MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
*Liberté*
*Égalité*
*Fraternité*

# LA LETTRE CYBER en Région Grand Est

Gendarmerie nationale

GENDARMERIE

NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

Août 2024

## LA THEMATIQUE DU MOIS:
## SECURISER SON SMARTPHONE

**Nous avons déjà parlé de ransomware, de DDOS, de sauvegarde etc. Toutes ces attaques qui touchent des « machines », des « VM », des « réseaux informatiques » mais finalement nous n'avons jamais parlé du matériel que nous utilisons TOUS, TOUT le temps et dont nous ne pourrions plus nous passer :**

# LE SMARTPHONE

## RESEAU

1. N'activez le Bluetooth qu'en cas de besoin uniquement.
2. Comme pour tout appareil nomade, évitez les réseaux publics et/ou inconnus, privilégiez votre réseau mobile. Il vaut mieux être seul sur son réseau qu'être avec des inconnus qui utilisent le même réseau que nous sans sécurité.
3. Réglez les **paramètres de géolocalisation** afin de toujours contrôler quand et par qui être géolocalisé. Cette fonctionnalité peut être très intéressante en cas de perte ou de vol, en revanche certains services n'ont pas forcément besoin de savoir où nous sommes pour fonctionner correctement.

## SECURITE PHYSIQUE

1. Utilisez des accessoires fiables et surtout des accessoires dont vous connaissez la provenance (câbles, chargeurs, prises, etc.).
2. Empêchez quiconque d'avoir un accès physique à vos appareils, et ne les laissez pas sans surveillance.
3. Attention au micro et à la caméra de votre appareil et pensez à ceux des autres. Évitez les conversations sensibles près de vos appareils électroniques. En effet, des options comme « SIRI » ou « OK GOOGLE » écoutent en permanence notre voix pour nous offrir leurs services.
4. Conservez toujours l'IMEI de votre appareil afin de permettre aux forces de l'ordre de demander le blocage du téléphone en cas de perte ou de vol.

# SECURITE DES LOGICIELS

**1. Téléchargez vos applications/fichiers uniquement depuis des sources officielles.**

Ces sources officielles contrôlent ce qu'elles mettent à disposition. Si vous ne connaissez pas la source, ce que vous installez pourrait être piégé et vous vous exposez à des pertes ou vol de données contenues dans votre téléphone. De même, lorsque vous installez une nouvelle application, assurez-vous bien qu'elle n'a accès qu'aux données dont elle a besoin pour fonctionner.

**2. Installez un antivirus et maintenez les fonctionnalités de protection intégrées à votre appareil.**

**3. Comme pour tout appareil, maintenez à jour votre smartphone et les applications**. Les mises à jour corrigent souvent des failles de sécurité qui pourraient être exploitées par des personnes mal intentionnées.

# CONSEILS D'UTILISATION

1. Attention aux conversations sensibles par messages. Utilisez un logiciel de messagerie chiffré et dans lequel vous avez confiance en fonction du niveau de confidentialité à respecter.
2. Faites des sauvegardes de vos données afin de les récupérer en cas de vol ou de perte de l'appareil.
3. Mettez en place un verrouillage automatique de l'appareil afin de ne pas laisser l'accès aux données en cas d'oubli. Choisissez un code solide, c'est-à-dire un code sans aucune signification (pas de date de naissance par exemple...) afin que personne ne puisse le deviner et rendre la tâche plus difficile à des "robots. Si vous conservez des données sensibles, mettez-les dans un container chiffré avec un mot de passe fort.
4. Vous pouvez également utiliser la biométrie afin de sécuriser votre appareil. N'oubliez cependant jamais que derrière cette biométrie, il y a un mot de passe qui, lui, peut être découvert...
5. Limitez et maîtrisez les informations que vous mettez dans votre smartphone… code, coordonnées bancaires, mot de passe, etc…

**POUR ALLER PLUS LOIN**

**Retrouvez les conseils détaillés de l'ANSSI et de la CNIL sur les liens suivants**

CNIL : https://www.cnil.fr/fr/comment-securiser-au-maximum-lacces-votre-smartphone

ANSSI: https://cyber.gouv.fr/publications/securiser-son-ordiphone

+ D'INFOS

CYBER MALVEILLANCE .GOUV.FR

PHAROS
PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

e-enfance 3018

CNIL. PROTÉGER les données personnelles ACCOMPAGNER l'innovation PRÉSERVER les libertés individuelles

ANSSI Agence nationale de la sécurité des systèmes d'information

Région de gendarmerie du Grand Est
**LA LETTRE CYBER en région Grand Est**

Directeur de la publication: GCA O.KIM
Responsable éditorial: COL L. GRAU
Rédacteur: ADJ M. KNOBLOCH

Si vous souhaitez recevoir cette lettre, envoyez un mail à :
Laurent.grau@gendarmerie.interieur.gouv.fr
Mathieu.knobloch@gendarmerie.interieur.gouv.fr

**Suivez l'actualité de la gendarmerie:**