GUIDE PRATIQUE

SÉCURITÉ NUMÉRIQUE

Projet d'Appui à la Résilience Digitale des Engagé.es (ARDEN)



Guide adapté par

UBUNTEAM
"Join us, Learn... Get Free"

Avec le soutien de

Digital Defenders Partnership

Hivos people unlimited

SOMMAIRE

Table des matières

01 **Mots de passe** 04
Créer des mots de passe forts · Gestionnaires · Authentification

02 **Communications sécurisées** 04
Applications de messagerie · Appels sécurisés · E-mails · VPN

03 **Téléphones et ordinateurs** 04
Sécuriser vos appareils · Mises à jour · Réseaux Wi-Fi · Chiffrement

04 **Fichiers et données** 04
Sauvegardes · Chiffrement de fichiers · Suppression sécurisée · Cloud

05 **Violences basées sur le genre facilitées par la technologie** 04
Reconnaître les violences numériques · Protection · Ressources d'aide

Un guide simple, pratique et accessible pour mieux se protéger en ligne et adopter des habitudes numériques plus sûres.

Pour les défenseur·e·s des droits humains et les organisations de la société civile.

- **Projet :** Appui à la Résilience Digitale des Engagés (ARDEN)
- **Organisation porteuse :** Ubunteam
- **Durée du projet :** 6 mois
- **Zones d'intervention :** Abidjan – Bouaké – Korhogo
- **Partenaires et ressources :** Guide inspiré de Security in a Box (Tactical Tech), avec le soutien de Digital Defenders Partnership
- **Ressource gratuite et téléchargeable sur :** arden.ubunteam.org

Préambule

Ce document est un **guide pratique de sécurité numérique** destiné aux défenseur·e·s des droits humains, journalistes, activistes, membres d'organisations de la société civile et, plus largement, à toute personne amenée à utiliser des outils numériques dans un contexte sensible.

Il a été conçu par **Ubunteam**, une organisation à but non lucratif basée en Côte d'Ivoire, engagée depuis plusieurs années dans la promotion des logiciels libres, la défense des droits numériques et le renforcement des capacités en sécurité numérique auprès des communautés et organisations locales.

Contexte de création du guide

Ce guide s'inscrit dans le cadre du projet **ARDEN « Appui à la Résilience Digitale des Engagés»**, mis en œuvre par Ubunteam. Ce projet vise à répondre à des menaces numériques de plus en plus fréquentes : piratage de comptes, surveillance, désinformation, cyberharcèlement, perte ou vol de données, et vulnérabilités liées à de mauvaises pratiques numériques.

L'un des constats majeurs à l'origine de ce projet est que **beaucoup de personnes sont exposées à des risques numériques sans en avoir pleinement conscience**, ou disposent de ressources trop techniques, peu accessibles, ou mal adaptées à leur réalité quotidienne.

Une ressource inspirée de *Security in a Box*

Certaines sections de ce guide sont adaptées de *Security in a Box*, développé par Tactical Tech et Front Line Defenders. Les contenus ont été reformulés et contextualisés pour être compréhensibles par des personnes peu ou pas techniciennes. Ce guide inclut également des contenus originaux sur la protection contre la violence basée sur le genre facilitée par la technologie (VBGFT). Toutes les sections, qu'elles soient inspirées de *Security in a Box* ou créées par Ubunteam, sont partagées sous licence Creative Commons Attribution ShareAlike (CC BY SA). Cela permet de réutiliser, adapter et partager le contenu, à condition de mentionner la source et de publier toute adaptation sous la même licence.



TACTICAL TECH

À qui s'adresse ce guide ?

Ce guide s'adresse avant tout à des personnes qui :



utilisent un téléphone, un ordinateur, des emails ou des **réseaux sociaux**



n'ont pas nécessairement de **connaissances techniques** avancées



souhaitent **mieux se protéger** sans devenir des expert·e·s en informatique.

Aucune connaissance préalable en sécurité numérique n'est requise pour le lire et l'utiliser.

Comprendre la sécurité numérique

Il est important de rappeler que **la sécurité numérique n'est jamais absolue. Il n'existe aucune solution 100 % sûre**, ni aucun outil magique capable de tout protéger. La sécurité numérique est :

- ☑ **évolutive :** les menaces changent, les outils évoluent ;
- ☑ **progressive :** chaque petite amélioration réduit les risques ;
- ☑ **contextuelle :** les bonnes pratiques dépendent de la situation de chacun·e.

Ce guide propose donc **des bases essentielles**, destinées à réduire les risques, et non à les éliminer totalement.

La sécurité numérique, ce n'est pas seulement des outils...

Installer une application ou utiliser un nouvel outil ne suffit pas, la sécurité numérique repose aussi sur : des **habitudes** ; des **réflexes** ; des **choix quotidiens** (mots de passe, partages, clics, sauvegardes, etc.).

Changer certaines pratiques dangereuses est souvent **plus important que télécharger un nouvel outil**. Ce guide insiste donc autant sur les **comportements** que sur les **solutions techniques.**

Un guide vivant et un accompagnement possible

Ce document n'a pas vocation à rester figé ni à remplacer l'échange humain. **Ubunteam reste disponible** pour :

- accompagner les lecteur·rice·s dans la compréhension du contenu ;
- organiser des sessions de formation pratiques ;
- répondre aux questions et besoins spécifiques ;
- adapter les recommandations à des contextes particuliers.

La **sécurité numérique est un apprentissage collectif**, qui se renforce par le partage, la pratique et la solidarité.

Comment utiliser ce guide ?

Ce guide est conçu pour vous aider à mieux protéger vos informations, vos appareils et vos communications numériques. Voici quelques conseils pour en tirer le meilleur parti :

Lire à votre rythme 01

- ☑ Vous n'êtes pas obligé·e de tout comprendre du premier coup.
- ☑ Allez section par section, prenez le temps d'appliquer les conseils simples avant de passer à la suite.
- ☑ N'hésitez pas à revenir sur les points que vous n'avez pas compris.

Commencer par les actions simples 02

- ☑ Certaines mesures sont faciles à mettre en place et apportent une protection immédiate.
- ☑ Par exemple, créer des mots de passe forts et uniques, activer la double authentification, ou faire des sauvegardes régulières.
- ☑ Même de petits changements dans vos habitudes quotidiennes peuvent réduire considérablement les risques.

Adapter les conseils à votre situation 03

- ☑ Chaque personne et chaque organisation a des besoins différents.
- ☑ Choisissez les mesures qui sont **réalisables dans votre contexte**, puis progressez graduellement vers des pratiques plus avancées.

Ne vous limitez pas aux outils 04

- ☑ Installer une application ou un logiciel ne suffit pas.
- ☑ La sécurité repose autant sur vos **habitudes et réflexes quotidiens** : mots de passe, vigilance face aux emails suspects, choix de partage de vos données.

Profiter de l'accompagnement possible 05

- ☑ Ubunteam est disponible pour **répondre à vos questions** et vous aider à appliquer les recommandations.
- ☑ Vous pouvez participer à des **sessions de formation pratiques** organisées par l'organisation.
- ☑ N'hésitez pas à demander de l'aide si une mesure vous semble complexe ou si vous voulez être sûr·e de la mettre correctement en place.

Considérer ce guide comme vivant

06

- ☑ Les menaces numériques et les outils évoluent constamment.
- ☑ Ce guide est un point de départ : continuez à vous informer, tester et adapter vos pratiques.
- ☑ Partagez vos expériences avec vos collègues et vos pairs : la sécurité numérique se renforce par la pratique et la solidarité.

01



CHAPITRE

MOTS DE PASSE

Les clés de votre maison numérique. Apprenez à les créer, les gérer et les protéger facilement.

Les **mots de passe** sont comme les **clés de votre maison numérique.** S'ils sont faibles ou mal protégés, n'importe qui peut entrer. Ce chapitre va vous montrer comment créer, gérer et protéger vos mots de passe facilement et efficacement.

01 Créer un mot de passe sécurisé

Un mot de passe sûr doit respecter trois règles simples :

- **Longueur :** au moins 12 caractères
- **Variété :** lettres (majuscules et minuscules), chiffres, symboles (! ? @ # %)
- **Pas d'infos personnelles :** éviter nom, prénom, date de naissance, nom des enfants, mots trop évidents comme "123456" ou "password"



ASTUCES

Utilisez une phrase facile à retenir et ajoutez chiffres/ symboles.

Exemple : *Cafe2026!Abidjan*

02 Ne jamais utiliser le même mot de passe partout

Mauvaise pratique

Un mot de passe pour tous vos comptes.

Bonne pratique

Un mot de passe différent pour chaque compte important.

ASTUCES
Utilisez un gestionnaire de mots de passe pour ne retenir qu'un seul mot de passe principal.

03 Gérer ses mots de passe en toute sécurité

Mauvaise pratique

- Écrire vos mots de passe sur papier visible
- Les envoyer par message ou email
- Les noter dans les notes de téléphone sans protection
- Stocker un fichier appelé "motdepasse.doc"

Solution recommandée

- **Gestionnaire de mots de passe** - Crée, stocke et protège vos mots de passe

Exemples fiables :
- ***Bitwarden*** *(gratuit, multiplateforme),*
- ***KeePassXC*** *(open source, hors ligne)*

04 Ajouter une protection supplémentaire : la double authentification (2FA)

Même un mot de passe fort peut être volé. La 2FA ajoute une deuxième étape de sécurité :

- Entrer votre **mot de passe**
- Saisir un **code temporaire** reçu par SMS ou via une application (Google Authenticator, Authy)

Activez la 2FA sur vos emails, réseaux sociaux et comptes professionnels.



05 Attention aux messages et emails suspects (phishing)

RÈGLE N°1

Ne cliquez jamais sur des **liens suspects**

RÈGLE N°2

Ne donnez jamais votre mot de passe par **message ou email**

RÈGLE N°3

Vérifiez toujours l'adresse de l'expéditeur

Aucune organisation sérieuse ne demandera votre mot de passe par message.



06 Vérifier si un compte a été compromis

Outil recommandé :
Have I Been Pwned



Entrez votre adresse email pour **savoir si vos données ont fuité**. Si oui :

- **changez** le mot de passe,
- **activez la 2FA** et ne réutilisez plus l'ancien mot de passe

À RETENIR

- **Mot de passe** = long, unique, protégé
- Utilisez **un gestionnaire** pour simplifier la gestion
- **Activez la 2FA** dès que possible
- **Méfiez-vous** des messages et **emails suspects**

MINI-GLOSSAIRE

Gestionnaire de mots de passe
Application qui stocke et sécurise vos mots de passe

2FA / Double authentification
Sécurité supplémentaire avec code temporaire

Phishing
Tentative de tromperie pour voler vos informations

CHECKLIST PRATIQUE

- [ ] Mes mots de passe sont longs, uniques et difficiles à deviner.
- [ ] J'utilise un gestionnaire de mots de passe pour stocker et créer mes mots de passe.
- [ ] La double authentification (2FA) est activée sur mes comptes importants.
- [ ] Je ne partage jamais mes mots de passe par email ou message.
- [ ] Je vérifie régulièrement si mes comptes ont été compromis.

Vos mots de passe sont maintenant solides et vos comptes protégés.

La prochaine étape ? **Sécuriser vos communications** pour que personne ne puisse espionner vos messages.

02



CHAPITRE

COMMUNI-CATIONS

Choisir les bons outils pour protéger vos échanges, vos appels et vos emails contre l'interception.

Vos messages et emails contiennent des informations précieuses. Sécuriser vos communications, c'est comme fermer les rideaux de votre maison : vous protégez ce qui se passe à l'intérieur et vous évitez que des inconnus puissent espionner vos échanges. Voyons comment faire simple et efficace !

01 Protéger ses comptes sur les réseaux sociaux

- Utilisez un **mot de passe fort et unique** (voir chapitre précédent)
- Activez la **double authentification (2FA)**
- Vérifiez régulièrement vos **paramètres de confidentialité :**
    - Qui peut voir vos publications ?
    - Qui peut vous envoyer des messages ?
    - Qui peut voir votre liste d'amis ?

Limitez l'accès aux **personnes de confiance uniquement.**

02 Se protéger contre le phishing

Le **phishing** = messages/pièges qui semblent officiels mais sont faux.

- Ne cliquez pas sur les **liens suspects**
- Ne téléchargez pas de **fichiers inattendus**
- Ne donnez jamais votre **mot de passe par message ou email**

En cas de doute : vérifiez d'abord, **ne faites rien impulsivement.**

03 Sécuriser ses emails

- ☑ Utiliser un **mot de passe fort et unique**
- ☑ **Activer** la 2FA
- ☑ **Vérifier** les connexions récentes
- ☑ **Supprimer emails** suspects ou urgents

04 Applications de messagerie sécurisée

Signal - Recommandé

Messagerie et appels chiffrés de bout en bout. Open source, gratuit, aucune publicité.



Whatsapp - Acceptable

Chiffrement activé, mais appartient à Meta. Métadonnées collectées.



Bonne pratique

☑ **Verrouillage** de l'app, vérifier **appareils connectés**, **désactiver sauvegardes** non chiffrées

05 Que faire si un compte est compromis

- ☑ **Changer** le mot de passe
- ☑ **Déconnecter tous les appareils** inconnus
- ☑ **Vérifier ou activer** la 2FA
- ☑ **Prévenir vos contacts** si nécessaire



À RETENIR

- Vos **communications** sont souvent **ciblées**
- **Protégez vos emails** et messages sensibles
- **Méfiez-vous des liens** et fichiers suspects
- Utilisez des **outils fiables**

MINI-GLOSSAIRE

- **Phishing**
  Tentative de tromperie pour voler vos informations
- **2FA / Double authentification**
  Sécurité supplémentaire avec code temporaire
- **Chiffrement**
  Rendre un message illisible pour les tiers

CHECKLIST PRATIQUE

- [ ] Mes paramètres de confidentialité sur les réseaux sociaux sont limités aux personnes de confiance.
- [ ] Je me méfie des liens et fichiers suspects (phishing).
- [ ] J'utilise des applications de messagerie sécurisée (ex: Signal) pour les échanges sensibles.
- [ ] La double authentification (2FA) est activée sur mes emails et messageries importantes.
- [ ] Je sais quoi faire si un compte est compromis (changer mot de passe, prévenir contacts, vérifier appareils connectés).

Maintenant que vos communications sont sécurisées, passons à vos appareils ! Téléphone et ordinateur sont vos clés d'accès au monde numérique. Dans le **prochain chapitre,** on va apprendre à les protéger pour que rien ne vienne mettre vos comptes en danger.

03



CHAPITRE

TÉLÉPHONES & ORDINATEURS

Vos appareils sont la porte d'entrée de votre vie numérique. Sécurisez-les avant tout.

Vos appareils sont comme vos poches dans le monde numérique : si quelqu'un les ouvre, il a accès à tout ce que vous possédez. Ce chapitre va vous montrer **comment sécuriser votre téléphone et votre ordinateur facilement,** sans devenir un expert en informatique.

01 Se protéger contre les virus et malwares

Ne téléchargez pas d'applications **hors des stores** officiels	**Ne cliquez pas** sur des **liens douteux**	**Ne téléchargez pas** de **fichiers inattendus**

02 Protéger son téléphone

Android



- **Code** de verrouillage **long** ou empreinte
- Verrouillage **automatique**
- **Applications** uniquement depuis **Google Play**, supprimer inutiles, refuser permissions inutiles

Iphone



- **Code** activé
- **Mise à jour** automatique
- **Sauvegardes** protégées **par mot de passe**

03 Protéger son ordinateur

- ☑ **Windows**
  Activer antivirus intégré, mises à jour, éviter logiciels piratés
- ☑ **Mac**
  Mises à jour, mot de passe au démarrage, applications fiables
- ☑ **Linux**
  Mises à jour, logiciels depuis dépôts officiels, éviter copier-coller sans comprendre



04 Chiffrement et verrouillage

Chiffrement des données | **Mot de passe fort** pour l'appareil | **Verrouillage** automatique

05 En cas de vol ou perte

- ☑ **Bloquer** l'appareil **à distance**
- ☑ **Changer les mots de passe** importants
- ☑ **Prévenir** votre organisation
- ☑ **Supprimer les données à distance** si nécessaire



À RETENIR

- Un **appareil non sécurisé** = tous vos comptes en danger
- Mises à jour essentielles
- Logiciels **piratés** = risques de **virus**
- **Verrouillez et chiffrez** toujours **vos appareils**

MINI-GLOSSAIRE

Malware
Logiciel malveillant qui peut voler vos données

Chiffrement
Sécuriser vos fichiers pour qu'ils soient illisibles sans mot de passe

Verrouillage automatique
Sécurité qui bloque l'appareil après une période d'inactivité

CHECKLIST PRATIQUE

- [ ] Mon téléphone et mon ordinateur sont à jour (système et applications).
- [ ] Je n'installe que des applications provenant de sources officielles.
- [ ] Mes appareils sont protégés par un mot de passe fort et un verrouillage automatique.
- [ ] J'ai activé le chiffrement des données si disponible.
- [ ] Je sais comment bloquer ou effacer mes appareils à distance en cas de perte ou vol.

Vos appareils sont maintenant protégés. Il reste un **dernier chapitre** : comment gérer, sauvegarder et sécuriser vos fichiers et données pour ne jamais perdre le contrôle de vos informations.

04



CHAPITRE

FICHIERS ET DONNÉES

Sauvegarder, chiffrer et effacer vos fichiers sensibles de manière sûre et organisée.

Vos fichiers sont vos souvenirs, vos preuves, vos informations sensibles. Les protéger, c'est comme **mettre vos dossiers importants dans un coffre-fort numérique**. Ce chapitre vous montre comment faire simple, sûr et efficace.

01 Identifier les fichiers sensibles

Listes de contacts, documents internes, photos/vidéos privées, échanges confidentiels, données personnelles. Tout fichier qui peut causer problème s'il tombe entre de mauvaises mains est sensible.

02 Protéger les fichiers sensibles

- ☑ **Ne pas laisser** sur appareil partagé
- ☑ **Ne pas stocker** tout au **même endroit**
- ☑ **Chiffrement recommandé** pour rendre illisibles les fichiers

03 Sauvegarder les fichiers

- Toujours une **copie dans un autre endroit** (disque dur externe, clé USB chiffrée, cloud sécurisé)
- **Sauvegarder régulièrement** et tester la sauvegarde
- **Protéger** la sauvegarde **avec mot de passe et 2FA**

04 Récupérer après perte ou incident

- Utiliser **sauvegardes**
- **Changer** mots de passe
- **Vérifier fuite** de données
- **Informer l'organisation** si nécessaire

05 Supprimer définitivement

"Supprimer" ≠ "détruire"

- Utiliser **outils de suppression sécurisée**
- **Réinitialiser** appareil avant de le céder

06 Détruire les informations d'identification

- **Scans** de documents, photos d'identité, anciens mots de passe
- **Garder uniquement** ce qui est **nécessaire**
- **Supprimer** le reste de **manière sécurisée**

À RETENIR

- **Identifier** les fichiers sensibles
- **Chiffrer** et s**auvegarder régulièrement**
- **Supprimer définitivement** ce qui n'est plus utile
- Moins **vous stockez**, moins vous prenez de risques

MINI-GLOSSAIRE

- **Chiffrement**
  Rendre un fichier illisible sans mot de passe
- **Sauvegarde**
  Copie sécurisée d'un fichier pour le récupérer en cas de perte
- **Suppression sécurisée**
  Destruction complète d'un fichier pour qu'il ne soit plus récupérable

CHECKLIST PRATIQUE

- [ ] J'ai identifié mes fichiers sensibles
- [ ] Mes fichiers sensibles sont chiffrés ou protégés
- [ ] J'ai au moins une sauvegarde sécurisée et récente
- [ ] Je sais supprimer définitivement les fichiers et appareils inutiles

Vous avez maintenant toutes **les clés pour protéger vos mots de passe, vos communications, vos appareils et vos fichiers.** En suivant ces conseils simples, vous pouvez naviguer en ligne et travailler en toute sécurité, tout en protégeant les autres autour de vous. Il reste une dernière partie qui aborde un risque particulier lié à la violence numérique ciblée: la VBGFT. Cette section vous aidera à mieux comprendre ce phénomène et à savoir comment vous protéger ou demander de l'aide si nécessaire.

05



CHAPITRE

VIOLENCE BASÉE SUR LE GENRE FACILITÉE PAR LA TECHNOLOGIE

Introduction

Vous connaissez peut-être déjà les violences basées sur le genre (VBG) : harcèlement, intimidation ou agressions dirigées contre une personne en raison de son genre.

Avec le développement d'Internet, des téléphones mobiles et des réseaux sociaux, ces violences peuvent désormais se produire aussi en ligne. Lorsqu'elles utilisent des outils numériques pour nuire à une personne, **on parle de Violence Basée sur le Genre Facilitée par la Technologie (VBGFT).**

Définition simple :
La VBGFT est une violence basée sur le genre qui se manifeste à travers la technologie. Elle peut prendre la forme de messages menaçants, de chantage, de diffusion d'images privées ou encore de contenus manipulés (comme des vidéos truquées appelées deepfakes) utilisés pour intimider ou discréditer quelqu'un.)

Qui peut être touché·e ?

La VBGFT peut toucher tout le monde, mais certaines personnes sont plus exposées :

- Les **personnes très actives sur les réseaux sociaux** ou qui publient leur travail en ligne
- Les **jeunes femmes** et **filles**
- Les **personnes visibles dans la vie publique** : militantes, journalistes ou femmes politiques

Exemple concret : une militante partageant ses activités sur Facebook peut recevoir des messages menaçants ou voir ses informations personnelles diffusées sans son accord.

La VBGFT peut concerner toute personne utilisant un téléphone, Internet ou les réseaux sociaux. Cependant, certaines personnes peuvent être plus exposées en raison de leur visibilité ou de leur engagement public. Il peut s'agir notamment :

- Des **personnes très actives en ligne** ou qui publient régulièrement leur travail
- Des **jeunes femmes** et des **filles**
- Des **personnes** engagées dans la **vie publique** : militantes, journalistes, responsables associatifs ou femmes en politique

La visibilité, la prise de position publique ou la défense de causes sensibles peuvent parfois attirer des attaques ciblées en ligne.

D'ailleurs, ***selon un rapport de ONU Femmes, les jeunes femmes et les filles sont parmi les plus exposées à la violence numérique,*** et les femmes défenseurs des droits humains, journalistes et femmes politiques figurent parmi les groupes particulièrement vulnérables en raison de leur visibilité publique.

Exemple concret : Une militante partageant ses activités sur Facebook peut recevoir des messages menaçants ou voir ses informations personnelles diffusées sans son accord.

ONU FEMMES
Entité des Nations Unies pour l'égalité des sexes et l'autonomisation des femmes

Comment reconnaître la VBGFT ?

Voici quelques situations typiques :

- Messages ou commentaires **menaçants ou humiliants**
- Partage de **photos ou vidéos privées sans consentement**
- **Chantage en ligne :** “si tu ne fais pas ceci, je publie tes photos”
- **Vol d’identité numérique** pour vous discréditer
- Publication **d’informations personnelles** : adresse, contacts, lieux fréquentés
- **Deepfakes** ou contenus manipulés pour vous faire dire ou faire des choses que vous n’avez pas faites



ASTUCES

Si une action vous met mal à l’aise ou vous fait peur à cause de votre genre, c’est probablement de la VBGFT.

La VBGFT n’est pas toujours évidente à identifier. Elle peut commencer par des comportements qui semblent “isolés” ou “sans gravité”, mais qui deviennent répétitifs, humiliants ou menaçants.

Voici quelques **situations typiques** :

- **Messages ou commentaires menaçants, humiliants ou à caractère sexiste,** envoyés en privé ou publiquement
- **Partage de photos ou vidéos privées sans consentement**
- **Chantage en ligne :** « si tu ne fais pas ceci, je publie tes photos »
- **Création de faux profils ou usurpation d’identité** pour nuire à votre réputation
- **Publication d’informations personnelles** (adresse, numéro de téléphone, lieux fréquentés)
- **Contenus manipulés (deepfakes)** : images, audios ou vidéos modifiés pour vous faire dire ou faire des choses que vous n’avez jamais faites

Repère simple : Si une action en ligne vous met mal à l'aise, vous intimide, vous fait peur ou cherche à vous humilier en raison de votre genre, il peut s'agir de VBGFT.

Conséquences possibles

Même si la violence est en ligne, elle peut avoir des effets réels :

- Peur, stress, isolement et même des envies de suicide
- Difficulté à travailler ou à poursuivre ses activités
- Perte de confiance en soi

Important : rien ne justifie ces actions envers une personne.

Comment se protéger facilement ?

- **Paramétrez la confidentialité** de vos comptes et publications
- **Ne partagez pas d'informations sensibles** (photos privées, adresse…)
- **Bloquez et signalez** les harceleurs
- **Conservez des preuves** (captures d'écran, messages…)
- **Demandez de l'aide** à une organisation de confiance, comme **Ubunteam**

Il n'est pas possible d'éliminer tous les risques en ligne, mais certains gestes simples permettent de réduire fortement l'exposition et de réagir plus sereinement en cas de problème.

01 Paramétrez la confidentialité de vos comptes

Vérifiez qui peut voir vos publications, vos photos et vos informations personnelles. Limitez l'accès à vos contenus aux personnes de confiance lorsque c'est possible.

02 Partagez avec prudence

Évitez de publier des informations sensibles comme votre adresse, votre numéro de téléphone, vos déplacements en temps réel ou des documents internes.

03 Bloquez et signalez

Si quelqu'un vous harcèle ou vous intimide :

- utilisez la fonction **bloquer** ;
- utilisez la fonction **signaler** sur la plateforme concernée.

Cela permet de limiter les interactions et d'alerter le service concerné.

04 Conservez des preuves

Si vous recevez des messages menaçants ou si du contenu est diffusé sans votre consentement :

- faites des captures d'écran ;
- conservez les messages ou les liens ;
- notez les dates et heures si possible.

Ces éléments peuvent être utiles si vous décidez de demander de l'aide.

05 Ne restez pas seul·e

- **Parlez-en à une personne de confiance** ou **contactez une organisation d'appui** comme Ubunteam.
- **Demander conseil** peut vous aider à comprendre vos options et à **agir avec plus de sérénité.**

CHECKLIST PRATIQUE

- [ ] Mes comptes en ligne ont des paramètres de confidentialité renforcés.
- [ ] Je ne partage pas d'informations personnelles sensibles.
- [ ] Je sais bloquer et signaler une personne qui me harcèle ou m'intimide.
- [ ] Je conserve des preuves (captures d'écran, messages, liens) si nécessaire.
- [ ] Je sais à qui demander de l'aide en cas de besoin (ex: Ubunteam).
- [ ] Je comprends que publier, travailler en ligne ou prendre la parole ne justifie jamais qu'on m'attaque ou m'humilie.

Vous savez maintenant **mieux reconnaître la VBGFT et quelles actions simples peuvent vous aider à vous protéger.** Comme pour les autres aspects de la sécurité numérique, quelques bons réflexes peuvent faire une grande différence. Passons maintenant à la conclusion de ce guide.

Fin du guide – Vous êtes mieux protégé·e !

Vous avez maintenant toutes les clés pour protéger vos mots de passe, vos communications, vos appareils, vos fichiers… et aussi pour faire face à la VBGFT.

Chaque geste que vous mettez en place, aussi petit soit-il, réduit les risques et renforce votre sécurité numérique. Vous n'êtes pas seul·e : Ubunteam est là pour vous soutenir, répondre à vos questions et vous accompagner si besoin.

Passez à l'action à votre rythme, partagez vos bonnes pratiques autour de vous et continuez à apprendre. La sécurité numérique, c'est un voyage : chaque étape compte, et vous êtes sur la bonne voie !

Ressources et contact – Ubunteam

Vous avez suivi le guide et êtes maintenant mieux protégé·e. Pour aller plus loin, Ubunteam reste à vos côtés pour vous accompagner.

Vous pouvez nous contacter pour :

- **Demander un training gratuit** pour vous ou votre organisation
- **Obtenir de l'aide** sur les astuces et recommandations du guide

Comment nous joindre :

Email : arden@ubunteam.org

Téléphone : +225 0797870787

Guide rédigé par

UBUNTEAM

"Join us, Learn… Get Free"

Dans le cadre du projet ARDEN



Avec le soutien de



Digital Defenders Partnership



Crédits et attribution

Ce guide a été conçu par Ubunteam dans le cadre du **projet ARDEN (Appui à la Résilience Digitale des Engagés)**.

Il s'inspire de contenus sélectionnés issus de ***Security in a Box***, développé par **Tactical Tech** et **Front Line Defenders**. Ces contenus ont été sélectionnés, adaptés et réorganisés afin de proposer un guide pratique et accessible, répondant aux réalités et aux besoins des publics francophones.

Le présent guide est publié sous la même licence que les contenus originaux de *Security in a Box*. Les références à des logiciels, services ou marques tiers sont fournies à des fins exclusivement pédagogiques et ne constituent pas une recommandation ou un partenariat.

Remerciements

L'adaptation, la production et la diffusion gratuite de ce guide, en versions imprimée et numérique, ont été rendues possibles grâce au soutien du **Digital Defenders Partnership** (DDP).

Ubunteam adresse ses sincères remerciements à D**igital Defenders Partnership**, ainsi qu'à **Tactical Tech** et **Front Line Defenders**, dont l'engagement en faveur de ressources ouvertes et accessibles en matière de sécurité numérique contribue à renforcer la résilience des communautés et à rendre possibles des initiatives comme ARDEN.

Ce guide est distribué gratuitement et peut être librement partagé conformément aux conditions de la licence applicable.