




Digital Security Training Curriculum

Version 1.1.3. Last updated: Nov 05, 2021

TABLE OF CONTENTS

Digital Security Training Curriculum	1
1.1 Background and Scope	2
1.2 Points of Contact	5
1.3 Document Organisation	5
2.0 Instructional Analysis	6
2.1 Needs and Skills Analysis	6
2.2 Development Approach	10
2.3 Issues and Recommendations	10
3.0 Instructional Methods	11
3.1 Training Methodology	11
3.2 Testing and Evaluation	11
4.0 Training Curriculum	12
Session 1: Personal Introduction and Pre-training Test	12
Session 2: Introduction to Digital Security	13
Session 3: Threat Modeling	15
Session 4: Awareness and Preparation on Digital Hygiene	16
Session 5: Malware, Antivirus' and Malware Removal Tools	18
Session 6: Browser Security	20
Session 7: Passwords, Password Managers, and 2FA	22
Session 8: Security and Privacy Settings on Social Media	24
Session 9: How the Internet Works	26
Session 10: Encryption and Encrypting Internet Traffic	28
Session 11: File and Folder Security	30
Session 12: Data Backup	32
Session 13: Email Encryption	34
Session 14: Mobile Phone Security	36
Session 15: End-to-end Encryption and Mobile Communication	38
Session 16: How to Prepare for the Next Training	40
5.0 Glossary	42



This is a digital security training curriculum developed by EngageMedia, to be translated and localised by country partners of the Greater Internet Freedom (GIF) project to suit their needs and contexts.

1.1 BACKGROUND AND SCOPE

Digital technology has become prevalent and ingrained in our ways of life today. These technologies are making our lives easier through faster communication, easy storing and sharing of information, among others. Everything is being digitised. However, these technologies come with great security risks. People can no longer solely rely on the usual security solutions, like antivirus software and firewalls. Cybercriminals are getting smarter, and their tactics are becoming more resilient to conventional cyber defenses. Digital threats can come from anywhere. And we must educate ourselves about simple social engineering scams, like phishing and more sophisticated cybersecurity threats, such as ransomware attacks, to protect ourselves from malicious attempts to steal intellectual property or personal data.

Digital security and privacy are important. For human rights advocates, journalists, activists, and ordinary citizens, the possibility of your communications being monitored or your personal identity or location being exposed present considerable risks, especially if you are working with sensitive information. A thorough digital security strategy is essential, as it will only be as strong as its weakest link.

The digital risks that activists, journalists, digital rights defenders, academics, and marginalised groups face have grown substantially over the past few years. Such risks often arise in authoritarian regimes pushing for digital policies that violate and criminalise citizens' fundamental rights, such as their right to assembly, association, and freedom of expression online. Both at the policy level and during implementation on the ground, many governments currently engage in the

circumvention of encryption and investment in mass surveillance technology, while censoring citizen voices online. Such common internet freedom challenges that transcend country borders led to the formation of the Greater Internet Freedom (GIF) project.

Training is a critical part of the GIF project and will help increase the capacity of civil society organisations (CSOs), media outlets, and individuals in both preventative and responsive digital safety approaches. It will also increase the number of local digital safety experts able to advance the digital safety capabilities of civil society and media organisations and individuals.

Through this training program, participants will be able to enhance their knowledge on the following digital security concepts:

- Risk assessment
- Digital hygiene
- Malware and protections
- Free and open source software (FOSS)
- Browser security and privacy
- Password management
- File and folder protections
- Backups
- Data and communication encryption
- PGP and email encryption
- How the internet works and network encryption with virtual private networks (VPN) and Tor
- Privacy and security on social media
- Risks associated with mobile phones and use of secure communication tools
- Training planning and preparations

1.2 POINTS OF CONTACT

The content of this training curriculum is based on previous training experience and may need to be adapted for specific contexts and training needs. Please feel free to contact the following for assistance with your training curriculum.

Role	Name	Contact
Project Lead	Vino Lucero	vino@engagemedia.org
Curriculum Developer	Md. Ashraful Haque	ashraf@engagemedia.org

1.3 DOCUMENT ORGANISATION

This curriculum document is created by EngageMedia for GIF country partners in designing their digital security curriculum.

The curriculum document is open source, licenced under [Creative Commons BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/). This means you are free to **share** (copy and redistribute the material in any medium or format) and **adapt** (remix, transform, and build upon the material) the document for any purpose, even commercially, as long as you **attribute** and give appropriate credit to EngageMedia, and **ShareAlike**.

2.0 INSTRUCTIONAL ANALYSIS

2.1 NEEDS AND SKILLS ANALYSIS

Before each training session, it is recommended that participants undertake a needs and skills analysis. Each participant is different and they have different work areas, which would translate to differences in their needs and the security risks they face. It is also good to know about the participants' existing knowledge level to choose the most appropriate topics and training methodologies.

Skill Assessment Template:

Please answer the following questions to determine your skills and needs. The results of this assessment will help us design a better training program for you. Please keep in mind that some questions may have two or more correct answers; choose what you think is best.

1. What is the most important principle in digital security?
 - Update antivirus program
 - Update operating system
 - Trust no one
 - Don't open email attachments
2. How many characters should your password have at minimum?
 - 8 characters long
 - 14 characters long
 - 20 characters long
 - 25 characters long

3. Why is password complexity important?

- It makes the password much more difficult to crack by using software techniques such as through brute force
- It makes the password encryption longer
- It makes the password more difficult to guess
- It makes the password more difficult to understand

4. How would you protect your computer from physical tampering?

- Format your hard disk
- Encrypt your entire hard disk
- Encrypt your documents
- Lock your computer

5. Where do you keep your backup files?

- On a separate drive on the same computer
- On a hidden folder on the same computer
- I do not keep any backups
- On a separate device and location

6. How do I check if a website is using HTTPS?

- I check for "https" in the header
- I look at the padlock in the URL bar
- I check the digital certificate
- I check the name in the URL

7. What is a secure way for sending and receiving emails?

- Secure mail
- SMTP
- FTP
- PGP

8. What would I need to send you an encrypted email?

- Your private key
- Your public key
- Both your keys
- None

9. What do you do with your open accounts (email, Twitter, Facebook...) before you turn off your computer?
- Just close the lid of the laptop
 - Close the browser then turn off the computer
 - Log out of the accounts, close the browser, then turn off the computer
 - Push the power button until the computer turns off
10. Should you save the passwords in your browser to be able to access your account easily?
- Yes
 - No
11. Should you use a different password for each account? Or one password for all accounts so you don't forget it and lose your account?*
- One for all accounts
 - A different password for each account
12. How would you know which operating system you have on your computer?
- By contacting the manufacturing company
 - It is written on the back of the computer
 - Right click on My Computer and click on Properties
 - I take it to the repair shop and they will tell me
13. Using more than one antivirus program provides more protection.
- Yes
 - No
14. What do rootkits do?
- Hide viruses and Trojans from detection
 - Hide files
 - Stop antivirus programs
 - Install malware
15. Is formatting a hard drive good enough to delete your data?
- Yes
 - No

16. In order to protect your computer from USB and CD viruses...
- I should not use any USB
 - I should disable auto run on Windows
 - I should scan my computer
 - I should do nothing
17. If you receive a link or attachment in an e-mail from your friend that you were not expecting, what do you do?
- Check it and decide whether to open it or not
 - Open it because you have a good antivirus that protects your computer
 - Contact the sender and check if he sent it, then check and open it
 - Open it because the firewall is activated; nothing can harm your computer
18. Before you install an app on your mobile, what should you check?
- What permission it needs
 - Who developed it
 - If it reveals my location
 - If it consumes a lot of bandwidth
19. If you have an important meeting and you don't want the mobile company to know your location, what do you do?
- Turn off GPS on the mobile
 - They can't know my location my phone is old and doesn't have GPS
 - Before the meeting starts, turn off the phone and remove the SIM card
 - Turn the mobile off and remove the battery before you leave home
20. To protect your mobile from anyone trying to access it:
- Use a passcode
 - Use full device encryption
 - Use a passcode for the SIM card
 - Use a pattern to unlock and open the phone

2.2 DEVELOPMENT APPROACH

There may be a need to redevelop or redesign this training curriculum. Please complete the needs and skills survey and analyse it before contacting EngageMedia for assistance with curriculum development and to discuss adjustments and possible next steps.

2.3 ISSUES AND RECOMMENDATIONS

Conducting a risk assessment before the training is recommended. Based on the assessment, make preparations and expect the unexpected. Always prepare a backup plan. While planning for a training session, consider the following:

- **What kind of training needs to be delivered – and to whom?** Session planning needs to be done based on the survey data of target participants. Choose relevant participants and topics.
- **Who conducts the training?** The outcome of the training mostly depends on the person who will facilitate the training program. Skilled and experienced trainers with good knowledge and command of the topics should be considered for training facilitation.
- **Who develops the training materials and environment?** While EngageMedia developed this curriculum template, each training program will need to be tailored to suit local contexts.
- **How will the training program cater to a diverse group of participants?** During the training, the participants will be from diverse communities and organisations. They will have different ages, genders, beliefs, work areas, etc. They will also have different learning habits and styles. The training program needs to be managed, keeping this diversity in mind.
- **What is the local environment like during the training?** Learn about the local political and social environment prior to organising the training to ensure a safe and suitable learning environment for participants.

3.0 INSTRUCTIONAL METHODS

3.1 TRAINING METHODOLOGY

While training methodology is contextual and varies for each training program, we recommend following the Activity-Discussion-Inputs-Deepening-Synthesis (ADIDS) training methodology. 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.

Learn more at: <https://level-up.cc/before-an-event/preparing-sessions-using-adids/>

3.2 TESTING AND EVALUATION

It is recommended to have multiple tests and evaluations during the course of the training program.

- **Pre-training** – To learn about a participant’s existing knowledge and to plan relevant sessions, an online survey is recommended. Ask a few questions related to the participant’s work and the training agenda.
- **In-training** – During the training, feedback from participants may be collected after each session to improve future sessions.
- **Post-training** – At the end of the training program, another test is recommended to assess improvements in participants’ knowledge and skills.

4.0 TRAINING CURRICULUM

SESSION 1

PERSONAL INTRODUCTION AND PRE-TRAINING TEST

DESIRED LESSON OUTCOMES

Participants and trainers get to know each other.
Participants' baseline knowledge and skills are measured.

Session Type:

- Introduction and activity

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none">1 Understand the concepts for this training.2 Get to know each other.3 Learn how to organise a pre-training test.4 Learn how to apply the concepts of the introduction session and apply it to future training.
ADDITIONAL RESOURCES	<ul style="list-style-type: none">• https://internews.org/• https://engagemedia.org/
SESSION GUIDE	<ul style="list-style-type: none">• Trainer will make an introductory speech about the training and self-introduction.• Trainer will open the floor for participants' introductions.• Trainer will set ground rules and the training environment.• Trainer will conduct the pre-training test with an online survey form. Questions should be related to the training and participants' work area

SUMMARY OF THE SESSION

N/A

SESSION 2

INTRODUCTION TO DIGITAL SECURITY

DESIRED LESSON OUTCOMES

Participants learn what digital security is and why it is important. They also learn about free and open source software (FOSS).

Session Type:

- Activity-Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none">1 Understand what holistic security is.2 Understand the importance of self-care in digital safety.3 Understand the relevance of holistic security in our lives and our work.4 Learn about free and open source software (FOSS).
ADDITIONAL RESOURCES	https://holistic-security.tacticaltech.org/
SESSION GUIDE	<ul style="list-style-type: none">• Trainer will play a short video about digital security incidents.• Trainer will discuss what holistic security is and why self-care is important for us.• Participants will share their thoughts on the topic.• Trainer will introduce FOSS.

SESSION 2

INTRODUCTION TO DIGITAL SECURITY

SUMMARY OF THE SESSION

Digital security is the collective term that describes the resources employed to protect your online identity, data, and other assets. These tools include web services, antivirus software, smartphone SIM cards, biometrics, and secured personal devices.

In a nutshell, digital security means protecting your computer, mobile devices, tablets, and any other internet-connected devices from intruders, which could be in the form of hacking, phishing, and more. Practicing digital security also protects your personal data from being used and sold by companies. Cybersecurity is important because it protects all kinds of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, and governmental and industry information systems. When any aspect of your digital security is relaxed, all of your personal information – your credit cards, bank accounts, email accounts, your whole identity – could be at risk.

Holistic security is an integrated approach to digital, physical, and psycho-social security for individuals and organisations. The aims of a holistic approach to security and protection of activists and human rights defenders (HRDs) include:

- Fortifying the sustainability of activism in the context of violence (as understood broadly and intersectionally)
- Fortifying activists' capacities to reflect, learn, and take preventive measures to improve their security and protection
- Fortifying activists' resilience and capacity to respond creatively during times of crisis.

FOSS: Open source software offers flexibility, collaboration, and enhanced security. Open-source software is computer software released under a licence where the copyright holder grants users the rights to use, study, change, and distribute the software and its source code to anyone and for any purpose. Open-source software may be developed in a collaborative public manner.

SESSION 3

THREAT MODELING

DESIRED LESSON OUTCOMES

Participants can assess and identify risks.

Session Type:

- Activity-Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none"> 1 Learn about threat modeling. 2 Learn to assess personal and organisational risks.
ADDITIONAL RESOURCES	https://ssd.eff.org/en/module/your-security-plan
SESSION GUIDE	<ul style="list-style-type: none"> • Trainer will present a threat modeling flowchart and discuss the processes step by step. • Trainer will present examples of organisational or personal risks. • Participants will be asked to assess the mentioned risk within the model. • Trainer will discuss participants' assessments of risk based on the discussed model and correct any errors or misconceptions.

SUMMARY OF THE SESSION

Security is a process, and through thoughtful planning, you can put together a plan that's right for you. Security isn't just about the tools you use or the software you download. It begins with understanding the unique threats you face and how you can counter those threats.

- What do I want to protect?
- Who do I want to protect it from?
- How bad are the consequences if I fail?
- How likely is it that I will need to protect it?
- How much trouble am I willing to go through to try to prevent potential consequences?

Once you have asked yourself these questions, you are now in a position to assess what measures to take.

Think of risk assessment this way: If your possessions are valuable, but the probability of a break-in is low, then you may not want to invest too much money in a lock. But if the probability of a break-in is high, you'll want to get the best lock on the market and consider adding a security system. Making a security plan will help you understand the threats that are unique to you and the likelihood of risks you face. This will enable you to better evaluate your assets, your adversaries, and your adversaries' capabilities.

SESSION 4

AWARENESS AND PREPARATION ON DIGITAL HYGIENE

DESIRED LESSON OUTCOMES

Participants are aware about the concept of digital hygiene and are prepared to put this in practice.

Session Type:

- Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none">1 Learn basic awareness on digital security.2 Learn about digital hygiene practices.
ADDITIONAL RESOURCES	https://coconet.social/digital-hygiene-safety-security/
SESSION GUIDE	<ul style="list-style-type: none">• Trainer will discuss basic awareness on digital security, including do's and don'ts, hardware and software security, understanding behavioural changes, etc.• Participants will be asked to share their current digital security practices.• Trainer will expound on the concept based on participants' input.

SESSION 4

AWARENESS AND PREPARATION ON DIGITAL HYGIENE

SUMMARY OF THE SESSION

No doubt, the internet can be an extremely useful tool for people. But instant messaging, chat rooms, emails and social networking sites can also bring trouble – from cyberbullying to invasion of privacy and identity theft.

Digital safety, frequently referred to as internet safety, media safety, online safety, or cyber safety, encompasses many things. At its core, digital safety is about protecting ourselves, our families, and others as we connect through digital devices. The new ways of interacting digitally facilitate real world interaction. Digital safety is important because it protects people from risks such as identity theft and fraud. If you follow the steps below, then your digital security will be strengthened and your information made more secure.

- 1 Do not share your financial information with anyone.
- 2 When you open an email, be sure to check the sender details.
- 3 Do not click on any links before confirming its destination.
- 4 Attachments can be dangerous; scan with antivirus before opening.
- 5 Always download the software from the original (official) website.
- 6 Prioritise using open source software.
- 7 Change your security habits online and offline.
- 8 Sign out of all accounts before shutting down the computer.
- 9 Always be careful. Understand where you are clicking – think before you click.
- 10 Do not open any of your accounts on another person's computer or mobile.
- 11 Do not lend your device to others. In case you need to do so, be sure to keep an eye on how your device is being used
- 12 Keep your device updated regularly.
- 13 Do not use hotels, cyber cafes or public networks unless you take necessary action to make the connection secure (such as connecting using VPN or Tor). If you need to use other computers, use a secure and portable OS like Tails.
- 14 Be aware of what you are publishing online.
- 15 Carry only the necessary personal data / information with you.
- 16 Maintain a pseudonym for your privacy.
- 17 Use encryption to exchange information.
- 18 Digital security is not just a matter of protecting yourself; help others protect their digital information as well.

SESSION 5

MALWARE, ANTIVIRUS' AND MALWARE REMOVAL TOOLS

DESIRED LESSON OUTCOMES

Participants learn about types of malware. They understand the importance of using antivirus software and the use of malware removal tools.

Session Type:

- Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none">1 Understand the dangers on the internet and everyday devices.2 Learn about different types of malware.3 Understand the importance of using antivirus software.4 Understand the differences between paid and free antivirus software.5 Learn different malware removal tools and methods.
ADDITIONAL RESOURCES	<ul style="list-style-type: none">• https://www.malwarebytes.com/ Malware removal tools• https://www.avira.com/ Free/paid antivirus• https://www.avast.com/ Free/paid antivirus• https://virustotal.com/ Online malware scanner• https://level-up.cc/curriculum/malware-protection
SESSION GUIDE	<ul style="list-style-type: none">• Trainer will discuss common digital threats on online and everyday devices.• Trainer will discuss types of malware.• Participants will be asked to share their experiences with encountering malware and the actions taken.• Trainer will discuss the importance of using antivirus software and the core similarities of free and paid antivirus software.• Participants will learn about malware removal tools and they will be asked to perform a malware scan during the session for a hands-on learning experience.

SESSION 5

MALWARE, ANTIVIRUS' AND MALWARE REMOVAL TOOLS

SUMMARY OF THE SESSION

Malware is a contraction of “malicious software.” Malware is intrusive software that is designed to damage and destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. To protect your system from malware, follow the steps below:

- Check the last part of the file name (extension). If the file extension is not familiar to you, do not open the file.
- Don't make a decision to open or run the file just by looking at the file icon. File icons can be altered using software.
- If the file extension is hidden, turn it on.
- In many cases, your computer can become infected by connecting an external device. To prevent this:
 - Keep your computer's operating system updated.
 - Disable autorun options on your computer.
 - Use an antivirus and scan properly before opening an external device.
- Do not use software obtained through untrusted and unverified sources. They may be carrying malware.
- Buy the antivirus, if possible, or use the free version.
- Keep the antivirus database updated regularly.
- Malware removal tools can fix infected files or systems. It is by no means an antivirus alternative.
- Most antivirus companies offer a variety of free malware removal tools.
- To be safe from malware or phishing links, make sure to scan any file, link or login page before opening it.

SESSION 6

BROWSER SECURITY

DESIRED LESSON OUTCOMES

Participants learn about web browser security and privacy.

Session Type:

- Activity-Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
<p>LEARNING OBJECTIVES</p>	<ol style="list-style-type: none"> 1 Learn how to choose a good browser. 2 Understand browser security settings and privacy using tools/extensions. 3 Learn the difference between HTTP and HTTPS. 4 Learn how to identify phishing and fake links. 5 Learn how to use DuckDuckGo or StartPage as search engines instead of Google.
<p>ADDITIONAL RESOURCES</p>	<ul style="list-style-type: none"> • https://brave.com/ Open-source browser • https://www.mozilla.org/ Open-source browser • https://www.eff.org/https-everywhere HTTPS redirection extension for browser • https://duckduckgo.com/ Google alternative search engine • https://adblockplus.org/ Advertisement and tracker removal extension for browser • https://level-up.cc/curriculum/safer-browsing/
<p>SESSION GUIDE</p>	<ul style="list-style-type: none"> • Trainer will discuss a few open-source web browsers and encourage their use. • Trainer will discuss some common browser security and privacy settings. • Trainer will discuss the importance of HTTPS and SSL. • Trainer will introduce participants to the search engines DuckDuckgo and StartPage. • Trainer will discuss phishing and fake links along with some common scams on the internet.

SESSION 6

BROWSER SECURITY

SUMMARY OF THE SESSION

An internet browser translates the code that computers use to create websites into the text, graphics, and other features of the web pages that we're used to seeing today. Web browsers have evolved significantly since they were first introduced in 1990. Any good web browser has to be very secure and able to protect you from any data breaches. Here are some setting suggestions:

- Use open-source web browsers such as Brave, Firefox, or Chromium.
- Never save your passwords in your browser settings.
- Do not install add-ons that are not trusted.
- Turn off browser history and regularly clear your browser cache and cookies. Alternatively, you may use private browsing, but keep in mind that it will not give you as much anonymity compared to using Tor.
- Disable Java and Flash if not needed.
- Use DuckDuckGo or StartPage for search privacy.
- Do not login to any site that does not have HTTPS. Be careful during online transactions.
- The HTTPS version of the web URL is more secure compared to HTTP.
- Fake login pages may look exactly the same as legitimate pages. Check the part before the first slash (/) in the URL.

SESSION 7

PASSWORDS, PASSWORD MANAGERS, AND 2FA

DESIRED LESSON OUTCOMES

Participants are able to create strong passwords and to manage passwords with a secure password manager. Participants learn how to use two-factor authentication (2FA).

Session Type:

- Activity-Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none"> 1 Understand the importance of strong and unique passwords. 2 Learn how to create a good password. 3 Learn about password safety. 4 Learn about using a password manager. 5 Learn about two-factor authentications.
ADDITIONAL RESOURCES	<ul style="list-style-type: none"> • https://keepassxc.org/ Open-source password manager • https://authy.com/ 2FA app and guides • https://ssd.eff.org/en/module/creating-strong-passwords
SESSION GUIDE	<ul style="list-style-type: none"> • Trainer will discuss the importance of a strong password and teach participants how to create a secure password. • Trainer will discuss the safety measures that should be taken when using passwords. • Trainer will introduce KeePassXC (an open-source password manager) and provide a step-by-step guide for participants. • Trainer will discuss 2FA, why it is important, and how to integrate it into digital security practices.

SESSION 7

PASSWORDS, PASSWORD MANAGERS, AND 2FA

SUMMARY OF THE SESSION

Passwords provide the first line of defence against unauthorised access into your computer and personal information. The stronger your password, the more protected your computer will be from hackers and malicious software. You should maintain strong passwords for all accounts on your computer. To create a strong password and to secure it, here are some suggestions:

- **Length** – Use a password of at least 14 characters.
- **Combination** – Use numbers, symbols, uppercase and lowercase letters, and spaces, if possible, in your password.
- **Random** – Do not use the same structure in all cases and avoid words that are in the dictionary.
- **Relationships** – Avoid using personal information in your password.
- **Remember** – Use a password that you can remember.
- **Privacy** – Keep it a secret; don't share your password with anyone.
- **Save** – Do not write your password on paper or in a text file.
- **Unique** – Do not use the same password elsewhere.
- If possible, add a security screen to your device. This prevents people in your immediate vicinity from seeing your device screen.
- When inputting a password, make sure that no one around you can view your password.
- Create a cover when entering the PIN at the ATM booth.
- Make sure there are no cameras or mirrors nearby.
- Do not enter your password on a device that is not your own.
- Understand the password recovery process for all of your accounts.
- When logging in, make sure that the website is using HTTPS and that the SSL certificate is valid.
- Enable non-SMS or call based 2FA where possible. Use an open-source app or hardware based 2FA.
- Use an open-source password manager that keeps the database encrypted. KeePassXC is a free and open-source password manager. It started as a community fork of KeePassX. It is a multi-platform application which can be run on Linux, Windows, and macOS.

SESSION 8

SECURITY AND PRIVACY SETTINGS ON SOCIAL MEDIA

DESIRED LESSON OUTCOMES

Participants can adjust their security and privacy settings on social media.

Session Type:

- Activity-Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none">1 Understand risks in using social networks and learn about precautions.2 Learn about social engineering.3 Learn about security and privacy settings on social network sites.
ADDITIONAL RESOURCES	<ul style="list-style-type: none">• https://youtu.be/F7pYHN9iC9I Video for social media awareness• https://level-up.cc/curriculum/social-media-safety/• https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering• https://www.csoonline.com/article/2124681/what-is-social-engineering.html• https://ssd.eff.org/en/module/protecting-yourself-social-networks
SESSION GUIDE	<ul style="list-style-type: none">• Trainer will play a video regarding social media awareness.• Trainer will discuss risks that users face on social media and how to prevent them.• Participants will be asked to share their personal or organisational experiences with social media usage and any previous incidents.• Trainer will discuss the concept of social engineering.• Trainer will guide participants in step-by-step adjustments of their security and privacy settings on popular social media platforms.

SESSION 8

SECURITY AND PRIVACY SETTINGS ON SOCIAL MEDIA

SUMMARY OF THE SESSION

Social engineering is a method of manipulating people so that they give up confidential information. The types of information social engineers seek vary, but when individuals are targeted, typically, they are usually trying to trick you into giving them your passwords or bank information. They may also try to secretly install malicious software that will give them control over your computer and access to your personal information.

- The risks you need to be aware of are:
 - cyberbullying (bullying using digital technology)
 - information theft and identity theft
 - invasion of privacy
 - offensive images and messages targeted to children
 - the presence of strangers who may be there to 'groom' other members
- Social engineering attacks come in many different forms and can be performed anywhere human interaction is involved. Social engineers manipulate human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps. Therefore, be wary whenever you feel alarmed by an email, attracted to an offer displayed on a website, or curious when you come across any kind of digital media.
 - Don't open emails and attachments from suspicious sources
 - Use multifactor authentication
 - Be wary of tempting offers
 - Keep your antivirus and /anti-malware software updated
- Social networks are full of dangers, which could have profound consequences on you or your business. You can avoid many of these pitfalls just by using these networks carefully. The following additional measures often help:
 - Set up your privacy settings so that only friends have access to your posts
 - Avoid posting personal information, holiday plans, etc.
 - Do not accept requests or messages from people you don't know
 - Avoid clicking on shortened URLs
 - Report suspect or insulting and threatening accounts
 - Keep personal and work accounts separate

SESSION 9

HOW THE INTERNET WORKS

DESIRED LESSON OUTCOMES

Participants learn how the internet works.

Session Type:

- Activity-Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none"> 1 Learn how the internet works and how data is transferred from one end to another. 2 Learn how many actors are involved in the network and the corresponding risks involved. 3 Understand basic router security.
ADDITIONAL RESOURCES	<ul style="list-style-type: none"> • https://academind.com/tutorials/how-the-web-works/ • https://www.youtube.com/watch?v=7_LPdttKXPc • https://vahid.blog/post/2020-12-15-how-the-internet-works-part-i-infrastructure/
SESSION GUIDE	<ul style="list-style-type: none"> • Participants will be asked to share their knowledge and understanding of how the internet works. • Trainer will present a video explaining how the internet works. • Trainer will explain how data transfer works over the internet by presenting an example (such as sending emails or use of website browsers) to explain how data travels from end to end. • Trainer will discuss all the possible actors involved in the network and the associated risks. • Trainer will discuss basic router security settings.

SESSION 9

HOW THE INTERNET WORKS

SUMMARY OF THE SESSION

- The internet is a worldwide computer network that transmits a variety of data and media across interconnected devices. It works by using a packet routing network that follows Internet Protocol (IP) and Transport Control Protocol (TCP).
- The internet is the wider network that allows computer networks run by companies, governments, and other organisations around the world to talk to one another.
- The internet simply moves data from one place to another, so that we can chat, browse, and share information.
- Physically, the internet is a collection of computers moving bits to each other over wires, cables, and radio signals.
- A wireless router connects directly to a modem by a cable. This allows it to receive information from – and transmit information to – the internet. The router then creates and communicates with your home Wi-Fi network using built-in antennas. As a result, all the devices in your home network have internet access.
- This is how you browse a website: Your device \leftrightarrow Router \leftrightarrow ISP \leftrightarrow DNS \leftrightarrow Web Server
- The internet is not always secure. If you do not take precautions, others may gain access to your unencrypted personal information.
- Basic router security settings:
 - Change default password.
 - Change the default wifi name.
 - Use a good password for wifi.
 - Use WPA2/3 encryption and avoid WEP.
 - Hide wifi ID if needed.
 - Do not share your network with others. If needed, create a guest network.

SESSION 10

ENCRYPTION AND ENCRYPTING INTERNET TRAFFIC

DESIRED LESSON OUTCOMES

Participants learn what encryption is and how to encrypt their internet traffic.

Session Type:

- Activity-Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none"> 1 Understand what encryption is. 2 Understand what a VPN is and how to choose a good VPN. 3 Understand what TOR is and how it works.
ADDITIONAL RESOURCES	<ul style="list-style-type: none"> • https://aesencryption.net/ Online text encryption platform • https://aescrypt.com/ Small tools to encrypt files with password • https://torproject.org/ Official site of TOR • https://www.tunnelbear.com/ Paid VPN <ul style="list-style-type: none"> • https://engagemedia.org/tunnelbear– free one-year TunnelBear VPN subscription • https://www.psiphon3.com/ Free VPN • https://www.f-secure.com/en/home/articles/6-things-to-consider-when-choosing-a-vpn • https://engagemedia.org/2021/indonesia-vpn/ • https://www.eff.org/pages/tor-and-https How HTTPS and Tor Work
SESSION GUIDE	<ul style="list-style-type: none"> • Participants will be asked to explain how they understand encryption. • Trainer will discuss what encryption is and why it is important. • Participants will be asked to share if they previously faced any website block or circumventions, and if so, how they solved these. • Trainer will discuss what a VPN is, how it works, and why we need to use VPNs. Trainer will explain what factors should be considered when choosing a VPN. • Trainer will explain how the TOR network works.

SESSION 10

ENCRYPTION AND ENCRYPTING INTERNET TRAFFIC

SUMMARY OF THE SESSION

- Encryption is the process of taking plain text, like a text message or email, and scrambling it into an unreadable format called “ciphertext.” This helps protect the confidentiality of digital data stored on computer systems or transmitted through a network like the internet.
- A virtual private network (VPN) protects your identity and browsing activity from hackers, businesses, government agencies, and other snoops. When connecting to the internet, your data and IP address are hidden by a type of virtual tunnel. This keeps others from spying on your online activity.
- When choosing a VPN:
 - Check the security experience of the VPN provider
 - Check your VPN’s privacy policy
 - Check the number of server locations
- Tor is free and open-source software for enabling anonymous communication. It directs internet traffic through a free, worldwide, volunteer overlay network consisting of more than 7,000 relays to conceal a user’s location and usage from anyone conducting network surveillance or traffic analysis.
- How Tor works:
 - It makes connections for you through three random Tor nodes.
 - None of the nodes know the origin and destination of the other connections.
 - All traffic from you to the last node is encrypted.

SESSION 11

FILE AND FOLDER SECURITY

DESIRED LESSON OUTCOMES

Participants can ensure file and folder security.

Session Type:

- Activity-Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
<p>LEARNING OBJECTIVES</p>	<ol style="list-style-type: none"> 1 Understand the importance of data security. 2 Know what metadata is and why it's important. 3 Learn how to encrypt files and folders with encryption tools. 4 Learn how to remove files and folders permanently. 5 Learn how to recover removed files.
<p>ADDITIONAL RESOURCES</p>	<ul style="list-style-type: none"> • https://veracrypt.fr/ File folder encryption tool • https://cryptomator.org/ • https://www.bleachbit.org/ Permanent file and folder removal tool • https://ccleaner.com/recuva Deleted file recovery tool • http://exif.regex.info/ Metadata verification platform • https://ssd.eff.org/en/module/why-metadata-matters
<p>SESSION GUIDE</p>	<ul style="list-style-type: none"> • Participants will be asked about their file and folder security practices. • Trainer will discuss the security of locally stored information. • Trainer will discuss metadata and why we need to be aware of it . • Trainer will present instructions on how to recover a conventionally removed file and how to permanently remove them from a computer. • Trainer will give a step-by-step guide of open-source file/folder encryption tools such as Veracrypt.

SESSION 11

FILE AND FOLDER SECURITY

SUMMARY OF THE SESSION

It's been said that data is now more valuable than oil because of the insights and knowledge that can be extracted from it. And it is very easy for cyber criminals to hack your accounts and breach your business once they collect your sensitive information. This is why cybersecurity for all your connected devices is very important.

Data security is when protective measures are put in place to keep unauthorised access out of computers, websites, and databases. This process also provides a mechanism for protecting data from loss or corruption.

- Reducing the risk of data breaches and attacks is very important. Applying security controls is crucial to prevent unauthorised access to sensitive information.
- The fundamental principles of information security are confidentiality, integrity, and availability.
- When you delete a file in the conventional way (e.g., moving it into the trash folder), it isn't actually deleted. It is still possible to recover a file deleted in this way. Deleting a file permanently on a normal magnetic hard disk (HDD) requires overwriting the same location.
- Beware of files like Temporary / History / Cache / Logs, etc. These carry other important information including your browser history and chat logs.
- Metadata is information about the digital communications you send and receive. Metadata carries a lot of important information which may pose a threat to your security. Make sure to try deleting or minimising metadata. Some examples of metadata include:
 - the subject line of your emails
 - the length of your conversations
 - the time frame in which a conversation took place
 - your location when communicating (as well as with whom)
- Turn on encryption if your operating system supports it. Or use free and open source software such as Veracrypt, which provides on-the-fly encryption. It can create a virtual encrypted disk within a file or encrypt a partition or the entire storage device with pre-boot authentication.
- Alternatively, you can also use Cryptomator to keep your data encrypted. If you use Cryptomator, you can create vaults that are hosted on a virtual drive. The data stored in the vault is then encrypted. The user can specify the location of the vault, such as a cloud provider, for example.

SESSION 12

DATA BACKUP

DESIRED LESSON OUTCOMES

Participants learn the importance of backups and how to do it properly.

Session Type:

- Activity-Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none">1 Understand the importance of backups.2 Learn how to create and store backups securely.
ADDITIONAL RESOURCES	<ul style="list-style-type: none">• https://duplicati.com/ Encrypted backup creation tool• https://www.duplicati.com/articles/Getting-Started/• https://support.microsoft.com/en-us/windows/backup-and-restore-in-windows-10-352091d2-bb9d-3ea3-ed18-52ef2b88cbef
SESSION GUIDE	<ul style="list-style-type: none">• Participants will be asked about their current practices for data backup.• Trainer will discuss the importance of backups.• Trainer will present a step-by-step guide for using open-source encrypted data backup tools such as Duplicati.

SESSION 12

DATA BACKUP

SUMMARY OF THE SESSION

What is the importance of a data backup? A data backup creates a secure archive of your important information – whether that’s classified documents for your business or treasured photos of your family – so that you can restore your device quickly and seamlessly in the event of data loss.

- Making backups of collected data is critical in data management. Backups protect against human errors, hardware failure, virus attacks, power failure, and natural disasters.
- Your device or important files may be damaged, stolen, or lost. Backups can help save time and money to restore important information if data loss occurs.
- Keep regular backups. More than one is recommended.
- Do not keep the original and backup data in the same place.
- Make sure the backup is encrypted.
- Use good and reliable tools for backup.
- Types of backup:
 - Full backup
 - Incremental backup
 - Differential backup
- On the Windows operating system, you can use the built-in backup feature. However, make sure not to back up files to the same hard disk that Windows is installed on. For example, do not back up files to a recovery partition. Always store media used for backups (external hard disks, DVDs, or CDs) in a secure place to prevent unauthorised people from having access to your files; a fireproof location separate from your computer is recommended. You might also consider encrypting the data on your backup.
- Duplicati is a free, open-source backup client that securely stores encrypted, incremental, and compressed backups on cloud storage services and remote file servers. Duplicati gathers all files to be backed up, deduplicates and compresses them, then sends them to your backup location in blocks or chunks to be stored for maximum efficiency. Duplicati supports not only various online backup services like OneDrive, Amazon S3, Backblaze, Rackspace Cloud Files, Tahoe LAFS, and Google Drive, but also any servers that support SSH/SFTP, WebDAV, or FTP.

SESSION 13

EMAIL ENCRYPTION

DESIRED LESSON OUTCOMES

Participants learn how to encrypt their email communications.

Session Type:

- Activity-Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none">1 Understand how email is sent, routed, and received, including where and how email contents can be read.2 Learn about ways to minimise exposure of email to unwanted scrutiny.3 Understand what GPG/PGP is and how it works, including various issues associated with using it (e.g., potentially “calling attention” to your usage of it, the limitations of being able to use it on mobile devices, etc.).4 Learn how to create a private/public keypair, upload a public key to a keychain, find and download others’ public keys, and authenticate others’ identities and keys.5 Learn how to send and receive emails that are signed or encrypted using GPG/PGP.
ADDITIONAL RESOURCES	<ul style="list-style-type: none">• https://www.openpgp.org/ Email encryption• https://mailvelope.com/ Email encryption browser extension• https://www.thunderbird.net/ Open-source mail client with PGP support.
SESSION GUIDE	<ul style="list-style-type: none">• Trainer will discuss how email communications work, the process of emails traveling from sender to receiver, the security risks involved, and how to mitigate these risks.• Trainer will present a step-by-step guide in using open-source email security browser extension Mailvelope.• Trainer will present a step-by-step guide in using Thunderbird, an open-source email client with openPGP support.

SESSION 13

EMAIL ENCRYPTION

SUMMARY OF THE SESSION

According to [this IRONSCALES report](#), over 90% of attacks on organisations start from a malicious email. Email protection is important because of cyber threats such as social attacks that target organisations via email. For example, phishing emails might trick users into giving up sensitive information, approving fake bills, or downloading malware that can go on to infect your company network.

- Emails, chat conversations, and instant messages always go through someone we don't know because of how the internet works.
 - Some people have this access by design (e.g., our ISP or mobile service provider).
 - Others may have it due to high-level access, which can be through legal means, such as a publicly court-ordered subpoena or through intelligence services, or through extralegal means.
 - Others can access it due to weaknesses in the systems (e.g., hackers).
- Pretty Good Privacy (PGP) is an encryption system used for both sending encrypted emails and encrypting sensitive files.
- Mailvelope is a browser extension that allows secure email communication based on the OpenPGP standard. It can be used with your current email to encrypt and sign electronic messages, including attached files, without the use of a separate, native email client.
- Thunderbird 78 has built-in support for two encryption standards, OpenPGP and S/MIME. OpenPGP has been enabled by default since version 78.2.
- Never share your private keys with others.
- If you don't want to use Thunderbird or Mailvelope, use a secure mail service such as Protonmail. But keep in mind that only mails sent to and from Protonmail are encrypted and secure. This means that if you send an email from your Protonmail account to Gmail, Yahoo, Hotmail, or other email services, it will not be encrypted.

SESSION 14

MOBILE PHONE SECURITY

DESIRED LESSON OUTCOMES

Participants learn about mobile phone security.

Session Type:

- Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none">1 Understand the associated risks of carrying and using mobile phones.2 Learn how to minimize those risks.
ADDITIONAL RESOURCES	<ul style="list-style-type: none">• https://level-up.cc/curriculum/mobile-safety/• https://ssd.eff.org/en/playlist/privacy-breakdown-mobile-phones• https://securityinabox.org/en/guide/basic-security/android/• https://securityinabox.org/en/guide/basic-security/ios/
SESSION GUIDE	<ul style="list-style-type: none">• Trainer will discuss various types of risks associated with using mobile phones.• The trainer will present recommended mobile phone settings for privacy and security, which participants will follow.

SESSION 14

MOBILE PHONE SECURITY

SUMMARY OF THE SESSION

Having a mobile phone has become a large part of our everyday life. Many underestimate the value a phone truly holds when it comes to the information it stores. Your phone has your entire life on it – it is a mobile bank, a communication device, and a social network hub. With so many functions in one device, it is necessary to protect the information stored within it.

Mobile security is a measure one takes to protect against a wide range of threats that seek to violate your privacy and gain unauthorised access to your phone. These attacks on your mobile device aim to take your private information, such as bank information, login information, and other data.

A mobile security threat is a means of cyber-attack that targets mobile devices like smartphones and tablets. Similar to a hacking attack on a PC or enterprise server, a mobile security threat exploits vulnerabilities in mobile software, hardware, and network connections to enable malicious, unauthorised activities on the target device.

It is possible for hackers to gain access to your mobile phone and do whatever they want, such as listening to your voice over the mic, recording your calls, taking photos, or recording videos. They can also call or send SMS texts from your device.

Here are some suggestions to protect your privacy:

- Keep your device's OS up-to-date.
- Always use a password on your mobile phone.
- Don't let others use your mobile phone.
- When installing a mobile app, consider what permissions you are allowing.
- Turn on full disk encryption.
- Turn off GPS.
- Don't jailbreak or root your phone
- Beware of unfamiliar messages or media.
- Do not connect to public wifi on your phone.
- Optimise your lock screen security.
- Don't carry your phone everywhere. If you want to attend a secure meeting or protest and you don't want to disclose your location, leave your mobile phone at home.

SESSION 15

END-TO-END ENCRYPTION AND MOBILE COMMUNICATION

DESIRED LESSON OUTCOMES

Participants learn about end-to-end encryption and how they can communicate securely using encrypted apps.

Session Type:

- Activity-Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none">1 Understand the method of end-to-end encryption.2 Choose encrypted apps for mobile communication.
ADDITIONAL RESOURCES	<ul style="list-style-type: none">• https://protonmail.com/blog/what-is-end-to-end-encryption/• https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work key exchange system (advanced)• https://signal.org/ Secure communication app• https://wire.com/ Secure communication app• https://briarproject.org/ Mobile app for offline secure communication
SESSION GUIDE	<ul style="list-style-type: none">• Trainer will discuss what end-to-end encryption is, how it works, and why it is important for security and privacy.• Trainer will share a handful of mobile communication apps that support end-to-end encryption.• Participants will be asked to download the apps and a group will be created on Signal/Wire for future communication among the participants or mentorship from the trainer.

SESSION 15

END-TO-END ENCRYPTION AND MOBILE COMMUNICATION

SUMMARY OF THE SESSION

End-to-end encryption (E2EE) is a method of secure communication that prevents third parties from accessing data during transfer from one end system or device to another. In E2EE, the data is encrypted on the sender's system or device and only the recipient is able to decrypt it. End-to-end encryption is currently the most secure way to transfer confidential data, which is why more and more communication services are switching to it.

- Avoid regular cellular calls if you want to keep information private.
- Always use open source and end-to-end encryption supported apps for mobile communication.
- Signal is a free, privacy-focused messaging and voice talk app that you can use on Apple and Android smartphones and via desktop. All you need is a phone number to join. Communications on Signal are encrypted end-to-end, which means only the message recipients can see the content of those messages – not even the company itself can view these.
- Wire is similar to Signal, but you can create an account on Wire without a mobile phone number. You can use either an email address or a phone number to create an account.
- Briar is a messaging app designed for activists, journalists, and anyone else who needs a safe, easy, and robust way to communicate. Unlike traditional messaging apps, Briar doesn't rely on a central server – messages are synchronised directly between the users' devices. If the internet is down, Briar can sync via Bluetooth or wifi, keeping the information flowing in a crisis. If the internet is up, Briar can sync via the Tor network, protecting users and their relationships from surveillance.

SESSION 16

HOW TO PREPARE FOR THE NEXT TRAINING

DESIRED LESSON OUTCOMES

Participants perform better in training facilitation.

Session Type:

- Discussion-Inputs-Deepening-Synthesis

SUBJECT	DESCRIPTION
LEARNING OBJECTIVES	<ol style="list-style-type: none">1 Learn the basic rules to perform better during training.2 Learn how to create a good presentation.3 Know the different things to consider before, during, and after training.4 Learn how to plan a session.5 Learn how to handle questions during training.
ADDITIONAL RESOURCES	<ul style="list-style-type: none">• https://level-up.cc/before-an-event/preparing-sessions-using-adids/• https://level-up.cc/you-the-trainer/golden-rules-of-effective-training/
SESSION GUIDE	<ul style="list-style-type: none">• Trainer will present various tips for participants in planning and conducting their next training.• Trainer will answer questions from participants and provide examples as needed.

SESSION 16

HOW TO PREPARE FOR THE NEXT TRAINING

SUMMARY OF THE SESSION

- Time management:
 - Keep an eye on the time. Encourage participants to follow the correct time and schedule.
 - Schedule according to the training content.
 - Make time for questions.
 - Pause as needed.
- Participants:
 - Show respect to participants.
 - Make sure they understand the topics.
 - Ask questions and encourage them to ask questions.
 - Note their emotional states (for example, if they are feeling annoyed).
- Understanding the situation:
 - Not everything will go smoothly. Be prepared to change plans.
 - Be creative and flexible depending on the situation.
 - Change the content according to the participants' needs or situation.
 - Structure the topics in an organised and relevant way.
 - Add ice breakers and fun time to keep participants active.
- Equipment and necessary arrangements:
 - Take the necessary security precautions.
 - Make sure the devices you need are working.
 - Ensure necessary tools are there for all participants.
- Presentation creation:
 - Keep the presentation simple and clean.
 - Use similar fonts. Avoid using extra colors.
 - Don't add too much text; just add some pictures.
 - Maintain the continuity of the topic. Discuss the problem first and then present the solution.
 - Keep up to date with the latest news on digital security.
 - Give examples related to participants' work areas and contexts.
 - Do not include any material that offends participants.
 - Include a summary at the end of each section.

5.0 GLOSSARY

Name	Definition/s
2FA	Two-factor authentication (2FA) is a security system that requires two separate, distinct forms of identification in order to access something.
Antivirus	Antivirus software, also known as anti-malware, is a computer program used to prevent, detect, and remove malware.
DNS	The Domain Name System (DNS) is the phonebook of the internet. It is composed of various servers around the world where domain names are checked to see which IP addresses they should direct to.
DuckDuckGo	DuckDuckGo is an internet search engine that emphasises protecting searchers' privacy and avoiding the filter bubble of personalised search results.
E2EE	End-to-end encryption is a system of communication where only the communicating users can read the messages.
Encryption	Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography.
FTP	File Transfer Protocol is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network.
GPS	Global Positioning System (GPS) tells you where you are on earth.
HRD	Human rights defenders
HTTP	Hypertext Transfer Protocol (HTTP) is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers, but it can also be used for other purposes.

Name	Definition/s
HTTPS	Hypertext Transfer Protocol Secure is an extension of the Hypertext Transfer Protocol. It is used for secure communication over a computer network, and is widely used on the internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security or, formerly, Secure Sockets Layer.
IP	An Internet Protocol address is a numerical label such as 192.0.2.1, which is connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.
ISP	The term Internet Service Provider (ISP) refers to a company that provides access to the internet for both personal and business customers.
Jailbreak	On Apple devices running iOS operating systems, jailbreaking is a privilege escalation executed to remove software restrictions imposed by the manufacturer.
Malware	Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.
Metadata	Metadata is data that provides information about other data, but not the content of the data, such as the text of a message or the image itself.
Open-source software	Open-source software is computer software that is released under a licence where the copyright holder grants users the rights to use, study, change, and distribute the software and its source code to anyone and for any purpose. Open-source software may be developed in a collaborative public manner.
OpenPGP	OpenPGP is an open and free version of the Pretty Good Privacy (PGP) standard, which defines encryption formats to enable private messaging abilities for email and other message encryption.
OS	An operating system (OS) is system software that manages computer hardware, software resources, and provides common services for computer programs.
PGP	Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication.
Phishing	Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software (such as ransomware) on the victim's infrastructure.
Root	Rooting is the process of allowing users of the Android mobile operating system to attain privileged control (known as root access) over various Android subsystems.

Name	Definition/s
SFTP	SFTP (Secure File Transfer Protocol) is a file transfer protocol that leverages a set of utilities that provide secure access to a remote computer to deliver secure communications.
SMTP	The Simple Mail Transfer Protocol is an internet standard communication protocol for electronic mail transmission. Mail servers and other message transfer agents use SMTP to send and receive mail messages.
SSH	Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH.
SSL	SSL (Secure Sockets Layer) and its successor, TLS (Transport Layer Security), are protocols for establishing authenticated and encrypted links between networked computers.
Startpage	Startpage is a Dutch search engine company that highlights privacy as its distinguishing feature.
TCP	The Transmission Control Protocol is one of the main protocols of the internet protocol suite. It originated in the initial network implementation where it complemented the Internet Protocol. Therefore, the entire suite is commonly referred to as TCP/IP.
Tor	Tor, short for The Onion Router, is free and open-source software for enabling anonymous communication. It is a worldwide network of servers used by people who want to greatly increase their privacy and internet freedom. After all, the Tor browser ensures your data traffic passes through different servers (nodes) located all over the world. This makes it a lot more difficult for online entities to track Tor users.
VPN	A virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
WebDAV	WebDAV is an extension of the Hypertext Transfer Protocol that allows clients to perform remote Web content authoring operations.
WEP	Wired Equivalent Privacy is a security algorithm for IEEE 802.11 wireless networks.
WPA	Wi-Fi Protected Access, Wi-Fi Protected Access II, and Wi-Fi Protected Access 3 are the three security and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.