

PROJET « DROITS DIGITAUX POUR TOUTES ET TOUS » — COTONOU, BÉNIN

GUIDE PRATIQUE DE SÉCURITÉ EN LIGNE

**Bien utiliser Internet et les
réseaux sociaux, sans danger**



NAFASI
magamba★

**DEFEND
DEFENDERS**



Ce guide est l'adaptation pour le Bénin du guide conçu par JAIE à Lomé, dans le cadre du projet « Droits Digitaux pour Toutes et Tous ». Il s'adresse aux jeunes et aux femmes qui utilisent Internet, WhatsApp, Facebook ou TikTok au quotidien, et donne des conseils simples pour se protéger des arnaques, du harcèlement en ligne et de la perte de ses données personnelles.

Il peut être lu seul, utilisé pendant des ateliers de formation, ou partagé avec sa famille et ses proches. Les sections clés se terminent par un encadré « Que faire ? » à retenir.

1. Choisir et protéger ses mots de passe

Le mot de passe est la première porte qui protège vos comptes (WhatsApp, Facebook, e-mail, MTN MoMo, Moov Money, Celtiis Cash). S'il est faible ou partagé, n'importe qui peut y accéder.

- Utilisez un mot de passe d'au moins 8 caractères, avec des lettres, des chiffres et un symbole.
- N'utilisez jamais votre date de naissance, votre nom, votre numéro de téléphone ou « 123456 ».
- Utilisez un mot de passe différent pour chaque compte important.
- Activez la vérification en deux étapes quand elle est proposée. Sur WhatsApp, créez un code secret à 6 chiffres (« Vérification en deux étapes ») pour empêcher quelqu'un de prendre le contrôle de votre numéro.
- Ne partagez jamais votre mot de passe ou le code reçu par SMS, même avec un proche ou une personne qui se présente comme un agent officiel (opérateur, banque, police).

Que faire si mon compte est piraté ?

- Changez immédiatement le mot de passe depuis un autre appareil si possible.
- Utilisez la fonction « compte piraté » du réseau social concerné.
- Prévenez vos proches que votre compte a été piraté, pour qu'ils ne répondent pas à des messages suspects (demandes d'argent, par exemple) envoyés en votre nom.

2. Protéger sa vie privée sur les réseaux sociaux

Ce que vous publiez peut être vu, copié et partagé par des personnes que vous ne connaissez pas, même après avoir été supprimé.

- Réglez vos comptes en mode « privé » et vérifiez régulièrement qui peut voir vos publications.
- Réfléchissez avant de publier une photo, une localisation ou une information personnelle (adresse, emploi du temps).
- N'acceptez pas les demandes d'amis ou de contacts de personnes inconnues.
- Vérifiez les paramètres de confidentialité des applications que vous installez.

3. Reconnaître les arnaques en ligne

Au Bénin, de fausses annonces (faux concours ou tirages au sort, fausses offres d'emploi ou de bourses, faux investissements à « rendement garanti ») circulent régulièrement sur WhatsApp, Facebook et TikTok pour voler de l'argent ou des informations personnelles.

- Méfiez-vous des messages qui promettent un gain d'argent facile, un emploi trop bien payé, un investissement qui « double » votre argent ou un cadeau surprise.
- Aucune administration, banque, opérateur (MTN, Moov, Celtis) ou entreprise sérieuse ne vous demandera votre code PIN, votre mot de passe, un code de confirmation ou une pièce d'identité par simple message ou appel.
- Si quelqu'un affirme vous avoir envoyé de l'argent « par erreur » et vous demande de le rembourser, vérifiez d'abord votre solde réel avec le menu officiel de votre opérateur avant de renvoyer quoi que ce soit.
- Vérifiez toujours l'information sur le site officiel de l'organisme concerné avant d'y croire ou de payer des « frais de dossier ».
- Ne cliquez pas sur des liens envoyés par des inconnus, même s'ils semblent urgents ou officiels.
- Si un message vous met la pression pour agir « immédiatement », c'est souvent le signe d'une arnaque.

Que faire face à une arnaque ?

- Ne répondez pas, ne payez pas, ne partagez pas le message.
- Signalez le message au bjCSIRT (csirt.bj), rubrique « Déclarer un incident ».
- Pour porter plainte, contactez l'Office Central de Répression de la Cybercriminalité (OCRC) : ocrc@dgpr.bj ou +229 65 48 78 74 / 63 09 51 62.
- Si vous avez déjà payé ou transmis des informations, appelez la Police républicaine (117) et prévenez immédiatement votre opérateur Mobile Money.

4. Faire face au cyberharcèlement

Le cyberharcèlement, ce sont des messages, moqueries, menaces ou insultes répétés en ligne. Il touche particulièrement les jeunes filles et les femmes. Ce n'est jamais la faute de la victime.

- Gardez des preuves : faites des captures d'écran des messages avant de bloquer la personne.
- Bloquez et signalez la personne ou le compte sur l'application concernée.
- Parlez-en à une personne de confiance (parent, enseignant, association locale) plutôt que de rester seul(e) face à la situation.
- Ne répondez pas aux provocations : cela n'arrête généralement pas le harceleur.

Que faire en cas de harcèlement ou de menace grave ?

- Conservez les preuves (captures d'écran, dates, noms de comptes).
- Signalez le compte à la plateforme et bloquez-le.
- En cas de menace, de chantage ou de diffusion d'images intimes, contactez la Police républicaine (117) ou l'OCRC : le Code du numérique béninois sanctionne ces actes.
- Si la victime est mineure, la Brigade des mineurs peut aussi être jointe au 160.

5. Protéger ses données personnelles et ses photos

- Ne partagez pas de photos ou vidéos intimes, même avec une personne de confiance : elles peuvent être diffusées sans votre accord.
- Faites attention aux photos de vos documents (carte d'identité, NPI, reçus Mobile Money) : ne les envoyez que si c'est vraiment nécessaire et à une source vérifiée.
- Faites régulièrement une sauvegarde de vos contacts et photos importantes.
- Supprimez les applications que vous n'utilisez plus.
- Si une entreprise ou un service utilise vos données personnelles de façon abusive, vous pouvez saisir l'Autorité de Protection des Données Personnelles (APDP), numéro court 150.

6. Sécuriser son téléphone

- Verrouillez votre téléphone avec un code ou une empreinte digitale, et ne le laissez pas à d'autres déverrouillé.
- Mettez à jour régulièrement votre téléphone et vos applications : les mises à jour corrigent des failles de sécurité.
- Évitez de vous connecter à des réseaux Wifi publics inconnus pour faire des opérations sensibles (Mobile Money, réseaux sociaux).
- N'installez des applications que depuis les magasins officiels (Google Play, App Store).

7. Les 10 réflexes à retenir

- 1 Je choisis un mot de passe fort et différent pour chaque compte.
- 2 J'active la vérification en deux étapes quand c'est possible.
- 3 Je ne partage jamais mon mot de passe ni les codes reçus par SMS.
- 4 Je réfléchis avant de publier une photo ou une information personnelle.
- 5 Je me méfie des messages qui promettent de l'argent facile ou un cadeau.
- 6 Je vérifie toujours l'information sur une source officielle avant d'y croire.
- 7 Je ne clique pas sur les liens envoyés par des inconnus.
- 8 En cas de harcèlement, je garde des preuves, je bloque et je signale.
- 9 J'en parle à une personne de confiance si je me sens en danger.
- 10 En cas d'urgence, j'appelle la Police républicaine au 117 ou je signale au bjCSIRT (csirt.bj).

8. Besoin d'aide ? Qui contacter

Situation	Qui contacter	Comment faire
Arnaque, piratage ou incident de cybersécurité	bjCSIRT — équipe nationale de réponse aux incidents de sécurité informatique	Site csirt.bj, rubrique « Déclarer un incident »
Plainte pour cybercriminalité (arnaque en ligne, chantage, usurpation d'identité)	CNIN (centre national d'investigation numérique)	+229 21 36 87 20 (ou le 151 comme numéro court d'assistance) Site web : cnin.bj
Urgence, menace, vol, agression, harcèlement grave	Police républicaine	Appel gratuit au 117 (24h/24)
Enfant ou mineur en danger	Brigade des mineurs	Numéro court 160
Contenu qui vous vise (harcèlement, photo diffusée sans accord, faux compte)	La plateforme concernée (Facebook, WhatsApp, TikTok...)	Utilisez le bouton « Signaler » ou « Report » sur la publication ou le profil
Fraude sur votre compte Mobile Money	Votre opérateur (MTN MoMo, Moov Money, Celtis Cash)	Service client officiel de l'opérateur, dès que possible
Utilisation abusive de vos données personnelles	APDP — Autorité de Protection des Données Personnelles	Numéro court 150



Sources : Police républicaine du Bénin
(numéros 116/117) ; ARCEP Bénin
(liste des numéros courts) ; CNIN ;
Contacts CNIN : +229 21 36 87 20 (ou
le 151 comme numéro court
d'assistance) Site web : cnin.bj

Adaptation pour le Bénin du guide
élaboré par JAIE dans le cadre du
projet « Droits Digitaux pour Toutes et
Tous », Lomé, 2026.

