Tabletop Exercise (TTX) Facilitation Guide for Digital Safety Training

Purpose and Introduction

This guide is intended to accompany a set of 11 digital safety-focused tabletop exercise (TTX) scenarios, which may be used to enhance digital security training. This guide is intended to be used by any person who wishes to design and facilitate TTXs as a digital safety training method. Within this guide, you will find brief explanations of what is a TTX, why TTXs can be valuable supplements to digital safety trainings, and how one can develop, plan, and facilitate TTXs.

The 11 scenarios included with this guide were co-developed with journalists in Central and Southeastern Europe as part of the Internews Journalist Security Fellowship (JSF) project and were used in trainings conducted by JSF fellows in the region. These sample TTXs, including some with versions localized into Central and Southeastern European languages and translated into Arabic and Spanish, can be accessed at the link here.

This guide was developed specifically with digital safety for journalists and newsrooms in mind, but it may be useful for planning TTXs for other target audiences as well.

What is a TTX, anyway? Why are TTXs valuable?

A tabletop exercise is a method of scenario-based training which often takes the form of an interactive discussion. TTXs provide an opportunity for training participants to apply newly acquired knowledge and skills by engaging in a fictional situation (referred to as a TTX scenario or scene) that approximates a real-life one. TTX scenarios can examine a large range of security situations such as an office raid, a data leak, a case of doxxing, or a sensitive investigation. While more traditional training methods might focus on transferring certain technical skills and knowledge, a TTX can help to:

Provide a low-risk space for training participants to practice preparing for and responding to security issues that they might encounter.

Stimulate critical discussion around digital security issues and how to best approach them in different contexts and situations. This might be especially helpful for training participants who work together regularly to consider their joint or organizational approach to safety.

Assess how well an individual or organization is equipped to deal with security issues that they encounter.

The point of a TTX is to identify individual, organizational, and community gaps in knowledge, strengths and limitations. A successful TTX goes beyond tools and basic practices, also highlighting what procedures or policies may be missing or need to be improved.

TTXs are most effective when used as supplements to enhance other training methods. This is because the goal of TTXs is not primarily to transfer new skills and knowledge but to further instill and solidify learnings via scenario-based practice, discussion, and assessment.

Components of the TTX scenario documents

Each of the 11 TTX scenes is loosely based on the persona of Sara, which we have outlined in this guide. Each scene furthermore includes the following components:

Goal - The overarching goal of the TTX scenario.

Learning Objectives – Options for general learning objectives to focus on during the TTX. Facilitators likely would benefit from selecting just a few learning objectives to focus on.

Skills/Behaviors to Train on Before or After TTX – Options for concrete and specific skills and behavioral changes for the TTX to focus on instilling in training participants. Facilitators would benefit from selecting just a few skills and behaviors to focus on, and these should align with the selected learning objectives and goal.

Scenario – This is the actual TTX scenario. It includes the following:

Introductory background and contextual information at the beginning

Additional pieces of context provided throughout the scenario

Questions and prompts for participants to discuss and respond to. These are marked by the letter Q followed by a number (e.g., Q1, Q2, Q3, etc.).

Underneath the questions and prompts are some possible responses. These should not be shared with participants during the TTX. They are intended to help the facilitator.

Some scenarios include injects (will be labeled as “Inject”). An inject is a piece of new information or a new development inserted by the facilitator into the TTX scenario at specific times to move the scenario forward or add complexity. An inject might change the TTX narrative and might call for action or response from the participants.

Annexes - Some scenarios (e.g., Scenario 3: Harassment and Doxxing) also include annexes, oftentimes used for the injects during the scenario.

Developing a TTX scenario

Eleven TTX scenarios were developed under the JSF project (linked here). Anyone can modify these, so they better fit the training needs of their community. One can also create their own from scratch. If you are considering revising one of the TTX scenarios or creating your own, consider the following.

Learning objectives should be set at the beginning of the design phase, complement one another, follow a logical order in terms of learning, be prioritized based on importance, and connect back to the overall goal of the TTX. To simplify the training process and make it easier to measure success, connect your learning objectives to concrete skills or behaviors that participants should focus on during the TTX. Ideally, you will set these learning objectives and concrete skills based on the needs and skill levels of your participants. You may know those already if you're working with a community you are familiar with. Alternatively, you may need to conduct an initial needs assessment (perhaps through key informant interviews or a pre-survey) to gather this information if you are less familiar with participants.

The scenario should be as close to real life as possible but generally should not name real people or organizations. Focus on real situations, challenges, and experiences. In rare cases, it may be appropriate to use real locations, but you should consider security risks and potential limitations of doing so. Listing real locations could, for example, mean that people spend too much time on remembering or researching details about them, and focus less on the scenario.

In terms of complexity, the scenario should not overshadow or distract from the learning. Choices can help participants understand the impact their decisions will have but remember that adding complexity and choices makes it harder to build a TTX and will also make the whole exercise much longer.

You can also use time as a design element during your scenario by assigning times to events occurring during the TTX, asking time-bound questions, or utilizing flashbacks or flashforwards. In any case, you should be clear about the use of time at the beginning of the scenario and maintain clarity throughout the scene.

Depending on the skill level of the facilitator and participants, you may consider the inclusion of technical elements within the TTX. This could mean participants are required to use a specific tool, software, or process to move through the scenario. If you do include a technical element, allow for extra time to complete these tasks, and always have a backup plan in case of technical issues or make the technical component optional to accommodate different skill levels.

You can also use injects within your TTX. Injects may be big or small and may be dependent on the participants or independent from them. Generally, injects are used in longer scenarios given the amount of time required. Injects are delivered by the facilitator and the timing is key. To successfully integrate an inject into a scene, facilitator resources are required both before and during the TTX facilitation. Your use of injects should be matched against the need to achieve the pre-determined learning objectives.

Planning a TTX

Before you start planning your TTX, take a moment to **think about your target audience** and how this will affect learning objectives. Are you reaching out to journalists, newsroom managers, security people? Each one of them will be working with very different information and be responsible for different decisions. Alternatively, some TTXs deliberately work with a much wider entity—for example a whole newsroom—to better understand how people communicate and make decisions therein. You might be working with participants who have very different levels of digital security skills, knowledge, and experience. Take some time to modify the TTX so that it best addresses their specific needs

Once you have your target audience, **plan out your learning objectives and consider specific skills or**

behaviors you will train on. Selecting concrete skills prior to your training is essential for helping you scope your focus as a trainer, setting tangible learning goals for participants, and will help set a benchmark for measuring whether the training was effective. See a list of sample skills under the subsection within each TTX document titled "Skills/Behaviors To Train On Before or After TTX." It might be tempting to cover as many learning objectives as possible within a single TTX, but it is more effective to hold a more limited training which covers specific learning objectives. Remember that your audience has a limited time and attention span.

Figure out how much time you will need for the TTX. While sometimes government agencies or corporations create TTXs that span multiple days, your audience might be much more pressed for time. Work, caregiving, and other life commitments of your participants should be taken into consideration. Typically, a TTX that has 4-6 questions or injects might take around 1 to 1.5 hours to complete. This is also very dependent on the size of your group. Bigger groups will typically take longer to complete a TTX. You will also need to factor in time for a debrief and to review the learning objectives and the concrete skills or behaviors you'd like participants to implement following the scene. Participants may require further training or follow-up to be able to successfully implement the concrete skills or behaviors.

Consider the space you have available for the activity. If conducted in person, it is ideal to facilitate the TTX in a space which allows for collaboration. A room with tables and comfortable chairs is likely more conducive for a TTX than a lecture hall. You may also need to ensure that there is quality Wi-Fi or other technological accommodations, such as a projector. Accessibility of the space should also be prioritized if able (e.g., wheelchair accessible, gender-inclusive bathrooms, convenient transportation options, etc.).

Decide on whether there will be multiple facilitation roles and what those will be. It might make the most sense for one facilitator to lead the TTX, with others helping with specific breakout rooms or sub-tasks. Facilitators also may wish to rehearse facilitating some elements prior.

Determine what resources you will need for the TTX. You may wish to create a slide deck, handouts, or other type of presentation materials to display the scene background, questions/prompts, and/or injects. It is also important to consider materials the participants may need for notetaking.

Facilitating a TTX

Facilitating a TTX differs from leading a traditional digital security training or upskilling session. In traditional digital safety training, trainers tend to speak a lot and are expected to share their knowledge with participants. In a TTX training, however, most of the speaking and work happens among the participants themselves, as they discuss the scenario and make decisions. The TTX facilitator plays the role of process holder, making sure that the TTX goes smoothly and meets its goals. The TTX facilitator introduces the exercise, context, and background; answers some basic questions; and adds injects. Other recommendations for TTX facilitation include:

- Make sure that you are deeply familiar with the TTX.
- Remember what the goal and learning objectives of the TTX are and direct the discussions so that participants can reach those goals.
- Communicate roles and expectations clearly at the beginning and throughout the TTX.
- Keep a close eye on the clock and make sure you are respecting and maximizing the time you have with participants.

- Make sure that the space is safe and welcoming and that many people can feel like their perspectives are heard and considered.
- When a participant mentions a good practice, highlight it! This can boost confidence and encourage further participation.
- If you don't know the answer to a question, don't be scared to say so and commit to follow up after the TTX. Utilize community spaces like Team CommUNITY's Mattermost instance to source answers to questions you may not be able to figure out on your own.
- If possible, collect feedback throughout the engagement and be ready to make micro-adjustments. If you plan on hosting multiple iterations of a TTX, you can also gather feedback at the end of the session to better understand how you can improve moving forward.
- If the TTX starts to go in another direction than originally intended, that is ok! Be flexible but make sure that it ultimately addresses the learning outcomes.

If you would like more detailed guidance, below are suggested step-by-step instructions to assist with facilitation.

1. Introduce yourself (and any other co-trainers), explain your role(s), and describe the broad goal of the TTX (for example: today, we will look at how a newsroom could respond to a security incident). This is an ideal time to also set some ground rules as a group.
2. Next, describe in further detail what will happen during the TTX. Explain that it is meant to simulate a fictional situation which approximates real life to better understand our responses and those of our wider community.
3. Depending on group size and composition, you may wish to split participants into breakout groups.
4. Present the introduction of the scene to the participants, including any background story which may be necessary.
5. Narrate the scene, prompt by prompt, as participants move through the TTX. Be available for questions and to help troubleshoot if participants get stuck.
6. Provide injects as needed.
7. Encourage participants to engage and respond to the prompts. Ask them to take notes where relevant or useful. Use your pre-prepared answers to assist if participants are struggling or need examples to get started.
8. After the participants complete the TTX, prompt them to discuss their main take-aways from the experience and their thoughts on TTXs as a training method. This is a great time to record feedback and consider incorporating improvements for future trainings.
9. Once the TTX is concluded, check if there are any concluding materials, follow-ups, or summaries which should be shared with participants.

Appendix 1: Background on Sara (a TTX Persona)

We created a single persona, Sara, to base the experiences in the example TTX scenarios around. This helped us to both add a sense of consistency to the TTXs and give a good starting point for journalists to think about threats and the wider context. We've included our introduction of Sara below, which facilitators can use to set the scene and provide background before launching one of our example TTX scenarios.

Sara is a 41-year-old journalist. She has worked for various local and international news organizations for several years in her country of birth and in neighboring countries.

Last year, Sara started working with an investigative news organization called 'Free Press Now' in her home country that frequently reports on a range of political issues. These include suspected human rights abuses by the sitting government, corrupt government officials, and government policies that make life harder for ethnic minorities in the country.

Because of their truthful and reliable reporting, Free Press Now has become a trusted and popular source of information for the local population.

Following a national election 5 months ago, the new government in power has started limiting press freedoms and last week authorities raided the homes of three prominent journalists in the capital. Recently, Sara's house was also raided, though those who carried out the raid only took several notebooks.

Tabletop Exercises Scenario
1: Missing Device

Created by Journalist Security Fellowship participants

Goal

To help participants plan and respond to a situation when one or more of their devices - which may contain sensitive information - goes missing.

Learning objectives

1. Identify approaches to ensure secure communication between journalists and their human sources
2. Build awareness around the risks of losing a device such as a phone or computer
3. Understand best practice around device protection and security
4. Share good approaches to organisation onboarding and offboard of staff, especially related to device security

Skills/Behaviors To Train On Before or After TTX

1. Installing, setting up and using Signal (or another secure messaging application)
2. Setting up and using an alternative end-to-end encrypted messenger (such as WhatsApp or Facebook Messenger Secret Chat)
3. Installing, setting up and using Mailvelope (or another option for encrypting email)
4. Encrypting a mobile device (setting up a password)
5. Setting passwords for individual applications on mobile device
6. Conducting and encrypting backups of data on mobile devices (using cloud services or external hard drive)
7.
8.

Scenario

A previously unknown source contacts Sara via Facebook Messenger, stating that he has sensitive information he wants to share with her. The file he wants to share contains information about the finances of the current Minister of Defence.

Wanting to keep the source safe, Sara would like to persuade him to transfer the information through a messenger that is end-to-end encrypted.

Q1 - How can Sara explain the concept of end-to-end encryption to convince the source of its importance?

- Nobody—not even the company which operates the messenger—will have access to the contents of the message. The content of the message will not be stored unencrypted on the servers of the company, either
- Law enforcement cannot access it from the chat provider
- If an attacker manages to hack the account which was used to send the message, they will not be able to access the contents of the messages, either (unless there were unencrypted backups)

Q2 - To ensure their communication is secure going forward, what forms of digital communication should Sara consider using with this source?

- Messengers with end-to-end encryption and disappearing messages
- Encrypted email

The source is glad that Sara is focused on making sure their communication is secure, but he is still not sure which method to prioritise. He asks Sara for some advice on messaging apps like Signal, Telegram, and Facebook Messenger, as well as about his email.

Q3 (Choice) - From a digital security perspective, what are some factors to consider when selecting and using different messaging applications?

- Phone numbers: most end-to-end encrypted messengers require phone numbers, and in many places phone numbers need to be registered, so the government knows which person is behind which phone number. This means that, if the government ever looked through Sara's or the source's phone, they could figure out that they were messaging, even if they used pseudonyms or disappearing messages (the only mitigation would be to delete the names from the contacts, messengers, and ideally wipe the phone)
- Secret chats: Facebook Messenger and Telegram offer two modes, only one of which is end-to-end encrypted. This mode is usually called a secret chat or something similar, though it is frequently buried in the settings
- Disappearing messages: pretty much every modern messenger has a disappearing messages feature, though in some it is only available in secret chat mode
- Deleting chats: this is quite straightforward, but it's important to recognise that some messengers only archive, rather than delete, chats
- Awareness around screenshots: any malicious party to the conversation could just take a screenshot or—if the messenger's features do not allow for this—simply take a photo of their phone screen
- Two Factor Verification (2FV): an attacker could take over a messenger account by taking over the phone number that was used to register the account and re-sending the verification SMS to it. This allows them to impersonate the owner of the account, though it does not typically give access to message history. Most messengers now have the option of requiring an additional password in addition

to the SMS code: this means that, even if an attacker managed to take over the phone number, they could not easily gain access to the account
- Strong passcodes or passphrases to log onto the device (phone) itself

Q4 (Choice) - From a digital security perspective, what are some factors to consider when communicating by email?

- The source should create a new email address just to communicate with Sara
- The new email should have a strong and unique password and solid two-factor authentication
- The source should also look out for phishing attacks and use technologies which could help mitigate them, such as physical security keys or password manager auto-fill
- Ideally, the source and Sara should communicate through PGP, for example by using Mailvelope. This means that, even if their accounts were somehow compromised, an attacked would still be unable to read the contents of their messages without their PGP key

The source securely sends the file to Sara and she views it on her mobile phone. She is happy to have that information and she goes out with her friends to celebrate. While at a party, she loses her phone and realises that she has a very simple password (1111) on it.

Q5 - What could happen to Sara's phone and the information inside it?

- Anyone who finds the phone can access the sensitive information if they figure out where it is
- Anyone who finds the phone could message Sara’s contacts and pretend to be her
- Anyone who looks though the information on the phone could either endanger the identity and safety of Sara’s contacts or collect information which could be used for social engineering
- Sara could seriously lose her credibility as a journalist

Q6 - What can Sara do now to limit the impact to her digital security?

- She can remotely wipe her phone, if she has set up this functionality
- She can sign in to her email and social media accounts on her other devices, change the password, and, if possible, click the “sign out of all logged in devices” link

Q7 - What are the pros and cons of telling the source that she lost the phone?

- Discussion with no exact correct answers.

Good news! A friend of Sara who has been with her at the party found the phone in his coat. He called her and returned the phone to Sara the next day.

Q8 - Now that Sara has her phone back, what steps can she take in terms of digitally securing the device in case she loses it again in the future?

- Consider using biometric unlock at times. There are advantages to it (nobody can look over Sara's shoulder while she enters her password, and it will not be captured by CCTV cameras, either) and disadvantages (it's easier to coerce Sara into unlocking her device) to that
- Use longer phone unlock passwords and passphrases. Avoid pattern unlocks (such as those which connect dots), since those can easily be identified by a person who's looking, a camera, or smudges on the screen
- Lock applications (such as messengers) with an additional password as well, if Sara is worried that her phone might be shared/ passed around sometimes
- Set up apps that can track down, locate, and remotely wipe devices

Q9 - From an organisational perspective, what does a good onboarding process look like for a new staff member to secure their devices, like mobile phones and computers?

- Ensure all staff, regardless of position, go through an onboarding process and understand its importance
- Organisations should list clearly the expectations of staff in following the organisations' digital security practices.
- Identify steps to take and people to contact when security might be compromised (like a phone is stolen or a password is hacked)
- IT support should be given to all staff that need it.

Tabletop Exercises Scenario 2:
Operational Security

Created by Journalist Security Fellowship participants

Goal

To help participants to ensure a high level of digital security awareness and best practice exists within their organization, co-workers, and/or freelance journalists.

Learning objectives

1. Theoretically, understand the concept of digital safety as an ongoing process not an end-goal
2. Talking to, teaching, and persuading others about the importance of digital security
3. Practically, discuss options for securely communicating through your mobile device
4. Ensure best practice around secure handling of files
5. Awareness around account settings for networked computers
6. Understanding the importance of threat modeling

Skills/Behaviors To Train On Before or After TTX

1. Setting up and maintaining permissions on collaborative platforms (i.e., Google Drive)
2. (If possible, since some of those features are only available on enterprise platforms) Looking at access logs on collaborative platforms such as Google Drive
3. Setting up and using two factor authentication, ideally with physical security keys or similar phishing-resistant mechanisms
4. Good password policies (using unique passwords, using long passwords, using passphrases) and password managers
5. Encrypting documents (using Mailvelope, etc.)
6. Installing, setting up and using Signal (or another secure messaging application)
    a. Using advanced features within secure messaging app (i.e., timed deletion of messages)
7. Installing, setting up and using Mailvelope (or another option for encrypting email)
8. Working securely with files and documents from sensitive sources

Scenario

Sara is putting together a team of journalists to investigate corruption in public procurement during Covid-19 done by the Ministry of Health. Not all the journalists in the team have the same level of digital skills/safety knowledge and practices. Sara knows one of her team members has some sloppy practices related to file protection.

Q1 - How can Sara encourage her colleagues to improve their approaches to digital safety? What should Sara do to ensure digital security practices when organizing a collaborative team?

- Explain why it is important to have good digital safety: this could include talking about how poor digital safety could significantly hamper a journalist's career, how sources and colleagues are likely to trust you more if you have good digital safety, and the need to protect people around us.
- Discuss what devices they are using, how are they protecting their user accounts, how do they store and exchange files, how are they accessing their work network (are they using their own devices or they are working on company's computers), if they use two factor authentication to secure user accounts and their password discipline (are they reusing passwords, are they using password managers).
- Decide how the team should communicate, store files and access the files. This is to ensure that everybody is following the same protocol related to previously mentioned activities.
- Consider training the team using any newly-established protocols. After setting out the rules the team should run through a dry-run, actually testing out the new ways of communication and see if there are any kinks in the process that need to be ironed out.

Q2 - How will Sara and her team store and share audio files & documents from sources?

- Limit who has access to various files and folders, use sharing settings in places like Google Drive carefully
- Discourage people from taking files and documents out of the work environment (usb keys, e-mail attachments...) which might expand the attack platform and increase the risk of leaks/hacks.
- Ask the team to only ever use work computers to access work files
- Limit what can be installed on work computers, ensure that they always have strong passwords and up-to-date software

Q3 - How will Sara and her team ensure that they communicate securely?

By onboarding the entire team onto the same platform and making sure everybody is comfortable with its usage, Sara can help their team establish a safe and secure way of communication between them.

Consider:
Moving most conversations to Signal, with disappearing messages, and copying over messages which need to be archived
Using PGP on email
Creating strong account security (unique password, 2FA) rules for email

Two weeks before publication for their report, Sara receives a phone call from the main government source in this investigation. Sara knows the source well and trusts them. On the call, the source simply says “The Government knows - there was a leak" and hangs up.

Q4 - From a digital security perspective, what are some of the first steps Sara should take in responding to a possible leak of information?

- Ask everybody within her team to change passwords, just in case an attacker obtained the password to one of their accounts.
- Consider the fact that the government did not necessarily need to break into her newsroom; it’s possible that they found out about the leak by, for example, investigating which government employees were printing what.
- Do a small investigation within the newsroom: check if everybody was following protocols, who had access to files and the information piece that was leaked and what exactly was leaked in the first place. Through the usage of access control and version control you can have an easier way of tracking access to individual data pieces you are working on.
- Think of whether you’d need to speed up publication.

Sara learns that the leak came from the inside of her organization. A designer had access to the organization's shared Google Drive. Sara learned of this by checking the Google Drive access control, realizing that the design team had access to everything on the network because of the nature of their work, and seeing that a designer had accidentally shared a document with a freelance client of theirs who worked for the government, rather than a friend in the newsroom who had the same last name.

Q5 - What could Sara’s team have done differently in this situation?

- Sara should establish secure protocols that apply to her investigative team only. She should ensure there is a clear permission system and that it is followed in practice.
- The team should work with designers in such a way that they only have information on an as-need basis: they should not be given any secret or sensitive details unless absolutely necessary for the publication.
- Sara should also consider security and privacy as a process and not as a state; it’s something that should be constantly iterated upon.

Tabletop Exercises Scenario 3:
Harassment and Doxxing

Created by Journalist Security Fellowship participants

Goal

To help participants conceptualise how to best prepare for and respond to doxxing and online harassment.

Learning objectives

1. Identify methods and mitigation measures for journalists dealing with social media harassment and doxxing
2. Understand how information on social media can be collected and used against journalists and newsroom staff
3. Explore the relationship of gender and harassment, and its security implications
4. Discuss considerations around how a media organisation can establish procedures and practices to protect staff and contractors who are targeted by harassment and doxxing
5. Consider contingency plans for journalists who do not have newsroom support (eg. Freelancers, external staff)
6. Security storytelling and persuading others, how we can talk to people who do not traditionally face harassment that it is a major problem which requires coordinated organizational action and support
7. Organizational security: setting policies within organizations, figuring out ways in which organizations can best support journalists who are facing harassment attacks[1]

Skills/Behaviors To Train On Before or After TTX

1. Managing and updating privacy settings on major social media platforms
2. Using safety tools on major social media platforms, such as reporting and blocking. This includes both understanding how to use such mechanisms and what exactly they do
3. Setting up and using two factor authentication, ideally with physical security keys or similar phishing-resistant mechanisms

Scenario

Sara is working on a new piece on ethnic minorities in her country and how government policies are leading to increased marginalisation of these groups. Over the past few weeks, Sara sees a spike in social media comments on her accounts where she also shares her work. She is also

[1] In most trainings, this would be a learning objective. If you are leading a session with media managers or other decision-makers and it's possible to measure organizational outcomes, you could also run this as a skill

starting to receive hateful and derogatory comments made by different online Trolls targeting her directly.

Q1 - What are some steps Sara can take to block and report the people making these comments?

- She can use the built in block and report functions found on most social media platforms.
- She can contact large social media companies (directly or maybe through her organisation) to report the large-scale harassment.
- Disable posts and replies on her profile
- Be more selective on who can find her on social media
- Choose not to be tagged on social media

Taking effort to block and report some of the main online instigators has annoyed the group of trolls, leading to an increase in hateful content against Sara. Some comments also suggest threats and violence towards her, either directly or indirectly.

Q2 - What are some ways Sara can investigate this aggression against her to determine if it is part of a larger, more coordinated campaign or something more organic.

- She can investigate the situation herself, as well as ask colleagues for investigative support
- She can check whether the trolls all use the exact same language, keywords, or hashtags. If they do, it's likely to be a coordinated campaign
- Depends on the platform. On Instagram, there's extensive options to see info about specific accounts—when was it created, how many people use it, how often has it changed its name, etc.
- Check if it's amplified by any media
- See most common posting time

She tells her colleagues about the posts, but most of the male team members, including her editor, tell her not to worry and that the problem will go away on its own. She is stressed, feels that her team does not listen or understand the problem.

Q3 - Instead of telling Sara not to worry, what are some ways her team and organisation can support Sara, especially in terms of her online presence and digital security?

- Help conduct a full assessment of the situation
- Review together with Sara her digital security practices and safety measures that are in place, and help improve the situation if needed.
- Get get practice and shared experience from others in the organisation
- Allow people you trust to manage your account or look through it so that you are not exposed directly to those words and threats but can still have a presence
- Org can help look for patterns in the harassments

- Track how the harassment takes through the organization's posts rather than just Sara's
- Escalate this to security team & help with investigation

One day, Sara's personal photos are leaked online by one of the trolls. The photos, which she posted on social media years ago, are personal and in some cases include some sensitive information.

Inject - Share between 1 and 4 photos with participants. (Photos can be found in the annex of this document). Photo examples include:

- Sara and her dog walking outside her house
- Sara smoking a marijuana cigarette
- Sara and a group of her closest friends on holiday
- Sara working inside her newsroom

Discuss with the group of participants why each of these photos might be sensitive.

Q4 - What are some ways someone could have accessed Sara's online information, such as old social media posts?

- Sara's friends posted photos with poor privacy settings
- Sara's accounts were broken into
- One of Sara's social media connections might have saved the photos to share later
- Sara's social media photos could have been indexed by a search engine

Q5 - What steps can Sara take to try and prevent further information about her from leaking online?

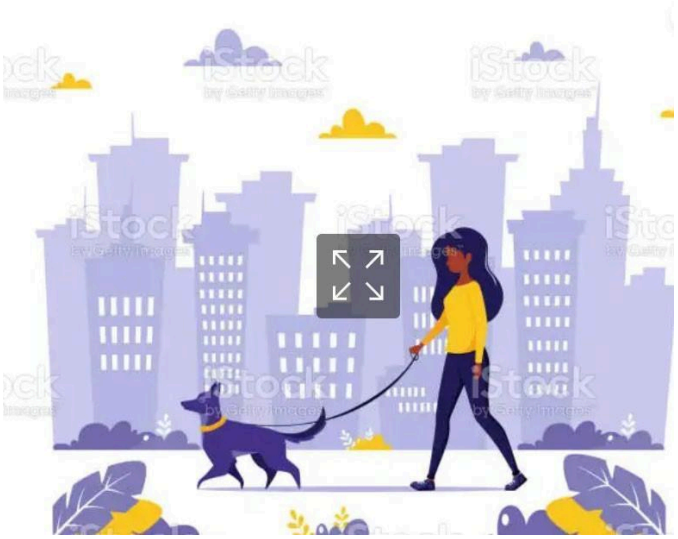
- Delete old photos
- Delete accounts
- Lock accounts
- Upload new photos but which leak little information about her
- Get a report from social media firm that summarises all the data they have on her
- Report the photos that have been posted recently/ report the accounts which have been posting them
- Continue posting work content, even if you post less personal content. If you drop from the internet, the trolls will have won
- Take a screenshot of the posts, document them as much as possible. Record the online aliases of the trolls

Q6 - What steps could Sara and her organisation have taken to prevent this information from being collected and leaked online, especially in terms of digital security?

- Create a group of close friends who are the only ones who see personal photos & personal posts on social media

- Don’t post sensitive information at all (like the photo with the joint)
- Don’t post photos which reveal private info like location
- Open business accounts so that she has an online presence that’s unrelated to her personal life
- Strong password and 2FA policies for social media accounts

Annex 1: Inject Photo Example



Tabletop Exercises
Scenario 4: Authorities entering a newsroom

Created by Journalist Security Fellowship participants

Goal

To help participants theoretical and practical response to the entrance of authorities into their newsroom.

Learning objectives

1. Ensure backup communication plans and technical components are in place in case access to a newsroom or personal device is no longer possible.
2. Understand best practice when it comes to securing digital devices inside a newsroom or organization.
3. Identify ways to secure different files on a digital device, such as a computer or mobile phone.
4. Plan for compromised information in response to authorities entering and raiding a newsroom.
5. Explore concepts around threat modeling and pre-planning for individuals and organizations.

Skills/Behaviors To Train On Before or After TTX

1. Using a tool such as VeraCrypt or similar to encrypt data on hard drives and external drives
2. Threat modeling, specifically in terms of dealing with authorities and office raids: how to assess risks, prepare for one, and debrief after one
3. Organizational and community security, specifically how to work with editors, managers, and lawyers during high-stress situations and identify what question to escalate to which person
4. Using settings within Microsoft Office and Google Drive to see which files have been recently accessed and when
5. (Advanced) If the organization has thorough access logs through a premium Google Drive or O365 subscription, accessing and working with such logs
6. Looking through search and file access histories on leading web browsers and operating systems

Scenario

Sara works in the newsroom of about 20 people. It's a busy Monday morning, with 15 journalists and other staff working from the newsroom, with another 5 colleagues working remotely.

At 10am, approximately 50 police officers arrive at the newsroom. They have a warrant that they show the editor, and then force their way in while at the same time demanding that all the journalists and staff leave immediately.

Sara and her colleagues meet outside and discuss ways to keep their media organization running in a safe and secure manner.

Q1 - What are some priorities in a situation like this?

- Get in touch with a lawyer to consult any next steps
- Contact colleagues who are working remotely
- Audit who has their mobile phones on them and which ones were left behind

Q2 - What are some ways Sara and her colleagues can communicate securely during this time?

- Create a groupchat on WhatsApp/ Signal
- Might be a good idea to communicate through personal, rather than work numbers. Otherwise, the chat might be synchronized to the devices which are still in the office

Q3 - How should Sara and her colleagues manage the organization's online accounts, like websites and social media accounts?

- Change passwords immediately
- If it's possible to remotely log out of the devices which are still in the office, do so but consult with lawyers first so that this isn't considered tampering with evidence (might very much depend on location/ jurisdiction)
- Consult with lawyers prior to posting about the police raid

Sara remembers that as she was leaving the newsroom, she saw the police start putting computers, devices, and papers into bags. Sara was able to leave with her phone, but her laptop was left in the newsroom. The group of colleagues quickly assess what information the police can possibly obtain?

Q4 - How should devices in the newsroom be secured?

- Computers locked with strong passwords
- Screen locks turning on after a short amount of time?
- Encrypted USB keys and external hard drives

During their discussion outside the office, the editor reveals that they did not manage to lock their computer when leaving the office.

The police leave the newsroom two hours later, allowing the journalists to return. The staff come together to discuss the possible information that could have been accessed by the police as well as discuss threats of similar nature going forward.

Q5 - What are some ways a newsroom can immediately assess the impact of a raid by authorities?

- Look at what paper files, if any, were taken away or rearranged (if files were rearranged, it means that police might have photographed them)
- Computers usually have a search/ file access / browser history, look through this as well. You can see recent files in Microsoft Word, and some history in browsers if you use Google Docs. If file history has been cleared, that also means someone might have tried to wipe signs
- It's unlikely that any malware would have been installed during the raid but if you are worried about this, consult with a professional specializing in malware forensics

Q6 - How should the organization ensure they are not further put at risk by this raid by the police?

- Change passwords, just in case
- Talk to a lawyer about what the police was and was not allowed to access during the raid
- If they were using codenames or pseudonyms for their research, rotate those

A few weeks later, the editor of the newsroom calls all the journalists and staff together. They want to understand any similar threats the newsroom might face in the future.

Q7 - In terms of threat modeling and digital security, how do individuals and organizations identify threats they might face?

- Ask the standard threat modeling questions: what information do they have, who might be interested in accessing it, and what would be the consequences if their adversaries succeeded
- When listing adversaries, think about both motive (what would they like to do and why) and capabilities (what are they actually capable of doing, what technical, legal, organizational, and financial means do they have?)

Tabletop Exercises
Scenario 5: Authorities entering journalist home

Created by Journalist Security Fellowship participants

Goal

To give journalists the theoretical and technical skills to ensure the best possible digital security in their home environment.

Learning objectives

1. Understand how to secure digital devices found at home
2. Applying safeguards around paper notebooks
3. Initiating remote file deletion and the positives and negatives around doing so
4. Limiting access to information that has been compromised
5. Preparing for entrance of authorities into journalist home
6. Get participants to think a bit about organizational and community security, specifically how to work with editors, managers, and lawyers during high-stress situations and identify what question to escalate to which person

Skills/Behaviors To Train On Before or After TTX

1. Using a tool such as VeraCrypt or similar to encrypt data on hard drives and external drives
2. Threat modeling, specifically in terms of dealing with authorities and home raids: how to assess risks, prepare for one, and debrief after one
3. Activating tools such as Apple's Find My or Android/ Samsung Find which could be used to remotely lock or wipe devices
4. Using settings within Microsoft Office and Google Drive to see which files have been recently accessed and when
5. (Advanced) If the organization has thorough access logs through a premium Google Drive or O365 subscription, accessing and working with such logs
6. Looking through search and file access histories on popular web browsers and operating systems

Scenario

Following a national election 5 months ago, the new government in power has started directing authorities to limit press freedoms and authorities raided the homes of three prominent journalists in the capital. In response, Sara and a few colleagues came together and discussed ways to protect themselves and their information should they face a similar scenario.

Q1 - What are some priorities in a situation like this?

- Store devices at home in a safe place

- Encrypt and password protect all devices
- Don't include sensitive source info such as names on documents
- Maintain an inventory of what info is kept where (but keep this secure too!)
- Non-digital info: be aware of physical copies
- If it's possible to not keep anything sensitive at home, consider doing such
- Following local laws as well as organizational policies
- Be aware of the legal ramifications of storing sensitive information at your home instead of your office.
- Think about who has access to your home and devices

Q2 (optional) - What are some best practices around storing paper notebooks at home?

- Consider destroying what you don't need
- Don't keep all notes in one location – less info to easily access
- Hide notebooks
- Safe, lock and key, keep it secure!
- What level of sensitive info should be kept at home?
- Using acronyms, pseudonyms, shorthand that only make sense to you

Q3 - What measures can be taken to secure as best as possible electronic devices (computers, harddrives, USB sticks, etc)

- Encryption
- Password protection
- Backing up data off-site
- Consider securely disposing of older devices, especially those no longer in use

Today, Sara left her home at 9am to get a coffee and pick up groceries. When she returned an hour later, the door to her apartment was open. Sara entered her apartment to find two men looking through her desk and bedroom. One of the men was reading through Sara's paper notebooks while the other was holding a bag with Sara's laptop inside. Sara sees that the USB keys and external hard drives on her desk are missing. The two men are wearing civilian clothing, but Sara assumes they work for the government in some way.

Choice 1 - Sara speaks with the two men briefly and is able to leave her home safely. She walks to a friend's place nearby.

Q4 (optional) - Knowing that some of her information, especially from her paper notebook, has been compromised, who should Sara inform about this incident?

- Inform the editor and the newsroom's lawyers
- Before contacting any sources who might have been mentioned in the notebook, talk to the editor and wider newsroom first, as well as to security professionals (if the sources were mentioned only by pseudonym but they receive a call the next day, this could allow security services to tie the source to the pseudonym). It might be wise not to reach out to them at first

Q5 - What could Sara do to further prevent access to her digital information while the two men are still inside her apartment?

- Do everything you can to follow the local law
- Insist that authorities follow local law as well (ie. Allow filming, witness, etc)
- De-escalation techniques
- Figure out who they are and if they have a mandate/ warrant/ permit
- Assess the situation for her own personal safety
- Seek legal advice, call newsroom
- Providing fake accounts and documents (may require some preparation)
- Deflection

Choice 2 - Sara is unable to leave her apartment. The two men ask her to take a set and demand that she provide the passwords to her computer and USB sticks. They threaten to take her to the police station if she does not provide this information. Sara asks for a warrant but they do not provide one.

Q6 - Knowing that she has sensitive information on her computer, including the identification of confidential sources, what options does Sara have in this situation?

- Assessing vulnerabilities and prioritising the most important issues first
- Remote logging out and remote deletion of sensitive accounts
- Identifying all the information stored that was stored at home
- Consider the positives and negatives of informing team members and sources who may be in danger. Maybe make this decision with newsroom support.
- Potential for remote file deletion

Q7 - Sara has a remote file delete programme set up on her computer. What should she consider before deleting her computer files?

- Could be a legal issue – obstruction of justice or destroying evidence
- Think about the potential repercussions, if possible, talk to a lawyer first
- If Sara does not have evidence that the people are from law enforcement but they seem like standard intruders or from a non-state security force, then this also changes the legal and threat landscape

Q8 (optional) - Knowing that some of her information has been compromised, who should Sara inform about this incident? Is the order in which she informs people important?

- Newsroom editor
- Newsroom security/IT team
- Newsroom legal team
- Consider contacting sources
- If a freelance journalist, consider sharing the situation with other freelancers.

Sara ultimately refuses to provide the password for her devices. After searching her apartment for 10 more minutes, the two men leave with Sara's computer, USB keys, and paper notebook.

Sara now has access to her apartment again. She sees that one of her two computers has been left behind along with one of her USB keys. All her paper notebooks have been taken from the apartment.

Q9 - What should Sara do now to ensure her information and security is not further compromised by the actions of the two men that while they were in her apartment?

- The men might have installed malware on Sara's devices; it might be a good idea to send those devices to a digital forensics specialist
- Consider that her apartment could be bugged
- Ask her organization what sort of support she could receive from them
- Talk to her organization, legal, and security advisors on whether it makes more sense from a safety and security perspective to publicly talk about the raid or not

Q10 (optional) - Aside from the digital security aspects of this scenario, what other precautions and responses could Sara have undertaken in order to keep herself and her information safe?

- Learn a bit more about how security forces in the country operate, if there are groups that try to intimidate journalists which are not associated with security forces
- Prepare with lawyers and editors on how to best respond to house raids
- Do not keep sensitive information at home if there are possibilities of house raids

Tabletop Exercises

Scenario 6: Doxxing

Created by Journalist Security Fellowship participants

Goal

Raise awareness about safe social media posting practices for journalists in order to avoid or minimize the risk of doxxing. This is especially difficult for journalists who are public figures and are expected to have a social media presence.

Learning objectives

1. Learning about doxxing.
2. Understanding safe social media posting practices.
3. Identifying potential threats.
4. Learning more about how digital and physical security intersect.
5. Understanding what basic open source research is, summarize how others could obtain information about them based on photos and other data that was publicly posted.
6. Differentiate between muting and blocking on social media, and how adversaries such as trolls could react to either.
7. Understand basic physical security measures in a home or office, such as clean desk policies, security cameras, and locks, and explain what types of attacks (targeted or opportunistic, sophisticated or unsophisticated attacker) they protect against.
8. Get participants to think a bit about organizational and community security, specifically how to work with editors, managers, and lawyers during high-stress situations and identify what question to escalate to which person.

Skills/Behaviors To Train On Before or After TTX

1. Updating settings on major social media platforms, such as the visibility of posts, whether it is possible to see where you were tagged, and possible to find you in search.
2. Setting up and using two factor authentication, ideally with physical security keys or similar phishing-resistant mechanisms.
3. Good password policies (using unique passwords, using long passwords, using passphrases) and password managers.
4. Setting up and using two factor authentication (2FA), ideally with physical security keys or similar phishing-resistant mechanisms.
5. Basic device security: checking for and installing software updates on iOS and Android.
6. Using a tool such as VeraCrypt or similar to encrypt data on hard drives and external drives.

Scenario

Sara is working with a sensitive source on a story about sexual harassment in the government in her country. Sara has a Facebook account where she posts about her daily life. She has played around with some privacy settings, but some of her posts remain public. Those include:

- A photo with colleagues in newsroom
- A photo of her garden and food
- A selfie in front of her house captioned home sweet home
- Pictures with her girlfriend at pride

Q1 - Look at the attached social media photos. What kind of information about Sara can you gather from them? And what other information could you find about Sara from her profile?

- Appearance of her home/ possibly location of her home (a determined attacker could figure out her neighborhood and the like from tools like Google Street View)
- Sexuality, appearance of her partner
- Contact info (email, phone number)
- Relatives and wider social network
- Where she went to school
- City where she lives

Sara's media outlet posts announcing that Sara's story about sexual harassment will go live on the site tomorrow. Trolls post threatening comments about Sarah's sexuality and that she should not be writing about the government.

Q2 - What can Sara do to protect herself from the situation escalating?

- Filter the comments
- Report the comments and the accounts which make those comments to the social media company
- Mute or block the harassing users
- Report the comments to the police
- Ask media org to turn off comments
- Check privacy settings
- Check friend list
- Ensure that her devices are secure
- Warn sources

Q3 - What social media settings should Sara check?

- Who can see her photos and her posts
- Her list of friends/ contacts/ people she follows
- Location settings
- What apps have access to her facebook

- How she can hide her contact information (phone number, email)

While checking her privacy settings, Sara realizes that some photos had been reposted publicly. One photo shows Sara and her girlfriend in front of their house, with the house number visible.

She also realizes that tagged photos were public. Sara's colleague tagged her in a selfie in the newsroom, where Sara's notes were visible, revealing details of the story. This has revealed the name of a sensitive source.

In the comments of the post by Sara's media organization, someone posts Sara's home address, encouraging others to harass her.

Q4 - What can Sara do right now to protect herself?

- Go somewhere safe (hotel, friend's house)
- Have her girlfriend leave the house and stay somewhere safe
- Report this to the police
- Report the comments to the social media company
- Create additional physical security measures, for example by putting cameras on her front door
- Keep her information safe in case her house is broken into (this might include things like encrypting all flashdrives, making sure that she keeps no notebooks with sensitive data at home)
- Deactivate her facebook account (at least temporarily)
- Speak with an NGO that provides shelter and support

Q5 - What can Sara do to protect her source?

- Make the source aware of what happened
- Advise source to practice caution
    - Do not answer calls from unknown numbers
    - Be aware that they might be under physical surveillance
    - Improve the physical security of their home
    - Improve their digital security, for example by enabling 2FA, locking down social media, etc.
- Tell the friend to remove the photo with the source's information
- Speak to an embassy if the source is from another country
- Speak with an NGO who provides shelter and support

Q6 - What could Sara do to prevent this from happening in the future?

- Audit social media privacy settings, reduce visibility of posts
- Create a policy of no photos in the newsroom
- Reduce the amount of content she posts on social media, do not post daily updates which could reveal too much information
- Be careful about accepting friend/ contact requests
- Never use an actual source name; always use pseudonyms

- Turn on the setting (it’s on Facebook, among other places) that requires Sara to review any images she’s tagged in before the tag is made public

Tabletop Exercises Scenario 7:
Account security

Created by Journalist Security Fellowship participants

Goal

Raise awareness on the importance of having secure accounts in a newsroom and develop relevant skills.

Learning objectives

1. Identifying the most vulnerable accounts that journalists use and thus need to protect the most (risk assessment/threat modeling).
2. Considering the best kind of tools for journalists to protect their accounts.
3. Enforcing security practices organization-wise.
4. Discussing the use of secure passwords/passphrases, 2FA
5. Recognizing a phishing attack and responding accurately and swiftly to it
6. Being aware that certain accounts should not be used for sensitive purposes
7. Understanding how organizations can set policies related to file access, passwords, 2FA, and secure collaboration[1]

Skills/Behaviors To Train On Before or After TTX

1. Good password policies (using unique passwords, using long passwords, using passphrases) and password managers
2. Setting up and using two factor authentication (2FA), ideally with physical security keys or similar phishing-resistant mechanisms
3. Secure communication: installing and communicating over Signal, using features such as disappearing messages
4. Sharing settings on Google Drive and O365: how to grant people access to documents, how to remove that access, and check whether they have access
5. Phishing safety: participants should be able to list some of the main signs which suggest that an email is a phishing email or malicious (strange phrasing, sense of urgency, suspicious URLs, suspicious sender address, does not list the recipient by name, and the like)
6. Organizational and community security: setting organizational policies related to file access, passwords, and 2FA, discussing secure collaboration with colleagues, deciding what accounts (private, organizational) should be used for which purposes

[1] In most trainings, this would be a learning objective. If you are leading a session with media managers or other decision-makers and it's possible to measure organizational outcomes, you could also run this as a skill

Scenario

A team of 4 journalists from different news outlets, led by Sara, has started investigating a criminal organization inside their country. They are working with a sensitive source inside the criminal organization, who is acting as a whistleblower, putting themself in great danger. They decide they need to discuss how to secure their accounts as they communicate with the team and with sources.

Q1: What should they be considering in order to communicate safely with each other and their sources?

- Have secure passwords unique to each account
- Make sure that they have an effective two-factor authentication method, ideally security keys
- Keep all software up to date on devices which are connected to the accounts
- Keep in mind connected accounts in social networks/applications etc
- Think about day-to-day communication and its implications

Q2: What kind of tools should they use to communicate safely?

- Password managers
- 2FA, including physical security keys
- Introduce a secure workflow for working with documents, for example Google Drive with very restricted access
- Messaging apps with end-to-end encryption and disappearing messages

Inject 1: During the investigation, the team acquired sensitive information through email, with this info being stored on Google Drive.
Sara received a phishing email, clicked on it, and entered her username and a 2FA code she got from her authenticator app. She does not remember whether or not she entered her password. She realized that this was a phishing page only after entering her credentials.

Q3: What are the first steps Sara should take?

- If possible, immediately change her password for the account which the phishing email targeted. If she used the same password for other accounts, she should change that as well.

If this is not possible:

- Ask her colleagues to change privacy settings on shared documents and drives, so that her account does not have access to them.
- Ask all team members to check their emails and audit what information they have shared with her account.
- Migrate sensitive info to other accounts or devices.
- Revise security protocols within the team to ensure that phishing resistant 2FA (such as physical security keys) is on.

Q4: How to regain access to the hacked account?

- Contact an IT expert/emergency response team for support.
- If possible, get in touch with the company running the account (Google, Microsoft, Proton) and escalate it to them.

The team worked with an emergency response team who determined the source was not revealed but some other information was leaked. They also determined that Sara had been using the same password for her Netflix account as her email account and her Netflix password was leaked.

Q5: How can the team avoid a similar incident in the future?

- Work on more thorough threat modeling: identify potential adversaries, organizational strengths, and weak points.
- Establishing a security protocol when it comes to communicating with fellow journalists and sources. This might include password and 2FA policies, policies on identity and pseudonyms, and others.
- Ensure everyone is keeping up with the above protocol.
- Conduct training on phishing attacks.
- Remind staff and sources that they should immediately report any security mistakes they make, that there's no shame and this is best for the team's security

Tabletop Exercises

Scenario 8: Travel Security

Created by Journalist Security Fellowship participants

Goal

Raise awareness of security dangers when crossing dangerous borders and ensure that information on and off devices is safe

Learning objectives

1. To know how to prepare yourself and your devices for travel
2. To know what tools to use and what not to use
3. Be aware of the legislation of the country you are about to enter
4. Safe ways to communicate once inside the country
5. How to maintain contact with the newsroom back in your home country
6. How to avoid or mitigate being tracked and surveilled
7. How to secure devices and data for border control
8. How to send information securely back home
9. Basic operational and travel security: understanding why it's important not to carry much data when traveling, why it might be inadvisable to publicly post photos of travels, understanding when to contact the newsroom, editor, or embassy when an incident happens during travel

Skills/Behaviors To Train On Before or After TTX

1. Secure browsing: understanding what HTTPS does and does not protect us from, how to clear browsing history
2. Using a tool such as VeraCrypt or similar to encrypt data on hard drives and external drives
3. Deleting message history on messaging apps such as Signal and WhatsApp
4. Finding and clearing search history on a mobile phone's search, as well as on leading maps apps (such as Google Maps) and email providers (such as Gmail)
5. Secure communication: installing and communicating over Signal, using features such as disappearing messages
6. Sharing files with a limited number of recipients through a tool such as Google Drive or O365
7. Managing and updating privacy settings on major social media platforms
8. Basic device security: setting a long unlock passcode for an iOS or Android device, checking for and installing software updates on iOS and Android
9. Compile a list of emergency contacts to carry with you while traveling (embassy/ consulate, newsroom, family), and make multiple copies of this list

Scenario

Sara is traveling to a war-struck authoritarian country, known for surveilling foreign journalists and where VPNs are illegal. She is set to meet with an organization working with the opposition, as she is working on a story.

Q1: What precautions should she take in order to prepare herself for traveling to this country? What situations could she be facing?

- Clear browsing history
- Uninstall VPNs
- Check privacy settings of applications
- Encrypt her hard drive
- If possible, travel with a separate device or at least delete all sensitive data from her device (she can keep such data with her newsroom) prior to travel
- Lock down her social media accounts
- Change the names of sensitive contacts to pseudonyms or delete them altogether

Q2: What kind of information should she audit before traveling?

- Her social media presence
- Photos on her devices, which could reveal a lot about her professional or personal life
- Her address book
- What accounts she is logged into on her devices
- Browser history

Inject 1: Arriving at the airport, she is stopped and searched by border police. They coerce her into unlocking her mobile. She sees that the police have scrolled through her contacts, her messengers, and have typed some things in but they did not take the devices into a separate room. She did prepare, and deleted sensitive information from her devices as well as the names of sensitive contacts, but she unfortunately forgot to clear her browsing history, where she searched for the location of the organization she is set to meet.

She is free to go, but she sees that the police wrote down something, most likely the location she had searched for. Thus, they are aware that Sara will meet with this organization. The security services assume that the organization will give Sara information that is damaging for the government.

Q2.1: What kind of information should she audit after the incident with the border police?

- If her device has a search history, look it up. Also look through the search history in apps such as Gmail (many apps unfortunately do not save search history) and Google Maps
- Check if there's anything new in the browser history
- See if any messages or emails have been forwarded to a new address

Q3: What should Sara do with regards to the organization she was going to meet? How should she reach out? What should she tell them?

- Since her devices were not taken away from her, we assume that they were just searched and not compromised. Given this, it's probably safe to just use that device and a secure messenger (WhatsApp, Signal) to reach out to them
- It might be a good idea not to be very explicit in her messages in case she is searched again, just say something along the lines of "border guards briefly looked through my phone"
- Using disappearing messages or a phone call might be ideal
- Save the name of the organization under a pseudonym and give them an innocent looking contact photo

Inject 2: Sara meets with the source and obtains sensitive info as text files and paper documents

Q4: Knowing what police can do, what should she do to securely get out of the country with the obtained information?

- Scan and then destroy the paper documents
- Send the scans and text files via Google Drive (or similar) to her newsroom, ask the newsroom to make several backups, and then delete the files
- Because of HTTPS, authorities and others monitoring her connection might know that she is on Google services but will not know what exactly she is doing there; she could be uploading photos from her trip, putting documents on Google Drive, or something else entirely. As such, they cannot tell that she is specifically sending through the files. This also means that there is no need to use a VPN

Q5: How does Sara prioritize her own and her source's safety?

- Basic operational security considerations:
    - Do not post locations or photos from travels on social media
    - Do not connect to sources on social media
    - Save source names under pseudonyms
    - Clear Maps history prior to travel
    - Delete all sensitive data (info she got from source, messages with source and the organization, any photos for the reporting) before travel. If the data is needed for her reporting, send it to a colleague who's out of the country first and ask them to make backups before Sara deletes the data
- Own safety: Only publish once out of the country
- Source safety: Be very careful when writing up and publishing, leave out any details which could identify the source
- Both own and source safety: practice good digital hygiene
    - Solid 2FA and password policies
    - Always keep software up to date
    - Use disappearing messages

Tabletop Exercises
Scenario 9: Secure Browsing & Persuading Sources

Created by Journalist Security Fellowship participants

Goal

- Teach journalists how to safely engage with data during sensitive investigations
- Teach journalists how to become good advocates for secure investigative practices

Learning objectives

1. Conducting effective threat modeling with regards to investigations
2. Secure practices regarding safe browsing (VPN, Tor, etc.)
3. Learn how to best use key tools
4. Secure collaboration with colleagues and sources
5. Persuading colleagues and others who might be unconvinced as to the need for secure practices
6. Secure browsing: understanding what information about you your telecom provider can, understanding what information the administrator of the website you visit can see, and how this changes when you use a VPN or Tor
7. Understanding how organizations can set policies related to file access, passwords, 2FA, and secure collaboration[1]

Skills/Behaviors To Train On Before or After TTX

1. Choosing, installing, and using a reputable VPN
2. Installing, and using the Tor Browser
3. Installing and using Dangerzone
4. Opening files on Google Drive or Dangerzone and why this might be preferable to opening them through a desktop application (might include a training with the canary tokens simulation)
5. Use archive.org to archive pages and access archived pages
6. Sharing settings on Google Drive and O365: how to grant people access to documents, how to remove that access, and check whether they have access
7. Secure communication: installing and communicating over Signal, using features such as disappearing messages
8. Organizational and community security: setting organizational policies related to file access, passwords, and 2FA, discussing secure collaboration with colleagues, persuading colleagues about why they should follow best practices
9. Managing and updating privacy settings on major social media platforms

[1] In most trainings, this would be a learning objective. If you are leading a session with media managers or

other decision-makers and it’s possible to measure organizational outcomes, you could also run this as a skill

Scenario

Sara is planning to do an investigative story about corruption. The story would concern a high level official with obvious conflicts of interest with a private company. Completing the story will require Sara to engage with extensive document collections from the government and private sector alike. The story is quite extensive, so Sara cannot complete it on her own and will need to do it in cooperation with colleagues.

Q1: Sara is preparing to start the investigation, which includes a research plan. What are the potential threats she should be looking out for when starting the investigation and downloading lots of documents?

- She will be both searching for and downloading documents from the websites
- If she keeps on being over-active on government and corporate websites, especially the parts of the website which host documents few others access, then her IP address could be logged and the government or corporate security teams alerted. Her IP address could be used to figure out her location or possibly her newsroom's office block
- If the government or corporation sees that many of its documents are being accessed, they could delete the documents from the website
- The documents could also potentially contain trackers
- Do the devices she uses meet appropriate levels of security (up to date software, etc.)?

Q2: Given the threats outlined above, what should her research plan and timeline look like? Which security precautions and tools should she use?

- She should use a reputable VPN or Tor to browse the company and government websites (VPN might be preferable, since Tor traffic might look weirder/ more suspicious)
- Her research plan could include browsing for data, downloading and categorizing documents, talking to sources, writing the story, editing, reaching out for right of reply, and then publishing
- She shouldn't access the webpage at the same hours every day, so it doesn't look like extremely scheduled and coordinated activity
- If there's a concern that documents or links could be moved or deleted, she should add them to an archive such as archive.org
- She should define roles within the newsroom—which colleagues is she collaborating with and who is doing what? What kinds of documents is she going to share with them? How and where will the documents be stored?
- Open documents on Google Drive or use a tool like Dangerzone to turn documents into PDFs before sharing them with colleagues. Alternatively, if possible, she can access the hard copy documents through the source inside the goverment

Sara has followed some of the above precautions. She realizes that she will also need to reach out to some sources to discuss the documents and the wider investigation. Sara has identified her sources and is planning to contact them.

Q3: What precautions and tools should Sara use when contacting sources?

- She should use end-to-end encrypted platforms
- She should choose a platform that is widely used in her region
- If possible, use a phone number that is not tied to her name or identity in any way
- Use pseudonyms for sources whenever possible
- Propose meeting in person, leave her phone at home when she does that. Especially useful when sources do not feel super confident

With the investigation growing in size and complexity, Sara realizes that she will need to conduct the project in collaboration with her colleagues. She has put together a team of trusted people she has worked with in the past in her newsroom. Since she has been put in charge of this project and team, Sara is also responsible for drafting the security protocols.

Q4: What measures should Sara adopt when working with her colleagues on the investigation, which might include sharing the documents she found with them?

- Only share documents which have been previously sanitized (for example through Dangerzone)
- Make backups of sensitive documents
- Use encrypted communication (Signal or encrypted emails)
- Work with as small a group as possible; only share documents on an as-need basis
- Create a fake name for the project
-

Inject: Sara holds a meeting with her team to explain the security protocols, but her colleagues are unconvinced. An experienced journalist with a good track record but poor digital security knowledge criticizes her, arguing that those measures are overkill.

Q5: What arguments could Sara use to successfully persuade her team to adopt the above measures?

- Talk about the risks first
- Refuse to invite others to the investigation unless they also follow the security measures
- Give examples, stories, and case studies of investigations which faces security issues in the past—and the consequences
- Explain how security is often gendered and how she could face a different series of threats than others as a result of that
- Offer to do a small workshop/ training for colleagues who feel less comfortable with technology

The investigation is coming to an end and Sara has to, in line with the right to reply, contact the politician. She knows that the politician will likely do extensive research on her and her newsroom and possibly be adversarial.

Q6: What steps should Sara take prior to reaching out to the politician?

- Remove some publicly available information about herself, for example from social media or the newsroom's website. Have a professional presence but not too much info
- Secure her environment at home
- Make sure to only leave contact details that she is comfortable with (for example, a phone or email that's only at work rather than a mobile where you can be reached at odd hours)
- Ensure that she has extensively archived (for example via archive.org) and taken screenshots of all webpages and documents in case they are rapidly deleted. She could a list of the documents currently online so you can spot deletions
- Have and test out special security measures, such as being ready to remotely wipe devices

Tabletop Exercises
Scenario 10: Sharing Files & Working with Untrusted Documents

Created by Journalist Security Fellowship participants

Goal

- Being aware of the risks of working with documents from unknown sources
- Sharing, verifying, and sanitizing such documents

Learning objectives

1. Learn about good practices and tools related to securely sharing and collaborating on documents
2. Learn about basic verification processes of documents
3. Learn how to sanitize suspicious documents and what the risks could be if you do not do so
4. Understand how organizations can set policies related to file access, passwords, 2FA, and secure collaboration[1]

Skills/Behaviors To Train On Before or After TTX

1. Installing and using Dangerzone
2. Opening files on Google Drive or Dangerzone and why this might be preferable to opening them through a desktop application (might include a training with the canary tokens simulation)
3. Sharing settings on Google Drive and O365: how to grant people access to documents, how to remove that access, and check whether they have access
4. Secure communication: installing and communicating over Signal, using features such as disappearing messages
5. Analyze document metadata and verify documents, for example following the advice outlined in this guide
6. Working with leaked documents and protecting sensitive sources (including this **SaferJourno** resource)
7. Use haveibeenpwnedor emailrep to figure out whether or not an email has already been seen in other places online, and whether it's therefore likely to have been newly registered

Scenario

After her prior investigation has proven to be an unmitigated success, Sara receives an email from an anonymous source who claims to have access to even more documents which would implicate more politicians within the corruption scandal. Given that the trove includes hundreds of

[1] In most trainings, this would be a learning objective. If you are leading a session with media managers or other decision-makers and it's possible to measure organizational outcomes, you could also run this as a skill

documents, she will need to collaborate with her colleagues in order to verify the documents and build a story on top of them. Since the investigation has propelled Sara to fame but deals with a politically sensitive subject, she is also afraid that the source might be either sending her misinformation or malware.

Q1: Sara received the documents as several zipped attachments sent from an anonymous email address. What could go wrong if she tries to open the documents and which precautions should she take?

a. What could go wrong?
    - The documents could contain malware, viruses, trackers
    - The documents could just be fake, an attempt at trolling
b. Precautions
    - You could open documents in Google Drive or something like Dangerzone
    - It's not an issue with downloading it but rather with opening it
    - Download the documents on a separate computer
    - Print those document out and then scan the printed ones on a different computer

Sara securely opened the documents but still has some doubts about whether the documents are authentic. Since the prior investigation embarrassed the governments, she suspects that some within the ministries would like to send through fake information as to undermine the credibility of Free News Now.

Q2: What steps could Sara take to confirm the validity of some of the documents? What steps could she take to do so safely?

- Analyze the documents in line with this guide recently published by Internews
- Check the metadata, for example file creation dates
- Compare information from those documents with that from other places
- Contact human sources about that information
- Work with colleagues on the documents together
- Think about the motivations of the source

Following a week-long analysis, Sara is increasingly confident that the documents are, in fact, legitimate.

Q3: Should Sara try to learn more about the anonymous source sending the email? How could she learn more about them—for example, is there a way to tell if the email was recently created or if it's been used a lot in the past?

- Sara should learn more about the source; maybe they obtained the documents illegally?
- If she learns more about the source, she can maybe understand their goals and aims

- If Sara suspects the source is benevolent: not that much research is needed, protect the identity of the source at all cost. If Sara has evidence or inklings of source being malicious, investigate their identity further
- For the email, look up the address on a search engine, a service like haveibeenpwned, and a service like emailrep to see how much it's appeared on the internet.

The email address has appeared multiple times on haveibeenpwned before. Because of this, Sara suspects that the source is benevolent but knows little about security since they did not even create a new email. Worried that she might uncover the source's identity, she decides not to investigate further.

Q4: How could Sara safely share those documents with colleagues and collaborate with them?

- She can share the printed and scanned documents
- She should share them with a small group of colleagues, ensure that the documents are only analyzed on work devices
- If the documents are on Google Drive, restrict sharing settings as much as possible
- Only communicate with colleagues through encrypted messengers

(The content below is optional; only discuss it if there is enough time and interest from the audience)

The investigative story is almost ready to be published. It has passed fact check, but Sara is debating with her editors what level of detail she should publish. Given the fact that the source has revealed no information about themselves, Sara is worried about potentially exposing them. She therefore does not want to publish the documents.

Inject: The day before the submission deadline, Sara's editor writes to and explains that they will publish the documents in full, unless she can reply with a very good reason why they should not. The editor is senior and very obsessed with Free News Now's reputation among journalists and sources alike.

Q5: What arguments could Sara use to persuade her editor not to publish the documents, but only publish a summary of what's in them?

- The exact leaked documents could be used to identify the leaker, for example through small differences in how they were typed up and drafted or through printer dots. Even if Free News Now publishes a small sample of the documents or an excerpt, they could still be tracked down
- Sara could publish a paraphrased version of the documents and explain that they are doing so to protect the identity of the source
- Sara could say that there is no public interest in revealing the identity of the source or publishing the documents in full—the revelations themselves are not enough

- She might argue that the documents contain personal data of people not involved in the corruption story and therefore should not be published
- Sara could say that, if the documents were classified or restricted, then only a very small number of people would have access to them, making it very easy to identify the source
- The outlet could face legal troubles for publishing classified or restricted documents, which they might not face if they merely possessed and reported on those documents

Tabletop Exercises
Scenario 11: Social Media Compromise

Created by Journalist Security Fellowship participants

Goal

Participants will learn how to prevent and respond to possible hacked social media accounts.

Learning objectives

1. How social media accounts are compromised and what we could do to mitigate that
2. Digital safety and security practices for social media
3. Secure log-in practices, including password policies and two factor authentication

Skills/Behaviors To Train On Before or After TTX

1. Good password policies (using unique passwords, using long passwords, using passphrases) and password managers
2. Setting up and using two factor authentication (2FA), ideally with physical security keys or similar phishing-resistant mechanisms
3. Secure communication: installing and communicating over Signal, using features such as disappearing messages
4. Phishing safety: participants should be able to list some of the main signs which suggest that an email is a phishing email or malicious (strange phrasing, sense of urgency, suspicious URLs, suspicious sender address, does not list the recipient by name, and the like)
5. Basic device security: checking for and installing software updates on iOS and Android

Scenario

Sara is a journalist who began work at a new magazine last week covering politics. Sara's editor sent her to the Prime Minister's office to watch his statement and to ask him two questions: Why is the government controlling social media and websites?
Why is the media not self-regulated?

This video has gone viral. Sara posted it on her social media, with a note further explaining the questions she asked. She received several harassing replies from trolls. Her account grew very quickly overnight and she now has over 1000 followers.

She continues to receive many messages, some encouraging and others including links.
She received one message including a link. The message says that the link leads to a photo of the prime minister in a compromising situation.

Inject: Sara opens the link, which asks her to log in to her social media page again. She enters her credentials and only afterwards does she realize that the URL looked a bit strange and that she entered her details into a phishing page.

Q1: What can Sara do now to protect herself?

- Try to recover her account, for example by logging in and changing her password, if this is still possible
- Report to cyber criminal department
- Alert the company running the social media network
- Secure other accounts (email, Instagram, Linkedin, Twitter, etc)
- Change passwords if she's been re-using any of them
- Set up 2FA
- Set up professional/verified accounts if she is using the accounts separately for work

The hacker uses her account to share similar phishing links with her friends, which will lead to their accounts being hacked as well.

Q2: How can Sara protect her friends?

- Alert her friends that her account was hacked and she does not have access to it
- Warn friends not to click links

Sarah reported this to Facebook and was able to recover her account!

Q3: What should Sara do now that she has recovered access to her Facebook account?

- Change password to a unique secure password
- Set up 2FA, ideally phishing-resistant 2FA such as physical security keys
- Think before she clicks links, use safety tools (such as password manager autofill) for opening links