



## **Appel à candidature :**

### **FORMATION DE 5 JOURS SUR LA SÉCURITÉ NUMÉRIQUE ET LA RÉSILIENCE DANS DES PAYS CIBLÉS EN AFRIQUE DE L'OUEST.**

WACSI, met en œuvre un projet de deux ans intitulé Projet de renforcement des capacités et de sensibilisation à la sécurité numérique. Dans le cadre de ce projet, WACSI a publié un récent rapport de recherche intitulé [Landscape Mapping of Civil Society Digital Security in West Africa](#) (Cartographie du paysage de la sécurité numérique de la société civile en Afrique de l'Ouest). Le rapport révèle qu'un pourcentage significatif d'OSC en Afrique de l'Ouest est confronté à un nombre croissant de menaces et d'attaques de sécurité numérique, et ce, plusieurs fois par an. Cependant, il y a un manque de sensibilisation et de préparation parmi les OSC, car beaucoup ne mettent pas en œuvre des mesures de sécurité de base ou n'allouent pas de ressources conséquentes à la sécurité de l'information. L'étude souligne le besoin urgent d'éducation à la sécurité numérique et de collaboration avec le gouvernement et les organisations pour protéger les outils numériques et les données des OSC. Le rapport souligne également l'importance des lois et des politiques solides en matière de sécurité numérique, ainsi que le besoin d'harmonisation en Afrique de l'Ouest.

En outre, les OSC manquent de formation et de compréhension des meilleures pratiques, ce qui les rend vulnérables aux violations. 70 % des personnes interrogées dans le cadre de cette étude, n'ont jamais participé à des cours de formation à la sécurité numérique qui leur ont appris à utiliser Internet ou des appareils numériques en toute sécurité et à protéger leurs appareils numériques. L'étude souligne également le manque de mesures de sécurité au sein des OSC, notamment l'absence de politiques de sécurité informatique et de l'information et les écarts par rapport aux politiques organisationnelles existantes. Pour relever ces défis, les OSC doivent investir dans la technologie, le personnel et des programmes de formation complets. Ce faisant, elles peuvent améliorer leur position en matière de sécurité numérique et poursuivre leur travail dans un environnement numérique plus sûr.

Dans ce contexte, WACSI invite les organisations de la société civile (OSC) de la Côte d'Ivoire, du Ghana, du Nigéria et du Sénégal à participer à une formation de 5 jours sur la sécurité numérique et la résilience. L'objectif de cette formation est de renforcer la sécurité numérique et la résilience des organisations de la société civile en Afrique de l'Ouest.

#### **Public cible**

La formation s'adressera à un total de quarante (40) organisations de la société civile, soit dix (10) organisations de chaque pays cible, à savoir la Côte d'Ivoire, le Ghana, le Nigeria et le Sénégal.

Chaque organisation devra envoyer deux représentants.

#### **Calendrier**

La phase de formation et de planification des actions à implémenter dans le cadre de ce projet s'étendent de juin 2023 à juillet 2024.

Après la planification de l'action, les organisations participantes se concentreront sur la mise en œuvre et s'engageront dans la sensibilisation et le plaidoyer auprès de la communauté, parallèlement aux engagements de la communauté de pratique, en assurant une collaboration et une participation continues.

Vous trouverez ci-dessous un aperçu des principales étapes de cette phase du projet, avant et après la formation.

- Sélection des organisations participantes (juin 2023)
- Évaluation de la sécurité organisationnelle (juillet-août 2023)
- Évaluation des besoins d'apprentissage (août 2023)
- Formation dans le pays respectifs (septembre - octobre 2023)
- Plan d'action et propositions de sensibilisation de la communauté (oct. - janv. 2024)
- Sensibilisation de la communauté et engagement des citoyens (mars-juin 2024)
- Documentation des récits de changement (avril - mai 2024)

Le processus de sélection débutera en juin 2023, marquant le début de la phase de renforcement des capacités du projet. Bien que le projet se clôturera en juillet 2024, l'engagement dans la communauté de pratique se prolongera au-delà de la clôture du projet, garantissant une collaboration et une participation continues.

## **Méthodologie**

La formation aura lieu en septembre et se déroulera présentiel. À l'issue de la formation, les organisations participantes devront élaborer et mettre en œuvre un plan d'actions visant à renforcer la résilience numérique de l'organisation et à orienter les efforts de sensibilisation de la communauté. En outre, les organisations participantes auront la possibilité de rejoindre une communauté de pratique dédiée à l'identification des lacunes dans les lois et les cadres juridiques en matière de cybersécurité en Afrique de l'Ouest. Cet effort collectif vise à identifier des points d'entrée potentiels pour le plaidoyer et à conduire un changement significatif dans la sécurité et la résilience numériques dans la région.

## **Critères de sélection**

- L'organisation doit être une organisation de la société civile et doit opérer en Côte d'Ivoire, au Ghana, au Nigeria ou au Sénégal.
- L'organisation doit être prête à nommer et à engager deux (2) membres clés de son personnel pour participer au programme de formation. Ces représentants doivent être responsables de la mise en œuvre des mesures de sécurité numérique au sein de l'organisation et de la défense des questions de sécurité numérique.
- L'organisation doit être prête à s'engager à long terme en faveur de la sécurité numérique au-delà du programme de formation. Cela implique la mise en œuvre d'un plan d'action visant à renforcer la résilience numérique au sein de l'organisation et à contribuer aux efforts de sensibilisation de la communauté.

- L'organisation doit démontrer qu'elle a clairement besoin de mesures de sécurité numérique en raison d'incidents antérieurs, de vulnérabilités, de risques rencontrés dans ses opérations numériques ou de l'alignement sur sa mission organisationnelle. Il peut s'agir de cas de menaces, d'attaques ou de violations de la sécurité numérique, ou de la capacité ou de l'engagement de l'organisation à participer aux efforts de sensibilisation et de plaidoyer de la communauté sur cette question.

Remarque : Le fait de répondre à tous les critères de sélection ne garantit pas la sélection, car la décision finale sera basée sur l'adéquation globale et la diversité des organisations sélectionnées.

### **Procédure de candidature**

Pour postuler, les OSC intéressées doivent remplir le [formulaire de candidature](#) au plus tard le **31 mai 2023**. Les organisations sélectionnées seront informées par courriel au plus tard le 23 juin 2023. Pour toute demande de renseignements, envoyez un courriel à [swowoui@wacsi.org](mailto:swowoui@wacsi.org) ou [wsegonna@wacsi.org](mailto:wsegonna@wacsi.org) tout en mettant en copie [techsoup@wacsi.org](mailto:techsoup@wacsi.org).

Nous encourageons toutes les organisations éligibles à postuler pour cette formation, car elle offre une opportunité unique d'améliorer votre sécurité numérique et votre résilience dans un monde numérique de plus en plus complexe. Nous encourageons également les organisations dirigées par des femmes à proposer leur candidature.

### **Avertissement !!!**

Veillez noter que toutes vos données personnelles soumises dans le cadre de ce projet ne seront utilisées que pour la mise en œuvre du projet de renforcement des capacités et de sensibilisation à la sécurité numérique et pour toute activité connexe relevant de la mission et du champ d'activités du WACSI ou de ses partenaires.

Ce projet est financé par la Fondation MOTT

