10 ARNAQUES EN LIGNE LES PLUS FRÉQUENTES

COMMENT LES ÉVITER ?

En 2021, une arnaque sur deux a lieu sur internet (selon l'Observatoire national de la délinquance) et beaucoup ont pour objectif de vous soutirer de l'argent. Comment les identifier ?

1 LES ARNAQUES À L'AMOUR

Le scénario est toujours le même : un faux profil, une rencontre virtuelle, la création d'un lien affectif, une webcam non fonctionnelle et un besoin d'aide pour des frais relatifs à la santé ou à un autre cas de force majeure. Profitant de la solitude de sa victime, l'escroc espère lui soutirer régulièrement de l'argent. Comme ces arnaques reposent sur du vol d'images et une usurpation d'identité, **passez les photos au crible d'un moteur de recherche pour voir si elles sont affiliées à un autre compte sur les réseaux sociaux**. Si au cours des échanges, votre interlocuteur trouve toujours une excuse pour ne pas vous rencontrer, c'est également un mauvais signe.

2 LES FAUSSES OFFRES D'EMPLOI

Ces mails vous proposent une offre d'emploi hors de votre champ de compétences avec un salaire alléchant. Ils sont envoyés par des fraudeurs usurpant l'identité de vrais recruteurs affiliés à des entreprises sérieuses. **Une fois l'offre acceptée par la victime, celle-ci reçoit une généreuse somme d'argent par chèque pour s'équiper.** Il lui est demandé de rembourser, dès son encaissement, le montant qui ne sera pas dépensé. Ce chèque, volé, sera rejeté quelques jours plus tard par la banque. Attention donc aux offres trop attractives. Ne transmettez jamais vos informations personnelles (RIB, numéro de carte bancaire ou de sécurité sociale…) sans savoir vraiment à qui vous avez affaire.

3 LES ESCROQUERIES À LA LOTERIE

« *Vous avez gagné 10 000 euros!* » Importantes sommes d'argent ou lots précieux, ce sont très souvent des arnaques. Ces escroqueries font croire à l'internaute qu'il a remporté un lot, puis **lui demandent ses renseignements bancaires en prétextant qu'ils sont nécessaires à la réception des fonds ou du cadeau.** Les hackers usurpent l'identité de compagnies comme la Française des jeux afin de duper leurs victimes. Pour éviter de tomber dans le panneau, partez du principe que, si vous n'avez pas joué, les chances de gagner sont presque nulles. En cas de doute, appelez l'organisme supposé être à l'origine de cette surprenante victoire. Si le message comporte un lien ou une pièce jointe, ne cliquez pas dessus.

4 LE FAUX SUPPORT TECHNIQUE

Par un message bloquant son ordinateur, le cybercriminel indique à sa victime la présence d'un souci technique pouvant lui faire perdre ses données ou endommager son appareil de manière irréversible. **L'usager est alors invité à contacter un service de maintenance technique** (déguisé en l'un des géants de l'informatique comme Microsoft) afin de le pousser à payer pour une opération de dépannage ou un logiciel de réparation. Pour vous protéger, mettez régulièrement à jour les systèmes de sécurité de vos appareils et assurez-vous d'avoir un bon antivirus ainsi qu'un pare-feu. Évitez également la navigation sur des sites illicites (streaming, téléchargement) et n'installez pas de programmes piratés.

Par **Nawal Benali**

ID-WORK/ISTOCK

5 LA FRAUDE 419 OU NIGÉRIANE

Le cybercriminel envoie un mail ou un message sur Facebook, en se faisant passer pour un riche héritier soucieux de faire sortir ses capitaux du pays. **Il requiert l'aide de sa victime afin que son compte bancaire accueille les fonds, en échange de quoi elle percevra une importante somme d'argent.** Si celle-ci tombe dans le piège, il lui sera demandé d'avancer des frais sous couvert d'excuses comme le paiement de taxes douanières, et de délivrer ses coordonnées bancaires. Si ce type d'escroquerie (« 419 » comme l'article du code pénal nigérian qui condamne cette pratique) paraît risible par son manque de finesse, son nombre est pourtant en hausse. Si vous recevez un mail de la sorte, n'y répondez pas.

6 LES ŒUVRES DE BIENFAISANCE

Sauvegarde d'un écosystème, protection d'une population ou catastrophes naturelles : les occasions de participer aux travaux d'organisations de bienfaisance sont multiples. **Certains escrocs du net sont de véritables experts en la matière et créent de faux sites afin de collecter des fonds.** Ils incitent les victimes à faire des dons directement par mail en insérant le lien de la page de la cagnotte. Pour savoir s'il s'agit d'une arnaque, regardez bien le site internet. En règle générale, un organisme caritatif sérieux aura un site affichant sa déclaration d'intention et ses documents d'exonération fiscale.

7 LES ARNAQUES « BOILER ROOM »

Il s'agit d'une forme d'arnaque à l'investissement. Dans la plupart des cas les escrocs se font passer pour des courtiers en bourse souhaitant aider les victimes à placer leur argent dans des actions supposées leur rapporter gros en un temps record. Ceci est bien trop beau pour être vrai, alors prudence. Méfiez-vous des personnes non sollicitées qui vous proposent ce type d'offres alléchantes : en général, la promesse d'un retour sur investissement rapide est souvent le signe d'une tentative de fraude. Vous pouvez aussi vérifier si la personne qui vous contacte dispose d'une autorisation de l'Autorité des marchés financiers.

8 LE PHISHING OU HAMEÇONNAGE

Cette technique vise à tromper l'utilisateur pour récupérer ses informations personnelles, professionnelles ou bancaires. Les arnaqueurs appellent ou adressent un mail ou un SMS à leurs victimes en se faisant passer pour leur opérateur mobile ou leur banque. Un rappel : **ne communiquez pas d'informations sensibles par message ou au téléphone.** S'il vous est demandé de délivrer vos renseignements par internet, ne cliquez pas sur le lien ou vérifiez son URL à la lettre près.

9 LE CHANTAGE À LA WEBCAM

Cette arnaque fait croire à l'utilisateur que ses webcams ont été piratées. L'arnaqueur contacte sa victime par mail dans la plupart des cas, en **se présentant comme un hacker en possession de vidéos compromettantes** de lui. Il somme alors son interlocuteur de lui verser de l'argent en coupon PCS ou en cryptomonnaies, sans quoi il enverra tout à son entreprise et sa famille ou postera les images sur internet. Pour éviter de vous retrouver dans ce genre de situations, utilisez des mots de passe différents pour chaque compte, évitez les sites peu sûrs et n'ouvrez pas les pièces jointes à des messages suspects. Et surtout, ne cédez pas à ce faux chantage.

10 LES OFFRES DE CASHBACK

Vous venez d'effectuer un achat sur un site comme Fnac.com ou Darty.com, lorsqu'une une fenêtre avec la même charte graphique vous propose de « continuer » pour bénéficier de 10 à 20 euros de réduction sur votre facture et vos prochaines emplettes. Intéressé, vous acceptez sans prêter attention aux minuscules mentions stipulant qu'il ne s'agit pas d'une offre du site, mais d'un « partenaire ». Résultat ? **Vous vous retrouvez prélevé directement sur votre compte bancaire** par ce service à hauteur d'une quinzaine d'euros par mois. Pour éviter de vous faire avoir, ouvrez l'œil, car cette pratique n'est pas illégale même si elle peut vous paraître moralement répréhensible.●