DIGITAL SECURITY TRAINERS' MANUAL

Prepared by:

ZAINA FOUNDATION

2021

Supported by:

accessnow

TABLE OF CONTENT

ZAINA FOUNDATION

1.0 ABOUT ZAINA FOUNDATION

Zaina Foundation is a non-governmental, non-profit sharing organization which was founded in 2017 and registered under NGO's Act of 2002 with the aim of promoting digital rights in Tanzania. Zaina Foundation's vision is to empower women in technology through digital security and privacy capacity building, workshops, and training. This is done through providing capacity building of digital security training to women and human rights defenders in Tanzania, localization of digital tools and content where we translate open source tools in Swahili language to allow Swahili users to access secured tools for their communication. Additionally, Zaina Foundation monitors internet shutdowns in Tanzania and through its UX Project the organization tests open-source tools, collects feedback from end users during training and shares them with developers, in the quest to help improve the tools friendlier for users.

Read more about us at www.zainafoundationtz.org
For more information, please contact us info@zainafoundationtz.org
Connect with us on twitter @ZainaFoundation

1.1 ABOUT THIS GUIDE

This manual is a collection of useful digital security methodologies, learning aids, tips and techniques that trainers from Sub-Saharan Africa can adopt during their Preparations for Digital Security Training for Human Rights Defenders freely available on the internet. It prepares trainers for the basics needed for training Device hygiene, password and password management, Secure Storage of data, two factor Authentication, Online Safety, Device Security, Mobile Security and Recommended further readings on Digital Security.

It also has paint points reported by some human rights defenders while using some of the methodologies provided.

Targeted group - This manual designed to support trainers during preparations of their Digital Security Training. Other groups include Journalists, Activists and Technologists.

Objective of this manual: Understanding Digital Security Skills and Open-source tools practice.

Learning Outcome: Strengthened capacity of Human Rights Defenders in Digital Security and tools practice.

What is special in this manual; designed to support trainers in preparation for all levels of digital security training.

Acknowledgement: Zaina Foundation thanks Access Now for supporting this guide. We acknowledge these trainers from their contributions in this manual; Neema Ndemno, Dorina Mathayo, Mariam Zaunga, Innocent Chambi, Deogratius Chambi, Vicensia Fuko, James Laurent

2.0 RISK ASSESSMENT

Time: 40 minutes
Methodology: Brainstorm, Discussion and Presentation
Teaching Aids: Flip chart, maker pen and stick notes.

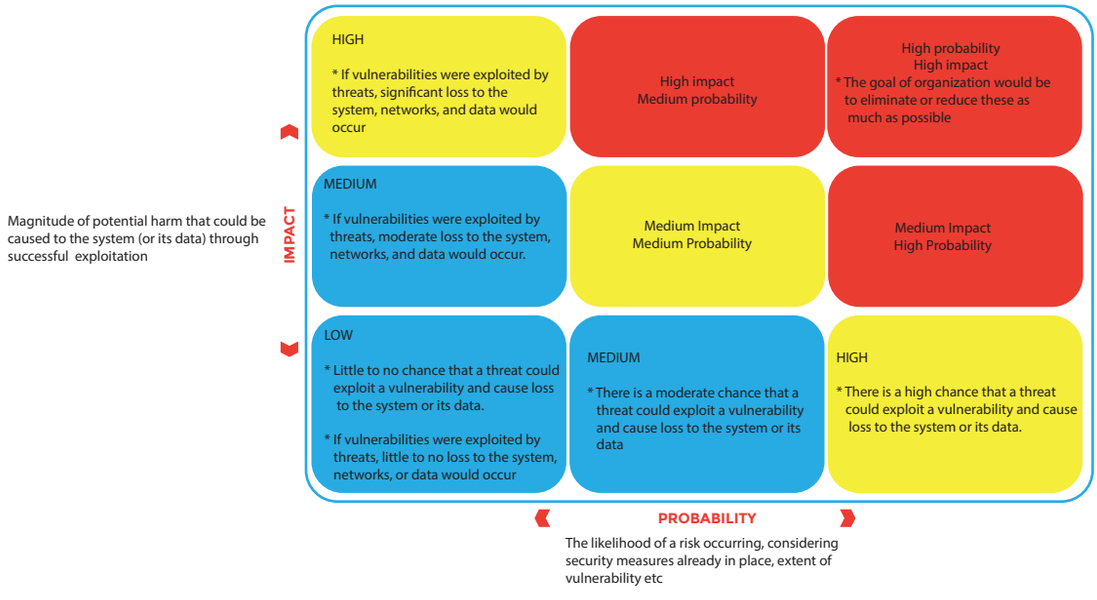
2.1 Learning Objectives

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

The goal of this exercise is to lead participants through a strategic critical thinking process to make decisions about specific digital security tools or practices that they will implement for themselves. However, it is important for us to remember that – as trainers and experts – our participants are under no obligation to either use the tools we teach, or to adapt to the practices that we deem to be "the safest".

Activity 1

RISK IMPACT VS PROBABILITY MATRIX



Activity 2
Ask participants to identify specific tools and practices for themselves. On a table or flat surface place the safety tools. Ask participants to come forward to the table, to select from among the tool figures on the table those which they think are important to them and their individual needs, and that they plan to continue practicing and using after the training process has completed. After they have chosen, ask them to explain why they chose that.

They should also mention if there were any tools that they wanted to choose but weren't able to because others had chosen it first.

Now, ask them if they think that there are any other tools missing from the table - even if they don't know the name of it (or even if it exists or not) ask them to say if they have any concerns remaining which are not readily addressed by any of the tools that were available to them

3.0 DEVICE HYGIENE AND DATA BACKUP

3.1. Device hygiene

Time: 45 minutes
Methodology: Practical
Learning Aids: Computers, Antivirus and wi-fi

3.1.1. Learning Objective

To gain knowledge and skills on how to protect devices

3.1.2. Learning Outcome

i) protected and skilled digital users
ii) safe and protected devices
iii) Encrypt device

3.1.3. Why device hygiene?

i) System choices: whether ios or Android? What are the safety concerns between various types of systems and what users should know?
ii) Safety against intruders and hackers.
iii) Choices of software such as Antivirus, licensed window, mac Os, ubuntu and other applications.
iv) Device maintenance - Cleaning, Scanning, Updating software and application.
v) Personal evaluation of device hygiene.
vi) Quiz
vii) Device hygiene examples; Computers (laptop & desktop) - MAC OS, WINDOW, Mobile phone (tablet, ipad, mobile) - ANDROID, IOS, Printers & Scanner.

3.2. Data Backup

Time: 1 hour
Methodology: Practical, Group work and skill share.
Teaching Aids: Data, Computers, Mobile phone and wi-fi

Data Backup means to archive, store, copy data from one device to another or to create a copy of the important information to different location to secure them for further use, i.e device backup: external hard drive, flash, Cloud backup: Google drive, One drive, Flexible storage

3.2.1. Learning Objective

Enhancing skills on how to secure data (information) in the devices

3.2.2. Learning Outcome

i. Protected data (information)
ii. Skilled users in data protection
iii. Encryption skills

3.2.3. Types of data backup are

i) Full backup
ii) Incremental backup
iii) Differential backup
iv) Mirror backup

3.2.4. Why data backup?

i) What's Data Backup?
ii) Data Backup Strategy
iii) Data backup safety and 3rd party software
iv) Network security/safety and its impact to data backup
v) Data backup encryption
vi) Protecting Backups - Having a Plan B for protection.
v) Practical Exercise- creating backup.
vi) Quiz

Activity 1

Relative Sensitivity	Computer Hard drive	USB/External Storage	Cloud	Another e.g. Smartphone, Print etc. depending on group
High				
Moderate				
Low				

Divide participants in smaller groups. Give each participant 2sets of sticky notes of different colors. Each should think of 5 data types they work with and write one type per note. For any data with duplicate location, they should represent with a different color. 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

4.0 PASSWORD AND PASSWORD MANAGER

(1 hour)

Learning Objectives

- Why passwords are important
- Creating a strong password
- The importance of using password managers and how to use them.

4.1 Passwords

What is a password?

A password is a secret code or phrase used to gain access to something. I compare a password with a key which helps a person to unlock a door or locker. Therefore, a password works as a key to help you enter a certain account to access something. It can be a unique string of character that allows you to access a computer or a system. Password can also be a secret word or combination of letters used to communicate with another person.

Therefore, having a password is an essential element of using digital /online platforms. We normally use passwords in our online accounts, email, computer, bank accounts, ATM, phone etc. Passwords can be in the form of PIN, numbers or phrases and patterns.

Why Passwords are important?

- It protects security and identity
- It keeps data safer and confidentiality
- It provides access to information
- It reduces chances of virus attacking your device
- It also protects hackers from accessing your information

How Can We Protect Our Passwords?

- Do not share your password
- Do not write down your password in a book or sticky note
- Don't say it loud
- Don't give hints about your passwords
- Avoid repeating your password
- Change the password regularly at least after six months
- Make it strong

How to create a Strong Password?

The rule is to create a password which is harder to guess and easy to remember. However, in creating a strong password two things must be considered.

a. Complexity in character - mix letters, numbers, and symbols for example Holy@Spirt2020

b. Length - use at least 8characters or longer. The longer the password the better.

c. Avoid using information about you or people around you

How to Remember the Password?

- Use memorable phrases e.g. IloveICEcre@m20
- Use password manager that can help you store your passwords in one place eg. Keepass etc

Activity 1

Make space for the participants to form a straight line. Once they are ready call out the following instructions:

- 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.

While everyone is still standing in their places, ask the participants the following questions:

- What do you think this activity was about?
- What do you think is a good password?
- Why do people not use good passwords?

4.2 Password Managers

Time:1 hour 30 minutes
Methodology: Brainstorm, Discussion and Presentation
Teaching Aids: Computers, Software ie KeepassXC, etc

Often most people/trainees find it a bit difficult to forge and memorize passwords that qualify to be strong passwords.

A password manager takes care of all that hustle by helping you create and manage multiple accounts with unique, long, complex randomly generated passphrases.

A password manager is essentially an encrypted digital vault that stores secure password login information you use to access apps and accounts on your computer, mobile device, websites and other services.

Think of a Password Manager as a Bank Vault or a Safe at home used for storing money, and locked safely with a PIN, only in this case, this vault is used to store usernames, passwords and user accounts and locked with a MASTER PASSWORD.

*Note: When setting up a password manager, the only password to memorise is the one and only MASTER PASSWORD.

4.2.1 Learning Objectives:

- Participants understand the concept of a Password Manager (HEAD)
- Participants appreciate the link between the previous Password creation process and Password Management for enforced account access security (HEART)
- Participants use recommended Password Managers to set up their Password Managers, and to generate and/or store their strong passwords in vaults (HANDS)

4.2.2 Learning Outcome

Why use a Password Manager? :

1. Storing your strong passwords in a secure vault from hackers and password cracking software
2. It's an alternative for forging or generating unique, long, complex and random passwords
3. Automatically fills in your log in user account credentials online
4. You won't ever have to remember or memorise any password you store in the vault apart from the MASTER PASSWORD

E. Recommended Password Managers:

1) LastPass Password Manager (Free version but limited access on one device type - 1 computer or 1 mobile)
2) KeePassXC (Free, Cross-platform and open source)
3) Bitwarden Open Source Password Manager

*F. Installing and Setting up Password Manager (Practical Exercise)

5.0 TWO FACTOR AUTHENTICATION

Time: 1 hour
Methodology: Practical, Discussion and Presentation
Teaching Aids: Computers, Mobile Phone, Wi-fi, email account and social media accounts

Two factor authentication (2FA) or two factor verification is a method of verifying your identity that adds a second layer of security to your account passwords. Having multiple barriers is always more secure and therefore recommended.

Types of 2FA include any of the following

- Something you know - a PIN, number, password or pattern password or personal identification number (PIN) that only you know
- Something you have - an ATM or credit card, mobile phone or security tokens in your possession
- Something you are - a biometric form of authentication such as your fingerprint or your voice or your face or your typing style.

Recommended 2FA methods:

1. Authenticator Apps (Twilio Authy, Google Authenticator, Aegil (for Android) and FreeOTP)
2. Hardware tokens (used mostly by banks and business companies)
3. Email authentication
4. Saved copy of One-Time Tokens (used as an alternative in case one has no access to internet or an authentication device or Authentication app)

Not Recommended 2FA methods:

- SMS or Phone call authentication (prone diversion of authentication codes by attackers or failure to use when abroad)
- Biometric Authentication (in case of an abduction or when asleep or intoxicated, one can be forced to authenticate a log in without their consent)

1. Steps to Set-up 2 Factor Authentication for G-mail, Facebook, Twitter and Instagram: Go to the Account page of your platform
2. Then to set up 2 Factor Authentication, Go to Security and Log In Settings
3. Then Go to Two Factor Authentication or Two-step Verification, depending on an account
4. Select one option among: Authentication App or Email Authentication or Security Key

After selecting a 2FA method, enter a code sent to your email or that appears on your Authentication App to verify your credentials. Then click DONE.

* This website, TwoFactorAuth is an excellent tool for looking up accounts and services that currently support two-factor authentication.

6.0 ONLINE SAFETY

Time: 3 hours
Methodology: Presentation, Practical, and Discussion
Teaching Aids: PowerPoint, Flip charts, marker pen, stick notes, Computers, VPN and wi-fi

6.1 Learning Objectives

- 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.

⋆Browser Basic Security settings

Trainer should consider to elaborate how the browsers namely firefox,Safari, chrome internet explorer to mention a few has to be set before the startup. he/she must consider to set the basic security that comes with the browser like history check ins and cross-site cookies and site data tracking also logins and password, also should consider about the geographical location of the device, microphones and camera should be turned off before browsing the internet.

⋆Online browsing

When browsing through different websites, you will notice that some web url on the address bar starts with HTTP and some start with HTTPS. It is important to be aware of HTTP and HTTPS as they tell how secure/safe you are on that particular website.

- HTTP (unsecured channel) stands for hyper-text transfer protocol. HTTP is an unsecured connection to the internet. Using HTTP is like sending a postcard in plain text, which means whoever handles this postcard will see/read the message on it.

- HTTP is okay when browsing insensitive content, however anyone who can pry or sneak around can see whatever you did online.

  Discussion: Look at circumstances where one needs secure internet browsing. Share experiences/scenarios on secure internet browsing. This initiates the following sub section which is HTTPS.

- HTTPS (secured channel) stands for hyper-text transfer protocol secure. HTTPS is a secured connection to the internet. Think of HTTPS as sending a letter that is sealed in an envelope/written in a language that no one understands except for the receiver of that letter. HTTPS secures online communications between the user and the service provider.

- We should note that some websites have the HTTPS version, however some browsers may not be able to automatically load it, which means you might not easily know that a certain website has the HTTPS version.

- In this case, it is important to install a browser extension known as HTTPS Everywhere that automatically searches for the HTTPS version of a website, and use it instead of the HTTP version, even when the user types in HTTP or follows links that omit the HTTPS. Also, HTTPS Everywhere prevents unsecured websites from opening through your browser.

- Conclude by insisting on secure internet browsing through HTTPS

★Security addons

To enhance safe browsing, trainers must consider the enhancement of browser security like installing other open-source programs/extensions which will add security during internet browsing, therefore addons like Noscript, HTTPS everywhere, Privacy Badger, uBlock Origin are highly suggested.

★Incognito web browsing

This is a browsing mode enabled through your browser, that only prevents your browsing activity and history from being logged on and stored on your computer/device. This does not make a user anonymous on the web, because the internet provider will still have access to your browsing activity.

★Take the participants through the practical process of enabling incognito web browsing

★Virtual Private Network (VPN)

Trainer is supposed to insist on the use of VPN when connecting to the internet. A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. It changes the geographical location and prevents censorship.The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

★Anonymous browsing (Tor Browser)

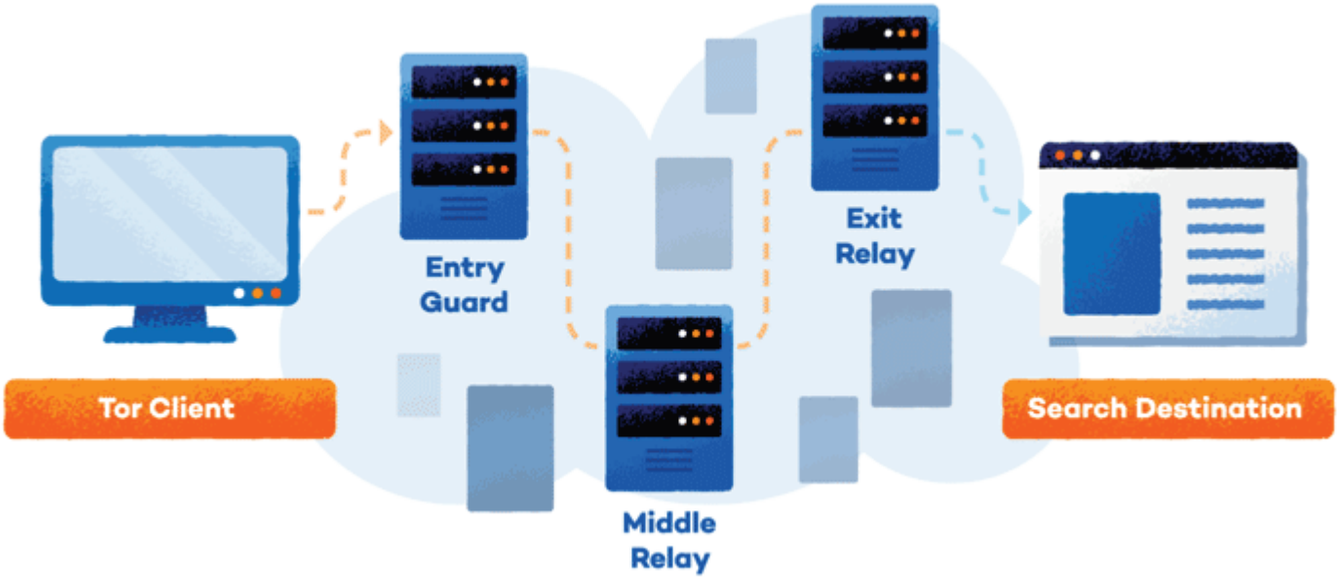
TOR: is like a bad travel agent. You say you want to travel from Dar es Salaam to Entebbe, but they send you on a flight to Kilimanjaro, a shuttle to Arusha, then a bus to Nairobi, then finally a flight to Entebbe. In the same way, Tor bounces you around the internet before arriving at the site you need. – Analogy adapted from Nick Asbury, Sideways Dictionary

Using TOR browser

TOR stands for The Onion Router. TOR is like other browsers, except that it is secure compared to other browsers. TOR browser facilitates advanced security features e.g bypassing surveillance and censorship, disguise online identity etc. The Tor browser can be used for Linux, Mac, Windows and mobile devices. The Tor browser protects your identity online. When using it, everything you do goes through their network and is encrypted, keeping your online activity private.

How TOR works

The TOR browser scrambles your identity online by routing your internet traffic randomly through a series of servers. With TOR browser the source and destination of your web traffic is kept from being seen through encryption. We all know what an onion looks like; it has a series of layers, so does the TOR browser. These are layers of encryption in which the web traffic is enclosed.



Source: Tor vs. VPN: What They Do and Which is Better - Panda Security

Remember to keep it safe when using TOR browser. Be cautious of the activities you do online and the extent to which they disclose your personal identifiable information in the process.

Advantages of TOR browser

- ★ It is user-friendly - Easy to use features
- ★ It is free - open-source software
- ★ Protects your privacy

Disadvantages of TOR browser

- ★Slow speed

- Phishing

Phishing is a type of spam (unsolicited junk mail) that attempts to get information by Making you take a certain course of action. For example, a phishing email could try to trick you into revealing sensitive personal information (e.g., account passwords, credit card information) or do something more dangerous, like downloading and running a malicious program that will secretly steal information from you or allow hackers to store a remote control to a device or install ransomware. For Example, is like when someone gives you a call and starts a conversation like you both know each other before. Or someone walks up to you at random and starts a conversation. They seem to have a credible story and might even make you a tempting offer, yet they want something from you. They do something alarming or interesting while you're distracted, they pick your pocket.

- Social media security setup

7.0 MOBILE SAFETY

Time: 2 hours
Methodology: Plenary Discussion
Learning Aids: Mobile phone, wi-fi and Software ie VPN

Phones indicate precisely geographic location to the operator at any given time. Phone is an excellent listening device and can be used to transmit any sound (and video) within an earshot without you knowing. For practical reasons consider mobile phone conversations not encrypted. Therefore, there should not rely on SMS messages services to transmit sensitive information securely. SMS can be intercepted, modified, stored by phone operators. Phones can also be infected with spyware, using USB, Internet, Bluetooth, WiFi, etc. Trainees must know that the operator (communication company) has full access to the calls, SMS, Internet connections. Trainer should recommend the Set-up SIM card lock, screen lock, security lock timer, device encryption. Turn off Wi-Fi, Bluetooth, GPS, mobile data, Internet tethering when not in use.

7.1 Learning Objectives

- Learn the basics of mobile telephony and how mobile networks function.
- Understand the implications of mobile infrastructure for information and personal security.
- Learn how to mitigate the vulnerabilities of feature phones

Activity 1

*This activity is mainly to explain how mobile phones work.

Choose one participant to play mobile phone and five others to be antennas and distribute themselves around the room. Each antenna should define their quadrant. Ask the mobile phone to close his/her eyes and locate the antennas by calling out Marco. The antennas can only respond to Polo when the mobile phone passes on their quadrant.

- Cell carriers operate antennas in different areas, each of which provides coverage for a specific zone (or quadrant)
- Mobile phones receive coverage by sending out a request to new antennas they encounter (“Marco”) as they move from place to place, which antennas then reply to (“Polo”) by providing cell coverage.

8.0 DRAFTED AGENDA FOR DIGITAL SECURITY TRAINING

8.1 DAY 1 AGENDA. VENUE_____ DATE_____

#	Time	Topic	Personnel
1.	9:00-9:30	Arrival, Introduction & Training Objectives	All
2	9:30 – 10:00	Risk Assessment	Trainer 1
3	10:00 – 10:30	Break	All
4	10:30 – 11:30	Device Hygiene	Trainer 2
5	11: 30 – 11:45	Break	All
6	11:45 – 13:00	Password & Password Manager	Trainer 1
7	13:00 – 14:00	Break	All
8	14:00 – 15: 00	Data Backup	Trainer 2
9	15:00 – 15:30	Recap of Day One & End	Trainers

8:3 DAY 2 AGENDA. VENUE_____ DATE_____

#	Time	Topic	Personnel
1.	9:00- 9:30	Recap of Day One & Games	All
2	9:30 - 10:00	Online Safety	Trainer 1
3	10:00 - 10:30	Break	All
4	10:30 - 13:00	Online Safety	Trainer 2
5	13: 00 - 14:00	Break	All
6	14:00 - 15:00	Digital Clinic 1	Trainer 1
7	15:00 - 15:30	Recap of Day Two & End	Trainers

8:4 DAY 3 AGENDA. VENUE_____ DATE_____

#	Time	Topic	Personnel
1.	9:00- 9:30	Recap of Day Two & Games	All
2	9:30 - 10:00	Mobile safety	Trainer 1
3	10:00 - 10:30	Break	All
4	10:30 - 13:00	Mobile safety Cont..	Trainer 2
5	13: 00 - 14:00	Digital Security Clinic 2	Trainers
6	14:00 - 15:00	Break	All
7	15:00 - 15:30	Networking Event	All
		Departure	All

9.0 REFERENCES

1.https://safesisters.net/wp-content/uploads/2019/09/Digital-Safety-Trainers-Assistant-smaller.pdf

2.https://digitalhumanrightslab.org/documents/22/simplified_digital_security_guide_for_activists_in_east_africa.pdf

3.https://brainstation.io/cybersecurity/two-factor-auth

4.https://sidewaysdictionary.com/#/

5.https://www.eff.org/deeplinks/2011/12/2011-review-ever-clearer-vulnerabilities-certificate-authority-system

6.https://www.eff.org/observatory

7.https://veracrypt.codeplex.com/

8.https://guardianproject.info/code/luks/

USEFUL HASHTAGS:

#DigitalRightstz
#OrgSec
#ResponsibleData
#InternetFF