BOOM DES ESCROQUERIES EN LIGNE: LES IDENTIFIER POUR ÉVITER LES PIÈGES

Covid-19 oblige, des millions de personnes se sont confinées durant de longues semaines. Internet et les réseaux sociaux sont devenus leurs seules fenêtres sur le monde. S'adaptant à cette nouvelle situation, les criminels ont eux aussi télétravaillé. Inventaire des escroqueries en ligne. TEXTE **SABINE PIROLT** ILLUSTRATION ORIGINALE DE **RAOUL GANTY**

Un cauchemar. L'escroquerie par Internet que décrit Quentin Rossy, professeur associé à l'École des sciences criminelles de l'Université de Lausanne, fait froid dans le dos. Elle n'a rien de fictif; c'est la police vaudoise qui lui a donné les détails de cette fraude aux faux supports techniques, mais sans préciser les chiffres.

Appelons-le Jean-Pierre. Ce Romand qui ne connaît pas grand-chose à l'informatique, panique lorsqu'il se rend compte que son ordinateur est bloqué. Sur son écran, un message estampillé Microsoft l'informe que le responsable de cette paralysie est un virus. Le message l'invite d'ailleurs à cliquer sur un lien. Jean-Pierre s'exécute et donne ses coordonnées. Rapidement, une personne sympathique l'appelle et le rassure: il va s'occuper de nettoyer son ordinateur. Mais pour ce faire, ce cyberzorro doit prendre le contrôle de sa machine. Confiant, Jean-Pierre obéit et permet l'installation d'un logiciel. Un certain temps s'écoule et l'informaticien lui annonce que tout est en ordre et qu'il faut le payer pour l'installation de ➡

EN LIGNE
Les fraudes ont suivi les développements technologiques.
© Raoul Ganty

GIULIA MARGAGLIOTTI ET QUENTIN ROSSY
Doctorante. Professeur associé. Tous deux à l'École des sciences criminelles (Faculté de droit, des sciences criminelles et d'administration publique).
Nicole Chuard © UNIL

➡ l'antivirus. Pourquoi ne pas le régler grâce au *e-banking* puisqu'il est devant son ordinateur? Soulagé d'avoir repris le contrôle de sa machine, Jean-Pierre obtempère: il entre son identifiant, son code et confirme encore son identité grâce à une application sur son *smartphone*, quand soudain, son cybersauveur change d'avis. En fait, il préfère des cartes cadeau iTunes. «Vous me donnerez le numéro de la carte et cela remplacera le paiement.» Quelle poisse, Jean-Pierre n'en a pas sous la main. Et s'il allait vite en acheter, lui suggère la voix sympathique? Jean-Pierre s'exécute, oubliant de refermer son accès *e-banking*.

On devine la suite, même si on peut légitimement faire preuve de scepticisme à l'écoute de cette édifiante mésaventure. Mais Quentin Rossy est formel: oui, il y a des gens qui se font avoir ainsi. «Ce sont des personnes vulnérables et les fraudeurs, qui ont du bagout, vont mettre leur interlocuteur en confiance. Ils vont peut-être même user d'autorité pour mettre la pression sur leur victime.»

Plus de peur que de mal

Si un tel cas ne se produit pas toutes les heures, l'ampleur du phénomène de la fraude ou de l'escroquerie en ligne ne fait plus aucun doute. Quentin Rossy: «La majorité des fraudes commises à l'encontre des personnes semble, maintenant, être liées à Internet. À l'instar des vols et des crimes contre le patrimoine dans l'espace physique, elles constituent la part majoritaire des crimes contre le patrimoine sériels et véhiculés par des espaces virtuels.»

De fait, selon l'Eurobaromètre de 2017, quelque 6% de la population est touchée par des crimes en ligne. Pour ce qui concerne le vol des données personnelles, on arrive à 8%. La crainte de tomber dans le piège semble pourtant plus grande que le risque réel. Selon une étude menée par Quentin Rossy pour le canton de Neuchâtel, 50% des citoyens ont peur d'être victimes de cybercriminalité. «On voit qu'il y a une vraie préoccupation de la population qui a l'impression d'assister à une explosion de la criminalité en ligne.» Si le Neuchâtelois constate que l'on observait déjà des fraudes au début des années 2000, c'est depuis 2010 que les choses ont vraiment changé.

«Les fraudes ont suivi les développements technologiques. Il y a eu une démocratisation de l'usage d'Amazon et des plateformes de e-commerce, ainsi qu'un développement des réseaux sociaux qui n'existaient pas au début du web. Le fait qu'il y ait de plus en plus d'usagers augmente le nombre de cibles et donc de victimes potentielles.» Et que ceux qui pensent être plus malins et ne courir aucun risque de tomber dans ce genre de piège se détrompent. «Il faut vraiment réaliser que nous sommes tous vulnérables, vraiment tous, car nous avons tous nos faiblesses.» Par exemple, certains ont besoin d'un appartement et sont prêts à verser une caution à un inconnu, d'autres ont honte de demander à leur médecin un médicament pour des problèmes érectiles et vont s'en procurer sur le Net, d'autres encore, souffrant de solitude, vont offrir leur cœur et leurs économies à un hypothétique faux compagnon idéal, vrai pro des arnaques à la romance.

Petites ou grandes vulnérabilités, un homme averti en vaut deux, dit le proverbe. Voici donc un inventaire des principales cyber-embuscades à éviter.

Faux vendeur et faux acheteur

Doctorante à l'École des sciences criminelles de l'Université de Lausanne, Giulia Margagliotti a fait de l'e-commerce son domaine de prédilection. Selon les sondages de victimisation faits par la police, ce phénomène est un enjeu majeur. «Dans le commerce en ligne, il y a deux grandes catégories: le faux vendeur et le faux acheteur et, à l'intérieur de ces deux groupes, on peut distinguer encore d'autres modes opératoires.» On l'aura deviné: le faux vendeur fait semblant de mettre en vente des biens qu'il n'a pas. Une personne intéressée va le contacter, verser de l'argent pour acquérir un objet et ne va jamais le recevoir. La doctorante évoque également des *shops online* éphémères. «Sur les réseaux sociaux, un magasin en ligne vendait des collants incassables pour un prix dérisoire. Beaucoup de femmes en ont acheté. Elles ont fourni les données de leur carte de crédit et n'ont jamais reçu les fameux collants.»

Si ne pas recevoir un produit commandé et payé est frustrant, risquer de voir ses données de carte de crédit transmises à des gens mal intentionnés n'est pas anodin. Dans le doute, mieux vaut donc en changer ou bien surveiller ses relevés de cartes de crédit, car il y a risque que les cybercriminels prélèvent de petites sommes régulièrement en espérant que la personne ne le remarque pas.

Le faux acheteur, lui, va s'intéresser à un objet mis en vente par un vendeur légitime qui va se retrouver à devoir verser de l'argent. Comment? «Certains auteurs exploitent des stratégies de paiements en excès. La fausse preuve de paiement indique un montant supérieur à celui prévu. Le fraudeur demande alors à la victime de lui verser l'excédent. Lorsque cette dernière réalise que le paiement n'a pas eu lieu, elle a déjà remboursé la différence.»

Le faux acheteur peut aussi convaincre le vendeur qu'il faudrait débloquer son paiement par PayPal, par exemple, en versant des frais. En fait, les escrocs vont envoyer un faux lien et le vendeur légitime se retrouvera à payer ces derniers. Pour ceux qui ne connaissent pas le fonctionnement de PayPal, c'est plausible. «Cela paraît paradoxal, mais les faux acheteurs arrivent à convaincre des gens de leur verser de l'argent ainsi.»

«IL Y A UNE VRAIE PRÉOCCUPATION DE LA POPULATION QUI A L'IMPRESSION D'ASSISTER À UNE EXPLOSION DE LA CRIMINALITÉ EN LIGNE»
QUENTIN ROSSY

Son conseil? Le plus sûr consiste à toujours remettre le bien en mains propres, mais, souvent, l'escroc affirme que ce n'est pas possible et il arrive à convaincre sa cible de faire le paiement. De fait, les fraudes sont beaucoup liées à la langue et à la culture. «Il faut pouvoir communiquer avec les gens pour les escroquer», explique encore Giulia Margagliotti qui conseille de bien détailler l'annonce pour repérer une faille. «Si elle est mal écrite ou que la personne a fait des erreurs, cela peut être un indice. On peut également vérifier si les mêmes images ne se retrouvent pas dans d'autres annonces.»

Avance de frais

Dans certains cas, le faux vendeur pratique également la fraude aux avances de frais. Prenons l'exemple d'une personne âgée dont le chien vient de décéder. «Il n'y a pas plus vulnérable: elle veut le même chien qu'auparavant», explique Quentin Rossy, qui raconte la mésaventure arrivée à une proche. Malheureusement, l'animal coûte cher et il n'y a que peu d'éleveurs en Suisse. Alors la voilà qui cherche son bonheur sur Internet parce que c'est le moyen le plus facile pour trouver ce qu'elle désire. Un vendeur à l'étranger la rassure: il lui promet un chiot très rapidement. «Patientez quelques jours, il arrive.» Contretemps: on doit encore le vacciner et c'est au futur propriétaire de payer les frais. Mais il ne faut pas s'inquiéter, il arrive. Zut, il est bloqué à la douane, ce qui implique des frais à payer. Ah, oui, le vendeur a oublié: il faut encore avancer les frais de transport. «Cette technique repose sur la stratégie commerciale du "doigt dans l'engrenage". Les fraudeurs débutent par des demandes peu coûteuses, puis les augmentent au fil du temps. La victime paie et paie encore, c'est sans fin. Au final, elle déboursera des milliers de francs sans jamais voir le chien.»

Autre piège récurrent: les avances de frais pour trouver un appartement dans les zones touchées par la pénurie de logements. «Vous allez commencer vos études? Vous avez un nouvel emploi? Vous voulez vous séparer? Vous n'avez pas le choix, vous avez besoin d'un logement et vous êtes donc vulnérable», constate Quentin Rossy. Évidemment, un deux-pièces pour 2000 francs, même au cœur de Lausanne, ça fait mal au porte-monnaie. Mais soudain, le futur locataire tombe sur une annonce alléchante, dans son budget. L'auteur lui dit: «Je suis un grand propriétaire immobilier et j'habite Londres. Comme je ne viens pas toutes les semaines à Lausanne pour faire des visites, je mandate une personne qui les organise pour moi. Comme je veux des locataires sérieux, si vous déposez votre dossier, il faut payer un loyer ou une caution.» On devine encore une fois la suite. Les avances de frais sont également un classique pour les locations de vacances qui figurent sur certaines plateformes comme Airbnb, Housetrip ou Wimdu. Le but des escrocs? Attirer la victime hors de la plateforme, en lui demandant son e-mail ou son numéro de portable, pour ➡

ainsi échapper à la vigilance des entreprises de location en ligne. En effet, ces dernières mettent en place des processus de contrôle et avertissent les utilisateurs lorsqu'une annonce paraît suspecte.

Faux patron

«Cette escroquerie demande du temps et ses chances de succès sont moindres, mais lorsqu'elle marche, c'est le jackpot», constate Quentin Rossy. Le principe? Après une phase initiale qui passe notamment par l'intrusion dans les serveurs e-mail d'une entreprise, le cyber-malfaiteur se fait passer pour le patron qui a besoin que son employé – ciblé dans certains cas – exécute une transaction urgente, soit le paiement d'une somme importante, dans le cadre d'une affaire qu'il est en train de monter dans un pays lointain. «Quand le montant est de 200 000 francs, il suffit que cela marche une fois sur mille. Les fraudeurs comptent sur la peur induite par une figure d'autorité. Ce sont potentiellement de nouveaux employés qui vont être victimes.» Les collaborateurs de l'École des sciences criminelles ont eux-mêmes fait l'objet d'une telle tentative. Des cyber-escrocs ont en effet usurpé l'identité du directeur et ont envoyé un message en son nom. «Deux personnes ont répondu. En l'occurrence, elles n'avaient pas forcément encore eu beaucoup de contacts avec lui. Heureusement, elles n'ont pas versé d'argent.»

Faux ami en difficulté

Autre cas d'usurpation d'identité: l'ami en difficulté à l'étranger qui envoie un message de détresse par e-mail ou WhatsApp. Bertrand s'est fait voler son porte-monnaie et son passeport et n'a aucun moyen de récupérer de l'argent. Heureusement, Western Union est fait pour ça et une «personne sympa» va venir au guichet d'un point de vente agréé avec Bertrand. C'est à son nom qu'il faut faire le versement, vu que Bertrand n'a plus de passeport. Pour récupérer l'argent, il suffit d'avoir le numéro de suivi du transfert (MTCN) que l'ami de Bertrand, future victime, lui transmettra par e-mail, ainsi que la pièce d'identité de la «personne sympa» sur place. Bertrand est un super copain, pas question de le laisser tomber. Le tour est joué et les fraudeurs ont gagné quelques centaines de francs.

Arnaque aux sentiments

Dans les cas de fraudes aux sentiments, les auteurs vont prendre contact avec les célibataires potentiellement en manque d'amour. Ces cybers «arnacœurs» vont prendre du temps pour tisser des liens et embobiner leur victime. Quentin Rossy: «Ils vont être en contact durant des semaines, voire des mois, puis à l'arrivée, une fois la confiance établie, ils vont pouvoir soutirer des dizaines de milliers de francs ou même des centaines de milliers de francs en prétextant des difficultés ou une situation d'urgence, par exemple un parent malade qui doit être opéré immédiatement.» C'est bien connu, quand on aime, on ne compte pas, surtout si on souffre de solitude. «Ces personnes ont une capacité magnifique de remplir la solitude. Vous êtes seul toute votre vie et du jour au lendemain, vous recevez des messages tous les jours, même trois fois par jour. Quel bonheur...» Finalement, les fraudeurs peuvent également faire du chantage pour extorquer de l'argent. Si la victime a eu la mauvaise idée de se dénuder devant sa caméra, son faux amoureux pourra le menacer de publier ces vidéos-là en ligne.

Alors que les auteurs de fraudes aux sentiments semblent provenir des pays de l'Afrique subsaharienne, la Malaisie et l'Afrique du Sud réunissent une part non négligeable de ces malfaiteurs.

«SI UNE ANNONCE EST MAL ÉCRITE OU QUE LA PERSONNE A FAIT DES ERREURS, CELA PEUT ÊTRE UN INDICE.»
GIULIA MARGAGLIOTTI

Cours pour les policiers

Fausse charité, fausse facture, faux emploi qui conduit à une activité illégale de blanchiment d'argent pour la victime, fausse loterie qui nécessite de verser de l'argent avant de recevoir le gros lot, faux investissements, la liste des escroqueries par Internet est bien plus longue que les exemples donnés ci-dessus. Mais que fait la police? Quentin Rossy constate qu'au même titre que le commun des mortels, la police a dû apprendre à reconnaître ces nouveaux problèmes. Et il a fallu un certain nombre d'années pour créer des cours pour les policiers. «Désormais, il y a une formation nationale sur le volet *cyber* qui permet au moins de reconnaître les problèmes de base. Pour l'étape suivante, c'est-à-dire mener une investigation sur ces cas-là, il s'agit de faire appel à des enquêteurs spécialisés et, restrictions budgétaires obligent, les cantons n'ont pas toujours créé beaucoup de nouveaux postes pour ce genre d'enquêtes.» Ce sont donc parfois les brigades financières et économiques qui s'occupent des cas de cybercriminalité, en plus de leurs tâches habituelles.

Actuellement, les fraudes en ligne reportées à la police ne sont pas forcément traitées au cas par cas, sauf si les pertes sont importantes ou qu'il y a une forme de violence. «L'idée est de détecter des séries et de les traiter dès le moment où l'on a identifié un problème qui émerge. Pour ce faire, une plateforme développée conjointement avec l'École des sciences criminelles nommée Picsel – plateforme d'information de la criminalité sérielle en ligne – est mise en place en Suisse.» Une fois que certaines formes d'escroqueries sont identifiées, comme les auteurs ne sont pas toujours sur le territoire suisse, la police met en place des stratégies de perturbation, en partenariat avec des plateformes comme Anibis, et organise des campagnes de prévention. En attendant, même si les méthodes de lutte contre la cybercriminalité se sont améliorées, mieux vaut être prudent. Un dernier conseil de Quentin Rossy? «Il faut être attentif à ses propres vulnérabilités et à celles de ses proches. Et dès qu'on réalise que l'on est victime d'une fraude, il faut stopper les contacts, prendre du recul et informer un proche ou la police directement.»

CELLE QUI REMONTE LE TEMPS

«Concernant mon job d'archéologue, je suis calme, patiente, à la limite de l'abnégation. Pour le reste, c'est le contraire, je bouge tout le temps!», lance avec un sourire lumineux Caroline Brunetti, à la tête de l'Office des recherches archéologiques du Valais depuis 2015. Notre interview est en effet animée: notre interlocutrice se lève, propose du café, guette l'arrivée du photographe, puis nous donne un flyer présentant l'ouverture au public du site archéologique Sous-le-Scex à Sion, qui a abrité une succession de cimetières depuis 5000 ans avant Jésus-Christ. «Malgré la Sionne à côté, rivière ravageuse, 300 générations ont choisi de vivre là. Ça me fascine.»

Les pieds sur terre

L'enthousiasme de Caroline Brunetti est contagieux, ses yeux bleus étincellent quand elle évoque l'archéologie. Une passion qui a débuté tôt. Âgée de sept ans, elle visite avec ses parents l'amphithéâtre romain d'Avenches: une révélation. Suivent une première fouille à 14 ans à Martigny, une maturité latin-grec et une licence en Lettres à l'UNIL, archéologie en branche principale. «C'étaient des études tribales, on vivait en communauté pendant des semaines lors des fouilles-école», s'amuse la spécialiste du mobilier en céramique et des Helvètes.

Sans attendre la fin de ses études, la Sierroise a participé à des fouilles d'urgence dues aux nouvelles autoroutes, en Suisse mais aussi à Bibracte (France), en Égypte, à Budapest. «Là-bas, j'ai bossé sur mon premier rempart. C'était en 1990, les pays de l'Est s'ouvraient. Un moment génial, il y avait une énergie folle», se souvient la docteure ès Lettres à l'UNIL, qui aime à la fois l'aspect rigoureux et scientifique de sa discipline, par exemple ce qui concerne la datation, et son côté très concret sur le terrain, à proximité des ouvriers des chantiers de construction, «ce qui nous fait garder les pieds sur terre».

Trésors valaisans

Caroline Brunetti a dirigé des fouilles d'envergure (notamment en tant que chargée de projet chez Archeodunum SA), comme celle du Mormont (Vaud) et son lieu de culte helvète d'importance européenne, datant de la fin de la période celtique, vers 100 av. J.-C. «Grâce à mes spécialisations, je n'ai jamais trop dû chercher du job. Mon premier entretien d'embauche était à 47 ans, pour mon poste actuel», confie-t-elle. Aujourd'hui, fini le terrain pour l'archéologue cantonale. «Mais je ne m'ennuie pas! J'adore en apprendre tous les jours sur le droit, l'économie, la politique et trouver des solutions pour fouiller le plus vite possible sans bloquer les chantiers». Ceci pour «faire fructifier la riche archéologie valaisanne», telle que la découverte à Sion en 2017 du squelette d'un guerrier, avec ses armes et bijoux (850 av. J.-C.). «J'aimerais que le public se rende compte que cet homme vivait pendant la période des pharaons d'Égypte et qu'on a aussi de beaux vestiges ici.»

Un patrimoine que cette mordue de photo et de BD souhaite faire connaître de façon novatrice, sans céder à une «disneylandisation» de la médiation ou au tout-numérique car «les vrais objets dégagent quelque chose». La scientifique désire faire rêver les gens sur son métier, qui analyse tous les aspects de l'homme, ses migrations, sa santé, ses lois... ou ses poubelles. **NOÉMIE MATOS**

CAROLINE BRUNETTI
Licence ès Lettres avec archéologie comme branche principale (1996), et doctorat en Lettres (2004), avec un Prix de faculté.

© Pierre-Antoine Grisoni / Strates

La communauté des alumni de l'UNIL en ligne: unil.ch/alumnil