# *Votre coffre-fort dans la poche*


Toute votre sphère privée est contenue dans ce petit appareil nommé smartphone, un vrai coffre-fort qui contient vos contacts, votre correspondance, vos photos intimes ou pas, vos codes et accès à divers services et loisirs, votre argent (Twint ou équivalence), l'accès à des jeux, de la musique, vos réseaux sociaux et votre géolocalisation, etc. et bientôt votre permis de conduire, carte grise de la voiture et plus encore. La plupart du temps, tout comme l'accès à l'appareil, ces accès sont ouverts en permanence parce que c'est plus rapide et plus confortable pour les utiliser,

A la maison, votre coffre-fort est généralement bien caché et surtout bien fixé au mur et la plupart du temps bien fermé avec un code de protection. Votre smartphone lui, est très souvent dans la poche arrière du jeans ou dans votre main près de l'oreille lorsque vous déambulez dans la rue, c'est une grande tentation pour les voleurs à l'arraché, car votre smartphone est une vraie mine d'or à exploiter une fois volé, sans compter son prix de revente. On peut aussi facilement le perdre ou l'oublier quelque part.

## Vol, détournement ou perte du smartphone

La perte de votre smartphone peut tourner à la catastrophe, surtout si cela survient à l'étranger : que va en faire la personne qui l'a subtilisé ou trouvé ? Et surtout comment éviter que cette perte n'impacte pas dramatiquement votre vie de tous les jours.

**Prévention**

- Effectuez régulièrement une sauvegarde de votre smartphone sur un disque externe ou sur un cloud indépendant *(pour aussi protéger votre sphère privée)* comme Swiss Backup.
- Utilisez le maximum de caractères possibles pour votre PIN code (exemple : pour trouver le PIN code 7649 = $4^{10}$ essais = 1'048'576 essais et PIN code 764925 = $6^{10}$ essais = 60'466'176 essais)
- Définissez un délai de verrouillage automatique. Cela empêche l'accès aux informations contenues dans le smartphone en cas de perte ou de vol.
- Notez le numéro « IMEI - International Mobile Equipment Identity », c'est le N° de série du smartphone et vous pouvez le faire bloquer en appelant votre prestataire en cas de perte ou de vol.
    - Identification unique de série de l'appareil - ***#06#** pour l'afficher

## L’UFED - Universal Forensics Extraction Device

L’UFED est produit de la société israélienne Cellebrite. C’est un logiciel d'enquête numérique pour extraire, décoder, analyser et générer des rapports sur les données de divers smartphones. Il est largement utilisé par les forces de l'ordre pour rassembler des preuves numériques.

Il permet le décodage et analyse des systèmes de fichiers et de mot de passe de toutes les données **(même supprimées)** des téléphones classiques, des smartphones, des appareils GPS portables, des tablettes et des téléphones même fabriqués avec des chipsets chinois.

Il est vendu uniquement à des organisations certifiées. Le prix catalogue initial est d'environ 6’000 $, mais on peut le trouver sur eBay pour moins de 1’000 $, ce qui fait le grand bonheur des pirates qui peuvent avec cet équipement faire un usage très approfondi des données de votre smartphone.

## Attaque par SIM swapping

Vous remarquez que votre smartphone perd soudainement le service mobile sans raison apparente, cela peut être un signe que votre numéro a été transféré à une autre carte SIM.

Déroulement de l’attaque :

1. Le hacker se procure sur les réseaux sociaux ou le darknet des informations personnelles sur sa victime, telles que son nom, son adresse, sa date de naissance, son adresse e-mail ou encore les services en ligne qu'elle utilise.
2. Il contacte la victime par téléphone ou par e-mail en se faisant passer pour son opérateur, sa banque, son fournisseur d'accès à internet ou tout autre service, en lui demandant de confirmer ou de fournir des informations personnelles.
3. Après avoir recueilli ces d'informations, le hacker contacte l'opérateur téléphonique de la victime en se faisant passer pour elle. Il prétend avoir perdu ou cassé son smartphone. et demande à ce que son numéro soit transféré sur une nouvelle carte SIM qu'il possède.
4. Le numéro de la victime est alors activé sur la carte SIM du hacker. Ce dernier peut alors recevoir les appels et les SMS de la victime, et accéder à ses comptes en ligne.

**En cas de vol, de perte ou de SIM swapping**

- Contactez rapidement votre opérateur téléphonique pour lui signaler le problème et demandez le blocage de votre numéro et de la carte SIM.
- Changez les mots de passe de tous vos comptes et logins utilisés avec le smartphone.
- Vérifiez régulièrement les transactions sur vos comptes bancaires pour détecter toute activité non autorisée.

- Portez plainte auprès des autorités compétentes et conservez les preuves du vol ou de la fraude (messages, notifications, relevés bancaires, etc.).

## Les arnaques

Votre smartphone n'est pas seulement un coffre-fort ambulant facile à subtiliser, c'est aussi un terrain de chasse idéal pour les arnaqueurs, pas besoin de faire du porte à porte pour trouver des victimes, il y a toutes les cibles et contacts possibles dans cet appareil : les arnaques au QR code, aux paiements Twint, aux appels frauduleux non seulement à votre intention, mais aussi à vos contacts.

### L'arnaque au QR code

De faux QR code sont indiqués dans l'offre affichée ou collés sur le QR code original (exemple bornes de parking).

*Prévention*

Observez si c'est un QR code collé ou dans le doute scannez le QR code avec une application qui affiche seulement le QR code et examinez-le, ne scanner surtout pas avec une application de paiement.

### Arnaques paiement par TWINT ou carte de crédit depuis votre smartphone

a) Vous recevez un message vous demandant suite à un problème ou une réorganisation de confirmer les coordonnées du compte en banque ou de la carte de crédit rattachée à votre compte TWINT. Le code QR ou les liens présents dans le message conduisent à un site web frauduleux ressemblant à s'y méprendre à celui de TWINT.

b) Vous vendez un objet sur « Le Bon coin » ou « Ebay » et l'acheteur potentiel vous demande plus de précisions sur votre compte TWINT pour qu'il puisse vous payer.

*Prévention*

- Utilisez un deuxième compte courant pour vous paiements TWINT. Ce compte contiendra une petite somme d'argent.
- N'utilisez pas votre smartphone pour vos autres transactions avec vos comptes bancaires.
- Vérifiez périodiquement l'état de ces comptes afin de détecter toute fraude.
- La police, les administrations publiques et les banques ne communiquent et ne demandent jamais d'information par téléphone.
- Ne transmettez pas votre n° de smartphone à n'importe qui.
- Prêter son smartphone à un enfant pour l'occuper avec des jeux présente des risques en matière de sécurité, de confidentialité et de contenus inappropriés.
- Activez dans le navigateur le mode privé pour vos transactions bancaires et achats.
- Utilisez une application de blocage d'appels non désirés (ex: Blacklist PRO).

- Faites périodiquement le ménage des vieux messages, sms et photos.
- Attention dans la rue si vous l'utilisez en marchant.

Si vous avez divulgué vos données, changez immédiatement vos mots de passe bancaires TWINT et bloquez le compte et les cartes de débit ou de crédit concernées,

**Florilège des arnaques courantes par smartphone**

Beaucoup d'arnaques connues sur le WEB sont aussi exploitables par smartphone, donc ayez la même prudence que vous pratiquez avec votre ordinateur.

- Arnaques aux noms de fausses autorités.
- Arnaques aux sentiments.
- Arnaques aux investissements financiers.
- Arnaques aux nouvelles normes écologiques.
- Arnaques aux modifications de vos comptes ou abonnements.
- Arnaques aux demandes d'assistance financière pour une bonne cause ou assistance d'urgence,
- Arnaques à l'héritage d'un lointain membre de la famille.
- Erreurs de facturation remboursables.
- Erreurs d'adresse ou changement de dates de livraison.
- Arnaques aux belles affaires et super actions (sites douteux).
- Arnaques DeepFake par fausses vidéos, voix et visages clonés.
- Méfiez-vous des sondages proposés, ils peuvent contenir des pièges pour obtenir des informations sensibles.

Sachez qu'avec l'IA, les arnaques deviennent de plus en plus subtiles et pernicieuses.

Soyez prudents – Claude Maury