GUIDE ANTI-ARNAQUE

Cédric Gourbault

Acheter et vendre en toute tranquillité sur Internet

EYROLLES

PERSONNE n'est à l'abri. Solange était persuadée d'avoir fait une bonne affaire, tout comme Dominique d'ailleurs, mais ils ont vite déchanté. Marianne, elle, pensait avoir trouvé le grand amour mais son prince n'avait en fait rien de charmant. Adopter une petite boule de poil, Lucie en rêvait ! Son rêve s'est pourtant très vite transformé en cauchemar...

Leur point commun ?

Ils se sont tous fait arnaquer sur Internet.

Depuis sa démocratisation, le Net est rapidement devenu un terrain de chasse idéal pour les arnaqueurs sans scrupule. Mais comment faire pour repérer ces truands des temps modernes qui se cachent derrière leurs écrans ? Le *guide anti-arnaque* 2014 vous aide à contourner les pièges tendus par ces escrocs 2.0.

Ce manuel décrypte les dangers d'Internet et résume de manière simple les points essentiels à retenir pour que vous surfiez en toute tranquillité.

Cédric Gourbault, fondateur d'Explorimo.com, FlashVisit.com, Quelproduitchoisir.com, est un multi-entrepreneur du Web depuis plus de 15 ans. En tant que président du site de petites annonces Trefle.com, il est confronté depuis sa création aux arnaques sur Internet et lutte quotidiennement avec ses équipes contre ce fléau.

www.editions-eyrolles.com

Code éditeur : G55822 • ISBN : 978-2-212-55822-7

GUIDE **ANTI-ARNAQUE**

Groupe Eyrolles
61, bd Saint-Germain
75240 Paris Cedex 05

www.editions-eyrolles.com

ISBN : 978-2-212-55822-7

Cédric Gourbault

avec la collaboration de
Charlotte Gorzala & Aurore Turpin

GUIDE ANTI-ARNAQUE

Acheter et vendre en toute tranquillité sur Internet

EYROLLES

SOMMAIRE

AVANT-PROPOS

Vous pouvez faire de très bonnes affaires sur Internet, surtout lorsqu'il s'agit de trouver ce qu'il vous faut dans des petites annonces. Pourtant, la liberté qu'offre Internet a aussi attiré quelques vendeurs malhonnêtes qui sont prêts à tout pour vous tromper. Avec plus de cinq millions de petites annonces sur le site trefle.com, nous combattons chaque jour ces escrocs. Alertés par certains de nos membres, nous avons souhaité vous fournir un outil facile d'accès afin de vous mettre en garde contre les arnaques les plus courantes. C'est pourquoi nous avons eu l'idée de rédiger ce guide pour lutter contre les arnaques.

Nos objectifs sont multiples :

- **Informer**
  Lister les arnaques actuellement en vigueur sur Internet et en décortiquer le fonctionnement.

- **Prévenir**
  Personne ne se sent vulnérable sur Internet. Et pourtant... nous vous donnons les indices qui doivent vous alerter.

- **Conseiller**
  Vous êtes en contact avec un vendeur et doutez de son intégrité ? C'est aussi pour vous que nous avons rédigé cet ouvrage. La diversité de situations que nous avons décrites

est suffisamment étendue pour que vous y trouviez le scénario que l'on vous oppose, si vous avez affaire à un escroc.

- **Orienter**
  Parce que, malheureusement, la prévention arrive trop tard, nous pensons aux victimes en leur expliquant quelles procédures juridiques engager et qui contacter. Pour répondre à vos questions, nous avons réalisé une véritable enquête d'investigation. Membres d'associations, psychologues ou encore gendarmes ont accepté de se prêter au jeu et de vous donner quelques clefs pour déjouer les pièges des escrocs et surfer en toute tranquillité.

Merci à toute l'équipe d'Ageo-group qui a participé à l'élaboration de ce guide.

Cédric Gourbault
Président d'Ageo-group

INTRODUCTION

Quels changements en 2013 ?

Internet est un formidable outil, que ce soit pour s'informer, pour communiquer et même pour acheter. Mais le monde virtuel constitue également un lieu de prédilection pour les arnaqueurs. Un élément qui accentue la dangerosité de ces truands d'un nouveau genre est qu'il s'adapte aux nouvelles technologies. Les pouvoirs publics ainsi que les associations cherchent à se tenir informés des nouvelles tendances afin de prévenir les victimes. Au cours de cette année, on remarque que le travail des associations commence à porter ses fruits. Les victimes sont de plus en plus informées et un véritable réseau de soutien s'est formé. Seul bémol, encore trop de victimes croient à la véracité des e-mails frauduleux.

Même si globalement en 2013, les scénarios des arnaques ne sont pas vraiment modifiés, on remarque tout de même des tendances inquiétantes.

En premier lieu, avec l'ascension des réseaux sociaux et notamment de Facebook, les escrocs ont plus facilement accès à vos informations. De même, Facebook est désormais le terrain privilégié des criminels. Ils peuvent entrer plus facilement en contact avec leurs victimes et quelque fois, usurpent des identités et se font passer pour vos amis.

En second lieu, il est avéré que les arnaqueurs n'hésitent plus à profiter de la naïveté des plus jeunes. Mais nous remarquons que de plus en plus de victimes ont moins de dix-huit ans. C'est pourquoi, il est aussi important de faire un travail de prévention auprès du jeune public.

Les 20 conseils
pour éviter les arnaques sur Internet

1. Les arnaqueurs sont des menteurs professionnels. Quelle que soit votre connaissance du Web et de l'informatique, ne vous croyez pas à l'abri d'une arnaque.
2. La valorisation endort la méfiance. Méfiez-vous des beaux parleurs qui vous disent ce que vous avez toujours voulu entendre !
3. Beaucoup d'arnaques sont menées depuis le continent africain. Lors de vos échanges marchands ou sentimentaux sur Internet, cessez tout contact dès lors que la personne se trouve en Afrique.
4. Aucune autorité judiciaire ne possède d'adresse mail gratuite de type Hotmail, Yahoo, Gmail... N'hésitez pas à vous rendre physiquement dans une gendarmerie, un commissariat ou votre mairie, ils sauront vous indiquer si le courrier que vous avez reçu provient d'une réelle institution publique. En cas de problème, ils vous orienteront vers les autorités compétentes.
5. Ne communiquez jamais d'informations compromettantes sur Internet. Ne communiquez pas non plus vos vidéos et/ou photos. Ces informations peuvent être exploitées par des personnes malintentionnées. Ne leur livrez aucun élément de chantage.

6. Ne divulguez pas d'informations personnelles sur Internet, prenez le temps de sécuriser vos comptes ainsi que ceux de vos enfants. Ne rendez pas visibles vos contacts sur Facebook.

7. Partez toujours de l'adresse https:// officielle et habituelle pour vous connecter à votre compte bancaire, à votre messagerie ou autres réseaux sociaux.

8. Ne donnez jamais vos codes secrets, mots de passe et autres identifiants par mail. Sous aucun prétexte. Aucun organisme financier ou autre ne demande à ses clients leurs codes confidentiels.

9. Lors d'un échange sur Internet avec une personne inconnue, saisissez son nom dans les moteurs de recherche afin de vous assurer qu'il ne figure pas dans un listing d'escrocs.

10. Pensez à vérifier l'adresse IP de votre interlocuteur. Si ce dernier vous ment au sujet de sa localisation, vous avez affaire à un escroc, surtout s'il se trouve à l'étranger.

11. Ne versez jamais d'argent par Mandat Cash ou Western Union à une personne que vous ne connaissez pas, que vous n'avez jamais rencontrée physiquement.

12. Votre souris d'ordinateur n'est pas une baguette magique ! Elle n'a pas le pouvoir de transformer un bien de valeur en un bien bon marché. Méfiez-vous des trop bonnes affaires.

13. Lors d'une transaction marchande entre particuliers, ne versez jamais d'argent en gage de votre bonne foi ! Ne payez que lorsque vous avez l'objet entre les mains.

14. Pour tout achat via Internet, privilégiez les transactions sur des sites protégés comme Paypal.

15. Ignorez les petites annonces qui vous demandent d'appeler un numéro commençant par 08. Il s'agit de numéros surtaxés.

16. Ne cédez jamais à la précipitation, surtout si votre interlocuteur prétexte un départ imminent à l'étranger.

17. Les « arnacœurs » ont quelques points en commun, ils se disent en France mais ont un accent étranger, ont une très belle situation financière, vous accaparent de manière immodérée, voyagent beaucoup, sont actifs dans des organismes humanitaires. N'ouvrez pas les portes de votre cœur à des inconnus trop rapidement, restez en alerte.

18. Le grand amour ne se nourrit pas d'argent. Ne donnez jamais d'argent à une personne avec qui vous entretenez une relation sentimentale virtuelle.

19. La meilleure arme contre le chantage est l'indifférence. Coupez tout contact avec votre maître chanteur dès la première menace. Ne payez jamais ce qu'il vous demande. Supprimez vos comptes de réseaux sociaux.

20. Ne vous rendez jamais à l'étranger pour effectuer une transaction financière d'argent liquide.

Nos experts

Christine Goubert, la présidente de l'Association des victimes d'escroqueries à la nigériane (AVEN France). Elles sont spécialisées dans les arnaques dites « à la nigériane » et les arnaques à l'amour. L'AVEN est une association à but non lucratif créée en 2009. Elle fonctionne grâce à des bénévoles qui aident et guident les victimes d'escroqueries.

Cyrille Le Jamtel, le psychologue. Ses éclairages nous sont précieux pour pénétrer les mécanismes psychologiques des arnaqueurs. Ils nous aident aussi à appréhender la détresse morale dans laquelle les victimes d'arnaque peuvent se trouver.

Jean-François Garnier, l'enquêteur spécialisé dans les nouvelles technologies au sein de la Gendarmerie nationale. Ses propos nous décryptent les méthodes qu'utilisent les arnaqueurs pour contourner la loi.

Joël Guillon, le président de l'association LesArnaques.com, de 2006 à 2013. Ses indications sont des repères pour les démarches à suivre en cas de litige avec un professionnel.

La Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF). La DGCCRF, dont le rôle est de protéger le consommateur, enregistre un grand nombre de plaintes chaque année notamment concernant la partie paiement. Elle nous éclaire sur nos recours.

« Zythom », l'informaticien et expert judiciaire qui met ses compétences au service de la justice. Grâce à sa connaissance du terrain ainsi que sa maîtrise du système informatique, il nous livre son expérience.

Les collaborateurs du site modèrent chaque jour des milliers d'annonces et doivent décrypter en permanence toutes les arnaques du Web nouvelles aussi bien qu'anciennes. C'est un combat de tous les jours que ces équipes nous font partager.

PARTIE 1

INTERNET, LIEU DE TOUS LES DANGERS ?

En quelques décennies, Internet est devenu un moyen de communication incontournable. En mars 2011, un dossier publié par l'Institut national de la statistique et des études économiques (Insee) nous révèle que seulement 12 % des ménages français avaient accès à Internet à leur domicile, en 2000. Dix ans plus tard, ils étaient plus de 64 %. En 2010, 80 % des Français affirmaient surfer quotidiennement sur Internet. Et si, les premières raisons qui nous poussent à utiliser le Net sont la recherche d'informations et la communication, nous sommes de plus en plus nombreux à faire des achats sur la Toile. Que ce soit sur des sites d'e-commerçants ou par l'intermédiaire des sites de petites annonces, les transactions en ligne se multiplient.

Avoir facilement accès à des biens de consommation sur Internet ne doit pas pour autant endormir notre méfiance. Les arnaqueurs existent depuis longtemps, avec Internet ils n'ont pas disparu, ils se sont simplement adaptés. Spams, escroqueries à la carte bleue, e-mails frauduleux... les arnaques sont multiples et les escrocs de plus en plus malins. Étant par essence sur des supports en perpétuelle évolution, les arnaqueurs se plient aux nouvelles technologies et adaptent leurs méthodes. Derrière leurs écrans, ils repèrent leurs victimes et tentent par tous les moyens de leur soutirer de l'argent. Ce n'est pas Internet, en soi, qui constitue une menace pour ses utilisateurs, le Net offrant à ses usagers de nombreux avantages. Cependant, via *Internet, il est plus simple pour les personnes malhonnêtes d'escroquer les victimes sans se faire prendre, grâce aux différents outils informatiques mis à leur disposition. Alors comment faire pour continuer à surfer en toute tranquillité en évitant de tomber dans les filets de ces criminels ?*

CHAPITRE 1
TERRA INTERNET DE CHASSE

Définitions

- **Mandat Cash** : moyen de paiement qui permet de transférer de l'espèce à partir d'un bureau de poste. Les arnaqueurs peuvent quelque fois demander à leurs victimes de leur envoyer de l'argent *via* ce mode de paiement.
- **Proxy** : programme qui fait office d'intermédiaire entre deux réseaux informatiques. Dans le cas d'arnaques, les escrocs l'utilisent pour ne pas être identifiés ; le « proxy » leur permet de modifier leurs adresses IP. Il ne sera alors plus possible de remonter jusqu'à eux.
- **Pseudonymat** : le fait d'utiliser un pseudo sur Internet. L'internaute masque sa véritable identité afin de ne pas être reconnu, en se créant une identité virtuelle. Cette notion ne doit pas être confondue avec l'anonymat. Sur Internet, malgré l'utilisation d'un pseudo, il peut être facile de retrouver une personne.

Solange B.

Internet est devenu le paradis des arnaqueurs. Leur terrain de chasse : le monde entier. Ici et là, ils sont rusés, sans scrupule, et connaissent mille et une méthodes pour vous prendre dans leurs filets. Bien sûr, ils ont une très bonne connaissance des rouages de l'Internet, mais vous pouvez aussi leur faciliter la tâche en dévoilant certains aspects de votre vie, alors prenez garde !

Témoignage

Solange B. se croit à l'abri derrière son écran d'ordinateur. Internet, elle connaît. Un jour, sa fille lui parle d'un site de ventes entre particuliers. Un site remarquable selon ses propres mots, qui permet parfois de trouver des objets dernier cri pour des sommes avantageuses. Dubitative, Solange va faire un tour sur ce site. Effectivement, elle y trouve des téléphones, des ordinateurs et de nombreux autres biens à des tarifs plus qu'alléchants. Elle y lit notamment une annonce émanant d'un vendeur du département voisin proposant un GPS quasiment neuf pour seulement 100 euros. Elle s'étonne d'un coût si peu élevé mais refuse de passer à côté d'une si bonne affaire. Contact pris avec le vendeur, elle apprend son départ imminent pour Londres et son désir de se débarrasser dudit GPS, qui ne lui sera plus d'aucune utilité. Solange se réjouit : elle, qui résistait à la tentation depuis plusieurs mois, découragée par le prix, venait enfin de trouver son bonheur ! Par commodité, le vendeur lui propose de régler par Mandat Cash Urgent. Un moyen de paiement très pratique, via *La Poste. Elle garderait avec elle le numéro du mandat et ne le transmettrait au vendeur par e-mail que le jour de*

réception du colis. Car sans numéro de mandat, impossible de retirer l'argent... en principe. La cliente s'empresse donc de remplir ce mandat et attend l'arrivée du GPS. Les jours passent sans que son facteur ne lui porte un quelconque colis.

Après cinq jours, la cliente s'étonne. Elle contacte son vendeur. Pas d'inquiétude, lui répond-il. Il habite une petite commune isolée et il arrive que les colis mettent un peu plus de temps à arriver. Il lui assure qu'elle le recevra dans la semaine à venir. Elle attend. Toujours pas de colis les jours suivants. Surtout qu'elle remarque, en recevant son relevé de compte, que les 100 euros ont été prélevés... Surprise pour la mère de famille, qui tente alors de joindre son vendeur pour lui demander des explications. Impossible de le joindre. Ses e-mails ne reçoivent aucune réponse, ses coups de fil sont toujours renvoyés vers une boîte vocale. En désespoir de cause, elle se rend à La Poste : comment le vendeur a-t-il pu retirer l'argent sans le numéro du mandat ? Mystère. Ce qui est sûr, c'est qu'il n'a pas été retiré dans le village voisin de Troyes, comme annoncé, mais à Rennes. En quelques semaines, Solange B. a perdu 100 euros, toutes ses illusions et la confiance qu'elle plaçait en le Net. Elle veillait à ce que ses enfants ne se fassent pas piéger et a négligé de surveiller sa propre sécurité.

Ce type d'histoire est monnaie courante. Depuis la démocratisation d'Internet, les arnaques tendent à se multiplier et à se diversifier. Si le Net est devenu un puissant moyen de communication, son universalité le rend dangereux. Et pas seulement pour les enfants. En quoi le Net est-il un terrain privilégié pour ces arnaques ?

Internet : le lieu où tout est possible ?

L'informaticien et expert judiciaire connu sous le pseudo « Zythom » met ses compétences au service de la justice, pour traquer les criminels sur le Net. Il nous résume parfaitement la situation : « Internet est un système d'interconnexion de réseaux et de machines. C'est le plus grand réseau informatique mondial. En tant que tel, il ne constitue pas une menace, pas plus que le réseau téléphonique ne constitue une menace pour l'être humain. La menace pour l'utilisateur lambda existe mais elle ne vient pas d'Internet, elle provient de la nature humaine : sur un grand nombre d'utilisateurs, vous trouverez toujours quelques personnes dangereuses qui vont profiter de la naïveté des plus faibles, ou d'une maîtrise technique supérieure pour abuser les novices. » Au sein de l'AVEN France, la présidente, Christine Goubert, a vu défiler nombre de victimes qui pensaient toutes faire l'affaire du siècle en achetant un objet de valeur à petit prix. Or sur Internet, comme dans une transaction avec votre voisin, chacune des deux parties veut être gagnante. Le vendeur souhaite retirer quelques bénéfices de sa vente ; quant à l'acheteur, il veut acquérir un article qu'il désire à un prix raisonnable. Et il est humainement impensable que quelqu'un se sépare d'un bien pour un prix bien inférieur à sa valeur initiale. Pourtant, ces principes de base du commerce, connus et acceptés de tous, semblent perdre toute valeur sur Internet.

Pour Cyrille Le Jamtel, psychologue, c'est toute la force de ce média : « Sur le Net, tout est dématérialisé. Il y a une sorte de mise à distance de la réalité. On évolue dans une sphère différente et les codes semblent donc, eux aussi, différents ». C'est pourtant totalement faux. Si un automobiliste s'arrête soudain à côté de vous et vous propose d'acheter son véhicule pour la moitié de sa valeur, vous allez vous méfier. Pourtant, la même situation sur Internet vous fait croire à une bonne affaire.

Face à un produit que l'on ne voit pas et dont on n'a pas forcément conscience de la valeur, Internet peut vite devenir votre pire ennemi. Sans le réflexe de comparaison avec d'autres sites ou avec les prix habituels du marché, l'internaute peut foncer tête baissée dans un piège sans se rendre compte du caractère frauduleux de l'annonce à laquelle il vient de répondre. « Dans notre société, analyse Cyrille Le Jamtel, les gens connaissent de moins en moins la frustration. On a tendance à tout vouloir, même ce dont on n'a pas besoin. Sauf que parfois, ce que l'on désire est inaccessible de par son prix. Et soudain, grâce à Internet, l'objet de notre désir est à portée de main. C'est tellement tentant qu'on en perd notre recul. C'est une véritable compulsion, on laisse la réalité de côté pour céder au caprice. On finit par avoir tellement envie de tel ou tel objet que toutes les alertes qui nous amèneraient à avoir conscience du danger sont mises à l'écart. En perdant notre capacité à juger objectivement les choses, nous nous fragilisons nous-mêmes ». De même, tout comme vous ne confieriez pas une grosse somme d'argent liquide à un inconnu croisé dans la rue qui vous promet un bien que vous n'avez jamais vu, pourquoi accepteriez-vous cette situation lorsqu'elle a lieu sur le Net ?

CONSEIL

Comparer les prix via *un site spécialisé ou tout simplement en le mettant en parallèle avec d'autres offres de particuliers vous donnera une vue d'ensemble et vous permettra déjà d'être plus méfiant à l'égard de certaines offres.*

Entre également en compte le désir que vous avez d'acquérir cet objet particulier. La démarche de chercher ce que vous souhaitez sur Internet est généralement précédée d'une phase de recherche réelle, hors de la sphère virtuelle. Le coût, ou la difficulté d'obtention de l'article souhaité, vous pousse donc à

vous tourner vers Internet pour bénéficier de l'offre d'un particulier, souvent plus intéressante que celle de gros distributeurs. Aveuglés par ce désir compulsif de possession, les acheteurs auront tendance à ne pas remarquer de petites incohérences dans le scénario ou à ne pas s'intéresser aux dangers des transactions par Mandat Cash ou par Western Union. Il est pourtant assez simple de repérer une arnaque, dès lors que l'on a dépassé l'envie de posséder à tout prix l'article convoité. Le premier réflexe à avoir, c'est tout simplement de comparer les prix. Quel que soit l'objet que vous souhaitez acquérir, un tarif particulièrement bas par rapport à sa valeur d'origine est souvent le signe d'une escroquerie. Mais il n'est pas toujours facile de connaître exactement le prix d'un GPS ou d'un ordinateur portable.

Un système difficile à comprendre

Internet est aujourd'hui à la disposition de tous. Une grande majorité des foyers est équipée d'une connexion Internet. C'est le moyen idéal pour toucher le maximum de personnes. Plus son terrain de chasse grandit, plus l'arnaqueur a de chances de trouver des victimes. Sur la proportion de connectés, il y en aura toujours quelques-uns pour croire aux scénarios des escrocs.

Ce qui fait surtout l'attrait d'Internet pour les arnaqueurs, c'est la complexité du système informatique. Qui sait réellement exploiter toutes les possibilités que lui offre son ordinateur ? Qui connaît les arcanes d'Internet ? Sans être un professionnel de l'informatique, qui sait seulement protéger ses informations personnelles ? À chaque fois que vous vous identifiez sur un site, des informations sont enregistrées, ne serait-ce que votre adresse mail et un mot de passe. Parfois, vous donnez des renseignements sur votre sexe, votre âge ou votre profession… L'expert en la matière s'appelle Facebook.

On se croit maître de ses données sans penser qu'elles sont parfois accessibles à tous, et que tout le monde n'est pas forcément bien intentionné. Lorsqu'un escroc a accès à votre nom, il a potentiellement accès aux informations de votre compte Facebook. Et par là même, il peut se procurer nombre de renseignements sur vous, sur vos contacts ou votre famille. Inintéressant dans l'absolu puisque l'arnaqueur ne va jamais s'amuser à vous traquer jusque chez vous. Mais s'il entre en possession d'une information compromettante – vidéo « hot », preuve d'infidélité… – ces données lui donneront un excellent moyen de pression. Il vous menacera de diffuser les documents compromettants et vous demandera de l'argent en échange de son silence. Dès lors, vous ne serez plus maître d'aucune information concernant votre vie : il sera déjà trop tard.

À SAVOIR

Verrouiller totalement son compte exige de bien lire toutes les clauses de confidentialité et de passer un certain temps à fouiner dans les recoins de votre compte pour le sécuriser au maximum. Peu de gens le font.

La complexité du système judiciaire favorise ainsi la multiplication des arnaques sur le Net. De plus, lorsqu'elles sont commises au-delà des frontières, il est encore plus difficile de suivre la trace des escrocs. En effet, les politiques de pays européens, et plus largement de toutes les nations du monde, sont loin d'être harmonisées. Un produit interdit en France peut être légal en Hollande ou en Lituanie. Si le site vendeur est hébergé par un de ces pays, alors la distribution du bien n'est pas illégale mais l'achat le devient. Il en est de même pour les arnaques : certains pays sont plus ou moins vigilants, plus ou moins répressifs que d'autres. D'où la difficulté d'harmoniser des interventions judiciaires dès que les arnaques s'étendent sur plusieurs pays.

Il serait pourtant faux de penser que toutes les arnaques proviennent de l'étranger. En France aussi, les arnaqueurs exercent sans scrupule. Il paraît logique que les poursuites soient longues et délicates quand les escrocs sont basés à l'étranger. En revanche, pour les Français, comment expliquer leur peu de crainte face aux lois de leur propre pays ? Tout simplement parce que la technologie permet aujourd'hui à certains d'entre eux de se faire passer pour des étrangers. Ce petit miracle est réalisé par des « proxys ». Ce « proxy » va littéralement s'interposer entre vous et l'arnaqueur. Il modifie l'adresse Internet, la fameuse adresse IP. Avec un « proxy », vous pouvez faire croire que vous êtes en Inde, alors que vous êtes en France. Du coup, il assure à l'escroc un anonymat beaucoup plus complet. Plus concrètement : vous voulez acheter une voiture et un escroc ivoirien a déposé une annonce en passant par un serveur proxy qui délivre une adresse IP en France. Si vous vous méfiez et tentez de remonter jusqu'à votre interlocuteur, vous croirez que votre vendeur est bien français. L'arnaque est en marche.

Certains arnaqueurs n'ont même pas besoin de se servir de ce type de stratagème. Lorsqu'ils sont basés dans des pays africains, la majorité des escrocs ne se connectent pas de chez eux. Leurs lieux de prédilection : les cybercafés. Même en traçant l'adresse IP lors de l'envoi d'e-mails, il est difficile de remonter exactement jusqu'à son rédacteur.

Un système faussement sécurisé

Outre sa disponibilité et son extrême accessibilité, Internet est un terrain de chasse privilégié pour les escrocs car il apparaît comme sécurisé pour les victimes. Cyrille Le Jamtel explique cela grâce à une notion assez nouvelle : le pseudonymat. « *On a l'impression de maîtriser et de ne montrer que ce que l'on veut. Dans cette illusion de contrôle, on perd sa sensibilité au danger* ».

Pourtant on dévoile tout le temps quelque chose sur soi, que ce soit lorsque l'on s'inscrit sur un site, comme Facebook, même en usant d'un faux nom ou encore lorsque l'on achète un objet en ligne. De plus, Internet permet de s'inventer une vie idéale. « *Sur le Net, les internautes ont tendance à enjoliver légèrement la réalité. Ils se disent un peu plus jeunes ou un peu plus grands. On a tous une part de narcissisme et Internet nous permet de la révéler et de l'exacerber. Avec ce moi idéal, on se sent à l'abri* ». Parce que ce profil idéalisé n'est pas vous, vous allez avoir l'impression que toutes les informations que vous dévoilerez ne pourront pas être retournées contre vous. Mais Internet n'est pas un espace d'anonymat. Parce qu'il y a toujours une trace de vos activités sur le Net. Que ce soit un historique de vos recherches, un mot de passe ou un numéro de carte bancaire automatiquement enregistré, le lieu d'où vous vous connectez, ou encore les plugins de votre navigateur, tous ces éléments sont retrouvés grâce à votre adresse IP. « *Internet est un miroir déformant. L'escroc joue là-dessus. Si vous publiez un profil un peu plus avantageux que la réalité, vous allez créer un moi idéal. Vous savez qu'il est faux, mais sur Internet, cela devient réalité. Si quelqu'un prend ces critères et les utilise pour vous flatter, pour vous valoriser et vous individualiser, vous finirez par vous prendre au jeu. Vous allez y croire et vous deviendrez une victime parfaite* », analyse Cyrille.

Les arnaqueurs : des menteurs professionnels

Internet est devenu un terrain particulièrement fertile pour les arnaques. La facilité d'accès qu'il offre partout dans le monde est une aubaine pour les escrocs. Jouant sur les difficultés juridiques à les poursuivre dans leur pays respectif, ils ont tout loisir de perfectionner leurs scénarios afin d'extorquer toujours plus rapidement et plus facilement un maximum d'argent à leurs proies. Ce sont des menteurs professionnels. Monter de toutes

pièces des histoires, qui, malgré leur caractère improbable, vont duper les gens, reste leur activité principale et ils savent parfaitement jouer sur les faiblesses des internautes pour parvenir à leurs fins.

Pourquoi les victimes placent-elles une telle confiance dans des vendeurs qu'elles n'ont jamais rencontrés ? Comment peut-on envoyer son argent sans, au préalable, prendre des mesures afin de sécuriser sa transaction ?

Si l'AVEN a référencé une quinzaine d'escroqueries principales, elles ont chacune des dizaines de variantes. La clef d'une arnaque menée à bien, c'est son adaptabilité : « *Un escroc va mener plusieurs arnaques en même temps. Pour chacune d'entre elles, il va garder le même scénario de base mais en fonction de la réaction de ses victimes potentielles, il va s'adapter pour leur soutirer un maximum d'argent sans éveiller leurs soupçons* ». Quand bien même auriez-vous quelques soubresauts de méfiance, ils ont réponse à tout, tout le temps. Et en un temps record. En effet, un arnaqueur a avant tout une incroyable capacité à parler. Venant majoritairement d'Afrique, l'orthographe et le vocabulaire des escrocs laissent souvent à désirer, mais qu'importe ! Ils n'en restent pas moins de grands bonimenteurs. Leur capacité à flatter leurs victimes est sans égale. Cyrille Le Jamtel l'explique : « *Lorsque l'on est flatté, on préfère se laisser aller à la satisfaction que de douter, et peut-être de découvrir que ce sont juste des mensonges pour endormir notre méfiance* ». Et parce qu'ils sont de beaux parleurs, ils ont aussi appris à avoir réponse à tout. Ils ne se laissent pas piéger par les questions de leurs proies et même le plus méfiant des consommateurs pense avoir affaire à une personne honnête. On n'imagine pas qu'un scénario d'arnaque puisse être suffisamment abouti pour parer à toutes les interrogations de la

À SAVOIR

Il y a autant d'arnaques que de victimes.

victime potentielle. Un système bien rodé qui vise à créer un lien privilégié entre l'escroc et sa proie.

Témoignage

Floriane D. en a, malgré elle, fait l'expérience. Lorsqu'elle a repéré ce charmant chiot Cavalier King-Charles sur Internet, elle a craqué. La famille qui l'avait vu naître devait partir en Angleterre suite à une mutation du chef de famille. Logée dans un appartement où le propriétaire ne voulait pas d'animaux, la famille était contrainte de livrer la petite boule de poils, à peine sevrée, aux bons soins d'une autre personne. Floriane a tout fait pour obtenir cet animal, gracieusement offert par ses propriétaires alors que cette race très demandée se vend généralement près de 1 000 euros. Ses échanges de mails puis les coups de téléphone aux généreux propriétaires ont toujours été très courtois. On lui parlait de la petite bête, on se ravissait à l'autre bout du fil de l'enthousiasme de la jeune fille et de son intérêt pour l'animal. On voulait s'assurer qu'elle traiterait bien le chiot et qu'elle saurait s'en occuper, puis l'on se montrait heureux de sentir la jeune femme prête à s'occuper d'un animal, malgré toutes les contraintes. Mais après plusieurs mois à attendre l'animal et à payer des frais de vétérinaire, de transporteur et d'autres dépenses imaginaires, Floriane D. a dû faire le deuil de son joli rêve. Le Cavalier King-Charles n'avait jamais existé et elle s'était fait berner.

En laissant entendre à sa victime qu'il la croit sérieuse, l'escroc va subtilement valoriser sa proie. Il va la persuader qu'elle est la seule personne capable de s'occuper de l'animal et créer ainsi une responsabilité : si la victime refuse de payer les frais vétérinaires

ou de douane, qui va s'en occuper ? Valoriser sa victime, c'est en un sens faire en sorte qu'elle se sente obligée de correspondre à l'image idéale qu'elle pense avoir donnée. Elle va se montrer disponible et prête à tout pour secourir la petite bête bloquée par des dépenses auxquelles sa famille initiale ne peut pas subvenir. Une technique que les arnaqueurs ont appris à décliner sous toutes ses formes. Elle s'adapte désormais à toutes les arnaques, qu'elles se fondent sur une vente d'objet, une location d'appartement ou encore lors d'une arnaque à l'amour.

Jouer sur votre confiance et votre pitié

Afin de créer un lien de confiance entre sa victime et lui, l'escroc n'hésite pas à jouer sur les sentiments. Il va tenter par tous les moyens de vous faire ressentir de la pitié ou de la culpabilité afin de mieux vous manipuler. Pour ce faire, il va mettre en place toutes sortes de scénarios pour vous faire tomber dans son piège. Parmi ces scénarios, le faux don d'animaux, est un exemple courant d'arnaque qui se fonde sur la confiance et la pitié des victimes.

Témoignage

Lucie T. se sentait un peu seule dans son petit appartement parisien, son récent statut de jeune professionnelle lui laissant peu de temps pour les divertissements. De plus, elle préférait rester au calme plutôt que de sortir tous les soirs pour le plaisir de boire entre copains. Un choix clairement assumé, mais qui la laissait donc quotidiennement en tête à tête avec son assiette de pâtes. Lui vient alors l'idée d'adopter un petit animal pour avoir une présence à ses côtés. Pas un chien, qui représente trop de contraintes et qu'elle avait du mal à

imaginer toute une journée seul à la maison. Pas de hamster, lapin, canari ou autre animal à enfermer dans une cage. Elle veut profiter de cette présence. Un chat semble donc plus adapté à ses exigences. Par conviction ou par idéal, elle refuse de se rendre dans une animalerie. L'idée d'un commerce fondé sur l'achat d'un animal lui est difficilement supportable. Hors de question de payer un animal comme elle achèterait n'importe quel objet de consommation quotidienne. Persuadée de trouver sur Internet une famille désireuse de donner des chatons, elle se lance à la recherche du minet qui la fera fondre. Très vite, la jeune femme se découvre une attirance particulière pour les chats persans. Une allure royale et de longs poils soyeux à caresser longuement devant la télévision un soir d'hiver... cette idée la fait rêver. Mais ce sont des chats de race et ils se vendent cher : 1 500 euros au moins. Une somme qu'elle se refuse à payer et, de toute façon, trop élevée compte tenu de ses moyens. Lucie s'était donc résignée, au bout de quelques semaines à adopter un chaton d'une race quelconque et avait enterré son idéal de chat persan. Pourtant, au détour d'une annonce, elle croise une ravissante photo. Une portée de trois petits félins de sa race de prédilection. Ce qui l'étonne et l'attire dans cette annonce, c'est le prix des animaux, qui n'apparaît nulle part. Étonnée, mais pleine d'espoir, elle contacte par mail la famille. Quelques jours plus tard, la réponse la ravit : effectivement, les animaux ne sont pas à vendre mais bien donnés. Leurs propriétaires viennent d'avoir un enfant qui s'est avéré allergique aux poils de chats. C'est donc avec beaucoup de regrets qu'ils doivent se séparer des

petits. Tout juste sevrés, ils n'attendent plus qu'une nouvelle famille aimante pour s'en occuper. La jeune femme est aux anges. Elle s'empresse de répondre, affirmant être prête à en prendre soin comme la prunelle de ses yeux. Rassurés, les propriétaires lui indiquent un transporteur spécialisé pour faire venir le chaton ; la distance géographique qui sépare acheteur et vendeur empêchant chacune des deux parties de se rencontrer pour procéder à ce don. La famille propose donc que chacun paye la moitié des frais de transport. Une perspective qui enchante Lucie. Elle accepte. Un peu plus d'une semaine plus tard, elle reçoit un e-mail dudit transporteur. La cage de l'animal n'est pas conforme et il refuse de le faire voyager dans ces conditions. L'acheteuse désemparée contacte donc la famille pour l'informer du problème. Les propriétaires réfléchissent puis lui proposent d'aller sur place régler le problème en achetant une nouvelle cage. Une fois de plus, ils partageront les frais. Elle n'aura qu'à leur envoyer par Mandat Cash la moitié de la somme. Mais les problèmes se multiplient : les vaccins ne sont pas à jour, le chaton est tombé malade, il faut payer un vétérinaire... À chaque fois, la jeune parisienne débourse de l'argent pour venir en aide à la boule de poils qu'elle veut absolument voir arriver au plus vite. Rapidement, elle doit avouer à la famille d'origine ne plus être en mesure de payer les frais. Aussitôt, le contact se rompt. Elle n'a plus de nouvelles de la famille, ni du transporteur. Elle tente en vain de les contacter et décide de retourner sur le site où elle avait vu l'annonce, pour leur signaler le peu de sérieux de leurs vendeurs. Quelle surprise

lorsqu'elle voit exactement la même annonce que celle à laquelle elle avait répondu, mais avec une adresse mail différente ! Alertée, elle se renseigne sur des forums et le couperet ne tarde pas à tomber : elle a été victime d'une arnaque et les ravissants chatons qui l'avaient fait craquer n'ont jamais existé, excepté dans les mensonges de ses escrocs. Lucie T. n'aura jamais son chat persan, mais son compte en banque, lui, a bien été amputé de près de 2 500 euros.

Pour les animaux comme pour les biens, ce qui a de la valeur n'est jamais gratuit, ni bradé. Un animal de race se vend cher. Son pedigree, la rareté de sa race et la forte demande en font un objet de convoitise. Il ne faut pas oublier que tout le monde veut faire une affaire sur Internet. Quelle famille se priverait d'une rentrée d'argent en donnant un animal que tout le monde vend ? Cela défie toute logique. Si toutefois vous avez envie d'y croire et que vous contactez la famille, cessez tout contact dès que l'on vous prétexte des frais pour incompatibilité de la cage, exigences du transporteur, frais vétérinaires... Dites-vous que l'animal n'existe pas et que ce n'est qu'une illusion pour vous soutirer de l'argent. À long terme, le coût financier des arnaques est particulièrement élevé pour la victime. Mieux vaut parfois se passer de l'objet désiré ou simplement accepter de le payer un peu plus cher, mais avoir la certitude de l'obtenir, en bout de course.

À SAVOIR

Il y a deux types d'arnaques qui vont faire appel avec beaucoup de subtilité à tout ce qui peut vous toucher : les arnaques à l'amour et les arnaques aux animaux.

Dans ces deux cas « on va essayer de s'en prendre à votre pitié, votre sensibilité, votre solitude… » explique Christine Goubert. Avec ce type d'escroqueries très abouties, les montants extorqués peuvent atteindre des sommets, souvent plusieurs milliers d'euros. S'il est impossible de dresser précisément un profil de l'arnaqué potentiel, on peut toutefois affirmer que celui ou celle qui a déjà été victime est parfois plus vulnérable. Car une fois la supercherie dévoilée, les proies mises face à la réalité ont généralement la même réaction : « Elles ont honte, elles se sentent coupables, naïves ». Le mécanisme psychologique qui s'enclenche est alors comparable, toutes proportions gardées, à celui d'un viol. « Dans les deux cas, analyse Cyrille, la première réaction que l'on a, c'est la honte. Parce qu'il y a un sentiment d'intrusion, on se sent pillé de l'intérieur ».

Des sites en tout point frauduleux

D'autres arnaqueurs, plus audacieux, poussent l'escroquerie plus loin, jusqu'à monter de faux sites Internet. Une démarche bien plus complexe que de simples escroqueries aux petites annonces, mais pas moins ingénieuse. Monter un site Internet sous une fausse identité, se faire transférer des fonds sur un compte offshore… Des pratiques qui pourraient sembler irréalisables. Et pourtant, l'adjudant-chef Jean-François Garnier nous démontre en quelques clics la facilité de falsifier son identité… et son activité. « Certains pays proposent par l'intermédiaire d'Internet d'obtenir un passeport moyennant finance

CONSEIL

On peut reconnaître les sites frauduleux basés à l'étranger aux fautes de français. Les phrases sont maladroites, la traduction automatique laissant à désirer.

et quelques pièces justificatives qui ne sont pas des plus difficiles à falsifier. Une fois fait, des dizaines de sites vous proposent de créer un compte bancaire offshore. Contrairement à ce que l'on peut penser, ce n'est pas illégal en soi. C'est l'activité d'où proviennent les fonds qui l'est ». Dans ces cas-là, le site sera spécialisé dans la vente d'un certain type de produit, les médicaments, par exemple. Vous paierez par carte, par virement bancaire, mais ne recevrez jamais votre marchandise.

Cependant, pour ceux qui sont gérés par des Français, il est bien plus difficile d'identifier un comportement douteux. Pour parer à toute éventualité, privilégiez les transactions *via* des moyens sécurisés, de type Paypal et autant que possible, surfez sur des sites connus où les arnaques sont moins nombreuses et plus faciles à identifier.

Néanmoins, ces arnaques restent une minorité comparées à toutes les annonces frauduleuses que l'on peut trouver sur les sites de petites annonces entre particuliers. Ces dernières revêtent un caractère plus discret que les escrocs auront tendance à privilégier. Un site entier, monté de toutes pièces, sera tout de suite bien plus voyant aux yeux des autorités.

En pratique

Signaler une arnaque

Le premier réflexe à avoir, une fois que vous avez repéré une arnaque ou une annonce qui vous paraît fausse, c'est de la signaler. Adressez-vous aux services de modération du site si vous vous trouvez sur un site de petites annonces et/ou directement à l'État si vous avez été confronté à un site frauduleux. Il existe pour cela de nombreuses plate-formes à alerter qui sont chacune spécifique à certains types de problèmes :

- **www.internet-signalement.gouv.fr** qui lutte contre les contenus illicites de l'Internet, pour signaler une arnaque.
- **www.signal-spam.fr** pour signaler les courriels frauduleux que vous pourriez recevoir (spams).
- **www.econsumer.gov/francais** pour signaler toute arnaque transfrontalière que vous auriez repérée.

EN RÉSUMÉ

- Les bases d'une transaction sont les mêmes dans la réalité et sur Internet. Une annonce trop alléchante cache souvent une arnaque. Renseignez-vous, comparez les prix et les produits avant d'acheter.
- Achat d'animaux : cessez tout contact si votre interlocuteur vous demande de l'argent sous prétexte de frais vétérinaires, de maladie, de transport...
- Internet n'est pas un lieu d'anonymat. Pour un arnaqueur, accéder à vos données personnelles peut être un jeu d'enfant, notamment grâce à Facebook.
- Verrouiller totalement son compte exige de bien lire toutes les clauses de confidentialité et de passer un certain temps à fouiner dans les recoins de votre compte pour le sécuriser au maximum.
- Les escrocs sont des menteurs professionnels. Ils s'adaptent facilement. Lors d'une rencontre sur le Net, restez vigilant.
- Les arnaqueurs tentent par tous les moyens de jouer sur votre confiance et votre pitié. Soyez méfiant.
- Privilégiez les paiements sur des sites sécurisés comme Paypal.
- Si vous remarquez une arnaque, n'hésitez pas à la signaler aux modérateurs ou aux instances compétentes.

CHAPITRE 2
ET VOUS ÊTES LA PROIE

DÉFINITIONS

- **Adresse IP** (*Internet Protocol*) : numéro d'identification attribué de façon permanente ou provisoire à chaque appareil connecté à un réseau informatique utilisant l'Internet. Il existe des adresses IP de version 4 (sur 32 bits, soit 4 octets) et de version 6 (sur 128 bits, soit 16 octets). La version 4, la plus utilisée, est généralement représentée en notation décimale avec quatre nombres compris entre 0 et 255, séparés par des points, ce qui donne par exemple : 212.85.150.134. Les plages d'adresses IP v4 étant proche de la saturation, les opérateurs incitent à la transition d'IPv4 vers IPv6 (*Wikipedia*).
- **Proie** : personne sur laquelle on peut exercer ou on exerce sa domination, sa violence, sa malhonnêteté (*Larousse*).

Dominique C.

Difficile d'établir un profil type de proie, devant l'écran, tout le monde est vulnérable... et vous aussi, même si vous surfez souvent. Bien sûr, certaines méconnaissances des règles de ce

monde virtuel peuvent vous attirer irrésistiblement dans une spirale de l'arnaque. Quoi qu'il arrive, restez vigilant !

Témoignage

Dominique C. est un homme prudent. Il achète assez peu sur Internet pour une raison toute simple : il a difficilement confiance dans un produit ou dans un acheteur qu'il ne connaît pas. Pourtant, le 6 juillet, il repère une annonce sur un site spécialisé dans la vente entre particuliers. Un autre internaute propose un téléphone portable pour 165 euros. Justement, le fils de Dominique a besoin d'un nouveau mobile : c'est une aubaine à ne pas manquer. Mais, toujours aussi prudent, l'acheteur demande des précisions. Il appelle son interlocuteur, lui envoie des e-mails... À chaque contact, le vendeur est aimable, parle un français parfait, ne fait pas de fautes d'orthographe... Il n'y a rien qui pousse Monsieur C. à se méfier : ce vendeur semble tout à fait digne de foi. De plus, son vendeur lui propose un paiement par Paypal, un moyen de transaction apparemment sans aucun risque. Il envoie donc 165 euros à l'adresse e-mail détentrice du compte Paypal avec l'assurance que le colis serait posté le lendemain. En effet, le lendemain, coup de fil du vendeur. « Je vous confirme avoir envoyé le colis aujourd'hui. Vous devriez le recevoir dans les jours à venir... ». Deux, trois, quatre jours plus tard, Dominique ne voit toujours aucun colis dans sa boîte aux lettres. Il contacte donc à nouveau le vendeur pour lui demander le numéro de recommandé. Aucune réponse. Pendant plusieurs jours, personne ne répond aux e-mails, ni aux appels répétés de l'acheteur. Irrité, il a alors l'idée de recontacter

son vendeur avec une autre adresse et de se faire passer pour un nouvel acheteur. Surprise ! Non seulement le vendeur réapparaît, mais il apprend que le téléphone est toujours en vente. Dominique se retourne alors vers Paypal et déclare un litige, puis, sans nouvelles, dépose une réclamation. Pour revoir son argent, il surfe un peu, cherche des solutions, pour, à défaut de recevoir le téléphone, revoir son argent. Il tombe alors sur un forum. Au milieu des centaines de réclamations ou demandes de conseils, il poste son message et demande de l'aide. Un modérateur tente alors de le rassurer : puisqu'il a réagi à temps en déposant un litige puis une réclamation via *Paypal, il a des chances de revoir son argent. Reste maintenant pour lui à être patient... et encore plus prudent.*

Ce type d'histoire est légion sur Internet. Les forums d'aide aux victimes regorgent de ce genre de témoignages. Et les victimes ne sont pas toujours celles que l'on croit. On imagine volontiers une femme d'un certain âge, pas vraiment initiée aux techniques d'Internet, se faire piéger par un jeune loup insouciant et sans scrupule. Pas du tout. Bien sûr, il existe ce cas de figure, mais tout le monde est vulnérable devant son écran. Malgré toutes les idées reçues, les victimes d'arnaques sont plus variées qu'on ne le croit. Vous ne savez pas à qui vous vous adressez. Il y a toujours un risque de tomber sur plus malin que soi. Vous ne pouvez pas estimer le niveau de compétence psychologique ou informatique de votre interlocuteur. Pour peu qu'il soit un tantinet plus qualifié que vous et que ses intentions soient tout sauf louables, vous courez un risque. Il est aisé de se croire à l'abri parce que l'on est jeune et que l'on croit maîtriser l'Internet. L'expert judiciaire connu sous le pseudo de « Zythom » l'a bien compris : « Tout le monde peut être un jour en position de faiblesse, par exemple

lors d'une dépression. Dans la vie réelle, quelqu'un peut se proposer pour vous aider à traverser la rue, avoir une attitude qui inspire confiance, et en profiter pour vous subtiliser votre portefeuille. Ce sont certains humains qui constituent une menace, pas Internet qui n'est qu'un réseau informatique ».

Christine Goubert, de l'AVEN, confirme cette idée : « *On me dit parfois que les victimes se font avoir parce qu'elles le veulent bien : c'est totalement faux* ». Pour elle et les membres actifs de l'association, reconnaître un escroc est d'une facilité déconcertante « *mais c'est parce que nous avons l'habitude* ». Si l'on en croit son expérience, les escrocs sont des experts en manipulation. « *Rien n'est perdu, il y a toujours un retour sur investissement. Ils vont jusqu'à prendre des cours de psychologie, de finance, de droit… pour affiner leurs arnaques, pour qu'elles aient l'air plus vraies que nature* ».

Qui sont les victimes ?

Même si le profil de l'arnaqué n'existe pas, on remarque toutefois trois principales catégories de victimes. Pour le psychologue Cyrille Le Jamtel, on peut distinguer les hyper consommateurs, les personnes isolées ou fragilisées et les internautes peu renseignés sur les dangers du Web. Ces trois types de victime sont répartis dans toutes les classes de population :

- « *Paradoxalement, la première catégorie de victime va être celle des hyper consommateurs ; assez jeunes et dynamiques, ils sont rodés aux codes du Web. Ils sont vulnérables car ils manquent d'attention. Ils ont le sentiment que leur habitude d'Internet les protège et se laissent piéger, parce que trop sûrs d'eux-mêmes* ».
- La deuxième catégorie semble plus évidente à cerner : « *Ce sont des gens isolés ou fragilisés par la maladie, une rupture sentimentale, un divorce ou encore le chômage… Il y a une multitude*

de paramètres. Leur vulnérabilité vient du fait qu'ils n'ont aucun effort à fournir pour se connecter. Dans la vie, il faut fournir un effort pour aller vers les gens ou acheter quelque chose. Avec Internet, c'est le monde qui vient vers eux sans aucune démarche de leur part. C'est l'attrait de cette facilité de contact qui va les rendre vulnérables ».

- La troisième et dernière catégorie est de loin celui qui offre aux escrocs le plus large éventail de proies. Elle cible la plus grande part de la population : « *La majorité de la population n'est pas une grande consommatrice sur le Net. Les gens sont généralement méfiants, mais chez eux, l'arnaqueur bénéficie d'un atout majeur : l'effet de masse. On a généralement tendance à estimer que si les autres achètent sur tel site, il n'y a pas de danger. C'est encore plus vicieux quand quelqu'un de votre entourage fait une bonne affaire. On se sent un peu bête de ne pas faire de même et à ce moment-là, on est particulièrement vulnérable car prêt à tomber dans n'importe quel piège* ».

À SAVOIR

Le seul trait commun qui connecte toutes les victimes : une confiance excessive à un moment donné. Confiance en soi, « je suis prudent, je ne risque rien », ou confiance dans le vendeur, « je pense que c'est quelqu'un d'honnête ».

Et parce que croire en l'autre garantit la sauvegarde des relations sociales, il est impossible à la plupart des gens de refuser d'établir une relation d'échange, même avec quelqu'un qu'ils n'ont jamais vu. Pour beaucoup, même si le scénario de l'arnaque est flagrant, l'attrait de gagner de l'argent ou d'entretenir une relation, qui plus est avec quelqu'un qui semble parfait, suffit.

Isoler pour mieux manipuler

Il peut paraître invraisemblable que des personnes, disposant parfois de ressources limitées, soient prêtes à s'endetter pour des personnes qu'elles n'ont jamais croisées dans la réalité. Et c'est pourtant souvent le cas.

Dans le cas des arnaques à l'amour, l'escroc qui sévit sur Internet peut se rapprocher du dealer. Les photos, les compliments et la valorisation qu'il va servir à sa victime font office de « première dose gratuite ». C'est un système aliénant. On refuse de se passer de sa dose quotidienne de compliments, on en a besoin. Ensuite, vous êtes accro et vous y retournez, quel que soit l'enjeu. Quelles que soient les alertes ou les avertissements que vous aurez eus, vous continuerez. Inconsciemment, vous allez rejeter la méfiance au profit du bonheur et de la joie immédiate que vous provoque la valorisation de l'arnaque. Même si l'on a conscience de l'arnaque, si les fils sont trop gros pour être ignorés, on aura tendance à continuer et à s'enfoncer. « *Parce qu'inconsciemment, on ne peut plus s'en passer* ».

« *Toute cette technique de flagornerie peut pourtant s'écrouler quand la victime fait partie d'un groupe solide – famille ou amis, par exemple* », nous rappelle Cyrille Lejamtel. L'objectivité des autres membres va les mener à se méfier et à douter de la sincérité des flatteries. Faisant part de leurs doutes à la victime potentielle, ils vont éveiller ses soupçons et peut-être lui permettre de sortir de l'arnaque.

Pour éviter ce scénario qui lui est défavorable, l'escroc va utiliser une technique bien connue des sectes, il va isoler sa victime. Par essence, on est seul devant son ordinateur lors de la connexion. L'arnaqueur va donc devoir couper sa victime de tous ses liens familiaux ou amicaux sans pour autant la braquer. Pour cela, converser par ordinateurs interposés est un atout. « *Les*

escrocs vont copier les codes habituels des consommateurs pour les rassurer. Visuellement, les sites frauduleux ressembleront à des plateformes connues. Et puis, généralement, lorsqu'on se connecte à Internet, on est chez soi. C'est un environnement que l'on connaît, qui nous est familier. On se sent à l'abri dans un univers rassurant. Psychologiquement, c'est très important », affirme Cyrille Le Jamtel.

Internet est un monde d'universalité. Malgré la solitude de l'utilisateur devant son écran, l'internaute va avoir une illusion de groupe, de communauté. « C'est l'effet "tous connectés". Il est notamment multiplié en temps de crise. Les gens sont psychologiquement affaiblis et ont l'impression d'être tous isolés. Sur Internet, c'est tout le contraire. Certains sites annoncent le nombre de personnes connectées au même moment que vous. Même si ce sont des gens que vous n'avez jamais vus et que vous ne connaissez pas, vous avez l'impression de ne pas être seul. Ce qui est dangereux, c'est que c'est totalement faux. On n'est jamais plus seul et vulnérable que devant son écran ».

Mais comment, par un simple lien virtuel, peut-on couper une victime de ses attaches ? La technique consiste en une sorte de harcèlement par e-mail ou par téléphone. Tant que la victime sera devant son écran à réfléchir ou à lire et répondre de façon la plus détaillée possible aux mails de son escroc, elle ne prendra pas le temps d'en parler à ses proches. Ce type de techniques s'avère particulièrement efficace dans le cadre des arnaques à l'amour. « *Une fois manipulé par l'escroc, on s'isole. On lui parle pendant des heures sur messagerie instantanée, on s'envoie des e-mails. Il suggère de cacher la relation pour faire la surprise plus tard… tout pour que la famille ne soit pas*

À SAVOIR

Quel que soit le nombre d'internautes connectés en même temps que vous, un groupe virtuel ne remplacera jamais un cercle d'amis réels et bien présents.

au courant », explique Marie, spécialiste de ces problèmes. Dans le cadre d'arnaques à l'amour, ce sont les proches qui sont les mieux placés pour remarquer l'arnaque. Sans regard, ni jugement extérieur, la victime isolée est plus facilement manipulable. Cyrille Le Jamtel acquiesce : « *Le groupe – famille, amis… – a un effet protecteur. Isoler sa victime sans alerter l'entourage est une mécanique simple mais délicate. La meilleure méthode consiste à flatter sa victime. Tout comme dans une secte, on va la valoriser pour la rendre unique et lui faire croire qu'elle a un rôle plus important que les autres. La flatterie endort la sensibilité au danger* ».

Il arrive souvent que la victime soit tellement manipulée par son arnaqueur, qu'elle refuse de voir la vérité en face. En effet, inconsciemment, le mal est plus profond. « *L'être humain n'aime pas avoir tort, affirme le psychologue. Il a du mal à reconnaître s'être trompé et va, sans en avoir réellement conscience, foncer tête baissée dans l'arnaque, malgré les signes qui l'auront alerté, pour ne pas avoir à l'avouer* ». Dans ce cas de figure, les avertissements de la famille n'ont parfois pas d'autre effet que d'isoler encore plus la victime qui se sent rabaissée et préfère s'illusionner dans le scénario de l'arnaque.

Si le groupe peut avoir un effet bénéfique sur l'arnaqué dans le sens où ses critiques peuvent éveiller la méfiance, les familles peuvent avoir l'effet inverse. « *Parfois, des gens nous appellent pour nous dire : "Mon père est en train de se faire arnaquer. Réussiriez-vous à lui montrer l'arnaque et à lui épargner plus de dépenses ? Car il n'écoute pas sa propre famille". Dans ces cas-là, nous intervenons directement auprès de la victime* », explique Marie. Une intervention nécessaire, mais qui risque de braquer la victime. Les victimes vivent très mal l'ingérence initiée par leur propre famille – généralement les enfants. « *C'est très délicat, avoue Cyrille. Quand on a quarante ou cinquante ans et que sa propre famille contacte une association pour raisonner son proche, on vit ça terriblement mal ! Ça infantilise et la plupart des gens ne le supportent pas. C'est un sentiment de honte qui s'ajoute à l'humiliation de s'être*

fait avoir par un escroc. Comme la nature humaine a tendance à ne pas reconnaître ses erreurs, on préfère généralement s'enfermer dans le déni… Et cela produit l'effet inverse de la réaction souhaitée : un isolement plus grand, une rupture avec la famille et une plus grande vulnérabilité ».

Prendre le temps de la réflexion

Nous sommes tous vulnérables sur Internet. Certaines personnes, notamment les novices, le sont plus que d'autres. Pourtant, derrière son ordinateur, on se sent à l'abri des influences extérieures. La majorité des gens estime qu'avec la barrière d'un écran, il est possible de réfléchir aux propositions à tête reposée, sans se sentir pressés par un interlocuteur physique. C'est faux. Les arnaqueurs vont tout tenter pour vous faire acheter le plus vite possible, vous ôter le maximum de temps de réflexion. Une technique particulièrement efficace lorsqu'il s'agit de produits technologiques très demandés, type iPad. *« Ils vont vous dire qu'ils ont d'autres acheteurs sur le coup, qu'ils veulent le vendre avant de partir à l'étranger, ils vont susciter du désir chez vous en disant que le produit est neuf, en le vendant à un prix attractif… »*, raconte Christine. L'acheteur va lui-même se mettre la pression et se forcer à réfléchir vite, pour acquérir à coup sûr ce bien qui lui plaît tant. Parce que pour endormir votre vigilance, il y a une méthode imparable : utiliser la corde sensible. Reste à trouver cette corde. Elle varie selon les arnaques :

- Lors d'une vente entre particuliers, l'escroc va généralement jouer sur la rareté du produit et la nécessité de l'acquérir immédiatement.
- Dans le cas de vente ou de location d'appartement, le vendeur va se montrer faussement méfiant et faire en sorte de retourner la situation. Vous allez fournir des justificatifs et

finir par envoyer un acompte pour prouver votre bonne foi et votre intérêt dans l'annonce.

Témoignage

C'est ce qui est arrivé à Annie V., étudiante en sociologie dans le sud de la France. Elle cherche un appartement à louer à Paris pour poursuivre ses études dans la capitale. Elle se met donc en quête d'un studio sans autres exigences qu'il soit intra-muros. Mais les annonces qu'elle trouve dans les agences immobilières indiquent des tarifs bien au-dessus de ses moyens. Elle se retourne donc vers les sites de particuliers. Elle trouve effectivement quelques propositions plus raisonnables, dont une, qui attire particulièrement son attention. Un petit deux-pièces, au prix d'un studio, en plein 13e arrondissement, tout près de sa faculté. Une aubaine, se dit-elle. Elle contacte donc immédiatement le vendeur, lequel se montre réticent. Il lui explique avoir déjà eu affaire à des plaisantins ou des acheteurs peu sérieux qui lui fixaient un rendez-vous pour visiter l'appartement et ne se présentaient jamais. Résidant à Rennes, il avait donc déjà fait plusieurs voyages jusqu'à la capitale pour rien et se méfiait désormais de tous ceux qui le contactaient. Annie tente de le rassurer. Elle a vraiment besoin de ce logement et assure pourvoir lui fournir tous les justificatifs qu'il demande pour appuyer sa demande. Afin de prouver sa bonne foi, le loueur lui demande une avance à hauteur de la moitié d'un mois de loyer. Il estime de cette façon que, si elle est prête à payer cet acompte, elle se présentera à la visite de l'appartement et sera une locataire sérieuse. La pénurie de logement en région

parisienne pousse donc Annie à lui faire un dépôt de 350 euros par Mandat Cash Urgent, comme convenu avec le loueur. Il lui assure ne pouvoir retirer l'argent que lorsqu'elle lui aura remis le numéro de reçu, numéro qu'elle doit lui transmettre lors de la visite et de la signature du bail. Au jour J, la loueuse potentielle se présente devant l'immeuble et patiente. Aucun vendeur à l'horizon. Elle tente de le joindre par téléphone : aucune réponse. C'est après vérification de son compte qu'elle remarquera que les 350 euros ont bien été retirés, mais à Lille, et non à Rennes. Et ce, sans le numéro de reçu.

Dans ce genre de cas, l'escroc va endormir la méfiance de son interlocuteur en se montrant encore plus frileux que lui. Le locataire potentiel va trouver normal que son interlocuteur se méfie et souhaite avoir affaire à des clients sérieux. Il va donc tout faire pour rassurer le vendeur, quitte à passer outre sa propre réticence et à envoyer de l'argent sans avoir vu l'appartement. Pour le psychologue, c'est une méthode très efficace. « C'est humain de se méfier. Mais dans ce cas-là, en se montrant hyper prudent, l'escroc va se faire passer pour honnête. Arnaqueur et victime vont alors partager la méfiance. Avoir un trait commun rapproche les individus et pousse à la confiance. Ensuite, tout est une question de dosage pour s'attirer la confiance de la victime, lui laisser croire qu'elle est le maître du jeu, et au final la presser de payer ».

Savoir déjouer leurs pièges

Tout le monde utilise aujourd'hui Internet. Mais seule une proportion très restreinte de personnes sait réellement en

exploiter toutes les capacités. Et pourtant, certaines petites astuces très simples pourraient permettre de déceler une arnaque dès le premier mail. Des moyens méconnus, qui sont pourtant à la portée de tous.

Le technicien « Zythom » nous donne son avis d'expert en informatique pour déjouer les pièges des arnaqueurs. Selon lui, il n'y a pas de règle absolue. Mais il ajoute, « les arnaqueurs vont jouer avec les leviers classiques de la psyché humaine. Si vous avez l'impression de faire une très bonne affaire et que vous avez envie de conclure au plus vite, c'est à ce moment que vous tombez dans le panneau d'une arnaque. Une trop belle affaire doit susciter la méfiance, pas la cupidité ». De même, l'expert judiciaire nous indique qu'il est préférable de passer des commandes sur des sites connus, ayant une bonne réputation. « *Il ne faut pas donner d'informations sensibles sans vérifier le site à qui vous allez les confier : sa réputation, le chiffrage des formulaires de saisie par exemple* ». Il nous rappelle également qu'aucun organisme sérieux ne demande de communiquer un mot de passe ou un code secret par e-mail. L'expert conclut ainsi : « *Le meilleur conseil que je puisse donner est le suivant : toujours demander un avis à une autre personne, ne jamais céder à une envie compulsive. L'arnaqueur connaît les astuces permettant d'isoler sa cible et agir sur ses points faibles. Le simple fait de parler à une personne de son entourage permet souvent d'être alerté et d'éviter le piège* ».

Outre ces conseils de base pour éviter les arnaques, les membres d'associations proposent d'autres astuces plus techniques pour vérifier si votre interlocuteur est bien celui qu'il prétend être. Nous nous sentons parfois démunis face à la complexité des outils informatiques, et même si la plupart des usagers d'Internet restent des néophytes, il peut parfois

À SAVOIR

Plus la relation s'étoffe, plus l'escroc dispose de moyens de pression sur vous.

s'avérer utile de connaître quelques rudiments en informatique. « *Savoir tracer une adresse IP, c'est très simple* », affirment les responsables de l'AVEN France. Cette technique, malgré toutes les connotations illégales que les mots "tracer" et "adresse IP" puissent véhiculer, est à la fois parfaitement légale et très efficace. En quelques clics, vous pouvez savoir (*cf.* page 78) si votre interlocuteur vous a contacté depuis Amiens, comme il l'affirme, ou à partir d'Abidjan. « *La plupart des utilisateurs du Net ne sont pas sensibilisés à ce genre de méthodes. Ils utilisent Internet avec insouciance et n'imaginent pas que de l'autre côté, il y a parfois des gens malveillants qui, eux, maîtrisent toutes les ficelles du Net et qui peuvent vous piéger facilement* ».

Facebook, notamment, est devenu une véritable mine d'or pour les arnaqueurs. Lorsqu'une relation se noue avec un escroc, qu'elle soit commerciale ou sentimentale, il dispose d'informations de toutes sortes. Vos noms et prénoms pour commencer, mais aussi votre ville de résidence par exemple, autant d'informations généralement visibles sur votre profil Facebook.

« *Il ne faut pas oublier que ce sont de talentueux manipulateurs. Ils vous demanderont des informations très personnelles de façon anodine : "Où est-ce que tu travailles ?", "Tu es mariée ?"...* », rappelle Marie de l'AVEN. « La plupart des gens ne sécurisent pas leurs comptes Facebook. Dans le cas d'une arnaque à la Webcam, l'escroc pourra facilement trouver tous les contacts de sa victime et la menacer de leur envoyer des vidéos compromettantes ». Des scénarios rarement aboutis. Même si la victime se montre réticente à payer ; pour les escrocs, diffuser la vidéo aux proches revient à se priver de son propre moyen de pression.

EN RÉSUMÉ

- Il n'y a pas de profil type de victime, personne n'est à l'abri sur Internet.
- Il est important de toujours se remettre en question. Les escrocs jouent sur notre confiance excessive en nos capacités.
- L'arnaqueur va isoler sa victime pour mieux la manipuler. Le simple fait de parler à une personne de son entourage permet souvent d'être alerté et d'éviter le piège.
- N'agissez pas dans la précipitation. Accordez-vous un temps de réflexion avant toute transaction.
- Renseignez-vous sur le site sur lequel vous surfez avant de démarrer une transaction ou de divulguer vos données personnelles.
- Sur Internet, sécurisez vos informations afin qu'elles ne soient pas à la portée de tous.

PARTIE 2

ARNAQUES 2.0

Des problèmes sur Internet, nous en rencontrons tous les jours. Nos boîtes mail sont inondées de courriers indésirables qui nous annoncent avoir gagné à la loterie ou être les heureux gagnants du dernier iPhone à la mode. Sur les réseaux sociaux nous sommes envahis par une multitude d'applications qui souhaitent avoir accès à nos informations, nos données personnelles. Et même lorsque l'on surfe sur un site sécurisé, il nous arrive d'être confronté à un litige avec un professionnel. Bien que le support soit virtuel, il ne faut pas oublier que les risques, eux, sont bien réels. Plus la proportion des connectés grandit, plus les escrocs tenteront leurs chances.

Même si, globalement, nous sommes tous conscients de ces problèmes, nous nous croyons à l'abri derrière notre écran. C'est une erreur ! Les arnaqueurs ont plus d'un tour dans leur sac pour nous soutirer de l'argent et n'hésitent pas à user de toutes les armes pour nous manipuler. Pour mieux se défendre face à ces menteurs professionnels, il faut sans cesse être vigilant. Comment faire alors la différence entre une véritable offre et une arnaque ? Comment savoir à qui on a affaire lorsque notre ordinateur nous sépare de notre interlocuteur ? Même si les arnaqueurs font preuve d'une grande adaptabilité, ils suivent généralement le même schéma de base. Pour atteindre leurs buts, ils utilisent différents moyens. Entre l'arnaque classique à la petite annonce et l'arnaque à l'amour, il existe tout un panel de variantes, utilisant des scénarios improbables. Il existe cependant des signes avant-coureurs permettant de déceler ces fraudes. Comment faire pour comprendre les méthodes utilisées par ces escrocs ?

CHAPITRE 3
DU LITIGE À L'ARNAQUE

DÉFINITIONS

- **Conditions générales de vente** : règles d'utilisation concernant un service, qui vont régir les rapports et les conflits qui peuvent naître entre l'éditeur du site et les visiteurs du site lors d'une transaction.
- **DGCCRF** (Direction générale de la concurrence, de la consommation et de la répression des fraudes) : mise en place par l'État, elle a pour but de lutter contre les pratiques anticoncurrentielles mais aussi de protéger les consommateurs.
- **Litige** : terme juridique désignant un différend entre deux parties, qui peut être réglé à l'amiable sans que des poursuites ne soient engagées. À ne pas confondre avec une arnaque.

Simon U.

Utilisé dans le langage courant, le terme « arnaque » s'apparente souvent à un simple litige. Vous surfez et faites un achat sur un site sécurisé, mais la transaction ne s'effectue pas comme vous le souhaitez. En ce cas, n'hésitez pas à porter plainte, les services de l'État dont la DGCCRF peuvent intervenir... Pour

éviter les différends sur Internet, pensez à lire attentivement les conditions générales de vente (CGV) du commerçant et gardez un maximum de traces de vos échanges et de vos paiements...

Témoignage

Simon U. voulait offrir à sa famille un voyage au Maroc pour Noël. Pour le faire dans la plus grande discrétion, il décide de se renseigner sur Internet et d'en commander un. Il fait donc le tour des voyagistes en ligne, et se détourne au maximum des sites trop succincts, ou trop mal notés par les internautes. Sur l'un d'entre eux, il trouve pourtant le voyage dont il avait envie ; 6 jours et 5 nuits à Marrakech, dans un hôtel quatre étoiles en pension complète. Parfait pour passer un Noël au chaud, entouré de superbes paysages. Ce qui le séduit dans le descriptif du séjour, c'est que tout est compris : les nuits d'hôtel, les repas en pension complète, les transports depuis l'aéroport... mais aussi certaines excursions, une balade à dos de dromadaire, une virée en 4x4 dans le désert... La décision de Simon est presque prise. Il ne lui reste plus qu'à jeter un œil aux photos des chambres : elles sont parfaites. Vue sur la piscine, lumineuses et spacieuses, elles ont tout pour faire de ce voyage un séjour réussi. En quelques clics, il se retrouve sur une page Internet sécurisée pour réserver. Billets d'avion, réservations d'hôtel, déplacements, tout est prévu par l'agence et il s'apprête à payer en toute confiance. On lui demande tout de même, avant de confirmer sa réservation, de lire attentivement les conditions générales de vente. Consciencieux, il clique sur le petit lien et voit s'ouvrir une nouvelle fenêtre. C'est en s'apercevant que la barre verticale de

défilement rétrécit et que la page se noircit de caractères, d'une taille tellement petite qu'ils en deviennent illisibles, que sa volonté d'en détailler chaque point s'étiole. Il lit les deux premiers paragraphes... puis renonce. Simon accepte les CGV, et valide son paiement. Quelques mois plus tard, toute la famille atterrit à Marrakech. Même si les enfants sont un peu surexcités de ce voyage à l'étranger pour les fêtes, tout se présente pour le mieux. Jusqu'à leur arrivée à l'hôtel. On leur attribue, comme prévu, deux chambres doubles, une pour les parents, l'autre pour la fratrie de jeunes ados qui les accompagne. Or, les chambres n'ont rien à voir avec ce que le père avait pu repérer sur le site du voyagiste. Bien plus petites que ce que les photos lui avaient promis, la vue qu'elles proposent donne surtout sur un terrain vague, et, au loin, un autre complexe hôtelier. Rien du tableau idyllique de piscine et de palmiers qu'il avait souhaité. Il tente de se plaindre à la réception : malheureusement, en période de fêtes, tous les lits sont occupés et il est impossible à l'hôtel de reloger la famille dans une chambre plus appropriée à ses exigences. Tant pis, elle prend son mal en patience. Mais la liste des déceptions ne fait que commencer. Le spa de l'hôtel est fermé pour plusieurs mois pour cause de rénovation. Les excursions, qui avaient séduit Simon, étaient, certes, prévues dans le prix, mais elles sont complètes : il fallait s'inscrire à l'avance. Il avait payé une prestation « all inclusive » pour que les enfants puissent se gaver de soda et pour que sa femme et lui profitent de leurs vacances pour s'accorder quelques dégustations d'alcools : une

prestation qui semble s'être perdue dans les méandres d'un ordinateur, entre son écran et celui de l'hôtel... À son retour de vacances, Simon est bien décidé à réagir. Il estime avoir eu affaire à des commerçants malhonnêtes et refuse de se laisser arnaquer sans demander des comptes. Il se rend donc tout d'abord sur le site du voyagiste pour se plaindre de la prestation fournie et menace d'un recours en justice s'il n'obtient pas une compensation financière. Dans le même temps, il poste sur des forums spécialisés des commentaires acerbes et raconte sa mésaventure. Sûr d'être dans son droit, il n'hésite pas à rechercher d'autres victimes afin d'avoir plus de poids face à la société prestataire du voyage. Pourtant, il déchante en recevant, quelques jours plus tard, la réponse du voyagiste. Tout d'abord, il était bien spécifié, en bas de page, que les photos vantant les chambres de l'hôtel n'étaient qu'un exemple et ne devaient en rien constituer une assurance d'obtenir la même prestation. Ensuite, le site s'engage clairement, dans les conditions générales de vente, à honorer les prestations qui sont de son ressort mais ne peut en aucun cas s'engager à la réalisation de celles qui sont prévues par l'hôtel. Le spa en rénovation ? C'est du ressort de l'hôtelier. Les excursions ? Il était stipulé sur le site qu'elles nécessitaient une réservation préalable relevant de la seule initiative du particulier. La prestation « all inclusive » qui n'avait pas été prise en compte ? Une erreur de l'hôtelier... Le voyagiste n'a pour seule prérogative que de faciliter les réservations de son client, mais ne peut se porter garant pour l'hôtel partenaire.

Des restrictions parfaitement claires et établies sans conteste dans les conditions générales de vente que le client est censé lire et accepter avant son paiement. Lors d'une transaction avec un commerçant professionnel, la loi oblige le vendeur à rendre visibles les conditions générales de vente. Elles constituent une sorte de contrat entre les deux parties, expliquant les prérogatives de chacun et les conditions dans lesquelles l'une des deux parties peut les rompre ou les rendre caduques. Il est donc indispensable de lire les CGV, même si elles sont indigestes, complexes et particulièrement longues. Mieux vaut prendre un moment pour les imprimer et en prendre connaissance, plutôt qu'être finalement en porte-à-faux par manque d'attention. Si vous avez un doute sur ces conditions ou si elles ne vous conviennent pas, abstenez-vous de la transaction chez ce commerçant, car il est indispensable d'accepter les CGV pour mener à bien une vente avec un professionnel. Souvent, il s'y dédouanera de soucis indépendants de sa volonté : problème d'acheminement d'un paquet par La Poste, litige avec un hôtelier partenaire...

Litige ou arnaque : comment faire la différence ?

Au-delà de l'attention que vous devez porter aux conditions d'une transaction entre votre interlocuteur et vous, il peut arriver que vous soyez en conflit avec un vrai vendeur professionnel. L'amalgame est alors vite fait entre une réelle arnaque et un litige avec un commerçant. Ainsi, une simple erreur peut être taxée d'escroquerie.

L'association LesArnaques.com est rompue à ce genre de situations. Son président de 2006 à 2013, Joël Guillon, l'explique : « Si l'erreur est non intentionnelle, on peut croire que le professionnel n'a pas souhaité vous tromper et on peut ouvrir une procédure civile afin de recevoir des dommages et intérêts.

Par contre, si on a la conviction, et les preuves, que le professionnel vous a trompé, dans ce cas, on peut ouvrir une procédure pénale afin qu'il puisse en rendre compte. À vous bien sûr, mais également au procureur de la République qui, dans un tribunal, représente l'État ».

Créé en 2001, le forum de l'association recueille nombre de témoignages de victimes. Des personnes flouées par des arnaques à la nigériane, ou encore des escroqueries à la petite annonce. Mais aussi des consommateurs confrontés à des litiges envers des commerçants. Joël et les bénévoles qui se sont joints à lui mettent donc à profit leurs expériences pour différencier arnaques et litiges, et surtout pour aiguiller les victimes. En effet, juridiquement, les actions ne s'intentent pas envers le même tribunal que l'on ait affaire à une escroquerie ou à un litige. « *Lorsque c'est une arnaque, c'est le tribunal pénal qui est compétent. Lorsque c'est un litige, c'est au tribunal de proximité qu'il faut s'adresser, si la somme au centre du litige est inférieure à 4 000 euros. Si, elle est comprise entre 4 000 et 10 000 euros, c'est au tribunal d'instance qu'il faut recourir* », explique Joël.

Pourtant, il y a tout un panel d'actions à entreprendre avant d'en arriver à des mesures juridiques. Il est courant de s'entendre à l'amiable. En effet, si, lors d'un litige, il n'y a pas de volonté de la part du commerçant de faire du tort à son client, les deux parties peuvent généralement se mettre d'accord sur un arrangement sans avoir à en référer à la justice. Sur le forum de l'association, lesarnaques.com, les modérateurs font souvent office de médiateurs. Un e-commerçant a parfois beaucoup de clients et peut ne pas voir ses propres erreurs. « *Souvent, les personnes qui nous contactent n'arrivent pas à joindre le professionnel et demandent de l'aide. Nous nous occupons alors de rediriger leur témoignage* », explique Joël. Une action qui intervient avant toute action en justice.

« Il arrive que le professionnel ait des problèmes de gestion de clients. Mais cela devient grave quand il ne prend pas la peine de contenter son client après qu'il se soit plaint », affirme le président de l'association. Aussi, le site prévient ses contributeurs : lorsqu'une victime demande de l'aide, l'association relaie son message vers le professionnel concerné. Au-delà de huit jours, si l'affaire reste sans suite et que le professionnel n'a pas recontacté la victime, il lui revient d'intenter des actions en justice.

À SAVOIR

Un problème avec un commerçant ne signifie pas forcément une arnaque, surtout quand on a affaire à un site marchand professionnel.

L'équipe de l'association peut vous donner un coup de pouce dans vos démarches, notamment en vous orientant et en vous donnant quelques conseils. *« Nous traitons les témoignages suivant le nombre de victimes contre une même enseigne. Idem si on a réellement affaire à un site Web illicite, nous essayons de rassembler les victimes afin de prouver devant le tribunal que les litiges sont nombreux, contrairement à ce que le commerçant pourrait vouloir faire croire ».*

Au-delà de son rôle de prévention active, l'association et son forum ont un rôle passif. Si un commerçant y est dénoncé, ses futurs clients sauront à qui ils ont affaire :

- soit le vendeur est digne de confiance, auquel cas il n'y a aucune raison pour que le litige déclaré ne se règle pas dans les meilleurs délais ;
- soit il ne l'est pas, et les témoignages déposés lui feront une assez mauvaise publicité pour alerter les futurs clients potentiels.

Toutefois, l'association se défend de tout jugement : *« Nous ne sommes pas juges et nous n'avons pas à intervenir directement en*

prétendant qu'une affaire est une arnaque ou un litige. C'est à nos lecteurs de juger si tel vendeur est fiable ou non au regard des précédents témoignages ».

L'État au service de vos litiges

Toutefois, il arrive que les sites concernés ne réagissent pas aux sollicitations de leurs clients mécontents.

Témoignage

C'est ce qui est arrivé à Célia M. Elle avait acquis sur un site spécialisé une série de meubles de jardin en bois. Sa commande, qui devait lui être livrée dans les cinq jours ouvrables, n'arriva que deux semaines plus tard... et dans la mauvaise couleur. Irritée du délai d'attente et de la méprise sur sa commande, elle contacte le vendeur pour demander un changement, ou, au pire, un remboursement. Réclamation à laquelle le site répond par un e-mail particulièrement sec : s'il fallait changer le mobilier, elle devrait se charger de payer les frais du transporteur. L'acheteuse refuse et exige un changement immédiat, aux frais du vendeur : l'erreur n'étant pas de son fait, elle estime n'avoir rien à payer. Son interlocuteur ne l'entend pas ainsi. Célia, greffier à la retraite, a une bonne connaissance des lois et refuse de se laisser faire. Elle demande cette fois un remboursement ou un échange aux frais du commerçant par lettre recommandée avec accusé de réception. Elle l'y informe de son intention d'en recourir à la justice si sa demande n'est pas prise en compte dans la semaine qui suit la

réception du courrier. La semaine passe sans que le site ne manifeste un quelconque signe. Elle engage donc quelques démarches. Après un passage au commissariat pour déposer une plainte elle retourne à son ordinateur, sur Internet. Elle visite forum sur forum et y poste à chaque fois un commentaire racontant son histoire, demandant aux futurs clients de se méfier et aux anciennes victimes de se manifester afin que la justice puisse constituer un dossier contre ce commerçant, somme toute peu scrupuleux. Célia signale ensuite son interlocuteur à la DGCCRF. Pour clore la journée, elle envoie un nouveau courrier en recommandé au commerçant, l'informant de ses démarches. Elle assure pourtant qu'elle retirera sa plainte si le commerçant récupère le mobilier de jardin et lui renvoie sa commande, dans la bonne couleur, dans les délais prévus sur le site et surtout à ses frais. Quelques jours plus tard, elle reçoit un e-mail du service client lui assurant que le commerçant régulariserait la situation et honorerait ses engagements dans les plus brefs délais. Célia, elle aussi, respecte sa promesse et retire sa plainte. Mais elle ne s'est pas portée garante pour toutes les autres victimes qui, entre-temps, ont intenté un recours en justice contre le commerçant.

Dans la majorité des situations, il est préférable pour les deux parties qu'une solution amiable résolve le litige. Pourtant, ce n'est pas toujours possible. Dans ces cas-là, la première chose à faire est d'exiger un remboursement, l'échange de la marchandise ou, plus largement, la résolution du problème, par une lettre recommandée avec accusé de réception. Par ce biais, si vous devez plus tard intenter une action devant les tribunaux, vous

aurez, par l'accusé de réception, la preuve que vous avez bien demandé réparation dans les délais imposés par le commerçant. Si vous ne recevez aucune réponse à vos demandes, vous pouvez contacter une association. Certaines, telles que LesArnaques.com, ont une grande expérience de la médiation et peuvent avoir un certain poids sur les commerçants. Si toutefois cette méthode ne porte pas ses fruits, il ne vous reste plus qu'à porter plainte et en informer le commerçant, une fois de plus, par l'envoi d'une lettre recommandée.

Malgré l'apparente inaction de l'État, il existe des organismes officiels chargés de surveiller et d'encadrer le commerce, aussi bien physique que virtuel. La DGCCRF en est une. « *Nous sommes compétents sur les sites commerciaux, mais aussi sur les annonces de particuliers. Il nous arrive aussi souvent d'être actifs sur les réseaux sociaux, car aujourd'hui, on y trouve des offres commerciales au même titre que sur des sites marchands* », expose la responsable de la communication de l'organisme. Un service dont l'objectif est simple : assurer le respect de la loi française. Si les litiges et les entorses à la législation font partie de ses spécialités, « *nous ne sommes absolument pas compétents en ce qui concerne les arnaques à la nigériane ou ce type d'arnaque* ».

Les actions de la DGCCRF s'articulent autour de deux axes : les plaintes des particuliers et la veille sur Internet.

- Dans le premier cas, « *ce sont des victimes qui portent plainte au commissariat, qui se signalent sur notre site ou en nous contactant par courrier. Il arrive aussi que nous soyons alertés par des internautes vigilants qui attirent notre attention sur telle ou telle pratique qui leur semble douteuse* ». Des actions essentielles, mais malheureusement peu relayées : la faible proportion des plaintes n'avantage pas le service qui sait pertinemment que le nombre de plaignants est largement inférieur à celui des victimes. Mais ce recours à la participation populaire n'est pas l'essentiel de leur travail.

- Les services de l'État recherchent sur Internet tout ce qui peut s'apparenter à un non-respect des règles. « *Notre mission principale, c'est de s'assurer que toutes les informations obligatoires soient présentes. Il faut que le site soit clair, transparent, que les offres commerciales respectent la loi, qu'il y ait un numéro de service après-vente ou encore que les conditions générales de vente soient parfaitement visibles* ». Lorsque l'organisme repère un élément suspect ou illégal, il enquête et affine ses recherches. Mais son action se limite à cela : « *Nous avons les mêmes pouvoirs que les forces de police. Nous relevons l'infraction et dressons un procès-verbal. Ensuite, le dossier nous échappe, il passe entre les mains de la justice lorsque nous le remettons au procureur. C'est ce dernier qui va décider des charges à retenir et des poursuites à entreprendre* ».

CONSEIL D'EXPERT

Si les lois limitent souvent l'action de la DGCCRF aux frontières françaises, c'est un frein qui tend à se desserrer : « il existe de plus en plus de procédures communautaires, notamment au sein de l'Union européenne ».

Tout système présente des failles

Les procédures sont surtout efficaces contre des vendeurs professionnels. Toutefois, il arrive que des litiges liés au paiement surviennent lors de transactions entre particuliers. Pour réduire les risques de mésentente ou d'arnaque, fuyez les transactions qui n'utilisent pas des moyens sécurisés du type Paypal. Toute solution ne pouvant être garantie 100 % sans risque, il arrive que certains litiges se déclarent suite à un problème de paiement, quand bien même vous auriez eu recours à Paypal. Si vous vous trouvez dans cette situation, nous vous décrivons la meilleure façon de procéder.

En pratique

Le recours auprès de Paypal

Vous avez effectué un paiement *via* Paypal et vous attendez votre commande. Si, après quelque temps, vous n'avez pas reçu votre paquet, vérifiez les informations de suivi, notamment en contactant le service d'expédition que vous aurez privilégié, tel que La Poste. Si le retard ne vient pas de lui, contactez le vendeur. Une franche communication entre les deux protagonistes peut désamorcer bien des situations délicates. Si, malgré des e-mails et/ou des coups de téléphone, votre problème ne se règle pas, il vous faut déclarer un litige auprès de Paypal. Commencez par chercher le numéro de transaction Paypal en vous connectant sur votre compte. Recopiez-le dans le gestionnaire de litiges, en tenant bien compte des majuscules et des minuscules. Une fois cette opération effectuée, expliquez la raison du litige (objet endommagé, de valeur inférieure à celle qui était prévue, non conforme...) Le dossier est alors entre les mains de Paypal qui va mener une enquête et envoyer un message au vendeur, l'informant de l'ouverture d'un litige. Si Paypal estime que vous êtes dans votre droit, ils demanderont un remboursement partiel ou intégral à votre interlocuteur. Paypal dispose de moyens très coercitifs. Si le vendeur accepte de reprendre son objet, vous recevrez un e-mail de Paypal et vous aurez dix jours pour renvoyer le bien, à vos frais, et fournir un numéro de suivi du colis. Vous ne devez jamais supprimer les messages que vous échangez avec votre interlocuteur. Dans le cadre d'une arnaque ou d'un litige, ils sont la preuve de votre bonne foi et peuvent être décisifs en cas de poursuites.

Des sites trompeurs

Sur le Net, certaines activités sont légales mais parfois qualifiées d'arnaques par les consommateurs français. Pourtant, juridiquement, les deux cas ne sont pas comparables. Vous tomberez souvent sur des publicités et des annonces vous vantant l'ingéniosité de mères de famille ayant trouvé le moyen d'avoir des dents plus blanches, de maigrir en très peu de temps ou encore d'effacer durablement les rides. Souvent, cliquer sur ces publicités vous entraîne sur le site d'un prétendu média qui n'est généralement que la vitrine d'une entreprise.

Nous avons fait le test sur une annonce vantant l'ingéniosité d'une mère de famille faisant prétendument pester les dermatologues suite à la découverte d'une recette miracle. En cliquant sur cette annonce, donc, vous êtes redirigé vers un site présentant tous les aspects d'un média traditionnel d'informations. Or si vous tentez de cliquer sur un onglet tel que « monde » « politique » ou « justice », vous atterrissez sur une page de publicité vantant les propriétés antirides d'un médicament. Coïncidence, c'est le même médicament qui est cité dans l'article comme l'un des composants de cette recette miracle. Beaucoup d'éléments sont ensuite étranges, ou pour le moins particuliers : l'article a été posté le 8 septembre à 13 h 01 or nous nous connectons le 8 septembre à 10 h 33, soit plus de deux heures avant... Comment ce miracle est-il possible ? On y assure que l'ingénieuse maman habite « la région ». Mais quelle région ? Elle n'est

CONSEIL

Quelle que soit la transaction dans laquelle vous vous lancez, lisez toujours attentivement les CGV. En cas d'arnaque ou de litige, elles vous permettront de vous en remettre à la justice.

jamais citée. Ces détails n'ont pour l'instant rien d'inquiétant. Intéressons-nous de plus près à la solution miraculeuse : elle allie l'utilisation de deux produits, qui, combinés, effaceraient littéralement les effets du temps. Deux produits qui bénéficient actuellement d'une offre promotionnelle, si bien que, frais de port compris, vous n'auriez pas à débourser plus de 6 euros. C'est en détaillant les termes et conditions que tout s'éclaire. Si, après dix jours calendaires à compter de l'envoi des articles, vous n'avez pas annulé votre inscription, vous serez automatiquement enregistré et recevrez tous les mois un nouveau flacon. Traitement qui vous sera facturé plus de 79 euros par mois.

Cette façon de faire n'est pas illégale, tout est détaillé dans les conditions générales de vente. Et il existe des e-mails ainsi que des numéros de téléphone pour vous désinscrire. Mais qui lit attentivement et jusqu'au bout les fameuses CGV ?

EN RÉSUMÉ

- Les actions ne s'intentent pas à travers le même tribunal que l'on ait affaire à une escroquerie ou à un litige. Lorsque c'est une arnaque, c'est le tribunal pénal qui est compétent. Lorsque c'est un litige, c'est au tribunal de proximité qu'il faut s'adresser, si la somme au centre du litige est inférieure à 4 000 euros. Si, elle est comprise entre 4 000 et 10 000 euros, c'est au tribunal d'instance qu'il faut recourir.
- Toujours privilégier les moyens sécurisés de paiement.
- En cas de litige, adressez-vous à la partie adverse avec une lettre recommandée avec accusé de réception. Elle vous servira de preuve en cas de conflit.
- Lors d'une transaction avec un professionnel hébergé sur le Net, lisez toujours les CGV avant de valider votre paiement.

CHAPITRE 4
AFRIQU'ARNAQUES

DÉFINITIONS

- **Arnaque à la nigériane** : terme qui désigne un type de fraude qui sévit sur Internet. L'arnaqueur contacte ses victimes *via* Internet et abuse de leur crédulité pour leur soutirer de l'argent. C'est le fameux mail qui indique que votre interlocuteur a besoin de vous pour faire sortir de l'or de son pays...
- **Scam 419** : nom donné par les tribunaux nigériens à ce type d'arnaque. Scam 419 ou fraude 419 correspond au numéro de l'article du Code nigérian sanctionnant ce type de fraude. Par extension, ce terme désigne souvent les arnaques commises sur le continent africain.

Guillaume R.

Souvent, l'arnaque dépasse le simple litige avec un professionnel. Le but de votre interlocuteur est de vous manipuler afin de vous dérober de l'argent. Même si les arnaqueurs sont nombreux, beaucoup proviennent de pays étrangers, en particulier situés en Afrique. Afin de débusquer les faux bons plans en tout genre, il suffit parfois de flairer les bonnes pistes. Pour acquérir ces

réflexes qui vous sauveront peut-être, apprenez ici à déceler les fraudes en provenance de l'étranger.

Témoignage

Internet, Guillaume R. est né avec. À 25 ans, étudiant dans une école de commerce et grand amateur de technologies, il passe ses journées sur son ordinateur portable à écumer le Net pour y débusquer les bons plans. C'est justement ce qu'il pense avoir trouvé lorsqu'il déniche une moto sur un site de petites annonces. Justement une de celles qu'il recherchait : une Italienne au jaune un peu criard ; parfait pour slalomer avec style dans les bouchons parisiens, frimer devant les amis et impressionner les filles. Rédigée dans un français parfait, l'annonce est particulièrement alléchante. 3 000 euros pour une moto d'occasion en très bon état. À en croire la description et la photo, c'était inespéré. Il contacte donc le vendeur dans la journée pour s'assurer de la validité de l'offre. La réponse ne se fait pas attendre. Quelques heures plus tard, il reçoit, par retour de mail, une confirmation : oui, la moto de ses rêves est toujours en vente ; non, le prix n'a, entre-temps, ni baissé ni augmenté. Le contact qui se noue entre les deux hommes est cordial. Ils échangent quelques e-mails, l'acheteur s'accorde quelques jours de réflexion mais s'assure, par des contacts réguliers, que le bien est toujours en vente. Quand il finit par se décider à acheter le deux-roues, son interlocuteur lui fait part d'un léger problème logistique : actuellement au Bénin pour régler quelques problèmes familiaux, il est dans l'incapacité d'encaisser les fonds en France. Mais il rassure au plus vite son acheteur, la moto est bien

en France, laissée aux bons soins d'un ami domicilié à Metz. Pour que tout se passe dans les meilleures conditions, il propose à l'acheteur d'envoyer l'argent par Western Union afin que le vendeur puisse retirer les fonds depuis l'Afrique. Dès qu'il aura déposé l'argent, l'ami français transmettra le bien par le biais d'un transporteur professionnel aux frais du vendeur. Guillaume reste sceptique. Toute cette histoire le met mal à l'aise et il craint un mauvais tour. Il feint d'accepter et demande à son interlocuteur quelques jours pour envoyer l'argent. L'acheteur profite de ce temps pour se renseigner. Il trouve en effet sur Internet une description détaillée d'arnaques aux petites annonces dont certaines suivent parfaitement le scénario qu'on vient de lui servir. Voulant croire à l'existence réelle de sa moto, il assure à son vendeur avoir transféré les fonds et attend de voir évoluer la situation. Quelques jours plus tard, nouveau mail de son interlocuteur ivoirien. Il n'a pas pu récupérer les fonds et un problème avec le transporteur le force à payer plus cher que prévu. Une somme qu'il ne peut débourser, puisqu'en difficulté financière, tant qu'il n'a pas reçu le paiement. Il propose donc à Guillaume de faire un nouvel envoi d'argent afin de régler la moitié des frais de transport. Guillaume est consterné par la tournure que prend l'affaire. Désormais assuré de l'arnaque, il tape le nom de son interlocuteur et son adresse e-mail dans un moteur de recherche afin de cesser tout contact avec lui sans aucun remord. Effectivement, son nom apparaît, au milieu de bien d'autres pseudonymes, dans un listing

d'escrocs. Le jeune homme cesse dès lors tout contact et signale l'arnaque au site de petites annonces en communiquant l'adresse e-mail pour qu'il la blackliste. Mais il ne perd pas espoir pour autant de trouver la moto de ses rêves. Quelques jours plus tard, il retrouve une annonce : même prix, même texte, même photo du deux-roues Ducati, mais adresse mail et pseudonyme différents.

Des arnaques mondialisées

Internet est aussi mondial. On y a accès presque partout dans le monde. Il ouvre ainsi un plus grand panel de risques. L'adjudant-chef Jean-François Garnier, enquêteur spécialisé dans les nouvelles technologies au sein de la Gendarmerie nationale : « *Internet est en soi formidable. Mais les escrocs ont toujours existé. Tant qu'il y aura des flux financiers, il y aura des gens malintentionnés pour en tirer profit. Avant l'accès au numérique, les arnaques étaient plus difficiles à mener. La facilité d'obtenir une connexion Internet aujourd'hui augmente les risques. Par téléphone ou par La Poste, c'est assez délicat de mener une arnaque. Avec Internet, les escroqueries se sont mondialisées. Il est maintenant possible de les mener depuis un pays lointain en se faisant passer pour un Français* ».

À SAVOIR

La majorité des arnaques connues aujourd'hui vient d'Afrique de l'Ouest.

Avant la démocratisation d'Internet, les arnaques provenant de ces pays ne pouvaient pas nous atteindre, ou en moindre proportion. Elles sont aujourd'hui les plus dangereuses et les

plus actives. « *On les appelle "arnaques à la nigériane* », explique Christine Goubert, présidente et fondatrice de l'Association des victimes d'escroqueries à la nigériane en France (AVEN France). Elles ont été mises en place au départ par des Nigérians. « *On les appelle aussi Scam 419, du nom de l'article du Code pénal nigérian, qui punit ces pratiques comme un crime de sang* ». Des escroqueries géographiquement très ciblées qui ont tendance à se répandre. Principalement anglophones, les Nigérians concentraient leurs attaques sur les pays de langue anglaise.

Compte tenu des collaborations entre Anglais, Américains et pouvoirs publics nigérians, les escrocs se sont déplacés de peur des représailles. Ils ont émigré vers les pays limitrophes : Ghana, Bénin, Togo, Côte d'Ivoire, Cameroun. Ce sont eux qui ont, en quelque sorte, formé les escrocs d'aujourd'hui. Tout cela s'est passé courant 2006. Ensuite, ils se sont divisés le monde. Les pays francophones escroquent le monde francophone, idem pour les anglophones.De la même manière, certains pays se sont spécialisés dans certains types d'arnaques :

- Le Ghana et le Nigeria sont surtout présents dans les arnaques à l'amour[1].
- Le Bénin est connu pour les arnaques à la petite annonce ou les faux prêts.
- La Côte d'Ivoire est réputée pour jouer sur l'ensemble du panel d'arnaques connues. Une arnaque est née dans ce pays : l'arnaque à la Webcam[2], dérivée des escroqueries à l'amour.

« *Quand bien même, les cybercafés en Côte d'Ivoire louent des plages d'adresse IP… Remonter jusqu'aux escrocs demande énormément de temps et de volonté, surtout si l'on veut connaître exactement la personne qui aura mené l'arnaque* », déplore Christine. Certaines escroqueries dépassent même les frontières. « *Ils ont créé des*

1 *Cf.* chapitre 5.
2 *Cf.* chapitre 5.

réseaux et agissent comme de véritables bandes organisées avec des ramifications en Europe. Quand les escroqueries sont poussées jusqu'à un haut niveau, on voit parfois des complices basés en Europe se déplacer jusqu'à la victime. On arrive comme ça à des escroqueries très particulières, avec des mallettes pleines de billets ». Même si elles figurent parmi les plus lucratives, ce genre d'arnaque est moins utilisé aujourd'hui. Mais l'Internet reste un formidable vivier à victimes pour les escrocs ambitieux. « *Comme rien n'est entrepris légalement en Europe contre les arnaqueurs, en raison de la territorialité de chaque pays, ils ont la voie libre. C'est un gros point négatif pour nous* », conclut la présidente de l'AVEN.

Parmi les pays concernés, seule la Côte d'Ivoire a su mettre en place une brigade spécialisée, la Plateforme de Lutte Contre la Cybercriminalité (PLCC), à Abidjan, mais ses moyens et ses ressources sont limitées face à l'ampleur du phénomène. Le Nigeria, quant à lui, possède depuis plusieurs années sa propre agence chargée des investigations sur les délits financiers, la Economic and Financial Crime Commission (EFCC). Malgré l'existence de ces établissements, la présidente de l'AVEN semble mettre en doute leur véritable efficacité concernant les victimes françaises : « *Il semble qu'il n'y ait aucune collaboration ou une collaboration très peu efficace entre la police française et ces services étrangers. Quoi qu'il en soit, les plaintes sont toujours systématiquement classées sans suite, sans enquête sur le terrain. À croire que les procureurs n'ont aucun pouvoir pour appliquer les réquisitions ou des commissions rogatoires dans les pays concernés* ». Le manque ou l'inefficacité des actions constitue le problème majeur de ces associations. La difficile communication entre les pays concernés et les instances françaises, cristallise la complexité de ces affaires.

Déceler les fraudes à l'étranger

Parfois, des incohérences dans les annonces permettent de repérer très vite ces arnaques. L'adjudant-chef Garnier, fait le test : « Sur cette annonce, on me propose à la vente deux motos Ténéré 600. Le vendeur dit être au Burkina Faso. Mais sur les photos, on voit clairement les plaques d'immatriculation. Et elles sont françaises. En l'occurrence, cette photo est d'assez bonne qualité pour que l'on puisse lire la plaque. Mais rien qu'en regardant les couleurs, on peut reconnaître une plaque française d'une plaque étrangère. Ces images ont été clairement trouvées sur Internet et n'appartiennent pas à l'auteur de l'annonce. Si en plus de cela, on la recoupe avec son prix, particulièrement bas, 2 000 euros, il devient évident que c'est une offre frauduleuse ».

Autre alerte, qui doit immédiatement vous rendre soupçonneux, une recrudescence des fautes d'orthographe ou des formules ampoulées. Chez les escrocs étrangers, la connaissance du français semble être particulièrement approximative. Par exemple, cette phrase, postée sur le forum du site lesarnaques.com, est particulièrement représentative : « *Cependant permettais moi de chercher votre aide honorable sur le projet d'investissement dans votre pays. Quoique nous ne nous soyons pas réunis face à face avant, je crois que vous pouvez m'aider dans ce projet honorable pour notre avantage mutuel* ». Tous les messages ne sont pour autant pas aussi facilement identifiables. Mais lorsqu'ils regorgent de fautes d'orthographe ou utilisent des mots rarement employés dans la vie de tous les jours : méfiance.

Souvent, des arnaqueurs ivoiriens disent à leur victime résider en France. Un mensonge qui peut être facilement éventé, il suffit pour ce faire de tracer l'adresse IP des e-mails que vous aurez échangés. Cette pratique, très simple à réaliser, est surtout tout à fait légale.

En pratique

Tracer une adresse IP

« Il suffit d'ouvrir l'en-tête du mail pour trouver l'adresse IP de l'expéditeur », explique Christine. Une manipulation simple quand on sait où chercher.

- Dans Gmail, par exemple, il vous faut cliquer sur la petite flèche à droite du bouton « répondre ». Parmi les propositions qui vous sont faites, sélectionnez « afficher l'original ». Vous arrivez sur une page au contenu somme toute assez effrayant, fait d'anglais, de chiffres et de formules incompréhensibles. Pas de panique. En l'observant calmement, vous trouverez une ligne similaire à celle-ci : « received : from [69.138.30.1] by web31804.mail.mud.yahoo.com ». [69.138.30.1] sera donc l'adresse IP de votre contact.
- La procédure est exactement la même si vous utilisez Hotmail : cliquez sur la flèche à côté de « répondre » et « affichez l'original ». Si toutefois cette manipulation s'avère impossible ou inefficace, vous pouvez en utiliser une autre : ouvrez votre message et enregistrez-le grâce à l'outil « enregistrer sous ». Puis, ouvrez le fichier XXXX.eml, avec le bloc-notes. Vous obtiendrez alors le code source et l'adresse IP.
- Sur Outlook, la procédure est un peu différente. Ouvrez votre e-mail et cherchez dans votre barre des tâches l'onglet « indicateurs » (marquer comme non lu, assurer un suivi...). Cliquez ensuite sur la petite flèche en bas à droite de cet onglet pour ouvrir une nouvelle fenêtre. Tout en bas de celle-ci sera affiché le code source contenant l'adresse IP.

- Si vous utilisez le service de Yahoo pour recevoir vos mails, cliquez sur le mail dont vous voulez trouver l'adresse IP. Il n'est pas nécessaire de l'ouvrir, juste de le contraster en cliquant une fois dessus afin de le sélectionner. Rendez-vous ensuite dans la barre d'outils et cliquez sur l'icône représentant un engrenage, dans la partie droite. Dans le menu qui apparaît, sélectionnez « afficher l'en-tête complet ». Cet en-tête s'ouvrira dans une nouvelle fenêtre et vous aurez accès à l'IP de votre correspondant. Il suffit ensuite d'en rechercher la localisation *via* un site spécialisé, ip-adress.com, utrace.de... afin de savoir si votre interlocuteur vous contacte bien de France comme il le prétend ou d'un autre pays.

Ces services ne vous renseignent que sur le pays d'où vient l'e-mail. Ne vous fiez pas, par exemple, à l'adresse qui sera indiquée sur la carte. En effet, une adresse IP est dite « dynamique », c'est-à-dire qu'elle peut changer à chaque connexion et une adresse IP libérée est presque aussitôt attribuée à quelqu'un d'autre. Trouver cette adresse IP ne vous permettra en aucun cas de trouver l'identité de celui ou celle qui vous a arnaqué. Ces données sont gardées par les fournisseurs d'accès et ils ne les dévoileront qu'à la police en cas de plainte.

Si cette méthode est indéniablement efficace, elle reste inutile si votre escroc utilise un proxy. Par essence, cet outil va lui permettre de se faire passer pour un internaute français en s'attribuant une adresse IP française (*cf.* chapitre 1, page 17 et 24).

En résumé, si l'IP indique un pays étranger, méfiez-vous ; si cela indique la France, rien ne vous garantit que la personne soit en France. Dans l'hypothèse où vous avez déjà été victime d'une escroquerie, surtout, ne jetez pas les e-mails que vous aurez échangés avec votre arnaqueur. Si vous ne disposez que

du fournisseur d'accès qui aura émis l'adresse IP, la police peut, elle, demander l'identité de son utilisateur. L'adresse IP étant dynamique, l'heure d'envoi du mail à la seconde est capitale pour retrouver l'expéditeur. Les forces de l'ordre, en fournissant l'heure et l'adresse IP de l'envoi, permettront au fournisseur d'accès de retrouver l'adresse et l'identité de l'internaute connecté à cet instant précis.

Transferts d'argent

Beaucoup d'escrocs étrangers utilisent Western Union ou les services Mandat Cash pour récupérer l'argent extorqué. Ces deux organismes n'ont bien sûr qu'un rôle passif, indirect et surtout involontaire dans ces arnaques. Mais leur fonctionnement a été exploité et détourné par les arnaqueurs. Utiliser ces agences de transfert de fonds donne une caution légale et sécurisée à leurs annonces, faisant ainsi passer leurs offres pour des annonces dignes de confiance.

CONSEIL

Afin de limiter les risques, et ce quelle que soit l'histoire que votre interlocuteur voudra bien vous raconter, dès qu'il est question de payer par Western Union ou Mandat Cash, cessez tout contact.

Les services de ces compagnies sont parfaits lorsque vous souhaitez transférer de l'argent à un proche, un bon ami ou de la famille. Si vous connaissez bien la personne en face et que vous placez depuis longtemps votre confiance en lui, ces services n'ont rien de dangereux. Mais lors d'une transaction avec un inconnu que vous n'avez jamais rencontré, même si vous avez l'impression qu'il est honnête, privilégiez des paiements de type Paypal ou mieux un échange en main propre.

Pourtant, dans le domaine des petites annonces, les escrocs décident parfois de se passer d'organismes de transferts de fonds. Aussi, n'envoyez jamais d'argent liquide par La Poste. Tout d'abord parce que ce n'est pas autorisé. Le service public l'explique clairement : « Sont interdits, quelle que soit la destination choisie, [...] les bijoux, métaux précieux, billets de banque, valeurs au porteur, or ou argent, et autre objet de valeur ». Toutefois, vers certaines destinations et sous des conditions particulières « un envoi recommandé » pour ces transactions est toléré.

Dans le cas d'un Mandat Cash, ou de l'envoi d'un recommandé, vous gardez une trace de l'envoi. Ce n'est pas le cas avec une enveloppe classique. Si vous réalisez avoir été victime d'une arnaque, vous n'aurez alors aucun moyen de prouver votre envoi d'argent. De la même façon, si vous recevez un bien et décidez d'envoyer du liquide en paiement, un vendeur peu honnête pourra affirmer ne jamais avoir reçu l'argent : là aussi, l'absence de preuve attestant de l'envoi peut vous desservir, voire vous obliger à payer une nouvelle fois.

À SAVOIR

Si vous décidez de passer outre l'interdiction et d'envoyer, sous pli habituel, des billets à votre interlocuteur, il vous faut être conscient du fait que vous n'aurez aucune trace.

Enfin, il arrive parfois que, sur une petite annonce, le vendeur demande à être contacté par téléphone. C'est une pratique tout à fait légale, mais restez attentif. Si le numéro que l'on vous demande de composer commence par 08, fuyez tout de suite cette annonce : le numéro est surtaxé. Vous passerez plusieurs minutes en attente sans ne jamais parler à personne et serez finalement débité de plusieurs dizaines d'euros, sans vous en rendre compte.

EN RÉSUMÉ

- Les annonces avec de grosses fautes d'orthographe et des formules ampoulées sont souvent écrites par des arnaqueurs étrangers. N'y répondez pas.
- Avant de démarrer une transaction, analysez les photos attachées à l'annonce. Si vous remarquez des incohérences, cessez toute discussion.
- Gardez tous les e-mails. Dans le cas d'une escroquerie, ils vous seront utiles.
- Les transactions *via* Western Union sont à réserver uniquement pour les personnes que vous connaissez personnellement. Ils ne doivent pas être un moyen de paiement lors d'un achat par l'intermédiaire d'une petite annonce.
- N'envoyez pas d'argent par la poste !
- Si on vous demande de téléphoner et que le numéro commence par 08, fuyez ! C'est un numéro surtaxé.

CHAPITRE 5
ARNACŒURS PROFESSIONNELS

DÉFINITIONS

- **Brouteurs** : nouveaux escrocs qui poussent leurs proies à des jeux érotiques devant la Webcam dans le but de les faire chanter.
- **Skype** : logiciel de voix sur IP permettant de téléphoner, après inscription, avec d'autres utilisateurs de Skype gratuitement, ou d'appeler un numéro fixe avec un abonnement.

Marianne R.

Le courrier du cœur... Un bon créneau pour les arnaqueurs professionnels qui maîtrisent l'art de la manipulation. Si une femme de 35-40 ans, avec une bonne situation professionnelle, seule, est une proie idéale pour ces escrocs aux histoires abracadabrantesques, un homme sera plus facilement touché par une arnaque à la Webcam... Bref, personne n'est à l'abri. Ici encore, découvrez toutes les ficelles pour ne pas tomber dans leurs pièges !

Témoignage

À 53 ans, Marianne R. n'espérait plus faire tourner les têtes du sexe opposé. Divorcée depuis quelques années, ses deux enfants faisant leur vie dans des villes différentes, elle se sentait seule et avait envie de retrouver les joies d'une relation de couple. Sans trop y croire, elle se rend donc sur un site de rencontres et se crée un profil. Âge ? Elle décide de se donner trois ans de moins. Elle met en avant ses traits de caractère les plus avantageux et choisit de publier une photo qui a déjà quelques années. Elle se trouve belle et espère que l'avis sera partagé par les hommes inscrits sur le site. Au fur et à mesure des jours, elle reçoit quelques réponses, consulte les profils, essaie de raviver les instincts charmeurs dont elle jouait dans sa jeunesse. Draguer sur Internet présente pour elle tous les avantages. Aucune crainte de se faire méchamment refouler, la barrière de l'écran la protège des malotrus. Elle peut avoir accès à ses mots doux au bureau, dans les transports ou dans n'importe quel autre endroit. Un jeu qu'elle n'assume qu'à moitié. Elle en parle peu à ses amies, et surtout le tait à sa famille. Un jour, elle reçoit un joli message d'un beau cinquantenaire. Selon son profil, assez peu fourni, « Patrick » a 56 ans, un beau bagage d'architecte derrière lui et une photo de profil particulièrement avantageuse. Cheveux poivre et sel voletant au vent avec quelques rochers et la mer en toile de fond... Marianne se surprend à sourire. Le message qu'elle a reçu est charmeur et elle a bien envie de tenter sa chance. Contact pris avec le bel inconnu, il l'invite à échanger leurs adresses mail pour

communiquer plus aisément, via *une messagerie instantanée. Elle accepte. Tous les jours, Patrick lui parle. De lui, de sa petite fille de 9 ans née tardivement d'un mariage, qui a tragiquement pris fin avec l'accident de voiture de sa femme. Maintenant veuf et esseulé, il cherche la douceur d'une femme pour réchauffer son foyer et combler la présence qui manque à sa fille depuis déjà trop longtemps. Il possède une belle maison près de Marseille et un cabinet privé florissant. Quand il parle à Marianne, il est doux, dragueur et romantique. C'est ce qui la charme. Il la traite comme une femme unique et désirable. En quelques semaines, c'est le grand amour et Patrick évoque déjà une vie à deux, pourquoi pas un mariage... C'est décidé, il viendra passer quelques jours à Paris pour qu'ils se rencontrent et pour qu'il puisse lui présenter sa fille qui n'attend que ça, connaître la fiancée de papa. Pourtant, une semaine avant la date de la rencontre, Patrick la contacte, peiné. Il s'était engagé dans un projet humanitaire visant à la construction d'une école en Côte d'Ivoire, mais l'association rencontre quelques difficultés et il est forcé de se rendre sur place pour superviser les travaux de construction. Une mission qui ne durera que quelques jours, quelques semaines au plus. Il propose donc de remettre la rencontre à plus tard. Marianne s'inquiète alors du sort de la petite fille, accompagnant son père dans un pays somme toute en grande instabilité politique en ce moment. Il la rassure immédiatement : ses grands-parents maternels habitent tout près, elle ira vivre chez eux le temps que durera la mission.*

Les deux amoureux se promettent de rester en contact tout le temps que durera le voyage et s'accordent sur une nouvelle date de rencontre. Dès son arrivée à Abidjan, il la contacte. Le voyage s'est bien passé, il quitte la capitale le lendemain pour partir sur son lieu de mission, elle lui manque beaucoup et il a déjà hâte de rentrer pour la voir. Mais dès le lendemain, plus rien. Il ne se connecte plus, n'envoie plus de mails... Pendant deux jours, Marianne n'a aucune nouvelle. Quand enfin elle reçoit un e-mail de Patrick, c'est une très mauvaise nouvelle qui l'attend. Agressé dans la rue, il est à l'hôpital. Rien de bien grave mais on lui a volé ses papiers d'identité, son passeport, et surtout, tout son argent. Or, selon ses dires, pour bénéficier de soins de qualité, il faut pouvoir avancer de l'argent. Entre deux supplications, il demande à sa bien-aimée de lui faire parvenir 1 700 euros afin de régler les frais d'hôpitaux. Argent qu'il lui rendra dès son retour, bien entendu. Marianne n'hésite pas un instant. Elle se rend dans la poste la plus proche et fait parvenir comme convenu 1 700 euros à Patrick via *Western Union. Quelques jours plus tard, nouveau contre-temps : il est dans l'incapacité de prendre l'avion pour rentrer. On lui a volé ses billets dans l'agression et il est impossible de se débrouiller seul pour obtenir des papiers d'identité dans un court délai sans graisser la patte de quelques fonctionnaires. Il demande donc successivement à Marianne entre 200 et 500 euros pour couvrir ses frais, pour payer une chambre d'hôtel, trouver un avion et se faire faire des papiers. La Française émet de plus en plus de réserves quant à verser*

l'argent. Le ton de son Don Juan se fait alors plus pressant, plus insistant. Il l'aime tant, ne l'aime-t-elle pas assez pour lui faire confiance ? Ne voudrait-elle pas l'aider à rentrer au plus vite ? Sa fille s'inquiète en France sans son père et Marianne refuse de l'aider à rentrer ? Malgré toutes les déclarations d'amour qu'il lui a faites ? Elle finit par céder mais ses ressources financières sont limitées, elle envoie l'argent par à-coups, autant qu'elle peut. À court de liquidités, elle finit par avouer à son amoureux qu'elle ne pourra plus l'aider financièrement. Aussitôt, il disparaît. Plus de mail, son numéro de portable reste sans réponse et il ne se connecte plus sur la plateforme de messagerie instantanée. Marianne s'inquiète et s'apprête à demander des conseils sur un forum pour reconquérir cet homme qu'elle croit vexé pour rester ainsi sourd à ses appels. C'est alors qu'elle découvre nombre de témoignages semblables au sien dénonçant des arnaqueurs. De « posts » en demande de conseils, on la dirige vers une association qui lui confirme qu'elle a bien été victime d'une arnaque. Malgré ses réticences, elle finit par se laisser convaincre et fait le deuil de cet amour imaginaire et sans aucun doute à sens unique. Patrick n'a jamais été qu'un arnaqueur et toute son identité, une vaste mise en scène, de sa qualité d'architecte à sa petite fille en passant par les plus obscurs méandres de ses déboires amoureux passés. Marianne R. a perdu près de 7 000 euros.

Les arnaques à l'amour font certainement partie des escroqueries les plus dangereuses. Leur coût financier et émotionnel est des plus élevés car elles font partie des histoires les plus poussées,

faisant appel à des mécanismes particulièrement complexes. Ce type d'escroquerie se fonde essentiellement sur les sentiments et les liens qui se seront créés entre l'escroc et sa cible. C'est cette relation de confiance, d'amitié, puis d'amour, qui va pousser la victime à envoyer de l'argent à son arnaqueur sans jamais se méfier. Tous les mécanismes psychologiques pour conditionner sa cible sont réunis dans ces arnaques : la valorisation de sa proie, son sentiment de sécurité ou encore l'impression d'avoir trouvé la perle rare.

L'arnaque parfaite pour un fin psychologue

Financièrement, ce sont les arnaques les plus lucratives. Elles ont tendance à se dérouler sur le long terme et nécessitent le versement de fortes sommes d'argent. Et malgré l'exubérance des sommes demandées, voire parfois l'illogisme du scénario, les victimes plongent tête baissée dans le piège. Le psychologue Cyrille Le Jamtel a une explication simple à cette mécanique : « *Le sentiment ne raisonne pas. Dans le cas des arnaques à l'amour, on n'a pas envie d'être raisonnable* ». Ce sont des histoires où vous avez été en relation avec quelqu'un qui vous a promis le grand amour, qui a su s'adapter à toutes vos demandes affectives pour devenir, en seulement quelques semaines, indispensable. « *Même si l'arnaque est évidente, on refuse de le croire parce qu'on refuse d'avoir tort. On a tous besoin de rêver* ». C'est ce qui fait des arnaques à l'amour des pièges parfaits pour qui sait s'adapter à son interlocuteur. Chaque proie aura des attentes différentes et si le scénario initial reste le même, il faut pouvoir y apporter quelques modifications afin de toujours répondre aux attentes de sa victime. Plus elle se sentira écoutée et aimée, plus elle aura l'impression de compter pour son interlocuteur et plus elle sera amenée à éprouver des sentiments pour lui.

On retrouve ici encore, le mécanisme des sectes. L'escroc va devenir une référence positive pour sa victime. Il va la valoriser et la rendre unique. « *On est ébloui. La valorisation endort la méfiance* » rappelle le psychologue. À côté de ce beau parleur qui nous dit tout ce que l'on a toujours eu envie d'entendre, la famille prend des airs paternalistes difficilement supportables. Elle est raisonnable, sensible au danger. La relation qui s'est établie entre l'escroc et sa proie n'existe pas avec les proches de la victime. Ils sont donc plus enclins à la méfiance et se laissent moins facilement aveugler par les flatteries de l'arnaqueur. Pour cette raison, l'escroc va pousser sa victime à taire sa relation, à se couper de ses proches. En l'accaparant sur Internet tout d'abord.

À SAVOIR

Chacun a besoin, et envie, de se croire désirable. Si l'arnaqueur arrive à flatter cette part de narcissisme qui sommeille en chacun de nous, il obtient une place privilégiée.

Marie, spécialiste des arnaques à l'amour au sein de l'AVEN France connaît bien la manœuvre : « *La rencontre s'effectue* via *un site sur lequel les deux internautes peuvent parfaitement discuter. Mais l'arnaqueur va préférer la messagerie instantanée. Il y a un an, ils opéraient* via *MSN. Désormais, MSN a fermé et a fusionné avec Skype. Aujourd'hui, c'est* via *Skype que les victimes sont contactées. C'est un terrain qui est familier à l'escroc et sur lequel il va pouvoir monopoliser sa victime sans crainte que la modération du site ne le signale comme potentiellement dangereux. Sur Skype, il va pouvoir discuter plusieurs heures par jour avec sa proie. Il aura le champ libre pour se renseigner sur la vie privée et professionnelle de sa cible. Tout le temps que l'escroc passera à discuter avec sa victime sera du temps qu'elle ne passera pas avec sa famille* ».

Les victimes auront de prime abord tendance à cacher leur inscription sur un site de rencontres : « *C'est encore un sujet*

tabou. On assume rarement cette démarche de rechercher l'âme sœur sur Internet », explique Cyrille Le Jamtel. Dès que les échanges se font plus intimes, l'arnaqueur va demander à son interlocuteur de ne pas en parler. Pour Marie, c'est très simple : « *ils vont dire "N'en parle pas à ta famille, on leur fera la surprise", ou bien "Ils risquent de désapprouver, laisse-nous un peu de temps et tu me présenteras quand je viendrai te voir"...* ». Des idées souvent approuvées par la victime. Ces secrets lui donnent l'impression de revivre des amourettes d'adolescence où les cachotteries aux proches faisaient forcément partie de l'équation.

Pourtant, il arrive que la victime en parle à son entourage. Mais les doutes émis sur la relation peuvent alors avoir l'effet totalement inverse à celui escompté. Là où l'arnaqueur va passer pour une personne douce et gentille par ses flatteries, la méfiance et le recul des proches passeront pour une infantilisation rarement acceptée par la victime. « *L'être humain accepte difficilement la critique. Encore moins quand elle provient d'un membre de la famille. C'est humiliant de se faire rappeler à l'ordre par ses enfants* », analyse Cyrille. Malgré les avertissements et les alertes, la victime préférera s'illusionner et s'enfermer dans cette belle histoire, même si elle s'avère fausse. Elle va donc s'isoler d'elle-même et être encore plus vulnérable aux boniments de son interlocuteur.

Des méthodes d'approche bien rodées

S'il n'existe pas de profil type de l'arnaqué, les victimes de ces escrocs ont tout de même quelques points communs. La raison est simple, l'escroc va cibler ses proies et choisir celles qu'il manipulera le plus facilement. Et surtout, il va sélectionner celles qui ont le plus gros potentiel financier. « *Les escrocs savent bien que plus la victime est jeune, moins elle a de chances de disposer de grandes ressources financières. Généralement, les victimes*

sont des femmes qui ont entre 35 et 40 ans. Après, il n'y a aucune limite. Qu'importe leur âge, tant qu'elles ont de quoi lui envoyer de l'argent... », analyse Marie.

Toutefois, à moins que la victime ne le renseigne sur son profil, l'escroc n'a aucun moyen de connaître exactement l'étendue des moyens financiers de sa proie tant qu'elle n'a pas donné son nom. Avec cette nouvelle information, il pourra effectuer des recherches plus approfondies, par exemple, à partir des réseaux professionnels comme Viadeo ou LinkedIn. Et peu importent les ressources de la proie. « *Ce qui compte pour les arnaqueurs, c'est que leurs cibles soient seules ou en demande affective pour pouvoir les manipuler. Il faut savoir qu'ils ne reculent devant rien. Si leurs interlocuteurs objectent ne plus avoir les moyens de l'aider, ils vont leur suggérer de vendre leur voiture, d'emprunter à la banque ou à leur propre famille. Au sortir de l'arnaque, quand nous sommes en contact avec ces victimes, nous sommes face à des gens complètement asphyxiés, qui n'ont plus la possibilité de se retourner* ».

Il est au départ difficile de comprendre comment un internaute peut transférer plus d'un millier d'euros à un individu qu'il n'a jamais vu. Pourtant, l'explication est simple : dans la mesure où les sentiments entrent en jeu, la victime est littéralement aveuglée et n'a plus les mêmes réflexes de méfiance. « *On pense que l'échange que l'on entretient est une relation à deux. On n'imagine jamais que la personne en face ne puisse pas penser ce qu'elle dit. Quand on regarde le profil de quelqu'un, il y a une photo, sur Skype aussi. Quand on commence une relation avec quelqu'un de charmeur et en tout point agréable, il n'y a aucune raison de penser que la personne ment sur son identité* ». Des escrocs qui n'hésitent pas à donner leur numéro de portable ou à appeler régulièrement leur victime, quitte à mettre à jour un accent parfois très prononcé. « *Il ne faut pas oublier qu'ils ont réponse à tout. Quand on leur fait remarquer leur accent ou leurs fautes d'orthographe, ils disent qu'ils ont grandi à l'étranger, que leur mère était étrangère...*

C'est leur métier, ils ont toujours la parade parfaite pour endormir la méfiance ».

Depuis peu, les membres actifs de l'AVEN ont remarqué que les escrocs avaient ajouté une variante importante à leur schéma habituel. Désormais, lorsqu'ils opèrent une arnaque aux sentiments, ils ne demandent plus systématiquement d'argent mais proposent plutôt d'envoyer un chèque à la victime afin qu'elle utilise les fonds correspondants. Comme il ne s'agit pas de ses propres fonds, la victime sera donc moins vigilante. Cependant, le chèque a en fait été volé. Certes, il est réel, généralement français et provient d'une société, mais il a été dérobé dans les centres de tri. Ainsi la victime l'encaisse, la banque le porte immédiatement au crédit du compte et informe la victime que les fonds sont à sa disposition. La victime suit ensuite les directives de l'escroc et utilise les fonds pour les envoyer à son interlocuteur. Quelques jours ou quelques semaines plus tard, la banque comprend qu'il s'agissait d'un chèque volé et réédite le montant du chèque sur le compte de la victime majoré de frais et d'agios en tout genre. La victime se retrouve alors à découvert, la banque la poursuit et porte plainte pour récupérer le découvert.

À SAVOIR

L'arnaque aux sentiments reste selon les associations l'arnaque la plus virulente, suivie de près par celle à la Webcam.

La présidente de l'AVEN déplore cette situation : « *Malgré les enquêtes approfondies par certaines brigades financières où les complices en France sont localisés et repérés par ces services, les procureurs ne prêtent aucune attention particulière, ni action rapide pour que les enquêteurs puissent agir, ce qui permettrait aux victimes d'être reconnues.* » Christine Goubert pointe également du doigt le manque d'action de la part des établissements bancaires. « *Cela revient aussi à dire que le système bancaire serait remis en*

cause dans leurs manquements aux obligations de rigueur envers les usagers des banques, mais aussi aux contournements des lois du Code monétaire et financier. Les tribunaux donnent souvent raison à la banque qui n'a pourtant fait aucune vérification. Les juges font une totale abstraction de la manipulation qui est opérée pour que la victime envoie de l'argent, toujours par Western Union. Ils considèrent que la victime était consentante. L'article 313.1 du Code pénal prévoit pourtant les manœuvres frauduleuses ». Christine Goubert nous livre même avec une pointe de désolation qu'ils ont également été témoins de cas où les chèques été directement arrivés à l'agence bancaire qui les a encaissés, sans que la victime ne soit actrice de la remise de chèques.

Des arnaques repérables

Les escrocs étendent au maximum leur terrain de chasse, mais les profils qu'ils diffusent sont, eux, toujours semblables. C'est d'ailleurs un moyen simple pour les reconnaître. Marie est habituée à les repérer dès le premier coup d'œil : « *Les profils sont en général attrayants avec des photos très attirantes. Souvent, elles sont usurpées à d'anciennes victimes ou ce sont des photos de mannequins, de people… Ce sont généralement des gens qui voyagent beaucoup, comme des hommes d'affaires, pour faire en sorte qu'après une première phase de séduction l'individu parte en voyage. Si ce n'est pas le cas, ils ont un métier qui peut les amener à partir à l'étranger dans le cadre d'organismes humanitaires : médecins, architectes… Quoi qu'il en soit, ils ont toujours une bonne situation professionnelle et une certaine aisance financière* ».

Il y a quelques règles simples à suivre pour se prémunir contre d'éventuelles arnaques et reconnaître les escrocs.

En pratique

Reconnaitre et déjouer les arnaques à l'amour

Une fois le contact pris avec votre interlocuteur, s'il insiste pour vous entraîner très vite sur une plateforme de messagerie instantanée, méfiance, c'est une des caractéristiques des escrocs. Mais ce qui, plus que tout, doit vous alerter, c'est la rapidité avec laquelle il va vous parler de grand amour. Les sentiments mettent, par essence, du temps à naître et à s'ancrer. En quelques semaines seulement, les escrocs vont passer de l'amitié virtuelle à des projets de vie à deux, voire de mariage. S'il part à l'étranger, notamment en Afrique, avant que vous l'ayez rencontré, alors vous pouvez être sûr, à 99 %, que c'est une escroquerie. Cerise sur le gâteau : s'il vous demande de lui envoyer de l'argent, ne vous perdez plus en suppositions ; c'est une arnaque, à coup sûr. « *Ils ont des dizaines d'idées pour demander de l'argent : "je me suis fait attaquer et on m'a volé tous mes papiers", "j'ai des problèmes avec mon business", "j'ai des problèmes avec la douane", "mes ouvriers sont en grève", "je me suis fait prendre avec des objets d'art à la douane", "je suis malade", "je suis à l'hôpital"... Et dans tous les cas, il lui faudra de l'argent liquide* ».

Il ne faut bien sûr pas rejeter en bloc tous les profils qui ressemblent à cette description, mais l'accumulation de tous ces points doit éveiller la méfiance. Dans le doute, demandez-lui de vous envoyer une photo particulière : lui avec une pancarte « je t'aime » et votre prénom, par exemple.

Toutefois, si vous décidez de mettre fin à un échange à l'issue de cette situation, n'ayez aucun regret : il n'y a jamais eu en face de vous qu'un arnaqueur sans scrupule.

Il ne faut pas non plus croire que les femmes sont les seules à être les victimes des arnaques à l'amour. Les hommes, parfois, se laissent aussi prendre au piège. En moins grande proportion toutefois. Et si le profil recherché par l'escroc reste similaire – à partir de 40 ans, bonne situation professionnelle, esseulé... –, le personnage créé pour attirer sa proie sera radicalement différent. « *Généralement, ce sont des femmes ou des hommes se faisant passer pour des femmes, de 20 à 35 ans et toujours très jolies. Contrairement aux hommes, elles ne cachent pas leur nationalité si elles sont ivoiriennes. Elles disent parfois vivre en Afrique et vont soutirer de l'argent en demandant de l'aide pour leurs familles, obtenir un visa et rejoindre leurs interlocuteurs en France, pour acheter leurs connexions Internet... Mais il peut aussi y avoir des soi-disant Françaises en déplacement pour des raisons humanitaires* ».

Cette différence de scénario s'explique assez simplement. Les femmes ont toujours tendance à rêver d'un compagnon jouissant d'une bonne situation professionnelle et financière. Sur un plan sentimental, ces escrocs se diront veufs ou célibataires, jamais divorcés, « *ça fait mauvais genre* », sourit Marie. Et lorsque c'est un homme qui se fait piéger il est plus enclin à assumer financièrement, pour un temps du moins, le voyage et l'installation de la jeune femme avec qui il aurait correspondu.

Escroqueries à la Webcam

Avec les sites de rencontres est apparu un nouveau type d'arnaque : les escroqueries à la Webcam. Elles font certainement partie des escroqueries les plus rapides à mener, mais pas des moins lucratives. « *En ce moment, il y a beaucoup d'arnaques de ce type. Moi qui suis habituée, je les cherche sur Internet, pour prévenir les gens, et j'en trouve entre cinquante à quatre-vingt par jour. En plus de cela, il y a quotidiennement une dizaine de personnes qui me contactent, paniquées, après s'être fait piéger* ».

Le principe de cette arnaque simple est essentiellement tourné vers les hommes : « *Ils font la connaissance de femmes sur des sites de rencontres ou des chats "hot". Ce sont des relations "éclair" : entre quinze minutes et une heure, au plus. L'escroc va discuter un peu avec sa victime pour en apprendre le maximum sur elle avant de passer une vidéo, souvent d'une professionnelle, pour "chauffer" son interlocuteur. Finalement, la personne va se masturber devant la Webcam et l'escroc va l'enregistrer. Ensuite, il va se contenter de lui faire du chantage : "Si tu ne me donnes pas de l'argent, je diffuse cette vidéo à tous tes contacts"* ». Car pendant que vous discutez avec votre interlocuteur, il va entrer en possession de certaines de vos informations personnelles : nom, ville de résidence, parfois lieu de travail... Avec ces informations, il peut vous trouver facilement sur Facebook.

Mais il existe aussi des variantes. Par exemple, des femmes qui ont été victimes d'une arnaque aux sentiments peuvent se retrouver victimes d'une arnaque à la Webcam si l'escroc réussit à persuader leurs interlocutrices de se montrer à la Webcam. Une fois de plus « les gens ne sécurisent pas leur compte. Il est facile de récupérer les contacts de quelqu'un et, au moment du chantage, d'en montrer un échantillon à sa victime pour lui faire peur. C'est d'une facilité déconcertante ! ».

Une fois l'arnaque menée, il va y avoir deux scénarios principaux pour extorquer de l'argent, le plus répandu étant la menace de diffusion aux contacts. Mais certains vont aller plus loin et raconter une histoire rocambolesque à leur victime : elle n'a en réalité pas correspondu avec une personne majeure et consentante, mais avec une adolescente. Découvrant l'affaire, sa mère ou un proche vous menace de porter plainte si vous ne lui envoyez pas d'argent.

Dans ce cas de figure, l'arnaque peut malheureusement aller encore plus loin : quelques jours après votre envoi d'argent, vous recevrez un e-mail d'un prétendu policier, d'un juge ou d'un

procureur qui vous informera d'une plainte déposée à votre encontre et d'une amende faramineuse qu'il vous faut payer pour mettre un terme aux poursuites. Une amende qui peut se chiffrer jusqu'à 5 000 euros et à envoyer par Western Union, évidemment… « Les gens ne sont pas au courant, déplore Marie. Quelqu'un représentant une institution d'État n'aura jamais d'adresse gratuite type Gmail, Yahoo ou encore Hotmail ! ».

Mais face à ce genre de menaces, la panique l'emporte généralement sur la raison et les victimes sont prêtes à tout pour que la vidéo disparaisse.

Or, payer est la pire des solutions. Car pour prouver leur détermination, les escrocs publieront la vidéo enregistrée sur YouTube avant même tout envoi d'argent. On retrouve dans ces cas-là deux types de victimes. Celles qui, paniquées, sont prêtes à payer au plus vite pour faire disparaître les preuves et celles qui tentent de négocier avec leur escroc. Ce sont, dans les deux cas, de mauvaises solutions. La vidéo existe, donc le mal est déjà fait. Tant qu'elle reste en possession de l'escroc, vous serez vulnérable et soumis à son chantage. La seule solution pour vous en sortir, c'est de supprimer vos comptes Facebook et Skype, ignorer ses messages et contacter une association afin qu'elle vous épaule dans vos démarches. Un escroc n'aura pas d'intérêt à vous harceler si, de votre côté, vous vous montrez indifférent à ses menaces. Encore une fois, une vidéo aura déjà été postée sur YouTube et si vous ne répondez pas à ses menaces, votre interlocuteur n'aura aucun intérêt à la diffuser à vos proches : il

PAROLE D'EXPERT

Ce qui importe dans une adresse e-mail, ce n'est pas le prénom ou le titre qui y est inscrit, c'est ce qu'il y a après l'arobase (@). Si l'adresse est « procureur@hotmail.com », c'est une arnaque. En France par exemple, les adresses officielles sont du type « xxxxxx@justice.gouv.fr

perdrait son moyen de pression. Un moindre mal, certes, mais qui n'est pas négligeable.

Reste la vidéo déjà en ligne sur un site de partage. Marie a l'habitude de s'en occuper : « *Quand une victime nous contacte, on demande à YouTube de retirer la vidéo et ils le font assez rapidement. Mais il ne faut pas oublier que, même si les images disparaissent, les textes qui y sont associés, les commentaires... restent visibles et peuvent toujours nuire. Quand je remarque des vidéos avant que l'on me contacte, je poste un commentaire pour prévenir la victime de l'arnaque et lui conseille de contacter l'association pour que nous l'aidions* ».

Youtube est pour le moment la plateforme de prédilection des arnaqueurs qui y déposent leurs trophées en masse. La raison : « *YouTube ne supprime ces vidéos que si la victime ou une association le demande. Si personne n'est au courant, ou ne sait pas comment faire, la vidéo va rester visible jusqu'à ce que quelqu'un la signale. Sur Dailymotion, par exemple, c'est différent, il y a une réelle modération effectuée sur les vidéos et les personnels du service les suppriment d'eux-mêmes* ».

Mais la méfiance, nécessaire pour surfer en toute quiétude, ne doit pas se transformer en paranoïa. Il existe de vraies professionnelles du sexe qui exercent par l'intermédiaire d'une Webcam. Pour éviter l'arnaque, demandez à votre interlocutrice, avant tout autre échange, de faire un geste qui distinguera sa prestation d'une vidéo préenregistrée : se toucher l'oreille droite avec la main gauche, par exemple, ou tout autre signe que vous choisirez. Quoi qu'il en soit, lors de ce type de relation par l'intermédiaire d'une Webcam, et par mesure de sécurité, ne donnez ni votre nom ni votre adresse, ne révélez même aucune autre donnée personnelle qui pourrait vous faire reconnaître.

Malgré la honte qu'on peut éprouver face à ce type d'arnaque, il est important de se faire connaître. Porter plainte, témoigner, c'est se dire que cela permettra peut-être d'arrêter l'escroc, mais surtout, cela empêchera d'autres personnes de se faire piéger.

Une volonté qui se retrouve dans certains témoignages. Les proies dénoncent leurs arnaqueurs pour mettre en garde et pour que leurs noms d'emprunt apparaissent sur des listings d'escrocs. Mais aussi pour faire partager leur expérience et pour que l'histoire à laquelle ils ont cru éveille la méfiance chez d'autres personnes, potentielles proies de ces mêmes scénarios.

Beaucoup pourtant ne franchissent jamais le pas de la plainte. Certaines victimes parce qu'elles n'osent pas, d'autres par ignorance, d'autres encore parce qu'elles essayent de régler seules le problème. La honte de s'être fait arnaquer cède la place à un besoin de résoudre le problème par soi-même, à la fois pour retrouver confiance en soi, mais aussi pour éviter d'en faire part à son entourage. « Ces gens-là ne réalisent pas combien leur situation est dangereuse, déplore Christine Goubert. On croise souvent ce genre de scénarios lors des arnaques à la Webcam. Les victimes pensent être plus fortes que leurs arnaqueurs. Si l'escroc demande 3 000 euros pour se taire et faire disparaître la vidéo, la victime va engager la conversation : "tu ne me fais pas peur", "tes menaces ne servent à rien", "je te file la moitié et on en parle plus"... Ils se croient à l'abri mais s'ils commencent à payer, c'est fichu. Parce que dans cette situation, c'est l'arnaqueur qui est puissant. C'est lui qui détient la vidéo, c'est donc lui qui a tout pouvoir de persuasion. La seule arme de l'arnaqué à ce stade, c'est l'ignorance. Feindre d'oublier son escroc, ne pas répondre à ses mails, ses sollicitations et ses demandes, c'est la meilleure façon d'enterrer l'affaire ». Un « laisser-faire » que certaines victimes ont du mal à accepter.

CONSEIL

Multiplier les mesures préventives rend peut-être votre recherche de l'âme sœur ou d'une relation de quelques heures plus compliquée, mais vous y gagnez en tranquillité et en sécurité.

EN RÉSUMÉ

- Le but de l'« arnacœur » est de vous devenir indispensable. Restez vigilants et ne vous coupez pas de votre environnement social.
- Les profils des « arnacœurs » sont souvent similaires. Ils se cachent derrière des profils usurpés. Ils sont riches, attrayants et exercent un métier qui les amène à beaucoup voyager ou font dans l'humanitaire.
- Si peu de temps après une rencontre sur Internet, on vous annonce un départ précipité pour l'Afrique, méfiez-vous, c'est sûrement une arnaque.
- Ne communiquez jamais vos données (nom, âge, adresse...) sur Internet.
- Il faut savoir qu'un représentant de l'État n'aura pas d'adresse gratuite type Yahoo ou Gmail. Il faut accorder de l'importance à la partie située après l'arobase (@).
- En cas de doute, demandez à votre interlocuteur de vous envoyer une photo personnalisée.
- En cas d'échange *via* la Webcam, demandez à votre interlocuteur de faire un signe distinctif afin d'être sûr que ce n'est pas une vidéo préenregistrée.
- Si vous êtes victime de chantage, ne tentez pas de négocier et ne payez pas votre arnaqueur. La meilleure des armes reste l'indifférence. Cessez tout contact avec lui et rapprochez-vous d'une association.

CHAPITRE 6
DES TECHNIQUES QUI ÉVOLUENT

DÉFINITIONS

- **Phishing** ou hameçonnage : technique utilisée pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. Cette technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance – banque, administration, etc. – afin de lui soutirer des renseignements personnels (mot de passe, numéro de carte de crédit, date de naissance, etc.). C'est une forme d'attaque informatique reposant sur l'ingénierie sociale qui peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques (*Wikipedia*).
- **Trojan horse** ou cheval de Troie : logiciel d'apparence légitime, conçu pour exécuter des actions à l'insu de l'utilisateur. La principale différence entre les virus, les vers et les chevaux de Troie est que ces derniers ne se répliquent pas. Ils sont divisés en plusieurs sous-classes, comprenant entre autres les portes dérobées, les logiciels espions, les droppers, etc. (*Wikipedia*).

Paula X.

L'escroquerie peut être poussée très loin. Il faut donc faire attention à tout... Faux e-mails, faux sites, fausses histoires... Si certaines astuces comme l'attention portée aux moyens de paiement sécurisés, si certains témoignages sur des situations douteuses peuvent vous éviter les plus gros ennuis, le système peut se retourner facilement contre vous. Avec les faux e-mails d'arnaqués, par exemple, vous deviendrez aussi arnaqueur à votre insu...

Témoignage

Paula X. rêvait d'un sac Lancel. Ses études dans le monde de la mode l'avaient habituée à voir défiler devant ses yeux des vêtements et des accessoires de grandes marques. Des produits largement inaccessibles au regard de ses finances restreintes. Elle s'était donc résignée à reléguer ses désirs au simple rang de rêves inaccessibles. Elle avait pris l'habitude de faire le tour des sites de petites annonces et y dénichait parfois quelques accessoires de couturier, légèrement usagés, vendus à un prix plus attrayant. Un matin, surfant, comme à son habitude sur les annonces déposées par différents particuliers, elle entrevoit une photo miniature qui ressemble étrangement à un BB, sac Lancel aux courbes très féminines. Intriguée, elle clique dessus et découvre une annonce présentant l'objet photographié sous toutes les coutures. Le cuir patiné beige du sac luisant sous le flash ravive sa soif de marques. Au fil de sa lecture de l'annonce, elle déniche nombre d'informations qui lui font croire que le sac est authentique. Rédigée dans un français parfait, la rapide description de l'objet en vante son parfait

état et surtout, son prix, étonnement bas : 375 euros. Un tarif qui fait sursauter l'acheteuse. Une telle pièce s'achète 880 euros en magasin et il lui paraît invraisemblable d'en trouver un si abordable. Étonnée, et surtout méfiante, elle contacte le vendeur et demande une explication à ce prix aussi bas. La réponse ne se fait pas attendre. Le prix s'explique simplement par une malfaçon dans la couture de la doublure intérieure. Si, d'apparence le sac est absolument parfait, l'intérieur n'est pas aussi soigné que ceux de ses cousins exposés en vitrine sur les grands boulevards. L'explication lui semble logique et le vendeur honnête. Ce sac, elle n'a pas osé l'espérer à son bras et voilà qu'il est à portée de main. Elle décide de prendre une soirée de réflexion avant de donner une réponse au vendeur. Son interlocuteur en prend note, mais lui rappelle la rareté d'une telle offre : il ne peut pas lui garantir, si un autre acheteur se présente, d'avoir toujours le sac en sa possession. Paula prend le risque. Pourtant, l'occasion qui se présente risque d'être unique. Et si un autre acheteur se présentait ? Et si elle laissait passer l'affaire de sa vie ? Ces questions occultent dans son esprit toute notion de sensibilité au danger. Surtout lorsqu'elle reçoit, en fin de soirée, un e-mail du vendeur, lui assurant avoir été contacté par une autre intéressée. La demoiselle décide donc de choisir son camp : elle investit dans l'accessoire. L'internaute avec qui elle convient de la transaction lui assure un envoi rapide de son colis par La Poste. Elle attend donc impatiemment son dû, guettant tous les jours le passage du facteur.

Paula reçoit son paquet quelques jours plus tard et déballe frénétiquement l'article tant désiré. Pourtant, entre ses mains, ce n'est pas le somptueux sac en cuir sombre brillant qui lui apparaît. La besace qu'elle vient de recevoir a, certes, la coupe du sac dont elle rêvait, mais ne possède ni la qualité de son cuir, ni la finition de ses coutures et le « léger défaut de fabrication de la doublure intérieure » s'est transformé en malfaçon généralisée sur l'ensemble de l'accessoire. Elle tente de se plaindre à son interlocuteur qui a pourtant mystérieusement disparu. Il ne répond à aucune sollicitation, pas même quand elle le menace d'une plainte. Il se sait protégé. Et son acheteuse a bien compris qu'elle venait de faire l'acquisition d'une piètre contrefaçon. Malgré toutes les promesses que le vendeur n'a pas honorées, la jeune femme n'a aucun moyen de se retourner et s'est rendue complice d'une arnaque en achetant une contrefaçon, même si, elle ignorait au départ les manigances de son interlocuteur.

De vraies fausses marques

Avec Internet, il est devenu de plus en plus facile d'écouler des marchandises frauduleuses, les contrefaçons en premier lieu. Malgré la modération très active effectuée par des sites de petites annonces gratuites tels que trefle.com, certaines marchandises passent au travers des mailles du filet et l'acheteur, pensant recevoir un véritable article de marque, se retrouve complice d'une escroquerie.

En pratique

Déceler la vraie de la fausse affaire sur Internet

Lors d'un achat sur le Net, deux indicateurs doivent vous alerter :

- Le prix est le premier indicateur. Même d'occasion, un vêtement, un sac de marque coûtera forcément cher. Si le prix vous semble particulièrement bas, comparez-le avec les véritables prix de la marque. Quand votre intuition se confirme et que les tarifs sont bien inférieurs aux prix initiaux, laissez tomber, vous avez souvent affaire à des arnaques ou à des contrefaçons.
- Le second indicateur est un peu plus subtil et réside dans les photos attachées aux produits. Certains détails peuvent vous mettre la puce à l'oreille. Les logos sont parfois mal reproduits, les couleurs sont peu ressemblantes ou bien certains éléments de la coupe sont suspects…

Dans le doute, abstenez-vous d'acquérir : même si vous étiez ignorant du caractère frauduleux de la vente, vous vous en rendrez complice en achetant le produit. Les sanctions peuvent alors être très lourdes : en plus de la confiscation du produit, l'amende peut s'élever jusqu'à une ou deux fois le prix du produit contrefait. Des sanctions douanières auxquelles peuvent se rajouter des dommages et intérêts pouvant aller de 300 000 à 500 000 euros si les marques flouées demandent réparation.

Les escrocs ont tendance à garder les mêmes scénarios, quelle que soit la victime à laquelle ils s'adressent. Ils l'adaptent, bien sûr, pour que les détails collent aux exigences de leurs interlocuteurs, mais les grandes lignes restent généralement les mêmes. Il ne faut pourtant pas se leurrer : le mensonge est leur source

de revenus et comme toute profession l'exige, aussi illégale et malhonnête soit-elle ici, ils se doivent d'innover sans cesse et de faire évoluer leurs histoires pour survivre. Les arnaqueurs en sont pleinement conscients, et c'est là que réside toute leur dangerosité : leur incroyable capacité à s'adapter. Les associations, en première ligne quand il s'agit de prévention, savent à quel point leurs adversaires sont prompts à se fondre dans la masse des internautes en singeant leurs codes.

À SAVOIR

Si Internet reste une sphère particulière, les codes y sont les mêmes que dans la vie. La confiance que vous placez dans votre interlocuteur ne doit pas supplanter votre sensibilité au danger.

De faux e-mails

N'oublions pas que si les spams existent toujours, c'est que cela fonctionne. On en distingue trois types :

- ceux qui reprennent dans les grandes lignes des scénarios d'arnaques pour vous demander de l'argent ;
- ceux qui se font passer pour des e-mails de votre banque ou votre opérateur pour récupérer vos identifiants ;
- ceux qui, envoyés depuis l'adresse de l'un de vos contacts grâce à un virus ou Trojan horse (cheval de Troie), vont vous attirer sur un site frauduleux, et infecter votre propre poste.

Les appels à l'aide

Le premier type de spam est sans doute l'un des plus faciles à repérer. Ce sont des e-mails de jeunes hommes ou femmes ayant récemment perdu toute leur famille dans un accident ou lors de

heurts armés en Afrique. La malheureuse famille aura tout de même eu la possibilité de léguer à son unique enfant survivant une somme faramineuse, et toujours en « dollars US ». Mais, coup du sort, il lui faut une aide extérieure pour faire sortir l'argent du pays sans payer de taxe sur l'héritage. Mais là aussi, le scénario peut connaître des retouches, des améliorations, jusqu'à atteindre des histoires de plus en plus rocambolesques.

Il arrive que ce soit un banquier qui vous contacte ayant découvert un immense fonds en dollars dormant dans sa banque et qui, non réclamé depuis plusieurs années, sera dans quelques jours propriété de l'État. Il vous demande donc de l'aide pour faire sortir l'argent du pays. Vous avancez un peu d'argent, une somme dérisoire par rapport à celle qu'il vous fait miroiter, et récoltez au final un beau pourcentage des fonds illégalement sortis du territoire africain.

Mais certains escrocs vont jusqu'à pousser l'invention bien plus loin, en prenant appui sur l'actualité, pourquoi pas...

« Bonsoir,

J'ai eu votre contact et voudrais partager une affaire très importante avec vous. Si ça ne vous intéresse pas, veuillez m'excuser beaucoup pour le dérangement. Je suis Monsieur Issam Majeed, je travaille en Iraq avec les militaires américains comme traducteur. J'ai des preuves pour vous le démontrer après. Dans une de nos opérations militaires en Iraq, nous avons découvert un coffre-fort dans la maison d'un homme d'affaire Iraqien dans la ville de Tikrit. Ce coffre-fort contient US $ 20 Millions. Nous avons immédiatement gardé ce coffre-fort dans un lieu sécurisé avec trois autres soldats. Après de longues délibérations entre nous pour savoir si nous devons remettre

ces fonds aux autorités américaines en charge du lieu ou pas, nous avons tous décidé de partager ces fonds entre nous. Pour le partage, chacun de nous a reçu la somme d'US $ 5 Millions. Pour ma part à cause des problèmes de sécurité en Iraq, j'ai décidé de m'arranger avec les agents de sécurités privées pour transférer ma part de ces fonds hors du pays, précisément à Londres. J'ai mis les fonds dans un colis comme étant des affaires familiales et je l'ai codé ce qui veut dire qu'aucune personne ne sait que ce colis contient de l'argent sauf moi. Ce que je vous raconte est la vérité et si nous traitons ensemble dans cette affaire, vous le verrez. Je vous contact donc pour voir si vous pouvez m'aider à récupérer le colis à Londres et le transférer dans votre pays ou je voudrais investir ces fonds. Je vous donnerais aussi quelques pourcentages de ces fonds pour avoir accepté de m'aider, le pourcentage nous en discuterons quand je recevrai votre réponse. Les insurgés iraquiens sont contre moi ce qui fait qu'ils me recherchent pour me tuer parce que je fais des traductions aux militaires américains. Je ne sors pas n'importe comment sans les militaires américains pour éviter le pire. Je n'utilise pas de téléphones ni ne reçois des appels ici. J'utilise seulement Internet et les walkies-talkies pour communiquer avec des militaires avec qui je travaille. Si cette transaction est bien conclue, je veux démissionner de ce travail parce que pour vivre ici en Iraq c'est trop risqué. Je vous remercie et j'attendrais votre réponse. Monsieur Issam Majeed. »

Si l'arnaque peut paraître évidente pour certains, le simple fait que ces e-mails existent et continuent de se répandre signifie qu'il y a des gens pour y croire. Et quand bien même cette situation serait réelle, la transaction que cet homme propose est d'une totale illégalité. Elle consiste à faire sortir d'un pays, sans le déclarer, des fonds qui ne lui appartiennent pas. Dans ce cas, voudriez-vous alors vraiment vous rendre complice d'un acte frauduleux ?

Le phishing

D'autres courriels vont reproduire un message d'une banque. En ouvrant votre e-mail, vous serez invité à cliquer sur un lien, sous un prétexte quelconque. Ce lien vous redirigera vers une page Internet où l'on vous demandera vos identifiants bancaires et, en toute confiance, puisque le mail provient d'une enseigne bancaire, vous les renseignerez. C'est une très mauvaise idée. Vous y aurez été attiré sous des prétextes divers : sécurisation de votre compte, brèche dans le système de sécurité qui force les équipes techniques à vous demander de vous identifier... et parfois même des excuses dignes du Monopoly : « Erreur de la banque en votre faveur ».

En pratique

Déceler un faux site bancaire

Même si le site ressemble au portail de votre banque, ce n'est qu'un leurre. Loin d'être aussi sécurisé, il aura été créé pour vous inciter à y déposer votre identité bancaire (numéro de compte, de carte bleue, mot de passe...). Si vous cliquez sur le lien attaché, vous pourrez aisément distinguer cette copie, ce « faux » du véritable site de votre banque en observant l'adresse. Celle du site de votre

banque, sécurisé, commencera par « https », tandis que celle du site des escrocs aura tendance à être tout à fait classique, c'est-à-dire en « http ». Toutefois, pour vous assurer une complète sécurité, ne cliquez pas sur le lien attaché. Ouvrez un nouvel onglet ou une nouvelle fenêtre du navigateur de votre choix et rendez-vous directement sur le site Internet de votre banque. Vous pourrez ainsi entrer vos codes et mot de passe, vérifier l'intégrité de votre compte… sans crainte de voir vos identifiants volés par un escroc.

Tout comme lorsque vous recevez un e-mail de votre banque, l'escroc va tenter d'abuser votre confiance en piratant le compte mail de l'un de vos contacts. La manœuvre est simple. Vous recevrez un e-mail d'une adresse connue qui vous signalera une promotion sur un site, ou mieux encore, vous recevrez un message du type « Hey ! J'ai vu ta photo sur ce site. Comment se fait-il que tu y sois ? ». Y sera collé le lien du site en question. La curiosité aidant, vous serez tenté de cliquer sur le lien. Tout ce que vous récolterez à cliquer sur ce lien, c'est hériter d'un virus qui non seulement permettra à l'escroc de prendre le contrôle de votre boîte mail, mais surtout fera de vous l'un des vecteurs de cette chaîne. C'est-à-dire qu'à votre tour, et surtout à votre insu, vous enverrez ces e-mails indésirables à toute votre liste de contacts.

« Beaucoup se font encore prendre par le phishing » insiste Christine Goubert. C'est sur ce point précis, qu'elle souhaite attirer l'attention. Elle rappelle qu'il ne faut pas communiquer ses coordonnées personnelles et bancaires à quelqu'un que l'on ne connaît pas. Les établissements bancaires ou encore la CAF, EDF et les fournisseurs d'accès à Internet ne demandent jamais ce genre d'information. Ils disposent déjà de vos coordonnées si vous êtes clients chez eux. De même, n'envoyez pas de copies de votre carte d'identité ou de votre passeport à un inconnu.

Ce dernier risque de vouloir usurper votre identité pour de prochaines arnaques.

Les réseaux sociaux

Les escrocs s'adaptent aux évolutions de la technologie et vont là où se trouvent les données intéressantes pour eux. Les réseaux sociaux et notamment Facebook sont devenus un véritable repère pour les arnaqueurs. La présidente de l'AVEN les compare à des « véritables marchés » pour les personnes malhonnêtes. La méthode reste là même, seul le support change. C'est pourquoi elle conseille de ne pas accepter quelqu'un que l'on ne connaît pas parmi ses contacts Skype, Facebook...

Mais plus que tout, il faut toujours avoir à l'esprit que les arnaques sont par essence extrêmement variées. Sur des sites de petites annonces ou des sites de rencontres, elles prennent généralement l'une des formes que nous vous avons décrites. Mais il en existe bien d'autres, qui prolifèrent sur différentes plateformes : Facebook est par exemple un média qui prend de plus en plus d'importance dans l'élaboration des arnaques. On vous fera miroiter un gain remporté dans une loterie à laquelle vous n'avez jamais participé, on vous proposera de savoir qui consulte votre profil Facebook ou de « liker » : des pages totalement bidon. Toutes ces manœuvres ont pour objectif de pirater votre compte et toutes les informations qui y sont stockées, voire parfois de

À SAVOIR

Les escrocs profitent de Facebook pour récupérer des identités ainsi que des photos qui, par la suite, seront utilisées pour créer des personnages et ainsi mener d'autres arnaques. Les usagers de Facebook sont ensuite directement contactés par ces faux profils.

vous pousser à vous inscrire à des services qui vous factureront leurs prestations par SMS. Christine Goubert affirme ainsi que Facebook est devenu, en 2013, le repère n° 1 des faux profils : « *Les gens ne se méfient pas et les arnaqueurs viennent faire leur marché* ».

« *Facebook n'est pas réactif à nos signalements. Les faux profils restent en ligne malgré nos signalements à répétition* », ajoute Christine.

CONSEIL

Un petit tour sur la page Facebook de l'AVEN permet de voir les nombreux faux profils recensés.

Si les réseaux sociaux sont de formidables moyens de communication, ils ne doivent pas être autre chose. Tous les services qu'ils proposent ont tendance à pousser les utilisateurs à toujours mettre à jour leurs statuts pour être sans cesse connectés. Vous y étalez votre vie et nombre d'informations qui peuvent devenir compromettantes. Alors ne cliquez pas sur n'importe quel lien, même si c'est un ami qui vous le propose : il n'est pas impossible qu'il se soit fait pirater son compte et vous envoie ces invitations à son insu. Une technique qui n'est pas nouvelle. Apparue avec les e-mails, elle n'a fait que s'adapter aux nouveaux moyens de communication.

Des victimes de plus en plus jeunes

La présidente de l'AVEN nous fait également part d'une nouvelle tendance : « *Désormais, même les adolescents de moins de 18 ans sont ciblés,* via *l'arnaque à la Webcam.* » Ces nouvelles cibles sont approchées sur des sites comme Bazoocam, l'équivalent Français de Chatroulette, ce site où il est possible de faire des rencontres

en utilisant la plateforme de chat. Pour Christine Goubert, ce site devrait êtrefermé. Elle nous indique également que les adolescents qui surfent sur Skyblog sont harcelés par de faux profils de jeunes pour fournir des photos « hot ». « *Les arnaques se sont étendues* via *les réseaux sociaux, Facebook, Badoo, Netlog, etc., de sorte qu'aujourd'hui, plus personne n'est à l'abri sur un site soi-disant sécurisé, plutôt qu'un autre* ».

L'expert judiciaire connu sous le pseudo « Zythom » nous met également en garde contre les dangers que constitue Internet pour le jeune public. Il nous rappelle que les cibles les plus vulnérables sont souvent les débutants, comme les personnes âgées ou encore les enfants. « *En tant qu'expert judiciaire, j'ai eu à traiter pour la justice de nombreux dossiers d'images pédopornographiques. J'en parle beaucoup sur mon blog (http://zythom.blogspot.com)* ». L'expert relate notamment sur son blog, l'histoire d'une adolescente, « Manon » qui est tombée dans les filets d'un internaute mal intentionné. « *J'ai moi-même trois enfants et je sais que qu'il n'y a pas de solution miracle permettant de les protéger de manière absolue. Néanmoins, je pense qu'il y a quelques fondamentaux que les parents devraient respecter* ». Zythom conseille ainsi aux parents de ne pas laisser un enfant accéder seul à Internet avant l'entrée du collège. « *Il faut rester avec lui et surveiller ce qu'il fait,* ajoute-t-il. *Si l'enfant montre très tôt une envie d'aller sur Internet, il faut installer un logiciel de contrôle parental avec une liste de sites autorisés, sélectionnée par les parents.* » Mais, prévient-il, « *malgré la présence de ce logiciel, il faut rester auprès de son enfant* ». Le bloggeur illustre alors son propos avec une analogie pertinente : « *On ne laisse pas un enfant se promener seul dans une forêt parce qu'on lui a mis un GPS dans sa poche !* ».

Outre le logiciel de contrôle, Zythom mise également sur la prévention. « Je pense qu'il faut parler très tôt des dangers d'Internet avec ses enfants, bien avant l'adolescence. Sans diaboliser Internet, il faut expliquer qu'il y a des personnes dangereuses et qu'il faut s'en protéger. On procède de la même manière

avec les enfants que l'on laisse partir seul à pied à l'école en leur expliquant qu'il ne faut pas accepter de bonbons d'un inconnu ou de monter dans une voiture avec quelqu'un que l'on ne connaît pas. » L'expert insiste alors : « Il faut expliquer à ses enfants qu'en cas de situation bizarre ou étrange, il faut absolument qu'ils préviennent leurs parents, ou au moins en parlent à un adulte. Même s'ils ont fait une bêtise… ».

EN RÉSUMÉ

- Au moment d'un achat par l'intermédiaire d'un site de petites annonces, il faut notamment prêter de l'attention au prix et aux photos attachées à l'annonce.
- N'effectuez de paiement que sur des sites sécurisés dont l'url commence par « https ».
- N'oubliez pas que la confiance que vous placez dans votre interlocuteur ne doit pas supplanter votre sensibilité au danger.
- Ne répondez pas aux e-mails présentant des scénarios rocambolesques, même s'ils viennent de vos contacts.
- Facebook est devenu le repère numéro 1 des arnaqueurs. Il faut redoubler de vigilance lorsque vous surfez sur le réseau social.
- Si vos enfants utilisent fréquemment Internet, pensez à installer un logiciel de contrôle parental.
- Ne laissez pas vos enfants surfer sur le Net tout seuls s'ils sont encore jeunes.

CHAPITRE 7
DES SCÉNARIOS ROCAMBOLESQUES

DÉFINITIONS

- **SPAM** (pourriel ou polluriel) : communication électronique non sollicitée, en premier lieu *via* le courrier électronique. En général, envois en grande quantité effectués à des fins publicitaires. En France, 95 % des messages échangés courant décembre 2006 étaient des spams. Ces pourcentages varient selon les articles publiés, mais la barre des 90 % est toujours dépassée. En mai 2009, Symantec annonce le chiffre de 90,4 %. Pour Microsoft, concernant la période de juillet à décembre 2008, la proportion de messages indésirables est de 97 % (*Wikipédia*).
- **Spearphishing** : technique d'hameçonnage ciblé où les « scammeurs » envoient des messages personnalisés à leurs victimes. Dans l'opération « Octobre Rouge », récemment découverte par le laboratoire d'anti-virus Kaspersky, tel diplomate a par exemple reçu une petite annonce de vente de voiture diplomatique. Le spearphishing se joue sur le long terme, explique *The Next Web*, un peu comme un voleur qui repèrerait les lieux plusieurs fois avant de cambrioler

une maison. De telle sorte que, lorsque le pirate envoie son maliciel (dans un mail se faisant passer pour votre banque et incluant même votre numéro de compte bancaire, récupéré en piratant votre boîte mail par exemple), la victime est beaucoup plus à même de se faire avoir (*Slate.fr*).

Au-delà des exemples cités, il existe bien d'autres arnaques, l'imagination des escrocs est sans limites. Voici quelques exemples supplémentaires de scénarios rencontrés sur le Net où l'on vous propose de payer votre bien immobilier en argent liquide, où l'on vous fait miroiter un gain de plusieurs milliers d'euros remportés dans une loterie à laquelle vous n'avez pas participé... Des histoires toutes plus incroyables les unes que les autres !

Un étranger est intéressé par votre bien immobilier

Vous proposez votre maison à la vente sur plusieurs sites immobiliers. Parmi les propositions que vous recevez, vous remarquez le mail d'un étranger, souvent se disant Israélien. Pour des problèmes de visa, il ne peut se rendre en France mais, très fortuné, il désire investir dans l'immobilier et acquérir votre bien sans en discuter le prix et, bien sûr, sans le visiter. Au fil des mails, l'arnaque se précise. Il vous propose d'abord de payer cette maison en liquide. Si vous acceptez, il vous faudra aller chercher l'argent chez son associé basé à Turin, Amsterdam, Bruxelles... ou une autre destination d'Europe. Si vous refusez, il insistera tout de même pour vous payer une petite partie de la somme en liquide, généralement 5 % du prix, là aussi à aller chercher auprès du collaborateur étranger. À partir de là, le scénario peut prendre plusieurs chemins :

- Vous vous rendez en Italie et obtenez effectivement la somme demandée en échange de la maison : félicitations, il y a de

fortes chances pour que vous ayez aidé vos interlocuteurs à blanchir leur argent !

- Vous vous rendez en Italie et l'on vous présente une mallette de billets en grande partie « noircis ». Il faut alors investir dans un produit spécial pour les « blanchir » une fois la frontière passée. Il faut débourser un peu d'argent pour graisser la patte à quelques fonctionnaires histoire de faire sortir les capitaux du pays en toute sécurité, une somme dérisoire comparée à celle que vous pourrez emporter…
- Vous ne vous rendez pas en Italie. Et votre acheteur reste en contact avec vous pendant des semaines prétextant des frais imaginaires qu'il vous faudra régler avec, bien sûr, une promesse de remboursement de la part de votre interlocuteur.

Lorsqu'un étranger ou un ressortissant français vous contacte, dirigez-le toujours vers votre notaire. En plus d'être obligatoire, cela vous permettra de filtrer les annonces les plus dangereuses : aucun escroc ne prendra le risque d'aller s'exposer devant un notaire. Mais plus que tout, mettez-vous à la place d'un acheteur :

- Vous investiriez dans un bien immobilier sans jamais le voir ?
- Si vous n'avez pas la possibilité de vous déplacer, vous ne mandateriez pas un expert immobilier ?
- Pourquoi insister pour payer en liquide alors qu'il est si simple, lorsque l'on est à l'étranger, de régler ses transactions par virement bancaire ?

CONSEIL

En cas de doute, adressez-vous à un notaire ou un expert immobilier. Ils sauront tous deux vous aider à vérifier la véracité des propos de votre interlocuteur et vous conseilleront en fonction de la situation.

Vous gagnez à la loterie

Comme tous les jours, vous allez faire un tour du côté de votre boîte mail pour y voir vos nouveaux messages. Quelle surprise quand vous découvrez un courriel qui vous annonce à grand renfort de bannières clignotantes que vous avez gagné des milliers d'euros à une loterie !

> *Très cher(e) Monsieur ou Madame / Mlle A l'occasion de la rentrée des classes 2011, la loterie LUCKYSURF (COCODY) en collaboration avec MICROSOFT et ses partenaires PÉTROLIERS, Princes SAOUDIENS, et INVESTISSEURS ANGLAIS, FRANÇAIS a organisé une Loterie concernant toutes personnes ayant une adresse électronique vivant en Afrique Europe et Amérique dans le cadre d'une semaine promotionnelle. Les adresses internautes ont été sélectionnées par un nouveau programme informatique en essai pour la lutte contre les spams. System aléatoire au cours duquel votre adresse mail attachée au numéro d'identifiant MMAP-007823-11-03-V a été tiré au sort. Aussi, conformément aux articles 43 et 49 du traité Européen autorisant tout ressortissant de l'Union européenne à promouvoir, prester et bénéficier d'un service (y compris les loteries et jeux d'argent) vous avez été promu grand gagnant du 5ième lot rattachée au numéro MMAP-007823-11-03-V de la loterie LUCKYSURF sans avoir participé directement. Le premier prix est deux jumelées villa (piscine, garage, en bordure d'eau) d'une valeur de 520 000 euros située à la Riviera GOLF (Abidjan). Le second prix, la somme de € 190 000 euros 3ième prix*

est un montant de € 132 000 euros 4ième prix un montant de € 112 000 euros 5ième prix un montant de € 95 000 euros 6ième prix un montant de € 70 000 euros Etc.... À l'issue de ce Tirage, vous avez été tiré à la 5ième place donc l'heureux (se) bénéficiaire de la somme de € 95 000 euros. Votre code de vérification est : (CB) : 196-635-C Nous vous envoyons cet e-mail pour l'affirmation des résultats du tirage au sort. Vous êtes l'heureux (se) gagnant (e) du lot numéro 5 d'où la somme de 95 000 euros. À la lecture de ce message, nous vous prions d'adresser un courrier en retour à l'huissier de justice de la supervision Me AKA BILE témoin du tirage, en lui précisant VOTRE :

Nom

Prénoms

Adresse géographique

Tél

Pays

Date de naissance

Ville

Profession

Code postal

Code gagnant

Afin que ce dernier puisse entamer la procédure de remise de gain ci-dessous les coordonnées de l'avocat de justice ; CABINET D'ÉTUDE MAÎTRE AKA BILE [Siège : Plateau résidence AKA 7e étage, porte 58] E-MAIL : dtombola@cpll.cn TEL : 0022 566 121 957 Pour des raisons de sécurité, nous vous prions de garder une confidentialité

absolue autour de ce message car des personnes autres que les gagnants nous envoi des codes et des messages se faisant passer comme tel. Madame RAYMONDE CAROLE DIRECTRICE DES OPÉRATIONS Copyright © 2011-2012 The Microsoft CI Lottery Inc. All rights reserved. Terms of Service - Guidelin

Ne rêvez pas, cela n'existe pas ! Le principe initial de la loterie est simple. Les joueurs payent un ticket papier ou une inscription Internet... le cumul de toutes ces petites contributions permettent à l'organisme de jeux de constituer une cagnotte. C'est cette somme qui sera gagnée par l'un des joueurs. Si vous êtes tiré au sort lors d'une loterie à laquelle vous ne vous êtes jamais inscrit, cela signifie qu'un organisme de jeux, dont l'objectif, il ne faut pas l'oublier, est aussi de s'enrichir, vous offre gracieusement une grosse somme d'argent. Quel intérêt a-t-il à faire cela puisqu'il n'en retire aucun bénéfice financier ? Même si ce sont des investisseurs richissimes qui vous permettent de gagner cet argent, quel intérêt y trouvent-ils ?

À SAVOIR

Malgré le caractère virtuel de la sphère Internet, les codes qui y ont cours sont les mêmes que dans la vie : personne ne vous fera cadeau d'une grosse somme d'argent s'il n'en retire aucun bénéfice.

Le fonctionnement de l'arnaque est simple. Si vous donnez vos coordonnées à l'huissier ou à l'avocat nommé dans l'e-mail, il vous harcèlera de mails et de coups de téléphone prétextant des frais de dossier, des sommes à débourser pour débloquer les fonds ou leur permettre de passer la frontière... des montants dérisoires, par rapport à la somme que l'escroc vous fait miroiter, mais que vous ne toucherez, évidemment, jamais.

On vous demande de faire sortir de l'argent du pays

Toujours par e-mail, vous recevez le message d'un orphelin découvrant avec stupeur que son papa récemment décédé lui a laissé une grosse somme d'argent en héritage. Malheureusement, son pays natal est d'une grande instabilité politique et sécuritaire. Il vous demande donc de l'aide pour faire sortir les capitaux du pays, en échange de quoi vous toucherez une partie de l'héritage. Dans ce cas de figure, une fois en contact avec l'arnaqueur, on vous demandera d'avancer des frais pour subvenir aux besoins de votre interlocuteur ; poursuivi, il doit se réfugier à l'hôtel mais n'a pas de quoi payer ; on l'a agressé puis on lui a volé tout son argent ; il est à l'hôpital et doit avancer des frais médicaux... Toutes les excuses sont bonnes pour que vous lui envoyiez de l'argent en attendant l'arrivée de l'héritage comme un retour sur investissement. Une fois de plus, ne rêvez pas, cet argent n'arrivera jamais jusque dans vos mains.

Ce scénario d'arnaque peut connaître quelques variantes. Vous pouvez être contacté par un banquier qui aura découvert un compte particulièrement approvisionné mais dont l'unique bénéficiaire est décédé. Il vous proposera donc d'en partager la somme moyennant une aide logistique et financière pour faire sortir en toute discrétion les capitaux du pays avant que, selon la loi, ils ne deviennent propriété de l'État. Parfois, on vous demandera de recevoir des Traveler's Cheques d'une certaine somme, de les encaisser et de renvoyer la même somme d'argent, par Western Union. Là aussi, c'est une arnaque : les Traveler's Cheques mettront quelques jours à être encaissés et, alors que vous aurez déjà envoyé l'argent à votre correspondant, votre banque vous informera que les chèques déposés ne sont pas valides. Inutile de dire que vous ne reverrez donc jamais votre argent.

On vous propose un échange

Vous déposez une petite annonce sur un site Internet pour vendre un bien. Après quelque temps, un acheteur qui semble tout à fait digne de confiance vous aborde avec l'intention d'acquérir ce que vous mettez en vente. En internaute prudent, vous donnez rendez-vous à l'acheteur potentiel afin que la transaction puisse se faire en main propre. À votre arrivée, pourtant, votre interlocuteur vous propose un échange : votre bien contre le sien en excellent état. Il possède tous les papiers légaux (assurance, certificat d'authentification, garanties, carte grise...). Pourtant, ce bien que vous acquérez n'est pas le sien : votre acheteur va simplement se servir de vous pour écouler une marchandise acquise de manière frauduleuse et souvent volée.

CONSEIL

Lorsque vous vendez ou acquérez un bien, contentez-vous des termes prédéfinis dans l'annonce :

- *si vous vendez un bien, n'acceptez que la compensation financière que vous attendiez, pas d'échange, pas de troc ;*
- *si vous achetez quelque chose, abstenez-vous des règlements non déclarés ou des petits arrangements que votre vendeur pourrait proposer.*

Lors d'une transaction sur un site de petites annonces, tenez-vous donc au montant prévu dans l'annonce et prémunissez-vous de toute manipulation qui pourrait être malhonnête et qui, à n'en pas douter, se retournerait contre vous.

Mais plus que tout, ne vous déplacez jamais à l'étranger ! Quel que soit le bien que vous souhaitez acquérir, il y a des moyens simples pour le faire porter jusque devant votre porte, que ce

soit par La Poste ou en ayant recours aux services d'un transporteur spécialisé.

Dans le cadre d'arnaques à l'amour, si vous proposez de vous rendre sur place, au mieux, vous risquez de ne trouver personne au rendez-vous fixé. Dans le pire des cas, vous risquez d'être agressé et dépossédé de tous vos biens. Des affaires rares, certes, mais suffisamment violentes pour être remarquées. On en trouve quelques exemples jusque sur Wikipédia (http://fr.wikipedia.org/ wiki/ Fraude_4-1-9) :

À SAVOIR

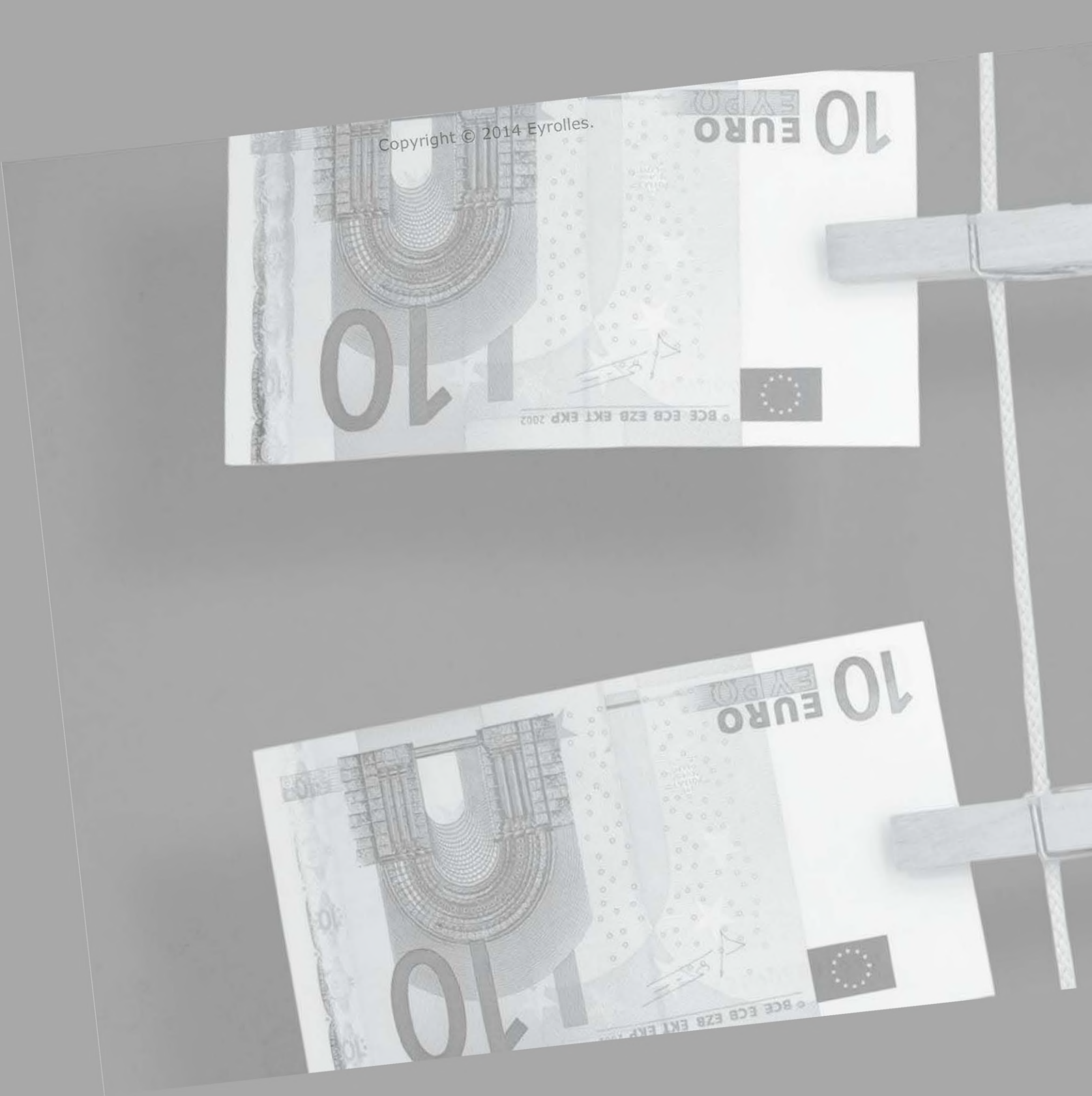
Vous déplacer à l'étranger, c'est prendre le risque de vous faire littéralement dépouiller.

- Un Américain a été assassiné à Lagos en 1995 alors qu'il tentait de récupérer son argent.
- Un Tchèque a tiré sur un diplomate nigérian qu'il prenait pour responsable de son escroquerie en 2003.
- En 2004, c'est un Grec qui a été victime d'une arnaque et qui, kidnappé à Durban, a été mutilé, puis tué.

L'imagination sans bornes des escrocs et leur capacité, sans cesse grandissante, à s'adapter aux exigences de leurs victimes en font des prédateurs particulièrement dangereux. Présents dans chaque recoin d'Internet, ils guettent leurs proies et sont très doués quand il s'agit de s'attirer leur confiance. Restez donc méfiant et, à moins que vous n'ayez rencontré en personne votre interlocuteur, abstenez-vous de transactions risquées. En cas de doute, demandez toujours conseil à votre banquier, votre notaire ou un avocat. Ils sauront vous orienter et vous faire éviter de tomber dans les griffes des arnaqueurs.

EN RÉSUMÉ

- Ne vous laissez pas avoir par des offres trop alléchantes. Gardez votre esprit critique en toutes circonstances.
- Si un étranger est intéressé par votre bien immobilier. N'entamez pas directement de négociations avec lui. Dirigez-le vers un notaire.
- Vous ne pouvez pas gagner à la loterie si vous n'avez pas participé. Méfiez-vous des e-mails vous garantissant le contraire.
- Lors d'une transaction sur un site de petites annonces, assurez-vous que votre interlocuteur respecte les règles prédéfinies. En aucun cas, n'acceptez de faire un échange.
- Dans tous les cas, suite à une transaction ou une rencontre sur Internet : ne vous déplacez pas à l'étranger !



PARTIE 3

QUELS SONT LES RECOURS ?

Que faire quand il est déjà trop tard ? Quand, malgré les précautions qu'on a pu prendre, l'escroc a su jouer sur nos failles et nous a arnaqué ? Souvent démunies, les victimes ne savent pas vers qui se tourner. Pourtant, il est important de se faire connaître et de dénoncer les arnaqueurs. La divulgation, par exemple, des pseudos utilisés pour ces criminels ainsi que leurs fausses adresses e-mails et leurs faux numéros, va empêcher d'autres victimes de tomber dans leurs pièges.

Les associations telles que l'AVEN, ou encore les sites tels que lesarnaques.com sont des lieux de rencontres et d'échanges entre les victimes. Elles font un gros travail de prévention et alertent les internautes des dangers du Net. Elles guident et aident les victimes qui, après une arnaque, se sentent souvent honteuses et n'osent pas en parler. Il est aussi commun de voir des personnes qui sont en véritable détresse et affaiblies psychologiquement après avoir été manipulées par un escroc sans scrupule. C'est pour les aider à reprendre confiance en elles et dénoncer les agissements du criminel que les associations se battent.

Même s'il est compliqué de traquer ces truands d'un nouveau genre jusque chez eux, le simple fait de porter plainte et de dénoncer leurs méthodes permettra de contrecarrer leurs arnaques. Actuellement en France, peu d'escrocs sont confondus. Plusieurs raisons expliquent cela : manque de moyens, difficultés techniques, coût de la procédure pour l'État... Pourtant, la multiplication des plaintes est le seul moyen pour stopper les fraudes. Quelles démarches faut-il, alors, entreprendre pour arrêter ces criminels ?

CHAPITRE 8
VOS PLAINTES, LEURS FEINTES

DÉFINITIONS

- **Escroquerie** : l'article 313-1 du Code pénal la définit comme *« le fait de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge »*.
- **Escroquerie en bande organisée** : selon l'article 132-71 du Code pénal, *« constitue une bande organisée au sens de la loi tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions »*. L'escroquerie en bande organisée est un délit passible, selon l'article 313-2 du Code pénal, de dix ans de prison et d'un million d'euros d'amende.

Charles G.

L'escroc a gagné, vous êtes tombé dans ses griffes. Mais vous n'avez pas dit votre dernier mot et vous souhaitez-vous en

remettre à la justice… Malgré votre plainte, les services judiciaires s'avèrent souvent inefficaces face à ces agissements frauduleux menés depuis l'étranger, même si certains accords facilitent l'enquête. Mais il faut savoir que plus il y aura de plaintes, plus les enquêtes auront des chances d'aboutir… Malgré toutes les mesures préventives prises, il peut nous arriver à tous d'être victime d'une arnaque. Dans ces cas-là, il est impératif de se faire connaître auprès de la justice. Des démarches qui permettent d'appréhender toute l'ampleur du problème mais qui ne sont pas toujours évidentes à mener.

Témoignage

Charles G. avait l'habitude de traquer les bonnes affaires sur un site de petites annonces entre particuliers. Ce jour-là, il tombe sur une annonce d'un jeune Français désireux de se séparer de son iPhone dans les plus brefs délais. Tarif de la vente : 110 euros. Ravi et croyant flairer la bonne affaire, Charles contacte le vendeur par e-mail. Il émet pourtant quelques doutes quant au prix, si bas, de l'appareil. Son interlocuteur affirme devoir partir en Côte d'Ivoire suite à une mutation professionnelle. Il y disposera d'un téléphone professionnel et arrivant en fin de forfait en France, son combiné ne lui sert plus à rien. Rassuré, l'acheteur décide de prendre quelques jours pour réfléchir avant d'acheter. Il en parle à sa compagne et tous deux décident d'acquérir ce téléphone si bon marché. Charles recontacte donc son vendeur qui lui apprend s'être déjà rendu en Afrique. Mais pas de souci, il prendra à sa charge les frais de transport. L'acheteur est ravi. Seulement, pour des raisons pratiques, on lui demande de transmettre l'argent par Western Union. Avant de se lancer dans un transfert

d'argent, le payeur se renseigne un peu sur Western Union. Présente dans une majorité des pays du globe, elle est notamment partenaire de La Poste en France. Rassuré de savoir un organisme de service public partenaire de l'entreprise, il se lance et transfère en toute confiance 110 euros vers la Côte d'Ivoire. Il contacte son vendeur pour lui assurer que la transaction est effectuée, lequel lui répond poster le colis dans le courant de la journée. Un peu plus d'une semaine après, ne voyant aucun colis arriver, Charles tente de recontacter son interlocuteur, en vain. Coups de téléphone et e-mails restent sans réponse et lui, sans colis. Il décide alors d'entreprendre quelques recherches. Après seulement quelques minutes, l'acheteur floué repère le nom de son vendeur et la description de la vente frauduleuse sur un listing d'arnaqueurs. Outré, il envoie un e-mail incendiaire à l'internaute étranger, le menaçant d'aller porter plainte s'il ne reçoit ni réponse ni remboursement de sa part. Silence radio. Déterminé à se faire dédommager, Charles G. se rend au commissariat le plus proche. Arrivé devant l'entrée, il hésite. D'abord parce qu'il se sent un peu honteux de s'être laissé prendre au piège de l'escroc. En effet, une fois la première vague de colère passée, il s'est senti bête : comment lui, d'ordinaire réfléchi et méfiant, avait-il pu se faire berner ? Avec toute la connaissance qu'il avait d'Internet, il pensait ne courir aucun risque... et il n'ose pas maintenant aller se confronter à un inconnu pour lui expliquer son histoire au risque de se sentir jugé et moqué.

Escroqueries : que dit la loi ?

La plupart des affaires d'escroqueries qui sont finalement jugées sont commises en bande organisée. Pourquoi ? Y a-t-il beaucoup d'arnaques ainsi commises ? Et surtout, qu'est-ce qu'une bande organisée selon la justice ?

Selon l'article 132-71 du Code pénal, « constitue une bande organisée au sens de la loi tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions ». Une définition juridique qui date de 1981. Elle avait alors été créée pour les affaires de vols avant de s'étendre en 1983 aux destructions et dégradations. La notion de bande organisée n'a alors pas cessé de s'étendre jusqu'à atteindre les rives de l'escroquerie en 1994. Punie par le droit français, l'escroquerie en bande organisée est un délit passible, selon l'article 313-2 du Code pénal, de dix ans de prison et d'un million d'euros d'amende. Le caractère complexe de la bande organisée fait de ces escroqueries des affaires de grande envergure, souvent bien au-delà du simple particulier qui va vous soutirer de l'argent en prétextant l'achat d'un objet. C'est justement l'ampleur du préjudice qui va pousser la justice à enquêter. Le préjudice subi par les particuliers sera tellement grand qu'il nécessitera l'intervention des institutions de l'État afin d'y mettre un terme.

L'escroquerie, même si elle n'est pas commise en bande organisée, est tout de même punie par la loi. L'article 313-1 du Code pénal la définit comme « *le fait de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge* ».

Afin d'être véritablement considérée comme telle par la justice, il faut que l'auteur de l'infraction ait eu l'intention de tromper sa victime en usant de l'un des trois moyens évoqués suivants :

- L'emploi de manœuvres frauduleuses doit être avéré : faux papiers, faux contrats...
- L'abus d'une qualité vraie : un médecin qui abuse de sa position pour soutirer de l'argent à un patient, par exemple.
- Le fait de soutirer quelque chose en usant d'un faux nom ou d'une fausse qualité : faux médecin, faux vendeur, faux avocat...

Un manque de plaintes

La honte de s'être fait piéger pousse souvent les proies à ne pas déposer plainte. Elles ont peur d'être jugées, d'être ridicules et préfèrent taire leur mésaventure. Or cela ne fait qu'accentuer le problème, ou tout du moins, cela lui permet de perdurer. « Il faut que chaque victime porte plainte en son nom propre. Plus il y aura de plaintes, plus les autorités auront conscience du problème et permettront de débloquer la machine ». Pour le psychologue Cyrille Le Jamtel, c'est une situation très délicate : *« C'est le même schéma que pour les victimes qui tentent de menacer leur escroc. La perspective d'une procédure longue, complexe, et surtout qui n'aboutira peut-être pas, c'est encore plus difficile à accepter. Le coût moral est énorme et cette longue poursuite empêche souvent les victimes d'aller de l'avant. Elles restent enfermées dans le schéma de l'arnaque. Elles sont donc psychologiquement toujours sous le coup de la colère ou de la honte »*. Christine tente malgré tout de persuader, de pousser, les victimes à porter plainte, *« car si ce n'est pas toujours primordial pour la victime, c'est indispensable pour, peut-être, dévoiler l'ampleur du problème et éviter à d'autres de se faire piéger. Quitte à en référer en plus haut lieu »*.

Christine et Marie ont été plusieurs fois confrontées à un problème plus délicat : le refus de plainte. « *Il arrive que lorsque les victimes arrivent au poste de police, elles soient face à un fonctionnaire qui refuse de prendre leur plainte. Le plus souvent, il tente de dissuader la victime, de lui dire que la plainte n'aboutira pas, que l'escroc est à l'étranger, que ça ne vaut pas la peine* », explique Christine. « Nous avons d'ailleurs appris récemment, que la chancellerie d'État, plus communément appelée ministère de la Justice, a diffusé aux commissariats et à la gendarmerie, une circulaire visant à ne plus prendre les plaintes des victimes des d'escroqueries sur Internet et de dissuader les plaignants de porter plainte ».

Une attitude décourageante pour les proies qui perdent tout de suite leurs espoirs et la confiance qu'ils plaçaient dans le système. « *Quand elles sont face à des refus de plaintes, j'essaie de faire en sorte que les victimes aillent directement porter plainte devant le procureur de la République. C'est une démarche qui est peu connue ; on a tendance à penser que l'on ne peut porter plainte que dans un commissariat mais on peut aussi le faire dans une gendarmerie ou, en l'occurrence, devant le procureur lui-même* ». La procédure est alors des plus simples puisqu'elle n'implique aucun contact physique, et donc, moins de risques de se sentir jugées.

En pratique

Porter plainte devant le procureur de la République

La démarche se fait au moyen d'une lettre, soit adressée par La Poste sous pli recommandé avec accusé de réception, soit déposée directement au service du procureur (parquet) du tribunal de grande instance le plus proche de votre domicile. Ces lettres étant particulièrement spécifiques, il est préférable, mais pas obligatoire,

de s'adresser à un avocat pour en rédiger le contenu et en assurer au mieux le suivi. Néanmoins, si vous souhaitez vous passer des services d'un défenseur, voici un modèle de lettre que vous pouvez utiliser pour adresser votre plainte.

Sur l'enveloppe, adressez votre courrier à :

Monsieur le procureur de la République du tribunal de grande instance de ..... (ville)
Palais de justice
(Adresse postale)

Pour la rédaction de la lettre :

À Monsieur le procureur de la République près le tribunal de grande instance de ..... (ville)

Je soussigné ..... (nom, prénoms, date et lieu de naissance, profession, domicile), (éventuellement : agissant en qualité de .....), ai l'honneur de vous exposer les faits suivants : ..... (faire un exposé succinct des faits).

C'est pourquoi j'ai l'honneur de déposer plainte entre vos mains pour ..... (nature du délit : abus de confiance, abus d'autorité, escroquerie, coups et blessures, etc.) contre M. ....., demeurant à ..... (ou : contre inconnu) (éventuellement : ainsi que pour complicité contre tout autre).

Je me tiens à votre disposition pour tout renseignement complémentaire qui serait nécessaire à vos services pour l'instruction de cette plainte et afin qu'il lui soit donnée la suite qu'il appartiendra.

Fait à ..... (ville), le ..... (date).

(Signature)

Des lois à l'épreuve des frontières

La question de l'internationalité des arnaques est certainement la plus délicate à aborder. Tout d'abord car la police nationale ou la gendarmerie, toutes deux capables de mener des enquêtes et d'empêcher un escroc de nuire, n'ont aucune habilitation pour exercer à l'étranger. En effet, leur juridiction s'arrête aux frontières terrestres et maritimes du territoire français. Il leur est donc juridiquement impossible de poursuivre un escroc dans d'autres pays et encore moins sur d'autres continents. Il existe néanmoins des conventions et des accords avec certains pays permettant la poursuite des enquêtes ou des recherches de criminels au-delà des frontières françaises. Souvent établis avec les pays de l'Union européenne (UE), ils permettent de poursuivre une enquête, malgré la barrière juridique de la frontière. « *On pourrait penser que les démarches sont facilitées entre pays de l'Union européenne. C'est le cas pour certains domaines, le droit commercial par exemple, mais en ce qui concerne la cybercriminalité, c'est bien plus difficile. Il n'existe pas de droit européen numérique, hormis pour la pédopornographie. Les législations sont tellement différentes d'un pays à l'autre qu'il est difficile de poursuivre au-delà des frontières françaises, en dehors des cas d'escroquerie en bande organisée* ».

La non-harmonisation des législations européennes entraîne plusieurs problèmes qui peuvent se rapporter à des arnaques. « *Certains produits pharmaceutiques par exemple, sont interdits en France parce que leurs effets ne sont pas prouvés, ou parce qu'ils sont jugés dangereux. Mais ils sont autorisés à la vente dans d'autres pays de l'UE. Faisons l'essai avec un produit bien connu de nos services et qui est interdit dans l'Hexagone. Je tape le nom de la molécule dans Google… et je clique sur le premier site. Voilà, il est basé aux Pays-Bas, mais tout est écrit en français. C'est clairement destiné aux consommateurs français. Le problème qui se pose, c'est qu'il est interdit d'en*

vendre en France, mais pas d'en acheter à l'étranger, puis de le faire importer et de le consommer en France ». Une pratique dangereuse au regard des autorités françaises mais pas seulement. Certains de ces sites peuvent cacher des arnaqueurs qui vous promettent l'envoi de la molécule miracle et encaissent votre argent avant de disparaître… sans jamais vous avoir envoyé votre médicament.

L'adjudant-chef Jean-François Garnier est un enquêteur spécialisé dans les nouvelles technologies. Gendarme basé en région parisienne, il a parfois été confronté à des enquêtes dépassant les frontières de la France. Et si les accords entre membres de l'Union européenne permettent parfois de faciliter les démarches, elles n'en restent pas moins complexes et exceptionnelles : « *Ce sont les polices locales qui reprennent le dossier. Les enquêteurs français ne sont pas autorisés à pénétrer dans le pays pour y mener leur enquête. Ils passent la main à leurs collègues locaux et nous ne reprenons le dossier que lorsque la personne est appréhendée et extradée. Mais nous gardons toujours un œil sur l'avancée de l'affaire par l'intermédiaire des gendarmes basés à l'ambassade ou au consulat français dans le pays concerné* ».

Quelle que soit l'infraction, quel que soit le crime ou le délit commis, la procédure en France ou à l'étranger est toujours la même. Un juge d'instruction doit émettre une commission rogatoire pour déléguer une partie de son autorité aux magistrats locaux. Une action simple, en théorie, mais qui nécessite des aménagements bien particuliers. En plus des nom et qualité du magistrat mandant et de l'autorité à laquelle la commission rogatoire est destinée, il doit y figurer l'identité complète de la personne recherchée.

Pour l'adjudant-chef Garnier, cette dernière obligation est généralement difficile à remplir lorsque l'on parle de cybercriminalité : « *Pour qu'une commission rogatoire soit valide, il faut l'identité de la personne : état civil donc, mais aussi son identité virtuelle ; son pseudo, s'il en a un. Dans le cadre de la cybercriminalité,*

il est très difficile de recueillir toutes ces informations virtuelles parce que les délinquants et criminels ont une maîtrise suffisamment bonne pour brouiller les pistes et nous donner des dizaines d'identités virtuelles à collecter. De plus, il est d'une facilité aberrante de se créer une fausse identité grâce à Internet. À partir d'une fausse identité, la procédure pour remonter à un véritable état civil est longue et complexe », donc onéreuse. Une complexité et un coût, qui, pour le gendarme, justifient que cette procédure soit rarement mise en œuvre. « *Ce genre de poursuites nécessite la mise en place de beaucoup de moyens. En face, le préjudice subi est individuellement important, mais socialement très faible, à tel point qu'il ne justifie pas la mise en place de tels moyens, policiers et judiciaires* ».

Des experts au service de la police

Pour contourner les barrières frontalières et techniques et confondre les arnaqueurs, la justice française fait parfois appel à des experts judiciaires qui ont pour domaine de compétence l'informatique. Ces derniers sont appelés en renfort pour traquer les cybercriminels. Sur son blog, l'expert qui a pour pseudo « Zythom » nous relate quelques-unes de ces affaires. Il nous rappelle cependant que l'expert judiciaire n'est pas un juriste. « C'est un technicien qui maîtrise son domaine d'expertise et est inscrit sur une liste gérée par une cour d'appel ou la Cour de cassation ». Lorsqu'il intervient sur une affaire, les magistrats et les officiers de police judiciaire ont déjà mené une enquête en amont. « Ils connaissent parfaitement les règles et les procédures internationales. Mon rôle est de les aider d'un point de vue technique, s'ils font appel à moi ».

Zythom a participé à plusieurs affaires. Il peut être contacté pour des arnaques classiques sur Internet : « *J'ai travaillé sur ce type d'affaire. Une histoire de voiture ancienne vendue un prix très bas sur Internet, avec un acompte permettant de réserver le véhicule.*

Bien entendu, le vendeur ne possédait pas de voiture ancienne et a disparu avec l'acompte ».

Au-delà de ces cyberarnaques assez classiques, l'expert travaille surtout sur des affaires de plus grande ampleur qui s'effectuent à un niveau international. Il nous raconte : « *Sur un dossier de recherches d'images pédopornographiques, j'ai pu mettre en évidence un réseau d'échanges d'images entre pédophiles. Il s'agissait d'un réseau international avec de nombreux pays en cause. J'ai donné des éléments de preuve à la police judiciaire, comme plusieurs experts judiciaires, en France et dans les pays concernés, et le réseau a fini par être démantelé. Il s'agit d'un travail collectif, coordonné par des magistrats aguerris aux procédures internationales* ».

Pour attraper les criminels, l'expert fournit un certain nombre d'éléments à la police : « *Il est tout à fait possible d'établir des preuves solides dans une arnaque sur Internet. Par exemple, il est possible de constater la présence d'un historique de navigation sur un ordinateur, la présence de courriers électroniques échangés entre tel et tel compte informatique. Il est possible de retrouver des éléments probants dans des fichiers effacés d'un disque dur, parfois même depuis longtemps* ».

Cependant, il attire notre attention sur le fait qu'en informatique il faut se méfier des raisonnements hâtifs. « *Par exemple : le compte informatique "Dupont" a été utilisé sur l'ordinateur appartenant à M. Dupont pour commettre une arnaque. Donc M. Dupont est coupable. Il est évident qu'un compte, même portant le nom du propriétaire de l'ordinateur, peut être utilisé par quelqu'un d'autre, son fils par exemple, voire par un logiciel malveillant piloté à distance. Il faut donc toujours être prudent et aborder une démarche scientifique rigoureuse, ce qui est le cas de tous les experts judiciaires expérimentés* ».

Cependant, l'identification des criminels peut dans certaines affaires s'avérer compliquée. L'expert nous explique « *Les méthodes utilisées par les cybercriminels sont les mêmes que*

celles utilisées par les honnêtes gens pour protéger leur intimité, les banques pour protéger leurs échanges, ou les lanceurs d'alertes pour rester anonymes : des techniques de chiffrages et des systèmes d'anonymisation ».

Il y a aussi des cas où retrouver leur trace relève de l'impossible. « *Je prends souvent l'analogie du réseau téléphonique : il peut être très difficile de retrouver un criminel qui passera un appel téléphonique d'une cabine publique. Souvenez-vous du corbeau dans l'affaire Grégory. Nous disposons des heures précises de ses appels, de l'enregistrement de sa voix, et pourtant personne ne l'a encore identifié, et cela depuis 1984* ».

Ceci, « *à condition d'avoir les moyens financiers de faire les enquêtes* », nuance l'expert.

À SAVOIR

Un criminel qui utilise Internet sur une longue période laisse des traces directes ou indirectes qui, à terme, ont de grandes chances de le faire repérer.

Au-delà de la complexité du système informatique, le manque de moyens financiers semble en effet être un frein majeur dans la capture des criminels. Zythom nous donne son avis : « *Il suffit souvent de mettre en œuvre les moyens nécessaires pour établir la vérité. Mais ces moyens ont un coût. De mon point de vue, les outils de lutte contre la cybercriminalité existent déjà et ne demandent qu'à être utilisés. Ce qui manque le plus, ce sont les moyens financiers : le budget de la justice française est l'un des plus bas d'Europe, les officiers de police judiciaires formés aux nouvelles technologies sont en nombre insuffisant et les experts judiciaires sont payés de leurs avances de frais avec plus d'une année de retard* ». L'expert conclut alors avec une certaine amertume : « *Mais c'est beaucoup moins cher et beaucoup plus voyant pour un gouvernement de faire voter une loi sécuritaire supplémentaire pour "défendre les victimes"* ».

Des procédures complexes

S'il est complexe de traquer les délinquants au sein même de l'Union européenne, on imagine aisément la difficulté accrue de les poursuivre au-delà des frontières de l'Union. Souvent situés dans des pays d'Afrique de l'Ouest, notamment en Côte d'Ivoire, les arnaqueurs restent la plupart du temps impunis.

S'il est difficile de connaître les raisons qui expliquent ce manque de poursuites, Christine Goubert, présidente de l'AVEN France, a sa propre hypothèse : « *Pour moi, il est certain que les systèmes de ces pays sont corrompus. À chaque fois que j'ai voulu faire avancer les choses, j'ai contacté les autorités sur place et envoyé des dossiers consistants avec les identités complètes des escrocs, leurs numéros d'adresse IP, les pseudonymes qu'ils utilisaient, les lieux d'où ils se connectaient… Et au final, il ne s'est rien passé. Donc tout ce que je peux imaginer, c'est que ces dossiers sont tombés entre les mains de personnes totalement désintéressées par le problème…* ».

Du côté des forces françaises de lutte contre le crime informatique, l'avis est plus nuancé. Pour l'adjudant-chef Jean-François Garnier, le problème vient plus d'un manque de moyens. « *Il est certain que les arnaques dans ces pays représentent une véritable économie parallèle. Même si le gouvernement local souhaite lutter contre, il se heurte à des freins logistiques énormes. Et il n'a pas forcément les moyens financiers de les dépasser* ».

Des freins logistiques également, tels que l'extrême mobilité des arnaqueurs qui changent d'adresse IP aussi facilement que de pseudonymes, ou la corruption au sein des différentes agences de transfert de fonds. Lors d'un transfert d'argent, le bénéficiaire doit fournir une pièce d'identité afin de retirer les fonds dans l'officine locale. Les escrocs présentent-ils alors de fausses pièces d'identité ? Ils n'ont même pas besoin d'aller jusque-là. « *Il suffit que le guichetier et quelques employés locaux soient dans*

la combine : quelques billets glissés de la main à la main permettent aux arnaqueurs de retirer, dans leur agence de prédilection, la somme extorquée sans jamais justifier de l'identité qu'il a donnée à sa victime », explique Christine Goubert.

Désintérêt ou impuissance des pouvoirs locaux, les associations aimeraient que les escrocs soient tout de même inquiétés et que les pouvoirs publics français tentent d'agir hors des frontières. « *C'est un problème de grande ampleur. Les sommes extorquées sont peut-être moindres en comparaison d'une escroquerie en bande organisée. Mais quand on soulève le coin du voile, on se rend compte que le problème est de taille et que les victimes sont loin d'être en tout petit nombre ! Pourquoi la justice ne tente pas de poursuivre les escrocs ? Pourquoi n'y a-t-il pas de travail avec Interpol, par exemple ? Quand nous avons un dossier, où que nous l'envoyions, il n'y a jamais de suite. Nous sommes désemparés face à tant de désintérêt. Si bien que je ne suis pas loin de penser qu'il y a des accords, des intérêts entre la France et la Côte d'Ivoire qui font que l'on ne cherche pas à remuer tout ça. Que l'on ne veuille pas faire frémir les relations politico-diplomatiques entre nos deux pays me semble la seule explication à une inaction pareille !* ».

Quelles que soient les hypothèses avancées par les associations pour expliquer l'inaction de polices étrangères et le peu de coopération entre la France et les pays étrangers, les associations restent toutefois perplexes quant au manque de poursuites en France contre les escrocs français. « Lors d'une arnaque au Mandat Cash, on se demande ce que font les forces de l'ordre. On a les numéros de portable des escrocs, on ne peut retirer ces mandats qu'en France, dans une poste, et on peut facilement savoir où ils ont été retirés. On peut aussi détenir l'adresse IP de l'arnaqueur et ses pseudonymes. On peut comprendre que les procédures soient compliquées à mener à l'étranger, mais en France, on devrait pouvoir mettre l'arsenal judiciaire au service des victimes ! Pourquoi n'y a-t-il jamais de poursuites ? C'est un mystère » s'insurge la présidente de l'AVEN France.

Du côté des gendarmes, et surtout des spécialistes de la cybercriminalité, l'explication est simple : tout comme lorsqu'il faut poursuivre un escroc à l'étranger, la procédure et les forces à mobiliser pour stopper l'escroc sont trop importantes au regard du préjudice subi. Nous y sommes. Car même une petite enquête va coûter à l'État au minimum 1 500 euros et sans être certain du résultat… alors pour des escroqueries de moins de 3 000 euros… Les escrocs ont encore de beaux jours devant eux.

Attention : croque-escrocs !

Malgré tout, pour certains, porter plainte et attendre la résolution de l'affaire ne suffit pas. La honte a fait place à la colère et quelques victimes ressentent le besoin d'agir. Décidées à pourrir la vie des arnaqueurs, ces proies, reconverties pour l'occasion en prédateurs, prennent à cœur de faire perdre un maximum de temps à ceux qui leur ont extorqué de l'argent.

Témoignage *Marie, après avoir été arnaquée, a décidé de rejoindre le cercle de ce que l'on nomme les « croque-escrocs ».*

J'ai tendance à dire que ça coûte moins cher qu'une psychanalyse. Mon rôle au sein de l'association, c'est d'aider les victimes. Mais parfois, pour ce faire, il faut contacter – ou se faire contacter – par un escroc, se faire passer pour une victime… Et ce genre de situation peut durer des semaines.

Une activité qui prend beaucoup de temps à ces prédateurs bénévoles… mais qui demande aussi beaucoup de discrétion. Car un seul faux pas peut éveiller la méfiance de l'escroc. Dans une telle situation, le piège peut se retourner. Il ne faut donc pas s'improviser croque-escrocs à la va-vite. Surtout que cette

activité n'a pas pour objectif initial de se venger froidement de celui qui vous aura extorqué des fonds.

L'intérêt de ces manœuvres est d'être en contact étroit avec les arnaqueurs pour rester au fait de leurs évolutions. « *Si on dit aux gens : "Méfiez-vous lorsque vous envoyez de l'argent par Western Union", et que finalement les escrocs se mettent à utiliser une autre entreprise de transfert de fonds, les scénarios auront beau être identiques, les internautes ne se méfieront pas. Pour connaître leurs évolutions, il faut que nous nous fondions dans la masse pour espérer prévenir les victimes potentielles des améliorations qu'ils vont apporter à leurs techniques* », détaille Christine. Une initiative qui permet parfois de prévoir les actions des escrocs et offre aux associations la possibilité de prévenir les victimes potentielles.

CONSEIL

Même si le scénario que l'on oppose à vos questions ne correspond pas mot pour mot aux mises en garde des associations, vous ne devez pas cesser de vous interroger.

C'est pourquoi certains croque-escrocs ont décidé de se fondre dans la masse. Facebook est en cela un formidable média. Il permet aux anciennes victimes reconverties en chasseurs d'escrocs de s'inventer une vie et d'infiltrer les réseaux de leurs cibles. Une méthode efficace pour rester à tout moment au fait des nouvelles idées : parfait pour adapter la prévention. Néanmoins, un peu de méfiance ne peut pas vous desservir.

Car une fois de plus, l'objectif initial n'est pas de se venger, c'est de faire avancer les choses. Pour Cyrille Le Jamtel, c'est ce qui importe le plus. « *Les victimes ont moins une volonté de vengeance que celle d'aider les autres* ». Surveiller les escrocs va parfois permettre de leur couper l'herbe sous le pied. Un désavantage pour les arnaqueurs, c'est sûr, mais surtout un moyen d'éviter à certains de se faire berner.

EN RÉSUMÉ

- En cas de refus de plainte, il est possible de vous adresser directement au procureur par le biais d'une lettre recommandée.
- Dans le domaine judiciaire, il existe des conventions et accords entre certains pays, dans l'Union européenne notamment. Dans ce cas, la police française transmet le dossier aux autorités étrangères, qui poursuivent l'enquête.
- Les coûts des procédures sont tels que les affaires menées en justice sont rares. Il s'agit principalement des escroqueries qui relèvent de bandes organisées ou lors d'un préjudice très élevé.

CHAPITRE 9
ARNAQUES, VICTIMES ET DROITS

DÉFINITIONS

- **Class action** : se traduit par « recours collectif » en français. C'est une action en justice qui permet à plusieurs personnes de poursuivre une seule personne pour recevoir des indemnités. Plusieurs plaintes individuelles à l'encontre d'une seule personne, souvent une entreprise ou une institution publique, sont alors réunies dans un procès unique.
- **Class action à la française** : reprend les principes de la class action à l'américaine, mais en limitant cette procédure aux litiges du quotidien, excluant les questions de santé publique et d'environnement. Le Sénat a voté le texte en septembre 2013.

Catherine Q.

Quand les arnaques fleurissent ici et là, il est un bon moyen de se prémunir du danger : s'informer. Certaines associations sont très actives sur ce créneau et tentent au maximum de limiter

les dégâts, le cas échéant, d'accompagner les victimes si elles souhaitent se tourner vers la justice.

Témoignage

Catherine Q. avait toujours rêvé d'un sac d'une grande marque. Un accessoire bien au-dessus de ses moyens. Sur un site de ventes entre particuliers, elle lit une annonce : une internaute propose de vendre son sac Dior pour 280 euros. Une chance, se dit Catherine qui saute sur l'occasion. Le contact avec la vendeuse se passe bien, elle reçoit les photos du sac et se prépare à l'acheter. Un sursaut de méfiance la pousse tout de même à contester le prix : elle demande à pouvoir payer la moitié tout de suite et la seconde moitié de la somme après réception du sac. Malgré quelques réticences, la vendeuse accepte. Un virement bancaire de 140 euros plus tard, l'acheteuse attend impatiemment son bien durant plusieurs jours, sans le voir arriver. Malgré ses nombreux appels à la vendeuse et tous ses messages, elle ne reçoit aucune réponse. Après quelques recherches sur Internet, elle repère le nom de son interlocutrice dans un listing... d'escrocs ! D'autres internautes avaient signalé les noms et adresses e-mail précédemment utilisés par son arnaqueuse. Catherine a fait le deuil de ses 140 euros et de son sac Dior. Elle n'a pour autant pas l'intention de la laisser s'en sortir aussi facilement. Mais face à la justice, la police ou encore les associations, la malheureuse acheteuse s'est sentie un peu perdue.

À qui s'adresser pour être efficace ? Un recours efficace contre un escroc, c'est surtout une mesure prise avant de se faire berner. S'il n'est pas toujours facile de reconnaître une arnaque, vous

pouvez toujours réduire les risques en vous méfiant de votre interlocuteur.

Prévenir, informer...

Avant de changer de nom, les escrocs usent leurs pseudonymes et leurs adresses e-mail jusqu'à « la corde ». Certains internautes, floués avant vous, n'auront pas hésité à inscrire le nom de leurs arnaqueurs sur le Web pour éviter à d'autres consommateurs de se faire avoir. Passer quelques minutes sur Internet à chercher le nom ou l'adresse e-mail de votre interlocuteur vous sera bien plus profitable au final que des centaines d'euros perdus dans une vente frauduleuse.

En pratique

Accéder au listing d'escrocs

En quelques clics, Marie, l'une des responsables de l'AVEN France, tente la manœuvre : « *Je vais sur un site de rencontres. Prenons cet homme ; moi je sais que c'est un escroc, mais partons du principe que c'est la première fois que je vois son profil. Je tape son nom et son prénom sur Google… voilà, le deuxième lien qui apparaît, c'est un listing d'escrocs. Je clique dessus… C'est effectivement un forum dédié aux arnaques où des utilisateurs dénoncent ce monsieur comme étant un arnaqueur. C'est une manœuvre très facile à faire. Mais personne n'y pense…* ».

Sa collègue, Christine, approuve : « *Les gens se renseignent généralement en bout de course, quand ils se sont déjà fait arnaquer. S'ils pensaient à se renseigner sur Internet avant de s'engager dans une relation, qu'elle soit commerciale ou sentimentale, on réduirait*

considérablement le nombre de victimes ». C'est d'ailleurs l'une des vocations des associations qui se sont créées autour des victimes.

La première association, créée en 2009 par plusieurs victimes, prévoyait une action de sensibilisation. Au-delà de l'aide apportée à celles et ceux qui sont déjà tombés dans le piège, elles souhaitent prévenir les proies potentielles et éveiller leur sensibilité au danger. Christine Goubert remarque que les efforts de l'association commencent à porter ses fruits. « *Nous constatons que les victimes sont de plus en plus rapidement averties par un proche ou par une connaissance à qui elle s'est confiée. Elles arrivent vers nous, de plus en plus, sans avoir envoyé de l'argent ou très peu et se renseignent* ». Ce bilan positif rend ainsi hommage au travail de prévention et d'information de l'AVEN.

Mais la présidente souhaite également mener quelques actions envers les pouvoirs publics français afin d'alerter le gouvernement et plus largement la classe politique sur la portée de ces arnaques en France. Grosse désillusion. La présidente de l'AVEN nous explique que les membres de l'association avaient écrit à Monsieur Hortefeux et Madame Alliot-Marie à l'époque où ils étaient au pouvoir. « *Nous n'avons eu droit qu'à des courriers types nous renvoyant vers les tribunaux de nos régions respectives. Nous avions également écrit à 106 députés et n'avons eu que 5 réponses* ». Aujourd'hui, les membres de l'association souhaiteraient être plus pris au sérieux et écoutés, « notamment par les ministres en charge de notre gouvernement » ajoute sa présidente. « *Nous avons remis un dossier complet à Monsieur Valls et à Madame Taubira, leur*

CONSEIL D'EXPERT

En France, la "class action" n'existe pas. Chacun doit intenter une action en justice. C'est la multiplication des plaintes qui mènera à des actions concrètes.

demandant d'en prendre connaissance ». L'association aspire ainsi à alerter les pouvoirs publics, notamment sur le rôle des sites hébergeant des escrocs, et leur demande de mettre en place des mesures. Mais l'association n'a pas eu de retour.

Se concentrant désormais essentiellement sur la prévention, les membres actifs veulent plus que tout « trouver les victimes pour les aider, les prévenir. On scanne Internet quasiment 24 h sur 24 pour mettre en garde les internautes ». Une action préventive qui n'occulte pas des actions juridiques. Malgré tout le travail des associations, il incombe aux seules victimes de porter plainte en leur nom.

Aux États-Unis, un groupe de personnes peut mener une action en justice au nom de leur problème commun. Cette procédure, appelée « recours collectif » ou « class action », est pour l'instant impossible en France, mais récemment, le ministre délégué chargé de l'Économie sociale et solidaire et de la Consommation, Benoît Hamon, a déposé un projet de loi visant à créer une « class action » à la française.

En pratique

Quand la class action est autorisée

Dans les pays où ce recours est autorisé, il s'effectue de la manière suivante : un groupe de personnes porte plainte en leur nom commun mais uniquement dans le cadre d'une association. C'est l'association qui va déposer un recours en justice et représenter l'ensemble de ses membres. Elle pourra donc déposer plainte avec constitution de partie civile et sera considérée comme une personne morale, c'est-à-dire équivalant à n'importe quel plaignant. Si l'association ne porte pas plainte, il faut que ce soit les individus lésés qui entament des procédures.

La présidente et fondatrice nous confie alors avoir fait appel à un juriste afin de constituer un dossier pour attaquer le partenaire français de Western Union pour défaut de conseil. « Cette entreprise dit avertir les gens mais après cinq ou six envois. En réalité, les agents demandent simplement si l'on connaît la personne à qui on transmet l'argent. Il suffit que la victime dise "oui", car elle pensera connaître son escroc, pour qu'il ne se passe rien d'autre. Il n'y a aucune prévention, aucun avertissement concernant les arnaques ». Cependant, le projet n'a pas abouti. Christine Goubert nous explique : « *Une fois encore, comme la " class action" n'est pas autorisée en France, l'avocat a, par conséquent, calculé ses honoraires par dossier* ». Or, l'association avait présenté plus de cent dossiers. « *La facture globale était exorbitante et nous avons renoncé* ». La présidente précise tout de même que 95 % de ces escroqueries se font *via* cette société de transfert d'espèces. Un problème que toutes les associations constatent sans pour autant avoir des moyens d'action, hormis la prévention. Mais les escroqueries sont tellement larges et diverses, qu'il est difficile de sensibiliser à toutes les formes qu'elles peuvent prendre.

... Et dénoncer

Quand la prévention ne suffit plus et que les victimes sont déjà tombées dans le piège des arnaqueurs, elles peuvent bien sûr porter plainte. C'est la multiplication des dossiers qui lui donnera tout son poids. Le plus éprouvant pour les victimes est la lenteur des procédures dans un cadre judiciaire ou personnel. Les cas les plus délicats concernent les arnaques à la petite annonce.

Témoignage

C'est ce qui est arrivé à Michel M., friand de nouvelles technologies. Il avait remarqué sur Internet une petite annonce : un iPad vendu 310 euros, soit la moitié

de sa valeur originale. Une affaire à ne pas louper, pensait-il avant de sauter sur l'occasion. Une affaire, certes, mais qui s'est avérée, au final, bien moins attrayante que prévu. Dès qu'il comprend l'arnaque, il se met en quête du vendeur. E-mails répétés sans réponse, coups de fil redirigés vers une boîte vocale... rien ne le décourage. Il décide donc de reprendre contact avec le vendeur en se faisant passer pour un nouveau client. La ruse aboutit : l'arnaqueur refait surface. Michel le menace. S'il ne lui rend pas tout de suite son argent, il contactera la police et déposera une plainte. L'escroc tente de l'en dissuader. De mensonge en mensonge, il invente des prétextes au retard de livraison : problèmes personnels qui l'ont forcé à différer l'envoi, problème avec La Poste, oubli... tout est bon pour faire durer l'affaire. Et l'acheteur commence à s'impatienter. Lettres recommandées avec accusés de réception menaçant d'une plainte, harcèlement par e-mail et par téléphone... il tente tout pour que son escroc, à bout, lui rende son argent. Mais rien n'y fait. Michel se résigne donc à déposer plainte au commissariat le plus proche et en informe immédiatement l'escroc. Il propose un ultime compromis : il retirera sa plainte s'il retrouve son argent. Silence de l'escroc. Après six mois de poursuite, le malheureux acheteur jette l'éponge.

Pour Cyrille, c'est une réaction logique et assez courante. « *C'est une véritable guerre psychologique à laquelle on se livre. C'est à celui qui craquera le premier. Un tel jeu du chat et de la souris, c'est absolument épuisant. Considérant le fait initial que les victimes ne parlent pas, ou très peu, de ce qu'elles ont vécu, elles sont seules face à leur arnaqueur. Le traquer, le harceler... Psychologiquement, c'est*

éprouvant. Pendant ce temps, on ne parvient pas à dépasser l'arnaque que l'on a vécue. Et après un moment, le coût nerveux et psychologique devient plus important que la perte financière. À ce moment-là, on laisse tomber, parce que, nerveusement, on n'en peut plus ». Une situation de plus en plus délicate pour les victimes. En plus de se sentir naïves d'être tombées dans une arnaque, elles se sentent faibles et dévalorisées de n'avoir pas pu récupérer leur argent par leurs propres moyens. Or, elles ne peuvent pas lutter contre les escrocs. Il ne faut surtout pas occulter le fait qu'il n'y a pas de dimension morale chez l'arnaqueur.

À SAVOIR

Cela ne pose pas de problèmes de conscience à l'escroc de soutirer illégalement de l'argent à ses victimes et de les laisser ensuite dans une situation financière, morale et parfois sentimentale déplorable.

Il ne sera donc pas gêné de recevoir des e-mails incendiaires, des menaces ou des plaintes. Il les ignorera avec la même facilité qu'il a eu à mettre de côté tout sentiment de culpabilité au moment de mener son escroquerie. Cette guerre des nerfs lui sera indifférente. Le seul problème que cela peut lui poser est un souci logistique : l'inonder d'appels et d'e-mails le gêne dans l'accomplissement de ses arnaques. Mais à l'usure, l'escroc sera gagnant. Il empoche l'argent que vous lui avez envoyé, il ne le rembourse pas, ignore les complaintes ou protestations sans aucun souci de conscience. Et en plus, au final, la victime – épuisée moralement – cesse de le harceler. Une démarche rarement menée à terme pour plusieurs raisons :

- La première raison, et certainement la plus difficile à surmonter : la honte de s'être fait piéger. Devoir exposer à tous la naïveté dont on a fait preuve face à un escroc a de quoi freiner les victimes qui n'osent pas se faire connaître auprès de la police.

- La seconde raison qui explique la faible proportion de plaintes comparativement au nombre de victimes déclarées sur les forums tient à un problème fréquemment évoqué par les associations : le refus de plainte.

Face à ces deux freins, très peu de victimes se font connaître et l'on ne peut pas avoir une idée précise de l'ampleur du problème. Si l'on ne connaît pas les victimes, les façons dont elles se sont fait piéger et par qui, comment les forces de l'ordre pourraient-elles endiguer le problème ? Comment les associations peuvent-elles leur venir en aide ?

Les missions des associations

L'activité principale des associations est l'aide aux victimes. Christine Goubert identifie deux missions principales :

- Épauler les arnaqués qui se font connaître, soit sur le forum de l'association, soit en contactant directement ses membres. « C'est notre vocation première. Quand une personne découvre l'arnaque dont elle a été victime, elle ne sait généralement pas quoi faire. Si elle témoigne sur notre forum ou nous contacte par e-mail, nous pouvons lui faire profiter de notre expérience pour l'orienter et lui expliquer les procédures à mener ».
- Aller au-devant des victimes pour leur ouvrir les yeux sur la situation. « *Il arrive que ce soit les proches qui nous contactent. Un parent ou un ami est embringué dans une arnaque et reste sourd à leurs avertissements. Dans ce cas, ils nous demandent de contacter la victime pour lui faire comprendre la réalité* ». Des situations très souvent mal acceptées par les arnaqués.

Aider les arnaqués qui se font connaître

Malgré la honte, il faut donc que les victimes se fassent connaître. Tout d'abord pour se faire aider. Les associations habituées à ce type de situations sauront vous conseiller, vous aiguiller et, le cas échéant, vous épauler pour porter plainte.

À SAVOIR

Le poids et les actions des associations seront différents selon le type d'arnaque dont vous aurez été victime.

Leur soutien est souvent indispensable pour permettre aux proies de surmonter leur honte et de faire face à la situation. Pour le psychologue Cyrille Le Jamtel, l'importance d'une association ne tient pas uniquement dans sa capacité à aider la victime à réagir. « *Pour une victime, se rapprocher d'une association, c'est se raccrocher à un groupe. Lorsqu'on est tombé dans le piège, on se sent honteux et on hésite à en parler à sa famille, à ses amis ou à la justice. On va donc s'isoler encore plus. Contacter une association, même sans y adhérer, c'est comprendre que l'on n'est pas seul à s'être fait manipuler. C'est un moindre mal, certes, mais cela permet aux victimes de se sentir écoutées et comprises sans se croire jugées* ».

Un rôle passif qui se ressent essentiellement dans les forums mis en place sur le Net par ces organismes. Ils regorgent de témoignages de victimes racontant leur histoire et les démarches qu'elles ont déjà entreprises pour tenter de retrouver leur argent. Des témoignages qui suscitent des dizaines de commentaires d'internautes avouant s'être fait berner par la même personne, ayant connu la même histoire ou ayant simplement tenté d'entreprendre les mêmes poursuites pour revoir leurs biens.

Un autre paramètre, apparu assez récemment, entre en jeu qui explique la relative facilité à s'exprimer sur un forum : le pseudonymat. Il peut être défini comme un semi-anonymat où les

données révélées paraîtraient contrôlées. « *Il y a sur un forum une liberté de parole absolue, explique Cyrille. Quel que soit son statut social, on est tous à égalité sur un forum. En plus, grâce au pseudonymat, tout le monde avance masqué. On peut choisir des éléments de sa vie et y apporter des retouches. Dans ces arrangements avec la vérité, on se crée une "vie bis" où l'on est qui l'on veut* ».

L'anonymat intervient quand la victime ne se fait pas connaître. Par définition, personne n'a d'information sur son histoire, son vécu et son ressenti de l'arnaque. Elle se fond dans la masse invisible et incontrôlable des proies. Tandis que la notion de pseudonymat induit que la victime se fait partiellement connaître. Là, intervient de nouveau le "moi idéal" que permet Internet : on va créer un personnage virtuel grâce à un pseudonyme. Et il sera plus facile de se confier par son intermédiaire. D'abord parce que l'on n'a pas d'interlocuteur physique en face de soi. Ensuite parce que ce personnage idéal sera distancié de la réelle personnalité de l'arnaqué.

Aller au-devant des arnaqués qui ne se reconnaissent pas victimes

Au-delà de l'infantilisation que provoque l'intervention d'une personne extérieure sur demande de la famille, certaines victimes vivent le travail des associations comme une intrusion dans leur vie privée. « *Il y a des gens qui refusent de voir la vérité. Assez peu, c'est vrai. Mais il arrive qu'elles soient agressives. Quand un inconnu vous téléphone pour vous dire "Vous êtes en relation avec Monsieur Machin, méfiez-vous, vous avez affaire à un escroc", on a tendance à se méfier. Même si on a eu des alertes auparavant, s'il nous est arrivé d'avoir des doutes, on a préféré les écarter pour se concentrer sur la belle histoire. Heureusement, la plupart des personnes que nous contactons finissent par être assez réceptives. Justement, ces alertes passées, même si l'on avait préféré les ignorer, finissent par remonter à la surface quand c'est un inconnu qui les réactive* ».

Pour en arriver à un tel retournement de situation, les membres d'associations doivent agir vite et sans aucune fausse note. Lorsqu'ils contactent les victimes et qu'elles refusent de croire dans la nature malsaine de leur relation, il faut démonter l'arnaque point par point. « *On va lui expliquer, lui raconter la façon dont elle s'est fait piéger* », explique Christine.

À SAVOIR

Toutes les arnaques ont la même trame. Avec le minimum d'éléments, les associations sont capables de dérouler avec la plus grande précision la façon dont les victimes ont été approchées, le type de messages que l'escroc leur a envoyé.

« *Quand un étranger vous déroule toute la relation que vous avez eue avec quelqu'un qu'il n'est pas censé connaître, ça a de quoi déboussoler. Mais heureusement, cela permet d'ouvrir les yeux à bon nombre de personnes* », se réjouit Marie, habituée aux scénarios d'arnaques à l'amour.

Parfois, les associations font face à des victimes trop manipulées pour accepter de se laisser ouvrir les yeux. Dans ce cas, Marie et Christine adoptent une méthode plus radicale : « *Nous contactons l'escroc et nous nous faisons passer pour la victime parfaite. En quelque sorte, nous rejouons l'histoire. L'escroc, qui ne se doute de rien, ne change pas son scénario. Par exemple : je me fais passer pour une femme sur un site de rencontres et je contacte le même homme que la victime. Il va m'envoyer les mêmes messages, les mêmes mails. Il va me parler de la même façon qu'à sa précédente victime. Et quand viendra le moment où il me demandera de l'argent, il va me donner les mêmes excuses. Avec ces preuves, je vais aller voir la victime et lui prouver qu'elle a été piégée. Ce n'est effectivement pas un moment agréable à passer, mais c'est un mal nécessaire. Il faut que ces arnaques s'arrêtent le plus vite possible !* ».

Certaines proies se retournent vers les forums ou les associations pour chercher du soutien et des conseils. « *Nous faisons vraiment tout pour aider les victimes. Il m'est même arrivé d'en recevoir chez moi pour leur expliquer en détail comment et pourquoi elles se sont fait avoir* », explique la présidente de l'AVEN. « *Mais il est déplorable qu'elles se tournent vers nous trop tard, c'est-à-dire après avoir été arnaquées. Et puis surtout, il y a ce que nous appelons les "serial victimes"* ». Ces victimes-ci sont les plus difficiles à sortir du système des arnaques. À chaque petit doute qu'elles émettront, l'arnaqueur va trouver une parade. Manipulés, les arnaqués vont avoir tendance à se contenter d'explications parfois bancales. Lorsque l'association essaiera de démonter l'arnaque dont elles sont victimes, « *elles trouveront toujours le moyen de dire : ça ne s'est pas exactement passé comme ça pour moi donc ce n'est pas forcément une arnaque* ». C'est généralement dans ces cas-là que la famille de la victime contacte l'association afin de limiter les dégâts. Malheureusement, la victime, qui se sera voilée la face tout au long de l'arnaque, aura déjà plusieurs fois envoyé de grosses sommes d'argent. Le système est bien rodé et les arnaqueurs n'ont aucun scrupule. Tous les moyens sont bons pour emmagasiner le plus d'argent possible. Y compris s'échanger les victimes les plus crédules.

Les internautes ne se rendent pas compte à quel point ces escrocs sont dénués de sens moral. Marie relate une histoire qu'elle a eu à traiter : « *Une personne s'est fait arnaquer par un Ivoirien. Il lui avait escroqué près de 5 000 euros. Quand elle avait enfin pu s'en sortir, elle a passé deux ou trois mois sans plus en entendre parler. Un jour, elle reçoit un mail d'un homme qui se prétend procureur à Abidjan. Il lui assure que la police a arrêté son arnaqueur et qu'elle sera remboursée de toutes les sommes qu'elle lui a versées. Le seul souci, c'est que pour conclure la procédure, il faut qu'elle fournisse certains documents justificatifs de cette arnaque, comme des copies des e-mails… et surtout, qu'elle verse de l'argent en guise de frais de dossier. Elle n'a même pas hésité à lui verser 700 à 800 euros par Western Union.*

C'était dérisoire comme somme comparé à ce qu'elle avait perdu. Et elle est tombée dans une nouvelle arnaque ». Le soulagement et la satisfaction de savoir un malfaiteur rattrapé par la justice de son pays suffisent souvent à combler le désir des victimes de se sentir « vengées ». Mais elles n'imaginent pas que cet argent a déjà été dépensé et qu'il est impossible d'indemniser, à hauteur de leurs pertes respectives, toutes les victimes d'un escroc. La perspective de revoir l'argent, que l'on venait à peine de se résigner à avoir perdu, suffit souvent à occulter toute tentative de méfiance. Surtout lorsque la personne qui vous contacte se dit procureur ou policier.

Aucune justification morale

Tous les spécialistes s'accordent à dire qu'il n'y a aucune dimension morale chez l'arnaqueur. On pourrait penser qu'une plus grande accessibilité aurait tendance à exciter les velléités d'escrocs en herbe. Ce n'est pas le cas. « *L'accessibilité ne légitime pas l'arnaque, explique Cyrille. Les escrocs pourraient se dire "puisque tout le monde y a accès, c'est moins grave"* ». Cela signifierait que l'arnaqueur chercherait à justifier ses actes pour soulager sa conscience. Or ils n'en ont pas besoin, pour la simple raison qu'ils estiment le plus souvent être dans leur bon droit. C'est une situation à laquelle les associations ont souvent été confrontées.

Les responsables de l'AVEN confient que « *lorsque nous entrons en contact avec des escrocs, nous tentons de leur expliquer la portée de leurs actes et le mal qu'ils font. Mais ça ne les touche pas. Ils nous rétorquent que ce n'est qu'un juste retour des choses. "La France s'est appropriée par la colonisation les ressources de pays d'Afrique. Maintenant, c'est à notre tour de vous prendre votre argent. C'est notre vengeance". Ça ne légitime en rien leurs arnaques mais ce sont leurs arguments. Ils s'arrogent le droit de nous voler comme une compensation* ».

Une justification qui explique leur dénuement total de jugement moral sur leurs propres actions. « *Parmi tous les arnaqueurs que nous avons trouvés et contactés, il y en a un seul dont je sais qu'il a arrêté, confie Marie. Je suis en relation avec lui, nous conversons parfois. Je lui ai expliqué à quel point ses arnaques étaient destructrices pour ses victimes...* ». Un retournement de situation bien rare malgré les efforts des associations.

Se tourner vers les professionnels

Déposer une plainte reste la seule chose à faire. Une démarche pas toujours évidente à mener. « Les victimes refusent assez souvent de porter plainte. Toujours parce qu'elles se sentent honteuses. Elles ont peur d'être jugées », analyse la présidente de l'AVEN France. La majorité des arnaqués ne se fait donc généralement pas connaître. Et quand les victimes arrivent à dépasser ce sentiment de honte, elles se sentent parfois un peu perdues dans la jungle judiciaire. Face aux services de police, à la gendarmerie ou directement à la justice, une victime se sent confuse et préfère renoncer plutôt que d'entamer des démarches qui lui semblent longues et psychologiquement éprouvantes. « *Une victime se sent seule face au système judiciaire. Elle n'envisage pas qu'il puisse y avoir beaucoup d'autres personnes dans son cas. Alors elle hésite à porter plainte, soit par honte, soit parce qu'elle ne sait pas à qui s'adresser* ».

Les associations telles que l'AVEN sont là pour épauler les victimes et les aider à trouver le bon interlocuteur. Pour Cyrille Le Jamtel, il est essentiel de dédramatiser sa propre histoire. Outre le fait de perdre de l'argent, ce qui est dangereux dans les arnaques, c'est l'état psychologique dans lequel se retrouvent les victimes après la révélation de l'escroquerie. « *En quelques minutes, on passe de l'hyper valorisation à une indifférence totale, voire parfois à un mépris de la part de l'escroc ou de la société. C'est*

une douche froide, une désillusion soudaine qui ramène très durement à la réalité ». On comprend alors à quel point les victimes peuvent se trouver dans la détresse. Pour pouvoir la surmonter, la victime doit déculpabiliser. Elle doit comprendre qu'elle n'est pas la seule à s'être fait avoir et surtout que ce n'est pas sa faute. Elle a eu affaire à un professionnel, qui passe ses journées à tenter de soutirer de l'argent à des internautes.

CONSEIL

Parce que vous serez toujours soumis à l'envie de tel ou tel produit, vous êtes une victime en puissance. La seule chose qui puisse vous protéger, c'est une méfiance accrue.

Être victime ne signifie pas être faible ou naïf. « *Il est tout naturel de songer avoir fait une bonne affaire ou vivre une belle histoire d'amour. L'important, après une arnaque, c'est de comprendre que l'on n'est pas seul dans ce cas et de se raccrocher à un groupe. Les associations aussi sont là pour ça !* », affirment en chœur responsables d'associations et psychologues.

Tout le monde est comme vous, tout le monde veut faire une bonne affaire en achetant ou en vendant sur Internet. Les cadeaux n'existent pas et les belles histoires sont très très rares.

EN RÉSUMÉ

- Avant de débuter une transaction sur Internet, passez quelques minutes sur les moteurs de recherche pour rechercher des informations sur votre vendeur. S'il n'est pas honnête, son nom d'emprunt ou son adresse e-mail seront recensés sur un listing d'escrocs.
- Si vous avez été victime d'une arnaque, n'hésitez pas à vous rapprocher d'une association et à porter plainte. En plus de permettre de répertorier et d'identifier précisément les modes opératoires des arnaqueurs, la multiplication des plaintes peut mener à des mesures concrètes des pouvoirs publics.
- Il est important de dépasser le sentiment de honte que l'on peut ressentir après avoir été victime d'un escroc. Acceptez l'aide des associations, elles sauront vous guider.

QUI CONTACTER ?

Vous avez repéré une arnaque sur le Web ? Vous êtes en contact avec quelqu'un et avez des doutes sur son intégrité ? Vous avez été victime d'une arnaque et ne savez pas qui contacter ? Cette rubrique est pour vous :

Vous avez repéré une arnaque, signalez-la auprès des services suivants :

- www.internet-signalement.gouv.fr pour toute arnaque ou contenu illicite.
- www.signal-spam.fr pour tout courriel frauduleux ou spam.
- www.econsumer.gov/francais pour toute arnaque transfrontalière.
- www.economie.gouv.fr/dgccrf pour tout site qui ne respecte pas les termes de la loi.

Vous avez des doutes, renseignez-vous auprès des services suivants :

- Info escroqueries : 08 11 02 02 17.
- Forum de l'AVEN : http://www.avenfrance.org/forum/
- Forum de l'association LesArnaques.com : http://forum.lesarnaques.com/
- Maisons de justice et du droit pour obtenir des conseils juridiques gratuitement : http://vosdroits.service-public.fr/F1847.xhtml

Vous avez été escroqué, prenez contact avec les structures suivantes :

- AVEN : http://www.avenfrance.org/
- Association LesArnaques.com : http://www.lesarnaques.com/
- Commissariat, gendarmerie ou bureau du procureur pour porter plainte sans délai.
- Site officiel de la Police nationale : http://www.police-nationale.interieur.gouv.fr
- Site officiel de la Gendarmerie nationale : http://www.defense.gouv.fr/gendarmerie
- Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) : http://www.prefecturedepolice.interieur.gouv.fr/Nous-connaitre/Services-et-missions/Missions-de-police/La-direction-regionale-de-la-police-judiciaire/La-brigade-d-enquetes-sur-les-fraudes-aux-technologies-de-l-information. Pour la région parisienne, vous pouvez déposer votre plainte directement auprès de la BEFTI : 122/126, rue du Château des Rentiers, 75013 Paris – Tél. : 01 55 75 26 19.
- Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) : http://www.interieur.gouv.fr/sections/contact/police/questionscybercriminalite. OCLTIC : 101, rue des Trois-Fontanot, 92000 Nanterre – Tél. : 01 49 27 49 27 ou www.internet-signalement.gouv.fr (portail officiel de signalement des contenus illicites de l'Internet) ou Info escroqueries – Tél. : 08 11 02 02 17.

REMERCIEMENTS

Ce livre a été réalisé grâce au concours et au soutien de tous ceux qui ont apporté des connaissances ou des conseils. Nous remercions donc toutes ces personnes qui ont bien voulu nous accorder un peu de leur temps pour témoigner ou nous diriger vers les interlocuteurs adéquats. Par ordre de rencontre, nous tenons à remercier :

- Olivier Zara[3], consultant en management et médias sociaux, qui m'a soufflé l'idée de ce guide.
- Christine Goubert, présidente de l'AVEN France, pour la rapidité avec laquelle elle s'est rendue disponible pour répondre à nos questions. Les informations qu'elle nous a fournies ont constitué une base très solide pour traiter du problème des arnaques sur Internet.
- Cyrille Le Jamtel, psychologue, pour sa disponibilité et son professionnalisme. En détaillant clairement quelques notions de psychologie, il nous a permis d'aborder l'état d'esprit des victimes et des escrocs.
- Jean-François Garnier, adjudant-chef, enquêteur spécialisé dans les nouvelles technologies au sein de la Gendarmerie nationale, pour son accueil et sa disponibilité pour nous expliquer son travail et éclaircir de nombreuses notions informatiques.
- Joël Guillon, président de l'association LesArnaques.com, de 2006 à 2013, pour ses précisions à propos de l'action menée par son association et des démarches à effectuer en cas de litige avec un professionnel.

3 *Réussir sa carrière grâce au Personal Branding*, Eyrolles, 2009.

- le service de communication de la Direction générale de la concurrence, de la consommation et de la répression des fraudes pour les informations concernant ses prérogatives et ses méthodes d'actions.
- tous les services qui nous ont permis de rencontrer ces personnes, notamment les services de presse et de communication des ministères de l'Intérieur et de la Défense.
- l'expert judiciaire « Zythom » qui a accepté de répondre à nos questions dans un délai de temps assez court.
- Charlotte Gorzala et Aurore Turpin sans qui ce guide ne serait pas.

INDEX