Guide de bonnes pratiques pour

protéger les smartphones

Version: 1.0 - 06/06/2022

الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique

الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
tunCERT
Tunisian Computer Emergency Response Team

De nos jours, Les appareils intelligents portables sont largement utilisés par l'homme moderne.

Sur le plan fonctionnel, les appareils mobiles, plus précisément les smartphones et tablettes informatiques, peuvent remplacer un ordinateur pour mener de front les exigences du travail, de la vie personnelle et des finances. Cependant, de nombreux utilisateurs oublient les risques de logiciels malveillants sur ces appareils cruciaux. Ils contiennent tout autant et plus d'informations sensibles ou permettent d'y accéder. Ils sont plus faciles à perdre ou à se faire voler.

Il est clair qu'il est nécessaire de mieux protéger ces appareils et de sensibiliser davantage les propriétaires à leurs vulnérabilités.

الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
tunCERT
Tunisian Computer Emergency Response Team

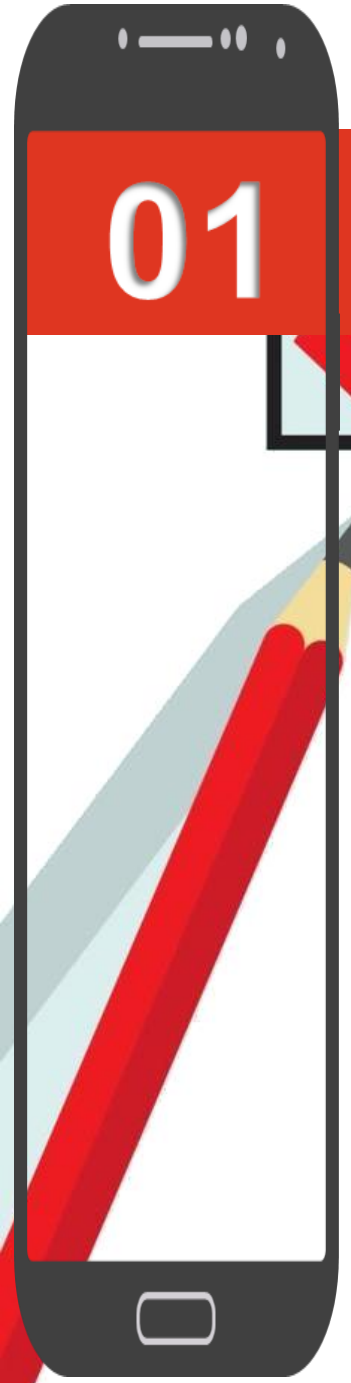
- Comme tout appareil connecté,

les smartphones et tablettes informatiques sont exposées à des risques dont on peut citer :

- Une mauvaise sécurité des mots de passe.
- Applications malveillantes.
- Fuite de données.
- Wifi ouvert.
- Attaques de phishing.
- Spyware.
- Fragmentation Android ou différentes versions du système d'exploitation (OS) Android

Voici les bonnes pratiques à adopter

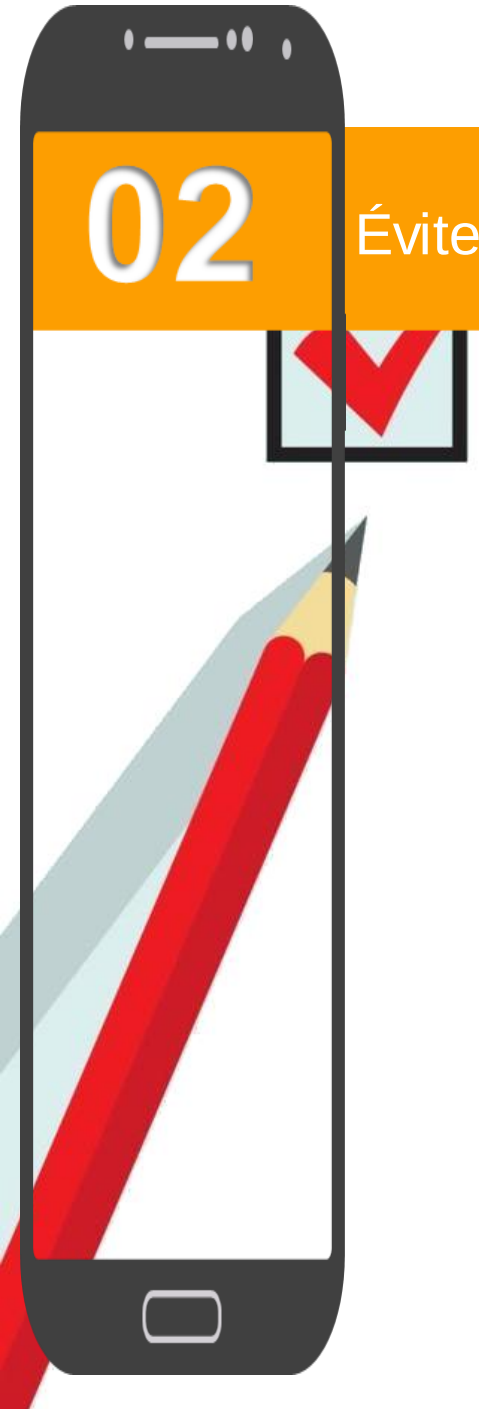
pour la sécurité de vos appareils mobiles



01 Verrouillez votre appareil

- **Définissez un code d'accès que vous êtes le seul à connaître, et tapez-le simplement avant d'utiliser votre téléphone.**
- **Utilisez un code PIN/mot de passe fort pour le verrouillage de l'écran : un code PIN à 6 chiffres est suffisant si l'appareil s'efface après 10 tentatives de mot de passe incorrect.**
- **Réglez l'appareil pour qu'il se verrouille automatiquement après 5 minutes.**
- **Si votre téléphone est équipé d'un lecteur d'empreinte digitale ou un scanner de rétine, vous pouvez les utiliser pour déverrouiller votre appareil ou certaines applications.**

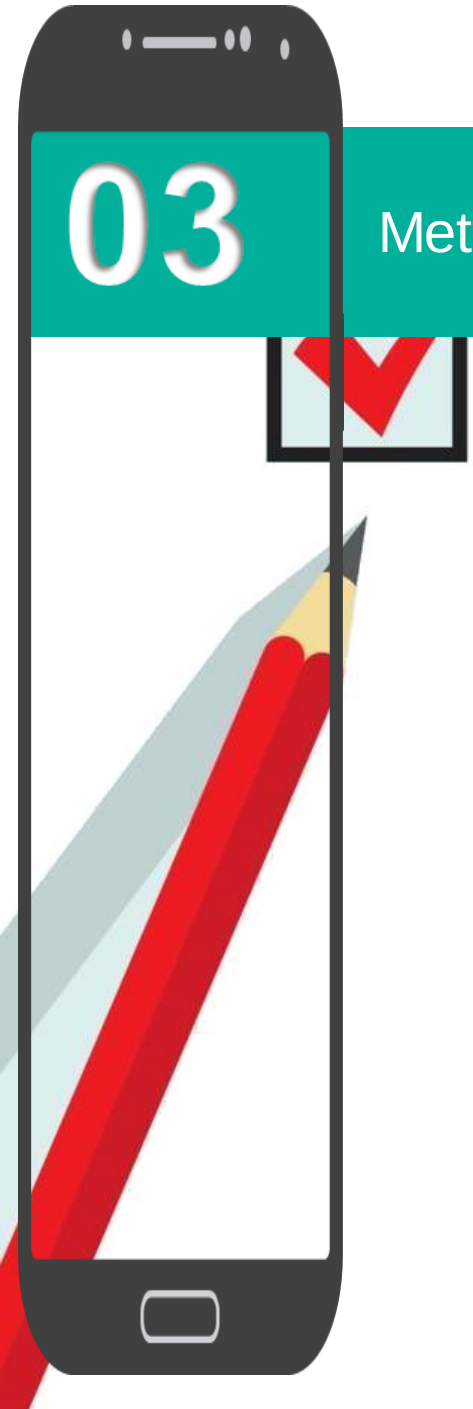
الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
tunCERT
Tunisian Computer Emergency Response Team



02 Évitez les liens suspects et évitez de donner des informations personnelles

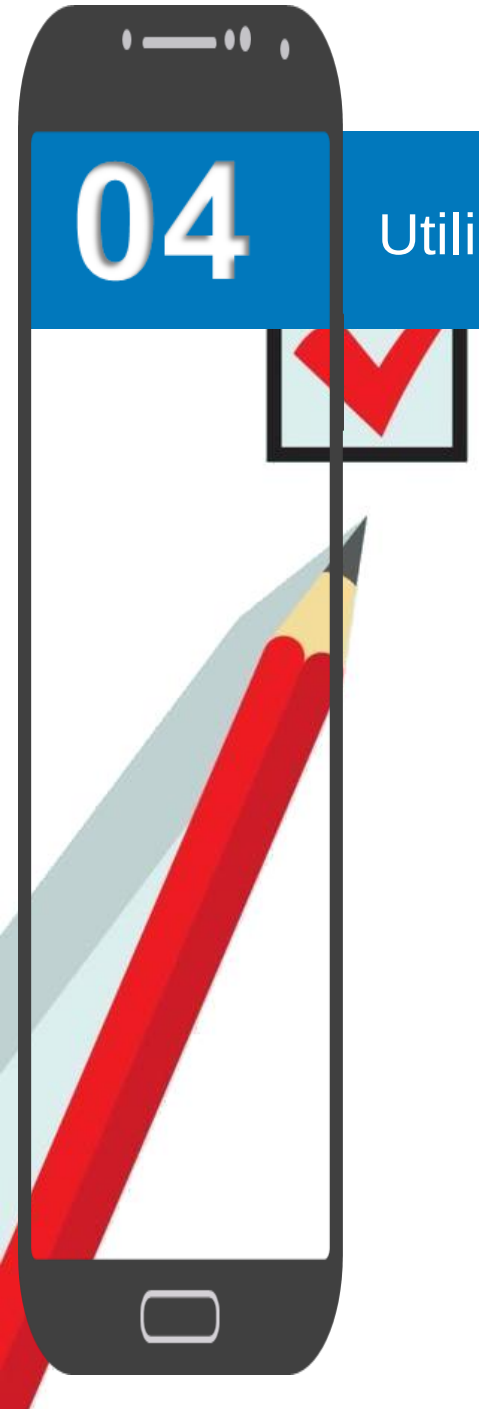
- **Si vous ne connaissez pas l'expéditeur, ne pensez même pas à cliquer sur le lien.**

- **Si vous connaissez l'expéditeur, assurez-vous qu'il a bien envoyé le lien avant de cliquer. Les faux comptes de courriel, de texte et de message se faisant passer pour une personne ou une entité que vous connaissez sont une astuce courante des cybercriminels, connue sous le nom de hameçonnage.**



03 Mettez vos logiciels à jour immédiatement

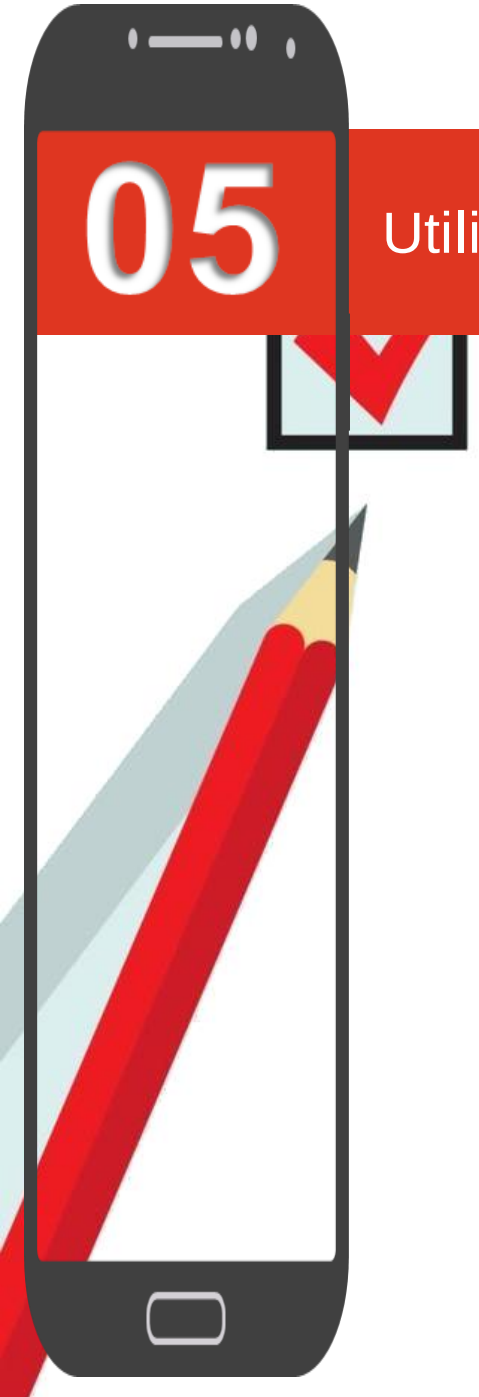
- **Dès qu'une mise à jour est publiée pour votre appareil, téléchargez-la et installez-la immédiatement.**
- **Ces mises à jour comprennent souvent des corrections de sécurité, des correctifs de vulnérabilité et d'autres opérations de maintenance nécessaires.**
- **Pour se faire, vous pouvez se référer aux guides suivants:**
  - Vérifier la version d'Android installée et la mettre à jour
  - Mise à jour de votre iPhone, iPad ou iPod touch



04 Utilisez des mots de passe uniques pour chaque compte en ligne

- **Évitez de réutiliser les mots de passe.**
- **Lorsque les cybercriminels mettent la main sur le mot de passe d'un utilisateur, ils essaient ce mot de passe pour tous les comptes de l'utilisateur.**
- **La meilleure pratique consiste à utiliser un gestionnaire de mots de passe pour créer des mots de passe uniques et difficiles à pirater.**

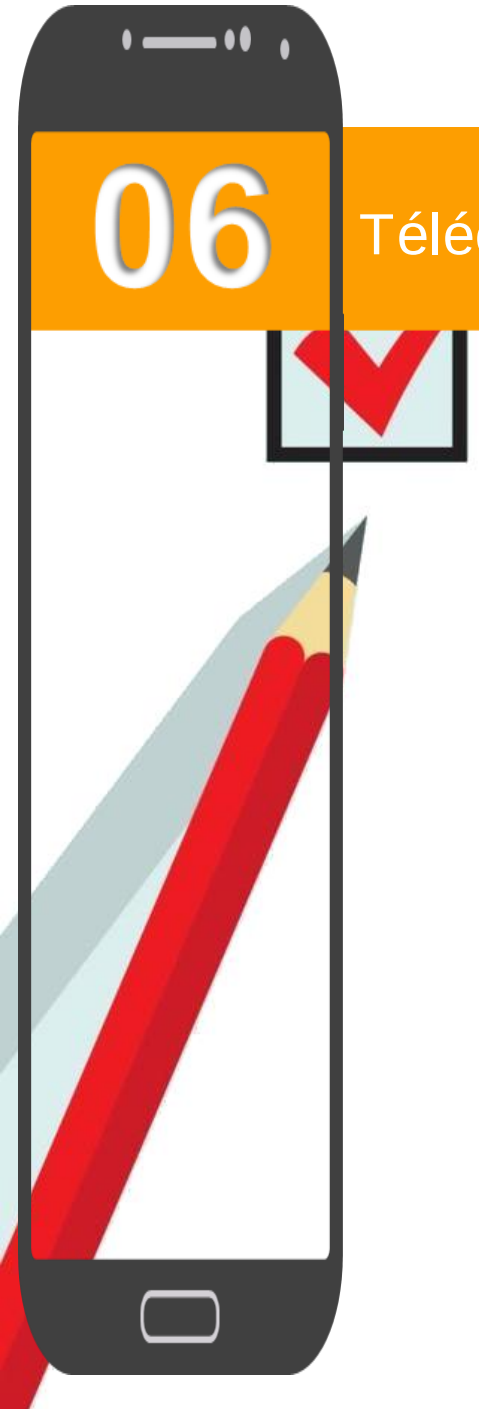
الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
tunCERT
Tunisian Computer Emergency Response Team



05 Utilisez un VPN sur les réseaux Wi-Fi ouverts

- **Il est difficile d'éviter d'utiliser le Wi-Fi ouvert - vous êtes occupé, vous êtes en déplacement et vous devez effectuer des transactions en ligne.**

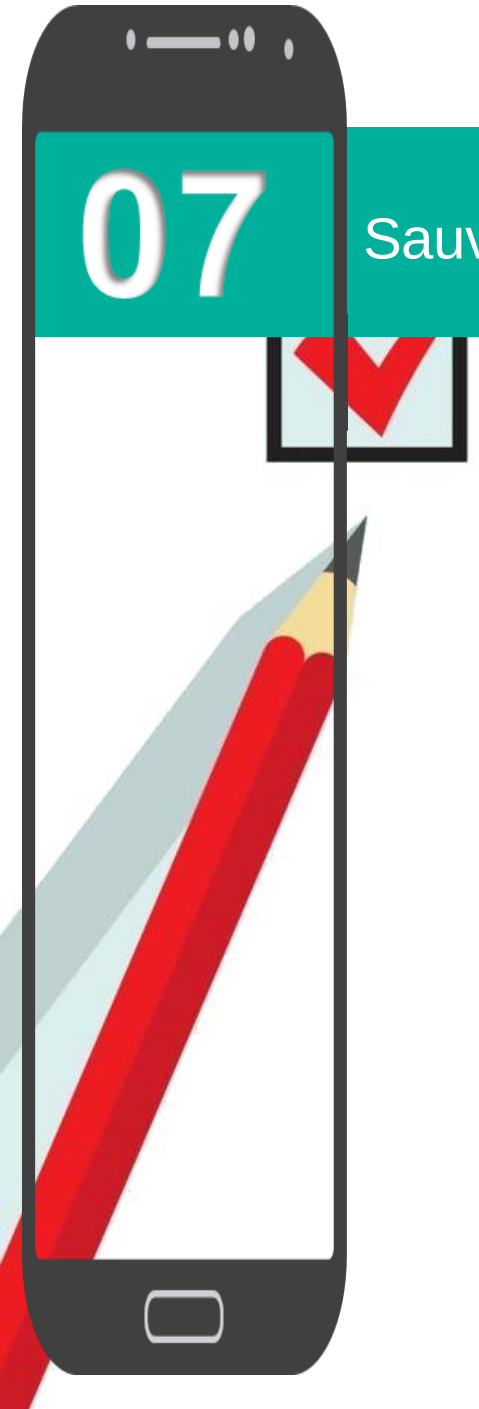
- **Si vous devez utiliser un réseau Wi-Fi ouvert dans une situation comme celle-ci, procurez-vous une application VPN pour votre appareil mobile. Elle vous rend anonyme en ligne et à l'abri des regards des cybercriminels.**



06 Téléchargez des applications à partir de magasins d'applications réputés

- **N'utilisez que les magasins d'applications officiels - la boutique Google Play si vous avez un appareil Android et l'App Store d'Apple si vous avez un iPhone ou un iPad.**

- **Il n'est que trop fréquent que les développeurs de logiciels malveillants créent de fausses applications malveillantes et les mettent en ligne sur des sites tiers douteux.**

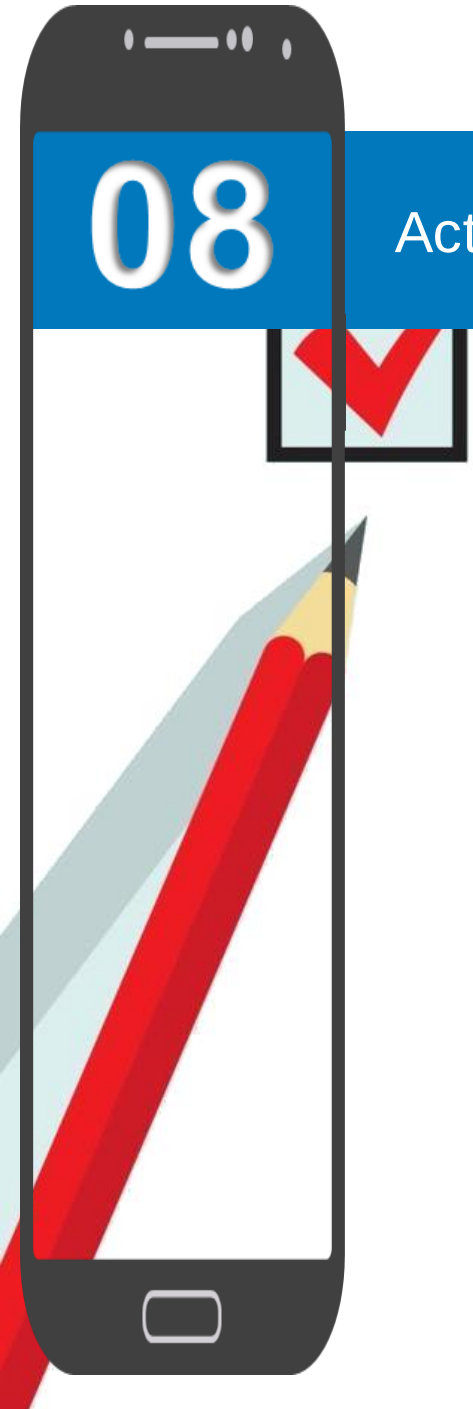


07 Sauvegardez vos données sur le cloud

- **Vous vous épargnerez bien des maux de tête si vous conservez une sauvegarde permanente de votre téléphone.**

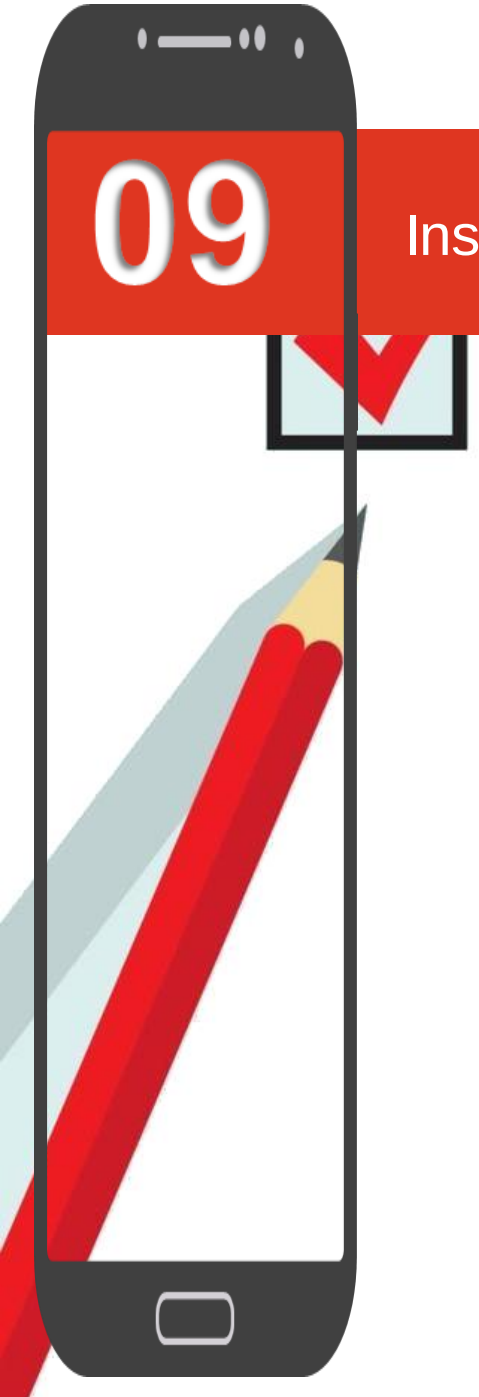
- **Ainsi, en cas de perte ou de vol, vous aurez toujours toutes les applications, les données et les comptes à jour dans votre sauvegarde.**

الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
tunCERT
Tunisian Computer Emergency Response Team



08 Activez l'effacement à distance de votre téléphone

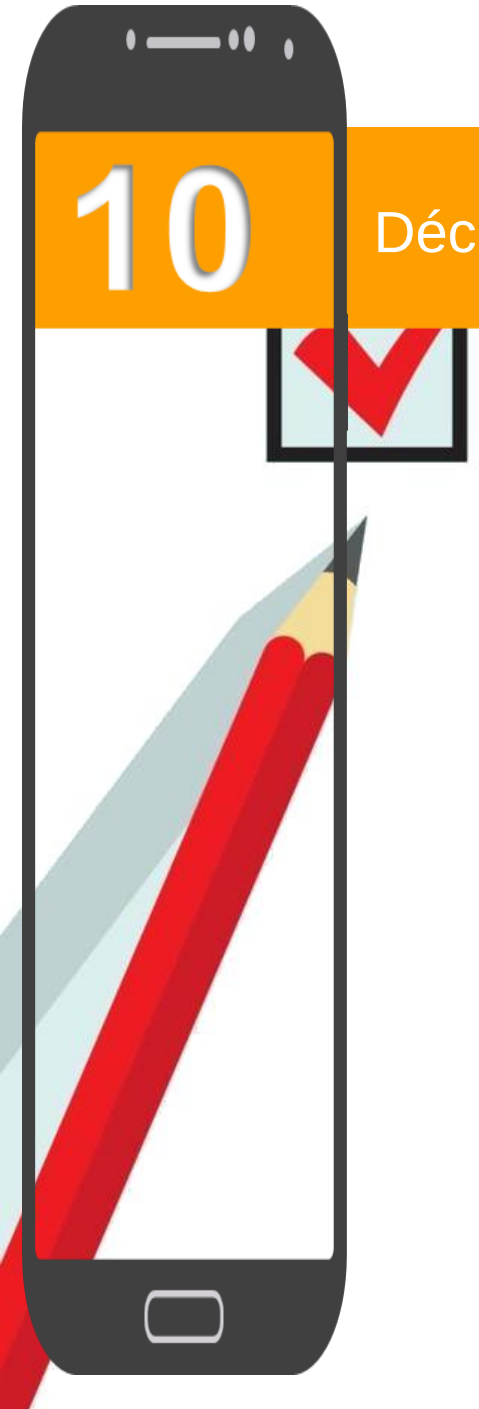
- **Dans le prolongement de la tranquillité d'esprit de la dernière étape, si votre téléphone est perdu ou volé, vous pouvez effacer toutes vos données personnelles de sa mémoire à distance.**



09 Installez un logiciel anti-virus

- **L'installation d'une application de sécurité solide vous permettra d'atteindre une protection totale.**

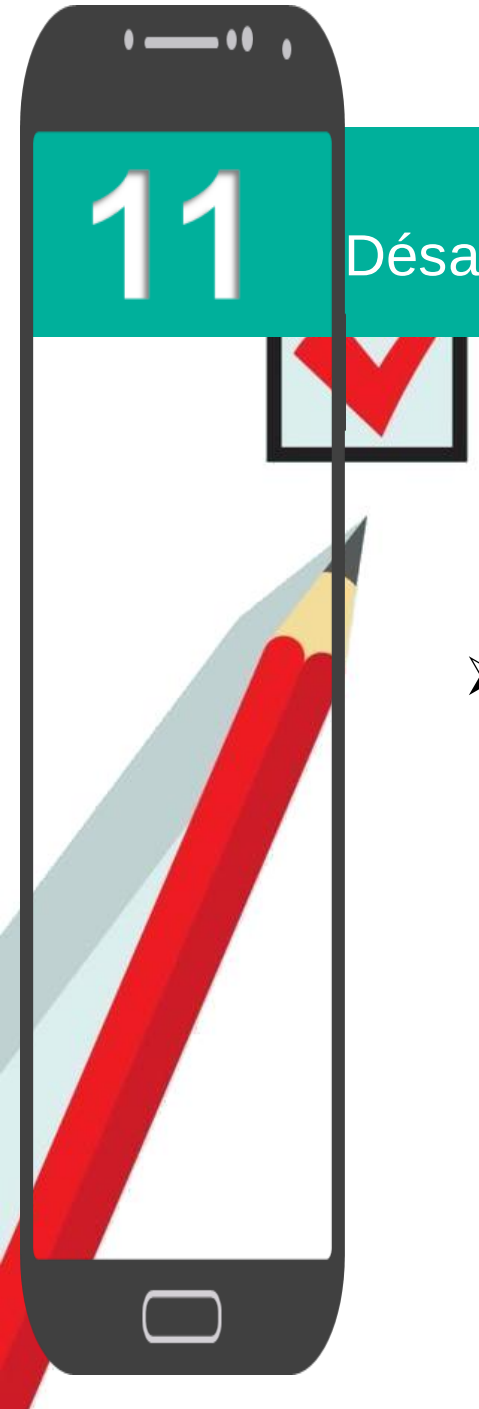
- **Ces applications travaillent en permanence et en arrière-plan pour s'assurer qu'aucun programme ou fichier inconnu ne s'introduit dans l'appareil.**



10 Déconnectez-vous des sites après avoir effectué un paiement

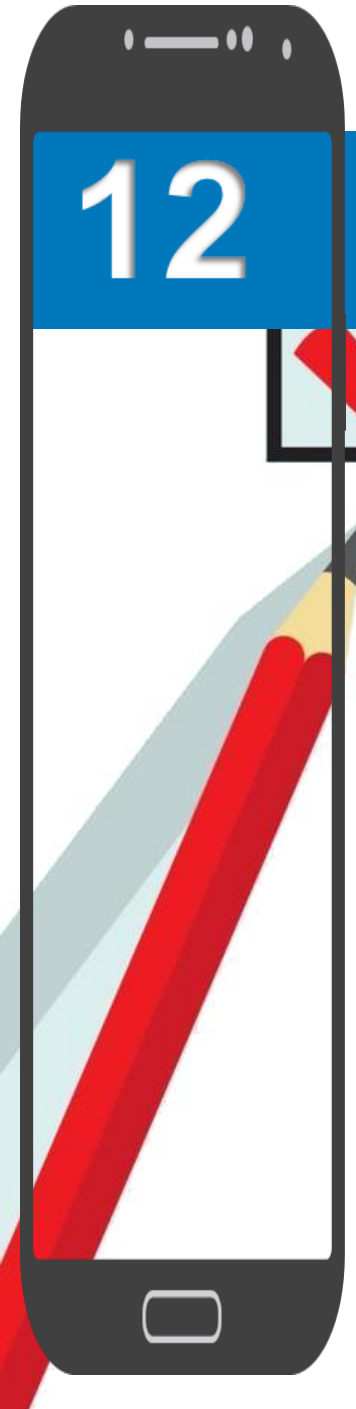
- **Si vous effectuez des opérations bancaires ou des achats depuis votre smartphone, déconnectez-vous de ces sites une fois vos transactions sont terminées.**

- **D'autres conseils consistent à ne pas stocker vos noms d'utilisateur et mots de passe sur votre téléphone et d'éviter les transactions lorsque vous êtes sur un Wi-Fi public.**



11 Désactiver le Wi-Fi/ Bluetooth/ Localisation lorsque vous ne l'utilisez pas

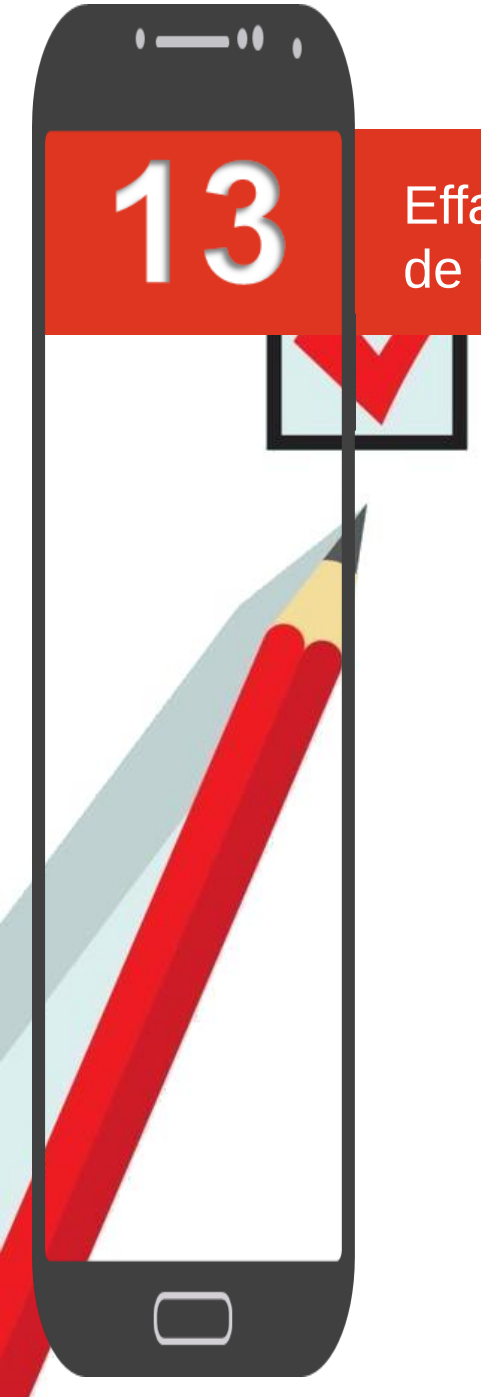
- **Vous pensez à eux comme à des moyens de se connecter à quelque chose, mais les voleurs peuvent les utiliser pour se connecter à votre appareil et accéder aux fichiers.**



12 NE PAS faire de jailbreak ou de root sur l'appareil

- **Il peut y avoir des avantages à essayer un nouveau système d'exploitation pour votre appareil, mais abandonner le système du fabricant peut aussi vous exposer à un risque accru.**

- **Assurez-vous de bien comprendre ce que le processus implique et toutes les fonctions de sécurité supplémentaires qui peuvent être nécessaires pour éviter les menaces de logiciels malveillants.**



13 Effacez en toute sécurité les informations personnelles avant de revendre ou de recycler votre appareil

- **Si vous envisagez de vendre ou de recycler votre appareil, supprimez toutes les données qui y sont stockées ainsi que toutes les applications avant d'effacer ou de sécuriser les informations personnelles.**

Contacts de l'ANSI

https://www.ansi.tn/

https://www.facebook.com/ansitn

https://www.youtube.com/channel/UCvDg94OdVjjEVPEcdaKdlLw/videos

abonnement@ansi.tn

incident@ansi.tn

الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
tunCERT
Tunisian Computer Emergency Response Team

Adresse : 49, avenue Jean Jaurès, 1000 Tunis
Tél : (+216) 71 846 020 / (+216) 71 843 200
Fax : (+216) 71 846 363