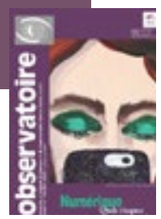

©Article paru dans l'Observatoire n° 110, avril 2022
Infos & commandes : www.revueobservatoire.be

Arnaque, ma belle arnaque, dis-nous qui tu es!

Aurélie JOURDAIN

Chargée de recherche en prévention à l'Observatoire du Crédit et de l'Endettement

a_jourdain@observatoire-credit.be

http://www.observatoire-credit.be

PHISHING, FAUX CRÉDITS, VENTES FRAUDULEUSES, PIÈGES AUX ABONNEMENTS, MULES FINANCIÈRES… LES ARNAQUES SUR LE NET NE CESSENT DE SE RENOUVELER ET DE SE MULTIPLIER. L'ESCROQUERIE EN LIGNE PEUT TOUCHER TOUT LE MONDE, AVEC DES CONSÉQUENCES PSYCHOLOGIQUES ET SOCIALES IMPORTANTES (PERTE DE CONFIANCE EN SOI, ISOLEMENT, CULPABILITÉ, ENDETTEMENT, ETC.). CEPENDANT, LES PERSONNES PLUS FRAGILES AU DÉPART SONT DES CIBLES PLUS VULNÉRABLES, ET DONC PLUS FACILES À GRUGER. COMMENT APPRÉHENDER CE PHÉNOMÈNE? QUI SONT SES VICTIMES? COMMENT RÉAGIR? PROFILS ET DESCRIPTION DE PIÈGES BIEN FICELÉS.

Mots-clés: arnaques, phishing, mule financière, pièges, endettement

Caché derrière un ordinateur, travaillant seul ou en réseau, l'arnaqueur a un profil aux multiples facettes. Ami, confident, prêteur ou vendeur, l'arnaqueur traque ses victimes sur la toile. Derrière son apparente bienveillance, son objectif est de dérober d'importantes sommes d'argent par l'intermédiaire de «pièges» appelés arnaques. Ces arnaques peuvent prendre de multiples formes que nous pouvons répartir en plusieurs catégories[1].

Les différentes formes d'arnaques en ligne

Une première catégorie concerne les fraudes à l'investissement et au crédit. Dans ce type de fraudes, les victimes investissent une certaine somme d'argent dans l'espoir de voir leur capital fructifier rapidement ou de recevoir un prêt qu'elles n'osaient plus espérer. Une fois la confiance installée et l'argent versé, les arnaqueurs disparaissent en laissant leurs victimes démunies. Ce type de fraudes est d'autant plus pervers qu'il touche des personnes ayant parfois de faibles moyens financiers. Si on prend, par exemple, le cas des victimes de fraude au crédit, il s'agit souvent de personnes dont le budget ne permet pas de contracter un prêt via un organisme bancaire classique. L'offre de crédit proposée, via divers réseaux, leur semble être une aubaine jusqu'à ce que le prêteur leur demande de payer certains frais (pour couvrir une assurance ou l'ouverture du dossier, par exemple) et se volatilise avec leur argent par la suite. N'ayant aucun scrupule, il arrive également que des arnaqueurs contactent les victimes pour leur proposer leur aide afin de récupérer les sommes investies moyennant une contribution financière[2]. Qui se fait arnaquer une fois ne devrait pas se faire arnaquer une seconde fois! Et pourtant, cela arrive!

La deuxième catégorie de fraudes concerne le *phishing*[3], le *smishing*[4] et les mules financières. Une personne reçoit, par exemple, un message semblant provenir du gouvernement promettant une intervention de 135€ sur sa facture de gaz et d'électricité. Le message est assez court et invite à cliquer sur un lien pour connaître les formalités administratives. En cliquant sur ce lien, la personne est dirigée vers un site internet sur lequel elle doit encoder ses informations bancaires pour recevoir la prime promise. L'arnaqueur dispose alors de toutes les informations nécessaires pour vider le compte de la personne. Face à ce vol, les victimes vont déposer plainte en donnant le numéro de compte sur lequel leur argent a été versé et espèrent alors retrouver le coupable, mais le piège est bien rodé et l'arnaqueur n'a évidemment pas transféré l'argent sur son compte personnel. Il a fait appel à une mule financière, c'est-à-dire une personne qui permet l'utilisation de son compte bancaire et/ou de sa carte bancaire et de son code PIN par des criminels à des fins de blanchiment d'argent. En contrepartie, la mule perçoit rapidement une somme d'argent. Celle-ci est alors tenue responsable par la justice (et devient également une victime) tandis que l'arnaqueur garde son anonymat.

La troisième catégorie d'arnaques concerne l'e-commerce[5] et plus spécifiquement les ventes frauduleuses et autres publicités trompeuses. «Echantillon gratuit», «cadeau», «voyage offert»… ces offres semblent intéressantes, mais à quel prix? En se laissant tenter, les personnes contractent parfois sans s'en rendre compte des abonnements annuels pour des produits ou des services alors qu'elles souhaitent en réalité uniquement bénéficier de l'offre proposée. Autre exemple aux conséquences plus problématiques: les arnaques sur les plateformes de vente et de location. Une personne trouve une annonce pour un logement de vacances sur une plateforme renommée. Belle villa luxueuse en bord de plage avec piscine, au calme, à prix modique: tous les ingrédients sont présents pour commencer à rêver. Au moment de procéder au paiement, le propriétaire propose de finaliser la transaction hors de la plateforme en évoquant quelques soucis techniques. Craignant de passer à côté de cette opportunité, la personne accepte et paie par virement bancaire. La transaction est alors conclue et la personne reçoit une confirmation de sa réservation via un mail semblant provenir de la plateforme. Toutefois, arrivée sur son lieu de vacances, la personne constate que l'annonce était une arnaque et que le logement n'existe pas.

La quatrième catégorie concerne les fraudes à l'identité. Faux banquiers, fausses sociétés de recouvrement, faux vendeurs, les usurpations d'identité sont très courantes et de plus en plus «professionnelles». Une personne reçoit, par exemple, un mail provenant d'une société de recouvrement de dettes située aux Pays-Bas. Ce mail explique dans un français approximatif qu'un abonnement contracté quelques mois auparavant n'a pas été payé et que, conformément aux conditions générales, le créancier a fait appel à une société de recouvrement de dettes pour tenter de récupérer sa créance avant d'entamer une procédure judiciaire. Dans le mail, la société de recouvrement insiste également sur le caractère urgent de sa demande de paiement sur le compte bancaire mentionné. La personne, mise sous pression, effectue rapidement le paiement exigé sans savoir de quel abonnement il s'agit et sans se rendre compte qu'il ne s'agit pas d'une véritable société de recouvrement mais plutôt d'un escroc caché derrière une fausse identité.

Enfin, la cinquième et dernière catégorie d'arnaques concerne ce que l'on peut appeler les fraudes à l'émotion: un mail d'appel à l'aide d'un ami en vacances à l'étranger, une rencontre amoureuse sur un site internet ou sur les réseaux sociaux… Nous retrouvons dans cette catégorie de fraude, les «meilleures» techniques de manipulation. Les escrocs jouent sur notre désir d'amour et d'amitié. Le profil des victimes est souvent étudié par les arnaqueurs: des personnes seules, isolées, venant de vivre une situation difficile (comme la perte d'un proche, une séparation ou la perte d'un emploi), étant psychologiquement plus fragiles et, par conséquent, plus vulnérables à la manipulation. Une fois les potentielles victimes choisies, les escrocs vont travailler selon des scripts bien structurés. Lors des premières prises de contact, l'arnaqueur va très vite créer une proximité affective avec la personne en échangeant sur sa vie et en se trouvant de nombreux points communs avec elle. Le profil de l'arnaqueur est étudié afin de paraître crédible aux yeux de sa victime. Une confiance s'installe dans la relation et l'arnaqueur échange quotidiennement avec sa victime pendant plusieurs mois. Soudainement, l'arnaqueur disparaît, laissant la personne seule. Lorsque l'arnaqueur réapparaît, il justifie son absence par une situation urgente nécessitant une intervention financière. La victime, confiante, n'ose pas refuser son aide. Cette situation se répète jusqu'à ce que la victime ne soit plus en mesure d'envoyer de l'argent et que l'arnaqueur mette alors fin à la relation.

Quelques chiffres

Le nombre de signalements d'agissements d'arnaqueurs sur la toile accroît d'année en année et la crise sanitaire a entrainé une recrudescence du nombre d'arnaques. On constate, par exemple, que le nombre de tentatives de *phishing* est deux fois plus élevé en 2020 (3.225.234 messages) qu'en 2019 (1.7 million). Ces chiffres ont continué d'augmenter en 2021 où plus de 3,7 millions de messages suspects ont été signalés à l'adresse mail du Centre pour la Cybersécurité Belgique (CCB) destinée à recevoir les messages suspects transmis par les citoyens[6]. En 2021, le centre a reçu en moyenne 12.000 plaintes quotidiennes. Le CCB constate régulièrement des vagues de tentatives de *phishing* en lien avec l'actualité. Par exemple, durant la pandémie, de nombreux messages

1. Cette catégorisation a été réalisée dans le cadre de l'organisation de webinaires consacrés à la prévention des arnaques. Ces webinaires peuvent être visionnés sur le site internet de l'Observatoire: https://observatoire-credit.be/fr/nos-evenements

2. Ce type de fraudes est appelé «recovery room».

3. En français: hameçonnage.

4. Forme de *phishing* par sms.

5. En 2021, 11,7 milliards d'euros ont été dépensés en ligne en Belgique. Sources: Communiqué de presse: Le commerce en ligne belge - Safeshops

6. suspect@safeonweb.be

concernaient le coronavirus: fausses offres pour des masques de protection, des gels hydroalcooliques, une indemnisation corona à demander au SPF Finances ou encore une fausse invitation pour la vaccination. Début 2022, c'est une vague de tentatives de *phishing* concernant une prime à l'électricité qui est apparue.

La crise Covid a également entraîné une importante augmentation en matière de fraudes aux sentiments durant laquelle le nombre de victimes a presque doublé. Durant le confinement, de nombreuses personnes se sont en effet retrouvées isolées et ont essayé de tisser des liens sociaux via Internet. Alors que le SPF Economie recensait 382 cas en 2018, le nombre de victimes s'étant manifestées est ainsi passé de 718 en 2019 à 1.317 en 2020[7] et ce n'est probablement que la face visible de l'iceberg.

Profil des victimes

Tout le monde peut être victime d'une arnaque, quel que soit son âge ou sa situation socioprofessionnelle. Même si l'entourage des victimes a souvent tendance à juger celles-ci comme étant trop naïves ou peu alertes, les arnaques sont tellement bien ficelées que tout un chacun peut en être victime. Il n'est nullement question d'intelligence ou de bon sens.

Toutefois, certaines arnaques ont tendance à cibler des profils plus spécifiques. Les seniors, par exemple, a priori susceptibles d'avoir davantage de moyens financiers et d'avoir constitué une épargne, sont en effet une cible privilégiée par les arnaqueurs en matière de fraudes aux sentiments. Leurs victimes sont généralement sélectionnées via trois canaux principaux: les applications de rencontre, les réseaux sociaux et les sites d'annonces de décès. Les victimes recrutées via des applications de rencontre sont des personnes souvent isolées, à la recherche d'attention et d'amour comme le démontre le documentaire «L'arnaqueur de Tinder»[8]. Les personnes veuves repérées via des sites d'annonces de décès sont davantage à la recherche d'amitié et de soutien. Sur les réseaux sociaux, les arnaqueurs vont davantage cibler des forums et groupes relatifs à des séries ou des chanteurs par exemple, en se faisant passer pour ceux-ci.

Les jeunes sont quant à eux une cible privilégiée par les recruteurs de mules financières. D'après une enquête de Febelfin[9] réalisée en 2021, 6% des jeunes interrogés, âgés entre 16 et 30 ans, ont déjà été approchés personnellement pour faire office de mules. 14% de ces jeunes seraient par ailleurs disposés à prêter leur carte bancaire et leur code PIN en échange d'argent alors qu'ils étaient 10% en 2019. 19% d'entre eux en ignorent les conséquences juridiques.

Des conséquences psychologiques et sociales

De manière générale, les victimes d'arnaque ont besoin de parler mais craignent d'être jugées par leur entourage. Prenons l'exemple des victimes des fraudes aux sentiments. Enfermées dans une relation exclusivement virtuelle, elles communiquent au quotidien avec leurs arnaqueurs. Des sentiments naissent. Manipulées, les victimes gardent leurs relations secrètes et ont tendance à s'isoler socialement. Lorsqu'elles ne sont plus en mesure d'envoyer de l'argent, les arnaqueurs disparaissent et les personnes se retrouvent seules. Elles se sentent trahies. Elles ont souvent envoyé d'importantes sommes d'argent et ont parfois même contracté des crédits. Les victimes éprouvent alors un sentiment de honte et n'osent pas parler de leurs difficultés financières à leur entourage. Elles perdent également toute confiance en elles et aux autres et craignent d'être à nouveau trompées.

L'asbl Neniu[10] aide par exemple ces victimes en leur offrant une écoute active et les guide dans la prise de conscience du mécanisme dont elles ont été victimes afin de les aider à faire leur deuil.

Quelques conseils

Attention aux informations transmises!

Les informations publiées sur les réseaux sociaux ou transmises sur des sites internet demandent une certaine réflexion. Une séparation, un voyage, un accident, une rencontre, un nouvel emploi, un mariage… nos profils sur les réseaux sociaux reflètent souvent les bons comme les mauvais événements de nos vies, mais il est important de ne pas partager ces informations avec n'importe qui. Photos, goûts musicaux, centres d'intérêt, lieux fréquentés, pages aimées: les arnaqueurs prennent le temps d'étudier les profils dans les moindres détails afin de toucher le plus justement possible leur cible.

Garder les yeux ouverts!

Un lien redirige vers un site internet sur lequel nous sommes invités à communiquer nos informations bancaires? Il s'agit certainement d'une tentative de *phishing*! Ces informations doivent absolument rester confidentielles et ne jamais être communiquées!

«Echantillon offert», «cadeau», «gain d'argent facile»... Ces offres ne sont-elles pas trop belles pour être vraies? Si c'est le cas, il faut mettre fin à la transaction, car il s'agit très probablement d'arnaques! Les produits sont-ils satisfaisants? Les produits arrivent-t-il à destination? N'oublions pas de vérifier la réputation du vendeur ou de l'interlocuteur en effectuant une recherche via un moteur de recherche afin de trouver des avis provenant de sources différentes et variées.

Le vendeur est-il bien identifiable? L'adresse postale est-elle mentionnée? L'adresse mail correspond-t-elle bien à ladite société? L'entreprise existe-elle réellement? L'identité du vendeur ou de l'interlocuteur doit aussi être vérifiée avant de finaliser toute transaction.

Il arrive parfois que l'on découvre dans les conditions générales des offres que le cadeau promis n'est en réalité offert qu'en souscrivant un abonnement annuel par exemple. Pour éviter l'arnaque, le temps de réflexion et la lecture du contrat et des conditions générales ne doit pas être négligés, avec une attention particulière pour les inscriptions en petits caractères.

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 donc à demander des précisions au vendeur; sans réponse concluante de sa part, il faut mettre fin à la transaction.

Adopter un comportement prudent en ligne

Mots de passe, codes PIN ou réponses de DIGIPASS doivent absolument rester strictement confidentiels. Ne jamais communiquer ces informations par téléphone ou sur des sites Internet.

Les paiements réalisés par carte de crédit ou via PayPal permettent d'effectuer des transactions sécurisées. Ils garantissent également 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 donnée. Ces moyens de paiement sont toujours à privilégier pour les achats réalisés plutôt qu'un paiement par virement bancaire.

Les fraudeurs essaient souvent d'amener leurs victimes à agir très rapidement afin qu'elles n'aient pas de temps pour entamer une réflexion, chercher des avis ou demander conseil à leur entourage. Prendre du recul et s'interroger par rapport aux offres proposées est donc indispensable avant de prendre toute décision!

Victime d'une arnaque? Comment réagir?

Que l'on soit soi-même victime d'arnaques ou que l'on accompagne des personnes vulnérables en souffrance suite à une escroquerie en ligne, il est important de savoir comment réagir. Il est souvent compliqué de découvrir l'identité réelle des fraudeurs et de récupérer son argent, mais il est tout de même important d'agir. Voici comment:

Contacter Card Stop au 078/170.170 pour bloquer immédiatement les moyens de paiement concernés (cartes, applications ou objets connectés). Les paiements ont été effectués avec des cartes de crédit ou de paiement Visa ou Mastercard dans un délai inférieur à trois mois? Une demande de contestation doit être introduite sur le site http://www.macarte.be afin de tenter de récupérer les montants.

Signaler l'arnaque, la fraude ou la tromperie au Point de contact Belgique du SPF Economie sur le site https://pointdecontact.belgique.be/meldpunt/fr/bienvenue. Après analyse de la plainte, le point de contact donnera un avis sur les recours possibles et communiquera les signalements aux services compétents. 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 emails, SMS et sites suspects doivent également être transmis à l'adresse suspect@safeonweb.be afin que les fraudeurs ne puissent faire d'autres victimes.

Déposer plainte auprès du bureau de police local, en veillant bien à communiquer tous les éléments possibles tels que les numéros de compte et de téléphone utilisés par le fraudeur, les en-têtes email, les sites internet, les pseudonymes, les photos et les comptes utilisés. Toutes ces informations vont permettre à la police d'enquêter de manière optimale.

L'Observatoire du Crédit et de l'Endettement a organisé fin 2021 une série de webinaires consacrés à ces différentes arnaques. Vous pouvez retrouver ces webinaires sur le site internet http://www.observatoire-credit.be. L'Observatoire a également compilé les principaux conseils des experts ayant participé aux différents webinaires dans une brochure[11]. Cette brochure reprend les conseils généraux pour reconnaître et éviter les arnaques, explique en détails quelques arnaques les plus courantes et conseille les victimes sur les actions à mettre en place.

7. Derniers chiffres disponibles.

8. Documentaire disponible sur Netflix

9. https://www.febelfin.be/fr/communique-de-presse/mules-financieres-14-des-jeunes-dispose-e-s-preter-leur-carte-bancaire-pour-de

10. https://www.neniu-assos.org/

11. Cette brochure est disponible sur le site de l'Observatoire: http://www.observatoire-credit.be