Wigington Security Group

Privacy consulting for individuals and families

Social Media Privacy Configuration

Lock down Facebook, Instagram, Twitter, LinkedIn, TikTok, and more

What You'll Learn:

- Why default privacy settings are designed to expose you
- Platform-by-platform privacy hardening walkthroughs
- What data each platform collects and how to minimize it
- Privacy-first posting habits and operational security
- Managing location data, facial recognition, and tracking
- Dealing with third-party apps and advertisers
- When to delete accounts vs. lock them down

Platforms Covered:

- Facebook & Messenger
- Instagram
- Twitter/X
- LinkedIn
- TikTok
- Snapchat
- Reddit
- General principles for all platforms

February 2026 • 32 Pages • Free Download

wigingtonsecurity.com

Contents

1 Understanding Social Media Privacy

1.1 The Privacy Paradox

Social media platforms have a fundamental business conflict:

- **You think** social media is free
- **Reality:** You are the product being sold
- **Customer:** Advertisers buying access to your attention and data
- **Business model:** Maximize data collection, maximize engagement, maximize ad revenue

CRITICAL

Every feature, every default setting, every design choice is optimized to:

1. Keep you scrolling longer
2. Collect more data about you
3. Share your information more broadly
4. Make privacy settings difficult to find and use

Privacy is not an accident—lack of privacy is the business model.

1.2 What's at Stake

1.2.1 Data Collection Scope

Social media platforms collect far more than your posts:

Category	What They Collect
Identity	Name, email, phone, birthdate, photos, biometric data (facial recognition)
Location	GPS coordinates, IP address, WiFi networks, check-ins, location tags in photos
Contacts	Phone contacts, email contacts, who you message, call logs
Behavior	Every click, scroll, pause, like, hover, time spent on each post
Connections	Your entire social graph—who you know, how you know them, relationship strength
Interests	Pages followed, groups joined, ads clicked, searches performed
Device Info	Phone model, OS version, browser, screen size, battery level, storage space
Off-Platform	Websites visited (via tracking pixels), purchases made, apps used
Communications	Message content (on some platforms), call duration, video chat participants
Media	Photos uploaded (even if not posted), videos watched, time spent on each video
Financial	Payment methods, purchase history, cryptocurrency holdings (some platforms)
Predictions	Inferred ethnicity, political views, income level, life events, mental health

1.2.2 Who Gets Your Data

Your data is shared with:

- **Advertisers:** Thousands of companies buy targeting access

- **Data brokers:** Aggregate and resell your profile
- **Third-party apps:** Games, quizzes, services you connect
- **Law enforcement:** Government requests for user data
- **Business partners:** Cross-platform tracking consortiums
- **Researchers:** Academic studies (often inadequately anonymized)
- **Bad actors:** Data breaches expose everything to criminals

1.2.3 Real-World Consequences

Personal safety risks:

- Stalkers use location data to track victims
- Burglars know when you're on vacation (posts, check-ins)
- Abusers locate people who have fled
- Kidnappers target children based on public photos and routines

Financial and professional risks:

- Employers screen candidates via social media
- Insurance companies adjust rates based on posts
- Landlords deny applications based on profiles
- Identity thieves use personal details for social engineering
- Scammers craft convincing phishing using your data

Privacy erosion:

- Your data creates permanent digital dossier
- AI trains on your content without compensation
- Facial recognition links your face across the internet
- Political microtargeting manipulates your views
- Future employers/partners can access your entire history

1.3 The Deletion vs. Lockdown Decision

Before hardening privacy, decide: stay or delete?

1.3.1 Consider Deleting If:

- You rarely use the platform (less than once a month)
- It causes more stress than value
- You have no professional need for it
- The platform's data practices are unacceptable to you
- You can maintain relationships through other means
- You're in high-risk situation (stalking, harassment)

Platforms most people can delete:

- Facebook (unless required for work/community groups)
- Twitter/X (unless professional need)
- TikTok (minimal professional utility)
- Snapchat (younger users may have social pressure)

1.3.2 Keep and Harden If:

- Professional networking is essential (LinkedIn)
- Business/brand presence required
- Primary communication with family/friends
- Community groups you value are platform-dependent
- Job searching requires visibility
- You use it mindfully and get value

Platforms worth hardening rather than deleting:

- LinkedIn (professional networking)
- Instagram (if managed carefully)
- Facebook (for groups/events only)
- Reddit (pseudonymous, community value)

Pro Tip

The middle path: Deactivate temporarily
Most platforms let you deactivate (hide your account) without fully deleting:

- Try 30 days deactivated
- See if you miss it
- If not, proceed to full deletion
- If you miss specific features, reactivate and harden privacy instead

This is a low-risk way to test life without a platform.

1.4 Privacy Hardening Philosophy

You cannot make social media truly private. The platforms are designed for sharing. But you can:

1. **Minimize data collection:** Disable tracking where possible
2. **Limit audience:** Control who sees what you post
3. **Reduce attack surface:** Remove unnecessary personal information
4. **Practice operational security:** Think before posting
5. **Audit regularly:** Settings change, new features add new exposure

Goal: Use social media on your terms, not the platform's.

2 Facebook Privacy Configuration

Facebook is the most data-hungry platform. This is the most important section.

2.1 Pre-Configuration Audit

Before changing settings, understand what Facebook already knows:

Action Items

Download your Facebook data:

Settings & Privacy → Settings → Your Facebook Information

Download Your Information → Request Download

Select: All data, JSON format, High quality media

Wait for download link (emailed within 48 hours)

Review what they have on you (prepare to be shocked)

What you'll find in your download:

- Every message you've ever sent (even "deleted" ones)
- Complete ad targeting profile
- Every advertiser who has your contact information
- Location history from your phone
- Facial recognition data
- Off-Facebook activity (websites visited)
- Shadow profile data from non-users who uploaded your contact info

2.2 Privacy Settings Walkthrough

Access main privacy settings: **Settings & Privacy → Settings → Privacy**

2.2.1 Who Can See What You Share

Settings → Privacy → Your Activity

Action Items

Configure these settings:

Who can see your future posts? → Friends

- Default is "Public"—change immediately
- Never leave as "Public" unless you understand implications

Review all your posts and things you're tagged in → Do this now

- Click "Limit Past Posts" to make all old public posts Friends-only
- Review tagged photos and remove tags where inappropriate

Who can see the people, Pages and lists you follow? → Only me

- Your follows reveal your interests, politics, beliefs
- No reason for this to be public

Who can see your story? → Friends or specific list

Who can see your friends list? → Only me

- Huge privacy leak—reveals your social graph
- Scammers use this to impersonate mutual friends
- No legitimate reason for this to be public

2.2.2 How People Find and Contact You

Settings → Privacy → How People Find and Contact You

Action Items

Who can send you friend requests? → Friends of friends

- "Everyone" allows random strangers
- Friends of friends is reasonable middle ground

Who can see your email address? → Only me

Who can see your phone number? → Only me

Who can look you up using email? → Friends

- "Everyone" means anyone with your email can find you
- Friends is more restrictive
- "Only me" breaks some legitimate friend discovery

Who can look you up using phone number? → Friends

Do you want search engines outside Facebook to link to your profile? → NO

- Prevents Google from indexing your profile
- Critical privacy protection

2.3 Profile and Tagging Settings

Settings → Profile and Tagging

Action Items

Who can post on your profile? → Friends or Only me

- "Only me" prevents friends from posting spam/embarrassing content

Who can see posts you're tagged in on your profile? → Friends

Review posts you're tagged in before they appear? → ON

- Critical: prevents auto-tagging in embarrassing photos
- You approve each tag before it shows on your profile

Review tags people add to your posts? → ON

Who can see posts you're tagged in? → Friends

When you're tagged, who can see it? → Friends

2.4 Location Services

Settings → Location

Action Items

Location Services → OFF

- Facebook doesn't need your precise location
- Delete location history: Settings → Location → Location History → Delete

Location History → OFF

Warning

Facebook tracks location even with this off—via IP address, WiFi networks, and photos with GPS data. But disabling prevents *precise* location tracking and historical logging.

2.5 Face Recognition

Settings → Face Recognition

☑ Action Items

Face recognition → NO

- Prevents Facebook from creating facial template
- Disables auto-tagging in photos
- Reduces ability to track you across photos

2.6 Apps and Websites

This is where huge data leaks happen.

Settings → Apps and Websites

☑ Action Items

Review all connected apps → Remove everything you don't actively use

- Click each app → Remove
- Apps can access: profile info, friends list, email, photos
- "Login with Facebook" is convenient but privacy disaster

Apps others use → Turn OFF all toggles

- Critical: prevents your friends' apps from accessing your data
- Your friends playing Candy Crush shouldn't access your info

Business integrations → Review and remove

Instant Games → If you don't play games, remove all

2.7 Ad Preferences

You can't stop Facebook ads, but you can limit targeting data.

Settings → Ads

☑ Action Items

Ad settings → Ad topics → See fewer of sensitive categories

- Alcohol, parenting, pets, politics, dating, gambling, etc.
- Click "See fewer" for categories you don't want targeted

Advertisers with your contact info → Review list

- Shows who uploaded your phone/email for targeting
- Usually hundreds or thousands of companies
- You can't fully opt out but can see who has your data

Your activity off Facebook → Manage

- See which websites report your activity to Facebook
- Clear history → Disconnect future activity

Data about your activity from partners → Turn OFF

2.8 Additional Security Settings

Settings → Security and Login

☑ Action Items

Two-factor authentication → ON

- Use authentication app (not SMS)
- Save recovery codes

Get alerts about unrecognized logins → ON

Review where you're logged in → Remove old sessions

Choose friends to contact if you get locked out → Select 3-5 trusted friends

2.9 Public Profile Cleanup

Make your profile less revealing:

Action Items

Edit Profile → Customize Your Intro:

- Remove or hide: Work, Education, City, Hometown, Relationship Status
- Remove phone number and email from public view
- Hide birthday (at minimum, hide year)
- Remove political views, religious views
- Set "About" section visibility to Friends or Only Me

Review Photos:

- Change old albums to Friends-only or delete
- Remove profile pictures that reveal location or family
- Delete photos with geolocation data

Posts and Activity:

- Use Activity Log to review and delete old posts
- Remove check-ins revealing home/work locations
- Delete posts revealing travel plans, daily routines

2.10 Facebook-Specific Best Practices

2.10.1 What to Never Post on Facebook

Warning

Never post:

- Real-time location or check-ins at home
- "Out of town" posts (advertises empty house to burglars)
- Children's full names, schools, or routines
- Photos with street signs, house numbers, or license plates visible
- Vacation plans before the trip (wait until you return)
- Relationship drama or employer complaints
- Financial information (purchases, income, debts)
- Health information (can affect insurance)
- Participation in protests or controversial events
- Anything you wouldn't want your employer, family, or future self to see

2.10.2 Friend List Hygiene

- Review friends list quarterly
- Remove: People you don't know, distant acquaintances, former colleagues
- Create custom friend lists for selective sharing:
  - Close Friends
  - Family
  - Work (separate from personal)
  - Restricted (see only public posts)
- Use "Acquaintances" list for people you want to stay connected with but share less

3 Instagram Privacy Configuration

Instagram (owned by Facebook/Meta) is photo-centric with different privacy concerns.

3.1 Account Privacy

Settings → Privacy

☑ Action Items

Account Privacy → Private Account

- Makes your account private (only approved followers see posts)
- Critical if you post personal content
- If you need public for business, be very selective about what you post

Activity Status → OFF

- Hides "Active now" and "Active today" status
- Prevents people from tracking your usage patterns

Story Sharing → Don't allow sharing

- Prevents people from sharing your Stories to their Stories

Allow story resharing → OFF

3.2 Interactions

Settings → Privacy → Interactions

☑ Action Items

Comments → Filter by keywords, hide offensive comments

Tags → Manually approve tags

Mentions → Allow from people you follow only

Messages → Don't receive requests from everyone

- Set to "People you follow" or "No one"
- Reduces spam and unwanted contact

Story replies → Allow from followers you follow back

3.3 Reels and Remix

Settings → Privacy → Reels and Remix

Action Items

Allow remixing → OFF

- Prevents others from creating content using your videos

Show account in remix suggestions → OFF

3.4 Photos and Videos

Settings → Privacy → Photos and Videos

Action Items

Hide story and live → Add people you want to hide from

Allow saving → Consider turning OFF

- Prevents people from bookmarking your posts
- More privacy but reduces engagement

3.5 Location Services

Settings → Privacy → Location

Action Items

Location Services → Never

- Or "While Using" if you must use location features
- Never allow "Always"

Don't add location to posts

- Especially never tag your home or work
- If tagging, use general area not specific location

3.6 Connected Accounts

Settings → Account Center → Accounts

Action Items

- Review linked Facebook account
- Consider unlinking if you don't need cross-posting
- Data sharing across Meta apps is extensive—minimize when possible

3.7 Data Download and Review

Settings → Security → Download Data

Action Items

- Request download to see what Instagram has on you
- Review: Messages, searches, location data, ad targeting
- Delete old data you no longer want stored

3.8 Instagram-Specific Privacy Habits

3.8.1 Photo Metadata Removal

Before posting photos:

- Strip EXIF data (GPS location, camera model, timestamp)
- Use tools: ExifTool, Metapho (iOS), Photo Exif Editor (Android)
- Instagram strips some metadata but not all
- Better to remove before upload

3.8.2 Story Privacy

- Stories disappear after 24 hours but are saved by Instagram
- Can still be screenshot by viewers
- Use "Close Friends" list for more personal Stories
- Never post home address, routine, or real-time location in Stories

3.8.3 Follower Vetting

- Review follower requests carefully
- Look for: No posts, no followers, stock photo profile, generic username
- These are often fake accounts, bots, or scammers
- Remove suspicious followers: Settings → Privacy → Blocked Accounts

4 Twitter/X Privacy Configuration

Twitter/X is more public by nature but still needs privacy hardening.

4.1 Privacy and Safety Settings

Settings → Privacy and Safety

☑ **Action Items**

Protect your posts → Turn ON for private account

- Makes account private (approve followers)
- Most users keep Twitter public—understand the tradeoffs

Photo tagging → Don't allow anyone to tag you

Direct Messages → Receive from people you follow only

Read receipts → OFF

- Prevents people from seeing when you read their DMs

4.2 Discoverability and Contacts

Settings → Privacy and Safety → Discoverability

☑ **Action Items**

Let people find you by email → OFF

Let people find you by phone → OFF

Sync address book contacts → OFF

- Never let Twitter upload your contacts
- Exposes your social graph

4.3 Location Information

Settings → Privacy and Safety → Location

Action Items

Precise location → OFF

Add location to tweets → OFF

Delete all location history

- Settings → Location → Delete location information

4.4 Data Sharing and Personalization

Settings → Privacy and Safety → Data Sharing

Action Items

Allow additional information sharing → OFF

Personalized ads → OFF

- You'll still see ads, just less targeted

Your advertiser list → Review and opt out

Inferred interests → Review and remove

4.5 Off-Twitter Activity

Settings → Privacy and Safety → Off-Twitter Activity

Action Items

Review which websites share your activity with Twitter

Disconnect data sharing for partners

Turn off future tracking where possible

4.6 Connected Apps

Settings → Security and Account Access → Apps and Sessions

Action Items

Review all connected apps

Revoke access for apps you don't use

Check permissions for remaining apps (minimize read/write access)

4.7 Security

Settings → Security and Account Access

Action Items

Two-factor authentication → ON

- Use authentication app or security key
- Avoid SMS (SIM swap risk)

Login verification → Enable

Password reset protection → Require email or phone

4.8 Twitter/X Privacy Habits

4.8.1 Think Before Tweeting

Warning

Twitter is the most public platform:

- Tweets are indexed by Google
- Screenshots live forever
- Deleted tweets can be retrieved from archives
- Employers routinely screen Twitter history
- Everything you tweet is permanently public record

Rule: Don't tweet anything you wouldn't say in a job interview.

4.8.2 Pseudonymous Accounts

Consider using pseudonymous account:

- No real name
- No personal photos
- Separate email address
- Don't link to other social media
- Allows freer expression without career/personal risk

4.8.3 Periodic Tweet Deletion

- Use tools like TweetDelete to auto-delete old tweets
- Keep tweets less than 6–12 months old
- Reduces your permanent digital footprint
- If you tweeted something controversial, delete it immediately

5 LinkedIn Privacy Configuration

LinkedIn is professional networking—different privacy calculus but still important.

5.1 Visibility Settings

Settings → Visibility

☑ Action Items

Profile viewing options → Private mode

- Tradeoff: Others won't see you viewed their profile
- But you also browse anonymously
- Good for job searching without alerting current employer

Edit your public profile

- Review what's visible to non-connections
- Consider hiding: Full work history, connections, recommendations

Who can see your connections → Only you

- Prevents connection list from being visible
- Stops recruiters from poaching your network

Who can see your last name → Connections only

Representing your organization → Turn OFF

5.2 Communications

Settings → Communications

☑ Action Items

Who can reach you → Set to Connections or Connections + InMail

Invitations to connect → Only people who know your email

Messaging experience → Control read receipts and typing indicators

Research invites → Turn OFF

5.3 How Others See Your Activity

Settings → Visibility → Activity

Action Items

Share profile updates → Turn OFF

- Prevents notification to network when you update profile
- Critical when job searching

Notify connections when you're in the news → Turn OFF

Mentions or tags → Control who can mention you

5.4 Data Privacy

Settings → Data Privacy

Action Items

How LinkedIn uses your data

- Review ad settings
- Opt out of ad tracking where possible

Job seeking preferences → Private to recruiters

- If actively searching, set preferences
- Make sure current employer can't see

Salary data → Don't share unless comfortable

5.5 Blocking and Hiding

Settings → Blocking and Hiding

Action Items

Block unwanted connections (former bosses, competitors)

Hide connections from specific people

Review followers and remove suspicious accounts

5.6 LinkedIn Privacy Considerations

5.6.1 Profile Completeness vs. Privacy

Balance professional visibility with privacy:

- **Include:** Current role, skills, education, summary
- **Consider excluding:** Full work history, exact dates, personal interests
- **Definitely exclude:** Phone number, full address, birthday, personal email

5.6.2 Connection Hygiene

- Only connect with people you actually know professionally
- Ignore random recruiter spam
- Review connections quarterly, remove dead connections
- Never upload contact list to LinkedIn

5.6.3 Posting Best Practices

- Assume every post is visible to current/future employers
- Keep it professional—no politics, religion, controversial topics
- Think: "Would I say this in a company all-hands meeting?"
- Use "Share with Connections" not public when possible

6 TikTok Privacy Configuration

TikTok collects enormous amounts of data. Consider deleting rather than hardening.

6.1 Privacy Settings

Settings → Privacy

☑ Action Items

Private account → Turn ON

- Makes all videos private by default
- Approve each follower
- Essential for personal accounts

Suggest your account to others → Turn OFF

Who can view your videos → Friends (if private account)

Who can comment → Friends or No one

Who can Duet/Stitch → No one

Who can send you messages → Friends or No one

6.2 Data Collection Controls

Settings → Privacy → Personalization and Data

☑ Action Items

Personalized ads → Turn OFF

Ad authorization → Revoke all

Download your data → Request to see what they have

- Review: Videos watched, searches, messages, IP addresses
- TikTok data collection is extensive

6.3 Discoverability

Settings → Privacy → Discoverability

☑ Action Items

Sync contacts → OFF

Find by phone/email → Turn OFF

Allow others to find you → Turn OFF

6.4 Location Services

Phone Settings → TikTok → Location

☑ Action Items

Set to Never

- TikTok doesn't need your location
- Reduces tracking and data collection

6.5 TikTok: Delete vs. Harden Decision

CRITICAL

Consider deleting TikTok if:

- You're concerned about Chinese government data access
- You have security clearance or sensitive job
- You value privacy over entertainment
- You can consume content elsewhere (YouTube Shorts, Instagram Reels)

TikTok's data collection exceeds most platforms. The app has access to:

- Clipboard contents (can read passwords you copy)
- Biometric data (facial recognition, voice)
- Precise location history
- Contact lists
- Calendar data
- And much more

TikTok is banned on government devices in many countries for good reason.

7 Other Platforms: Quick Reference

7.1 Snapchat

Snapchat Privacy

☑ Action Items

Settings → Who Can... → Contact Me: Friends only

Who Can... → View My Story: Friends only

Who Can... → See My Location: Ghost Mode (always)

Snap Map → Ghost Mode (prevents real-time location sharing)

See Me in Quick Add → Turn OFF

Ad Preferences → Opt out of personalized ads

Memories → Never save to Camera Roll (reduces data exposure)

Snapchat-specific risks:

- Screenshots of "disappearing" messages
- Snap Map reveals precise real-time location
- Facial recognition (filters) builds biometric profile
- Popular with younger users—teach children privacy settings

7.2 Reddit

Reddit Privacy

☑ Action Items

User Settings → Profile → Content visibility: Hide

Show active communities: OFF

Personalized ads: OFF

Location services: Never allow

Connected accounts: Disconnect Google/Apple

Search history: Delete regularly

Use throwaway accounts for sensitive posts

Reddit privacy tips:

- Create separate accounts for different topics
- Never use real name in username
- Don't link to other social media
- Delete posts with identifying information after getting answers
- Use Reddit primarily in pseudonymous mode
- Review post history quarterly and delete old posts

7.3 WhatsApp

WhatsApp Privacy

☑ Action Items

Settings → Privacy → Last Seen: My Contacts or Nobody

Profile Photo: My Contacts

About: My Contacts

Status: My Contacts

Read Receipts: Turn OFF

Groups: My Contacts (who can add you)

Live Location: Never share

WhatsApp considerations:

- End-to-end encrypted (messages secure)
- But metadata shared with Facebook/Meta
- Contact list uploaded to Meta servers
- Consider Signal or Telegram for more privacy

7.4 Telegram

Telegram Privacy

Action Items

Settings → Privacy → Phone Number: Nobody

Last Seen: Nobody

Profile Photo: My Contacts

Groups: My Contacts

Use Secret Chats for sensitive conversations

- End-to-end encrypted
- Self-destruct timers

7.5 Discord

Discord Privacy

Action Items

User Settings → Privacy → Allow DMs from server members: OFF

Use server-specific nicknames: ON

Activity Privacy → Display current activity: OFF

Use privacy controls: Restrict who can add you as friend

Connected accounts: Disconnect unnecessary integrations

Two-factor authentication: Enable

8 Universal Social Media Privacy Principles

These apply to ALL platforms, current and future.

8.1 The Five Privacy Principles

8.1.1 1. Minimize Data Collection

- Turn off location services for all social media apps
- Don't upload contact lists
- Deny permissions the app doesn't need (microphone, camera when not in use)
- Use app in browser instead of installing app (more privacy)
- Clear app cache and data regularly

8.1.2 2. Limit Your Audience

- Default to private accounts or friends-only posts
- Never post publicly unless you have specific reason
- Use friend lists/close friends for selective sharing
- Review who can see what quarterly
- Remove followers/friends you don't know

8.1.3 3. Think Before Posting

☑ Action Items

Before posting anything, ask:

Would I be comfortable with my employer seeing this?

Would I be comfortable with this on the front page of a newspaper?

Could this information be used against me or my family?

Am I revealing location, routine, or security information?

Will I regret this in 5 years? 10 years?

Is this worth the permanent digital record?

8.1.4 4. Control Third-Party Access

- Never use "Login with Facebook/Google" for other services
- Review and remove connected apps monthly
- Deny app permissions that aren't essential

- Don't play games or take quizzes that request data access
- Revoke access for services you no longer use

8.1.5 5. Audit Regularly

Action Items

Monthly:

- [ ] Review connected apps and revoke unused ones
- [ ] Check who you're following and who follows you
- [ ] Review recent posts for privacy leaks

Quarterly:

- [ ] Complete privacy settings review (use this guide)
- [ ] Remove/unfriend inactive or unknown connections
- [ ] Delete old posts revealing personal information
- [ ] Update security settings and password

Annually:

- [ ] Download your data to see what platform has
- [ ] Decide: Keep using this platform or delete?
- [ ] Review all privacy settings from scratch
- [ ] Update recovery email and phone number

8.2 What Never to Post

Warning

NEVER post:

1. **Real-time location** — "At the beach!" = not home = house empty
2. **Travel plans before trip** — Wait until you return to post vacation photos
3. **Children's schools, routines, or full names**
4. **Home address indicators** — Street signs, house numbers, landmarks
5. **Work complaints or confidential information**
6. **Financial information** — Income, purchases, debts, account numbers
7. **Medical information** — Can affect insurance, employment
8. **Documents with personal info** — Tickets, IDs, bills
9. **Boarding passes or travel documents**
10. **Answers to security questions** — Pet names, mother's maiden name, first car
11. **Photos with metadata** — Strip EXIF data first
12. **Check-ins at home or work**

8.3 Photo Privacy

8.3.1 Before Posting Photos

Action Items

- [ ] Remove EXIF data (GPS, camera info, timestamp)
- [ ] Check background for identifying information
- [ ] Blur faces of people who haven't consented
- [ ] Crop out street signs, house numbers, license plates
- [ ] Consider: Could this photo be used to locate me?

8.3.2 Children's Photos

CRITICAL

Special considerations for posting children:

- Children can't consent to having their lives documented publicly
- Photos create permanent digital identity they don't control
- Predators use social media to target children
- School names, uniforms, routines reveal dangerous information
- Consider: Would you want your childhood documented online?

Recommendations:

- Never post photos showing school name, uniform, or location
- Don't post daily routines (bus stop times, activity schedules)
- Use private sharing (Google Photos shared albums, not social media)
- Face away from camera or crop face
- Never include full name in posts with photos
- Set very strict audience (close family only)

9 Social Media Operational Security

9.1 Account Security

Action Items

Essential security measures for every platform:

- Unique password (use password manager)
- Two-factor authentication enabled (app-based, not SMS)
- Security key registered (YubiKey for high-value accounts)
- Recovery email is secure, private, monitored
- Recovery phone number is accurate
- Login alerts enabled
- Review active sessions monthly
- Log out of old devices/browsers

9.2 Recognizing Social Engineering

Social media is prime hunting ground for scammers.

9.2.1 Friend Request Red Flags

Warning

Suspicious friend requests:

× Profile photo is stock image or celebrity

× Almost no posts or very recent account creation

× Few or no mutual friends

× Generic name ("Sarah Johnson")

× Inconsistent information (says lives in US but broken English)

× Immediate message after accepting ("Hi dear, how are you?")

× Profile seems too good to be true (attractive, successful, interested in you)

These are usually: Scammers, catfish, bots, or data harvesters.

9.2.2 Message Scam Patterns

- **Impersonation:** "This is Facebook Support, your account will be deleted..."

- **Urgency:** "Click this link in 24 hours or lose access..."
- **Too good to be true:** "You won a prize! Claim here..."
- **Romance scams:** Fast-moving relationship, then financial request
- **Investment scams:** "I made $10K with this crypto method..."
- **Fake job offers:** "Work from home $5000/week..."

Rule: If unsolicited, unexpected, or urgent → it's a scam.

9.3 Device Security for Social Media

9.3.1 Mobile App Security

☑ Action Items

Download apps only from official stores

Review app permissions regularly

- iOS: Settings → [App] → Permissions
- Android: Settings → Apps → [App] → Permissions

Deny unnecessary permissions (microphone, location, contacts)

Enable biometric login (Face ID, fingerprint)

Don't save login credentials in browser

Clear cache and data quarterly

Update apps promptly (security patches)

9.3.2 Browser Security

☑ Action Items

Use private/incognito mode for social media browsing

Install privacy extensions:

- uBlock Origin (ad blocking)
- Privacy Badger (tracker blocking)
- Facebook Container (isolates Facebook tracking)

Clear cookies and cache weekly

Disable third-party cookies

Use browser password manager or dedicated password manager

9.4 Public WiFi Precautions

Warning

On public WiFi:

- Use VPN before accessing social media
- Don't log in to social media on untrusted networks
- Enable HTTPS-only mode in browser
- Disable auto-connect to WiFi networks
- Turn off WiFi when not needed (prevents tracking)

10 Account Deletion Guide

Decided to delete? Here's how to do it properly.

10.1 Pre-Deletion Checklist

Action Items

Before deleting any account:

- Download your data (photos, posts, messages you want to keep)
- Inform close friends/family of your departure
- Save contact information for people you want to stay in touch with
- Remove account from other services using it for login
- Disconnect linked apps and services
- Delete old posts manually if you want them gone faster
- Consider deactivating for 30 days first (trial run)

10.2 Platform-Specific Deletion

10.2.1 Facebook

1. Download your data first (Settings → Your Facebook Information → Download)
2. Settings → Your Facebook Information → Deactivation and Deletion
3. Select "Permanently delete account"
4. Click "Continue to account deletion"
5. Enter password and click "Continue"
6. Click "Delete Account"
7. You have 30 days to change your mind (don't log in)
8. After 30 days, deletion is permanent

Note: Messages you sent to others remain in their inboxes.

10.2.2 Instagram

1. Must use browser (can't delete from app)
2. Go to: https://www.instagram.com/accounts/remove/request/permanent/
3. Select reason for leaving
4. Re-enter password

5. Click "Permanently delete my account"
6. Account disabled immediately, deleted after 30 days

10.2.3 Twitter/X

1. Settings → Your account → Deactivate your account
2. Read information and click "Deactivate"
3. Enter password and click "Deactivate account"
4. Account deactivated for 30 days
5. Don't log in for 30 days for permanent deletion
6. After 30 days, deletion is complete

10.2.4 LinkedIn

1. Settings → Account preferences → Account management
2. Click "Closing your LinkedIn account"
3. Select reason
4. Enter password
5. Click "Close account"
6. Deletion is immediate (no grace period)
7. Download data first if you want to keep it

10.2.5 TikTok

1. Profile → Menu (3 lines) → Settings and privacy
2. Account → Delete account
3. Follow prompts
4. Account deactivated for 30 days
5. After 30 days, permanently deleted

10.3 Post-Deletion Cleanup

Action Items

After deleting account:

- Clear browser cookies for that site
- Uninstall mobile apps
- Remove email forwarding rules (if any)
- Check data broker sites—your profile may still exist
  - Use our guide: *Complete Data Broker Removal*
- Search your name on Google—old cached posts may appear
- Request removal of cached pages from Google
- Monitor for impersonation accounts after deletion

10.4 Alternatives to Full Deletion

10.4.1 Deactivation (Temporary)

Most platforms allow deactivation:

- Account hidden but not deleted
- Can reactivate anytime by logging in
- Good for testing life without the platform
- Recommended: Try 30-day deactivation before permanent deletion

10.4.2 Extreme Privacy Lockdown

If you must keep account but want maximum privacy:

- Delete all posts, photos, and personal information
- Change profile photo to generic image
- Remove name, location, work, education
- Set everything to private/friends only
- Unfollow everyone
- Remove all followers
- Use account only for specific groups or features
- Check in once a month to maintain access

This creates "ghost account"—technically exists but has no data.

11 Complete Privacy Hardening Checklist

11.1 Platform-by-Platform Checklist

Action	FB	IG	TW	LI	TT	SC
Private account					N/A	
2FA enabled						
Location off						
Face recognition off		N/A	N/A	N/A	N/A	N/A
Contact sync off						
Third-party apps removed					N/A	N/A
Search engine indexing off			N/A		N/A	N/A
Ad personalization off						
Download data reviewed						N/A
Old posts deleted/hidden						N/A
Profile info minimized						
Friends/followers pruned						

11.2 Ongoing Maintenance

Action Items

Weekly:

- Review what you posted this week—anything too revealing?
- Check friend/follower requests
- Be mindful of what you're sharing

Monthly:

- Review connected apps and revoke unused ones
- Check login sessions and log out old devices
- Review followers/friends—remove suspicious accounts
- Audit recent posts for privacy issues

Quarterly:

- Complete privacy settings review (use this guide)
- Update passwords for all social media accounts
- Review and tighten audience settings
- Delete old posts with personal information
- Check what Google shows for your name

Annually:

- Download data from each platform to see what they have
- Decide: Keep using each platform or delete?
- Complete privacy audit from scratch
- Review all profile information
- Update recovery information
- Consider: Has my threat model changed?

11.3 Success Metrics

You've successfully hardened your social media privacy when:

Action Items

- Strangers cannot see your posts or profile information
- Your address, phone, email are not publicly visible
- Location services are disabled on all social apps
- You have fewer than 10 connected third-party apps (ideally zero)
- Search engines don't index your profile
- You think carefully before posting anything personal
- Your friends list contains only people you know
- Ad targeting is minimal (generic ads vs. creepily specific)
- You've enabled 2FA on every platform
- You're comfortable with everything currently posted

12 Conclusion: Taking Back Control

12.1 The Bottom Line

Social media companies profit from your data. Every feature, every default setting, every design choice is optimized to extract maximum information from you.

But you have power:

- **Power to configure:** Use privacy settings aggressively
- **Power to limit:** Post less, share carefully
- **Power to delete:** Remove platforms that don't serve you
- **Power to choose:** Decide which platforms are worth the privacy cost

12.2 Realistic Expectations

You cannot make social media truly private. The platforms are designed for sharing. But you can:

- Dramatically reduce your exposure
- Control who sees what
- Minimize data collection
- Make yourself a harder target
- Use platforms on your terms, not theirs

Perfect privacy is impossible. Better privacy is always achievable.

12.3 Behavioral Change Matters More Than Settings

Settings are important, but behavior is critical:

- **Think before posting**—this is 80% of privacy
- **Assume everything is public**—even with privacy settings
- **Post less**—the best privacy is not posting
- **Question your habits**—do you need to share this?
- **Teach others**—help family and friends protect themselves

12.4 Next Steps

1. **This week:** Configure privacy settings on your top 2 platforms
2. **This month:** Complete all platform configurations
3. **This quarter:** Evaluate which platforms to keep vs. delete
4. **This year:** Maintain privacy through regular audits

12.5 Additional WigSec Resources

Download our other privacy guides:

- Complete Data Broker Removal Guide (24 pages)
- Password Manager Setup Guide (18 pages)
- Breach Response Playbook (16 pages)
- Email Security & Privacy Guide (20 pages)
- Phone & Device Hardening Checklist (28 pages)
- Digital Estate Planning Guide (22 pages)

All guides free at: https://wigingtonsecurity.com/guides

Need Help With Social Media Privacy?

We offer personalized privacy audits and configuration assistance.

Services:

- Personal Privacy Audit ($150)
- Hands-on Configuration Session ($100)
- Family Privacy Training ($200)
- High-Risk Individual Consultation ($250)

Contact: https://wigingtonsecurity.com/contact
Schedule: https://wigingtonsecurity.com/services

Specialized support for stalking victims, public figures, and high-security needs

Document Version 1.0 • February 2026

https://wigingtonsecurity.com