Fraudes et arnaques au quotidien, comment déjouer les fraudes.

Les fraudes et arnaques sont multiples et constituent une réelle menace à laquelle chacune et chacun d'entre nous est confronté dans son quotidien, qu'il s'agisse d'arnaques en ligne ou de fraudes liées à la « vente hors établissement »

Internet, le grand hypermarché des fraudes et arnaques en tout genre

Les fraudes et arnaques qui « fleurissent » actuellement, ont un point commun : elles utilisent toutes les possibilités offertes par internet, média auquel recourent tous ses usagers (grandes, voire très grandes entreprises, PME, services de l'Administration, collectivités locales et bien évidemment l'ensemble des particuliers).

Selon le dernier rapport de la Banque de France, 1,3 million de ménages ont été escroqués en 2020, pour un montant total de 740 millions d'euros.

Deux chiffres permettent de mieux comprendre la réalité des faits : selon l'INSEE, 52,6 millions de français sont des utilisateurs actifs sur les réseaux sociaux et 94% des personnes qui se connectent sur internet utilisent les réseaux sociaux (You tube, Instagram, Facebook, Linkedin etc...) qui sont un véritable phénomène de société, jusqu'à devenir le prolongement de l'identité d'un individu et faire office d'identité numérique, au même titre que la carte d'identité ou le passeport.

Or, les cyber escrocs, les plus connus, les **hackers** *(de to hack qui signifie bidouiller, modifier)* ont un objectif commun : s'introduire dans un appareil, un système ou un réseau pour le détourner et voler les identités via les réseaux sociaux, qu'ils utilisent ensuite pour leur propre compte ou qu'ils revendent sur des sites du « dark net ».

Les principaux mécanismes utilisés par les cyber criminels

- **le hameçonnage ou phishing** consiste à envoyer des courriels frauduleux, en se faisant passer pour une personne de confiance ou un tiers de confiance (impôts, CAF, banque) afin de récupérer des données personnelles (le plus souvent bancaires) et soutirer de l'argent à leur victime.

Ce type d'arnaque, le plus répandu, peut s'appliquer dans de très nombreuses situations de la vie courante (locations saisonnières, achats sur internet etc…).

- **le rançongiciel ou ransomware** consiste à installer un logiciel malveillant qui bloque l'accès de l'utilisateur à son ordinateur ou à différents fichiers en les cryptant et en réclamant le paiement d'une rançon, pour obtenir le déchiffrage des données.

Parmi les principaux rançongiciels on peut citer :

- **le chantage à la webcam** (courriel dans lequel le cybercriminel fait croire qu'il détient des images du destinataire en train de regarder une vidéo pornographique et réclame le paiement d'une rançon pour prix de son silence).

- **l'arnaque au faux support technique** qui consiste à faire croire que l'ordinateur du consommateur a un problème grave (virus, erreur du système, blocage de l'écran) et que la réparation passe par l'appel d'une plateforme (en tout point semblable à celles des services techniques de Windows ou Microsoft) qui moyennant un paiement immédiat par CB (de 150 à 500 euros) reconfigurera l'appareil.

- **Focus sur les fraudes bancaires**

Les hackers disposent de techniques pour contourner les différents moyens de sécurisation des paiements en ligne (dont l'authentification renforcée). Bien que le sachant, les banques renâclent à rembourser leurs clients.
Parmi les fraudes les plus utilisées on peut citer :

- **l'arnaque au faux conseiller bancaire** dans laquelle on réclame au client ses identifiants et coordonnées bancaires pour faire échec à une soit disant opération frauduleuse en cours de réalisation.
- **l'arnaque au virement** dans laquelle l'escroc a réussi à accéder à l'espace client et à effectuer un virement au profit d'un bénéficiaire inconnu du titulaire du compte.

Pour ces deux types d'arnaques bancaires, le principe posé par les textes réglementaires est celui du droit au remboursement du client lésé, sauf agissements frauduleux ou négligence grave, sachant que c'est à la banque de prouver l'existence de ces manquements.

- l'**arnaque au faux RIB** consiste pour l'escroc à intercepter un mail adressé par un créancier avec une facture et un RIB pour remplacer ce dernier par le sien.
Le client procède au règlement sans se rendre compte que l'adresse mail et le RIB ont été modifiés. Ainsi les fonds ont été en réalité transférés directement à l'escroc et non au créancier.

Ce cas de figure est le seul dans lequel les chances d'obtenir un remboursement sont faibles. En effet la réglementation considère que les banques n'ont pas à vérifier l'adéquation entre le nom mentionné sur le RIB et le détenteur du compte.

Les arnaques liées à la vente « hors établissement »

- **la vente hors établissement** est une technique de vente qui consiste à solliciter le consommateur en dehors d' un établissement commercial, soit à domicile, soit dans un espace privé non habituel pour le commerce (hôtel, restaurant , magasin éphémère) afin de lui faire souscrire un contrat pour l'achat d'un bien ou d'un service.

- **Elles concernent les secteurs d'activité suivants** : les produits en lien avec l'habitat, les travaux de rénovation énergétique, les fournisseurs d'énergie et d'accès à internet ainsi que les contrats de services.

- **Quatre dispositions réglementaires sont prévues pour protéger le consommateur et faire échec aux pratiques frauduleuses :**

    1. une information précontractuelle
    2. la remise obligatoire d'un contrat
    3. un délai de rétractation de 14 jours
    4. l'interdiction de percevoir une contrepartie financière pendant un délai de 7 jours

    - **Le démarchage téléphonique s'il n'est toujours pas interdit est soumis à une réglementation de plus en plus contraignante :**

    - **une loi d'avril 2020** crée un nouvel article du code des assurances qui fixe des obligations aux assureurs,
    -
    - **une loi de juillet 2020** interdit le démarchage téléphonique dans le domaine de la rénovation énergétique,

    - **depuis le 1er janvier 2023** obligation pour les plateformes de démarchage téléphonique d'utiliser des préfixes déterminés (09-48, 09-49 etc...) en lieu et place des 01 à 05 ou 06 et 07,

    - **depuis le 1er mars 2023** le démarchage commercial téléphonique n'est plus autorisé que du lundi au vendredi de 10h à 13h et de 14h à 20h.

Au final, quelle que soit la situation concernée, il est primordial de faire preuve de prudence, de prendre le temps de la réflexion. La vigilance s’impose pour ne pas s’exposer aux arnaques en tout genre.