ZAINA FOUNDATION

A SECURE COMMUNICATION

FOR HUMAN RIGHTS DEFENDERS

ABOUT THIS GUIDE

Zaina Foundation is a Non-Governmental Organization (NGO) which was founded in 2017 and registered under the NGO's Act of 2002 with the aim of promoting digital rights and inclusion in Tanzania. Zaina Foundation was also registered in Zanzibar in 2022 according to the Society Act No 6 of 1995.

Our Mission is to create safe spaces for women online while ensuring adherence to digital rights. We do envision a world where digital rights for women are protected and respected through advocacy on internet freedom, digital security skills, policy reforms, collaborations, workshops and convening.

In line with this mission, Zaina Foundation has developed this guide to provide essential guidelines for Human Rights Defenders (HRDs) to safeguard their digital presence, particularly during election periods when they are most targeted and vulnerable. The guide addresses various scenarios HRDs might face, such as losing a device or access to an account, receiving suspicious messages, encountering malware, website downtime, online impersonation, harassment, data loss, defamation campaigns, doxxing, surveillance, and the arrest of associates. This provides immediate actions and preventive measures to help HRDs evaluate their situation and respond effectively.

03

A Better Tommorow

SCENARIO AND SUGGESTED RESPONSE

Each possible scenario is provided with the most effective strategy that HRDs can use to respond immediately to the threat they are facing.

01 LOST MY DEVICE

Response/Guide:

Lock or Erase the Device: Use Find My Device (Android) or Find My iPhone (iOS) to lock or erase the device remotely. This prevents unauthorized access to your data.

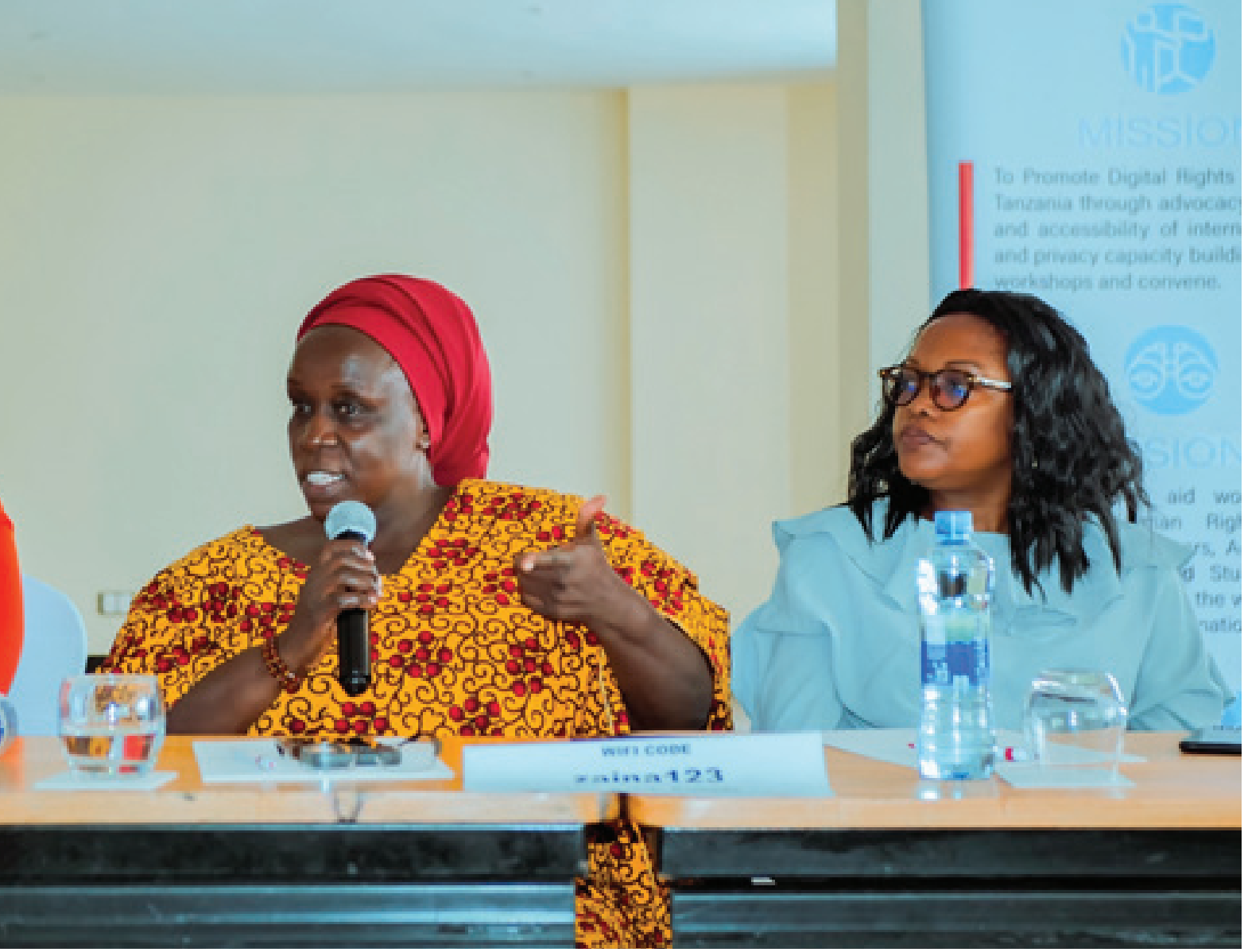
Change Passwords: Immediately change passwords for critical accounts, especially email, banking, social media, and any other services logged in on the lost device.

Inform Contacts: Notify important contacts about the loss to prevent them from responding to potential phishing attempts from your compromised accounts.

Call and notify your mobile service provider about the situation and to temporarily suspend service.

File a Police Report: Report the loss to local authorities such as Police and Tanzania Communication Regulatory Authority (TCRA) so as to have an official record.

Monitor Accounts: Keep a close watch on all accounts for any suspicious activities.



02 I Lost Access to My Account

Response/Guide:

Use Account Recovery Options: Follow the platform's account recovery process, such as "Forgot Password" links and answering security questions.

Check for Backup Codes: Use backup codes if two-factor authentication (2FA) was enabled.

Contact Support: Reach out to the platform's support for help. Provide necessary identification details to verify your identity.

PREVENTIVE MEASURES:

Enable Two Factor A uthentication and passkeys: Ensure two-factor authentication and passkeys are enabled on all accounts to add an extra layer of security.

Keep Backup Codes: Store backup codes securely for future use.

03 I Received a Suspicious Message:

Response/Guide:

Do Not Interact: Avoid clicking on links, downloading attachments, or replying to the suspicious message.

Verify the Sender: Check the sender's email address or profile for authenticity. Look for signs like misspelled domains or unverified accounts and any other suspicious signs about the message.

Report the Message: Report phishing attempts to the platform (e.g., social media site, email provider) or authorities such as TCRA. Many platforms have specific reporting tools for such messages.

Block the Sender: Block the sender to prevent further messages.

Educate Yourself: Learn about common phishing tactics to recognize future attempts.

04 My Device is Acting Suspiciously

Response/Guide:

Run Antivirus/Antimalware Software: Use reliable antivirus software to scan and remove potential threats. Schedule regular scans to keep your device clean.

Check for Unusual Activity: Look for unusual behavior, such as slow performance, unexpected pop-ups, or unknown apps. Monitor data usage for any spikes.

Update Software: Ensure the device's operating system and applications are up to date to patch known vulnerabilities.
Preventive Measures:

Install Security Updates: Regularly install security updates for your operating system and apps.

Avoid Untrusted Sources: Only download apps and files from trusted sources.

05

My Website is Down

Response/Guide:

Check Hosting Service Status: Verify if the hosting service is experiencing issues. Look for any maintenance announcements or outage reports.

Examine Server Logs: Look at server logs for errors or suspicious activity that might indicate hacking attempts or server problems.

Contact Support: Reach out to your web hosting support team for assistance. Provide them with any error messages or logs you have.

Preventive Measures:

Regular Backups: Ensure regular backups of your website to quickly restore it if needed.

Security Measures: Implement security measures like firewalls, malware scanners, and intrusion detection and prevention systems.

06

Someone is Impersonating Me Online

Response/Guide:

Report Fake Profiles: Use the platform's reporting tools to report impersonation. Provide evidence to support your claim, such as links to your genuine profiles.

Inform Authorities and your Contacts: Notify regulatory authority such as TCRA for recourse and your contacts about the impersonation to prevent them from being misled.

Seek Legal Advice: Consider legal actions if the impersonation causes significant harm, such as defamation or fraud.
Preventive Measures:

Regular Monitoring: Regularly monitor online platforms for any fake profiles.

Educate Contacts: Inform your contacts about the possibility of impersonation and how to verify your identity.

07

I'm Being Targeted by Online Harassment:

Response/Guide:

Document Everything: Keep records of all harassing messages, including screenshots, dates, and any related information.

Report to Platforms: Use platform tools to report harassment. Provide all documented evidence to support your report.

Inform the regulatory authority such as TCRA and the Tanzania Personal Data Protection Commission for available legal recourse.

Self-Care: Take breaks from online spaces and seek support from friends, family, or professionals. Consider talking to a mental health professional if needed.

Increase Privacy Settings: Enhance privacy settings on accounts to limit interactions to trusted contacts.

Legal Recourse: Consider legal actions if harassment escalates to threats or becomes particularly severe. This can be done through TCRA, The Personal Data Protection Commission and other law enforcement mechanisms.

08

I'm Being Targeted by a Defamation Campaign:

Response/Guide:

Monitor Online Mentions: Use tools like Google Alerts or Mention to track online mentions of your name or organization. Stay updated on what is being said.

Public Statement: Consider issuing a public statement to address false claims. Provide evidence to refute the defamation and clarify your position.

Legal Actions: Seek legal advice to address severe defamation. Consider pursuing defamation lawsuits if necessary.
This can be done through the respective regulatory/enforcement mechanisms such as TCRA, The Personal Data Protection Commission and other law enforcement mechanisms.

Engage Supporters: Mobilize your supporters to counter false claims and spread accurate information.

Media Strategy: Work with media professionals to manage your public image and respond to defamation.

This can be done through the respective regulatory/enforcement mechanisms such as TCRA, The Personal Data Protection Commission and other law enforcement mechanisms.

Engage Supporters: Mobilize your supporters to counter false claims and spread accurate information.

Media Strategy: Work with media professionals to manage your public image and respond to defamation.

09

Someone is Sharing My Personal Information

Response/Guide:

Contact Platforms: Request the removal of doxxed information by reporting to the platform where it was shared. Provide evidence to support your request.

Monitor Online Presence: Stay alert to additional doxxing attempts. Use tools to monitor the web for any further sharing of your personal information.

Legal Recourse: Consider legal actions if necessary, especially if the doxxing leads to harassment or threats. This can be done through TCRA, The Personal Data Protection Commission and other law enforcement mechanisms.

Increase Privacy Settings: Enhance privacy settings on your social media and other online accounts.

Educate Contacts: Inform your contacts about the doxxing and advise them to be cautious with their information.

10

I Think I'm being surveilled

Response/Guide:

Limit your Digital Footprint: Minimize sharing personal and sensitive information online. Be cautious about what you post on social media and other platforms.

Consult Experts: Reach out to organizations specializing in digital security for advice and support. They can help you identify and mitigate surveillance risks.

Use Secure Communication: Utilize circumvention technology like Tor browser, TunnelBear, and Signal for sensitive conversations.

Regular Digital Security Audits: Conduct regular digital security audits of your devices and accounts to identify vulnerabilities.

Increase Physical Security: Be aware of your surroundings and take steps to ensure your physical safety as well.

11

Someone I Know has Been arrested/ abducted

Response/Guide: Supporting Arrested/Abducted HRDs

Secure Their Data: Ensure their devices and accounts are secure to prevent unauthorized access. Change passwords and revoke access where necessary.

Coordinate Support: Work with legal and support organizations to provide assistance. Ensure they have legal representation and support networks in place.

Protect Yourself: Take steps to ensure your own safety, such as avoiding discussing sensitive information online and being cautious about your own digital security.

Public Awareness: Raise awareness about the arrest/abduction through social media and other channels. Mobilize support and advocate for their release.

Legal Support: Ensure the arrested have access to legal support and representation.

The importance of proactive security measures is far more amongst the strategies to effectively practice and enjoy our digital rights.

Measures like regular software updates, the use of encrypted communication, enabling two-factor authentication and passkeys, and maintaining regular backups must be part of our practices as HRDs and digital citizens.

Also, the need for HRDs to stay informed about potential threats and to seek support from digital security experts when necessary is highly important. It is our belief that by following these comprehensive guidelines, HRDs can better protect themselves, their work and digital rights.

REFERENCES

1. https://safesisters.org/wp-content/uploads/2019/04/Safe-Sister-Guide-revised.pdf
2. https://digitalfirstaid.org/
3. https://www.whrdnuganda.org/download/online-gbv-handbook/
4. https://www.frontlinedefenders.org/en/digital-security-resources
5. https://securitylab.amnesty.org/digital-resources/
6. https://defenddefenders.org/about-us/contact/

zainafoundationtz