LE GUIDE DES ARNAQUES A DISTANCE LES PLUS FREQUENTES

. Arnaques de communications

📱 Phishing / Hameçonnage

- Emails, SMS ou messages qui imitent des organismes officiels (banques, impôts, sécurité sociale, SNCF, La Poste, etc.) pour voler vos identifiants ou vos coordonnées bancaires en vous poussant à cliquer sur un lien frauduleux.

📲 Smishing

- Phishing par SMS : messages disant que votre colis est bloqué, que votre compte est suspendu, que vous avez 24heures pour payer un excès de vitesse etc., avec un lien vers un faux site.
  Exemple fréquent : *« Votre colis n'a pas pu être livré, cliquez ici pour régulariser »*.

📞 Vishing – Hameçonnage vocal

- Appels téléphoniques où l'on vous fait croire que vous parlez à votre « conseiller bancaire » ou à un organisme officiel pour vous soutirer des informations sensibles ou vous convaincre de faire un virement. Si cela vous arrive raccrochez et dites que vous allez rappeler ; encore mieux inventer un nom « bidon » de conseiller vous verrez tout de suite la supercherie

📢 Usurpation de numéro / Spoofing

- Les escrocs peuvent faire afficher un numéro de banque ou d'administration authentique alors qu'ils ne sont pas légitimes. Cela augmente la crédibilité de l'arnaque.

📜 Quishing – QR codes frauduleux

- Faux QR codes (par SMS ou affichés sur des documents publics) qui redirigent vers des sites de phishing ou recueillent vos infos. Il convient d'être aussi méfiant par exemple des personnes collent des QR codes sur des bornes de paiement de stationnement

💳 2. Arnaques financières et bancaires

🏢 Faux conseillers bancaires / faux agents anti-fraude

- Quelqu'un se fait passer pour votre banque, vous dit qu'il y a un problème et demande un virement de sécurité. Cette arnaque est très répandue et a fait des **milliers de victimes** en France.
- Il peut aussi vous dire que votre carte bleue est périmée et il vous envoie un coursier pour la récupérer
- Dernière en date la fausse carte bleue avec le logo de votre banque envoyée à votre domicile en vous demandant de flasher le QR Code pour l'activer

📉 **Escroquerie à l'avance de fonds**

- On promet un gros gain (loto, héritage, fortune, etc.) mais il faut d'abord envoyer une somme ou des infos personnelles.

💰 **Fraudes à l'investissement**

- Faux investissements — crypto, placements miracles ou opportunités trop belles pour être vraies — ils demandent d'envoyer de l'argent ou de transférer des fonds.

💻 3. Arnaques techniques et d'intrusion

🛠️ **Support technique frauduleux**

- Pop-ups ou appels prétendant venir de Microsoft, Apple ou un service de sécurité vous disant que votre appareil est infecté et vous demandent de payer ou d'installer un logiciel de contrôle à distance.

🕳️ **Ransomware / rançongiciels**

- Logiciels qui cryptent ou bloquent vos fichiers et demandent une rançon pour les débloquer. Certains vous disent aussi que vous avez été sur des sites peu fréquentables et vous menacent de le faire savoir

📂 **Piratage de comptes**

- Vol de mots de passe ou accès à vos emails / réseaux sociaux puis utilisation de vos comptes pour escroquer d'autres personnes ou voler vos données.

📸 **Scams via fichiers multimédias infectés**

- Images (ex : même) reçues par WhatsApp ou autre plateforme qui contiennent des malwares une fois téléchargées.

🛍️ 4. Arnaques courantes liées au commerce

🛒 **Faux sites marchands**

- Sites qui vendent des produits qui n'existent pas, ne sont jamais livrés ou volent vos cartes bancaires. Quelques fois ils ressemblent comme deux gouttes d'eau au vrai site

📦 **Arnaques de livraison**

- Faux messages sur des colis bloqués avec liens vers des sites piégés pour voler vos infos bancaires.

🏖️ **Fraudes aux voyages / hébergement**

- Offres de vacances, voyages fabuleux ; locations ou billets à prix cassés qui n'existent pas. Il est très facile aujourd'hui de créer une fausse annonce avec l IA ; un principe de base a adopter « c'est trop beau et pas cher pour être vrai »

💬 5. Arnaques relationnelles et psychologiques

❤️ Arnaques sentimentales

- Escrocs créent des relations émotionnelles en ligne, demandent de l'argent, parfois pour soi-disant des urgences puis disparaissent

📣 Escroqueries aux dons / œuvres de charité frauduleuses

- Sollicitations qui exploitent la générosité, en particulier après une catastrophe ou pour une cause touchante.

🚩 Signaux d'alerte fréquents

Voici des **indices** qui doivent éveiller la méfiance :

- Demandent **des informations personnelles ou bancaires** par SMS, mail ou téléphone.
- Vous poussent à cliquer sur un lien ou à télécharger un document urgent.
- L'offre est **trop belle pour être vraie** (gains importants, remboursement instantané).
- Pression à agir **rapidement** sous prétexte d'une menace ou d'une date limite.
- Communication provient d'un numéro ou d'une adresse inconnue ou bizarre.

🛡️ Bonnes pratiques de prévention

- Ne jamais répondre à un SMS ou mail suspect.
- Ne pas cliquer sur des liens dans des messages inattendus.
- Appeler directement l'organisme prétendument émetteur (sans utiliser les coordonnées du message).
- Installer des **mises à jour de sécurité** et un logiciel anti-malware de qualité.
- Utiliser des mots de passe forts et différents pour chaque compte. Les changer de temps a autre
- En cas de doute, **ne pas se sentir obligé de répondre tout de suite**.
- Autrefois les arnaqueurs faisaient des erreurs et beaucoup de fautes d'orthographe mais aujourd'hui avec l IA ils sortent des documents de plus en plus pointus

---

📞 En cas de suspicion

Si quelqu'un pense être victime d'une arnaque en France :

- Déposer plainte auprès des autorités compétentes (PHAROS, gendarmerie/police).
- Signaler les messages suspects (ex : via SIGNAL SPAM ou les services anti-fraude recommandés par les opérateurs).
