BÉNIN RÉVÉLÉ

ANSSI
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
PRÉSIDENCE DE LA RÉPUBLIQUE DU BÉNIN

## RÈGLES D'HYGIÈNE DE BASE POUR UNE

# SÉCURITÉ NUMÉRIQUE

## PERSONNELLE AMÉLIORÉE

Avril 2020 - 1ère Edition

# EDITORIAL

L'utilisation croissante des moyens du numérique dans tous les secteurs d'activités de la vie humaine, nous expose à divers risques. Il est donc vital de revoir nos habitudes quotidiennes en matière d'hygiène numérique, car les conséquences sont souvent désastreuses.

C'est dans cette optique que l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI-Bénin), en vue de sensibiliser les citoyens sur les meilleures pratiques à adopter individuellement, lance ce livre blanc qui se veut être un recueil de bonnes pratiques minimales et surtout faciles à respecter.

Ainsi, espérons-nous contribuer efficacement à la sécurisation du cyberespace béninois par le renforcement des acteurs et de la citoyenneté numérique.

Bonne lecture !

**Ouanilo Jérôme Médégan**

Directeur général de l'Agence Nationale
de la Sécurité des Systèmes d'Information

# TABLE DES MATIÈRES

## ENJEUX DE LA SÉCURITÉ NUMÉRIQUE

La digitalisation des services au Bénin, l'explosion des échanges monétaires électroniques, l'usage sans cesse croissant des services de l'internet fixe et mobile (taux de pénétration de l'internet de 53.03% en 2019 selon l'ARCEP), sont autant de facteurs qui exposent les utilisateurs que nous sommes aux menaces du cyberespace.

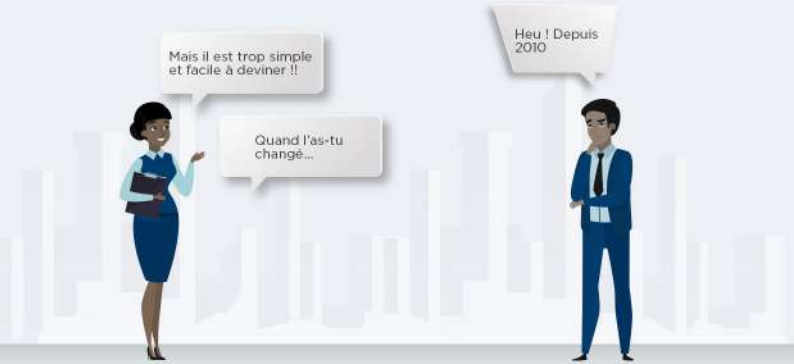
Les vols de données d'entreprises étant des risques classiques de nos jours, nous notons la recrudescence des arnaques ciblant les individus sur les réseaux sociaux ainsi que le phénomène de prolifération de fausses informations connues sous le vocable de "fake news". Ces nouvelles formes d'attaque sont davantage l'œuvre de cybercriminels agissant en bandes organisées. L'impact de ces attaques est parfois néfaste : indisponibilité des services, pertes financières, atteinte à la réputation et à l'image d'un individu ou d'une entreprise, etc. Les utilisateurs peu conscients de ces risques constituent le maillon faible de la chaine. En effet, il suffit souvent de respecter de simples règles d'hygiène en matière de sécurité numérique pour endiguer le phénomène.

Ce livre blanc de bonnes pratiques de sécurité numérique est à destination des usagers des services numériques n'ayant pas forcément un profil technique. Il est une compilation de recommandations qui permettront de réduire l'exposition des usagers des services numériques aux attaques informatiques.

# RECOMMANDATIONS SUR LES MOTS DE PASSE

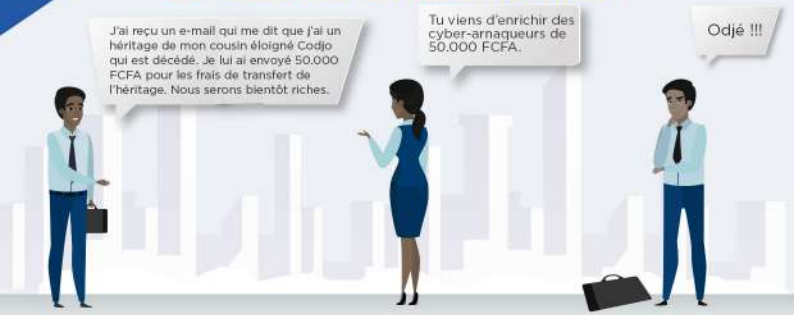

Du téléphone portable au compte bancaire en passant par les réseaux sociaux, le mot de passe est l'indispensable de l'authentification, très souvent associé à un nom d'utilisateur. Étant la première défense contre les attaques cybercriminelles, il fait objet de convoitise. Autrement dit, plus il est fort, plus il sera difficile pour un attaquant de le trouver et mieux votre compte sera en sécurité.

- **Utiliser la double authentification ou authentification à double facteur :** c'est une méthode qui vous impose de fournir deux preuves différentes de votre identité avant d'accéder à vos applications, plateformes et services.
- **Choisir des mots de passe d'au moins douze (12) caractères :** aujourd'hui avoir un mot de passe de huit (08) caractères n'est plus fiable car facilement « cassables ».
- **Un mot de passe doit contenir :** au moins une lettre majuscule, un chiffre et un caractère spécial, le tout contenu dans une phrase.
- **Le mot de passe ne doit rien révéler sur votre profil** ou votre personnalité. Évitez d'utiliser des mots qui existent dans le dictionnaire.
- **Changer régulièrement votre mot de passe soit une fois tous les six mois ou** dès que vous suspectez un vol de données.
- **Éviter d'utiliser le même mot de passe sur toutes les plateformes auxquelles vous avez accès.**




- **Éviter de vous connecter à vos comptes quand vous utilisez un wifi public.**
- **Ne jamais enregistrer vos mots de passe dans le navigateur d'un ordinateur partagé.**
- **Utiliser toujours des sites en HTTPS** (cadenas gris : 🔒) pour saisir vos mots de passe.
- **Toujours vérifier attentivement l'identité (adresse url) d'un site web même si vous avez l'habitude de l'utiliser.**

# RECOMMANDATIONS SUR LA MESSAGERIE ÉLECTRONIQUE




La messagerie électronique est devenue l'un des principaux moyens d'échanges d'informations. C'est aussi l'un des moyens les plus utilisés dans les campagnes d'hameçonnage. Pour preuve, le nombre d'e-mail envoyés par jour dans le monde est de 293 milliards (hors spam) selon « arobase.org : le guide de e-mail ». Malgré les filtres anti-spams, nous en recevons tous un bon nombre.

En cliquant sur des liens dans les e-mails, vous pourriez télécharger des logiciels malveillants compromettant ainsi la sécurité de votre appareil et vous exposant aux arnaques.

## Lorsque que vous recevez un e-mail :

**Vérifier correctement l'adresse électronique de l'expéditeur :** si l'adresse vous semble suspecte et si vous n'attendiez pas un e-mail de cette personne, faites une recherche Google sur le contenu de l'e-mail pour vous assurer qu'il ne s'agit pas d'une campagne de vol d'identifiants.

**Vérifier les informations d'entêtes** et celles relatives à la sécurité. Contrôler si l'e-mail a été chiffré avec le standard TLS dans son entête.

**Se méfier des pièces jointes et les scanner** avec votre antivirus (mis à jour régulièrement) avant de les ouvrir.

**Éviter au maximum de cliquer sur des liens** contenus dans un e-mail.

**Ne remplir aucun formulaire** si vous n'êtes pas absolument certain de la source de la destination des informations saisies et de l'usage qui sera fait de ces dernières.

## Lorsque vous envoyez un e-mail

**Ne pas mettre d'informations sensibles ou confidentielles dans un e-mail qui n'est pas chiffré :** Le chiffrement et la signature d'un e-mail assurent sa sécurité et sa confidentialité.

**Vérifier que vous avez entré le bon destinataire** afin qu'une information sensible ne tombe dans de mauvaises mains.

**Ne pas utiliser vos adresses électroniques professionnelles pour vous enregistrer dans des forums, des sites de marketings, etc.**

**Signer vos e-mails grâce à la norme OpenPGP :** OpenPGP est une norme qui décrit toute technologie permettant le chiffrement cryptographique utilisé pour la signature de données, le chiffrement et le déchiffrement de textes, d'e-mails, de fichiers, de répertoires, de partitions et de disques entiers pour accroître la confidentialité et l'intégrité des données en transit ou repos. Elle est disponible entre autres, grâce à l'implémentation libre et gratuite GnuPG.

**Contacter si possible votre service informatique pour l'utilisation d'une solution implémentant OpenPGP afin de chiffrer le contenu des e-mails confidentiels.**

# RECOMMANDATIONS SUR L'USAGE DES TÉLÉPHONES MOBILES

Les smartphones, tablettes, montres et objets connectés sont devenus des moyens de communication et de connexion indispensables dans la vie quotidienne. Toutefois, ces derniers nous exposent à de multiples risques : vol, fraude, usurpation qui peuvent représenter un risque financier certain.

**Activer une protection antivirus pour mobiles**

Le rôle des smartphones dans la vie quotidienne croît de manière exponentielle. En réaction, les cybercriminels accordent davantage d'attention à la qualité des logiciels malveillants utilisés. Afin de réduire le risque d'infection, l'utilisation de logiciel antivirus pour mobile devient une nécessité. Vous devez faire le téléchargement du logiciel antivirus depuis un store officiel (Google Play store ou Apple store).

Action : Téléchargez depuis Google Play store officiel, un antivirus tel que Avast, Avg, Kaspersky.

**Toujours verrouiller les écrans de vos mobiles**

Le verrouillage systématique de vos écrans vous protègera contre les accès extérieurs non autorisés. Privilégier le verrouillage par empreinte digitale. Les verrouillages par mot de passe et par schéma n'offrent pas assez de complexité et sont faciles à reproduire.

Action : Sur votre téléphone Android, allez dans: Paramètres-->Sécurité--> Verrouillage de l'écran.

**Verrouiller vos applications sensibles avec un mode ou un code de verrouillage différent de celui utilisé pour le verrouillage de votre écran**
L'accès aux applications contenant des données sensibles tels que vos messageries électroniques, applications de chats, stockage de fichiers doit être systématiquement verrouillé avec un schéma ou code différent de celui utilisé pour verrouiller votre écran.

**Chiffrer vos mobiles**
Le chiffrement du mobile se fait dans les paramètres de sécurité du téléphone. Il constitue le premier rempart en cas d'échec des autres mesures de sécurité. Ainsi, tant que le cybercriminel ne possède pas la clé de déchiffrement, les données qu'il aurait recueillies demeureront inutilisables. Il est néanmoins important d'avoir un mot de passe de déchiffrement long et complexe que vous devrez absolument mémoriser. Nous conseillons à ce titre un mot de passe d'au moins douze (12) caractères.
**Attention : perdre son mot de passe rend le téléphone inutilisable.**
Action : Sur votre téléphone Android, allez dans Paramètres-->
Sécurité-->Chiffrer le téléphone.
Cette action doit se faire avec le mobile complètement chargé.

**Télécharger vos applications seulement sur les Store Officiels**
Le principal vecteur d'infections des appareils mobiles est l'installation d'applications venant de sources non sûres. C'est un phénomène en pleine croissance : les applications malveillantes se multiplient directement au sein des app store non officiels. Elles parviennent à récupérer des données sensibles ou des identifiants de connexion. Certaines peuvent également installer automatiquement des logiciels malveillants sur votre appareil grâce auxquels les pirates informatiques peuvent prendre la main sur d'autres fonctionnalités de votre appareil, surveiller vos activités, connaître les sites web que vous visitez ou plus encore ce que vous écrivez.

**Suivre votre téléphone à la trace**
Les téléphones perdus sont aujourd'hui la principale cause de fuites de données. Photos, emails, SMS et applications sont comme des portes ouvertes pour les cybercriminels qui accèdent ainsi aux informations personnelles, aux données relatives à la vie privée et aux finances des individus. Vous pouvez installer sur votre mobile des outils d'antivols qui permettent de bloquer et de localiser ce dernier en cas de perte.

**Bloquer l'installation des programmes de sources inconnues**
dans les paramètres de votre mobile. Par défaut, l'installation d'applications venant de sources inconnues est bloquée. Vous pouvez tout de même vérifier que c'est le cas sur votre appareil.

**Ne pas contourner les restrictions de l'appareil**
au risque de faciliter l'accès à votre mobile aux cybercriminels.

**Installer les mises à jour du système et des applications**
dès qu'elles sont disponibles afin de corriger les vulnérabilités et d'assurer la protection continue de votre appareil.

**Sauvegarder les données de votre mobile**
pour assurer une restauration des données en cas de changement ou de perte de votre appareil.

# CINQ ASTUCES POUR PROTÉGER VOTRE VIE PRIVÉE EN LIGNE

Aujourd'hui plus que jamais, une grande partie de notre vie quotidienne se déroule en ligne, ce qui fait de la protection de la vie privée en ligne un aspect important si celle-ci venait à être compromise. Fournisseurs de services internet, gouvernements, publicitaires, pirates informatiques, nombreux sont les acteurs intéressés par nos données personnelles. Nous fournissons ici quelques outils et astuces qui vont renforcer votre vie privée en ligne.


HTTPS Everywhere est un outil qui tend à forcer votre navigateur à traiter en canal sécurisé (HTTPS) partout où cela est possible, c'est-à-dire qu'il force la navigation chiffrée sur tous les sites qui supportent le HTTPS mais qui ne le proposent pas par défaut.
**Disponible sur : Mozilla Firefox, Mozilla Firefox Android, Google Chrome, Opera.**


Il surveille et vous avertit des sites qui essayent de traquer vos habitudes de navigation.
**Disponible sur : Mozilla Firefox, Mozilla Firefox Android, Google Chrome, Opera.**
**Alternatives : Do Not Track Me , Ghostery, Disconnect Private Browsing.**


Cette application vous protège du pistage en ligne des annonceurs publicitaires. AdBlock Plus bloque des millions de publicités de par le monde. Vous pouvez faire des exceptions pour des sites au besoin. Adblock plus a également son navigateur mobile dédié au blocage des publicités : Adblock Browser (Android) et Adblock Browser (iOS)
**Disponible sur : Mozilla Firefox, Mozilla Firefox Android, Google Chrome, Opera, Safari Mac, Safari iPhone, Samsung Internet Android.**

**Alternatives : uBlock Origin, NoScript (Firefox), ScriptSafe (Chrome).**

**NETCRAFT**

NetCraft est un service disponible depuis 1995 qui sonde le Web à la recherche de sites internet. Son extension dispose d'un système anti-hameçonnage pour être averti lorsque l'on tente de se connecter sur un site frauduleux d'hameçonnage avec un navigateur web.
**Disponible sur : Microsoft Edge, Google Chrome, Mozilla Firefox, Opera.**
**Alternatives : Stop Phishing (Chrome)**

**PASSWORD CHECKER**

Password Checker est une extension qui permet de vérifier que le mot de passe que vous saisissez dans un champ sur un site n'a pas été retrouvé dans des brèches de données des grands sites internet. Rassurez-vous, votre mot de passe n'est envoyé à un quelconque serveur pour vérification. Plutôt, Password Checker envoie les cinq premiers caractères de l'empreinte (hash) de votre mot de passe et reçoit un ensemble d'empreintes comme résultats, qu'il vérifie maintenant avec le vôtre.
**Disponible sur : Google Chrome**