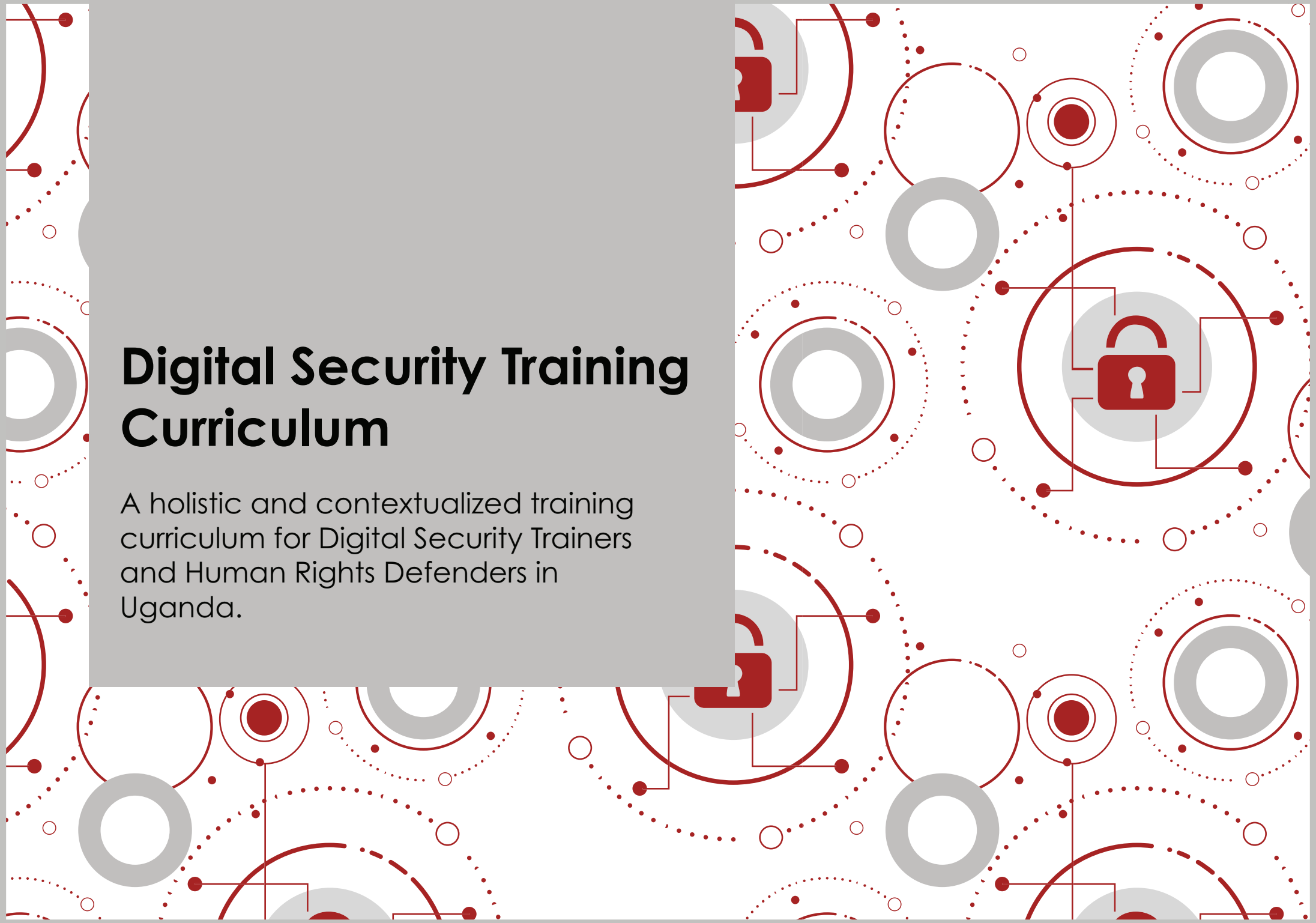
Digital Security Training Curriculum

A holistic and contextualized training curriculum for Digital Security Trainers and Human Rights Defenders in Uganda.



Acknowledgments

The design of this Digital Security Training Curriculum to provide a comprehensive and holistic reference for Human Rights Defenders and other Digital Security trainers in Uganda was supported by a diverse network of individuals and organizations. These included the **DHRLab Project**.
We thank each of them for their valuable contribution to the development process of this curriculum, as well as for their ongoing efforts to increasing digital security awareness in Uganda.

The content was shaped and greatly enriched by the following people who contributed their knowledge, insights and first-hand experience throughout the consultative process. In particular, we would like to thank **Andrew Gole**, (Encrypt Uganda) **Lindsey Kukunda**, (Her Empire) **Kelly Daniel Kigonya,** (IFreedom) **Brian Byaruhanga,** (DPI), **Joseph Kasozi** (HRCU), **Fred Drapari** (DPI) **Sandra Kwikiriza** (Her Internet) **Kettie Kahume** (Her Internet) **Innocent Adriko** (DLI), **Emma Magambo** (HRNJ), **Ruth Apolot, Sonia Karungi, Ruth Atim, Shane Senyonga** (Cloud & Pillar), **Ben Kerry Mawejje, David Idoru** (NGO Forum), and **Eddie Muhumuza** (Her Internet).

Credits

DESIGN WITHOUT BORDERS Africa.
digital HUMAN RIGHTS lab
dpi DEFENDERS PROTECTION INITIATIVE
german cooperation DEUTSCHE ZUSAMMENARBEIT
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

How to Use this Curriculum

This Curriculum uses the **Activity-Discussion-Inputs-Deepening-Synthesis approach**, also referred to as the **ADIDS approach** to learning. All the content to guide trainers using this curriculum has been organised according to this approach.
This is an adult learning approach that has been used effectively in advocacy and skills training on human rights issues. It has been found to be useful in helping participants with minimal technical knowledge better understand concepts as complex as digital security and Online safety. For trainers, it can also provide a useful framework when creating lesson plans.

The operating principle behind the ADIDS approach is that adult learners benefit most from information presented in stages, and in a variety of formats – i.e., group activities, case studies, slide and audiovisual presentations, facilitated discussions, group work, hands-on practice, and reflection.
This approach creates a comprehensive learning environment by taking into consideration the needs of kinesthetic learners (who need to do something physically to understand), as well as visual learners (who rely on pictures, diagrams and video) and auditory learners (who learn through hearing material such as lectures).

"Adults learn best when they take responsibility for their own learning" - Malcolm S. Knowles (The Modern Practice of Adult Education: From Pedagogy to Andragogy) Andragogy, which comes from the Greek word 'andr' (relating to "man" or an adult) and 'gogy' meaning "led". Andragogy, as a learning model, then, means adult-led, adult-focused, and adult-driven learning.

"Adults learn best when they take responsibility for their own learning"- Malcolm .S. Knowles

These five statements summarize Knowles' theory:

1. Adults need to understand and accept the reason for learning a specific skill.
2. Experience (including error) provides the basis for learning activities.
3. Adults need to be involved in both the planning and evaluation of their learning.
4. Adult learning is problem-centered rather than content-oriented.
5. Most adults are interested in learning what has immediate relevance to their professional and social lives.

The ADIDS Approach

Activity (easing into the topic): Each module begins with an Activity that illustrates the material that is to follow. These act as "icebreakers" for new participants and will ease them into thinking about a topic that may be new to them.

Discussion (providing context): Discussion sessions follow each of the Activity sessions. These sessions are designed to engage participants in a conversation about the topic (and the preceding session).

Input (interacting): After the two previous steps (Activity and Discussion) the participants will be guided through an effective Input session in which participants are engaged with a range of materials, including case studies, that will facilitate a give-and-take in knowledge sharing between the trainer and the participants.

Deepening (hands-on activities): This session includes the application of skills, software and learning to use them. This is possibly the most important session in the training, as this is where participants learn new skills by doing them. It follows the previous three segments so that the participants understand why they are learning a particular skill.

Synthesis (reflection): Lessons benefit from practice and review, and learning is reinforced by reflecting on the knowledge acquired. In this session the knowledge and skills that have just been addressed are summarized, with the participants encouraged to ask questions and seek clarification.

Each of the curriculum modules herein is designed around a topic-based training session, which is in turn composed of a number of distinct parts - this resource explains the basic structure of a session module, and the logic behind this structure.
This curriculum has been developed following the Activity-Discussion-Inputs-Deepening-Synthesis, or ADIDS approach, to adult learning and has organized its training sessions according to this design. ADIDS has been used effectively in advocacy and skills training on human rights issues, and we have found it to be useful in helping participants with minimal technical knowledge better understand the complexities of digital security and Online safety. For trainers, it can also provide a useful framework when creating lesson plans.

Each topic is structured using the ADIDS module approach that addresses relevant tools, practices and approaches to the overarching digital security topic.

DISCLAIMER:
Each ADIDS element in this curriculum can be used as is or adopted to be delivered in a way that supports the context of the targeted participants.

The trainer is free to customize their agenda to suit the specific needs of the training and the participants.

4. Additional resources.
https://www.umsl.edu/~henschkej/articles/a_The_%20Modern_Practice_of_Adult_Education.pdf
https://www.level-up.cc/leading-trainings/training-curriculum/email-security/full

Methodology

The five symbols below are to be used as guides throughout this curriculum to indicate to the Digital Security Trainer each time there is need to engage participants in either of the five core ADIDS elements.

Activity (easing into the topic): Each module begins with an Activity that illustrates the material that is to follow. These act as "icebreakers" for new participants and will ease them into thinking about a topic that may be new to them.

Discussion (providing context): Discussion sessions follow each of the Activity sessions. These sessions are designed to engage participants in a conversation about the topic (and the preceding session).

Input (interacting): After the two previous steps (Activity and Discussion) the participants will be guided through an effective Input session in which participants are engaged with a range of materials, including case studies, that will facilitate a give-and-take in knowledge sharing between the trainer and the participants.

Deepening (hands-on activities): This session includes the application of skills, software and learning to use them. This is possibly the most important session in the training, as this is where participants learn new skills by doing them. It follows the previous three segments so that the participants understand why they are learning a particular skill.

Synthesis (reflection): Lessons benefit from practice and review, and learning is reinforced by reflecting on the knowledge acquired. In this session the knowledge and skills that have just been addressed are summarized, with the participants encouraged to ask questions and seek clarification.

Table of Contents

1 Digital security

Introduction

Digital Security is the protection of one's digital personality, as it represents the physical identity on the network you are operating on or the internet service in use. Digital Security includes the tools which one uses to secure his/her identity, assets, and technology in the Online and mobile world. Simply put, let's think of digital personality as the human body. We have a duty to protect our body from harm which we could term as 'digital security'. There are a number of methods (tools) that we use to protect our bodies. We eat and live healthily and put ourselves out of harm's way. The same applies to our digital personality.

Objectives

During this module, the participants will gain an understanding of the following key topics:

- What is Digital security
- Common myths and misconceptions
- Human behavioral limitations
- Psychosocial well-being

Tools required

Trainer

These tools will be necessary for the trainer to prepare before conducting the training.

Devices

- Laptop
- Smartphone

Resources

- Flip charts
- Markers
- Blue tack
- Pens
- Note books
- Internet
- Masking tape
- Illustrations

Trainee

These tools will be necessary for the trainee to have during the training.

Devices

- Laptop
- Smartphone

Resources

Prerequisite knowledge

Prior to participating in this training, the participants should at least have an understanding of:

- Basic computer knowledge (how to use a laptop & smartphone)
- How to use the Internet e.g. using browsers, accessing websites and social media platforms.

Definitions

Digital ecosystem: A digital ecosystem is the relationship between a person's Online/ offline activities, and information technology resources that they interact with.

Digital Identity: A digital identity is a representation of a person's social identity Online or offline. In short, it is information about a person stored on a computer.

Digital Assets: A digital asset is a digital entity owned by an individual or company. Examples include digital photos, videos, and songs. These assets are not tangible, meaning they have no physical presence. Instead, they are files that reside on storage device, such as a local computer or a cloud-based storage network.

Digital technology: Digital technology is any hardware or software that generates, stores and process data or content. Hardware like computers, mobile phones; and software like Microsoft Office, Social media networks like Facebook etc.

Common myths and misconceptions

People nowadays do not pay much attention when they surf the web at home or at work. There are new data breaches and exploits on a daily basis, and not taking any precautions may result in catastrophic consequences.

Even the biggest corporations are paying millions of dollars so they can improve their cybersecurity and remain safe.
However, if you still believe in some of the cybersecurity myths you may put your own devices or even your entire organization at risk.

Here are the common myths and misconceptions about Digital Security:

Your organization is too small to be a victim of a cyber attack
This is one of the most prevalent digital security myths that need to be debunked. Most Small organizations think that they are safe from any kind of digital threats because they're 'off the radar'. That's certainly not the case. Hackers don't care about the scale of your organization to target it.
Of course, there are some who'd prefer to hack the United Nations, but most hackers would settle for smaller organizations. Always be cautious. Doesn't matter if you have10 employees or 10,000, your organization is at risk of a cyber attack.

Anti-virus/Anti-malware is good enough
No anti-virus or anti-malware can keep your system safe from all types of digital attacks. These softwares rely on a large database that has information about all the malware/viruses out there. However, if the hackers use a new kind of malware to infect your network or computer then there's a high chance that these anti-virus software won't be able to detect those. So, don't solely rely on such software. They are only the first line of defense for your system and you should always have multiple defending options available.

Only the IT department is responsible for digital security
It is not wrong to say that the IT department is responsible to implement new processes and policies to keep digital security in a top-notch state. However, they don't have a magic wand to protect all of the computers in the network. In reality, each employee should be extremely careful when receiving and opening different e-mail messages from colleagues or third parties. It is dangerous since the infection can spread across all of the departments within the organization and this, for example, may cause a further data breach.

Our passwords are strong
Most people think that their regular passwords are strong enough to stand against multiple break-in attempts. However, that's a wrong mentality right there. No password can be 100% secure, no matter how many numbers and special characters you use in your passwords, there's always a possibility that they can be cracked or leaked in some way. This is why it's very important to keep changing your passwords on a regular basis. It could be weekly, bi-weekly, or monthly, but you need

to regularly change your passwords, and have your employees change theirs.

Threats are spread only through the Internet
Some users may think that disconnecting from the internet will prevent the threats from spreading around the network and they are completely wrong. An employee may plug in an infected flash drive and all of the computers in the network can get infected, resulting in the loss of valuable company information.

You could also have your information device stolen at a store. Threats are not only Online, but in our daily life and we need to be very careful and take care of our personal information.

Threats are carried out by external parties
Most people will tell you that cybersecurity threats come from the outside. Some hackers sitting in a dark basement trying to hack into your organization's network. In reality, research shows that nearly 75% of data breaches are a result of someone on the inside.

A disgruntled employee, an ex-employee with a grudge, or just an ignorant user on your network can grant access to your entire organization's data resulting in a massive data breach. It's always a good idea to train your employees and teach them about digital security threats.

I don't have anything worth protecting
You might think your data isn't worth anything. You might think because you're broke, no one cares about your data. You might also think that since you have nothing to hide, there's no point in protecting your identity or information. This so called 'petty data' could be compiled and or analyzed to build a bigger profile to steal ones identity.
In other circumstances ones device could be used for malicious purposes.

Why use paid applications when there are free ones available
There is nothing that is wholly free of charge.
When using free applications, you don't have control and or accountability of the use of your personal data.

One's personal data could very easily be distributed to third parties and used maliciously.
Quite a number of developers embed malware in free application.

It should be noted that not all free applications are dangerous i.e. 'Signal' is notably a secure messaging application. However quite a number of unscrupulous developers target their victims through free applications.

Activity

Threat Model activity.
Core objectives of conducting this activity:

- To understand the threats and vulnerabilities a person is exposed to when using ICT for work and leisure activities.
- The trainer invites the participants to take part in an activity to detail the threats and vulnerabilities they are exposed to in their work as HRDs while using digital tools and devices.

Conducting the Activity

1.The trainer starts off by unexpectedly confiscating participants' devices e.g. smartphones and laptops, and attempts to gain access to their contents.

2. The participants document the threats and vulnerabilities they are exposed to in line with their work on a flip chart or using sticky notes.

3. The trainer helps the participants understand the relationship between the identified threats and vulnerabilities and their digital devices and explains how they can utilize digital security tools and practices to mitigate these threats or vulnerabilities.

Discussion

Following the activity, the trainer can now further lead the participants through a detailed discussion on issues that arose from the activity. Further discussion can be done to include the following, among other topics:

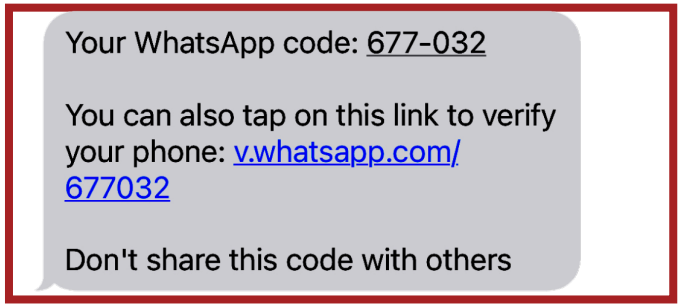
- Share real life scenarios of digital safety threats and solutions to said threats.
- Give relevant examples to demonstrate the relationship between threats/vulnerabilities and the digital devices people use. Then suggest or request feedback from participants on possible digital security solutions.
- Share familiar case examples involving digital security violations.

Input 1

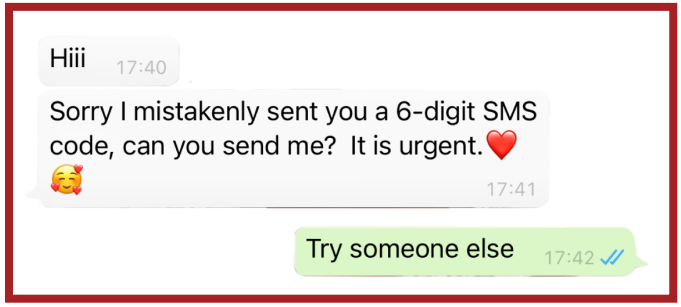
Occurrence: **Account Hijacking**
Year: **2021**
Device: **Mobile Phone**

Learning Outcomes

It is important to properly read and understand the terms and conditions of security related message before one responds to them. Use example below:



Whatsapp Code SMS _ Activation SMS



Whatsapp Hijack text message.

Unscrupulous individual takes control of Whatsapp account using another device through the following steps:
01 - Register for Whatsapp using your phone number.
02 - Whatsapp sends verification SMS code to your phone number.
03 - Intended victim receives Whatsapp message asking them to forward the SMS code.

Once the intended victim sends the Code, their account is Hijacked.

Input 2

Occurrence: **Blackmail**
Year: **2021**
Device: **Computer**

Learning Outcomes

It is important to include a confidentiality clause in the employee contract and/ or Human Resource manual in order to protects company privileged information (including digital assets). Use example two below:

Example 2
A disgruntled employee of a client organization threatened to expose privileged case information of the said organization.

Input 3

Occurrence: **Loss of Data**
Year: **2020**
Device: **Flash disk**

Learning Outcomes

One should endeavour to go the extra step of encrypting data on storage devices. Use example 3 below:

Example 3
The flash drive, which contained confidential data was misplaced and whoever found its used the data without the owners permission.

Input 4

Occurrence: **Police arrest**
Year: **2020**
Device: **Mobile Phone**

Learning Outcomes

One should always have a password on their device to protect their data.
Its also important for all individuals to know and effect their right to privacy. Use example 4 below.

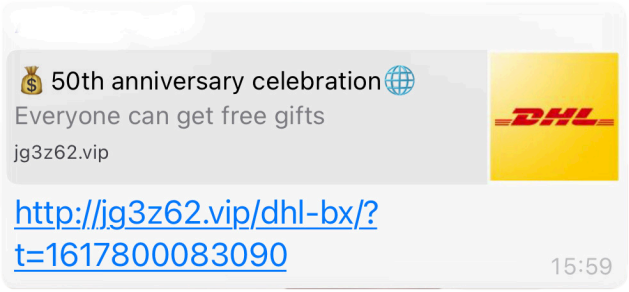
Example 4
Once an individual is arrested, the police confiscates their belongings including their mobile phone. A situation arises when the police wants to access the content on the mobile phone but the individual refuses to unlock the phone because the police does not have a court order to that effect.

Input 5

Occurrence: **Data Phishing**
Year: **2020**
Device: **Computer/ Mobile device**

Learning Outcomes

One should endeavor to go the extra mile to study and verify that the URL belongs to the company in question e.g. in the example above, DHL will use its official website if thy were giving away gifts. Use example 5 below.



Phishing Link in Whatsapp text message

Example 5
An individual experiences data phishing when they receive a Whatsapp message prompting them to click a link to get free gifts from a renowned company.

TIPS

- Keep your software up to date. Turn on automatic system updates for your device, make sure your desktop web browser uses automatic security updates, and keep your web browser plugins updated.
- Use anti-virus protection & firewall. These software block malware and other malicious viruses from entering your device and compromising your data.
- Use Strong Passwords & Use a Password Management Tool. Opt for something that is not complicated and is easy to remember. It should have at least 8 characters and a max. Length of 64 characters. Don't use the same password twice.
- Protect your sensitive Personal Identifiable Information, that can be used by a cybercriminal to identify or locate an individual. This includes name, address, phone numbers, date of birth, IP address, or any other physical or digital identity data.
- Backup your data regularly. A recommended rule is the 3-2-1 backup, where you keep 3 copies of your data on 2 different types of media (local and external hard drive) and one copy in an off-site location (cloud storage).
- One should consider using two factor verification in their security protocol.

FACTS

There is a hacker attack every **39** seconds

The global average cost of a data breach is **$3.9** million across small & medium businesses.

Since the Covid-19 outbreak, there has been a **300%** increase in reported cybercrimes worldwide.

95% of cybersecurity breaches are due to human error.

Most companies take up to **6** months to detect a data breach

Deepening

Exercise 2 (30 minutes)

This exercise builds on the previous exercise. The trainer guides the participants through the following steps to deepen their understanding further:

A. Participants install and use Find My Phone to remotely locate and/or wipe their device to protect their data from being accessed by a third party.

B. Participants install Google Drive, Dropbox and other back-up options that automatically upload and store their data Online/on cloud.

Synthesis

1. Assign participants topics for engagement in a mock training session per participant.

2. Test participants' knowledge verbally to ascertain effectiveness of the training.

3. Engage participants in a feedback session.

4. Recreate a real life scenario of a digital security threat and have participants solve it.

5. Use games and other forms of entertainment (Online or offline) to refresh participants' knowledge of lessons learned.

2 Digital Literacy

Introduction

Digital literacy refers to having the skills one needs to live, learn, and work in a society where communication and access to information is increasingly done through digital technologies like internet platforms, social media, and mobile devices.

Objectives

During this module, the participants will gain an understanding of the following key topics:

- How the internet works
- Digital citizenship and digital rights
- Uganda legal framework
- IoT and how it works
- Understanding user data
- Empathy
- Practicing digital literacy
- Acknowledging the digital divide
- Practicing digital wellness
- Securing digital devices
- Relationship between Human Rights and Digital Rights
- Data privacy, right to information, freedom of expression.

Tools required

Trainer

These tools will be necessary for the trainer to prepare before conducting the training.

Devices

- Laptop
- Smartphone
- Projector
- Internet

Resources

- Flip charts
- Markers
- Tack
- Pens
- Note books
- Internet
- Masking tape
- Audio and visual

Trainee

These tools will be necessary for the trainee to have during the training.

Devices

- Laptop
- Smartphone
- Internet

Resources

Prerequisite knowledge

Prior to participating in this training, the participants should at least have an understanding of:

- Basic computer knowledge (how to use a laptop & smartphone)
- How to use the Internet e.g. using browsers, accessing websites and social media platforms.

Definitions

DNS (The Domain Name System) - A hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

IP Address - A unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

HTTP (Hyper Transfer Text Protocol) - A protocol which allows the fetching of resources, such as HTML documents.

HTTPS (Hypertext transfer protocol secure) - The secure version of HTTP, which is the primary protocol used to send data between a web browser and a website.

Definitions contd.:

Data - Units of information/a set of values -, often numeric, collected to represent a given situation.

Digital Wellness - Digital wellness is a way of life, while using technology, that promotes optimal health and well-being in which body, mind, and spirit are integrated by the individual to live more fully within the human, natural, and digital communities.

Digital divide - Digital divide refers to the gap between demographics and regions that have access to modern information and communications technology, and those that don't or have restricted access.

Digital empathy - The cognitive and emotional ability to be reflective and socially responsible while strategically using digital media" **(Friesem, 2015)**

Digital Footprints/Shadows: refers to one's unique set of traceable digital activities, actions, contributions and communications manifested on the Internet or digital devices. E.g. Online purchases, social media posts, search engine searches etc.

Psychosocial well-being: refers to inter- and intra-individual levels of positive functioning that can include one's relatedness with others and self-referent attitudes that include one's sense of mastery and personal growth.

Activity

Evolution of the internet:

Participants document when and what/how they were introduced to the internet using post it notes to show what applications or tools they were introduced to on the internet.

Discussion

The Trainer and participants at this point can have an informal engagement to discuss the following:

- What the Internet looked like upon arrival
- When they joined it
- What they used it for
- How it has evolved over the years
- How has the internet affected their lifestyle e.g. opportunities it has created and challenges it has created.

How the internet works

The **Internet** is the global interconnection of computers that form a network through which they communicate using a standardized protocol.
Information on the Internet moves from one computer to another in the form of bits, through mediums such as cables that include ethernet cables, fiber optic cables, and wireless mediums.

The transfer of data through the above physical medium is aided by protocols and the **Domain Naming System (DNS)**.
Because the Internet is a global network of computers each computer connected to the Internet must have a unique address. Internet addresses are in the form of four series of decimal numbers from 0 - 255 e.g. **789.554.321.089**. This address is known as an IP address (Internet Protocol address).

When your computer is connected to the Internet and has a unique address, what enables it to 'talk' to other computers connected to the Internet are known as protocols. A protocol is a set of rules specifying how computers should communicate with each other over a network.

The Internet uses DNS (Domain Name System) to enable people to use words instead of the long and confusing numbers for Internet addresses. DNS is a distributed database that keeps track of computer's names and their corresponding IP addresses on the Internet. You can think of DNS as an In internet address book, mapping domain names to IP addresses.

Information transfer on the Internet from one device to another is done in the form of packets which are small amounts of data sent over a network. Each packet includes a source and destination as well as the content (or data) being transferred.
One of the most commonly used services on the Internet is the **World Wide Web (WWW)**.
The application protocol that makes the web work is **Hypertext Transfer Protocol (HTTP)**. HTTP is the protocol that web browsers and web servers use to communicate with each other over the Internet.

Learning Objectives:

- How web browsers work e.g. cookies and website tracking, browsing history etc.
- How search engines work.
- Understanding the difference between HTTP and HTTPS.
- Tools of mitigation e.g. clearing cookies, ad blockers, firewalls, enabling privacy controls etc.

Internet of Things

The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data. IoT can be further explained as a system of interrelated computing devices, mechanical and digital machines, objects, animals, or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.
Examples of IoT devices are Smart home appliances and Industrial sensors.

IoT brings the power of the internet, data processing, and analytics to the real world of physical objects. For consumers, for example, this means interacting with the global information network without the intermediary of a keyboard and screen; many of their everyday objects and appliances can take instructions from that network with minimal human intervention.

There are over 50 billion IoT devices worldwide as of 2020, and those devices will generate 4.4 zettabytes of data in 2021. (A zettabyte is a trillion gigabytes.) By comparison, in 2013 IoT devices generated a mere 100 billion gigabytes. The amount of money to be made in the IoT market is similarly staggering; estimates on the value of the market in 2025 range from $1.6 trillion to $14.4 trillion.

How IoT works

An IoT ecosystem consists of web-enabled smart devices that use embedded systems, such as processors, sensors, and communication hardware, to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices, for example, to set them up, give them instructions or access the data.

Input

Learning Outcomes

Understanding how the internet works allows for its users to appreciate how the communication of objects through the internet takes place.

1. Participants are each given pieces of paper representing one part of the chain of the flow of information Online **(Computer, WiFi, Gateway, ISP, Internet ... etc)**

2. Participants are asked to arrange the papers in the order they consider is correct to represent how an email travels through the Internet to reach another computer.

3. Once the papers are arranged, the facilitators will correct any mistakes, and will do a run-through explaining the process to everyone.

The trainer must also give some time to clarify doubts related to this process.

Deepening

Following the previous 'In Put' exercise;

1. Participants will be asked to paste each piece on a long paper (from a roll) that will be left on the floor.

2. At this point, the facilitators will go through the chain again, this time to point out and explain the vulnerabilities at each stage (and hint at good practices to keep participants calm and confident).

3. The trainer can also add any other practice or threat that is applicable to the context or that is relevant to mention to the participants.

Synthesis

1. Trainer divides the group into smaller groups that can "adopt" one of the vulnerabilities discussed in the previous exercise and ignite a conversation proposing the possible digital security solutions for each.

2. At the end, the groups will be given a minute to present their ideas to the rest of the group (while one of the facilitators takes notes and makes additions to what is reported back by the groups).

3. Facilitators will float around the groups giving brief explanations and answering questions, and mostly promoting discussion among all the participants.

Digital citizenship

Digital citizenship refers to the responsible use of technology by anyone who uses computers, the Internet, and digital devices to engage with society on any level.

It also refers to regular positive engagement with digital technologies. As the rate of technological advancement continues to increase, the Internet is being depended on globally for day-to-day activities. According to Karen Mossberger (et al) of the Massachusetts Institute for Technology, digital citizens are "those who use the internet regularly and effectively.

Who is a digital citizen?

It is someone who has the ability to use technology in an appropriate and responsible way.
Being a responsible digital citizen encompasses digital literacy, Online safety, and an acknowledgment of data privacy regulations. Some of the concepts categorized under Digital Citizenship include; Empathy, How the Internet works, Understanding user data, Practicing digital literacy, Acknowledging the digital divide, Practicing digital wellness, and Securing digital devices.

Three principles of digital citizenship:

1. Engage positively: Be aware of your own behaviour Online, respect others, discourage anti-social behaviour like Online bullying, stalking and bashing.

2. Know yourself and your Online world: Know what skills you have (think about My Digital Me), and understand how to use technology and devices.
Learn new skills and know your digital footprint.

3. Choose consciously: Make well informed decisions if you participate Online. Know how to protect yourself and the ones around you.

Activity

The trainer may opt to start this sub topic with this activity;
A. Who is a digital citizen?
Harvest some examples of digital citizenship from the group. What do they think this means?
Examples they might give:
•Someone who uses laptops
•Someone who is Online
•Someone who participates on social media
•Someone who participates in Online discussions etc.

B. Invite all participants to stand up from their chair and share that you are going to explore their current level of digital citizenship. Emphasize there is no right or wrong, we are all here to learn!

Start by explaining that the length of the training room is a scale from 0-10. The task is for the participants to move to the figure that fits their current digital citizenship.

The trainer then goes ahead to ask people why they stand where they stand.
Why did they pick this position?
What do they want to learn?

Encourage your participants! It is great that not everyone is standing on level 10, we are here to learn together!

Engage positively: I am always aware of my own behaviour Online, I respect others all the time, and discourage anti-social behaviour like Online bullying, stalking, bashing. Where do you stand?
Know yourself and your Online world:
I know what skills you have (think about My Digital Me), and understand how to use technology and devices. I always try to learn new skills and know my digital footprint. Where do you stand?

Choose consciously: I make well informed decisions if you participate Online. I know how to protect myself and the ones around me. Where do you stand?

Digital footprint

Digital footprint

A digital footprint is a trail of data you create while using the Internet. It includes the websites you visit, emails you send, and information you submit to Online services.

A "passive digital footprint" is a data trail you unintentionally leave Online. For example, when you visit a website, the web server may log your IP address, which identifies your Internet service provider and your approximate location. A more personal aspect of your passive digital footprint is your search history, which is saved by some search engines while you are logged in.
An "active digital footprint" includes data that you intentionally submit Online. Sending an email contributes to your active digital footprint, since you expect the data to be seen and/or saved by another person.

Discussion

A. Invite Participants to watch the video on Digital Footprint **(5 mins)**
https://www.youtube.com/watch?v=OBg2YYV3Bts
The Trainer then proceeds to ask the participants, what they learn from this video?
What is new for you?
What did you already know?

B. The trainer leads the participants in a discussion to summarize what a digital footprint is **(10 min)**

Input

For participants to understand digital footprint further, use the following practical example.

Learning Outcomes

Understanding how the internet works allows for its users to appreciate how the communication of objects through the internet takes place.

A. Hand out an A4 papers and markers to each participant and challenge them to visualize their digital footprint. Ask participants to reflect on their own digital footprint. What do they think they leave behind? What are they most proud of? What would they like to be erased from the web?
TIP: start with Googling yourself what do you find? (20 minutes)

B. Stick all A4 papers to the wall. Let participants check each other's digital footprints. What stands out? What similarities and differences do they spot? What are good ways to control your digital footprint?

Digital wellness

Deepening

Digital wellness

Digital wellness is the practice of refraining from indulging in the Internet and digital media for unreasonable amounts of time.

In other words, it's the practice of knowing when to "take a break" from screens.

Digital wellness is important because too much screen time can have adverse effects on anyone. Strangely enough, the best way to practice digital wellness is to leave digital devices for a few hours every day!

Reflections and Synthesis

Discuss with the participants how screen time can impact trans-active memory, empathy, and even grey matter.

Digital platforms:

The trainer invites each participant to search for their paired participant and gives them 5-8 minutes to find out on as many different platforms that person is currently active on. Walk around for support if participants struggle to use a search engine for this.

Start a flip-chart and list each digital platform and then ask how many people found their partner there. Add the number of participants behind it, for example:
Facebook (10)
Instagram (8)
Twitter (3) Etc.

After that start an open sharing on the advantages and disadvantages of each platform, by asking the participants to share user experiences. Participants can also share other things they noticed during their search.
Address any questions and move to the next exercise.

Digital Rights

The definition of digital rights is having the right and freedom to use all types of digital technology. Digital rights are merely an extension of the rights set out in the Universal Declaration of Human Rights by the United Nations as applied to the Online world.

The main objective of the declaration is to guarantee access to the Internet, in an effort to cover the digital divide and the proper use of the network as a global asset. It is however unfortunate that there is no international consensus on Digital Rights which has forced each country to develop its own Digital Rights Charter.

Digital rights include; the right to digital access, the right to freedom of expression, the right to privacy, the right to credit for personal works, and the right to digital identity.

Legal frameworks in Uganda

Uganda for long relied on the 1950 Penal Code Act, the 1950 Criminal Procedural Act, and
The 1996 Police Act to fight cyber-related crime. These laws however did not provide a direct legal solution to cyber-related crimes.
The first specific statutory law on cyber-related crimes enacted in Uganda was the 2006 **Copyright and Neighboring Rights Act**, to provide for the protection of literary, scientific, and artistic intellectual works. This was followed by the 2010 **Regulation of Interception of Communication Act** and the 2011 **Computer Misuse Act**, which provided for the lawful interception and monitoring of certain communications.

The Data Protection And Misuse Act, 2015: An Act to protect the privacy of the individual and of personal data by regulating the collection and processing of personal information; to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processors and data controllers; to regulate the use or disclosure of personal information; and for related matters Anti-Pornography Act: An Act to define and create the offence of pornography; to provide for the prohibition of pornography; to establish the Pornography Control Committee and prescribe its functions; and for other related matters.

The most recent legal provision on cyber related crime is the 2011 Computer Misuse Act to make provision for the safety and security of electronic transactions and information systems, to prevent unlawful access, abuse, or misuse of information systems including computers, and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters. It provides definitions of cybercrimes, related penalties, and some procedural measures that law enforcement authorities can use in their fight against cybercrimes.

Activity

Invite the participants to share what they know about Human Rights. Harvest their answers on a Flip Chart and make sure at minimum the following aspects are mentioned

They include the right to:

- Education
- Marriage and family
- Freedom of expression
- Freedom of thought
- Against discrimination
- Privacy, etc.

1. Uganda for long relied on the 1950 Penal Code Act, the 1950 Criminal Procedure Act, and the 1996 Police Act to fight cyber-related crime. These laws however did not provide a direct legal solution to cyber-related crimes.

2. The first specific statutory law on cyber-related crimes enacted in Uganda was the 2006 Copyright and Neighboring Rights Act, to provide for the protection of literary, scientific, and artistic intellectual works.

3. This was followed by the 2010 Regulation of Interception of Communication Act and the 2011 Computer Misuse Act, which provided for the lawful interception and monitoring of certain communications.

4. The most recent legal provision on cyber related crime is the Data protection and Privacy Act (2019)

Discussion

Invite the participants to share any cyber related legislation in Uganda, it is important that digital security trainers are well aware of the legal framework in Uganda.
The trainer will lead the participants through a discussion on the legal framework around digital rights in Uganda and it should include:

Divide the participants in groups of 3-4. Hand out a Flip Chart and markers to each group and invite them to create a Digital Rights "mind-map". Write "Why are Digital Rights important" in the middle and note associations around it.

After 10 minutes, stick the flip-charts to the wall and reflect on the different mind maps. What have participants noted? Did they make relations between Human Rights and Digital Rights?

Make sure that the following is emphasized or added if not addressed by the group. Digital rights are important because they are part of Human Rights. The UN Human Rights Council and the African Commission on Human and Peoples' Rights (ACHPR) both confirmed that the "same rights that people have offline must also be protected Online."

Input

Practical Example

If Human Rights are important? Why are Digital Rights important too?

Individual case study refer to Police Arrest, pg. 15.

Let participants step back every time so they can start afresh for each statement. Use as few or as many statements as you deem fit.

The trainer calls out ‘Cross the line if you’:

1. Know fully what Facebook is doing with your private data.
2. Have been blocked from a social media account.
3. Had your private pictures shared without your knowledge or permission.
4. Experienced hate speech or bullying Online.
5. Were not able to access a certain internet source because your government blocked it.
6. Had to block or unfriend someone because of the way they were talking to you Online.
7. Have read comments on social media that made you feel uncomfortable.

The trainer is free to include other appropriate and relevant statements, to suit the participants. The trainer can also ask (a) participant(s) to come up with a statement.

Deepening

The Trainer invites the participants to an open space where a line from masking tape is in the middle of the floor. Ask all participants to stand on one side of the room.

Read out statements and ask participants to step over the line to the other side of the room if the statement applies to them. After each statement you ask participants to look around the room and see who is standing where. Check in with participants to hear their experiences.

Synthesis

The trainer groups the participants to form 3 separate groups.

Group 1: data privacy,
Group 2: access to information,
Group 3: freedom of expression.

The trainer them challenges each group to discuss their assigned digital rights, their experiences? How are the rights safeguarded in their country? And What are positive and negative examples?

Each group is given a couple of flip-chart sheets to reflect, discuss and write down their answers to which they will make a 5 minute presentation.

Following the exercise, the trainer asks the participants if they are aware of the laws that protect the digital rights in their country. And to name the different laws that protect their digital rights.

3 Secure Communication

Introduction

Secure communication involves preventing unauthorized interceptors from accessing telecommunications in an intelligible form, while still delivering content to the intended recipients.

Objectives

During this module, the participants will gain an understanding of the following key topics equipping them with skills to send and receive secure messages:

- Messaging
- Secure voice calls
- Secure access platforms

Tools required

Trainer

These tools will be necessary for the trainer to prepare before conducting the training.

Devices

- Laptop
- Smartphone
- Projector
- Internet

Trainee

These tools will be necessary for the trainee to have during the training.

Devices

- Laptop
- Smartphone

access

Prerequisite knowledge

Prior to participating in this training, the participants should at least have an understanding of:

- Messaging Application security
- E-messaging
- Device settings on communication

Definitions

Messaging - The sending of written or spoken messages using a computer or another electronic device such as a mobile phone.

Email security - Describes various techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss, or compromise.

Phishing - Is the fraudulent attempt to obtain sensitive information such as usernames and passwords by posing as a legitimate person or entity.

WWW (World Wide Web) - Also known as a Web, it is a collection of websites or web pages stored in web servers and connected to local computers through the internet.

Internet - A vast network that connects computers all over the world. Through the Internet, people can share information and communicate.

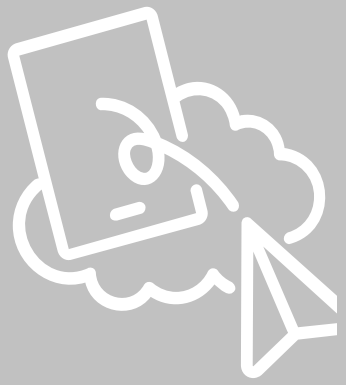
Activity

Installation of SIGNAL messaging app on an individual device. I.e. mobile phone, laptop and/ or desktop computer.

Signal was created by a small group of privacy activists in 2013.
Signal is a non-profit organization. Messages sent can be set to disappear after a particular (customizable) time frame. Signal Android users can send private messages and make secure calls to other Signal users anywhere in the world for free over the internet.

Installation process resources:

https://signal.org/download/android/
https://signal.org/download/ios/
https://signal.org/download/windows/
https://signal.org/download/macos/
https://signal.org/download/linux/



Messaging

Messaging is the sending of written or spoken messages using a computer or another electronic device such as a mobile phone.

Secure messaging
Messaging applications make it easy to communicate and connect with people around the world. However, with new ways to communicate and connect via technology, there are also new ways for your privacy and security to be breached. Private messages could potentially be read by third parties, the organizations behind the apps, and governments who collect private information on their citizens.
An application will qualify to be secure when it supports the following; End-to-end encryption, multi-mode messaging, and synchronization among different platforms/devices.

End-to-end encryption is a way of creating a secure messaging application by encrypting information so that only the players engaged in communication can read the messages, excluding Internet service providers, the application maker, the government or anyone else. From the moment a message is typed, to the time it spends in transit, to the second it's received, no one else can see that message.

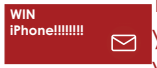
Multi-mode communication allows for users to send messages through texts, videos, and audios When a platform allows for messages to be send via multiple modes, it usually allows the user to delete whatever kind of message comes through.

Multi-platform support provides the opportunity to sync messages across mobile, web, and desktop platforms. If a user feels more secure storing private messages in one location and deleting them off of another, this can up one's data privacy.

Examples of secure messaging applications include
Signal Private Messenger, Wire, Threema, Telegram, Viber, Silence, iMessage, Line.

FACTS

Your contacts tell you they're receiving spam emails from you



There are messages in your sent folder that you did not send

You receive multiple failed delivery emails

Your account's location login history doesn't match your recent activity

How to tell if your email was hacked

Email Security

Email security describes various techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss, or compromise.

Why do we need email security?

- To protect confidential information
- To avoid identity theft
- To avoid phishing
- To prevent malware

Email security best practices

1. Use email encryption for both email content and attachments
2. Never open attachments or click links from unknown senders
3. Never share your password including co-workers
4. Use spam filters and an anti-virus software
5. Change password often and use best practices for creating them
6. Implement a data protection solution to identify sensitive data and prevent it from being lost via email
7. Be sure to log out every time you sign into your account
8. Use a different password for each of your accounts
9. Learn how to recognize phishing
10. Always check your email activity and settings

Phishing

This is the fraudulent attempt to obtain sensitive information such as usernames and passwords by posing as a legitimate person or entity.

Securing your email

You can control who accesses your email by the use of Two-Factor Authentication (2FA).

What is 2FA?

It is a security process in which the user provides two means of identification from separate categories of credentials or adds a second level of authentication to an account log-in. The two credentials are known as authenticating factors.

Or

An extra layer of protection used to ensure the security of Online accounts beyond just a username and password.

Email encryption

Email encryption is a way of sending secure emails. It involves encrypting, or disguising, the content of email messages in order to protect potentially sensitive information from being read by anyone other than intended recipients.

TIPS
How to identify phishing attacks

How to identify phishing attacks

- Emails with generic greetings
- Emails requesting personal information.
- Emails requesting an urgent response
- Emails with spoofed links.

Resources

GPG for MAC

https://gpgtools.org/
https://help.runbox.com/installing-gpg-os-x-gpg-tools/

GPG for Windows

https://gnupg.org/download/
https://help.runbox.com/installing-gpg-on-microsoft-windows/

Enigmail

https://www.enigmail.net/index.php/en/user-manual/installation-of-enigmail

Input

Practical Example

How to communicate with an encrypted email.
Installing GPG and Enigmail

Note:
To receive encrypted messages from other people, you must first send them your public key;
To send encrypted messages to other people, you must receive and store their public key;

Synthesis

10 TIPS ON HOW TO PROTECT YOURSELF FROM A PHISHING ATTACK

Tip 1: Don't trust the display name
A favorite phishing tactic among cybercriminals is to imitate the display name of an organization's email.

Tip 2: Look but don't click
Hover your mouse over any links embedded in the body of the email. If the link address looks weird, don't click on it. If you want to test the link, open a new window and type in website address directly rather than clicking on the link from unsolicited emails.

Tip 3: Check for spelling mistakes
Brands are pretty serious about email. Legitimate messages usually do not have major spelling mistakes or poor grammar. Read your emails carefully and report anything that seems suspicious.

Tip 4: Analyze the salutation
Is the email addressed to a vague "Valued Customer?" If so, watch out—legitimate businesses will often use a personal salutation with your first and last name.

Tip 5: Don't give up personal information
Legitimate banks and most other companies will never ask for personal credentials via email. Don't give them up.

Tip 6: Beware of urgent or threatening language in the subject line
Invoking a sense of urgency or fear is a common phishing tactic. Beware of subject lines that claim your "account has been suspended" or your

Synthesis continued.

account had an “unauthorized login attempt.”

Tip 7: Review the signature
Lack of details about the signer or how you can contact a company strongly suggests a phish. Legitimate businesses always provide contact details.

Tip 8: Don’t click on attachments
Including malicious attachments that contain viruses and malware is a common phishing tactic. Malware can damage files on your computer, steal your passwords or spy on you without your knowledge. Don’t open any email attachments you weren’t expecting.

Tip 9: Don’t trust the header from email address
Fraudsters not only spoof brands in the display name, but also spoof brands in the header from email address

Tip 10: Don’t believe everything you see
Phishers are extremely good at what they do. Just because an email has convincing brand logos, language, and a seemingly valid email address, does not mean that it’s legitimate. Be skeptical when it comes to your email messages—if it looks even remotely suspicious, don’t open it.

4 Risk Assessment

Introduction

Risk Assessment is a process that helps you identify and manage potential threats that could harm, damage and disrupt your digital assets.

The purpose of this module is to encourage training participants to think critically about digital security risks, and furthermore support the development of personalized, context-specific strategies to mitigate such risks.
Human Rights Defenders handle sensitive information and the devices that contain them on a daily basis. Few have considered the risks to these assets and the potential consequences of losing control of them during a theft, confiscation or natural disaster.
This module will include some tools for assessing digital and physical threats and will encourage participants to consider:

- The value of their work and the information they depend on for their work (e.g., contacts).
- Personal habits that may put their work at risk.
- A practical level of safety and privacy in an office.

Objectives

- Enable participants to overcome any frustrations with their digital security practice, and reassure them that building their skills is an iterative process requiring time and patience.

- Identify the specific risks that participants face, allowing them to design individual security plans and protocols to address these risks.

- Support participants as they design strategies to facilitate post-training implementation of their security plans and protocols.

Tools required

Trainer

These tools will be necessary for the trainer to prepare before conducting the training.

Devices

- Laptop
- Smartphone
- Projector
- Internet

Resources

- Flip charts
- Markers
- Tack
- Pens
- Note books
- Internet

Trainee

These tools will be necessary for the trainee to have during the training.

Devices

- Laptop
- Smartphone
- Internet

Definitions

Risk - Is any chance or probability that could cause a loss of, or damage to computer hardware, software, data, information or processing capability.

Threats - Are malicious acts that seek to damage data, steal data, or disrupt digital life in general.

Vulnerability - Is a weakness which can be exploited by a threat to gain unauthorized access to or perform unauthorized actions on a computer system.

Incident- Is an event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed.

Risk mapping - Is identifying the risks associated with an organization, project or other system in a way which enables an organization to understand the risk better.

Threat hunting - The process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.

Threat model - Threat modeling is a process of identifying potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, through which risks can be enumerated, and mitigations can be prioritized.

Security policy - A Security Policy lays out the rules and procedures for all individuals accessing and using organizational IT assets and resources.

Ransom-ware - This is a form of malware (malicious software) that attempts to encrypt (scramble) your data and then extort a ransom to release an unlock code to regain access your computer system.

Risk impact - An estimate of the potential losses associated with an identified risk. standard risk analysis practice to develop an estimate of probability and impact.

Preparation

Prior to the start of the class, the trainer prepares the "risky space" with several risks left intentionally visible. These might include:

- Open windows.
- Door with key hanging from the lock.
- Laptop(s) without a locking cable on a desk.
- Wires or cables for devices that have been strewn on the floor where someone would need to step over them.
- Power plugs dangling loosely from a power strip near paper.
- Open desk drawers, with an external hard drive sticking out.
- Passwords written on a "sticky note" or other paper taped to a monitor or onto the surface of a desk.
- An open bag with a smartphone, camera or other valuable device exposed in it.
- A flash drive, left in a computer's USB socket.
- Computer left unattended with active Outlook, Gmail, Skype or other communication application open and visible.
- Laptop(s) without a locking cable on a desk.

NOTE: This is only a list of a suggestions. This can be modified to fit the requirements of the participants and a risky habit practiced by participants that trainers want to draw attention to.

Conducting the Activity

At the start of the exercise, the trainer explains that the purpose of the module is to learn ways to identify risks to journalists and their electronic devices. Since human rights' defenders e.g. journalists often have to be good investigators, this activity should be perfect for them. The trainer then:

- Invites participants to walk up to or around the prepared space (or view a prepared photograph) for five minutes and take notes of risks they see.
- Organizes participants into groups of two or three and asks them to work together to share their findings with each other, and to then take five minutes to write their observations on a sheet of chart paper.
- Reminds participants that some "risks" will be obvious while others may not be obvious to all members in the group, and encourages discussion among participants to explore their views.
- When 10 minutes are left in the activity, asks teams to take turns •presenting their "risks list" and to explain why individual items on the list might create a risk.
- Takes some time to point out any prepared risks that the group has not identified.

Activity

Risk hunting:

This activity invites participants to explore a mock room or a "risky space" (a place that has been set aside in the training venue, or a separate room) to identify potential risks to equipment and data. Participants will be guided through a mock exercise with prior set "system risks" to simulate thinking on various security risks in their working environment. In this activity, the space is prepared in advance and the trainer will keep a list of risks that have been intentionally left for participants to find.

Useful questions:

1. Did anything in the exercise remind you of your office or your workspace? Did it look similar? Very different? In what ways?
2. Why do you think risks like these are common in organizations?
3. Do you think these risks only affect the person using the workspace or would other people in the organization be affected by these risks? How?
4. What kinds of risks are present in public spaces? Do you see similar issues in IT cafes, for instance?
5. Do you know of examples where:
◦A journalist's personal safety was compromised? Do you know what happened?
◦A journalist's property or data was compromised? How did that happen?
6. What kinds of precautions do you take to protect your physical safety or the safety of you work?
7. Has anyone in this group conducted a risk assessment? If someone has, ask the person to explain how he or she went about in the exercise.

Discussion

Frequently, the Risk Hunting activity (above) leads to an extended discussion on its own when teams take turns presenting their findings. However, if time remains, trainers may wish to have participants sit in a circle or semicircle, so they can address one another. The following questions may help start the discussion. Trainers are welcome to add to this list or improvise as they see fit.
As always, trainers should encourage each person to speak up. It is likely that some have thought carefully about the issues; others may not have thought too much. This exercise will likely reveal some interesting practices, which makes for a rich discussion.

Risk classification refers to the grouping of organizational assets by their likely impact or estimated costs, occurence and any measures required to counter them. There are three main categories of risks in Digital security. These include:

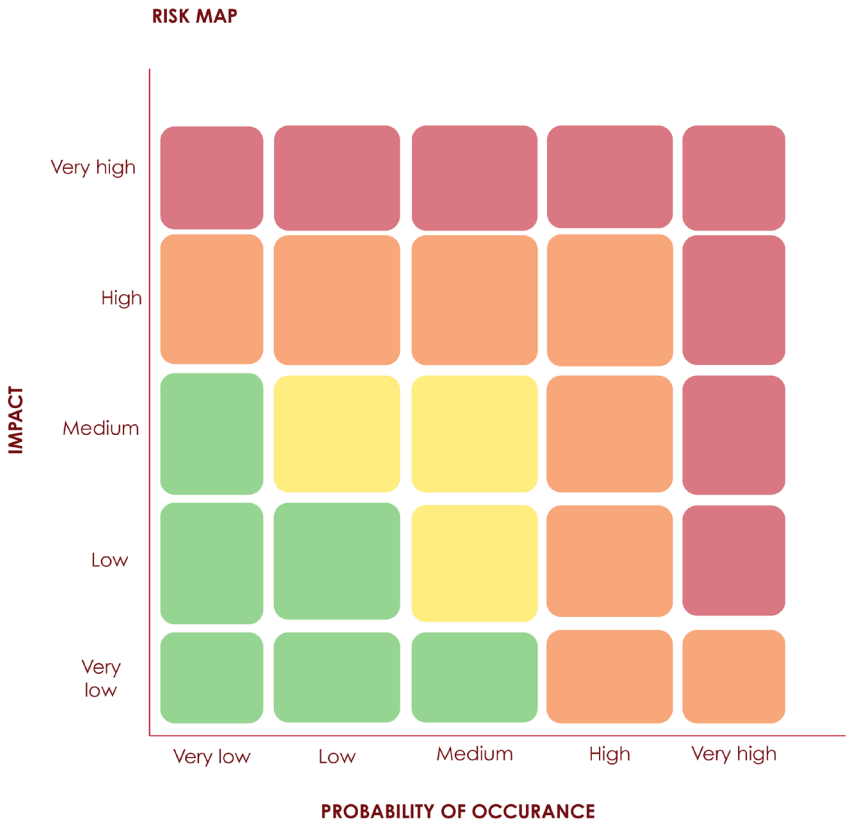
1. No Risk:
These are organizational assets that if breached pose no risk whatsoever to the organization. Such assets may include office furniture and any other asset that doesn't store data.

2. Low Risk:
Organizational assets that store data that if breached, pose no serious risk to the organization. Such assets usually store data that is intended for public disclosure and therefore if breached would have no effect on the organization's mission, finances, operation and life safety.

3. Medium Risk:
Organizational assets are classified as medium risk if the data stored on such assets is not generally available to the public, or
The loss of confidentiality, integrity, or availability of the data or system has:
- No impact on the organization's mission and potentially a moderate risk to reputation,
- At most a mild impact on the organization's finances,
- At most a mild risk to the security of other systems protecting data,
- No risk to life safety.

4. High Risk:
Organizational assets are classified High risk if:
- The loss of confidentiality, integrity, or availability of the data or asset could have a significant adverse impact on the organization's mission, safety, finances, and/or reputation.

Example of risks
- Organization or individual data loss.
- Safety or health risks related to a location, lifestyle, occupation or activity. ...
- Potential to stop or delay an ongoing project thereby affecting its sustainability
- Financial loss incurred when trying to recover
- Time taken to recuperate from loss
- Negative impact on the reputation of the institution or individual affected.



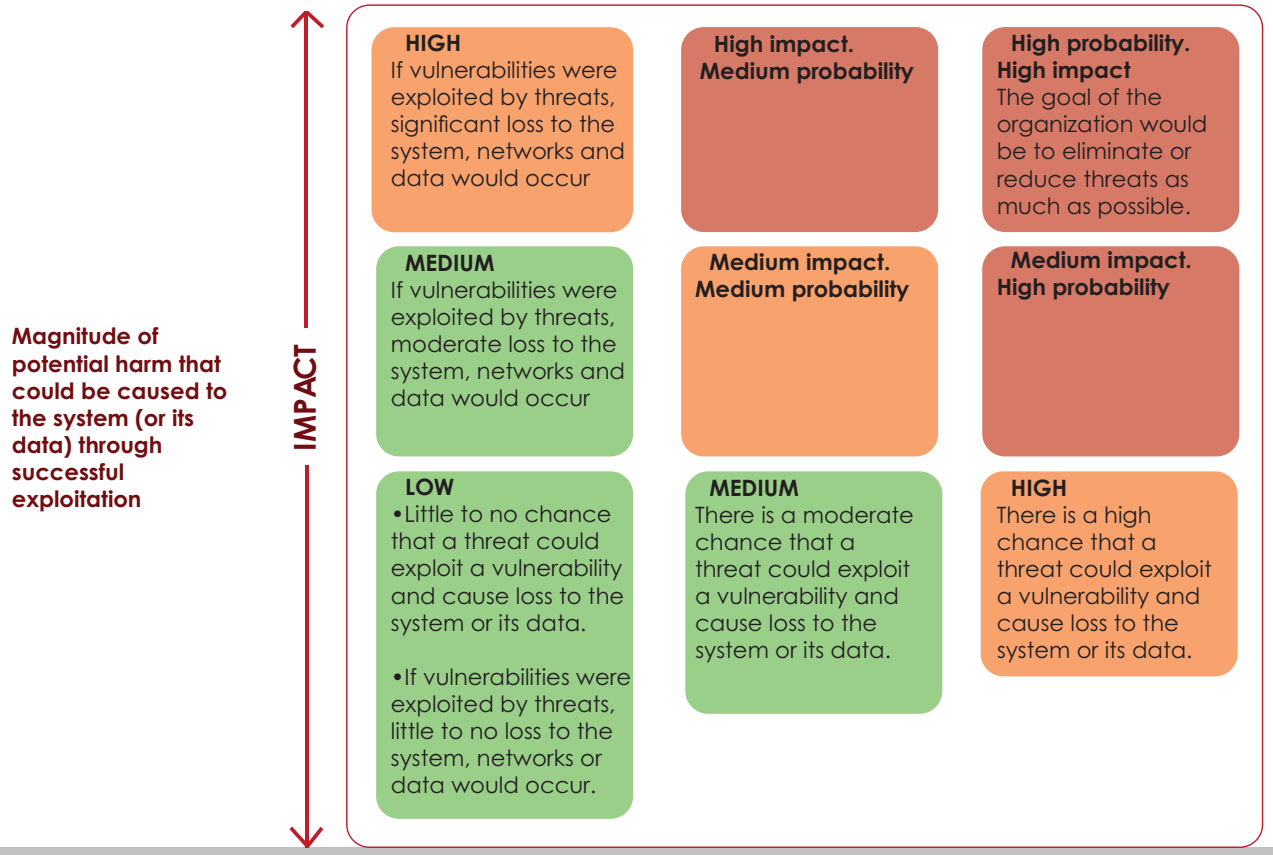
Risk impact

Risk impact is an estimate of the consequences associated with an identified risk. It is a standard risk analysis practice to develop an estimate of probability and impact.

Plotting the Risk matrix

This matrix is based on measuring the risk probability against impact. The matrix iterations depend on what measures are put in place to mitigate impact.

RISK IMPACT VS. PROBABILITY MATRIX



Security plans & protocol

A security plan is an outline of key changes that an organization, collective, or individual has identified as requirements for increasing their digital security. Plans are a defined process, with a beginning and an end.

A security protocol is a set of measures or actions related to digital security that are each connected to a specific activity or process within an organization or collective. Protocols are ongoing practices that remain in effect even when a digital security plan has been fully implemented, and will evolve over time in response to changes in risk and threat environments.

Creating an Organizational Security Plan and Protocol

The following sections need to be filled in by the participants with the help of the facilitator. A new row should be started for each risk or threat identified.

(Form provided in appendix)

Identified vulnerabilities (Which of our practices as individuals, or circumstances as an organization, could expose us to harm?)	**Strengths & Capacities** (What strengths do we have as an organization that give us an advantage in responding to identified threats and risks?)	**Mitigating actions** (What kind of measures do we need to take in order to mitigate the risks? To be better prepared for identified threats?)	**Resources needed** (What resources (economic, human, etc.) would we need to implement these actions?)	**Who Needs to be Involved?** (Which areas or people within our organization need to be involved in implementation? Will any sign-off or other permissions be required?)

Digital footprint

A digital footprint is data that is left behind when users have been Online. There are two types of digital footprints which are passive and active.

A **passive footprint** is made when information is collected from the user without the person knowing this is happening.
An example of a passive digital footprint would be where a user has been Online and information has been stored on an Online database. This can include where they came from, when the footprint was created and a user IP address. A footprint can also be analyzed offline and can be stored in files which an administrator can access. These would include information on what that machine might have been used for, but not who had performed the actions.

An **active digital footprint** is where the user has deliberately shared information about themselves either by using social media sites or by using websites.
An example of an active digital footprint is where a user might have logged into a site when editing or making comments such as on an Online forum or a social media site. The registered name or profile can be linked to the posts that have been made and it is surprisingly easy to find out a lot about a person

from the trails you leave behind.

Reviewing Participant's Digital Footprints

A simple exercise can be done to evaluate the participants' digital footprints. Each participant is assigned another participant to google. Let each participant try to find out from the internet information about another participant. They can compile the information into a profile for the other participant to see how much of their information is Online.

Examples of threats & vulnerabilities

1. MALWARE

As pointed out earlier, new malware is being created all the time. However, while the statistic of 360,000 new malware files a day sounds daunting, it's important to know one thing: Many of these "new" malware files are simply rehashes of older malware programs that have been altered just enough to make them unrecognizable to anti-virus programs.

Over the years, however, many different kinds of malware have been created, each one affecting the target's systems in a different way:

Ransom-ware. This malicious software is designed to encrypt the victim's data storage drives, rendering them inaccessible to the owner. An ultimatum is then delivered, demanding payment in return for the encryption key. If the ransom demand isn't met, the key will be deleted and the data lost forever with it.

Trojans. This references a kind of delivery system for malware. A Trojan is any piece of malware that masquerades as a legitimate program to trick victims into installing it on their systems. Trojans can do a lot of damage because they slip behind your outermost network security defenses by posing as something harmless while carrying a major threat inside like a certain infamous horse did to the city of Troy in Homer's "Iliad."

Worms. Worms are programs that can self-replicate and spread through a variety of means, such as emails. Once on a system, the worm will search for some form of contacts database or file sharing system and send itself out as an attachment. When in email form, the attachment is part of an email that looks like it's from the person whose computer was compromised. The goal of many malware programs is to access sensitive data and copy it. Some highly-advanced malware can autonomously copy data and send it to a specific port or server that an attacker can then use to discreetly steal information.

Basic anti-virus can protect against some malware, but a multi-layered security solution that uses anti-virus, deep-packet inspection firewalls, intrusion detection systems (IDSs), email virus scanners, and employee awareness training is needed to provide optimal protection.

2. UNPATCHED SECURITY VULNERABILITIES

While there are countless new threats being developed daily, many of them rely on old security vulnerabilities to work. With so many malware looking to exploit the same few vulnerabilities time and time again, one of the biggest risks that an organization can take is failing to patch those vulnerabilities once they're discovered.

It's all too common for an organization or even just the individual users on a network to dismiss the "update available" reminders that pop up in certain

programs because they don't want to lose the 5-10 minutes of productive time that running the update would take. Updating is a nuisance to most users. However, it's a "nuisance" that could save an organization untold amounts of time, money, and lost data later.

The easy fix is to maintain a regular update schedule a day of the week where your IT team checks for the latest security patches for your organization's software and ensures that they're applied to all of your organization's systems.

3. HIDDEN BACK-DOOR PROGRAMS

This is an example of an intentionally-created computer security vulnerability. When a manufacturer of computer components, software, or whole computers installs a program or bit of code designed to allow a computer to be remotely accessed (typically for diagnostic, configuration, or technical support purposes), that access program is called a back-door.

When the back-door is installed into computers without the user's knowledge, it can be called a hidden back-door program. Hidden back-doors are an enormous software vulnerability because they make it all too easy for someone with knowledge of the back-door to illicitly access the affected computer system and any network it is connected to.

4. SUPERUSER OR ADMIN ACCOUNT PRIVILEGES

One of the most basic tenets of managing software vulnerabilities is to limit the access privileges of software users. The less information/resources a user can access, the less damage that user account can do if compromised.

However, many organizations fail to control user account access privileges allowing virtually every user in the network to have so-called "Superuser" or administrator-level access. Some computer security configurations are flawed enough to allow unprivileged users to create admin-level user accounts.

Verifying that user account access is restricted to only what each user needs to do their job is crucial for managing computer security vulnerabilities. Also, ensuring that newly-created accounts cannot have admin-level access is important for preventing less-privileged users from simply creating more privileged accounts.

5. AUTOMATED RUNNING OF SCRIPTS WITHOUT MALWARE/VIRUS CHECKS

One common network security vulnerability that some attackers learned to exploit is the use of certain web browsers' (such as Safari) tendencies to automatically run "trusted" or "safe" scripts. By mimicking a trusted piece of code and tricking the browser, cybercriminals could get the browser software to run malware without the knowledge or input of the user who often wouldn't know to disable this "feature."

While keeping employees from visiting untrustworthy websites that would run malware is a start, disabling the automatic running of "safe" files is much more reliable and necessary for compliance with the Center for Internet Security's (CIS') AppleOS benchmark.

6. UNKNOWN SECURITY BUGS IN SOFTWARE OF PROGRAMMING INTERFACES

Computer software is incredibly complicated. When two or more programs are made to interface with one another, the complexity can only increase. The issue with this is that within a single piece of software, there may be programming issues and conflicts that can create security vulnerabilities. When two programs are interfaced, the risk of conflicts that create software vulnerabilities rises.

Programming bugs and unanticipated code interactions rank among the most common computer security vulnerabilities and cybercriminals work daily to discover and abuse them. Unfortunately, predicting the creation of these computer system vulnerabilities is nearly impossible because there are virtually no limits to the combinations of software that might be found on a single computer, let alone an entire network.

7. PHISHING (SOCIAL ENGINEERING) ATTACKS

In a phishing attack, the attacker attempts to trick an employee in the victim organization into giving away sensitive data and account credentials or into downloading malware. The most common form of this attack comes as an email mimicking the identity of one of your organization's vendors or someone who has a lot of authority in the organization.

For example, the attacker may say something like: "This is Mark from IT, your user account shows suspicious activity, please click this link to reset and secure your password." The link in such an email often leads to a website that will download malware to a user's computer, compromising their system. Other phishing attacks may ask users to give the attacker their user account credentials so they can solve an issue.

The basic goal of this strategy is to exploit an organization's employees to bypass one or more security layers so they can access data more easily.
There are several ways to defend against this attack strategy, including:
Email Virus Detection Tools. To check email attachments for malware that could harm your network.

Multi-factor Authentication (MFA). Using multiple authentication methods (such as biometrics, one-use text codes, and physical tokens) for giving users access to your network makes it harder for attackers to hijack user accounts with just the username and password.

Employee Cybersecurity Awareness Training. An educated employee is less likely to fall for phishing schemes than one who doesn't know basic cybersecurity protocols. Cybersecurity awareness training helps to provide employees with the basic knowledge they need to identify and avoid phishing attacks.

Defense in Depth. Using a defense-in-depth approach to network security adds extra layers of protection between each of the individual assets on the network. This way, if attackers bypass the outermost defenses of the network, there will still be other layers of protection between the compromised asset and the rest of the network.

Policy of Least Privilege. Enacting a policy of least privilege means restricting a user's access to the minimum amount needed to perform their job duties. This way, if that user's account privileges are misused, the damage will be limited.

8. INSIDERS

The biggest security vulnerability in any organization is its own employees. Whether it's the result of intentional malfeasance or an accident, most data breaches can be traced back to a person within the organization that was

breached.

For example, employees may abuse their access privileges for personal gain. Or, an employee may click on the wrong link in an email, download the wrong file from an Online site, or give the wrong person their user account credentials allowing attackers easy access to your systems.

Some of the same prevention techniques mentioned in the anti-phishing bullets can be applied to prevent data breaches caused by employees.

For example, using a policy of least privilege keeps users from having access to too much data at once, making it harder for them to steal information. Additionally, cybersecurity awareness training helps employees spot phishing attempts and other social engineering-style attacks so they won't fall for them.

COMMON DEVICES THAT CAN BE ATTACKED

The Internet of Things (IoT) encompasses many "smart" devices, such as WiFi capable refrigerators, printers, manufacturing robots, coffee makers, and countless other machines. The issue with these devices is that they can be hijacked by attackers to form slaved networks of compromised devices to carry out further attacks. Worse yet, many organizations don't even realize just how many IoT devices they have on their networks, meaning that they have unprotected vulnerabilities that they aren't aware of.

These unknown devices represent a massive opportunity to attackers and a massive risk for organizations.

To minimize the risk from IoT devices, a security audit should be performed that identifies all of the disparate assets on the network and the operating systems they're running. This way, these IoT devices can be properly accounted for in the organization's cybersecurity strategy. Such audits should be performed periodically to account for any new devices that may be added to the network over time.

Title: Sharing Files Can Put Lives at Risk

Story: An organization in Uganda was using Dropbox for file sharing. It was a collaborative project and everyone working on the project had access to all the files and folders, including sensitive information. No one was keeping track of what was in the shared folder, who had access to specific files, and which of the many members could share or had shared which folders with other individuals not connected to the project.
During the course of the project, one of the team members was asked to leave the news organization. As he left, he returned all the hardware (including laptop, camera, and flash drives) that he had in his possession. However, no one remembered to revoke his permission to the Dropbox folder.

The outgoing team member joined another organization and released all the information that his former colleagues had so painstakingly collected. In the process, he also revealed the identity of a source that wished to remain anonymous and sensitive information that could be traced to the source. The source had to be spirited out of the country.
The trainer asks participants what they think the organizations could have done differently.

Input

Case study:
Introduction: As human rights defenders, we're constantly researching and sharing information. Even as we take steps to ensure the protection of our data, this case reminds us that it is just as important,internally within the media organization, to pay attention to who has access to that information.
This is especially important to remember when reporters rely on the Cloud to share files.

- What could the organization have done to ensure that they did not lose control of their information and to reduce the chances of damage?

- Could a policy of updating the list of people with access to shared folders have helped?

- What would you do in a similar situation?

The trainer can make the following points:

1. Depending on the security environment, any file can be considered sensitive.
2. Control where information is shared and sent. Information should not be shared with anyone outside of a need-to-know basis, and controls should be in place to ensure that people receiving information do not share it repeatedly.
3. Reviewing access and changing passwords at regular intervals is a good idea.

Input

Additional case studies

Risk of cyber attacks increasing, says report
Cybercrime shoots up during the Covid-19 lock-down

Exercise 1 (60 Minutes)
The trainer distributes the assessment worksheets at the start of this session (provided in the appendix)
Assessment Worksheet: Physical Environment

The goal of this exercise is to provide participants with a team-based approach and some tools to begin a risk assessment for their workplace. The trainer guides the participants through the following steps:
1. Divides participants into two teams, one of which will focus on physical safety and the other on digital safety.
2. Explains that 30 minutes will be spent on identifying risks and prioritizing them. Everyone should return to the training room at that point and be prepared to contribute to a group list of identified risks
3. At the end of 30 minutes, collects the participants and facilitates a discussion in which he or she writes on chart paper a collective list of risks spotted by participants.
4. Asks the class to prioritize the risks based on the likelihood of each threat and what level of impact the threat could have. For example, earthquakes are potentially devastating no matter where they occur (high impact), but they may be rare in some regions (low likelihood).

Deepening

This section is divided into risk assessment and safety plan exercises. We recommend the trainer set aside approximately 60 minutes for the first exercise and 30 minutes for the second.
Participants should be told at the outset that the purpose of the exercises is to help them start a practical risk assessment and action plan.

1. Divides participants into two teams and alerts the teams they will have 20 minutes to build on the work they just concluded.
2. Asks Team A to brainstorm ways to avoid or mitigate the risks that were identified in Exercise 1. Participants should list these on a single list of chart paper. Team A should take the following into consideration:
◦Assuming they may not have all the answers, who are the key people they could ask for help and recommendations?

3. Asks Team B to create guidelines that their office (or any office) might follow when trying to conduct a comprehensive risk assessment and the safety plan (or action plan) to implement recommended solutions. Team B should take the following into consideration:
◦Who are the key colleagues who would have to be involved in any comprehensive risk assessment? (Generic titles are fine: e.g., "managing editor.")
◦Who will have to make key decisions in order for safety-related changes, such as new policies, to be implemented?
◦What would a reasonable schedule look like?
◦What tools could be used in the office to educate colleagues about changes in security policies when they are rolled out?

4. When 10 minutes are left, asks teams to present their findings.

Deepening

Exercise 2 (30 minutes)

This exercise builds on the previous exercise. The trainer guides the participants through the following steps:

Useful questions:

- Outside the work environment, do you think risk assessments have a practical use for you personally?
- Based on some of the topics we've discussed, is there anything that you know you do, or that you see in your office, that you would change immediately?
- What do you think will be the biggest challenge in trying to conduct a risk assessment and create a Safety Plan for yourself or the organization that you work with?
- What challenges do you foresee in implementing the safety plan?
- What do you think of this statement "physical security, personal (data) security and network security are not separate things, and instead are dependent on one another."

Synthesis

We recommend that trainers use this wrap-up session for informal questions to the group, reviewing the material that has been covered in the module. The following questions may help participants think about using what they have learned:

5 Data protection & Privacy

Introduction

This section contains training modules related to safely storing, backing up, and protecting important or sensitive data, and practices which training participants can adopt to perform regular data backups, create stronger passwords, and make informed decisions around how and where they keep their data. Topics addressed include data backup procedures, creating and managing multiple strong passwords, and detailed options for data storage.

Objectives

During this module, the participants will gain an understanding of the following key topics:

- Backing up data.
- Understanding information maps.
- Understanding the role of encryption in data protection.
- Vulnerability to data security.

Tools required & definitions

Trainer

These tools will be necessary for the trainer to prepare before conducting the training.

Devices

- Laptop
- Smartphone
- Projector
- Internet access

Resources

- USB flash drive
- Suitable space
- Colored electric tape
- Hands-on guides
- Whiteboard
- Post-it notes (multiple colors)
- Markers (multiple colors)
- Flip-chart paper

Trainee

These tools will be necessary for the trainee to have during the training.

Devices

- Laptop
- Smartphone

Data Type - It can be many things (point to the matrices for examples). Many users decide to back up an entire device instead of having tailored backup plans for different data types; others may need to create specialized backup policies. Specialized policies are especially important for particular data types due to issues related to the sensitivity of the data, travel (particularly crossing borders), and the amount of changes to one data type versus another over time (e.g., a large volume of video editing or sound recordings, an organization's email database).

Master Copies - The "original" version of the data - for example, the original photo or video taken, the first version of a document, etc. For most people, this would be whatever is on their laptop or their mobile device.

Duplicates - Backup version of the master, or original, copy of the data in question.

Backup Location - This is where a data backup is physically located - this can refer to everything from a laptop hard drive or USB drive to an email account or cloud storage account.

Storage Device - This could be an external hard drive, a corporate cloud service (Google Drive, Dropbox), your own Online server (ownCloud), or a small portable storage device like a USB flash drive.

Information map - A research-based method for writing clear and user focused information, based on the audience's needs and the purpose of the information.

Encryption - This process converts the original representation of the information, known as plain-text, into an alternative form known as cipher-text. Under encryption only intended recipients can open the email or text. This happens when a set of keys private and public keys are created and only a public key is exchanged with the other party.

Cloud - A cloud is just a server that's located out of your physical reach but can be accessed with the use of an internet network.

Activity

Information mapping

Preparation
Include an axis denoting the relative sensitivity of data **(illustrated in Table 1)**. This adds time to the activity, but can help reinforce risk management as a theme during your training.

Running the Activity

In an ideal scenario, the participants have a high level of trust with each other and will be comfortable speaking freely. In situations in which participants are unfamiliar to one another, trainers may want to try to break a larger group up into teams or small groups that share similar situations.

Social Engineering

Social Engineering is a tactic frequently to exploit human vulnerabilities, which typically involves impersonating a user to a company to have your password reset, as seen in this example case.
Phishing and spear-phishing are common examples of social engineering.
Resetting a password by correctly answering the "privacy questions" for an account, using personal information available Online, is another example.
This is how a number of celebrities and other high-profile accounts have been "hacked" in recent years, but not only celebrities have information about personal "answers" available Online.

False Account Alerts

Sometimes users receive notifications, from social media sites or other Online services, alerting "You've had your account hacked" or "Someone may be attempting to access your account" - these can mean a number of things:
Sometimes it's completely out of a user's control, and a service or a company has been compromised with your username, password, and (sometimes) other information falling into the wrong hands (this has happened with LinkedIn and Twitter, most notably).
Another possibility is that the email is not actually from the site or service it claims to be, but rather is a phishing or spear-phishing attempt, where a third-party creates an email that looks

How are passwords commonly compromised?

exactly like one that might be sent by a website asking users to "reset" their passwords - in reality, the current password entered will be captured and then used to access your accounts.
It can also mean that you've been specifically targeted, and someone with enough incentive and resources wants access to your account enough to try to break into them, or hire someone to do so.

Since the activity includes several discussions, the trainer finally concludes the activity with a discussion on:

1. How would it feel to lose all this information?
2. Has anything similar happened before, are there any personal examples we can learn from?
3. If we were doing the exercise again, what would they do differently? What would they back up?

Risk classification

Step 1: Where is Our Data?

Explain to participants that this session will cover an information mapping activity, the purpose of which is to get a sense of what and where our important information and data actually is. Start by listing the different places where our information is stored, according to participants.
If no suggestions are forthcoming, trainers can prompt participants with some of the more common storage media and locations:

- Computer hard drives
- USB flash drives
- External hard drives
- Cellphones
- CDs & DVDs (and BDs)
- Our email inbox
- Dropbox, Google Drive, SkyDrive, etc
- Physical ("hard") copies in the office
- Video tapes, audio recordings, photographs, etc.

Add these titles to the sheet or whiteboard and construct the matrix (example above) around them if you have not already done so.

Step 2: What is Our Data?

As a next step, begin to elicit from participants what types of information or data they have in each of the above places. Some examples might include (again, these are useful to kick-off with if no suggestions are forthcoming):

- Email correspondence and messages
- Contact details, such as a member contact database
- Reports and/or research documentation
- Budget and financial accounts, spreadsheets, etc.
- Videos and images
- Audio recordings or files
- Private messages on Social Networks

To encourage participant interaction, write one of the above examples on a post-it note and affix it to the appropriate box within the matrix; then, ask whether there is another copy of this data in another storage medium or location. If there is, you can use another sticky (preferably of a different color) and affix it within the appropriate box for where the duplicate is kept.

You can use this moment to teach the difference between **master copies** and **duplicates.**
Repeat this process with another example, hopefully provided by a participant.

Optional
If including the sensitive / non-sensitive axis, refer back the two examples and introduce the axis representing sensitivity. The higher on the chart, the more sensitive the data - place the two stickies on this axis, in locations representing their relative sensitivity.

Step 3: Participant-Created Matrices

For this step, now divide the group into smaller teams - it helps if there are relatively clear thematic distinctions within the group, such as nationality, type of work, supported community, etc. Have a large sheet of paper with an unfilled matrix ready for each group. **(Example illustrated in appendix)**

Next, walk your participants through the following set of instructions:

1. Each group will be given two sets of post-it notes, each set a different color, and each participant should think of the 5 most important types of data they work with. They should write one type per note.

2. For any type of data that has a duplicate location, they should represent this with a different colored post-it note. For instance, if the two post-it colors are Yellow and Pink, have all master versions of the data be Yellow and any duplicates of that master be pink.

3. When each participant in a team has their top 5 most important data types created, they should go to the team's matrix and affix their completed post-it notes within the relevant boxes.

4. Give participants 5-10 minutes to work on identifying their types of data. Once the time is up, there should be one completed matrix per team.

5. It might be useful to go from team to team, identifying interesting characteristics of each matrix. For example, note where there is particularly heavy dependence on one device, or where there's a lack of duplicate stickies, etc.

Step 4: How Could Things Go Wrong?

Explain that this exercise helps to give us a useful, visual sense of where our data is stored.

Elicit from participants whether or not the information represented on these matrices, in their opinion, covers all the data we generate?
The answer is, in reality, no.

It demonstrates only a small percentage of the data we all generate each day, whether we are aware of it or not. Referring to one of the teams' matrices, for example, mention the information that is shown as kept on their computer hard drive - this will usually be the fullest part of many matrices produced during this exercise, otherwise mention whichever storage location appears to have the most data stored on it.

Using the example of the computer hard drive, elicit from the group some examples of things that can cause a computer to stop working or otherwise make the data stored on it inaccessible.
Perhaps take a show of hands - who has had this happen to them?

- Virus or malware attack could destroy or corrupt data stored on a hard drive.
- A computer could be stolen or confiscated.
- Infrastructural problems, like a power failure or a power surge, could render it

inoperable.
• Unstable software or operating system could potentially brick a computer.

So, what if any of the above happens? What happens to all this data?
• Dramatically remove each of the stickies from the column, maybe throw them on the floor, etc.
• Gesture to the remaining stickies in the other columns - this is all that we'll be left with!

So what can we do to avoid this? We should put more copies into different locations - this is called backing up.

(Optional) Step 5: Sensitive Data in the Wrong Hands

The sensitive / non-sensitive distinction in the matrix is optional, and should only be done with enough time to drive adequate discussion about the relative sensitivity of information. It can also be presented as a scale rather than a dichotomy.

Take the example of a second team's data if possible, and/or another column on the matrix of the first team:
• What if your computer hard drive, mobile phone, etc. Is stolen or your sensitive account password is cracked?
• Remove the stickies from the column but keep them in your hand and read them.
• Use this to represent a third-party with unwanted access to this information.
• What could they do with it? What are you, the user, left with?

Data backup basics

This addresses basic practices for users, at both individual and organizational levels, for successful and safe backup of important information. Similarly, to help participants better visualize their personal "information map", this module also emphasizes the importance for users of understanding the what (type or format) and the where (storage location) of such valuable or sensitive data.

Learning Objectives

At the conclusion of this subtopic, the participants should ideally:
- Become more aware of the possibility of data loss, and how it can potentially happen.
- Understand the importance of data backup and how it is best accomplished.
- Learn how to create data backup policies, either individually or at organizational levels.
- Learn how to establish a schedule of regular data backups

Cloud storage considerations

Before choosing which type of cloud storage to apply, a few considerations that may help you determine the best option include:

1. Data sensitivity

How sensitive is your data? This encompasses identifying information that has to be secured and protected from unauthorized access or disclosure. This may include emails, documents forms, health data.

2. Types of cloud storage platforms

You may choose a particular cloud storage option depending on whether it's an open source platform or a proprietary one.

Open source cloud platforms are those where the copyright holder grants users the rights to use, study, change, and distribute the software to anyone and for any purpose e.g. next cloud. It is built using open source software and technologies.

Proprietary clouds are ones where a source code is hidden and only managed by the owner. There's usually a certain storage offered at no cost and a fee levied for one to use in case of an upgrade.
Examples include, icloud, Google drive, Dropbox.

Input

Safe data backup practices

Step 1: What is a data backup policy?
Step 2: Where might important data be found?
Step 3: Why or why not use the cloud?
Step 4: When should backups take place?
Step 5: Which backup type is best?

Safe data backup practices

Step 1: What is a Data Backup Policy?

While anti-virus, firewalls, encryption, and all the various steps we take to ensure the safety of our data are valuable and fantastic ideas, it's still not a question of if you are going to lose data, but rather a question of when. There are simply too many variables at play that could cause things to go wrong.
Preparing for "the worst" is just as important as defending against it; that is to say, you need to have a data backup policy as part of your own security plan. But what might a backup policy look like? What are its dimensions?
The first step to crafting an effective a backup policy is getting a sense of what data you have, and where it is. The Data Backup Matrix Activity & Discussion is one way of doing this; however, another way would be by making a list of the different kinds of data you maintain and where you store each kind.

Step 2: Where Might Important Data Be Found?

Essentially, a backup means having your information stored in at least two locations. Elicit or share some of the ways that different kinds of (digital and physical) information can be backed up:
- Electronic documents can be backed up using software such as Cobian Backup.
- Program databases can be backed up in the same way, once you have determined their location.
- Email this can be backed up using an email client like Thunderbird.
- Mobile phones will usually come with software installed on a phone.
- Printed documents these should be scanned and backed up as electronic documents where possible.

Where should we back up our digital documents? Elicit the possibilities, which should have already been covered in the Activity & Discussion:
- USB memory sticks & flash drives
- CDs/DVDs
- External hard drives
- Separate accounts with different passwords
- Remote Server(s)

Step 3: Why or Why Not Use the Cloud?

The topic of cloud-based storage solutions may very well arise during this session, which can kick off a discussion about the security of sensitive information on the cloud. Given both the popularity and array of options available for cloud storage services, this discussion on the advantages and disadvantages has been included as a separate step.

In general, using various cloud options to store sensitive data should be avoided if:
- Users can't get clear details on how a cloud service provider manages and handles their data, or;
- The information they do obtain about

a given cloud service make storing sensitive data there risky or unsafe.

Emphasize the need to have a physical distance between the devices storing master copies and backups of files. You may elicit examples for this, such as if there's a fire, natural disaster, office raid, etc.

Questions to ask during this discussion can include:
1. Can the cloud service provider or others access your data or read your information?
2. Is your data encrypted as you upload and download it? 3. What kind of encryption is used to store it?
4. If they do store it encrypted, do only you have the ability to decrypt the data, or does the company hosting it also have this ability?
5. If a cloud service provider can access your data and client software.

Step 4: When Should Backups Take Place?

When or how often one should backup their data depends on a number of personal and organizational dynamics; however, some questions to kick off this conversation and guide the decision-making process is:

1. How much data do I generate?
Depending on how much data you or your organization generates, you may need to backup more frequently. For example, an organization that generated up to 1TB of data a day cannot afford to wait a week to backup. Such an organization may have to explore an appropriate backup type **(see Step 5: Types of backup**)

2. How much work can I afford to lose and have to repeat?
It's also worth mentioning that some types of data may need to be backed up more frequently than others. Considering a layered approach could be useful, wherein all of your data is regularly backed up on a recurring basis, with more frequent backups taking place for certain more important or sensitive kinds of information in between the larger, overall organizational structures, or individual activities, may require a more tailored approach to regular data backup, it can regardless be a good practice to backup your important data at least once per week.

Step 5: Which Backup Type is Best?

There are four common backup types which are generally used in most back-up programs and protocols. A type of backup actually defines how data is copied from source to destination, and lays the groundwork for a data repository model (or, how the backup is stored and structured on the chosen medium or storage location).

Here below are basic explanations for each of the four common data backup types, which you may walk your participants through:

Full Backup
The starting point for all other types of backup, containing all the data in the selected folders and files. Because full backup stores all files and folders, frequently enacting full backups results in faster and simpler restore operations.

Differential Backup
This backup type contains all files that have changed since the last Full Back-up. The advantage of a differential backup is that it shortens restore time compared to a full backup or an incremental backup, as it works only with data that has been altered.

Incremental Backup
Stores all files that have changed since

the last Full or Differential, or previous Incremental Backup. The advantage of an incremental backup is that it takes the least time to complete. This can also make historical versions of your data available - OSX's Time Machine is an example of a popular Incremental Backup tool.

Mirror Backup
Identical to a full backup, with the exception that the files are not compressed in .zip files (as they might normally be) and they cannot be protected with a password. A mirror backup is most frequently used to create an exact, mirror-image copy of the source data.

Deepening

Learning how to back up you data

Before moving forward with a Deepening option (see Deepenings A and B below), either review or hand out the Backup Policy Form that includes definitions below - these are covered as well in both the Input section and the second page of the Backup Policy Form, but are useful for review nonetheless.

Deepening A: Backup tool hands-on session

Step 1: What, Where, Why, When, and Which

Begin this session by referring back to the What, Where, Why, When, and Which questions covered in the structure of the previous Input session on this topic:
1. What is a data backup policy?
2. Where might important data be found?
3. Why or why not use the cloud?
4. When should backups take place?
5. Which backup type is best?

These will be valuable framing questions as we look at the tool (or tools, if training on different tools for various operating systems) we'll be covering in the Deepening. It will be useful to take these questions into consideration, with participants configuring the chosen tool(s) according to the "answers" to these questions we've identified already.

Step 2: The Initial Backup

Have participants install or open whichever tool they'll be configuring for their device and/or operating system. Introduce them to the basic features, and demonstrate how to conduct a backup, remembering (due to timing) to start with backing up a sample file as opposed to an entire drive.

Give everyone enough time to make their first, test backup, and to get a feel for the interface and features. Once everyone has successfully made their first backup, review the various settings for the backup tool(s), and discuss the option of scheduling backups regularly. If there are other key features for the tool, review these now as well.
Explain that backups, especially for a very full hard drive, can take a substantial amount of time, so are best done when the computer is stationary for a long period of time (for laptops) in a safe place.

If participants are backing up data to external hard drives, they should also encrypt those drives. If encryption has already been covered with participants, trainers may wish to review what their options are for local disk encryption; if it has not, trainers should refer to backups (the same backups even) when leading a session on encryption.

Step 3: Backup Locations How Many Locations Should You Back-up To?

Discuss options for at least two backups, and how to design a backup policy and plan that has considered what the various "worst case scenarios" might be given their particular circumstances, such as:

- Office raids (by law enforcement or otherwise)
- Confiscation of devices
- Loss of password or access control (forgotten, departing staff, etc.)
- Natural disasters (floods, fire, earthquake, etc.)

Base your recommendations on the concerns raised by participants for their particular situations and environments. Mention that you'll be focusing on these also during the wrap-up for the session, to help solidify strategies for using the selected tool(s) for this session in the implementation of their backup policies.

Trainer's Note
Consider that for one or more particular data types (e.g., videos or photos) they may also need to have multiple backups in different locations, at least one of which is accessible without a network connection of some kind. Participants should be aware that hard drives can fail or be lost, and having only one backup can be risky in case something happens to that drive (especially for a large

Deepening B: Backup Policy Hands-on Session

If leading a backup policy hands-on session, either in supplement to or in place of a tool-focused session, there are a few different approaches trainers can take - below are included several such options:

Option 1
Go through each of the elements in a backup policy and the definitions involved, building off of the background established during the previous Input section. Depending on the group, you may want them to create either personal or organizational back-up policies, keeping in mind that sometimes an organizational policy might also include individual policies as well.

Have participants either:
1. Break up into small groups, to work on policies collaboratively - especially useful for organizational policies;
2. Work alone to start drafting a policy; however, if crafting individual policies, either collaborative or individual can be encouraged.

When participants regroup, trainers may choose to have them share and discuss what they've come up with (preferable); however, if time is short, wrapping up with questions during the Synthesis part of the module is another option.

Option 2
If you are limited for time, hand out the **Backup Policy Form** and list of definitions above. Ask them to work on it either after the workshop - be available to answer any questions they have, especially if the group will not be re-convening following this session.
If you do this, you should follow up remotely to ask how their Backup Policy is coming along, be encouraging and remind them of the benefits of backing up, and answer any questions they may have.
If participants are able to send encrypted attachments, the circumstances or context call for it, and there is sufficient trust between trainers and participants, trainers may also provide feedback directly to participants' drafted policies.

Check whether the information given during the session has been understood, by eliciting the information already taught. This can be done by eliciting a discussion with questions such as:

- Why is conducting backups useful and important?
- What is the cost and/or benefit of different approaches?
- Do you feel you can create a backup policy that works for you?
- If you didn't regularly do backup before now, why do you think that was a challenge?
- Do you think you will be doing backups from now on?
- What will you be doing differently?
- What will you back up?
- Where will you back it up?
- Where will you store the hardware?
- How often will you back up?

Synthesis

Synthesize this session by inviting participants to write up a backup policy to inform the discussion points below. Provide participants backup policy form to fill out, either alone, or in groups. They can keep this to themselves or share it with the group, if there is additional time to discuss what they've written.

Basic protection & privacy

Learning Objectives

Within this subtopic, the trainer should take note of the following:

- Highlighting to participants both the physical and the digital aspects of device and data protection.
- Reinforcing the importance of regularly backing up data to participants along with basic practices for doing so.
- Introducing fundamental concepts of encryption, as well as different types of encryption available to users.

This explores the relationship between physical and digital security, as it relates to the protection of both our devices and the data that they contain. The difference between the degree with which people tend to value their devices, versus the amount of time they spend on maintenance and care, is often quite wide - and many practices related to device safety are as related to physical security as they are to digital security.

- No risk to life safety.

555884
477772

Encryption

Introduction to Encryption

This introductory session will explain to participants the concept of encryption, as well as a brief overview of the different types of encryption available to users.

Part 1 – Have You Used Encryption Before?

Step 1: Explain that this is an introductory session for encryption as a concept, so you will not yet be going into great depth on any of the encryption tools that participants have likely heard about before (GPG/PGP in particular).

Step 2: Split participants up into pairs, and then start the session by demonstrating a few examples of encryption techniques. Here are a few examples that you can prepare ahead of time to share with the group:

The BLUEPRINTS Code

Each of the letters in the word "Blueprints" is assigned a number:

B L U E P R I N T S
0 1 2 3 4 5 6 7 8 9

This is a specific example using a specific word, but can be broadly applied to any number and letter sequence - for instance, if you use the same system as above, the sequence of numbers 8 2 5 7 9 would spell T U R N S when "decrypted". You could also switch the order of the numbers, so that instead of the above sequence, it now goes:

B L U E P R I N T S
9 8 7 6 5 4 3 2 1 0

In this instance, the sequence of numbers 8 2 5 7 9 would now spell L N P U B (which isn't a word) when "decrypted"; however, you could now "decrypt" the sequence 4 3 2 0 6 as R I N S E.

Old-Fashioned Text Messaging

Use an image of an older-style phone keypad (see below) to demonstrate another kind of "encryption" that participants may be familiar with:

Part 2 – Explaining Encryption

Step 6: Building on the common elements of encryption identified by participants in Part 1, you should now expand on some further basics and practices for the group:

- **Encryption Methods:** Take time to explain how encryption works, referring back to the examples from Part 1 as well as by showing a few example screenshots of what a GPG-encrypted email looks like. Highlight common implementations of encryption – in partic-

ular, spend time reviewing HTTPS, end-to-end encryption and GPG/PGP encryption.

• **Keys and Key-pairs:** Explain how encryption key-pairs work, and the algorithmic relationship between public and private keys. Go back through the example implementations previously mentioned (HTTPS, end-to-end and GPG/PGP) and explain for each of these where their respective keys are stored and/or visible to the user.

• **Encryption Practices:** Highlight some of the critical best practices associated with common implementations of encryption, such as fingerprint verification and key-signing. To demonstrate, ask participants to locate where within Signal one can verify another user's fingerprint; similarly, if participants already have GPG/PGP keys you can discuss the benefits and disadvantages of signing and distributing public keys. This is also a good time to discuss end-to-end encrypted messaging for chat apps such as Signal, Telegram and Whatsapp – remind participants that end-to-end encryption on some of these services is not always enabled by default.

• **Encrypted Backups:** Building off the GPG/PGP example above, ask participants whether they think it is a good idea to backup their GPG private key, and if so, how might they go about doing so?

Ask participants how they would use this keypad to spell different words – one example you could use would be to have each participant explain how they would use the keypad to spell their name.

For instance, a participant named Luisa would spell her named by typing the sequence 5 5 5 8 8 4 4 4 7 7 7 7 2.

Step 3: Once you've completed the above examples, ask participants if they have ever used other kinds of encryption – either like the above, or any other examples they can think of (e.g. a common instance of encryption used by many people every day is HTTPS).

Step 4: Close this part of the session by following-up with another question: What are the common elements they can identify from these different examples of encryption?

Step 5: Keep in mind that some email services such as Gmail have to be configured to allow the use of Thunderbird as a third party application.

Input

How to secure your computer

Part 1: introduction
Part 2: Physical environments & Maintenance
Part 3: Software safety
Part 4: Data protection & privacy

How to secure your computer

Part 1 – Introduction

Step 1: Ask participants how much they value their computers - How useful or essential is it to their personal and work lives? How much information they store in their computers?

Step 2: Now ask them - How much time do they spend on maintenance of their equipment? The difference between the degree with which people tend to value their devices versus the amount of time they spend on maintenance and care is often quite wide. Explain to the group that this session will focus on basic practices for protecting devices.

Part 2 – Physical Environments and Maintenance

Step 3: Mention to the group that many practices related to device safety are in fact more related to physical security than digital security (this is a good way to reinforce the holistic focus of this curriculum). A good example of this is the importance of cleaning devices – to get rid of dirt or residue that might get inside – and to conduct regular physical inspections of equipment to identify any alterations or physical intrusion attempts. In that regard, you can recommend basic digital practices – like using a password to lock a device if they won't be in its immediate vicinity while it is switched on – as well as physical protections, such as using a keyboard protector or an anti-theft cable chain to prevent unwanted access or theft.

Make sure to note here how the most critical aspect of their devices' physical safety: awareness. Being aware of where a device is at any given moment – whether on their person, in the other room, or secured in another location – is essential!

Step 4: Ask each participant to recall the details of their workplace - Which physical risks are present? Is their computer exposed to being stolen? Are there any misplaced cables? Is it possible that their computer might be exposed to extreme heat, cold or moisture? These are other important awareness points – physical awareness isn't just about making sure an adversary doesn't get a hold of their device(s), but also about the potential damage that a device's immediate environment might present.

Part 3 - Software Safety

Step 5: Explain to participants the risks of using pirated software (high likelihood of downloading malware, can't regularly update in the same way as with licensed software, etc.); However, licensed software is also frequently quite expensive.

Osalt: http://www.osalt.com
Open a browser and navigate to Osalt – this is a website that presents free and

open source alternatives to many major licensed software platforms and suites (for example, using Ubuntu instead of Windows; LibreOffice instead of Microsoft Word; Inkscape instead of Adobe Illustrator).

TechSoup | http://www.techsoupglobal.org/network
Via TechSoup, human rights activists and their organizations may be eligible to receive free, or heavily discounted, versions of commercial software: users may look for official distributors among local ICT service providers and request for a non-profit or public sector license discount. A large distribution network for donated software is run by TechSoup - the link above contains a list of partners and the countries in which they operate.

Step 6: Explain to participants the importance of keeping all their software updated - first and foremost, it protects against security vulnerabilities. All software and updates should only be downloaded from trusted sources; for example, when updating Adobe Acrobat Reader, one should only use updates downloaded directly from Adobe, not third-party websites.

Step 7: Next, explain to participants the importance of having an anti-virus program on their computers - provide some background that can help demystify some of the common myths related to anti-virus, such as:

- "Using two or more anti-virus programs offers more protection."
- "Mac and Linux don't need anti-virus software because they can't get viruses."
- "It's perfectly safe to use a pirated version of anti-virus software."
- "Free anti-virus programs are not as safe or reliable as paid programs."
- "A physical firewall can be used to enhance security on the internet in offices of your organization."

Step 8: Share these, along with any others that participants share with you – then, discuss some basic safe practices for using anti-virus software and protecting against malware (see Input session "Malware and Other Malicious Software"). Some useful ones to highlight here, in case you haven't already covered them in the Malware & Viruses session in this module, are:

- Using the uBlock origin browser plug-in to avoid clicking on ads that might download malicious malware files onto their computer.
- Being aware of phishing attempts, suspicious links or attachments found within emails in particular, that appear to be sent from unknown accounts or from accounts that appear similar to those of trusted contacts.
- This is a good opportunity to mention firewalls – these offer an automated layer of protection in their computers. Share tools like Comodo Firewall, ZoneAlarm and Glasswire. Newer (licensed) versions of Windows and Mac OS also have robust firewalls already installed.

Part 4 - Data Protection and Backups

Step 9: Ask participants - How often do they backup their files? Share examples of best practices related to data backup, such as keeping the backup in a safe place that is separate from their computer, backing up their information on a frequent, regular basis and - depending on the information that is being backed up - to consider also encrypting the hard drive or storage media where data will be stored.

Step 10: Share with participants the backup format template below, and have them start filling it in individually. Explain to the group that this is a useful

way of creating a personal data backup policy – they can refer to this after the training, as a useful resource for keeping track of where their data is stored and how often that data should be backed up.

Backup Format Template highlighted in appendix (Table 2)

Step 11: Explain next that, although there are backup automation tools available such as Duplicati or Cobian, participants may find it easier to start doing their backups by manually dragging and dropping files to the backup storage media. This ultimately depends on the complexity or amount of data they have to manage – for the average user however, manual backups should be more than sufficient.

Step 12: To follow-up on secure data backups, re-visit briefly the concept of encryption for storage media. Explain to the participants what it means to do, and why encrypting their hard drives or storage media can be useful. VeraCrypt is a relatively popular utility for implementing file or disk encryption, and could be mentioned here as an option for participants to explore. On Linux there is the Duplicity application for performing automatic and encrypted backups.

Part 5 - Deleting Files and Recovering Them

Step 13: Read aloud the following statement:

From a purely technical perspective, there is no such thing as a delete function on your computer.

Ask the group what they think about this – Does this statement make sense? How can it be that there is no such thing as a 'Delete' function? Remind the participants that they can drag a file to the Recycle Bin on their computer desktop, and then empty the bin, but all this does is clear the icon, remove the file's name from a hidden index of everything on your computer, and then tell their operating system that the space can be used for something else.

Step 14: Ask the group - What do you think happens to the data that is 'deleted'? Until the operating system uses that newly free space, it will remain occupied by the contents of the deleted information, much like a filing cabinet that has had all its labels removed but still contains the original files.

Step 15: Now explain that because of how a computer manages this storage space for data, if they have the right software and act quickly enough, they can restore information deleted by accident; likewise, there are also tools available that can be used to permanently delete files (not just remove them from the file index until the space is occupied). Take this opportunity to present Eraser and/or Bleachbit as tools that can be used to delete files and Recuva as an option to recover deleted files.

Storage & Encryption

Part 1 – Data Backups and Planning

Step 1: Ask participants - How often do they backup their files? Share examples of best practices related to data backup, such as keeping the backup in a safe place that is separate from their computer, backing up their information on a frequent, regular basis and - depending on the information that is being backed up - to consider also encrypting the hard drive or storage media where data will be stored.

Step 2: Share with participants the backup format template below, and have them start filling it in individually. Explain to the group that this is a useful way of creating a personal data backup policy – they can refer to this after the training, as a useful resource for keeping track of where their data is stored and how often that data should be backed up.
(Table in appendix)

Part 2 – Storage and Backup Encryption

Step 3: Now that participants have filled out the backup format template, ask them to review the types of information (and their respective importance or value) on their lists again – as they do so, have them consider what might happen if that information were to fall into the hands of an adversary, or if they were to lose that information entirely. What kind of impact would this have on them personally or on their organization?

Step 4: Now, introduce the concept of encryption to the group – explain that they likely encounter encryption quite often in their daily routines, as it is used in different ways across different tools and platforms. You can share, for instance, that HTTPS is itself a form of encryption for data "in transit" (data en route from point A to point B) whereas in this session, you will be discussing encryption for data "at rest" (data that is being stored in one location).

Step 5: Remind participants about how they were asked to download either Veracrypt or LUKS onto their computers. Give participants time to install and test out these tools, using external storage media (such as USB drives) and dummy files that they have prepared specifically for this session. Especially for beginner level participants, it is not advisable to do a full-disk encrypt of a computer hard drive just yet - you don't want to run the risk of a participant accidentally losing access to any of their data during the training!

Ask participants if they have questions before completing the session.

Answer any questions that were tabled during the session to be answered later - exclude any issues that require one-on-one assistance or explanation, to be addressed independently from the group.

You may also wish to ask specific questions to make sure some concepts are clearly understood.

Ask participants what was the most useful or interesting thing that they learned during this session.

Remind participants the importance of keeping there devices and applications updated.

Participants should consider analyzing the amount of data they produce so as to inform an effective backup policy.

Synthesis

Trainers use this wrap-up session for informal questions to the group, reviewing the material that has been covered in the module.

Safer browsing: A. Anonymity and Circumvention

Learning Objectives

Within this subtopic, the trainer should take note of the following:

- Understand how Internet censorship works, and at what levels it can occur.
- Understand what Anonymity is and isn't, as well as what it provides users.
- Likewise, understand what Circumvention is and isn't, and how it's different from Anonymity.
- Understand the difference between a Proxy, a VPN, and an Anonymizing Proxy (such as Tor).
- How to access blocked content, and prevent websites you visit from knowing your location.

Additional Resources:

- Electronic Frontier Foundation's resource on using **Tor vs. HTTPS**
- MIT's video resource on **How Tor Works**
- **VPN Tutorial** from Google Privacy
- **https://myshadow.org/ckeditor_assets/attachments/189/datadetoxkit_optimized_01.pdf**
- **https://myshadow.org/train**
- **https://myshadow.org/how-to-increase-your-privacy-on-firefox**
- **https://securityinabox.org/en/guide/firefox/linux/**

Offline Circumvention

This Activity and Discussion will outline how internet proxies work to disguise IP addresses, moving through three different scenarios: traffic routed over HTTP, traffic routed through a VPN, and traffic routed over the Tor network.

Step 1: Browsing Without Circumvention
Step 2: Browsing With a VPN
Step 3: Browsing With the Tor Network

Browsing without circumvention

Step 1: Browsing Without Circumvention
Have participants gather in a U-shape, a circle, or any suitable shape that permits them to still be able to see everyone else in the room. Hand each participant a numbered post-it to wear on their shirt. Assign someone to be a Sender of a message and a Recipient:
• E.g.: Trainee A is Sender, Trainee B is Recipient;
• E.g.: Trainer is Sender, Trainee A is Recipient
With a pen or marker, write the name of the Recipient on the piece of paper and hand this to the next person in line. Ask them to hand it on down the line until the paper reaches the Recipient:

• At this point, explain that this is typically how we reach websites. Our PC connects to something nearby, perhaps to a WiFi hotspot, and then to our service provider, and then to many other players in a chain.
• All of these learn what website we want to visit thanks to information we provide when we open our browser and type an address, or click on a link.
• If someone - say, our service provider, does not want us to visit a website, they can stop us by looking at our request.

Step 2: Browsing With a VPN
Using the same piece of paper again, place it inside one of the small envelopes (representing a VPN) and write the number of a participant who is in the middle of the 'chain'. Hand the envelope to the person closest to you and ask them to "send" the message down to the person with the number you have chosen (the person should be several "steps" away).
• When the envelope arrives at the person with the number you have chosen, ask that person to open the envelope. When they see the name of the Recipient, they should then pass the message along.
• Have the Recipient open the envelope and read what's in it; trainer(s) should provide extra explanations as needed.
• At this point, explain that this is how a VPN can help us to reach websites that otherwise may be blocked. When we use a VPN, our PC visits the location of the unblocked VPN instead of the website.
• Our 'real' request is protected until it reaches the VPN, and the VPN can pass our request along.

Explain that a VPN is like a "tunnel" with an exit point, and that exit point is usually a server at a point where the pages are being requested.

• The VPN you're using knows what you're requesting, as well as the sites delivering your requests Online.
• Send down papers with a variety of types of data and protocols down the line in the VPN envelope, in order to illustrate the difference between a VPN and having an HTTP connection to a

website in a browser (for example, an HTTP request; a PGP/GPG-encrypted email; an IM message).
• Try to use protocols and data types that your participants are likely to already be familiar with at this point in the training.

Step 3: Browsing With the Tor Network
Place the piece of paper inside one of the small envelopes and, picking at random, write the number of one of the participants on the outside. Place the small envelope inside the medium envelope, this time writing the number of a different participant on the outside.

• Repeat with the large envelope: place the medium sized envelope inside the large one and write a third participant's number on the outside.
• As in the previous demonstrations, "send" the message down the line.

When the large envelope reaches the participant holding the correct number, ask that person to open only the large envelope and call out the number they see on the medium envelope. Before they pass the envelope on, ask them:

• Who sent the large envelope? (Answer: You);
• Then ask: Who is my final recipient? (Answer: They do not know);
• Thank them and ask them to continue sending the medium envelope along the line.
When the medium envelope reaches the next participant, ask them to open only the medium envelope and call out the number they see on the small envelope inside. Before they pass the envelope on, ask them:

• Who sent the medium envelope? (Answer: The previous participant);
• Then ask: Who is (the previous participant's) final recipient? (Answer: They do not know).
• Thank them and ask them to continue sending the small envelope along the line.

When the small envelope reaches the next participant, ask that person to open it. Before they pass the piece of paper to its final destination, ask them:

• Who sent the message? (Answer: The previous participant);
• Then ask: Who is (the previously participant)'s final recipient? (Answer: Now, they know);
• Thank them and ask them to continue sending the message

At this point, explain that this is a very simplified representation of how the Tor network can help us reach blocked websites while also making it difficult for people on the Internet to determine where we are located.

Discussion

Leading the Discussion

Ask participants to describe their observations about how the message was sent in each demonstration.

- How was the VPN demonstration different from the first one?
- How was it different from using Tor?

Participants may observe issues like: having to know where final recipient is, but path can be random and non-sequential; at any point along the journey of the message being sent the message could be seen; etc.

- Did this show participants anything they didn't know about the Internet?
- Are there examples in which circumvention may be useful?

Explain that you will begin by describing a typical Internet transaction or, if you've already offered a general session on how the internet works using the We Are The Internet, then a brief review should suffice. After that, you will address how requests for certain content can be blocked; then, you will explain how to bypass Internet censorship using proxies and other tools.

Input

How Censorship and Circumvention Work

Many tools and strategies to circumvent Internet restrictions are in existence today. However, some tools offer more security features than others, and may be better for your unique needs for security than others. Thus, it's important to know the difference between the most common types of circumvention technologies.

How Censorship and Circumvention Work

Step 1: How the Internet is Supposed to Work

Explain that you will begin by describing a typical Internet transaction. We suggest using the whiteboard to draw out the process by which a browser requests a webpage; however, if you prefer, you can show a favorite video, discuss a pre-made diagram, etc. Regardless, it is not uncommon for participants to have questions about this introductory material.
The example below starts with a computer on a local area network (LAN), but applies equally well to any Internet-connected device. If your training is focused on mobiles, you should probably use a smartphone in your example - you can either explain that the device is connecting through WiFi, or modify a few of the terms below to account for the differences between mobile data services (3G, Edge, GPRS, etc.) and traditional ISP connections.

Step 2: What's Happening on your Device (with a normal connection)

In this scenario, you are requesting a webpage with your browser. You click on a link and wait for the page to load. Meanwhile, your request is "routed" to the web-server that "hosts" the page you've requested. The server then sends you the content of that webpage, and your browser displays it for you.

Internet Protocol (IP) Addresses

Each Internet-connected device has a public IP address, assigned by its ISP, that it uses to send and receive data. This includes personal computers, Internet-connected smartphones, printers, game consoles, web-pages and Online services such as email providers and social networking sites.
• The ISPs that most people use hand out new public IP addresses from time to time (but they also maintain records of who had which address at any given moment).
• The ISPs that most *servers *use, on the other hand, assign public IP addresses for longer periods, which makes them easier to find.

That said, you will rarely request content using a server's IP address directly. Instead, your Web browser will typically ask a domain name service (DNS) server to look up the domain name of the URL in the link you clicked (say, level-up.cc) and translate it into a public IP address (say, 88.80.189.190). Your browser will then request the specific content you want (say, "leading-training/training-curriculum/input/circumvention") from the server at that public IP address.

Local Area Networks & Local IP Addresses

Most of the devices you will use directly, such as laptops and smartphones, have local IP addresses that are unreachable

from the public Internet. Devices on the same Local Area Network (LAN) frequently share the same public IP address.
• The router (sometimes called a gateway or an access point) in your home (or office, school, internet cafe, etc.) hands out local IP addresses, sends your devices' requests off to the Internet, and then manages the process of directing each response to the appropriate device.
• Your local IP addresses is a little bit like your name, as it appears on the first line of an envelope that someone has mailed to you. It is the rest of the address that allows the postal service to deliver your envelope to the right house. (After all, your delivery person wouldn't know what to do with a letter addressed simply to "Alice.")

Assuming you share a home with other people, however, your name becomes important once the envelope arrives at your door.

Your Internet Traffic

Depending on where you live and what type of Internet connection you have, both your request and the corresponding response will pass through a number of different computers along their respective "routes."
Internet traffic makes its way from one IP address to another as a series of "packets," which are small units of data that travel according to a physical path determined by the various routers they encounter along the way.
Different packets may travel along different routes even if they are part of the same request, response or data submission (such as a when you submit a Web search or an email message).

Routing

These routes will vary depending on where you live and where the webpage you're requesting is located, among other factors. Your request will typically pass through your local router, then on to your ISP. After that, things get a bit complicated.
Your local ISP can talk to other ISPs, any one of which might provide Internet connectivity for the server hosting the webpage at the IP address you have requested.
Most likely, your request will pass through several ISP networks before reaching its destination. And, if that server is located outside of your country, then your request might even pass through an undersea cable to a large ISP in another country.
It might then be routed through a number of smaller ISPs before arriving at the IP address you requested.
Assuming all goes according to plan, the server at that IP address will then answer your request by sending the specified webpage back to your public IP address (by way of one or more equally complex paths).
When it arrives at your local router, it will be forwarded to your local IP address, then (finally) displayed in your Web browser.

Step 3: When the Internet is Censored

Your access to information Online may be blocked for a variety of reasons. Parents and school administrators frequently try to control the material to which children are exposed; companies have regulations about acceptable use of the Internet in the workplace; countries pass laws and establish policies that not only criminalize the publication of certain content within their jurisdiction, but that prohibit access to similar content published elsewhere.
Increasingly, technical means are being used to enforce these controls.
Your employer might block requests to gaming sites and social media platforms from within the corporate firewall, and your government might

require that your ISP return a "Page not Found Error" in place of an opposition website or a podcast produced by independent media. Because governments, ISPs, and administrators of public and private access points can monitor at least some aspects of your Online activity, they can limit access to content they find objectionable.

Blocking and **Filtering** are the two terms most frequently used to describe the different mechanisms through which internet censorship takes place.

Blocking - Refers to the banning or blacklisting of certain web-pages, types of content, access channels, or protocols.
Filtering - Refers to the process of analyzing traffic data in order to determine whether or not it is attempting to access anything that has been banned or blacklisted.

Step 4: Where Internet Censorship Happens
Internet filtering usually takes place at one of five locations:

1. On the device you are using;
2. At the access point through which you are connecting to the Internet;
3. Somewhere within your ISP's network;
4. At the point where your Internet traffic leaves the country;
5. On the server from which you are requesting content.

A national censorship regime might have influence over any of these, though we typically focus on (3) and (4) when discussing state-level filtering.

Step 5: What's Happening on Your Device (over a "censored" connection)

Many computers in schools, libraries and Internet cafes (and even some in homes and businesses) contain software that directly prohibits requests for certain content. This sort of filtering is often associated with shared, publicly accessible devices or personal devices that are administered by someone in a position of authority (such as a parent or a corporate IT department).

At Public or Private Internet Access Points

There could be locally installed internet filtering software at your workplace, library, Internet cafe, etc. Technically, such software could be installed on any of the routers between you and the server you are trying to access, but we typically associate access point filtering with businesses, shared computers and publicly accessible (freely available or for-fee) Internet connections.

At ISP and Country Level

Your ISP, which naturally has the ability to see any direct requests you make Online, can implement filtering either by preventing your request from reaching its destination, or (less frequently) by preventing the response from reaching you.

- Some countries take a more hands-on approach, requiring that certain types of Internet traffic be routed through servers that are under the direct control of a particular government agency.
- This technique is sometimes applied specifically to requests for international content, as governments often take a more direct approach to the censorship of material that is hosted on servers located within their borders.

Many national filtering policies are implemented at the ISP level - in fact, many ISPs are government-owned and operated.
On the Server You're Attempting to

Access

Online services are sometimes "defaced," in order to prevent them from responding to requests for content, regardless of where those requests might be coming from.
•The most frequently used form of such 'defacing' is when a site is overloaded by denial of service (DoS) attacks, that weigh down a site's servers with 'fake' requests to the point that it cannot serve content to 'real' user requests.
•Such attacks can be carried out by anyone with access to the right software and a large enough network of computers (or who can afford to "rent" the necessary resources).

Finally, while we don't usually think of it as a "blocking" or "filtering," a service can prevent you from accessing its own content based on any number of things: your IP address, the country from which your request was sent, the preferred language specified by your browser, etc.

Step 6: How Internet Censorship Happens

Besides using legal or socio-cultural means to curtail access to particular types of information Online, the following are common technical methods used to prevent access to Online content.

Internet Protocol (IP) Address Blocking
Access to a particular IP address is denied. When information is sent over the Internet, it is broken up into a number of packets. In addition to the actual data being sent, each packet contains information about how to route the packet itself.
•This information contains both the IP address from which the packet was sent and that of its destination. Filtering software installed along the route taken by this packet can monitor for blocked IP addresses.
•If it recognizes a blocked IP address, it can replace the original packets with a request for an "access denied" page (or it can simply "drop" them).

If the target is on a "shared hosting" server (one of the more affordable ways to put up a website), then all sites on that server will be blocked. Similarly, IP blocking cannot be used to filter a particular video or Facebook profile.

Domain Name System (DNS) Filtering
If a DNS server is configured to filter content, it consults a "blacklist" of blocked domain names. When you enter a URL in a Web browser, the first thing the Web browser does is ask a DNS server to look up the domain name referenced in the URL and supply the corresponding IP address.
•When a browser requests the IP address for one of these 'blacklisted' domain names, the DNS server can give an answer that actually points to an "access denied" page, or it can give no answer at all.
•Because DNS traffic is rarely sent in a secure manner, even using an international

DNS server does not prevent this form of filtering, as your requests (and the corresponding responses) can be modified in transit.
DNS filtering has limitations similar to those of IP filtering, and also tends toward unintentional over-blocking.

Uniform Resource Locator (URL) Filtering
When requesting content over HTTP (versus encrypted HTTPS) the entire URL can be scanned for banned keywords. Regardless of the actual domain name or IP address you are trying to reach, filtering software can prevent access based on the presence of these key-

words.
• This technique may be used to block access to an entire domain, to one particular website on a "shared hosting" server, or to a specific piece of content such as a video or Twitter profile.
• Keyword filtering can be applied to more than just URLs. With the right infrastructure, an ISP or government can inspect all unencrypted packets and block those containing certain keywords.

This process is often called "deep packet inspection" and refers to the process of monitoring traffic and censoring requests for banned content by performing a "Deep inspection" of the content of individual data packets sent as part of a request.

Port Blocking
Servers listen on different numbered ports in order to provide different services. Ports are infrastructure within the larger communication framework of the internet, that serve as channels for different protocols or traffic types - each is referred to by a number.
One port (typically 465) might allow users to send emails securely, and another to receive them (993).
Another port is commonly used to communicate with HTTP websites (80), and yet another for encrypted Web traffic (443), etc.
These ports are generally consistent, so blacklisting a given port number will block a particular type of traffic, regardless of the actual server to which a request is being sent.

Portal Censorship
Major international Web platforms that serve content to people all over the world—such as Google's search engine, YouTube, Twitter and Facebook—have at times complied with requests from governments to remove certain content from their portals. This renders content invisible to people who do not know where else to find it. Unfortunately, censorship circumvention tools are generally unable to get around this sort of blocking.

Internet Shutdown
In extreme cases, such as during a popular uprising, some governments have been known to disable their citizens' access to the Internet entirely. Once again, there is little that traditional circumvention solutions can do to address this form of censorship. Fortunately, such blockades tend to be extremely unpopular, and are rarely left in place for long.

Step 7: Bypassing Censorship

To get around technical website filters, most circumvention tools simply ask a server in some other country to fetch blocked websites for them. This server is known as a proxy.
As long as the censorship software you are trying to bypass has not added your proxy to its blacklist, in addition to the blocked content itself, this technique works quite well.

That said, there are a few other considerations to keep in mind when choosing circumvention software.

Choosing a Proxy
Before choosing a proxy, it is important make sure that it meets the following criteria:

You must trust the provider.
While the ISP may not be able to see the full scope of your internet activity when you use a proxy, whoever is running the proxy server can.
Because you are relying on this server to relay your requests to the desired website (and deliver its responses back

to you), it is important that you trust the tool provider to not submit your Internet activity to a third party. The proxy provider's Terms of Service or Privacy Policy might be a good place to start.

It should provide an encrypted connection for your traffic.
When you use a tool to proxy your Internet traffic, it is important that your connection to the proxy server be encrypted. In addition, you must ensure that the connection between your proxy server and the destination site is also encrypted.
This assumes that you are requesting content from a secure server, such as an HTTPS website; not all website-based proxies provide this level of security.

It should provide an encrypted connection for other sensitive data.
Furthermore, even a website-based proxy that does encrypt both ends of the proxied connection may itself be able to access your sensitive content, including your passwords.
This generally presents an unacceptable risk, so you are almost certainly better off using a technology that is known to provide a single, encrypted tunnel all the way from your device, through one or more proxies, to the content you are trying to access. Examples include VPNs and Tor, as discussed below.

Types of Proxies

1. Virtual Private Networks (VPNs)
VPN software, which you may have to install on your PC or mobile device, provides a secure tunnel between you and a VPN server on the Internet. All of your Internet traffic will be sent through that tunnel before being routed to its destination.

As long as your VPN server is located somewhere that is not subject to filtering, this will allow you to access blocked content. Trust is still important, as your VPN provider could easily maintain a list of the websites you visit, but at least they will not be able to access the traffic send to (or receive from) encrypted services like HTTPS websites.
Important Points to Highlight for VPNs:

- As with all proxies, your connection is not fully secure unless you are visiting a secure service, such as an HTTPS-encrypted website.
- Your connection is not anonymous - your VPN service can see and record what you are requesting.

2. Anonymizing Proxies
Anonymity networks typically "bounce" your Internet traffic between various secure proxies in order to disguise where you are coming from and what you are trying to access.

Tor is the most well tested and widely used anonymizing proxy network. By tunneling your traffic through a randomly selected series of encrypted relays, Tor offers a secure, reliable, publicly accessible means of circumvention that saves you from having to worry quite so much about the extent to which you trust your ISP, the organization that runs your proxy servers, or the filtered websites themselves.

Important Points to Highlight for Anonymizing Proxies include:
- You must still ensure that you have an encrypted, HTTPS connection to a secure website before exchanging sensitive information, even if you are using Tor.
- Unfortunately, in countries where Internet speeds are slow to begin with, some users find that Tor has a significant impact on the performance of complex websites and other Internet services.

Deepening

Using the Tor browser bundle

In this Deepening session, participants will learn how to use the Tor Browser Bundle for anonymity and circumvention, to conduct safer browsing actions while accessing sensitive or blocked content Online. Participants will use the Tor Browser Bundle to create an anonymous connection, confirm that it is working, and change their Tor exit relay.

Step 1: Public IP Address of the Training Site
Step 2: Public IP address of the Tor exit relay
Step 3: Selecting a new path through the Tor
Step 4: Replicate the process with participants

Using the Tor browser bundle

Step 1: Public IP Address of the Training Site

In a browser, visit either What Is My IP? Or What Is My IP Address, which includes a map to show perceived location.

- Explain the concept of sites like these, which is to show users by which IP address their device and its current location are being identified - in the case of this step, the location indicated on either website should align with the actual location of your training.
- Invite participants to visit the site themselves, using their own devices. Unless any of the participants are using VPN clients or any other kind of proxy tool, the IP Address and location for everybody should appear to be the same.

Step 2: Public IP Address of the Tor Exit Relay

Demonstrating for the group, close all web browsers and launch the Tor Browser Bundle, either by running "Start Tor Browser.exe" or clicking on a desktop/toolbar icon, and then clicking "Connect".

Wait until a Tor connection is established and a new browser window has opened - note that this could take several minutes. Tor Browser should load a page that says: "Congratulations. This browser is configured to use Tor." If for some reason your Tor connection fails, it will say: "Something Went Wrong! Tor is not working in this browser."

Using the Tor Browser window, again visit either What Is My IP? Or What Is My IP Address and show how the IP Address detected has now changed, and if using What Is My IP Address, point out the changed geographic location on the map.

Step 3: Selecting a New Path through the Tor Network

Explain that Tor could conceivably select an Exit Relay in the same country as the user. Define for participants that an Exit Relay is the Tor server from which one's outgoing traffic leaves the Tor network, and through which one's incoming traffic enters it. This is not good for anonymity - it is also one reason why a Tor Browser user might want to select a new exit relay. This can be done by clicking on the green onion icon to the left of the browser's address field and clicking "New Identity".

Request a new identity, then refresh the webpage for What Is My IP? What Is My IP Address. Note that the IP address should have now changed, and highlight this to participants.

Step 4: Replicate the Process with Participants
Once participants have in turn downloaded and installed the Tor

Risk classification

Browser bundle (either before the workshop, or during time allotted during this session) ask them to repeat this exercise themselves on their own devices, until they demonstrate that they can use the Tor Browser Bundle successfully. Then, explain the following:

- Though Tor encrypts your traffic on its way to the first Tor Relay, and while it travels through the Tor network, it cannot automatically encrypt your connection between the Exit Relay and the website you are visiting.
- Therefore, if you are visiting a site that does not support HTTPS, the Exit Relay operator (who could be anybody) can potentially see everything you send and receive. They might not know who you are, unless there are hints in the traffic itself (which is not uncommon), but they can see everything else.
- So, it is still important to use secured HTTPS web services, even while using the Tor Browser or otherwise connecting to the Tor Network.

Trainer's Note
Here, you might want to use this **visualization from Electronic Frontier Foundation** on Tor and HTTPS traffic (see resources).

Step 5: What the Tor Browser Bundle Can and Cannot Do

In order to take advantage of Tor's anonymity and circumvention properties, you must launch the Tor Browser Bundle and use the browser client that comes packaged with it - this is special version of Firefox that is specifically configured to relay traffic via the Tor Network.

- Other installed browsers, such as Google Chrome, regular Firefox, or Internet Explorer, will not automatically use the Tor network.
- Explain that unlike with a VPN, non-browser Internet traffic such as that from email clients like Thunderbird and Outlook, or instant messaging programs like Pidgin and Adium, will not benefit from Tor's anonymity or circumvention properties.
- When using Tor Browser, you might want to visit **check.torproject.org** and verify that Tor is indeed functioning as you might expect it to.

Trainer's Note
As with all security software, it is important that you use the **latest version** of the Tor Browser Bundle. When Tor Browser opens, the page it displays will tell you if a newer version is available; however, it will not update itself automatically. Any updates will have to be done manually by the user - see the **Safer Software Updating module** here on LevelUp for supporting training material on this topic.

Ask participants if they have questions before completing the session:
• Answer any questions that were tabled during the session to be answered later - exclude any issues that require one-on-one assistance or explanation, to be addressed independently from the group.

You may also wish to ask specific questions to make sure some concepts are clearly understood:

- Ask participants what was the most useful or interesting thing that they learned during this session.
- Can they describe the difference between circumvention and anonymity?
- Can they describe what a proxy is?
- Can they distinguish between the tools mentioned (or trained on during the Deepening section)? [For example, between a VPN and Tor?]
- Is HTTPS/SSL still important if you use a circumvention tool? Why?
- When would they consider using any of the tools mentioned or covered during this session?

Remind participants the importance of keeping these tools (as with everything else, such as operating systems) up to date.

Synthesis

Trainers use this wrap-up session for informal questions to the group, reviewing the material that has been covered in the module.

Safer browsing: B. HTTPS and SSL

This subtopic illustrates one of the most common Internet encryption protocols - secured HTTPS connections between users and websites using the Secure Socket Layer (SSL) protocol. Trainers may wish to confirm however, when preparing for in-class demonstrations, that they are not directing participants to visit websites that have been banned.

Learning Goals for Participants

At the conclusion of this subtopic, the participants should ideally:
- Learn the difference between unprotected (HTTP) and protected (HTTPS) traffic.
- Learn what kinds of information can be exposed in both cases.
- Learn to spot a secure SSL connection in a Web browser.
- Learn to install and use HTTPS Everywhere.

How Does the Internet Work?

This session builds basic understanding of information flows across the Internet, and the different vulnerabilities and related good security practices at each point in the chain.

Definitions

HTTP: Hyper Text Transfer Protocol. It is the way that a web server communicates information to your browser.

HTTPS: Secure Hyper Text Transfer Protocol. It uses a strong encryption system called SSL (Secure Sockets Layer) to create a special encoded connection between your computer and the web server that no one can see inside. HTTPS preserves confidentiality.

Man-in-the-Middle attack (MITM): Where a malicious individual intercepts your communications and pretends to be your intended destination. This individual will see all your traffic before handing it off to your intended target. MITM spoofs an authentic website in order to violate your confidentiality.

SSL Certificate: A special type of file that a computer like a web server can use to identify itself uniquely. Certificates can be issued by "Certificate Authorities" which are a strong proof that a web server is in fact who it says it is. "Self-signed certificate" are those certificates which are verified by the entity who owns the web address. SSL certificates establish authenticity.

Certificate Error: A certificate error is when your browser detects some sort of problem in the certificate identifying a web site; this can indicate that the server is not who it says it is. Certificate errors indicate a website is inauthentic.

"SSL Pinning": A term for certificates your browser trusts in advance without needing to ask a Certificate Authority for its validity.

Activity

Part 1 - How the Internet Works (Flow of Information and Points of Vulnerability)

Part 2 - Vulnerabilities

Part 3 - Good Practices for Digital Security

How the internet works

Part 1 - How the Internet Works – Flow of Information and Points of Vulnerability

Step 1: This part of the workshop will begin as a game. Participants will be given pieces of paper representing one part of the chain of the flow of information Online (modem, computer, ISP building, etc) and will be asked to arrange themselves in the order they consider is correct to represent the way an email travels through the Internet to reach another computer.

Step 2: Once the group is arranged, the facilitators will correct any mistakes, and will do a run-through explaining the process to everyone. Then a volunteer will be asked to repeat that explanation. It is recommended that the complete explanation is made at least three times; but, to give variety to this exercise, the facilitator can change the email illustrations that are used, and the extreme where the demonstration begins. The trainer must also give some time to clarify doubts related to this process.

Step 3: You can also use a video like this one (https://www.youtube.com/watch?v=7_LPdttKXPc) to help participants identify any mistakes that they have in the way they arranged themselves.

Optional: To adapt this for larger groups - rather than giving out one piece per person, assign one piece to a pair; for smaller groups, they can place the pieces on the floor, debating their order.

Part 2 - Vulnerabilities

Step 4: When the previous process has been completed, participants will be asked to paste each piece on a long paper (from a roll) that will be left on the floor. At this point, the facilitators will go through the chain again, this time to point out and explain the vulnerabilities at each stage (and hint at good practices to keep participants calm and confident).

Step 5: Some of the vulnerabilities are mentioned next. You can also add any other practice or threat that is applicable in your own context or that is relevant to mention to the participants. You can also share a few examples of practices that other collectives you work with have to help participants think of what might be some of their own good or bad practices.

- Device 1 (computer/phone): Physical insecurity; loss of information
- Modem 1: WiFi sniffing; lack of encryption
- Telephone pole/optic fiber underground: N/A
- Internet Service Provider: Data and metadata requests from local/national governments
- Google Servers: International surveillance; password insecurity and phishing, requests from national governments
- Telephone pole/optic fiber underground 2: N/A
- Modem 2: Security problems using other people's connections (like at Internet cafes)
- Device 2: Malicious software; insecure deletion

Part 3 - Good Practices for Digital Security

Step 6: After focusing on vulnerabilities, it will be time to break the group into smaller ones that can "adopt" one of the vulnerabilities discussed in the previous exercise and propose creative solutions for it. To make it less overwhelming for less experienced participants, each group will be given a piece of paper including one solution proposal that can ignite conversation.

Step 7: At the end, the groups will be given 30 seconds to a minute to present their ideas to the rest of the group (while one of the facilitators takes notes and makes additions to what is reported back by the groups). Facilitators will float around the groups giving brief explanations and answering questions, and mostly promoting discussion among all the participants.

Step 8: It's important that, as this activity progresses, facilitators explain the basics of each solution. Also, depending on the level of interaction and speed of the workshop, it may not be possible to cover all the proposals.

Some of the ones that are consider most important to share are:

- Physical insecurity: reduce the exposition of devices in your organization to strangers
- Physical insecurity: use computer locks at your office and home
- Loss of information: keep a backup somewhere other than your office or home
- Loss of information: put someone in charge for everyone's backups in your organization
- WiFi sniffing: Take off all the signs displaying the password of your WiFi

- WiFi sniffing: Change the password of your WiFi every couple of weeks

- Lack of encryption: Go to a cryptoparty in your city/come to workshop X

- Lack of encryption: Read Security in a Box on encryption

- Data and metadata requests from local/national governments: Work with digital rights organizations to find out ways to protect yourself legally

- Data and metadata requests from local/national governments: Find out what laws in your country say about the intervention of communications

- International surveillance: Switch to secure services for search, mail, hosting and communications in general
- Password insecurity: use long and complex passwords!

- Password insecurity: use KeePass to remember the many passwords you should have

- Phishing: Think before you click (be mindful of where you put your login information)

- Using other people's WiFi: Always log out

- Using other people's WiFi: Tell us – what should you not be checking when you're on someone else's WiFi?

- Malicious software: install anti-virus software and run it manually every week

Discussion

Part 4 - Leading the Discussion

Step 9: The point of this part of the session is to gather questions that are related to digital security but maybe haven't come up until now in the workshop, as well as discuss topics relevant to the participants' specific community. It's a good time to provide resources for everyone to learn more and stay updated. The facilitator will gather questions of the audience, hint potential answers, and mention references that can be used to answer them.

Input

How the Internet Handles Authenticity and Confidentiality

In this Input session, participants are introduced to HTTPS and SSL connections and how they maintain confidentiality between a user and a server over a network connection.
The purpose of this session is emphasize the importance of HTTPS/SSL because of its ability to reliably authenticate and maintain confidentiality when a user communicates with a website.

Risk classification

Step 1: What's the Worst that Could Happen?

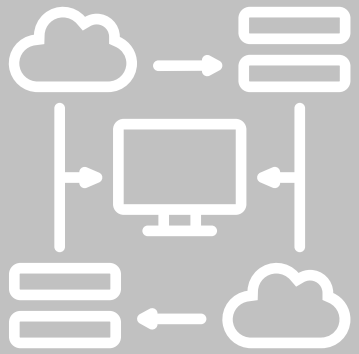
What happens when a connection is not confidential?
•Someone can capture, search and read all of the text and images on all of web-pages you get from websites.
•Someone can capture, search and read all of the text and images that you upload and send to websites.

What happens when the website you're visiting is not authenticated?
•A malicious person could intercept your encrypted web traffic by masquerading as a trusted server.
So what's the worst that could happen?
•Someone could passively or actively collect, read, publish or sell information contained in or attached to all of your sent and received emails if you're connecting with HTTP.
•Someone could passively or actively collect your passwords and account information sent via HTTP, use them now or later to "pwn" your account, download your personal information (or that of your contacts), attempt to pwn your other accounts, sell your account information and data Online.
•Someone could masquerade as HTTPS-protected website and trick you into sharing sensitive information.

Step 2: Some Real-World Scenarios
1. Using a public access point or an Internet café, you log into a web service that is not protected by HTTPS. Someone on the same network is running Wireshark and sees your username and password as they travel up to the website. The hacker takes the opportunity to log in as you, changing your password and pwning your account.
2. Your email service provider encrypts your login using SSL (HTTPS), but removes that protection after you have logged in. Government authorities have tapped into the connection at your local service provider or elsewhere, capturing all the traffic and can read the messages you write or receive. The NSA's XKeyscore system is one example of massive network surveillance that scoops up Internet traffic for analysis.
3. You visit your bank's website using https://. As the page loads, you see a certificate error. This is unusual, but you decide to click through anyway and arrive on a page that appears to be authentic. You enter your login infor-

mation for your account. Later, however, you find out that a malicious organization was running a "man in the middle attack" to capture login credentials of users before sending them to the real bank site. With your information, they can now login to steal your money or they can sell your login details to criminals who will.

The purpose of this exercise is to illustrate how the HTTPS Everywhere plug-in can help protect user network connections. This tool directs a browser to use SSL connections over HTTPS, either when an SSL version of a website is available or when the website has been included in the pre-populated list that HTTPS Everywhere's developers update regularly.



Using HTTPS Everywhere

Step 1: HTTPS by Default

Explain that some websites always provide a protected SSL (HTTPS) connection; for instance, all Google services offer session-wide, or from log-in to log-out, secure HTTPS connections. Twitter also now has this protection by default, as does Facebook.

Sometimes, though, a website will have a SSL connection available, but it won't force users to connect via HTTPS - it's also not always obvious that a website offers HTTPS in the first place if it isn't forced.
To demonstrate, visit a website that provides both HTTP and HTTPS connections, but does not force that HTTPS protected connection - an illustrative and relatively well-known example is the Microsoft website:

- Visit the HTTP version of the site.
- In the URL bar, add "s" to "http://" to create an HTTPS connection; then, reload the page.
- Highlight the relevant icon - usually a small, locked padlock icon - that signals HTTPS is active.
- Remind participants that HTTPS connections are available on some websites, but not always automatically.

Mention immediately afterwards, if it has not yet been highlighted, that a browser add-on called HTTPS Everywhere can be useful in some of those cases!

Step 2: Installing HTTPS Everywhere
Go to **Electronic Frontier Foundation's**, the developer of HTTPS Everywhere, official website in order to then demonstrate to participants how to install the plug-in. Note that, in the case of using Chrome browser, users will be redirected to use the Chrome Web Store.
- After installing HTTPS Everywhere, return to Microsoft.com to continue the demonstration for users.
- Point out that the browser automatically visits the HTTPS version; if desired, also visit the site in another browser that does not have HTTPS installed to emphasize that only the browser with the extension has the added protection.

Then, ask participants to replicate these steps, downloading and installing HTTPS Everywhere on their browsers. Encourage them to test HTTPS with one or two of their favorite websites or news sources. Make a brief pass around the training area, confirming that participants have the add-on correctly installed.

Step 3: Additional Talking Points

As participants experiment with using HTTPS Everywhere themselves, take the opportunity to remind participants once more of the following key points:

- This tool directs a browser to use SSL connections over HTTPS, either when an SSL version of a website is available or when the website has been included in the pre-populated list that HTTPS Everywhere's developers update regularly.
- The SSL encryption protocol used by HTTPS, while quite strong and reliable in many cases, only encrypts the channel through which data is traveling and not the data itself.
- A helpful comparison to make is to that of a drinking straw - if a straw is clear, an observer can see what kind of liquid is passing through it; if it is opaque, the liquid cannot be seen.

- Which is secure: HTTP or HTTPS?

- Why is HTTPS important?

- If I am instant messaging my friend and the connection isn't protected, what could someone in the middle – like an employee at my service provider – see?

- If I use a secure connection, does it make me anonymous? (Answer: No, only the content of what send to or receive from a website is protected.)

- If I use a secure connection, can a website see what I'm doing on their site? (Answer: Yes. HTTPS protects our connections to websites, but – as was shown in Activity and Discussion #1, the website has access to what we're sending once it arrives.)

- How can I tell if I am connected to a site over an HTTPS connection? (Answer: The address should start with "HTTPS" and – if the browser has a lock icon, that icon should show the lock closed.)

- How can I tell if my mobile phone is using HTTPS? (Answer: EFF.org now supports a version of HTTPS Everywhere for the Firefox browser on Android. Also, mobile browsers let you type the address you wish to visit just as on a PC, so it's possible to explicitly request the HTTPS version of a site, if that protected connection is not automatic.)
- Is it ever okay to just use HTTP? Even just quickly? (Answer: It depends. J Often, you won't have a choice – not all websites support SLL connections. In those cases, you can decide for yourself whether you are comfortable sending information – such as posting on a blog, sending an instant message – without protection.)

Synthesis

A final wrap-up and closing session for participants, for the Safer Browsing - HTTPS and SSL module.
Ask participants if they have questions before completing the session. If time allows, refer to the essential questions listed in the Input section to see if the information has been understood. Some questions might include:

Safer Browsing: C. Identity Protection and Privacy

This subtopic, which expands on theme of safer browsing techniques, addresses questions of privacy Online and how informed use of web browsers and browser settings can help users to gain more control over their Online identities. This includes ways to reduce the amount of identifying information users leave behind when visiting websites, and available plug-ins and tools that support these techniques.

Learning Objectives

At the conclusion of this subtopic, the participants should ideally:

- Learn what browser cookies are and how they can be used to track users.
- Understand that web browsers leak additional information that can identify users.
- Discover what settings and plugins are available to make browser sessions more private.
- Explore the Tor Browser Bundle, HTTPS Everywhere, and other solutions for improved browsing privacy and security.
- Understand what Big data is and how your information is used.

Definitions

Browser
A web browser is software that navigates websites - Firefox and Chrome are examples.

Cookies
Designed to be a mechanism for websites to remember useful information about a user's current session on a website, their functionality can be over-extended to remember all kinds of information about users, across individual sessions and entire sites.

Plug-in
These are a kind of software designed to add functionality to an existing web browser. They are also referred to as browser "extensions" or "add-ons".

Data
Refers to any information that is retrieved, sent, stored or can be accessed using a web browser or plug-in software.

Content
Refers to the entire content of a web page, including the URL, text, images, and any hidden content.

Tracking
Also known as website visitor tracking (WVT), this is the monitoring of visitor behavior on a website - for example, page views, duration of visit, clicks, and referral sources. This can also extend across other sites, multiple sessions, and even long periods of time depending on how the tracking is done. Tracking for advertising purposes seeks to build user identity profiles (age, gender, race, income, location, etc.) in order to refine user targeting.

Definitions

Browser and Environment Characteristics
This includes information about a browser's software, including version, configuration and plugins. Additionally, this can extend to data on system fonts, installed applications, operating system, preferred languages, etc.

Account Information
Usernames, passwords and sometimes mobile numbers and other authentication information that is associated with a user's Online account with a given service, company, or other entity.

Browsing History
The detailed log of the websites you have visited and when, often maintained by a browser unless directed to do otherwise via configuring its settings.

GPS
Stands for Global Positioning System, which offers precise location information gathered by a global positioning system device - this is what powers the functionality of many websites, apps, and devices known as geo-location.

IP Address
Each Internet-connected device has a public IP address, assigned by its ISP, that it uses to request and receive data. Approximate geo-location and ISP information is implicit.

Activity

Secret friend

In this session, you will explain the concept of anonymity and lead participants through a hands-on practice that will sensitize them to its importance.

Part 1 – Introduction
Part 2 – Time to Play!
Part 3 – Closing Circle

Secret friend

Part 1 – Introduction

Step 1: In this exercise, each participant will share an entirely new identity for herself, which they will have prepared ahead of time – it must be completely made up and not based on a real person.

Step 2: Explain that in building this new identity, participants can exercise complete freedom: they can be women, or men, or even a place - whatever they come up with. The key here is to develop their new identity to the full extent possible – this means developing everything from their name and where they come from, to their work, family and even hobbies.

Part 2 – Time to Play!

Step 3: Once you've introduced the exercise, begin the next step by introducing briefly the concept of anonymity. Ask participants why they think anonymity could be important to the work that they do, as well as to their personal lives or relationships.

Once you've completed the introduction and overview of anonymity, the exercise itself should be facilitated using the following steps:

Step 4: Each participant must arrive to the exercise with an already well-defined to their work, family and even hobbies, etc. Before the exercise begins, have each participant share with you the name of their new identity so you can keep track (this will be important for the exercise).

Step 5: Everyone must write on a slip of paper the name they have chosen for their new identity. Collect each of the slips and place them in a bowl.

Step 6: Walk around the room and allow each participant to draw one name from the bowl - if they take their own identity, they should put it back and draw another slip of paper. The name that each participant draws will be their secret friend.

Step 7: Everybody should now take a few minutes to write their secret friend a letter describing (from the perspective of their own created identity) who they are, where they are from, what their hobbies or work are, etc.

Step 8: Once they have finished writing their letters, they will place them inside an envelope. The name of their secret friend should be written on the outside of the envelope. Make sure that participants aren't able to see each other as they write, to avoid giving away any details.

Step 9: Go around the room and collect each envelope – referring to your list of which identity corresponds to which participant, pass each letter back out to their intended concept of their new identity - everything from their name and where they come from, recipients (again, making sure that participants can't see the names written on any of the envelopes other than the one that is intended for them).

Step 10: One by one, invite each participant to the front of the room, where they will sit on a chair and put on a blindfold. They will then share the details of the letter they received, including the name of their secret friend.

Step 11: As each participant describes their letter, their secret friend should get up and sit in another chair that has been placed next to the volunteer.

Step 12: When each participant finishes describing their letter, ask her to guess who from among the other participants they think their secret friend is. Once they guess a name, remove the blindfold and tell them to look at who is sitting next to them to see if they guessed correctly.

Step 13: Continue the exercise, repeating the process above until all identities are discovered.

Part 3 – Closing Circle

Step 14: Once the exercise has completed, ask the group – did they guess correctly who their secret friend was? How were they able to guess, or what was their thought process for attempting to guess? How difficult was it for them?

Step 15: Close the exercise with a reflection on the importance of anonymity and being able to fully protect one's identity, but also how easy it can sometimes be for others to hide their true identities (as well as their intentions).

BIG DATA

Big Data is a collection of data that is being generated across the globe from Online platforms at an unprecedented rate. This data could be either structured, unstructured or semi-structured.

Structured data: Any data that can be stored, accessed and processed in the form of fixed format.

Unstructured data: Any data with unknown form or the structure is classified as unstructured data. In addition to the size being huge, unstructured data poses multiple challenges in terms of its processing for deriving value out of it.

Semi-structured data: Semi-structured data can contain both the forms of data. We can see semi-structured data as a structured in form but it is actually not defined

Discussion

Who Does Big Data Think I Am?

Advertising networks look for detailed information about who you are, from your age to your postal code and everything in between. This activity works best if participants are using their personal computers and the browser that they normally use day-to-day. Still, some might not have browser profiles - which is great for their privacy, but boring for this activity. Keep this in mind while planning your agenda.

Who does big data think i am?

Step 1: Bluekai Registry

On a demonstration PC, visit Bluekai Registry (http://www.bluekai.com/registry) to show participants what information Online advertisers are associating with your browser.
Digital security experts often don't have browser profiles! So, to demonstrate Bluekai, you might want to build a new profile. This is possible with a cookie editor plug-in for Chrome or Firefox, though be warned: it is potentially unsafe.

- Instruct participants to open a browser, and then go to Bluekai Registry to see what their Online profiles look like to advertisers.
- If participants use more than one browser, they may wish to test each one - let your participants spend time exploring the information that they're sharing.
- Participants won't need to know how cookies work before this activity – they will likely be alarmed enough as it is!

Before proceeding to the next step, you may want to take this opportunity to ask participants how accurate the information Bluekai shows them appears to be. Note that, if participants are using rented equipment or devices during the workshop, the profile information is likely to be blank or unrelated to their personal habits.

Step 2: Vortex
Introduce the video clip for Vortex - Rachel Law, the student behind Vortex, is a Parsons School of Design graduate who gained attention for her project which allows users to confuse websites by exposing, mining and manually tweaking profile information.
Vortex was also made into a Mine craft-like game, as a means of visualizing its purpose and functionality - the plugin remains a work in progress and might not be released to the public, but it is a great visual representation of how cookies work.

Trainer's Note
The video is a bit too short to fully describe everything that's going on with the Vortex plugin, and it might raise more questions than it answers. For an audience that is likely to be utterly confused by the Mine craft reference, stop the video at 2:39 - trainers can then go on to simply describe the second function of Vortex, which is to obtain cookies in order to edit them.

Leading the Discussion
Use this time to take questions and reactions to the activity. Then, break down Vortex and lead participants through a discussion of the activity and the implications of browser profiles:

Vortex does two things:
1. First, it allows friends to share and swap identities easily, privacy implications notwithstanding.

2. Second, it turns profile building into a game. Rather than eradicating one's profile entirely, the plugin lets you build a profile that gets you cheaper prices for goods sold Online.

Profiles are built in two ways:
1. First, Rachel remixed the game Mine craft to help people mine for cookies on popular sites.
2. Second, she included a cookie editor, which allows users to set the value of the cookie (e.g. White, Male, Aged 50, Retired; Asian, Female, Aged 22, Student; etc.)

So, who are you?
1. Increasingly, we use the Internet exclusively through the Web, spending most of our time "Online" by using a web browser. We're Online more and more each day.
2. This means that our web browsers accumulate a great deal of information about us.

Ultimately, this session is about…
What does your web browser say about you?
Who has access to that digital identity?
How can we take control over our digital identities?

Input

Anonymity
In this session, you will introduce participants to the concept of Online anonymity, along with relevant tools and practices that can help preserve this anonymity.

Safe browsing
This session provides an introduction to safe web browsing practices, including an overview of plug-ins and other utilities that can be used to create a safer browsing environment.

Anonymity

Part 1 – Introduction to Online Anonymity

Step 1: Start the session by asking participants – What does anonymity mean to them? After you've heard a few answers from the group, present the concept of anonymity in more detail to the group, explaining the following:

- Explain what the benefits of learning more about anonymity are, and why it can be relevant to human rights work.
- Provide examples to participants of Online data traces that could potentially identify somebody – these could include data such as a username, social media posts, devices used, locations, and other kinds of metadata;
- Talk about how anonymity can be applied in levels or layers, explaining to participants that they can anonymize either a single activity or connection, or an entire profile or user session.

Part 2 – Identifying Data and Preserving Anonymity

Step 2: In the previous part of the session, you discussed the different kinds of Online data traces that could potentially identify somebody. Now, you will highlight one that is especially relevant to an Online context – the IP address:

- What is an IP address? Explain to participants what it is, its purpose, and how in an Online context it can be an especially crucial piece of information (especially when attempting to navigate anonymously in Online spaces);
- To demonstrate some of the anonymity implications of IP addresses to the group, have them use a website like https://whatismyipaddress.com/ to find out their individual IP addresses, and how they reveal other kinds of potentially sensitive or identifying information.

Step 3: Now, you will present the following tools to participants and explain how each is important to preserving anonymity Online – note that each one provides anonymity in a different way or to a different level:

- Tor Browser: **https://www.torproject.org/download/download-easy.html.en**
- Virtual Private Network (VPN): **https://en.Wikipedia.org/wiki/Virtual_private_network**
- Tails (The Amnesiac Incognito Live System): **https://tails.boum.org/**
- HTTPS Everywhere: **https://www.eff.org/https-everywhere**

It is important to explain some of the key practices to consider to use each of the above tools safely, and to allow enough time for participants to install and practice using them.

Part 3 – Some Hands-On Practice

Step 4: Ask participants to check again their IP on https://whatismyipaddress.com/ - they should do this once while using a VPN, and a second time while using Tor Browser. Do they notice a difference in the IP address, or with anything else?

Step 5: This is a good opportunity to address another point of frequent confusion for users: Incognito Mode. Many times, users think they are browsing anonymously while using Incognito Mode on their browsers – here, you should ask participants to check their IP address while using only Incognito Mode (or its equivalent, depending on which browser they are using). What do they notice about their IP address now?

Safe browsing

Part 1 – Choosing a Browser

Step 1: Begin the session by asking participants which web browsers they use and what other options they have heard of. Present Firefox - explain the benefits of using it, and discuss briefly the difference between it and other common browsers such as Google Chrome or Internet Explorer.

Part 2 – Safer Browsing Practices

Step 2: There are quite a few safer browsing practices to discuss that can be shared with participants – while you don't need to cover every single one of them, it is recommended to share enough to give your participants options (also remember to keep your content contextualized by sharing practices most relevant to participant context).

Step 3: Explain to the group that you will be reviewing some safe browsing practices with them, but not yet focusing on specific tools other than the browsers themselves. Some participants might already be willing to change browsers, but others may not yet be – so before discussing more specific tools like browser plug-ins, it's important to keep the discussion grounded first in practice.
Here are some example practices you can discuss:

- Being vigilant of phishing and spear phishing attempts;
- Blocking embedded ads and pop-up ads;
- How cookies work – be sure to talk about how convenient they can be, but that they also have downsides;
- Disabling and erasing cookies from the browsers;
- Deleting browsing history;

Not saving passwords in your browser settings;

- Checking the extensions that you add to your browser;
- Enabling the Do Not Track option in your browser;
- Google search alternatives (such as Duck Duck Go)
- Who implements Online tracking and why? (Both https://trackography.org/ and https://www.mozilla.org/es-MX/lightbeam/ are good resources about this);
- Discuss HTTP versus HTTPS;
- What is a VPN (Virtual Private Network) and when should these be used?
- What exactly does Incognito Mode do, and when should it be used?
- Remove sensitive passwords stored in browsers (be careful not to remove stored passwords that you do not remember!).

Part 3 - Tools and Extensions for Safer Browsing

Step 4: Explain, now that you've addressed some basic practices for safer

browsing, that you can also suggest certain tools – specifically browser plug-ins – which can help automate or otherwise facilitate adoption of some of these practices.

Step 5: Present the following tools, explaining how each of them works, and remember to also share the links to download them with participants. It is essential that participants understand why each of the tools shared is important and useful; if not explained clearly, it can lead to participants making ill-informed decisions about their privacy or anonymity Online:

Desktop Browser Tools:

- No Script: https://noscript.net/
- Adblock Plus: https://adblockplus.org/es/
- Privacy Badger: https://www.eff.org/es/privacybadger
- HTTPS Everywhere: https://www.eff.org/https-everywhere
- Click & Clean: https://www.hotcleaner.com/
- Tor browser: https://www.torproject.org/download/download-easy.html.en
- uBlock Origin: https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/
- Disconnect: https://disconnect.me/
- uMartix: https://addons.mozilla.org/es/firefox/addon/umatrix/

Mobile Browser Tools:

- HTTPS Everywhere: https://www.eff.org/https-everywhere
- Avast: https://www.avast.com
- Orfox: https://guardianproject.info/apps/orfox/
- Orbot: https://www.torproject.org/docs/android.html.en
- Tor for iPhone: https://mike.tig.as/onionbrowser/

Part 4 - What Can Be Seen by Your Local Network Administrator?

Step 6: Explain that there is a lot of information available to those who manage a local network, internet service providers, or anyone else with some access to the network that is being used to connect. Examples of information visible in this case include metadata, packet content (via deep packet inspection), websites visited, patterns of browsing behavior, version of browser used, your operating system, and more!

Other Practices & Features:

Incognito Mode (InPrivate Mode)

This is a feature that frequently causes confusion as it is not well understood - participants might not have a clear understanding of how Incognito mode works as a browser feature, and when it is useful. Explain how Incognito (and similar) modes work, and offer some examples of when they can actually be helpful features to take advantage of.

Safe WiFi Practices

Finally, take some time to discuss, and if possible demonstrate, a few basic safe practices on for WiFi connections - this includes practices such as changing the default password of the modem, and showing participants how to monitor which devices are connected to their WiFi network.

Maintaining Privacy While Browsing the Web

In this session, participants learn that advertisers (and others) may know more about us than we think, due to the data that we produce when surfing the web.

Step 1: Defining Terms
As with many digital security topics, it's important to make sure everyone has a common language before moving forward. Definitions also indicate some of the risks and mitigations that you'll go into more detail later.
To avoid presenting the content solely as a lecture, and to get a better sense of your participants' knowledge, you can present this section by asking participants how they would define the following terms, then correct their definitions as needed (highlighted in the next page)

Step 2: What Does Your Browser Say About You?
Now that some key terminology has been defined it would be a good time to check in with the group, to see what they know about what is really going on behind the scenes when they browse the Web.
Set up some flip-chart paper and ask participants what kind of data is available to the websites they view. You can also add things they may have missed:

As a user, here is the various data that you create and potentially share each time you open your web browser:
- Browser characteristics
- Stored information: Any information you allow the browser to store such as passwords, addresses or credit card information
- Browsing history: all of the websites you have visited in the past
- Content: URL, text and images, and hidden content of past and current browsing
- Your precise, physical location
- IP address of the device being used to connect

Step 3: What Else Are We Sharing?
When you visit a website, your intention is to have confidential communication with the server that hosts the website – and only that server. You might also intend to share web-pages with social media when you click a button that says "like" or "share".

However, there are many hidden ways that you share your browsing data without your explicit consent.

Refer back to your notes on the type of data created while browsing. Connect and explain these vulnerabilities - the table below outlines some of the vulnerabilities and how they connect back to certain types of data. **(Illustrated in Table 3)**
At this point, you may wish to demonstrate some of these vulnerabilities by opening a browser and visiting Panopticlick and an IP query site such as What Is My IP.

Step 4: So, What Can We Do?
Because of the way web browsers are designed to work with website code to improve user experience, it is surprisingly difficult to protect our privacy. The diversity of this data we've mentioned, and the diversity of techniques that can be used to capture it, calls for a diversity of mitigation tactics. There are a variety of fixes for each kind of vulnerability.

Trainer's Note

The number of countries where the use of encryption is illegal has decreased, but legal concerns are still very real for some participants. Before a training, review the laws of where your participants live and work, as well as the laws of where you're conducting the training, to confirm that the use of technologies highlighted in this section and in Deepening sessions, including the Tor Browser Bundle, is allowed.

Tor browser bundle

Because browser fingerprinting is made easier by customizations to browser settings, the simplest solution is to use Tor Browser without additional plugins and using default configurations.
At this point, you may wish to demonstrate the benefit of using the Tor Browser Bundle.

Open the Tor Browser Bundle and re-visit Panopticlick and What Is My IP to illustrate that the browser is no longer leaking information.

This can also serve as a segue into the Deepening session for the Tor Browser Bundle. If using the Tor Browser, don't use other plugins or change the default settings to prevent unique browser fingerprinting!

HTTPS Everywhere

HTTPS (Secure Hyper Text Transfer Protocol) ensures that a connection between a user and a website is authenticated and confidential. It uses a strong encryption system called SSL (Secure Sockets Layer) to create a special encoded connection between a computer and the web server, into which nobody can see.
• It may also be worth noting here to participants that HTTPS only encrypts the channel through which data is traveling - not the data itself.

Some websites always provide a protected SSL (HTTPS) connection; for instance, Google services offer session-wide (from log-in to log-out) HTTPS. However, some websites will have a SSL connection available but won't force users to connect through it – it may very well not even be obvious that it's there.

• To demonstrate, visit a website that provides both an HTTP and HTTPS connection, but does not force that HTTPS protected connection. An illustrative and relatively recognizable example is Microsoft.com.

This can also serve as a segue into the Deepening session for HTTPS Everywhere.

Step 5: Other Solutions

Browser History
Advise participants that in order to prevent someone from reading their browser history, they can change their browser settings to not store browsing history, clear existing browsing history, or browse in an "incognito" tab or mode where history is not recorded.

Stored Information
Change your browser settings to never allow your browser to store sensitive information like passwords, addresses or credit card details. In Chrome, for instance, this setting is located under Settings -> Show advanced settings -> Passwords and Forms.

Do Not Track
Change your browser settings to enable "Do Not Track", in order to notify websites you don't want to be tracked for (strictly) advertising purposes. It's modeled after "do not call" lists for telemarketers in some countries.

Clear Cookies
Change your browser settings to clear cookies after you end a session, block cookies from specific websites or even disallow cookies completely. If you find that certain websites require your browser to accept a cookie in order to log into an account, you can give those sites permission just for your current session. In Firefox, for instance, this Exception list is located under Tools -> Options -> Privacy (tab) -> Exceptions.

GPS and Location Services
Turn off GPS capability on your mobile device, or restrict applications' access to this data.

Disable Certain Data Collection
Privacy Badger, developed by Electronic Frontier Foundation (EFF), is a browser plug-in that can be used to block user data from being sent to a number of known, third-party servers.

Disable JavaScript
Configuring browser settings to disable JavaScript from running on all sites by default can be accomplished through the use of one of several browser plug-ins.

JavaScript is a widely used protocol for generating web-based content, that can also gather potentially identifying information from users.

- The NoScript extension for Firefox
- The ScriptSafe extension in Chrome

Update Browsers
Keeping browser software up to date prevents malicious code embedded in websites from collecting data. See Safer Software Updating here on LevelUp for supporting training material on this topic.

Deepening

More Online identities

Part 1 – Connected Online Identities
Part 2 – Separating and Managing Online Identities

More Online identities

Part 1 – Connected Online Identities

Step 1: Begin the exercise by having participants make a list of any Online identities they have; you may also simply ask the group if anyone among them currently uses more than one Online identity. For any participants who indicate that they manage multiple Online identities, ask them if they would be comfortable sharing their reasons for doing so with the rest of group and what they use them for.

Step 2: Building off any examples shared by the group, explain that using multiple Online identities is not an uncommon practice among HRDs – offer some example scenarios:

- HRDs who use Facebook to manage Online campaigns, but don't want to use their personal profile or identity to administer the campaign's page;
- HRDs who conduct sensitive research Online, and want as few of the digital traces they leave behind to be traceable back to them;
- HRDs who have been documenting cases of government human rights abuses, and are planning to expose this information by publishing a major report or public statement.

Step 3: Now ask participants to gather in pairs and identify other circumstances under which it might be useful for them to create a new identity that is not linked to their personal one. Have them reflect on how much they combine their personal identities with their activism work:

- Do they mix their accounts? Do they mix their identities?
- How linked is their personal digital life with their activist life?

What are some Online activities that could put them at risk of exposing themselves if done using their real identities? Examples of this might include:

- Requesting information from government agencies;
- Visiting government websites to gather information to share Online;
- Managing the social media account(s) of their organization or collective);

Part 2 – Separating and Managing Online Identities

Step 4: Again building off the group reflections from the previous step, illustrate to the group three options for managing their Online identities:

- Creating an entirely new, fake Online identity;
- Creating separate personal and professional profile identities;
- Leaving their identity as it is now (not changing anything);

Step 5: Provide for each of the above options at least one real-life, relevant example and explain to participants what each of these options implies, for example:

• Creating an entirely new, fake Online identity will most likely require it to be completely disconnected from anything that could be related back to your real identity to be effective. This means creating new email addresses and social • Separating professional from personal identities may only require users to change privacy configurations on their accounts, either to limit the amount of information that is available publicly, or to specifically manage what level of information is visible to specific friends, followers or contacts; in other cases though, separating these identities could imply the need to maintain entirely separated set of profiles and accounts for each (meaning that a new set would need to be created for either the personal or professional identity).

• Leaving an identity as it is would likely only require users to change privacy configurations on their accounts, either to limit the amount of information that is available publicly, or to specifically manage what level of information is visible to specific friends, followers or contacts.

Step 6: Now, ask participants to discuss in their same pairs (from Step 3) what some of the pros and cons of each of these options could be, either in a general sense or specifically for themselves and their context. Among the issues that will likely arise during these discussions are those of practicality and credibility – be prepared to speak to those questions specifically when participants share some of their discussion takeaways with the group.

Part 3 – Hands-On Practice and Recommendations

Step 7: Explain to participants that they are welcome to choose any of the three options presented for the next part of the exercise (the steps below though will use the example of creating an entirely new identity).

Step 8: Give each participant 1-2 sheets of flip-chart paper and some markers, and ask them to start drafting characteristics of their new identity – some specific considerations for them to think about include:
• What is the name they would use? (Be aware that some social media platforms, notably Facebook and Google, can identify and take down accounts with fake names, so participants should think creatively);
• What would their interests and hobbies be?
• Where are they from and where do they live?
• What avatar or profile photo would they use?
• Could any of these details be traced back to their real identities?

Step 9: Once participants have drafted the details of their new profiles and identities, share with them some digital security recommendations that will help them avoid exposing their real identities:

• Using different machines or devices for each identity – similar to the above, this further compartmentalizes their different identities and separating activities, helping users avoid mistakes that could compromise a new identity. Participants could do this by using separate physical computers or phones, setting up a separate virtual machine on their laptops, or by using an alternative operating system like Tails (see the Deepening session "Let's Reset!" for more information);

• When setting up a new profile, and ideally when logging into the associated accounts in the future, participants should consider using a separate browser in incognito mode different from the one they primarily use for their current profiles – this will help them to avoid linking the accounts, or accidentally logging into one over the other and sharing information that could compro-

mise the separation of their identities. Consider though that even when using different browsers, the same IP address will be recorded by an ISP.

• Review general safe browsing habits with participants – you could build on this by talking about the concept of browser 'fingerprints', and the impact that could have on the separation of their identities (https://panopticlick.eff.org/static/browser-uniqueness.pdf); furthermore, you could also review how to obscure IP addresses that could potentially reveal location details;

• Participants should not follow anybody friends, family or their organization using their new identities – this could very quickly allow anyone looking closely enough to draw a connection between that identity and its real counterpart;

• Remind participants to be aware of metadata and how it could potentially reveal information about themselves. Review how metadata is created, and how they can erase it from their files before posting images or videos, or before sending files from their new identity accounts.

Now participants can begin creating the profiles and accounts for their new Online identities!

• https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual#Creating_and_managing_identities_online
• https://mat.boum.org/
• https://guardianproject.info/apps/obscuracam/
• https://securityinabox.org/en/lgbti-mena/metanull/windows/
• https://panopticlick.eff.org/static/browser-uniqueness.pdf

Refer to Using HTTPS Everywhere
Refer to Using Tor browser bundle

Useful questions:

Ask participants if they have questions before completing the session. If time allows, trainers may want to confirm that the participants understood the essential points. Some suggested questions:

- What was the most useful thing you learned from this session?
- If you wanted to explain to a friend what a browser cookie is, what would you say?
- Can you remember some of the things that our browsers may expose when we visit a website?
- What could you do to fix some of the leaks or vulnerabilities we talked about?
- Is there a situation in which you might not want to block cookies?

Synthesis

Identity Protection and Privacy
We recommend that trainers use this wrap-up session for informal questions to the group, reviewing the material that has been covered in the module.

A final review and question & answer session for techniques and tools for increased protection of identity and privacy while browsing the web.

6 Password Management

Introduction

Passwords are the first line of defence for information in any form. Data at rest (storage) and data in transit. Best password strength and other key practices evolve over time depending on behaviour and formation of various threats.

Objectives

During this module, the participants will gain an understanding of the following key topics:

- Provide information and guidance on account security;
- Explore the use and benefits of password managers;
- Outline common security issues;
- Creating passwords that are harder to guess and crack;
- How accounts are hacked and ways to reduce your risk; and
- Proper account and password management.

Tools required

Trainer

These tools will be necessary for the trainer to prepare before conducting the training.

Devices

- Laptop
- Smartphone
- Projector
- Internet access

Resources

- USB flash drive
- Suitable space
- Colored electric tape
- Hands-on guides
- Whiteboard
- Post-it notes (multiple colors)
- Markers (multiple colors)
- Flip-chart paper

Trainee

These tools will be necessary for the trainee to have during the training.

Devices

- Laptop
- Smartphone

Resources

Definitions

Password - A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Passphrase - A passphrase is a manipulated sequence of words or other text used to control access to a computer system, program, or data.

Password Manager - A password manager is a computer program that allows users to store, generate, and manage their passwords for local applications and Online services. Examples include; Last -Pass Keepassxc, One password, Google Password Manager, etc.

Hacking - Unauthorized access by a third party to a confidential/private computer system or account e.g. Brute force

Conducting the Activity

At the start of the exercise, the trainer explains that the purpose of the module is to understand the difference between strong and weak passwords, The trainer then:

- Asks participants to spend a few minutes coming up with passwords.
- Each participant then types their password into the 'how secure is my password' website.
- Ask participants to share the results displayed on the website

Resources:

- **Website:** https://howsecureismypassword.net OR https://www.experte.com/password-check OR www.haveibeenpwned.com.
- **Information:** The most commonly used passwords.
- **Projector or smartboard to present to the class.**

Activity

How secure is this password?

This activity invites participants to create various passwords to see which passwords are the most secure.

Useful questions:

1. What have you learnt from this activity?

2. Why do people not use good passwords?

3. What do you think is a good password?

Discussion

1. Compare their list against the most commonly used passwords.

2. Explain to the participants why it is important to avoid using a common password (include examples) by drawing on the background information.

Input

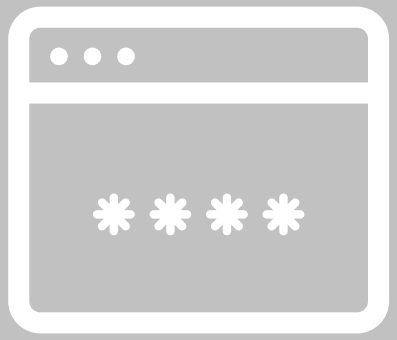
Time to put the common passwords to the test and see how long it would take them to be cracked! Launch https://howsecureismypassword.net OR https://www.experte.com/password-check, enter each password and see the result.

Begin to use increasingly complex passwords (length and variation of characters) and see how the time frame changes. In doing this, help the participants work out which numbers and symbols are easily exchangeable for letters. For example:

- Chocolate, chocolatemilkshake, Ch0c0l@t3, Ch0c0l@t3M1lksh@k3!

Deepening

Importance of passwords.
Impact of compromised passwords.
How passwords are commonly compromised.
Making stronger passwords.
Creating passphrases.
Common myths and misconceptions.



Password Basics

Why are Passwords Important?

Passwords provide access to a number of crucial important accounts such as email, banking accounts, social networking sites, etc.
These accounts often contain sensitive information, and also allow us to "be ourselves", permitting organic interaction with others using various digital services - this might entail sending a social networking message, sending an email, making an Online purchase, etc.
They may also allow us to impersonate others- anyone with access to an account password can, in effect, act Online as if they were the account owner.
Passwords also provide access to WiFi access points, mobile devices, computers, decrypting of devices, files and more.

What Can Happen if Your Password is Compromised?

Important information or files could be stolen (copied) or deleted; if they are stolen, you may or may not realize it immediately. This could be anything from sensitive documents and files, to address book contacts and email messages.
Money and other funds could be stolen or spent, via access to credit cards or bank accounts.
Email or social media accounts could be used to send spam, or to impersonate you, your friends, family, or colleagues.
Account access could be held in exchange for a form of "ransom" - this could include money, access to contacts, or access to other accounts.
Someone with a password could use this access to monitor communications and activities without your knowledge.
Access to your email could set off a "domino effect" where it is used to reset passwords to other accounts by requesting password reset links, eventually locking you out of several accounts if the password remains unchanged.

How Are Passwords Commonly Compromised?

When they are shared with others, or stored in an easily discoverable way - a commonly seen example is a computer login password written on a post-it note, and then stuck onto the same computer or nearby.
When someone witnesses a password being entered on your screen and writes it down, or remembers it.
Using an email client without SSL session-wide, only at the login page leaves passwords and other information vulnerable as they are visible by anyone with access to the connection after logging in.

Password Basics

A device is physically accessed, and passwords are obtained through “Save My Password” or “Remember Me” settings saved on websites via a browser - this is especially possible if full-disk encryption isn’t used on a device.
Malware, such as a keylogger which can document every keystroke on a device and send it to a waiting third-party, can reveal not just passwords but potentially a great deal more personal or sensitive information.

Secure Passwords

How Can We Make Our Passwords Stronger?

Most of the advice on passwords will have to do with the complexity of characters involved, and how to avoid a combination of words and letters that are easily guessed; however, equally crucial is the length of a password. No matter how complex a password is, if it's short, it can be guessed in a short period of time regardless of its complexity. Therefore - the longer, the better.

Length: We are often told that a password needs to have at least 8 characters, but 12 is a strongly suggested minimum, and 20 characters is even better.

Complexity: We are told to use a password that's alpha-numeric, using upper and lower cases, with special characters. This is one approach for creating a 12 character password.

Change Regularly: Regularly change your passwords, particularly for your most sensitive accounts. Definitely change them if you get an authenticated (not phishing) email telling you that a particular service has had user accounts and passwords compromised.

Think pass-phrase, not password! In the appropriate context, a helpful aid could be [this comic from XKCD] (https://xkcd.com/936/) on Password Strength, to illustrate the true strength of a passphrase versus password.

Creating a Passphrase

Try not using words that are commonly found together. A new trend in password cracking is pulling words that frequently accompany each other, in phrases from Wikipedia and other sites (in various languages), and compiling word lists from these for cracking long passphrases.

Another technique is to use a sentence, pulling the first letter from each word in a long phrase or sentence; for example, "Organizing and Leading Trainings is Hard Work, but Worth It!" becomes the pretty difficult to guess "OaLTiHW,bWI!").

Also, typos can be your friend! In a passphrase, if a password dictionary, which is used to guess passwords, is using correct spellings, a typo in a word can help reduce the chances of it being guessed.

Again, don't use the most common passwords, and don't reuse passwords, especially for your most important accounts - these are the first thing that an adversary will try to use or guess.

Myths & Misconceptions

Why Don't More People Use Strong Passwords?

Remember that, both in this training session and in many other resources (and even in the media), users are being told that the best passwords they can create to protect themselves are also the hardest to remember.
The number of passwords that we must regularly maintain is growing quickly, and isn't showing any sign of slowing down.
We now have so many passwords, and are adding more every day. How are we supposed to memorize all of these strong and hard to remember passwords?
When participants raise the point that it quickly becomes "too many to remember!", Take the opportunity to identify password managers (such as KeePass) as crucial aids that can help support more sustained use of strong passwords. Remind them that the next portion of this session will cover these helpful tools.

Common Myths and Misconceptions

Account Privacy Questions will keep my password and account totally safe

The personal privacy questions many accounts frequently allow or require users to setup are offered as an alternative means of verifying your identity, and as a way to unlock your account should it be compromised. The types of questions provided are, frequently, ones for which the answers could very easily be guessed; it's surprising how many correct answers to these questions can be found through a simple Google search. A good workaround, when asked to provide answers to these personal "privacy questions" that are used to authenticate you as well as allow you to reset your password, is to consider not answering them truthfully in a way that you can remember.

Account Lockouts protect me!

Many systems - primarily Online accounts for most average users, along with PIN codes - will lock out after 3+ incorrect login attempts. While this can add some protection against those trying to access your account, this isn't full protection. If someone wants to gain access to an account badly enough, and has the resources to do so, they might be able to obtain an encrypted version of its password (called a hash), decrypt it offline (by conducting billions of mathematical comparisons/ guesses per hour, depending on the computing power they have available), and then log into this account without getting locked out using a pre-cracked password.

Myths & Misconceptions

Using non-English words will make my password secure.

If an adversary has enough of an incentive and the resources to target you for your password to access your accounts, they will probably know quite a bit about you, including what language(s) you speak. When they (or someone they hire) attempts to brute-force your password, they will put words relevant to you in the word list they use to "guess" your password. This is likely to include words in your primary language and words particularly relevant to you, such as names of family members, locations (where you were born, where you've lived or travelled), and dates (e.g., your date of birth, when your child was born, when you were married).

Authentication

Passwords are primarily tools for accessing information, from the point of view of the services you use them for, which is one of the most fundamental properties of information security. This is often confused with authentication - proving that you are indeed the same person who owns the account; because your password can be given or taken and used by someone else, this means they are a weak form of authentication but a relatively stable form of controlling access.

A Note on Two-Factor Authentication

If you or your training participants are individuals at high-risk of being targeted by an adversary with resources, who wants to access accounts and their information, using two-factor authentication for services that offer it is highly recommended. Google, for instance, has stated that the use of two-factor authentication has drastically reduced the number of compromised accounts.

Further services, aside from Gmail and other Google tools, offering two-factor authentication include Facebook, Dropbox, and Twitter. This website (https://2fa.directory/) is an excellent tool for looking up accounts and services that currently support two-factor authentication.

It is important to use extreme caution, when using two-factor authentication systems that rely on text messages.

Recent research has indicated some popular sites, such as Facebook, being compromised by intercepting the verification codes contained within such text messages (which are not sent in any kind of encrypted format). Additionally, if you travel often and change your phone number when you do, it is important to note you can be locked out of your computer if you are not using an app like Google Authenticator.

Useful questions:

1. What is the main lesson or realization that you took from this session?
2. Are there any habits you realized you need to take steps to address or change? What changes might you make?
3. What steps or actions would you take first, if a password or account of yours were to become compromised?
4. What would you need in order to ensure that you are able to keep using a password manager?

Synthesis

We recommend that trainers use this wrap-up session for informal questions to the group, reviewing the material that has been covered in the module. The following questions may help participants think about using what they have learned:

Conducting the Activity

At the start of the exercise, the trainer explains that the purpose of the module is to learn ways to identify the variations in password strength among the trainees. The trainer then asks the participants to step forward if:

- If you use your birthday for your password, take 2 steps forward.
- If you use your [mom's / dad's / child's / sister's / brother's / partner's] name in your password, take 2 steps forward.
- If you use your phone number or anyone else's phone number for your password, take 2 steps forward.
- If you use 'Password' as your password, take 3 steps forward.
- If you use '1234567890' as your password, take 3 steps forward.
- If you use the same password for at least 2 social networking accounts, take 4 steps forward.
- If you use the same password for your email and your social networking accounts, take 6 steps forward.

Activity

Running the race:

Ask all the participants to stand on one end of the room in a line. The goal of the race is to see who gets to the other side of the room first.

Useful questions:

1. What do you think this activity was about?
2. What do you think is a good password?
3. Why do people not use good passwords?

Discussion

Frequently, the running the race (above) leads to an extended discussion on its own when teams take turns presenting their findings. However, if time remains, trainers may wish to have participants sit in a circle or semicircle, so they can address one another. The following questions may help start the discussion. Trainers are welcome to add to this list or improvise as they see fit. As always, trainers should encourage each person to speak up. It is likely that some have thought carefully about the issues; others may not have thought too much. This exercise will likely reveal some interesting practices, which makes for a rich discussion.

Input

Safe password practices

Use this time to also go over with participants some of the most commonly misunderstood advice, and popularly held “myths”, about using strong passwords and managing different user accounts Online.

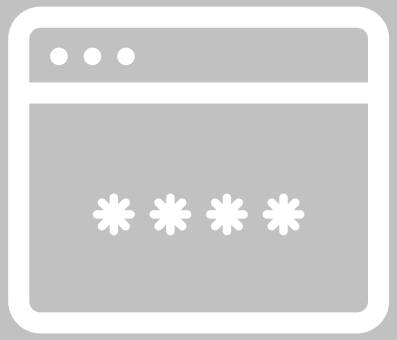
Using a password Manager

Materials to Prepare:
- USB flash drive for each participant, loaded with Portable Apps version of KeePass for Windows users, KeePassX for OSX and Linux users - you may also have participants simply download and install any of these directly from the developer websites, instead of using the Portable Apps version.
- Relevant Hands-On Guides for users from Tactical Tech's Security-in-a-Box resource: KeePass for Windows, KeePassX for OSX, KeePassX for Linux
- Whiteboard or flip-chart and markers; display the notes describing features of a strong password from the Safer Password Practices Input for reference
- Projector to demonstrate hands-on steps

Deepening

Trainer's Note

Testing any new versions available of KeePass/KeePassX before your workshop is recommended, to reduce potential challenges either you or participants could potentially encounter. Check for updated Hands-On Guides for KeePass Windows, and other up-to-date, step-by-step installation and use guides for OSX and Linux as available, if you know ahead of time that you'll be including this tool in your training.
Also recommended for this session - have a KeePass or KeePassX database pre-made, populated with a number of dummy entries, to show participants how they can organize their own databases. This also helps illustrate the utility of using a password database by showing how many entries an average user has.



Password Managers

Getting Started

Walk participants through the installation and/or launch process for either tool, depending on whether they are using a Portable Apps version already provided on USB (launching) or downloading a **.exe** directly from the developer website (installing). You are ready to move on once every participant has the initial screen up for creating their Master Password.
Explain that with KeePass/KeePassX, users can create one or more "databases" for storing their passwords - think of each database as an individual container holding many different passwords, and each container requires its own "master" password in order to be opened. Users might have multiple databases for different reasons, such as separate databases for passwords related to different projects, different kinds of user accounts, "work" and "personal" account passwords, etc.
A created database is saved individually as a **.kdb** file - these can be transferred to and re-opened on other devices with KeePass or KeePassX installed. One of the crucial features of KeePass is that the databases are encrypted. This means that even if someone else gets a copy of a user's database .kdb file, they cannot open it without its Master Password.

Creating a Master Password

Now ask that each participant create a Master Password for their first password database - ideally, this will be a dummy or "test" database for practice purposes.

Have participants use the techniques and practices from the Safer Password Practices Input to make a strong password, as this will be the password that protects all other passwords in that same database.
If participants forget the Master Password they've set for the first database they create, remind them they can create another database.

Creating a New Entry

Once inside their first database, briefly explain the features and layout of the database screen - this includes the larger pane where each entry will be displayed **(Title, Username, Passwords, URL, etc.)** and the smaller pane where users can create different folders within the database for different passwords or categories of passwords.
Next, have the group navigate to "Add Entry" and demonstrate the entry screen and data fields included within it - review the data fields available and the main ones used (Title, Username, Password, URL, etc.).

Password Managers

Explain how users can input the password to be saved into the Password field, or how they can use KeePass/KeePassX auto-generate new, unique passwords. Explain that, in order for the feature to auto-generate a more randomized, and thus stronger, password, the more entropy that needs to be fed into it as the new password is created - be sure to explain what **entropy** is in the process.

Saving a New Entry and Saving a Database

Once each participant has created a new entry for their database, ask everyone to click OK to save it - once done, the new entry should appear in the larger pane of their main database screen, with all the relevant information they included displayed in each column. Now, explain that since they've made a change to their new database, that database must also now be saved in order to maintain the updated information.
Some versions (KeePass for Windows) require saving the entire database before closing it - in this case, the name of the database (e.g. "filename.kdb") will be displayed in the upper left-hand corner with an asterisk (e.g. "filename.kdb*") indicating that the database hasn't been saved since the last change was made to it; others (KeePassX) will auto-save the database before closing it. Be sure to clearly note any differences between versions you're training on.
For practice, once each participant has created and saved a new entry, have them close the database after saving it as well - then, they can practice inputting their Master Password by re-opening this database.

Further Options and Features

If there is enough time, or depending on the particular needs of the group, you can review the further options and features of KeePass/KeePassX that are available to users, including:

- Organizing passwords within a database into groups and subgroups, and assigning each a different icon as desired.
- Copying passwords, usernames, and URLs, by right-clicking on an entry and then pasting this information when and where necessary, all without opening the entry itself.
- Changing the amount of time passwords, usernames, and URLs remain available to be pasted after copying them - it's highly recommended that participants set a time limit for these.
- Enabling the Auto-locking feature for the database after a period of inactivity, and the ability to auto-lock the database when the window is minimized.
- Setting up reminders to change passwords - it's highly recommended that users change their most important passwords every 3-6 months.
- Using the "Notes" section in a given entry for storing any useful information relevant to that password or account, such as storing the answers to "security questions" for various accounts.

Password Managers

Changing Account Passwords

Note to participants that, while worthwhile in the long run, making a shift to password managers takes an investment of time and effort upfront; however, emphasize that it will save them time overall and make their passwords and accounts much safer. Devote some time in the session for participants to add several of their most important passwords to their databases. If they have passwords they know they should change based on the advice in this training session - especially any passwords shared between multiple sensitive accounts, or passwords that are one of the top 25 most common passwords - they may choose to start with those.

Password Database Backup

As briefly mentioned in Step 1, one of the key features of KeePass/KeePassX is that users can control where their databases are stored and who can access them - database .kdb files can be moved between devices, and opened using the Master Password on any of these devices where KeePass/KeePassX is also installed. Note that the version of the KeePass/KeePassX that was used to create the database may limit which version you need to reopen your database on another computer.
Remind participants that one of the crucial features of KeePass is that the databases are encrypted. This means that even if someone else gets a copy of a user's database .kdb file, they cannot open it without its Master Password. Highlight that users can make multiple copies to save in various locations - they can be stored on a USB or external hard drive, backed up cloud storage, sent to oneself via email, or saved on a mobile device.
Backing up passwords databases allows them to be accessed elsewhere, in the event that your laptop or computer is damaged or lost. To do this, users need to be sure to back up their databases on a regular basis - they can set up reminders for themselves to do this regularly if they wish.

Trainer's Note

If you would like to address the topic of data backups more in-depth, either during this session or in a later session of your workshop, refer to the Protecting Data: Data Backup Basics module on LevelUp for more detailed exercises and talking points.

Other Password Management Systems

It's reasonable to expect that in the course of this session, participants may raise the subject of other password management tools that they have used in past, or have heard about from their friends or colleagues. In addressing this topic, there are some key points to ensure that you cover when discussing the pros and cons of other options (either LastPass or 1Password are likely to be mentioned, for example) versus KeePass/KeePassX:

Password Managers

Do these solutions provide any kind of encryption, or any other option for protecting password data?
For example, The built-in Key chain utility for OSX is an excellent password manager, although it lacks some of the features of KeePassX, such as areas for Notes, an option for creating identical encrypted backups, "change password" reminders, syncing features, etc.

Are these tools open source? If not, how can we be certain of how safe our data will be with them?
Because their source code is available for anyone capable of reading it to review or audit, the transparency of open source software and tools permits them a greater degree of trustworthiness when it comes to how safe data shared with them is (or isn't).

If they're cloud-based, are you confident that the company who owns the service cannot access any password data?
This would also mean that they would not be able to disclose your passwords if their systems become compromised. It may be effective to mention that compromises have occurred with some of these cloud-based managers. One such example can be found here. This can also provide you with an opportunity to cover the qualities of KeePassX that make it more trustworthy that a company's cloud-based system.

What is the participant(s)' level of tolerable risk for using these applications?

This is important to discuss - in some cases, neither the real nor perceived risk(s) could be severe enough to rule out one of these other options.

Useful questions:

1. What is the main lesson or realization that you took from this session?
2. Are there any habits you realized you need to take steps to address or change? What changes might you make?
3. What steps or actions would you take first, if a password or account of yours were to become compromised?
4. What would you need in order to ensure that you're able to keep using a password manager?

Synthesis

We recommend that trainers use this wrap-up session for informal questions to the group, reviewing the material that has been covered in the module. The following questions may help participants think about using what they have learned:

7 Device Management

Introduction

Device management is the process of managing the implementation, operation and maintenance of digital devices and its applications/software. It includes various administrative tools and processes for the maintenance and upkeep of a device.
Device management is broken down into three aspects: Device security, Device hygiene, and application security.

Objectives

During this module, the participants will gain an understanding of the following key topics:

- Identifying and Interpreting device vitals warnings
- Troubleshooting and fixing
- Learn to keep their device software up-to-date
- Learn how to install and uninstall software
- Device security awareness

Tools required

Trainer

These tools will be necessary for the trainer to prepare before conducting the training.

Devices

- Laptop
- Smartphone
- Projector
- Internet access

Resources

- USB flash drive
- Suitable space
- Colored electric tape
- Hands-on guides
- Whiteboard
- Post-it notes (multiple colors)
- Markers (multiple colors)
- Flip-chart paper

Trainee

These tools will be necessary for the trainee to have during the training.

Devices

- Laptop
- Smartphone

Resources

Definitions

Application (Software, App): Is a computer program designed to carry out a specific task typically to be used by end-users.

Patches (Software Updates): These are changes to a computer program/application/ software intended to fix, or improve it. This includes fixing security vulnerabilities and other bugs.

Vulnerabilities: weaknesses in the application which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application.

Anti-virus: These are programs created to help protect your device from malware. It mainly looks at data — web pages, files, software, applications.

Bug, Glitch, (Software bugs): A digital footprint or digital shadow refers to one's unique set of traceable digital activities, actions, contributions and communications manifested on the Internet or digital devices.

An exploit: This is a piece of software that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware.

Piracy: This is the illegal copying, distribution, or use of software.

License software: is a document that provides legally binding guidelines for the use and distribution of software. There are 2 types of software license; proprietary or open source.

Definitions

Malware: An umbrella term for Malicious Software, very likely containing a virus or an otherwise malicious software application.

Virus: Viruses are usually attached to a program or file. They are generally executable files and can only be run when ordered to do so by the user.

Trojan: This is malware which comes disguised as "legitimate" software - often in cracked versions of proprietary software. They are often designed to steal information and transmit it over the internet. This is one reason that genuine software is always preferable to pirated, cracked software.

Spyware: Malware which records users' activities on a computer; a common example of this is a keylogger, but it can be far more advanced.

Worm: Worms are similar to trojans but have the unique characteristics of being able to copy and send themselves from computer to computer (or other devices). A well-known example was the I Love You worm.

Definitions

Digital technology: Digital technology is any hardware or software that generates, stores and process data or content.

Digital FootPrints/Shadows: A digital footprint or digital shadow refers to one's unique set of traceable digital activities, actions, contributions and communications manifested on the Internet or digital devices.

Mobile device- A piece of portable electronic equipment that can connect to the internet, especially a smartphone or tablet computer.

Safety- A condition of being protected from or unlikely to cause danger, risk, or injury.

Mobile safety-is the protection of smartphones, tablets, and laptops from threats associated with wireless computing.

Activity

Software Treasure Hunt:

In this Activity, participants take a close look at the software on their computer and answer key questions regarding each application's safety and status. This then leads into a Discussion about key habits for safer management of existing software, and for downloading new software.

This activity will highlight the differences in software versions for each participant's computer. At the end, the discussion will focus on teasing out current practices (or lack thereof) for keeping software up to date, and then lead to the Input section where best practices will be presented.
When making the matrix, leave enough space to fit everyone's version number in as they share them out.

The training participants will be asked to:

- Identifying the operating systems participants are using.
- Checking the first line of defence e.g. screen locks.
- Checking the update center for any device updates .
- Checking device storage to make sure they are clean and not full.
- Monitoring device behavior. 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.
- Games for testing knowledge e.g. Kahoot!
- Reviewing mobile application permissions.

Software Treasure Hunt

Step 1: Common Applications

Ask participants to try to find the version number of the applications that you have listed in the left-hand column of the matrix.

- Some participants will be able to find version numbers, but others will need direction. If they are running Windows, you can instruct them to open 'Add or remove software' from Windows Control Panel or to open the program and find the version number under the "Help" or "About" menu.
- Have participants call out their version numbers one at a time.
- Leave the operating system for last. Ask participants to open Windows Update and find the date of last update. Add that to the matrix.

Step 2: Suspicious Applications

Ask participants to open Add or Remove Software (Control Panel->Programs->Programs and Features).

- Ask participants to examine it for software they don't recognize or that have suspicious names (e.g. "SuperSpam-u-lator").
- Add those programs to the matrix in the far-left "Program" column.
- Make a notation in the corresponding "Reputation?" box in the third column.

Step 3: Pirated Applications

- Ask participants if any of them know of a pirated application they have installed on their PC (remind them you're not the Software Police!).
- Provide some popular examples - good ones include Photoshop, Microsoft Office Suite programs, NitroPDF, and Adobe Acrobat. Add these new programs to the left-hand "Program" column.
- Make a notation in the corresponding "Licensed?" box in the fourth column.

Step 4: Filling out the Matrix
Looking through the list once again, ask the group to help complete the matrix. Ask where people got all their software? As you review individual applications, use these guidelines:

In cases where the application is FLOSS** (Free/Libre open source software)
- Mark 'free/open source' in the License? Column.

In cases of suspicious software,** ask the group what they think:
- Who uses the application?
- What was the source for the application?

Discussion

Useful questions:

1. What are the advantages of installing software updates?
2. Why is setting a screen lock after a period of inactivity important?
3. What are the disadvantages of running out-dated software?
4. Why should one troubleshoot their devices?

Device Security

The disadvantages of running out-dated software
• Out-date software is a program that's no longer supported by the vendor and it has the following disadvantages: System failure, devices can easily be hit by malware, hackers can easily access the system.

Advantages of installing software updates.
•Software updates include repairing security holes that have been discovered and fixing or removing computer bugs. •Updates can add new features to your devices and remove outdated ones.
• Updates help patch security flaws
• Hackers can take advantage of the weakness by writing code to target the vulnerability. The code is packaged into malware short for malicious software.

The importance of setting screen lock after certain time of inactivity
• Locking your computer while you are away will help protect confidential documents, client information, financial statements and employee information.

Need to state the importances of troubleshooting your device.
Have a record of all hardware so you know what your estate looks like
Have a record of all installed software to ensure it is properly patched/updated
Utilize secure configuration / hardening guides for all devices
Manage data in and out of your network
Minimize administrative accounts

Establish an incident response plan
Enforce similar levels of security across the supply chain.
Ensure suitable security controls in any service agreements (including cloud services)

Application Security

Identify how participants obtain applications. Try to discourage application sharing using xender, Bluetooth, etc.
Identify the security measures that are implemented by the participants. I.e. how do they access their applications. E.g. setting passwords for your applications, hiding your application

Device Hygiene

Device hygiene relates to the practices and precautions users take with the aim of keeping devices and data organized, safe, and secure.

Device hygiene encompasses behavioural practices, maintaining their devices, checking their computer's vitals, (interpreting red flags, probing slowness), etc, and how people understand and handle the technology they 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 analyze.

- Probe with participants about disk space allocations (system drive, data drive). They need to understand that making more space for the system drive is important for the functioning of the operating system.
- Cleaning the device i.e. deleting temporary files, organizing desktop, using shortcuts, etc.
- The Action Centre will enable you to discuss the following aspects as they are listed in The Security drop-down menu.
- Monitoring device behavior. 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.

Title: Phishing attack

Story:

Alphonso is a company that builds applications on Google PlayStore for children. The application requires compulsory microphone permission, the microphone was then used to listen in to the environment around a user to collect data of adult's TV usage. The collected information was sent to relevant parties in the television industry to influence what viewers see.

The trainer asks participants what they think the organizations could have done differently.

Learning outcomes:
Check the permission settings of all the applications on your devices.
When installing an application, pay attention to the permission settings the application requires

Input

Title: Data Breach

Story: The hackers were able to access the credit reporting agency's data through a known vulnerability in a web application. A fix for this security hole was actually available two months before the breach, but the company failed to update its software. This was a tough lesson, but one that we can all learn from. Software updates are important because they often include critical patches to security holes.

The trainer asks participants what they think the organizations could have done differently.

Learning outcomes:
Regularly check for software updates
Do not postpone software updates.

Input

Deepening

Device Security
This session is hands-on. It will introduce participants to practical skills on how to:
1. Enable windows updates
2. Enable screen lock and password,
3. Clean of temporary files,
4. Enable windows firewall,
5.Uninstall unwanted software

Software Updates

Windows operating system
1. Open Windows Update by clicking the Start button in the lower-left corner. Or Press Windows key on your keyboard.
2. In the search box, type Update, then, in the list of results, click either Windows Update or Check for updates
3. Click the Check for updates button and wait while Windows looks for the latest updates for your computer
4. If you see a message telling you that important updates are available. Click Install updates.

Installing Updates on IOS
1. Choose System Preferences from the Apple menu , then click Software Update to check for updates.
2. If any updates are available, click the Update Now button to install them. You might be asked to enter your administrator password for your icloud account.
3. After the update, the system will notify you that your Mac is up to date,The Updates installed applies to all other applications running on the system

Enabling Automatic updates on MAC OS
1. Choose System Preferences from the Apple menu , then click Software Update to check for updates.
2. Select "Automatically keep my Mac up to date." Your Mac will notify you when updates require it to restart

Mobile Devices
How to enable and install updates on phones

iPhone
Make sure your phone is fully charged and it has an Internet connection

1. Click Settings on your screen
2. Click General
3. Tap Software Update. You will be notified if your phone is up-to date.

Android
Make sure your device is connected to the Internet and its fully charged

1. Open Settings on your phone
2. Scroll down and Select About Phone.
3. Tap Check for Updates.
4. If an update is available, an Update button will appear and then Tap it.
5. Click Install.

Software Updates

Enabling Windows Firewall
1. Click the Windows key button on your keyboard.
2. Type Control Panel.
3. Select Control panel on the windows that appear.
4. Scroll and Click on System and Security.
5. Click on Windows Defender Firewall and a Windows Firewall panel will appear.
6. On the screen that appears, click Turn On Windows Defender Firewall for both private and public networks.

Enabling and setting screen Lock
Windows OS

Automatic Screen lock after certain time of inactivity
1. Press Windows button on your keyboard
2. Type screen lock settings
3. On the results that appear click screen lock settings and a lock screen window will appear
4. Click on screen saver settings
5. On the dialogue box that appears, click on resume, display log on screen. You can also set a time for how long your PC should wait before starting the screen saver.

Manual screen lock on Windows
1. Press and Hold Windows button and press the Press L button on your keyboard. Hit the Windows key and the L key on your keyboard. Keyboard shortcut for the lock!

Device Security

Set or change a screen lock
Important: To ensure your automatic and manual backups are encrypted with your screen lock, use a PIN, pattern, or a password.

1. Open your phone's Settings app.
2. Tap Security.
If you don't find "Security," go to your phone manufacturer's support site for help.
3. For screen lock options, tap Screen lock (If you've already set a lock, you'll need to enter your PIN, pattern, or password before you can pick a different lock.)
4. Tap the screen lock option you'd like to use. Follow the on-screen instructions.

Standard locks
Pattern: Draw a simple pattern with your finger.
PIN: Enter 4 or more numbers. Longer PINs tend to be more secure.
Password: Enter 4 or more letters or numbers. A strong password is the most secure screen lock option.

Configuring Computer Login Password

1. Open Start Menu. Go to the desktop of your computer and click on the Start menu button.
2. Select Control Panel (settings). Open the Control Panel.
3. Select "User Accounts and Family Safety".
4. Select change Windows Password.
5. Change Password
6. Enter Password.

Clearing your junk files
Windows
To remove temporary files on Windows

1. Open Start Menu. Go to the desktop of your computer and click on the Start menu button.
2. Select Control Panel (settings).
3. Click on System
4. Click on Storage.
5. Under the "Local Disk" section, click the Temporary files option.
6. Select the temporary files you want to remove
7. Click the Remove files button

ON mobile

1. On your Android device, open Files by Google.
2. On the bottom left, tap Clean
3. On the "Junk Files" card, tap. Confirm and free up
4. Tap See junk files.
5. Select the log files or temporary app files you want to clear
6. Tap Clear
7. On the confirmation pop up, tap Clear

Useful questions:

How do you update your mobile device?
How is a phone secured?
How do you protect your device from an authorized access?
Is it necessary to have a password on your device?
What are the challenges of outdated software on a device?
How do you check for updates on a windows computer?
Is it necessary to lock your device's screen when not in use?

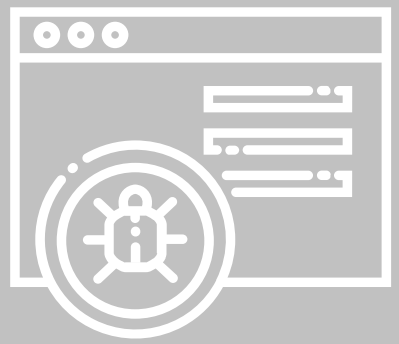
Synthesis

We recommend that trainers use this wrap-up session for informal questions to the group, reviewing the material that has been covered in the module. The following questions may help participants think about using what they have learned:

The trainer can find a game to play.
There are millions of public kahoots available on the platform.

Step 1: Launch the game so players can join Change the game settings if you like (for example, randomize the order of questions, etc) and click on Classic or Team mode to start letting players join your game. A unique Game PIN will be displayed at the top of the screen. Players enter this PIN to join the game in the Kahoot! app for iOS and Android. Alternatively, if they cannot install the app on their device, they can join by going to kahoot.it in their browser.

Step 2: Click Start once you can see all the players' nicknames in the "lobby" or waiting screen. During gameplay, you can use the spacebar or your mouse to go to the next question. At the end of the game, click Get Results, and then View Reports or Save Results to view and download a game report, or play this kahoot again.



Malware protection

This section contains training modules related to protecting devices and data from malicious software (malware), and practices which training participants can adopt to lessen their exposure to it. Topics addressed include what malware is, how devices can become exposed to it, and how to mitigate the risks malware poses.

Safer Software Updating

This fundamental level subtopic habits and practices for more safely downloading and updating software on a device. As this module includes tasks to download and install software, it is recommended that the trainer confirm prior to class that the websites featured in these activities are unfiltered and genuine.

Learning Objectives

- Discover what applications are on installed on the PCs in the class.
- Learn the process for updating applications and operating systems.
- Learn the process for installing and uninstalling applications.
- Identify which websites are the safest to use when downloading software.
- Understand what risks come with pirated software, as well as the risks of not updating genuine software.

Useful questions:

Ask participants to share their habits related to software updates:

- Do they allow automatic Windows updates?
- Do they skip or put off automatic updates? If so, why? (Are they concerned their PC will stop working?)
- Do they assume all other software is updating itself automatically?

Discussion

Leading the Discussion

Highlight the differences in version numbers, and point out examples where participants have out-of-date software.

Title: Malware Attack Files

Story: In August 2019, Facebook experienced a data breach by unknown hackers that affected 530 million users who woke up to find their accounts unaccessible after the malware attacked Facebook's system. Their phone numbers, full names, locations, some email addresses, and other details from user profiles were posted to an amateur hacking forum. The leaked data included personal information from 533 million Facebook users in 106 countries.

Learning outcomes:

- Have strong passwords.
- Enable two step verification to avoid personal information being leaked.

Safer Software Practices

Step 1: Defining Terms
Put the following terms on a flip-chart and ask participants to define them, writing answers where correct or providing clarifications as needed. All of them will be addressed before the session concludes:

Input

Bugs/"Buggy"
Vulnerability
Exploit
Patch
Piracy
Alpha release
Beta release
License

Safer Software Practices

Software Development & Updates

Ask participants to describe how software is developed (or to guess, if they aren't sure). Explain that software is written by development teams consisting of programmers, designers, and other specialist roles, depending on the project - also:

While it is being built, an application goes through alpha and beta versions (early versions/draft versions) which are not released to the public, but are tested internally. With open source software, the testing may be a carried out by a community of volunteers to test software. When problems are found, testers alert the developers – they file "bugs".

- Software is almost never 'final' or 'perfect', but is released when it is just good enough for public use, with the expectation that the development team will continue to work on new releases which contain fixes to existing problems.
- Each new release is an Update, or a Patch. These updates might improve or change features, the user experience or security.

Ask participants what software on their PC receives updates. See what gets listed or left out. Some examples to get the list going include:

- Browsers
- Adobe Reader
- Microsoft Office
- Windows / Operating System
- Anti-virus

As you work through the list, see what other examples participants can think of and contribute - add these, and see how long you can get the list to be.

Vulnerabilities

Vulnerabilities discovered in software are a major problem for governments and companies, and for individuals, too. They are tracked by people who want to protect themselves as well as by people who want to exploit them – hackers. Show on screen the most recent records listed at:

- The US National Vulnerability Database: **https://web.nvd.nist.gov/view/vuln/search-results?query=&search_type=all&cves=on**
- Exploit Database: **http://www.exploit-db.com**

Highlight the number of total vulnerabilities published (for example, over 31,000 on Exploit Database and 66,000 on the US National Vulnerability Database as of Dec 2014).

Safer Software Practices

•Look through the titles of some of the software for which vulnerabilities have been published, or search for common software titles such as 'Adobe' and 'Office'.
•Point out that vulnerabilities are linked to particular software version numbers, meaning that newer versions are not vulnerable.

Automatic and Manual Updating

•Ask participants how their software gets updated, and if any of their software is getting old and out of date.
•Explain the difference between manual and automatic updates: some software can be set to update automatically, others will require users to manually go through the process whenever a new update is available.
•Discuss the increasing prevalence of 'App Stores' such as the Mac and iOS App Store, Google Play Store and Microsoft Store, which simplify updating by putting several updates in one location - these can also can be set to auto-update.
•Mention Linux systems like Ubuntu Software Centre or general Linux model of repositories these streamline updates.

Turn on Your PC's Alerts

When you install software or update it, you are making a change to your computer. Operating systems have a way of warning users before they allow software to make changes.
•The User Account Control (UAC) window that pops up when installing something in Windows is one example. It was introduced in Windows Vista (if you are running something older – such as Windows XP, you won't see this warning pop-up window).
•If you don't see this warning when you install an application, you probably have UAC switched off, which is dangerous. It can be turned back on in the Windows Control Panel (Control Panel -> Action Center -> Change User Account Control Settings).
•On Mac and Linux comparable presentations can be made warning users before software is installed with administrative rights (usually a window requesting the admin password).
•Because software makes changes to users' computers, and these changes may be good or may be bad, it is important that users know that they are installing safe software which will not harm their computers.

Use the Most Direct Sources

When downloading an application, try to get it from the developer's official website. That gives you the best chance of avoiding fake versions that may contain viruses and other malware.

Safer Software Practices

Where do participants get their software from?
Some example questions to ask participants may include:
- Downloading from websites (ask which website)
- From friends and colleagues
- Purchased discs from vendors or technicians
- Purchased Online or from stores on original media

If participants use download aggregators like download.com, filehippo.com or others, suggest that they find the vendor's websites to get original software. Using Google instead of less well known search engines should bring up the vendor's website within the top search results.

Give several software examples including a mixture of free and paid software, and ask participants to tell you how to obtain it. Good examples include: Firefox, Skype, NitroPDF, Office, PortLocker, CCleaner, Photoshop.

Avoid Bad, Dangerous, and Unnecessary Software & Toolbars

Some software can be unwittingly installed by users while installing other, free applications. Free software distributors earn revenue by leading their users to install additional applications during the installation process.
- Adobe, for instance, usually asks users of free versions of Adobe Reader or Adobe Flash to install an application from anti-virus application maker McAfee.
- The open source application Axcrypt (http://axantum.com) that comes with OpenCandy bloatware, is one example.

Removing the Bad Stuff

Applications
Show the Add or Remove Programs dialogue box in Windows, or the Applications folder on Mac OS X. Review the list and see if there is odd-sounding or unknown software (you could pre-install unwanted software in advance as a demonstration). Show how uninstallation can be done from this window.

Plug-ins
Explain that plugins that get installed into a browser may compromise the security of their Online activity and accounts. Open up Firefox and/or Chrome and access the Extensions or Plug-ins page and review for unknown or odd-sounding extensions. Show how to delete and deactivate plugins from this page.

Safer Software Practices

Potentially Unwanted Applications
Explain that this is a class of software recognized by anti-virus as software that may have been unintentionally installed by users. The following anti-virus applications can scan for so-called PUPs (potentially unwanted applications):
- AVG: http://free.avg.com/us-en/homepage
- Avast!: https://www.avast.com/en-us/index
- Kaspersky: http://usa.kaspersky.com/products-services/home-computer-security/
- ESET: http://www.eset.com/us/home/windows-antivirus/
- McAfee: http://home.mcafee.com/Default.aspx?rfhs=1

Using FLOSS Alternatives

Ask participants to list some of the most desired software which is both a) commercial and b) not free of charge (e.g. Windows, Microsoft Office and Photoshop.) Point out that these are frequently pirated due to cost, but that piracy brings certain risks:

- Governments and criminals release software with malware in order to compromise computers.
- Governments often use piracy as a pretense to crackdown on independent organizations.
- Many users do not know how to vet where their pirated software comes from.
- Pirated software is often blocked from receiving important security updates.
- Pirated software often has disabled features, or causes issues after installation.

Open a browser and navigate Osalt (http://www.osalt.com). Present free and open source software as an alternative to the dangers of piracy. For instance:

Linux/Ubuntu instead of Windows
LibreOffice/OpenOffice instead of Microsoft Office, Gimp/Gimpshop instead of Photoshop or commercial (paid) software platforms, human rights activists and their organizations may be eligible to receive free, or heavily discounted, versions of commercial software:
- Users may look for official distributors among local ICT service providers and request for a non-profit or public sector license discount.
- A large distribution network for donated software is run by TechSoup.
- The following page contains a list of partners and the countries in which they operate: http://www.techsoupglobal.org/network

Step 10: Obtaining Software and Updates in Countries with Content Blocking

Safer Software Practices

Users may be frustrated when trying to update software if they live in a country blacklisted from receiving 'software exports' from countries like the United States, or where ISPs are instructed to block downloads from certain sites. If this is the case, users can use circumvention tools to access the original sources for software. Refer to training content on Anonymity and Circumvention here on LevelUp.

Warning
Use of circumvention technology or encryption is not allowed in some countries. Please review the laws for your country before attempting to use.

Deepening

Step 1: Windows Updates
Step 2: Changing Settings
Step 3: Checking Last Updates
Step 4: Explaining Flexera PSI
Step 5: Cleaning up and Patching
Step 6: Display and Walk-through

Step 1: Windows Updates

Explain that Microsoft issues security and other updates for the Windows operating system, usually on the second Tuesday of every month, though sometimes more frequently when emergencies strike. This exercise will get participants acquainted with the Windows Updates feature.

Changing Settings

Instruct participants to open Windows Updates in the Control Panel. (Control Panel -> type "Windows Update".) Ask participants to click "Change Settings" to review their current status. Before moving forward, please confirm that:
- Install Updates Automatically (recommended) is selected.

Make sure the box for installing updates to "Microsoft products and new optional Microsoft software" is also selected.

Checking Last Updates

Return to the main Control Panel page for Windows Update and ask users to check the last date updates were checked and installed.
- If participants have out-of-date systems, ask if Windows Update is now downloading updates.
- If not, advise that participants review Update History and Hidden Updates to find failed updates and seek specific solutions for those updates, or refer to a local technician.

Explaining Flexera PSI

Ask participants to open the Add/Remove Programs dialogue box from the Windows Control Panel.
- Remind them that this is a list of all the software on their computer and that security vulnerabilities in these applications can put their system at risk.
- Unfortunately, Windows Update doesn't support applications that weren't developed by Microsoft.

An application called Flexera PSI will help:
- Flexera PSI compares applications on your PC to a database, checking for the latest versions.
- This application is free, but not open source. Paid versions are aimed at enterprises and corporate networks.

Cleaning up and Patching

Ask participants to take this opportunity to uninstall software they do not need or do not recognize. We recommend that you confer with each participant before they uninstall applications to avoid someone unintentionally bricking their PC.

Display and Walk-through

Instruct participants to install Flexera PSI and scan their computers.
- Invite discussion about the number of applications that need updates following everyone's first completed scan results.
- If the connection capacity allows, ask that participants update at least one application, using the shortcut icons provided within the application.

Ask participants if they have questions before completing the session.
• Ask for a volunteer to summarize what they have learned about safe software practices.
• If important points have been missed, ask others to chime in.

You may also ask specific questions to make sure some concepts are clearly understood. As a final group activity, explain that you have some challenging scenarios prepared and that you are seeking the participants guidance (as they are now experts!) about what to do.

What would they advise?
• You may choose to have each of these as an individual slide in a presentation, or you may simply read the scenarios aloud:
• A windows update notification asks if I would like to install now or later. I am busy so I press ignore. I am always busy!
• I need to edit some documents for school/work, but my new computer doesn't have Microsoft Office. The local technician says it costs (Insert reasonably unaffordable price in local currency)! Instead, I go downtown and pick it up on a CD for cheap.
• I am installing software, and the installer asks if I would like to install the Free CandyFish Toolbar with Translation Widget and the CandyFish Searchbox. Continue or No Thanks?
• My friend just told me about a security app that will help protect all my documents. She puts the installer file on a flash drive and gives it to me to install on my computer.
• I read an article recommending a free application that might speed up my computer called CCleaner. The article links to a site where I can download it called www.awesomesoftware.com. I go there, download the app and install it.
• I am using Windows XP.

Synthesis

We recommend that trainers use this wrap-up session for informal questions to the group, reviewing the material that has been covered in the module. The following questions may help participants think about using what they have learned:

Using Anti-virus Tools

This fundamental level module addresses the basics of what malware is, how user devices can become exposed to it, and how to mitigate the risks that malware poses through safe behaviors, basic practices, and informed use of anti-virus software.

Learning Objectives

- Learn the basics of what malware is and where it comes from;
- Understand how devices become exposed to malware;
- Learn to identify the various components of a potentially harmful e-mail;
- Understand how harmful emails can be targeted to users, including phishing, e-mail spoofing, URL obfuscation and similar-domain attacks;
- Learn what anti-virus software is, its importance, and how to use it safely and intelligently.

Conducting the Activity

Display a suspect phishing email and ask the participants to analyze it and identify markers that confirm that it is an illegitimate email

Activity

Analyzing a Potentially Harmful Email:

In this exercise participants will examine an email for clues about its authenticity, including its origin, content, and context. From this analysis, participants will be better equipped to determine whether or not it potentially contains harmful malware or could otherwise lead to a user compromising their identity or personal information.

Useful questions:

Discussing the Email

- Show participants how to check the full header of the message. Are participants able to spot some inconsistencies?
- Hover the cursor over links in the email (without clicking) - are participants able to spot anything suspicious? Explain URL shorteners, what they consist of, and why they pose a security threat. Explain how most short URLs can be previewed.
- Any observations about the sender? The addresses of those cc'd (if any)?

Discussing the Attachment

- What happens when they open the attachment?
- After participant input on this, open the EICAR file on your computer being projected and show how your own anti-virus prevents the computer from being infected).
- On the flip-chart, write phishing and malware and explain the meaning of these words.
- What would they do if they spotted an email they suspected as a phishing email? Delete or mark as spam? Tell co-workers/colleagues/ friends?

Discussing the Website

- If you mirrored a website, now is a good time to show participants what a phishing website looks like.
- Note the subtle URL variances between the original website and the "fake" one.

Discussion

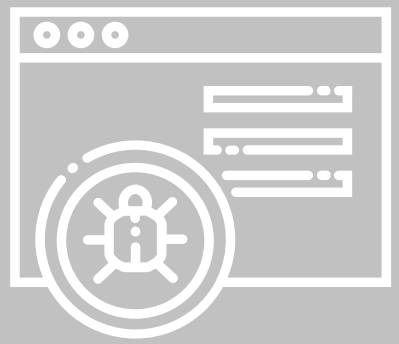
Once the email is shared, you can lead a discussion as participants explore its content and components. Items to cover as you have participants explore the email:
What are participants' initial observations?

- Facilitate further discussion among participants: Do they have their own techniques for identifying phishing attacks and avoiding infections through email and websites?

Input

This input session includes definition of basic malware terms, reviewing how users are exposed to malware, and how users can prevent malware infections or handle existing ones. Current trends in threats move ` fast, and can either be warnings to include in trainings or examples to use. Keep up to date on vulnerabilities, social engineering trends, etc., for your workshops - particularly if you're training on operating systems that you're less up-to-date on.

When it comes to talking about malware, a definition of terms is helpful so that participants can understand the different types and the distinctions between them. To avoid presenting the content solely as a lecture, and to get a better sense of your participants' knowledge, you can present this section by asking participants how they would define the following terms, then correcting their definition(s) as needed:



Exposure to Malware

One easy way to organize this, again so as not to bore participants with a lecture-only session, is to elicit input and ideas from the experiences of participants and write them on a flip-chart.

Supplement any crucial answers they haven't suggested and add them to the list; to save time, you may wish to prepare the following questions (leaving suggested answers blank, of course), on individual pages of flip-chart paper before the session, with one question per page:

How Do We Get Malware?
Answers:
- From infected hardware such as USB keys.
- By clicking malicious links to download viruses, like those found in fake advertisements.
- By downloading malicious e-mail attachments containing it.
- "Drive-by downloads" or malware downloaded from websites - exploits a number of vulnerabilities in unpatched, outdated, or "cracked" operating systems and browsers.
- Using unlicensed or "cracked" software - a common example of this are unlicensed versions of Windows, often bought because users cannot afford a licensed version, and often sold by non-hostile sellers though they leave users very vulnerable.
- Software that seems legitimate (e.g., Skype, Tor, Firefox) but is downloaded from hostile sources, and usually repackaged with malware.
- Through social engineering attacks; for example, when someone impersonates a friend or colleague and invites you to click on a link that downloads malicious software onto your device.
- By downloading them through scams on social networking sites.

How Do We Get Phished?
Answers:
- Emails that ask you to log into your Online banking account.
- Emails that ask you to log into your social network accounts.
- Private messages on Twitter with shortened links which bring you to a fake login screen.
- Facebook wall posts and links which bring you to a fake login screen.
- Email attachments.
- Instant messages from unknown accounts or from known contacts who have had their accounts compromised.
- More sophisticated attacks - explain what spearphishing is, what it looks like, and ask if participants have experienced it.

Exposure to Malware

What are Common Misconceptions or "Myths" about Viruses and Malware?

Only Windows machines get malware!
False: Both OSX (Apple) and Linux operating systems can also be vulnerable to malware, although most malware targets Windows because it is the most commonly used operating system worldwide. With the increasing number of OSX users, more malware is made to target OSX; however, because the number of Linux users are far fewer, Linux malware is far less prevalent.

Malware is only spread by devices that are also "infected" by malware!
False: Computers can pass on malware to other devices as "carriers." An example of this is a computer with OSX, passing on Windows malware to a Windows device, even though that malware didn't "infect" the OSX device because this malware was designed for Windows. That malware still successfully infected a Windows device, and because of this, users should have anti-virus software that also scans for malware designed for other operating systems.

If I don't notice anything "strange" happening with my computer, it's okay!
False: Malware may or may not be noticeable - sometimes it will have dramatic impact on a device's performance, other times a device will continue functioning in an apparently "normal" manner.

Anti-virus will catch any malware I have!
False: Anti-malware tools can only identify malware that is known; they cannot protect against "undiscovered" or "new" malware. This doesn't mean you shouldn't use anti-malware tools, however!

Once each list is made from this section, hang them up, but leave space next to each list for the list of solutions, both technical and non-technical, that will be covered in the following section.

Avoiding Malware

Go to Survival Time to calculate the average number of minutes it takes for an unpatched computer without anti-virus and a firewall to become infected - at time of writing, it took on average 5 minutes.

Below is a list of solutions for avoiding malware to cover together as a group - begin each question by soliciting solutions from participants and adding them to the list, then supplementing additional solutions and missing information as needed.

Exposure to Malware

Place each list of solutions next to the respective list of how users are exposed from the previous section - the avoidance questions below are numbered the same (I or II) as the exposure questions (I or II) from the previous section. Keep them up during the training so participants can refer back to them.

How Can We Avoid, or Reduce Our Exposure to, Malware?

By Using Updated Operating Systems and Applications
One of the most important ways to protect yourself from malware is to have an updated and licensed operating system, whether open source (Linux), or proprietary (Windows and OSX). Malware takes advantage of outdated and cracked software and operating systems to infect them.
- If using open source (or FLOSS) applications, only download them from known projects - for those who are interested, the website osalt offers suggestions for open source alternatives to popular proprietary applications.
- Only download software from official sources, or trusted download sites via official websites.
- Be wary of using unknown and untrusted third-party sites or file-sharing sites.
- The experience of Syrians being targeted with malware in a number of ways is a useful cautionary example, as well as the Tibetan community.

Using SHA or MD5 Hashes
To verify downloads whenever possible. Suggested tools for this include FileInfo Professional (Free, OSX), HashTab (Paid, OSX), HashCheck (Free, Windows), Rapid CRC Unicode (Free, Windows).

By Downloading over an Encrypted Connection
Usually SSL in the browser, whenever possible; similarly, turn on auto-updates for the operating system and applications you use - Flexera for Windows is a free tool that will check to make sure your installed software is up to date.

By Enabling the Firewall
On your device to protect yourself; this can also help reduce the spread of malware if you are infected. If you have OSX users, mention that Apple devices are sold with the Firewall OFF by default. Direct them to where they either confirm that it is turned ON or turn it ON themselves (Preferences -> Security & Privacy -> Firewall). Windows usually has firewalls ON by default; to confirm or to turn ON, go to (Control Panel -> Security -> Windows Firewall).

Exposure to Malware

By Using Anti-Malware Tools
There are different types of anti-virus and anti-malware tools. However, just to make it more confusing, some tools are combined into one, and others have various capabilities enabled depending on whether or not they've been paid for.

If participants ask for a place to compare tools, you can point them to AV Comparatives' Summary Reports for both Windows and OSX tools.
Types of anti-virus and anti-malware tools to describe and differentiate for participants include:
- Anti-virus (more on these below)
- Anti-malware scanners (like Malwarebytes)
- Anti-Spyware scanners like SuperAntiSpywareFree

Have an active and updated anti-virus program that checks for malware for other operating systems as well, not solely the one on the device it's installed on - this is to avoid the spread of malware that doesn't affect one kind of operating system to devices using other operating systems that may be affected. This is most relevant for OSX and Linux operating systems.
Free anti-virus apps for Windows include:
- Avast! (also checks for software updates)
- ClamWin (open source)
- Avira
- AVG

Free anti-virus apps for OSX include:
- Avast!
- Avira
- ClamXav (open source)

Have an anti-virus program that has active monitoring capabilities, or "real-time protection", and use it. This allows the program to actively monitor your computer's activities to alert you to potential malware, instead of discovering malware during scans alone.

Do not run more than one anti-virus/ anti-malware tool that provides active monitoring capabilities.
- Program your anti-virus program to conduct regular scans.
- If you can afford it, use an anti-virus tool that provides "web browsing" protection if you have a Windows device.
- This can help protect you from "drive-by downloads" when browsing the web, which can even happen on seemingly innocuous websites that have been exploited.

Exposure to Malware

II. How Can We Avoid Phishing?

By Practicing Safe Email Habits

- If you receive an email from your bank for anything besides routine updates, quarantine the email and contact them directly.
- If you receive an email in your work account that looks suspicious (or a message to your organization via social media accounts), alert your IT team or manager immediately.
- If necessary, email an alert to your co-workers as well if they're also addressed in the email. Your organization may be experiencing a spearphishing attack that can affect the entire organization.
- Double-checking with a contact if they appear to have sent you an attachment you weren't expecting.

By Practicing Safe Web Browsing, Social Media and Chatting Habits

Be very suspicious of private messages on social networking sites or IM which prompt you to:

- Click on links of "pictures of you" that don't exist or look suspicious.
- Download a tool or piece of software that looks appealing.
- Download games that looks harmless.
- Ask you to provide any type of sensitive information.

C) By Always Examining URL links

On websites, social networking sites, and IM (as well as in emails). Sometimes this may be the only way to realize you've been redirected to a (sometimes very convincing) login page.

D) By Always Checking the URL

When you're unexpectedly directed to a login screen, or if you're redirected to an unfamiliar "warning" page of any kind for a service that you use.

E) By Staying Alert for Phishing Attacks

Which are becoming far more effective and harder to recognize - examples to share include this fake Google login page and this fake Apple Store ID reset page.

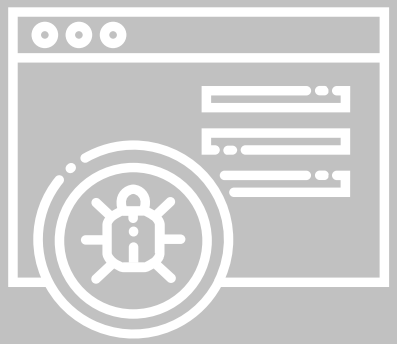
- Approaching links shared over social networking sites with extreme caution, especially if they're posted by unknown people.
- Avoiding any advertisements that appear to be scams.
- Similar to avoiding phishing attacks in email, hover over URLs and hyperlinks to check where they lead.
- Examine links from URL shorteners like bit.ly before clicking on them: Copy them into the browser and adding a "+" at the end of the URL.
- If you're unsure about a URL, check it at VirusTotal.

Exposure to Malware

Step 4: Closing Exercise
Go through each list and identify each type of exposure to malware and each solution to malware as either technical or non-technical. Use this to illustrate how being safe Online is a combination of technical and behavioral solutions

Trainer's Note
If participants are using pirated copies of Windows, this is extremely dangerous and they should prioritize buying a license if they want to continue using proprietary software (Windows and OSX). If there are a number of participants who cannot afford licenses and are unlikely to use open source, try to see if you can find an organization to provide them with licenses. Otherwise, they should consider using open source operating systems instead.

Trainer's Note
For a case study of how an organization can be compromised by a spearphishing attack, this may be useful - it also illustrates how exploited email accounts of IT staff can be used once the initial email has been successful.



Malware and other Malicious Software

This session addresses the basics of what malware is, and how user devices can become exposed to different kinds of malware, in the context of risks most typically encountered by women human rights defenders.

Introduction to Malware

Step 1: Explain to participants what malware is, and review a few of the types of malware that exist – at a minimum, it is recommended to cover the following:
Trojan Horse
Spyware
Ransom-ware
Keylogger
Viruses

Ransom-ware and keyloggers are increasingly common types of malware encountered by women human rights defenders in Latin America; if you are working with a group of women from that region, these will be important to address. Likewise, in general, make sure to include case studies and examples of malware that are commonly encountered in the context of the participants attending your training.

Part 2 – How Can You Get Infected?

Step 2: Explain some of the most common ways that devices become infected with malware, and the unsafe practices that can lead to such infections. It is also important to explain the different purposes or motivations behind malware deployments:

- Some malware is broadcast on a wide-scale with no particular target;
- Other kinds are specifically targeted at activists, journalists or dissidents to gain access to their data or communications;
- Still other kinds are targeted at individuals known to be connected to a number of activists, journalists or dissidents in the hope of infecting multiple targets across a network.

Part 3 - Share Examples Involving Women & Human Rights Defenders

Step 3: Finish the session by sharing examples of malware infection scenarios typically encountered by women and HRDs; you can also share specific case studies involving women and HRDs (from blogs, news or personal experience – always anonymize these unless you have explicit permission from the target to share their name)
Here there are a few general examples of cases, and you might also know similar cases to these in your context as well:

Malware and other Malicious Software

- A woman who received an email about an opportunity to get free tickets for a concert; the link within the email infected her smartphone with malware.
- A woman activist that received a message from what appeared to be the email of a colleague; after clicking the link within the email, her computer hard drive "encrypted" and a message appeared on her screen requiring payment in order to regain access to her information.

Other References:
https://anti-virus.comodo.com/blog/computer-safety/malware-vs-viruses-whats-difference/

Using Anti-virus Tools & Software

Walk through the most common scenarios for what to do when malware is found:
- Quarantining and removing malware
- What boot-time scans are
- When to use tools like Avira Rescue System
- The importance of conducting regular backups
- Being ready to re-install everything

Using Anti-virus on Work and Personal Computers

If participants are using their daily work computers or personal computers in the workshop, have them carry out a scan of their drives in the evening and have the anti-virus program quarantine any identified malware:
- Allot time on the next day of the training to ask what they found, if anything.
- If participants are finding malware, show them how to remove it, and show them how to perform a boot-time scan on the second evening of the training.
- If any infections require more in-depth assistance, set aside time for one of the trainers to provide 1:1 help.

If participants are not using work or personal computers, that aren't good candidates or available for scanning, instruct them on what to do when they return home:
- Download a non-portable apps version of anti-virus software from those suggested above, or one that you recommend.
- Scan their drives when they return home, remove any malware identified.
- Perform boot-time scans, and then any additional steps as needed.

If at all possible, work with the host organization and the participants to identify a trusted individual with the skills assist them, if necessary.

Deepening

Ask participants if they have questions before completing the session:

- Review the flip-chart notes from the session and see if any participants have questions.
- If any questions were tabled from previous sessions, revisit and answer them.

Approaches to dealing with malware should be both technical and behavioral. Using the lists from the Input section on "How we are Exposed to Malware," and "How to Avoid Malware," ask participants to identify which means of exposure and which solutions are behavioral or technical in nature, or a combination of both. Reiterate how technical solutions are not enough on their own.

You may also wish to ask specific questions to make sure some concepts are clearly understood:

- Ask participants what their plans are to protect themselves from malware.
- Do they feel like they have what they need going forward?
- Do they have colleagues or friends who can help them if they have questions or need in-depth assistance?

Reiterate if needed: Having a free version of an anti-virus application is better than no application at all, or a cracked version of a paid application.

Synthesis

We recommend that trainers use this wrap-up session for informal questions to the group, reviewing the material that has been covered in the module. The following questions may help participants think about using what they have learned:

However, many free versions of anti-virus programs do not protect against Trojans or Worms (you would have to visit the website of the developer for more details). For more complete protection, it's preferable to have a subscription version. Whereas most malware targets desktop computers, remind participants that mobile devices (as well as tablets) are also vulnerable.

Optional Activity
Quiz participants on the definitions of different types of malware, different ways it is transferred, and strategies for identifying suspected sources of malware and keeping your devices malware-free.

Synthesis

Optional Activity

Quiz participants on the definitions of different types of malware, different ways it is transferred, and strategies for identifying suspected sources of malware and keeping your devices malware-free.

Mobile safety

Learning Objectives

•Participants will learn how to protect their Smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing. Mobile security is also known as wireless security.
•After completing this module, participants will be able to turn off services like location and Bluetooth when not in use.

Other Resources
Here are some links that the trainer can make reference to.

1.https://whatis.techtarget.com/definition/mobile-security
2.https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/mobile-devices/
3.https://preyproject.com/blog/en/phone-security-20-ways-to-secure-your-mobile-phone/
4.https://searchmobilecomputing.techtarget.com/definition/smartphone

Introduction

Mobile safety is the practice of defending mobile devices against a wide range of cyber attack vectors that threaten users' privacy, network login credentials, finances, and safety. It comprises a collection of technologies, controls, policies, and best practices.

Activity

Phone swap:

This activity analyses the security of participants' phones in order to demonstrate how the lack of a code or password can leave their information vulnerable.

Conducting the Activity

- Ask the participants to swap phones
- Ask them to try accessing that phone they have been given.

The participant whose phone is accessed means that it wasn't secured.
When 10 minutes are left in the activity, asks teams to take turns •presenting their "risks list" and to explain why individual items on the list might create a risk.

Rewards like sweets can be given to those whose phones were difficult to access.

Discussion

1. Let the participants know why the activity is important.
2. Take the participants into a discussion to share their experiences of when their mobile devices were accessed by a third party just because it was not secured and ask these questions.

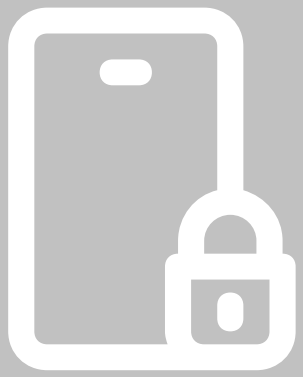
How did you react when your mobile device was accessed without your permission.

Did you have any compromising images/ messages on it.

If I asked for your phone right now, will bi be able to guess the password?

Deepening

Trainer gives the participants tips on how to ensure safety of their phones. This includes information on:
Phone passcodes.
Location sharing.
Bluetooth.
Privacy & security settings.



Phone Safety

1. Put a passcode on your phone.

Tell the participants that the easiest thing for them to do is to put a passcode on their phone. Having a passcode will make it harder for someone to pick up your phone to scroll through, access your accounts, or install something malicious. Also let them know that in the event that their phone gets stolen or they lose it, it'll make it a bit harder for others to get into their phone.

2. Turn off location sharing.

Encourage the participants that turning off location sharing is not only safe but also helps to increase the battery life on their phone.

3. Turn off Bluetooth when not using.

Tell participants that Bluetooth allows their phones to communicate with other devices, and if accessed by someone else though, they could misuse it to access their information or intercept calls. Turn off the Bluetooth on your phone and turn it on only when you need to connect with another device.

4. Encourage participants to check their privacy & security settings.

They can find these controls through the settings on the phone or through the settings of a specific app. These settings may allow you to limit an application's access to the data on your phone, including access to your location, pictures, contacts, notes, etc.

5. Encourage participants to review the apps they download

Because some apps could be accessing private information or could be a monitoring program that someone suspiciously installed.

6. Also encourage participants not to store sensitive information on their phone.

Although it may be tempting to store information such as passwords, account numbers, or personal information on their phone, the less sensitive information you have, the less likely someone else can access it. Advise them to consider deleting sensitive text messages or voicemails so they're not stored on their phone.

7. Train participants on using anti-virus and anti-spyware software on their phones.

They can search for programs in the app stores though some phones come with built-in software that they won't want to override.

Useful questions:

1. What is the main lesson or realization that you took from this session?
2. Where can you find the data an application has access to?
3. What would you do if a non-calling application required microphone permissions?

Alternative exercises include:

1. Fun exercises to test their knowledge on interpreting device problems
2. A test to see if participants can install applications

Synthesis

We recommend that trainers use this wrap-up session for informal questions to the group, reviewing the material that has been covered in the module. The following questions may help participants think about using what they have learned:

Appendix a.

Useful web resources:

Chapter 1 Digital Security:
YouTube videos on Digital Security
-Outsourced digital security content for trainer
knowledge enhancement e.g. COMP-SYO, Security
in a Box etc.
-Data collected in relation to digital security e.g.
policy papers, published digital security news etc.
-Information gathered during working career e.g.
focus group discussions, Online surveys etc.
-Digital tools e.g. VPNs, anti-virus protection, TAILS
-Digital Security Manuals and Handbooks (for
trainees) i.e. Decoding Online violence Handbook

Chapter 2 Digital Literacy:
Watch Vint Cerf, one of the 'fathers of the Internet' explain
how the Internet works through the links provided below:
•https://youtu.be/Dxcc6ycZ73M
•https://youtu.be/ZhEf7e4kopM
•https://youtu.be/5o8CwafCxnU
•https://youtu.be/AYdF7b3nMto

Chapter 3 Secure communication:
https://betterhumans.pub/how-to-communicate-privately-in-the-age-of-digital-policing-cf78ff2a79a7
https://searchsecurity.techtarget.com/definition/two-factor-authentication
https://www.youtube.com/watch?v=AMOtB7XkTT4

Chapter 4 Risk Assessment:
Refer to Risk assessment matrix
https://www.securityinabox.org
https://www.myshadow.org
Video: "SSL explained" (by Google)
Browser add-on: HTTPS Everywhere (by EFF.org)
Slides: The SSL Observatory (by EFF.org)
Article: All About HTTPS (Wikipedia)
Article: Vulnerabilities in the Certificate Authority System

Chapter 5 Data Protection and Privacy
Back up policy form https://level-up.cc/assets/files/backup_policy-blank.pdf
https://seguridaddigital.github.io/segdig/
https://securityinabox.org/en/guide/malware/
https://level-up.cc/curriculum/malware-protection/using-antivirus-tools/
https://securityinabox.org/en/guide/avast/windows/
https://securityinabox.org/en/guide/ccleaner/windows/
https://securityinabox.org/en/guide/backup/

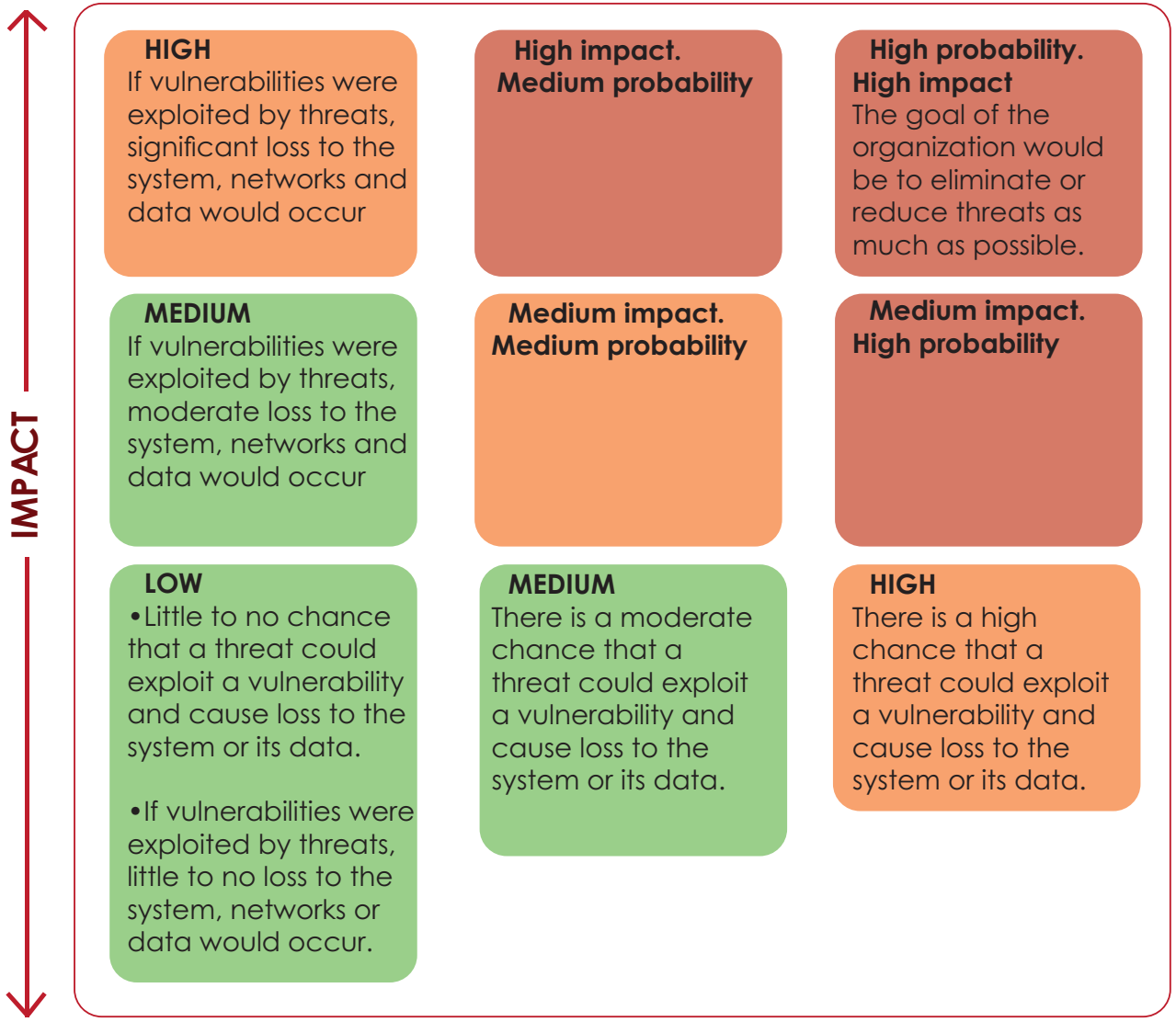
Chapter 6 Password management:
A simplified explanation of the Internet from WebFX
A great lesson on how the Internet works

Chapter 7 Device management:
https://securityinabox.org/en/guide/destroy-sensitive-information/
https://chayn.gitbooks.io/advanced-diy-privacy-for-every-woman/content/advanced-pclaptop-security.html
https://eraser.heidi.ie/
https://www.bleachbit.org/
https://www.piriform.com/recuva
https://veracrypt.codeplex.com/
https://guardianproject.info/code/luks/

Appendix b.

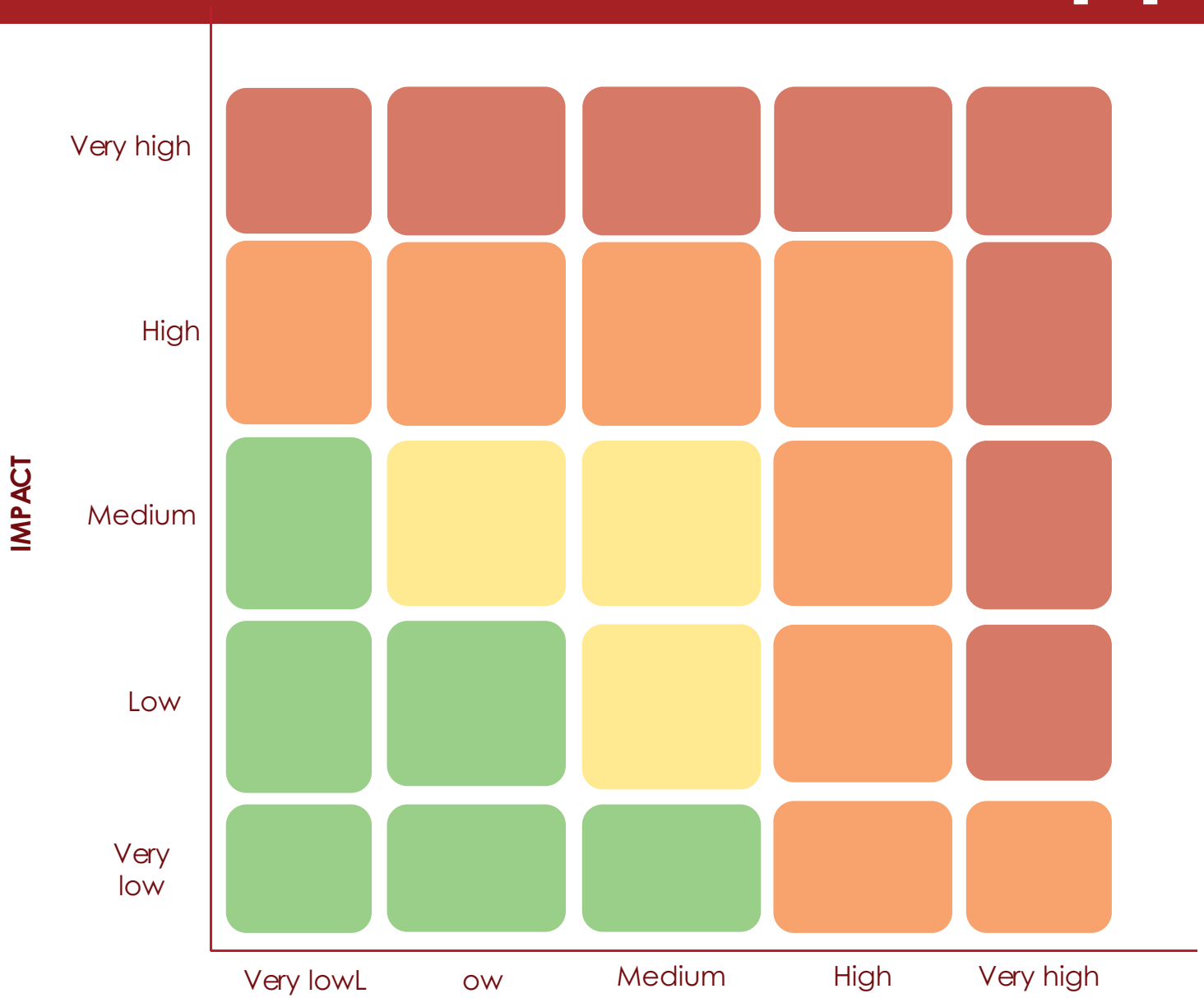
RISK IMPACT VS. PROBABILITY MATRIX

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



RISK MAP

Appendix c.



Appendix d.

ORGANIZATIONAL DIGITAL SECURITY PROTOCOL

Identified vulnerabilities (Which of our practices as individuals, or circumstances as an organization, could expose us to harm?)	**Strengths & Capacities** (What strengths do we have as an organization that give us an advantage in responding to identified threats and risks?)	**Mitigating actions** (What kind of measures do we need to take in order to mitigate the risks? To be better prepared for identified threats?)	**Resources needed** (What resources (economic, human, etc.) would we need to implement these actions?)	**Who Needs to be Involved?** (Which areas or people within our organization need to be involved in implementation? Will any sign-off or other permissions be required?)

BACKUP POLICY FORM

Appendix e.

Data Type	Master location	Backup location	Storage type	How often?	Type of backup (Full, incremental, Differential, Mirror)

DEFINITIONS

Data Type: A data type can be many things, ranging from a music file to an address book to a list of preferences for an application. Many people simply decide to back up an entire device instead of having tailored backup plans for different data types. Others may need to create specialized backup policies for particular data types due to the sensitivity of the data, travel (particularly crossing borders), and the amount of changes to one data type versus another over time (e.g., a large volume of video editing or sound recordings, an organization's email database), or to save space in the backup device.

Master copies are the "original" version of the data (e.g., the original photo or video taken, the first version of a document, etc.) For most people, this would be whatever is on their laptop or their mobile device.

Duplicates are a backup of the master copy.

Backup Location: This is where a backup is physically located.

Storage Device: What type of storage device are you using? This could be an external hard drive, a corporate cloud service (Google Drive, Dropbox), your own online server (ownCloud), or a small portable storage device like a USB flash drive.

Types of Backup: There are four common backup types implemented and generally used in most Backup programs: full backup, differential backup, incremental backup and mirror backup. A type of backup actually defines how data is copied from source to destination and lays the grounds of a data repository model (how the back-up is stored and structured).

Full Backup: The starting point for all other types of backup. Contains all the data in the folders and files selected for backup. Because full backup stores all files and folders, frequent full backups result in faster and simpler restore operations.

Incremental Backup: Stores all files that have changed since the last full, differential or incremental backup. The advantage of an incremental backup is that it takes the least time to complete. This can also make historical versions of your data available. (OSX's Time Machine is an example of an Incremental Backup.)

Differential Backup: Contains all files that have changed since the last FULL backup. The advantage of a differential backup is that it shortens restore time compared to a full backup or an incremental backup.

Mirror Backup: Identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the source data

Appendix f.

RISK ASSESSMENT WORKSHEET 1

Date:
Group:
Name/ Organization:

1. AWAY FROM THE OFFICE

VULNERABILITY	SOURCE OF RISK	RISK LEVEL (Low, medium, high)	POSSIBLE SOLUTION
Do you or your colleagues travel with lap tops and phones and have a way to make these devices physically secure where you stay? (Do you keep your devices with you at all times or have a lock to physically secure them?)	Examples: Loss (forgotten) Theft from other travelers or pickpockets Confiscation by authorities	Example: Medium	Example: Bring cable and lock on trips Keep laptop in carry-on luggage and keep carry-on nearby Keep phone hidden inside pocket
Do staff members take office laptops and work information home? What precautions are taken to reduce the risk of theft?			

Additional notes/discussion points about security away from the office:

RISK ASSESSMENT WORKSHEET 2

Date:
Group:
Name/ Organization:

Appendix g.

2. YOUR BUILDING

VULNERABILITY	SOURCE OF RISK	RISK LEVEL (Low, medium, high)	POSSIBLE SOLUTION
Are points of entry to the office (doors and windows) protected with locks?			
Do you or your colleagues stand outside the office with the doors open (to smoke, to make personal cell phone calls)?			
Are windows at ground level normally open during the day and left unattended?			
Is your office Internet and telephone con nection easily accessible from a circuit box on the outside of your building?			
As far as you know, is your office current ly under surveillance from a neighboring building?			
How does your office monitor office visitors prior to giving them entry into the office? (Does it have a glass door, peep hole, video cameras and/or other means to monitor visitors?)			
Does the office have security protocols for allowing visitors that may not be known to all staff members (ID check, cell phone deposit, metal detector, body scan, etc.)?			

Additional notes/discussion points about security in your building:

RISK ASSESSMENT WORKSHEET 3

Date:
Group:
Name/ Organization:

Appendix h.

3. IN THE OFFICE

VULNERABILITY	SOURCE OF RISK	RISK LEVEL (Low, medium, high)	POSSIBLE SOLUTION
Can guests who walk into the office imme diately see your computer screen(s), white boards or other places where business information is visible?			
Are story meetings and team meetings held in open spaces where visitors who are not involved may hear?			
Are network devices like your routers, hubs or modems kept in secure rooms or cabinets so that intruders won't have direct access to them?			
Are your desktop computers and laptops attached to a security cable with a lock to prevent theft?			

Additional notes/discussion points about security away in the office:

RISK ASSESSMENT WORKSHEET 4

Date:
Group:
Name/ Organization:

Appendix i.

4. COMMON ELECTRIC RISKS

VULNERABILITY	SOURCE OF RISK	RISK LEVEL (Low, medium, high)	POSSIBLE SOLUTION
Do power strips or wall sockets consis tently spark when you plug a device into them, indicating a fire hazard?			
Are computers and other sensitive equip ment kept in direct sunlight, which could potentially lead to overheating?			
Do computers kept inside cabinets have adequate ventilation to avoid overheating?			
Do you use an uninterruptible power sup ply (UPS) in your office? (A UPS stabilizes the power reaching your PC and can provide temporary power in the event of a blackout.)			
Are your PCs and cables kept clear from hallways, reception areas and other places where people walk frequently?			
Are your network cables away from win dows where rain might damage them and cause an electrical short?			

Additional notes/discussion points about common electrical risks:

Appendix j.

RISK ASSESSMENT WORKSHEET 5

Date:
Group:
Name/ Organization:

5. MOBILE PHONES

VULNERABILITY	SOURCE OF RISK	RISK LEVEL (Low, medium, high)	POSSIBLE SOLUTION
Do staff members leave phones in plain view when meeting in public places (e.g., on the table at a cafe)?			
Do staff members keep phones with them at all times? (This is advised during the work day, unless reporters wish to avoid broadcast ing their physical location.)			

Additional notes/discussion points about common electrical risks: