



SOCIAL MEDIA SAFETY CHECKUP

Practical settings for Facebook, Messenger, Instagram, TikTok and X

DO THESE ON EVERY ACCOUNT

Settings vary by app, account type, device and region

- 1 Unique password**
Never reuse an email, banking or shopping password.
- 2 Second sign-in step**
Use a passkey, authenticator app or security key.
- 3 Review devices**
Sign out devices and locations you do not recognize.
- 4 Limit contact**
Restrict requests, comments, tags, calls and groups.
- 5 Reduce visibility**
Hide personal details; consider private accounts.
- 6 Remove connections**
Delete old apps; disable unneeded contact syncing.

f FACEBOOK AND MESSENGER

- 1 Run Privacy Checkup**
Menu > Settings & privacy > Privacy Checkup
Review sharing, discoverability, data and security.
- 2 Turn on two-factor authentication**
Accounts Center > Password and security
Prefer an authenticator app or security key; save recovery codes.
- 3 Review logged-in devices**
Accounts Center > Where you're logged in
Log out unfamiliar devices. Change the password if suspicious.
- 4 Limit posts and personal details**
Settings > Audience and visibility
Use Friends for personal posts; hide unneeded profile details.
- 5 Reduce requests and searches**
How people find and contact you
Limit requests and discovery by phone, email and search engines.
- 6 Approve tags first**
Profile and tagging
Turn on review for posts and tags before they appear.
- 7 Restrict Messenger requests**
Messenger > Privacy & safety > Message delivery
Send strangers to requests or choose Don't receive.
- 8 Remove apps; block suspicious accounts**
Settings > Your activity > Apps and websites
Remove unknown services. Block and report suspicious profiles.

IG INSTAGRAM

- 1 Consider a private account**
Settings and activity > Account privacy
Approve followers and remove people you do not know.
- 2 Turn on two-factor authentication**
Accounts Center > Password and security
Prefer an authenticator app; save recovery codes.
- 3 Review logged-in devices**
Accounts Center > Where you're logged in
Log out unfamiliar devices and change the password.
- 4 Control message requests**
Messages and story replies > Message controls
Restrict strangers, group adds and unexpected calls.
- 5 Limit tags and mentions**
Settings and activity > Tags and mentions
Allow people you follow or no one; approve tags manually.
- 6 Use Hidden Words**
Settings and activity > Hidden Words
Hide offensive comments and suspicious message requests.
- 7 Limit story visibility**
Settings and activity > Hide story and live
Use Close Friends; avoid public travel or live-location posts.
- 8 Remove connections**
Accounts Center > Your information and permissions
Review apps and contacts; block and report suspicious accounts.



SOCIAL MEDIA SAFETY CHECKUP

Reduce unwanted contact, public exposure and account takeover risk

T TIKTOK

- 1 Run Security checkup**
Settings and privacy > Security & permissions
Confirm recovery details and address every warning.
- 2 Turn on 2-step verification**
Security & permissions > 2-step verification
Choose at least two methods; never share a code.
- 3 Review trusted devices**
Security & permissions > Manage devices
Remove devices you do not recognize or use.
- 4 Consider a private account**
Privacy > Private account
Approve followers and keep sensitive details out of your bio.
- 5 Restrict direct messages**
Privacy > Direct messages
Use Requests or Don't receive for unfamiliar people.
- 6 Control comments, mentions and tags**
Privacy > Comments / Mentions and tags
Limit interactions and add keyword filters.
- 7 Turn off downloads**
Privacy > Downloads > Video downloads
Reduce strangers' ability to save and reuse your videos.
- 8 Restrict Duet, Stitch and reuse**
Privacy > Reuse of content
Limit reuse to Friends or Only you where available.

X X

- 1 Turn on two-factor authentication**
Security > Two-factor authentication
Use an authenticator app or security key when possible.
- 2 Review sessions and apps**
Security and account access > Apps and sessions
Log out unfamiliar sessions and revoke old apps.
- 3 Consider protecting posts**
Privacy and safety > Audience, media and tagging
Only approved followers see posts; review existing followers.
- 4 Restrict Direct Messages**
Privacy and safety > Direct Messages
Turn off requests from everyone unless needed for outreach.
- 5 Limit discoverability**
Privacy and safety > Discoverability and contacts
Disable discovery by email or phone; remove uploaded contacts.
- 6 Control photo tagging**
Audience, media and tagging > Photo tagging
Allow people you follow or turn tagging off.
- 7 Limit audio and video calls**
Direct Messages > Audio and video calling
Turn calls off or restrict callers and enhance privacy.
- 8 Block, report and filter**
Suspicious profile or post > More options
Report impersonation and deceptive pitches; mute repeated terms.

IF A FRIEND'S ACCOUNT MAY BE STOLEN

Stop the conversation. Do not send money or codes. Call the person using a number already in your contacts, then report and block the suspicious account.

IF YOUR ACCOUNT IS TAKEN OVER

Use the official recovery page, change reused passwords, sign out unknown devices, remove unfamiliar recovery details or apps, and turn on two-factor authentication.



FULL STEP-BY-STEP GUIDE
TNElderJusticeCoalition.org