2022

DIGITAL SAFETY WOMEN JOURNALISTS TRAINING

25th-26th of March
Venue: Gran Melia, Arusha

TABLE
Of Content

1.SUMMARY OF THE REPORT

This report is about Digital safety training for women journalists held in Arusha Tanzania at Gran Melia. A total of 15 women journalists were convened to learn about the skills that one needs to have, learn, and work in a society where communication and access to information are increasingly done through digital technologies like internet platforms, social media, and mobile devices. The training was positioned at the confluence of digital safety, internet freedom, and human rights as fundamental freedoms in Tanzania's legal and political context.

1 BACKGROUND INFORMATION

Development in Information Technology has significantly transformed and impacted socio-economic, infrastructure, and general human well-being. After the eruption of Covid – 19 around the world a specialist without physical contact (e-health) can treat a patient, staff can complete work, online meetings, and other discussions and one can acquire an online bachelor's degree (courtesy of distance- learning), and business can swiftly be done through social media marketing, e-business, blogs, e-banking, mobile money, and on-line shopping). In a nutshell, ICT has increased production and efficiency. Not only, in general, has economic development but also in digital communication incredibly enhanced information and data sharing.

Tanzania is one of the countries in Africa with 30 million users of the internet and mobile phones while a total of 55,173,780 had Subscriber Identity Module (SIM) cards. Women Journalists are among the beneficiaries of the revolution in communication in Tanzania. Women Journalists are women who work in the media organization as producers, presenters or even editors. Women Journalists are normally in the business of exposing a diversity of issues related to breach of human rights, violence during elections, updates on Covid-19, corruption, tax evasion, gender-based violence (GBV), womanizers, human traffickers, etc. These people hold, generate, and transmit a bulk of sensitive and confidential data and information on their electronic device's daily basis.

Women Journalists do not use secure tools in Tanzania due to language barrier 70% of Women Journalists in Tanzania are comfortable browsing the internet by using the local language which is Swahili. During election October 2020 Women Journalists left offline due to insufficient skills on using circumvention tools and most of the open-source tool are in English. The use of VPN was important during the Internet shutdown on the eve of an election. These skills are still missing to Women Journalists in Tanzania.

Experience shows that in Tanzania most Women Journalists especially are using unsecured electronic devices characterized with weak passwords, weak device guards (anti-virus) or not at all, using unauthentic software, using unsecure tools, and counterfeit electronic devices. Moreover, when browsing on the internet, most Women Journalists are totally 'necked' because they are not using security Tools like virtual private network (VPN), therefore, exposing their Internet Protocol address (IPs). Furthermore, the majority are using public Wi-Fi leaving behind a lot of 'footprints'

Violation of the right to privacy is common during and after elections in Africa. For instance, by October 2020 and December 2020, disruptions of the internet and blocking of sites and tools like Tor Browser and Signal related to elections have been witnessed in Tanzania. Moreover, until now you cannot access tweeter unless you connect to a VPN.

Opening Remarks session

DAY 1

3.1 SESSION1

3.2 DEVICE HYGIENE

- Device hygiene session was the first after introductions and objectives and cases sharing from participants. Common threats in our daily communications Organization/individual

- In hygiene session participants were encouraged to be responsible for their device not to share with anyone, don't leave them unattended but also participants were trained on different types of malicious which affect our device through sharing our devices and click link we received from unauthorized people (hackers)

- Phishing is a kind of email we receive from hackers for the purpose of getting our data and money. Phishing is very common once you click that means you granted authorities of unknown people to access your data.

- Rootkit is another kind of hacking which is specific for getting specific credentials like passwords, photos, addresses and accounts.

3.3 How to overcome threats:

- Use an anti-virus. The number one recommended anti-virus is Kaspersky. Its project your accounts online and devices
- Activate your firewall. This is the natural software installed in your computer to protect your devices.

- Use software which is up-to-date. For the purpose of getting new security layer from new version
- Avoid clicking every email unless you know the source. Some emails we receive can destroy our data and devices because they might contain some malicious content.

3.4 Data Security:

Is the process of protecting data from unauthorized access throughout its lifecycle

3.5 How to Secure Data:

- Encrypt your data
- Web Browser Security - Make sure your browser https site is not http. Do not enter your credentials in http site that means your data is in plain text.
- Email Security- Use email encryption to secure your communication during email communications because if you do not encrypt your email that means hackers can hack your communications and all your contacts.

4.0 SESSION 2: INTERNET AND ITS VAST BENEFITS

Strengthening the internet and its benefit overview

Internet users in Tanzania is 30M, more than 90% access the internet through mobile phone

Results indicate that the majority (83.2%) of respondents used the internet for academic purposes, 61.3% used for searching news and 50% for communication, slightly more than a half 52% of respondents were using the Internet for games and entertainment while only (43%) used it for social networks.

- Most common broadband service in Tanzania is given through 2G connections, which offers a speed of up to 0.3 Mbps and is used by 90% of mobile
- July 2020 Tanzania introduced the electronic and postal communication (online content) regulations, 2020.
- Under the regulations, a person shall only provide online content service after having obtained a license from Tanzania Communications Regulatory Authority

4.1 Benefit of Internet

- Internet as a tool of democracy with easier communication/political views
- Reshaping the daily processes of decision-making at all levels of government.
- Online activism and protest.
- Facilitates participation and connection
- Freedom of expression, privacy and trust

4.2 Other benefits of the internet from participants

- Sharing information on time
- Help to meet with new people
- Easy to connect worldwide (networking)
- Source of income through views
- Increasing influence within community
- It saves time
- To disseminate information easily through online platforms
- Increase source of Information (being updated)
- Source of opportunities (jobs, tender etc)
- Source of Knowledge

4.0 SESSION 3: ONLINE SAFETY

5.1 Quiz

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

5.2 Social networking

- Who has access to the shared information?
- Who controls and owns the information once it is on a social networking site?
- What information about me could my contacts pass to other people?
- Would my contacts be concerned if I shared information about them?
- Do I trust everyone I am connected to?
- Meta-data, settings, groups (public| closed | secret)

5.3 Online safety (social media safety)

- Facebook - worldwide, there are over 2.41 billion monthly active
- Instagram
- Twitter is a total of 1.3 billion Twitter accounts, but only 328 million are active, there are 500 million Twitter user

5.4 Social Networks safety Tips

- Reduce the amount of personal information
- Control who can access your profiles, status updates, photos, and other data
- Reduce the amount of information online
- Use your mobile alone
- Change password time after time

5.5 Internet challenges in Tanzania

- Cost, speed, coverage, accessibility
- Policies and regulations
- Surveillance of privacy and security
- The proliferation of fake news
- Increase of OGBV (Cyberbullying)
- Breaches of privacy and security

6.0 MOBILE SAFETY

- Participants learned about the importance of not sharing your mobile phone and making sure you have a strong password on your phone. Make sure you enable two-factor authentications in order to allow second authorization to your phone. 2FA is important due to the increase in hack ing incidents and the essentiality in data protection.
- Participants were encouraged to use an up-to-date phone because they have a high level of secu rity for your data protection and privacy.
- Participants practiced on how to set an Authenticator for their mobile phone by using special apps from the App Store and Play store.
- The current operating system for Android is 12.0 and iOS is 15.4. Participants were advised to update their phones to get current software.

6.1 Tips for mobile security

- Do not leave your phone unattended.
- Set a password in your phone and change it regularly
- Enable remote wipe features if not available

6.2 Transmission security in your phone

- Encrypt your phone
- Switch off your wireless and Bluetooth
- Hide your wireless connection
- Use VPN when using public wi-fi ie. hotels, campus, malls, shops etc.

DAY 2

During OBGV Session

7.0 ONLINE GENDER BASED VIOLENCE (OGBV)

Online Gender Based Violence (OBGV), Case study from Tanzania

Online or Technology- facilitated gender-based violence is a form of gender injustice and discrimination that takes place in online spaces.

- It includes stalking, harassment, bullying, and unsolicited pornography, among other actions
- Girls are being targeted online just for being young and female
- Perpetrators are now using digital tools, such as social media and GPS tracking, to cause harm alongside in-person violence.
- Digital tools have also opened the door to new intruder

8.1 Common forms of OGBV

- Cyberbullying- bullying with the use of digital technologies
- Doxing- revealing or publishing private information about a person online
- Cyberstalking- the use of the internet to stalk or harass another person
- Non-consensual pornography- distribution of sexually graphic images without consent.
- Trolling - deliberately upsetting other people by posting inflammatory content

3 Key Facts to Know About Online Gender- Based Violence

- 51% of girls online have reportedly experienced some form of online GBV personally
- Of these, 85% said they have experienced multiple forms of harassment
- 39% of girls across major cities in Africa are very concerned about their safety online.

Who is most Affected by Online GBV and Why?

- Women and girls are often particularly targeted and especially so if they are politically outspoken, are black, or have a disability
- Activists

Impact on online GBV and the Fights Against Extreme Poverty?

- Online GBV isolates women's and reaffirms patriarchal norms that tend to silence them and limit their freedoms
- Existing legal frameworks are insufficient to deal with online GBV and there is very little social support.

8.2 OGBV in Tanzania

- Infringement of privacy
- Surveillance and monitoring
- Tarnishing reputation
- Online reputation

Action to reduce OGBV

- Joint school/university clubs for education girls and boys
- Joint awareness campaign online and offline
- Report to police

1.INTERNET SHUTDOWN & CIRCUMVENTION TOOLS

According to Access Now: Internet shutdown & circumvention Tool: Internet shutdown is an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable.

8.1 Types of Internet shutdown

- Full breakout shutdown
- partially shutdown
- Social media blackout shutdown

8.2 Causes

- Election marred with a lot of irregularities
- Nation Exams
- Government order due to unknown reasons
- Security reasons
- Protests
- Diplomatic Gatherings

Who orders shutdowns & why?

- Normally authorities or Government order telecoms companies to shutdown internet. The main reason is to control flow of information especially during sensitive period when people need to access information. Example during election period, most of African countries shutdown internet i.e., in 2020 Tanzania, Burundi and Chad internet was not available.

1. MEASURING INTERNET CENSORSHIP

OONI – the Open Observatory of Network Interference (OONI) is a non-profit free software project that aims to empower decentralized efforts in documenting internet censorship around the world by using OONI probe you can run test direct from your country and all data served in OONI explore.

Since 2012 the OONI community collected million of network measurements from 200 countries, shedding light on many cases of internet censorship around the world.

OONI Probe is not a privacy tool. Anyone monitoring your internet activity (e.g. ISP) will know that you are running OONI Probe.

Types of tested URLs include provocative or objectionable sites (e.g. pornography).

By default, OONI measurements are openly published in OONI Explorer.

During measuring Internet Censorship session

10.1 CIRCUMVENTION TOOLS

During this training all participants tested three tools: Signal mobile app, Psiphon and OONI Proble.

They downloaded then installed and practiced how to use these tools.

1.INTRODUCTION TO MAILVELOP

Introduction to Mailvelop is a free software for end-to-end encryption of email traffic inside of a web browser that integrates itself into existing webmail application.

The facilitator explains the meaning of mailvelope with how to install and practice on it and explain about public key and private key and how they work

Types of encryptions

- symmetric and
- asymmetric

Uses of Open PGP

Advantage of PGP

- Sensitive information is protected
- Secure communication channels
- Encryption happen locally
- Simple Key management

1.CYBERCRIME ACT 2015 - TANZANIA

Overview of cybercrime act & Electronic and Post (Online Contents) Regulations of 2020 - EPOCA

- Security for women journalist
- Explain about security
- Who protect you online?
- How he/she protect you
- Why being protected online

The facilitator explains Cybercrime Act 2015

- Error publishing child pornography Article 13, -(1)
- Publishing false information 16.
- Discrimination error Article 13(5)
- Racist insults
- Message sent without consent Article 20. -(1)
- Error of pretending to be someone else Article 15. -(1)
- Making false statements

The facilitator explains in Summary the importance of Law

Challenges and Lesson learned

- Time management for day 1, participants arrived late in the venue which affected our timetable. Next time we recommend training and provide accommodations to all participants.

1. CASES FROM PARTICIPANTS

Janet Mushi *from Mwananchi Communication. Challenge: Restrictions in using office email. All emails from sent from her office email not delivered.*

Hilda: *Radio 5; Challenge: Call and messages diverts and she felt violated her rights to privacy.*

Tonie: *Her call Diverted by unknown people for unknown reasons.*

Shakila: *Phishing due to fake link: People sent her sms without her consent for friend request.*

Grace Macha: *Challenge: Email: Phishing email for fake email for conference in US, she was required to send $300 for visa application*

Regina; *Mega FM: Fake friend, Call Divert by his lover for surveille her communication.*

MARY- CILAO: *Fake news through her status*

Jennifer: *Call divert: Discuss about her marriage with her sisters about her husband who is a military person*

Susan: *TBC Radio Arusha: Call divert. Hacking of Facebook accounts for more than 3 times.*

1. RECOMMENDATIONS

Participants requested for more training on digital safety for women journalists and next time event can include livestreaming in order to give chance for other women journalists to join virtually. Last Zaina Foundation was advice to continue advocacy for Data Protection law in Tanzania.

1. CONCLUSION

This training addresses why it is critical for journalists to understand how the internet works and how to protect themselves within the internet ecosystem. That is, from the time communication is initiated until communication with another user in a different geographical location is received. The training emphasizes why it is critical for Tanzanian journalists to factor in security protocols while performing their roles of protecting and defending human rights. The training was successful in achieving the following goals.

- General understanding of the digital world and how the internet works in the current times of digital security and its significance to Journalists
- Appreciating the interlinkages between digital security and human rights and fundamental freedoms in Tanzania
- Appreciating the gendered dimension of digital security in Tanzania

MORE EVENT PHOTOS

Bobkevin from Mailvelop presented about email mailvelop