Call For Application:

5-DAY TRAINING ON DIGITAL SECURITY AND RESILIENCE IN TARGETED COUNTRIES IN WEST AFRICA.

WACSI is implementing a 2-year project titled Digital Security Capacity Strengthening and Outreach Project. As part of this project WACSI has published a recent research report titled Landscape Mapping of Civil Society Digital Security in West Africa. The report reveals that significant percentage of CSOs in West Africa face a growing number of digital security threats and attacks, and this, multiple times a year. However, there is a lack of awareness and preparedness among CSOs, as many do not implement basic security measures or allocate resources for information security. The study emphasises the urgent need for digital security education and collaboration with government and organisations to protect CSOs' digital tools and data. The report highlights the importance of robust digital security laws and policies, as well as the need for harmonisation across West Africa.

Additionally, 70% of respondents have never participated in any digital security training courses which taught them how to use the internet or digital devices securely and how to protect their digital devices. CSOs lack proper training and understanding of best practices, leaving them vulnerable to breaches. It also emphasises the lack of security measures within CSOs, including the absence of computer and information security policies and deviations from existing organisational policies. To address these challenges, CSOs must invest in technology, personnel, and comprehensive training programmes. By doing so, they can enhance their digital security posture and continue their work in a safer digital environment.

It is in this context that WACSI invites applications from Civil Society Organisations (CSOs) in Cote d'Ivoire, Ghana, Nigeria, and Senegal for a 5-day training on digital security and resilience. The aim of this training is to enhance the digital security and resilience of Civil Society Organisations in West Africa.

Target audience

The training will target a total of forty (40) Civil Society Organisations, consisting of ten (10) from each target country, namely: Cote d'Ivoire, Ghana, Nigeria, and Senegal.

Each organisation will be expected to send two (2) representatives.

Timeframe

The training and action planning phase of this project spans the period June 2023 – July 2024.

Post-action planning, participating organisations will focus on the implementation and engage into community outreach and advocacy, alongside community of practice engagements, ensuring ongoing collaboration and participation.

Below is an outline of key steps involved in this phase of the project, before and after the training.

- Selection of to Participating Organisations (June 2023)
- Organisational Security Assessment (July - Aug 2023)
- Learning needs assessment (Aug 2023)
- In-country training (Sep - Oct 2023)
- Action Planning and Community Outreach Proposals (Oct – Jan 2024)
- Community Outreach and Citizens' engagement (Mar– Jun 2024)
- Documentation of change stories (Apr – May 2024)

Methodology

The training is scheduled to take place in September and will be conducted in-person. Following the training, participating organisations will be expected to develop and implement an action plan to enhance organisational digital resilience and guide community outreach efforts. Additionally, participating organisations will have the opportunity to join a community of practice dedicated to identifying gaps in cyber security laws and legal frameworks in West Africa. This collective effort aims to identify potential entry points for advocacy and drive meaningful change in digital safety and resilience in the region.

Criteria for selection:

- The organisation must be a civil society organisation and must operate in Cote d'Ivoire, Ghana, Nigeria, or Senegal.
- The organisation must be willing to nominate and commit two (2) key staff members to participate in the training programme. These representatives should be responsible for implementing digital security measures within the organisation and advocating for digital security issues.
- The organisation must be willing to make a long-term commitment to digital security beyond the training programme. This involves the implementation of an action plan to enhance digital resilience within the organisation and contribute to community outreach efforts.
- The organisation should demonstrate a clear need for digital security measures due to previous incidents, vulnerabilities, risks faced in their digital operations, or alignment with their organisational mission. This could include instances of digital security threats, attacks, breaches, or capacity or commitment to join community outreach and advocacy efforts on the issue.

Note: Meeting all the selection criteria does not guarantee selection, as the final decision will be based on the overall suitability and diversity of the selected organisations.

Application Procedure

To apply, interested CSOs are required to fill the **application form** no later than **May 31, 2023**. Selected organisations will be notified via email by June 23, 2023. For any enquiry send a mail to swowoui@wacsi.org or wsegonna@wacsi.org and cc techsoup@wacsi.org.

We encourage all eligible organisations to apply for this training, as it provides a unique opportunity to enhance your digital security and resilience in an increasingly complex digital world. We also encourage Women-led organisations to apply.

Disclaimer!!!

Kindly note that all your personal data submitted in the scope of this project will only be used for the implementation of the Digital Security Capacity Strengthening and Outreach Project and for any related activities falling within the WACSI's or its partners' mission and scope of activities.

This project is funded by the MOTT Foundation

CHARLES STEWART MOTT FOUNDATION