



OJCS

Organisation des Jeunes pour un Cyberspace Sécurisé

GUIDE PRATIQUE · ÉDITION VACANCES

10 réflexes pour vous protéger en ligne

Un réflexe par page. À lire, à partager et à garder près de soi, pour profiter des vacances l'esprit tranquille.

 Phishing

 Pages Facebook

 Mots de passe

 WhatsApp

 Signalement

« Pour un cyberspace sûr et responsable »

ojcs-cybersafe.org

Guide de sensibilisation gratuit · Reproduction autorisée pour un usage non commercial · © OJCS



Sommaire

Dix gestes simples qui protègent vos comptes, votre argent et vos proches.

1		Reconnaître un e-mail ou SMS de phishing	HAMEÇONNAGE
2		Vérifier une page Facebook avant d'y croire	RÉSEAUX
3		Sécuriser ses mots de passe	COMPTES
4		Activer la double authentification (2FA)	COMPTES
5		Protéger son compte WhatsApp	MESSAGERIE
6		Déjouer les offres de vacances trop belles	ACHATS
7		Sécuriser ses paiements Mobile Money & en ligne	PAIEMENT
8		Vérifier un lien avant de cliquer	NAVIGATION
9		Se protéger sur le Wi-Fi public	MOBILITÉ
10		Signaler un incident et réagir vite	RÉACTION

Pourquoi ce guide ?

Pendant les vacances, on est plus détendu, plus pressé, plus connecté... et certaines personnes malveillantes en profitent. Fausses promos, faux billets, comptes compromis : ces pièges reposent presque toujours sur l'**urgence** et la **confiance**. Ce recueil vous apprend à les reconnaître et à adopter le bon réflexe, à chaque fois.

1

Reconnaître un e-mail ou SMS de phishing



— Pourquoi c'est important ?

Le phishing (hameçonnage) est le piège le plus répandu. Un faux message imite votre banque, votre opérateur ou un service de livraison pour obtenir vos codes ou votre argent. Pendant les vacances, ces messages se multiplient et jouent sur l'urgence : « votre colis est bloqué », « votre compte va être fermé ».

— Comment faire ?

- 1 **Ne cliquez jamais dans l'urgence** : aucune structure sérieuse ne réclame vos codes par message.
- 2 **Vérifiez l'expéditeur** : une adresse ou un numéro inconnu doit vous alerter.
- 3 **Repérez les fautes** d'orthographe et les formules alarmistes.
- 4 **Saisissez vos identifiants** uniquement en tapant vous-même l'adresse officielle du site.
- 5 **Ne communiquez jamais** mot de passe, code PIN ou code reçu par SMS.

À RETENIR



En cas de doute, ne cliquez pas : vérifiez toujours par le canal officiel.

2

Vérifier une page Facebook avant d'y croire



— Pourquoi c'est important ?

De fausses pages copient le nom et le logo de vraies marques. Elles annoncent des produits ou des séjours à moitié prix, encaissent des acomptes... puis disparaissent. Une belle page ne garantit ni l'honnêteté, ni même l'existence du vendeur.

— Comment faire ?

- 1 **Ouvrez « À propos » et « Transparence de la page »** : regardez la date de création et le pays des administrateurs.
- 2 **Méfiez-vous d'une page récente** qui promet d'énormes promotions.
- 3 **Lisez les commentaires** et cherchez le nom de la page suivi de « avis » pour repérer d'éventuels signalements.
- 4 **Faites « Rechercher l'image »** sur la photo du produit : si elle est partout, elle est volée.
- 5 **Ne payez jamais d'avance** vers un compte personnel, sans contrat ni garantie.

À RETENIR



Prix trop bas + paiement d'avance à un particulier = danger probable.

Sécuriser ses mots de passe



— Pourquoi c'est important ?

Un mot de passe court, réutilisé partout ou basé sur votre vie privée (prénom, date de naissance) se devine en quelques secondes. Or un seul compte forcé peut ouvrir l'accès à tous les autres, surtout votre boîte mail.

— Comment faire ?

- 1 **Privilégiez la longueur** : une phrase de passe d'au moins 12 caractères.
- 2 **Un mot de passe unique** pour chaque compte important (mail, banque, réseaux).
- 3 **Créez une phrase facile à retenir** mais difficile à deviner.
- 4 **Utilisez un gestionnaire de mots de passe** pour tout mémoriser en sécurité.
- 5 **Protégez en priorité votre boîte mail**, la clé de tous vos comptes.

À RETENIR



Un compte = un mot de passe long et unique. Jamais le même partout.

4

Activer la double authentification (2FA)



— Pourquoi c'est important ?

Même un bon mot de passe peut fuiter lors d'une fuite de données. La double authentification ajoute une seconde barrière : un code temporaire demandé en plus du mot de passe. Sans ce code, la personne malveillante reste bloquée à la porte.

— Comment faire ?

- 1 **Activez la validation en deux étapes** dans les réglages « Sécurité » de vos comptes.
- 2 **Préférez une application d'authentification** (codes qui changent) au simple SMS.
- 3 **Notez vos codes de secours** et gardez-les dans un endroit sûr, hors ligne.
- 4 **Commencez par le plus sensible** : mail, banque, Mobile Money, réseaux.
- 5 **Ne communiquez jamais le code reçu**, même à un « service » qui le réclame.



À RETENIR

La 2FA vous protège même si votre mot de passe est volé.

Protéger son compte WhatsApp



— Pourquoi c'est important ?

En vous soutirant votre code à 6 chiffres, une personne malveillante peut prendre le contrôle de votre compte. Elle écrit ensuite à tous vos contacts en votre nom pour leur réclamer de l'argent. Le piège se propage très vite, de proche en proche.

— Comment faire ?

- 1 **Ne partagez JAMAIS le code de vérification** reçu par SMS, même avec un proche.
- 2 **Activez la vérification en deux étapes** : Réglages → Compte → créez un code PIN.
- 3 **Vérifiez toute demande d'argent** par un appel vocal : une voix, pas un simple message.
- 4 **Contrôlez les « Appareils connectés »** et déconnectez ce que vous ne reconnaissez pas.
- 5 **Méfiez-vous des liens** « cadeau » ou « gagnez un lot ».



À RETENIR

Votre code à 6 chiffres ne se partage JAMAIS, avec personne.

6

Déjouer les offres de vacances trop belles



— Pourquoi c'est important ?

Billets d'avion bradés, locations de rêve à moitié prix, séjours « dernière minute » : les offres attirantes se multiplient pendant les vacances. Beaucoup sont de fausses annonces conçues pour encaisser un acompte avant votre départ, pour un logement ou un billet qui n'existe pas.

— Comment faire ?

- 1 **Comparez les prix** : une offre très en dessous du marché doit vous alerter.
- 2 **Achetez sur des plateformes reconnues** et gardez une trace écrite de la transaction.
- 3 **Résistez à la pression** (« dernière place », « offre qui expire dans 10 min »).
- 4 **Vérifiez l'existence réelle** du vendeur ou de l'hébergement (adresse, téléphone, avis).
- 5 **Refusez tout virement direct** vers un compte personnel.



À RETENIR

Si c'est trop beau pour être vrai, c'est probablement faux.

7

Sécuriser ses paiements Mobile Money & en ligne



— Pourquoi c'est important ?

Les pièges au « faux transfert » et au faux agent visent à vider votre portefeuille Mobile Money. Un simple SMS peut être imité pour vous faire « rembourser » un argent que vous n'avez jamais reçu, ou pour vous soutirer votre code PIN.

— Comment faire ?

- 1 **Ne communiquez jamais votre code PIN** : aucun agent ni service ne le demande.
- 2 **Vérifiez le nom du bénéficiaire** affiché avant de valider un transfert.
- 3 **Contrôlez votre solde réel** avant de « rembourser » un dépôt douteux.
- 4 **Payez en ligne** uniquement sur des sites sûrs et identifiés (https).
- 5 **Appelez le service client officiel** au moindre doute.

À RETENIR



Votre code PIN est secret. Un SMS ne remplace jamais la vérification de votre solde.

8

Vérifier un lien avant de cliquer



— Pourquoi c'est important ?

Un lien peut afficher un texte rassurant tout en menant vers un faux site. Une seule lettre changée dans l'adresse (par exemple « faceboook.com ») suffit à imiter un site connu et à voler vos identifiants dès que vous vous connectez.

— Comment faire ?

- 1 **Survolez le lien** (ou appui long sur mobile) pour voir la vraie adresse avant d'ouvrir.
- 2 **Lisez le nom de domaine en entier** : une lettre ou un tiret en trop, et c'est un piège.
- 3 **Méfiez-vous des liens raccourcis** venus d'un expéditeur inconnu.
- 4 **Ne vous fiez pas au cadenas « https »** : il chiffre, il ne garantit pas l'honnêteté.
- 5 **En cas de doute**, tapez vous-même l'adresse officielle.

À RETENIR



On ne clique jamais à l'aveugle : on lit d'abord l'adresse complète.

Se protéger sur le Wi-Fi public



— Pourquoi c'est important ?

Les réseaux Wi-Fi ouverts des hôtels, aéroports et cafés peuvent être surveillés. Une personne malveillante peut même créer un faux réseau au nom presque identique pour intercepter tout ce que vous tapez : mots de passe, codes et numéros de carte compris.

— Comment faire ?

- 1 **Évitez les opérations sensibles** (banque, Mobile Money, achats) sur un Wi-Fi public.
- 2 **Vérifiez le nom exact du réseau** auprès de l'établissement.
- 3 **Préférez votre connexion mobile** (4G) pour tout ce qui touche à l'argent.
- 4 **Désactivez la connexion automatique** aux réseaux ouverts.
- 5 **Utilisez le partage de connexion** de votre téléphone plutôt qu'un Wi-Fi inconnu.

À RETENIR



Sur un Wi-Fi public, aucune opération d'argent. Préférez votre 4G.



10

Signaler un incident et réagir vite

— Pourquoi c'est important ?

Par honte ou par peur, beaucoup de personnes se taisent : cela laisse ces pratiques se poursuivre et faire d'autres victimes. Réagir vite permet de limiter les dégâts, de récupérer parfois votre argent et de protéger votre entourage.

— Comment faire ?

- 1 **Changez immédiatement** les mots de passe des comptes concernés.
- 2 **Prévenez votre banque ou opérateur Mobile Money** pour tenter de bloquer la transaction.
- 3 **Conservez les preuves** : captures d'écran, numéros, messages, références.
- 4 **Signalez aux autorités compétentes** de votre pays.
- 5 **Parlez-en autour de vous** pour éviter d'autres victimes.

À RETENIR



Signaler n'est pas une honte : c'est se protéger et protéger les autres.



Restez **vigilant**, même en **vacances**

Vous connaissez désormais les 10 réflexes. Partagez ce guide avec votre famille, vos amis et vos élèves : la meilleure protection, c'est une communauté informée.

Organisation des Jeunes pour un Cyberspace Sécurisé (OJCS)

L'OJCS renforce les capacités des jeunes face aux risques du cyberspace et promeut un usage éthique, conscient et inclusif du numérique, à travers la sensibilisation, la formation et l'accompagnement des publics.

SENSIBILISER • FORMER • PROTÉGER



ojcs.benin@gmail.com



ojcs-cybersafe.org

« Pour un cyberspace sûr et responsable »

© OJCS — Organisation des Jeunes pour un Cyberspace Sécurisé
Guide de sensibilisation gratuit · Reproduction autorisée pour un usage non commercial