الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

Guide de sécurité Smartphones et tablettes

Version	Date de la version	Modification apportée
1.0	20/03/2015	Premier draft

Document Publique Document Interne Document Confidentiel Document Top-Secret

Comme les ordinateurs, les appareils mobiles sont exposés à toutes sortes de menaces dès lorsqu'ils sont connectés à Internet. De plus, ils sont plus exposés au vol.

Voici quelques conseils pour renforcer leur sécurité :

- **Installer une suite de sécurité :**

  Installer une suite de sécurité comporte plusieurs fonctionnalités qui vous protège des virus, des spams, des SMS piégés, des sites malveillants, des logiciels dangereux etc.

  Elle propose aussi de vérifier les mises à jour des applications installées aussi, la possibilité de retrouver et sécuriser votre smartphone ou tablette à distance, ainsi que la possibilité d'effectuer des sauvegardes de votre appareil.

  Elle permet aussi de localiser votre téléphone (depuis un autre appareil ou l'interface web) et déclencher une alarme afin de le retrouver plus facilement.

  Les principales fonctions d'une suite de sécurité pour un smartphone :

  - Moteur antivirus : protège des virus ainsi que des logiciels malveillants (Comprend l'analyse des SMS)
  - Pare-feu (appareils rootés uniquement).
  - Gestionnaire d'applications (les droits d'accès et les intentions de vos applications)
  - Fonction de localisation (Anti-vol).
  - La possibilité d'effectuer des sauvegardes de votre appareil.

  NB : N'installer pas les applications à partir de n'importe quelle source, certaines peuvent endommager votre appareil ou vous nuire personnellement. Vous pouvez choisir de valider les applications afin d'empêcher l'installation de logiciels dangereux sur votre appareil.

- **Code de verrouillage :**

  Utilisez toujours les codes de sécurité ou le numéro d'identification personnel (PIN) de la carte SIM en changeant le code PIN fournie par défaut par l'opérateur.

- **Verrouiller l'écran :**

  Vous pouvez sécuriser votre téléphone ou votre tablette en définissant un verrouillage d'écran. Chaque fois que vous allumez votre appareil ou réactivez l'écran, vous êtes invités à déverrouiller l'appareil.

Comment Configurer ou modifier le verrouillage de l'écran :

1. Ouvrez le menu **Paramètres** de votre appareil.
2. Sous la section "Personnel", appuyez sur **Sécurité**.
3. Sous la section "Sécurité de l'écran", appuyez sur **Verrouillage de l'écran**. Si vous avez déjà défini un verrouillage, vous devez saisir le schéma, le code PIN ou le mot de passe avant de pouvoir choisir un verrouillage différent.
4. Appuyez sur le verrouillage d'écran que vous voulez utiliser et suivez les instructions.

➢ Chiffrer ses appareils :

Une fois les données chiffrées, il n'est possible de les lire qu'à condition de disposer des identifiants appropriés. Cela peut vous assurer une protection accrue en cas de vol de l'appareil.

- **Comment Chiffrer un appareil équipé d'Android 4.4 ou version inférieure :**

Avant de chiffrer votre appareil, procédez comme suit :

1. Définissez un code PIN, un schéma ou un mot de passe de verrouillage d'écran.
2. Branchez votre appareil sur le chargeur.
3. Prévoyez au moins une heure pour l'opération de chiffrement. En cas d'interruption de la procédure, vous perdrez une partie, voire l'intégralité de vos données.

Lorsque vous êtes prêts à activer le chiffrement, procédez comme suit :

4. Ouvrez le menu "Paramètres" de votre appareil.
5. Dans la section "Personnel", appuyez sur Sécurité.
6. Dans la section "Chiffrement", appuyez sur Chiffrer la tablette ou sur Chiffrer le téléphone.
7. Lisez attentivement les informations relatives au chiffrement.

La luminosité du bouton "Chiffrer la tablette" ou "Chiffrer le téléphone" est atténuée si votre batterie n'est pas chargée ou si votre appareil n'est pas branché. Si vous changez d'avis quant au chiffrement de l'appareil, appuyez sur Précédent .

1. Appuyez sur **Chiffrer la tablette** ou sur **Chiffrer le téléphone**. **Avertissement** : Si vous interrompez la procédure de chiffrement, vous perdrez une partie, voire l'intégralité de vos données.
2. Indiquez le code PIN, le mot de passe ou le schéma de verrouillage de l'écran, puis appuyez sur **Continuer**.
3. Appuyez de nouveau sur **Chiffrer la tablette** ou sur **Chiffrer le téléphone**.

La procédure de chiffrement commence et sa progression s'affiche. Sachez que cette opération peut prendre une heure ou plus, et que l'appareil peut redémarrer plusieurs fois pendant le processus.

Une fois le chiffrement terminé, vous êtes invité à indiquer votre code PIN, schéma ou mot de passe. Par la suite, vous devrez indiquer votre code PIN, schéma ou mot de passe chaque fois que vous allumerez votre appareil.

- **Comment Activer le chiffrement avec le verrouillage d'écran sur des appareils équipés d'Android 5.0 ou version ultérieure :**

Pour accroître la protection des données de votre appareil chiffré, procédez comme suit :

1. Ouvrez le menu "Paramètres"  de votre appareil.
2. Dans la section "Personnel", appuyez sur **Sécurité**.
3. Dans la section "Sécurité de l'écran", appuyez sur **Verrouillage de l'écran**.
4. Sélectionnez "Schéma", "Code PIN" ou "Mot de passe" comme verrouillage d'écran.
5. Vous serez invité à accroître le niveau de protection des données de votre appareil en exigeant la saisie de ce code, schéma ou mot de passe au démarrage de votre appareil. Par défaut, ce paramètre est activé.

   Avertissement : Un service d'accessibilité tel que TalkBack ou un appareil associé en mode Bluetooth ne fonctionne pas lors du démarrage de votre appareil. Cela signifie que vous devrez indiquer votre code PIN, votre schéma ou votre mot de passe sans l'aide d'un service tel que TalkBack pour démarrer Android. Si vous avez besoin d'un service de ce type, ne configurez pas de verrouillage d'écran.

6. Définissez votre code PIN, schéma ou mot de passe, puis appuyez sur **Continuer**.

➢ Protéger vos données privées :

Lorsque vous faites réparer votre appareil protégez votre carte SIM et votre carte mémoire supplémentaire, puisqu'elles peuvent contenir des renseignements importants comme des coordonnées personnelles et des messages SMS et ne pas les laisser à l'atelier de réparation. Lorsque vous vous débarrassez de votre appareil, assurez-vous de ne laisser aucun renseignement dans la mémoire interne du téléphone ou sur la carte SIM (même si le téléphone ou la carte SIM sont brisés ou défectueux)

➢ Contrôle parental :

Installez un logiciel de contrôle parental sur l'appareil de votre enfant

N'hésitez pas à demander l'assistance du personnel du

tunCERT de l'ANSI :

E-mail : assistance@ansi.tn
Tél : 71 843 200

الهاتف: Tel: +216 71 846 020 - الفاكس : Fax +216 71 846 363

ansi@ansi.tn www.ansi.tn