Internews Journalist Security Fellowship

Training Tips and Recommendatons

INTRODUCTION TO THIS GUIDE

We designed the following resources for people working within journalist communities or small media outlets who would like to become digital safety ambassadors. Each resource includes a summary of key ideas related to the topic and tips for sharing these topics with others. We use the term "training" throughout the document, but we recognize that engagements with journalists will vary based on circumstances and need. Feel free to adapt, modify, translate, and share these documents however you see fit!

HOW TO BE A GREAT AMBASSADOR FOR DIGITAL SAFETY

"IT IS BETTER TO TEACH PEOPLE *HOW* TO LEARN SECURITY RATHER THAN GIVE THEM FACTS ABOUT SECURITY" *

- Good security makes journalists more **confident.** Run engagements that make journalists feel **calmer** and more in **control**, not more fearful.
- You will not know the answer to every question. It's ok to step back, do some research, and follow up afterward. Being **transparent** and **honest** about your own limitations is key.
- Every engagement is **different**. No matter how many times you introduce an individual or group to a topic, tool, or practice, there will always be **new questions** and **new things** to learn.
- To make lessons more effective, make sure to **read the room**. Observe if people are listening, reacting, or making eye contact. If you feel like you are losing the training participants' attention, think of how to regain it.
- Use **personas**, or talk about others' experiences, to allow participants to speak about security without revealing too much about themselves.
- Talk to participants about moments when they felt that they were really **heard.** Ask what you could do to reproduce this in your engagements.

THINKING + TALKING ABOUT TOOLS

- Tools can be incredibly exciting, but make sure not to focus on tools alone. **Tools are a means to an end.**
- When talking about a tool, first **explain** what problem it solves, then **introduce** the tool.
- Don't just talk about the tool; **show** people how it works and why it can make their lives easier and better. If time permits, introduce hands-on exercises.
- There are **no one-size-fits-all** solutions or dogmas. Make sure that you **listen** to participants and tailor your recommendations to address their specific needs.
- Technology and best practices are **constantly evolving** to match emerging threats. A successful ambassador is eager to **learn** and **stay up to date** with the latest trends, tools, and practices.

MAKING SECURITY WORK FOR ALL

- People don't like to be **forced** to follow security rules, particularly when those rules do not fit neatly into their existing workflows. They want to **understand** why those rules exist. In an ideal case, talk to journalists and **co-create** security rules with them, making sure that they fit well into their current work and processes.
- Think of and discuss a security rule that was not followed in an organization, and why. Ask what could have been done better.

Internews

*Mitchell et al, https://geminiimatt.medium.com/how-to-give-a-digital-security-training-4c83af667d40

Secure Messaging

KEY IDEAS:

- **End-to-end (E2E) encryption** means that the message can't be read while in transit. But messages can be read other ways; for example, if a phone is seized and unlocked.
- Use **disappearing messages** as often as possible, especially for sensitive chats.
- Different messengers work for different threat models—there is **no perfect tool.**

TOOLS WE RECOMMEND

Signal is the secure messenger we usually recommend. It offers E2E encryption, collects no metadata, and has been analyzed and endorsed by leading security experts.

WhatsApp is also a good alternative. While it gives Meta access to all your metadata, it's E2E encrypted and more common so you are less likely to stand out when using it.

If journalists do not want to reveal their phone numbers, we recommend they use **Wire** (however, it is less common, so it might stand out and be difficult to convince sources to use it).

Telegram is more common than Wire, but you must explicitly enable E2E encrypted chats and dig through the settings to hide your phone number.

GOOD PRACTICES TO REMEMBER

- Take time with your participants to go through a **messenger's settings.** This might involve enabling disappearing messages, disabling unencrypted cloud backups, and hiding your profile from users not in your contacts list.
- Most messengers offer some sort of **two-factor authentication**, where anyone who wants to activate your account on a new device needs to enter a special password. Discuss such authentication during your training, and enable it for all participants who use messengers for sensitive communication.

TRAINING TIPS

- Ask participants to flag moments when **E2E encrypted messages** could be read (for example, a border crossing). This highlights what encrypted messages do and don't protect us from.
- Discuss if it's practical to use **disappearing messages**. If you need an archive of messages, talk about alternative ways to save them (screenshots that are sent to your newsroom then deleted, hand writing in a notebook, etc.).
- Not everyone is comfortable sharing phone numbers. Talk to participants about this and **alternative apps** like Wire or Telegram for such cases.

TRAINING TIPS

- Encourage participants to install messengers from **reputable** places, like an official app store, and make sure that they do not install any unofficial versions. Many unofficial and potentially insecure versions of WhatsApp and Telegram circulate across app stores and the web. Make sure to **double check** the publisher of the app before installing or only follow app store links from the app's official website. If you're interested in learning more about this topic, check out this article that tracks clones and unofficial versions of another application called Psiphon.

Internews

Account Security

KEY IDEAS:

- Enable **two-factor authentication** whenever possible. Physical security keys are best, followed by authenticator apps. Two-factor authentication through SMS is the least secure, but much better than nothing.
- A password must always be **unique**. Never repeat passwords or use similar ones. Passphrases, consisting of multiple random words, are best.
- **Password managers** are amazing tools; use them as often as possible. In-browser ones work great, too! You can also keep other important and confidential data, like passport numbers, in your password manager.
- Learn to recognize **phishing emails** (formatting errors, sent from weird addresses, links to unusual pages, gives off a sense of urgency) but also use physical security keys and password manager auto-fill as extra protection.

TOOLS AND PRACTICES TO KEEP IN MIND

- Remind journalists that many of them can receive free or low-cost **physical security keys,** through Yubico's Secure It Forward program or from an organization like Internews.
- Some password managers we recommend include **1Password** (free for journalists), **KeePassXC,** and **BitWarden.** Spend a bit of time familiarizing yourself with some of their features. KeePassXC, for example, allows you to store all your passwords on your device (and not the cloud), while 1Password warns you if one of your passwords was leaked or part of a security breach.
- Go through **advanced features** in password managers, like auto-fill in web browser windows, which can protect against some phishing attacks. Each password manager's advanced settings will look a little different.

TRAINING TIPS

- Password managers aren't always easy to set up or implement; you might need to do a **step-by-step training** on how one works.
- Don't let the **perfect** be the **enemy** of the **good.** If someone already uses a reputable password manager or has good opinions about one, don't move them to another one unless there's a strong reason to do so. Similarly, while physical security keys are best, overemphasizing them might lead participants to think that two-factor authentication is just too hard and abandon it altogether.
- Show your training participants how they can download and store two-factor **backup codes** which they can use to log in if they lose their phone or security key.

TRAINING TIPS

- Spend time discussing **physical security keys and authenticator apps.** Explain how physical security keys are resistant to many types of **phishing**. A sophisticated adversary could set up a fake webpage where users type in passwords and second factor keys; physical security keys are specially crafted to stop these attack.
- Explain defense in depth, and how we use many different steps (password managers, two-factor authentication, auto-fill, unique passwords) so that if one defense fails, you are still protected. Use the analogy of COVID precautions (masks and vaccines and testing and distance).

Internews

Secure Browsing

KEY IDEAS:

- When using **HTTPS**, a telecom or government can see the site you're on (for example, wikipedia.org) and maybe how much time you spend there, but not which page you're reading.
- **VPNs** can be a great tool. They form an encrypted tunnel between you and the webpage you visit. This means your telecom or government can't directly see what you're browsing, but your VPN provider can. Since they will have access to your metadata, choose a reputable provider. An unreliable VPN might be more of an adversary than an ally.
- The **Tor Browser** is a fantastic anonymizing tool. It routes your web traffic through a series of other computers, which makes it incredibly hard for any adversary to track your browsing. At the same time, many websites can block Tor connections, either explicitly (by refusing to connect) or implicitly (for example by asking you to constantly select pictures of traffic signs). If you use the Tor Browser most or all the time, you might need to modify some of your browsing habits.
- Websites you visit will know your location (for example, which city you're currently in) unless you use a **VPN or Tor**. If you use a VPN or Tor, they (along with your telecom or government) will probably know that you're using one of those tools.

GOOD PRACTICES

- Teach participants how to check in their web browser if a website is **HTTPS**. Nowadays, most browsers treat HTTPS as the default, flagging HTTP-only webpages as 'insecure'.
- Teach participants how to select **reputable VPNs**. Don't forget that the VPN landscapes regularly changes, so recommendations quickly go out-of-date.
- Look for VPNs that have been **audited**, have a good reputation among security professionals you **trust**, and have **transparent** ownership and terms of service
- Use **Tor Browser** when you require an even higher level of anonymity than VPNs provide, for example when researching very sensitive topics.

TOOL RECOMMENDATIONS

TunnelBear is a Canadian VPN service. Contact Internews for a free license!

Mullvad is an open-source commercial VPN service based in Sweden.

ProtonVPN is a Swiss VPN service.

OTHER RESOURCES

Tor Browser is an open source security tool. Review the JSF workshop recording to learn how to use it, what protects you against, and how it works.

Review the NYT **Wirecutter's** methodologies for how to best choose a VPN.

TRAINING TIPS TO REMEMBER

- If people are working with a free VPN or an untrustworthy one, it's important to move them to a **reputable** one as soon as possible, especially if they are working with **sensitive information.**
- When discussing online tracking, explain its exact **consequences**. Could it sink an investigation if a telecom or government knows what pages you visit?
- In some countries it's **illegal** to use Tor or a VPN. Ask participants if they work in any such countries, what the consequences of using Tor or a VPN might be, and what other steps they could take to protect their privacy.

https://www.

Internews

Secure File Sharing & Collaboration

KEY IDEAS:

- A cleverly crafted malicious file, such as an Office Document, could infect a journalist's device. For this reason, it's best to open suspicious files on your phone or within Google Drive or Office 365. **Avoid desktop apps**.
- **SecureDrop** is great if you want to receive tips and documents anonymously, but can be hard to use. A public **Signal** number is easier. Making both options available to sources is best.
- It's easy to forget how many people have access to our documents on Google Drive. Watch out for **permissions creep.** If somebody no longer needs access to a document, remove this access.

TOOLS AND PRACTICES TO KEEP IN MIND

If you are working with very technical journalists, you can introduce them to **SecureDrop** (which requires the Tor Browser to access).

Check out an app called **Dangerzone**, which turns potentially suspicious documents into safe and readable PDFs. Reputable programmers actively develop it, which means it gets better and better with each version.

There are several good ways to securely share files. You could upload them to **Google Drive** and share them with specified Google users. Alternatively, you could use a tool like **Tresorit Send.**

OnionShare is probably the most secure way of sharing files, but both the sender and recipient need to be online at the same time, and one of them needs to have the Tor Browser installed.

Have a procedure for removing somebody's **access** to all files, logins, and social media posting privileges the moment they leave the project, team, or organization.

TRAINING TIPS TO REMEMBER

- Don't tell journalists not to open suspicious files. It's their job to do so. Teach them how to do so **safely.**
- If a media outlet is interested in running their own **SecureDrop,** get in touch with the Internews team.
- When you are sharing and storing files, think about the country **where** you are doing so. Are you storing your files in a country that has good **legal protections** for journalists? Do you have any reason to be afraid of security services in this country? If so, it might make sense to store your most sensitive files with colleagues in safer countries.

Internews

Building Your Anti-Harassments Toolbox

KEY IDEAS:

- Remember that harassers, who often target members of disadvantaged communities, want to **discourage** journalists from public life altogether.
- Effective **support networks** are crucial. Journalists and their organizations should spend time investing in networks of friends, mental health professionals, and experts who can help them when things get tough.
- Photos that you post publicly could easily give away your **location.** Try not to publish photos from your neighborhood or places you're currently travelling to.

TOOLS AND PRACTICES TO KEEP IN MIND

- Journalists who want to know what information others could find about them online might ask a **trusted friend** to try and doxx them. This would involve asking the friend to search the web for their name, analyze their social media from the perspective of a stranger, and summarize any information that they can find. This exercise can feel incredibly vulnerable and expose sensitive details. Journalists should only ever do this with people they absolutely trust, and it should never be done in a workshop setting.
- **The Block Party App** can help reduce harassment on Twitter by muting or reducing the visibility of harassing content and identifying those who spread it.
- Read up about social media platforms' content and moderation **policies**. When you report a troll or harasser, quote the exact policies they have violated. This makes it much more likely that their content ends up being removed and their account flagged.
- In many cases, trolls thrive off **attention and publicity**. As such, do not engage them if you can; they will see that you reacted and try to annoy you further. If possible, mute rather than block trolls—you will no longer see many of their replies, but they will not know they are muted.
- When you need to criticize a troll, it's best to take a **screenshot** of their post and comment on that, rather than quoting or replying to the original post. That way, you can show the troll's statement to others without notifying them or getting recommendation algorithms to promote the post.

TRAINING TIPS TO REMEMBER

- Remember that this is a sensitive topic, and some people might find it difficult to talk about. Be **careful** and **sensitive** when designing engagements, be ready to listen to everybody, and don't force people to talk.
- Talk to participants about how they could reach out to their communities and loved ones about trolling. Often, loved ones don't need to understand what a trolling campaign is or how it starts—they just need to be able to **listen** to and **be there** for those who face one.
- Discuss the steps newsrooms could take to better **support journalists** targeted by trolls. Those could include providing hotel rooms or temporary accommodation for journalists whose home address was leaked, allocating resources for psychosocial support such as therapy, paying for subscriptions to apps and services like Blockparty, and training digital security teams or others to support those who are being harassed.

Internews