

Digital Safety Checklist

Use this checklist to tighten access to your accounts and take control of your data. You'll find simple steps that you can take to get started with:

- Self-Care and Support
- Account Security
- Privacy
- Data, Brokers and Breaches
- Social Media
- Additional Resources

For more detail on any of these steps, check out:

- Field Manual Against Online Harassment: <https://onlineharassmentfieldmanual.pen.org/>
- Digital Safety Snacks: <https://pen.org/digital-safety-snacks/>

Self-Care and Support

Check in with yourself. Addressing digital safety, especially if you've experienced online hate and harassment, can bring up a range of reactions—from frustration and confusion to anger and overwhelm. If it's useful, take a moment to think about what helps ground you—whether it's taking deep breaths or going for a walk outside—and try a few of those things as you work through this list. Take breaks and take care of yourself.

Gather your support system. Safety is a community effort. Think about the people, groups, or organizations you trust. As you take steps to lock down your digital footprint, who can you ask for help? And who will have your back?

Get started. Protecting yourself online is a process. You don't have to do everything all at once. Doing any of the items in this checklist will help to make you and the people close to you safer. We hope that, by breaking up what you need to do into concrete tangible steps, the process will feel more manageable and empowering.

Account Security

Let's start by locking down your online accounts and making them harder to hack.

Make a list of your 5-10 most sensitive accounts—this could include your bank account, your healthcare app, your social media accounts, your personal or work email, etc.:

Take the following steps to secure these accounts:

Get a password manager

What is it? A password manager automatically generates long secure passwords, stores them safely for you, and fills them in for you automatically when you need to log into your accounts.

- Sign up for a secure, encrypted, high quality password manager, such as [1Password](#) or [DashLane](#). 1Password has a [free service for journalists](#).
- Create a long complex password to log into your password manager and don't forget it!
- Don't forget to save your backup codes!

TIP: Set up both the browser extension & mobile app.

Create unique, long passwords for each account

What is it? To protect yourself from hacking, it is critically important to practice password hygiene by creating long complex passwords for all of your accounts and using a different password for each account.

- Use at least 16 characters with numbers or symbols (eg: correcthorsebatterystaple22!)
- One-to-one rule: use different password for EVERY account

TIP: Invent security questions (avoid Google-able answers, like your mother's maiden name)

Set up Multi-Factor Authentication for each account

What is it? Multi-Factor Authentication (MFA) is also often called Two-Factor Authentication (2FA). If you try to log in to your account from an unrecognized device, you will be asked to "authenticate" your identity (to prove you are not a hacker). There are a few common ways to set up MFA: 1) code sent via SMS/text to your cell phone, 2) code generated by an authenticator app on your cell phone, or 3) a physical security key. The physical key is the most secure option, text messages are the least secure option, and authenticator apps are both easy and secure. Think of your password as the first lock on your door and MFA as the second lock.

- Download an authenticator app like [Authy](#), [Duo](#), or [Google Authenticator](#)
- Start with your most sensitive accounts, log into each account, and set up MFA by connecting them to the authenticator app

TIP: When you set up MFA/2FA on an account, save your backup codes somewhere safe, like your password manager!

❑ **Protect your cell phone number from theft (aka SIM jacking)**

What is it? Hackers call your mobile provider pretending to be you, claim you've "lost" your SIM card, then request your phone traffic be routed to a new SIM card (in hacker's hands).

- Call your mobile provider and ask that a PIN be added to protect your account. You may also be able to do this online— AT&T users can [follow the instructions here](#) to use Wireless Account Lock; [T-Mobile users](#) and [Verizon users](#) can also enable SIM swap protection online.

TIP: Don't use your birthday as your PIN!

❑ **Update software and mobile apps**

What is it? Companies use updates to (quietly) fix security bugs. If you do not regularly update apps and software, your accounts will be more vulnerable to hacking.

❑ **Check on 3rd party apps**

What is it? When you create a username and password for a new software or platform and you "sign in" automatically via Google, Facebook, or Twitter, you are giving this new software or platform a backdoor to your Google, Facebook, or Twitter account. We recommend that you do NOT grant 3rd party apps access to your accounts.

TIP: See "Social Media Audit" below for ways to undo this on social media platforms.

Privacy

Be strategic about where you share your personal contact information and use privacy tools.

❑ **Set up multiple cell phone numbers**

What is it? With at least two cell phone numbers, you can share one publicly for work and keep the other one private for trusted contacts. Your public/professional cell number protects your private/personal cell number if you get doxed.

- Option 1: Ask your cell provider if they offer virtual or secondary phone numbers
- Option 2a: In the US, set up a virtual number via [Google Voice](#)
- Option 2b: Outside the US, set up a virtual number via [Sudo](#) or e-Sims like [HolaFly](#)
- Option 3: Get a second SIM card and/or cell phone.

❑ **Set up multiple email addresses**

What is it? With at least two email addresses, you can share one publicly for work and keep the other(s) private for trusted contacts. You could also use one account solely for spam. Your public email address protects your private email address if you get doxed or face message bombing. Using a contact form or an alias email can also help add further levels of privacy.

- Check out our [Email Safety Toolbox](#) for more email tools and strategies to consider.

TIP: Consider the privacy practices of different email providers. Some, like [Proton Mail](#), are encrypted, which makes them more secure (see below re encryption).

❑ **Use encrypted messaging apps**

What is it? An end-to-end encrypted messaging app scrambles all of your text messages so that external actors (like governments!) cannot read them.

- Download an end-to-end encrypted messaging app such as [Signal](#). WhatsApp is also encrypted, but it is owned by Meta. We advise against using Telegram for sensitive communications.

TIP: Some encrypted messaging apps offer even more privacy protections, such as the ability to auto-delete messages after a certain period of time.

Data, Brokers and Breaches

Take steps to understand what personal information is already available online and take action to remove it.

❑ 'Dox' yourself (not really)

What is it? Doxing is the publishing of private, sensitive info (home address, cell, ID#, etc.). By searching for yourself online, you can see what information about you is available and take steps to have it removed. For more, see "self-doxing" guide: <https://bit.ly/2TVS050>

- Google yourself and look past the first few pages of search results.
- Try other search engines. DuckDuckGo is a privacy-preserving search engine, and Yandex and Baidu are popular in Russia and China, respectively.
- Use "Google Dorking" tips to refine your search (<https://bit.ly/2Q27Hqm>). We especially recommend searching by filetype.
- [Reverse image search](#) – search your name → click on "Images" → right click on images of yourself → select "Search Google" to see where your images are being used
- [Google Alerts](#) – set up alerts for your name, cell, home address, and other sensitive info
- What to do if you find abusive content or private data: for social media, report it to the platform; for websites, [report it to Google](#) and also see data scrubbing below

TIP: In some countries, you may be able to use copyright law to remove an image of yourself online, but you will need to consult with a lawyer.

❑ Scrub your data

What is it? Data brokers are companies that collect your private information online and sell it to companies, individuals, or other data brokers, which can facilitate doxing. There are dozens of data brokers (such as Spokeo and White Pages). This is a problem mostly in the U.S.

- Scrub your data the hard, free way – opt out of each data broker site manually by using Yael Grauer's Big Ass Data Broker Opt-Out List: (<https://github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List>)
- You can also check out Consumer Reports' [Permission Slip app](#) which has free and paid data removal options
- Scrub your data the easy, paid way – pay for a data scrubber subscription such as [EasyOptOuts](#), [DeleteME](#) (discount code: PEN20), [Kanary](#), or [Optery](#)

TIP: If you choose to scrub your data yourself by opting out of each data broker manually, keep in mind that they may add your data again at a later date (ie, you cannot opt out in perpetuity). Set a calendar reminder to check on these sites biannually.

❑ Check for data breaches

What is it? Hackers break into companies and steal private information about their users, such as usernames and passwords (which can be used to hack into your accounts!).

- Check to see if any of your accounts were part of a data breach: <https://haveibeenpwned.com/>
- If you discover that one of your accounts was part of a data breach, change the password on that account and never use that password again.

TIP: Set up an alert to see if your accounts are part of future data breaches (see "Notify me" tab): <https://haveibeenpwned.com/>

Remove personal information from professional bios & Google

What is it? Information that you have shared in bios, professional pages, or other accounts online could become vectors for online abuse.

- Review all the places that you have posted your personal information (such as your birthday, home city, partner's name, etc.) and remove it
- While you are at it, take a look at what is [shared about you on Google](#). You might be able to remove sensitive information. Their new 'results about you' feature makes this even easier: <https://myactivity.google.com/results-about-you>

Review your mobile app permissions

What is it? Many mobile apps, including social media, are tracking your activity ALL the time.

- Check which apps you have given access to your contacts and location and revoke access where you can.


Social Media

Be strategic about which platforms you use for which purposes. If you're using a platform for personal reasons (eg, sharing photos with friends and family), tighten your privacy settings (see below). If you're using a platform professionally, you may decide to have the settings set to public – in that case, best not to include sensitive personal info and images (family member's names and photos, home address, cell, etc.).


These steps were adapted from two excellent resources: [The New York Times' Self-Doxing Guide](#) and Reuters' internal self-doxing training for staff.

Instagram Privacy Settings


Set a strong, unique password

- From your profile, tap  → *Accounts Center* → *Password and security* → *Change password*


Enable two-factor authentication

- From your profile, tap  → *Accounts Center* → *Password and security* → *Two-factor authentication*

Review where you are logged in and revoke unfamiliar sessions

- From your profile, tap  → *Accounts Center* → *Password and security* → *Where you're logged in*
 - Select any unknown devices and press "Log Out"

Revoke unauthorized applications that are linked to your account

- From your profile, tap  → *Your app and media* header → *Website Permissions* → *Apps and websites*

Turn on manual "Tags" approval

- From your profile, tap ☰ → *How others can interact with you* header → *Tags and mentions* → Manually Approve Tags
 - Toggle on tag controls
- ❑ Turn on manual “Mentions” approval
 - From your profile, tap ☰ → *How others can interact with you* header → *Tags and Mentions* → Allow mentions from people you follow
- ❑ Set account to private (if not for professional use)
 - From your profile, tap ☰ → *Who can see your content* header → *Account Privacy*
 - Toggle on Private account
- ❑ Remove any uploaded contacts and disable contact sync
 - From your profile, tap ☰ → *Accounts Center* → *Your information and permissions* → Upload Contacts
 - *Toggle off connect contacts*
- ❑ Allow political content
 - From your profile, tap ☰ → *What you see* header → *Content preferences* → *Political content* → *Select See more*
- ❑ Post quietly
 - This used to be a much easier feature on instagram, now it is a bit more complicated but still possible
 - From your profile, tap the “+” button in the middle at the bottom of the screen → select the photos you want to post → click “next” → “next” again, locate and click on the the “audience” button → select “close friends”
 - **Note:** Setting the post to “close friends” will still be visible to those who you have selected as close friends’ if you want to make it not appear for anyone, you will need to edit your close friends list and select one person that doesn’t follow you back (typically a celebrity or an account which would never look at your account) and the post will only appear to them
 - To edit close friends list, tap ☰ → navigate to “Close Friends” → select those you want in close friends

X/Twitter Privacy Settings

[Cyd.Social](#) and [Tweetdeleter](#) can help you to download an archive of your twitter data and delete likes and direct messages.

- ❑ Delete private information from your profile.

- ❑ Set your birthdate to “Only You” or leave it blank.
 - *Profile → Edit profile → Birth date*

- ❑ Set a strong, unique password
 - *Under More → Settings and privacy → Your account → Change your password*

- ❑ Enable two-factor authentication
 - *Under More → Settings and privacy → Security and account access → Security → Two-factor authentication*
 - Save backup codes somewhere safe (like password manager!)

- ❑ Enable password reset protection
 - *Under More → Settings and privacy → Security and account access → Security → Password reset protect*

- ❑ Review apps linked to your account (but not iOS!) & where you are logged in → revoke unfamiliar sessions & unauthorized apps
 - *Under More → Settings and privacy → Security and account access → Apps and sessions → Connected apps and Logged-in devices and apps*

- ❑ Consider limiting who can see your Tweets to people who follow you.
 - *Under More → Settings and privacy → Privacy and safety → Your X activity header → Audience and tagging → “Protect your Posts” and “Protect your Videos”*

- ❑ Adjust photo tagging (disable)
 - *Under More → Settings and privacy → Privacy and safety → Your X activity header → Audience, media and tagging → Photo tagging*



- ❑ Decide if you want to receive direct messages from anyone or just from your followers
 - *Under More → Settings and privacy → Privacy and safety → Your X activity header → Direct messages*
 - Consider disabling audio and video calling
 - *Settings and Support → Privacy and safety → Your X activity header → Direct Messages → Turn off “Enable audio and video calling”*

- ❑ Edit who can look up your profile using your email or phone number
 - *Under More → Settings and privacy → Privacy and safety → Your X activity header → Discoverability and contacts*

- ❑ Consider removing all contacts you’ve synced to Twitter, especially if they include sensitive sources

- *Under More → Settings and privacy → Privacy and safety → Your X activity header → Discoverability and contacts → Toggle off “Sync address book contacts” and (if needed) press “Remove all contacts”*
- ❑ Review your settings for Muted, Blocked, and Notifications
 - *Under More → Settings and privacy → Privacy and safety → Your X activity header → Mute and block*
 - What are my options? Blocked accounts, muted accounts, muted words, and muted notifications
- ❑ Disable precise location information on Tweets
 - *Under More → Settings and privacy → Privacy and safety → Data sharing and personalization header → Location information → Precise location*
- ❑ Consider turning off personalization based on inferred identity
 - *Under More → Settings and privacy → Privacy and safety → Data sharing and personalization header → Inferred identity*
- ❑ Consider turning off all targeted ads and personalization (less tracking = more random ads)
 - *Under More → Settings and privacy → Privacy and safety → Data sharing and personalization header → Ads preferences*

Facebook Privacy Settings

- ❑ Do a thorough check through [Facebook’s Privacy Checkup](#). Follow up with the instructions below.
- ❑ Check what private info you’ve made available on your profile (if public) and delete anything not strictly necessary. The path below lets you see your public profile as it appears to others. Be sure to set your birthdate to “Only You” or leave it blank.
 - Mobile: *Menu → Settings & privacy → Settings → Audience and visibility header → Profile details*
 - Desktop: Go to your Profile →  → View As  → *Edit Profile [if needed]*
- ❑ Set a strong, unique password
 - *Menu → Settings & privacy → Settings → See more in Accounts Center → Password and Security → Change Password*
- ❑ Enable two-factor authentication
 - *Menu → Settings & privacy → Settings → See more in Accounts Center → Password and Security → Two-factor authentication*
 - What are my options? SMS, Authentication App or Security Key

- Save recovery codes somewhere safe (like password manager!)
- ❑ Review where you are logged in and revoke unfamiliar sessions
 - *Menu → Settings & privacy → Settings → See more in Accounts Center → Password & Security → Where You're Logged In (See all)*
 - Review where you are logged in and revoke unfamiliar sessions
- ❑ Turn on login alerts
 - *Menu → Settings & privacy → Settings → See more in Accounts Center → Password & Security → Login alerts*
- ❑ Review the apps and websites that have access to your account and delete any not strictly necessary.
 - *Menu → Settings & privacy → Settings → See more in Accounts Center → Your information and permissions → Your activity off Meta technologies*
- ❑ Decide who can see future posts, past posts, and the people, pages, and lists you follow (recommended: friends)
 - *Menu → Settings & privacy → Settings → Audience and visibility header → Profile and Tagging → Viewing and sharing header*
- ❑ Hide your friend requests and friends list from Public view (recommended: friends)
 - *Menu → Settings & privacy → Settings → Audience and Visibility header → How People Find and Contact You → Your friends header*
- ❑ Edit who can look up your profile using your email or phone number (recommended: No one)
 - *Menu → Settings & privacy → Settings → Audience and visibility header → How people find and contact you → Who can Facebook suggest your profile to based on your phone number or email address? header*
- ❑ Disallow search engines from linking to your profile
 - *Menu → Settings & privacy → Settings → Audience and Visibility header → How people find and contact you → Do you want search engines outside of Facebook to link to your profile? header*
- ❑ Review who can post on your timeline and see what others post on your timeline (recommended: Only me/Friends)
 - *Menu → Settings & privacy → Settings → Audience and visibility header → Profile and tagging → Viewing and sharing header*
- ❑ Review who can see posts you're tagged in (recommended: only me/friends)
 - *Menu → Settings & privacy → Settings → Audience and visibility header → Profile and tagging → Tagging and implied mentions header*

- ❑ Approve posts and pictures you're tagged in before they appear on Facebook or your profile
 - *Menu → Settings & privacy → Settings → Audience and visibility header → Profile and Tagging → Reviewing header*

- ❑ Decide who can follow you and who can comment on your posts (recommended: Friends/Friends of friends)
 - *Menu → Settings & privacy → Settings → Audience & visibility header → Followers and public content*

- ❑ Review who can like or comment on your public profile info (recommended: Friends/Friends of friends)
 - *Menu → Settings & privacy → Settings → Audience and visibility header → Followers and public content → Who can comment on your public posts?*

- ❑ Turn off location services and location history
 - *Menu → Settings & privacy → Settings → Your Activity header → Device Permissions → Location → See info → Update settings*
 - Disable "Location Services" (Recommended: Never) and "Location History"

- ❑ Disable Off-Facebook Activity tracking and clear history
 - *Menu → Settings & privacy → Settings → See more in Accounts Center → Your information and permissions → Your activity off Meta technologies → Manage Future Activity → Disconnect future activity*

- ❑ Review ad preferences and turn off/don't allow (less tracking = less personalized ads)
 - *Menu → Settings & privacy → Settings → See more in Accounts Center → Ad Preferences → Manage info (check your preferences for each one)*

TIP: Be conscious of the privacy settings of friends you routinely interact with on Facebook. Your comments or likes on their pages, and their comments and likes on yours, may be discoverable. Even if you're not tagged, the truly dedicated may look through people connected to you, such as family and co-workers, or people who have interacted with public parts of your Facebook page, such as liking your cover picture or profile picture, in the hope of finding tidbits about you. While you may not have any control over your friends' settings, you can be mindful of your comments.

LinkedIn Privacy Settings







- ❑ Set a strong, unique password
 - *Click on your profile icon → Settings and Privacy → Sign in & security → Change password*




- ❑ Enable two-factor authentication

- Click on your profile icon → *Settings and Privacy* → *Sign in & security* → *Two-step verification*
 - What are my options? 😞 SMS or 😊 Authenticator App
- ❑ Review your active sessions and sessions that are unfamiliar
 - Click on your profile icon → *Settings and Privacy* → *Sign in & security* → *Where you're signed in*
- ❑ Consider toggling off sync calendar and contacts
 - Click on your profile icon → *Settings and Privacy* → *Account preferences* → *Syncing Options* header → *Sync Contacts* → *Manage all Synced Resources (remove all synced contacts or calendar)*
- ❑ Revoke access for any unauthorized applications that are linked to your account
 - Click on your profile icon → *Settings and Privacy* → *Account preferences* → *Partners & services* header
- ❑ Check what private info you've made available on your profile and delete anything not strictly necessary for professional networking. For example, you might want to remove your high school from LinkedIn.
 - Click on your profile icon → *Settings and Privacy* → *Visibility* → *Visibility of your profile & Network* header → *Edit your public profile* → *Edit Content*
- ❑ Consider disabling the visibility of your profile to non-LinkedIn users; Decide if you want your LinkedIn profile to appear on other partnered platforms and toggle "Off" under "Your Profile's Public Visibility" if you do not
 - Click on your profile icon → *Settings and Privacy* → *Visibility* → *Visibility of your profile & Network* header → *Edit your public profile* → *Edit Visibility* header
- ❑ Update the visibility of your email address or last name
 - Click on your profile icon → *Settings and Privacy* → *Visibility* → *Visibility of your profile & Network* header → *Who can see or download your email address/Who can see your last name*
- ❑ Consider limiting who can follow your updates
 - Click on profile icon → *Settings and Privacy* → *Visibility* → *Visibility of your LinkedIn activity* header → *Followers*
- ❑ Consider limiting who can see your connections, especially if you have connected with sensitive sources
 - Click on your profile icon → *Settings and Privacy* → *Visibility* → *Visibility of your profile & Network* header → *Who can see your Connections*
 - Toggle connection visibility on or off
- ❑ Edit who can look up your profile using your email or phone number

- Click on your profile icon → *Settings and Privacy* → *Visibility* → *Visibility of your profile & Network* header → *Profile discovery using email address/phone number*
- ❑ Review ad preferences and turn off/don't allow (less tracking = less personalized ads)
 - Click on your profile icon → *Settings and Privacy* → *Advertising data* → *Profile data/Activity and inferred data/Third-party data* (check your preferences for each one)
- ❑ Consider ensuring that when you view someone else's profile, they don't know it.
 - Click on your profile icon → *Settings and Privacy* → *Visibility* → *Visibility of your profile & Network* header → *Profile viewing options* → *Select Private Mode*

TikTok Privacy Settings

- ❑ Set a strong, unique password
 - From your profile, tap  → *Settings & Privacy* → *Account* → *Password* → [enter code that was sent to listed phone number] → *Change password*
- ❑ Enable two-factor authentication
 - From your profile, tap  → *Settings & Privacy* → *Security & permissions* → *2-step verification* → *select at least 2 verification methods (verification code on phone number/email or enter a password when you log in)*
 - Save backup codes somewhere safe (like a password manager!)
- ❑ Set account to private (If not being used in a professional manner)
 - From your profile, tap  → *Settings & Privacy* → *Privacy* → *Turn Private Account on or off*
- ❑ Check unusual account activity
 - From your profile, tap  → *Settings & Privacy* → *Security & permissions* → *Security alerts*
- ❑ Decide who can comment on your videos
 - From your profile, tap  → *Settings & Privacy* → *Privacy* → *Comments* → *Allow comments from* → *Toggle between "Everyone," "Followers that you follow back," and "No one"*
 - From your profile, tap  → *Settings & Privacy* → *Privacy* → *Comments* → *Filter keywords in comments* (you can also enable *Comment Care Mode*)
- ❑ Consider who can mention or tag you

- From your profile, tap  → *Settings & Privacy* → *Privacy* → *Mentions* → *Choose who can mention you in their descriptions, stickers, comments, and stories*
- ❑ Edit who can see your following list
 - From your profile, tap  → *Settings & Privacy* → *Privacy* → *Following list*
- ❑ Choose who can Duet with your videos
 - From your profile, tap  → *Settings & Privacy* → *Privacy* → *Reuse of content* → *Allow reuse of content from and Manage Duet and Stitch posts (if your account is Private, you can't Duet with others)*
- ❑ Edit who can send you Direct messages
 - *Settings & Privacy* → *Privacy* → *Direct Messages (you can enable filtered requests)*
- ❑ Manage app permissions
 - *Settings & Privacy* → *Security & Permissions* → *Apps & service permissions*
- ❑ Request your data
 - *Settings & Privacy* → *Account* → *Download your data*
- ❑ Review and Update your ads settings
 - *Settings & Privacy* → *Ads* → *How your ads are personalized/Mute Advertisers*
 - *Settings & Privacy* → *Ads* → *Manage your off-TikTok data* → *Toggle off "Targeted ads" AND clear off-TikTok data*

Venmo Privacy Settings

- ❑ Set account to private
 - From your profile, tap *me* → *Settings (gear icon)* → *Privacy* → *Toggle to "Private"*
- ❑ Set location to private
 - From your profile, tap *me* → *Settings (gear icon)* → *Privacy* → *Location* → *"Tap to go to app permissions"* → *Location* → *"Never"*
- ❑ Make past transactions private
 - From your profile, tap *me* → *Settings (gear icon)* → *Privacy* → *Past transactions* → *"Change all to private"*
- ❑ Turn off "Friends list" visibility

- From your profile, tap *me* → *Settings (gear icon)* → *Privacy* → *Friends list* → *Toggle to “Private”*
- ❑ Enable pin
 - From your profile, tap *me* → *Settings (gear icon)* → *Biometrics & Passcode* → *Enable Passcode (PIN)*

Bluesky Privacy Settings

- ❑ Delete private information from your profile.
- ❑ Set a strong, unique password
 - *Settings* → *Account* → *Password* → *Request Code*
- ❑ Enable two-factor authentication
 - *Settings* → *Privacy and Security* → *Two-factor authentication*
 - Save backup codes somewhere safe (like password manager!)
- ❑ Enable app passwords when logging into Bluesky on third-party applications
 - *Settings* → *Privacy and Security* → *App Passwords* → *Add App Password*
 - App Passwords are randomly generated every use and ensure you do not have to use your main login password
- ❑ Consider enabling Logged-out visibility so Bluesky does not show your profile and posts to logged-out users
 - *Settings* → *Privacy and Security* → *Toggle on Logged-out visibility*
 - **This is not the same as making your account private**
- ❑ Consider limiting who can interact with your posts
 - *Settings* → *Moderation* → *Moderation tools* header → *Interaction Settings* → *Reply settings* header → Consider allowing reply settings only from *Mentioned users*, *Users you follow*, and/or *Your followers*
 - You can also limit replies for specific posts
 - *Settings* → *Moderation* → *Moderation tools* header → *Interaction Settings* → *Quote settings* header → Toggle on or off *Allow quote posts*
- ❑ Consider turning off external media preferences
 - *Settings* → *Content and media* → *External media* → Toggle off all media players
- ❑ Consider exporting your public data records to review what information you’ve shared that can be publicly accessed
 - ❑ *Settings* → *Account* → *Export my data* → *Download CAR file*

Additional Resources

You made it all the way to the end, congratulations! In case you want to keep learning more, here are some resources to consider:

- PEN America Online Harassment Field Manual <https://onlineharassmentfieldmanual.pen.org/>
- PEN America Digital Safety Snacks <https://pen.org/digital-safety-snacks/>
- PEN America [What To Do If You've Been Doxed Or Put On A Watch List](#)
- [New York Times Self-Doxing Guide](#)
- Consumer Reports' [Security Planner](#)
- [Pirih Resource and Reporting Platform](#)
- [Freedom of the Press Foundation's Digital Security Guides and Resources](#)
- [Electronic Frontier Foundation's Surveillance Self-Defense](#)
- [Security-in-a-Box](#)
- [Access Now Digital Security Helpline](#)