# Escroqueries

## Avec le Covid, les cyberarnaques se sont multipliées !

**Depuis le début de la pandémie, les escroqueries sur internet ont été nombreuses et souvent adaptées au contexte particulier que nous vivons. Voici les plus fréquentes et des conseils de prévention pour ne pas se faire avoir.**

Pendant que nous nous sommes confinés, les cyberarnaques, elles, se sont déconfinées! Les pirates du web ont profité de notre regain de temps passé devant l'écran, mais également de la fermeture de nombreux établissements et de l'incertitude liée à la crise du coronavirus pour adapter certaines de leurs attaques. «La plupart des cyberarnaques qui se sont développées durant la pandémie sont des phénomènes qui existaient déjà avant, mais qui ont été adaptées au goût du jour, confirme le criminologue neuchâtelois Olivier Beaudet-Labrecque, de l'Institut de lutte contre la criminalité économique. Celui-ci a participé à la mise en ligne du site coronafraud.ch, destiné à analyser à des fins scientifiques la délinquance économique en temps de crise, qui a «tendance à se multiplier». Pour preuve, à la Fédération romande des consommateurs, les ventes par internet se sont placées dans le trio de tête des cas les plus souvent dénoncés en 2020. «L'usurpation d'identité est un problème récurrent, que la pandémie n'a fait que renforcer», note Jean Tschopp, son responsable Conseil et juriste.

Grâce à l'aide de spécialistes et des diverses polices cantonales — qui conseillent toutes de les contacter si on a des questions, des suspicions ou que l'on a été victime —, *générations* a listé les 10 cyberarnaques actuellement les plus fréquentes, arnaques dont les fraudeurs peinent souvent à être confondus.

FRÉDÉRIC REIN >>>

Prudence, avec la pandémie, les arnaqueurs ont mis le turbo.

iStock

# COMMENT SE PRÉMUNIR DES CYBERARNAQUES

**Les escrocs ont leur terrain de chasse préféré. Les sites de rencontres bien sûr, les fausses annonces, mais aussi la crypto-monnaie ou l'usurpation d'identité. Soyez particulièrement prudents.**

## L'ESCROQUERIE AUX SENTIMENTS

Elles rêvaient du grand amour. De ces moments de complicité et de partage sans contrepartie. Seulement voilà, l'histoire à l'eau de rose a vite tourné en eau de boudin pour ces victimes d'escroquerie aux sentiments, les princesses et princes finissant par montrer un visage peu charmant *(lire encadré)*! Après un premier rendez-vous très prometteur sur un site de rencontres, elles ont été confrontées et ont cédé face à des demandes d'argent dont les motifs étaient évidemment fallacieux (frais d'héritage, soins médicaux…). «En Valais, nous avons enregistré les plaintes de trois personnes qui ont récemment perdu des sommes de 90 000 et 118 000 et 400 000 francs!», atteste Christian Zuber, de l'Unité Communication et Prévention de la Police cantonale valaisanne. «Cette fraude a connu une recrudescence en raison du télétravail, de la fermeture des lieux de rencontres et de la diminution drastique de la vie sociale», constate Olivier Beaudet-Labrecque.

**Conseils de prévention** Garder à l'esprit que, sur internet, tout peut être falsifié (photos, profils…); favoriser une rencontre physique ou une visioconférence; se méfier si votre interlocuteur parle du grand amour avant la première rencontre; ne pas accepter les demandes d'ajout d'amis sur les réseaux sociaux de personnes que vous ne connaissez pas dans la vraie vie; couper net tout contact si on vous demande de l'argent.

TÉMOIGNAGE

## «C'était valorisant de voir cette jeune et belle fille s'intéresser à moi»

**Pierre*, victime d'une escroquerie aux sentiments**

Même si les faits datent d'il y a 4 ans, Pierre a encore la gorge serrée au moment d'en parler. «Je sortais d'un divorce et j'ai commencé à fréquenter un site de rencontres, avoue, sous couvert d'anonymat, ce sexagénaire romand. Léa était jeune, jolie et attentionnée, je me suis senti valorisé. Je suis rentré dans sa vie au fil des photos qu'elle m'envoyait régulièrement et des discussions — d'abord amicales, puis amoureuses — que nous avions. Nous aurions dû nous voir à plusieurs reprises, mais elle a toujours trouvé des excuses pour annuler à la dernière minute. Un jour, elle m'a parlé de ses difficultés financières. Je l'ai naturellement aidée.» Pierre lui versera une bonne vingtaine de milliers de francs. «Quand j'y repense, l'arnaque semble évidente, mais j'avais tellement envie d'y croire», avoue-t-il. Les deux «amoureux» vont jusqu'à échanger des vidéos érotiques. Vient alors le jour où elle commence à le faire chanter. «Elle m'a demandé encore plus d'argent, menaçant de dévoiler les films à ma famille», se souvient-il. A force de messages où il lui annonce qu'il va signaler son cas à la police, il finit par arriver à mettre un terme à cette «relation» sans que son entourage n'en ait vent. Mais, aujourd'hui, Pierre peine encore à digérer sa mésaventure, qui restera encore longtemps un crève-cœur!

*NOM CONNU DE LA RÉDACTION

## LE CHANTAGE AU SEXE

Un jour, on reçoit un e-mail dans lequel des escrocs prétendent avoir pris le contrôle de notre webcam et de notre ordinateur. Ils nous menacent de publier les images et les vidéos à caractère sexuel qui s'y trouvent si on ne verse pas une rançon — qui doit souvent être payée en bitcoins (monnaie virtuelle). Appelée spam ou fake sextorsion, cette variante de la «sextorsion», terme anglais qui vient de la contraction des mots sex et extorsion, est très en vogue actuellement. Les arnaqueurs envoient leurs courriels en masse et espèrent que des destinataires, en particulier ceux ayant récemment visité des sites pour adultes, se sentiront visés et accepteront de payer, même si les maîtres chanteurs n'ont aucune preuve en leur possession.
**Conseils de prévention** Ne pas ouvrir ce type d'e-mails et les supprimer immédiatement; ne jamais payer; modifier et/ou changer sans délai vos mots de passe en les complexifiant; en cas de doute, faire vérifier votre ordinateur par un expert.

## LES FAUX INVESTISSEMENTS

La crypto-monnaie (argent numérique) a le vent en poupe, comme le prouve le cours record atteint par le bitcoin en avril. «Elle attire donc aussi les escrocs, remarque Christian Zuber. «Ces derniers temps, de nombreux particuliers ont perdu le capital qu'ils avaient cru investir dans la crypto-monnaie — mais aussi sur le marché Forex, les matières premières, etc.» Tout commence par une prise de contact par courriel ou par le biais des réseaux sociaux. Les victimes sont alors dirigées vers un pseudo-courtier qui finit par leur demander le virement d'un dépôt initial. Au début, le lésé reçoit parfois même un peu d'argent, afin de l'inciter à augmenter la mise. Il peut aussi être amené à installer un logiciel qui permet à son interlocuteur de prendre le contrôle de son ordinateur. Enfin, le jour où il veut récupérer son argent, la plateforme n'est plus accessible et le lien définitivement rompu. La RTS a récemment relaté le cas d'un Vaudois de 82 ans qui a cliqué sur le lien d'un article internet présentant un système de trading. Il s'est inscrit sur la plateforme chypriote ROinvesting et a investi à perte 5500 euros. De nombreux seniors en ont fait de même, se laissant notamment convaincre par de fausses interviews de Roger Federer ou de Darius Rochebin.
**Conseils de prévention** Vérifier si le fournisseur a une licence de l'Autorité fédérale des marchés financiers FINMA et ne pas investir si ce n'est pas le cas; favoriser les plateformes reconnues en Suisse, comme Swissquote; ne jamais accorder l'accès à votre ordinateur à un inconnu; ne jamais livrer les codes d'accès de votre session e-banking ou de votre carte de crédit.

## LE FAUX E-MAIL

Il y a peu, Francis a reçu un e-mail de l'Office fédéral de la santé publique (OFSP). L'aspect officiel du courriel lié au fait que l'on soit en période de pandémie l'a incité à ouvrir le fichier joint, ce qui a engendré l'installation sur son ordinateur d'un logiciel malveillant, cette correspondance s'avérant en effet être fausse. Voici un exemple typique de phishing (hameçonnage, en français), à savoir une technique couramment utilisée par les fraudeurs pour obtenir des renseignements personnels dans le but d'usurper une identité.
**Conseils de prévention** Etre attentif et critique face aux e-mails que l'on reçoit; vérifier l'adresse de messagerie de l'expéditeur, surtout la partie du nom de domaine qui apparaît après le «@»; prêter attention aux fautes d'orthographe et de français; ignorer et supprimer les e-mails suspects; ne pas ouvrir les pièces jointes et ne pas cliquer sur les liens; en cas de suspicion de phishing, changer immédiatement les mots de passe de tous vos comptes (bancaires, réseaux sociaux, e-mail, etc.).

## LES FAUSSES ANNONCES

Voici un classique de la cyberarnaque: le lésé souhaite acheter un objet sur un site de petites annonces ou sur un réseau social. Il contacte le vendeur, qui lui transmet des coordonnées bancaires ou Twint pour faire le versement. Le lésé effectue le paiement, mais ne reçoit jamais l'objet qu'il a payé. Récemment, de nombreux cas ont concerné des animaux, dont l'adoption a été très en vogue en période de confinement. Là, le vendeur se trouve généralement à l'étranger et vous propose de mandater une société de transport pour assurer son envoi. Cette dernière vous contacte, vous demande de payer des frais imprévus pour diverses raisons (frais de douane, cage non adaptée, etc.), mais l'animal n'arrivera jamais.
**Conseils de prévention** Privilégier une rencontre physique avec votre interlocuteur; se rappeler que La Poste ou une société de transport, telle que DHL ou UPS, n'envoie pas d'animaux; ne jamais effectuer un versement bancaire à une personne dont l'identité ne semble pas correspondre à celle du vendeur; en cas de doute, appeler le vendeur sans passer par une application du type WhatsApp (utiliser le réseau téléphonique); ne jamais sortir de la plateforme de vente lors des négociations.

> *«La plupart des cyberarnaques ont été adaptées au goût du jour»*
>
> OLIVIER BEAUDET, CRIMINOLOGUE

## LA MULE FINANCIÈRE

Pourquoi ne pas compléter ses revenus, à l'instar de sa rente AVS, grâce à «un temps partiel au salaire confortable que l'on peut réaliser depuis son domicile»? La proposition, présente sur les réseaux sociaux ou sur des sites de petites annonces, est tentante, mais peut s'avérer périlleuse, car il s'agit en réalité de transférer de l'argent sale, une activité illégale. Rapidement, l'employeur demande au lésé de mettre à disposition son compte bancaire pour y recevoir des versements de ses clients, puis d'envoyer l'argent par virement bancaire ou >>>

iStock, DR

via des agences de transfert de fonds (Western Union, MoneyGram, etc.) à l'un de ses partenaires professionnels, devenant un acteur de ce système de blanchiment d'argent. A cette occasion, il se peut aussi que le lésé soit incité à ouvrir de nouveaux comptes bancaires pour cette activité, à envoyer les cartes de crédit liées à une tierce personne et à transmettre ses identifiants e-banking.
**Conseils de prévention** Ne jamais mettre à disposition son compte bancaire pour faire transiter de l'argent.

> « La crypto-monnaie attire aussi les escrocs »
>
> CHRISTIAN ZUBER, POL CANT VALAIS

## LES FAUX MAGASINS DE PRODUITS MÉDICAUX

Comme les masques de protection faisaient défaut au début de la pandémie, Lucien et Raymonde, la soixantaine, ont décidé d'en commander en ligne. Malgré leur paiement, ils n'ont jamais reçu la marchandise. Heureusement pour eux, ils ne se sont pas fait voler leurs données bancaires, ce qui arrive parfois dans ce type d'arnaque. «Ces faux sites marchands, qui proposent des rabais et de bonnes affaires, se répandent de plus en plus en Suisse, constate Olivier Beaudet-Labrecque. S'ils existaient bien avant la pandémie, cette dernière a toutefois engendré une multiplication de ceux spécialisés dans la protection contre le coronavirus.»
**Conseils de prévention** Etre attentif et critique vis-à-vis des offres sur internet; avant de commander, se renseigner sur le fournisseur; s'il n'y a pas de conditions générales, de conditions de paiement ou de mentions de contact, c'est douteux; se connecter aussi aux sites officiels des boutiques en ligne correspondant, car, bien souvent, ceux-ci publient des avertissements; si la description du produit mentionne des termes comme «semblable à» ou «dans le style de», ne pas acheter; ne pas oublier de comparer les prix.

## LA FAUSSE ASSISTANCE MICROSOFT

Serge a d'abord reçu un coup de téléphone. A l'autre bout du fil, une personne lui explique travailler pour Microsoft et lui signale des problèmes sur son ordinateur. Son interlocuteur lui demande d'installer un logiciel de prise de contrôle à distance (TeamViewer, AnyDesk, par exemple), puis de se connecter à son compte e-banking pour soi-disant acheter une mise à jour — mais cela aurait aussi pu être pour acheter un antivirus ou simuler un paiement pour appâter les hackers qui l'auraient piraté. C'est à ce moment-là que des virements depuis le compte e-banking de Serge ont été effectués, le dépouillant de quelques milliers de francs!
**Conseils de prévention** Ne jamais donner le contrôle à distance de votre ordinateur et ne pas installer un logiciel à la demande de quelqu'un par téléphone, d'autant plus qu'aucun service d'assistance ne vous contactera par téléphone sans que vous l'ayez préalablement demandé; ne jamais se connecter au système e-banking à la demande d'un tiers inconnu.

## ARNAQUE À L'AVANCE DE FRAIS

Vous possédez un objet qui vous encombre et dont vous souhaitez vous débarrasser? Pourquoi ne pas passer une petite annonce sur internet? Attention toutefois si l'intéressé vous annonce avoir mandaté une société qui viendra le chercher à votre domicile et vous remettra la somme d'argent fixée. Lors de cette arnaque, vous recevez ensuite un e-mail de cette société (DHL par exemple, en réalité usurpée) vous demandant de payer des frais pour débloquer la vente — généralement en achetant des cartes cadeaux de type Google Play, iTunes ou des Paysafecard, puis en transmettant au fraudeur le codes PIN qui y figure et permet de les utiliser. «On a constaté une augmentation des demandes de sommes supposées couvrir des amendes liées au coronavirus», souligne Olivier Beaudet-Labrecque.
**Conseils de prévention** Ne jamais payer des frais pour un objet dont on est le vendeur; privilégier une rencontre physique avec votre interlocuteur; il faut savoir qu'aucune entreprise légitime ne demande de payer des frais en achetant des cartes cadeaux; ne pas valider un paiement par Twint dont on ne connaît pas le destinataire.

## ARNAQUE AUX DONS ET CAGNOTTES

Madeleine a été profondément touchée par les difficultés rencontrées par le monde du spectacle. Cette amatrice de culture a donc décidé de répondre à un appel aux dons reçu par e-mail. Son argent n'a malheureusement profité qu'à l'auteur du courriel. «Cette arnaque surfe sur l'élan de générosité des particuliers, explique Olivier Beaudet-Labrecque. Les escrocs n'hésitent d'ailleurs pas à investir les plateformes de financement participatif.»
**Conseils de prévention** S'assurer de la réalité de la collecte en se renseignant auprès de l'organisme qui est mentionné et se méfier des appels aux dons pour le personnel médical.

> « L'usurpation d'identité est un problème récurrent »
>
> JEAN TSCHOPP, JURISTE FRC

DR