DIGITAL SAFETY TRAINER'S ASSISTANT

Guidance and suggestions for new and experienced trainers.

Internews

Table of Contents

Acknowledgments

This guide was developed and written by **Natasha Msonza**,
a Zimbabwean digital security specialist.

I created the content from my experiences as a new and upcoming trainer many years ago, and thus have included the kind of content and advice that I would have liked to have received, that would have made my journey significantly easier.

I would like to extend a special thanks to the following organizations and individuals who made this guide possible: Internews for supporting the development of this guide into a tangible product that would be used by Safe Sisters and other trainers interested in going back to basics.

The ISC Project for being an inspiration behind which this protracted training model approach was first piloted in Zimbabwe. Defend Defenders for providing relevant project support and testing grounds for this guide.

The following are some of the individuals who took the time to peer-review the guide and provide meaningful feedback:

- **Helen Nyinakiiza (Uganda)**
- **Sonia Karungi (Uganda)**
- **Azeenarh Mohammed (Nigeria)**
- **Aumarh Ikwueme (Nigeria)**
- **Szeming Ming (Malaysia)**
- **Soraya Okuda (USA)**
- **Norman Shamas (USA)**
- **Tawanda Mugari (Zimbabwe)**

This guide was first tested in a Safe Sisters training of trainer's workshop held in Entebbe, Uganda in April 2018. Thanks to all the Safe Sisters for patiently trying out the guide and providing valuable feedback.

About This Guide

This guide is intended for anyone charged with the responsibility of teaching or assisting others with digital security. It may be especially useful to digital security trainers — people who have engaged in a digital security training of trainers (TOT) program—who are still finding their feet in this area but who often have to train others.

The author of this guide was one of 10 digital security trainers who underwent a rigorous and advanced TOT program with experts. They were coached on how to deliver the topics in this guide and received constructive criticism about their training methods. The creation of this guide is based largely on the author's experience, as well as incorporates information that in retrospect would have been useful to have during the TOT stage.

We believe that a trainer can open the pages of this guide, find a topic, follow the step-by-step approach, and deliver a uniquely comprehensive training.

Let this guide be a friend that sits in the back of the training room.

What is different about this guide?

As there is already a plethora of training guides and handbooks out there (check out the Useful Resources chapter), this particular guide does not seek to reinvent the wheel. At the same time, the author hopes to fill some critical gaps in the journey of digital security trainers who are still trying to find their feet or establish themselves, or even trainers who want to remind themselves how to get back to basics.

The guide is organized in such a way that it:

• Simplifies the training methodology by presenting topics in a logical and sequential flow to fulfill a very basic two-to-three-day agenda with non-advanced participants (see appendices for a sample agenda that follows the flow of this guide).

Essentially, it provides a list of topics to discuss in logical order, as some topics must ideally be trained ahead of others. The ideal ratio is one trainer to 10 participants (max) per training.

• Highlights where the trainer needs to have prior knowledge or use of some technical skills, software, or programs, as well as links to excellent existing resources to 'self-teach' a particular tool.

• Provides talking points and ensures that nothing important is left unsaid, as often happens when trainers are just starting out, nervous, or simply under pressure.

• Provides suggestions regarding the most effective, appropriate, or relevant methods of delivering training on specific topics. (Not everything has to be a PowerPoint presentation!)

• Suggests how much time to dedicate to a particular session. This helps trainers to know how to better plan sessions and what will or won't be possible to cover in a given amount of time. It also helps them to practice session timing accordingly and cover all the essentials of a topic.

The myriad existing guides and handbooks tend to focus more on content and less on logistical issues related to organizing and working through a training. In contrast, this guide will serve a helpful purpose for upcoming and new trainers. It also endeavors not to put things in absolutes, as technology, in particular, is in a state of constant change. Where possible, the guide also endeavors to place emphasis on security behavior rather than security tools, which can either change or become obsolete with time.

In the Useful Resources chapter, you will find a range of existing digital security guides, handbooks, and resources useful for trainers. While the list is comprehensive, it is not exhaustive. Ultimately, new trainers have to find their tribe and utilizing these initial resources opens them up to endless possibilities and networks.

Top Tips for Trainers

1. Always bring a USB drive with all the (updated) versions of the free and/or open-source software and apps that you will use or reference. This helps when there is a slow internet connection at your training venue. The ideal scenario is to have a USB for each participant, preloaded with software for both Mac and Windows. Standard 4GB USBs are sufficient to carry all the software you need. Avoid sharing USB drives to prevent the spread of viruses.

2. Include portable versions of apps in case participants do not want to install certain software or are simply unable to perhaps because they lack admin access.

3. Come prepared for a possible tech fail—and plan what you will do in such a situation. Imagine that the projector stops working or there is loss of power.

4. We recommend that you follow the standard ratio of one trainer per 10 participants. It may be useful to find a co-trainer for a big group, particularly if you will have a lot of hands-on exercises. A co-trainer can look out for participants who are lost, ensure that everyone keeps up while you are training, and help make sure that you keep to your allotted time.

5. There is no shame in not having answers to all questions. Rather than pretending or lying, you can always say that you aren't sure but are happy to check some things with other trainers in the community and get back to your participants.

6. Avoid training more than one database-based tool on the same day—for example, KeepassXC and Veracrypt. While these may be worlds apart for a trainer, some participants are easily confused when trying to remember which is which.

1

Needs Assessment

Needs Assessment

Often, we are charged with training groups of people we do not know or whose security habits and technological competencies we are not aware of. And yet, having an idea of who they are is crucial, as that is what helps us prepare accordingly.

In general, a needs assessment is based on an analysis of either the problem to be resolved or the knowledge that needs to be established. The aim is to establish the information, time, and resources necessary to complete a successful training. A basic needs assessment exercise conducted ahead of digital security training will turn the objectives of the training into a reality.

There are many approaches to establishing participants' needs. What is key, however, is to consult your participants and involve them in the process.

Ideally, you should undertake this exercise in advance of your training. This will acquaint you with the types of people you will be dealing with and will help you determine the materials to prepare, including (among other things) relevant software compatible with prevalent operating systems or the amount of time to allocate to a session.

Conducting Needs Assessment

1. Ahead of the training, prepare a short survey that asks relevant questions to provide a good picture of the participants' profiles. Potential questions might include: what work does the participant do? (this gives you a sense of the security risks they encounter); what computer or phone operating system do you use? How comfortable do you feel using computers? A generic survey is attached in the Appendix.

2. About a week or two before the training, if possible—distribute the questionnaire to the participants, either through email or an online survey link. Use the participants' responses to determine the topics you want to address during your training. Use the feedback you receive from the needs assessment and the risk assessment to start planning your training agenda. Keep in mind the logical flow of topics and the amount of time you will have available to conduct the entire training. A sample schedule for a typical three-day introductory training can be found in the Appendix.

Top Tip

The trainer should leave room for flexibility in the agenda, recognizing that people can sometimes over- or underestimate their tech knowledge, risks, etc. In many cases, the initial results are different from reality once the trainer meets and starts speaking to participants.

You will notice that there is a Needs Assessment session included on the first day of the sample-training schedule in the appendices. At this point it can be a discussion about the needs assessment that the trainer conducted in advance.

This discussion sets the tone of the workshop, whereby the trainer briefly describes key findings and the fact that those findings to a large extent, informed the content and approach used in the training. It is also time you can use to physically distribute the needs assessment questionnaire, in the event that there was poor or no response when you attempted to do it in advance. In such a case, you will need to utilize the first break to consolidate your training approach after quickly analyzing the completed questionnaires.

2

Risk Assessment

Risk Assessment

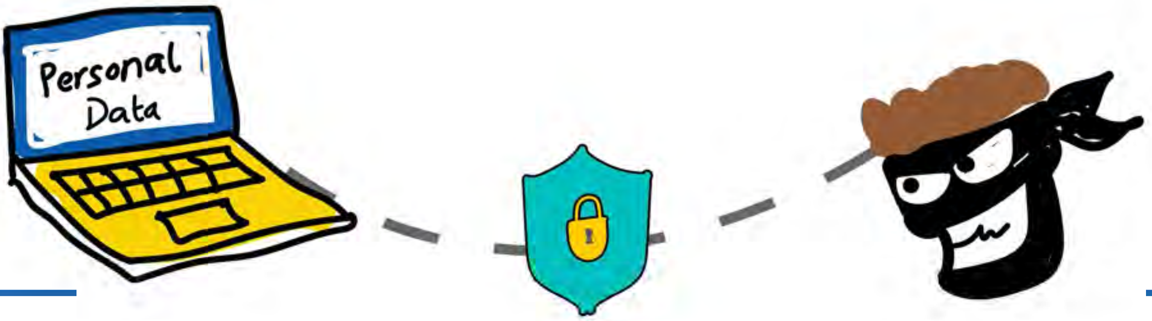
Ahead of any digital security training, there is value in establishing and understanding the participants' **threat model.** This can be done by conducting a **risk assessment exercise** before the training. Although it happens on the first day of training, the process of addressing the threat model forms an important part of creating the agenda. Remember that the agenda is fluid, and can constantly be adjusted according to different factors as they arise.

Undertaking a risk assessment means that you are committed to creating a training agenda that is appropriate, relevant, and addresses the participants' specific needs. The session is about helping the participants identify and understand the unique threats that confront them in their work, with the ultimate goal of countering them. At this point, even though you already have a draft agenda, doing this exercise is mostly for the sake of the participants and obtaining buy-in: i.e for them to gain a better contextual understanding of why they are having this training (namely to address the issues that affect them in their use of technology).

At its most basic level, threat modeling is about grouping different types of threats, vulnerabilities, and risks to determine what is most damaging and/or likely to happen. It is a process that should be done regularly, as threats against individuals and organizations are constantly evolving. While there are many ways of conducting a risk assessment, we will discuss one of the simpler approaches here.

Dashboard

Proposed Method of Delivery	Interactive brainstorming followed by plenary discussion
Materials You Will Need	Flipchart paper, markers, sticky notes, sticky tack/tape (for sticking paper to walls)
Estimated Time Spent on Activity	120 minutes
Useful Analogy/Metaphor	**THREAT MODELING:** It's like deciding between whether to worry about someone stealing your family heirloom or your wallet. Even though you love the heirloom, it's a lot more likely that someone will try to take your wallet. – Analogy adapted from Hannah Masuga, Sideways Dictionary
Useful Related Resources	https://rorypecktrust.org/getmedia/f8ca7438-3202-4890-89e3-c1d8dba80bad/Rory-Pe



A way of narrowly thinking about the sorts of protection you want for your data. It's impossible to protect against every kind of trick or attacker, so you should concentrate on which people might want your data, what they might want from it, and how they might get it. – Electronic Frontier Foundation

1. The first step in conducting a risk assessment is to consult with the participants whose expertise and experience will be integral to the training design. It is important to seek the opinions of end users to establish exactly what risks confront them in their work/operational environment.

2. The second step is to identify the specific security threats confronting the participants. This constitutes their threat model.

Process

- Distribute 5–7 sticky notes per participant.

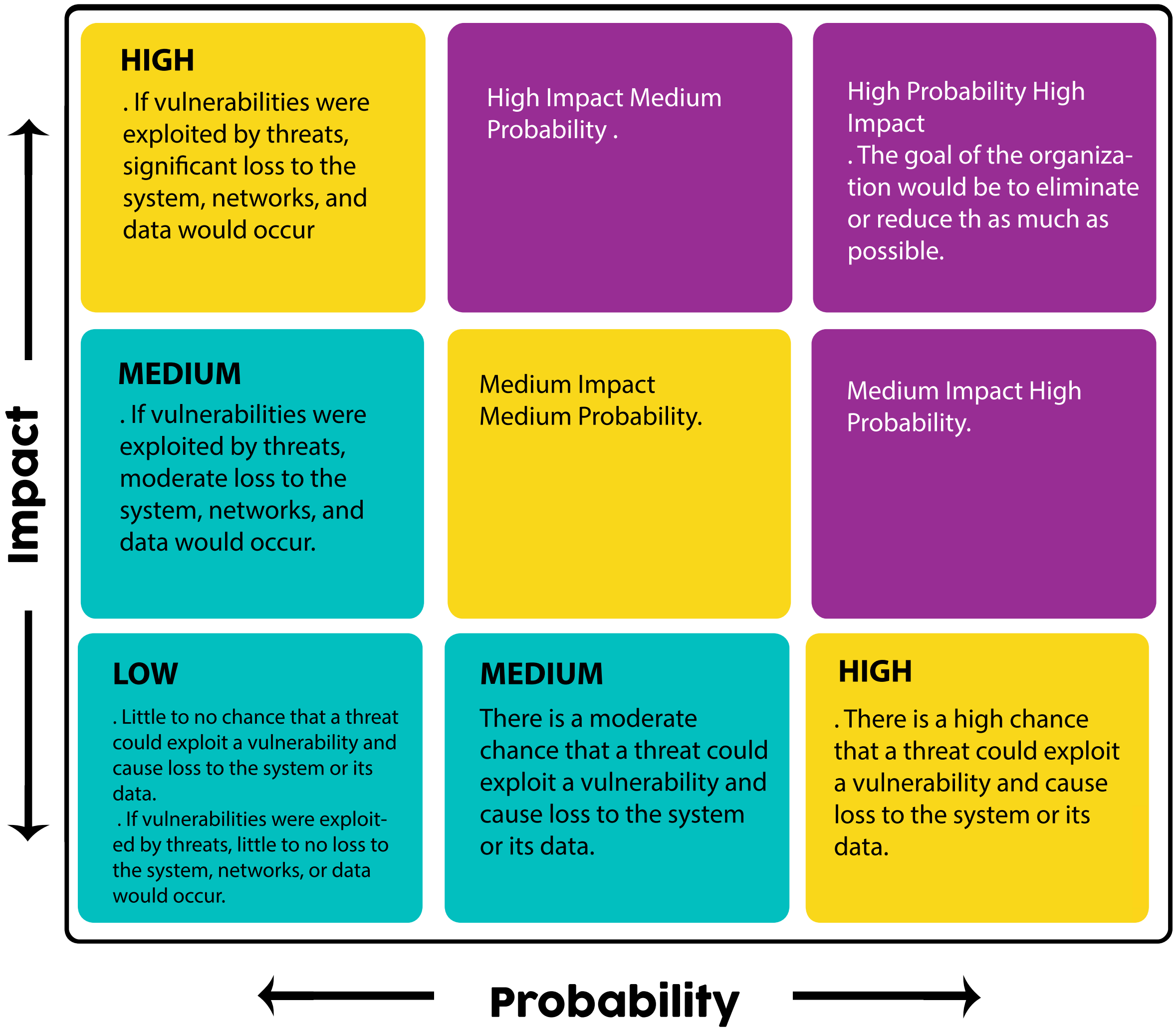
- Have a mini-discussion about the task you want them to do, namely individually writing down a few key words about their perceived information and digital security risks. (Risk is the probability of an identified threat actually occurring.) Ask them to write down the security issues they are most concerned with regarding their use of digital spaces and technologies. Ask the participants to reflect on the following questions to guide them in thinking about the issues (they should use markers to write legibly on each sticky note):

o **What do I want to protect?**
o **Whom do I want to protect it from?**
o **How bad are the consequences if I fail?**
o **What is my current ability/inability to address the potential risks identified?**

- Give the participants about 15 minutes to complete this task. Take note of the risks identified. Depending on the nature of their work, these may include: loss of devices through theft and possible information breaches, email hacking, malware infections, etc.

- In the meantime, draw a **Risk Impact vs. Probability Assessment Matrix** (see example below) on at least two large papers taped together. Stick this onto the wall somewhere in the room.

Risk Impact vs. Probability Matrix



HIGH . If vulnerabilities were exploited by threats, significant loss to the system, networks, and data would occur	High Impact Medium Probability .	High Probability High Impact . The goal of the organization would be to eliminate or reduce th as much as possible.
MEDIUM . If vulnerabilities were exploited by threats, moderate loss to the system, networks, and data would occur.	Medium Impact Medium Probability.	Medium Impact High Probability.
LOW . Little to no chance that a threat could exploit a vulnerability and cause loss to the system or its data. . If vulnerabilities were exploited by threats, little to no loss to the system, networks, or data would occur.	**MEDIUM** There is a moderate chance that a threat could exploit a vulnerability and cause loss to the system or its data.	**HIGH** . There is a high chance that a threat could exploit a vulnerability and cause loss to the system or its data.

Impact

Magnitude of potential harm that could be caused to the system (or its data) through successful exploitation

Probability

The likelihood of a risk occurring, considering security rneasures already in place, extent of vulnerability etc.

- Explain how the matrix works. Ask the participants to place each of their sticky notes into the section of the matrix they deem most appropriate for the risk or threat identified.

- Have the participants sort of 'mosh pit' and map the sticky notes accordingly. You might want to stand close by and fact-check that some participants are, in fact, placing stickies into the correct sections.

- The goal of the exercise is to establish the types of themes that emerge and the extent to which participants agree in terms of their gravity and the probability that these risks and threats will occur.

- On the Risk Impact vs. Probability Assessment matrix, the goal is to work toward reducing/eliminating all elements that fall in the red sections.

- Considering the perceived risk and the factors that point to that risk actually materializing will determine where someone places their note along the matrix.

  For example, if there are some measures in place to prevent a fire, then the probability of loss of equipment and data through these means is significantly less than if such measures did not exist.

3. The third step is to have a plenary discussion to establish the solutions that may be required, available, or possible to address the identified risks. This process is also helpful in determining whether some stickies are placed incorrectly.

4. The fourth and final step is to explore the issues that may be addressed through training and recognizing that it is up to senior management and other key stakeholders to identify other issues and allocate appropriate finances and resources to address them accordingly.

3

Device Hygiene and Account Security

Device Hygiene and Account Security

KNOW BEFORE YOU START:

This session requires prior knowledge of how to use a password manager such as ***KeepassXC.***
Learn how to use ***KeepassXC*** here:
https://securityinabox.org/en/guide/keepassxc/windows/

This is where digital security begins—with basic things like how people secure their devices, the antivirus program they use (if any), whether they know where and how to check their computer's vitals, etc.

This is one of the topics you want to discuss early in your training—how people understand and handle the technology they currently use. Device hygiene and maintenance is about raising users' awareness of their computers' security features, where to find them, and how to set the optimal settings. There are many possible approaches to discussing device hygiene. In this guide, we will give an example of a method that has been tried, tested, and generally found to work.

Please note: This example will be most applicable to Windows users. In most cases, the majority of participants will likely be using Windows computers. However, Mac users should not be alienated. The trainer should mention the equivalent security settings for those users during this discussion.

Dashboard

Proposed Method of Delivery	Making use of Windows Action Center and interchangeably showing your computer screen and writing key terms for discussion
Materials You Will Need	Projector, flipchart stand, butcher paper, and markers
Estimated Time Spent on Activity	90 minutes
Useful Analogy/Metaphor	**PASSWORD MANAGER:** is like putting all your eggs in one basket (database), but with some safety mechanisms to ensure that the eggs (passwords) never break – Anon.
Useful Related Resources	https://level-up.cc/curriculum/protecting-data/creating-and-managing-strong-passwords

Key Process Points

• Kick-start the discussion by asking how many people have a password on their computer. Make it a fun and interactive short session by teasing out questions like

'Why don't you have passwords?' and

'Why do you have passwords?'

The purpose of this discussion is to help participants understand why securing their devices is important.

• From your computer, open and show the Windows **Action Center**—usually, you can find this by searching for **Action Center** or by navigating through the Control Panel settings. The Action Center contains **Security and Maintenance** dropdown settings.

Refer to various key components listed under **Security** (not necessarily everything). This is important because it is where participants will check and configure their computers' vitals. Note that while some later versions of Windows may not have a distinct Action Center, they will have relevant **Security and Maintenance** settings in the **Control Panel.**

Key points to highlight

- Reading the color codes: for example, red usually points to something in a critical state that should not be ignored. This is a convenient way for the user to review the state of their system and immediately locate Security and Maintenance issues that need attention.
- The Action Center will enable you to discuss the following aspects as they are listed in the Security dropdown menu.

Windows Updates

- Write 'Updates' on the flipchart, and ask the participants to define this term. Investigate and discuss with the participants why some of them potentially do not install updates.
- Explain the purpose of updates and recommend to them that they should enable the setting to automatically download and install updates.
- At the same time, discuss the 'Check for updates' setting, which notifies the user about non-critical software updates, either for Windows components or for other Microsoft products.

Malware and virus protection

- Write 'Malware' on the flipchart, and ask the participants to define this term.
- Explain what malware is (derived from the combination of the two words 'malicious' and 'software') and how it manifests as Trojans, worms, spyware, adware, ransomware, rootkit, etc.
- Write the word 'Virus' on the flipchart, and ask the participants to define this term. Discuss the various kinds of viruses and how they may be acquired: many device infections are caused by users unwittingly visiting untrustworthy websites or downloading malicious software.
- Discuss signs that indicate the presence of malware, as well as the occurrence of viruses when antivirus protection is not installed, is disabled, or has outdated definitions.
- Discuss the recommendation to install antivirus protection; show participants how to turn on antivirus software (if already available) or update antivirus definitions (also if already available).

Other useful discussions to have:

- How to know/check what antivirus program one currently has.

- How to know which antivirus software to get. Some users decide on the basis of perceived popularity or settle for whatever was preloaded on their device. A useful recommendation is to make reference to av-test.org, a site dedicated to testing and comparing antivirus programs. A good indicator in selecting an antivirus program is to check if one's preferred program appears there at all or how its performance is ranked among others.

- The importance of having an antivirus program, even a free one. Take time to explain that free does not necessarily mean less effective than the paid version; it often just means that the paid versions tend to have extra features, such as tech and customer support or backup.

- Point out that the ideal antivirus program also depends on the user's needs. For example, a user who spends a lot of time on the internet might do well with an application with a strong focus on internet security. Mention the basic features of a good, all-inclusive antivirus program: protection against various types of known viruses, performance of automatic and regular security scans, and little to no impact on the device's performance.

- Discuss 'endpoint security' software suites (e.g., Sophos or Kaspersky) and the features they provide. Often, they can provide more than just malware protection, but include things such as checking patching, etc.

- Talk about why two antivirus programs should not be installed at the same time. This is a common occurrence among some users who feel that the extra program does what the other can't. This is not correct—two antivirus programs trying to perform the same job potentially slow down the device, resulting in a conflict and, ultimately, no protection. While no antivirus application is perfect, users can choose the one that gives them the best possible protections.

- Finally, there tends to be a common misconception that Mac computers are immune to viruses and malware. Take the time to explain that although Macs indeed tend to be hardier, they are not immune to attacks. Historically, fewer viruses were created for the Mac operating system (since fewer people could afford the costly equipment, it would not be very profitable for virus manufacturers). However, there has been a recent increase in Mac-targeted malware as more and more Apple products are being sold, making their users an attractive target for hackers. A number of free and paid antivirus programs are available for Mac OS.

Network firewall

- Write 'firewall' on the flipchart, and ask the participants to define this term.
- Explain what a firewall is and the important role it plays, including that it should be set to ON. A useful analogy: 'A firewall is like the intelligent doorman or security guard who observes all the traffic going in and out and stops suspicious-looking characters from automatically entering.'
- The firewall is essential in recognizing malware.

Locking devices

- Ask participants if they have enabled screen lock settings that require a password to gain entry to their computers. Discuss the importance of locking computer screens when the user steps away or the computer is not in use. Locking the computer is an easy but often overlooked way to keep information safe. Locking the computer each time you step away, even if for a few minutes, may feel inconvenient, but when your computer is unlocked and unattended, you leave important information vulnerable to anybody passing by. It's important to always imagine the type of sensitive information that could be accessed easily if a computer is left unlocked.

- Casually ask why some may not have screen lock enabled. In some cases, users simply do not know or have forgotten where to enable or change their screen lock password. Demonstrate the different ways to enable or change the screen lock setting. In Windows, the following options often apply:

o Combination of the Ctrl+Alt+Del keys
o Using the Control Panel and selecting a screen saver, with a password requirement to use the computer again
o Pressing the Windows key + L
o Start button + Lock

Passwords

This is an important discussion to have because passwords are often the first line of defense in protecting both devices and people's online accounts.

- Ask the participants what makes a good password. They will likely give a combination of responses that involve mixing capital letters, numbers, and special characters. Good passwords are:

o Unique—as in not using the same password on multiple accounts.
o Long—current password standards from NIST emphasize length as the most important factor.
o Constructed in vernacular languages other than English. Most password cracking tools work off wordlists (the majority of which are in English). Using multiple languages or non-English in your passwords will:

a) Make the number of options exponentially greater (a hacker would have to use multiple language dictionaries) and done in a way that the person trying to crack the password would have to figure out the other language.

b) Reduce the chances of it appearing in known password caches.

• Since many people struggle to create and then remember long passwords, do a short interactive exercise here. Demonstrate on the flipchart examples of how to create long, complex, but memorable passwords. The usual tricks include:

o Thinking of something memorable, like an old nursery rhyme, favorite song, or favorite bible verse, and then using the first letter of each word to create a password or passphrase. **Example**:

Baa, baa, black sheep, have you any wool? Yes, sir, yes. sir; three bags full...

This becomes: **bbbshyawysys3bf.**

For further play on this, creatively substitute some of the letters with symbols or special characters. For example: bX3s#y@wysys3bf.

o Try substituting or mixing different languages into passphrases.
o Because the password for each account must be unique, and because people have many accounts, it may not be entirely realistic to engage in this process for every account—not to mention the difficulty of remembering which password goes with which account. This makes for a good segue into the next part of the discussion: using password managers.

o A useful thing for the trainer to point out can be some of the current NIST standards on passwords. At the time of developing this guide, one of the standards stipulated that passwords needed only be changed when there is good reason to do so (such as when there has been a password breach on the user's account service).

Password Managers

• Check to see if any participants currently use password managers. Talk about what password managers are: apps that create and remember your passwords and store them in a secure database. All of them tell you how secure each of your passwords is. Some password managers alert you when the services you use are hacked and tell whether you were personally exposed.

• Discuss how offline and web-based password managers are available, and give examples of commonly trusted and used options (e.g., 1Password, LastPass). 1Password has a partnership with haveibeenpwned.com to notify a user if their password has been found in a breach. Some password managers are not free.

• Although there are several good web-based password managers, an important recommendation is to opt for locally stored solutions as much as possible. Information that is stored online is generally susceptible to different types of information leaks. A free and open-source password manager may also be sustainable in the long run.

• Show your screen, and do a walk-through of how KeepassXC works to create and store passwords locally and how to retrieve passwords from the database for use on accounts.

• Talk about KeepassDroid/MiniKeepass and other available alternatives (mobile version) to address concerns about portability.
The database can also be saved in encrypted or unencrypted form on a USB flash drive or in the cloud so it can always be retrieved for use. However, the user will need to protect it with a very strong password and will require a copy of KeepassXC software to be able to open the database.

4

Mobile Security

Mobile Security

Many everyday technology users depend largely on smartphones and other mobile devices. This makes them highly susceptible to a number of security risks, as more and more, cyber criminals look for ways to exploit vulnerabilities in apps, software, and operating systems.

Dashboard

Proposed Method of Delivery	Mostly discussion
Materials You Will Need	Smartphone, flipchart, and markers
Estimated Time Spent on Activity	60 minutes
Useful Related Resources	https://securityinabox.org/en/android https://level-up.cc/curriculum/mobile-safety

Key Process Points

Kick-start a plenary discussion of the different ways people secure their mobile devices. The participants themselves might have a range of practices they currently use. Some things that can be included in the discussion are:

- A lot of what applies to computers also applies to phones. After all, smartphones nowadays are basically computers, only smaller.

- **Antivirus**—If we view smartphones as mini-computers, this means that they also need protection against viruses and malware. Most popular antivirus providers also have a version for mobile.

- **Screen lock**—Invoke some of the lessons from the session on passwords. If a device is lost or stolen, a strong screen locking mechanism can prevent intruder access to personal information. With mobiles, it might be useful to explore the various options for locking devices (including PIN and Pattern to Passphrase), along with the merits and disadvantages of each.

    o **Pattern:** Point out how a pattern can become discernible over time, literally leaving a pattern that is almost visible to a keen observer. There are also very limited permutations that a keen intruder could attempt before potentially getting it right.

    o **PIN:** With PIN codes, many people are guilty of using the simplest and sometimes most obvious code, such as their year of birth, street address, etc.

    o **Passphrase:** While longer, the passphrase tends to be a more secure option, though it should not be obvious/easy to find or guess information about the user.

    o **Biometric:** Use of biometric authentication features (e.g., facial recognition or a fingerprint scanner) tends to make device security more difficult to crack. However, it's important to mention that people can sometimes be threatened and forced to place their finger on the sensor or look into the device camera.

An important dimension to this discussion should include setting mobile devices to automatically lock after a set short time without activity.

- **Updates**—As with computers, a smartphone's software, apps, and operating system need to be updated regularly. New vulnerabilities are constantly being discovered, and updates are the main avenue through which software vendors provide necessary patches as soon as they become available. An important thing to discuss here is that devices occasionally need to connect to the internet for major updates; Wi-Fi is the best and cheaper route.

A lot of basic smartphone users are often confounded by how their devices just suddenly 'hang'—become extremely slow or stop working—without realizing that part of the problem is lack of important system updates.

- **Downloading apps from reputable or trusted sources**—This may be subjective, depending on the user. However, certain third-party app stores have proven to be vendors for malicious apps. In general, trusted sources for Android and iPhone users are the Google Play Store and the Apple Store, respectively. Encourage users to practice due diligence by checking reviews or comments on the app page before downloading and avoiding applications that require access to device services for which they have no direct need or use.

⚠

An important dimension to this discussion is the importance of reviewing the scope of app permissions. Apps sometimes require more than basic default permissions. Encourage participants to be vigilant about checking that the apps they install only have access to features they absolutely need. For example, a weather app should not need to access your pictures or contacts. It is important to review what permissions apps are currently allowed to use, as subsequent updates and bugs might have the potential to cause them to leak user data. Participants should take a moment to review a few apps on their devices and determine the types of information they access.

- **Making use of built-in security features**—and, most importantly, knowing how/where to find them. If possible, briefly show the participants with smartphones how to find and navigate their phone settings and enable security features such as passwords, device encryption, disallowing app installation from unrecognized third parties, etc.

- **Limiting location access and Bluetooth**—A good recommendation is to enable location services only while the app that needs it is in use, versus always having it on. This helps to prevent malware-ridden apps that are running in the background from stealing a device's location information. This practice should also extend to ensuring that social media privacy settings are controlled. Some sites broadcast by default things like the user's location to the public.

- **Avoiding connections to unsecured Wi-Fi**—Most people like free things, including free Wi-Fi. Public Wi-Fi hotspots are often not secure and can expose user devices to a multitude of risks. If connecting cannot be avoided, users should especially avoid logging into key accounts or financial services while on public networks. They can also use a VPN, which is a good way to secure data sent and received online (more on VPNs can be found in the chapter on Secure Information Storage).

Top Tip

Demonstrate how easy it is to set up a hot spot and rename it. This is good to do in advance so that it's easy for participants to see if they login to it without knowing whose it is. Setting up this harmless trap drives home the point that anyone can set up a rogue access point through which they can trick unsuspecting users into connecting to what they believe is a legitimate network. This can enable a cyber-criminal to view a user's sensitive information.

A final discussion could address secure messaging apps. This is a good place to talk about apps like Signal and Wire and what makes them more secure than apps like WhatsApp.

Discuss what end-to-end encryption means and some important security features contained in the apps that people sometimes overlook or simply do not know about. For example, WhatsApp now has two-factor authentication. Talk about how chat 'fingerprints' work to verify the people we chat with, options for a passphrase to lock the Wire app, etc.

5

Secure Information Storage

Secure Information Storage

KNOW BEFORE YOU START:

This session requires prior knowledge of how to use a file encryption tool like **Veracrypt.** Learn Veracrypt here: https://securityinabox.org/en/guide/veracrypt/windows.

This session focuses on protecting sensitive files on devices using encryption or 'hiding' technologies. At the beginning, it is important to check whether the use of encryption technology is legal in the users' country.

Dashboard

Proposed Method of Delivery	Discussion, screen showing
Materials You Will Need	Projector, Veracrypt software
Estimated Time Spent on Activity	120 minutes
Useful Analogy/Metaphor	**ENCRYPTION:** is like keeping important information in a locked safe. The safe can only be opened with a key or combination (or a passphrase in the case of computer devices), known only by the owner, to access the contents inside.
Useful Related Resources	How to use Veracrypt: https://securityinabox-.org/en/guide/veracrypt/windows

Key Process Points

- Start the session by launching a discussion about circumstances when participants need to be able to protect or 'hide' sensitive information, including what types of information people may want to keep from prying eyes. Computer login passwords may not offer sufficient protection, as they can be easy to crack.

- Highlight that in this session, the focus will be on preventing unauthorized access to sensitive information through encrypting and hiding important files using free and open-source software. Write down the word 'encryption' on the flipchart, and ask the participants to define it.

- Explain that encryption is a way to make one's files unreadable by anyone without the correct passphrase or permissions. The trainer can opt to briefly talk about the built-in encryption options available on Mac and Windows OS and how these offer good solutions.

- Although there are many options for full or partial disk encryption, including built-in OS options, the trainer may introduce Veracrypt as the tool of choice because of its advanced features. Veracrypt is a free and open-source program that enables the user to create 'encrypted volumes' (virtual safes or containers within which a number of files can be stored securely).

- Depending on how you are distributing the software, show participants how to download it or locate it on a preloaded USB drive (if you are in a position to give out drives already preloaded with the security software to be used throughout the training).

Top Tip

If you encounter a situation where some users cannot install the software (due to admin restrictions) or do not want to for any reason, seat these users next to someone who will install it as they follow your onscreen directions. The trainer should also be sure to share portable versions of apps with the participants in case they cannot or do not want to install.

• You now have the option to demonstrate how to install Veracrypt, create a virtual container, move files into it, etc. Partial disk encryption is often recommended as a first step. This process works well if you move step by step with the participants as they do it on their computers.

• Encourage participants to make use of their new virtual 'safe' to store important files and remember what they named each file. This 'safe' can be backed up like any other file on the computer, and its login details can be stored in a password manager.

• At the end of the session, it is important to point out that the 'safe' or Veracrypt volume should always be 'unmounted' when not in use or before inserting an untrusted USB flash stick or other external storage device.

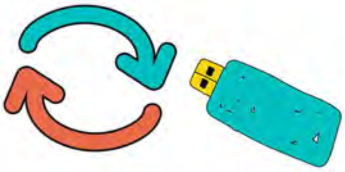
• It is possible to access and store one's Veracrypt volume on a USB flash stick or in the cloud. However, one would need to have a copy of the Veracrypt program in order to open it.

• It is sometimes useful to mask the identity of the Veracrypt volume by changing its physical appearance in the computer's documents. Demonstrate how to do this by changing the default .hc to, for example, .mp3 and show the transformation. This does not affect the contents of the file or how it opens.

6

Secure Information Storage

Backups



Backing up is an overlooked but critical subject to discuss in basic digital security. It refers to having a replicated copy of your important files available in some separate form in case you run into problems with the original device where the files are stored. Having a backup enables the user to keep their important files or data safe from unforeseen events. These could include accidental deletions, computer viruses, hard drive failures, or device theft.

Dashboard

Proposed Method of Delivery	Mostly discussion
Materials You Will Need	Flipchart paper, markers, USB drive, external hard drive, projector
Estimated Time Spent on Activity	60 minutes
Useful Analogy/Metaphor	**BACKUP:** is like making copies of your valuable possessions, such as academic transcripts, and storing them in a safe place separately from your originals. In the event that your original documents are compromised or destroyed, you will still have a copy of your valuables somewhere else. – Sonia Karungi
Useful Related Resources	https://level-up.cc/curriculum/protecting-data/data-backup-basics

Key Process Points

- Start by asking the participants what 'backup' means. It is important to highlight that some are probably already doing it without realizing—e.g., when they save valuable information in different locations, etc.

- Discuss the logical processes to follow when performing a backup. For example, the first important step is to determine what information one wants to back up and make sure to organize it in a manner that makes it easy to locate. This is important because people carry a lot of things that may not be important enough to include in a backup, such as movies or other types of multimedia content.

- Ask the different methods that participants currently use to perform backups, what sorts of information they are backing up, and why. During this discussion, list on the flipchart some of these things and backup methods mentioned. You might hear different solutions, such as backing up on USB drives, in the cloud, on external hard drives, etc.

- Remind participants that a backup refers to a duplicate copy of the original that is kept away from the original. Very often, people store or carry around the original and backup together. It is not a backup when it can potentially be lost or compromised along with the original.

- Discuss the pros and cons of the different methods of backing up. While no one backup method is perfect, some might be better and more effective than others, depending on circumstances. Below are some useful pointers:

Backup Platform	**Pros**	**Cons**
USB Flash Drive	• Easy to carry	• Not the most stable • Easy to carry but easy to lose •Usually has limited space
Cloud Virtual servers accessible from anywhere with an internet connection, e.g., Google Drive, Dropbox	• Convenient in terms of ability to access anywhere with an internet connection	• Data not accessible without an internet connection • Limited storage, or payment necessary for more storage • Data is at the mercy of corporations • Many cloud providers do not consider the security of users' data to be their concern Involves trusting your important data to corporations and servers you may not know well.

Backup Platform	Pros	Cons
CDs/DVDs	• Cheap and fairly easy to get	• Scratch easily and might not work well in the long run • Have very limited storage capabilities • Increasingly, many current or new computers do not have CD-ROM drives
External Hard Drive—preferably portable (obtaining power directly from the computer itself)	• Most recommended	• Depending on use habits, this device is also susceptible to viruses or being corrupted. It is recommended that backup hard drives are used strictly for that purpose and are not shared with many people or used for file transfer across computers. The trainer can refer participants to this re source for more useful information on how to select external hard drives.

How to perform a backup

A lot of people perform backups simply by copying and pasting specific files to new locations. Depending on the nature of the files and how organized they are, this may be working for them. However, this is not ideal, as it is possible to miss some critical system/program files that may not be located in the preferred backup site.

At this point, you can opt to demonstrate where and how to perform a backup in Windows. This is easy to set up in most Windows versions—simply go into the **System and Security** settings in the **Control Panel**. In Windows, the system allows the user to 'set up backup' as well as select the device to which they would like to back up. The user can allow Windows to decide what to back up, or they can choose the files to back up and also set a backup schedule.

Some key points to emphasize:

- The storage method that will work best for a user depends mostly on what they would like to store and how they prefer to access their data. For example, external hard drive storage might be the best and most secure option for businesses that store proprietary or confidential information. If convenience and flexibility are the user's top priorities and security is not a major issue, cloud-based data storage would work well and would allow information to be accessed over an internet connection. This option is especially handy for users who travel often.

- Users need to back up important information regularly. There is no right answer for how frequently backups should be performed, but when it is needed, the backup is only as good as the day it was last done. Anyone who values his or her information will endeavor to back it up as frequently as possible. This includes ensuring that backups are performed whenever changes are made to critical files.

- Testing is an important but often overlooked process in maintaining an effective backup. One may think they have a good backup, but without occasionally checking that it actually works/can be restored, there are chances of disappointment.

- Physically separating the backup from the original. Keeping backup USB drives and hard drives together with the primary device is pointless. Proper backup copies should be stored in fireproof locations, preferably in a building other than where the original is stored.

- It's good to suggest encrypting files before uploading them to cloud storage.

- Recommend the use of a combination of cloud and external hard drive storage. This spreads data across multiple locations to ensure maximum security.

7

Online Safety

Online Safety

Dashboard

Proposed Method of Delivery	Combination of discussion and screen showing
Materials You Will Need	SmartphoaProjector, flipchart stand, butcher paper, markersne, flipchart, and markers
Estimated Time Spent on Activity	90 minutes
Useful Analogy/Metaphor	**TOR:** is like a bad travel agent. You say you want to travel from London to New York, but they send you on a train to Manchester, a bike to Glasgow, a flight to Singapore, a boat to Australia, then finally a hot air balloon to New York. In the same way, Tor bounces you around the internet before arriving at the site you need. – Analogy adapted from Nick Asbury, Sideways Dictionary. **VPN:** is like a tunnel, not an open road. If you're working remotely, it's like having a secure tunnel to your office, carrying the information back and forth, safe from prying eyes. - Analogy adapted from Nick Asbury, Sideways Dictionary. **TAILS:** is like a tent. It can keep you safe from the elements while you are in the forest. But when it's time to leave, you pack up and empty everything and put it away. - Anon
Useful Related Resources	https://level-up.cc/curriculum/safer-browsing

Securing online accounts

- Talk about being prepared to tinker with privacy and security settings and getting comfortable with doing this regularly with all accounts. When we share things online, there is always a risk that we will unwittingly expose some stuff that was not meant to get out or expose it to the wrong people. Users should be encouraged to rethink what they are sharing and to check the security and privacy settings on their social networks. Platforms like Google and Facebook, for example, offer their own free 'privacy check-up' services to help users avoid over-sharing.

- It may be helpful to show an example of settings for an online account such as Facebook and to walk through the different types of security and privacy settings available, where they can be found, and what some recommended settings might be.

- Remind participants that it is important for users to check on and keep track of their online footprint. They should be aware that when a lot of personal data is floating about on the internet, a determined adversary could easily collect enough of it to impersonate the user and possibly gain access to things they shouldn't. A user can receive a notification whenever a new mention of their name appears online by setting up Google Alerts option.

• **Incognito Web Browsing**—Explain that this does not make you anonymous on the web, it only keeps your browsing activity and history from being logged and stored on your computer (but the internet provider will still have access).

• **HTTP vs. HTTPS**—It is important to discuss the differences between these two.

- **HTTP** is generally ok when doing ordinary, non-sensitive internet browsing. Http://— stands for *hyper-text transfer protocol*. However, it is important to note that communication is sent in plain text, which means that those who know how to snoop can see very clearly what we are doing or transacting online.

- When one uses http instead of https, it is like sending a postcard in plain text. Everyone that handles it gets to see/read the message—unlike a letter that is in a sealed envelope.

- Discuss circumstances where one needs to have a secure connection to a service being accessed online: e.g., when doing online banking, using a platform where one must enter personal identification information or credit card details, etc.

- **HTTPS** is the solution to securing communications online between the user and the service provider. The S in https actually stands for secure.

- Note that some websites that have an HTTPS version of their site, but sometimes your browser does not load this version automatically—it does not force or suggest that you use it, which means you might actually not know that a certain website has a secure version.

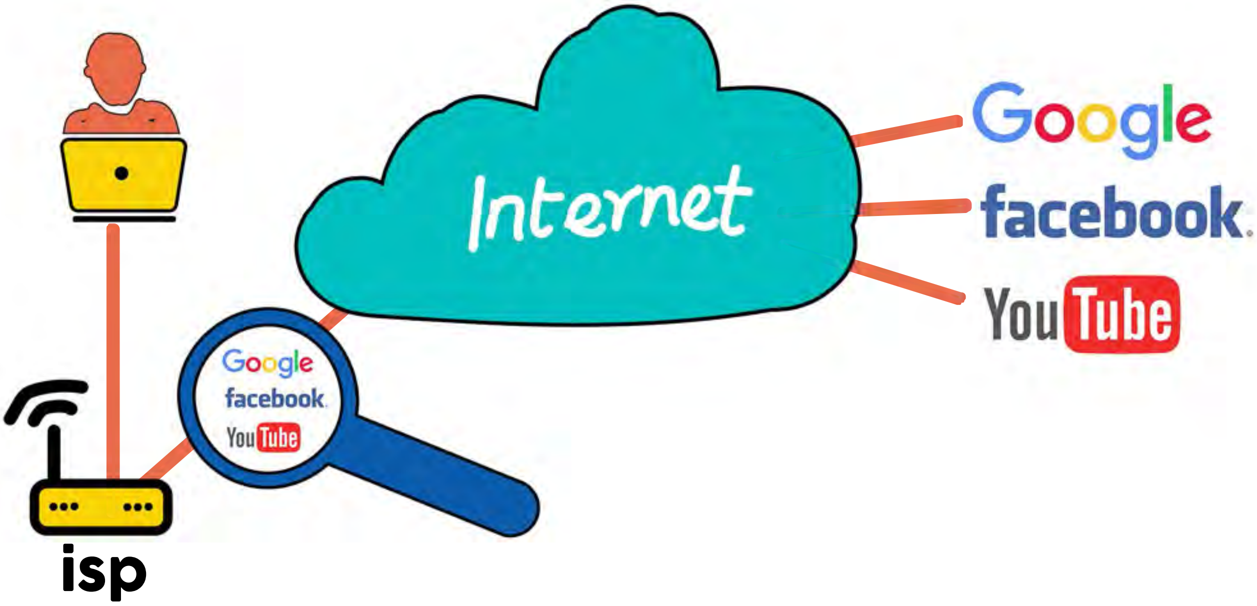
- Installing the browser extension called HTTPS *Everywhere* (available for most common browsers) means that browsers automatically search for the HTTPS version of a site, and use that instead of the HTTP version, even when the user types in http or follows links that omit the HTTPS prefix.

- **Using Virtual Private Networks (VPNs)**

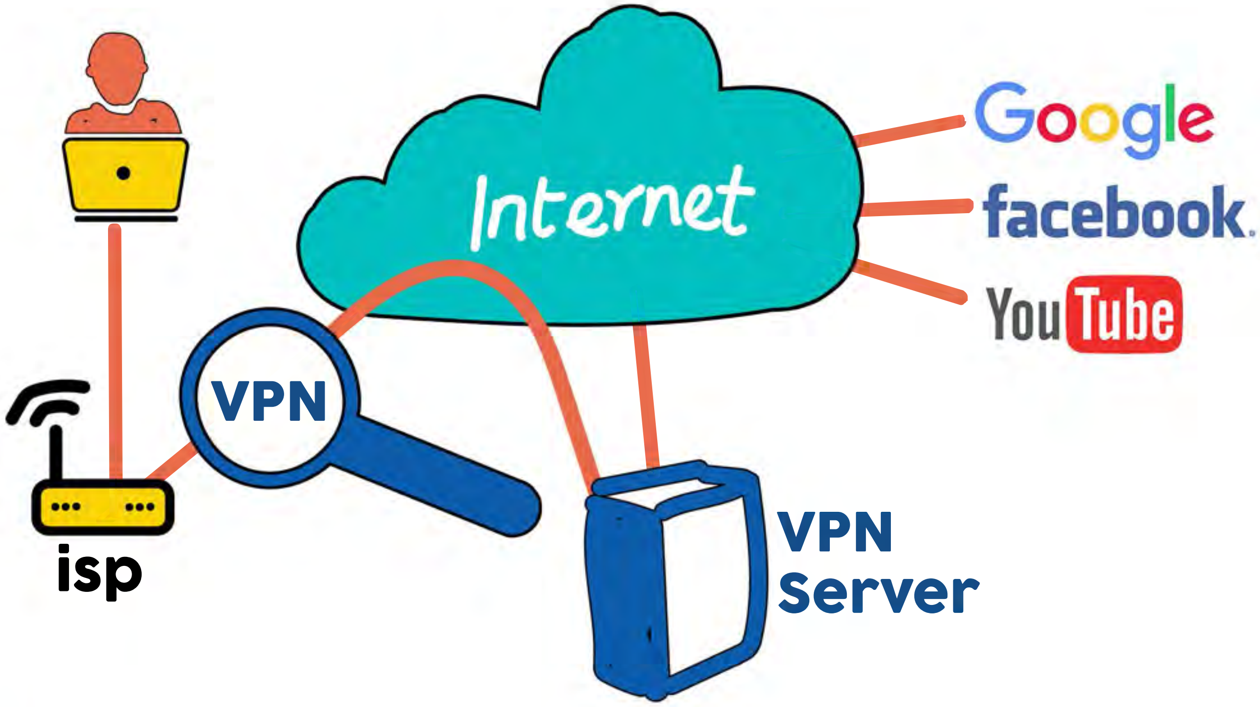
  - Talk about how VPNs are designed to protect the user's privacy by encrypting data, changing their geolocation, and preventing censorship.

  - It may be useful to show diagrams similar to the ones below to show how a VPN works.

Connecting to the Internet without VPN



Connecting to the Internet with VPN



- In the diagrams above, indicate how the ISP is able to see what sites the user visits.

- A service that enables a user to surf the internet from an assumed location conceals their online activities so that they cannot be tracked by the ISP or spies. VPN can sometimes be used to bypass some local internet restrictions—for example, the inability to view certain content from a certain country.

- If demonstrating a VPN on your screen, you can demonstrate how VPNs can mask a user's identity on the internet, by visiting an IP location identifier (such as iplocation.net). First try it with the VPN off, and then with it on. This will show using a VPN can obscure the user's current geographical location.

- Discuss a few available free VPN options that participants can download for themselves. Some free VPNs may not be as effective as the paid versions, and they may also record user data. Therefore, it is good to review a VPN's services and features before downloading.

- **Using the Tor web browser**

- Show participants the Tor browser, its branding, and how it is an actual browser similar to Chrome or Firefox. The only difference is that Tor has advanced security features (e.g., not storing any surfing history, disabling cookies automatically, etc.).

- You can also perform the location test (iplocation.net) and show how Tor masks one's geographical location through a randomly assigned IP address.

- Tor—which stands for 'The Onion Router'—is a secure browser and a free tool that randomly routes web traffic through a maze of servers all over the world, effectively making it impossible for anyone to monitor or trace a user's activity. The fact that traffic is bounced around like this means that websites and other services being accessed online will load slowly, and this worsens when one's connections are forwarded through countries like China and Brazil among others.

- It's important to point out that there are safe and unsafe ways to use Tor. Simply using the browser does not automatically make one anonymous, as there are other factors at play—for example, the types of activity the user engages in online and the extent to which they reveal personally identifiable information in the process. Make sure to tell participants the correct place to download the Tor browser

8

Secure Communication and Email Hygiene

Secure Communication and Email Hygiene

KNOW BEFORE YOU START:

This session requires prior knowledge/experience of setting up **two-factor authentication** and how to use the freemium hosted secure open-source encrypted email service **Tutanota.**
Learn **Tutanota** by getting it here: https://tutanota.com/.
Learn Two-Factor Authentication here: https://sec.eff.org/topics/two-factor-authentication.

Email is one of the most important and frequently used online services. Securing email is important to avoid potentially serious consequences that come with email compromise and the exposure of personal privacy. In this session, we will look at the important features and considerations to take into account when selecting an email service in the context of secure communications and privacy. We will also briefly discuss one example of a free, easy-to-use, and trusted encrypted email service.

Dashboard

Proposed Method of Delivery	Plenary discussion, screen showing
Materials You Will Need	Flipchart paper, markers
Estimated Time Spent on Activity	60 minutes
Useful Analogy/Metaphor	**TWO-FACTOR AUTHENTICATION:** is like having a guard dog by your front door. If someone steals the key to your door, they still have to get past the guard dog, which has to recognize your unique scent, your face, and your voice before you can get in. - *Analogy adapted from Nick Asbury, Sideways Dictionary*
Useful Related Resources	Check out http://prxbx.com/email/—a chart that outlines many popular email services and compares their (security) features.

Key Process Points

• Get started by asking the participants what email services they are currently using and listing these on the flipchart. Ask their reasons for choosing those options and whether are paid services. You may find that the majority use one or more of the following: Gmail, Yahoo!, Hotmail.

• Explain that selecting an email service should be a deliberate and informed decision that considers the user's needs and threat model. Important considerations when selecting a secure and privacy-based email service might include:

Cost

- Many people have always used free email and believe this is the way things should be. It has long been established that when a service is free, you are the product. A lot of free and popular email services make their money through scanning, mining, and even selling the contents of private emails to advertisers. Essentially, this means that they make their money by selling your data and run their mail service by showing you advertisements based on what they know about you.

- Not all free email services thrive on this model. Some, like Riseup, run as charitable services funded through donations.

- The key thing to note here is that if the user opts for a free email service, they should be guided by considering and understanding the provider's revenue stream and business model.

History & Privacy Policy

- Some email services have a known history of handing over customer data to certain agencies or governments. An example of such is Hushmail, which allegedly buckled under the pressure of a court order and submitted plain-text emails of targeted users. It is important to know the extent to which an email service provider can comply with authoritative demands and whether the circumstances in which they do so are fair or justifiable. It also matters whether one's email service is hosted locally or internationally.

- The **privacy policy** of an email service provider should help users decide whether to use it. For example, if a privacy policy states that the email service provider shares user data with third parties, it may not be the best option. Instead, one whose privacy policy states that it does not collect IP addresses, never shares user data, and stores information in an encrypted format might be a safer service to use.

Security Measures

- Ideally, you want to select a service that offers **two-factor authentication** (e.g., through receiving an SMS, an app on your phone, or plugging in a specific USB in order to log in). Two-factor authentication currently makes it significantly more difficult, if not impossible, for emails to be hacked.

Encryption

- Most email services encrypt the connection between the user and the mail server using Secure Sockets Layer/ Transport Layer Security (SSL/TLS). However, not all of them encrypt the messages on the servers themselves. Encryption of email servers (where the mail is stored) protects against two parties: the people who run the server and any third parties that want to gain unauthorized access to the server.

• At this point, you may demo how an encrypted email service works and highlight some of its important key features. Although there are several examples of services that can do this, a simple, recommended option (especially for first-time users of encrypted communications) is **Tutanota,** which is automatically end-to-end encrypted and is open source.

• Demonstrate how a person who receives an encrypted email from the user will be unable to view the subject, attachment, or message unless they produce a password (which must have been agreed upon previously) that will unlock the contents of the message.

• The trainer could also talk about **Mailvelope** as an alternative, depending on users' needs.

Other email options and services to check out (for advanced users):

- **ProtonMail** offers end-to-end encryption so that not even ProtonMail can see your messages. The user's account is anonymous, and the company does not store IP logs. A paid account on this service enables the use of one’s own domain—e.g., myemail.chooseyourdomain.com.

- **Enigmail** with Thunderbird end-to-end encryption is another, slightly more complicated, option.

9

Phishing: Understanding and Preventing Attacks

Phishing: Understanding and Preventing Attacks

The key objective of the session is to increase users' vigilance when reading messages and provide them with protective steps they can realistically take to avoid falling victim to potential phishing attacks. Concentrating on dangerous or safe actions, or scaring your audience with convincing phishing emails, is far less effective than simply providing solutions.

Dashboard

Proposed Method of Delivery	Plenary discussion
Materials You Will Need	Flipchart paper, markers, screen projection
Estimated Time Spent on Activity	60 minutes
Useful Analogy/Metaphor	**PHISHING:** is like when someone hustles you on the street. Someone walks up to you at random and starts a conversation. They seem to have a plausible story and might even make you a tantalizing offer, yet they want something from you. They do something alarming or interesting...then, while you're distracted, they pick your pocket. – Analogy adapted from Ean Moody, Sideways Dictionary
Useful Related Resources	Google Jigsaw's Phishing Quiz https://phishingquiz.withgoogle.com

Key Process Points

- Write the word 'phishing' on the flipchart. Ask participants to define it.

- **Phishing** is a type of spam (unsolicited junk mail) that attempts to get information by making you take a certain course of action. For example, a phishing email could try to trick you into revealing sensitive personal information (e.g., account passwords, credit card information) or do something more dangerous, like downloading and running a malicious program that will secretly steal information from you or allow attackers to remotely control your device or install ransomware.

- Although phishing attacks happen in different ways, like through phone calls or text messages, they most commonly target email accounts because they are very rich data mines. This is because people use their primary email addresses for a lot of things, such as connecting to social media or bank accounts. Most importantly, email accounts can be used to reset passwords for many services on the internet. This means that if your email is compromised, everything else about your digital identity is put at great risk.

- In most cases, phishing emails are crafted to resemble correspondence from trustworthy sources (Google, a legal entity, a bank, etc.) and often dupe users into clicking on malicious embedded links. More sophisticated phishing emails execute hidden code if the mail is simply opened on the target's computer. The key is to get users to understand the risks of opening email attachments or clicking on links from unfamiliar sources, as these can lead to malware or virus infections.

- It may be useful to show locally relevant examples of several phishing emails and have a participatory activity where participants try to pinpoint the telltale signs of phishing emails. Alternatively, you can show a phishing test such as this one: **https://phishingquiz.withgoogle.com/**. The more people are exposed to examples of what phishing attacks look like, the better able they will be to recognize them in their regular experience.

Common phishing tactics to discuss

- A link embedded in an email that redirects the user to an unsecure website that requests sensitive information.

- Unwittingly installing a Trojan—for example, by downloading a malicious email attachment that enables an intruder to exploit system loopholes and obtain sensitive information.

- Spoofing the sender's address (for example, pretending to be from your bank) in an email to appear as a reputable source and request sensitive information.

- Entering a username and password into a website that is made to look like the legitimate thing.

- Attempting to obtain sensitive information over the phone through the social engineering technique of impersonating a known vendor or IT department.

- **Spear phishing** is a targeted phishing attack where the attack is tailored to the victim and may use familiar language and references, so the message looks more convincing than mass phishing, and is more likely to be opened.

Some best practices to avoid falling victim to phishing attacks

- Never enter your email password on websites that are not your email provider or client

- Check the URL. It is often possible to see the true destination of a URL or link by dragging your cursor and hovering over it without clicking. Malicious links will likely not match up with the email or link description. Instead of clicking on links, always type the address directly into the address bar. It is important to note that a clever tactic used by phishers is to disguise some links with lookalike characters, or use replica domain names that look very similar to the legitimate sites—perhaps just one letter off and not easy to detect.

- Check shortened URLs (like bit.ly) using a tool such as **https://www.checkshorturl.com/** to see their true destination.

- Think twice when an email asks you to click on something or download an attachment. It is generally a good practice to avoid downloading attachments, especially if they are unexpected or come from unknown persons. Attachments commonly accompany phishing emails and can carry malware or viruses. Upload and open untrusted documents only in Google Docs; this is a 'sandboxed' environment that enforces separation between the documents you open and the device you use. Doing this converts the document into an image or HTML, which in turn prevents it from installing malware onto your device.

- Verify with colleagues (using a different channel if possible) that they actually sent you unexpected communication with links to click/download. Learn to read emails carefully, looking at everything and being more discerning. Some phishing emails JDLR (just don't look right).

- Enable two-factor authentication on accounts that have this capability.

Two-factor authentication

- **Two-factor authentication** makes online services more secure by accessing them with something you know (e.g., your password/ passphrase) and something you have (physical access to your phone or Yubikey). With 2FA, each log requires an extra step after entering your password—this often entails entering a six-digit code that is displayed only on a device within your control. This code can be received via SMS from the service itself (as is the case with Gmail) or be uniquely generated by an app on your phone (such as Google Authenticator). In this way, if someone somehow gets your password, they would still need to have physical control over your second factor, e.g., your phone, as well.

- Keep all systems current with the latest security patches and updates. Some phishing attacks use malware that depends on existing software bugs. Keeping updates current limits malware risks that can be used for phishing attacks.

- Things like bad grammar, misspellings, emails addressed to many or the user in BCC, and claims of having won a big award—these are often popular characteristics of phishing emails.

- Avoiding over-sharing personal information on social networking platforms, as this can potentially be used for social engineering purposes.

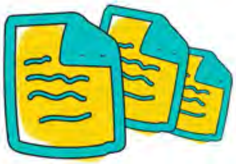
- Avoid using important email addresses to access/register for too many services online. The more emails are exposed, the higher the chances they will be targeted with spam.

- Use password managers with an autofill feature. Password managers intelligently keep track of the correct sites to which login credentials and passwords belong. Using a password autofill feature decreases the chance that you will enter passwords into fake login pages.

10

Useful Resources for Trainers

Useful Resources for Trainers



Awareness is critical for a digital security trainer. Staying on top on new, relevant, and pertinent developments in the sector is key. Included below are lists of resources, many of which are updated in near-real time to stay current. They will help you on this journey.

Please note: Not all resources listed here are updated regularly. It is good practice to always check when they were last updated before considering/making use of information as factual. The websites referenced here are also generally good resources to watch for new information related to digital security developments.

Name of Resource	Developed By	Brief Description
Digital Security Resources Index	@BeckLindsay and community owned	An extensive database that contains a multitude of important/useful digisec resources and some in different languages. Lists resources referenced in this guide and more.
Guides & Training	Freedom of the Press Foundation	Simplified guides and security tools/concepts useful for media practitioners and others.
Sideways Dictionary	Jigsaw Washington Post	Online tool with helpful analogies/examples/metaphors to simplify and explain otherwise complex technical concepts.

Name of Resource	Developed By	Brief Description
Level-Up	Community owned, network maintained	An open resource for the global training community. Covers key topics typically explored by trainers.
Security in a Box	Tactical Technology Collective & Frontline Defenders	Useful guide for both trainers and end users; incorporates detailed software guides, security strategies, hands-on guides, and how-tos for key digital security tools. Generally updated regularly.
Security Education Companion	Electronic Frontier Foundation	An excellent guide for first-time trainers and people who teach digital security to others. It has modularized lessons on selected digital security topics, not in any particular order.
Surveillance Self-Defense	Electronic Frontier Foundation	Tailored for safer online communication—unpacks online surveillance and includes useful guides for privacy and security tools.
Umbrella	Security First	App for context-based physical and digital security advice in a mobile handbook.

Here are some easy ways to stay updated more quickly (sometimes before resources are updated):

1. Subscribe to mailing lists where other digital security trainers around the world congregate—for example, the OrgSec mailing list, LevelUp mailing list, etc.

2. Read. A lot. Follow authoritative voices of individual technologists and organizations in various online spaces for guidance on things to read to help you stay updated. By following some or many of these, you will discover other notable and knowledgeable voices to follow:

- Electronic Frontier Foundation—@EFF
- Tactical Technology Collective—@info_Activism (credited with co-author ing the popular Security-in-a-Box manual and 'bible' for security trainers)
- Frontline Defenders—@FrontLineHRD (also credited with co-authoring the Security-in-a-Box manual)
- The Engine Room—@EngnRoom
- Internews—@Internews
- Access Now—@accessnow (organizers of RightsCon and credited for their Digital Security Helpline, which provides rapid response assistance to HRDs)
- Security First—@_SecurityFirst (credited for creating the Umbrella App)
- Security Without Borders—@swborders
- Privacy International—@privacyint
- Internet Freedom Festival—@InternetFF
- Open Technology Fund—@OpenTechFund
- Mozilla—@mozilla
- The Tor Project—@torproject
- Citizen Lab—@citizenlab
- Article 19—@article19org
- Ushahidi—@ushahidi
- Edward Snowden—@Snowden
- Jillian York—@jilliancyork
- Martin Shelton—@mshelton (writes largely on Medium on digital security and technology developments, mostly targeted at journalists. Credited for keeping an updated blog on the same.)
- Matt Mitchell—@geminiimatt

1. Useful hashtags to follow:
#OrgSec
#ResponsibleData
#InternetFF

Emergency Digital Security Support

Sometimes, trainers encounter threats or work with individuals who require extraordinary support. Below is information about organizations that offer various forms of emergency digital security support ranging from rapid response grants to remote technical support.

⚠ **Please note:** Always consult relevant websites to see if some services are still offered.

WHO	WHAT	HOW
Frontline Defenders	Protection grants to pay for practical security needs of human rights defenders and urgent actions	Emergency 24-hour phone line for human rights defenders operating in Arabic, English, French, Russian, and Spanish
Access Now	24/7 assistance for a range of digital security challenges or incidents experienced by at-risk users. HRDs under attack can access rapid response emergency assistance.	Digital Security Helpline

Appendices

Needs Assessment Questionnaire

Check for a more structured & simplified online version here: https://goo.glZ-forms/XZ9MG7S7UOxKR8Be2

This questionnaire can and should be modified according to the trainer's needs. In some contexts, it may be more important to understand role/job function than to collect demographic information. If demographic information is needed for reporting or some other purpose, there may be value in asking what pronouns people use instead.

1. Sex:
2. Age:
3. Work profile (e.g., blogger, journalist, etc.):
4. How many years have you used computers?
5. What is your computer's operating system?
6. List the computer programs you use for your work:
7. Who solves problems with your computer? Describe:
8. List the services you use on the internet. Describe what you use them for:
9. Who do you share computer(s) with?
10. Does your computer have antivirus protection? If yes, which one?
11. Do you make backups of your information? How
12. What are the common ways in which you share/receive information from your colleagues and/or sources? What steps do you take to make this information secure?
13. Have any of your or your organization's computers or other equipment ever been stolen/confiscated? Did you lose information? Describe:
14. What phone model are you using? Do you use it for your work?
15. Have you ever participated in digital security training? If yes, please briefly describe what you learned:
16. Have you experienced some form of cyber bullying? Please describe briefly:
17. What do you perceive to be digital threats that can potentially affect your current work currently?
18. What would you like to learn? Specifically, what topics would you like to see covered during the digital security workshop?

Basic Training Agenda

Please note: This agenda can be adjusted time-wise to cover three days, depending on the participants' learning pace and the time available. This can also easily be a three-day agenda because sometimes participants will have over- or underestimated their tech capabilities. Leaving room for flexibility enables the trainer to cover all the basics.

DAY 1		
TIME	**ACTIVITY / DESCRIPTION**	**FACILITATOR**
0900–0930	Introductions; Needs assessment	
0930–1030	Risk Assessment	
1030–1100	**BREAK**	
1100–1200	Device Hygiene and Account Security	
1200–1300	Device Hygiene and Account Security: Hands on: Password Manager	
1300–1400	**LUNCH**	
1400–1500	Mobile Security	
1500–1600	Wrap up of Day 1	

DAY 2		
TIME	ACTIVITY / DESCRIPTION	FACILITATOR
0900–0930	Recap of Day 1	
0930–1030	Secure Information Storage	
1030–1100	BREAK	
1100–1300	Backups	
1300–1400	LUNCH	
1400–1500	Online Safety	
1500–1600	Secure Communications	

DAY 3		
TIME	ACTIVITY / DESCRIPTION	FACILITATOR
0900–0930	Recap of Day 2	
0930–1030	Secure Information Storage	
1030–1100	BREAK	
1100–1300	Use for anything you didn't get to, or follow-ups from Days 1 and 2	
1300–1400	LUNCH	
1400–1600	Use for anything you didn't get to, or follow-ups from Days 1 and 2	

DIGITAL SAFETY TRAINER'S ASSISTANT

2019

Internews