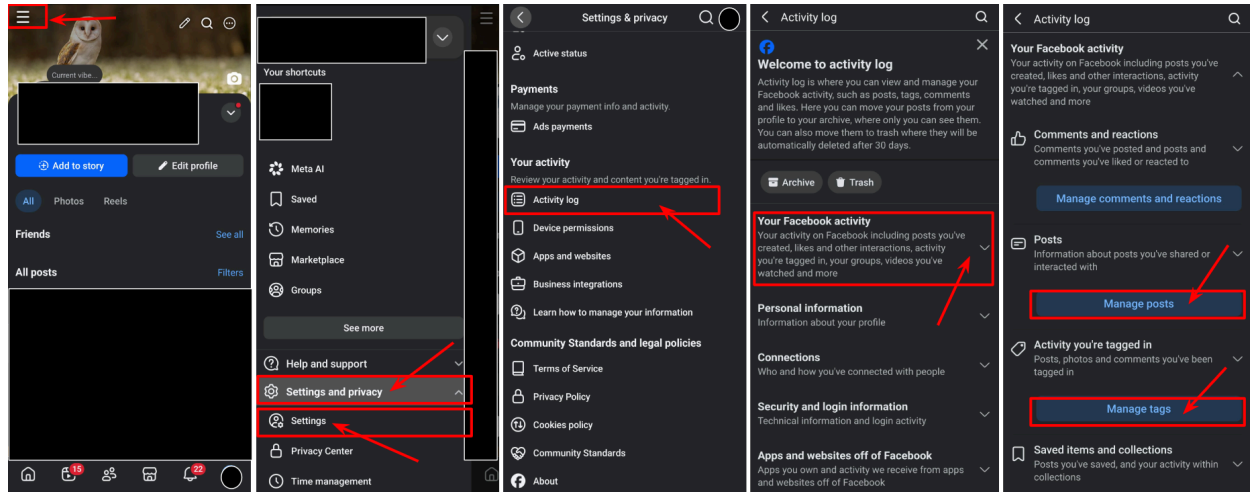
1. From Your Profile page, tap the **Menu Icon** (≡) in the top left.

2. Select **Settings and privacy** (⚙️) then **Settings**
3. Scroll down under *Audience and Visibility* and choose **Followers and public content**
4. Adjust settings for **Who can see your followers on your profile**, **Who can see people, Pages and lists you follow**, & **Who can comment on your public posts**
 - Customize these options based on your privacy preferences.



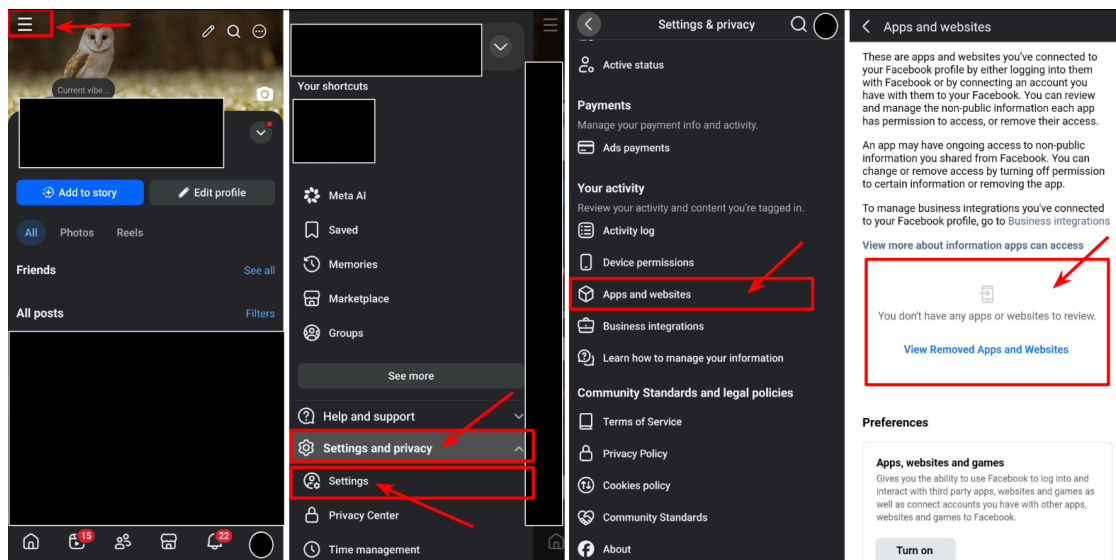
Manage Tags in Posts:

1. From Your Profile page, tap the **Menu Icon** (≡) in the top left.
2. Select **Settings and privacy** (⚙️) then **Settings**
3. Scroll down under *Your Activity* and choose **Activity Log > Your Facebook Activity**
4. Adjust settings in **Manage Posts & Manage Tags**
 - Customize these options based on your privacy preferences.



Manage Apps and Websites Access to Your Facebook Account:

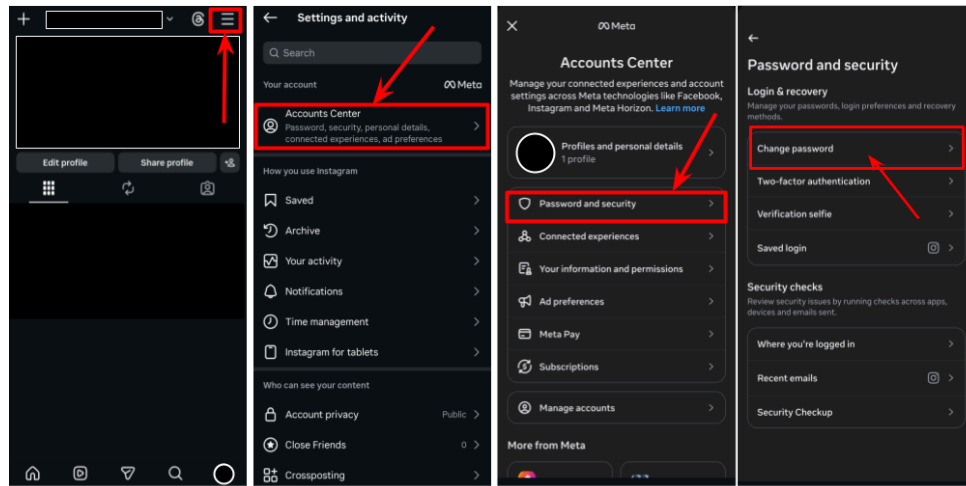
1. From Your Profile page, tap the **Menu Icon** (≡) in the top left.
2. Select **Settings and privacy** (⚙️) then **Settings**
3. Scroll down under *Your Activity* and choose **Apps and websites**
4. Review apps or websites with access and change or remove access based on preferences



1.3 Instagram

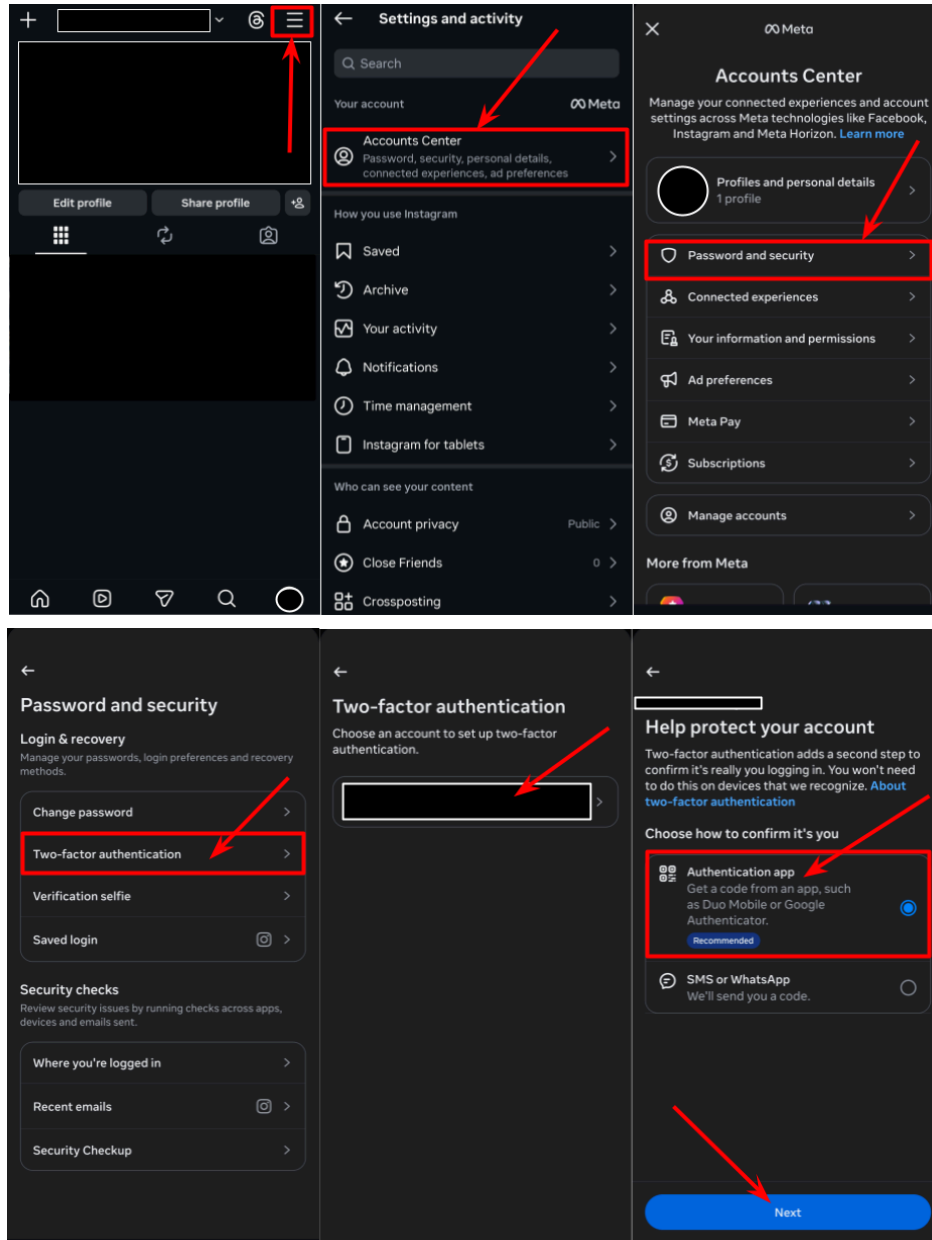
Updating Your Password to a Strong and Unique One:

1. From your **Profile Page**, tap the **Menu Icon** (≡) in the top right
2. Select **Account Center** > **Password & Security** > **Change Password**
3. Select the account you want to update and Enter a new, strong password



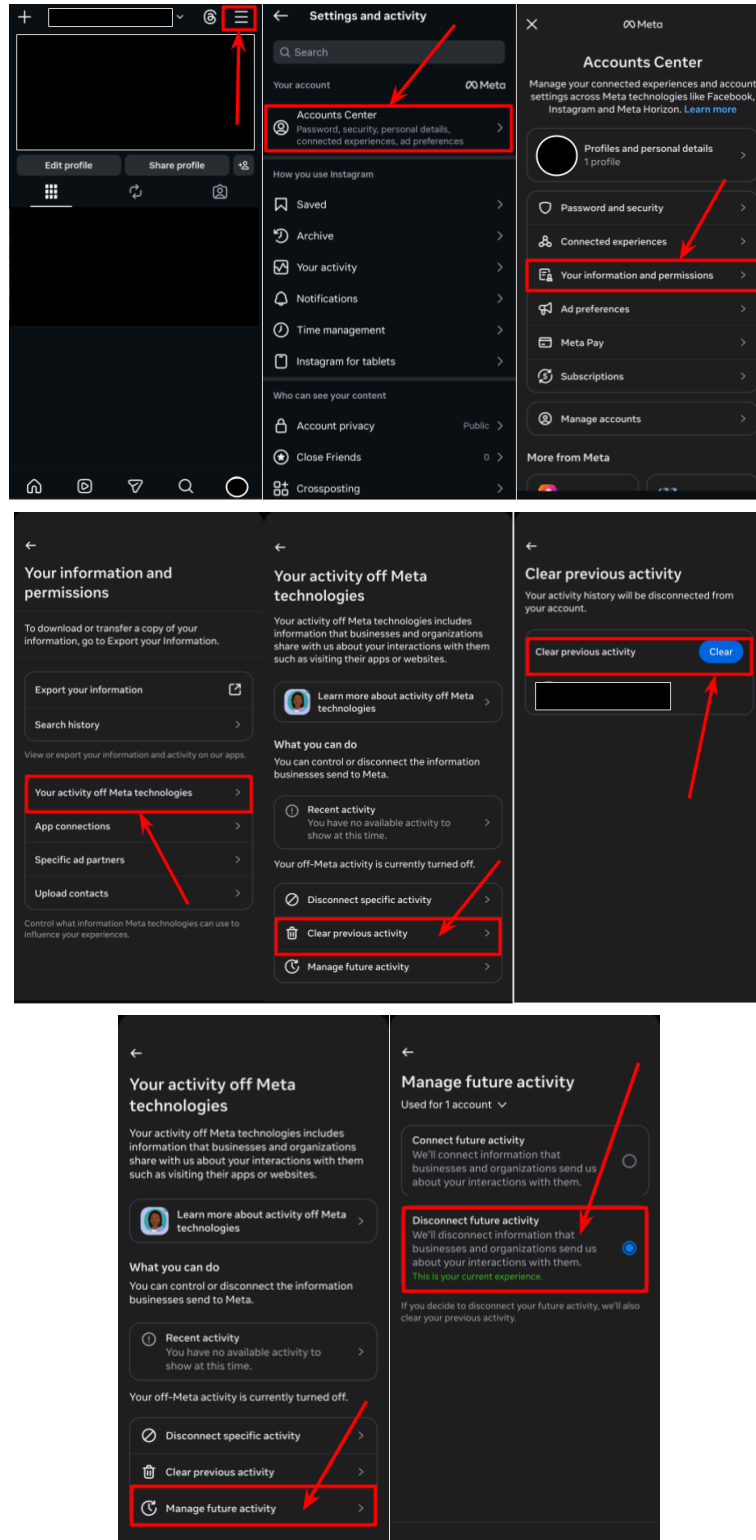
Setting Up Two-Factor Authentication (2FA):

1. From your **Profile Page** and tap the **Menu Icon** (≡) in the top right
2. Select **Account Center** > **Password & Security** > **Two-Factor Authentication**.
3. Choose the account you want to secure.
4. Select **Authentication App** as the security method and follow the on-screen instructions.



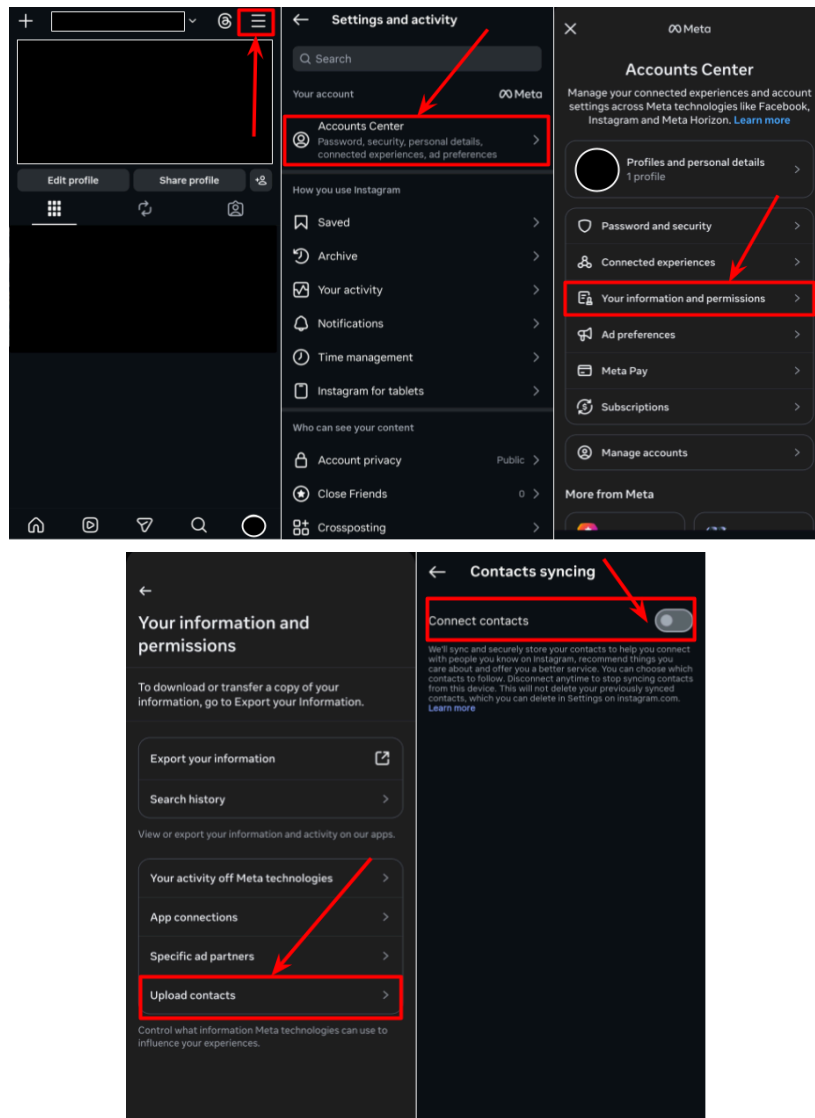
Managing Your Data & Activity Outside Meta:

1. From your **Profile Page** and tap the **Menu Icon** (≡) in the top right
2. Select **Account Center** > **Your Information and Permissions** > **Your Activity Off Meta Technologies**.
3. **Clear Previous Activity:** Remove data linked to external sites and apps.
4. **Manage Future Activity:** Select **Disconnect Future Activity** to prevent tracking from external sources.



Removing Uploaded Contacts:

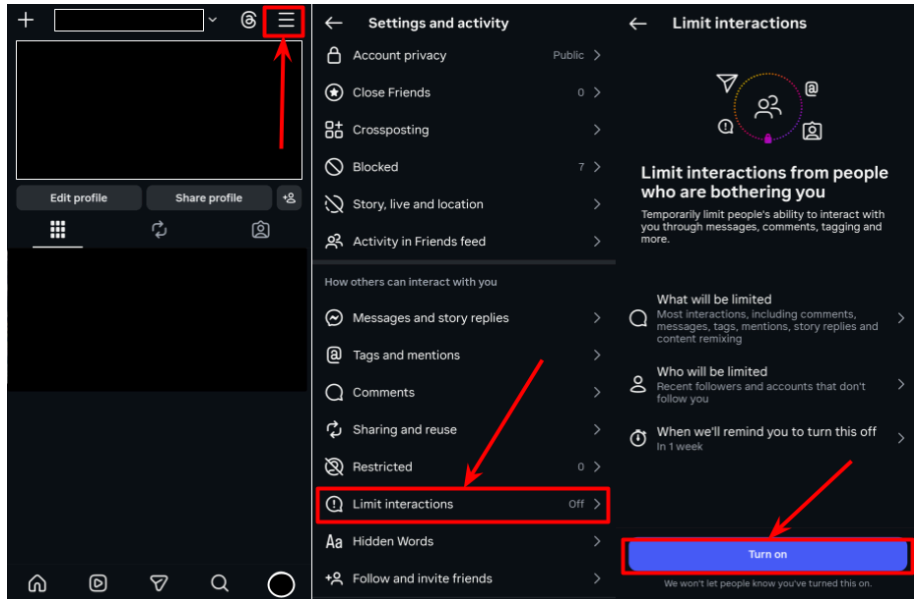
1. From your **Profile Page** and tap the **Menu Icon** (≡) in the top right
2. Select **Account Center** > **Your Information and Permissions** > **Upload Contacts**.
3. Toggle **Connect Contacts** **OFF** to stop Instagram from accessing and storing your contacts.



Temporarily Limiting Interactions to Avoid Harassment:

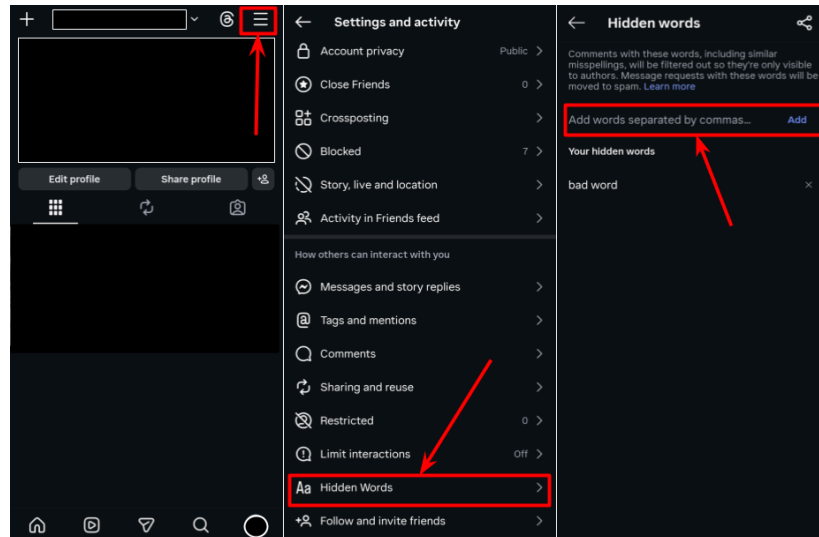
If you're experiencing unwanted interactions, you can temporarily limit engagement from certain users.

1. From your **Profile Page** and tap the **Menu Icon** (≡) in the top right
2. Scroll down under *How others can interact with you* and Select **Limit Interactions**.
3. Adjust settings for **What will be limited** (e.g., comments, messages) & **Who will be limited** (e.g., accounts that don't follow you or recent followers).
4. Set the **duration** of your choosing (maximum of 4 weeks) and then **turn ON**



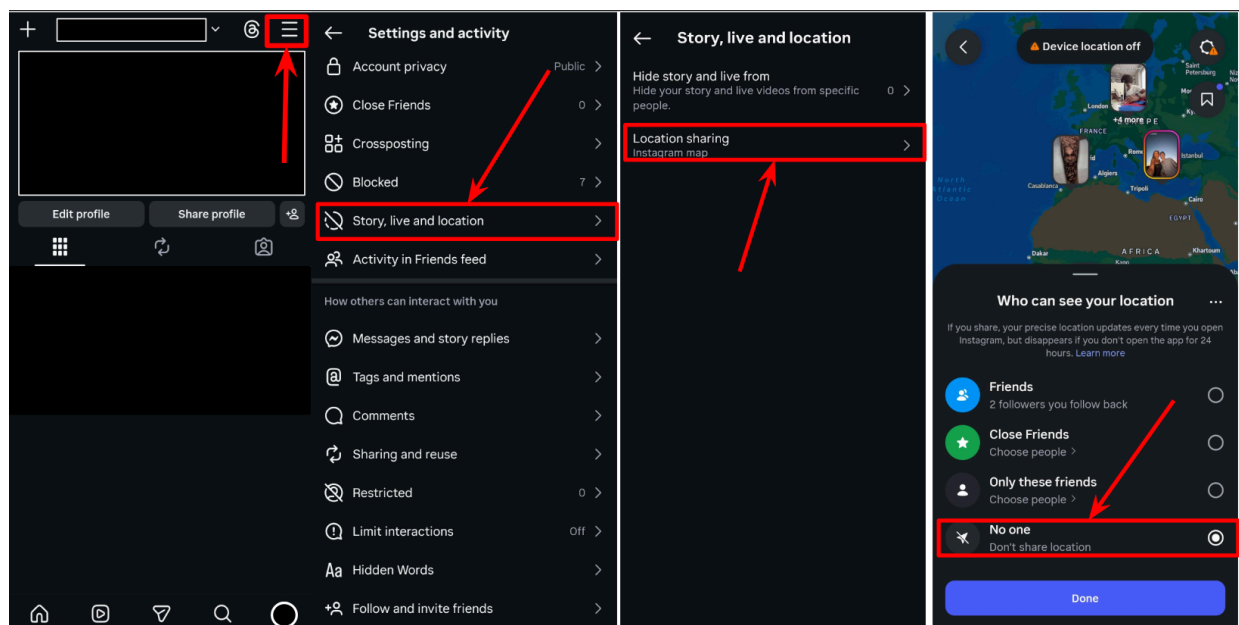
Filtering Out Offensive Words & Phrases:

1. From your **Profile Page** and tap the **Menu Icon** (≡) in the top right
2. Scroll down under *How others can interact with you* and Select **Hidden Words**.
3. Create **Your Hidden Words List** by adding specific words, phrases, or emojis you don't want to see
 - ⚠️ Content Warning for the sample list below: The example list of “bad words” contains profanity, slurs, and sexually explicit terms that may be offensive or disturbing. Please review the list only if you're comfortable doing so.
 - Check here for a sample list of bad words to filter out.
 - i. <https://docs.google.com/document/d/10irgql6yCVPEqYHRqRe72SGMeBcENAH5CeebHylpL6A/edit?tab=t.0>



Disable Location Sharing:

1. From your **Profile Page** and tap the **Menu Icon** (≡) in the top right
2. Scroll down under *Who can see your content* and Select **Story, live and location**
3. Select **Location Sharing**
4. Toggle **No One** to stop sharing your location with others

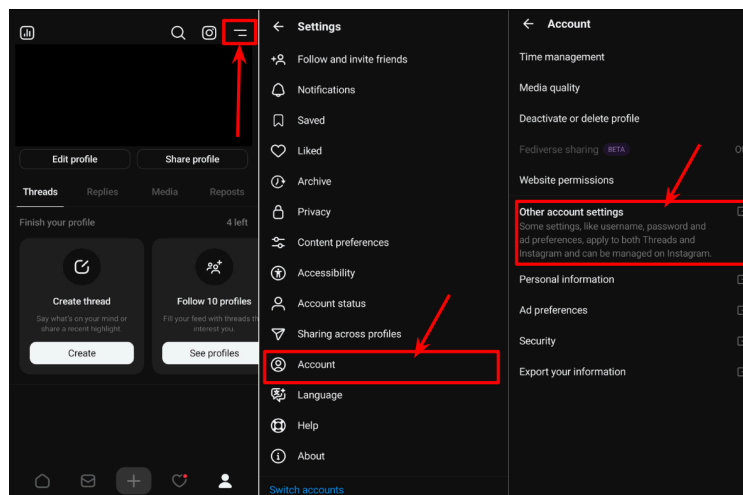


1.4 Threads

Updating Your Password to a Strong and Unique One:

1. From your **Profile Page**, tap the **Menu Icon** (≡) in the top right
2. Select **Account** > **Other Account settings**
3. You will be redirected to Instagram settings
4. Follow steps on Instagram from section 1.3

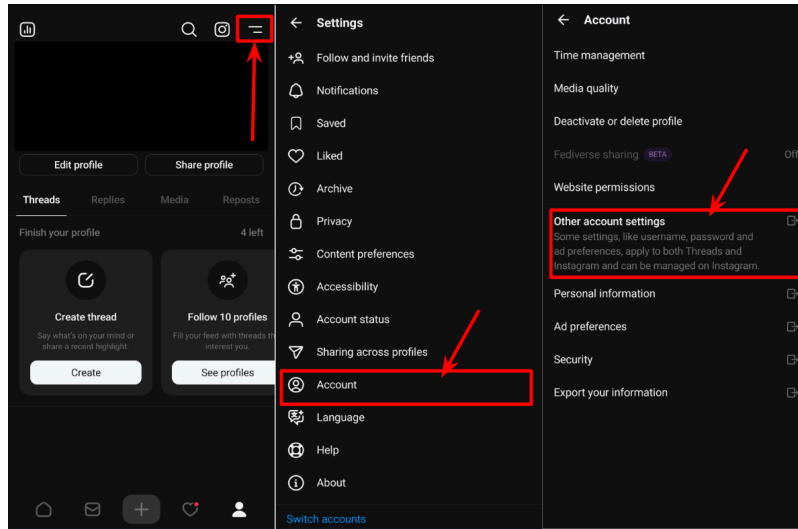
Note: Threads is linked to your Instagram account so any changes made via Threads applies to your Instagram account



Setting Up Two-Factor Authentication (2FA):

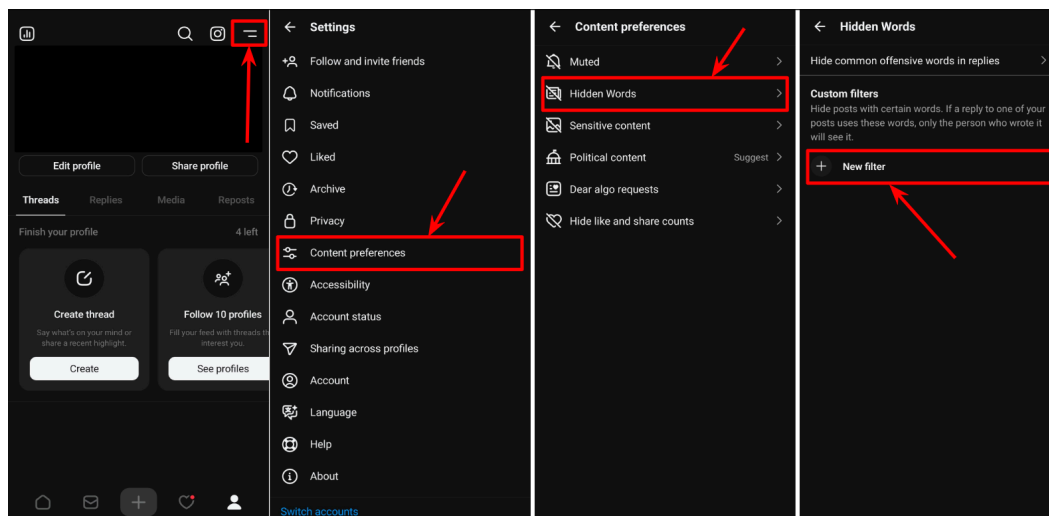
1. From your **Profile Page**, tap the **Menu Icon** (≡) in the top right
2. Select **Account** > **Security**
3. You will be redirected to Instagram settings
4. Follow steps on Instagram from section 1.3

Note: Threads is linked to your Instagram account so any changes made via Threads applies to your Instagram account



Filtering Out Offensive Words & Phrases:

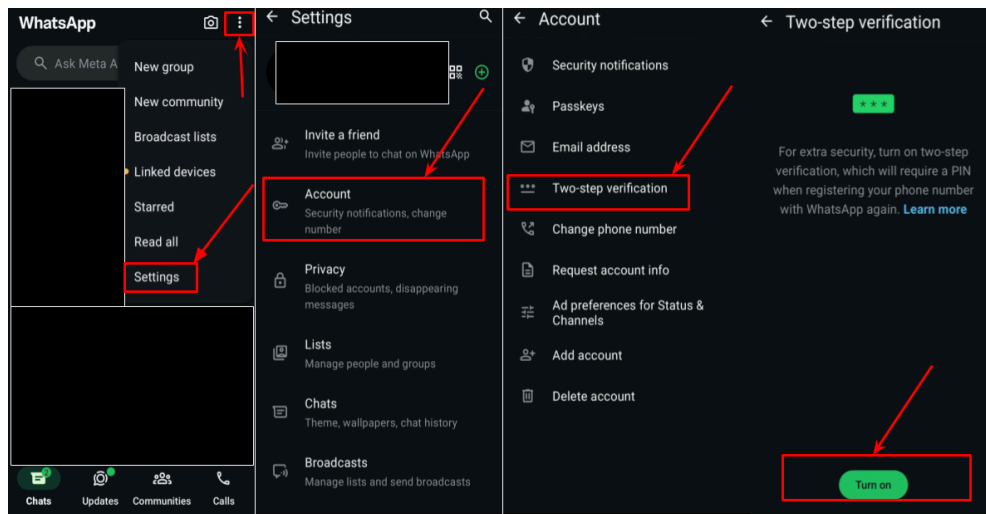
1. From your **Profile Page**, tap the **Menu Icon (≡)** in the top right
2. Select **Content Preferences > Hidden Words**
3. Create **Your Hidden Words List** by adding specific words, phrases, or emojis you don't want to see
 - ⚠️ Content Warning for the sample list below: The example list of “bad words” contains profanity, slurs, and sexually explicit terms that may be offensive or disturbing. Please review the list only if you're comfortable doing so.
 - Check here for a sample list of bad words to filter out.
 - i. <https://docs.google.com/document/d/10irgql6yCVPEqYHRqRe72SGMeBcENAH5CeebHylpL6A/edit?tab=t.0>



1.5 WhatsApp

Set Up Two-Factor Authentication (2FA):

1. Tap the **Menu Icon** (⋮) in the top right.
2. Go to **Settings > Account > Two-Step Verification**.
3. Tap **Turn On** and create a **6-digit PIN**.
4. This PIN will be required the next time you log in with your phone number.



Enable a Passkey for Added Security:

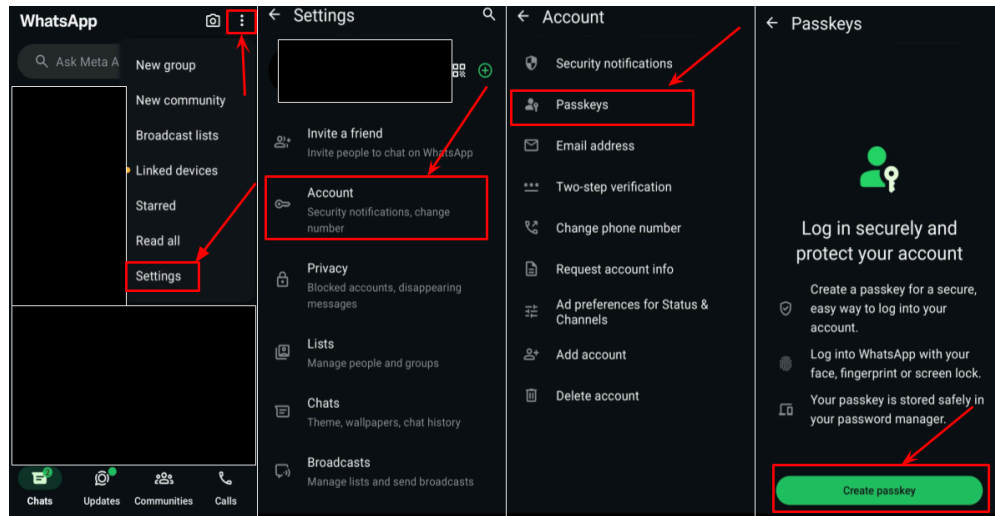
Passkeys allow you to log in securely using **Screen Lock** instead of a PIN.

1. Tap the **Menu Icon** (⋮) in the top right.
2. Go to **Settings > Account > Passkeys**.
3. Tap **Create Passkey** and follow the instructions.
4. It is recommended to use **Screen Lock** *not* Face ID or Fingerprint

It is not recommended that you use any biological identification (e.g., Face ID, Fingerprints), for your digital devices, or for personal or workplace identification, as it poses a safety risk for yourself and those around you. Face ID is also sensitive to size and shape, and is especially not recommended for those considering undergoing future physical changes or gender affirming care. Screen locks and numerical pins are always the strongest and safest option, and cannot be unlocked without legal permission by a member of law enforcement.

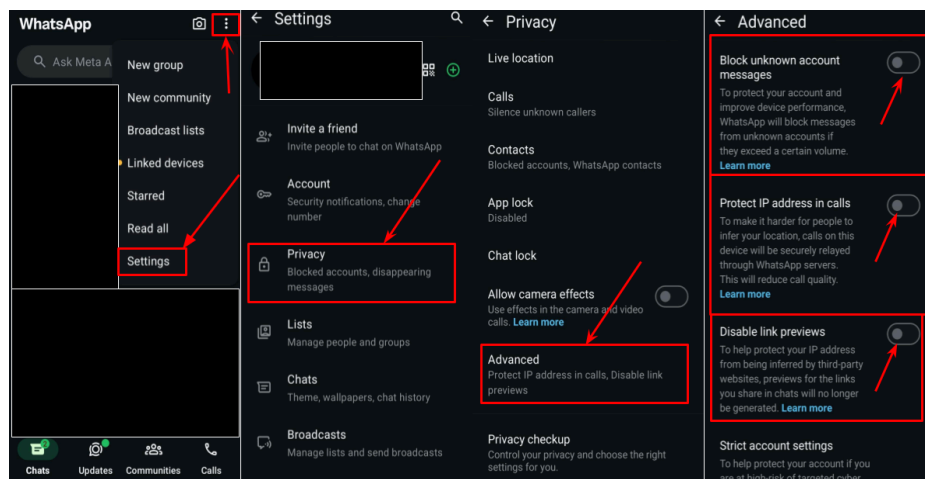
For individuals with precarious immigration status, this is especially important. Border agents can compel biometrics without a warrant, but they cannot legally force you to disclose a numerical pin or password. Please note that border patrol can reject your entry to a country if

you do not provide access to a device when requested. If you are concerned, please use an alternative device for travel if needed.



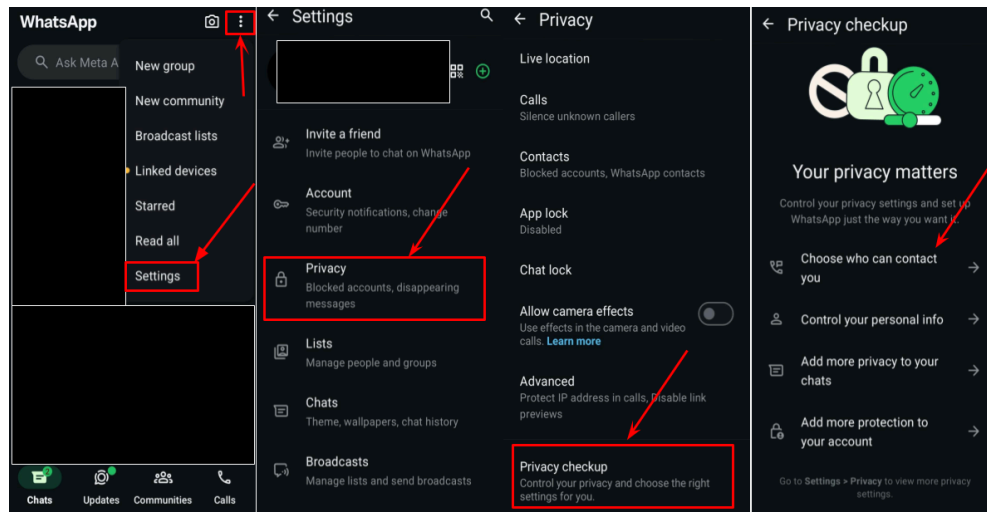
Protect Your IP Address & Block Unknown Accounts:

1. Tap the **Menu Icon (⋮)** in the top right.
2. Go to **Settings > Privacy > Advanced**.
3. Enable the following options:
 - **Block Unknown Account Messages** – Prevents messages from unverified contacts.
 - **Protect IP Address in Calls** – Hides your IP address during calls for better security.
 - **Disable Link Previews** – Prevents link previews from revealing your data.



Perform a Privacy Checkup:

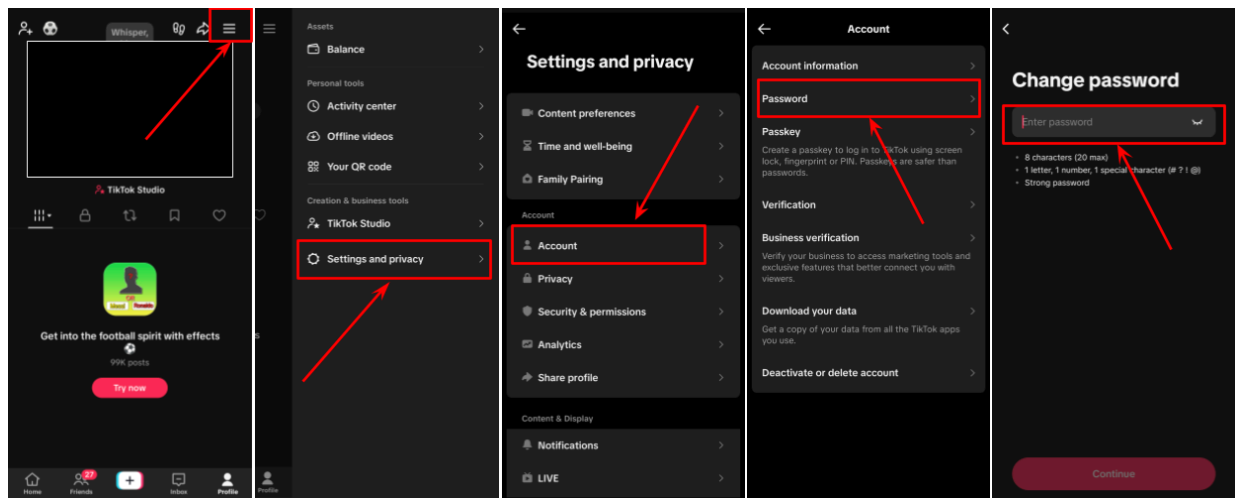
1. Tap the **Menu Icon** (☰) in the top right.
2. Go to **Settings > Privacy > Privacy Checkup**.
3. Adjust settings to:
 - Choose **who can contact you**.
 - Control **your personal information visibility**.
 - Add **extra privacy to chats**.
 - Strengthen **account security and protection**.



2. TikTok

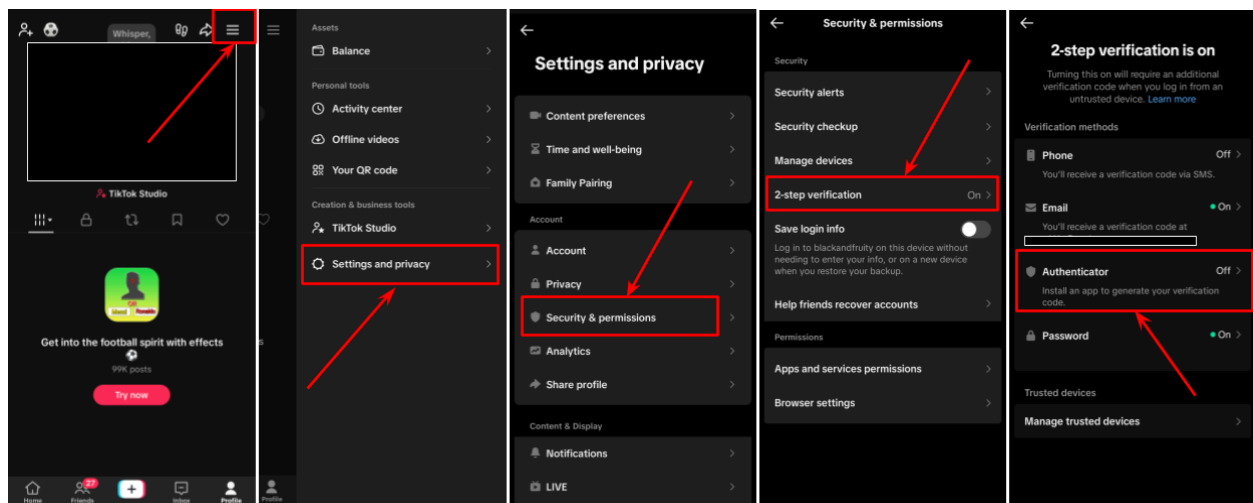
Updating Your Password to a Strong and Unique One:

1. From your Profile page, tap the **Menu Icon** (≡) in the top right.
2. Select **Settings and Privacy** > **Account** > **Password**
3. Verify your email and follow on-screen instructions to enter a new, strong password



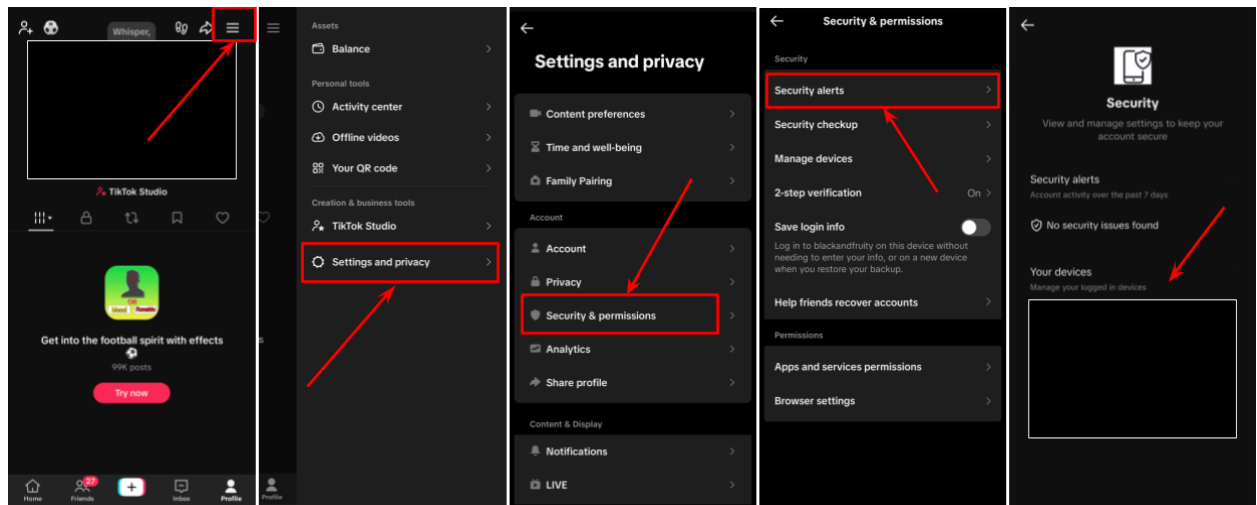
Setting Up Two-Factor Authentication (2FA):

1. From your Profile page, tap the **Menu Icon** (≡) in the top right.
2. Select **Settings and Privacy** > **Security & Permissions** > **2-Step Verification**
3. **Turn ON** at least 2 verification methods including **Authenticator**



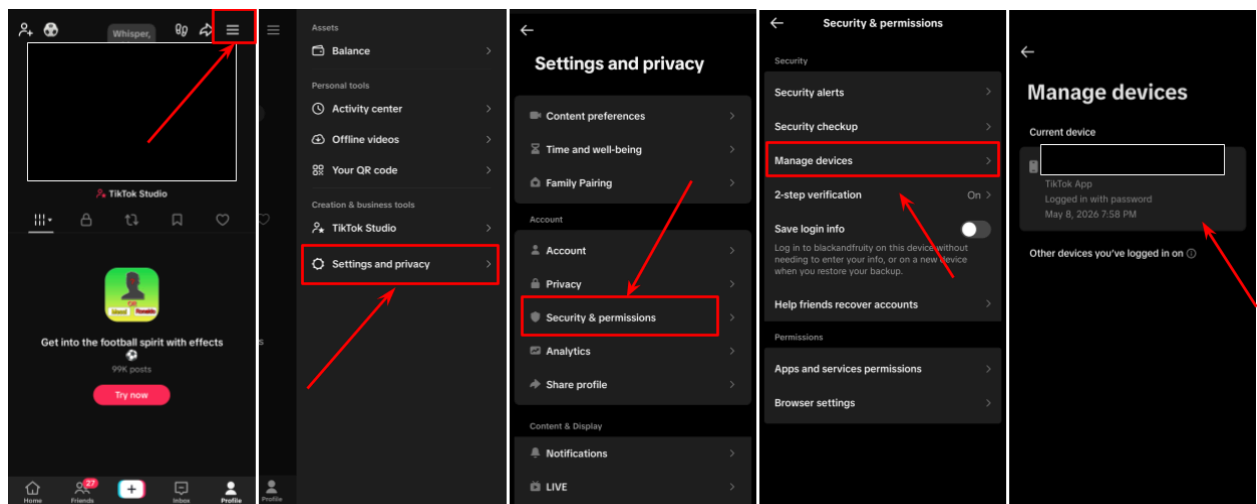
Review Security Alerts Detected:

1. From your Profile page, tap the **Menu Icon** (≡) in the top right.
2. Select **Settings and Privacy > Security & Permissions > Security Alerts**
3. Review any security alerts of unusual activity in the last 7 days
4. Manage devices logged into your account and remove access for any devices you do not recognize



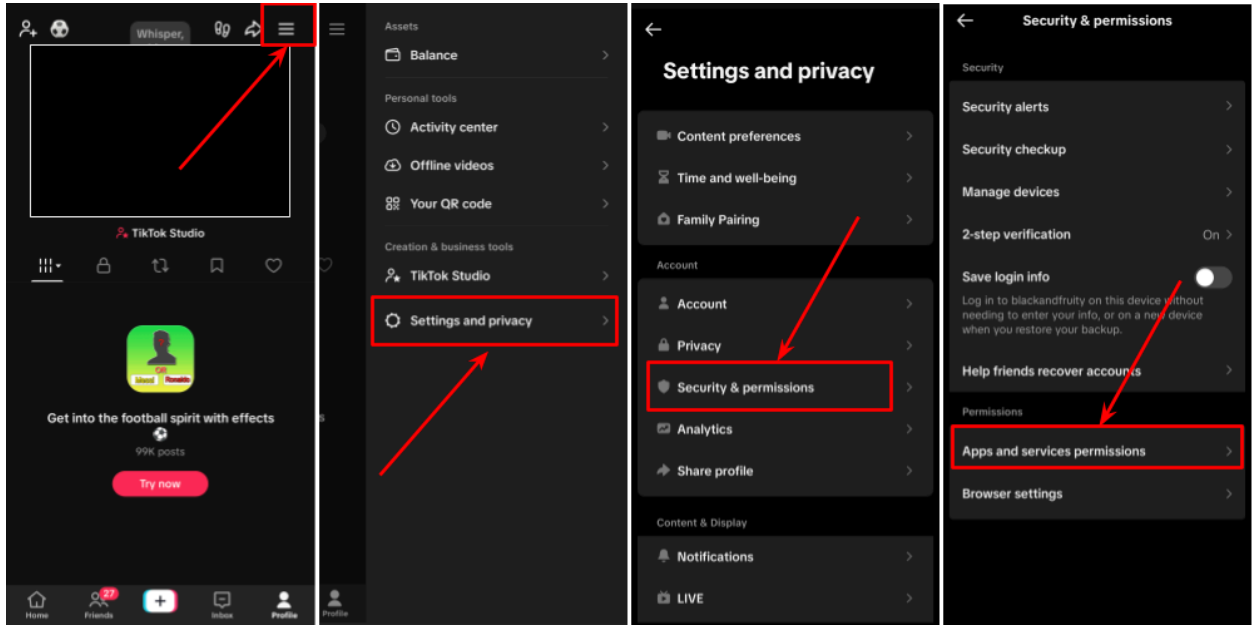
Review Devices Logged into your Account:

1. From your Profile page, tap the **Menu Icon** (≡) in the top right.
2. Select **Settings and Privacy > Security & Permissions > Manage Devices**
3. View list of devices logged into your account and delete any unfamiliar devices



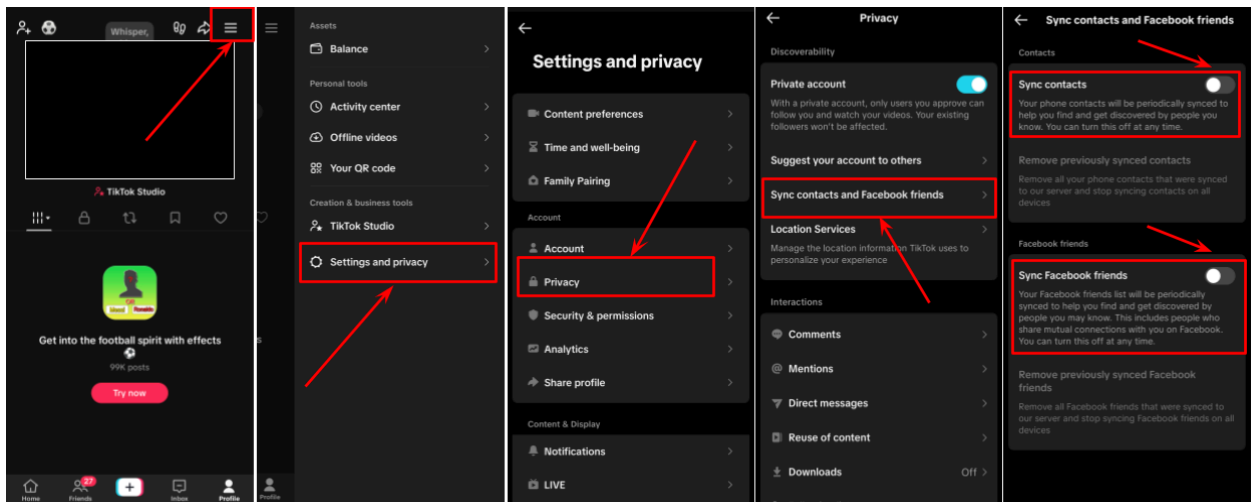
Disconnect Third Party Apps from Connecting to your Account:

1. From Profile, tap the **Menu Icon** (≡) in the top right.
2. Select **Settings and Privacy > Security & Permissions > Apps and Services Permissions**
3. Disconnect any authorized apps from connecting to your TikTok account



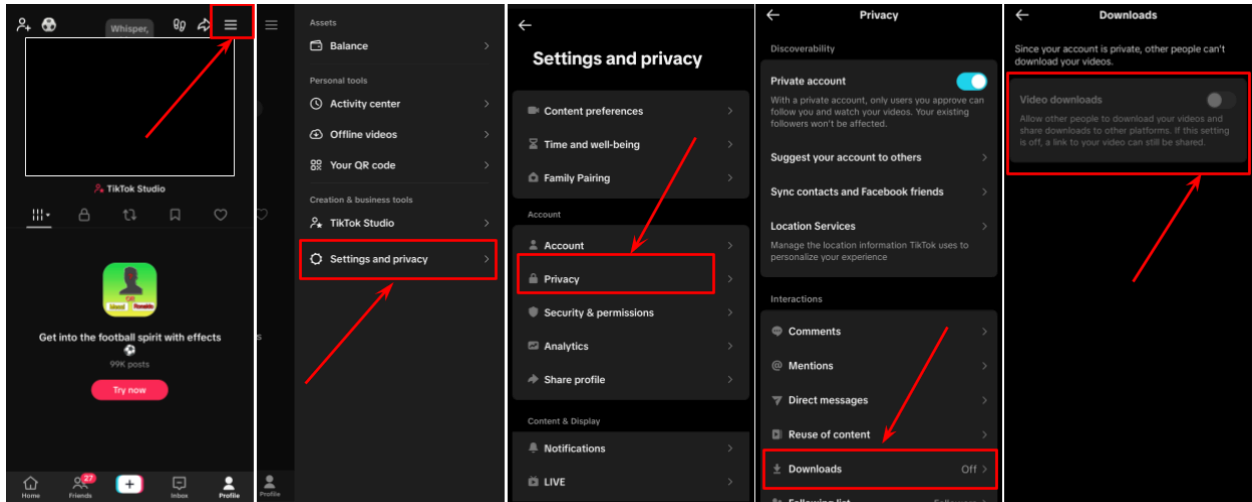
Disconnect Contacts and Facebook Friends:

1. From Profile, tap the **Menu Icon** (≡) in the top right.
2. Select **Settings and Privacy > Privacy > Sync contacts and Facebook Friends**
3. **Toggle OFF Sync Contacts & Sync Facebook Friends**
4. Make sure to remove previously synced contacts and Facebook friends



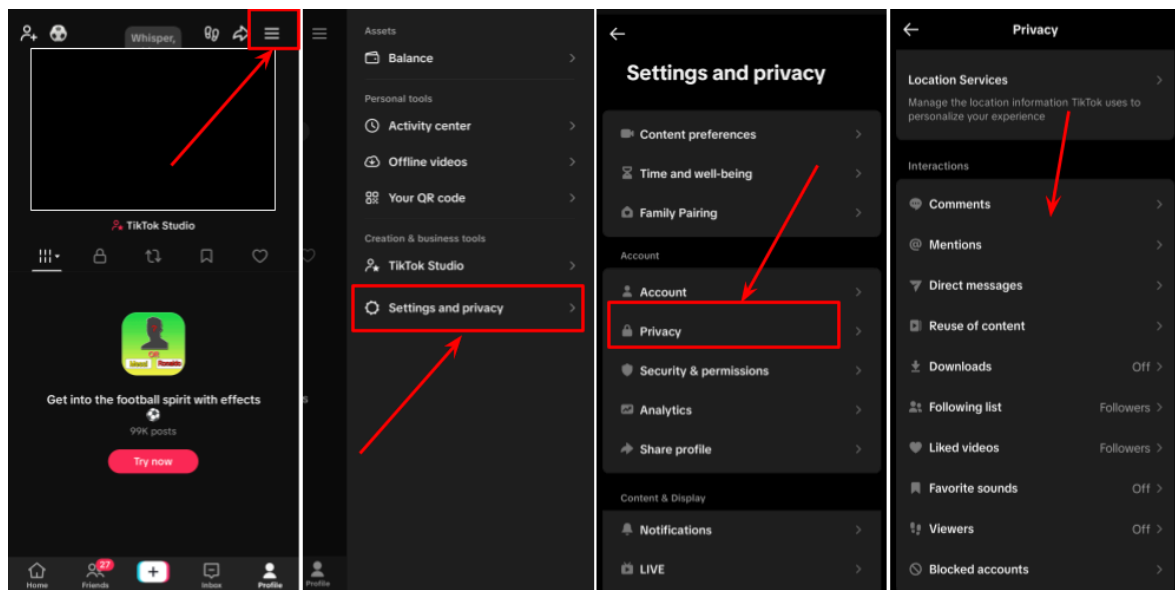
Disable Downloads from Others:

1. From your Profile page, tap the **Menu Icon** (≡) in the top right.
2. Select **Settings and Privacy > Privacy**
3. Scroll down under *Interactions* and select to **Downloads**
4. **Toggle Video Downloads OFF** so other people can't download your videos



Adjust Additional Privacy Settings for Account Interactions:

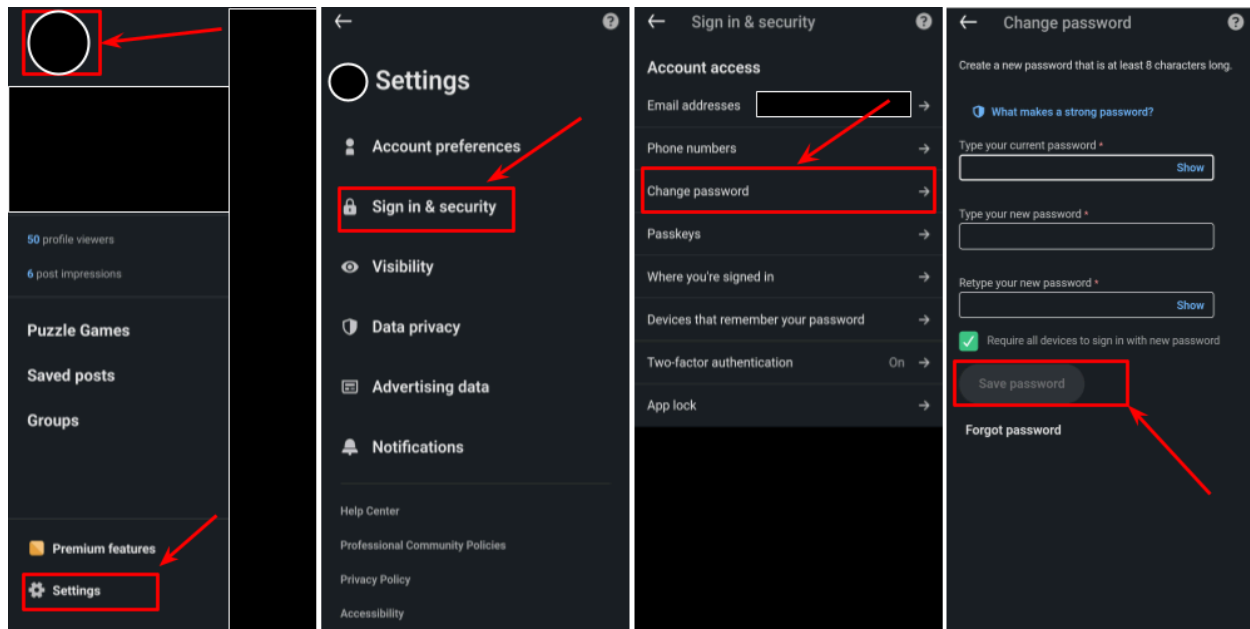
1. From Profile, tap the **Menu Icon** (≡) in the top right.
2. Select **Settings and Privacy > Privacy** > Scroll down to the *Interactions* section
3. Adjust settings based on preferences for Comments, Mentions, Direct Messages, Following List, Views etc.



3. LinkedIn

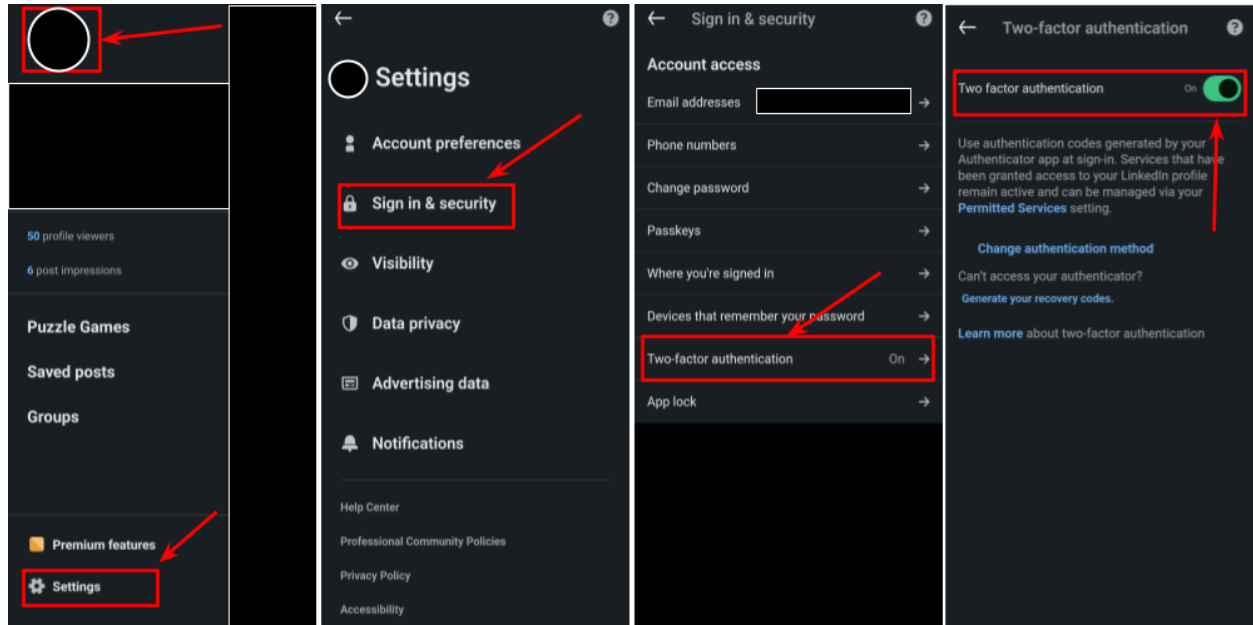
Update Your Password to a Strong and Unique One:

1. Tap your **Profile Picture**.
2. Go to **Settings > Sign In & Security > Change Password**.
3. Enter your current password, then create a strong, unique password that follows best security practices.



Set Up Two-Factor Authentication (2FA):

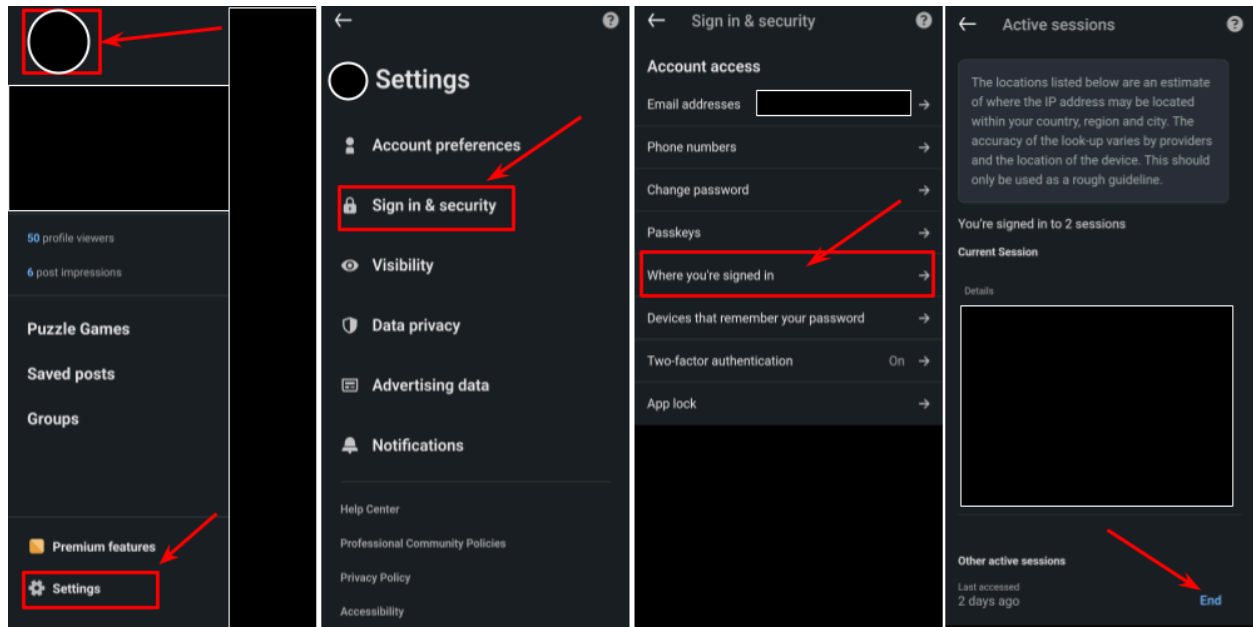
1. From your Activity Feed, Tap your **Profile Picture** in the top left
2. Select **Settings > Sign In & Security > Two-Step Authentication**.
3. Follow the on-screen instructions to enable 2FA using an authentication app.



Review Active Sessions & Sign Out of Unrecognized Devices:

Regularly check where your account is logged in to ensure no unauthorized access.

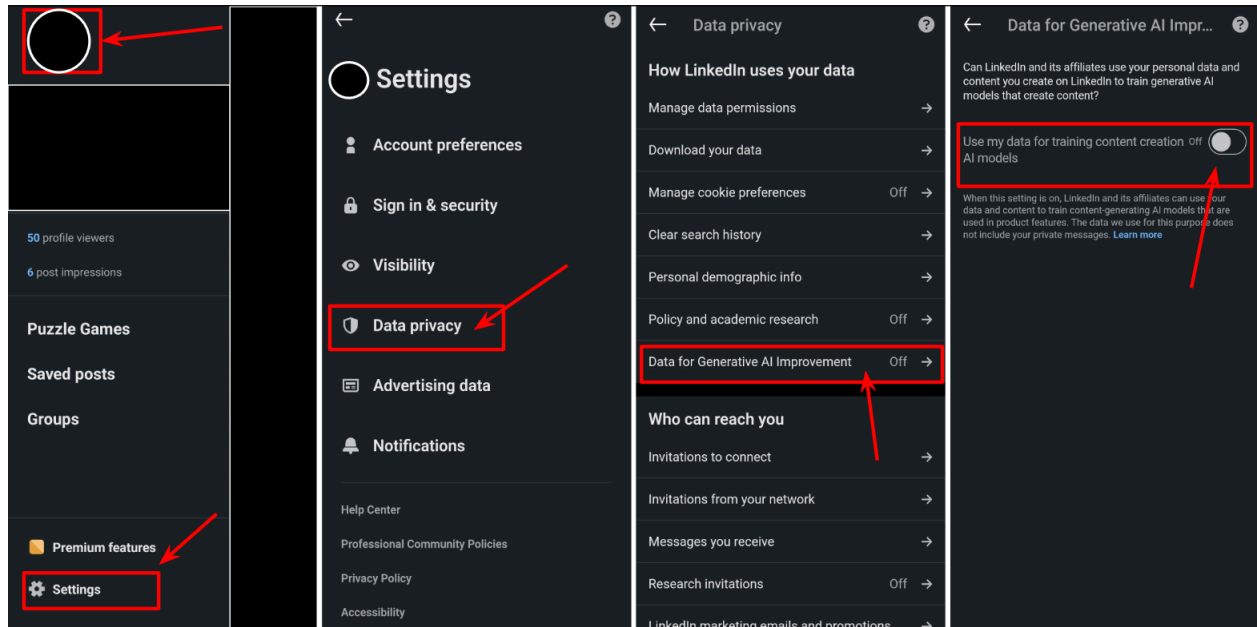
1. From your Activity Feed, Tap your **Profile Picture** in the top left
2. Navigate to **Settings** > **Sign In & Security** > **Where You're Signed In**.
3. Review the list of active sessions.
4. If you see any unfamiliar locations or devices, select **End Session** to log out immediately



Turn off Generative AI from using your Personal Data:

LinkedIn automatically uses your content to train its AI. LinkedIn holds a lot of personal information such as full names and work/education history that should not be processed through an AI tool. Opt out of AI so your content is not being processed through an AI tool, being shared with unknown vendors, or training AI to directly harm your community.

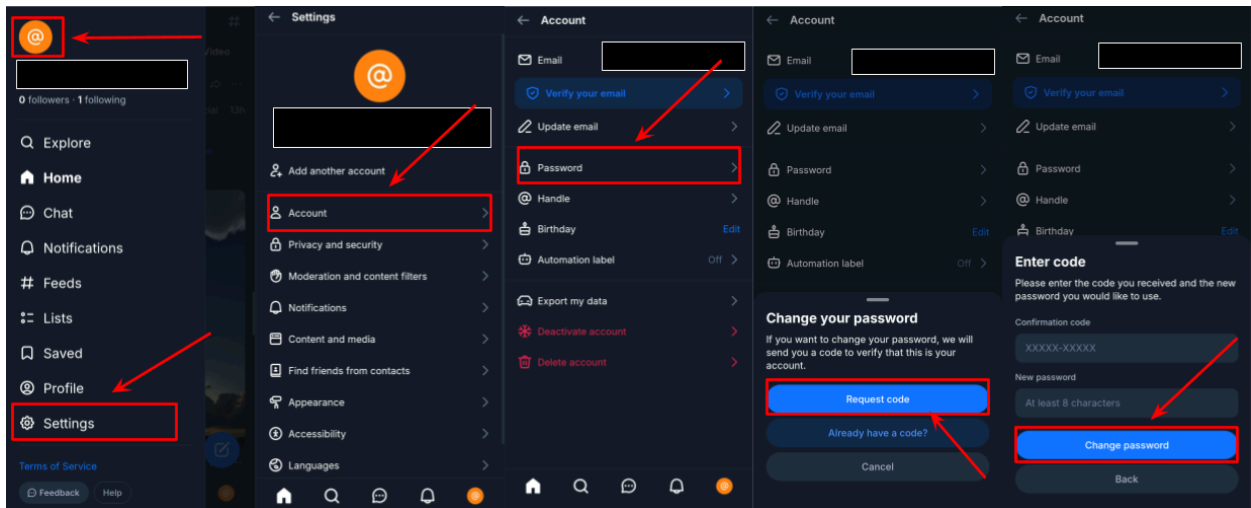
1. From your Activity Feed, Tap your **Profile Picture** in the top left
2. Navigate to **Settings > Data privacy > Data for Generative AI Improvement**
3. **Toggle Use my data for training content creation OFF**



4. Bluesky

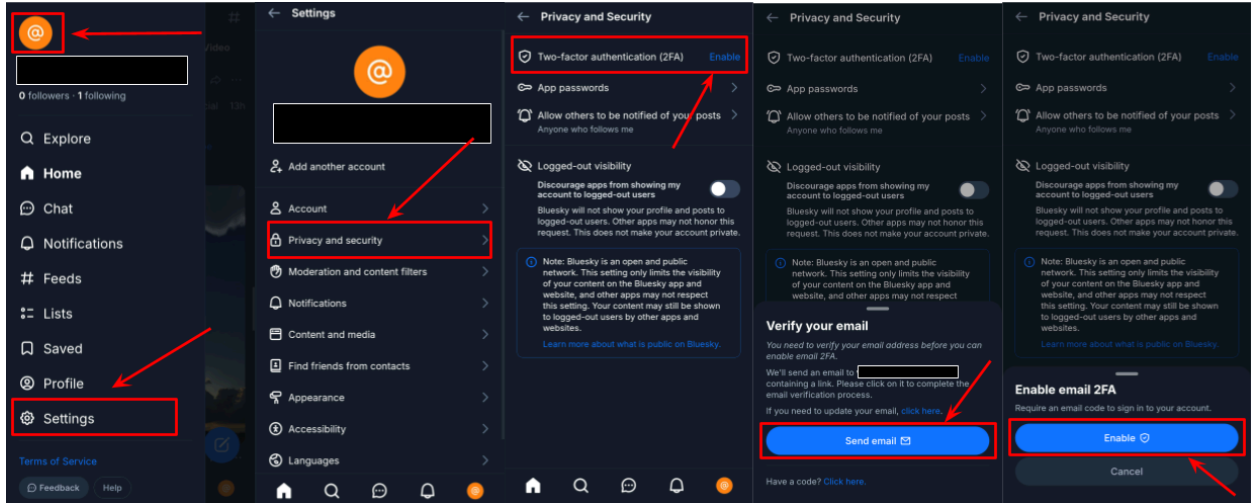
Update Your Password to a Strong and Unique One:

1. From your activity feed, Tap the **Menu Icon** (≡) in the top left.
2. Select **Settings** (⚙️) > **Account** > **Password**
3. Follow the on-screen instructions to verify your account and change your password



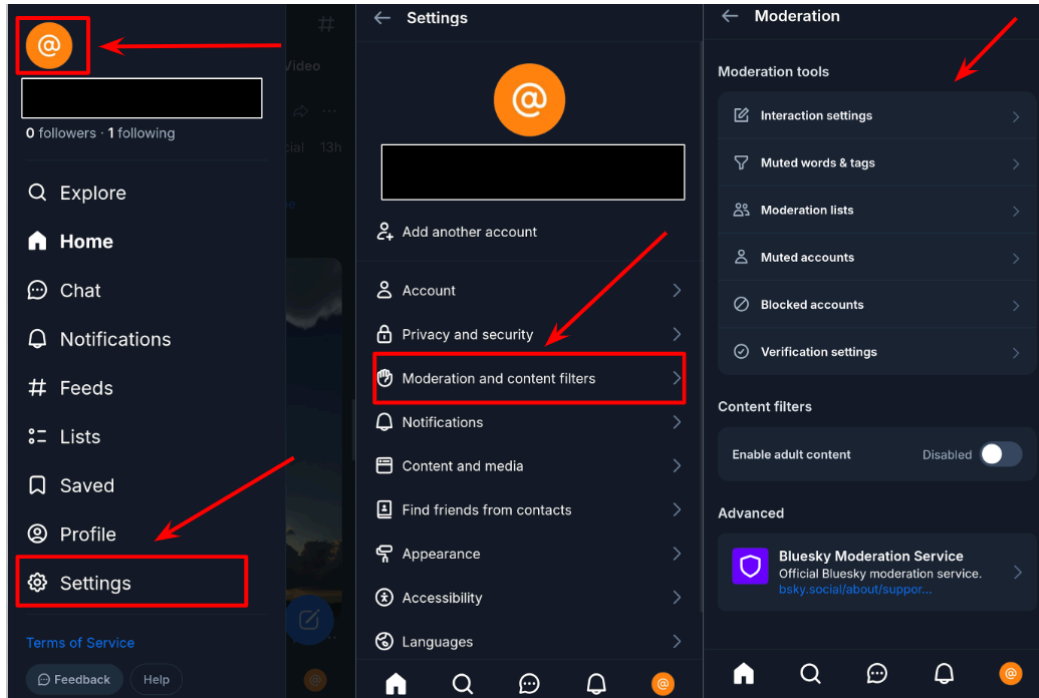
Setting Up Two-Factor Authentication (2FA):

1. From your activity feed, Tap the **Menu Icon** (≡) in the top left.
2. Select **Settings** (⚙️) > **Privacy and security**
3. Enable **Two-factor authentication (2FA)** and follow on screen instructions
 - BlueSky only enables email as the additional verification method



Word Filters:

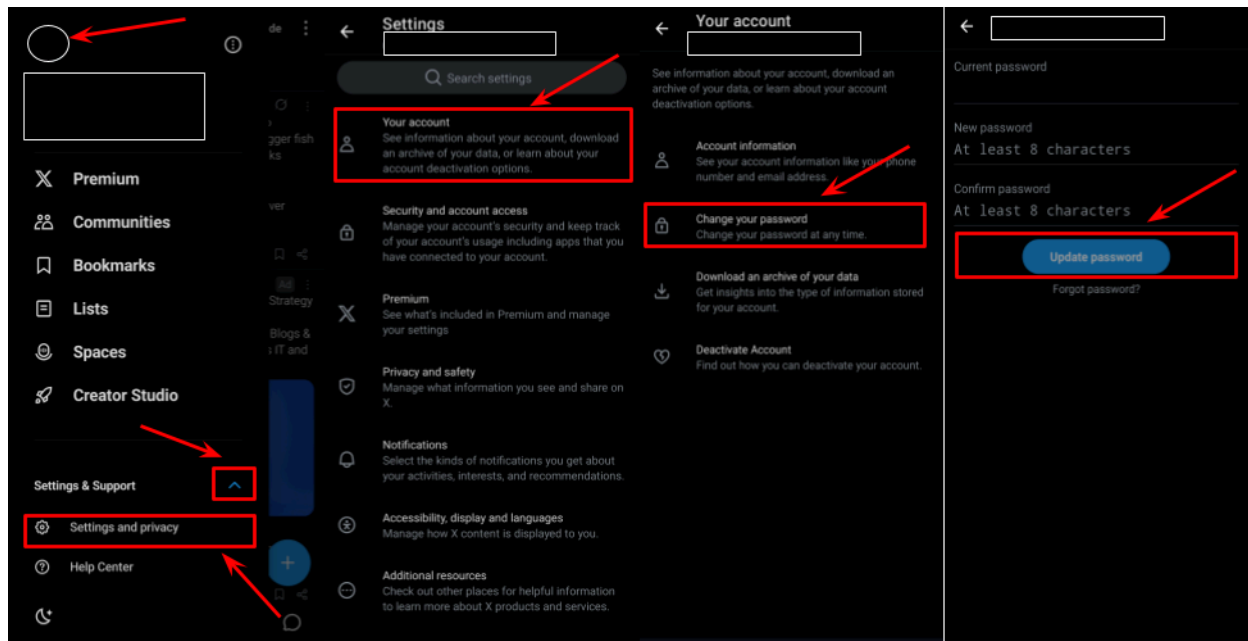
1. From your activity feed, Tap the **Menu Icon** (≡) in the top left.
2. Select **Settings** (⚙️) > **Moderation and content filters** > **Muted words & Tags**
3. Add specific words, phrases, or emojis you don't want to see
 - ⚠️ Content Warning for the sample list below: The example list of “bad words” contains profanity, slurs, and sexually explicit terms that may be offensive or disturbing. Please review the list only if you're comfortable doing so.
 - Check here for a sample list of bad words to filter out.
 - i. <https://docs.google.com/document/d/10irgql6yCVPEqYHRqRe72SGMeBcENAH5CeebHyLpL6A/edit?tab=t.0>



5. X formerly Twitter

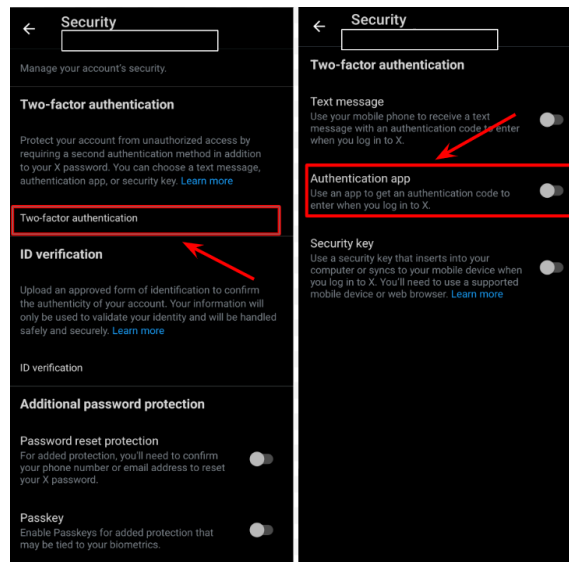
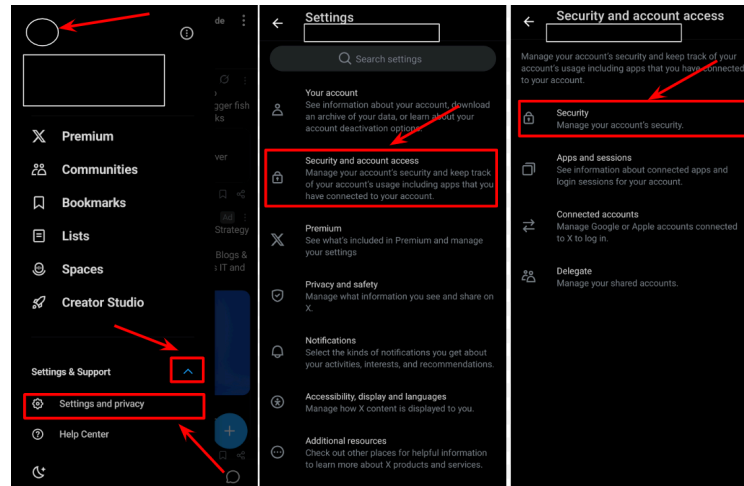
Update Your Password to a Strong and Unique One:

1. Tap your **Profile Picture** then the Drop Down Icon (V) beside **Settings & Support**
2. Go to **Settings and Privacy > Your Account > Change Your Password**.
3. Enter your current password, then create a strong, unique password that follows best security practices.



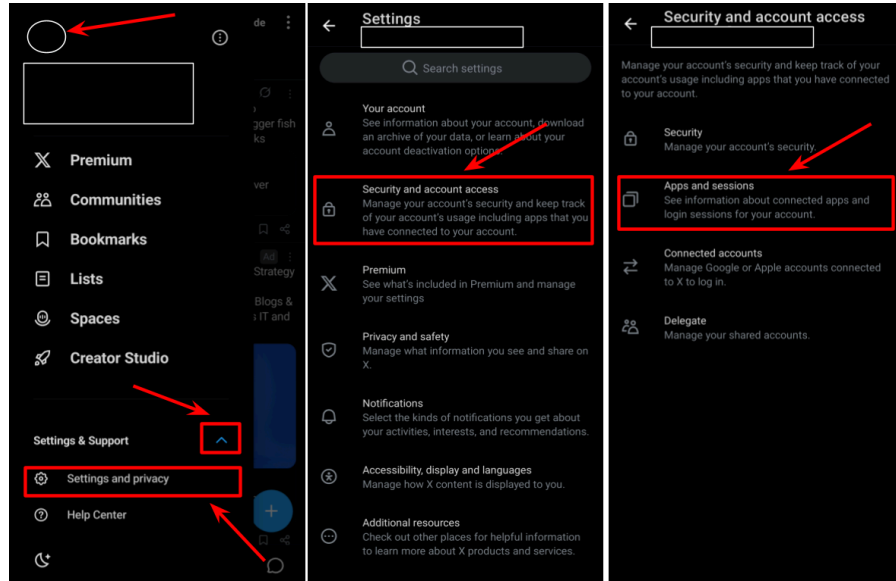
Setting Up Two-Factor Authentication (2FA):

1. Tap your **Profile Picture** then the Drop Down Icon (V) beside **Settings & Support**
2. Go to **Settings and Privacy > Security and account access > Security > Two factor authentication**
3. **Toggle ON Authenticator App**
4. Follow the on-screen instructions to enable 2FA using an authentication app.



Review Login Activity & Sign Out of Unrecognized Devices:

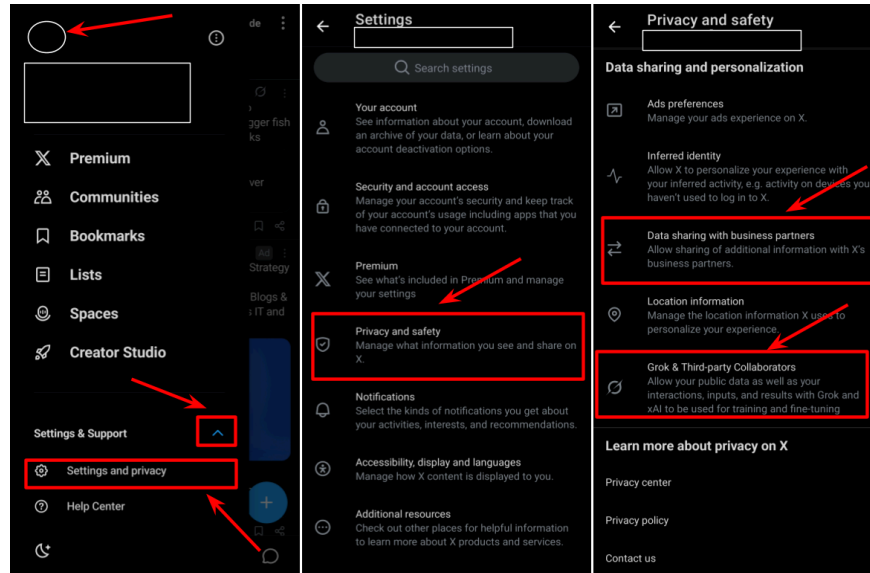
1. Tap your **Profile Picture** then the Drop Down Icon (V) beside **Settings & Support**
2. Go to **Settings and Privacy > Security and account access > Apps and sessions**
3. In **Sessions**, check devices where your account is logged in and log out of any unfamiliar devices
4. In **Account access history**, check for suspicious activity from any apps then go to **Connected apps** to remove access
5. In **Logged-in devices and apps**, check which browsers, devices and information Twitter is using to "personalize your experience" and turn off any that are unnecessary



Block AI Training & Third-Party Data Sharing:

Twitter/X's automatically uses your content and interactions to train its AI called Grok. Opt out of AI so your content is not being processed through an AI tool, being shared with unknown vendors, or training AI to directly harm your community.

1. Tap your **Profile Picture** then the Drop Down Icon (V) beside **Settings & Support**
2. Go to **Settings and Privacy > Privacy and safety**
3. In **Grok & Third-party Collaborators**, **Toggle OFF** all settings to prevent AI from using your data and **Delete conversation history**
4. In **Data sharing with business partners**, **Toggle OFF** all settings to stop sharing your data



For more information on securing your social media profiles check out these sources below:

- How to Change your Meta Settings
 - <https://www.johnoliverwantsyourraterotica.com/>
- Social Media Security & Privacy Checklist
 - <https://docs.google.com/document/d/1ud1ILFklG0BeLX9jlzJMxCpM8-cSeqPjU60nkhUPYA8/edit?usp=sharing>
 - The checklist is from a New York Times article:
 - Kozinski, K. & Kapur, N. (2020, February 27). *How to Dox Yourself on the Internet*. New York Times.
 - <https://open.nytimes.com/how-to-dox-yourself-on-the-internet-d2892b4c5954>
- How to filter, block and report harmful content on social media
 - <https://rainn.org/articles/how-filter-block-and-report-harmful-content-social-media>.



References

Akomea, C. B. (2025, June 11). *Incident response for ddos attacks and the way forward*. Cyber Security Cue. <https://cybersecuritycue.com/incident-response-for-ddos-attacks/>

Cyberhaven. (2026, February 12). *What is a ddos attack?*. <https://www.cyberhaven.com/infosec-essentials/ddos-attack>

Dach, P. (2025, September 7). *Dogpiling (internet) and online harassment*. Go2Share. <https://www.go2share.net/article/dogpiling-internet>

Ferriss, T. (2026, June 23). *How to stop dogpiling on social media?*. SkyJob Net.Com. <https://skyjobnet.com/how-to-stop-dogpiling-on-social-media.html>

Gonzalez, C. (2023, May). *Coalition against online violence | Mapping report 2024*. International Women's Media Network. <https://onlineviolenceresponsehub.org/wp-content/uploads/2024/01/CAOV-MAPPING-REPORT-2024.pdf>

Johnson, K. (2025, March 11). *Incident response for web application attacks*. Tech Target. <https://www.techtarget.com/searchSecurity/feature/Incident-response-for-web-application-attacks>

Knutsson, K. (2026, January 9). *Cloned on Facebook? Here's how to take back control*. CyberGuy. <https://cyberguy.com/security/cloned-on-facebook-heres-how-to-take-back-control/>

ODLAN. (2025). *Digital safety procedural policy*. <https://odlan.ca/digital-safety-procedural-policy/>

PrivacyOn. (2026, April 30). *Privacy guide for LGBTQ+ individuals: Protecting your identity online*. <https://www.privacyon.com/blog/privacy-guide-for-lgbtq-individuals>

Terassa, D. (2026, January 31). *How to detect if a website is blocking you by region*. Technobits. <https://tecnobits.com/en/Web-blocking-by-region/>

TSPA. (2023, July 31). *Responding to and preventing doxing: A TSPA resource*. https://www.tspa.org/wp-content/uploads/2023/07/Responding-to-and-Preventing-Doxing_-_A-Resource-For-the-public.pdf