FEMME ACTUELLE – Comment déjouer les arnaques sur Internet ?

Arnaques : attention à ces 6 mails frauduleux les plus fréquents.

Article de Anissa Nassr

Arnaques : attention à ces 6 mails frauduleux les plus fréquents© Kwanchanok Taen-on / iStock

Certaines arnaques fonctionnent mieux que d'autres, et les escrocs l'ont bien compris. Femme Actuelle a recensé six mails frauduleux les plus utilisés. Ne vous faites plus avoir.

Les malfrats sont toujours aussi nombreux à ressortir leurs bonnes vieilles méthodes pour vous amadouer et vous soutirer de l'argent. Alors, si vous recevez un de ces six mails, prenez garde ! Il s'agit probablement d'une arnaque. On fait le point.

Comment déjouer les arnaques sur Internet ?

L'arnaque à la vignette Crit'Air

La mécanique : vous recevez un mail qui vous rappelle que votre véhicule n'est pas muni de la vignette Crit'Air 2023 et qu'à ce titre, vous risquez une amende si vous ne la récupérez pas au plus vite. La victime est alors invitée à cliquer sur un lien pour se procurer le précieux sésame. Un lien évidemment frauduleux. C'est ce que l'on appelle du **phishing, hameçonnage en français**.

Le bon réflexe : comme le rappelle le site du gouvernement, aucun mail n'est envoyé aux usagers pour acheter des vignettes. Pour rappel, pour obtenir le précieux sésame, **il faut débourser 3,70 € (prix de la vignette + prix de l'affranchissement)**, selon le tarif en vigueur au 1er juillet 2022. En cas de doute, vous pouvez toujours demander conseil auprès du Service de délivrance du certificat qualité de l'air par téléphone au 0800.97.00.33 (du lundi au vendredi de 9 à 17 heures, appel gratuit depuis un téléphone fixe).

L'arnaque au paiement PayPal

La mécanique : si vous recevez un mail vous disant que vous avez reçu une importante somme d'argent et vous indiquant de cliquer sur le lien pour la récupérer, vous êtes sans doute la cible de phishing, **ne cliquez pas sur ces liens**.

Le bon réflexe : vérifiez l'adresse de l'expéditeur de ce message en vous assurant qu'il provient bien des services de PayPal. Dans le doute, connectez-vous à votre compte PayPal en passant directement par votre navigateur internet (donc sans cliquer sur le lien), une fois connecté à votre compte vous pourrez en surveiller l'activité et voir si le message reçu était vrai ou pas.

L'arnaque à la connexion inhabituelle

La mécanique : vous avez reçu un mail vous alertant sur une *"connexion inhabituelle"* sur votre boîte mail Hotmail, Live ou encore Outlook ? Attention, il s'agit peut-être d'une arnaque. Ces dernières semaines, de nombreux utilisateurs auraient reçu un faux courriel semblant provenir de l'équipe des comptes Microsoft. Il s'agit là d'une tentative de phishing visant à récupérer les identifiants et mots de passe de votre boîte mail et ainsi dérober toutes vos données personnelles.

Le bon réflexe : les véritables alertes de connexion inhabituelles sont toujours envoyées par des adresses se terminant par *"@accountprotection.microsoft.com"*. Si ce n'est pas le cas, il s'agit d'un message frauduleux à ignorer. Les faux courriels de ce type sont aussi souvent truffés de fautes d'orthographe voire de syntaxe. Si vous avez l'œil, vous pouvez tenter de les repérer.

"Quelqu'un qui me connaissait a voulu me faire du mal" : retrouvez le témoignage d'Aurelie, victime d'une usurpation d'identité.

L'arnaque sur votre facture d'électricité

La mécanique : les escrocs surfent sur les préoccupations des Français pour les duper et dérober leurs données personnelles voire leurs coordonnées bancaires. À l'heure de la sobriété énergétique et de l'augmentation du prix de l'énergie, ils n'hésitent pas à usurper l'identité d'Engie, d'EDF ou encore des institutions publiques pour vous proposer des bons de réduction, des remises ou encore des avoirs exceptionnels… et vous piéger !

Le bon réflexe : méfiez-vous des promesses trop alléchantes… Gardez bien en tête que vos coordonnées bancaires ne vous seront jamais demandées par courriel par les institutions publiques et les grandes entreprises. Pour vous assurer une protection forte et éviter les piratages, mieux vaut également activer la double authentification sur votre boîte mail.

L'arnaque à la livraison Chronopost

La mécanique : la plateforme de livraison Chronopost vous informe par mail qu'un problème est survenu lors de l'envoi d'un colis. Pour confirmer votre adresse, vous devez alors cliquer sur un lien qui renvoie vers un site imitant à la perfection celui de l'entreprise. Vos coordonnées personnelles sont alors demandées afin de reprogrammer la livraison. Très mauvaise idée : en réalité, vous risquez surtout de vous faire voler vos données personnelles et bancaires.

Le bon réflexe : si le mail provient de la plateforme, il sera forcément envoyé par l'une de ces adresses mail : ne-pas-repondre@chronopost.fr, enquetesatisfaction@chronopost.fr, noreply.chronopost@myviseo.com, livraison.chronopost@network.pickup.fr, avisage-ne-pas-repondre@chronopost.fr, chronopost@e-facture.net et chronopost.fr@infosae.docapost-dps.com. Si vous recevez un courriel venant d'un autre expéditeur, passez votre chemin ! Aussi, l'URL du site internet doit indiquer www.chronopost.fr et non une autre adresse. Attention, parfois une petite lettre en plus peut être dissimulée dans l'URL pour vous induire en erreur.

L'arnaque à la fausse convocation à la police

La mécanique : un mail vous informe que vous faites l'objet d'une enquête pour *"avoir visualisé des vidéos à caractère pédopornographiques, des photos/vidéos dénudées de mineur"* et que vous êtes, à ce titre, invité à comparaître devant un tribunal. Bien que ce courriel soit (très) effrayant, il n'a bien évidemment rien de vrai. Il s'agit encore une fois d'une opération d'hameçonnage visant à récolter vos données, voire vous extorquer des sous.

Le bon réflexe : si vous êtes concerné par une enquête, les gendarmes ou les policiers se présenteront à votre domicile pour vous en informer (et non par mail). Sachez aussi que les instances officielles ne vous réclameront aucun règlement en ligne. Seules les contraventions liées aux infractions au Code de la route peuvent être payées de cette façon. Enfin, les mails officiels de la gendarmerie nationale se terminent toujours par *"gendarmerie.interieur.gouv.fr"*. Si vous recevez un courriel provenant d'un autre expéditeur, direction… la corbeille !