# 1. Introduction

Civic activists and civil society organizations increasingly rely on digital tools for communication, organizing, and advocacy. At the same time, they face rising digital threats – from surveillance and account hacking to malicious attacks aimed at silencing their voices. This handbook is a comprehensive guide to digital security for activists with entry to mid-level knowledge. It focuses on practical steps anyone can take to protect their accounts, communications, devices, and data. The goal is to empower you with habits and tools that keep you and your community safer online, no matter where you are in the world.

**Why Digital Security Matters:** Around the globe, activists have learned the hard way that digital security is essential. For example, in 2011 Azerbaijani activists were detained even before a scheduled protest simply for promoting it on Facebook – authorities had monitored the public event page and moved pre-emptively. Such experiences are not unique. Human rights defenders, civic activists and journalists across Wider Europe have all encountered attempts to spy on their communications or steal their data. In Belarus, merely sharing or "liking" opposition-related social media posts has led to people being interrogated or even jailed. Digital threats can quickly translate into real-world harm.

**How to Use This Handbook:** This resource is organized into thematic chapters covering core areas of digital security: protecting your accounts, using secure communication tools, securing devices and data, recognizing phishing attacks, ensuring mobile phone safety, using social media wisely, sharing files securely, and preparing for incidents. Each chapter breaks down best practices in clear, actionable language aimed at non-technical readers. You'll find short real-world examples that illustrate why these precautions matter, as well as bullet-point checklists and tables you can reference or print as cheat-sheets.

No single tool or checklist can guarantee 100% security, but by applying the layered approaches in this guide, you will significantly reduce risk and become a harder target for adversaries.

**A Practical, Habit-Based Approach: Effective digital security is less about using one "magic" app and more about building good habits and awareness.** Throughout this handbook, we emphasize assessing your own situation and adopting practices that fit your risks. Security is a continual process, not a one-time setup. By routinely thinking about what needs protection and how you might be attacked, you can make informed decisions rather than "shooting in the dark." Even simple hygiene steps – like keeping software updated, using two-factor authentication, and being skeptical of unexpected messages – go a long way in protecting you and your colleagues.

This handbook is region-agnostic, meaning the advice applies broadly regardless of country. However, always be mindful of your local context: laws and threats differ (for instance, some countries restrict encryption use or heavily surveil social media). Use the principles here and adapt them to your environment. Each section ends with

a Checklist summarizing key steps, which you can use as a personal or organizational to-do list. In the Appendix, you'll also find quick-reference tables, including a comparison of communication channels and a list of recommended secure tools.

Let's get started on fortifying your digital security, one step at a time. In the next section, we begin with the foundation of any security plan: understanding your threat model – in other words, thinking about who or what might threaten you online, and what you can do about it.

# 2. Threat Modeling: Assessing Your Risks

Digital security for activists begins with threat modeling – a structured way to assess your risks and priorities. Threat modeling is essentially asking yourself: What am I protecting, and from whom? How might those threats materialize, and what would the consequences be if they succeed? By answering these questions, you can focus on the risks that matter most in your situation. Every activist's context is unique – a grassroots organizer in a democracy faces different threats than a dissident in an authoritarian state – so you should tailor your security approach to your reality. This section will help you create a simple threat model to guide the rest of your security decisions.

## 2.1 What Is Threat Modeling?

Threat modeling is the process of thinking systematically about threats and defenses. It starts with understanding that security needs are personal and subjective. There's no one-size-fits-all solution. Instead, it's about habits and awareness: regularly reflecting on changes in your work or environment that might introduce new threats, and adjusting your practices accordingly. Over time, this becomes a routine part of how you plan and operate. To start threat modeling, ask yourself questions like:

- **What do I want to protect?** – Identify your critical assets. These can be information (emails, contact lists, chat logs, documents, photos), accounts (email, social media, cloud drives), or even people whose data you hold. Essentially, list anything that, if revealed or tampered with, could harm you or others. ***Tip:*** Think about both ***confidentiality*** (secrets that shouldn't leak) and ***integrity*** (information that shouldn't be altered or faked).
- **Who do I need to protect it from?** – Identify your potential adversaries. These could be government agencies, abusive authorities, hostile political groups, hackers, or even disgruntled insiders. Consider their capabilities: do they have legal power to demand data? Technical skills to hack accounts? Money to buy spyware? Are they a persistent, well-resourced threat or more opportunistic? The more powerful the adversary, the more extreme your precautions might need to be.

- **How might these threats materialize?** – Think through the tactics your adversaries might use: hacking your passwords, intercepting unencrypted messages, phishing your team with fake emails, bugging your office, confiscating devices at the border, etc. Different adversaries use different methods – a corrupt local official might try to steal your phone, while a state security service might attempt sophisticated cyberattacks. Imagining scenarios helps you prepare.
- **What are the consequences if I fail?** – Determine the impact. What's the worst that could happen if each asset were compromised? Could leaked data lead to someone's arrest, violence, or smear campaigns? Could a stolen account be used to discredit your organization? By listing potential outcomes ("If my email is hacked, my contacts could be identified and harassed; if my laptop is seized, unencrypted files could incriminate others," etc.), you can prioritize which scenarios to prevent. Focus on the most damaging and likely threats.
- **How much trouble am I willing to go through to prevent these?** – Finally, decide on your security comfort level. More security often means more inconvenience, so it's a balance. Given the risks you've identified, which protective measures are worth it to you? If the consequences of failure are extremely high (e.g., exposing an at-risk whistleblower), you might accept a lot of inconvenience – such as using very secure but clunky communication methods. On the other hand, if the worst outcome is minor, you might opt for simpler precautions. The key is to recognize that doing nothing is not a safe option – security exists on a spectrum, and you want to be as high on that spectrum as necessary. **Security improvements often come with sacrifices in convenience and efficiency.** For example, using encrypted e-mail services instead of regular ones might slightly slow down your workflow, but it dramatically improves privacy. Decide what trade-offs you and your team are willing to make. Start with changes that have high security benefit for low effort (like enabling two-factor authentication (2FA), using a password manager, etc.), then ratchet up as needed.

Threat modeling doesn't need to be a long or formal process – even a short brainstorming session can clarify your priorities. You can do this as an individual or as a group exercise with your organization/team (sometimes collective threat modeling brings out issues one person might not think of). The outcome can simply be a list or document that guides your next steps. For example, you might write a brief statement like: ***"Our main assets: member contact database, private Signal group chats, leadership email accounts. Adversary: likely state security services and hostile hacktivists. Likelihood of attack: context dependent. Worst case: context dependent. We will implement: device encryption, move chats to a more secure app, etc."*** This becomes a reference point whenever you consider new tools or face new situations.

## 2.2 The Five Key Questions

As outlined above, **threat modeling centers on five key questions (what, who, how, impact, and effort)**. These help you break down a nebulous concept ("I'm worried about digital threats") into actionable insights. It's worth revisiting these questions periodically, since your situation and adversaries can evolve. Threats can change over time – say, your campaign gains visibility, or a new law is passed increasing surveillance – so revisit these questions periodically or when starting a new project. Many activists integrate risk assessment and threat modeling into their project planning. For instance, before a big event or report release, they'll ask: ***"Could this trigger retaliation? Are our comms protected accordingly?"*** This proactive mindset ensures you're not caught off guard by emerging risks.

To summarize, the five questions provide a framework to identify and prioritize your risks:

1. **What do you want to protect?** (List your critical digital assets and info.)
2. **Who do you need to protect it from?** (Identify adversaries and their capabilities.)
3. **How could those threats occur?** (Think of attack methods or scenarios.)
4. **What would the impact be if an attack succeeded?** (Envision worst-case outcomes.)
5. **How much inconvenience can you accept to prevent it?** (Decide on your security level.)

By answering these, you create a tailored threat model that guides your security decisions.

And of course, keep that threat model confidential and protected. 😊

## 2.3 Real-World Example: Knowing Your Adversary

To illustrate how threat modeling works in practice, let's look at a real scenario. In early 2024, a network of independent NGOs and journalists in Eastern Europe found themselves under targeted digital attack. A spear-phishing campaign sent highly tailored fake emails to staff members, attempting to steal their account credentials. The attackers clearly understood their targets' context: in one case, an email impersonated a secure email provider and warned of a login issue, urging the user to click a link – a link that led to a counterfeit login page designed to capture their password. In another instance, within hours of a prominent activist's arrest making news, colleagues received an email purportedly from a trusted NGO partner with an attachment about the arrest – perfectly timed to exploit their concern. Given these groups were already facing government pressure, the adversary (likely state-

sponsored) was very motivated and kept adjusting tactics (even creating fake websites and messages that mimicked real services). They even probed ways to intercept two-factor authentication codes, showing persistence. The consequences if these attacks succeeded were severe: a compromised email account or document store could lead to further arrests, raids on offices, or the shutdown of organizations, as authorities would gain insight into sensitive communications and contacts.

What can we learn from this example? First, the activists had accurately identified their adversary (a state security apparatus) and anticipated an elevated likelihood of attack during a crackdown. They treated unexpected emails with caution and quickly involved security researchers when something seemed off, which helped in detecting the phishing attempts. Second, they were aware of the worst-case consequences – knowing that if the government accessed their confidential files or conversations, it could endanger people's freedom and safety. This understanding likely spurred them to adopt protective measures like strong passwords and 2FA on key accounts, which indeed forced the attackers to evolve new tricks to try to get around those defenses. Lastly, the NGOs were willing to invest in security (collaborating with expert groups, running forensic analyses on suspicious messages, etc.), showing a high commitment to preventing dire outcomes. In essence, the activists' threat model was validated: it correctly predicted both the nature of the adversary (a well-resourced, persistent actor) and the kinds of attacks used (spear phishing of accounts), allowing them to respond effectively and shore up their defenses.

For an activist in a different situation – say, a local environmental group campaigning against a powerful company – the adversary might be a private investigator or corporate-hired hacker rather than a government agency. The methods might differ (maybe attempts to hack the group's website or infiltrate their social media pages, rather than targeting personal email). But the same threat modeling questions apply. Knowing who is after you and what they want will guide you to appropriate defenses.

One more example: the 2011 Belarusian "silent protests" highlight a lower-tech threat. As an organizing tactic, activists coordinated mass demonstrations via public social networks – which allowed the authorities to monitor plans in real time. The adversary (Belarus's security police, the KGB) simply watched the openly shared announcements, and the consequence was spoiled protests as police preemptively deployed to arrest participants. In response, activists tried moving to more private communications, but even those were penetrated – in one case the KGB detained a social media administrator and forced him to hand over user data, exposing the organizers. The threat model in that case pointed to the need for closed, secure channels for planning (e.g. encrypted group chats or invite-only forums instead of public pages). Indeed, Belarusian organizers later adopted more secure messaging apps for sensitive coordination, emphasizing the lesson that activists must expect that "governments and potential adversaries monitor" open channels. Good threat

modeling would have suggested using private, encrypted tools for critical planning, a topic we'll cover in later chapters.

## 2.4 Turning Threat Models into Action

After defining your threat model, the next step is to choose security measures that address the risks you've identified. In the rest of this handbook, we will cover specific practices and tools in detail – consider those as a menu of options. Your threat model tells you which options matter most for you. For example:

- If your adversary is likely to try hacking your accounts, you'll want to prioritize strong **Account Protection** (Chapter 3), such as strong passwords and two-factor authentication, to thwart those login attacks.
- If you worry about eavesdropping on your calls or messages, then focus on **Secure Communication** tools (Chapter 4) like end-to-end encrypted messengers and avoiding insecure channels.
- If device seizure or theft is a big concern (common in raids or border crossings), pay special attention to **Device and Data Protection** (Chapter 5): encrypt your devices, minimize sensitive data you carry, and have backups.
- For high risk of targeted malware or phishing (perhaps from state-sponsored actors or well-resourced opponents), read Chapters 6 and 7 closely (**Phishing** and **Mobile Safety**) to learn how to spot malicious attempts and lock down your phone's security.
- If online harassment or doxing is part of the threat (common for outspoken activists), our **Social Media Security** chapter (Chapter 8) will help you adjust privacy settings and prepare for such scenarios.
- Always have an **Incident Response** plan (Chapter 10) matching your threat model: e.g., if account compromise is a top worry, have a plan for quickly recovering or locking accounts; if physical safety during arrest is a worry, know steps like remotely wiping a device or revoking access tokens.

Lastly, threat modeling is not a one-time task. Threats can change over time – maybe your campaign gains visibility, or a new law increases surveillance – so make it a habit to periodically re-evaluate. Even a brief check-in can ensure you're not caught off guard by new risks. Many activists build threat modeling into their routine: for instance, before a major event or publication, ask "Could this attract new threats, and are we prepared?" This proactive mindset will help you adapt and stay ahead of adversaries.

**Checklist: Threat Modeling (Use this checklist to review your risk assessment)**

- **Identify Assets: I have listed the digital assets I most need to protect (e.g. key accounts, sensitive documents, contact lists, devices with important data).**
- **Identify Adversaries: I have considered who might want to breach or sabotage those assets (specific agencies, groups, individuals) and what their capabilities are (technical skills, legal power, resources).**
- **Assess Likelihood: I have evaluated how likely these adversaries are to act against me or my organization, especially in light of our current activities or upcoming events.**
- **Assess Impact: I have thought about the worst-case consequences if each asset were compromised – and which scenarios would have the most serious impact on safety or operations.**
- **Set Security Level: Based on the above, I know how far I'm willing to go with security measures. I'm prepared to adopt stronger (possibly less convenient) measures for high-risk assets and situations.**
- **Prioritize: I know which areas (accounts, communications, devices, etc.) need the most urgent protection improvements given my situation.**

***(Now that you understand your risks and priorities, let's proceed to concrete protections. In the next chapter, we tackle Account Protection, often the first line of defense.)***

# 3. Account Protection: Safeguarding Your Online Accounts

## 3.1 Strong Passwords and Password Managers

Your accounts – email, social media, messaging apps, etc. – are often the first targets for attackers because a compromised account can expose a lot of sensitive information or be used to impersonate you. The foundation of account security is a strong, unique password for each account. Reusing passwords or choosing weak ones makes it easy for adversaries to break in.

- **Use Long, Unique Passwords:** A strong password is long (at least 12–15 characters) and unpredictable. Avoid dictionary words or common phrases. Instead, consider using a passphrase (a string of random words) or a completely random string of letters, numbers, and symbols. The key is that it should be unique to that account – never reuse a password on multiple services. Attackers often try known passwords from one breach on other

accounts ("credential stuffing"), so one leak can otherwise snowball into many compromised accounts.

- **Password Managers:** Since it's impossible to remember many complex passwords, use a reputable password manager app (like Bitwarden, KeePass, 1Password, etc.). These tools generate and store strong passwords for you, encrypted with one master password. You only have to remember the one master passphrase, which unlocks the vault. A password manager lets you have a different 20-character random string for every account without memorizing them. It also helps guard against phishing – many password managers will autofill only on the correct website, so a fake login page won't get your credentials.
- **Avoid Common Pitfalls:** Don't use personal info (names, birthdays, pet names) in passwords – those can be guessed or found via social media. Avoid patterns like "Summer2023!" or trivial variations – attackers know those tricks. Also, be cautious with security questions (which sometimes act as a backup password); treat answers like additional passwords or use random answers stored in your password manager, so attackers can't guess them from your public details.
- **Check for Breaches:** Consider using a service like "Have I Been Pwned" to see if any of your accounts have been in data breaches. If a password was exposed, change it immediately (and anywhere else it was used – though ideally you weren't reusing it). Some password managers and browsers have breach alert features too.
- **Master Password and Key Safety:** Make sure your master password (for your password manager, or your primary email account) is extremely strong and not reused anywhere. This is the "keys to the kingdom." Enable two-factor authentication on your password manager if possible. Also, configure a secure method to recover your password manager data (for example, a secure paper backup of your master key or recovery phrase stored in a safe place) so that you're not locked out if you forget the master password.

Remember, using a password manager and strong unique passwords might feel like extra work, but it dramatically improves your security. Most account breaches still stem from weak or reused passwords – this is a simple fix that pays huge dividends in safety.

## 3.2 Two-Factor Authentication (2FA)

Even the strongest password can be compromised (through phishing, malware, or data breaches). Two-factor authentication (2FA), also known as multi-factor authentication, adds a vital second layer of security to your accounts. It means that in addition to your password, you need another "factor" (like a one-time code or

physical token) to log in. This makes it **much harder** for someone to hack into your account, because knowing your password alone isn't enough.

- **Common 2FA Methods:** The most common second factor is a one-time code generated by an app (like Google Authenticator, Authy, or Microsoft Authenticator) or sent via SMS. You enter this code after your password to confirm it's really you. App-based codes are preferable to SMS, since SMS can be intercepted or SIM cards hijacked. Another method is "push" notifications (your phone gets a prompt to approve the login) – convenient if supported. The strongest 2FA method is a physical security key (like a YubiKey or Google Titan Key) that you plug in or tap to authenticate. Security keys use encryption to verify the login and are resistant to phishing.
- **Enable 2FA Everywhere Possible:** Turn on 2FA for all accounts that offer it – certainly for email, social media, cloud storage, banking, and any account that holds sensitive info. Most major services support 2FA. Check your account settings for "two-step verification" or "login security." Typically, you'll scan a QR code with an authenticator app to set it up, or register a phone number for SMS codes.
- **Backup Codes:** When you enable 2FA, many services provide backup codes – one-time use codes to access your account if you lose your 2FA device. Treat these like passwords: store them securely (e.g., in your password manager or a locked safe). They can save you from being locked out if, say, your phone is stolen.
- **Phone Numbers and 2FA:** Some services require a phone number for account recovery or 2FA. Be mindful of where you use SMS-based 2FA – if your threat model includes targeted attackers, they might try a "SIM swap" (tricking your phone provider to activate your number on their device) to intercept codes. If you suspect this risk, use app codes or security keys rather than SMS for 2FA, and add a PIN/password to your mobile carrier account to prevent unauthorized changes.
- **Authenticator Apps vs. SMS:** As mentioned, apps are generally more secure. They work offline and codes change every 30 seconds. If you switch phones, remember to transfer or disable 2FA on accounts first (or use the backup codes) – otherwise those code generators won't work. Some authenticator apps can cloud-sync (with end-to-end encryption) to ease phone migrations, but assess the security of that feature.
- **Physical Security Keys:** For high-value accounts (email, admin accounts, etc.), consider using a security key. Many services (Google, Facebook, Twitter, Microsoft, etc.) support them via standards like U2F/WebAuthn. You register the key to your account, and then when logging in, you insert/tap it when prompted. It's phishing-resistant because the key won't work on a fake site – it checks the domain. The downside is you must have it with you (consider a

backup key in a safe spot). But for activists facing serious threats, keys can dramatically improve security.

Enabling 2FA may add a few seconds to your login process, but it shuts down a **lot** of common attack paths. A hacker who somehow gets your password will still be stopped cold unless they also have your code or key, which is unlikely. It's one of the most effective steps you can take to protect your accounts.

## 3.3 Account Recovery and Monitoring

Securing your login is one side of the coin; the other is making sure you have control of your account recovery settings and keeping an eye out for any suspicious activity on your accounts.

- **Update Recovery Information:** Regularly check that your account recovery info is up-to-date and secure. This means your backup email and phone number (for account resets) should be ones you control and are themselves secure. Avoid using an old email you no longer check, or a friend's number – if someone else can access your recovery channel, they could reset your account. If you no longer have access to a listed recovery email/number, remove it. Use strong 2FA on your primary email, since it's often the top recovery method for all your other accounts.
- **Beware of Social Engineering:** Many account takeovers happen not through technical hacking, but by tricking customer support. An adversary might call your email provider or phone company pretending to be you and use personal info to answer security questions. Where possible, set secondary passwords/PINs with your mobile carrier or any service that can perform account actions by phone. Minimize the personal details you share publicly that could be used to impersonate you (birthdate, etc.).
- **Alerts for New Logins:** Turn on notifications for logins or new device access, if the service has them. For example, Google and Facebook both have settings to alert you (via email or phone) if a new device or location logs into your account. If you get an unexpected alert ("new login from Chrome on Windows, location X"), act immediately: secure your account by changing your password (from a safe device) and review what was accessed. These alerts can be early warning signs of breach.
- **Review Account Activity:** Many services allow you to review recent activity or active sessions. For instance, Google's account dashboard shows recent logins and devices; Facebook and Twitter show current logged-in sessions/browsers. Make a habit of checking these. If you see devices or locations that you don't recognize, that's a red flag – use the option to "log out of all sessions" and change your password. In some cases, you can see if any unusual actions were taken (like emails forwarded, settings changed).

- **Use Admin Features for Organizations:** If you help manage accounts for a group or organization (say, multiple people access the same social media account), use the collaboration features instead of sharing passwords. For example, Facebook Pages and Twitter allow adding team roles – use those rather than giving out the master credentials. This way each person uses their own account (with 2FA) to log in, and you can easily remove access for one person without a password reset if needed.
- **Clean Up Old Accounts:** Old accounts you no longer use can become backdoors if not monitored (especially if they tie to a current email or have reused passwords). Delete or secure accounts for services you've abandoned. This reduces your "attack surface."
- **Phishing Education:** Be cautious with emails claiming "Your account has a problem, click here to fix." Always verify through another path. Go to the site directly or use their official app to check your account, rather than clicking a link in an email that could be fake.

By proactively monitoring your accounts and having a plan to respond, you greatly increase the chances of catching an intrusion early – or preventing one altogether. Many attackers rely on slipping in unnoticed. Don't give them that advantage.

### Checklist: Account Security Basics

- **Passwords for all my important accounts are strong (lengthy, random, unique) and stored in a secure password manager. I do not reuse passwords.**
- **Two-factor authentication is enabled on all accounts that support it (especially email, social media, financial, and messaging accounts). I use an authenticator app or security key where possible, rather than SMS.**
- **My account recovery information (backup email, phone number) is accurate and secured. I've set up additional protections (PINs, security questions with random answers) to prevent unauthorized resets.**
- **I have removed or updated any old accounts or profiles I no longer use, so they can't be hijacked and used against me.**
- **I have enabled login alerts or activity notifications on my major accounts, and I periodically review active sessions or account activity for anything unfamiliar.**
- **For any shared or team accounts, we use proper multi-user access controls (instead of sharing passwords) to manage collaboration safely.**

- **I have a plan for what to do if an account is compromised despite these measures (who to contact, how to regain access, how to inform contacts if needed).**

***(With your accounts fortified, we next turn to keeping your communications private.)***

# 4. Secure Communication: Keeping Your Conversations Private

Digital communication is the lifeblood of activism – from coordinating plans to sharing sensitive information. Unfortunately, communications can be intercepted or monitored by adversaries if not properly secured. This chapter covers how to communicate safely: using encryption to protect messages and calls, choosing the right channels, and being mindful of metadata and anonymity.

## 4.1 Why Encryption Matters

Encryption is a technical defense that scrambles your messages or calls so that only the intended recipient can read or hear them. It's like putting your letter in a locked box that only the recipient has the key to. Without encryption, anyone who intercepts your communication (your Internet Service Provider (ISP), a government surveillance system, a hacker on the Wi-Fi, etc.) could potentially read the content. With strong encryption, even if they intercept it, all they see is gibberish.

- **End-to-End Encryption (E2EE):** This is the gold standard for private communication. E2EE means that your message is encrypted on your device and only decrypted on the recipient's device. No intermediary – not even the service provider – can read it. Apps like Signal, WhatsApp (for chats), and Wire provide end-to-end encryption by default for messages and calls. When you send "We meet at 8pm at location X" via an E2EE app, anyone intercepting that message sees only scrambled text, not the actual plan. Only your friend's device can decrypt it to read "We meet at 8pm at location X."
- **Transport Encryption (HTTPS/TLS):** Most mainstream services use HTTPS, which means the communication between your device and the service's servers is encrypted. This protects against casual eavesdropping on the network. For example, your connection to Gmail or Facebook is encrypted in transit (others on the network can't easily snoop on the content). However, the service itself ***can*** see the content because it gets decrypted on their server. So, HTTPS is good (always look for the padlock icon in your browser on webmail or sites – that means HTTPS is on), but it's not as private as E2EE. With HTTPS, outsiders can't spy on the traffic, but the service provider (and

anyone who can access their data, such as via government request or a breach) might still access your communications.

- **Why Activists Need E2EE:** If you're coordinating a protest or discussing sensitive topics, you don't want there to be any "middle man" who could hand your conversation to an adversary. End-to-end encrypted messengers ensure that even if, say, the company running the app is pressured or hacked, they can't give away your chats because they simply don't have the keys. It's a fundamental shift from "trust the service with my data" to "trust only the people I'm talking to."
- **Verifying Keys:** Some E2EE apps allow you to verify the encryption keys of your contacts (often via a safety code or QR scan) to ensure no one is secretly intercepting ("man-in-the-middle" attack). This is a higher-level step; for most users, just using E2EE apps is sufficient. But if you're at high risk, verifying keys (like scanning your friend's Signal safety number in person) adds extra assurance that your encryption hasn't been compromised.
- **Limitations of Encryption:** It's important to note what encryption doesn't do. It protects content, but not necessarily metadata. For example, even if your email is PGP ("Pretty Good Privacy") encrypted, an eavesdropper might still see who you emailed and when (unless you take additional steps to hide that). Similarly, using Signal hides ***what*** you said, but an observer could still see that you're communicating with a certain number (although Signal's "sealed sender" feature and other practices can obscure even some of that). We'll discuss metadata more in section 4.4. Also, encryption doesn't protect you if an adversary compromises your actual device – if your phone is infected with spyware, it could capture messages after you've decrypted them to read, for instance. So device security and encryption go hand in hand.

In summary, strong encryption is one of the best tools we have to ensure privacy in communication. Activists around the world have adopted encrypted messaging for day-to-day coordination to prevent surveillance and protect their sources, partners, and communities.

## 4.2 Secure Messaging and Voice Calls

Choosing the right messaging app or platform is crucial. Not all communication tools are equal in security. Here we outline some popular options and best practices for messaging and calls.

- **Signal:** Signal is a widely recommended secure messaging app (for iOS, Android, and desktop) that provides end-to-end encryption for texts, group chats, voice calls, and video calls by default. It's open-source and run by a nonprofit. Signal collects minimal data (not even storing metadata like who you've chatted with, as far as technically possible). It's considered the gold

standard for activists. Use Signal for sensitive communications whenever you can. It also supports features like disappearing messages (messages auto-delete after a set time) which can be useful for limiting what records exist.

- **WhatsApp:** WhatsApp (owned by Meta/Facebook) also uses the Signal encryption protocol for chats and calls, meaning communications are end-to-end encrypted. It's very popular globally. However, WhatsApp does collect more metadata (like who you contact and when, and group membership) and stores backups by default on cloud services that might not be encrypted. If you use WhatsApp, turn off cloud backup of chats or ensure backups are encrypted, since an iCloud/Google Drive backup could be accessed by a warrant. Also be mindful that WhatsApp is tied to your phone number, which can be an identifier.
- **Wire, Element, Others:** Wire is another secure messenger option (European-based) with strong encryption and team collaboration features. Element (which uses the Matrix protocol) is an open-source encrypted messaging system that can be self-hosted – good for tech-savvy groups or those needing a custom solution. There are also others like Threema, Session, etc. The key is to use one that is end-to-end encrypted and preferably open-source (so its security claims can be audited).
- **Old SMS and Unencrypted Apps:** Regular SMS texts and normal phone calls are **not secure** – they can be intercepted by phone companies or governments, and SMS in particular is easy to snoop on with the right equipment. Likewise, avoid sending sensitive info over Facebook Messenger, Telegram (unless in "Secret Chat" mode), or other platforms that do not have E2EE by default. If a platform offers an E2EE option (like Telegram secret chats or Facebook's Secret Conversations), use it for anything sensitive, but note it's best to stick with dedicated secure apps like Signal whenever possible.
- **Voice Calls and Video:** Signal and WhatsApp both provide encrypted voice and video calls. Apple's FaceTime is also end-to-end encrypted (and quite robust security-wise) if both parties have Apple devices. Zoom has an option for end-to-end encryption (must be enabled in settings) – otherwise assume calls could be accessed by the provider. For highly sensitive meetings, consider alternatives like Jitsi (an open-source encrypted video conferencing you can self-host) or meet in a secure platform that offers E2EE.
- **Using Code Words:** Even on encrypted channels, some activists use code names or shorthand for extremely sensitive topics (out of an abundance of caution, or in case a phone gets seized while unlocked). This can be an extra layer, but be careful it doesn't cause confusion. Generally, if you trust the encryption and the participants, speaking plainly is fine – focus on securing the tools and devices.

- **Group Chats:** Encryption protocols handle group chats slightly differently, but apps like Signal and WhatsApp do encrypt group messages. Be aware of who's in the group – any one member could compromise confidentiality (through their device being compromised or even just copying info out). Keep sensitive group chats to a minimal necessary audience. On some apps, you can lock down groups so that only admins can add new members – use that to prevent an adversary from sneaking in a new number pretending to be someone.
- **Backup and Archives:** If your app offers encrypted backups (Signal can create an encrypted backup file, WhatsApp has encrypted backup option), use them if you need backups. But also consider whether you want long-term logs at all. In some cases, it's safer not to retain conversation history once it's no longer needed. Disappearing messages or manual deletion can reduce the amount of data that could be exposed if your account or phone is compromised.

In short: for day-to-day chats and calls about organizing, try to use end-to-end encrypted apps as much as possible. It might take a bit of onboarding (getting colleagues or partners to install a new app), but it significantly raises your communications security. Even if someone hacks your email or taps your phone line, they won't get anything from your Signal/WhatsApp calls or messages.

## 4.3 Email Security and Alternatives

Email is an older technology and was not built with strong encryption by default. Activists should be cautious with email for anything sensitive. However, email is often unavoidable and useful for certain tasks, so here's how to make it as safe as possible – and when to consider alternative tools.

- **PGP Encryption for Email:** It is possible to encrypt email contents using PGP (Pretty Good Privacy), but it's notoriously complicated and not user-friendly. Both the sender and receiver have to set up encryption keys and exchange public keys beforehand. If you and your contacts are comfortable with it, PGP can secure the content of your emails (the subject and metadata, however, remain visible). There are tools like Enigmail for Thunderbird, or Mailvelope for webmail, but they require training. Realistically, unless you already use PGP, it might be better to use a different channel (like a secure messenger or share files via encrypted link) for the very sensitive content.
- **Encrypted Email Services:** Services like **ProtonMail** or **Tuta** offer end-to-end encryption for emails within their system. For example, ProtonMail (based in Switzerland) automatically encrypts emails stored on their servers, and if you send from one ProtonMail address to another ProtonMail user, it's E2E encrypted such that even ProtonMail's servers can't read it. If you email someone on a different service, ProtonMail lets you encrypt the message with a password (you share the password via another channel, and they use it to

decrypt the mail in a browser). These services also have features like self-destructing emails. While not as universally adopted as Gmail, they provide a higher baseline of privacy without requiring PGP setup. Consider using them, especially for activist organizations – even for the perception benefits (showing you care about privacy).

- **Secure Alternatives for Attachments/Links:** One common use of email is sending documents or links. For sensitive files, consider using a secure file-share service or encrypt the files before emailing (see Chapter 9 on file sharing). For sharing info, you might just send a message on Signal or an invite to a secure document collaboration platform instead of email text.
- **Account Security for Email:** Since email is often a recovery channel for other accounts, securing your email account with a strong password and 2FA is ***critical***. Gmail, Outlook, Yahoo, etc. all support two-factor auth – use it. Also beware of phishing emails that target email credentials – they are common.
- **VPN and TOR for Anonymity:** If you are worried about the tracking of ***who*** you email or your IP address, consider using a VPN when accessing email, or even **Tor Browser** for sensitive sessions. This can hide your location from both the email provider and anyone monitoring traffic. Some activists create separate email accounts under pseudonyms for certain activities – if you do, be careful not to browse them from an account or device linked to your identity (to avoid linking the alias to you via IP logs or cookies).
- **Use Email Wisely:** Perhaps the best approach is to use email for less sensitive correspondence (logistics, public information) and not for private strategy or personal details. If you must discuss something confidential and only email is available, keep the message brief and consider encrypting the content. Also, think about the recipients – don't put people at risk by CC'ing their real names or mixing groups of people who might not want to be identified together. Operational security includes how you address emails and manage replies (e.g., **using BCC to hide recipient lists when needed**).
- **Beware of Attachments:** Email attachments can carry malware. Be extra cautious opening any attachment you didn't expect. If someone says "here is the report" but the email style looks slightly off, verify with them out-of-band. Ideally, have an antivirus or sandbox for opening attachments from unknown senders, or use a service like **VirusTotal** to scan a file. But even those aren't foolproof, so **skepticism and verification are key**.

In summary, **treat email as potentially public postcards** unless you've taken specific measures to encrypt it. It's a useful tool but not the most secure for sensitive matters. When privacy is paramount, you have better options – but when you do use email, lock down the account and think about what you write.

## 4.4 Protecting Metadata and Anonymity

Even if your messages' content is encrypted, information about your communications (the metadata) can still reveal a lot: who talked to whom, when, and how often. In some cases, activists also need to hide their identity entirely when communicating or publishing information. This section covers strategies for those concerns.

- **Understanding Metadata:** Metadata is the "data about data." For communications, that could include the sender, recipient, time, location, and duration of communication, as well as the service or protocol used. For example, an email's metadata (the headers) show the sender's and receiver's email addresses and the timestamps. A phone call's metadata shows the numbers involved and call length. Intelligence agencies have noted they can learn almost as much from metadata as from content – patterns of who contacts whom can map out an organization's network. End-to-end encryption typically does not hide metadata; it only protects content. However, some tools minimize metadata. Signal, for instance, has taken steps not to keep logs of who contacts whom. Decentralized systems like Matrix or the Fediverse spread out metadata among servers (though not fully hiding it).
- **Using Anonymous Accounts/Aliases:** If you fear surveillance tying your communications to you, consider using pseudonymous accounts. For instance, you could have a secondary email or chat identity that isn't clearly linked to your real name. Activists in high-risk areas often use code names internally. Make sure to create such accounts in a way that doesn't link back (e.g., don't use your personal phone number to register a secret Telegram account – get a secondary SIM or use an **anonymous number service**, like Sideline, Slynumber, or Tossable Digits). Also, be mindful of how you use the alias – don't log into your anonymous account from the same browser or device session as your personal accounts (cookies, fingerprints can connect them). Some people **use separate devices or user profiles for different personas**.
- **Tor and VPNs:** To mask your IP address (which can reveal your approximate location or home/work network), you can use Tor or a reputable VPN service. Tor Browser routes your traffic through multiple encrypted hops, hiding your IP and making activity hard to trace back to you. It's slower and some sites may block Tor, but it provides strong anonymity. VPNs are simpler and faster, but require trusting the VPN provider. A VPN will make it look like your connection comes from a different location (where the VPN server is), useful to avoid local surveillance or censorship. Activists often use VPNs on mobile devices too, especially when traveling or using untrusted Wi-Fi. **Remember, even with Tor/VPN, if you log into an account tied to your identity, you're deanonymized** – these tools mostly hide location and browsing from observers, they don't magically make an identified account anonymous.

- **Burner Phones and Apps:** In situations where anonymity is crucial (e.g., organizing a protest in an environment with heavy surveillance), some activists use "burner" devices or accounts – a phone or SIM card obtained without their name, used only for a short time or specific purpose, then discarded. For example, using a prepaid SIM bought in cash to coordinate on the day of an action, then throwing it away. This can help avoid tying your main identity to the activity. **If using a burner phone, be cautious about ever turning it on or carrying it near your personal phone** – cell site data could correlate the two if they move together consistently. This is an advanced tactic for high-risk cases.
- **Minimizing Metadata in Tools:** Some platforms offer features to reduce metadata leakage. For example, **SecureDrop** is a system for whistleblowers to submit documents to journalists anonymously (over Tor). In normal tools, consider steps like turning off location tagging in messages or photos, and be aware that file metadata (like an image's EXIF data) can contain info like GPS coordinates of where a photo was taken. Before sharing media, remove metadata if needed (many secure messengers do this automatically, but not all – Chapter 9 discusses metadata in files).
- **Omitting Sensitive Details:** Finally, an old-school method: simply don't put certain details in writing at all. If you worry that even encrypted comms might one day be compromised or reveal patterns, keep the most sensitive plans offline or face-to-face. Use communications tech to arrange safe in-person meetings, for instance, rather than detailing every aspect of a plan online. It's hard to intercept a conversation in a park (especially if you're mindful of phones being left behind).

Metadata and anonymity protections are a complex topic, and not every activist will need extreme measures. But understanding the traces your communications leave is important. Even if you decide you don't need heavy anonymity, being aware (e.g., knowing that an unencrypted email exposes not just content but also who you talked to) can inform your strategy. Use the right tool for the job: if you require anonymity, choose tools and techniques designed for that purpose.

### Checklist: Secure Communication Practices

- **I use end-to-end encrypted apps (Signal, etc.) for sensitive messaging and voice/video calls, and I encourage my contacts to do the same.**
- **For less secure channels (email, standard SMS), I avoid sharing highly sensitive information. I've considered encrypted email options or add-ons for when I must use email securely.**
- **I have enabled disappearing messages or I periodically clean out sensitive chats so that old conversations don't linger unnecessarily.**

- **I'm careful with attachments and links I receive – I verify with senders if something is unexpected, to avoid phishing or malware.**
- **I know which of my communication channels reveal metadata and identity, and I take steps (VPN/Tor, pseudonyms, separate devices) in high-risk situations to reduce the trails I leave.**
- **I've turned off geotagging and unnecessary metadata in the apps I use (for example, my messaging app isn't freely sharing my location or syncing contacts without my consent).**
- **When needed, I have a plan for anonymous communication (such as using a secondary "clean" device or number that isn't linked to me, or using Tor for online activity that needs to be dissociated from my identity).**
- **I regularly update my communication apps to ensure I have the latest security improvements and patches.**

***(Next, we will focus on securing the devices and data you use – because even the most secure app won't help if your phone or computer is compromised.)***

# 5. Device and Data Protection: Securing Devices and Files

Activists rely on various devices – smartphones, laptops, tablets, external drives – to do their work. These devices hold sensitive data and also serve as gateways to your accounts and communications. If a device is compromised (lost, stolen, hacked, or infected with malware), it can lead to a cascade of security breaches. For example, an infected computer might log your passwords, or a confiscated phone might reveal your entire Signal chat history if not properly protected. This chapter focuses on how to secure your devices (both physically and digitally) and protect the data stored on them. We'll cover essential practices like keeping devices updated, using strong device locks and encryption, defending against malware, safe Internet use, and backing up data securely. We'll also discuss minimizing data exposure (for instance, carrying only what you need when traveling to risky areas) and safely deleting sensitive information when it's no longer needed.

## 5.1 Device Security Best Practices (Computers & Phones)

Keeping your personal devices secure is foundational – after all, they are the tools through which you do all your communications. Here are key best practices:

- **Keep Devices Updated:** Software updates often include critical security patches. Running an outdated operating system or app is like leaving a window open for attackers. Always install updates for your device's OS (Windows, macOS, Linux, Android, iOS) and major apps/browsers as soon as possible.

Activists have been targeted using exploits of unpatched vulnerabilities. For example, **advanced spyware (like Pegasus) often relies on bugs in iPhone or Android** – Apple and Google push fixes regularly, so updating is a key defense. Enable automatic updates where feasible. If you use older hardware that no longer receives updates (e.g., an old Android phone stuck on an ancient version), consider replacing it if you can; it may have unfixable holes.

- **Use Strong Device Locks:** Make sure all your devices are protected by strong authentication. For smartphones, use at least a 6-digit PIN or, better yet, an alphanumeric passcode. Avoid easy 4-digit PINs or simple swipe patterns (patterns can often be guessed from screen smudges or observed by someone watching you unlock). Biometric locks (fingerprint, face) are convenient and generally secure against casual threats, but note that in some jurisdictions authorities can legally compel you to use your finger or face to unlock, whereas they cannot force you to divulge a memorized password as easily. If you anticipate possible confiscation or forced unlock situations (e.g., at a border or protest arrest), a strong passcode might be safer than biometrics. Some phones allow a combo (e.g., require the PIN on boot even if fingerprint works when active). On laptops, set a password for login and have the system auto-lock when not in use. Configure a short auto-lock timeout (like 5 minutes of inactivity). **But the golden rule is to manually lock the device whenever you step away, even briefly.**
- **Full-Disk Encryption:** Ensure that your device's storage is encrypted. This means if the device is off (or locked) and someone takes it, they can't read the data without your password. Modern smartphones encrypt storage by default (iPhones do; newer Android phones do once you set a PIN). For computers: Windows has BitLocker (on Pro editions – turn it on and save the recovery key safely), macOS has FileVault (enable it in Security settings), and most Linux distros offer encryption during installation. **Encryption is a critical safeguard** – for instance, if your laptop is stolen at a protest or your office is raided, encrypted drives will prevent adversaries from easily accessing your files. Note that encryption protects data at rest (when device is off); if you're actively using the device while unlocked, files are accessible to someone with immediate access. But **it hugely mitigates loss/theft risks**. Don't forget to also encrypt external drives and USB sticks that contain sensitive data (you can use tools like VeraCrypt or built-in OS options to create encrypted vaults on those).
- **Secure Your Passwords and Keys on Devices:** Even with disk encryption, if your device is unlocked an attacker could try to grab sensitive files quickly (like password manager vaults or private keys). Use a device-based password manager that requires your master password or biometric each time you open it (or after a short period of inactivity), rather than leaving it always accessible. Avoid storing passwords in plain text anywhere on the device. Similarly, if you

use encryption keys (PGP, etc.), keep them in an encrypted part of the disk or use keyring software that requires a passphrase.

- **Beware of Malware (Anti-Virus/Anti-Malware):** Activists are regularly targeted by malware hidden in email attachments, documents, or links. Use reputable antivirus or anti-malware tools, especially on Windows and Android which are common targets. Keep these tools updated and do regular scans. They're not foolproof (especially against state-level "zero-day" exploits), but they can catch known threats and act as another line of defense. **Be cautious of what you download or plug into your devices** – for example, a random USB drive found on the street could be loaded with malware (this has actually been used to target NGOs). **Only install apps from trusted sources** (official app stores, etc.), and even then, consider whether that flashlight app really needs all those permissions.
- **Safe Browsing and Downloads:** Use browsers that receive regular security updates (Chrome, Edge, Firefox, Brave, etc.). Enable features like Chrome's Enhanced Safe Browsing or Firefox's warnings for deceptive sites – these can alert you to known malicious websites. **Consider using script-blocking browser extensions** (like uBlock Origin or NoScript) to reduce risk from harmful scripts on websites, but know that blocking scripts can break site functionality and is more for advanced users. When downloading files, **be extra suspicious of Office documents or PDFs that prompt to "enable macros"** or unusual permissions – **those can launch malware**. If you have the capability, opening potentially risky files in a sandbox or virtual machine (an isolated environment) can contain any harm.
- **Physical Security:** Don't overlook physical threats. An unattended laptop or phone could be stolen or tampered with (e.g., someone could quickly install a hardware keylogger or a **malicious charger**). In shared spaces, keep devices with you or use cable locks for laptops if you must leave them briefly. Be mindful at borders or police encounters: if a device is seized unlocked, they can access everything. In some situations, you might shut down devices in advance (since a powered-off encrypted device is safer than one that's on and unlocked). Consider whether you need to carry certain sensitive data at all when traveling or going to a high-risk event – if not, remove it or use a separate "clean" device with minimal data.
- **Extra Hardening:** If you face high threats (like targeted government hacking), there are more steps: e.g., enabling "developer options" on Android to turn on USB debugging only when needed (to prevent unauthorized data access via USB), using secure boot options and firmware passwords on laptops, etc. Some activists use specialized privacy-focused systems (a Linux distro like Tails for secure work, or GrapheneOS on Android for hardened security) – these require technical know-how but can further lock down a device. At the very least, familiarize yourself with your device's security settings and enable

the ones that make sense (for example, on Android, the setting that requires your PIN when the device boots, not just the usual swipe pattern – this ties into encryption).

- **Pegasus and Advanced Spyware:** As noted, **no device is 100% safe from a very determined, well-resourced adversary.** Spyware like NSO Group's Pegasus can infect phones without any click (via zero-day iMessage or WhatsApp flaws, etc.) and is very hard to detect. The risk is low for most activists, but if you work on highly sensitive issues and suspect government targeting, you might operate under an assumption that your phone could be compromised. In such cases, you might keep especially critical info off phones entirely, or **regularly reboot the phone** (some spyware doesn't persist after reboot), and use features like Apple's new "Lockdown Mode" which restricts many functions to reduce attack surface. The average activist likely won't encounter this, but it's important to be aware that it exists.

Implementing these device protections significantly reduces the chances that a lost, stolen, or hacked device will result in a catastrophe. It's about creating multiple hurdles: a thief has to get past your lockscreen, your encryption, your passwords, and maybe your 2FA – all before any damage is done.

## 5.2 Protecting Data at Rest (Encryption and Backups)

We touched on full-disk encryption above for devices. Here we delve a bit more into protecting the data you store – both in terms of confidentiality (encryption) and ensuring you don't lose it (backups).

- **Full-Disk vs. File Encryption:** Full-disk encryption (FDE) covers everything on the drive when the system is off, which is great for loss/theft scenarios. In addition to FDE, you can encrypt specific files or folders (useful if, say, you want an extra layer on a particularly sensitive set of documents, or if you're storing them in cloud storage). Tools like **VeraCrypt** can create an encrypted container (like a folder that you unlock with a password to access files inside). Many archive tools (7-Zip, etc.) can also encrypt archives with strong AES encryption – use that if you need to send or store an individual file securely. Just remember that if you decrypt and open a file, a plaintext copy might linger in temporary storage or recent file lists – so it's often better to work on encrypted volumes or use secure file viewers that don't leave traces.
- **Securely Deleting Files:** When you "delete" a file normally, it often isn't truly erased – it might just move to a trash folder or the space is marked as free but the data remains until overwritten. If you have sensitive files you want truly gone, **use secure deletion tools** or settings that overwrite the data. For example, on a solid-state drive (SSD), enabling whole-disk encryption and then forgetting the key is a way to effectively make data unrecoverable. There are

software like BleachBit or CCleaner that have secure erase options for specific files or free space. Be cautious: secure deletion on SSDs is tricky (due to wear leveling, the drive may have extra copies), so encryption is the safer bet from the start. As a rule, minimize retaining data you no longer need – it can't be leaked or seized if it doesn't exist.

- **Regular Backups (Encrypted):** Protecting data isn't just about keeping it secret, but also ensuring you don't lose it. Activists can't afford to lose important contacts, evidence of abuse, research notes, etc. Always have backups of critical files or information, ***and encrypt your backups***. For example, if you back up to an external hard drive, use an encrypted backup program or encrypt the drive itself – so if that backup drive is lost or stolen, it's protected. If you use cloud backup, choose services that offer encryption (or use your own tools to encrypt before uploading). Some secure cloud storage options: SpiderOak, Tresorit (with EU-based servers), etc., or using Cryptomator to encrypt files before putting them on Dropbox/Google Drive. Ensure that backup drives are stored in a safe place (and not right next to your laptop – a fire or theft that takes the laptop might take the backup too if they're together).
- **Backup Frequency and Strategy:** Follow the **3-2-1 rule** if possible: 3 copies of data, on 2 different media, 1 off-site. For example, one copy on your computer, one on an external drive at home, one in a cloud service. The idea is to have redundancy. How often you backup depends on how much work you can afford to lose. Daily or weekly backups are common. Automate it if you can (there are many tools that can run scheduled backups). Don't forget to include your phone data in backups too – e.g., Signal allows an encrypted backup of messages (Android) or if not, at least have contacts and 2FA recovery codes saved.
- **Special Case – Contacts and Address Books:** Your contacts list can be very sensitive (it essentially maps your network). Many people sync contacts to cloud accounts (like Google/Apple). Consider whether that's okay under your threat model. You might keep certain contacts only in a locally stored form (or use codenames). If you do sync, ensure your cloud account is very secure.
- **External Drives and USBs:** If you use USB drives or external disks to transfer data, those should be encrypted too if they contain anything sensitive. It's easy to lose a tiny USB stick. Modern OSs often have options to encrypt USB drives (BitLocker To Go on Windows, or macOS can encrypt external volumes via Disk Utility). Alternatively, only put already-encrypted archives on them. If you're handing a drive to someone, consider the trust level – you might be handing them the data in plaintext, which is fine if they need it, but be aware.
- **Cloud Storage Risks:** Cloud is convenient for sharing and backup, but keep in mind that unless you encrypt files client-side, you are ultimately trusting the

provider. They could be compelled to turn over data or could have a breach. Some providers do zero-knowledge encryption (meaning they don't have the keys), which is ideal. If you're using mainstream clouds (Google Drive, Dropbox, etc.) for convenience, you might at least encrypt particularly sensitive files before uploading (even just putting them in a password-protected ZIP archive can be a basic layer, though use a strong password). Also, be mindful when sharing cloud files – links can be forwarded. Prefer to add explicit collaborators instead of open links, and disable link sharing if not needed. **Always clear out data you no longer need online; don't treat cloud drives as archives for sensitive info unless you've locked it down.**

- **Managing Metadata of Files:** This overlaps with communication, but note that files (documents, PDFs, photos) often have metadata. A Word doc might have the author name, a photo might have GPS coordinates. Before sharing files publicly or with untrusted parties, scrub metadata if it could reveal something (there are tools like ExifCleaner for images, and you can turn off metadata in Office exports, etc.). Also, when publishing PDF reports, be careful – there have been cases where activists accidentally left author info or edit history in a document.

**By encrypting your stored data and keeping secure backups, you achieve two goals: adversaries can't easily read your info even if they get physical access, and you won't be crippled if devices are taken or destroyed.** Losing a laptop to theft is unfortunate, but it shouldn't mean losing the only copy of your evidence or your whole contact list – nor should it expose those to the thief. **Device security and data security go hand in hand.**

## 5.3 Malware Defense and Software Updates

Malware (malicious software) is a broad term for any program or code designed to do harm – whether it's spying, stealing data, or damaging systems. Phishing (covered in Chapter 6) often delivers malware, and activists can be targeted with custom malware by adversaries. Here's how to defend against these digital attacks and the importance of keeping software current.

- **Antivirus (AV) and Anti-Spyware Tools:** As mentioned, using security software is a basic line of defense. Windows 10/11 comes with Windows Defender, which is actually pretty decent these days – just keep it updated. There are also third-party AV suites (Avast, Bitdefender, etc.), though some activists avoid certain brands for trust reasons. On Mac, malware is less common but not unheard of; tools like Malwarebytes can be used for scanning if needed. On Android, only install apps from Google Play (and consider an AV app if you often handle lots of files). iPhones don't allow AV apps (the system is sandboxed), so your best defense there is simply updating iOS quickly and being careful with profiles or certificates you install (a common way iPhones

get compromised is via configuration profiles or enterprise certificates that load dodgy apps – don't install those unless absolutely sure).

- **Firewalls:** A firewall can prevent unauthorized connections. For most, the built-in OS firewall (Windows Defender Firewall or macOS Application Firewall) is enough and should be on. Be cautious if an app wants you to allow incoming connections and you're not using that feature. For advanced users or organizations, network firewalls can block known malicious domains or traffic patterns.
- **Avoiding Suspicious Links/Apps:** This is less a tool, more a behavior: **be very cautious with anything sent to you unexpectedly.** If someone emails a file or a link you didn't ask for, verify it. Attackers often craft emails or messages that look like they're from a colleague or ally. Double-check the sender's address (is it their exact email or a lookalike?), and when in doubt, reach out separately to confirm. On messaging apps, if an acquaintance sends you an odd file out of the blue, confirm they really sent it (their account could be hijacked).
- **Limiting Attack Surface:** Only keep software on your device that you actually need and trust. The more apps or plugins, the more potential vulnerabilities. Remove browser extensions you don't use (some could be taken over and turned malicious). If you installed some random video player or PDF converter once and no longer need it, uninstall it. Activists have at times been compromised through seemingly innocent apps that turned out to be backdoored or auto-updated to include spyware. **Stick to well-known apps from official sources as much as possible.**
- **Use Secure Messaging for Links:** Phishing links can be dangerous if clicked in email. One interesting approach: if someone needs to send you a link (say to a document or site), doing so via a secure messenger can actually add a layer of verification (since you know the contact and the channel is encrypted). Email is easier to spoof. That said, always be vigilant regardless of channel.
- **Zero-Days and High-End Threats:** If you're a high-profile activist or journalist, you might be targeted with "zero-day" exploits (attacks using unknown vulnerabilities). These can infect devices without any obvious user action (like receiving but not even answering a malicious WhatsApp call exploited a bug to install Pegasus). Defending against these is tough – this is where quick OS updates, using things like iOS's Lockdown Mode, and possibly segregating risky activities to a separate device comes in. Realistically, most activists won't face a zero-day; adversaries use them only if you're very high value. But it's good to be aware that it's a possibility in worst-case scenarios. If you suspect something (strange behavior on device, or you get a notification from a service about "state-sponsored attackers may be targeting you" – which Google, Facebook, etc. do send in some cases), seek expert help like from **Access Now's helpline or Citizen Lab**.

- **Handling an Infection:** If you discover or strongly suspect malware on your device, act quickly. Disconnect it from the internet (to stop data exfiltration). If you have access to tech support or an expert, consult them. If not, you might consider backing up important files (cautiously, in case they're infected), then wiping the device and reinstalling the OS from scratch. Change passwords to accounts using a ***different*** clean device (since **keyloggers** could capture them on the infected one). Inform colleagues if there's a chance data about them was compromised. It's better to err on the side of caution – malware can be very stealthy.
- **Isolation for High-Risk Tasks:** Some activists use separate devices for different tasks to contain potential compromises. For example, **a basic practice is not to use your primary work computer for random web browsing or personal email** – use a secondary device for that, or at least a separate browser profile. In a more extreme form, some use one phone for messaging and another "clean" phone for sensitive calls, or a dedicated laptop that only connects through Tor for certain research. It's not practical for everyone, but **compartmentalizing** can ensure that even if one device gets hit with malware, the others remain safe (so a spy program on your browsing laptop won't see your confidential documents if they're only on a different offline computer).
- **USB Security:** Be careful with USB drives or accessories. As mentioned, don't plug in drives from unknown sources. Also **beware of USB charging stations** ("juice jacking" attacks can load malware via a USB charging port) – **use your own charger or a USB data blocker** (a little adapter that allows only power, not data, through). If someone hands you a USB drive to share files, ideally scan it first, or better yet, have them upload files via a secure cloud method instead.
- **QR codes infection threat:** Scanning random QR codes poses significant security risks as attackers can easily embed malicious links or payloads into them, leading unsuspecting users to harmful websites, phishing pages, or automatic downloads. QR codes can redirect devices to fraudulent login portals designed to harvest credentials, trigger malware installation on poorly secured phones, initiate payment requests, or alter device settings through deep-linking exploits. In some cases, attackers replace legitimate QR codes in public spaces—such as parking meters, restaurants, or transit stops—with malicious "quishing" codes that mimic trusted services. Since users cannot visually detect what a QR code contains, **scanning random or unverified codes can expose devices and personal data to infection**, credential theft, or financial fraud.

Staying malware-free requires a mix of tools and mindful behavior. By keeping systems updated, using security software, and treating unexpected files/links with skepticism, you eliminate the vast majority of threats. **The goal isn't to be paranoid,**

**but to be prudently cautious** – once you establish these habits, they become second nature and greatly reduce your risk of a successful cyberattack.

## 5.4 Physical Security of Devices

We've largely covered digital threats, but physical security of your gear is equally important. Activists often operate in unpredictable, sometimes hostile environments – devices might be seized in raids or at border checkpoints, stolen during travel, or tampered with when you're not looking. Here's how to handle those scenarios:

- **Plan for Borders and Checkpoints:** When crossing international borders (or domestic checkpoints in certain countries), authorities may have legal powers to search devices. If you're entering a high-risk country, consider carrying "clean" devices – only the data/apps you need for the trip, nothing sensitive. Use cloud storage to download what you need once inside (preferably over VPN), or carry data separately in a secure form (e.g., on an encrypted USB that you can choose not to divulge). Some activists use throwaway accounts or secondary phones when traveling. At the very least, power off devices (so that full-disk encryption is in effect) before reaching the checkpoint. If asked to unlock, know the laws/risks: refusing might lead to confiscation or worse, so it's a personal decision. Some protections: both iOS and Android have a feature that after several failed unlock attempts will auto-wipe (you must enable this – e.g., on iPhone, "Erase Data after 10 failed passcode attempts"). Just remember if you enable it, it will truly erase if an inquisitive officer or child plays with it and hits the limit.
- **Traveling Light (Data-Wise):** Don't carry data you don't need. Before traveling to a protest or through a sensitive area, purge especially risky info from your devices (and make sure it's securely backed up elsewhere). Think of it as "**If my phone is taken right now, what would I not want on there?**" – then remove that. For example, maybe clear out Signal chats that have done their purpose, or sign out of accounts that could be used if forced to unlock. Some apps have a "travel mode" (ProtonMail has one for their app, for instance, that can temporarily remove data). You can also simply delete an app (like a password manager) before a risky event, and reinstall later.
- **Prevent Device Access If Seized:** If you see that a raid or arrest is about to happen, and you have a moment, you could quickly power off or at least lock your device. On iPhone, there's a shortcut: rapidly pressing the side button 5 times will trigger an SOS mode that also disables Touch ID/Face ID (requiring the passcode to unlock). That's handy if you're worried someone might forcibly use your finger or face. On Android, **remove trusted face/finger unlock in security settings if anticipating trouble**, so only the PIN works. If you have time and it's really dire, you might factory reset the phone – but that's

extreme and you'd lose your data (hopefully backed up). Better is planning ahead so nothing too sensitive is on it.

- **Anti-Theft Tools: Enable device-finding and remote-wipe features.** Both Apple (Find My iPhone) and Google (Find My Device for Android) allow you to locate a lost device and remotely erase it. This requires the device to be online though. Still, if something is stolen, you might log in to your account on a safe computer and hit erase – at least as soon as the thief connects it, it will wipe (assuming they haven't immediately put it in a Faraday bag or turned it off). Don't attempt to physically recover a stolen device yourself if it's in unsafe territory – the data safety is priority, not the hardware.
- **Tampering and "Evil Maid" Attacks:** This refers to an attack where someone has brief physical access to your device (like a maid in a hotel room) and they install something malicious. To mitigate: **Keep devices with you as much as possible.** Use a laptop lock for longer unattended stretches. You can get tamper-evident tape or seals to put on your device screws or ports – at least you might tell if someone opened it. In high security mode, you might not trust a device that was out of sight – you might re-install OS if you suspect something. This is usually only a concern if you're targeted by very sophisticated adversaries (intelligence agencies). But unsurprisingly, confiscating laptops and returning them with malware is rather the rule than the exception in some regimes. If you suspect that, stop using it until it can be checked by an expert (or nuke and pave – wipe and reinstall everything).
- **Protecting Devices in Crowds:** At protests or public events, pickpocketing or snatch-and-grab thefts can happen. Use a strap or keep phones in a front pocket. **Consider using a privacy screen filter on your phone** if you're worried about shoulder-surfing (someone looking over your shoulder at messages). Also be mindful who's around if you're unlocking your phone – shield your PIN entry.
- **Durability:** Not security per se, but consider rugged cases or waterproof pouches if you expect harsh conditions (rain, tear gas, rough handling). A destroyed device won't leak data if encrypted, but you also lose your tool. Some activists carry older backup phones (with minimal data, but at least a means to communicate) in case their main phone is out of commission.
- **Human Element – Coercion: No security measure on a device can withstand coercion.** If someone forces you under threat to unlock, you may have to. This is where having nothing sensitive there (or having layers, like a hidden encrypted partition with a different password – a concept called plausible deniability) comes in. **Some full-disk encryption tools allow a decoy password that unlocks a harmless set of data, while the real data remains hidden.** This is advanced and can be risky if done wrong. Use of such features is not very common, but it exists (VeraCrypt offers hidden volumes, for

example). More practically, think about your personal security plans: if arrested or detained, at what point would you comply with device access? It might be safer to sacrifice the device/data than to suffer personal harm. It's a tough call that each must make for themselves and their context. Ideally, strong encryption means even if you do comply, the truly sensitive info isn't there or isn't accessible.

In summary, treat your devices as valuable assets that adversaries might attempt to physically obtain. By preparing for that (through encryption, minimized data, strategic device use, and quick action when needed), you can substantially mitigate the damage if it does happen. Losing a device is annoying and possibly expensive, but it shouldn't expose your entire organization or network. Always consider both the digital and physical dimensions of security – they complement each other.

### Checklist: Device & Data Protection

- **All my devices (phones, computers, external drives) are protected with strong passcodes/passwords and encryption. I have enabled auto-lock and my devices lock quickly when not in use.**
- **I keep my device software up-to-date, and I only install apps/software from trusted sources. Unneeded or outdated apps have been removed.**
- **I run antivirus/anti-malware and I'm careful with attachments or links, especially from unknown sources. I also use a firewall and avoid using administrator rights unless necessary.**
- **I have secure, encrypted backups of important data, stored separately. I've tested that I can recover files from my backups. I do not rely on a single device as the sole holder of critical information.**
- **I have a plan for travel or high-risk situations: carrying minimal data, possibly using alternate devices or accounts, and knowing how to remotely wipe a device if needed.**
- **My devices have tracking/remote-wipe enabled. If a device were lost or stolen, I know how to locate or erase it (or who to contact for help).**
- **I practice good physical security: devices stay with me or are locked up when unattended. I'm cautious about plugging in unknown USBs or chargers. I also consider the physical safety of where I store backups or sensitive papers.**

- **I understand that no device is 100% secure; I have thought about what I would do if my device was compromised or seized. I have identified particularly sensitive data and taken extra steps to shield or compartmentalize it (or I've consciously decided not to keep it on my personal device at all).**

***(Having secured your accounts, communications, and devices, we'll now move on to a major threat that often targets activists: phishing and social engineering – essentially, the "hacking" of humans through deception.)***

# 6. Phishing and Social Engineering: Staying Vigilant Online

Not all attacks involve technical wizardry – many of the most effective ones **simply trick you into letting the attacker in**. Phishing and social engineering are about conning people, via email, messages, or calls, into revealing passwords, downloading malware, or otherwise doing something against their interest. Activists, NGO staff, and journalists are frequently targeted by these tactics because it's often easier to **ask** someone for their password (under false pretenses) than to technically hack into a system. In this chapter, we'll explain common phishing methods, how to recognize the signs, and how to respond.

## 6.1 Understanding Phishing Tactics

"Phishing" generally refers to **fraudulent attempts to get sensitive information** (like login credentials) or to **get you to run malicious code, by posing as a trustworthy entity.** While "phishing" originally described broad, generic bait (like mass emails saying "Your bank account is locked, click here"), many attacks on activists are **spear phishing** – highly targeted and personalized lures, sometimes even mentioning your work or appearing to come from someone you know.

- **Email Phishing:** This is classic – you receive an email that looks like it's from a service (Google, Facebook, Office365) or a colleague/partner. It often contains an **urgent call to action**: ***"Your account will be suspended, log in here to verify"*** or ***"Check out this important document immediately."*** The link provided typically goes to a fake login page that steals your password, or triggers a malware download. The email may use logos, spoofed addresses (e.g., account-security@google.com but actually sent from a lookalike domain), and sometimes personal touches (your name, or context that makes it believable).
- **Spear Phishing Examples:** Activists have faced campaigns where the phishing emails were extremely convincing. For instance, in one case, after a well-known activist was arrested, their colleagues received an email that appeared to be from a familiar NGO ally with an attachment named "ArrestWarrant_[ActivistName].pdf" – given the chaos, someone might

urgently click it, but it was a booby-trapped file. In an Eastern European country, an attacker cloned Google login pages with slight URL tricks (e.g., "accountsgoog1e.com" using a "1" instead of "l") to phish civil society members' credentials. These are real examples of how tailored phishes can be.

- **Other Social Engineering:** Beyond emails, phishing can come via text messages (SMS phishing is called "smishing"), via messaging apps, or phone calls ("vishing"). You might get a text like ***"Your WhatsApp code is 123-456. If this was not you, visit example.com/support"*** (where the site is fake and asks for your info). Or someone calls claiming to be tech support: ***"Hi, I'm from [Big Tech], we detected a problem with your account. We need to verify your identity – could you confirm your password for us?"*** Or ***"We need you to install this security app to fix the issue."*** **These pretexts are all about urgency and authority to lower your guard.**
- **Watering Hole Attacks:** Another variant – instead of directly baiting you, attackers may compromise a website that their targets are known to visit (like a forum or a resource site for NGOs), and plant malware there. When you visit, it might prompt you to download something (like "update your Flash player"). This is less personal but can ensnare many in a community. Essentially the attacker poisons a "watering hole" where the target group frequents.
- **Bait with Something Positive:** Not all phishing is scary warnings. Some offer enticing things: ***"Congratuations! You've received a grant/invitation, open the attached document for details."*** Activists could be lured with promises of funding, conference invites, media opportunities, etc. Always verify such offers through other channels if they're unsolicited.
- **Multi-Step Attacks:** Sometimes phishing is one part of a larger plan. For example, an initial phish might steal your email password. The attacker then logs in, and uses your email to reset passwords on other accounts or to phish your colleagues (since an email from you is trusted). Another scenario: they phish an account that's not their end goal, but from it gather info or contacts to go after a bigger target (maybe they compromise a small partner NGO to eventually reach the larger organization). **Be aware that a single lapse can cascade.**
- **Why It Works: Phishing preys on human traits – trust, fear, urgency, curiosity. The messages are designed to make you act without thinking.** They often impersonate legitimate entities convincingly. And technically, they often use lookalike domains or URLs, and sometimes even valid SSL certificates (the padlock in browser) so the fake site looks secure. For instance, an email might link to http://security-google.accounts.com/verify – glancing quickly, you see "google" and "secure" in there, but it's a bogus domain (notice it's actually under "accounts.com" domain). These tricks can fool even careful people who are busy or distracted.

Understanding these tactics is the first step. **You realize that any unexpected communication asking for sensitive info or strange actions must be treated skeptically, no matter how authentic it appears.** In the next section, we'll get into specific red flags that often betray a phishing attempt.

## 6.2 Common Signs of Phishing Attempts

While phishing emails and messages can be very crafty, they often have tells – little inconsistencies or suspicious elements – that give them away. **Train yourself to pause and inspect anything that asks you to enter credentials or click a link.** Here are some red flags:

- **Mismatched or Strange URLs: Before clicking, hover over links** (on a computer) or long-press (on mobile email apps) to preview the URL. Is it actually the site it claims? For example, an email says "Update your Gmail settings" but the link goes to http://mail.google.verify-acc.com. That's not Google – it's a lookalike. Attackers register domain names that resemble real ones (using parts of the name or swapping characters). Check the domain carefully. If it's not an exact match for the official site (and by that we mean the part right before the .com or country domain), be very wary. Even better, don't click the email link – **go manually to the service's known website if you suspect an issue.**
- **Urgency or Threats:** Phishing often tries to scare you: ***"Immediate action required – your account will be closed in 24 hours!"*** or ***"Your organization will lose funding if you don't respond now."*** **That pressure is designed to make you panic.** Real services generally don't threaten account closure via such short notice emails. Likewise, **any coercive language like "legal action will be taken" is suspect** if it comes via email out of the blue.
- **Grammar and Spelling:** Many phishes come from overseas or are thrown together quickly. They might have odd phrasing or typos. Example: ***"Dear Gmail Customer, You account have problem, click verify link immediatly."***. Obvious mistakes like that are a dead giveaway. However, note that some spear phishers are very fluent – so absence of errors doesn't guarantee legitimacy. But if you see errors and weird capitalization or **generic greetings ("Dear Customer" instead of your name)**, be on high alert.
- **Odd Sender or Reply-To:** Check the sender's email address. It might say "Google Support" in the name, but the actual email might be support@accounts.gooogle.com (with a triple o) or something completely unrelated like fjk23@mail.ru. Also watch for the Reply-To header: sometimes the email says from a legitimate address but if you hit reply it goes to a different one. That's a sign of trickery. If it's supposedly your friend emailing, is it their exact address or one letter off? Some targeted phish use lookalike individual

addresses (like john.doe@activistgrp.org vs. the real john.doe@activistgroup.org).

- **Unexpected Attachments:** If an email you didn't expect comes with an attachment, especially a strange file type (e.g., a .zip or .exe, or an Office document with macros), be extremely cautious. A common phishing ploy is to send a document titled innocuously (agenda.docx, invoice.pdf) but it contains malware. If the email is supposedly from someone you know but the tone is odd ("Here is the file you asked for" when you didn't ask), verify with them before opening. Modern Office documents can carry macro malware; unless you're sure, don't enable editing/content if prompted.
- **Requests for Sensitive Info: Legit companies will never ask for your password via email.** Banks and services also won't email you asking to confirm personal details like your full social security number or credit card – they usually direct you to log into your account normally. If an email is directly asking for passwords, private keys, one-time 2FA codes, etc., it's almost certainly a scam. Also beware of links to what looks like a login page – that's the phish goal. **Always consider: who initiated this? If it's not you, be suspicious.**
- **Too Good to Be True:** Just as threats are suspicious, so are windfalls. "You've won a prize!" or "We want to donate $10,000 to your cause, just fill this form" – spam and phish often dangle money. **Use healthy skepticism.** Why would someone out of nowhere offer this, and why via a generic email? **Real donors or opportunities usually come after some prior interaction or are addressed personally.**
- **Context Mismatch:** Phishers sometimes don't get details exactly right. For instance, you get an email from "Microsoft Office 365" about your mailbox – but your organization uses Gmail, not Office 365. Or a security warning from a service you don't even use. Obvious mismatch – delete it. Sometimes the clue is subtle: maybe they mention an old company name, or reference a "recent transaction" you never made. These clues say it's a mass phishing attempt that isn't tailored correctly.
- **Unusual Contact Method:** If someone you know suddenly emails from a different address claiming their main one is broken and asking you for something odd, or a stranger gets very friendly and asks for help with a favor (that leads to clicking a link), these can be social engineering setups. It's not always about credentials; could be to gain trust and then ask for other info. Essentially, question when the mode or tone of communication deviates from the norm: e.g., a colleague who always calls you, but now sends an urgent email to wire money – likely their email was hacked or spoofed.

**Keep these signs in mind and share them with your team so everyone is aware.** Phishers often send to many staff in hopes one will bite, so all it takes is one person

not recognizing the signs. Next, we'll outline how to systematically defend against phishing attempts and respond if you suspect one.

## 6.3 Real-World Example: Targeted Spear Phishing

To underscore how convincing phishing can be, consider a real campaign targeting civil society in Azerbaijan. In January 2020, a veteran human rights lawyer received an email that appeared to come from a colleague, with a link to download case documents. Given the context – it arrived amid a sensitive legal battle – he felt pressure to open it. However, the email was a fake: the attackers had mimicked the colleague's address and used a seemingly legitimate file-sharing link that actually delivered spyware. In another incident from the same campaign, multiple NGOs got emails supposedly from a Council of Europe committee with a WeTransfer link from an official-looking sender. The link contained malware that, once opened, would silently install and give the attacker full access to the device. These spear phishing attempts were carefully timed and crafted to exploit trust and urgency.

Another example: cybersecurity researchers reported phishing attacks against Eastern European activists that impersonated Google login alerts. The emails looked like Google warnings and directed users to "verify" their accounts on a site that at first glance seemed like Google's domain. In reality, the attackers had registered attacker-controlled domains with minor spelling alterations (for instance, using a Cyrillic letter that looks like a Latin one in "google.com") to host fake login pages. Dozens of such lookalike websites were set up to capture credentials, showing the lengths phishers will go. Some campaigns even evolved to employ "man-in-the-middle" phishing kits – essentially proxy websites that pass through to the real site after stealing your login, allowing them to potentially grab 2FA codes as well by acting in real-time. This demonstrates that for high-value targets, phishers can innovate and use very sophisticated tricks.

However, even these advanced attacks had tells: slightly odd URLs, unexpected sources, or out-of-place requests. For example, the Azerbaijani lawyer noticed the email was sent only to a small group and something "felt off," prompting him to double-check by contacting the colleague through a different channel – which saved him from infection. And in the Google impersonation case, only users on high alert caught that the domain wasn't exactly google.com; others who were less attentive fell for it. It highlights that **a critical eye can make the difference.**

A stark reminder of phishing's danger came to light when information obtained via phishing was used to persecute activists. In Russia, for instance, state-linked hackers stole email passwords through phishing and then used the contents of private communications to build criminal cases accusing activists of being "foreign agents" or traitors – leading to arrests and imprisonments. All it took was a series of well-crafted "account verification" emails and fake login sites to compromise those accounts.

These examples reinforce why constant vigilance is needed. Even the most security-savvy person can slip momentarily – especially if caught at a busy or stressful time. That's why multi-layered defenses (like 2FA, browser warnings, and good backups in case malware hits) are important: they provide safety nets. But fundamentally, your mindset is the best defense. **Assume that unexpected requests for your login or for running a file are malicious until proven otherwise.** It's a bit like healthy paranoia – trust, but verify through another channel.

## 6.4 Defending Against Phishing and Scams

Here are concrete steps and habits to defend yourself and your organization against phishing and social engineering:

- **Slow Down and Verify: Cultivate a habit of not reacting impulsively to any email or message** that asks you to do something involving credentials, clicking a link, or opening an attachment. Scammers rely on that knee-jerk reaction. Take a breath and inspect. If "Google" emailed you, don't click the email link – instead, go open your Google account via your usual method (bookmark or type the address) and check for any alerts there. If your "bank" texted you a number to call, use the official number on your card instead. If a "colleague" sends a weird request, call or message them on a known channel to confirm. Essentially, whenever something asks you for sensitive action, use a second factor: a secondary communication or method to verify it's legitimate.
- **Hover or Preview Links:** Always check where a link is actually going **before** clicking. On a computer, hover your mouse over the link and look at the status bar or right-click and "Copy Link" (then paste it somewhere safe to see it). On mobile, you can often long-press the link to see the URL. If it's not clearly the official domain you expect, do not proceed. Also, be aware of URL shorteners (bit.ly, tinyurl) – those obscure the destination. If an official email uses a shortener, you can use a URL expander service to see the real link or just be extra cautious. When in doubt, navigate to the site yourself rather than through the provided link.
- **Educate Your Team: Phishing often succeeds by hitting the most unaware person in an organization.** It's crucial to regularly share tips and examples with colleagues. **Consider circulating particularly convincing phishing examples you've seen** (or from reports) so people know what to watch for. Encourage a culture where if anyone receives a strange email, they can easily ask your IT person or just share in the team chat, "Hey, I got this – is it legit?" without feeling stupid. It's much better to double-check than to silently fall victim. Some organizations even do periodic internal phishing drills (sending fake phish to staff to see who clicks, then training them), but at minimum, keep the

conversation alive. Emphasize it's not about blame – attackers are sneaky, and we all have to watch each other's backs.

- **Technical Safeguards:** Use the anti-phishing features available. Many email providers (Gmail, Outlook) automatically flag emails that look phishy (like those coming from domains similar to your company). Pay attention to those warnings. Enable two-factor authentication on accounts so that even if a password is phished, the attacker can't log in (as we discussed in Account Protection). If your email system allows, implement SPF/DKIM/DMARC – these are anti-spoofing technologies that make it harder for attackers to send emails pretending to be from your domain (this is more for your IT admins, but it's good to know it exists – it can reduce how many fake emails get through). Also, modern browsers and even some email clients have gotten better at warning about known phishing sites – don't ignore those red screens or alerts.
- **Browser and Software Settings:** Ensure your browser's phishing and malware protection is on (most are by default – e.g., Chrome's Safe Browsing). If your organization uses a managed IT environment, consider adding known malicious domains to a block list at the network level. Some advanced users run web content through isolators or use virtual machines for risky activities. At least, try to open potentially sketchy links in a secure environment – e.g., if you really want to check a link, you could use an isolated browser profile or a service like VirusTotal's URL checker to see if it's reported malicious.
- **Multi-Factor Everything: As repeated, 2FA is a lifesaver in many phishing cases.** Even if you accidentally hand out your password, most phish won't also get your second factor unless it's a highly sophisticated live attack. Use app-based or key-based 2FA, as SMS codes can be phished more easily (attackers can trick you into giving the code). Some attackers have started using reverse proxies to nab 2FA tokens (as mentioned), but those are rarer; and methods like physical security keys can thwart them. So layer up your login defenses.
- **Password Managers Clue:** One fringe benefit of password managers: **if you use one that autofills passwords, it typically only fills on the correct domain.** So if you go to a fake site that looks real but isn't, your password manager ***won't*** auto-fill because the URL doesn't match. That's a big red flag – if usually you click Gmail and it fills, but this time it doesn't, you might be on a phishing page. So, using a manager can actually serve as an early warning system too (besides making your creds strong).
- **Limit Public Info that Helps Phishers:** Social engineers often gather info about you from social media to craft a believable message (this is called OSINT – open-source intelligence). Be mindful of what you share publicly – like maybe don't post that you just applied for a certain grant, or details that could be used to guess your security questions, etc. **The less they know, the harder it is to**

**personalize a phish.** Also, be cautious when sharing your work email on public sites – using a format like "name [at] org.org" can prevent automated scraping.

- **If in Doubt, Ask:** Really, a key defense is a skeptical mindset. If something feels a bit "off" or too coincidental, don't dismiss that gut feeling. It's better to verify with a colleague or tech support than to ignore it. Attackers try to exploit embarrassment (you might think "I should know if this is real or not, I won't ask" – don't fall for that). Phishing is not always obvious; smart people get duped. So it's absolutely fine to get a second opinion whenever. I.T. support or a savvy friend would much rather take a minute to say "yep that's fake" than have to deal with a breach aftermath.

And finally, **be prepared**: Despite best efforts, one day someone might click something. Make sure you have good backups, incident response plans (as in Chapter 10) and know how to reset accounts quickly. That way, a phishing slip-up remains a nuisance, not a catastrophic loss.

### Checklist: Phishing Prevention

- **I and my team are aware of common phishing tactics (urgent requests, lookalike addresses, etc.) and we make a habit of verifying unusual messages through secondary channels.**
- **We never enter passwords or sensitive info on sites that came via an email link without double-checking the URL or navigating to the official site ourselves.**
- **We have enabled two-factor authentication on our accounts, providing an extra hurdle against phishing. We treat any unexpected request for our 2FA code as highly suspicious.**
- **We use tools like email spam filters, browser safe browsing, and possibly corporate safeguards to reduce phishing emails. We pay attention to any warnings these systems give us.**
- **We update our software (especially browsers and email clients) so that we have the latest security protections. Our email provider's anti-phishing measures (like Gmail's warnings) are active.**
- **Our organization encourages a culture of "ask before you click." If any staff member is unsure about an email or link, they know who to ask, and they won't be blamed for erring on the side of caution.**

- **We regularly back up critical data and have an incident plan, so if a phishing attack does lead to malware or account compromise, we can respond quickly to contain damage.**

***(Having armored yourself against phishing, the next section will address keeping your mobile devices safe – since phones require some extra considerations beyond general device security.)***

# 7. Mobile Safety: Protecting Your Smartphone

Smartphones deserve special attention in digital security. Activists rely on them heavily – for communication (calls, messaging), coordination (social media, maps), and documentation (photos, videos). But phones also carry unique risks: they're mobile (easy to lose or steal), often always online, and continuously generating data (location, etc.). They also tend to integrate personal and work life in one device. This chapter covers how to safeguard your mobile device from both digital threats (like spyware or malicious apps) and physical/world threats (like confiscation at protests or border searches).

## 7.1 Securing Access to Your Mobile Device

The first line of defense is controlling who can access your phone. Many of the device security principles from Chapter 5 apply, but let's reiterate and add mobile-specifics:

- **Strong Unlock PIN/Password:** Use a strong PIN or password to unlock your phone. As mentioned earlier, 6 digits minimum for PIN (10^6 possibilities), or an alphanumeric password for even better security. Avoid common patterns (123456, birthdates, etc.). Yes, typing a long password on a phone is a bit slower, but consider the sensitivity of what's on there. If a short PIN is your compromise, at least ensure it's not trivial (and consider using an extended length PIN if your phone allows, e.g., 8 digits).
- **Biometrics – Pros and Cons:** Fingerprint or face unlock is very handy. It's generally secure enough for typical scenarios (difficult for someone to spoof your fingerprint or face without effort). However, as discussed, in some situations like an arrest, authorities might physically force or trick you into unlocking with biometrics. It has happened – police have held phones up to protestors' faces. So, if heading into a risky situation, it might be wise to disable Touch/Face ID temporarily (both iOS and Android have shortcuts or settings to do so). On iPhone, squeeze the side buttons or rapidly press power 5 times to disable FaceID until the passcode is entered. On Android, you might find a similar lockdown mode in settings or via a power menu option depending on the device.

- **Auto-Lock Quickly:** Set your phone's screen to auto-lock after a short period of inactivity (like 1 or 2 minutes). It's inconvenient if it locks while you're reading something, but you can always tap to keep it awake. The danger of a long auto-lock (5-10 mins or never) is if someone snatches it or you leave it briefly, it's wide open. Also, enable the setting to lock immediately when the screen is turned off (some Androids have an option to delay locking after screen off – don't use delay).
- **SIM PIN:** Most SIM cards can have a PIN code such that if the phone restarts or the SIM is put in another device, the PIN must be entered to connect to the mobile network. This prevents someone from stealing your SIM and using it (or pulling your contacts off it, though nowadays contacts are usually in cloud). It's an extra layer and definitely recommended if SIM swap attacks are a concern or if you're in a situation where device might be taken (the adversary might otherwise remove SIM to avoid remote tracking or to put in another phone to get 2FA SMS, etc.). Just don't forget your SIM PIN or you'll need the PUK code from the carrier to reset.
- **Secure Lock Screen Settings:** Most phones let you hide notification content on the lock screen. Use that, so incoming texts or messages don't display their content unless unlocked. **Otherwise someone could glean verification codes or sensitive info from a locked phone.** Also disable things like lock screen access to Siri/Google Assistant for sensitive tasks. For example, older iPhones allowed asking Siri "show contacts" even when locked (Apple has mitigated many of these, but check settings like "allow access on lock screen" and disable anything you don't need). Similarly, limit what can be done from lock screen (replying to messages, etc., may allow some access).
- **Anti-Theft (Find My Phone):** Enable find-my-phone features (Find My iPhone or Google's Find My Device). Not only do these help you locate a lost phone, they let you remotely erase it. Ensure these are active and tested. On Android, also check that you have a Google account associated that you know the credentials for, as that's needed to use the service. With iPhones, "Find My" ties to your Apple ID and also activates Activation Lock (meaning even if wiped, your Apple ID must sign in to reactivate the device – deterring theft resale).
- **Updates on Mobile:** Mobile OS updates often fix serious security flaws. Both Android and iOS frequently patch things like privilege escalation or remote code execution bugs. Apply updates promptly. On Android, fragmentation is an issue (not all get latest OS), but at least ensure you get monthly security patches from your manufacturer. If your phone stops receiving updates (older than ~3 years), consider that a security liability especially if you're a high-risk user – you might need to upgrade for the sake of security patches. Also update apps via Play Store/App Store; many phone compromises happen via outdated app vulnerabilities.

- **Limit Lock Screen Info:** As an extra, consider putting owner info or an emergency contact on your lock screen (many phones allow a custom message). This is more for if a good Samaritan finds your phone, they know who to reach. But don't put your full address (no need to help stalkers); something like an email or alternate number is fine.
- **Backups for Phones:** Use the cloud backup options (iCloud backup, Google backup) or a local encrypted backup (e.g., via iTunes or Android's adb backup) regularly. Phones can be lost or seized – having a backup means you can restore your data to a new device or once returned. Just ensure backups are secure: iCloud backups are encrypted but Apple holds keys (except for certain data like Health or if you enable advanced data protection); think about what's in your backup. If you have especially sensitive data, maybe exclude it or back it up separately with encryption.
- **Panic Passwords:** Some devices (very few, mostly specialized or with third-party apps) can have a duress PIN that does something different (like wipe the phone or call a certain number). Most folks won't have this, but it's worth knowing such concepts exist. For instance, certain secure phone ROMs/OSs or apps offer a feature where one code opens a decoy environment. If that's something you absolutely need (maybe in extreme authoritarian regimes), it requires technical setup and practice to use right.

Securing access is all about making sure if your phone ends up in the wrong hands, it's hard for them to get in. Combined with the encryption that's on by default on modern phones, a strong lock means your data remains confidential. Now let's address safe use of apps and settings that can leak info.

## 7.2 Safe App Use and Device Settings

Our smartphones are only as safe as the apps we install and the settings we configure. Activists should be deliberate about which apps to use for sensitive communications and how to configure privacy on their devices.

- **Choose Trusted Apps:** Stick to official app stores (Google Play, Apple App Store) for app downloads; they are not foolproof but at least have some vetting. Third-party app stores or direct APKs on Android could be risky unless you fully trust the source (some activists in censorship regions use alternative stores – if so, limit that to a spare device if possible). Research apps before installing: does this app really need these permissions? E.g., a simple game requesting access to your contacts and microphone is suspicious. Prefer apps that are well-known and open-source for critical functions (for secure messaging, use Signal or WhatsApp rather than some random new chat app).
- **App Permissions:** Audit your app permissions regularly. Both iOS and Android let you view what permissions each app has (camera, location, contacts, etc.).

Revoke anything that isn't needed. For instance, if you have given a photo editing app access to your location and it has no reason for it, turn that off. Newer OS versions even allow one-time permissions or "only while using app" – utilize those for things like location or camera if possible. Be especially careful granting Accessibility permissions on Android or the equivalent power-user permissions – malware often tricks users into enabling Accessibility, which then gives it broad control (like reading screen content, entering keystrokes). Only give that to known apps that truly need it.

- **Messaging and Calling Apps:** Use end-to-end encrypted apps for calls and texts whenever you can (as discussed in Secure Communication). Also be aware of what data messaging apps store on the device. For example, WhatsApp encrypts chats in transit, but stores them on your phone (possibly in backup too) – secure your phone and consider enabling WhatsApp's own encrypted backup feature now available. Signal by default keeps everything only on the device (no cloud backup unless you enable a local encrypted backup). Some apps like Telegram are not E2EE by default (cloud-based chats), so use their Secret Chat feature for anything sensitive or use a different app. Also note, many messaging apps have settings for screen lock or registration lock – for instance, you can set a PIN for Signal that's required when registering your number on a new device (prevents SIM swap hijackers from stealing your Signal account). Use those features.
- **Email on Mobile:** If you access email on phone, consider which app. The official Gmail/Outlook apps are fine, but if you use a generic email client, ensure it uses encryption (IMAP over SSL, etc.). Many email apps cache a lot of email locally – which is fine under phone encryption, but just be aware that if someone has device access, those emails might be accessible. Some secure email providers have their own apps (ProtonMail). Using those can add extra layer (since they might not store data if you log out).
- **Browser and WebViews:** If clicking links from messages on mobile, same phishing cautions apply. Mobile browsers show less of the URL by default, which phishers exploit. You can usually tap the address bar to see full URL. Avoid entering login credentials on a mobile browser unless you are absolutely sure – if possible, use the service's official app or known bookmarked site. Also be careful of in-app browsers (WebViews) – e.g., Twitter opening a webpage inside the app. Those might not show the URL clearly or might not have the same protections. If needed, copy the link and open in your main browser.
- **VPN for Mobile Internet:** If you connect to public Wi-Fi frequently, use a VPN on your phone as well to encrypt your traffic (just like on a laptop). Public Wi-Fi can lead to snooping or fake hotspots. On Android and iOS, there are many VPN apps – choose a reputable service (and remember, the VPN provider can see your traffic, so pick one with a good privacy track record, or use something like the TOR Browser app for specific browsing).

- **Location Services:** Phones are constantly generating location data. For personal safety and privacy, review which apps have location permission. Does that weather app need background location or can you set city manually? Both iOS and Android now often show a little icon if an app is using location in background – pay attention to that. Also consider turning off precise location for apps that don't need it (iOS allows giving approximate location). **If you're going to a sensitive location (like a protest or a meeting), and you don't need your phone's location on, you could toggle Location off in quick settings temporarily or enable airplane mode** (though then you lose connectivity). Note that even with GPS off, the cell network can approximate location, but it's less precise. Some activists carry **faraday bags** to fully block signals when travelling to secret locations (this means phone is unusable until out).
- **Device Analytics & Cloud Sync: Opt-out of sharing device analytics/usage data with Apple, Google, or app developers** if possible (both platforms have settings to limit sending diagnostics – small thing but adds privacy). Be mindful of what you sync to cloud. For example, many people have all their photos auto-upload to Google Photos or iCloud Photos. Think about whether any images could endanger someone if cloud were breached or accessed. Maybe have a separate non-cloud camera app for highly sensitive captures.
- **Jailbreak/Root Caution: Avoid jailbreaking or rooting your phone** unless you really know what you're doing and have a specific need. It disables many built-in security features, and you could inadvertently allow malicious apps deeper access. An un-rooted phone is harder for malware to deeply infect.
- **Bluetooth, Near-Field Communication (NFC), etc.:** Turn off radios when not in use. Bluetooth (BT) has had vulnerabilities and can potentially be used for tracking. If you don't need it, disable it, especially in sensitive meetings (there is known Bluetooth-based malware and certainly BT can leak device name and presence). Similarly, NFC or other services (AirDrop) – only turn them on when needed and set them to not accept from unknown contacts by default.
- **App Updates:** Update your apps frequently because patches fix security issues. Both mobile OS can auto-update apps (or at least notify). Try to keep that on Wi-Fi to not kill data. Outdated apps might have known exploits an attacker with physical access could leverage, for example.

With careful selection of apps and attention to permissions and settings, you greatly reduce the phone's attack surface. One key is also minimizing the sensitive data apps have access to, so even if one gets compromised, the damage is limited.

## 7.3 Travel and Protest Considerations for Phones

Mobile safety in the field – whether attending a protest, crossing a border, or visiting a high-risk region – requires some additional precautions:

- **Burner Phone vs. Main Phone:** In some situations, activists use a basic secondary phone (or a cheap smartphone with minimal data on it) when they expect possible confiscation or surveillance. For instance, **at a protest where police might snatch phones, you might carry a phone that doesn't have your entire digital life on it** – maybe just a means to communicate. If detained and it's taken, your main data is safe at home. If traveling internationally, consider a travel-only device with just the necessary contacts and info. The downside is inconvenience and expense of extra device, but it's a trade-off for security/privacy. At least consider removing especially sensitive data from your primary phone before such events (e.g., log out of certain accounts, uninstall some apps).
- **Pre-Event Checklist:** Before going to a protest or sensitive meeting, review what's on your phone. Delete any messages, call logs, or photos that could be misinterpreted or used against you or others if the phone is searched. Many messaging apps let you clear chat history (Signal can auto-delete messages after set time – use that if needed leading up to event). Also, ensure your phone is fully charged (so if something happens, you can communicate as long as possible). Disable fingerprint unlock as discussed, so that only your memorized code can open it.
- **During Protests – Secure Comms:** Use encrypted messengers for coordination (like Signal private groups) rather than open channels like standard SMS or public social media, for tactics talk. If you must use a platform like Telegram, stick to secret chats for sensitive stuff, or use disappearing messages. Be mindful that authorities may be monitoring social media in real-time – they have in many places. That doesn't mean don't livestream or post if it's part of activism, just be aware operational details should be kept in secure channels.
- **Capturing Evidence:** Often activists want to film or photograph wrongdoing (police brutality, etc.). This is crucial work, but think about the safety of that media. If you capture critical footage, try to back it up or send it to someone offsite quickly (in case your device is taken or destroyed). You could, for example, use an app that auto-syncs photos to the cloud (though ensure the cloud is secure and you have credentials memorized). Even a quick email or messaging of the file to a colleague helps. If someone yells "they're confiscating phones," consider removing your SD card (if your phone has one with footage) and hiding it on you, since often they just grab the device and might not check card slot (admittedly risky/hard in the moment). And of course, if confronted by aggressive authorities, weigh the risk – sometimes it might be better to comply than to have them use force to get the device (which could injure you).
- **Airplane Mode & Network:** Some protesters **use airplane mode or turn off phones when not actively needed, to prevent location tracking and**

**microphone snooping.** If tens of thousands are present, targeted tracking is harder, but if you personally are a target, know that cell towers generate logs of all devices present. A Faraday bag (a pouch that blocks signals) can completely isolate the phone, but then you're unreachable. Another approach: use mesh communications (Bluetooth or direct Wi-Fi-based apps like Briar or FireChat used in some protests) if mobile internet is shut down or insecure – but those require others to use same app.

- **Emergency Contacts and Info:** Set up in your phone's emergency settings a contact or some medical info if you have a condition – on many phones, this can be accessed without unlocking to help you in case of an emergency. More security-wise: memorize a couple of important phone numbers (lawyer, close colleague). If your phone is seized or destroyed, you might need to call them from memory later.
- **At Borders:** Border agents in some countries can demand access to devices. Refer to Section 5.4 for device preparation. Specifically: log out of social media apps (some even uninstall them) to avoid casual scrolling by an agent seeing your feeds. Remove messaging apps if feasible, or at least ensure nothing sensitive is in them. If you're comfortable with it, one tactic is to carry a completely blank phone and say you don't use one – but that can raise suspicion. Alternatively, travel with a clean phone but with just enough believable personal data (like generic photos, some contacts) so it doesn't look wiped. It's a cat-and-mouse game; research your rights in each jurisdiction.
- **Post-Event Actions:** After returning from a risky event, consider that your phone could have been tampered with or infected if it was ever out of sight. If you suspect something, maybe do a factory reset and restore from your backups (especially if you were detained and the device was with authorities, assume compromised). Check for unknown apps or configuration changes (like new VPN profiles, admin permissions granted, etc.). Change any account passwords that you might have entered while there, in case of keylogger.
- **Psychological Aspect:** Using a phone amidst chaos is stressful. You might have to make quick decisions (film this vs hide phone vs call for help). Running drills or at least mentally planning can help. For example: "If they deploy tear gas and I have to run, my phone is in an easily reachable pocket or strapped, not likely to fall. If I'm about to be arrested, I'll quickly hit lock and toss the phone to a trusted friend nearby if possible." These split-second plans rarely go perfectly, but **thinking ahead can help you react better.**

Mobile devices are often the most vulnerable point if not prepared, but with thoughtful precautions they can be our tools and not our undoing.

**Checklist: Mobile Device Security**

- **My phone is locked with a strong PIN/password, and I disable Touch/Face ID when entering high-risk scenarios (protests, borders) where I could be compelled to unlock.**
- **The phone's storage is encrypted (most are by default), and I've set it to auto-lock quickly. I also have SIM PIN enabled to protect my number.**
- **I periodically check and prune sensitive data on my phone (messages, logs, etc.), especially before going somewhere risky. I use disappearing messages or archive chats that aren't needed.**
- **App-wise, I only install from trusted sources and limit permissions. I've reviewed which apps can access my location, camera, mic, contacts, etc., and cut it down to the minimum necessary.**
- **I keep my phone's OS and apps updated. Auto-updates or regular manual checks are in place so I get security patches timely.**
- **I have set up "Find My Device" or equivalent. I know how to remotely locate or erase my phone if it's lost or seized, and a trusted friend could help trigger that if I'm indisposed.**
- **Before traveling across borders or attending high-risk events, I take extra measures (remove certain apps or data, use a secondary device, log out of accounts, etc.) to minimize exposure if my phone is searched.**
- **I have key contacts memorized or written somewhere safe (not only in my phone), in case I lose access to the phone.**
- **I understand how to quickly turn off connectivity (airplane mode or a Faraday bag) if I need to avoid tracking at some point, and I'm aware of trade-offs (losing ability to communicate when I do).**
- **After any incident where my phone was out of my control, I audit it for signs of tampering or unknown new apps/settings, and if in doubt, I reset it and restore from a clean backup.**

***(With your mobile device secured, next we'll delve into using social media safely – which is a double-edged sword for activists, offering voice but also opening new risks.)***

## 8. Social Media Security: Safe and Effective Use

Social media is a powerful tool for activists to spread messages, organize events, and document injustices. But it also introduces personal risks: harassment, doxing, surveillance by adversaries, and even legal trouble if posts are used against you. This chapter focuses on how to navigate social media safely and strategically – protecting

your privacy, managing your audience, and handling common threats like trolls or doxers.

## 8.1 Privacy Settings and Audience Management

First, take control of who sees what on your social accounts:

- **Lock Down Your Profiles:** Review the privacy settings on platforms like Facebook, Twitter, Instagram, etc. Default settings often lean towards over-sharing. Change them to limit who can see your posts, who can find you via contact info, and who can tag you or post on your profile. For example, on Facebook you might set posts to "Friends only" by default, limit past posts visibility, and approve tags manually. On Twitter/X, consider whether to make your account protected (so you approve followers) – though that limits reach, it may be appropriate for sensitive roles. On Instagram, a private account means only approved followers see your content.
- **Separate Personal and Activism:** It might be wise to separate your personal life profile and your activist persona, especially if using real name on one could cause trouble. Many activists have an alias for activism online. Even if you don't hide identity, you might at least compartmentalize content: e.g., one account for family/friends (locked down) and another for public campaigning. That way, the public one can be all business, and your personal connections remain more private and insulated from hostile observers. Compartmentalization can prevent an adversary (or just an internet rando) from easily digging up personal details from your social media. Remember though, maintaining two accounts diligently is effort, and you must avoid cross-linking them inadvertently (like posting personal info on the activist account).
- **Audience Restrictions on Posts:** Many platforms allow per-post audience choices. Use these when needed. For instance, if you're coordinating logistics for a protest, maybe post that only in a private group or to a limited friend list, not publicly. On the other hand, broad calls to action you might want public. Know the difference and double-check the audience selector each time you post something sensitive. Also be aware that even if you restrict a post, someone in that audience could screenshot and share – privacy settings deter casual exposure but determined snoops or traitors could leak. Still, it's an important layer.
- **Don't Overshare Sensitive Info:** Avoid posting things like your address, phone number, or real-time location (unless intentionally, like livestreaming a protest for safety). Also be cautious sharing others' info – you don't want to inadvertently dox fellow activists or family members. For example, maybe don't post group photos with everyone's face visible and tag their full names without consent, especially if some prefer anonymity. Another overshare

could be details that pinpoint someone's whereabouts or routines (e.g., "Meeting every Thursday at X Cafe") – this can put people at risk of surveillance or attack. You can share operational info in closed channels instead.

- **Follower/Friend List Hygiene:** Who you connect with can be sensitive. Some activists periodically audit their followers or friends to remove unknown or suspicious accounts. Fake profiles (impersonating supporters) are regularly used to infiltrate activist circles. On Facebook, you can curate friend lists (create a restricted list for acquaintances vs close friends). On Twitter/X, check new followers; if an account has zero followers and was just made, maybe block it or at least be mindful of what you let it see (if your account is public though, you can't easily restrict beyond going fully protected). For high-profile activists, some assume many followers are adversaries watching – that's fine as long as you post with that in mind.
- **Use Groups and Circles:** Some platforms offer nuance. Facebook Groups: If organizing, prefer a private or secret group rather than an open one. That way membership is controlled and content isn't visible to outsiders (just be aware group members could still leak). Twitter/X doesn't have groups, but something like WhatsApp/Signal groups or email lists might be better for internal communication than open DMs or tweets.
- **Location Tagging:** We touched on this – it's generally best to keep location turned off for social posts unless it's necessary (like raising visibility of an event you are currently at and want people to know – but even then consider safety). Posting home location or frequent hangouts can allow stalking. If you want to share a location afterward, maybe do it once you've left. Some activists deliberately obfuscate dates/locations in posts if the timing isn't critical, to make it harder to track where they are.
- **Search Engine Visibility:** Check if your profile is indexed by search engines. Facebook has a setting to allow/disallow search engines linking to your profile. If you prefer not to be easily searchable by name via Google, turn that off. It's an easy way for adversaries to find all your online presences by a single query.
- **Think Before You Accept Friend Requests:** Especially if you're an admin of a sensitive group or page, be wary of adding new friends you don't know well. They might be sockpuppets to glean more of your locked content or to **phish you via Messenger**. If you suspect one, it's okay to ignore or even block. If an account looks like a clone of someone you know, contact your friend via another channel to verify. **Cloning and sending friend requests to their network is a common scam.**

By tailoring privacy settings and audiences, you can still leverage social media for outreach while minimizing unintended exposure of your personal details or movement's internal plans. **It's a balance between being visible to supporters and**

**your audience but opaque to adversaries in your private sphere.** Next, we'll address oversharing and how to avoid doxing risks.

## 8.2 Avoiding Oversharing and Doxing Risks

"**Oversharing**" means posting information that could be used against you or others. And "**doxing**" is when someone gathers and publishes personal info (home address, phone, family details, etc.) to harass or endanger you. Activists need to guard against both self-inflicted info leaks and malicious doxing by opponents.

- **Be Conscious of What You Post:** This seems obvious, but **social engineering often works because people freely post things that help adversaries piece together a profile**. For example, posting pictures of your workspace might show documents on the desk or a laptop screen in the background (people have inadvertently leaked passwords that way). Or saying "Off to meet with Jane Doe about our legal strategy" publicly – now that meeting is exposed. Before posting, especially publicly, think: Could this jeopardize someone's safety or our plans if seen by the wrong person? It's fine to share personal life stuff if your profile is locked down and you trust your friends, but once it's online there's always a chance it spreads. **Many activists follow this rule: no photos that reveal home street view or exterior, license plates, children's faces, schools, etc., on social media.** Consider adopting similar guidelines.
- **Strip Metadata from Photos:** When you share images, especially publicly, remember they can contain metadata like GPS coordinates (if your camera app tags them). Also, reflective surfaces or background items could reveal things. A famous overshare example was an activist posting an office selfie that accidentally had a password visible on a Post-it in the background. For safety, turn off camera location tagging as we mentioned, or use tools to scrub metadata (there are several apps and desktop tools to remove EXIF data). If you want to share images of a protest or group, consider double-check you're not exposing someone who asked not to be identified. Blurring faces of bystanders or colleagues in certain contexts might be wise before posting (there are apps for quick face blurring).
- **Watch Out for Context Collapse:** That means information you think is okay in one context might be misused in another. Keep sensitive personal logs out of any realm that could leak. Private support groups or closed chats might feel intimate, but assume anything could leak if one member decides to screenshot (like a mole).
- **Doxing Defense – Personal Info Hygiene: Google yourself (and your family if relevant) to see what's out there.** If your home address or phone is easily found via publicly available resumes, WhitePages or similar, consider asking for removal of the content or opting out of those people search directories –

many have processes to remove your info upon request. **Lock down privacy on who can see your friends list** (doxers often pivot from target to their family/friends). Consider using a P.O. Box or office address for public filings or contact needs (if you run an NGO and have to list an address, don't use your home). Some activists register their domains or accounts with pseudonyms or privacy services to avoid address exposure in WHOIS or similar records.

- **WHOIS and Public Records:** If you own a website, use domain privacy to hide your personal address from the public WHOIS database. Be careful when registering for events or petitions online – sometimes organizers accidentally publish signatories' contact info. Only share what you wouldn't mind made public in those forms. On social profiles, decide whether to list your real email/phone – maybe provide a work contact or none at all.
- **Challenge Doxing Content:** If you do get doxed (someone posts your private info), most platforms have policies against that (because it's harassment). Report it to the site – e.g., Twitter/X and Facebook will usually remove posts with personal data like addresses, and possibly suspend the user. Get friends to report it too for faster action. And alert your community privately so they know to watch out for impersonation or scams that might follow (because **often doxing is followed by targeted phishing or swatting attempts**). Also consider informing local police if threats accompany it, and ensure they take note if you fear physical danger.
- **Password Security to Prevent Account Doxing:** Sometimes doxing info comes from hacking an account (like an old email that had personal details). Make sure accounts (especially those where you might have exchanged personal info) are secure – strong passwords, 2FA. You don't want an attacker to break into your email and dig up old emails with attachments like a utility bill (common proof of address, which then they publish).
- **Encourage Allies to Protect Your Info:** Maybe you are careful, but your family members are not necessarily. Educate family and friends that when it comes to you, they should think twice about what they share, given your role. Perhaps **ask them not to post about your location or personal matters without asking you.** It's an awkward conversation sometimes, but important. You can make it general: "There are some nasty trolls who target activists, so I'd appreciate if you don't put my address or routine out there on social media."
- **Use Aliases When Appropriate:** For example, if you run a personal blog or account, you might not need your real last name visible. Some activists, to avoid doxing, use only their first name or a nickname on public sites. It's not about hiding from being known (many know who they are), but it prevents automated data aggregators from easily pulling all info on them. If an adversary tries to dox you and can't even figure out your last name or find your relatives because you don't link those publicly, it's a bit of a shield.

In summary, treat personal data like sensitive material that adversaries ***will*** exploit if they find it. **Share what advances your cause, but keep the rest out of easy reach. Err on the side of caution and assume the internet is forever and public, even if you use privacy controls.**

## 8.3 Handling Harassment and Trolls

Online harassment is, unfortunately, rampant for activists and journalists. Trolls (people who provoke or abuse for reaction or to intimidate) can sap your energy, derail conversations, or worse, cause psychological harm and credible threats. Having strategies to deal with them is key to staying effective and sane online.

- **Don't Feed the Trolls (Selective Engagement):** The age-old wisdom is not to give obvious trolls the attention they crave. Often, it's best not to respond to random hate comments or bait. Responding can encourage them or expose you to further abuse. This doesn't mean ignore all criticism or questions, but **learn to differentiate between good-faith disagreement and bad-faith trolling.** A user with 0 followers saying "You're all terrorists, hope you die" – block and move on, do not attempt to reason. But someone respectfully challenging a point, you can engage if you want. **Remember, trolls often *want* to lure you into an outburst to screenshot it** and claim you're "angry" or "unhinged." Keep your cool or choose silence.
- **Use Platform Tools (Block, Mute, Report):** Twitter/X, Facebook, Instagram etc. all have block features – use them liberally for harassers. "Mute" is useful on Twitter/X if you don't want them to even know you blocked (their replies won't show up to you but they won't realize you muted them, which can avoid fueling their martyr complex). Reporting is important especially for threats or targeted harassment campaigns – even if the platform response is slow, the more reports, the more chance of action. If someone is sending you private threats, definitely report to the platform and consider law enforcement if they're credible and local. Don't feel bad about blocking; your online space, especially personal profile, is like your living room – you have the right to kick out those who come to spit on you.
- **Filter Features:** Some platforms allow filtering of comments/messages by keyword or by who can reply. Twitter/X has "Quality filter" and you can mute certain words (e.g., slurs or your address if you worry it might spread). Facebook allows comment moderation on pages – you can blacklist certain words so comments containing them are auto-hidden. Instagram lets you hide comments that contain words you specify or that its algorithm suspects are offensive. **Make use of these to reduce the volume of toxic stuff you see**. Also on messaging: consider turning off open DMs on Twitter /X (only receive from people you follow) if you get too many abusive private messages.

- **Safety in Numbers (Allies Help):** Don't suffer alone. If you're under troll attack, inform your trusted network. Allies can help mass-report the worst content, provide emotional support, or even publicly defend you if that's helpful. Sometimes calling out harassment can backfire (feeding trolls more), but a coordinated push by reputable voices can cause platform to pay attention or shame the harassers into backing off. In any case, having friends aware means if you need to step back for mental health, they understand why you might go quiet for a bit. There are also organizations and hotlines for online harassment (like TrollBusters, HeartMob) where you can seek advice or assistance.
- **Document Serious Threats:** For mere annoyances, blocking is fine. But **if you get threats of violence or other serious stuff, screenshot them (with usernames and timestamp)**. Save these in case needed for evidence. Many harassers delete or Twitter/X bans them, so having proof is useful for any follow-up. It's also evidence of pattern if someone is repeatedly making new accounts to harass (ban evasion is against rules – more cause to get them booted permanently if you show it).
- **Protect Your Mental Health:** Constant negativity can take a toll. It's okay to take breaks from social media. Use scheduling tools so you don't have to be online as much in real-time. Don't be afraid to lock your account temporarily if a storm is too much (you can always unlock later). Curate your feed – maybe separate an account that you use only to broadcast activism updates and you don't read replies, versus a personal account you engage with friends on. Many activists have spoken about needing to compartmentalize like this to avoid burnout. If it becomes overwhelming, consider talking to a counselor or support group – online abuse is real abuse, and its trauma can accumulate.
- **Legal Options:** Depending on your jurisdiction, repeated harassment or credible threats could be illegal (stalking, hate speech, etc.). Some activists have pursued restraining orders or police reports against their worst abusers. Law enforcement's understanding of online harassment varies, so it might or might not be fruitful. But keep it in your toolbox if someone crosses from mere trolling to sustained targeted harassment or doxing. Consult a lawyer if needed (some orgs offer free advice for journalists/activists facing this).
- **Alternate Communication Channels:** If you find that being on a particular public platform yields too much harassment, consider focusing your efforts on channels where you have more moderation control (like moderated forums, email newsletters, Telegram channels where only admins post, etc.). It's not "defeat" to move – it's strategic. For example, if Twitter/X is unusable due to trolls, maybe you funnel your followers to a safer space like Bluesky, an email list or a Discord server you moderate. The downside is reach might drop, but quality of interaction may improve.

- **Plan for Waves:** If you're about to publish something controversial or appear in the media, anticipate a possible influx of trolls. Maybe preemptively mute certain keywords or even lock down temporarily. Mentally prepare or arrange a friend to help screen your mentions for any actual constructive feedback among the garbage. That way you get the useful stuff and miss the raw sewage. Knowing it might happen can blunt the shock if it does.

Harassment is ultimately aimed at silencing you or distracting you. By managing it assertively – controlling what you see, blocking the offenders, getting help – you deprive them of their power and keep control of your narrative and mental space. It's easier said than done, and each person's threshold differs, but you have every right to protect yourself.

## 8.4 Alternatives and Off-Platform Strategies

Finally, consider the broader approach to social media: sometimes the safest or most effective move is to diversify beyond the big platforms or have backup channels.

- **Decentralized and Niche Networks:** In response to harassment or censorship on mainstream sites, some activists migrate to alternatives like Bluesky. Just note, smaller platforms might have smaller reach. But for internal collaboration or support, they can be great. Similarly, there are private subreddit communities, Diaspora, and others. Gauge if your audience is likely to follow you there or not. Even if not for broad comms, maybe use them for peer networking.
- **Self-Hosted Blogs or Websites:** Don't rely solely on third-party sites to keep your content up. Having your own website or blog (even if just a simple WordPress) means you have a home base that can't easily be censored (assuming you secure it). Social media can drive people to your site, but if you were banned or brigaded off a platform, your website stands. It's like having an anchor. Ensure it's secure (Chapter 9 covers web security a bit in sharing files, but a site needs updates and anti-DDoS maybe).
- **Email Newsletters:** Old-school but effective and harassment-free (mostly). Encouraging supporters to subscribe to an email newsletter (via a service like MailChimp, Substack, etc.) gives you a direct line that's not at the mercy of algorithms or trolls. You can disable replies or handle responses privately. It's one-way mostly, so no public comment section to moderate, and if someone harasses via reply you can ignore or filter it.
- **Collaboration Platforms:** For actually doing work (planning, chatting with fellow activists), don't use social media – use collaboration tools like Slack, Mattermost, Nextcloud, etc. These off-platform tools allow closed, moderated environments for teamwork and discussion, away from public eye. Slack even

lets you integrate some social feeds if you need them, so you can monitor things in one place while staying in a team context.

- **If Deplatforming Occurs:** Be prepared for the possibility your account could be suspended (unjustly or by mass-report from opponents). **Have backup admin accounts for important pages** or groups (so one ban doesn't orphan the group). Keep a list of key followers or contacts offline (so you can reach out if needed – e.g., via email – to say "my account was banned, follow the new one here").
- **Content Mirroring:** If you produce content (videos, articles), mirror it across platforms. For instance, if you upload a video to YouTube, maybe also put it on PeerTube or Vimeo or archive.org. If YouTube ever pulls it, you still have a version up. This also helps circumvent selective blocking – maybe one site is blocked in a country but another isn't.
- **Community Guidelines:** If you run a Facebook page or group, set clear rules and enforce them. Remove hateful or off-topic comments, ban repeat offenders. It's your space – by having stated guidelines, you can moderate without feeling guilt of "censorship," because you set a standard (like "no ad hominem, stick to issue, no slurs"). This fosters a healthier environment that might automatically dissuade some trolls. State that you will ban for violations – and follow through.
- **Building Allies on Platforms:** Sometimes you can coordinate with other friendly pages/accounts to watch each other's backs. For example, if someone is harassing climate activists broadly on Twitter/X, a network of them can collectively report or call it out. Or co-promote content to drown out troll noise (like, 10 allies retweet your campaign tweet at once to outshine the 3 trolls in replies). There's strength in numbers, even online, and showing solidarity can discourage some harassers who realize you're not isolated prey.

In essence, don't feel confined to a platform that isn't serving you. Use alternative approaches and be creative. The goal is to get your message out and build community – if that can happen in a safer corner of the internet rather than the digital equivalent of a screaming mob, that's perfectly valid.

### Checklist: Social Media Safety

- **I have reviewed and adjusted privacy settings on all my social accounts. I know exactly who can see my posts, who can contact me, and I use friend/follower management features to keep out unknowns when needed.**
- **I think before I post personal or detailed information. I avoid sharing things that could expose sensitive locations, plans, or personal data about me or colleagues. I also scrub metadata from photos and am careful with tagging people.**

- **I actively use block/mute/report on harassers or trolls. I do not engage with obvious bad-faith actors. I've also set up filters or moderation tools (like keyword blocking or limited replies) on platforms that support it, to reduce seeing abuse.**
- **I have contingency plans if I face mass harassment or deplatforming: alternate communication channels (like an email list or secondary account) to reach my audience, allies who can help moderate or support me, and backups of important content.**
- **Where possible, I operate in safer online spaces for organizing and internal discussions (secure chat groups, private forums, etc.) rather than relying on public social media for everything.**
- **I periodically search for my own info online (the way a doxer might) and take steps to remove or secure any sensitive data I find (like home address or phone).**
- **I set boundaries for my social media usage to protect my mental health. Whether it's limiting daily exposure, using a pseudonym in certain spaces, or taking breaks, I prioritize my well-being over feeling compelled to respond to every poke or mention.**
- **I have established clear rules in any online communities I manage and I enforce them, to keep those spaces constructive and safe from abuse.**

***(With social media covered, we'll move on to the next chapter about sharing files securely – because activists often need to share documents, images, etc., and doing so safely is another piece of the puzzle.)***

# 9. Secure File Sharing and Storage: Handling Sensitive Files

Activists handle a variety of files – spreadsheets of contacts, legal documents, photos from protests, reports to publish, etc. Improperly shared or stored files can be a serious liability (think leaked participant list, grant data, or an unencrypted hard drive seized). This chapter discusses encrypting files and drives, using cloud storage carefully, sharing files via links or email securely, and scrubbing metadata. These practices ensure that when you're exchanging or stashing information, it doesn't fall into the wrong hands or reveal more than intended.

## 9.1 Encrypting Files and Drives

Protecting data at rest (when it's stored on your device or an external drive) often means encryption. We covered full-disk encryption in Device Protection, but here we'll focus on file-level encryption and specific use cases:

- **Encrypt Sensitive Documents:** If you have individual files that are highly sensitive (say, a list of confidential informants, or credentials for accounts), **consider encrypting those files themselves in addition to any disk encryption.** That way, even if the file is accidentally emailed or stored in the cloud, it's unreadable without a password. Tools: 7-Zip (on Windows) or Keka (on Mac) can create encrypted archives (choose AES-256). Or use a dedicated encryption tool like VeraCrypt or GnuPG (GPG) for files. For instance, you can use GPG to encrypt a file to specific recipients (so only their private key can decrypt). That's more complex but good for email attachments to someone who has GPG.
- **Whole Drive Encryption:** We did this, but to reiterate: USB sticks and external drives should be encrypted if they carry any sensitive data. **It's easy to lose a USB drive.** Windows BitLocker can encrypt external drives (Pro edition and up). Mac's Disk Utility can create an encrypted volume on a USB drive (Mac OS Extended (Journaled, Encrypted) or APFS Encrypted). There are also cross-platform solutions like VeraCrypt containers – you create a file that acts like a secure vault that you mount with a passphrase. Then you can put that file on a USB or cloud.
- **Use Strong Passphrases:** When encrypting files or archives, use a strong passphrase (long and not guessable). Many people use zip encryption with a weak password and think it's secure – password cracking tools can rip through common passwords easily. A passphrase of 4-5 random words or a random string of 12+ characters is advisable for manual encryption tasks. Write it down in your password manager or a secure note if you worry about forgetting.
- **Double Layer for Cloud:** If you must store extremely sensitive docs in cloud services (like you have team data on Google Drive or Dropbox), one strategy is to add your own encryption on top. For instance, store things in a VeraCrypt container file on Dropbox – so even if Dropbox is breached or pressured, they only see an encrypted blob. There are apps like Cryptomator or Boxcryptor (EU product) that integrate to encrypt files on the fly before uploading to cloud. This way, you get convenience of cloud but the provider never sees plaintext.
- **Mobile Device Files:** For files on your phone, note that device encryption covers them, but if you want to email or share from phone, there are apps that zip and encrypt too. Or you can upload to a secure cloud app that handles encryption (like ProtonDrive).
- **Shredding/Deleting:** We touched on secure deletion: when you encrypt a file and then delete the original plaintext version, make sure the deletion is secure. On SSDs, as said, that's tricky; encryption from the start is better. But for mechanical drives or USBs, you can use a tool to overwrite free space after deleting (BleachBit, CCleaner's Drive Wiper, etc.). Simpler: move all sensitive files into an encrypted container from the get-go, then delete the originals and

fill the free space with innocuous data if you want to push out remnants (or physically destroy old drives if retiring them).

- **Labeling and Organizing Secrets:** Human error is often the issue. If you have a mix of encrypted and unencrypted files, clearly label the encrypted ones or have a system to avoid confusion. Example: maybe put all sensitive stuff in one folder that you keep locked with VeraCrypt. If it's strewn all over, you might accidentally copy an unencrypted version to a USB or email. Tight organization helps – e.g., "Secured Archive – NEED PASS" folder name as a reminder. Also, avoid leaving decrypted copies lying around; once done using a file, either delete it or move it back into an encrypted location.
- **Training Team Members:** If you work in a team, ensure everyone knows how to handle encrypted files. It's no use if one person encrypts a document and another person later saves a decrypted version to the shared drive by mistake. Agree on workflows: for instance, "When working on the budget sheet, always open from the encrypted vault, and when done, don't save a copy outside of it." Perhaps use password managers to share the encryption password securely among the team, so nobody has excuse to leave something decrypted.
- **Don't Rely on Obscurity:** Renaming a file from "plan.pdf" to "vacation.jpg" is not encryption. People sometimes try to hide info by filename or extension trickery, but that won't stop a determined person. The file's contents are intact. Real encryption is the only reliable way to secure content.

Encrypting things might add an extra step to your routine, but it dramatically raises the bar for an adversary. Even if a device or cloud account is compromised, they'd still face the encryption wall. Next, we'll discuss using cloud storage more safely in general:

## 9.2 Safe Cloud Storage and Collaboration

Cloud storage (Google Drive, Dropbox, OneDrive, etc.) is ubiquitous, and activists use it for good reason – easy sharing, backup, remote access. However, **putting files on someone else's server has inherent risks**. Let's manage those:

- **Choose Providers Wisely:** Not all clouds are equal. Some have better privacy policies or security features. For highly sensitive work, consider using services that offer **end-to-end encryption or zero-knowledge storage** (where they can't read your data). Examples: ProtonDrive, Tresorit, SpiderOak are oriented towards privacy. They may have limitations (less integration with third-party tools, etc.), but for certain data it's worth it. If using mainstream providers like Google or Microsoft, just be aware that they can access your files (and therefore can be compelled to hand them over to authorities or might scan them for violations of the Terms of Service).

- **Access Controls and Sharing Links:** Cloud platforms make it easy to share via links. **But make sure you set permissions appropriately.** Don't give edit access to people who only need view. **Use link passwords or expiry dates if available.** For instance, Dropbox allows setting a password on a shared link (paid accounts). Google Drive doesn't provide link passwords, so maybe use other methods if needed (e.g., put file in encrypted zip and share zip with a separate channel for password). Also, regularly audit who you've shared folders with – sometimes people leave an organization but still have access to a shared Google Drive because nobody removed them. Clean up old collaborators. Also clear out old data that doesn't need to be online anymore.
- **Beware of Public Sharing: If you set a folder or document to "Public/Anyone with link can view," treat that link as if it were published on the web – because essentially it is, just unlisted.** Only use that setting for files you intend to be public (press releases, etc.). If you accidentally post a public link in a wrong place, someone could find it. If you use "Anyone with link" for convenience internally, ensure that link doesn't leak – maybe still put a random password on the document itself if platform allows (you can in PDF or Office docs).
- **Account Security for Cloud: Use strong 2FA on cloud storage accounts!** They are treasure troves. If one gets phished, an adversary might quietly browse and you wouldn't know. Google will sometimes flag "unusual activity in Drive" but don't rely on that. Keep an eye out for weird file changes. Some services let you see active sessions or devices connected – check that occasionally, revoke any unfamiliar ones.
- **Device Sync Pitfalls:** Many have desktop sync apps (e.g., Dropbox client, OneDrive sync). If your laptop is stolen and you had an active login in the sync app, that thief can potentially access cloud files (unless you remotely unlink device quickly or it was locked behind OS password). **Similarly, if malware hits a synced folder, it could encrypt or delete cloud data too** (ransomware might scramble your local files, sync then dutifully syncs the scrambled versions to cloud). Prevent that by ensuring you have backups of cloud files (some cloud services have version history – enable it if it's not default, or periodically export a backup set). If using a shared team folder, maybe restrict delete permissions so one account can't wipe everything. Or use services that allow setting up recovery codes.
- **Privacy vs. Collaboration Trade-off:** Using an E2EE cloud like Tresorit means the provider can't read data, but it also means you can't use Google's web editors or such on it because those require data to be processed by them. So sometimes activists use a hybrid: sensitive raw data stored in private cloud or encrypted container, but less sensitive collaborative docs (like a draft of a blog post) on Google Docs for ease of multi-editing. That's fine – classify your data: e.g., "Operational plans & contact lists must be E2E encrypted, but public

outreach content or non-critical notes can be on Google's servers." This way you limit what you truly need to protect strictly.

- **Data Localization: If relevant, consider where your cloud data is stored.** Some choose services that store data in certain jurisdictions with stronger privacy laws (or at least not in the country of your adversary). E.g., maybe you avoid a cloud that stores everything in Country X that has a history of seizing activist data. It's a nuanced call; encryption matters more, but jurisdiction can be a layer of defense or vulnerability.
- **Revoking Access and Offboarding:** When a volunteer or staff who had access to cloud storage leaves, remove their account or change passwords/links. It's easy to forget that an ex-member still knows the password to an encrypted .zip in Dropbox – update those if needed. Similarly, if you shared a drive link widely for a coalition project that's now over, disable it or move the files.
- **Terms of Service (ToS) and Content Scans:** Recognize that some providers scan for certain content (child exploitation imagery, or even copyrighted material). While activists wouldn't have illegal stuff, there have been cases like police subpoenaing footage from cloud if they think a crime was recorded, etc. If you have sensitive photos or videos that might be incriminating for participants if accessed, strongly consider client-side encryption. The cloud AI won't be able to scan an encrypted file.
- **Use of Institutional vs Personal Accounts:** If possible, use organizational accounts for organizational data (e.g., an NGO's Google Suite or Office 365 enterprise, with admin controls) rather than everyone using their personal Google Drives to share work stuff. Central admin means if someone leaves, you can cut off their access, and you might get advanced security features (like DLP – data loss prevention). Personal accounts can vanish or get locked if Google thinks something's up, with no recourse. With paid org accounts, you often have some support or at least admin oversight.

In short: **take advantage of the convenience of cloud, but don't treat it as inherently secure** – add your own safeguards and keep watch on access.

## 9.3 Sharing Files Securely (Links, Email, P2P)

When you need to send files to someone else, what's the safest method? Options include secure link sharing, encrypted email, or peer-to-peer transfers:

- **Secure Link Sharing:** Instead of emailing large attachments, you might upload a file to a cloud service and send the link. To do this securely: if using a standard service (Google, Dropbox), set link access minimal (maybe direct share to their email if possible rather than open link). If you must do open link, set a password on it (if service allows). Another approach is use a service specifically for secure file sending, e.g. OnionShare (an open-source tool that uses Tor to send

files directly). OnionShare lets you share a file via a .onion link; as soon as the recipient downloads, you can terminate the share. It's highly private (no servers in between except Tor relays). It's a bit technical but a great tool for whistleblowers or sensitive docs.

- **Email Attachments:** Regular email is not secure (unless both parties use PGP/GPG or the service uses end-to-end encryption like ProtonMail-to-ProtonMail). So, if you send a sensitive file via Gmail, assume Google or any intermediate server can read it. If you must email, encrypt the file before attaching (like make it a password-protected zip or document). Then share the password through a different channel (e.g., Signal). Many times, you can avoid emailing by using a link as above or a secure portal (like some organizations set up a Nextcloud with password-protected share link).
- **Use of PGP:** If you and recipient both have PGP set up, you can encrypt the file directly to their public key (using GPG tools) and email that. Only they can decrypt with their private key. This is very secure but requires the whole PGP infrastructure which is often a barrier.
- **Peer-to-Peer (P2P):** If you're on the same network or can connect directly, sending files via a secure messaging app might be easiest (Signal and others allow file attachments up to certain size – those are E2E encrypted in transit). If physically near, transfer via AirDrop (Apple's local wireless transfer) or a USB drive hand-delivered – that's offline and can be secure if the drive's encrypted or if you trust handing it over.
- **Transfer Services:** Some activists use services like WeTransfer, Smash, etc., to send big files. Be cautious: unless you add your own encryption, those services have the file. If you do use them, always enable their password option for the transfer and share the password separately. Without a password, anyone who gets the link can download.
- **Double-Check Recipients:** This seems basic, but when sharing sensitive files, triple-check you're sending it to the correct person. **Email autocomplete accidents are infamous**.
- **Time-Limited Access:** If the file shouldn't live around forever, consider expiring links. Some platforms allow setting that (Dropbox Pro, OneDrive for Business, etc.). Or just remember to go delete the file from the server after confirming they got it. At least clear it from any public-facing URL to reduce lingering risk.
- **Large Sensitive Transfers (e.g., evidence videos):** These can be tricky. If internet is slow, uploading huge encrypted files might fail. In such cases, physical shipment of an encrypted drive might be safer (like copy to a USB, encrypt it, and mail it via a trusted courier). Or break the file into parts and send separately.

- **Metadata & Formats:** If you're sharing a document (like a Word doc), remove metadata first if it goes outside trusted circles. Word docs often contain author name, possibly edit history or comments. Convert to PDF when final (and scrub PDF metadata too). Also consider that Office docs can contain macros that trigger security alerts or be blocked by some email filters – PDF is generally safer for recipients. For images, remove EXIF as said. There are tools (like MAT2 – Metadata Anonymization Toolkit) that can clean files for sharing.
- **Receiving Files Securely:** Encourage partners to send you files securely too. Provide them with a method (like "here's an upload link to my secure Nextcloud" or "please Signal me the file"). It's part of training your network; otherwise, you secure everything on your side but someone might just email you a password list in plain text. Share these practices with allies.

The key concept is using multiple channels or steps when needed (encrypt then send; or send link + separate send key). Yes, it's slightly more effort, but if the file is that sensitive, it's worth it.

## 9.4 Removing Metadata and Traces

We've mentioned metadata a few times – here let's summarize key things to wipe and how:

- **Document Metadata:** Word, Excel, PDF, etc., can contain info like author, organization, date edited, maybe even revisions or comments. To remove in Office: there's Inspect Document feature (File > Info > Check for Issues > Inspect Document) which can remove personal info. For PDFs, use "Save as optimized" in Acrobat and select to discard metadata, or print to PDF which often flattens most info (though it might remove things like links). You can also use command-line tools (exiftool works on many file types to strip metadata).
- **Image Metadata:** Photos can have a ton of data (camera model, serial, GPS, date, thumbnails). Exiftool or MAT2 can scrub images. On Windows, you can right-click > Properties > Remove Properties and Personal Information (but it doesn't remove all types, I'd trust a specialized tool more). There are also smartphone apps (ViewExif on iOS, Photo Exif Editor on Android) to remove GPS from photos before you share them, etc.
- **Video metadata:** Videos also have some, though not as rich as images. There are tools like HandBrake to transcode and possibly drop metadata. Or even upload to YouTube as unlisted then re-download it (YouTube likely strips original metadata and compresses). But be careful, uploading anywhere could imprint an ID on it. You can also take the manual route: open video in an editor and export it, which usually doesn't carry original metadata.

- **Hidden Data in Files:** Sometimes documents have hidden content (like a white font text in a doc, or previous edits visible via undo). Converting to a different format (doc to pdf) often helps, but to be sure, thoroughly inspect. The Office inspector is good for that – it can find comments, hidden text, etc. Remove those.
- **Cache and Temp Files:** When working on sensitive docs, remember your computer might have temp files or backups. For example, Office creates AutoSave files. Ideally, use disk encryption so those are protected at rest. If you really need to ensure nothing recoverable is left, consider using a secure erase tool on temp directories or working inside an encrypted container (so even temp files are within encryption).
- **Cloud and Trash:** If you delete something from a cloud drive or your system, empty the trash and also check if cloud has a separate trash that retains files (Google Drive, Dropbox do keep deleted files for some time unless you purge). Purge it if necessary.
- **Version History:** Be mindful of collaboration platforms' version history. Google Docs and others let collaborators see previous versions or "suggestion mode" changes. Before making a document public or sending it out, either make a clean copy (no history) or use tools to remove that if possible. Google does not include version history when you export a doc, so exporting to PDF or Word and sharing that is one way to "freeze" it without the backstory. Just don't accidentally share edit access if you don't want people looking at revision history.
- **URLs and IDs in File content:** Sometimes people put hidden notes like references or IDs in files that might be meant for internal use. Check any unique IDs or links inside a doc before sharing widely – e.g., you might have a Google Analytics tracking code in a PDF link that identifies your organization – if you want to share the PDF anonymously, remove that or any fingerprinting info.

One motto: assume any file you release will be combed through by an adversary. If there's anything that could reveal something you don't want, remove it beforehand.

### Checklist: File Sharing & Storage

- **I encrypt files or archives that contain highly sensitive information, especially before uploading or sending them through channels that aren't end-to-end encrypted. I use strong passphrases and share those via a different secure channel.**
- **My team and I use cloud storage with caution: we set appropriate sharing permissions (no wide-open access unless intended), we remove access for**

**people who no longer need it, and we avoid putting extremely sensitive data unencrypted in the cloud.**

- **We have backups of important cloud-hosted files, and we utilize features like 2FA and activity alerts on our cloud accounts to detect any unauthorized access.**
- **When sending files to others, we prefer secure methods (like private links or encrypted email) rather than attaching in plain email. We coordinate with recipients to ensure they know how to open encrypted files or we agree on a common tool (e.g., both using OnionShare or a shared Nextcloud folder).**
- **We routinely strip out metadata from files (documents, images, PDFs) before distributing them externally or publishing. We double-check that no hidden revision history or comments are left in final documents.**
- **We securely erase files or drives when they are no longer needed or before disposal. For example, we wipe old USB drives or use full-disk encryption keys (then forget the key) to effectively destroy data.**
- **For particularly sensitive exchanges (like whistleblower info or legal evidence), we consider using specialized secure drop services or direct person-to-person transfer rather than any cloud or email.**
- **In summary, we treat files with the same care as we do communications: protecting confidentiality with encryption and controlling who can access them at all stages.**

***(Next, we'll tackle what to do when things go wrong – incident response – but by applying all the practices above, we hope to minimize those events or at least contain their damage.)***

# 10. Incident Response: What to Do When Things Go Wrong

Despite best efforts, security incidents can happen. An account gets hacked, a device is stolen, a malicious link was clicked, etc. How you respond can make a big difference in limiting harm. This final chapter guides you through recognizing signs of a security incident, steps to take in common scenarios (account compromise, malware infection, device loss), and when/how to seek help. Having an incident response plan ensures you're not scrambling in panic if the worst occurs – you'll have a checklist to follow and hopefully reduce the fallout.

## 10.1 Signs of a Security Incident

Being able to tell that something is wrong is the first step:

- **Unusual Account Activity:** For accounts (email, social media, bank), watch for signs like: login alerts from unknown locations/devices, password reset emails you didn't request, messages marked read that you didn't read, sent items you didn't send, or new contacts/followers you don't recognize. If friends say they got weird messages from you, that's a red flag your account might be sending spam or phish. Many services like Google, Facebook have a page listing recent logins – check it if you suspect something.
- **Device Oddities:** On computers or phones, malware might cause: sudden slowness or crashes, new icons or apps you didn't install, lots of network or disk activity when you're not doing anything, pop-ups or strange error messages ("Your device is infected! call this number"). Also, files appearing or disappearing unexpectedly. If you notice your webcam light flickers on without reason, that could indicate remote access. Some advanced spyware tries to hide, but it might still glitch or conflict with legitimate software causing malfunctions.
- **Antivirus or Browser Warnings:** If your antivirus flags a threat, take it seriously (unless you're sure it's a false positive with some special software you use). If your web browser blocks a site or download, do not bypass it casually – that likely prevented a malware drop. Similarly, if people you collaborate with inform you "Hey, I got a weird file/link from you" and you have no idea, that's a sign something's up (account compromise or spoofing).
- **Unusual Emails or Accounts Created:** If you suddenly get emails about account registrations you didn't do, or two-factor code texts you didn't trigger, someone might be trying to access your stuff or using your email to sign up for things. Don't ignore those – could be a harbinger of attempted breach.
- **Data Leaks / Public Mentions:** Sometimes you learn of an incident because information that should be private goes public (e.g., an internal memo appears on Twitter/X). That means someone's account or device with that info was compromised. Or you might be alerted by a third-party – e.g., a cloud provider warning "documents in your account were publicly accessible due to X". Pay attention to such notifications.
- **Physical Signs:** If you suspect a device was tampered with (like screws on your laptop look disturbed, or it was in someone's possession out of sight for a time), consider the possibility of a hardware keylogger or rootkit, though that's rare and targeted. Likewise, if a locked phone is returned and suddenly battery drains quickly or it's warm often, maybe some spyware is active. These are subtle; you often have to rely on digital signs, but stay observant.

Many times victims don't realize until way later that they were hacked. Early detection is crucial, so build a habit of reviewing logs (even monthly) and keeping an eye out. If something feels off, trust your gut and investigate.

## 10.2 Responding to Account Compromise

If you suspect or know an account (email, social media, etc.) has been compromised (hacked):

- **Regain Control:** First, try to log in and change the password to something strong ***immediately***. If you still have access, do it and also kick off any active sessions (most services have a "log out of all devices" function). Then enable 2FA if not already. If you cannot log in (attacker changed password), use account recovery options – click "Forgot password" and go through email/phone verification. If those are also changed, contact the service support ASAP – many have hacked account processes (Twitter/X, Facebook, Google all do). It might take time to prove identity though.
- **Check Connected Apps:** Once in, check if the attacker added any backdoors like alternative recovery email, phone, or authorized apps. (E.g., Google Accounts -> Security -> check recovery info and devices; Facebook -> Settings -> Security & Login -> check authorized logins and apps.) Remove anything suspicious (like unknown browser named or forwarding rules in email). Attackers often set up an email forward (e.g., forward all mails to their address and then delete them so you don't see). Look for filters or forwarding rules in email. Also for social, see if any new admin were added to your pages/groups; remove them.
- **Notify Affected Parties:** If the account was used to contact others while compromised (like spamming your friends with scam), let people know not to click any recent weird links, etc. Post a quick message like "I was hacked earlier today; do not trust any unusual messages from me in the past X hours". This helps limit damage and also helps restore trust that the content wasn't really you.
- **Scan for Other Compromises:** The way they got in might be via your device (keylogger) or reused password. So, if a random account got hacked and you're sure it's because you reused password which got leaked – change that password everywhere it was reused. If unsure of cause, assume worst that maybe your computer is infected; run AV scans or even do a clean OS reinstall (especially if multiple accounts start getting compromised out of the blue, which hints at device-level breach). Also think if any email account was hit – that's very critical, because attackers with your email can do password resets on other sites. **So if email was hacked, secure it first, then secure everything else.**
- **Use Secondary Channels if Locked Out:** If you cannot quickly regain account (platform support is slow), focus on limiting harm: announce via other channels that account is compromised (so your community knows). For example, if your organization's Twitter/X account is hacked and spewing disinfo, post on your website or other social accounts to warn "Don't trust

tweets from @OurOrg for now, we're working to recover it." People can spread that word.

- **Preserve Evidence:** If it's serious (like sensitive data leaked or you suspect it's targeted attack), you may want to document what happened. Save chat logs with support, or any unusual login records. Small chance law enforcement might get involved if it's a big crime, but even for your internal post-mortem, evidence helps to analyze how it happened. Also, if you have cybersecurity help available, they'll want logs/evidence to look at the attack path.
- **Professional Help:** If an important account is at stake (say your NGO's main email or site) and you can't recover it easily, consider reaching out to security orgs (Access Now Helpline, etc.) or even the service's reps if you have any contact. Sometimes whisper networks can expedite recovery if you know someone who works at the company. If not, persistence with official channels and community pressure (if you tweet "hey @TwitterSupport our human rights org account was hijacked" others might amplify).
- **Aftermath Steps:** Once secured, do a thorough audit: Was any data stolen or tampered with? For instance, check email Sent folder for what they forwarded out or emailed. Check social account content (did they delete any posts or steal DMs?). If so, you'll have additional steps like informing affected partners "hey, emails you sent me might be exposed" or reposting content that was removed.
- **Psychological Aspect:** It can feel violating to have an account hacked. Remind yourself it happens even to very tech-savvy people. Use it as a learning moment to bolster security (maybe your team takes training on phishing after this, etc.). Don't overly blame whoever might have clicked something (unless gross negligence) – use a blameless post-mortem approach: find root causes and fix them, e.g., "we didn't have 2FA, now we do; we weren't aware of X, now we are."

## 10.3 Responding to Device Loss or Malware Infection

If a device is lost/stolen, or you discover malware on it:

- **Device Loss/Theft:**
  - **Remote Wipe:** If you had a "find my device" service active, log in and trigger a remote wipe or lock as soon as possible. Even if the device is offline, the command often queues and executes when it goes online. This can save data from falling into hands if they eventually turn it on.
  - **Change Credentials:** Assume a thief might crack into the device (especially if no strong PIN). Change passwords for accounts that were logged in there. Also, if that device had 2FA setup (authenticator app,

etc.), take steps to secure those accounts (you might need to revoke those tokens and re-enable 2FA with new device).

- **Notify and Monitor:** Let your organization or friends know the device is gone, so they treat any message from it (if someone uses it) as suspect. File a police report if needed (maybe required for insurance). Keep an eye on accounts for any unauthorized use which might signal they got in.
- **Replacing:** When you replace the device, ensure to secure it better this time (lessons learned). If it was stolen during a specific event (e.g., an arrest), there's concern authorities might forensically analyze it if not wiped. In such cases, consider those data potentially compromised and act accordingly (e.g., warn contacts if your phone had their info).

- **Malware Infection:**
  - **Isolate:** Disconnect from networks (unplug ethernet / turn off Wi-Fi, put phone in airplane mode) to prevent further spread or data exfiltration.
  - **Identify and Remove:** Run a full anti-malware scan with a reputable tool. Many malware get removed by antivirus if detected. If something is found and removed, reboot and run again to be sure. For serious persistent malware (rootkits, etc.), the safest bet is to backup files (carefully, not including suspicious ones) and then wipe/reinstall the OS from scratch. Especially if it's something that stole passwords, treat the machine as untrusted until a clean install.
  - **Change Passwords:** Malware could have logged into accounts or captured keystrokes. Use a different device you trust to change passwords for key accounts (email, bank, etc.) in case they were compromised while the malware was present. Also, if you have 2FA codes or certificates on the infected device (like in keychain), consider those potentially copied; maybe reset 2FA secrets (generate new QR codes) for accounts if you suspect targeted attack.
  - **Restore from Clean Backup:** If you have backups from before infection, restore them instead of keeping possibly infected files. At least, do not automatically restore system settings that might reintroduce malware (like don't restore an entire system image if it might have infected components).
  - **Inform Stakeholders:** If the malware incident might have affected others (e.g., it sent them spam or you had confidential data about them), let them know the situation so they can be alert (like "My computer had malware from X date to Y date; be vigilant of any unusual emails that might have come from me in that period.").

- **Analyze Entry:** Try to figure out how the malware got in: Was it a bad email attachment opened? Outdated software exploit? It is important to identify and fix root cause. If you can't tell, at least patch everything and consider user training if someone clicked something. If you think it was an infected USB drive or something, eliminate that threat in future.
- **Professional Help if Needed:** For high-value systems or severe attacks (ransomware locking files, etc.), sometimes consult cybersecurity experts. They might retrieve data or ensure eradication. There are also non-profits (e.g. Access Now) that help civil society with incident response if targeted by state-level malware.

- **Ransomware Situations:** If files are encrypted by ransomware, first contain it (remove infected machine from network, so it doesn't encrypt shared drives). If you have backups, you can restore without paying – wipe the machine and bring data back. If no backups, see if the ransomware is decryptable (some older ones have free tools). Law enforcement or infosec orgs sometimes have keys if it's a known strain. Paying ransom is generally discouraged (no guarantee they decrypt and it funds criminals), plus activists often can't afford it anyway. Instead, chalk it up to big lesson learned for backups. Also, ransomware often means there's a breach vector that needs closing (phish or open RDP port, etc.) – fix that before restoring.
- **Future Hardening:** After any device incident, strengthen defenses: enable stronger AV, turn on a firewall or enable stricter OS protections (e.g., Windows has Controlled Folder Access to prevent unknown programs modifying files, which helps against ransomware). Maybe segment your network (use a separate computer for risky browsing, or use a virtual machine for opening untrusted files).
- **Emotional Impact:** Especially if malware resulted in data loss or breach, it's easy to panic or feel defeated. Try to approach systematically: what can I salvage, who do I need to tell, how to rebuild securely? Reach out for support – others can help with recovery steps (like colleagues could temporarily take over some tasks while you fix machine, etc.). Keep communication open so the incident doesn't spiral into a bigger crisis due to miscoordination.

## 10.4 Seeking Help and Reporting Incidents

When under-resourced, don't hesitate to leverage available help:

- **Digital Security Helplines:** There are organizations like Access Now's Digital Security Helpline (24/7 global support for activists/journalists), Front Line Defenders, etc., who can advise or assist. They've seen lots of cases and can guide on what to do, and sometimes can analyze suspect files or attacks for you.

- **Law Enforcement:** This depends on context. In some countries, police can be allies if you're a victim of cybercrime (identity theft, etc.). In others, law enforcement might be the adversary or not trustworthy with activist data. So use judgment. For serious threats (death threats from harassers, etc.), reporting can create a paper trail. Even if they do nothing, you have documentation that you attempted to involve authorities. For politically motivated incidents (like state hacking), local police might not help or might even increase risk if they seize devices to "investigate." Maybe instead connect with international bodies or trusted third-party security researchers.
- **Platform Support Channels:** If your issue involves a platform (like account compromise or harassment on Twitter/X), escalate through their support. Use any channels you have – sometimes prodding via social media or asking allied organizations to help signal-boost can get a response if normal support is slow. If you have a media contact, an inquiry from press to the company can magically speed things up (sad but true).
- **Donor or Partner Resources:** If you're funded by or partnered with larger NGOs, see if they have security teams willing to assist. Some big orgs extend help to smaller partners in crises.
- **Community Knowledge:** Situations like phishing waves or malware campaigns may not just target you. Alerting your activist networks ("hey, we got a strange email attachment claiming to be from XY donor, be careful") can uncover that others saw it too, and you can share mitigation info. Collective awareness is protective.
- **Incident Reporting (Responsible Disclosure):** If you found a bug or flaw (like your website was hacked via a vulnerability in a platform), report it to the developers if appropriate, so they can fix it and others are safer. For example, if a WordPress plugin had a zero-day that hit you, letting the maintainer know helps patch it for all. This is more about tech issues than targeted hacks, but it's good karma and improves ecosystem security.
- **Learning and Improving Plan:** After immediate fire is out, have a debrief with your team. What worked, what didn't, how to prevent again? Update your security policies accordingly. If you didn't have an incident response plan written down, now after going through it, write one for future: steps to take, contacts to call (IT support, helpline, etc.), who is responsible for communications during an incident, etc. And integrate these learnings into trainings for staff or volunteers (e.g., if the cause was a phishing email clicked, maybe do a refresher training on phishing).
- **Mental Health and Legal Help:** If incident leads to psychological stress or legal trouble (e.g., doxing leading to threats, stolen data used in court), seek professional help. Legal aid organizations might assist if you fear consequences of leaked info. Therapists or counselors who understand trauma

from online attacks can be invaluable. The toll of incidents isn't just technical; acknowledge the human aspect and get support as needed.

### Checklist: Incident Response Planning

- **I know the common warning signs of a security incident (strange account behavior, device anomalies, etc.) and will act quickly if I spot them.**
- **I have a plan for key scenarios: if an account is hacked, I have ways to recover it or notify others; if a device is lost or infected, I know how to remotely secure it (wipe/lock) and have backups to restore data.**
- **All critical accounts have updated recovery information and I'm familiar with the providers' account recovery process (in case I'm locked out).**
- **I keep an inventory of important devices and accounts, so that in an incident I can methodically check and secure each one (rather than forgetting something critical in the heat of the moment).**
- **I have contact info for resources that can help (digital security helpline, IT support person, emergency phone tree in my org, etc.) readily available offline (in case my computer is down, I have it on paper or phone).**
- **My team and I have discussed how to handle an incident: who takes lead on tech steps, who handles public communication if needed (e.g., telling our community we were hacked), and how to support each other through it.**
- **We practice good logging and evidence preservation (where feasible) so that if something happens, we have data to analyze and to provide to support or authorities if required.**
- **Importantly, we maintain an attitude of learning not blaming with security – if something goes wrong, our focus is on fixing and improving, not punishing the person who clicked a bad link (unless it was gross negligence, but generally we recognize we're all human and attackers are crafty).**
- **After any incident, minor or major, we do a retrospective to update our security measures accordingly. We treat near-misses (like catching a phish in time) as lessons to further harden our practices.**

***(Conclusion: Remember that digital security is an ongoing process. By implementing the layers covered in this handbook – from threat modeling and account protection to secure comms, device safety, careful social media use, file security, and having an incident game plan – you greatly reduce risks. Stay vigilant, keep learning, and you will significantly enhance your resilience against threats.***)

## Conclusion and Next Steps

**Digital security is not a one-time checklist to mark as "done." It's a continuous practice of adapting to new threats and technologies. The landscape will keep evolving – adversaries find new tactics, and developers create new tools for defense. The key is to remain aware and proactive.**

We've covered a wide range of topics in this handbook. At times it may feel overwhelming, but you don't need to implement everything at once. Start with the basics that give the most bang for your buck: strong unique passwords, 2FA everywhere, device encryption, and being cautious with links and attachments. Those alone mitigate a huge percentage of common attacks. Then build on that foundation: introduce secure messaging for your group, routinely update devices, configure backups and incident plans. Perhaps run a team training session to practice phishing detection or a drill of "what if a phone gets seized at a protest – what do we do?"

Security is also a collective effort. Share knowledge with your peers – if you find a great tool or a strategy that works, let others know (keeping in mind not to tip off adversaries to specific defenses). Cultivate a culture where your organization or network values security: that might mean having a brief "security moment" in meetings to remind folks of a tip, or making sure new members get an orientation on safe communications.

Remember that no one is 100% secure. The goal is to make yourself a harder target and to minimize damage if something does happen. By layering multiple defenses (what's often called "defense in depth"), you ensure that even if one layer fails (say someone cracks a password), other layers (like 2FA and encryption) still protect you.

Finally, digital security is about empowering yourself. It may seem like extra work, but it pays off in peace of mind and the freedom to carry on your activism without as much fear of lurking threats. Just as you take precautions in the physical world (locking doors, meeting in safe spaces), doing so online becomes second nature with practice.

Technology can be a liberating force for activists – connecting, documenting, amplifying voices – as long as you take smart steps to manage the risks. With the knowledge and tools from this guide, you are well-equipped to fortify your digital life. Stay curious (keep learning about new threats and defenses), stay skeptical (question unsolicited messages or too-good-to-be-true offers), but also stay confident. By actively managing your digital security, you seize back power from those who aim to undermine you.

Keep this handbook as a reference. Revisit the checklists periodically and see if there are improvements to make or new items to add as your context changes.

Thank you for taking the time to strengthen your security. Every step you take not only protects you, but also your colleagues, sources, and the communities you serve. In an era of pervasive digital surveillance and attacks on civil society, these efforts

are not just about personal safety – they are an integral part of activism and advocacy. Secure activists are effective activists.

Stay safe out there, and remember: security is a journey, one step at a time. You've already taken many steps by reading this. Now, onwards – apply these practices, share them with your peers, and continue the crucial work you're doing, with greater digital resilience than before.

**About the Transatlantic Foundation**

The Transatlantic Foundation is the European and EU-registered arm of the German Marshall Fund of the United States based in its Brussels office. The purpose of the Foundation is to independently promote better cooperation and understanding between the United States and Europe on transatlantic issues and the world, and to support democratic reform and resilience across the transatlantic community.

Ankara • Belgrade • Berlin • Brussels • Bucharest

Paris • Warsaw • Washington, DC

**gmfus.org/transatlantic-foundation**