Social Media and Communications

- Best Practices for Secure Communications
- Tips for Using Facebook and Meta Accounts Safely
- Moving Sensitive Communications to Signal or WhatsApp
- How to Keep Your Facebook Account Private
- Protecting Your Zoom Meetings from Unauthorized Recording

Best Practices for Secure Communications

1. **Use Encrypted Platforms**

- Use Signal for sensitive discussions. It offers end-to-end encryption, minimal metadata retention, and open-source transparency .
- Turn on disappearing messages, registration lock, and screen lock.

2. **Secure Accounts and Devices**

- Use strong, unique passwords and enable two-factor authentication (2FA) or passkeys on all communication apps.
- Store passwords in a manager such as 1Password or Bitwarden.
- Keep apps and operating systems updated to close security vulnerabilities.
- Use long log-in passwords on your devices and disable message previews on lock screens.

3. **Protect Shared Files and Metadata**

- Before sharing, strip metadata from Word and PDF files using the Document Inspector in Word or Remove Hidden Information in Adobe Acrobat .
- For highly sensitive material, share sanitized versions via encrypted services such as Tresorit, which provides end-to-end encryption.

4. **Establish Organizational Communication Protocols**

- Designate which platforms are approved for which types of communication (e.g., Signal for private, email or Slack for non-sensitive).
- Use separate channels for internal and external communication.
- Label sensitive topics and documents clearly.
- Include secure-comms guidance in your incident response plan (who to contact, when to switch to encrypted tools).

5. **Minimize Data Exposure**

- Collect and share only essential personal information. Avoid over-collection in communication platforms and forms.
- Train staff on privacy principles and proper use of encrypted tools.

6. **Maintain Privacy in Collaboration and AI Tools**

- Avoid uploading personal or confidential data to generative AI systems; use placeholder text in drafts.
- Keep advocacy or campaign plans off open systems unless sanitized.

Tips for Using Facebook and Meta Accounts Safely

1. Use Strong, Unique Passwords

- Don’t reuse the same password on more than one website.
- Make it long, using a mix of letters, numbers, and symbols.
- Never share your password with anyone, even if they claim to be “Meta support.”

2. Use a Password Manager

- A password manager stores all your passwords safely in one place.
- It can create strong passwords automatically so you don’t have to remember them.
- You only need to remember one master password for the manager itself.
- Good options include 1Password, Bitwarden, or Dashlane.

3. Turn On Two-Factor Authentication (2FA)

- This adds a second step — like a text code or app confirmation — when you log in.
- Go to Settings → Security and Login → Two-Factor Authentication to turn it on.
- Even if someone steals your password, they still can’t get in without that second code.

4. Try Passkeys (Newer and Safer Login Option)

- Passkeys let you log in using your phone’s fingerprint, Face ID, or device PIN — no password needed.
- They’re stored securely on your device, not in the cloud.
- Meta now supports passkeys — turn them on in Facebook Settings → Password and Security → Passkeys.
- Passkeys protect you from phishing attacks because they only work on the real Facebook site.

5. Watch for Fake Messages

- Hackers send fake warnings that look like they’re from Facebook or Instagram. Never click links in these messages.
- Check official notices at facebook.com/security instead.

6. Review Your Security Settings Regularly

- In Facebook’s Settings → Security and Login, review:
- Devices you’re logged into

- Apps connected to your account
- Where you've used your password
- Log out of devices or apps you don't recognize.

7. Keep Everything Updated

- Always install the newest updates for your Facebook app, phone, and browser.
- Updates fix bugs and close security holes.

8. If You Think You've Been Hacked

- Go to facebook.com/hacked immediately.
- Change your password and review your recent logins.
- Turn on 2FA or passkeys right away to prevent future hacks.

Moving Sensitive Communications to Signal or WhatsApp

Moving Sensitive Communications to Secure Messaging

Email and workplace chat platforms like Slack are not designed for sensitive communications. While convenient for daily operations, they create permanent, searchable records that are vulnerable to subpoenas, breaches, and surveillance. This guide explains when and how to move sensitive conversations to encrypted messaging platforms, primarily Signal and WhatsApp.

Concerns about Email and Slack

Why Email is Insecure for Sensitive Communications

Fundamental Vulnerabilities:

- Email travels between servers as plain text (encrypted "in transit" but viewable by Google, Microsoft, etc.)
- Messages are stored permanently on multiple servers (from senders and receivers)
- Subject lines are never encrypted
- Easy target for subpoenas and legal discovery
- Metadata (who, when, to whom) is always visible
- NOTE: Even "secure" email from Proton isn't encrypted if the recipients are Google or Microsoft users

When Email is Acceptable:

- Public communications (press releases, newsletters)
- Routine coordination that isn't sensitive
- Communications that you'd be comfortable being publicly disclosed

Why Slack/Teams Aren't Secure Channels

Critical Limitations:

- No end-to-end encryption (providers can read all messages)
- Complete message history stored on company servers (for paid accounts)
- Administrator access to all conversations
- Vulnerable to subpoenas, e-discovery, and data requests
- Often mistaken as secure due to business/professional use
- Compliance tools may monitor all activity

When Slack/Teams are Acceptable:

- General team coordination
- Project management discussions
- Non-sensitive organizational communications
- When transparency and searchability are priorities

Secure Messaging

What Makes Messaging Platforms Secure?

End-to-End Encryption (E2EE):

- Messages encrypted on your device
- Only the recipient can decrypt
- Service provider cannot read message contents
- Protection from server breaches and legal requests

Additional Security Features:

- Disappearing messages (auto-delete after set time)
- Screenshot notifications
- Minimal metadata collection
- Open source code (for verification)

Signal

Why Signal is Recommended

Technical Security:

- End-to-end encryption by default for all communications
- Trusted open source protocol audited by security researchers
- Minimal metadata collection (phone numbers encrypted)
- Disappearing messages for all conversations

Organizational Structure:

- Operated by Signal Foundation, a nonprofit
- U.S.-based but with strong privacy commitments
- Limited data to provide in response to legal requests (no messaging data and almost no metadata)
- Transparent about government requests (publishes reports)

Practical Features:

- Voice and video calls (also encrypted)
- Group messaging with admin controls
- File sharing (encrypted)
- Desktop applications available
- Relatively simple to use -- feels like a "regular" chat app

When to Use Signal

High Priority Scenarios:

- Campaign strategy discussions
- Legal strategy or attorney communications
- Confidential partner communications
- Internal discussions about sensitive operations
- Anything you wouldn't want leaked to opposition or adversaries
- Communications involving vulnerable individuals
- Financial or donor information discussions

Organizational Use Cases:

- Executive team sensitive discussions
- Board communications on confidential matters
- Crisis response coordination

- Incident response team communications
- Legal compliance discussions
- Sensitive conversation with external partners

Signal Best Practices

Setup and Configuration:

1. **Enable Registration Lock**: Prevents someone from registering Signal with your number
2. **Set Disappearing Messages**: Default to 1 week or 4 weeks for most conversations
3. **Enable Screen Security**: Blocks screenshots (on Android)
4. **Use PIN**: Protect account recovery with secure PIN

Operational Security:

- Create dedicated Signal groups for specific sensitive projects
- Name groups descriptively but not identifiably ("Project Alpha" not "Litigation Strategy")
- Regularly review group membership
- Use Signal for sensitive one-on-one check-ins
- Turn on disappearing messages

WhatsApp

Understanding WhatsApp's Security

What WhatsApp Does Well:

- End-to-end encryption using Signal Protocol
- Encrypted voice/video calls
- Enormous, global existing user base (easier adoption)
- Feature-rich (compared to Signal)
- Disappearing messages available

Critical Limitations:

- Owned by Meta (Facebook company)
- Collects extensive metadata (who you talk to, when, how often)
- Shares metadata with Meta for advertising/analytics
- Cloud backups not end-to-end encrypted by default
- Terms of service allow data sharing within Meta companies
- Subject to Meta's broader surveillance advertising business

Metadata Risks:

- Social graph mapping (who knows whom)
- Communication pattern analysis
- Geographic tracking
- Device information collection
- Contact list upload

Lower-Risk Scenarios (when it's ok to use WhatsApp):

- Communications with international partners where WhatsApp is standard
- Coordination that isn't highly sensitive but needs encryption
- Communities where Signal adoption would be a major barrier
- When the content is sensitive but metadata exposure is acceptable (it's ok to expose who you're talking to)

WhatsApp Risk Mitigation

If you must use WhatsApp:

1. **Minimize Metadata Exposure:**
   - Don't use it for highly sensitive contacts
   - Assume Meta knows you're communicating with this person
   - Consider what communication patterns reveal
2. **Secure Settings:**
   - Enable disappearing messages
   - Disable read receipts
   - Turn off automatic media download
   - Disable cloud backups (or ensure they're encrypted)
   - Enable two-step verification
   - Advanced Chat Privacy: Admins can turn this on, users can't save media to their device or export chats
3. **Behavioral Safeguards:**
   - Use for logistics, not strategy
   - If possible, move highly sensitive conversations to Signal
   - Don't use for communications involving vulnerable people
   - Assume metadata is being collected and potentially shared

How to Keep Your Facebook Account Private

Facebook is designed for sharing with friends, so you can't make a profile that hides everything from friends too. The closest you can get is:

- Hide everything from non-friends (the public).
- Use the "Only me" setting on individual fields you don't want anyone to see, including friends.
- Put specific friends on a Restricted list so they only see what you make public.

A few things stay visible no matter what: your name, your profile picture, your cover photo, and your activity in public groups.

Basic protections

Go to **Settings & privacy** → **Settings** → **Privacy** (or **Audience and visibility** on newer layouts). Set each item below.

Your posts and stories

- Who can see your future posts: **Friends** (or **Only me** if you want a quiet profile)
- Limit past posts to friends: **Yes**
- Who can see your stories: **Friends**

Your profile details (under **Profile details** or **Profile information**)

- Set each field (birthday, hometown, current city, relationship, email, phone, employer, education) to **Only me**. This hides them from friends too.

Your friends list

- Who can see your friends list: **Only me**

Pages you follow

- Who can see the pages you follow: **Only me**

Finding you

- Who can send friend requests: **Friends of friends**
- Who can look you up by email or phone: **Friends**

- Search engines linking to your profile: **Off**

Tagging

- Review tags before they appear on your profile: **On**
- Who can see posts you're tagged in: **Friends** or **Only me**

Active status

- Show when you're active: **Off**

Hide things from specific friends without unfriending them

Add them to your Restricted list: **Settings** → **Privacy** → **Blocking** → **Restricted list**. They stay friends, but only see what you post as Public.

Check what others actually see

On your profile, click the three dots near your name → **View As**. This shows your profile from a non-friend's perspective. Anything you still see there is still public.

What you can't hide

- Your name, profile picture, and cover photo are always public.
- Posts you make in public groups are visible to anyone in those groups.
- Comments you leave on public posts are visible to anyone who can see that post.
- Facebook itself sees everything regardless of these settings.

While you're in there: lock the account

- **Settings** → **Security and login**: turn on **two-factor authentication** (authenticator app, not SMS, if possible) and **login alerts**.
- Use a unique password from your password manager.

Protecting Your Zoom Meetings from Unauthorized Recording

The Issue

A company called WebinarTV has been scanning the internet for public Zoom links, sending bots into meetings as silent attendees, recording everything, and publishing the results as AI-generated podcasts, without notifying participants. This isn't a data breach in the traditional sense: no passwords were stolen. WebinarTV treated your meeting link as a public invitation.

The culprits are browser extensions with calendar access combined with publicly posted meeting links. If your meeting link was never public and no attendees had compromised extensions, the risk is lower. For most organizations hosting educational webinars with broadly shared links, though, the risk is real. These steps address the known vectors.

Immediate Actions

1. Treat your meeting link like a key, not a flyer. If you wouldn't post it on a public bulletin board, don't share it in a newsletter, social post, or broadly forwarded email. The link itself is the attack surface. WebinarTV and similar services crawl for publicly accessible Zoom URLs.

2. Require registration and manually approve attendees. This is the most effective single control for sensitive calls. Bots register with fake email addresses, often at unusual domains. Manual review catches them before they join. Enable under Zoom: Security > Registration > Manually approve.

3. Audit every browser extension with calendar or meeting access. AI note-taking tools, transcription assistants, and meeting automators are the primary vector. Any extension with calendar permissions can read your meeting invitations and links. Open your browser's extension list, remove anything unfamiliar, and turn on permission prompts so extensions must ask before accessing calendar data.

4. Search for yourself on WebinarTV.us now. Search your name and your organization's name. If anything appears, request removal at remove@webinartv.us and document everything before submitting.

Zoom Settings to Enable

Watermarking. Zoom's watermarking embeds participant information into video, creating accountability and deterring unauthorized recording. Account Settings > Recording > Watermark.

Recording consent notifications. This prompts participants when recording starts and requires acknowledgment. It doesn't stop external screen recorders, but creates a documented notification

event. Settings > Recording > Recording Consent.