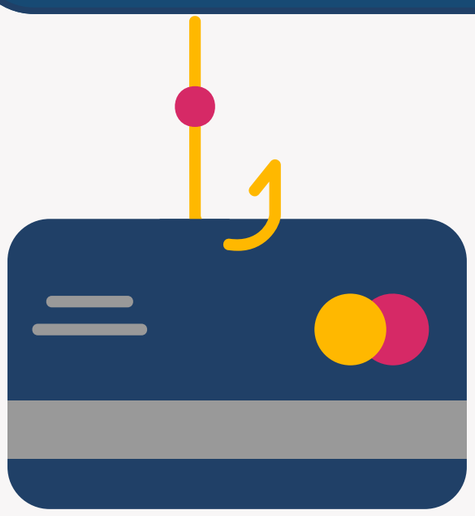
TÉLÉPHONIE MOBILE

Principaux risques et conseils pour les éviter

Vol de données : Récupération des données personnelles stockées sur le téléphone mobile d'une personne, soit par un acte physique (perte ou vol de l'appareil), soit par un acte virtuel (par exemple un virus installé sur le téléphone lors du téléchargement d'une application).

SPAM ou SPAMMING : Envoi massif de messages électroniques dans un but promotionnel ou publicitaire à des personnes avec lesquelles l'expéditeur n' a jamais eu de contact mais dont il a récupéré les informations de façon irrégulière.



Hameçonnage ou Phishing : Vol d'identités ou d'informations confidentielles par subterfuge. Les escrocs se font le plus souvent passer pour un organisme de confiance (par exemple un organisme bancaire) et invitent les usagers, par message, à visiter le site frauduleux - qui ressemble au site authentique - et à partager des informations sensibles.

Vishing : Issue de la contraction de « *voice* » (voix) et « *phishing* », cette arnaque par appel téléphonique ou message vocal a pour objectif d'obtenir les données bancaires ou personnelles de la victime, en se faisant passer pour une source fiable.

Ping-Call ou SPAM Vocal : Arnaque répandue qui consiste à pousser la victime à rappeler le numéro surtaxé qui l'a contactée. En fonction des cas :

- le téléphone sonne une fois puis raccroche ;
- le téléphone raccroche après qu'un message vocal ait répondu à la personne.

Intelligence Artificielle (IA) : Technologie qui peut renforcer les pratiques d'arnaques existantes grâce à l'usage de correcteurs, d'aide à la reformulation des textes, rendant de plus en plus difficile la reconnaissance des messages frauduleux. L'IA peut également reproduire/usurper la voix d'une personne dans le but de tromper un tiers et lui extorquer des fonds en se faisant passer pour un proche en difficulté.

Pour plus d'information voir la fiche pratique « *Lexique du parfait hacker* »

APDP
AUTORITÉ DE PROTECTION DES DONNÉES PERSONNELLES

Comment sécuriser son téléphone ?

EN AMONT

1. Modifier le code PIN lors de la 1ère utilisation du téléphone
2. Mettre en place des codes d'accès différents, en utilisant si possible plusieurs moyens d'accès
3. Conserver une copie de son code IMEI hors de son téléphone
4. Mettre en place un écran « *anti-espion* »

AU QUOTIDIEN

5. Effectuer régulièrement les mises à jour
6. Effectuer des sauvegardes
7. Vérifier régulièrement les autorisations des applications
8. Installer des applications uniquement à partir de sites ou magasins officiels
9. Protéger les informations confidentielles stockées sur son téléphone

BONS RÉFLEXES

10. Ne jamais laisser un tiers utiliser son téléphone sans surveillance
11. Éviter de se connecter aux réseaux WIFI publics ou inconnus
12. Ne pas répondre aux numéros de téléphone inconnus
13. Ne jamais transmettre de données bancaires ou d'informations personnelles par téléphone