# Five Steps To Stronger Cybersecurity

*A CISI tip sheet for journalists, advocates, and knowledge workers*

*By Joan Donovan, PhD and Rick Valenzuela*

The Critical Internet Studies Institute (CISI) builds stakeholder capacity in order to combat misinformation-at-scale, ensure community safety and privacy, and build capacity for a public interest internet. **Strengthening institutional resilience means supporting collective privacy and security, starting with the individual.** This **introductory CISI tip sheet on digital security** gives practitioners, especially journalists and civil servants, **five basic steps** to take when protecting their work fostering more timely, accurate, and local knowledge (TALK).

With all the ways we can communicate today come varying degrees of risk – to your data, your personal information, to your conversations with and about friends, family and your livelihoods. The threats to you can range from basic to targeted. For the most part, though, they're basic.

Targeted attacks are different, but thankfully, not so much in methods. Specialized "movie hacker" attacks are really reserved for high-value targets. Just think: these kinds of attacks cost lots of money, time and effort, and when they're used, they're exposed to discovery. Most governments and entities aren't trying to use them, except on prioritized targets.

But one major threat that's often overlooked is our own profiles, especially if we handle sensitive information as knowledge workers. Nearly everything we do is tracked and sold by data brokers, including information gained from our cars, our watches, our phones, the license plate readers in the parking lots where we shop. Going back to targeted attacks, think about it: **why should an adversary use a pricey exploit when they can simply buy the data?**

Because **knowledge workers** are increasingly implicated in institutional power struggles, you may now consider your digital security risk profile plausibly higher. This CISI tip sheet covers basic steps to strengthen your security posture, including **five basic things to do** to minimally raise your protections. Those who feel like they're facing an amplified threat will need specialized and individualized assistance; see more resources at the bottom.

Apart from methods and measures, the one essential lesson about protecting yourself digitally is that security is a process. You don't have to get to everything in one go. Once you have a list of the things you need to do, make a plan and knock off those tasks on a schedule. Keep coming back to it. Corporate and enterprise security people often tout an adapted Pareto Principle to discuss the priority security measures: 20 percent of control mechanisms will thwart 80 percent of attacks.

Doing **these five things** will greatly reduce your risk. We will detail these at length later:

- Use a password manager
- Use multifactor authentication (MFA)
- Use an end-to-end-encrypted app for chats and voice/video calls
- Enable automatic updates (and do them – not "later")
- Manage backups regularly

The first step to improving your digital security is understanding your risks and practices: Your basic profile, a list of what you generally do, and an inventory of whatever software and devices you use to do them. Profiles for some specific practitioners who work with community knowledge–journalists, civil servants, and activists—follow below.

Really, this is little more than noting, for instance, that you have a personal iPhone, personal Macbook, work Windows machine, Gmail on all of them, and a handful of social media accounts. From there you should make a list of the things you want to protect, and what you're protecting them from. This doesn't mean hiding *everything* from *everyone*. A lot of the process of building up security defenses involves **deciding on tradeoffs based on the consequences of the disclosure**. It probably won't matter if your newspaper subscription password is all that unique, but for your email, two-factor authentication should be a high priority.

## *How To Evaluate Your Risk Level*

Making a risk assessment involves asking, "Who poses a palpable, or even **simply plausible threat**?" This determines security measures, including an honest answer about what you're willing to do to raise security.

Start broad with a rough description of yourself:

- "I'm a **journalist** and I talk to sources, and my colleagues at the main office."
- "I'm an **academic researcher** and I monitor and sometimes interact with violent people and their victims."
- "I'm one of a small group trying to **unionize** our company staff."
- "I work in **government** and I make sure payment systems are secure and operating."

Then consider what you use to do those things, such as a phone and laptop, email and chat app accounts. Don't forget your watch, or your car if it's new and connected. IoT devices are often overlooked. Start broad, and fill in more details as you go about an average day noting how you move between physical spaces, devices, and software systems.

Assume that if your employer issues you a phone or laptop, they could have access to all its contents, text messages, call logs, notes, and keystrokes. If you sign into a VPN, either at work or through a personal or public WIFI, then all Internet activity on that device is visible to an administrator with those access privileges. If you use your personal devices on workplace WIFI, your activity could also be monitored. While there are laws against wiretapping, when employers own your cell phone they can also track your movements.

This isn't spycraft, so much as everyday workplace surveillance, which extends the vision of bosses beyond the physical job site and offers a window into your personal life online.

*Bifurcation of work devices and home technology, albeit annoying, is key to closing the shades.*

Consider which basic details about you an attacker would begin with. This is the beginning of the process called **threat modeling**. It's asking yourself:

- What are you protecting?
- From who or what?
- How likely is this threat?
- How bad are the consequences?
- What am I willing to do to avoid surveillance?

For example, maybe you're a community organizer and you want to disseminate information to a group of people who signed up for an email list. You gather info, you maintain a list of group members, and you send them information. Who might want that list? Who wants to stop that information from circulating? What can you do to protect that material from going public? In this scenario, the security of the software you choose to use will be critical. Services like Signal and RiseUp.net are designed specifically for protecting this type of communication.

*The goal here is to simply make it harder to get hacked.*

For help filling in these details, Consumer Reports has an easy-to-use Security Planner guide to walk you through itemizing what you have and adjusting settings.

So what might a security plan look like for different people? Let's start with fundamentals that apply to everyone. The common analogy to defending against adversaries is likening it to escaping a bear attack – you don't have to be able to outrun a bear, you just have to be faster than the other potential victim.

## *Five Basic Security Measures To Take*

### *Password managers*

These are now commonly built into your computer or phone, in web browsers, or from third-party apps and services. Using any of these is better than none. They'll help you manage your passwords so you only have to remember the one for the app. This is a single point of failure, but the tradeoffs are notable and the risk can be mitigated. Attackers know that password reuse is common, so when they get one, they'll try that login info on other popular sites. Password managers help keep track of unique, long passwords for each site. Autofill also protects against misleading, fake sites set up to steal credentials by only pasting to designated websites.

Third-party password managers offer more features than MacOS's Passwords or Windows' Credential Manager, or the ones built in Firefox, Chrome or other browsers. They have more compatibility and syncing options across different devices and platforms, options for password generation, evaluation of password strength, monitoring for your credentials in data breaches, encrypted notes or file

storage, and email masking. Risk can be mitigated by using a good master password and enabling MFA if possible. Options for third-party managers include 1Password, LastPass and the open source Bitwarden. Sure, you're putting trust in that one company. LastPass has been the victim of breaches, notably in 2015 and 2022. In the latter incident, attackers even captured users' password vaults. In both cases, though, the users who were vulnerable to the most severe consequences had weak master passwords. Make that password a good one – that is, long and random, or several unrelated words. It's not even a bad idea to write it down, if that paper is kept in a good place. (Think: your home desk in a book: good; locked in a typical office drawer with a flimsy key: bad.) For those who want to avoid a cloud-based service at all (read: don't mind manually syncing vaults), the longtime go-to app is KeePassXC, which is also free and open source.

## *Multifactor Authentication*

Again, any is better than none, but here the differences are significant. The simplest of these are getting codes sent by email, phone call or text message. A level up would be using an app that generates codes. Another level up is an app that prompts you to accept or deny the login, and the highest security would come from a physical object, whether that's a piece of hardware in a USB key or from the built-in security chip that's made for this embedded in your phone or computer. A great chart and rundown of these are written in this blog post by security researcher Daniel Miessler.

## *End-to-end encrypted communication*

Toward the end of last year, the FBI advised moving communications away from phone network calls and text messages toward end-to-end encrypted apps. Only a few years earlier, though, it had rekindled a confrontation over regulating cryptography: The first Crypto War was in the 90s, when the Clinton administration first sought backdoor access to encrypted communication. The FBI picked this up again in 2016 against Apple, seeking to unlock the San Bernardino shooter's iPhone. But in November, the FBI released a joint statement with the Cybersecurity and Infrastructure Security Agency warning that Chinese attackers have an ongoing foothold in multiple telecommunication companies. A CISA official told Ars Technica, "Encryption is your friend, whether it's on text messaging or if you have the capacity to use encrypted voice communication." Signal and WhatsApp chats are encrypted by default for both one-to-one and group messages.

One of the primary differences between them is that Signal is fully open source and has been security audited. WhatsApp uses a modified version of Signal, but its code is not open to public review. While neither app can see your messages unencrypted, Signal doesn't store anything on its servers, nor does it collect information about chat users, whereas WhatApp does collect metadata; this info about your conversations, contacts, and network connections can be correlated with other Meta platforms, like Facebook and Instagram, as well as sold or shared, whether with a partner, data broker, or law enforcement. That said, WhatsApp is more popular than Signal, and therefore easier for many as a start. Both offer settings for automatic timely deletion of messages. Consider the tradeoffs according to your threat model. The Telegram social media app has an encrypted chat feature called Secret Chat, though it's limited to one-to-one conversations. Like WhatsApp, Telegram is closed source.

## Enable automatic updates

This is an easy one, but one that many people ignore right out of the gate. Updates pile up, the notifications get annoying, and you're even more loath to do all of them. The easiest way out of this is to turn on the setting enabling automatic updates. If you want to set yourself up right, toggle this setting on and allow all the updates that were waiting for you. From there on out, it's the one security measure that's mostly "set it and forget it." Future updates will run in the background, probably overnight, apart from some critical updates and ones that require more free storage space or a reboot afterward.

In general, be alert when receiving such notifications that they make sense: that they're from official software vendors and arrive in expected contexts, like through a system or in-app notification, and not from a web browser popup or link sent by email or text. If you get a notification, you could always Google it and check the official websites or app store.

Updates are how you'll get security flaws patched, but another reason to do them is that once patches are available, attackers will reverse engineer them to understand the vulnerabilities, and then successfully use them against the people who are slow to patch. More and more we see these types of attacks occurring through text messages, so it's advisable not to click any unsolicited links.

## Manage backups

Most devices and some apps will have a feature to make a backup and store them encrypted in the cloud (i.e., through something like iCloud or Google One). Use that or a service you feel comfortable with. You might also want to use an external drive, and your computer will have a way to copy full backups or selected files and folders to that. Having more than one backup – redundancy – is ideal.

If you lose your personal device or your employer impounds your work device unexpectedly, backups are the easiest way to continue your work and also not lose files, photos, and videos. This is the ultimate resilience against ransomware.

These are the fundamentals to make it nontrivial to attack you. From here, let's look at how different people might augment their security to serve their specific threat models. These personae are composites of common stakeholders often entrusted with bridging institutions with local knowledge, and are not intended to reflect any specific individual.

## *Three Archetypes And Risk Profiles*

### Journalist

Verizon publishes an annual report on data breaches that puts cyber attacks on journalists in perspective. Overwhelmingly, the attacks are from financially motivated attackers. This could mean ransomware-ing your organization or otherwise searching for information that could be leveraged for profit. Last year's report noted a mild increase in espionage as a motive, increasing to 14 percent from 8 percent in 2023. It also noted a small increase in the percentage of threat actors affiliated with governments, but that share was still 15 percent last year, whereas organized crime was more than 60 percent. But with all the changes at the heads of government agencies and shifting allegiances of technology corporations, preparation beats paranoia.

The basic security measures described earlier will go a long way to fending off crime, and it's important to apply them to personal devices and accounts too. A lot of targeted attacks begin with researching employees and going after personal email or other user profiles, such as information we freely post about ourselves on social media and LinkedIn.

*It's crucial here to remind friends and family that your profession may impact them if they follow you online or frequently post or acknowledge your relationship.*

When at NBC News, Ben Collins was doxed and threatened after taking on Elon Musk. His parents' address was revealed and local law enforcement had to be notified of the potential for swatting.

Consider carefully what kinds of stories you're reporting; it may warrant trying to clean up your OSINT trail, like scrubbing social media posts, pruning public followers, or even asking friends and family to remove image tags and not follow you. Data removal services such as DeleteMe can help manage removing your information from people search sites and data brokers. If you began reporting on riskier topics later in your career, this could be a monumental task and it's possible that you'll need specialized and individualized advice from an organization or your newsroom.

If you work for a news organization, consult your editor and whoever is in charge of information and physical security. If you're a freelancer, several nonprofits have programs offering planning support as well as emergency guidance. Access Now has operated a long-running 24/7 Digital Security Helpline in nine languages. It's also a partner in the umbrella organization Online Violence Response Hub, which was set up by the International Women's Media Foundation, the International Center for Journalists and dozens of other groups and aimed at helping women journalists. Computer security expert Runa Sandvik worked at the Tor project and The New York Times before launching the startup Granitt to help journalists and at-risk people.

Compromised credentials or devices can then be leveraged to gain access to work environments, so delete your messages on internal systems routinely. For the password manager, the company 1Password has a program offering service for journalists who qualify.

Backups are crucial for maintaining work in the face or severe attacks or interruptions such as ransomware or overloaded and inaccessible servers. For business continuity planning, it's also important that colleagues have an established plan to communicate, such as a backup chat app, in case the company's infrastructure is down.

In addition to the fundamentals, two great protections are available for iPhones and Gmail. On iOS, the above mentioned Lockdown Mode is a smart thing to enable, as seen in the advice from Citizen Lab. It's been observed effectively blocking so-called zero-click exploits, where the attack doesn't require user interaction, but can work on its own silently. Google's Advanced Protection Program locks down your email and other parts of your Google account by requiring stronger forms of MFA (a hardware token such as a Yubikey or a passkey, which you can do with your phone or laptop). It also limits third-party-app access to your account information, and has stronger protections on downloads and browsing, among other things.

Another great tool that journalists might want to use is Dangerzone, developed by Micah Lee. The app runs locally on your computer and will sanitize the document by taking the information and putting it into a clean PDF, preventing an attack through malicious code embedded in files you may receive.

When doing research, be aware that online connections will reveal information about your connection to the service or website. This could be important, especially if you're connecting from a company office. In a great guide targeted to investigative work for the Global Investigative Journalism Network, computer security expert Runa Sandvik notes how a company was alerted to a potential New York Times investigation because an IP address belonging to the newspaper repeatedly showed up as connecting to the company's website. A VPN or a service such as Tor would mask this connection by becoming a relay between the endpoints. If you're a staff journalist, consult your manager and IT department to avoid having the VPN connection itself flagged by your own security. Remember though, while a VPN may hide your IP from being seen by the site you're connecting to, the connection is visible to the VPN, much like that information would be known by your ISP without the VPN. Tor solves this by bouncing your connection through a series of hops. Similarly, the popular Mullvad VPN recently announced a new service partnering with another VPN Obscura that masks your connection so neither service knows the two endpoints.

## *Three Archetypes And Risk Profiles*

### Civil Servant

The above advice to secure personal devices and accounts also applies to government employees. It's crucial for civil servants to avoid using government devices for personal communications. *Hackers, supervisors, and administrators are limited by access to you physically and digitally.* Limiting their visibility into your personal social world is becoming more and more crucial in today's technologically dense environment.

As the new administration purges the inspectors general as well as the longtime directors of agencies and departments, employees will face great scrutiny over communications. While some of these actions are intended to intimidate employees to leave their jobs or to avoid words like "diversity, equity, and inclusion," their workplace surveillance is not panoptic.

Much of the guidance given to government employees is about avoiding a foreign cyber attack, but these tactics are available to anyone. For example in 2016, Hillary Clinton's campaign chair, John Podesta, fell victim to a spearphishing attack – a deception to get targeted individuals to reveal sensitive information. Podesta simply clicked a link and thought he was logging into Gmail. Using two-factor authentication would greatly increase the difficulty and effort for the attackers, and a password manager would not autofill login credentials to a realistic-looking but fake Gmail page.

You do not have to be a direct target of surveillance or a cyberattack to be caught in its web.

Given the adversarial posture of the executive branch to other government departments and agencies, it's crucial to be aware of workplace surveillance. Beyond cameras and digital badges tracking your movements, spyware for businesses has become so popular that PCMag even has a category for it. Workplace surveillance tools often operate under the innocuous names such as "productivity tracking," "bossware," or "tattleware."

While enterprise software is not typically associated with workplace surveillance, services like Zoom, Slack, Google Workspace, and the Microsoft Teams, provide tiered permissions to those with administrative privileges, who may be able to track and access direct messages, emails, and meeting notes or data.

*If you do not own the device or if you are using your workplace email to log into a service, assume someone else could see or intercept those communications.*

Particularly, if you are calling into a service, assume that your phone number will be logged. If your employer has provided you with a cell phone, they may be able to track your movements, monitor text messages, and see who you are calling.

If you sign into a workplace virtual private network (VPN), your employer is able to know everything that happens on that device while on that network. Even if you're working from home, your activities may be visible to an admin when logged

into the VPN. Avoid carrying out any tasks like checking your personal email, bank, or texts, while on the VPN or on a work device. Turn them off when not in use. Conversely, if you sign into the workplace WIFI on your personal devices (cellphone, laptop, wearables), an administrator may be able to access that information. We advise that if it is possible, **leave workplace devices at work** and turn off WIFI access to your personal devices.

Completely eliminating workplace surveillance is unlikely. Therefore, reducing risk and increasing preparation is the key to future cyber civil defense. To that end, start today by establishing a strict (albeit inconvenient) bifurcation of work and personal communications. Never cross the streams, especially if you are a government worker.

Most importantly, it's difficult to predict if you will ever become the target of a direct surveillance operation, nevertheless the ambient recording of so much of our lives became the new normal after the pandemic began. That reality directly advantages those with the power to access data and make it actionable. While national security experts spend a lot of time guarding against foreign adversaries and threats from outside the system, it's becoming increasingly apparent that, in addition to external risks, there are real and immediate risks from inside as well.

It's no surprise that government workers are providing journalists with an enormous number of leaks as purges and resignations are forced across the workforce of two million people. Because workplace surveillance is so ubiquitous, it's crucial to protect yourself and colleagues. If you do come across information that reveals fraud, corruption, or political malfeasance while doing your job, consider becoming a whistleblower.

## *Three Archetypes And Risk Profiles*

### Protester

If you're going to attend a protest and feel uncertain about your communications, the most basic thing you could do is leave your phone at home, or turn it off completely while at the protest site. Make sure that you have a good passcode set to unlock your phone or laptop, as fingerprints or FaceID can be bypassed easily by force or coercion. Disable unlocking by fingerprint or facial recognition.

If you have an iPhone, also consider turning on Lockdown Mode. This would disable 2G, an older form of cellular connection, which is commonly used as a fallback. Android users can explicitly disable 2G in settings too. These connections aren't encrypted and are susceptible to interception, such as from IMSI-catchers, sometimes called by a brand name Stingray.

The UK recently enacted regulations for their use by law enforcement after notably using them to monitor protests, and American counterparts have used them without a warrant. Even the basic connection information is enough for law enforcement to then request account details from cellphone providers. Apple's Lockdown mode also blocks some features in iMessage and basic web browsing. Citizen Lab from University of Toronto is well known for researching Pegasus spyware found on victim devices, and in May last year Citizenlab said it had so far not seen an infection on a device with Lockdown Mode enabled. (Advanced technologists might find this Mobile Verification toolkit from Amnesty International helpful.)

For conversations in chat apps with fellow protesters or contacts, assess whether you should enable disappearing chats.

*Don't save what you don't need. And if your threat model includes arrest and possible criminal charges, you may want to thoughtfully consider what digital devices you're bringing.*

If you can get a separate phone, you may want to run that stripped down to essentials, with a minimal contact list and only necessary communication apps, potentially with separate accounts.

This isn't a burner phone; if you think you need to go to that level, you'll have to actively do a lot more planning and care for the steps you take. Watch a 3-part series from Black Hills Information Security titled "How to Live like a Criminal - Privacy Tips for the Non-Criminal". It covers a lot more ground on planning to purchase and activate a burner and the risks to safely maintain it, as well as awareness of how much information on you from data brokers would be available — whether to law enforcement, other investigators, or criminals.

## More Resources

For additional information, the Electronic Frontier Foundation publishes guides on digital security practices, including configuration details for different apps and devices. Human rights defenders, journalists and civil society organizations can also seek guidance and emergency consultation from Access Now's Digital Security Helpline, and the Freedom of the Press Foundation offers guides aimed at journalists as well as training. CISA also has a site for digital security training and resources for high-risk communities, as does its UK counterpart, the National Cyber Security Centre.

## About CISI

Led by co-directors Dr. Chris Gilliard and Dr. Joan Donovan, the Critical Internet Studies Institute (CISI) fosters knowledge mobilization with the goal of turning intelligence into action. We bridge exceptional research collaborators to creative engagement programs that help the public–and those who serve them–combat misinformation-at-scale, ensure community safety and privacy, and build capacity for a "public interest internet." For more information on our research and programs, see criticalinternet.org.