Outil

Réagir face aux arnaques et les détecter

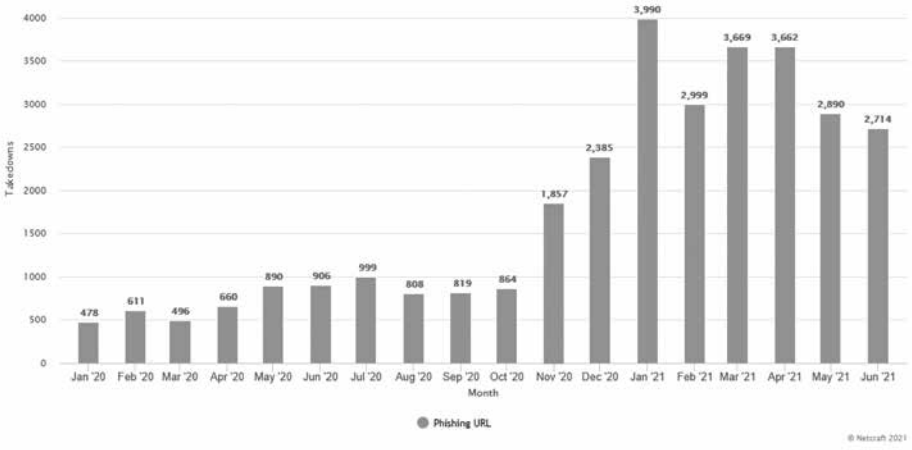
Le nombre d'arnaques en tous genres s'est multiplié sur fond de crise Covid, ainsi que ses conséquences économiques et sociales. 2021 a été une année record en termes de signalements. Face à cette problématique, l'Observatoire du crédit et de l'endettement a invité des experts à prendre la parole durant cinq webinaires pour prévenir ces arnaques et informer le public cible et les professionnels relais. Retour sur ces webinaires.

Appelées hameçonnages (*phishing*), mules financières, fausses agences de recouvrement, faux crédits, fraudes aux sentiments ou encore fraudes à l'investissement, les arnaques[1] peuvent prendre de multiples apparences, mais ont un point commun: tromper leurs victimes dans l'unique but de leur dérober de l'argent. La Toile est devenue le terrain de jeu favori des arnaqueurs, qui se renouvellent constamment.

Le nombre de signalements s'accroît d'année en année. On constate par exemple une augmentation significative des tentatives de phishing depuis novembre 2020 et, rien qu'en 2021, plus de 3,7 millions de messages suspects (pour une moyenne de 12.000 plaintes quotidiennes) ont été signalés à l'adresse suspect@safeonweb.be. Autre exemple: en matière de fraude aux sentiments, dans le cadre de rencontres à distance, le nombre de victimes a presque doublé durant la crise Covid, passant de 718 cas en 2019 à 1.317 en 2020.

Types d'arnaques

Face à ces chiffres, il est essentiel d'informer et d'outiller les personnes relais afin qu'elles puissent guider les victimes d'arnaques.



Croissance significative du (des tentatives de) phishing depuis novembre 2020

Les arnaques pouvant prendre de multiples formes, nous les avons réparties en cinq catégories: les fraudes à l'investissement et au crédit (les prêteurs frauduleux, les fraudes au crédit…); les fraudes à la banque en ligne (hameçonnages, mules financières…); les ventes frauduleuses et publicités trompeuses (les produits gratuits conditionnés à des abonnements, les voyages offerts…); les fraudes à l'identité (faux bureaux de recouvrement, boutiques en ligne…) et les fraudes à l'émotion (lettres nigérianes ou fraude 419, fraude sur les réseaux sociaux…).

L'OCE a organisé une série de cinq webinaires[2] durant le dernier trimestre de l'année 2021. Les webinaires ont été suivis par près de 550 participants, venus écouter les conseils de spécialistes du secteur provenant notamment de l'AB-REOC, de l'asbl Neniu, du CEC Belgique, de Febelfin, de la FSMA ou du SPF Économie qui réalise des campagnes de sensibilisation sur le sujet.

Quels conseils pour reconnaître et éviter les arnaques?

- «Échantillon gratuit», «cadeau offert», «gain d'argent facile» ou encore «logement de vacances luxueux à petit prix»: ces offres ne sont-elles pas «trop belles pour être vraies»? Si c'est le cas, il est plus prudent de refuser, car il s'agit très probablement d'une arnaque!
- Toujours vérifier l'identité de l'interlocuteur avant de finaliser toute transaction. L'adresse postale est-elle bien mentionnée? L'adresse e-mail correspond-elle bien à ladite société? L'entreprise existe-t-elle réellement? Le site internet semble-t-il suffisamment professionnel et existe-t-il depuis un certain temps? Le site permet-il d'effectuer des transactions bancaires sécurisées? Trouver des réponses à ces questions est déjà un gage de sécurité sur le Net.
- Vérifier la réputation du vendeur ou de l'interlocuteur. Le vendeur est-il digne de confiance? Les produits sont-ils satisfaisants? Les produits arrivent-ils à destination? Que pensent les clients des produits reçus? De nombreuses sociétés publient directement des avis d'utilisateurs sur leur site internet. Ne pas se fier à ces évaluations, mais

1 *Ces différentes arnaques sont présentées dans la brochure consacrée aux arnaques de l'Observatoire disponible sur son site internet http://www.observatoire-credit.be*

2 *Thématiques des différents webinaires:*
1er webinaire: Les ventes frauduleuses et autres publicités trompeuses
2e webinaire: Les arnaques à la consommation liées aux bureaux de recouvrement frauduleux
3e webinaire: Les offres d'investissement et de crédit
4e webinaire: La sécurité des données bancaires: hameçonnage et mule financière
5e webinaire: Les fraudes aux sentiments.

plutôt effectuer une recherche externe via un moteur de recherche afin de trouver des avis provenant de sources différentes et variées.

- Prendre le temps de la réflexion et lire le contrat et les conditions générales des offres, en étant particulièrement attentifs aux inscriptions en petits caractères. Il arrive parfois que l'on découvre dans ces conditions générales que le cadeau promis n'est offert qu'en accompagnement d'un abonnement annuel, par exemple.
- Vérifier que les informations sont suffisamment détaillées. Toute entreprise pratiquant la vente de biens ou de services doit clairement s'identifier, présenter les caractéristiques de son offre et permettre aux consommateurs d'appliquer leur droit de rétractation. Ne pas hésiter à demander des précisions aux vendeurs. Il est plus prudent de mettre fin à la transaction si le vendeur ne peut pas donner de précisions complémentaires.
- Ne JAMAIS communiquer par téléphone des informations telles que mots de passe, codes PIN ou réponses de DIGIPASS. Ces informations doivent absolument rester strictement confidentielles! Si ces données ont été communiquées à des tiers, il est nécessaire de bloquer les moyens de paiement en contactant Card Stop (078/170.170).
- Privilégier les paiements par carte de crédit ou via PayPal lors des achats sur le Net. Ces moyens de paiement permettent d'effectuer des transactions davantage sécurisées et garantissent une protection sur les achats en cas de fraude, si le bien n'est jamais réceptionné ou s'il ne correspond pas à la description du vendeur.
- Prendre du recul et s'interroger par rapport aux offres avant de prendre toute décision. Les fraudeurs ont tendance à créer l'urgence auprès de leurs potentielles victimes pour les amener à agir rapidement sans prendre le temps de réfléchir. Les décisions prises hâtivement sont rarement les meilleures.

Victime d'une arnaque ? Comment réagir ?

Aujourd'hui, les arnaques sont tellement bien ficelées qu'il est souvent compliqué de découvrir l'identité réelle des fraudeurs et d'obtenir justice. Il reste peu de marge de manœuvre aux victimes, mais il est important d'agir.

Des paiements ont-ils été effectués ? Des informations bancaires confidentielles ont-elles été dérobées ? Les victimes peuvent contacter Card Stop pour bloquer les moyens de paiement (cartes, applications ou objets connectés) concernés. Si les paiements ont été débités avec des cartes de crédit ou de paiement Visa ou Mastercard, il est possible d'introduire une demande de contestation sur le site macarte.be afin de tenter de récupérer les montants (si les transactions ont été effectuées dans un délai inférieur à trois mois).

Les consommateurs ou entreprises dont les droits n'ont pas été respectés ou les victimes de fraudes, de tromperies, d'arnaques et d'escroqueries peuvent signaler leur problème au Point de contact Belgique du SPF Économie (https://pointdecontact.belgique.be/meldpunt/fr/bienvenue). Après analyse des plaintes, le Point de contact donne un avis sur les recours possibles et communique les signalements aux services compétents. S'il s'agit d'un litige impliquant une société dont le siège se situe dans un autre pays européen, le litige peut également être dénoncé sur le site du CEC Belgique (https://www.cecbelgique.be/complaint-wizard-page). Les e-mails, SMS et sites suspects peuvent être transmis à l'adresse suspect@safeonweb.be pour éviter que les fraudeurs fassent d'autres victimes.

Même s'il y a peu de chance que le dossier aboutisse, les victimes sont invitées à déposer une plainte auprès du bureau de police locale. Attention de bien veiller à communiquer tous les éléments possibles tels que les numéros de compte et de téléphone utilisés par le fraudeur, les en-têtes d'e-mails, les sites internet, les pseudonymes, les photos et les comptes utilisés. Toutes ces informations permettront à la police d'enquêter de manière optimale.

Aurélie Jourdain,
chargée de recherche en prévention à l'Observatoire du crédit et de l'endettement

Pour re(visionner) les webinaires, rendez-vous sur https://observatoire-credit.be/fr/nos-evenements.

Quelques outils disponibles

L'Observatoire a compilé les principaux conseils des experts ayant participé aux différents webinaires dans une brochure. Elle reprend des conseils généraux, quelques arnaques les plus courantes et conseille les victimes sur les actions à mettre en place. Une partie est également consacrée aux outils et aux sites internet utiles. Cette brochure est disponible sur le site de l'Observatoire: http://www.observatoire-credit.be.

Le CEC Belgique propose sur son site internet le «Webshop Check», afin de vérifier la fiabilité d'un site de vente en ligne avant de passer commande (https://bit.ly/3NaI0zQ). La FSMA propose aux consommateurs de répondre aux questions du test «Suis-je victime d'une arnaque ?» afin de vérifier la fiabilité d'une offre d'investissement (https://www.fsma.be/fr/attention-aux-fraudes).

Le Centre pour la cybersécurité et Febelfin ont mis en place l'application Safeonweb (https://www.safeonweb.be/en/safeonweb-app) permettant de rester informé de manière simple et rapide sur les cybermenaces et les escroqueries en ligne. Safeonweb propose également de nombreux conseils sur son site internet https://www.safeonweb.be/.