

GUIDE 2026 • ÉDITION CONDENSÉE ET IMPRIMABLE

Guide de sécurité numérique

Pour les journalistes, activistes et défenseurs des droits humains

Menaces, impacts et solutions : comprendre les risques numériques, adopter les bons réflexes et réagir efficacement face à une cyberattaque, dans le contexte ouest-africain.



À propos de ce guide

Projet

Ce guide a été élaboré dans le cadre du projet « Renforcer l'espace civique et promouvoir les droits de l'homme au Mali : vers une société démocratique et inclusive », financé par l'UE



Consortium

Le projet est mis en œuvre par le consortium

ARTICLE 19, Avocats Sans Frontières (ASF-Mali) & l'Institut Panos Afrique de l'Ouest (IPAO)



Auteur

Ce guide a été élaboré par El Hadj Daouda Diagne, expert en cybersécurité.

Reproduction

Cette production est sous la licence Creative Commons Attribution _ Pas d'utilisation commerciale _ Partage dans les mêmes conditions 4.0 (CC BY-NC-SA 4.0).

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Les analyses et recommandations contenues dans ce guide n'engagent que leurs auteurs et ne reflètent pas nécessairement les opinions des organisations partenaires ou de l'Union européenne.

ABRÉVIATIONS & ACRONYMES

- **2FA** _ Authentification à deux facteurs
- **CEDEAO** _ Communauté économique des États de l'Afrique de l'Ouest
- **VPN** _ Virtual Private Network
- **CADHP** _ Commission africaine des droits de l'homme et des peuples
- **DDoS** _ Distributed Denial of Service
- **PIDCP** _ Pacte international relatif aux droits civils et politiques
- **IP** _ Internet Protocol
- **RSF** _ Reporters sans frontières
- **IT** _ Information Technology
- **ASF / IPAO** _ Avocats Sans Frontières / Institut Panos Afrique de l'Ouest

Table des matières

I.	Introduction & contexte	03
II.	Menaces & impacts	08
III.	Protection juridique	13
IV.	Hygiène numérique essentielle	17
V.	Gestion d'incident	22
VI.	Glossaire & ressources	27
VII.	Check-lists détachables	30

Comment utiliser ce guide. Les pages de la section VII sont conçues pour être détachées et gardées à portée de main lors des missions de terrain ou en cas d'incident.

I.

Introduction & contexte



Un espace civique en ligne de plus en plus exposé

En Afrique de l'Ouest, les journalistes, activistes et défenseurs des droits humains évoluent dans un environnement numérique de plus en plus exposé aux cybermenaces.

La multiplication des cyberattaques, telles que le hameçonnage (phishing), le piratage de comptes, la désinformation, la surveillance illégale ou les rançongiciels, affecte directement la liberté d'expression, la confidentialité des sources, la sécurité des données ainsi que la crédibilité des médias et des organisations. Dans plusieurs contextes sensibles, ces menaces sont également utilisées comme outils d'intimidation, de pression ou de censure contre les acteurs de l'information et de la société civile.

Principes directeurs



Priorisation

Distinguer l'essentiel du secondaire.



Simplicité

Procédures courtes, check-lists actionables.



Protection des personnes

Confidentialité des sources.



Contextualisation

Adaptation à l'Afrique de l'Ouest.

Objectifs du guide

- Comprendre les menaces prioritaires
- Choisir des outils adaptés au contexte local
- Adopter des réflexes d'hygiène numérique
- Réagir efficacement en cas d'incident

Ce qui fonctionne, ce qui manque encore

✓ Bien fait

- Une majorité utilise des mots de passe complexes
- Bonne prise de conscience des risques de piratage

✗ Lacunes critiques

- Seulement 50 % activent la 2FA
- Réaction souvent tardive, après l'incident
- Manque de ressources, en temps et en budget

Besoins identifiés

01

Protéger efficacement les données grâce au chiffrement et aux sauvegardes.

02

Savoir réagir à une crise numérique à l'aide de protocoles clairs.

03

Préserver l'anonymat et la sécurité en ligne.

04

Bénéficier d'une formation pratique en sécurité numérique.

Public visé

Niveau

Débutant à intermédiaire.

Contexte

Fortement exposé, sous contrainte de temps.

Équipement

Smartphone ou ordinateur, budget limité.

Priorité

Protection des personnes et du travail journalistique.

II.

Menaces & impacts



Quatre menaces prioritaires

Piratage de comptes, pertes de données, attaques par déni de service et désinformation concentrent l'essentiel du risque pour les acteurs de l'information en Afrique de l'Ouest.

MENACE	NIVEAU	VECTEURS COURANTS	SIGNAUX D'ALERTE	IMPACTS TYPIQUES
Pertes de données	CRITIQUE	Vol, confiscation, rançongiciel, panne	Fichiers manquants, appareil indisponible	Exposition des sources, chantage
Piratage de comptes	CRITIQUE	Phishing, credential stuffing	Alertes de connexion, messages suspects	Vol d'identité, désinformation
Attaques DDoS	ÉLEVÉ	Botnets, requêtes massives	Site très lent ou inaccessible	Indisponibilité, perte d'audience
Désinformation	ÉLEVÉ	Faux comptes, bots, deepfakes	Pics de mentions, contenu manipulé	Atteinte à la réputation, risques psychosociaux

Piratage de comptes : gros plan

Modes opératoires

- **Phishing** — faux e-mails imitant des services légitimes
- **Credential stuffing** — exploitation de fuites de données
- **SIM swap** — transfert frauduleux de numéro
- **Ingénierie sociale** — manipulation psychologique

Contre-mesures

- 2FA obligatoire, via application plutôt que par SMS
- Gestionnaire de mots de passe
- Mots de passe uniques par compte
- Séparation des usages professionnels et personnels

Qui sont les attaquants ?

PROFIL	CAPACITÉS	SIGNAUX	PROTECTION
États & gouvernements	Surveillance, censure, pression judiciaire	Convocations urgentes, blocages géolocalisés	Chiffrement, canaux de repli, audit mensuel
Groupes organisés (cybercriminels)	Intrusions ciblées, rançongiciels, mercenariat numérique	E-mails contextualisés suspects, messages d'extorsion	Antivirus, sauvegardes 3-2-1, isolation de la machine
Individus isolés (trolls, hacktivistes)	Harcèlement, doxxing, force brute	Pics de mentions, éléments de langage identiques	Paramètres de confidentialité, modération proactive

Impacts multi-niveaux

Liberté d'expression

- Autocensure par crainte
- Indisponibilité de la diffusion
- Confusion informationnelle

Sécurité personnelle

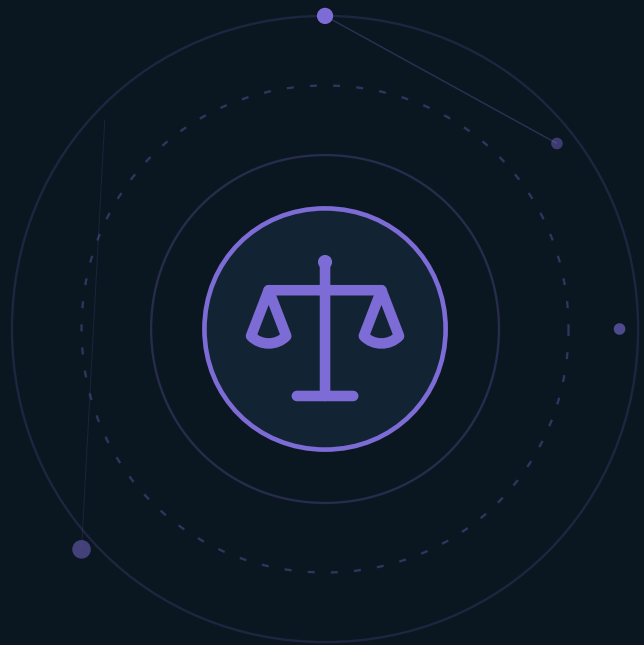
- Doxxing, atteinte à la vie privée
- Intimidations en ligne
- Stress post-incident

Crédibilité

- Manipulation de la réputation
- Usurpation d'identité
- Perte de confiance des sources

III.

Protection juridique



Des cadres à mobiliser

Face à l'augmentation des atteintes à la liberté d'expression, plusieurs instruments juridiques régionaux et internationaux protègent les acteurs de l'information dans l'espace numérique.

Instruments régionaux

CEDEAO

Règlement C/REG.4/05/14 sur la protection des données personnelles, article 20.

Union africaine

Charte africaine des droits de l'homme et des peuples, article 9.

CADHP

Déclaration de principes sur la liberté d'expression et l'accès à l'information en Afrique.

Instruments internationaux

PIDCP

Article 19 : liberté d'expression.

Déclaration universelle des droits de l'homme

Article 19 : liberté d'opinion et d'expression.

UNESCO

Recommandation sur la sécurité des journalistes et la question de l'impunité.

Documenter, signaler, se faire assister

01 · Documentation

Documenter toutes les violations (captures d'écran, échanges, preuves) et les conserver de manière sécurisée.

02 · Assistance

Contactez un avocat spécialisé en droits numériques et signaler aux organisations de défense des droits humains.

03 · Organisations

ARTICLE 19, Reporters sans frontières, Amnesty International, commissions nationales des droits humains.

Bon à savoir. La connaissance des instruments juridiques et des recours disponibles renforce votre capacité à vous protéger et à défendre vos droits en ligne.

Contacts

CADHP	communications@achpr.org
ARTICLE 19 Afrique de l'Ouest	senegal.westafrica@article19.org
Access Now (24 h/24, 7 j/7)	help@accessnow.org
Paradigm Initiative	info@paradigmhq.org

IV.

Hygiène
numérique
essentielle



Des réflexes simples, au quotidien

La sécurité numérique repose avant tout sur l'adoption de bonnes pratiques quotidiennes, pour réduire les risques de compromission des comptes, des appareils et des données.

Protéger vos comptes et vos données

01 · Mots de passe

- Longs et uniques
- Gestionnaire dédié
- Jamais réutilisés

02 · Authentification 2FA

- Sur les comptes sensibles
- Application plutôt que SMS
- Codes de secours en lieu sûr

03 · Sauvegardes

- Automatiques
- Stockage externe ou cloud sécurisé
- Restauration testée régulièrement

Protéger vos équipements

Verrouillage

PIN, mot de passe ou biométrie ; jamais 1234 ou 0000.

Chiffrement

Disque dur chiffré pour protéger les données en cas de perte.

Antivirus

Fiable, à jour, analyses régulières.

Vérifications

Applications à jour, permissions contrôlées.

Réseaux sociaux

Confidentialité

Paramètres vérifiés régulièrement.

Contacts

Accepter uniquement les personnes connues.

Sources

Ne jamais exposer une source ou une localisation.

À éviter

Liens suspects, sur-partage personnel.

Protections essentielles

Sécurité des comptes

- ☐ Mot de passe fort
- ☐ 2FA activée
- ☐ Gestionnaire de mots de passe

Sécurité des appareils

- ☐ Verrouillage actif
- ☐ Antivirus installé
- ☐ Système à jour

Sécurité des communications

- ☐ Messagerie sécurisée
- ☐ Chiffrement activé
- ☐ Vérification des contacts

Protection des données

- ☐ Sauvegardes régulières
- ☐ Données chiffrées
- ☐ Accès sécurisé

Communications sécurisées, en un coup d'œil



Utilisateur

Envoi d'un message
ou d'un fichier



Chiffrement

Message chiffré
avant transmission



Application sécurisée

Signal ou Proton,
par exemple



Réception

Seul le destinataire
peut lire le message

V.

**Gestion
d'incident**



Face à une cyberattaque, la rapidité compte

Un protocole clair et structuré permet de contenir l'incident, de sécuriser les comptes et de rétablir rapidement un environnement fiable.

PHASE 01 • 0 À 15 MIN

Réaction immédiate

- Déconnecter l'appareil compromis
- Ne pas l'éteindre brutalement
- Utiliser un appareil sain
- Capturer les preuves

PHASE 02 • 15 À 60 MIN

Sécurisation

- Changer les mots de passe
- Vérifier les comptes liés
- Activer la 2FA manquante
- Révoquer les sessions actives

PHASE 03 • 1 H ET PLUS

Alerte & assistance

- Informer l'organisation
- Contacter un expert ou une ONG
- Documenter la chronologie
- Basculer sur des canaux sécurisés

Scénarios spécifiques

Suspicion de phishing

- Ne pas cliquer sur les liens ou pièces jointes
- Transférer l'e-mail au service IT
- Vérifier les règles de transfert
- Changer le mot de passe si nécessaire
- Scanner l'appareil

Compromission de compte

- Signaler via les formulaires officiels
- Contacter le support de la plateforme
- Informer les contacts
- Sauvegarder les preuves
- Renforcer la sécurité après récupération

Plan d'urgence

- 01 Effacement à distance de l'appareil (Find My Device, iCloud).
- 02 Changer tous les mots de passe sensibles.
- 03 Révoquer les accès aux applications.
- 04 Bloquer la carte SIM ou les cartes bancaires si nécessaire.
- 05 Déclarer le vol auprès des autorités compétentes, si applicable.

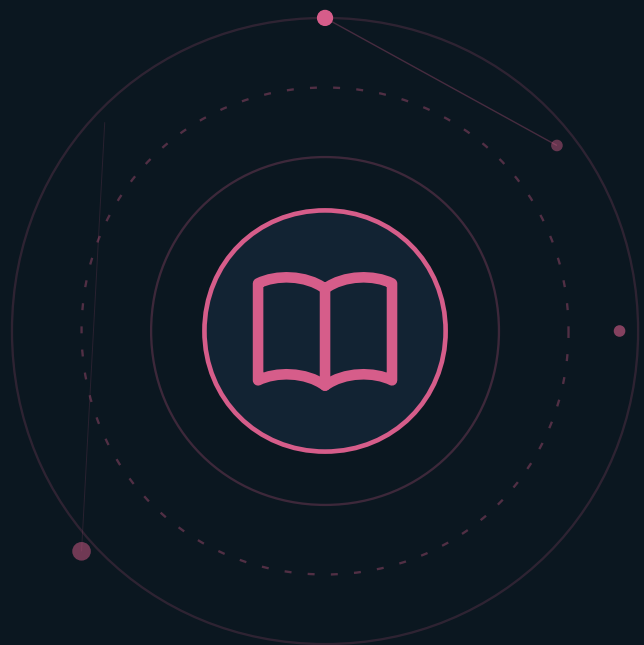
Contacts d'assistance d'urgence

Access Now Digital Security Helpline Ligne 24 h/24, 7 j/7	help@accessnow.org
ARTICLE 19 Afrique de l'Ouest	senegal.westafrica@article19.org
Paradigm Initiative	info@paradigmhq.org
Media Foundation West Africa	info@mfwf.org

Post-incident. Rédiger un rapport interne (causes, impacts, mesures prises), partager les leçons apprises, mettre à jour le plan de sécurité, former l'équipe, séparer les usages professionnels et personnels, tester les sauvegardes.

VI.

Glossaire & ressources



Les notions clés, en clair

- **2FA** — méthode nécessitant deux preuves d'identité pour accéder à un compte
- **Mot de passe fort** — long, unique et difficile à deviner
- **Chiffrement** — rend les données illisibles sans autorisation
- **DDoS** — attaque visant à rendre un service inaccessible par surcharge
- **Phishing** — fraude visant à voler des informations via de faux messages
- **Ingénierie sociale** — manipulation visant à obtenir des informations sensibles
- **Malware** — logiciel malveillant conçu pour infiltrer ou endommager un système
- **Données sensibles** — sources, documents, identifiants nécessitant une protection particulière
- **VPN** — sécurise la connexion Internet et masque l'adresse IP
- **Sauvegarde** — copie de données permettant leur récupération en cas de perte

Outils recommandés

Sécurité des comptes

Bitwarden, 1Password ; Google Authenticator, Authy.

Communications

Signal, pour la messagerie chiffrée ; ProtonMail, pour l'e-mail.

Appareils

Antivirus fiables, outils de chiffrement du disque.

Qui contacter, où se former

INGO

- Digital Security Helpline
- Reporters Sans Frontières (RSF)
- Amnesty International

ONG régionales

- ARTICLE 19 Afrique de l'Ouest
- Paradigm Initiative
- Media Foundation West Africa

Exemples de Guides pratiques

- Security in a Box
<https://securityinabox.org/en/>
- Tactical Tech Collective
<https://tacticaltech.org/>
- Surveillance Self-Defense (EFF)
<https://www.eff.org/>

Bonnes pratiques, en résumé. Activer la 2FA sur tous les comptes, utiliser des mots de passe uniques, sauvegarder régulièrement ses données, mettre à jour ses appareils, utiliser des outils sécurisés.

VII.

Check-lists détachables



Check-list sécurité quotidienne

Authentification (hebdomadaire)

- ☐ Vérifier les sessions actives des comptes principaux
- ☐ Contrôler les alertes de sécurité reçues
- ☐ Tester le bon fonctionnement de la 2FA
- ☐ Mettre à jour le gestionnaire de mots de passe

Appareils (quotidien)

- ☐ Verrouillage automatique activé
- ☐ Mises à jour système et applications installées
- ☐ Antivirus à jour et actif
- ☐ Sauvegardes automatiques vérifiées

Communications (à chaque usage)

- ☐ VPN activé sur les réseaux publics
- ☐ Vérifier les expéditeurs des e-mails
- ☐ Utiliser des messageries chiffrées pour les sujets sensibles
- ☐ Vérifier les paramètres de confidentialité des réseaux sociaux

Check-list mission terrain

Préparation (48 h avant)

- ☐ Téléphone dédié minimal configuré
- ☐ Contacts d'urgence synchronisés
- ☐ Sauvegardes complètes effectuées
- ☐ Plan de communication de crise défini
- ☐ Codes de récupération 2FA imprimés

Sur le terrain

- ☐ VPN activé en permanence
- ☐ Géolocalisation désactivée
- ☐ Communications via canaux chiffrés uniquement
- ☐ Photos et vidéos publiées sans métadonnées
- ☐ Verrouillage biométrique et PIN combinés

Retour de mission

- ☐ Changement des mots de passe sensibles
- ☐ Analyse antimalware complète
- ☐ Transfert sécurisé des données collectées
- ☐ Effacement sécurisé des données temporaires
- ☐ Débriefing sécurité avec l'équipe

Check-list incident cyber

Réaction immédiate (0 à 15 min)

- ☐ Déconnexion de l'appareil compromis
- ☐ Basculement vers un appareil sain
- ☐ Capture des preuves (photos, journaux)
- ☐ Notation des symptômes et des horaires
- ☐ Isolation du réseau si nécessaire

Sécurisation (15 à 60 min)

- ☐ Changement des mots de passe depuis un appareil sain
- ☐ Révocation des sessions actives
- ☐ Vérification des comptes liés
- ☐ Activation de la 2FA si manquante
- ☐ Alerte des contacts sensibles

Assistance & suivi (1 h et plus)

- ☐ Contacter un expert ou une ONG en cybersécurité
- ☐ Informer la rédaction ou l'organisation
- ☐ Documenter la chronologie complète
- ☐ Évaluer l'étendue de la compromission
- ☐ Définir un plan de restauration

Monitoring mensuel sécurité

- ☐ Audit des connexions sur tous les comptes principaux
- ☐ Test de restauration d'une sauvegarde
- ☐ Mise à jour du gestionnaire de mots de passe
- ☐ Révision des paramètres de confidentialité
- ☐ Vérification des applications installées, suppression des inutiles
- ☐ Contrôle des espaces de stockage cloud
- ☐ Formation sur les nouveaux outils et les nouvelles menaces
- ☐ Mise à jour des contacts d'urgence

Conservez ces pages détachées à portée de main, sur votre bureau ou dans votre sac de mission.

ARTICLE 19 est une organisation internationale de référence engagée dans la défense et la promotion de la liberté d'expression à travers le monde. Son action vise à renforcer les mouvements locaux et internationaux œuvrant pour ce droit fondamental, afin que chaque personne puisse faire entendre sa voix et exercer pleinement sa liberté d'expression.

En collaboration avec ses partenaires, ARTICLE 19 produit des recherches approfondies, ainsi que des analyses juridiques et politiques de haut niveau destinées à influencer les réformes et les politiques publiques.

Présente sur le terrain grâce à neuf bureaux régionaux répartis dans le monde, l'organisation agit au plus près des réalités locales tout en contribuant à faire progresser le mouvement mondial pour la liberté d'expression par l'innovation et l'action collective.

Ses interventions s'articulent autour de cinq priorités stratégiques :

- promouvoir l'indépendance des médias ;
- améliorer l'accès à l'information ;
- protéger les journalistes ;
- renforcer l'espace civique ;
- veiller à ce que les droits humains occupent une place centrale dans le développement de l'environnement numérique.

*« Dans un monde connecté, votre sécurité numérique
est votre liberté d'expression. »*