Guide de survie aux arnaques

Si c'est trop beau, y a un loup !

L'arnaque	La parade
1. Vous recevez une proposition d'investissement « exclusive » trop alléchante, d'un tiers que vous ne connaissez pas.	Ne répondez pas, consultez éventuellement votre banque. Attention ! Chercher sur Internet peut vous permettre d'identifier une escroquerie, mais aussi de tomber sur des sites laudateurs montés par les malfaiteurs. Exercez votre esprit critique.
2. Par téléphone, SMS ou via des réseaux sociaux, des parents ou amis en détresse sollicitent le versement urgent d'une somme d'argent. Souvent, ils vous informent qu'ils ont changé de n° de téléphone ou d'adresse de courriel.	Contactez le parent ou ami sur son « ancien numéro » ou via son courriel habituel pour vérifier l'appel Soyez attentif à tous les signes ou tournures de phrase inhabituels. Posez des questions dont seul votre vrai correspondant connaît la réponse. Ne vous laissez pas envahir par le sentiment d'urgence que votre correspondant tente de vous communiquer. Attention ! Avec l'AI, il est possible de simuler une vidéo ou un ton de voix. Cette arnaque est en plein développement. Toute demande d'argent doit vous alerter.
3. Les codes QR sont populaires. Des escrocs collent des codes QR malveillants sur des affiches, des documents, des parcmètres, ou tout autre support dans un espace public.	Vérifiez toujours sur quelle adresse internet ces codes vous envoient. En particulier si ces sites vous proposent un formulaire vous demandant des données d'identification ou bancaires. Stoppez alors la connexion. Attention ! si le code QR se trouve sur un papillon collé sur un document d'aspect authentique, redoublez de vigilance.

4. Des escrocs ouvrent de faux sites de vente, généralement à des prix attractifs, vous promettant de livrer un produit, payable via carte bancaire.	Tenez-vous en à des sites connus (en faisant attention au code pays final de l'adresse). Vérifiez le site sur Trustpilot ou Signal-Arnaques. Pour limiter votre risque, utilisez une carte bancaire avec protection d'achat demandant une validation via itsme ou tout autre système reconnu. Attention ! le faux site web peut être convaincant par sa qualité apparente.
5. Quelqu'un vous contacte par téléphone ou même par courrier postal pour - Vous informer que vous bénéficiez d'un héritage - Vous avez gagné à une loterie - Vous allez être livré d'un produit gratuit. - Vous avez droit à une subvention ou à une aide d'Etat Mais bien sûr, pour bénéficier de tout cela, il y a des frais de dossier à payer d'emblée.	Ne payez jamais pour quelque chose que vous n'avez pas demandé. Attention ! un héritage passera obligatoirement par un notaire.
6. Vous recevez une facture qui vous paraît authentique mais qui ne précise pas correctement ce qui vous est facturé ou qui vous informe que le compte bancaire du fournisseur a changé. La facture peut prendre la forme d'une facture de rappel pour des dettes imaginaires.	Vérifiez auprès du fournisseur, par un appel que vous initiez, que le changement de compte bancaire est réel. Ne tenez pas compte d'un appel que vous recevez. Ne payez pas une facture dont l'objet n'est pas clair et qui ne correspond pas à ce que vous avez commandé.
7. Quelqu'un vous contacte par téléphone ou même par courrier postal pour vous informer que votre ordinateur a été piraté ou est compromis. On vous propose de corriger cela soit en téléchargeant un logiciel, soit en vous guidant pour modifier vos paramètres système.	Rompez aussitôt le contact. Ne faites aucun changement dans vos paramètres. Si besoin est, rompez votre connexion wi-fi Attention ! Ni Microsoft ni Apple ne vous appelleront directement
8. Quelqu'un se présente à votre domicile pour procéder à l'échange de votre carte bancaire. Il vous demande votre code PIN.	Appelez la police. Ne donnez jamais ni votre carte, ni votre code. Attention ! Eventuellement, faites tout de suite opposition à votre carte via card stop.
9. Quelqu'un vous appelle en se prétendant de votre banque et sous le prétexte de confirmer votre identité, vous questionne sur vos données personnelles et bancaires.	Ne répondez pas, informez votre correspondant que vous allez rappeler votre chargé de relations bancaires et ne répondez à de telles questions que si vous avez initié l'appel à un numéro connu d'avance. Attention ! N'utilisez en aucun cas un numéro de téléphone donné par un inconnu pour valider quoi que ce soit.

10. Quelqu'un va jouer sur vos bons sentiments en vous parlant du cas tragique d'un enfant qui a besoin de votre aide pour avoir des médicaments ou qui doit payer un voyage pour être opéré.	Rompez aussitôt le contact. Vous pouvez faire un don à une action caritative connue. Mais il n'y a aucune chance qu'un tel appel soit légitime. Attention ! Cette demande peut être précédée de contacts visant à établir un lien sentimental avant la demande d'argent.
11. Quelqu'un va jouer sur vos mauvais sentiments en vous proposant contre rémunération de blanchir une somme d'argent.	Ne laissez personne utiliser votre compte bancaire comme véhicule pour ses opérations financières propres. Attention ! A la fin, le seul pleinement identifiable dans cette chaine financière, c'est vous, qui devrez répondre à la justice du crime de blanchiment, possiblement aggravé.

Lire aussi

Les principales arnaques en fiches pratiques | SPF Economie

Victime d'une arnaque ? Que faire ? | SPF Economie

06/07/2025