ANSI
LE NUMERIQUE AU SERVICE DU DEVELOPPEMENT

GUIDE DE PROTECTION NUMÉRIQUE

Août 2024

Pour commencer

Votre smartphone ou tablette ne se limitent plus à passer des appels. Ils sont devenus des outils polyvalents pour stocker des données, capturer des photos et vidéos, enregistrer des mémos, passer des commandes en ligne, et même gérer nos finances personnelles.

Cependant, la sécurité mobile est souvent sous-estimée par de nombreux utilisateurs, qui ignorent les dangers potentiels liés à une utilisation imprudente du monde numérique.

Étant donné leur portabilité et leurs multiples fonctions, les smartphones sont particulièrement vulnérables aux cybermenaces telles que les logiciels malveillants, les programmes espions, et les tentatives de phishing. Ces menaces peuvent compromettre à la fois l'appareil lui-même et les informations précieuses qu'il contient.

Les cybercriminels profitent souvent de l'imprudence des utilisateurs avec leurs appareils connectés. Pour vous protéger contre les menaces les plus courantes en matière de sécurité mobile, voici quelques mesures préventives essentielles à adopter.

Maintenez vos appareils et applications à jour

Un système régulièrement mis à jour renforce la sécurité de votre smartphone ou tablette en corrigeant les vulnérabilités qui pourraient être exploitées. Si vous préférez éviter les mises à jour automatiques, surveiller les notifications de mises à jour logicielles et les rappels qui apparaissent sur votre écran, et prenez le temps d'installer ces correctifs manuellement dès que possible.

Désinstallez les applications que vous n'utilisez plus

Les applications anciennes et non utilisées, surtout si elles ne sont plus mises à jour, peuvent présenter des failles de sécurité importantes, compromettant ainsi la sécurité de votre appareil.

Prenez le temps de parcourir vos applications et supprimez celles dont vous n'avez plus besoin. Cette action rendra vos applications préférées plus faciles à trouver, mais contribuera également à renforcer la sécurité de votre appareil.

Sauvegardez régulièrement vos données

Les cartes mémoire pour appareils Android permettent de stocker une grande quantité de contacts, messages, fichiers, vidéos et photos. Toutefois, il est crucial d'effectuer des sauvegardes régulières de vos données pour vous protéger en cas de vol ou de compromission, telle qu'une attaque de ransomware.

Ne répondez pas ou raccrochez immédiatement aux appels téléphoniques suspects

Les fraudeurs et escrocs peuvent également tenter de vous contacter par téléphone. Comme tout cybercriminel, ils chercheront à vous persuader que leur offre est authentique ou que leur appel est légitime. Si l'on vous demande des informations personnelles, des numéros de compte bancaire, des codes PIN, ou des numéros de carte de crédit, raccrochez sans hésiter. Les menaces ou les tentatives d'intimidation sont aussi des signes évidents de fraude.

Protégez-vous contre les attaques de smishing et de phishing

Tout comme le phishing, le smishing (hameçonnage par SMS) vise à inciter les destinataires à cliquer sur un lien malveillant via un message texte. Ces attaques s'appuient sur des tactiques d'ingénierie sociale pour tromper les victimes, les poussant à divulguer des informations personnelles ou à télécharger des logiciels malveillants sur leur appareil.

Soyez prudent face aux SMS non sollicités, en particulier ceux qui prétendent provenir de votre banque et demandent des informations personnelles ou financières.

Lorsque vous consultez vos e-mails, méfiez-vous des messages non sollicités qui tentent de créer un sentiment d'urgence ou de panique. Souvenez-vous que si une offre paraît trop belle pour être vraie, elle l'est probablement.

Supprimez tous les messages inattendus reçus par SMS ou e-mail, et ne répondez pas à l'expéditeur.

Verrouillez votre smartphone avec un code PIN, un mot de passe, ou une empreinte digitale

Assurez-vous de toujours verrouiller votre smartphone avec un code PIN, un mot de passe, ou une empreinte digitale. Cela empêche les personnes non autorisées d'accéder à vos données si votre appareil est perdu ou volé. Optez pour un code PIN ou un mot de passe complexe plutôt que des options simples comme «1234» ou «0000». L'utilisation de la reconnaissance faciale ou de l'empreinte digitale ajoute une couche de sécurité supplémentaire, rendant l'accès encore plus difficile pour les intrus.

Évitez d'utiliser les réseaux Wi-Fi publics non sécurisés

Les réseaux Wi-Fi publics sont rarement sécurisés, ce qui les rend vulnérables aux tentatives de compromission de votre appareil.

Lorsque vous envoyez des informations sensibles via un réseau Wi-Fi public, vous vous exposez à diverses menaces, notamment le vol de données personnelles telles que vos identifiants de connexion et vos informations financières.

De plus, les cybercriminels peuvent créer des réseaux Wi-Fi publics qui imitent ceux légitimes, un procédé connu sous le nom d'attaque de l'homme du milieu (man-in-the-middle attack).

Les utilisateurs se connectant à ces réseaux frauduleux risquent de voir leurs données volées, d'être infectés par des logiciels malveillants, ou de subir des détournements financiers.

Limitez les permissions des applications

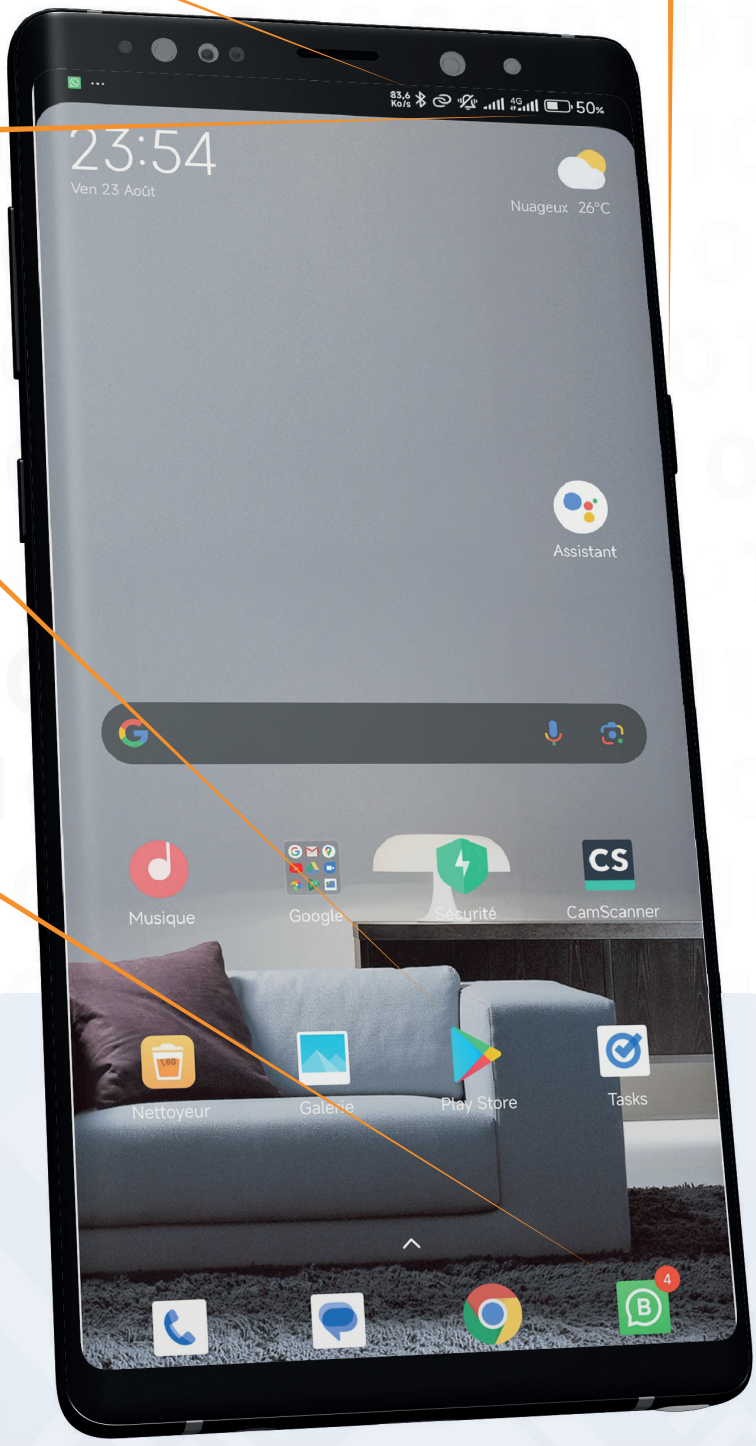
Lorsque vous installez une nouvelle application, prenez le temps de vérifier les permissions qu'elle demande. Certaines applications sollicitent un accès à des données ou des fonctionnalités dont elles n'ont pas réellement besoin, ce qui peut exposer vos informations personnelles à des risques inutiles. Pour protéger votre vie privée, n'accordez que les permissions strictement nécessaires au bon fonctionnement de l'application, et revoyez régulièrement les permissions des applications déjà installées.

Les menaces contre les appareils mobiles se multiplient et deviennent de plus en plus sophistiquées. Les utilisateurs souhaitent exploiter pleinement les fonctionnalités de leurs appareils, mais beaucoup de ces options, bien qu'elles offrent commodité et praticité, compromettent souvent la sécurité. Ce guide de bonnes pratiques propose des mesures concrètes que les utilisateurs peuvent adopter pour mieux protéger leurs appareils et leurs informations personnelles.

Désactivez le Bluetooth® lorsque vous n'en avez pas besoin.

Redémarrez votre appareil une fois par semaine.

Ne laissez pas votre smartphone en charge toute la nuit. Débranchez-le quand il atteint 80-90 % pour prolonger la durée de vie de la batterie.



Installez uniquement les applications dont vous avez vraiment besoin, de sources fiables. Évitez les applications tierces pour réduire les risques de sécurité.

Limitez les informations personnelles que vous partagez sur WhatsApp et activez la vérification en deux étapes pour sécuriser votre compte.

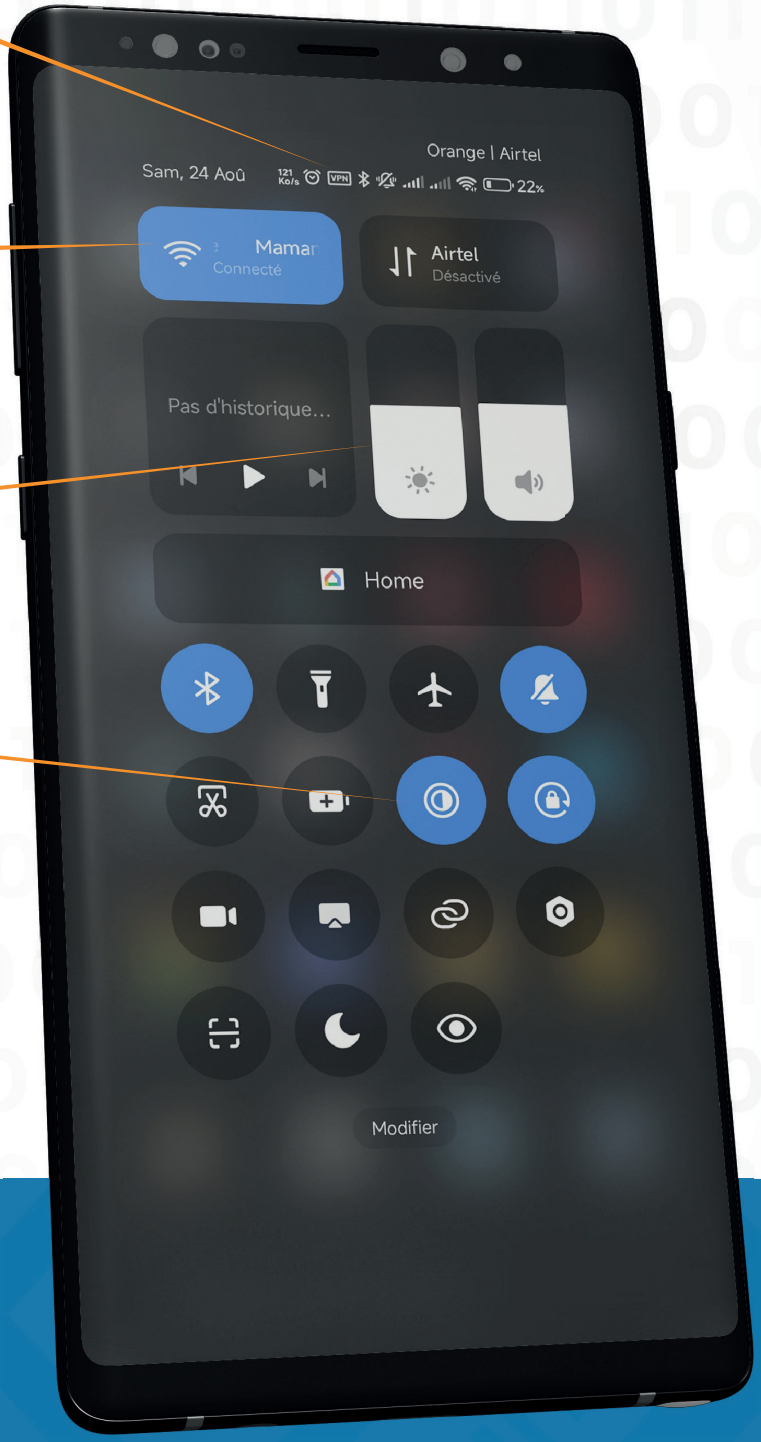
Utilisez un VPN pour sécuriser votre connexion, surtout lorsque vous utilisez des réseaux Wi-Fi publics. Cela protège vos données en chiffrant votre trafic internet.

Évitez de vous connecter aux réseaux Wi-Fi publics. Désactivez le Wi-Fi lorsque vous ne l'utilisez pas, et supprimez les réseaux Wi-Fi inutilisés de votre liste de connexions.

Réduisez la luminosité de l'écran pour préserver la batterie et réduire la fatigue oculaire, surtout dans des environnements peu éclairés.

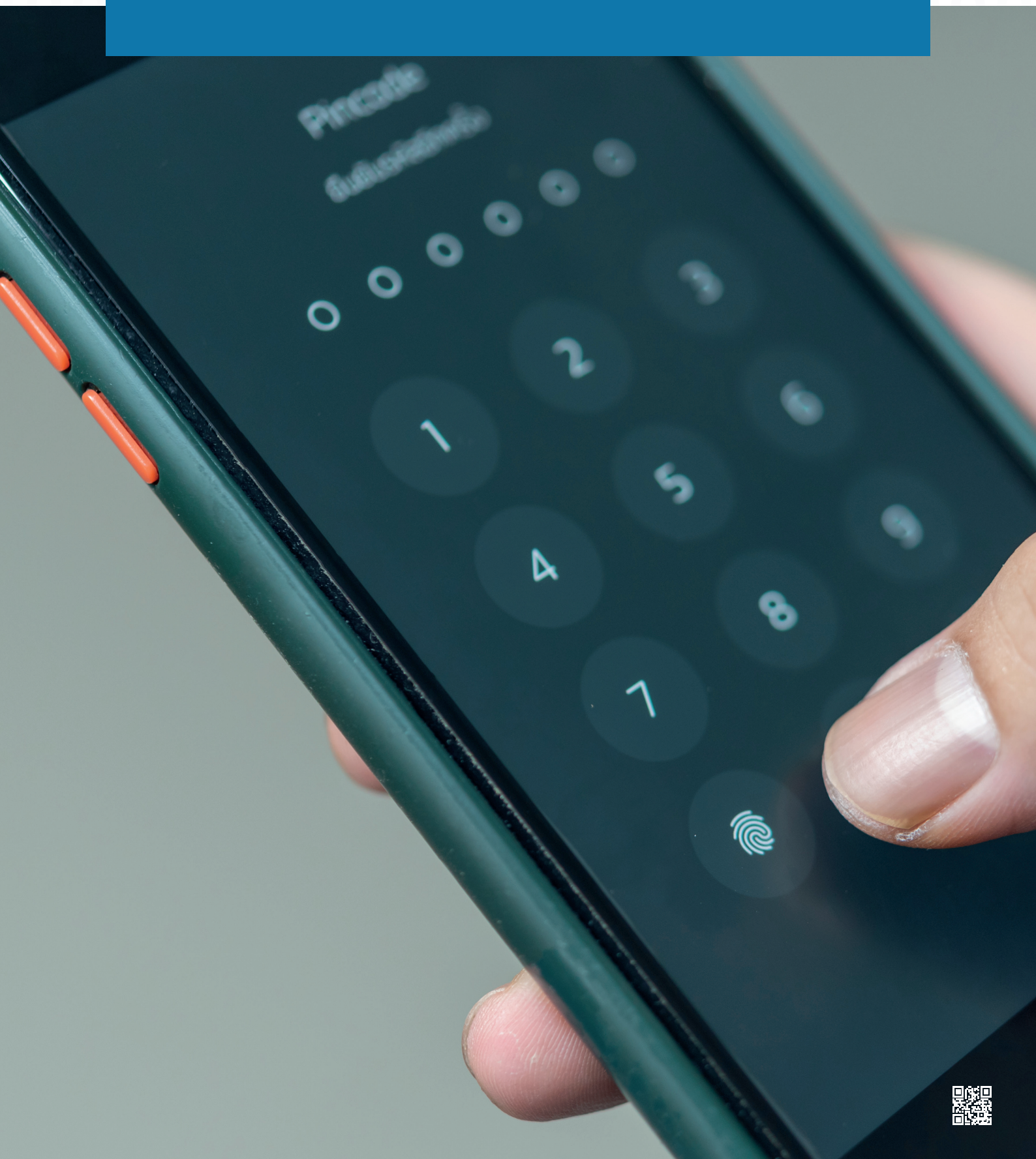
Activez le mode sombre pour réduire la fatigue oculaire et économiser la batterie, surtout sur les écrans OLED.

Évitez d'avoir des conversations sensibles à proximité d'appareils mobiles qui ne sont pas configurés pour gérer les communications vocales de manière sécurisée.



Utilisez des codes PIN/mots de passe d'écran verrouillé forts : un code PIN à 6 chiffres est suffisant si l' appareil se réinitialise après 10 tentatives de mot de passe incorrectes.

Réglez l'appareil pour qu'il se verrouille automatiquement après 5 minutes.



GUIDE DE PROTECTION NUMÉRIQUE

© 2024 Agence Nationale pour la Sociétéde d'Information (ANSI).
Tous droits réservés.

Adresse 11138 Rue de la Sirba
Niamey, Niger
contact@ansi.ne