HORS-SÉRIE

LA LIBERTÉ Magazine

PRINTEMPS 2023

CYBERCRIMINALITÉ

POUR E-VOIR PLUS CLAIR

Décryptage d'un phénomène qui balaye la vie d'individus, de familles et d'entreprises. Des experts en cybercriminalité nous aident à mieux comprendre ses rouages et ses répercussions.

Message de la rédactrice en chef

Sophie Gaulin

sgaulin@la-liberte.mb.ca

Si l'avènement d'Internet a facilité nos vies dans bien des domaines, force est de constater qu'il a aussi largement profité aux bandits 2.0.

Des pans entiers de nos vies, nos informations personnelles et même les données les plus sensibles de nos entreprises sont stockés sur la toile, fournissant alors aux malfaiteurs un immense terrain de jeu pour opérer.

Ces cybercriminels ont en effet accès à une multitude d'informations pour nous faire chanter et faire trembler nos dirigeants d'entreprises, nos organisations, et même nos gouvernements.

Si le phénomène du cybercrime est de plus en plus répandu et balaye la vie de personnes, de familles et d'entreprises, les Canadiens et Canadiennes se sentent souvent impuissants face au crime sans visage.

Pourtant nous avons encore de la difficulté à agir en amont des attaques, et parfois même de la réticence à nous protéger, que ce soit en raison d'un déni de réalité ou d'une dette technologique que nous estimons trop lourde.

Pourtant, le constat est sans appel : la cybercriminalité est là pour rester. Nous n'avons donc pas d'autre choix que de nous informer, nous former, communiquer en toute solidarité, dénoncer, légiférer et nous protéger.

Nous avons collectivement ces responsabilités face à la montée de cette criminalité.

Ce magazine a pour objectif de jeter les bases pour mieux comprendre ce phénomène et s'en prémunir. Il aborde donc l'importance d'adopter une bonne hygiène numérique, de veiller aux dangers qui guettent nos entreprises, nos institutions, de comprendre les risques de l'inaction mais aussi d'encourager les lecteurs et les lectrices à veiller aux membres les plus vulnérables de notre société, comme les personnes en prise ou en perte d'autonomie.

Et c'est dans cet esprit de solidarité et de mise en commun de nos expertises que ***La Liberté*** a débauché le temps de l'élaboration de ce magazine, Fyscillia Ream et Akim Laniel-Lanani de la Chaire de recherche en prévention de la cybercriminalité de l'Université de Montréal, également cofondateurs de la Clinique de cyber-criminologie ainsi que Bertrand Milot, conférencier en cyberintelligence et président de Bradley & Rollins, une entreprise experte dans le domaine. Merci à chacun et chacune d'avoir généreusement donné votre temps et votre expertise pour le bénéfice de nos lecteurs et lectrices.

Notre collaboration illustre parfaitement la volonté et la nécessité de créer une lutte solidaire contre les cybercriminels. Ensemble, assurons-nous de partager et d'adopter les pratiques numériques les plus responsables et sécuritaires afin de contrer ce fléau.

L'équipe

Rédactrice en chef :
Sophie Gaulin

Administratrice :
Lysiane Romain

Comité de direction scientifique :
Akim Laniel-Lanani
Bertrand Milot
Fyscillia Ream

Coordonnatrices :
Meggan Bault
Camille Harper
Ophélie Doireau
Fanny Demeusy

Journalistes :
Hugo Beaucamp
Jean-Baptiste Gauthier
Camille Harper
Mehdi Mehenni
Morgane Lemée

Graphistes :
Tarik Oumokrane
Abdelhamid Souissi
Yahia Lahrech
Popy Bâcle

Illustrateurs :
Tanguy Maerten-RIENNEPRESS
Yahia Lahrech

Photographe :
Marta Guerrero

Merci à Jose Maria Lopez Bueno et Hernán Popper de nous avoir inspirés ce magazine et de nous avoir aidés à le démarrer.

La Liberté Magazine sur la *cybercriminalité* a été rendu possible grâce à :

THE MANITOBA LAW FOUNDATION

Société de la francophonie manitobaine

Québec

Et merci à nos partenaires :

AJEF Manitoba inc.

Chambre de commerce francophone de Saint-Boniface

Adresse de la rédaction : 201-123 rue Marion, Winnipeg, MB, R2H 0T3 • Téléphone : 204-237-4823 • www.la-liberte.ca
ISSN 0845-0455

Coût à l'unité du magazine : 5,50 $ + taxes

Message du comité de direction scientifique

Bertrand Milot
Président - directeur général de Cybersecurity Bradley & Rollins et conférencier en cyberintelligence

Fyscillia Ream
Coordonnatrice scientifique Chaire de recherche en prévention de la cybercriminalité et cofondatrice de la Clinique de cyber-criminologie

Akim Laniel-Lanani
Cofondateur et directeur de la Clinique de cyber-criminologie de l'Université de Montréal

Il n'y a pas une semaine ou même une journée sans que la presse ne nous annonce une cyberattaque, ou l'arrêt de fonctionnement d'une organisation, d'un service en ligne ou d'un site internet.

Mais qui, comment et pourquoi? « Ils », « les pirates », « les cybercriminels » ne nous laissent qu'une représentation floue et abstraite d'une machine malicieuse multi-facettes, bien huilée.

Dans ce magazine, on tente de vous faire découvrir ce qui se trouve sous les capots de ces organisations criminelles. Leur créativité n'a d'égal que leur appât du gain sans limite.

Comme Sun Tzu, l'un des plus anciens stratèges militaires, l'a si bien dit « Celui qui excelle à vaincre ses ennemis triomphe avant que les menaces de ceux-ci ne se concrétisent ». Alors nous vous invitons au fil de ces pages à développer votre meilleure défense, qui passe par la connaissance du monde des cybercriminels. Et devenir ainsi de très mauvaises victimes, voire même des cibles inintéressantes. Voici notre pari.

Je souhaite tout d'abord remercier l'équipe de ***La Liberté*** pour l'invitation à collaborer sur ce numéro spécial ainsi que leur volonté d'accroître la visibilité et l'importance des enjeux de cybersécurité et de cybercriminalité.

Les nouvelles technologies sont partie intégrante de nos vies et il est important que nous puissions tous en bénéficier et les intégrer dans notre quotidien en toute sécurité. Pour cela, rien de tel que d'adopter une bonne cyberhygiène que ce soit dans notre vie personnelle ou professionnelle, de continuer à s'éduquer sur le sujet et à échanger avec ses proches.

Mon souhait est qu'à la fin de la lecture de ce numéro, la cybersécurité devienne un automatisme pour les lecteurs, un peu comme mettre sa ceinture de sécurité lorsque l'on monte dans une voiture.

En tant que directeur d'une organisation qui vient en aide aux victimes de cybercriminalité, j'ai accepté de collaborer à ce magazine car je crois fermement en l'importance de sensibiliser et d'informer le public sur les enjeux de la cybercriminalité et les bonnes pratiques de cyberhygiène.

Si nous souhaitons renverser l'augmentation de la cybercriminalité, nous devons travailler ensemble et cela commence par une prise de conscience collective. En partageant nos connaissances sur les bonnes pratiques en matière de cybersécurité, nous pouvons contribuer à créer un environnement en ligne plus sûr pour tous et toutes.

J'espère que cette édition hors-série de *La Liberté* encouragera les lecteurs à adopter des pratiques de cyberhygiène saines et sécuritaires et à sensibiliser leur entourage. En prenant des mesures simples pour se protéger en ligne, nous pouvons y arriver.

Messages de nos partenaires

Angela Cassie
Présidente de la Société de la francophonie manitobaine

La Société de la francophonie manitobaine est fière d'être partenaire de ce magazine dédié à la cybersécurité.

Nous profitons de l'occasion pour vous présenter Infovictimes, le nouveau portail où vous pourrez trouver les services offerts en français aux victimes d'actes criminels ici au Manitoba. Nous tenons à remercier nos partenaires dans ce projet, Pluri-elles, l'Association des juristes d'expression française du Manitoba et Infojustice Manitoba.

Nous tenons également à remercier ***La Liberté*** pour avoir mis en lumière le sujet important et évolutif de la cybersécurité.

Tarik Daoudi
Directeur général de l'Association des juristes d'expression française du Manitoba

La cybersécurité présente une multitude de défis qui touchent tout le monde. Être bien préparé face à ces défis revient à essayer d'atteindre une cible mouvante qui évolue sans cesse avec les progrès constants de la technologie - qui eux-mêmes ne font que s'accélérer. Il est donc de notre devoir commun et permanent de nous entraider, jeunes et moins jeunes, particuliers et entreprises, pour nous assurer que nous restons bien informés et vigilants.

Sylvie Laurencelle
Présidente de la Chambre de commerce francophone de Saint-Boniface

Aujourd'hui, la cybersécurité est l'affaire de toutes les entreprises, petites ou grandes. Listes de fournisseurs, d'abonnés, données financières, ou encore données personnelles sur les employés, ce sont autant de cibles d'intérêt pour les cybercriminels. Et être victime d'une attaque cybercriminelle peut entraîner des dommages importants et coûteux aux entreprises.

La Chambre de commerce félicite *La Liberté*, d'avoir déployé tant de ses ressources pour publier ce magazine hors-série sur la cybercriminalité, afin de fournir des ressources fiables qui aideront nos entrepreneurs à agir en amont et se munir de pratiques cybersécuritaires.

Hernán Popper
Président - directeur général de Popp3r Cybersecurity

C'est un plaisir pour moi de collaborer avec *La Liberté* sur ce sujet crucial. La cybersécurité est un domaine multidimensionnel, complexe et en constante évolution, qui ne peut être abordé qu'en favorisant la collaboration entre l'industrie, le monde universitaire et le gouvernement.

Alors que beaucoup pensent que la cybersécurité est un problème informatique, nous nous concentrons sur l'aspect humain. Le plus grand défi est de savoir comment gérer le risque humain, car les personnes sont impliquées dans plus de 80 % de toutes les violations cybercriminelles. Notre objectif est de gérer et de mesurer efficacement le risque humain en modifiant le comportement des personnes et en instaurant une solide culture de la sécurité.

Sommaire

Tout au long du magazine, le genre masculin a été utilisé pour faciliter la lecture et n'a aucune intention discriminatoire. C'est le cas du terme cybercriminel, par exemple.

section 1

Les rouages de la cybercriminalité

Internet : un grand terrain de jeu pour les criminels

La notion de cybercriminalité est particulièrement vaste. Dans une volonté d'en simplifier la définition, Hernán Popper, dirigeant d'une entreprise manitobaine en cybersécurité, explique que « les crimes sont aussi vieux que l'humanité… À la naissance d'Internet, il était inévitable que les criminels commencent à se servir de ce grand terrain de jeu. »

Écrit par **Hugo BEAUCAMP et Jean-Baptiste GAUTHIER**

« De nos jours, lorsque l'on parle de cybercrimes, la référence à Internet est inévitable. » Hernán Popper nuance tout de même ses propos. « Les cybercrimes existaient avant l'invention d'Internet, mais ils étaient différents de ceux que l'on connaît aujourd'hui. »


Hernán Popper

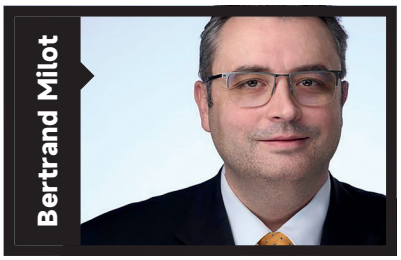
Pour cause, si l'on se fie à la définition donnée par la Gendarmerie royale du Canada (GRC), qui reconnaît comme cybercrime deux catégories : *les infractions prenant pour cible la technologie et les infractions où la technologie est l'instrument*, on peut remonter la piste de la cybercriminalité jusqu'à plus de 100 ans avant l'invention d'Internet.

Ainsi, entre 1834 et 1836, deux hommes détournent le réseau de télégraphie optique français afin de connaître la clôture des cours de la Bourse de Paris. Aujourd'hui, lorsque l'on parle de cette affaire, on parle de piratage ou encore de cyberattaque. Mais concrètement, il s'agissait de détourner l'un des tout premiers moyens de télécommunication moderne à des fins criminelles.

« Ce n'est pas très différent des crimes de la vraie vie », déclare Hernán Popper, avant de poursuivre que « les nouvelles technologies sont autant de nouvelles plateformes pour les criminels. La difficulté pour les autorités, c'est que les cybercrimes peuvent être commis depuis n'importe où, sans laisser de preuves physiques ».

Des motivations variées

Pour Bertrand Milot, fondateur et président d'une entreprise québécoise et conférencier en cyberintelligence, bien que l'arrivée d'Internet ait rendu concrète la notion de cybercriminalité, c'est surtout l'arrivée des transactions numériques qui a fait évoluer la cybercriminalité en ce qu'elle est aujourd'hui.


Bertrand Milot

« La cybercriminalité existait déjà dans les années 1980-1990. Mais dans la grande majorité des cas, il n'y avait pas d'objectif

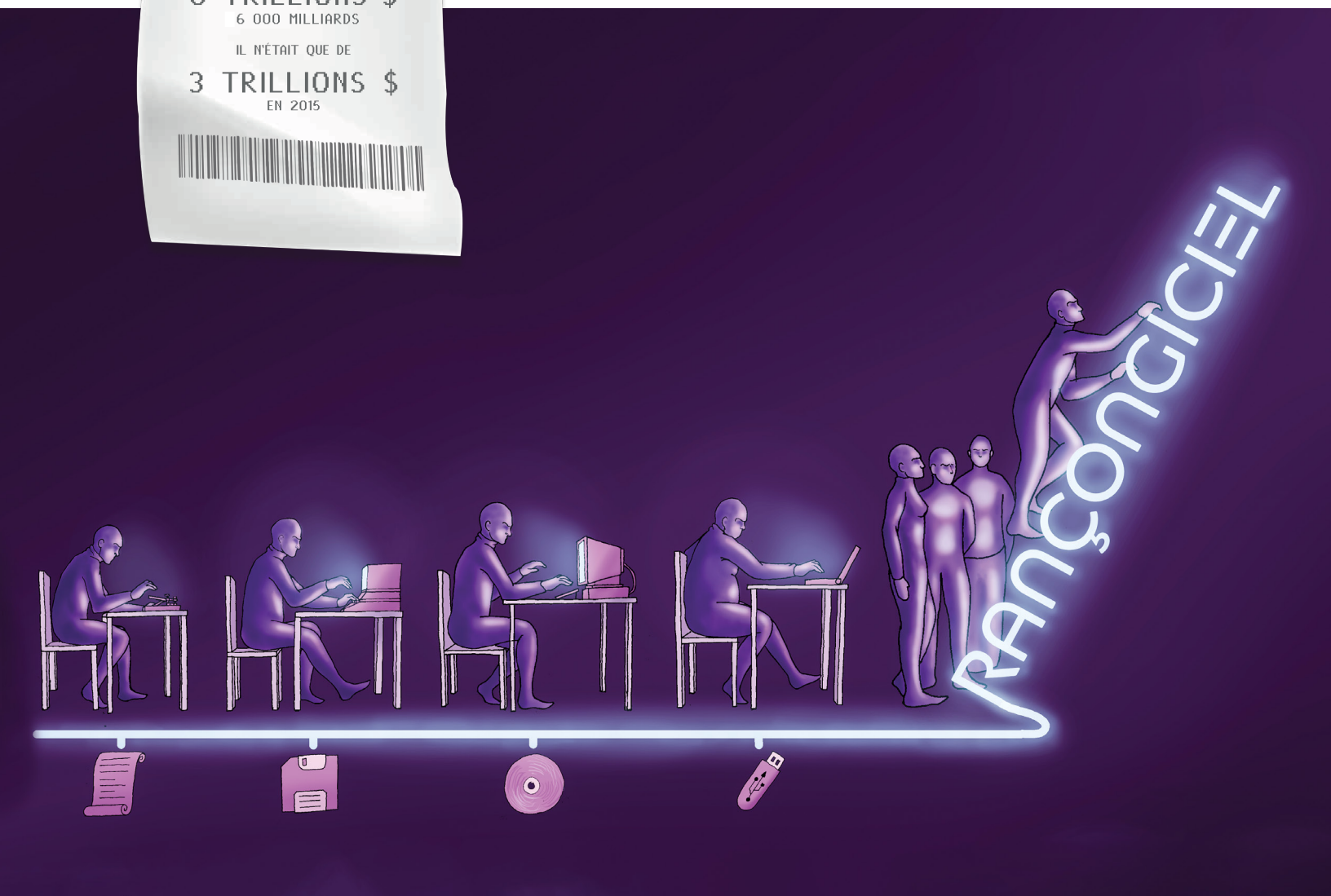
Illustration : RIENNEPRESS - Tanguy Maerten | Photos : Marta Guerrero / Gracieuseté

de rentabilité. Bien sûr, il y a toujours des exceptions. En 1994, des pirates informatiques avaient ciblé le système informatique de gestion de la trésorerie de la banque américaine Citibank, parvenant à voler plus de 10 millions de dollars.

« Malgré quelques actions pécuniaires ciblées, les cybercriminels avaient des motivations liées à la notoriété, à l'envie d'obtenir des trophées et de relever des défis techniques. On parlait alors de cyberterrorisme, d'activisme et de vandalisme. L'un de ces défis était de pouvoir faire imploser la nouvelle bulle d'Internet à la fin des années 1990. »

Dans les années 2010, la cybercriminalité va connaître deux évolutions majeures. Dans un premier temps, l'arrivée dans le secteur numérique d'algorithmes ayant un chiffrement plus sophistiqué, comme le chiffrement asymétrique RSA, permettant aux cybercriminels d'utiliser des logiciels malveillants plus difficilement décodables pour les victimes touchées. Dans un second temps, selon Bertrand Milot, l'arrivée des cryptomonnaies en 2010 a fait évoluer les motivations des cybercriminels, les rendant majoritairement pécuniaires.

« Cette monnaie présente l'avantage pour les cybercriminels d'être difficilement traçable et permet de ne pas créer d'espaces physiques de rencontre entre le donneur et le receveur, rendant les transactions anonymes. L'arrivée des cryptomonnaies a transformé l'industrie de la cybercriminalité. » (Voir articles en page 23 et 24.)



Le vaste éventail des cybercriminels

De nos jours, il est de plus en plus difficile d'établir un profil type pour les cybercriminels. La représentation du génie de l'informatique assis derrière son écran d'ordinateur et portant un pull à capuche est dépassée. En réalité, la motivation même du cybercriminel va le plus souvent influencer son domaine d'activité, sa taille et son type de cybercrime.

Écrit par **Jean-Baptiste GAUTHIER**

Entre la notoriété, l'argent et l'envie de satisfaire des pulsions et désirs, les motivations d'un cybercriminel ont un grand impact sur sa nature même. Pour mieux expliquer ce qu'est un cybercriminel, Akim Laniel-Lanani, directeur de la Clinique de cybercriminologie de l'Université de Montréal, revient aux origines mêmes de la cybercriminalité, dans les années 1980.

« Certaines personnes qui avaient de grandes compétences technologiques ont commencé à s'attaquer à la plus grande révolution de la fin du siècle dernier, Internet. Ces "premiers cybercriminels" avaient des choses à prouver, de par leurs compétences numériques. Ils agissaient le plus souvent seuls, en quête de prestige et de gloire », explique-t-il.

Le nombre de personnes s'intéressant à la cybercriminalité a ensuite explosé, de par la facilité et l'accessibilité de pouvoir gagner de l'argent en réalisant des crimes en ligne.

« Dans les années 2000, avec l'arrivée du *Dark Web*, le boom qu'ont connu les sites Internet et les forums, et le plus grand accès à des ordinateurs personnels, il est devenu de plus en plus facile de s'informer sur la cybercriminalité. Un grand nombre de cybercriminels, qui cherchaient à se faire rapidement de l'argent en conservant leur anonymat, sont donc apparus », détaille Akim Laniel-Lanani.

Au départ agissant seuls, les cybercriminels ont commencé à se regrouper en petites communautés se partageant des informations et des outils malveillants pour leur bon développement individuel. Jusqu'à l'émergence de vrais groupes et entreprises cybercriminels.

« Aujourd'hui, des groupes cybercriminels existent et fonctionnent comme de vraies entreprises, souligne Bertrand Milot, fondateur et président d'une entreprise québécoise en cyberintelligence.

« Les grandes entités cybercriminelles sont le plus souvent gérées par des personnes qui ne se dévoilent jamais, se protégeant ainsi de la loi. Ils placent à la tête de leur organisation des directeurs techniques, financiers et marketing, qui vont assurer son bon fonctionnement. Et ils vont bien sûr chercher à recruter du personnel », explique celui qui est également conférencier en cyberintelligence.

Un recrutement qui va attirer par exemple de jeunes cybercriminels cherchant à faire leurs preuves.

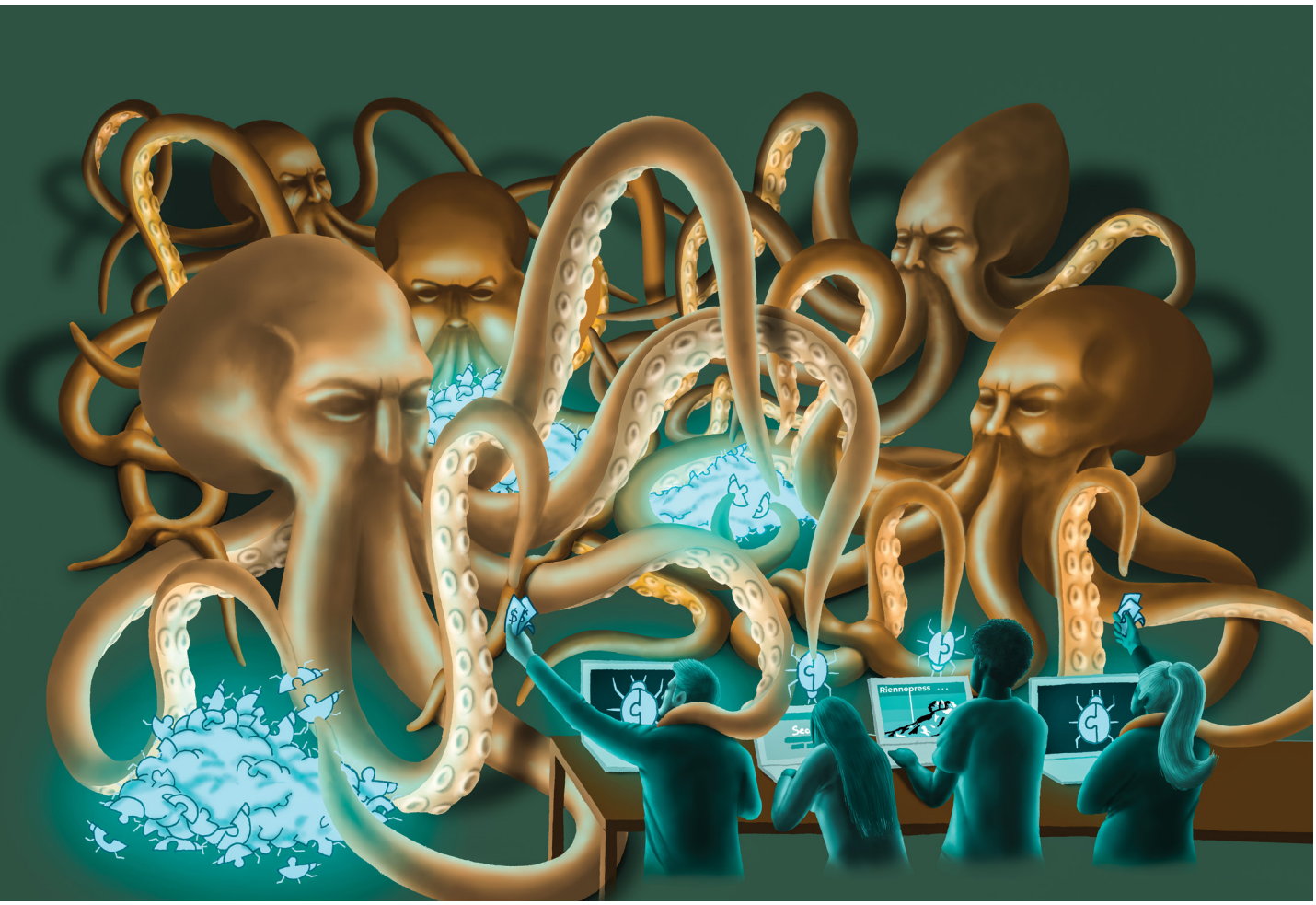


Illustration : RIENNEPRESS – Tanguy Maerten

L'organisation va les tester et juger s'ils sont capables de faire partie de l'organisation, pour devenir des employés et des sentinelles de ce groupe cybercriminel.

Bertrand Milot ajoute que le recrutement de cybercriminels peut aussi se réaliser sur de simples sites de recherche d'emploi.

« Des personnes sont recrutées pour effectuer de simples tâches administratives et elles n'ont absolument aucune idée de la nature criminelle de leur travail, encore moins des personnes qui sont à la tête de l'organisation. La hiérarchie est ainsi protégée. On parle alors de victimes ou de complices qui ignorent leur statut de cybercriminel. »

LES MOTIVATIONS DES CYBERCRIMINELS

1) L'argent : L'appât du gain est la principale motivation des cybercriminels d'aujourd'hui, qui cherchent à se faire de l'argent rapidement et facilement.

2) Le prestige : Les cyberattaques sont souvent un moyen pour les cybercriminels de tester leurs compétences technologiques.

3) Le désir : Des personnes ayant des pulsions ou des désirs malsains vont vouloir détenir ou voler du contenu interdit, le plus souvent à caractère sexuel.

* Cette liste n'est en aucun cas exhaustive. Dans l'histoire de la cybercriminalité, d'autres motivations sont apparues comme la vengeance, la curiosité, la victimisation antérieure par la cybercriminalité, le désir de vaincre les systèmes de sécurité, la perception d'un faible risque de punition, ou encore l'acceptabilité apparente de la cybercriminalité sur le plan social et moral.

Une cybercriminalité plus accessible

Avec la plus grande accessibilité aux outils de la cybercriminalité et leur facilité d'utilisation de plus en plus importante, Bertrand Milot assure qu'il n'est plus nécessaire d'être un génie de l'informatique pour être considéré comme un cybercriminel.

« Avec le *Dark Web* et les applications de messagerie sécurisées, nous pouvons acheter tout ce qu'on désire avoir sur l'Internet d'aujourd'hui, sans même avoir conscience d'acheter un produit illicite. Les cybercriminels utilisent des outils malveillants devenus plus faciles à utiliser avec les années, conséquence de la démocratisation des techniques de la cybercriminalité », regrette-t-il.

Akim Laniel-Lanani appuie les propos de Bertrand Milot : « Beaucoup de cybercriminels ne vont plus exploiter la technique, mais la manipulation des sentiments et la psychologie de leur cible. Ils ont juste besoin de se créer de faux profils sur les réseaux sociaux et ensuite d'engager le dialogue avec une potentielle victime. Cela demande d'être un bon vendeur avec de bonnes compétences en marketing, et non pas un as de l'informatique », détaille le directeur de la Clinique de cyber-criminologie de l'Université de Montréal.

La cybercriminalité est-elle devenue plus simple avec le temps? « Pas forcément, répond Akim Laniel-Lanani. L'augmentation des mesures de cyberdéfense a rendu plus difficiles les attaques des cybercriminels contre les entreprises, notamment le vol des données.

- Suite page 12 -

TROIS CORPS DE "MÉTIERS"

Les activités des cybercriminels diffèrent selon leur nature, leur taille ou leur position géographique, mais nous pouvons définir trois grands types de "métiers" dans la cybercriminalité.

- La **production** des services de cybercriminalité. Ce sont des cybercriminels qui fabriquent des logiciels malveillants, comme les rançongiciels. Des supports physiques sont également fabriqués, comme des kits de cartes bancaires frauduleuses ou des ordinateurs programmés pour réaliser des campagnes de pourriel par courriel.

- La **distribution** des services de cybercriminalité. Des cybercriminels achètent des logiciels malveillants qu'ils vont vendre à d'autres malfaiteurs. Ils ne sont donc pas en contact direct avec une potentielle victime. Ces cybercriminels se contentent juste d'acheter et de distribuer ou de vendre un service.

- L'**utilisation** des services de cybercriminalité. Ce sont des cybercriminels qui sont en contact direct avec une potentielle victime, et qui vont utiliser le service pour voler, frauder, la faire chanter et lui extorquer de l'argent.

En tant que cybercriminel ou groupe de cybercriminels, les "métiers" de la cybercriminalité sont souvent interconnectés, explique Fyscillia Ream, coordonnatrice scientifique à la Chaire de recherche en prévention de la cybercriminalité de l'Université de Montréal et cofondatrice de la Clinique de cyber-criminologie :

« Certains cybercriminels vont agir dans les trois grands types de "métiers" de la cybercriminalité, tandis que d'autres vont se focaliser sur un seul type, pour mieux se protéger ou par manque d'expertise technique. Nous pouvons citer l'exemple d'un jeune malfaiteur qui va acheter un logiciel malveillant sur le *Dark Web*, avec un manuel d'utilisation pour l'utiliser facilement sur de potentielles victimes. »

Akim Laniel-Lanani ajoute que même des kits de piratage et des fichiers d'utilisateurs piratés sont à vendre sur le *Dark Web*, pour seulement quelques centaines de dollars.

« Les cybercriminels n'ont pas tous de grandes compétences techniques. Il suffit d'avoir une connaissance de base des concepts, de la volonté (mal intentionnée) et un peu d'argent. Le piratage est devenu quelque chose de tristement facile à réaliser », note Fyscillia Ream.

« Mais bien souvent, les cybercriminels essayent de se rassembler avec un objectif commun. Des groupes de cybercriminels s'attaquent alors aux données d'une entreprise en associant leurs compétences et leurs outils contre leur cible. »

Akim Laniel-Lanani ajoute que la cybercriminalité évolue et qu'il est parfois difficile de savoir qui sont les cybercriminels.

« Il y a plein de façons de faire de la cybercriminalité. Ce qui va définir un cybercriminel, cela va être à la fois ses motivations, sa cible, ses congénères, mais également son métier. »

Des méthodes en évolution

Depuis 2019, les cybercriminels ont aussi développé leur approche aux victimes. Alors que leur approche se concentrait majoritairement sur un contact en ligne, sans approche physique, les activités hybrides sont apparues.

Hernán Popper, dirigeant d'une entreprise manitobaine en cybersécurité, explique le fonctionnement de l'une d'entre elles, les *card skimmers* ou *appareils d'écrémage*, qui permet de s'adonner à de la fraude à la carte bancaire sur des petites localités.

« La méthode est assez courante et peut prendre diverses formes. Les malfaiteurs se procurent et utilisent une carte bancaire qui contient une puce détachable. Lorsque le criminel entre en contact physique avec le commerçant, il va insérer sa carte dans le terminal de paiement, ce qui va permettre de déposer la puce frauduleuse à l'intérieur même de la machine.

« Quelques jours plus tard, le criminel va effectuer la même opération pour récupérer la puce. Entre ces deux opérations, toutes les informations bancaires des clients du commerçant auront été récupérées par la puce frauduleuse. Nous appelons cela de la cybercriminalité locale et hybride. »

Les cybercriminels changent donc leur méthodologie suivant les évolutions de la technologie. Ils ont leurs propres contraintes et

problèmes, comme le trop grand nombre de données stockées, ou encore la difficulté de bien définir les grandes cibles potentielles à partir des informations récoltées.

Et toute personne peut être victime d'un cybercrime, toutefois notre statut de victime sera différent selon notre réponse aux sollicitations.
(voir article page 13 et 14)

La nécessité de développer une **saine méfiance** et une **bonne cyberdéfense**

Les personnes qui s'intéressent peu ou pas à la cybercriminalité ignorent souvent qu'elles peuvent en être victimes. Cette grande erreur les amène donc à négliger leur hygiène numérique et à utiliser dangereusement les nouvelles technologies.

Écrit par **Jean-Baptiste GAUTHIER**

Dans le monde de la cybercriminalité, les victimes ont une valeur et un statut. D'entrée de jeu, Bertrand Milot, fondateur et président d'une entreprise québécoise et conférencier en cyberintelligence, tient à préciser : « Je ne connais personne qui puisse totalement éviter d'être une victime de cybercriminalité. »

Les cybercriminels vendent et achètent les informations de leurs victimes. Pour comprendre son statut de victime, il faut se mettre dans la tête d'un cybercriminel, notamment lors d'une prise de contact frauduleuse.

Pour l'expert du domaine en cyberintelligence, les réactions et la réponse de la victime face à la tentative de fraude vont la catégoriser aux yeux du cybercriminel.

« C'est un monde qui répond aux mêmes règles que les autres : essayer de se faire le maximum d'argent le plus rapidement possible », souligne-t-il.

Le concept de rentabilité va influencer la manière dont un cybercriminel voit sa victime. Lors d'une tentative d'approche malveillante, un cybercriminel va évaluer sa cible suivant le temps passé à essayer de lui extorquer de l'argent. Plus la victime tombe dans le piège rapidement, plus le cybercriminel y gagne sur tous les fronts de la rentabilité.

Pour Bertrand Milot, on devient une cible moins attrayante quand l'échange entre un cybercriminel et sa cible devient trop long. Le temps de négociation expose le cybercriminel, il peut se faire repérer et surtout, sa cible ne devient plus rentable.

« Il est évident que le temps de négociation influe sur notre statut de victime et notre rentabilité. Mais le plus important, c'est de s'assurer d'avoir une bonne hygiène numérique, pour faire en sorte de réduire les risques d'une cybervictimisation », interpelle-t-il.

C'est en adoptant des pratiques sécuritaires qu'on devient une cible moins intéressante pour les cybercriminels. Nous parlons alors d'une saine et sécuritaire utilisation de ses outils technologiques. Une nécessité pour Akim Laniel-Lanani, directeur de la Clinique de cybercriminologie de l'Université de Montréal.

« Avoir une bonne cyberhygiène est le facteur de protection principal contre la cybercriminalité. En grande majorité, un cybercriminel ne va pas perdre son temps à vouloir attaquer une personne qui va adopter les bons comportements quant à son usage numérique », relève-t-il.

Mais comment adopter une bonne cyberdéfense ? Akim Laniel-Lanani recommande de s'informer sur les bonnes pratiques de base, tout en étant dans un état de constante méfiance.

« Avoir une bonne hygiène numérique passe par se demander sur quel lien je suis en train de cliquer, si ce courriel est fiable ou encore si la personne avec qui je communique par téléphone

Illustration : RIENNEPRESS - Tanguy Maerten

est bien mon conseiller bancaire. C'est en vérifiant de potentiels doutes que nous pouvons devenir de meilleures mauvaises victimes » de la cybercriminalité, conseille-t-il.

Il en va de même pour les entreprises, comme l'ajoute Akim Laniel-Lanani, qui considère qu'une organisation se doit aujourd'hui de prendre de grandes dispositions pour protéger l'accès à ses données et son infrastructure. La cyberdéfense doit être un service à part entière d'une entreprise et ses employés doivent être formés et informés en matière des bonnes pratiques numériques.

Au Canada, le nombre total de cybercrimes déclarés par la police en 2021 était de 70 288. Pour se faire une idée de l'ampleur qu'a pris le phénomène, en 2014 on en comptait seulement 15 184. Un chiffre qui fait pâle figure par rapport aux données les plus récentes, mais qui reste révélateur d'une chose : la problématique ne date pas d'hier.

PERSONNE N'EST À L'ABRI

Hernán Popper, dirigeant d'une entreprise en cybersécurité, fait écho aux propos de Bertrand Milot et Akim Laniel-Lanani, en soulignant que « toute personne doit se considérer comme la potentielle cible d'un cybercriminel ».

« Nous avons pris beaucoup de retard dans notre compréhension de la cybercriminalité. Il y a beaucoup d'ignorance et d'inconscience sur le sujet. Nous avons un schéma de pensée qui nous fait demander : *mais pourquoi quelqu'un me ciblerait-il ?* », souligne-t-il.

Illustration : RIENNEPRESS - Tanguy Maerten

Bertrand Milot ajoute que « nous sommes tous des cibles à partir du moment où une personne a des données personnelles, des accès faciles et directs à des informations de son entourage, un compte bancaire, des comptes sur des sites de vente en ligne, etc. Tout le monde peut être visé, que cela soit par des appels téléphoniques, des messages sur son portable, par courriels, des appareils intelligents connectés ou encore sur les réseaux sociaux ».

Pour Hernán Popper, les gens font trop confiance aux appareils technologiques. « Il est faux de penser que nos appareils numériques sont sécurisés à 100 %. Dans de nombreux cas, la cybersécurité n'a même pas été réfléchie lors de la fabrication de l'appareil.

« Prenez l'exemple d'une ampoule que vous allumez à l'aide d'appareils connectés et qui a été fabriquée dans un pays étranger. Comment pouvons-nous savoir qu'elle n'est pas utilisée pour recueillir des informations ou pour servir de moyen de pirater à distance votre ordinateur ? Il faut absolument comprendre le comportement du produit acheté et savoir, avant l'achat, si des informations peuvent être récoltées et transmises à un tiers. »

Bertand Milot avertit : « C'est notamment le cas des caméras de sécurité résidentielles. Elles introduisent un faux sentiment de sécurité et elles peuvent être facilement accessibles par les cybercriminels. D'ailleurs, de nombreuses vidéos pédopornographiques, provenant de caméras de surveillance de chambres d'enfants, sont accessibles sur le *Dark Web.* » Une prise de conscience des risques technologiques et une meilleure hygiène numérique sont essentielles pour ne pas devenir une cible trop facile des cybercriminels.

Dans les profondeurs du net

Internet est un monde immatériel, par conséquent, il est difficile d'en imaginer la superficie. À la manière du monde réel qui se compose de plusieurs continents, le web, lui, est constitué de trois niveaux distincts : le Clear Web, le Deep Web et enfin, le Dark Web.

Écrit par **Hugo BEAUCAMP**

L'image qui revient le plus souvent pour parler des différents niveaux de web, c'est celle de l'iceberg. Elle est assez parlante, en tout cas pour les deux premières couches de l'Internet. En effet, l'ordre de grandeur entre la partie visible et immergée de l'iceberg est assez fidèle à la réalité.

En revanche, sous la glace se trouvent les profondeurs quasi infinies de l'océan. Or, nous le verrons, le *Dark Web* n'est pas la partie la plus importante du web. On retiendra surtout que les profondeurs sont plus difficiles d'accès et qu'il est bien plus compliqué de mettre la main sur ce qui s'y cache.

Le *Clear Web* ou web de surface

Ici, rien de bien complexe. Tous les individus ayant déjà allumé un ordinateur connecté à un réseau sont familiers avec cette partie de l'Internet. Akim Laniel-Lanani, directeur de la Clinique de cyber-criminologie à l'Université de Montréal, explique en quelques mots à quoi se résume le web de surface : « Il s'agit de tout ce qui est accessible par moteur de recherche. Tout ce qui est trouvable et recensable. »

En 2017, on estimait à environ 980 millions le nombre de sites web indexés, soit une taille d'à peu près 19 Térabit (Tb). Grâce à l'utilisation de robots d'indexation (1), aussi appelés *crawlers*, on estime que le *Clear Web* représente environ 10 % de la surface totale de l'Internet.

Cependant, tout ce qui se trouve sur le *Clear Web* n'est pas nécessairement légal, comme le précise Akim Laniel-Lanani : « Des forums de pirates et des points de vente de produits illicites peuvent y être trouvés, entre autres. »

Le *Deep Web*, la partie immergée de l'iceberg

En comparaison avec la partie « visible » du web, la partie immergée de l'iceberg est immense. Elle englobe tout ce qu'on ne souhaite pas accessible. Pour l'illustrer plus simplement, le *Deep Web* est généralement accessible suite à une authentification, un nom d'utilisateur et un mot de passe, et il contient principalement des choses jugées inoffensives.

« Il s'agit en fait de pages qui ne sont pas indexées et qui ne concernent que l'utilisateur lui-même, explique Akim Laniel-Lanani. Par exemple, il existe 3 milliards d'utilisateurs sur Facebook. Cela équivaut à 3 milliards de comptes qui existent sur le *Deep Web* qui ont tous leurs propres particularités. »

En fait, à partir du moment où un individu entre ses informations pour se connecter à un compte, il entre en réalité dans le *Deep Web*. Cela comprend aussi les informations académiques, les dossiers médicaux, les informations bancaires.

On estime la taille du *Deep Web* à environ 7 500 Tb, soit près de 400 fois plus grand que le web de surface. Mais là encore, difficile de définir précisément l'envergure de cette strate de l'Internet, étant donné qu'elle consiste principalement en des pages non répertoriées et que ces estimations datent de 2017. Or, le web est en perpétuelle expansion.

Le *Dark Web*, ou les profondeurs

Un peu à tort, lorsque l'on parle de l'envergure du *Dark Web*, on a tendance à l'associer au *Deep Web*. Toujours est-il qu'à elles deux, ces couches représentent les 90 % restants de la surface du net. Mais le *Dark Web* est plus « profond », pas forcément plus grand, et surtout on y accède différemment.

« Les entreprises classiques n'ont pas grand intérêt à être sur le *Dark Web*. Les sites sur le *Dark Web* veulent être trouvés mais pas par tous. C'est pour ça que contrairement aux idées reçues, il est moins étendu que le web de surface », souligne Akim Laniel-Lanani.

En revanche, toutes les idées reçues ne sont pas fausses : une grande partie de ce que l'on trouve sur le *Dark Web* est bel et bien illégal. C'est d'ailleurs pour ça que le fonctionnement intrinsèque de cette partie de l'Internet arrange bien ceux qui y naviguent, peu importe de quel côté de la loi ils se trouvent.

Le directeur montréalais explique l'intérêt d'utiliser le *Dark Web* pour héberger son site : « Ces sites web-là ne sont accessibles qu'en passant par un outil de chiffrement de navigation, comme le réseau Tor (The Onion Router). Ce dernier, accessible à tous, permet de se rendre sur des sites cachés, mais il ne s'agit pas d'un moteur de recherche à proprement parler », souligne-t-il.

La technologie qu'utilise le réseau Tor a été créé à la base par la Défense américaine, mais le réseau est aujourd'hui maintenu et mis à jour par une communauté d'utilisateurs. La manière dont le réseau fonctionne permet d'assurer un certain degré d'anonymat : plutôt que de voyager d'un point A à un point B par le chemin le plus court, l'information encryptée va se déplacer d'un ordinateur à un autre, et ces ordinateurs vont eux-mêmes utiliser des relais pour envoyer l'information d'un point à un autre, puis un autre, et ainsi de suite jusqu'à destination.

Illustration : Yahia Lahrech

Identifier le point d'origine de l'information devient alors particulièrement difficile, l'identité de l'utilisateur est donc bien protégée. Quant aux sites, « ils sont difficilement identifiables puisqu'ils n'utilisent pas les noms de domaine simples auxquels nous sommes habitués sur le *Clear Web*. Ici, les adresses URL sont de longues séries de chiffres et de lettres qui changent constamment. Sur le *Dark Web*, on trouve .onion à la fin des adresses URL. Le *Dark Web* est comme un grand bal masqué numérique ».

Visite du *Dark Web*

Mais alors, que trouve-t-on concrètement sur le *Dark Web* ? En réalité, un peu de tout. Des forums de discussions, des médias sociaux, des sites de nouvelles, des sites marchands, de la pornographie, des renseignements personnels, des groupes terroristes, des sectes religieuses, de la drogue, des médicaments, des films piratés... La liste est longue. À titre informatif, la rédaction s'est rendue, accompagnée d'Akim Laniel-Lanani, sur un cryptomarché hébergé sur le *Dark Web*.

On est en effet assez loin de l'image que l'on pourrait s'en faire. D'abord, l'accès à ces sites est beaucoup plus sécurisé que n'importe où sur le net, et ce pour une raison simple qu'Akim Laniel-Lanani explique : « Les sites sont constamment menacés, par les autorités, mais aussi par d'autres cybercriminels qui lancent des attaques par déni de service (DDoS) (2).

« Cette compétition entre les marchés, cette menace constante et le besoin d'être opérationnel rapidement, font en sorte qu'ils investissent peu dans le design du site (qui ressemble beaucoup à ce qu'on pouvait trouver dans les années 90 sur le *Clear Web*). En revanche, les systèmes de sécurité et de *captcha* (3) sont beaucoup plus poussés. »

Une fois sur le site, une liste de règles apparaît, un système qui n'est pas sans rappeler les termes et conditions générales d'utilisation de sites plus communs. Parmi les nombreuses règles, on peut lire : *pas de vente d'arme, interdiction de vendre quoi que ce soit en rapport avec le terrorisme, pas de pornographie, pas de fentanyl (drogue dure particulièrement dangereuse), pas de vente de rançongiciel, pas de vaccin contre la COVID-19, pas de partage d'information personnelle, interdit aux organisations affiliées à la Russie ou la Biélorussie.*

Alors, biensûr si ces règles existent, on peut supposer que de telles choses, si elles sont interdites ici, se trouvent ailleurs sur le *Dark Web*.

Une fois les règles lues et acceptées, on trouve sur le site les choses suivantes, entre autres : de la drogue, des contrefaçons, des cartes de crédit dérobées, des comptes PayPal, des films et des séries, des objets divers et variés, des bijoux, mais aussi des services de pirate, de sécurité, de programmation et d'ingénierie sociale.

En quelles proportions ?

Une fois encore, le *Dark Web* abrite de tout, mais il est particulièrement difficile de savoir dans quelles proportions.

Parmi les choses les plus sombres que l'on peut trouver dans les abysses du web, on notera la présence d'environ 50 000 groupes terroristes, des services de tueurs à gages dont les prix vont de 20 000 $ pour une personne "ordinaire" à 100 000 $ pour quelqu'un jugé "important", mais aussi de la pornographie juvénile.

À propos de cette dernière catégorie, Akim Laniel-Lanani dit ceci : « La pédopornographie est très mal vue par la communauté. Les sites les plus populaires ne veulent pas y être affiliés car ces contenus sont particulièrement ciblés par les autorités. »

Mais contrairement aux idées reçues, notre expert en cybercriminalité précise que la pédopornographie ne se trouve pas exclusivement sur le *Dark Web*. Il ajoute même que « les sites abusifs sont plutôt isolés. Sur le *Dark Web*, ce sont les drogues et les services de pirate qui prédominent ».

Finalement, il est assez délicat de savoir exactement quels sont les sites et les contenus les plus consultés. Une étude menée en 2016 par les chercheurs Owen Gareth et Nick Savage tente d'apporter un début de réponse. Pendant six mois, ils ont observé les requêtes faites sur le *Dark Web*.

Il est important de noter que l'étude s'est déroulée sur une période de temps relativement courte et sur quelques serveurs seulement. Mais même si elle n'est pas nécessairement représentative de la totalité des utilisateurs du réseau Tor, cette étude indique que les sites d'abus (pornographie juvénile) figurent parmi les plus

Illustration : Yahia Lahrech

populaires (158 000 requêtes par jour en moyenne sur 12 jours).

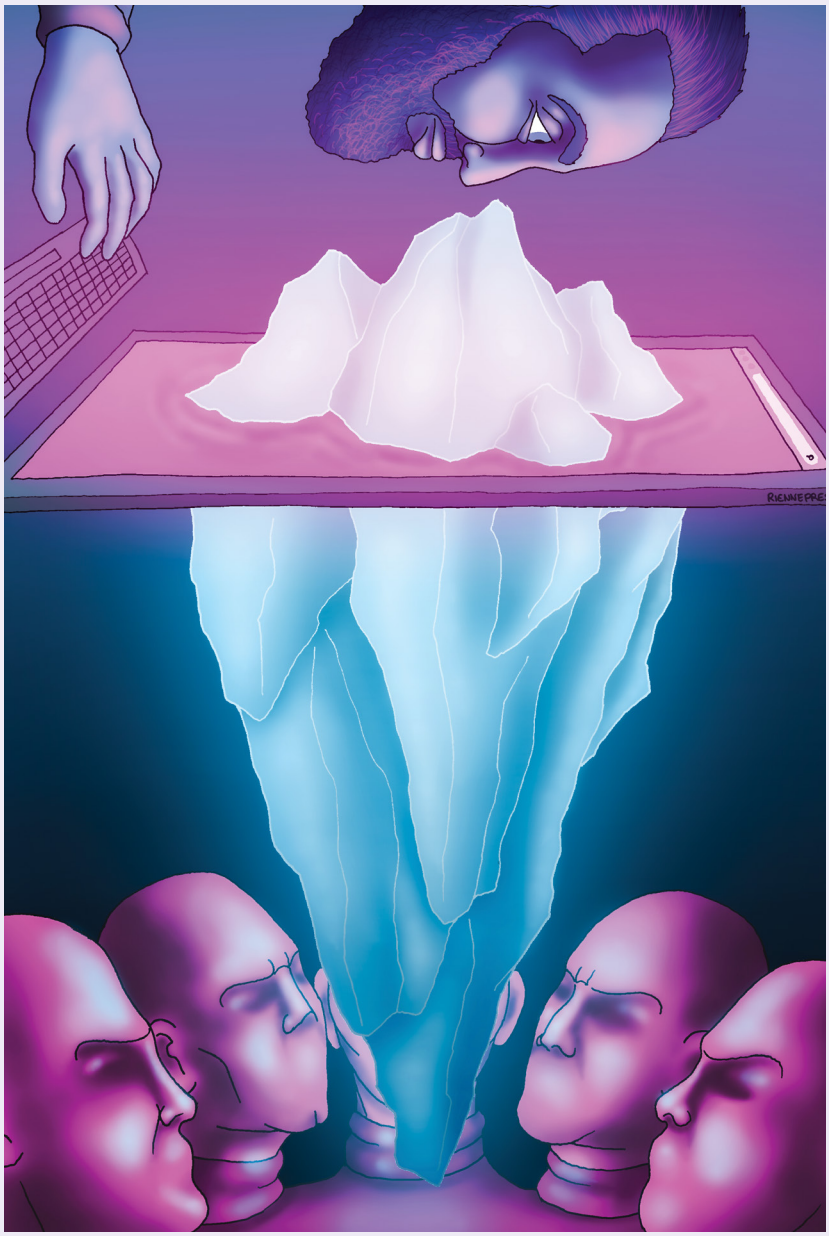
Seulement, les données collectées se frottent à plusieurs limites qui pourraient expliquer cette moyenne élevée. Premièrement, les moyens techniques n'existent pas pour distinguer le clic de l'individu, ce qui signifie qu'un même individu ayant effectué la même requête trois fois est comptabilisé trois fois au lieu d'une.

Deuxièmement, les contenus illégaux et particulièrement mal vus comme la pédopornographie sont plus difficiles d'accès. Les trouver requiert donc plus de requêtes. Enfin, les sites d'abus sont fréquemment surveillés par les autorités, ce qui aurait, une fois encore et pour de bonnes raisons, pu faire augmenter les chiffres collectés.

Tout n'est pas sombre

Le *Dark Web* n'a pas seulement vocation d'abriter des activités illégales et ce n'est d'ailleurs pas la seule chose que l'on y trouve. Par exemple, de par l'anonymat qu'il procure, de nombreux services secrets gouvernementaux l'utilisent pour communiquer avec leurs agents à travers le monde. De grands groupes médias ont aussi un site Internet sur le *Dark Web* pour préserver l'identité des lanceurs d'alertes ainsi que de leurs sources.

C'est également un refuge pour les dissidents politiques et les activistes qui luttent contre des systèmes oppressifs. À noter que naviguer sur le *Dark Web* n'a absolument rien d'illégal en soi, encore une fois tout dépend des activités auxquelles les utilisateurs s'adonnent.



Et naviguer dans les profondeurs du web n'est pas synonyme de nager avec les requins. « Les cybercriminels se rendent sur le *Dark Web* pour cacher leurs activités, leurs achats, leurs ventes. Mais c'est principalement une question d'anonymat, ils peuvent faire tout ça dans le *Clear Web* », termine Akim Laniel-Lanani.

En ce qui concerne la recherche de victimes, les requins nagent là où il y a le plus de baigneurs : en surface.

(1) Logiciel qui explore automatiquement le Web. Il est généralement conçu pour collecter les ressources, afin de permettre à un moteur de recherche de les indexer.

(2) Attaque qui met hors ligne tout le système informatique.

(3) *Le Captcha* est une mesure de sécurité de type « authentification par question-réponse ».

Sources :
- Nick Routley. (2017, 8 juillet) The Dark Side of the Internet. *Visual Capitalist*
- Owen, G., & Savage, N. (2015). *Empirical Analysis of Tor Hidden Services*. (pp. 113-118). The Institution of Engineering and Technology.

Illustration : RIENNEPRESS - Tanguy Maerten

rançons

payer ou ne pas payer ?

De plus en plus de voix s'élèvent pour inciter les gouvernements à interdire les paiements de rançons, à l'exemple de Masarah Paquette-Clouston, professeure adjointe à l'Université de Montréal. Elle appelle à favoriser le bien-être collectif sur l'intérêt personnel. Une start-up québécoise victime de cyberattaque explique aussi son choix de ne pas avoir payé.

Écrit par **Mehdi MEHENNI**

La communauté internationale demeure partagée sur la légitimité des paiements de rançons par les entreprises victimes de cyberattaques. Certains pays, comme l'Algérie, l'interdisent. D'autres pays, et le Canada en fait partie, comptent des compagnies qui offrent carrément leurs services pour la négociation et le paiement de rançons au nom des victimes de cas d'attaque, comme le relève Masarah Paquet-Clouston, professeure-adjointe à l'École de criminologie de l'Université de Montréal.


Masarah Paquet-Clouston

« Il est vrai qu'il y a plusieurs enjeux. La crainte de perdre ses clients en fait partie. Mais cela dépend de la manière dont l'entreprise décide de percevoir ces risques. Et si c'est sa réputation qu'elle valorise le plus », souligne l'universitaire.

Mais Masarah Paquet-Clouston met quand même en garde les entreprises qui pensent que le paiement de rançon est une réponse définitive au problème. En plus d'une mauvaise réputation liée au paiement d'une rançon, rien ne garantit à l'entreprise le recouvrement de ses données et de son portefeuille client. Ce qui constitue une double perte.

« Il y a une multitude de considérations à avoir lorsqu'une entreprise est victime d'une attaque aboutissant à une demande de rançon. Face à une telle tragédie, une entreprise va souvent vouloir minimiser ses pertes et protéger ses actifs. Or ce que l'on devrait chercher dans ces moments-là, c'est l'intérêt commun », souligne la spécialiste.

Elle précise sa pensée de façon claire et catégorique : « Pour le bien commun, il ne faut pas payer parce qu'il ne faut pas donner à ces organisations criminelles assez de motivations pour continuer. »

Interdire ou non la rançon ?

À la question de savoir si le Canada devrait continuer à laisser le choix aux entreprises d'accepter ou de refuser le paiement de rançons, Masarah Paquet-Clouston tranche en faveur d'une interdiction générale. Elle ne croit pas que cela constituerait une entrave à la liberté d'entreprendre.

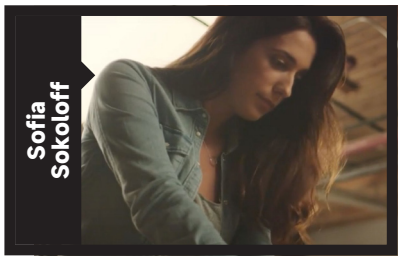
« Je pense que c'est une partie fondamentale de la solution que d'interdire le paiement de rançons. C'est ainsi que les entreprises penseront à investir dans la cybersécurité et dans des programmes de résilience qui leur permettront de savoir comment réagir adéquatement quand leurs données sont publiées en ligne. »

Masarah Paquet-Clouston soulève que : « S'il y a des entreprises qui paient des rançons mais qui ne souhaitent pas en parler

Photo : Gracieuseté

publiquement, c'est bien la preuve qu'elles ont conscience qu'il y a, en quelque sorte, une désapprobation sociale. »

En revanche, une entreprise québécoise, qui a refusé de payer la rançon tout en réussissant à récupérer ses données, en parle fièrement.



Sokoloff Lingerie donne l'exemple

Sofia Sokoloff passe, depuis 2019, pour une héroïne dans le monde des startups canadiennes ayant été victimes de rançongiciels.

Lorsque la patronne de cette entreprise de fabrication de lingerie fine a reçu un faux courriel d'Instagram, elle n'avait aucune idée de l'infortune qui l'attendait au bout d'un clic.

« Comme je commercialise des sous-vêtements, c'est assez fréquent qu'Instagram m'envoie des courriels pour me dire que telle ou telle image est jugée trop sexy. Mais, cette fois-ci, c'était un cybercriminel qui se cachait derrière le lien. En une fraction de seconde, j'ai perdu tous mes accès à Instagram », raconte-t-elle.

Une bonne partie des revenus de Sokoloff Lingerie passait par son compte Instagram, qui comptait 55 000 abonnés. En outre, Sofia Sokoloff allait faire l'objet d'actions de harcèlement simultanées.

« Le pirate avait commencé à me contacter et à me mettre de la pression chaque jour à partir d'un nouveau compte Facebook. J'avais l'impression d'avoir affaire à plusieurs personnes, mais le message était le même : si vous voulez récupérer votre compte Instagram, vous devez payer. Une fois, c'était à partir du compte Facebook d'un utilisateur résidant à Vancouver. Une autre fois, c'était à partir du compte Facebook d'une jeune femme du sud des États-Unis… C'était déroutant ! », témoigne-t-elle.

Sofia Sokoloff a fini par découvrir que le maître chanteur agissait à partir de l'Europe. Les comptes Facebook à travers lesquels le cybercriminel la contactait avaient également été piratés, ce qui lui permettait de brouiller les pistes.

Autre fait intriguant, l'entrepreneure affirme que le pirate ne lui avait pas parlé d'une somme précise à lui payer. « Je crois qu'il voulait d'abord savoir si j'étais d'accord sûr le principe et sonder mon état d'esprit avant d'entamer les négociations et fixer un prix. Mais je ne suis pas entrée dans le jeu », fait-elle savoir.

Akim Laniel-Lanani, directeur de la Clinique de cybercriminologie de l'Université de Montréal, explique que, dans le cas de Sofia Sokoloff, le pirate attendait de diriger la victime vers d'autres moyens de communication pour parler du prix et de la façon de payer.

« C'est pour une question de traçabilité. Facebook et Messenger n'offrent pas le même niveau d'anonymat aux cybercriminels, comme WhatsApp, Telegram et Signal le font », explique-t-il.

La technique de dissociation des comptes

Selon l'universitaire, un compte de réseau social a plus de valeur et le cybercriminel craint de le perdre si jamais il est signalé aux administrateurs de la plateforme.

« Il y a un investissement de temps et d'efforts de la part des cybercriminels dans la création de profil ou dans le vol de ces comptes afin d'avoir un premier contact réussi qui permet de faire baisser les gardes de leurs cibles et débuter la conversation », précise-t-il.

Il ajoute qu'en dirigeant les cibles vers d'autres canaux de communication comme WhatsApp, les fraudeurs s'assurent qu'il n'y a pas de lien entre les deux comptes et que les activités criminelles de l'un ne peuvent pas être associées à l'autre.

Pour les cybercriminels, l'avantage d'utiliser plusieurs plateformes de communication repose dans l'assurance de ne pas voir disparaître totalement le travail accompli. Par exemple, si son compte Facebook venait à être signalé comme frauduleux et suspendu, le cybercriminel aurait toujours un moyen de rester en contact avec sa victime via un autre médium.

« Sans la certitude et des preuves qu'un compte Facebook a enfreint les règles d'utilisation, aucune action ne sera prise pour le fermer et les fraudeurs ne voient pas leur investissement perdu. Cette logique n'est pas une règle, donc le choix d'agir ainsi ou non revient

Photo : Gracieuseté

entièrement au cybercriminel », note Akim Laniel-Lanani.

Une autre raison qui explique l'approche du pirate face à l'entreprise québécoise de lingerie fine, souligne l'universitaire, est que les forces de l'ordre doivent surmonter beaucoup d'obstacles afin d'arriver à peut-être identifier le cybercriminel.

« Les applications de messagerie comme WhatsApp compliquent les enquêtes policières, car il est facile de se débarrasser du compte ou de s'en créer un nouveau s'il est banni ou suspendu. Il est compliqué et ardu pour les forces de l'ordre d'obtenir suffisamment d'éléments de preuves afin d'envoyer une ordonnance de communication à l'entreprise pour obtenir les informations du propriétaire de compte », conclut-il.

La ruse comme solution

En allant finalement se renseigner sur des blogues, Sofia Sokoloff constate que les entreprises ne récupèrent pas forcément leurs réseaux sociaux après le paiement de la rançon. Ce qui confortera son choix de ne pas entrer dans le jeu du cybercriminel.

« J'ai exploré toutes les options de récupération disponibles sur Instagram, mais cela n'a servi à rien. Je déconseille d'ailleurs cette option aux professionnels. Au début, c'était un robot qui me répondait, ensuite j'ai commencé à clavarder avec un employé en Malaisie. À force d'insister, l'employé a fini par me téléphoner, mais c'était pour me dire qu'ils ne pouvaient rien contre le piratage », regrette-t-elle.

La fondatrice de Sokoloff Lingerie a fini par avoir une personne physique au téléphone, du bureau d'Instagram à Toronto. Elle a dû cependant passer par le *business manager*.

« J'ai dû tricher un peu. Comme il y a de l'argent qui rentre, ils mettent de vraies personnes dans ces services », dit-elle sur un ton désabusé.

L'entrepreneure s'est arrangée pour se faire assister par une entreprise de sécurité numérique. Un agent s'est joint à la communication téléphonique qu'elle a eu avec le service commercial d'Instagram à Toronto.

« L'agent, qui m'a servi en quelque sorte d'avocat, leur a demandé des renseignements sur leur département légal. Il leur a signifié que si nous subissions des pertes, ils allaient être tenus en partie responsables. Le soir même, j'ai reçu mes accès à la première adresse courriel qui avait servi à la création du compte », soupire-t-elle au souvenir de son soulagement.

Sofia Sokoloff, aujourd'hui fière de ne pas avoir cédé au chantage du cybercriminel, affirme que c'est grâce au partage de son histoire sur les réseaux sociaux qu'elle avait réussi à recouvrir son compte professionnel.

« Les premiers temps, je me faisais contacter au moins trois fois par semaine par des entreprises victimes de cyberattaques et qui me demandaient de les aider à récupérer leurs comptes », témoigne-t-elle.

Au même titre que l'universitaire Masarah Paquet-Clouston, la patronne de la start-up québécoise considère que payer une rançon à un cybercriminel revient à l'encourager à poursuivre son crime.

Illustration : RIENNEPRESS - Tanguy Maerten

Publi-reportage

LA CYBERSÉCURITÉ

Caisse Groupe Financier

...et les 8 signes avant-coureur d'une arnaque d'hameçonnage

À un moment ou à un autre, la plupart d'entre nous sont tombés sur une arnaque d'hameçonnage. Il s'agit d'une tentative par un cybercriminel de vous inciter à révéler vos informations personnelles en envoyant des courriels, des textos, des messages vocaux et des messages directs à l'apparence convaincante, qui semblent provenir d'une organisation légitime. Il est souvent facile de repérer un message frauduleux, mais pas toujours.

Afin de vous aider à devenir un peu plus vigileant·es, nous avons demandé à l'expert en cybersécurité de Caisse Groupe Financier, David Rheault, de partager sa liste de signes avant-coureurs.

Que ce soit au travail ou à la maison, lorsqu'il s'agit de la sécurité des courriels : Réfléchissez avant de cliquer. Surtout si...

1. L'adresse « DE » est fausse
Le courriel provient d'une personne qui n'est pas une connaissance et/ou l'adresse courriel de l'expéditeur provient d'un domaine étrange. (Par exemple, @domaine.ca est @dornaine.ca, c'est un manque facile).

2. Le « À » vous semble bizarre
Vous avez reçu un courriel qui a également été envoyé à un groupe de personnes inhabituel. Vous devriez vous demander : est-ce que c'est légitime ? Pourquoi suis-je inclus dans ce groupe ?

3. Le texte et « l'hyperlien » ne correspondent pas
Lorsque vous survolez votre curseur (souris) sur un lien hypertexte mis en évidence dans le message électronique, le lien apparaît pour un site Web différent de celui qui est annoncé.

Voici un exemple :

4. La « date ou l'heure » est bizarre
Avez-vous reçu un courriel que vous recevez normalement durant la journée, mais qui a été envoyé à une heure inhabituelle, comme 3 heures du matin ? Il se peut qu'il soit légitime, mais vous devriez en penser deux fois.

5. La ligne « Objet » contient des informations supplémentaires
Vous voyez petit « RE : » ou « TR : » dans la ligne d'objet du courriel, alors que vous n'avez aucun souvenir de l'avoir vu auparavant ? C'est suspect.

6. Il y a une « pièce jointe » inattendue
Vous remarquez une pièce jointe avec une extension de fichier potentiellement dangereuse, comme .html, que vous n'attendiez pas. Réfléchissez-y deux fois avant de cliquer dessus.

7. Le « contenu » comporte des erreurs grammaticales
Un autre signe que vous avez affaire à un courriel frauduleux est qu'il comporte des fautes de grammaire ou d'orthographe.

8. Quelqu'un joue la carte « C'EST URGENT »
Le courriel donne un sentiment d'urgence, exigeant une action pour s'assurer que vous ne perdez pas d'argent, d'accès à votre compte ou d'informations importantes (données, messages vocaux ou courriels). Il existe également une arnaque populaire dans laquelle quelqu'un se fait passer pour votre patron ou une connaissance et vous demande d'acheter des cartes-cadeaux. Méfiez-vous de cela !

Ces signes ne signifient pas nécessairement que le courriel est frauduleux. Ils doivent néanmoins donner lieu à une réflexion. Si vous n'êtes toujours pas sûr, pensez à demander un deuxième avis à un collège ou à un·e ami·e avant de répondre ou de cliquer sur un lien ou une pièce jointe.

Gardez ces signes avant-coureurs à l'esprit pour vous protéger des cybermenaces !

Cryptomonnaie et la montée des rançongiciels

L'arrivée des transactions en cryptomonnaie en 2010 a fait évoluer les motivations des cybercriminels. Bertrand Milot, fondateur et président d'une entreprise québécoise et conférencier en cyberintelligence, y associe également l'arrivée de nouvelles techniques cybercriminelles.

Écrit par **Jean-Baptiste GAUTHIER**

« En 2010, les cybercriminels commencent à utiliser les premiers rançongiciels (*ransomware)*, utilisant la cryptomonnaie comme moyen de paiement, explique Bertrand Milot. Ces logiciels malveillants consistent à bloquer et à chiffrer les fichiers et systèmes informatiques d'une victime, pour ensuite les faire chanter contre une somme d'argent majoritairement payable en cryptomonnaie.

« Rançongiciel était un mot peu connu avant 2013. La création de Cryptowall, un type de rançongiciels, a démocratisé cette pratique de rançonnage numérique. D'après la Cyber Threat Alliance (CTA), en 2015, les recettes provenant du ransomware CryptoWall 3.0 se chiffraient à 325 millions USD, dans la cryptomonnaie de l'époque. En 2022, avec l'effet multiplicateur et l'augmentation de la valeur de la cryptomonnaie, on estime que cette somme aurait une valeur de 19 milliards USD. »

Car la cryptomonnaie est une monnaie, un bien, qui évolue avec le temps. Sa grande sécurisation et la démocratie de son utilisation par la communauté a fait augmenter sa valeur marchande.

Utilisée par un nombre restreint de personnes durant ses premières années, la cryptomonnaie va connaître une première explosion de sa valeur fin 2017, quand plusieurs fonds spéculatifs et des particuliers commencent à investir dans le Bitcoin, avec comme objectif d'obtenir de meilleurs rendements sur des placements financiers.

Le Bitcoin est considéré comme la cryptomonnaie la plus connue et facile à obtenir. La valeur d'un jeton de Bitcoin est passée de 1 000 CAD à plus de 20 000 CAD en 12 mois. Après plusieurs chutes de valeur, le Bitcoin connaîtra ensuite une autre grande explosion avec l'investissement de l'entreprise Tesla, début 2021, où sa valeur côtoie alors les 60 000 $. Cette explosion est aussi due à un grand nombre d'investissements privés, influencés par la démocratisation de son utilisation.

Une aubaine pour les cybercriminels, qui voient donc désormais en la cryptomonnaie non seulement une façon de réaliser des transactions anonymes et fiables, mais également une occasion d'investissement pour l'avenir.

Cryptomonnaie et anonymat

Une transaction en cryptomonnaie consiste en un envoi numérique entre deux personnes, qui ne sont identifiables que par un numéro de compte appelé portefeuille de cryptomonnaie.

Pour procéder à la validation de la transaction, l'échange

monétaire doit être validé par un protocole et inscrit à un registre de vérification appelé la chaîne de blocs. Toute transaction approuvée peut être retrouvée publiquement sur la *blockchain*, mais il n'y a aucun moyen direct de déterminer le propriétaire d'un portefeuille de cryptomonnaie.

La *blockchain* présente l'avantage de créer une connexion directe et rapide entre l'acheteur et le vendeur, contrairement à un virement bancaire classique qui fait intervenir une banque pour vérifier le nom des parties prenantes et l'origine des fonds envoyés.

Pour Bertrand Milot, « c'est donc à partir de 2013 que la cybercriminalité a vraiment évolué de "simple virus" à un processus purement pécunier, avec l'utilisation de la cryptomonnaie et la transformation massive du *Dark Web* en une plateforme de vente de produits illicites, comme par exemple des drogues, des armes à feu et des données volées.

« Un changement de mobile du crime qui a donc amené l'arrivée de plusieurs techniques cybercriminelles, comme les rançongiciels. Une évolution rapide et soudaine qui a fait en sorte que les services de cyberdéfense étaient inefficaces lors des premières années et, tout comme les victimes, sans solutions. »

Illustration : RIENNEPRESS - Tanguy Maerten

LE RAPPORT DES BANQUES À LA CRYPTOMONNAIE

L'évolution de la valeur de la cryptomonnaie a de plus en plus intéressé les systèmes financiers mondiaux, et notamment la finance américaine. Une porte-parole de la banque d'investissement Goldman Sachs a confirmé l'existence en 2022 d'un prêt d'argent liquide dans une opération garantie par des Bitcoins. Une affirmation ambiguë sachant que plusieurs échanges publics de cryptomonnaie se font régulièrement pirater. En mai 2021, la Banque centrale du Canada a déclaré que posséder des actifs numériques, comme le Bitcoin, était très risqué, malgré leur adoption par les investisseurs institutionnels.

Blanchiment : les planques invisibles de l'argent du cybercrime

Avec les différentes plateformes de cryptomonnaie abritées dans les paradis fiscaux, il devient de plus en plus difficile de retracer l'argent du cybercrime. Des spécialistes universitaires et des experts de la Gendarmerie royale du Canada (GRC) expliquent les rouages du marché financier parallèle et comment le Canada y fait face.

Écrit par **Mehdi MEHENNI**

L'émergence d'un marché financier parallèle durant les dix dernières années a amplement profité au blanchiment de l'argent issu du cybercrime.

Bertrand Milot, conférencier en cyberintelligence, explique qu'avec l'émergence d'entités non bancaires mais facilitatrices de paiements en ligne, comme Advcash.com, la question de la traçabilité de l'argent est devenue plus complexe qu'avant.

Contactée par ***La Liberté***, la GRC confirme par le biais d'un porte-parole : « L'évolution des systèmes de paiement en ligne a élargi les moyens par lesquels les fraudeurs et les cybercriminels peuvent monétiser leurs activités malveillantes. Les modes de paiement nouveaux et divers, comme les cryptomonnaies et l'utilisation illicite de cartes-cadeaux, posent un défi constant pour l'application de la loi. »

La GRC ne cache pas d'ailleurs le fait que la diversification des services financiers numériques a compliqué la lutte contre la cybercriminalité et la fraude.

« Ces technologies ont facilité le transfert de fonds à des fins malveillantes et ont élargi la portée mondiale de ces activités. La nature transnationale de la cybercriminalité, conjuguée aux tentatives des criminels pour brouiller leur identité, complique en effet la tâche des organismes d'application de la loi », note le porte-parole.

Que fait le Canada ?

Pour s'adapter à ces nouvelles réalités et lutter contre le phénomène, indique de son côté Akim Laniel-Lanani, directeur de la Clinique de cybercriminologie de l'Université de Montréal, le Canada se fie aux recommandations du Groupe d'action financière (GAFI) qui dirige la surveillance et la lutte contre le blanchiment d'argent et le financement du terrorisme.

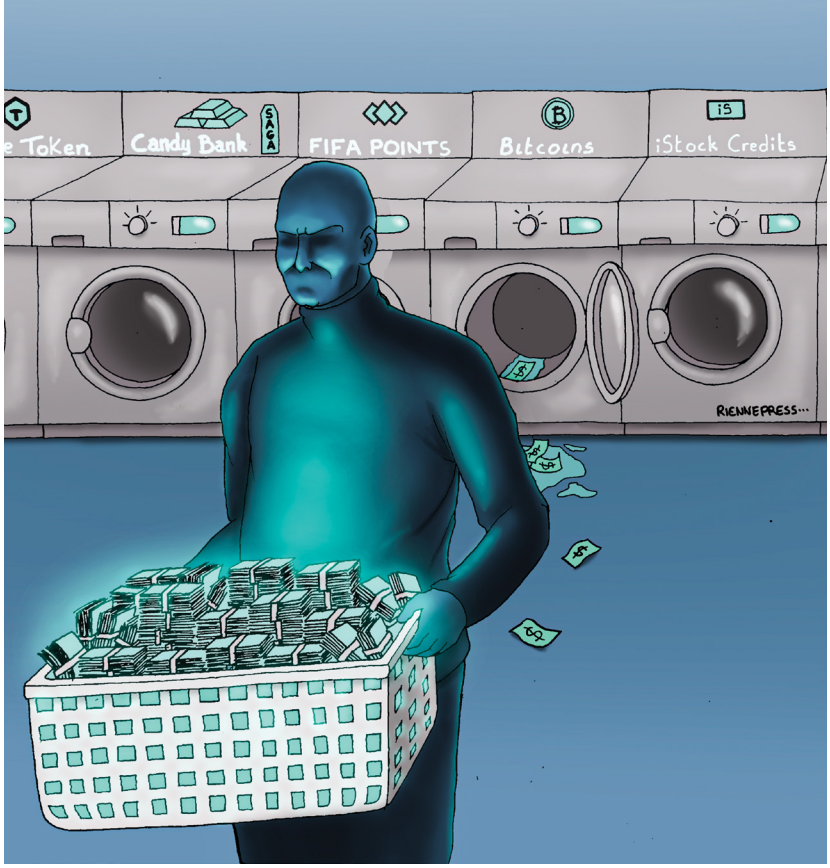
Cette institution internationale, basée à Paris, compte 39 pays membres. Plus de 200 pays et juridictions se sont engagés à mettre en œuvre ses normes.

« Le GAFI publie des recommandations sur les pays et les institutions à risque et le Centre d'analyse et de surveillance des opérations et déclarations financières du Canada (CANAFE) prend le relais pour analyser les informations et les données financières », explique l'universitaire.

Cette unité du renseignement financier, basée à Ottawa, enquête sur tout ce qui facilite et profite au crime. Elle établit des rapports entre des réseaux de blanchiment d'argent, puis remet ces renseignements aux services de police rattachés à la lutte contre le blanchiment d'argent. Mais jusqu'à quel point le CANAFE peut-il retracer l'argent du cybercrime ?

Comment l'argent se perd

Si, dans le marché régulier, la circulation de l'argent est contrôlée, même s'il y a des points morts comme le blanchiment à travers



l'immobilier ou les œuvres d'art, Akim Laniel-Lanani explique que les labyrinthes du marché parallèle offrent aux cybercriminels des planques difficiles à repérer.

« La cryptomonnaie offre elle-même différentes manières de faire du blanchiment d'argent », note-t-il.

L'expert en cybercriminologie explique que les plateformes d'échange de la crypto ont un fonctionnement similaire à celui de la bourse. Le cybercriminel va acheter une crypto à un prix donné pour la revendre à un prix plus haut ou plus bas, puis échanger sa crypto contre d'autres, pour en acheter encore d'autres, et ainsi de suite.

« Au final, le cybercriminel fait un retrait de fonds à partir d'un portefeuille autre que celui qui a servi préalablement à injecter de l'argent dans la plateforme d'échange. C'est ainsi qu'on perd la trace de l'argent, qui peut même être recyclé dans de nouveaux portefeuilles d'argent licite », éclaire-t-il.

Ainsi, poursuit l'universitaire, « même si les autorités de réglementation, dont le CANAFE, exigent des plateformes l'identification des détenteurs de portefeuilles, le problème réside dans les autres plateformes d'échanges qui existent dans les paradis fiscaux. Dans certains pays, qui ont d'autres règles de fonctionnement, il n'est pas exigé des plateformes de communiquer des informations aux autorités sur leurs clients ».

La mission n'est pas impossible

L'ensemble de ces combines fait que la proportion d'argent d'origine criminelle injectée dans les plateformes d'échanges est en constante évolution. En 2022, environ 69 % des fonds en circulation dans ces plateformes provenaient de sources d'origine criminelle, contre seulement 19 % en 2021.

À l'échelle canadienne, les chiffres communiqués par la GRC ne sont pas moins alarmants.

Du 1er janvier au 30 novembre 2022, le Centre antifraude du Canada (CAFC) et le Centre national de coordination en cybercriminalité (CNC3) ont reçu 65 395 signalements de la part de 34 295 victimes de fraude ou de cybercriminalité, ce qui représente des pertes d'environ 490,5 millions $.

Néanmoins, si ces aspects compliquent les enquêtes sur la cybercriminalité, la GRC assure que cela « ne les rend pas impossibles pour autant ».

« Les mesures de répression dans cet espace sont facilitées par les liens solides que la GRC a tissés avec ses partenaires d'application de la loi dans le monde entier, notamment par l'entremise du Groupe d'action conjoint sur la cybercriminalité d'Europol à La Haye », indique le porte-parole de la GRC.

Il reste que si le phénomène dépasse le cadre national, Akim Laniel-Lanani relève que les frontières se rétablissent lorsqu'il est question d'émettre un mandat d'arrêt contre un criminel. Ce qui peut prendre beaucoup de temps, dépendamment du pays avec lequel il faut négocier l'extradition du cybercriminel.

Dans le domaine de la cybercriminalité, il note cependant qu'un pays a réussi à imposer une coopération internationale suivant ses propres règles : les États-Unis.

Illustration : RIENNEPRESS - Tanguy Maerten

Vivre avec les séquelles d'une fraude

Photo : Marta Guerrero

■ En mars 2021, Mélanie Cwikla a été victime de cyberfraude, des cybercriminels ont créé une entreprise en utilisant son nom.

Il y a deux ans, Mélanie Cwikla a vécu ce qu'elle appelle un cauchemar. Des cybercriminels ont créé une entreprise en utilisant son nom. Bien qu'elle ait réussi à prendre des mesures à temps pour prévenir la fraude financière, l'inquiétude, les questions et les séquelles psychologiques sont toujours présentes.

✎ Écrit par **Morgane LEMÉE**

C'était en mars 2021. Mélanie Cwikla reçoit un courriel provenant de l'Office des compagnies du Manitoba, qu'elle soupçonne comme de l'hameçonnage. Pourtant, une fois ouverts, les fichiers PDF sont bel et bien officiels. C'est la confirmation de l'enregistrement d'une compagnie à numéro (apparemment de textiles) en son nom.

Tous les éléments sont là : formulaires remplis, relevé de dépôt signé, reçu de 120 $, et puis son nom, son véritable numéro de téléphone – qui n'est pourtant pas public – et une adresse qui n'est pas la sienne.

Mais Mélanie Cwikla n'a jamais fait de demande pour enregistrer une compagnie. « C'est comme si mon cœur s'était arrêté de battre. La pression monte. Je suis complètement paniquée. Je me demande : *Mais qu'est-ce qui se passe ?!* Je n'attends pas pour appeler l'Office des compagnies du Manitoba. »

À l'autre bout du fil, on ne comprend pas le problème. « On me dit que c'est la première fois que l'on enregistre une compagnie au nom de quelqu'un d'autre, à l'insu de cette personne. Ils me disent : *Ne paniquez pas madame, on va faire les suivis.* Mais moi, je viens de me faire voler mon identité ! »

Les questions se multiplient : Qu'est-ce que l'on veut faire avec cette entreprise ? Quelles autres informations ont-ils ? Mélanie Cwikla imagine le pire. Elle a été fonctionnaire et est actuellement directrice de l'École technique et professionnelle de l'Université de Saint-Boniface. Elle sait que son salaire annuel des 20 dernières années est une information publique. Que va-t-il se passer s'ils mettent la main dessus ? Quelles vont être les pertes financières ?

Démarches immédiates

Mélanie Cwikla contacte la Gendarmerie royale du Canada (GRC), l'Agence du revenu du Canada, et ses institutions financières. Alors que certains se montrent compréhensifs et à l'écoute, d'autres sont pris au dépourvu et se lancent la patate chaude. On lui dit que c'est du jamais vu et qu'il faut patienter en attendant de trouver des réponses.

Bertrand Milot, fondateur et président d'une entreprise québécoise et conférencier en cyberintelligence, décrit une course contre la montre. « Elle ne sait rien de cette compagnie ni de ses actes, et elle ne peut ni la contrôler, ni la défaire. La seule manière de se désengager, c'est de prouver que ce n'est pas la sienne. Mais c'est compliqué. On comprend alors la charge mentale et la course contre la montre que ça représente. »

On se pose alors la question : comment l'Office des compagnies permet-il l'enregistrement d'une entreprise ? Il se trouve qu'aucune pièce d'identité n'est requise à l'enregistrement.

Contacté par ***La Liberté***, le ministère des Finances du Manitoba explique par courriel : « Lorsqu'une personne signe physiquement ou soumet un formulaire en ligne, elle confirme qu'elle est bien la personne qu'elle prétend être et qu'elle est la personne légalement habilitée à agir au nom de l'entité. »

Pour Bertrand Milot, il faut également prendre en compte la période durant laquelle cet évènement est arrivé. « Ça s'est fait en temps de COVID. Je suppose que la complexité bureaucratique à ce temps a dû se simplifier d'une manière ou d'une autre. C'est justement avec la dématérialisation du processus de création d'entreprise que ce scénario de cyberfraude a été possible. »

En résumé, n'importe qui peut créer une entreprise. Mais comment faire pour déceler celles qui sont frauduleuses ? Bertrand Milot parle là encore d'un système complexe. « S'il y avait une solution magique, des cas comme celui de Mélanie n'arriveraient pas. Le problème, c'est que le nombre de fois où ce genre d'anomalie est détecté est faible.

« Cela peut mettre un an, voire deux, avant de lancer une procédure d'enquête sur une entreprise qui ne paie pas ses impôts, par exemple. Pendant ce temps-là, l'entreprise frauduleuse a le temps de faire bien des choses. Alors, les registraires disent que ça ne leur est jamais arrivé, ou très rarement. Alors que dans la réalité, ça arrive des milliers de fois. C'est majeur. »

Pour Bertrand Milot, ce genre de cyberfraude, apparue dans les années 1990, a très souvent pour but le blanchiment d'argent. « En créant une compagnie avec un homonyme, il n'y a plus de traçabilité entre l'activité, la personne en elle-même et la façade légitime.

« Le mobile de ces compagnies est faux, mais ce sont des vraies compagnies, tenues dans de vrais livres. Il y a des secrétaires de direction qui ne savent pas qu'elles font partie d'une entreprise de blanchiment d'argent et qui vont rester au service de cette entreprise pendant 15 ou 20 ans. »

Le soulagement, ou presque

Finalement, le 23 avril 2021, Mélanie Cwikla reçoit la confirmation par courriel que la compagnie n'est plus active et que l'information a été partagée avec l'Agence du revenu du Canada. Notamment parce que la transaction de 120 $ a été confirmée comme transaction frauduleuse par le propriétaire de la carte de crédit volée.

Mais aujourd'hui, plus d'un an plus tard, beaucoup de questions restent sans réponse. Les préoccupations sont toujours là.

« Je ne sais toujours pas comment cette compagnie, qui avait été créée en mon nom, a été utilisée. Quel en était l'objectif ? Où est-ce qu'ils ont pris mon nom ? Est-ce qu'ils ont eu le temps de faire des demandes financières ? Que se serait-il passé si je n'avais pas appris la création de cette compagnie ? Même si je pense avoir pris les bonnes mesures à temps, il y a la crainte que ça ressorte à un moment donné. On vit dans l'incertitude. »

Aujourd'hui, Mélanie Cwikla a changé quelques habitudes de vie. Elle fait beaucoup plus attention aux informations partagées en ligne et à ses mots de passe. « Je vérifie mes comptes bancaires de près, beaucoup plus qu'avant. Quand il y a quelque chose de bizarre dans mes dossiers, le premier réflexe que j'ai, c'est : *Est-ce que c'est lié à ce vol d'identité ?* Je me sens comme si le vol d'identité fait partie de notre réalité quotidienne, et que ça peut arriver à n'importe qui. »

Fraude ou usurpation d'identité ?

Dans le cas de Mélanie Cwikla, un cybercriminel a créé une entreprise à l'Office des compagnies du Manitoba avec son vrai nom, mais avec des coordonnées qui ne correspondent pas complètement aux siennes. Peut-on parler d'usurpation d'identité ?

« Pas à 100 %, précise Bertrand Milot. Les seuls informations en commun ici sont l'adresse courriel et le numéro de téléphone. Mais c'est compliqué, parce qu'en réalité, est-ce que quelqu'un qui crée un homonyme en se servant d'une de tes informations personelles comme fondement usurpe vraiment ton identité ? C'est plus la création d'une fausse identité.

« C'est un scénario compliqué parce que oui, il y a usurpation d'identité aux yeux de l'Agence du revenu du Canada, qui pense que c'est bien elle parce que son nom est très peu commun. Mais en réalité, c'est une autre identité qui a été créée. »

Bertrand Milot explique qu'habituellement, une usurpation d'identité se fait par un ATO (*account take over*). C'est-à-dire que le cybercriminel prend le contrôle d'un compte. Ça peut être n'importe quel compte : carte de crédit, compte Facebook, compte de téléphone… Il prend le compte qui t'appartient et l'utilise à ta place.

« Là, ce n'est pas vraiment un ATO. On a utilisé un homonyme de son nom pour un compte à l'Office des compagnies qui n'est pas à elle.

« On comprend alors la supercherie du cybercriminel. On pourrait penser qu'il préfèrerait prendre un nom très commun. Mais non, parce que les registraires sont habitués aux John Smith ou Bernard Dupont. Ils vont vérifier, parce qu'il y a beaucoup d'homonymes. Mais sur les identités où il y a très peu d'homonymes, voire pas du tout, ils se posent moins de questions. »

Infovictimes Manitoba

Êtes-vous victime ou témoin d'un acte criminel ou êtes-vous un proche de la victime?

Nous savons que lorsque vous avez été victime d'un crime, il est difficile de savoir ce qu'il faut faire ensuite. Vous ne savez peut-être pas où aller pour obtenir de l'aide ou qui peut vous aider. Il est important de se rappeler que vous n'êtes pas seul·e et que de l'aide est disponible si vous en avez besoin.

C'est pourquoi nous avons créé ce nouveau portail : pour que vous puissiez obtenir de l'aide, quels que soient votre âge, votre expression de genre, la nature et la gravité de l'acte criminel, le moment où il a été commis ou le fait que vous ayez porté plainte ou non.

Le portail Infovictimes s'adresse à vous. Vous pourrez y retrouver les services offerts en français pour les victimes d'actes criminels ici au Manitoba.

Infovictimes.ca

Notre nouveau site Web sera disponible bientôt!

Manitoba

Ce projet est rendu possible grâce à la généreuse contribution du gouvernement du Manitoba.

Société de la francophonie manitobaine

Pluri-elles

AJEF Manitoba inc.

Infojustice Manitoba

section 2

Cyberdéfense des corporations : un enjeu de taille

Vigilance et formation comme premier rempart contre la cybercriminalité

Les entreprises et organismes sont des cibles privilégiées de cybercriminels. La raison : elles détiennent un nombre conséquent de données et n'ont souvent pas d'autre choix que de continuer leurs activités, même pendant une cyberattaque. Pour s'en prémunir, des spécialistes recommandent d'agir plutôt en amont, en misant sur une formation adéquate des employés.

Écrit par **Jean-Baptiste GAUTHIER**

Avec l'arrivée de la cryptomonnaie comme moyen de paiement en 2013, les cyberattaques contre les entreprises ont explosé. Les deux techniques les plus utilisées par les cybercriminels sont les rançongiciels et la fraude au président.

« Le nombre de rançongiciels s'est multiplié dans les années 2010, ainsi que leur facilité d'utilisation. Dans la majorité des cas, l'objectif des cybercriminels est de soutirer des données et de l'argent à leurs victimes, explique le fondateur et président d'une entreprise québécoise et conférencier en cyberintelligence, Bertrand Milot.

« Le rançongiciel est un logiciel malveillant ayant pour objectif de se déployer le plus largement possible sur tous les équipements informatiques, pour ensuite récupérer les informations contenues sur les ordinateurs infectés. Son but est également de chiffrer ces informations pour les rendre inutilisables par son propriétaire et de les tenir en otage pour ensuite échanger les clés de déverrouillage contre une rançon.

« Les rançongiciels peuvent être envoyés par le biais d'un lien ou d'une pièce jointe sur le courriel d'un employé de l'entreprise, ou par SMS ou messagerie privée. Cliquer sur ce lien relâche ensuite un logiciel malveillant qui va infecter le réseau de l'entreprise. »

Pour les entreprises, le rançongiciel est d'autant plus inquiétant que lorsqu'un ordinateur appartient à une entreprise, il est connecté à un réseau interne. Si un appareil au sein de l'organisme est compromis, les criminels peuvent donc facilement exploiter les données et les privilèges de l'utilisateur, puis se propager, ou en termes techniques "pivoter", sur d'autres appareils.

Bertrand Milot accorde beaucoup d'attention aux procédés d'approche des cybercriminels, mais souligne que les réactions humaines sont tout aussi importantes que les techniques de cyberdéfense.

« Les techniques cybercriminelles sont nombreuses, mais de manière générale, tout le processus repose sur l'erreur humaine. Une fois que le rançongiciel s'infiltre dans l'entreprise, les cybercriminels peuvent très bien utiliser l'ingénierie sociale pour manipuler un employé, et ainsi récupérer des informations supplémentaires et procéder à un chantage financier. »

Masarah Paquet-Clouston, professeure en cybersécurité à l'École de criminologie de l'Université de Montréal, précise que l'ingénierie sociale est « la manière la plus simple d'infecter

Illustration : RIENNEPRESS - Tanguy Maerten

une entreprise car la plus grande vulnérabilité qui existe, c'est l'humain. On peut avoir les meilleures défenses, les murs les plus hauts, si quelqu'un est là pour ouvrir la porte, ça ne sert à rien ».

Bertrand Milot donne l'exemple d'une entreprise de e-commerce « qui se fait bloquer son système informatique par un rançongiciel la veille de la journée de Noël.

« Étant donné qu'il est important pour cette victime d'exercer son activité dans cette période propice à de nombreuses ventes, le cybercriminel peut aisément utiliser les mécanismes d'angoisse pour obliger l'entreprise à payer une somme d'argent en lui promettant qu'elle retrouvera accès à son support de vente.

« Les rançongiciels ne sont pas forcément l'apanage des plus grands cybercriminels. Ces logiciels malveillants sont facilement procurables sur le *Dark Web* et les kits sont faciles d'utilisation, ce qui permet à de plus petits cybercriminels d'attaquer couramment des entreprises. »

L'exemple de la fraude au président

Une des utilisations les plus courantes de l'ingénierie sociale contre les entreprises se réalise par le biais d'une fraude bien rodée : la fraude au président. C'est un procédé qui exploite le rapport hiérarchique entre un criminel qui se fait passer pour une personne en position d'autorité de l'entreprise ou de l'organisme, et un cadre qui a accès, de par sa fonction, à des données sensibles et confidentielles de l'entreprise.

« Son origine vient d'un escroc franco-israélien, Gilbert Chikli, qui s'est fait passer pour le patron de grandes entreprises françaises pendant 18 mois, entre 2005 et 2006. Son objectif était de demander à des cadres une somme d'argent en prétextant vouloir défendre de bonnes causes, comme la lutte contre le terrorisme », explique Bertrand Milot.

Cette approche a engendré un nombre important de scénarios dérivés, touchant à la fois les entreprises de toutes tailles et les organismes à but non lucratif. Chaque fois, c'est le même *modus operandi* : le cybercriminel usurpe l'identité d'une personne en position d'autorité ou de confiance, afin d'adresser une demande urgente et sous pression à un responsable financier pour transférer des fonds ou effectuer le paiement d'une facture.

« Imaginez-vous être le comptable d'une entreprise. Vous venez d'être contacté par votre institution financière qui vous dit, d'un ton calme et sérieux, que ses applications seront indisponibles pendant plusieurs jours et qu'il vous appelle pour vous aider à vous reconnecter à ses services. La personne vous laisse un numéro de téléphone pour pouvoir vérifier sa bonne information.

« En appelant, vous tombez sur un message automatique identique à la banque de votre entreprise, confirmant ainsi son identité. La personne va ensuite vous convaincre de vous réenregistrer sur le site de votre banque à la suite des problèmes techniques, en vous demandant de fournir à nouveau les accès bancaires de votre entreprise.

« Sans le savoir, vous venez de transmettre les informations de votre entreprise à un cybercriminel utilisant une copie ressemblante de l'interface de votre banque, présentée comme un système de secours. »

Dans ces types de scénarios, les cybercriminels vont venir générer de l'angoisse chez la cible, mais parfois aussi un désir de reconnaissance ou de bienveillance, comme l'explique Akim Laniel-Lanani, directeur de la Clinique de cybercriminologie de l'Université de Montréal.

« Un des scénarios dérivés de la fraude au président est d'exploiter la reconnaissance hiérarchique qu'un nouvel employé peut éprouver dans une entreprise. Son désir d'être reconnu pour son travail peut faire de lui ou elle une cible facile pour les cybercriminels.

- Suite page 34 -

Illustration : RIENNEPRESS - Tanguy Maerten — Photo : Gracieuseté

« L'exploitation de cette situation, associée à une demande urgente de régler une facture reçue par courriel, peut les pousser à ne pas être attentifs à l'adresse de l'expéditeur. Le résultat final étant que l'employé paie une facture fictive et qu'il envoie des fonds à un cybercriminel. »

Protéger son entreprise en formant son équipe

Face à la hausse constante des cyberattaques contre les entreprises, la cybersécurité est devenue un enjeu essentiel du bon fonctionnement d'une structure. L'une des meilleures manières d'augmenter la cyberdéfense de son entreprise est de sensibiliser son équipe à la cybersécurité et aux bonnes pratiques des outils technologiques.

L'humain est une source de vulnérabilité souvent exploitée par les cybercriminels dans une entreprise, comme nous l'avons vu avec l'exemple de la fraude au président. Une méconnaissance des employés des bonnes pratiques de la cyberdéfense expose grandement l'entreprise.

Mieux vaut donc prévenir que guérir. Pour David Décary-Hétu, chercheur et professeur en criminologie à l'Université de Montréal, la solution passe par la formation et la sensibilisation des employés à ces problématiques.

« L'objectif, c'est de pouvoir identifier les menaces plus rapidement pour les minimiser à la source. Les entreprises ont les moyens de lutter, la question c'est de savoir si elles considèrent la cybersécurité comme une priorité. »

Des simulations d'attaques peuvent, par exemple, permettre de détecter les vulnérabilités humaines d'une entreprise. Bertrand Milot mentionne un test simple pour connaître le degré de connaissance des employés en matière de cybersécurité dans une entreprise donnée : déposer une clé USB à côté de la voiture de l'employé située dans le stationnement de l'entreprise.

« Il s'agit d'un test très simple pour voir si un de vos employés va prendre un dispositif étranger et l'utiliser sur son appareil professionnel. En utilisant cette clé USB, cette personne peut mettre en danger son entreprise en mettant en contact un dispositif pouvant être compromis - s'il contient par exemple un rançongiciel - avec un appareil sain de l'entreprise. »

Emeline Manson, formatrice en prévention des fraudes et cybersécurité exerçant au Québec, est aussi d'avis que la sensibilisation des employés et des dirigeants aux diverses menaces est des plus essentielles pour restreindre le succès des attaques des cybercriminels.

« La formation et la sensibilisation des équipes est essentielle, y compris pour ceux et celles qui ont déjà les bons réflexes.

« Cela permet de créer une confiance, pour ensuite propager les bonnes pratiques numériques au sein de l'entreprise », souligne-t-elle.

Emeline Manson conclut en rappelant que les entreprises doivent également se demander si leurs employés ont été assez sensibilisés aux dangers de la cybercriminalité.

« Il arrive trop souvent que les entreprises congédient les employés responsables d'être tombés dans le piège des cybercriminels, mais on peut se demander à quel point leur responsabilité est véritablement engagée. Dans la plupart des cas, l'entreprise n'a pas suffisamment formé et accompagné son employé sur les questions de cybersécurité. »

Illustration : RIENNEPRESS - Tanguy Maerten | Photo : Gracieuseté

Le vol de Données

une industrie à part entière

Le vol de données est monnaie courante dans le milieu du cybercrime. Mais pour les néophytes, il est difficile de s'imaginer les enjeux qui les entourent et ce qu'elles représentent pour les criminels.

Écrit par **Hugo BEAUCAMP**

Dans le monde du cybercrime, le méfait qui revient le plus souvent, c'est le vol de données. Mais de quoi s'agit-il précisément ? En fait, lorsque l'on parle de données, on sous-entend « informations ».

Quant à la nature de ces informations, Fyscillia Ream, coordinatrice scientifique à la Chaire de recherche en prévention de la cybercriminalité à l'Université de Montréal, apporte quelques précisions.

« Il existe plusieurs types de données. Au sein d'une entreprise, il s'agit généralement des informations concernant les employés, comme leur numéro d'assurance sociale, leurs informations bancaires, leur adresse personnelle, leur numéro de téléphone. Finalement, tout ce qu'un individu est susceptible de fournir à son employeur. »

David Décary-Hétu, chercheur et professeur en criminologie à l'Université de Montréal, élabore : « Les délinquants peuvent s'intéresser à différents types de données. Cela dépend de leurs motivations. S'ils cherchent à faire de l'espionnage industriel par exemple, alors les informations personnelles ne sont pas forcément leur priorité. »

Naturellement, si les motivations varient, il en va de même pour les profils. Le professeur en criminologie développe : « Il faut comprendre que tout un script se met en place lorsque l'on parle de vol de données. Certaines personnes sont douées pour s'emparer des données de comptes bancaires, mais elles ne vont pas nécessairement s'y connecter et tenter de faire des transferts frauduleux. Elles vont plutôt vendre ces informations à ceux qui sont spécialisés dans l'exploitation des données. On voit alors toute une chaîne de collaboration qui se met en place entre les délinquants. »

Des crimes plutôt bien organisés

Masarah Paquet-Clouston, professeure en cybersécurité à l'École de criminologie de l'Université de Montréal, parle "d'organisation criminelle".

« Ce n'est pas vraiment une mafia, mais un marché spécialisé, presque une industrie du cybercrime au sein de laquelle les criminels s'échangent des services. »

C'est en cela que les données sont si intéressantes pour les cybercriminels. Qu'importe leur niveau d'expertise dans l'exploitation de ces dernières, une fois acquises, elles ont toujours une valeur monétaire.

« Il existe des magasins automatisés sur lesquels on peut trouver la liste des entreprises infectées, explique David Décary-Hétu. Les informations sont alors disponibles à l'achat sur le site, dans n'importe quel type de cryptomonnaie. Sinon, on peut trouver des forums de discussion sur lesquels les criminels échangent en privé et négocient les prix directement entre eux. »

Au sujet de l'exploitation des données, au-delà de la revente sur le marché noir, les données peuvent être utilisées et détournées par les délinquants de differentes manières. « Les informations récoltées servent parfois dans des affaires d'usurpation d'identité » (voir le témoignage de Marie-Chantal Perron en page 39), raconte Fyscillia Ream qui, en parallèle de son poste à l'Université de Montréal, a également cofondé la Clinique de cyber-criminologie.

Cependant, dans la grande majorité des cas, l'objectif des cybercriminels est de soutirer de l'argent à leurs victimes. Et si les particuliers peuvent aussi

Photos : Gracieuseté

être victimes de rançonnage, les entreprises restent des cibles bien plus intéressantes pour ce type de cyberattaque.

Lorsque les organisations criminelles parviennent à prendre le contrôle total de l'infrastructure en raison de la désuétude de leurs systèmes de défense, « les entreprises sont souvent dans l'obligation de payer une rançon pour retrouver l'accès à leurs systèmes et à leurs données », explique Masarah Paquet-Clouston.

David Décary-Hétu précise que « c'est très rare, mais certaines rançons peuvent atteindre des centaines de millions $ ». (voir article au sujet des rançons en page 19)

La professeure en cybersécurité reprend : « Aujourd'hui, les données des entreprises sont souvent stockées sur ce qu'on appelle des "sauvegardes", qui sont externes au réseau et qui permettent aux organismes de continuer à fonctionner s'ils sont victimes de chiffrement de données.

« Cependant, les cybercriminels se sont également adaptés en compromettant certaines sauvegardes de données, et en menaçant de rendre publiques les informations récoltées. »

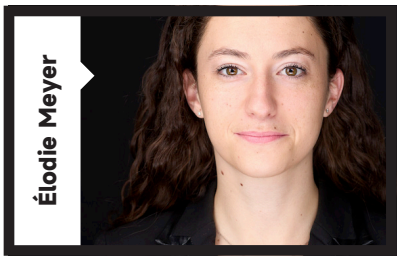
De plus, ce ne sont plus seulement les données de l'entreprise qui peuvent être ciblées, cela peut également être les données de ses employés et de ses clients, comme cela a été le cas pour Marie-Chantal Perron, cliente de la caisse populaire Desjardins lors de la fuite de données en 2019 (voir article en page 39).

On parle alors d'attaques croisées. Citons l'exemple de l'entreprise BRP qui, en 2022, a vu une cyberattaque s'emparer des données personnelles de ses employés, ainsi que de ses fournisseurs. La problématique de la cyberattaque s'étend donc au-delà des entreprises, et la loi a dû s'adapter.

Une loi pour la transparence

La ***Loi fédérale sur la protection des renseignements personnels et les documents électroniques*** (LPRPDE) s'applique aux entreprises privées partout au Canada, à l'exception de trois provinces, « le Québec, l'Alberta et la Colombie-Britannique, où des lois provinciales ont été développées et jugées plus efficaces pour protéger les renseignements personnels. Dans ces provinces, la loi provinciale prend le pas sur la LPRPDE », détaille Me Élodie Meyer, avocate spécialisée en cybersécurité et droit des technologies.

Elle poursuit : « Pour faire simple, la LPRPDE régit le consentement lors de la collecte de données, l'accès à ces données, et les obligations légales des entreprises en cas d'incident de sécurité. » En cas de fuite de données, les compagnies ont donc un certain nombre d'obligations à observer.



Parmi la liste donnée par Me Élodie Meyer, on peut retenir l'obligation d'avertir les personnes concernées par ces vols, mais également de notifier le commissaire fédéral à la protection de la vie privée. À savoir qu'un commissaire provincial est nommé là où la LPRPDE ne s'applique pas.

Illustration : Yahia Lahrech — Photo : Gracieuseté

Mais alors, quelles sont les différences entre la loi fédérale et celles adoptées par les provinces ? « Les obligations à respecter par les compagnies sont sensiblement les mêmes. La principale différence se trouve au niveau des sanctions, et la loi fédérale prévoit des sanctions qui n'encouragent pas son application.

« En effet, certaines entreprises ont réalisé que mettre en place ce qui était requis par la loi leur coûterait plus cher que les sanctions elles-mêmes. Au Québec par exemple, dès septembre 2023, les sanctions pourront aller jusqu'à 10 millions $ voire 25 millions $ si ça relève du pénal. Mais pour le moment, les montants sont compris entre 5 000 $ et 100 000 $. »

Les entreprises sont donc tenues par la loi de protéger à la fois les données de leurs employés, mais aussi celles de leurs clients. En cas d'attaque cependant, elles ne sont pas forcément sanctionnables.

L'avocate explique : « C'est le commissaire à la protection de la vie privée qui va prendre la décision de poursuivre ou pas la compagnie. Les individus concernés peuvent eux aussi poursuivre l'entreprise s'ils subissent un préjudice, encore faut-il prouver que la compagnie est responsable des actes ayant causé ce préjudice. » C'est alors qu'intervient la notion d'omission et de négligence.

Les niveaux de négligence

Me Élodie Meyer détaille : « Il existe différents niveaux de négligence : on parle de "négligence simple" ou "grossière", ou de "faute lourde", tout dépend de la gravité de l'omission.

« Par exemple, si pour des raisons pratiques une compagnie se sépare de ses mesures de sécurité, on entre dans le cadre de la faute lourde. En revanche, si une attaque cybercriminelle est un succès car la mise à jour des systèmes de protection n'a pas été faite, alors on peut parler de simple omission.

« C'est assez compliqué de prouver qu'il y a eu négligence. Les victimes dont les données ont fuité doivent prouver qu'elles ont bien subi un préjudice et que c'est de la faute de l'entreprise. Et ça, c'est très difficile à démontrer. »

À ce propos, Bertrand Milot ajoute : « Surtout qu'il est parfois difficile de retracer les données exfiltrées. Lorsque des données sont volées, elles sont ensuite corrélées à d'autres données et d'autres méfaits contre d'autres victimes. »

Finalement, même si les entreprises font leur maximum pour protéger au mieux les données qu'elles ont en leur possession, force est de constater que cela ne suffit pas toujours. En effet, les techniques de cyberattaque pour l'obtention de données sont très nombreuses et, de manière générale, le processus repose souvent sur l'erreur humaine.

Un vol d'identité aux RÉPERCUSSIONS MULTIPLES

Marie-Chantal Perron, jeune Montréalaise travaillant dans la stratégie marketing, a vu son identité et ses informations bancaires utilisées pour lui extorquer de l'argent mais aussi déposer en son nom des demandes d'aides gouvernementales illégales.
En 2019, le groupe financier Desjardins subit un vol important de données personnelles et confidentielles de plus de 2,7 millions de ses membres et clients. Elle en faisait partie.

Photo : Gracieuseté

■ En août 2021, Marie-Chantal Perron voit son identité et ses informations bancaires exploitées par des cybercriminels.

Écrit par **Jean-Baptiste GAUTHIER**

En août 2021, Marie-Chantal Perron découvre avec surprise que deux transactions financières étrangères d'un montant d'une centaine d'euros ont été effectuées avec sa carte de crédit. En contactant sa banque américaine Capital One pour bloquer les opérations, elle découvre la triste réalité.

« Quand j'ai voulu déclarer la fraude, on m'a signalé qu'il n'y avait rien d'anormal dans ces deux transactions financières, car elles avaient été validées avec mes renseignements personnels. La banque avait appelé mon numéro et je leur avais renseigné mon nom, mon adresse et ma date de naissance, ce qui était bien évidemment faux.

« J'ai lancé un appel sur Facebook et j'ai été contactée par Emeline Manson, formatrice en prévention des fraudes et cybersécurité exerçant au Québec, qui m'a signalé que j'avais sûrement eu affaire à un vol d'identité. Je sais maintenant que son origine vient du fait que ma carte de crédit Capital One était liée à mon compte Desjardins, le groupe financier victime d'une grande fuite des données, en 2019 ! », s'exclame-t-elle.

Mais Marie-Chantal Perron n'est pas au bout de ses surprises. En demandant une aide financière au gouvernement canadien destinée aux travailleurs indépendants, *la Prestation canadienne de la relance économique*, on lui signale que sa requête est impossible car elle vient déjà de démarrer une demande de chômage.

« Un cybercriminel a utilisé mon dossier et mes renseignements pour réaliser cette demande en mon nom. Or, on ne peut pas cumuler deux demandes d'aide à la fois. Il faut savoir que la pandémie de COVID-19 a grandement affecté mon activité professionnelle. J'ai perdu beaucoup de contrats avec mes clients et en septembre 2021, je me suis retrouvée en grande nécessité de ressources financières. »

La jeune Montréalaise réussit à joindre le gouvernement et à bloquer la demande effectuée par les cybercriminels. Mais alors qu'elle cherche à reprendre le contrôle de son identité, débute une longue période de neuf mois où les services du gouvernement canadien se trouvent incapables de régler sa situation.

Illustration : Yahia Lahrech

Des administrations gouvernementales peu réactives

« J'ai commencé à contacter les services appropriés du gouvernement fédéral, et il s'est avéré que le Régime d'assurance emploi et l'Agence du revenu du Canada n'arrivaient pas, entre eux, à régulariser mon dossier en annulant la candidature malveillante de chômage, tout en acceptant ma demande d'aide financière.

« Dans les cas d'un vol d'identité numérique, je trouve cela ridicule que le gouvernement ne fasse pas preuve de collaboration et de rapidité. J'ai pu seulement toucher cette aide financière en février 2022. Les enjeux de la cybercriminalité ne sont pas encore compris par nos dirigeants politiques », regrette Marie-Chantal Perron.

« Je n'ai même pas tenté de joindre la police pour m'aider dans cette affaire. Inconsciemment, je me suis persuadée qu'ils ne m'aideraient pas assez vite, alors j'ai décidé de gérer mon vol d'identité toute seule. »

Depuis cette mésaventure, la jeune femme a pris de nouvelles dispositions de sécurité.

« Je me suis inscrite à un service de contrôle de crédit, Equifax, qui sollicite un contrôle important de mon identité à chaque transaction bancaire.

« De plus, le gouvernement fédéral a enfin réussi à associer mon numéro d'assurance sociale à un *red flag*. Dès que mon identité doit être contrôlée, je reçois un appel du gouvernement qui me demande de répondre à plusieurs vérifications importantes », explique-t-elle.

Au moment d'écrire ces lignes, Marie-Chantal Perron ne savait toujours pas si son identité était finalement sécurisée.

« Depuis la fin de 2021, mon nom et mes informations personnelles n'ont pas été utilisés par les malfaiteurs. Mais je n'ai aucune certitude pour l'avenir. Emeline Manson m'a alertée sur le fait que malgré la mise en place de mesures de protection, il y aura toujours un petit risque que mon identité soit un jour réutilisée par un cybercriminel », souligne-t-elle.

Pas de quoi décourager la jeune Montréalaise, pour qui l'argent ne doit pas être une priorité dans la vie. « Je relativise en me disant que mon identité aurait pu être utilisée pour des crimes beaucoup plus graves que des fraudes financières, conclut Marie-Chantal Perron. Je ne suis pas quelqu'un qui vit dans le passé, alors oui, je suis beaucoup plus vigilante qu'auparavant, mais j'ai juste décidé de continuer à vivre pleinement ! »

POUR SE PROTÉGER D'UN VOL D'IDENTITÉ, PLUSIEURS CONSEILS ET SOLUTIONS SONT IMPORTANTS À CONNAÎTRE :

- Consultez et contrôlez vos factures et relevés bancaires de manière régulière, au minimum une fois par mois, pour y détecter toute opération suspecte.
- Optez pour une double authentification pour vos comptes personnels, comme un mot de passe associé à une vérification de vos données biométriques sur une application de votre téléphone cellulaire.
- Détectez les signes de fraude ou de vol d'identité en vous abonnant à un service de surveillance de vos opérations de crédits, comme Equifax ou TransUnion.
- Créez des mots de passe complexes et uniques pour protéger l'accès à vos comptes sur les applications et les sites Internet. Un gestionnaire de mot de passe est également envisageable pour centraliser et sécuriser vos méthodes d'authentification. Par exemple 1Password, une compagnie canadienne, propose des abonnements familiaux à environ 5,99 $ par mois pour les familles de cinq personnes. D'autres applications telles que Bitwarden l'offrent gratuitement avec leur plan de base.
- Évitez d'ouvrir et de cliquer sur des liens intégrés à des messages ou des courriels dont vous ignorez la provenance et la fiabilité de l'expéditeur.
- Limitez les informations et les photos que vous partagez sur vous et votre famille sur vos réseaux sociaux. Ils pourraient vous nuire et être exploités par des cybercriminels.
- Évitez de sauvegarder vos informations personnelles ou professionnelles sur votre navigateur web comme vos mots de passe, vos informations bancaires ou votre adresse.
- Déchiquetez tous les documents physiques qui contiennent des informations personnelles avant de les mettre au recyclage.
- Assurez-vous que votre système informatique soit muni d'un antivirus. Pour une utilisation classique d'Internet, un antivirus gratuit comme Windows Defender peut faire l'affaire, à condition que la fonction mise à jour automatique soit activée pour votre appareil et les logiciels installés.

Hacking
le parcours du combattant d'une PME montréalaise

Cibles privilégiées des hackers, nombreux sont les entrepreneurs canadiens qui souffrent dans le silence. La propriétaire d'une petite entreprise montréalaise a bien voulu partager son témoignage avec *La Liberté*.

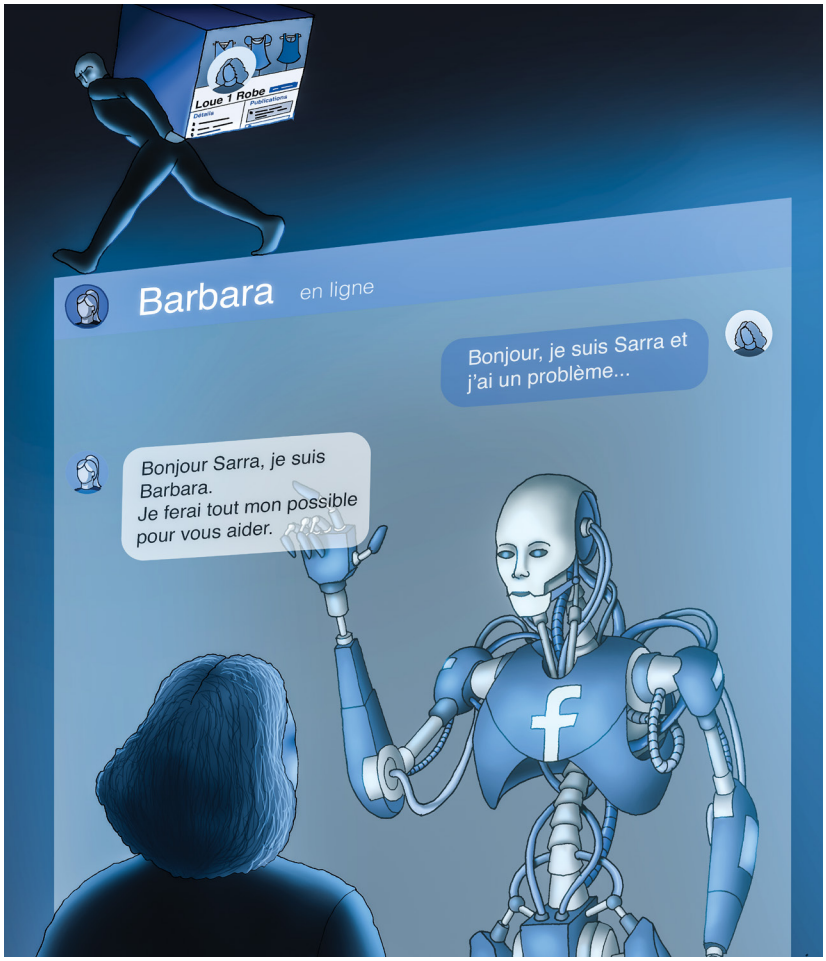


Illustration : RIENNEPRESS - Tanguy Maerten

Écrit par **Mehdi MEHENNI**

Rien ne prédestinait Sarra Ghribi, propriétaire de la PME montréalaise Loue 1 Robe, une boutique qui propose des robes de mariage, de bal ou autres grandes occasions à la location, à un tel parcours de combattante. Juillet 2021 tirait à sa fin et la pandémie enregistrait un recul.

La jeune entrepreneure avait alors grand espoir de voir une reprise de son activité commerciale. « Je pensais que j'allais enfin sortir la tête de l'eau, avec la reprise des mariages », lance-t-elle avec un grand soupir.

Peine perdue. Au même moment, à des milliers de kilomètres du Canada, au fin fond de l'Asie du Sud, un hackeur avait décidé de bouleverser l'existence de Sarra Ghribi, et ses affaires aussi.

« J'ai reçu une alerte m'indiquant qu'un individu basé en Inde tentait de récupérer la page facebook de ma PME. Et il a finalement réussi à le faire ! », s'exclame-t-elle.

Puisque le compte Facebook personnel de Sarra Ghribi, le compte Instagram de Loue 1 Robe et sa carte de crédit étaient tous reliés à la page, le hackeur a tout récupéré, en plus d'avoir extorqué une somme de 750 $. La banque a remboursé le montant subtilisé, mais pour les réseaux sociaux de l'entreprise, Sarra Ghribi a dû entamer des procédures à n'en plus finir. En vain.

« J'ai adressé des dizaines de correspondances à l'administration Facebook, j'ai envoyé des copies de mes documents d'identité, j'ai mis à leur disposition mes données personnelles, mais sans succès », déplore-t-elle.

Elle affirme que ce sont des robots se nommant tantôt "Sophie", tantôt "Barbara", ou autre, qui lui répondaient. Sans jamais savoir ce qui allait advenir des copies de ses documents d'identité.

Après avoir pris sept années pour cumuler une communauté de plus de 20 000 abonnés entre la page Facebook et le compte Instagram de Loue 1 Robe, et avoir acheté, pendant au moins six années, de la publicité au géant des réseaux sociaux, l'entrepreneure est alors effondrée.

« À partir du moment où je débourse un dollar, je suis en droit de faire des réclamations. Facebook gagne assez d'argent pour mettre à la disposition de ses utilisateurs et de ses clients un personnel capable de prendre en charge leurs doléances », proteste-t-elle.

Le coup de gueule

Sur le moment, et ne voyant pas de réponse favorable venant de Facebook, Sarra Ghribi, qui avait perdu un tiers des rendez-vous pris par les clients sur sa page Facebook, a décidé de tout reprendre à zéro. Facebook étant son outil de travail principal, elle a lancé une nouvelle page. Résultat : deux mois après, le volume de sa nouvelle communauté ne franchissait guère la barre des 300 abonnés, le chiffre d'affaires de l'entreprise ne cessait de baisser, et les revenus avaient chuté de moitié environ. « Un désastre », commente-t-elle.

En dernier recours, l'entrepreneure a pris sur elle de faire éclater l'affaire au grand jour. À travers un coup de gueule largement relayé sur les réseaux sociaux, notamment sur LinkedIn, des médias commencent à s'intéresser à l'histoire.

Surprise. Dans les trois heures qui ont suivi le passage de la propriétaire de Loue 1 Robe à la télévision, le compte Instagram de son entreprise lui est restitué. Quinze jours plus tard, elle récupère également la page Facebook, mais jamais son compte personnel.

« Ma peine est double. Mon oncle est en train de mourir d'un cancer et tous mes souvenirs avec lui, que ce soit des photos, des vidéos, des blagues ou des chansons, étaient sur mon compte personnel. C'est perdu à jamais », regrette-t-elle.

Quand Sarra Ghribi a annoncé la récupération de ses médias sociaux, beaucoup d'entrepreneurs l'ont contactée pour partager avec elle leurs expériences. Leur désarroi, surtout. Certains lui ont même demandé de l'aide, à l'exemple d'un jeune producteur de miel qui s'était fait pirater les réseaux sociaux de sa PME.

« Je n'ai pas pu les aider. Moi-même je n'aurais rien pu faire si les médias traditionnels ne s'étaient pas saisis de l'affaire », reconnaît-elle.

Le constat de Sarra Ghribi est donc sans appel : nombreux sont les entrepreneurs qui souffrent dans la solitude et dans le silence, par peur ou par honte, quand ce n'est pas par manque d'accompagnement. Elle l'a appris à ses dépens.

LE BON RÉFLEXE

Écrit par
Hugo BEAUCAMP

Laura Hawkins est la propriétaire d'un escape game à Winnipeg. Victime d'une histoire similaire, elle a eu le bon réflexe.

Lors d'un voyage d'affaire, elle réalise que quelque chose ne va pas sur sa page Facebook professionnelle (7 000 abonnés). Elle vient de se faire hacker.

Dans ce cas de figure, aucune tentative d'extorsion ou d'arnaque, les coupables ont simplement posté des messages laissant sous-entendre que l'entreprise était en train de mettre la clef sous la porte.

« J'étais complètement dévastée, se souvient-elle. Ça m'a rendu malade, mon intimité avait été violée, j'avais perdu le contrôle et j'étais impuissante. »

Pour s'être déjà heurtée à un mur par le passé, Laura Hawkins n'envisage même pas de se tourner vers Facebook pour obtenir de l'aide.

Elle a eu le bon réflexe. Elle s'est rapprochée directement d'un professionnel en cybersécurité, Hernán Popper, dirigeant d'une entreprise manitobaine de cybersécurité. Ce dernier a pu récupérer l'accès à son compte professionnel assez vite pour éviter que sa compagnie ne souffre de sérieux dommages.

« On a eu beaucoup de chance, explique Hernán Popper. Les options pour retrouver l'accès au compte commençaient à se faire mince. Mais il s'est avéré que la reconnaissance faciale était activée sur le téléphone de Laura Hawkins. Nous avons donc pu la reconnecter à son compte et rapidement changer le mot de passe, déconnectant ainsi le hacker. »

Un CYBERCRIMINEL presque voisin

Victime d'un piratage de son compte Google, Marie-Luce (1), une jeune Montréalaise, a souvent dû se défendre seule. Elle a même été jusqu'à identifier et rencontrer physiquement le cybercriminel qui l'avait attaquée et vivait proche de son domicile.

Écrit par **Jean-Baptiste GAUTHIER**

Marie-Luce a lancé son entreprise de traduction en décembre 2020 et sauvegardé ses informations personnelles sur son compte Google. Compte qui sera piraté quelques mois plus tard.

« Je pensais mon système sécuritaire jusqu'à ce que je remarque trois transactions frauduleuses réalisées avec mon compte PayPal le 5 mai 2021. Je me suis empressée de faire annuler ces opérations avec ma banque, mais quelques jours plus tard, tous mes comptes bancaires personnels et professionnels étaient victimes d'un piratage, et mes comptes épargne avaient été vidés d'un total de 10 000 $ », se souvient Marie-Luce.

La jeune femme commence alors à paniquer et à rechercher le cybercriminel qui lui a extorqué de l'argent. « Je m'aperçois très vite que l'une des trois premières transactions frauduleuses sur PayPal est au nom d'une personne vivant à Montréal, comme moi. » C'est pour Marie-Luce l'ouverture de la boîte de Pandore.

« En retraçant son adresse IP et ses mouvements sur ses réseaux sociaux, je m'aperçois que cette personne m'observe depuis plusieurs jours et qu'elle a vérifié la localisation de mon domicile avec l'application Google Maps », s'inquiète-t-elle.

Au moment où Marie-Luce retrace le fil de ces opérations malveillantes, elle se rend compte que tous ses mots de passe ont été changés et qu'elle n'a plus accès à ses différents comptes.

« J'étais vraiment effrayée de voir ma vie entre les mains d'un cybercriminel qui habitait si proche de chez moi », se remémore-t-elle.

Besoin de preuves ou de contact

Dès qu'elle commence à détenir des informations sur le malfaiteur, Marie-Luce décide de contacter la police de Montréal pour monter un dossier de fraude.

« Au départ, ils m'ont clairement signalé qu'ils ne pouvaient pas considérer mon dossier et que la police ne pouvait pas gérer le trop grand nombre d'affaires comme la mienne. Une façon de me dire qu'ils étaient débordés et que mon dossier ne serait jamais traité à temps, sauf avec la présence de preuves évidentes ou d'un contact physique entre le criminel et moi. »

Il n'en fallait pas plus à Marie-Luce pour tenter de rentrer en contact avec le fraudeur et permettre ainsi l'intervention des forces de l'ordre. « En observant les transactions frauduleuses sur mon compte bancaire, j'ai remarqué que le cybercriminel était en contact avec une entreprise de réparation de voitures. »

La jeune femme décide alors de contacter l'entreprise et lui explique la nature malveillante du cybercriminel. « L'entreprise a été très bienveillante avec moi. Grâce à elle, j'ai pu organiser un faux rendez-vous qui a poussé le cybercriminel à venir sur place le 7 mai 2021, soit seulement deux jours après le début des transactions frauduleuses, raconte-t-elle.

« Pendant la rencontre entre l'entreprise et le criminel, j'ai attendu seule, cachée dans ma voiture, la peur au ventre, en m'attendant au pire. J'aperçois alors un jeune homme que je n'imagine même pas majeur. Un gamin qui m'avait démontré dans les dernières heures qu'il n'avait pas entièrement conscience de ce qu'il faisait. D'où ma facilité d'accéder à ses informations sur ses réseaux sociaux. Les cybercriminels ne sont pas tous des as de la cyberdéfense! », ironise Marie-Luce.

Partie d'un réseau ?

« Quand le contact physique est établi entre l'entreprise et le malfaiteur, je décide d'appeler la police en leur expliquant que je viens juste de leur transmettre un dossier de fraude et que le jeune cybercriminel est devant moi. Ils décident alors d'intervenir et l'adolescent est placé en garde à vue pendant 24 heures.

« J'apprends alors qu'il est effectivement mineur. La police prend également mon témoignage en me disant que les parents du jeune criminel vont venir le chercher et qu'il va être relâché. On me signale qu'il fait potentiellement partie d'un réseau plus grand que lui, mais la police n'a aucune preuve de cette affirmation. »

À la sortie de cette rencontre, Marie-Luce se sent déçue et frustrée de la gestion de cette affaire par les forces de l'ordre.

Durant les jours suivants, la jeune femme voit ses informations bancaires être de nouveau utilisées pour tenter de lui extorquer de l'argent, dans différents coins du Canada. « Je n'avais aucun moyen de savoir si cela venait de lui ou de son réseau. Cela a été une période de stress intense », explique-t-elle.

Des délais judiciaires trop longs

Marie-Luce a décidé de transmettre au jeune cybercriminel une lettre de mise en demeure le 21 juin 2021 avec un avocat. Mais pour poursuivre le fraudeur et lancer officiellement l'action en justice, encore faut-il avoir en sa possession les preuves rassemblées par les forces de l'ordre.

« Pratiquement un an plus tard, la police m'a rappelée en me signalant que mon dossier allait enfin être traité et que les enquêteurs l'avaient ouvert pour la première fois le 14 avril 2022, déplore-t-elle.

« Je ne veux pas taper sur le système judiciaire et sur la police, mais je ne crois pas me tromper

Illustration : Yahia Lahrech

en disant que nous sommes dépassés par la malveillance de la cybercriminalité. Mes poursuites judiciaires sont encore en attente auprès de mon avocat, le temps que la police finisse son rapport. »

Le problème, c'est qu'au Canada, dans le cas d'affaires judiciaires comme celle de Marie-Luce, les poursuites criminelles ont un délai de prescription d'un an et les poursuites civiles de trois ans.

« Mon avocat m'a signalé que j'allais avoir du mal à obtenir des dommages et intérêts. Le délai des poursuites criminelles est déjà dépassé, et le temps que les preuves soient rassemblées, il est plus que probable qu'il y ait aussi prescription pour les poursuites civiles », regrette-t-elle.

Des mesures de protection qui ne soulagent pas sa peur

Marie-Luce a pu se faire rembourser toutes les transactions frauduleuses réalisées en son nom avec ses informations bancaires. La jeune femme a également mis en place des mesures de protection importantes pour protéger son identité et ses données :

« J'ai souscrit un abonnement à des services de contrôle de crédit, Equifax et TransUnion. Ces organismes de surveillance contrôlent toutes vos opérations financières en vous appelant pour vérifier l'origine des transactions. Je peux vous dire que durant les premiers mois, cela sonnait souvent à la maison ! J'ai également augmenté la sécurité de mon système informatique et j'ai maintenant un pare-feu efficace », explique la jeune femme.

Malgré ces initiatives, Marie-Luce a pourtant été victime d'une autre tentative d'intrusion par courriel, en mai 2022.

« Je sais que mes données ont été partagées sur le *Dark Web*, donc il faut que je me fasse à l'idée d'être attaquée à tout moment à l'avenir. Mais je trouve cela très difficile… Je me sens résignée et désabusée », déplore Marie-Luce, avec tristesse.

Elle conseille à toutes les personnes de prendre conscience de la vulnérabilité de leurs informations personnelles sur Internet.

« Nous pensons toujours que cela arrive juste aux autres, mais la réalité, c'est que nous sommes tous des cibles relativement faciles pour les cybercriminels. Maintenant, les cybercriminels peuvent même outrepasser la reconnaissance faciale que nous utilisons pour déverrouiller nos comptes bancaires. D'ailleurs, c'est comme ça que mon agresseur a pu s'identifier auprès de ma banque, en montrant mon visage ! », conclut Marie-Luce. (Voir encadré les risques de l'utilisation de nos données biométriques.)

(1) Seul le prénom Marie-Luce est donné pour protéger l'anonymat de la victime.

LES RISQUES DE L'UTILISATION DE NOS DONNÉES BIOMÉTRIQUES

Les données biométriques sont de plus en plus utilisées dans notre quotidien, notamment avec la grande utilisation des téléphones intelligents où des capteurs d'empreinte et de reconnaissance vocale sont utilisés pour déverrouiller l'utilisation de l'appareil.

Il en va de même pour certaines applications bancaires qui utilisent la reconnaissance faciale pour une bonne authentification de leurs clients.

Mais ces données biométriques peuvent aujourd'hui être contrefaites et utilisées par des cybercriminels. Par le biais de l'intelligence artificielle, la technologie du *deepfake* permet notamment de recréer un visage et une voix identiques à une personne à partir d'une quantité suffisante de ses photos et vidéos partagées en ligne, notamment sur ses réseaux sociaux.

Après le vol des données, les cybercriminels peuvent alors utiliser ce montage facial et vocal pour s'authentifier sur les applications bancaires de leur cible, comme cela a été le cas dans l'histoire de Marie-Luce.

Les données biométriques sont un outil de verrouillage utile, mais qui reste vulnérable. Il est donc toujours important d'opter pour une authentification à deux facteurs, comme associer une protection par mot de passe avec une authentification par empreinte digitale, qui est la protection biométrique la plus sécurisée aujourd'hui.

Clinique de
Cyber-Criminologie

Victime de cybercriminalité ? contactez-nous.

Nous offrons des services GRATUITS aux victimes ainsi qu'à leurs proches.

Vous avez besoin...

→Informations, conseils pratiques et techniques

→Assistance pour porter plainte à la police

→ Guide vers les bonnes ressources

Victime de fraude ?

Partagez votre histoire avec la communauté !

www.fraude-alerte.ca

Suivez-nous !

Écrivez-nous !

info@clinique-cybercriminologie.ca

CRPC | Chaire de recherche en prévention de la cybercriminalité

www.clinique-cybercriminologie.ca

Université de Montréal

LE PRIX À PAYER POUR SA CYBERSÉCURITÉ

S'il est impossible pour une entreprise de prévoir le coût d'une solution réparatrice en cas d'attaque cybercriminelle, les experts s'accordent à dire qu'un budget alloué à la prévention en cybersécurité peut réduire drastiquement le risque de perdre gros.

Écrit par **Hugo BEAUCAMP**

Les entreprises sont des proies de choix pour les cybercriminels. Elles sont donc les premières concernées par les questions de défense. Comme tous les services, la réponse à un incident de cybersécurité a un coût.

Un coût difficile à évaluer, comme l'explique William Georges Khouri, architecte en cybersécurité au sein d'une compagnie spécialisée en cyberintelligence : « Les prix vont dépendre du temps que nous prend l'intervention, mais aussi du périmètre sur lequel nous devons intervenir ».

Le "périmètre" est la surface d'intervention, c'est-à-dire le nombre d'appareils mais aussi les serveurs et réseaux qui doivent être défendus.

« En cas d'attaque, une entreprise qui n'a pas été préparée, tant au niveau de la prévention que de la protection et du recouvrement, pourrait ne pas s'en relever. Les interventions suite à une cyberattaque peuvent durer plusieurs semaines et coûter entre 200 000 $ et 500 000 $ pour une PME, et jusqu'à plusieurs millions $ pour une grosse entreprise. »

William Georges Khouri poursuit : « Si l'entreprise n'a pas les outils de sécurité de nouvelle génération nécessaires pour avoir suffisamment de visibilité sur l'environnement et les actions des cybercriminels, alors tout l'environnement compromis doit être remonté car c'est plus sécuritaire. Mais c'est aussi plus coûteux. »

Prévenir vaut mieux que guérir

En tout cas, une chose est sûre, quitte à payer, mieux vaut le faire en amont. Une fois de plus, difficile de détailler la répartition d'un budget de cybersécurité car là encore, de nombreux facteurs entrent en compte. Notamment la taille et le type de l'entreprise, mais aussi le type de données que celle-ci récolte.

« De manière générale, j'estime qu'entre 1 et 3 % du budget IT d'une entreprise devrait être consacré à la prévention », explique l'expert.

Beaucoup de compagnies se voilent encore la face sur les risques de cyberattaques et pensent que cela n'arrive qu'aux autres. L'architecte en cybersécurité se remémore l'histoire d'une réponse à incident qu'il a vécue récemment.

« Cette entreprise avait été abordée par une compagnie de sécurité qui avait recommandé l'installation d'un antivirus de nouvelle génération, aussi appelé EDR [détection et réponse des points d'accès]. La protection aurait coûté environ 1 000 $ à l'entreprise. Elle a refusé.

« Un mois après, la compagnie a été victime d'un rançongiciel qui l'a complètement encryptée, y compris ses sauvegardes.

Entre les coûts de consultation de compagnies de sécurité, le rachat et l'installation de matériel, ainsi que les pertes d'exploitation, ça lui a coûté 700 000 $! »

Photo : Gracieuseté

Le prix moyen d'un antivirus nouvelle génération (EDR) efficace se situe entre 30 $ et 80 $, par an, par employé et par machine. À noter que l'efficacité d'un antivirus est grandement liée à sa configuration, et que le prix total est toujours relatif au périmètre à défendre.

Quant à la raison pour laquelle ces antivirus relativement onéreux sont à privilégier aux antivirus classiques gratuits, c'est parce qu'ils offrent un tout autre niveau de protection.

« Aujourd'hui, on estime que 100 millions de nouveaux *malwares* sont créés tous les ans, poursuit William Georges Khouri. Les nouveaux antivirus dits EDR se basent sur le fonctionnement des logiciels malveillants et sont capables de détecter les comportements malicieux ou les caractéristiques d'un rançongiciel, par exemple. Ils couvrent un bon nombre des nouvelles vulnérabilités et des nouveaux virus. »

Illustration : Envato.com

Article sponsorisé

Ne mordez pas à l'hameçon ! Comment vous protéger contre l'hameçonnage ?

Au cours des six premiers mois de 2020, plus de 30 % des Canadiens ont subi une attaque par hameçonnage. Elles se sont multipliées pendant la pandémie alors que les cybercriminels ont exploité les angoisses et besoins des Canadiens. Ces attaques sont toujours monnaie courante, il faut rester vigilant.

- Par Diane Amato

La cybercriminalité est en hausse au Canada, ciblant les particuliers, les familles et les entreprises. Voilà pour la mauvaise nouvelle. Heureusement, assurer sa cybersécurité n'est pas si complexe. La clé : savoir comment empêcher les pirates informatiques et les escrocs d'accéder à ses systèmes et à ses comptes. Notre série Cybersécurité 101 vise à vous donner des outils et des conseils de base pour vous protéger, vous, votre famille et vos données dans le monde numérique.

Au fil des ans, les cybercriminels recourent à des méthodes de plus en plus sophistiquées, ce qui rend la détection des tentatives d'hameçonnage plus difficile. Néanmoins, il existe des moyens simples de se protéger contre les attaques par hameçonnage.

Qu'est-ce que l'hameçonnage ?

L'hameçonnage est une pratique qui consiste à envoyer des courriels, des messages textes ou des messages sur les médias sociaux qui semblent provenir d'entreprises réputées.

L'objectif est de vous inciter à fournir des renseignements personnels comme des mots de passe ou des numéros de carte de crédit. Souvent, les attaques par hameçonnage contiennent :

- Une menace qui vous vise (p.ex. « La police est en route » ou « Vous allez recevoir une amende du gouvernement »).
- Une récompense financière (p.ex. « Vous avez gagné un voyage gratuit »), ou
- Un message selon lequel votre aide est requise (p.ex. « Je ne peux pas utiliser ma carte de crédit, peux-tu m'acheter une carte-cadeau » ou « Peux-tu me donner ton numéro de carte de crédit pour que je puisse réserver un billet et rentrer à la maison »).

Comment vous protéger contre l'hameçonnage

Si les courriels, messages textes et autres messages peuvent sembler provenir d'une source légitime, il est possible de détecter une fraude avec un examen approfondi du contenu.

Voici quelques indices et conseils pour vous protéger des fraudes :

- **Prenez un moment pour réfléchir avant d'ouvrir** et de répondre à un courriel inattendu. Suivez votre instinct. Si quelque chose ne vous semble pas normal, il vaut mieux prendre un moment pour évaluer la situation. Il est possible que le message provienne d'une personne avec laquelle vous ne communiquez pas souvent par courriel ou par message texte. Peut-être que l'usage inhabituel d'un mot dans le message vous semble étrange. Vous avez peut-être été informé que le compte avec lequel vous visionnez des films et des émissions de TV est bloqué, alors que vous l'utilisiez encore la veille.
- **Passez un appel pour vérifier les demandes**. Comme les attaques par hameçonnage semblent provenir d'une personne que vous connaissez, il est préférable de la contacter par un autre moyen pour confirmer l'origine du message. Par exemple, si cette personne vous a envoyé un courriel, appelez-la ou envoyez un message texte au numéro que vous avez déjà, mais ne répondez pas au message que vous avez reçu.
- **Vérifiez si le texte comporte des erreurs de grammaire** ou d'orthographe et si le langage est inhabituel. Il n'y a généralement pas d'erreurs dans les messages provenant d'entreprises réputées.
- **N'ouvrez jamais de pièces jointes que vous ne vous attendiez pas à recevoir**. Il est possible que vous receviez une facture « en attente de paiement » ou un bon pour un produit gratuit. Ces pièces jointes peuvent contenir des programmes/virus (logiciels malveillants) ou des liens vers de faux sites Web, il ne faut donc pas cliquer dessus.
- **Ne donnez aucun renseignement personnel ou confidentiel**. Si une institution financière, une société de télécommunications ou toute autre entreprise peut communiquer avec vous par courriel ou message texte, elle n'inclura jamais un lien pour mettre à jour vos renseignements sur le paiement ou vos coordonnées bancaires.

Cet article a été initialement publié sur le portail Découverte et apprentissage de RBC. *decouverte.rbcbanqueroyale.com*

section 3

Tous Ensemble CONTRE la cybercriminalité

Les drapeaux rouges de la malveillance

Les cybercriminels misent sur les failles psychologiques de tout être humain, notamment le sentiment d'urgence, l'excès de curiosité et la cupidité, pour accéder aux informations et données de leurs victimes. Il est donc essentiel de bien reconnaître et comprendre ces mécanismes émotifs humains qui sont liés à l'utilisation des technologies numériques, afin de limiter notre vulnérabilité.

Écrit par **Jean-Baptiste GAUTHIER et Camille HARPER**

Emeline Manson, formatrice en prévention des fraudes et cybersécurité exerçant au Québec, identifie le sentiment d'urgence comme l'une des émotions dont les cybercriminels se jouent souvent. Un sentiment qui peut toucher tout le monde.

« Quand vous consultez vos courriels et que vous y trouvez un lien ou une pièce jointe qui demande d'envoyer une information vitale, ceci vous amène souvent à ressentir un sentiment d'urgence. *Que va-t-il se passer si je ne réagis pas ?* »

Cette peur et cette culpabilité d'ignorer un acte qui aurait pu être important, ce sont justement, selon l'experte, les types d'émotions fortes que les cybercriminels exploitent.

Le sentiment d'urgence n'a d'ailleurs pas besoin d'être négatif pour constituer une porte d'entrée aux cybercriminels.

Parfois, les individus sont victimes de leur bienveillance. « La plupart du temps, la personne est contactée par un ami, un membre de sa famille ou un collègue, qui lui demande de lui rendre un service souvent monétaire. Sauf que sans s'en apercevoir, elle parle en fait à un cybercriminel », prévient Emeline Manson.

La curiosité

La curiosité naturelle de l'être humain est un autre obstacle à une bonne hygiène numérique. La formatrice en prévention des fraudes et cybersécurité explique : « L'être humain est tellement curieux qu'il va porter attention à toutes les choses qui lui paraissent étranges ou qu'il ne peut pas contrôler.

« Prenez les quiz sur Facebook par exemple. Ce sont souvent des cyberattaques déguisées qui poussent les gens à donner leurs informations personnelles, et les gens le font car ils sont curieux de savoir s'ils ont bien répondu aux questions. C'est un moyen très simple pour les cybercriminels de récupérer des informations personnelles en grand nombre, puis de les exploiter pour réaliser une fraude ou un vol d'identité », prévient Emeline Manson.

Parfois même, l'être humain est conscient du danger mais il se convainc par curiosité qu'il peut être ignoré. À tort. Emeline Manson se souvient d'une anecdote :

« Un ami avait reçu un lien bizarre dans un courriel. Il savait très bien que c'était étrange, mais il m'a demandé s'il pouvait quand même l'ouvrir avec son cellulaire, pour vérifier. Il arrive

Illustration : RIENNEPRESS - Tanguy Maerten — Photo : Gracieuseté

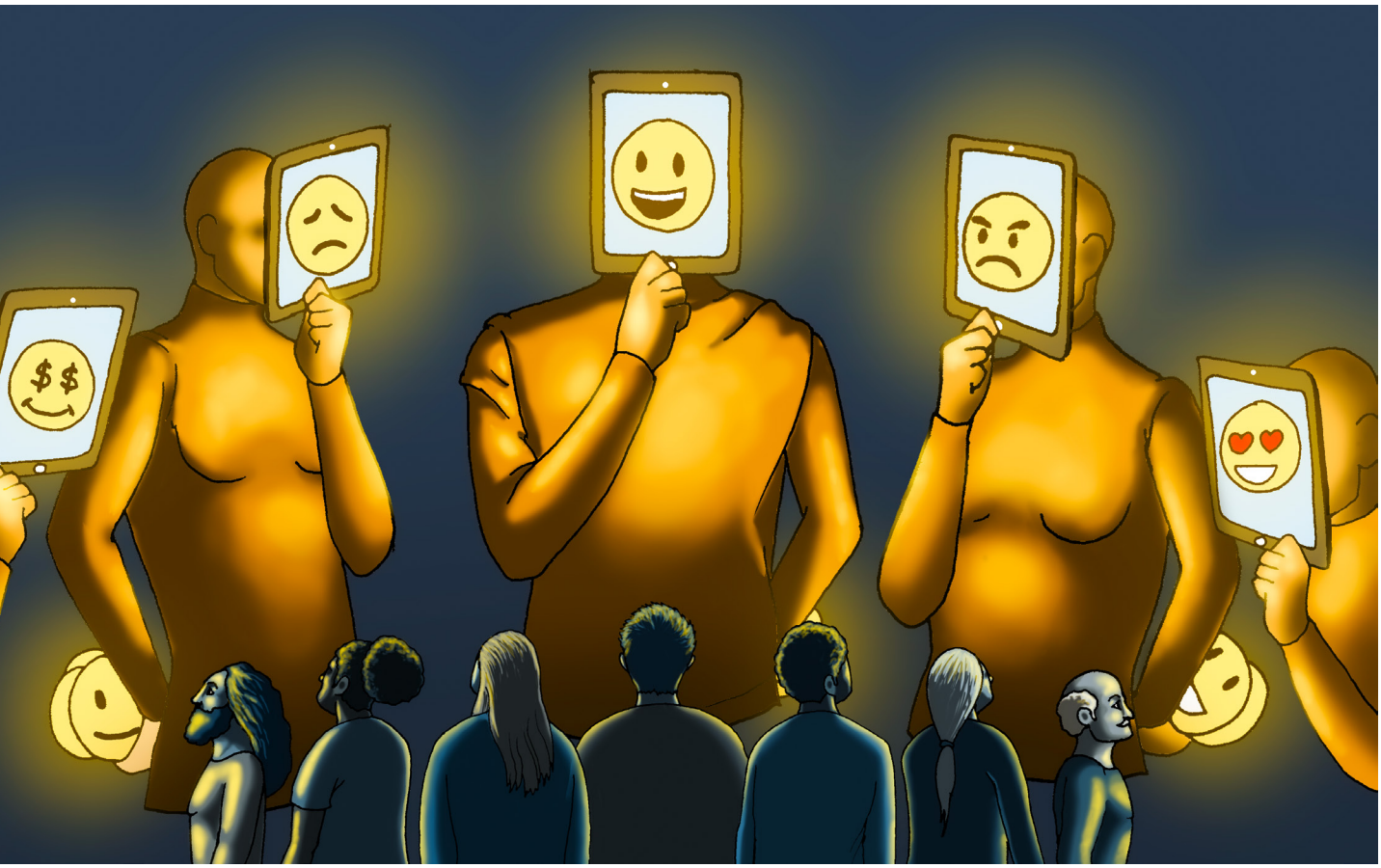


Illustration : RIENNEPRESS - Tanguy Maerten | Photo : Gracieuseté

parfois qu'on fasse des raccourcis, poussés par la curiosité. Penser qu'une cyberattaque sur notre ordinateur n'aura pas d'effet sur notre cellulaire, par exemple. »

Pour la formatrice, une bonne utilisation d'Internet doit donc nécessairement s'accompagner d'une volonté de ne pas toujours chercher à savoir.

La cupidité

Tout comme la curiosité, l'appât du gain peut pousser l'être humain à prendre des risques sur les plateformes numériques.

« La cupidité peut nous pousser à croire qu'on a gagné un concours sur Internet, même si au fond de nous, on sait bien qu'on n'a jamais participé à aucun concours, par exemple. Mais on donne quand même notre numéro de carte de crédit pour gagner le prix. La cupidité mène à la rapidité d'exécution », déplore Emeline Manson.

Un constat partagé par Fyscillia Ream, coordonnatrice scientifique à la Chaire de recherche en prévention de la cybercriminalité de l'Université de Montréal : « Sur Internet, il existe ce réflexe et cette envie de gagner de l'argent rapidement et facilement. Prenons l'exemple de la célèbre *fraude* 419, ou fraude du *prince nigérian*.

« Cette fraude consiste à promettre à la victime une grosse somme d'argent en échange d'une aide financière au préalable. Ça peut être des frais de transport, administratifs, de dossier, etc. La victime va alors être tentée de payer les frais pour obtenir la grande somme d'argent promise à la fin.

« Ce sentiment de cupidité est problématique, remarque celle qui est aussi cofondatrice de la Clinique de cybercriminologie de l'Université de Montréal, car cela peut amener la victime à être jugée moralement coupable. »

L'excès de confiance

Que ce soit la curiosité ou la cupidité, ces deux réactions chez l'être humain sont souvent activées grâce à un rapport de confiance établi par le cybercriminel avec sa victime. « Les fraudeurs savent très bien

utiliser l'art de l'exclusivité de l'information et transmettre un sentiment de fierté et d'importance à leurs cibles, explique Fyscillia Ream. Ceci crée une bulle de confiance qui amène souvent la victime à croire le cybercriminel. »

De même, notre confiance naturelle peut parfois nous porter à oublier que toutes nos actions sur Internet peuvent avoir un impact sur la sécurité de nos données. Pour limiter cela, Emeline Manson préconise une "saine paranoïa". « Ma saine paranoïa me pousse à tout vérifier. Je pense que c'est essentiel pour avoir une bonne hygiène numérique. »

Pour illustrer son propos, elle reprend une analogie de Jacques Sauvé, spécialiste des technologies de l'information, qui compare la bonne hygiène numérique au 1er avril : « Ce jour-là, les personnes savent très bien qu'elles pourraient être victimes d'une blague, et ceci se traduit par une grande vigilance toute la journée. Cette hypervigilance, c'est ce qu'on devrait retrouver dans notre utilisation quotidienne des outils numériques afin d'éviter de devenir des cibles faciles. »

Des indices importants

En faisant attention aux comportements en ligne, que ce soit au niveau des échanges textuels, de la voix ou même du ton utilisé lors des communications verbales, il serait possible de détecter la malveillance.

Ce n'est pas facile à faire car on ne voit pas son interlocuteur en ligne, mais c'est possible selon Christine Gagnon, spécialiste en analyse du comportement et en sémantique linguistique, et formatrice à l'École des sciences de la gestion de l'Université du Québec à Montréal.

« Un cybercriminel communique souvent par des échanges rapides ayant pour objectif de créer un sentiment d'urgence chez leur victime potentielle. Celle-ci va alors se sentir dans l'obligation d'agir vite, sans avoir pris le temps de réfléchir. C'est la même méthodologie qui est utilisée dans le marketing. »

La spécialiste recommande donc de prêter attention aux mots choisis, mais aussi au ton, au timbre, au rythme des échanges. Le verbal et le paraverbal.

Au téléphone par exemple, « un cybercriminel va avoir tendance à contrôler la communication et l'espace sonore de sa cible, explique Julie Salvador, synergologue et analyste de la voix et des indicateurs paraverbaux à Montréal. Il va chercher à attendrir sa victime ou faire figure d'autorité en utilisant des mécanismes de bienveillance et d'angoisse, pour créer une action urgente à réaliser, comme un transfert d'argent ».

Elle conseille d'ailleurs, dans ce cas, de « toujours faire rappeler son interlocuteur. C'est un bon moyen de décourager un cybercriminel. Il ne faut pas non plus hésiter à faire répéter pour désamorcer la situation d'urgence ressentie.

« La règle d'or, c'est de toujours se demander : *Suis-je en contrôle de la situation actuelle ?* et *Essaie-t-on de me faire faire quelque chose que je ne ferais pas habituellement sans y réfléchir longuement ?* Si on a des doutes, il faut raccrocher. »

L'erreur est humaine

C'est d'autant plus important de garder à l'esprit tous ces drapeaux rouges qu'une telle cyberattaque a des conséquences non seulement sur la victime, mais aussi sur son entourage.

Emeline Manson explique : « Un cybercriminel peut exploiter à

Photo : Gracieuseté

la fois les données de sa victime et celles de son carnet d'adresse, en utilisant le nom et le rapport de confiance de la victime avec ses proches pour les contacter via les messages privés, les réseaux sociaux ou les courriels.

« Si une personne s'est fait pirater son compte Google, par exemple, le cybercriminel qui a fait cela pourrait aussi parcourir son agenda et envoyer des messages à toutes les personnes récemment en contact avec sa victime.

« Le fraudeur peut notamment leur envoyer un simple lien de partage de document, soi-disant pour donner suite à une rencontre, mais ce lien est en réalité un lien d'hameçonnage pour récupérer leurs propres informations de compte. Les cybercriminels utilisent beaucoup Facebook pour ces envois. »

La formatrice en prévention des fraudes et cybersécurité tient toutefois à rappeler que personne n'est à l'abri de tomber dans le piège des cybercriminels, pas même les experts.

« Il y a beaucoup de stéréotypes qui font penser qu'une personne victime de la cybercriminalité est forcément idiote, mais il faut absolument relativiser cela. Il est normal d'avoir des moments de vulnérabilité ou d'inattention. Parfois, cliquer sur un mauvais lien ou transmettre des informations personnelles à un tiers fait vraiment du sens. »

Elle-même en sait quelque chose. En 2021, deux semaines après s'être fait cambrioler et voler son Mac, son conjoint reçoit un courriel lui disant que son ordinateur a été localisé, avec un lien frauduleux. « C'est un expert en cybersécurité, et pourtant il a cliqué sur le lien. Parce qu'à ce moment-là, cela répondait à sa réalité. Il a eu une réaction rapide, motivée par un sentiment d'urgence.

« Le fraudeur a sûrement envoyé ce courriel à des milliers de personnes, et la majorité des gens ont dû prendre cela pour un spam. Mais quand une cyberattaque, par le hasard, trouve une résonance dans ton actualité, alors même avec la plus grande attention, tu peux tomber dans le piège. Voilà pourquoi il est toujours important de reconnaître la part de l'humain dans notre manière d'aborder la cybercriminalité. »

DES TALENTS D'ENQUÊTEURS

Si leurs intentions sont mauvaises, il n'en est pas moins vrai que les cybercriminels démontrent souvent de grands talents d'enquêteurs, comme le souligne Emeline Manson, formatrice en prévention des fraudes et cybersécurité exerçant au Québec :

« Internet est un puzzle où nous dispersons plein d'éléments de notre vie, sur les réseaux sociaux notamment. Mais pour un cybercriminel, ce n'est pas compliqué de rassembler toutes ces pièces pour connaître l'identité numérique d'une personne. Les cybercriminels feraient d'excellents enquêteurs, et certains d'entre eux le sont même devenus après avoir mis un terme à leurs activités frauduleuses. »

C'est notamment le cas de l'ancien pirate informatique Kevin Mitnick, qui depuis les années 2000 est devenu consultant en sécurité informatique et auteur de plusieurs livres et formations sur l'ingénierie sociale pour les entreprises et les organismes gouvernementaux.

Fraude amoureuse & téléchargement furtif, deux attaques fréquentes et sournoises

L'ingénierie sociale est utilisée à des fins d'extorsion par les cybercriminels, en profitant de la vulnérabilité émotionnelle humaine. Associé à une hygiène numérique défaillante, cet art de la manipulation a engendré un grand nombre de scénarios et de techniques qui vont servir à manipuler et à soutirer une somme d'argent et des informations aux victimes de la cybercriminalité. C'est le cas de deux grands styles d'extorsion en ligne, la fraude amoureuse et le téléchargement furtif.

Écrit par **Jean-Baptiste GAUTHIER**

Les principales cyberattaques allient souvent l'exploitation d'un système informatique vulnérable et la manipulation des émotions et des comportements humains. Dans le cadre d'une extorsion monétaire ou de données personnelles, le malfaiteur utilise les courriers électroniques, les médias sociaux ou les plateformes de communication pour entrer en contact avec sa victime.

Nous pouvons citer deux grandes techniques d'extorsion en ligne, le "téléchargement furtif", qui va exploiter une mauvaise hygiène numérique, et la "fraude amoureuse", où l'art de la manipulation va être grandement utilisé par les cybercriminels. Deux techniques sournoises qui, pour Akim Laniel-Lanani, directeur de la Clinique de cyber-criminologie de l'Université de Montréal, représentent parfaitement cette cybercriminalité à deux têtes, à la fois humaine et technologique.

La fraude amoureuse

« La fraude amoureuse amène souvent un cybercriminel à créer un lien intime de confiance avec sa victime, dans le but de lui faire du chantage affectif et financier par la suite.

« Le premier contact est technologique. Le fraudeur effectue une recherche au préalable sur sa cible. Il lui envoie ensuite un message de confiance en personnalisant son approche, et réalise ainsi un harponnage, plus connu sous le nom de *spear phishing* en anglais. »

En d'autres mots, le harponnage est un type d'hameçonnage auquel le cybercriminel ajoute des éléments personnels au sujet de sa cible pour lui faire baisser sa garde.

« Une fois que la victime est prise dans les filets et en contact avec son agresseur, le cybercriminel va se servir de l'ingénierie sociale pour manipuler les émotions de sa cible, en utilisant des mécanismes de bienveillance dans un premier temps, pour créer un lien de confiance, puis en testant sa victime avec des mécanismes d'angoisse.


Akim Laniel-Lanani

« Le cybercriminel va par exemple arrêter de communiquer pendant quelques jours, pour voir si la personne s'est attachée à lui. Si c'est le cas, il expliquera que son silence était dû à un accident ou un incident

Photo : Gracieuseté

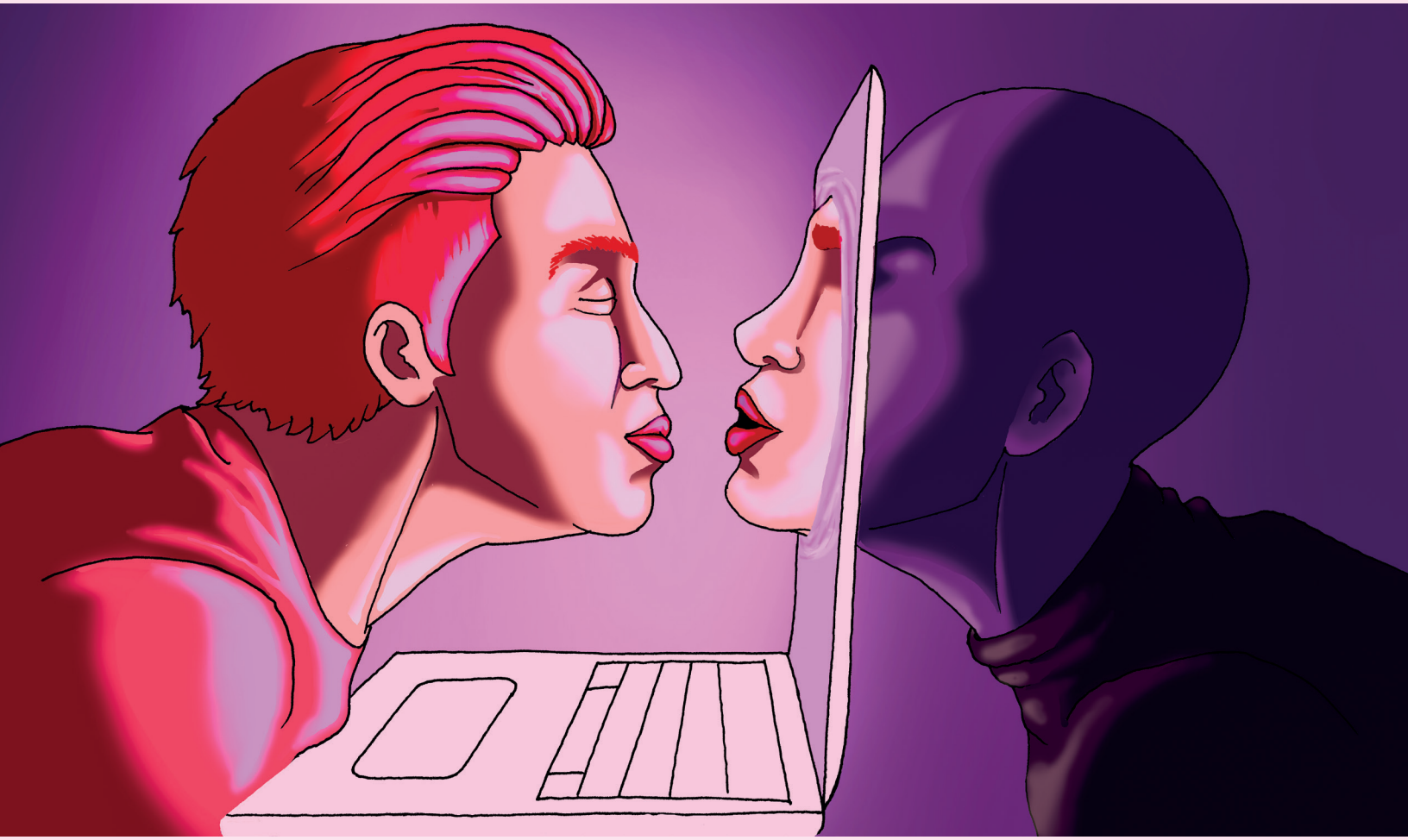


Illustration : RIENNEPRESS - Tanguy Maerten — Photo : Gracieuseté

quelconque, et il en profitera pour commencer à demander des sommes d'argent, que cela soit pour payer des frais médicaux, régler des problèmes financiers, ou pour rejoindre la personne si elle vient d'un pays étranger par exemple », affirme-t-il.

La fraude amoureuse peut également évoluer en sextortion. Le cybercriminel va alors affirmer avoir en sa possession des données compromettantes de sa victime, « comme des photos nues ou des vidéos de relations sexuelles », explique Fyscillia Ream, coordonnatrice scientifique à la Chaire de recherche en prévention de la cybercriminalité de l'Université de Montréal.

« La victime sera souvent invitée à payer une rançon ou bien ouvrir un lien pour télécharger un logiciel, qui sera en fait malveillant et fera encore plus de dégâts sur ses systèmes informatiques, malheureusement.

« Les contacts de fraudes amoureuses et ses dérivés sont majoritairement réalisés par courriel. C'est un support de communication avec un nombre important de fonctionnalités qui facilitent le piratage et l'escroquerie, comme l'envoi de pièces jointes et de liens frauduleux.

« C'est sûrement le support le plus efficace et le moins coûteux pour les cybercriminels, mais il

ne faut tout de même pas négliger l'utilisation des réseaux sociaux et des messageries privées dans les fraudes amoureuses », souligne Fyscillia Ream.

Il y a cependant plusieurs moyens de reconnaître une attaque de fraude amoureuse, comme l'explique Akim Laniel-Lanani : « Un fraudeur a souvent le réflexe d'exprimer très rapidement ses (faux) sentiments à sa victime.

« De plus, il aura tendance à diriger la conversation vers une messagerie privée et plus sécuritaire pour son anonymat, comme WhatsApp, Signal, ou encore Telegram, une application souvent utilisée par les cybercriminels. »

Un avis partagé par Christine Gagnon, spécialiste en analyse du comportement et en sémantique linguistique, et formatrice à l'École des sciences de la gestion de l'Université du Québec à Montréal :

« Lors d'une fraude amoureuse, un cybercriminel a tendance à accélérer le partage de ses sentiments. De plus, il ne va jamais vouloir allumer sa caméra ou se montrer en vidéo.

« Un jour, une amie est venue me demander son aide en pensant être victime d'une fraude amoureuse sur une application de rencontre en ligne. J'ai commencé à dialoguer par téléphone avec son interlocuteur et j'ai remarqué que son rythme de voix était calme, reposé, détendu, et qu'il agissait sans stress.

« De plus, j'entendais derrière lui plusieurs voix, ce qui me laissait clairement penser que cette personne n'était pas dans un cadre propice à une rencontre amoureuse, et donc qu'elle avait très probablement des intentions malveillantes », raconte Christine Gagnon. Si tout le monde peut être victime de fraude amoureuse, les cybercriminels savent bien détecter certaines vulnérabilités qu'ils s'empressent d'exploiter, comme l'explique Gilles Michel Ouimet, psychologue et Docteur en psychologie clinique à Polytechnique Montréal.

« Une victime de fraude amoureuse va souvent éprouver un besoin affectif qui sera détecté par le cybercriminel. Il va la valoriser en faisant monter son estime d'elle-même. Même si la victime arrive à détecter les signaux malveillants, elle va inconsciemment les ignorer. Elle veut continuer à croire en son bonheur. »

Pour se protéger d'une potentielle attaque à la fraude amoureuse, Akim Laniel-Lanani conseille aux gens de ne pas envoyer d'informations intimes pouvant être utilisées contre eux, comme des photos nues.

« Il ne faut surtout pas se mettre dans une position de vulnérabilité. Lors d'une relation virtuelle, il est également important de vérifier l'identité de la personne avec qui vous parlez en effectuant quelques recherches sur le nom d'utilisateur ou encore parmi les images utilisées par le profil qui vous approche.

« Et il faut éviter de faire confiance à ce que vous voyez à l'écran. La technologie des hypertrucages *Deepfakes* est de plus en plus accessible », déclare-t-il. Cette technologie permet de truquer des sons, des photos ou des vidéos dans le but de se faire passer pour une autre personne.

Le *deepfake* s'appuie sur une vraie base de données pour créer un avatar qui aura son propre visage et sa propre voix. Pour Akim Laniel-Lanani, il sera bientôt très difficile de déterminer s'il s'agit du vrai visage de la personne avec qui nous parlons.

Le téléchargement furtif d'un logiciel malveillant

Le *Drive-by download*, ou téléchargement furtif, est une vieille technique qui est toujours utilisée en nombre par les cybercriminels pour infiltrer un ordinateur avec un logiciel malveillant, et ainsi créer une situation de chantage avec la victime.

« Le téléchargement furtif peut se déclencher à l'ouverture d'un courriel ou bien à la consultation d'un site internet infecté par une publicité malveillante. Le simple fait de visualiser cette publicité va alors télécharger discrètement et automatiquement un programme malveillant sur votre système informatique, explique Akim Laniel-Lanani.

« En 2011, la BBC a vu plusieurs de ses pages web se faire pirater. Des cybercriminels avaient

inséré un code malveillant dans une annonce publicitaire. Chaque personne qui visite les pages web contenant la publicité infectée est la proie du maliciel sans qu'elle ait à cliquer sur quoi que ce soit. »

Le téléchargement furtif exploite les failles de sécurité persistantes dues à une cyberhygiène défaillante, comme des versions obsolètes des navigateurs web et des paramétrages de sécurité de l'ordinateur, afin d'introduire un maliciel dans l'appareil.

Cette porte d'entrée permet ensuite aux cybercriminels d'utiliser l'ingénierie sociale, comme l'explique Akim Laniel-Lanani : « Les cybercriminels exploitent les données volées pour faire du chantage à sa victime, en bloquant son système informatique ou en menaçant d'afficher des informations sensibles sur Internet. »
Pour le professionnel de la cybercriminologie, une des meilleures façons de se protéger des téléchargements furtifs est de « s'assurer que son système d'exploitation et ses logiciels sont à jour », ainsi que d'être « en possession d'un bon antivirus ».

« Je conseille également aux gens d'utiliser un profil invité sur leurs ordinateurs, qui ne contient pas les pouvoirs d'un profil d'administrateur. On ne peut donc pas y installer de logiciels sans le mot de passe maître. Cela nous rend ainsi moins vulnérables. Si notre appareil est infecté, le pirate n'aura accès qu'à un nombre limité de fichiers et de possibilités de chantage. »
Le directeur de la Clinique de cyber-criminologie de l'Université de Montréal conclut avec la grande règle de base d'une bonne hygiène numérique :

« Les données sensibles de chaque personne doivent être sécurisées. À partir du moment où votre téléphone ou votre ordinateur contient des données que vous ne voudriez pas voir diffusées au grand public, ces données sensibles doivent être conservées et verrouillées ailleurs que sur l'appareil. Conservez-les par exemple sur un périphérique de stockage physique, tel qu'une clé USB sécurisée à empreinte digitale. »

TÉMOIGNAGE D'UNE TRAHISON

Les réseaux sociaux sont des plateformes privilégiées par les cybercriminels pour identifier leurs cibles. C'est le cas de Madame V. (1), victime d'une fraude amoureuse.

Début janvier 2022, Madame V. est contactée par un certain William sur Instagram. L'homme communique de plus en plus régulièrement avec elle et lui propose de continuer leurs échanges par messages privés.

« Je découvrais les réseaux sociaux et Instagram, se souvient-elle. Je trouvais cette relation courtoise et amicale. Il m'envoyait des photos de lui et de sa fille et je n'avais aucune idée de sa nature malveillante. »

Cette relation de confiance s'est poursuivie plusieurs semaines en appel vocal par téléphone jusqu'à ce que William prétexte un voyage en Angleterre pour lui demander la somme de 500 $ CAD. « Il m'a dit qu'il ne pouvait pas se servir de sa carte bancaire et qu'il n'arrivait pas à contacter ses proches pour le dépanner. Communiquer avec lui m'a mis du baume au cœur, alors je l'ai cru et je lui ai envoyé l'argent », déplore-t-elle.

Au final, Madame V. n'a jamais revu ses 500 $ CAD. Elle reconnaît être tombée de son petit nuage en découvrant la supercherie. « Je me disais juste que j'avais rencontré quelqu'un de bien. » (2)

(1) Le nom Madame V. a été utilisé par *La Liberté* pour protéger l'anonymat de la victime.

(2) Madame V. a signalé sa fraude sur fraude-alerte.ca, la plateforme de partage de la Clinique de cyber-criminologie de Montréal.

Leurre et sextorsion : le récit glaçant du Centre canadien de protection de l'enfance

Pendant que les pouvoirs publics continuent de miser sur une hypothétique autorégulation de l'espace numérique, des organismes comme le Centre canadien de protection de l'enfance (CCPE) tirent la sonnette d'alarme sur une hausse des cyberviolences sexuelles. L'impuissance du législateur face à l'irresponsabilité des géants de l'Internet est pointée du doigt.

Écrit par **Mehdi MEHENNI**

Les chiffres sont effarants. Alors qu'on croyait la recrudescence de la cyberviolence contre les enfants, durant les deux dernières années, intimement liée à la pandémie et au confinement sanitaire, de nouvelles données viennent invalider cette hypothèse.

Du 1er mars au 31 août 2022, le Centre canadien de protection de l'enfance (CCPE), organisme désigné officiellement par le gouvernement fédéral pour recevoir les alertes de cyberviolences à l'égard des enfants, a en effet enregistré une hausse de 39 % des signalements d'exploitation sexuelle provenant du cyberespace. René Morin, porte-parole au CCPE, dresse un tableau sombre.

« C'était loin d'être conjoncturel. La courbe ascendante se poursuit, alors que la pandémie est presque derrière nous », alerte-t-il.

Ce qui est préoccupant pour René Morin, c'est surtout la hausse des cas de leurre, ce que le ***Code criminel du Canada*** définit comme une infraction qui consiste pour un adulte à communiquer électroniquement avec un enfant dans un but sexuel.

Les signalements de cas de leurre ont augmenté de 43 %, soit 496 incidents recensés durant la même période allant de mars à août 2022.

Le dernier bilan publié en février 2023, qui recense les cas de leurre durant les cinq dernières années, fait ressortir un nombre de signalements jamais vu au Canada, selon le CCPE.

La plateforme Cyberaide.ca, qui représente la centrale canadienne de signalement des cas d'exploitation et d'abus sexuels d'enfants sur Internet, a, en effet, vu son volume de signalements de leurre passer de 220 cas en 2018 à 2 013 cas à la fin de l'année 2022, soit une augmentation de 815 %.

« Pendant longtemps, on disait que le principal problème d'exploitation sexuelle des enfants sur Internet était la pornographie juvénile. Ce qui consiste en la diffusion d'images. Il ne faut certainement pas minimiser cela, mais lorsqu'on parle de leurre, on parle d'une interaction entre un prédateur et sa victime », détaille René Morin.

Plus nombreux et plus inquiétants encore sont les cas de sextorsion au Canada. Une fois l'interaction entre l'adulte et l'enfant établie, le sextorqueur va chercher à obtenir par différents moyens quelque chose de l'enfant. Il s'agira souvent soit d'obtenir d'autres images, soit de l'argent.

Dans cette catégorie de cyberviolence, le CCPE a enregistré 1 009 incidents entre le mois de mars et le mois d'août de l'année 2022, soit

une hausse de l'ordre de 56 % à travers le pays. « Effrayant », commente René Morin.

Il ne s'agit pourtant là que des signalements faits au Centre canadien de protection de l'enfance via Cyberaide.ca, une plateforme nationale dont le projet pilote a été lancé en 2002 à Winnipeg, au Manitoba.

Mais il y a aussi des victimes ou des parents de victimes qui vont s'adresser directement aux services de police, ou encore qui ne vont rien dire à personne. « Lorsque de jeunes victimes nous contactent et qu'on leur demande s'ils ou elles en ont parlé à quelqu'un de leur entourage, la réponse est le plus souvent négative. Et c'est généralement désespérés qu'ils ou elles vont finalement s'adresser à nous », regrette-t-il.

Les stratagèmes

Les stratagèmes décrits par le porte-parole du CCPE pour attirer les enfants dans ce guet-apens font froid dans le dos. La méthode la plus classique pour les sextorqueurs consiste à trouver des victimes sur les médias sociaux, et René Morin assure qu'Instagram et Snapchat sont les plus en usage.

« Les sextorqueurs se lient d'abord d'amitié avec les enfants et communiquent avec eux. Certains vont prendre leur temps, d'autres vont agir rapidement. Mais une fois que le contact est établi, ils proposent de poursuivre la conversation sur une plateforme vidéo qui permet un échange plus direct, un à un. Et là, la caméra est allumée », avertit-il.

Après cette étape, René Morin explique que toutes sortes de tactiques sont utilisées. Il cite le cas de garçons qui vont se retrouver en présence d'une jeune fille, ou plutôt de ce qui leur est présenté comme étant une jeune fille. Sans se rendre compte qu'ils sont, peut-être, en train de regarder des images pré-enregistrées.

À ce point, la fille va commencer à se dévêtir, invitant probablement le garçon à faire de même. Celui-ci, sans trop se poser de questions, s'exécute. Des images de ce qui est diffusé à l'écran sont captées à son insu.

« Tout de suite, la dynamique change complètement. Le sextorqueur revient à la charge pour montrer à l'enfant ses images intimes. Il le fait chanter et lui réclame de l'argent », prévient René Morin.

Et certains extorqueurs, pour démontrer à leurs victimes leur capacité à leur faire du mal, peuvent aller très loin dans leur chantage.

« Ils peuvent aller jusqu'à leur envoyer des colis par la poste à leur nom, à leur domicile ou à leur école, pour leur faire comprendre un message clair : *Allô, j'ai ton adresse, je sais où tu habites, je sais dans quelle école tu vas. Tu devrais me prendre au sérieux. Quand je te demande de l'argent, tu vas m'en donner, sinon j'envoie tes images à tout le monde* », précise René Morin.

Illustration : RIENNEPRESS - Tanguy Maerten

C'est à ce niveau-là, celui de la protection des enfants et de leurs données personnelles, qu'il pointe du doigt le manque de responsabilité mais aussi d'imputabilité des géants des réseaux sociaux.

Le diktat des géants de l'espace numérique

René Morin estime que les cas de sextorsion surviennent avant tout sur les médias sociaux et les applications que les jeunes ont sur leur téléphone. « Sur ces plateformes-là, vous avez des adultes qui vont pouvoir communiquer de manière directe avec des enfants. Et c'est là, à notre avis, que l'État doit intervenir et imposer un cadre réglementaire », martèle-t-il.

Mais comment le faire ? René Morin recommande de s'inspirer de ce qui se fait dans la vie réelle.

« Prenons l'exemple d'un bar. On ne peut pas laisser accéder des enfants là où des adultes consomment de l'alcool, donc on a adapté les lois pour empêcher cela. Ce qui n'est pas le cas sur ces plateformes où il n'y a aucun rempart, aucune mesure de sécurité pour empêcher les dérives.

« Un autre exemple inspiré de la vie réelle, c'est celui des fabricants de structures de jeux pour les parcs publics. Eux vont devoir respecter toutes sortes de normes, afin que leurs appareils soient sécuritaires pour les enfants.

« À l'inverse, lorsque vous arrivez sur Internet, il n'y a aucune règle à respecter. Vous faites ce que vous voulez et le résultat, c'est ce qu'on voit aujourd'hui : Internet est devenu un paradis pour les prédateurs d'enfants », dénonce-t-il.

Pourtant, René Morin rappelle que les gros joueurs dans l'industrie, comme Facebook, Twitter et autres, « se font des tonnes d'argent à travers leurs utilisateurs ». Ils devraient donc, selon lui, « se doter d'un effectif de modération proportionnel à leurs failles ». À leurs gains aussi.

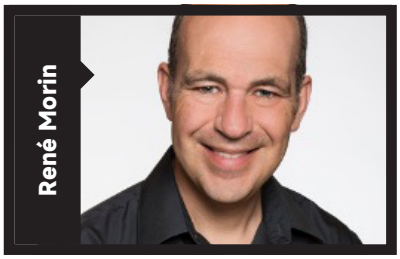
Que peut faire le gouvernement ?

Le porte-parole du CCPE considère que l'approche du gouvernement fédéral a été pendant longtemps de laisser le secteur Internet s'autoréglementer. Mais au final, il fait observer qu'on ne peut pas compter sur l'industrie pour prendre elle-même des mesures et protéger ses utilisateurs.

« Il faut qu'il y ait quelque chose au-dessus de cette industrie, relevant de l'État, qui impose certaines règles », interpelle-t-il.

Pour ce faire, René Morin ouvre d'autres pistes. Avec Cyberaide.ca, le CCPE a développé le logiciel Arachnid, qui parcourt Internet à la recherche de contenu illégal dans le but d'envoyer des demandes de suppression aux entreprises qui l'hébergent.

Certains hébergeurs ne vont pas donner suite à leurs demandes de suppression. D'autres vont prendre beaucoup de temps pour le faire. Une des mesures qui pourrait être prise par le gouvernement, suggère René Morin, serait de forcer les hébergeurs à retirer rapidement les images qui leur sont signalées sous peine d'amendes assez salées.



Cette mesure n'existe pas encore au Canada. L'idée commence, par contre, à faire son chemin au Royaume-Uni et dans l'Union européenne, selon l'expert.

L'avenir ? René Morin ne perd pas espoir. Surtout que son organisation travaille sans cesse à faire pression sur les pouvoirs publics. Début octobre 2022, le CCPE a réuni, autour de la même table, trois ministres fédéraux et des victimes. Des femmes et des hommes, aujourd'hui adultes, qui ont été abusés sexuellement durant leur enfance. Encore aujourd'hui, des images des pires moments de leur vie circulent sur Internet.

« On a permis à ces victimes de s'adresser directement aux représentants du gouvernement pour témoigner de leur quotidien et montrer à quel point elles avaient peur de sortir de chez elles, de se présenter en public », rapporte-t-il.

En attendant de voir si les choses finissent par bouger du côté d'Ottawa, de telles initiatives permettront, peut-être, de forcer la réflexion des pouvoirs publics sur la problématique.

Photo : Gracieuseté

CONSEILS AUX PARENTS ET TUTEURS

Comment réduire les risques ?

- Renseignez-vous sur la problématique des abus pédosexuels ainsi que les comportements et les situations qui présentent des risques pour les enfants et les adolescents. Téléchargez gratuitement la brochure *Les abus pédosexuels : ça vous concerne*, disponible sur protegeonsnosenfants.ca.
- Observez les interactions entre les adultes et les enfants et intervenez s'il y a lieu. Si la façon dont un adulte agit envers un enfant vous dérange, faites quelque chose. Pour savoir comment faire un signalement, consultez la page Agir du site.
- Apprenez à votre enfant à se protéger. Consultez enfantsavertis.ca pour obtenir des ressources âge par âge.
- Investissez-vous dans la vie de votre enfant. Participez à ses activités et observez les interactions entre les adultes et les enfants; voyez avec qui votre enfant se tient.
- Examinez attentivement les politiques de protection de l'enfance propres aux activités et aux organismes auxquels votre enfant est associé. Pour savoir comment bien choisir, téléchargez *3 étapes pour choisir un organisme soucieux de la sécurité des enfants*, disponible sur protegeonsnosenfants.ca.
- Soyez attentif aux changements. Un enfant peut avoir de bonnes et de mauvaises journées, mais l'important, c'est d'être attentif à tout changement dans son comportement habituel. Un enfant en détresse communique davantage son état d'âme à travers son comportement qu'à travers des mots.

Comment parler à votre enfant ?

Quand vous parlez à votre enfant, assurez-vous que votre discours soit adapté à son âge. Évitez de parler d'abus pédosexuels avec de jeunes enfants et inculquez-leur plutôt des notions d'autoprotection, par exemple :

- Les bons mots à utiliser pour les parties du corps, y compris les parties intimes que personne d'autre ne doit voir ou toucher.
- La différence entre un bon secret que l'on peut garder (p. ex. une fête surprise) et un mauvais secret qu'il faut dire à un adulte de confiance (p. ex. un secret entourant des attouchements ou des photos).
- Les techniques d'affirmation de soi. Le droit de dire non si quelque chose ou quelqu'un le trouble ou le met mal à l'aise.
- Les adultes de confiance dans l'entourage de l'enfant.
- Comment obtenir l'aide d'un adulte de confiance.
- Le respect de l'intimité au moment de se changer, de prendre son bain et d'aller aux toilettes.
- Comment identifier ses sentiments.

Des études montrent que les abuseurs s'intéressent moins aux enfants qui sont susceptibles de parler en cas d'abus. Inculquer aux enfants des notions sur l'autoprotection et les limites est un bon moyen de les rendre moins vulnérables. Pour des suggestions de sujets à discuter avec votre enfant selon son âge, consultez le site Enfants avertis.

Informations du Centre canadien de protection de l'enfance.

Le numérique chez les enfants : dialoguer restreindre ou interdire ?

L'utilisation d'Internet, très présent dans nos vies quotidiennes, est-elle vraiment si dangereuse pour les enfants ? Entre interdire, restreindre et dialoguer, des experts apportent des éléments de réponse sur les comportements à adopter en tant que parents.

Écrit par **Jean-Baptiste GAUTHIER et Mehdi MEHENNI**

Nina Duque, doctorante en communication sociale et publique, chercheuse dans les usages socio-numériques des adolescents et enseignante à l'Université du Québec à Montréal, propose d'abord de remonter aux origines de la peur de « l'étranger invisible » que peuvent éprouver les parents.

Elle explique que cette « peur du numérique » découle d'une grande campagne de prévention à destination des familles contre les contacts étrangers, dans les années 1980.

« Une étude réalisée par la chercheuse britannique Sonia Livingstone a démontré que cette campagne a eu pour conséquence d'enfermer nos enfants, notamment pour mieux contrôler leurs activités et les protéger du monde extérieur », souligne-t-elle.

Vanessa Lalo, psychologue clinicienne spécialisée dans les pratiques numériques, renchérit que jusque dans les années 1950, les enfants parcouraient en moyenne 10 kilomètres seuls par jour. Aujourd'hui, ce chiffre a baissé à 1 km.

Or, les statistiques montrent que le danger vient en grande majorité des gens que nous connaissons. Pour Nina Duque, c'est un bon point de départ pour relativiser le danger que peut représenter Internet.

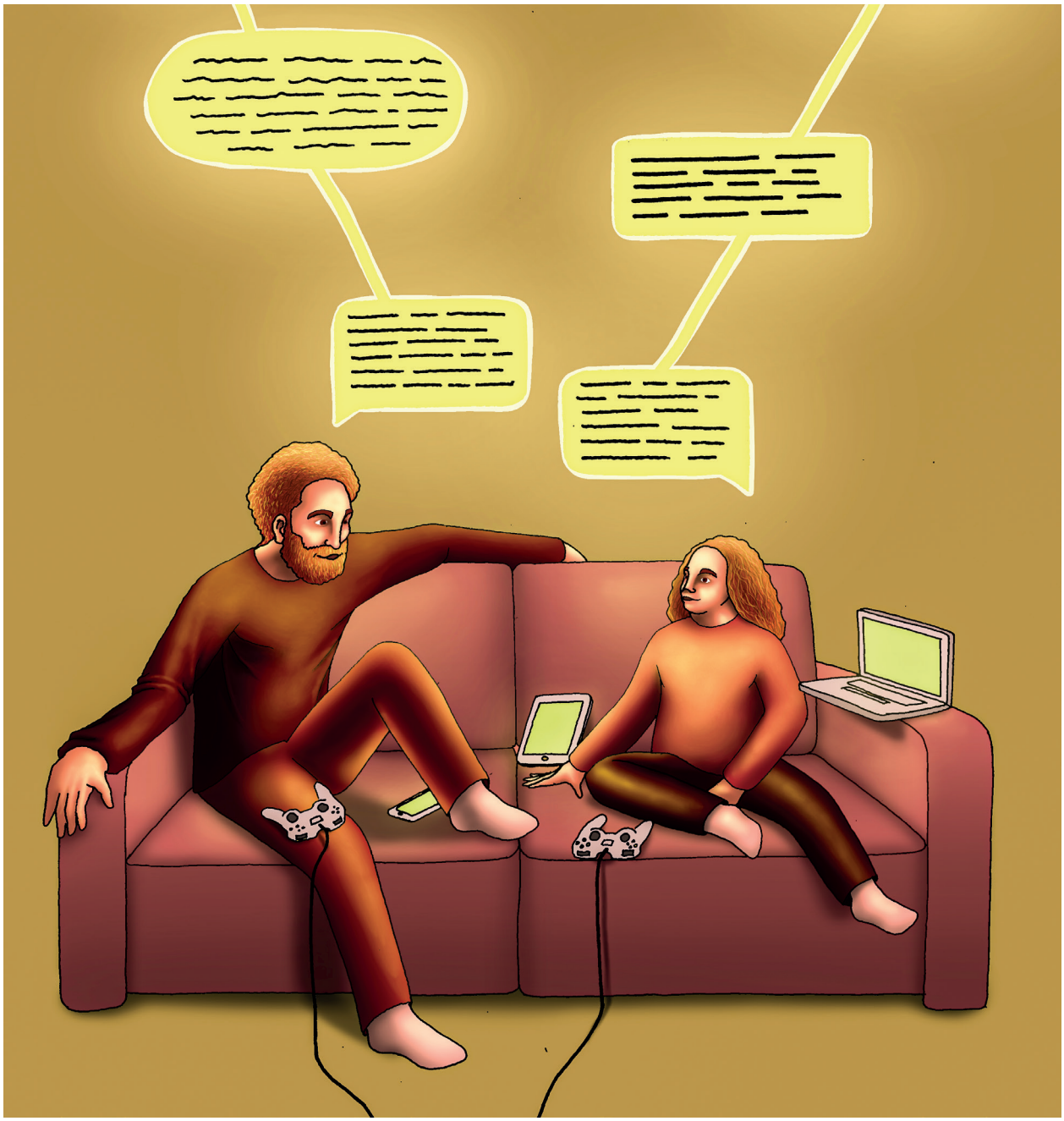
« En parlant avec un nombre important de jeunes, j'ai pu constater que les plus fréquentes agressions numériques sont en réalité réalisées par des connaissances proches. On parle notamment de cyberintimidation. Mais ce n'est pas le numérique qui a créé cela. Il y a toujours eu de l'intimidation, qu'Internet existe ou pas », souligne-t-elle.

Elle nuance tout de même son propos : « Avant, les jeunes rentraient chez eux et se réconfortaient loin de leurs agresseurs. Aujourd'hui, avec les réseaux sociaux et l'utilisation massive des téléphones intelligents, ce n'est plus possible. »

Le fossé technologique des parents

Vanessa Lalo ne considère pas Internet forcément plus dangereux que le monde réel. « La différence entre le réel et le numérique, c'est que dans la rue, nous connaissons les risques et les enjeux.

Ce qui nous angoisse en tant qu'adultes, c'est que nous manquons souvent de repères et de connaissances pour comprendre les risques qu'encourent nos enfants sur Internet.



« En quelque sorte, cela rassure les parents de matérialiser cette peur dans un ordinateur ou un téléphone intelligent. Il suffit alors d'éteindre l'appareil ou d'en limiter son utilisation pour faire disparaître la menace ». (1)

Pourtant, René Morin, porte-parole au Centre canadien de protection de l'enfance (CCPE), met en garde contre cette approche parentale. Il recommande plutôt d'accompagner son enfant.

« Il faut établir un parallèle avec ce qui se passe dans la vraie vie. Vous n'allez pas laisser votre enfant apprendre seul à traverser la rue, vous allez l'accompagner pour lui apprendre comment le faire en toute sécurité. Il faut faire la même chose avec Internet », indique-t-il.

Une étude britannique menée en 2019 auprès de plus de 2 000 parents d'adolescents de 13 à 16 ans, par le groupe Talk Talk, principal fournisseur en télécommunication au Royaume-Uni, révélait que plus de 70 % des parents s'inquiétaient du temps que leurs enfants passaient en ligne.

Pourtant, seulement 35 % d'entre eux déclaraient limiter le temps

Illustration : RIENNEPRESS - Tanguy Maerten

que leurs enfants passaient sur Internet et sur les outils technologiques. Une majorité de parents semblaient donc laisser leurs enfants sans contrôle, malgré leurs inquiétudes.

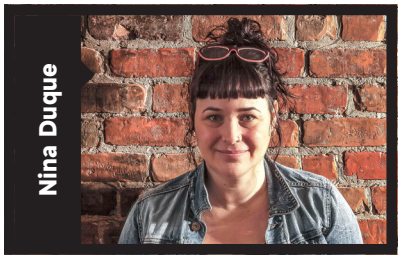
L'étude démontre que ce faible taux peut être attribué au fait que plus d'un tiers des parents (37 %) confiaient ne pas savoir pas comment aider leurs enfants à gérer ou à utiliser Internet et la technologie en toute sécurité.

Pourquoi interdire n'est pas la solution

En réponse à ses propres craintes, un parent va donc souvent avoir le réflexe d'interdire à son enfant l'accès aux outils numériques ou aux réseaux sociaux. C'est une erreur selon Damien Bancal, journaliste français spécialisé dans la lutte contre la cybercriminalité et fondateur du site zataz.com qui traite de la délinquance informatique. Il considère que cette interdiction peut aussi avoir des conséquences négatives chez l'enfant ou l'adolescent.

« Dans la plupart des cas, quand un jeune va se voir interdire l'accès à son ordinateur, il cherchera d'autres moyens d'avoir accès au monde virtuel. Cela peut être dans la cour de l'école avec ses amis, ou encore sur un téléphone cellulaire », explique-t-il.

Damien Bancal donne aussi l'exemple « d'une jeune fille qui, après s'être fait interdire l'accès à son compte Facebook par sa famille, a recréé 24 comptes Facebook différents en cachette. Il faut comprendre par là qu'elle a 24 versions de son identité numérique en libre accès sur Internet, ce qui l'expose davantage aux attaques cybercriminelles comme la fraude amoureuse, par exemple ».



L'enseignante et doctorante Nina Duque abonde dans le même sens. L'interdiction totale peut mener à des histoires qui font peur.

« Par exemple, une jeune adolescente de 13 ans me racontait que ses parents coupaient Internet le soir pour qu'elle puisse se coucher. Sa réaction ? Elle attendait que tout le monde se couche pour sortir, en pleine nuit, pour capter du wifi gratuit avec son cellulaire », raconte-t-elle.

Pour Vanessa Lalo, il faut même aller plus loin : c'est la responsabilité d'un parent de veiller à une bonne éducation numérique de son enfant.

« Un parent peut très bien interdire l'usage technologique à son enfant, mais que fera-t-il quand le numérique s'installera naturellement dans sa vie, lorsqu'il sera plus âgé notamment ? », questionne-t-elle.

Pour la psychologue clinicienne, il est important de ne pas laisser son enfant seul face aux apprentissages du numérique, en particulier tant que l'enfant n'a pas une bonne conception morale et un bon esprit critique.

Pour ce faire, René Morin pense que le parent doit manifester un certain intérêt aux activités en ligne de son enfant, en lui posant des questions comme : *Est-ce que ce sont des gens que tu vois dans la vraie vie ou à l'école ?* ou *Est-ce qu'on peut regarder ensemble les paramètres de sécurité, et comme ça on verra comment faire en sorte que des inconnus ne puissent pas te contacter spontanément sur Internet ?*

Le dialogue, une nécessité

Se basant sur des recherches universitaires, Nina Duque conseille elle aussi de privilégier une communication parentale positive axée sur le dialogue. Selon la spécialiste, les parents qui ont tendance à juger « peu intéressantes » les activités des jeunes sur Internet vont s'apercevoir, en s'y intéressant, que c'est surtout une mine d'or d'information et de sociabilisation.

Le dialogue va permettre à la fois aux parents de mieux connaître les habitudes de leurs enfants sur Internet, et d'y détecter de potentiels dangers.

« La meilleure prévention numérique a comme départ un parent qui s'intéresse aux activités numériques de son enfant.

- Suite page 67 -

Photos : Gracieuseté

Pluri-elles

Ça me regarde.

CONTRE LA VIOLENCE, TU AS UN RÔLE À JOUER.

Pluri-elles, un organisme à but non lucratif mis sur pied en 1982, vous procure les outils nécessaires pour grandir sur les plans personnel et professionnel.

Nos programmes et services touchent les domaines de l'éducation, la formation, l'économie, l'emploi, la culture, la santé et les services sociaux.

Nos services sont ouverts aux Manitobains et Manitobaines de tous les âges, y compris les hommes, les femmes et les enfants.

La violence sexuelle, c'est aussi la cybercriminalité sexuelle contre les enfants.
Ne laissez pas vos enfants seuls devant l'écran!

VALÉRIE WILLIAMME
Coordonnatrice - alpha familiale
v.williamme@pluri-elles.mb.ca

DANNICA MOROZ BSW
Conseillère - Entraide et counselling
d.moroz@pluri-elles.mb.ca

FATIHA SIOUANI
Conseillère - Entraide et counselling
f.siouani@pluri-elles.mb.ca

Pluri-elles offre ses services dans plusieurs régions du Manitoba
Pour plus d'informations, vous pouvez visiter notre site Web : www.pluri-elles.mb.ca ou nous suivre sur Facebook.
Vous pouvez également vous rendre dans nos locaux, au : 420, rue Des Meurons, unité 114, Winnipeg (Manitoba) R2H 2N9
Téléphone : 204-233-1735, poste 201 / Sans frais : 1-800-207-5874, poste 201

Il faut l'inviter à parler de ses passions et à se livrer naturellement, dans un dialogue positif avec de l'humour, si possible », conseille Vanessa Lalo.

Pour étayer ses propos, la psychologue clinicienne incite les parents à s'associer aux pratiques numériques de leurs enfants. « Cela peut être de jouer ensemble aux jeux-vidéo, d'aller sur les réseaux sociaux ou de découvrir leurs sites Internet préférés. »

En créant ce lien avec l'enfant, renchérit René Morin, « le parent va faire en sorte que si jamais, malgré toutes les précautions, quelque chose de malveillant survient, l'enfant aura le réflexe de se tourner vers son parent pour avoir de l'aide. Il se sentira suffisamment en confiance pour lui parler de ce qu'il voit dans son environnement numérique ».

Il sera ainsi beaucoup plus facile pour un parent de poser un cadre et des limites. Pour Vanessa Lalo, c'est avant tout une bonne connaissance des pratiques numériques qui amène une meilleure prévention ciblée selon l'âge de l'enfant, sa maturité critique et le contenu qu'il visionne sur Internet. La prévention ciblée doit surtout être liée à la qualité du contenu regardé, plus qu'à la quantité. (2)

Elle recommande les balises 3-6-9-12 (3) imaginées par le psychiatre français Serge Tisseron, qui permettent aux parents de réguler leur propre consommation pour donner le bon exemple et de mieux juger comment introduire les écrans à chaque âge.

Elle tient, cela dit, à rassurer les parents qui ne se sentent pas légitimes à aborder ces sujets avec leurs enfants, par crainte d'une méconnaissance en matière d'éducation numérique.

« C'est une conséquence du fossé générationnel, mais il ne faut pas croire que les enfants connaissent tous Internet. Ils cliquent peut-être plus vite que leurs parents, mais ils ont aussi de grosses lacunes dans la perception critique et morale des choses, ainsi que sur la priorisation de l'information », souligne-t-elle.

Il reste que « pour combler leurs méconnaissances et établir ce lien si précieux, les parents peuvent user d'une technique astucieuse qui consiste à demander à ses enfants de nous expliquer ce qui se passe sur Internet, quelles sont les applications qu'ils utilisent, comment elles fonctionnent. Les enfants se sentent alors valorisés dans leur tâche d'éduquer leurs parents », affirme René Morin.

Ne pas juger

Si les experts estiment le dialogue nécessaire, Nina Duque recommande de ne pas forcer la conversation. « C'est un travail éducatif. Il paraît peut-être contre-intuitif car nous voulons souvent obtenir vite nos réponses, mais il faut laisser le temps à l'enfant de venir vers son parent. Il doit sentir que l'adulte l'aborde sans juger son utilisation des outils numériques. »

Damien Bancal renchérit : « Un parent ne doit pas hésiter à demander à son enfant *Comment ça marche ?* Il faut tester les outils numériques avec lui et ne surtout pas juger les joies que cela peut lui procurer. (4) Ce qui pousse un enfant à ne pas parler de ses plaisirs à ses parents, c'est très souvent la crainte de se faire juger. »

Le journaliste français spécialisé dans la lutte contre la cybercriminalité considère que le numérique doit être un partage et que « ce n'est pas seulement un clavier, un écran et une souris. C'est aussi discuter, apprendre et ne pas être dans une démarche d'autorité ».

Les moyens mis à disposition des parents

Par ailleurs, René Morin rappelle que les parents peuvent aussi se renseigner pour être au courant des enjeux. « Au CCPE, on met à la disposition des parents quelques outils qui peuvent être très utiles. »

Le CCPE a, en effet, créé le site ParentsCyberAvertis.ca, qui suit les tendances sur Internet et renseigne les parents sur divers enjeux clés. Selon lui, l'intérêt de ce site est que les parents vont trouver de l'information en fonction de l'âge de leurs enfants. Les dangers sur Internet changent au fur et à mesure que les jeunes grandissent.

« En bas âge, ça va être la question des jeux en ligne et le risque d'intrusion d'un inconnu. À l'adolescence, c'est plutôt toute la question des données personnelles sur les médias sociaux, qui deviennent une mine d'or pour les pédo-prédateurs », relève-t-il.

Il recommande également aux parents de s'inscrire aux alertes de Cyberaide.ca, une plateforme canadienne qui reçoit des milliers de signalements par an.

« Ces signalements nous en disent long sur ce qui se passe sur Internet et sur comment s'y prennent les pédoprédateurs pour s'en prendre à nos enfants. Périodiquement, on lance une cyberalerte sur les tendances qu'on a remarquées. S'il y a par exemple de nouvelles applications qui apparaissent, on tient les parents informés sur les dangers encourus et les mesures à prendre pour protéger leurs enfants », éclaire René Morin.

Le CCPE a aussi développé sur son site Internet le programme ***Enfants Avertis***, qui apprend aux jeunes comment se protéger, autant sur Internet que dans la vraie vie. « Les mêmes principes sont applicables dans les deux environnements», précise René Morin.

Raison pour laquelle il tient à relativiser sur la question de savoir si Internet est plus dangereux que la vraie vie : « Que vous laissiez votre enfant se promener seul le soir au centre-ville de Winnipeg, ou que vous le laissiez seul face aux plateformes numériques, vous l'exposez au même danger », conclut-il.

(1) Pour les parents sceptiques, Vanessa Lalo recommande le livre *Votre enfant devant les écrans : ne paniquez pas, ce que disent vraiment les neurosciences* (2020, De Boeck Supérieur) écrit par Nicolas Poirel, professeur de Psychologie du Développement à l'Université de Paris Cité.

(2) Nina Duque conseille les ressources pédagogiques *Habilo Médias*, proposées par le Centre canadien d'éducation aux médias et de littératie numérique: https://habilomedias.ca/ressources-p%C3%A9dagogiques

(3) Programmes éducatifs.
Site web : https://www.3-6-9-12.org

(4) *Children, risk and safety online: Research and policy challenges in comparative perspective* (2012, Policy Press)

La double victimisation des aîné(e)s

Les personnes aînées sont de plus en plus vulnérables aux cyberfraudes. À cela s'ajoute la double victimisation par la société et les institutions.

Écrit par **Mehdi MEHENNI**

La cyberfraude fait, année après année, davantage de victimes parmi les personnes aînées, au Canada. Les chiffres communiqués à ***La Liberté*** par le Centre antifraude du Canada donnent le tournis, tant la courbe est particulièrement ascendante : l'estimation de l'argent subtilisé en ligne à cette frange de la société est passée de 13,2 millions $ en 2017 à 51,8 millions $ en 2021. Soit une hausse de 292 %.

Akim Laniel-Lanani, cofondateur et directeur de la Clinique de cyber-criminologie de l'Université de Montréal, admet que de manière générale, et indépendamment des types de cybercrime, la cybercriminalité a augmenté de façon fulgurante depuis les cinq dernières années. Néanmoins, il note chez les personnes aînées que la fraude amoureuse et surtout celle liée à l'investissement sont montées en flèche.

Les statistiques du Centre antifraude du Canada le confirment davantage s'agissant de ces deux aspects.

Si la fraude amoureuse en ligne est passée d'une valeur de 8,6 millions $ en 2017 à 15,7 millions $ en 2021, la fraude liée à l'investissement a fait un bond encore plus spectaculaire, passant de 1,9 à 26,9 millions $ durant la même période.

Les raisons de l'ampleur que prend ce phénomène sont évidentes aux yeux d'Akim Laniel-Lanani : « Les personnes aînées sont de plus en plus nombreuses et présentes en ligne mais ont encore une méconnaissance et une mécompréhension des méthodes utilisées par les cyberfraudeurs. « Lorsqu'on parle des personnes aînées, on parle de personnes d'une autre génération qui n'ont pas eu les mêmes apprentissages que nous aux nouvelles technologies. C'est donc normal que cette frange de la population soit davantage représentée dans ces statistiques », explique-il.

L'universitaire met en évidence le fait que les personnes aînées n'ont pas les mêmes mécanismes de défense et de méfiance vis-à-vis des « étrangers » qu'on peut rencontrer en ligne.

Raison pour laquelle il estime que la fraude aux grands-parents fonctionne si bien : « Les fraudeurs vont jouer sur le sentiment d'urgence, la notion de bienveillance du grand-parent, et son désir de venir en aide à son soi-disant petit-fils ou petite-fille qui se trouve face à un problème urgent. Et ce, sans forcément réfléchir aux conséquences ou penser vérifier auprès des parents. » D'où la question de savoir si le Canada, tant au niveau de la société que des pouvoirs publics, fait assez pour protéger

Illustration : Yahia Lahrech

les aînés. « Certainement pas », lance Akim Laniel-Lanani.

Sensibiliser sur le terrain

D'abord, le dirigeant de la Clinique de cyber-criminologie fait remarquer qu'au Canada, en général, on fait de la sensibilisation seulement une ou deux fois dans l'année. « Au mois de mars pour la fraude et en octobre pour la cybersécurité. »

Ensuite, il souligne que les actions de sensibilisation peuvent se limiter à des publications en ligne, et que cela ne va pas forcément rejoindre les personnes aînées.

« Si on parle des personnes de 65 à 74 ans, on peut les rejoindre parce qu'elles sont un peu plus présentes en ligne. Mais si on parle des personnes âgées de 75 ans et plus, ce n'est pas adapté à leur réalité », explique-il.

Pour rejoindre ces personnes, Akim Laniel-Lanani suggère de passer par leurs familles. D'après lui, certaines études ont démontré que la meilleure sensibilisation passait par les proches, les enfants et les petits-enfants étant plus disposés à leur présenter les nouvelles technologies pour assurer leur transition numérique. Mais là encore, les populations ont-elles les connaissances et les compétences pour sensibiliser d'elles-mêmes leurs proches ?

En tout cas, Akim Laniel-Lanani pense qu'il y a toujours place à l'amélioration, à commencer par définir des campagnes de sensibilisation « dépendamment du public qu'on cible.

« Il faut arrêter de penser qu'on peut rejoindre un maximum de personnes dans l'espace numérique. Il faut aussi être présent dans le monde réel et aller dans les résidences pour personnes âgées, les bibliothèques municipales et les organismes communautaires », recommande-t-il.

Illustration : RIENNEPRESS - Tanguy Maerten

Ceci exige plus d'effectifs et de ressources. Et c'est là que réside toute la problématique, à en croire la Fédération des aînées et aînés francophones du Canada (FAAFC).

Un manque d'appui

Pour Jean-Luc Racine, directeur général de la FAAFC, son organisme « aimerait être plus actif sur le dossier, mais c'est difficile parce qu'il n'existe pas de ressources, en ce moment, pour ce genre d'initiative dans les programmes annoncés par le gouvernement ».

Entre 2010 et 2016, la Fédération a monté des équipes de bénévoles pour animer des ateliers de sensibilisation auprès des personnes aînées, à la suite d'un financement du gouvernement fédéral.

Les six années de financement épuisées, l'organisme a tenté de poursuivre l'initiative avec ses propres ressources. Cela n'a pas duré longtemps.

« On n'a pas fait de nouvelles demandes, parce qu'il n'y a pas de programmes de financement disponibles dédiés à ce genre d'initiative. Les seules ressources qui existent sont dans le communautaire, et donc à l'échelle provinciale, une année de financement à la fois. Avec des fonds de 25 000 $ pour une initiative nationale, on ne va pas bien loin », déplore-t-il. Mais la Fédération ne reste pas pour autant les bras croisés. Des capsules vidéo présentant des situations de fraude potentielles et expliquant comment s'en prémunir ont été lancées sur son site Internet.

On y présente, par exemple, le cas d'une personne âgée vivant seule qui commence à recevoir de petits gestes d'attention, comme des fleurs chez elle. Puis tout à coup, le cyberfraudeur commence à lui parler d'argent pour venir lui rendre visite. Sans jamais le faire, mais en lui demandant, à chaque fois, un peu plus d'argent.

Un cas dont Jean-Luc Racine a déjà été témoin dans son entourage et qu'il trouve d'une « grande tristesse ». Il imagine d'ailleurs tous les autres cas qui sont tus, en raison du jugement négatif que peut avoir la société sur la victime.

Les victimes ne sont pas coupables

Le jugement porté sur les victimes de fraudes peut être sévère de la part de l'entourage. « Lorsqu'une personne est agressée physiquement dans la rue, elle est unanimement considérée comme victime. Mais dès lors qu'elle se fait voler son argent sur Internet, l'entourage a tendance à la culpabiliser. « On doit pourtant encourager les gens à dénoncer, en créant des espaces où les victimes vont se sentir à l'aise de parler », estime Jean-Luc Racine. Le directeur de la Clinique de cybercriminologie de l'Université de Montréal, Akim Laniel-Lanani, n'en pense pas moins.

Il trouve dommage que la société banalise l'impact d'une cyberfraude, ne reconnaisse pas le statut de cybervictime, et pire, qu'elle en vienne même parfois à rejeter le blâme sur la victime. « En rejetant la faute sur la victime, on contribue à sa victimisation », avertit-il.

Pour le spécialiste de la cybercriminalité, ces situations contribuent à garder la personne aînée dans le silence lorsqu'un tel scénario vient à se produire. Et comme la victime a honte d'en parler et de demander de l'aide, elle va rester dans son monde où elle n'aura ni les ressources ni les outils pour s'en sortir.

La preuve, avance le cofondateur de la Clinique de cybercriminologie, est que c'est très commun de cibler à nouveau les personnes qui ont été victimes une première fois.

Akim Laniel-Lanani conclut en rappelant que si la société persiste à ne pas reconnaître la gravité d'un cybercrime et de la fraude en ligne, le législateur ne sentira pas la pression nécessaire pour adapter la loi aux réalités du moment.

Photo : Gracieuseté

section 4

Cybersécurité : une priorité nationale

Porter plainte pour obtenir les moyens nécessaires

En matière de cybercriminalité, le constat est sans appel : le nombre de plaintes et de signalements déposés par des particuliers est bien en-deçà du nombre réel estimé d'attaques. Pourtant, une meilleure représentation de la réalité est essentielle pour faire de la cybercriminalité une priorité des gouvernements.

Écrit par **Camille HARPER**

Selon l'***Enquête canadienne sur la cybersécurité et le cybercrime*** de Statistique Canada publiée en octobre 2022, 18 % des entreprises au Canada ont été touchées par un incident de cybersécurité en 2021. Ceci représente environ 58 000 entreprises.

En revanche, la proportion d'entreprises victimes qui rapportent ces incidents à la police a diminué, passant de 12 % en 2019 à 10 % en 2021.

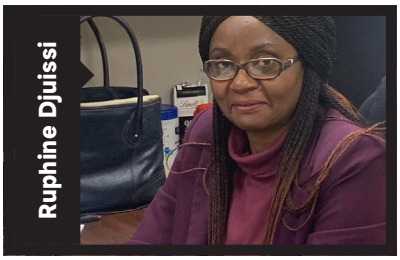
Pour Bob Gordon, conseiller stratégique de l'Échange canadien des cybermenaces (Canadian Cyber Threat Exchange - CCTX), « il y a plusieurs raisons qui peuvent expliquer ce pourcentage aussi bas et en baisse. Ça peut être que les entreprises pensent que c'est juste un petit incident qui n'a pas besoin d'être rapporté à la police, ou encore que s'ils rapportent une cyberattaque, cela risque de porter préjudice à la réputation de leur marque. Le plus inquiétant, c'est le petit nombre qui rapporte. 90 % des entreprises cyberattaquées ne rapportent pas ces incidents, et ceci a de lourdes conséquences sur les ressources allouées à la lutte contre la cybercriminalité.

Il s'explique : « Si un département de police veut demander plus de ressources pour lutter contre la cybercriminalité mais que les chiffres officiels de signalements sont bas, c'est très difficile d'obtenir une réponse favorable.

« C'est la même chose au niveau des gouvernements qui veulent faire approuver des projets de loi. Si les nombres laissent croire que peu de gens sont concernés par le problème, ce ne sera pas une priorité pour les parlementaires. Ils préféreront mettre leur temps, leur énergie et leurs ressources sur d'autres dossiers. Et plus encore quand le pourcentage déjà faible a davantage chuté. »

Brandon Trask, professeur adjoint à la Faculté de droit de l'Université du Manitoba et ancien procureur en Nouvelle-Écosse, a notamment constaté le manque de ressources allouées aux cas de cybercriminalité de nature non sexuelle ou non mortelle.

« Partout, la police et les procureurs ont de la difficulté à résoudre les cybercrimes qui ne sont pas à caractère sexuel par manque de ressources. Les cybercrimes non sexuels sont souvent très complexes et difficiles à retracer, par conséquent les provinces choisissent de garder leurs ressources pour d'autres crimes ayant une meilleure probabilité d'atteinte de résultats et pour les cybercrimes de nature sexuelle. »



Les particuliers aussi

Tout comme les entreprises, les individus victimes d'une cyberattaque devraient eux aussi prendre des mesures de signalement. Me Ruphine Djuissi, avocate à Infojustice Manitoba : « Un cybercrime peut avoir de graves conséquences,

Illustration : RIENNEPRESS - Tanguy Maerten | Photo : Gracieuseté

alors il est recommandé que les particuliers qui en sont victimes signalent l'incident au Centre antifraude du Canada, au Centre canadien pour la cybersécurité et à la police, afin d'aider ces organismes à accroître leur surveillance. »

Elle ajoute à ceci une dimension psychologique, sécurisante : « Un signalement peut également aider à atténuer les effets du cybercrime sur l'individu en soutenant ses efforts, et dissuader de nouvelles attaques à son encontre. Cela permet aussi de mieux le protéger contre toute mauvaise utilisation de ses données à l'avenir. »

Fyscillia Ream, cofondatrice de la Clinique de cyber-criminologie de l'Université de Montréal, nuance toutefois : « Certes le signalement permet de faire face à la victimisation, encore faut-il savoir gérer ses attentes envers les corps policiers. En effet, souvent, les victimes d'un cybercrime ont des attentes très élevées envers ce que va faire la police après un signalement, notamment qu'elle arrête les criminels. C'est rarement le cas en cybercriminalité. »

Signaler tout incident de cybercriminalité, que ce soit par les particuliers ou les entreprises, reste essentiel pour mieux mesurer l'ampleur du problème et adapter les réponses. « Les signalements permettent aussi au Centre antifraude de maintenir le public averti et à jour sur les nouveaux stratagèmes de fraude, et ainsi réduire le nombre de victimes potentielles », termine Me Ruphine Djuissi.

Une autre façon de jouer son rôle

Parfois aussi, les individus n'estiment pas que leur situation nécessite de solliciter la police, ou ne souhaitent pas son intervention. Ils peuvent quand même jouer un rôle clé pour s'assurer que d'autres personnes ne subiront pas la même fraude.

La Clinique de Cyber-criminologie de l'Université de Montréal a lancé, en octobre 2022, la plateforme en ligne et en français Fraude-alerte. Très facile d'accès et d'utilisation, c'est un lieu où quiconque peut venir signaler une fraude, mais aussi y voir toutes les fraudes déjà enregistrées par d'autres utilisateurs. On y trouve également des informations utiles telles que les noms d'utilisateurs de fraudeurs, les numéros de téléphone, les courriels, etc.

Illustration : RIENNEPRESS - Tanguy Maerten

Akim Laniel-Lanani est cofondateur et directeur de la Clinique de cyber-criminologie : « Fraude-alerte permet aux Canadiens francophones de retrouver plus efficacement et plus facilement les informations d'une cyberfraude au Canada. Si une personne signale une fraude, son action va donc permettre à une autre personne d'éviter d'être potentiellement victime de la même fraude. »

Outre la solidarité dans la lutte contre la cyberfraude que cette plateforme encourage, Fraude-alerte permet aussi aux utilisateurs de bénéficier de conseils et de ressources d'experts adaptés à chaque situation.

« Les analystes de la Clinique de cyber-criminologie regardent les commentaires et les signalements pour donner des conseils pertinents selon le cas », explique Akim Laniel-Lanani.

La Clinique de cyber-criminologie de l'Université de Montréal utilise également les données de Fraude-alerte.ca afin de sensibiliser et d'informer la population, tout en contribuant à la réalisation de projets de recherche dans le domaine de la cybersécurité et de la prévention de la cybercriminalité.

L'essentielle solidarité des forces de l'ordre

Le cybercrime est en constante évolution et les techniques utilisées par les assaillants du net sont de plus en plus sophistiquées. Pour y faire face, les forces de l'ordre travaillent constamment à adapter leurs capacités et coordonner leurs efforts. Une plateforme nationale dédiée à récolter et analyser les signalements des victimes de cyberattaques devrait être opérationnelle avant la fin 2023.

Écrit par **Mehdi MEHENNI**

Pour Chris Lynam, haut gradé de la Gendarmerie royale du Canada (GRC), la menace de la cybercriminalité sur les citoyens et les entreprises au Canada a pris des proportions telles que le gouvernement a pensé, ces dernières années, à créer une organisation nationale chargée de coordonner les efforts pour faire face à cette menace permanente.

Il s'agit, en effet, du Centre national de coordination en cybercriminalité (CNC3). « L'objectif du Centre est de travailler avec tous les services de police du Canada, mais aussi avec les homologues et les partenaires à l'international, pour pister et neutraliser les cybercriminels », explique Chris Lynam, qui dirige le CNC3 depuis sa création en avril 2020.

Bien que des équipes d'investigation existent au sein de la GRC et que certaines provinces et municipalités ont créé leurs propres équipes de policiers spécialisés dans la lutte contre le cybercrime, l'absence d'une chapelle fédératrice a fait que les capacités des forces de l'ordre sont restées éparpillées.

En termes de ressources déployées pour lutter contre la cybercriminalité, les provinces n'ont effectivement pas toutes la même réponse. « Tous les services de police au Canada n'ont pas d'unités spécialisées en cybersécurité. Ce serait impossible autant à financer qu'à combler tous les postes, justifie Bob Gordon, conseiller stratégique de l'Échange canadien des cybermenaces (Canadian Cyber Threat Exchange - CCTX).

« Mais la Police provinciale de l'Ontario a sa propre unité spécialisée dans le cybercrime, la police de la Ville de Toronto aussi, ainsi que la Sûreté du Québec. De plus, la police de Calgary a un ou deux agents spécialisés dans la lutte contre la cybercriminalité. »

Il ajoute que « d'autres services de police à travers le Canada, surtout ceux de grande taille, ont probablement aussi une certaine capacité locale en matière de lutte contre la cybercriminalité ».

Étant donné que les services de police provinciaux n'ont pas forcément le mandat international, ni l'accès ouvert à un certain niveau de l'information, le rôle du CNC3 est justement d'établir des ponts et des liens permettant à l'information de circuler de façon sécurisée et coordonnée. « Notre rôle principal est de déterminer avec quels services de polices municipaux et quelles équipes nous travaillons dans le cadre d'une enquête. C'est ainsi qu'un service de police municipal peut, à travers le Centre, se connecter avec des organisations à l'international comme Europol, lorsqu'une enquête en cours l'exige », précise Chris Lynam.

Élargir le champ d'action

Le CNC3, qui a la qualité d'un service de police national, et qui est basé à Ottawa, disposait à fin 2020 de 80 employés entre gendarmes, fonctionnaires civils, analystes du renseignement et spécialistes techniques.

« Comme les cybercriminels sont innovatifs, nous devons avoir une équipe diversifiée et multitâches pour élargir notre champ d'action et pouvoir ainsi s'adapter aux différentes situations qui se présentent. Cela exige des profils particuliers qui sont attirés par les défis et les nouvelles technologies », indique-t-il.

Il reste cependant que certains services de police ne sont pas membres de l'organisation, en plus du fait que le Centre ne soit pas présent dans toutes les

provinces. Ce qui peut entraver le partage de l'information. Il faut comprendre que le nombre d'employés dont il dispose peut paraître inadapté par rapport à l'importante mission qui lui échoit.

Chris Lynam, reste tout de même optimiste : « Nous sommes un nouveau Centre et cela prend du temps pour établir des relations avec les différents services de police. Ce qui est intéressant, c'est que les différents services de police canadiens sont particulièrement motivés pour travailler et lutter ensemble contre la cybercriminalité », assure-t-il.

Il précise également qu'il s'agit d'un domaine très complexe et qui exige une certaine connaissance et une maîtrise des outils nécessaires pour lutter contre la cybercriminalité.

« Cela va prendre un peu de temps pour que la communauté puisse améliorer ses capacités, mais la motivation est là. C'est justement le rôle du Centre d'aider les différents acteurs et organisations à améliorer leurs capacités », ajoute-t-il.

Le directeur général du CNC3 reconnaît, toutefois, que toute organisation qui jouit de plus de moyens, a forcément un meilleur rendement.

Coopération internationale

Mais le Centre canadien de lutte contre la cybercriminalité compte déjà un bon exploit à son actif.

Fin 2021, une compagnie basée en Alberta s'était rapprochée de la police municipale après avoir été la cible d'une cyberattaque. Ce signalement a aussitôt permis au CNC3 de se connecter à une enquête internationale

et de recenser, plus tard, une centaine de victimes au Canada. L'opération surnommée "GoldDust", qui a connu la participation de 17 pays, a permis, en novembre 2021, l'arrestation d'un large réseau de cybercriminels notamment en Europe de l'Est.

« Il y a eu quelques arrestations en Ukraine, peu avant la guerre. Quelques mois plus tard, la Russie a arrêté des suspects connectés au groupe principal nommé Rival. Leur matériel a été saisi », raconte fièrement Chris Lynam.

Pour le haut gradé de la GRC, les États-Unis sont un partenaire clé, mais son organisation travaille régulièrement avec des agents de la police européenne (Europol) et en Australie aussi.

Le Canada et les États-Unis font aussi partie d'une organisation du nom de Joint Cybercrime Action Taskforce (J-CAT). Dix-huit pays y siègent à travers leurs agences fédérales ou leurs services de police. La GRC y compte deux représentants permanents qui travaillent à même le siège de l'organisation, situé aux Pays-Bas.

« Il y a un lieu où tous les représentants sont réunis et cela nous permet de recevoir l'information en temps réel, à travers nos deux agents », ajoute-t-il.

Avenir et perspectives

Sur un autre chapitre, et afin d'avoir une vision nationale sur le cybercrime, le CNC3 travaille présentement sur une plateforme pancanadienne pour recueillir les signalements des citoyens et des entreprises victimes de cyberattaques.

« Notre objectif est de parvenir à faciliter la tâche aux usagers et de leur permettre d'effectuer des signalements, tout en constituant, en arrière-plan, une base de données qui nous permet de faire le lien entre les différentes attaques », explique-t-il.

Le CNC3 a actuellement mis sur pied un prototype de plateforme qui reçoit un maximum de 25 signalements par jour, en attendant le lancement du nouveau site web qui devrait être fonctionnel d'ici fin 2023.

Illustration : RIENNEPRESS - Tanguy Maerten

Une **législation fédérale** en constant **besoin d'améliorations**

Sous l'impulsion de l'Europe, le Canada a fait de la cybersécurité une priorité en 2010. Mais quelles que soient les stratégies mises en place et les lois adoptées, la cybercriminalité restera toujours un défi impossible à contrôler pleinement.

Écrit par **Camille HARPER**

La question de la cybercriminalité est une préoccupation majeure pour le Canada depuis près de 15 ans. En 2010, une première Stratégie fédérale pour la cybersécurité a vu le jour suite à l'arrivée du premier rançongiciel actif et rentable : Xorist.

Bob Gordon, architecte de cette stratégie à l'époque et aujourd'hui conseiller stratégique de l'Échange canadien des cybermenaces (Canadian Cyber Threat Exchange - CCTX), précise : « Elle avait pour objectif de renforcer la façon dont le gouvernement protégeait les informations qu'il détenait.

« Mais, le paysage de la cybersécurité évoluant constamment, une deuxième Stratégie a remplacé la première en 2018. » De cette deuxième Stratégie est notamment né le Centre national de la coordination de la cybercriminalité (CNC3) de la Gendarmerie royale du Canada, qui devrait être pleinement fonctionnel en 2023-2024, et le Centre canadien pour la cybersécurité.

De nouveau aujourd'hui, les menaces sont devenues de plus en plus variées. « Ce ne sont plus seulement les gouvernements qui sont attaqués, ce sont aussi les entreprises et les individus », mentionne Bob Gordon.

Au niveau des lois

Dans la législation canadienne, les trois dispositions les plus pertinentes entourant la cybercriminalité portent sur l'interception de communications (article 184 du *Code criminel* (1)), l'accès et l'obtention frauduleuse de services d'un ordinateur (article 342.1), incluant l'abus de dispositifs comme utiliser un cloneur de carte de crédit par exemple, et les méfaits à l'égard de données informatiques (article 430.1.1).
En cas de dépôt d'argent, l'article 380 sur la fraude est également à prendre en compte. Et s'il y a vol d'identité, ce sont les articles 402.2 et 403.

La loi fédérale dit aussi que toute personne ayant été victime d'une attaque informatique doit en aviser le Commissariat à la protection de la vie privée.

Me Nicolas Vermeys, professeur titulaire de droit à l'Université de Montréal, précise que « ces dispositions ont été retouchées et modernisées en 2015 pour mieux respecter la *Convention de Budapest*, signée par le Canada

Illustration : Yahia Lahrech | Photo : Gracieuseté

le 23 novembre 2001 et ratifiée le 1er novembre 2015 » (2).

L'influence européenne

En effet, si la cybercriminalité est incluse dans le *Code criminel* canadien depuis le gouvernement de Stephen Harper, c'est l'Europe qui a précipité cette inclusion.

Me Nicolas Vermeys raconte : « Le point de départ des modifications au *Code criminel* du Canada pour y inclure des lois entourant les cas de cybercriminalité, ça a été la convention européenne sur la cybercriminalité, dite *Convention de Budapest*. En la signant, le Canada s'est engagé à faire des modifications à ses lois pour mieux répondre aux exigences de la convention quand il traitait les cybercrimes. »

La *Convention de Budapest* est le premier traité international qui aborde les crimes informatiques et à travers Internet, dont la pornographie juvénile. Son objectif est d'harmoniser les lois nationales et d'améliorer la coopération internationale et les techniques d'enquête en matière de cybercriminalité, mais aussi de rehausser la protection des droits et libertés des citoyens et citoyennes des pays signataires.

Me Nicolas Vermeys précise que « la Convention n'a aucune force de loi comme telle, mais elle engage les pays qui la signent à modifier leurs lois ».

En octobre 2022, 67 pays avaient ratifié la *Convention de Budapest*. (voir encadré.)

Par ailleurs, la naissance de la ***Loi sur la protection des renseignements personnels et les documents électroniques*** (LPRPDE), en 2000, avait également été précipitée par l'Europe.

Me Vermeys : « En 1995, une directive européenne a déclaré que si une entreprise canadienne voulait faire affaire avec l'Union européenne, elle devait être soumise à une loi équivalente à la loi européenne. Comme le Canada fait beaucoup affaire avec l'Europe, une loi fédérale a été adoptée. »

Des lois à la traîne

Il ajoute que « les clauses du *Code criminel* entourant la cybercriminalité ont été rédigées de façon très large afin de couvrir la plupart des innovations technologiques récentes et à venir. La notion "d'ordinateur", par exemple, inclut tout dispositif informatique, entre autres les guichets automatiques ».

« C'est là le nœud du problème en matière de cybersécurité, fait remarquer Me David Davis, avocat spécialisé en cybercriminalité à Winnipeg : Internet évolue trop vite, donc il est quasiment impossible de faire une loi qui couvre tout. Quand on croit y parvenir, par le temps que le projet de loi est adopté et la nouvelle loi proclamée, il est déjà trop tard. Les cybercriminels ont trouvé d'autres moyens d'agir et il y a des nouveaux problèmes sur lesquels il faudrait légiférer.

« On ne peut pas non plus accélérer le processus d'adoption des lois car en démocratie, il est essentiel de donner la parole aux différents groupes d'intérêts concernés avant chaque vote de loi. »

Des lois inefficaces

En outre, les quelques lois qui existent au Canada n'ont pas assez de force pour dissuader les criminels d'accomplir leurs méfaits, et la majorité des démantèlements ne touchent que les cybercriminels du "coin de la rue", autrement dit les moins dangereux. C'est le constat de Me Brandon Trask, professeur adjoint à la Faculté de droit de l'Université du Manitoba, qui a été procureur en Nouvelle-Écosse de 2016 à 2020 et a jugé des cas de cybercriminalité.

« La loi n'est pas à la hauteur. Tout d'abord, les chances de se faire attraper sont très minces car il est très difficile et coûteux en temps et en argent de prouver le crime au-delà de tout doute raisonnable. Si on ne peut pas obtenir de preuves, on ne peut pas poursuivre en justice. »

Bertrand Milot, fondateur et président d'une entreprise québécoise et conférencier en cyberintelligence, confirme qu'il est « très difficile de réussir à relier un méfait à un cybercriminel. Or pour réussir un démantèlement, il faut pouvoir prendre le cybercriminel la main dans le sac ».

Me Brandon Trask ajoute que « même quand un criminel est déclaré coupable, en particulier pour des crimes de nature non sexuelle, la sentence n'est souvent pas si élevée en comparaison avec les centaines de milliers de dollars que peut coûter l'enquête. Pour les Provinces, ce n'est juste pas rentable. »

Photo : Gracieuseté

« Les cybercriminels utilisent de la cryptomonnaie, ce qui est très difficile à récupérer ou confisquer, précise Bertrand Milot. L'argent criminel récupérable est souvent lié au compte bancaire légitime de l'individu, qui lui-même est en général assez vide. »

Les lois canadiennes actuelles ne prévoient pas non plus d'amendes pour les entreprises qui ont failli à leur devoir de protéger les données personnelles d'employés ou de clients en leur possession. Ceci pourrait toutefois changer si le projet de loi C-26 est adopté.

« Les entreprises auraient alors l'obligation d'avoir un véritable plan de cybersécurité et d'être préparées à tout scénario de cyberattaque, sous peine d'amende. Ce serait un progrès », déclare Me David Davis.

Quelle juridiction ?

L'ancien procureur néo-écossais constate par ailleurs que « dans les cas de cybercrimes non sexuels, la coopération entre les pays est moins développée que pour les cybercrimes à caractère sexuel ou les crimes à enjeu léthal. Donc même s'il est techniquement possible de poursuivre quelqu'un en dehors du Canada si la victime est canadienne, en pratique, c'est très difficile ».

Me David Davis renchérit : « Le problème, c'est qu'Internet est un monde sans frontières. Le plus souvent, le cybercriminel est dans un tout autre pays que la victime. Dans ce cas, quelle juridiction doit s'en occuper ? Qui va contrôler ? Si un pays s'occupe de la justice dans un autre pays, c'est souvent considéré comme de l'ingérence.

« Nous n'avons pas encore trouvé la solution à ce problème. Il faudra peut-être une législation internationale contre le piratage informatique, à laquelle tous les pays pourront adhérer. On doit réfléchir à des moyens de poursuivre les cybercriminels, même lorsqu'il ne s'agit pas de pornographie juvénile ou de crime à enjeu léthal. »

Le directeur de la Clinique de cyber-criminologie de l'Université de Montréal, Akim Laniel-Lanani, rappelle cependant que « les lois sont toujours en retard sur les cybercriminels, donc le défi dépasse largement la simple question d'une loi.

« Le problème, c'est surtout le manque de connaissances sur la cybercriminalité, de ressources humaines, financières et technologiques au niveau mondial, ou encore de pression sur les décideurs. Un droit international comme la signature d'une convention ou d'un traité pourrait au moins imposer qu'il y ait plus de fonds alloués à la lutte globale contre la cybercriminalité. »

L'expert en cybercriminologie ajoute que « les dernières recherches académiques mettent beaucoup plus l'accent sur les partenariats public/privé comme solution que sur un simple changement ou ajout de loi contre le piratage informatique.

« Dans ce cas, il faudrait néanmoins modifier la loi pour faciliter la coopération et le partage de renseignements entre le public et le privé, toujours dans le respect des droits de la personne ».

(1) Code criminel (LRC (1985), ch. C-46)

(2) Conseil de l'Europe - Convention sur la cybercriminalité (STE n° 185)

(3) *The Personal Information Protection and Electronic Documents Act (PIPEDA) - Office of the Privacy Commissioner of Canada*

LES 67 PAYS SIGNATAIRES DE LA CONVENTION DE BUDAPEST SONT :

- Albanie
- Allemagne
- Andorre
- Argentine
- Arménie
- Australie
- Autriche
- Azerbaïdjan
- Belgique
- Bosnie-Herzégovine
- Bulgarie
- Canada
- Cap Vert
- Chili
- Chypre
- Colombie
- Croatie
- Danemark
- Espagne
- Estonie
- États-Unis d'Amérique
- Finlande
- France
- Géorgie
- Ghana
- Grèce
- Hongrie
- Île Maurice
- Islande
- Israël
- Italie
- Japon
- Lettonie
- Liechtenstein
- Lithuanie
- Luxembourg
- Macédoine du nord
- Malte
- Maroc
- Moldavie
- Monaco
- Montenegro
- Norvège
- Panama
- Paraguay
- Pays-Bas
- Pérou
- Philippines
- Pologne
- Portugal
- République dominicaine
- République tchèque
- Roumanie
- Royaume-Uni
- Saint-Marin
- Sénégal
- Serbie
- Slovaquie
- Slovénie
- Sri Lanka
- Suède
- Suisse
- Tonga
- Trinité-et-Tobago
- Tunisie
- Turquie
- Ukraine

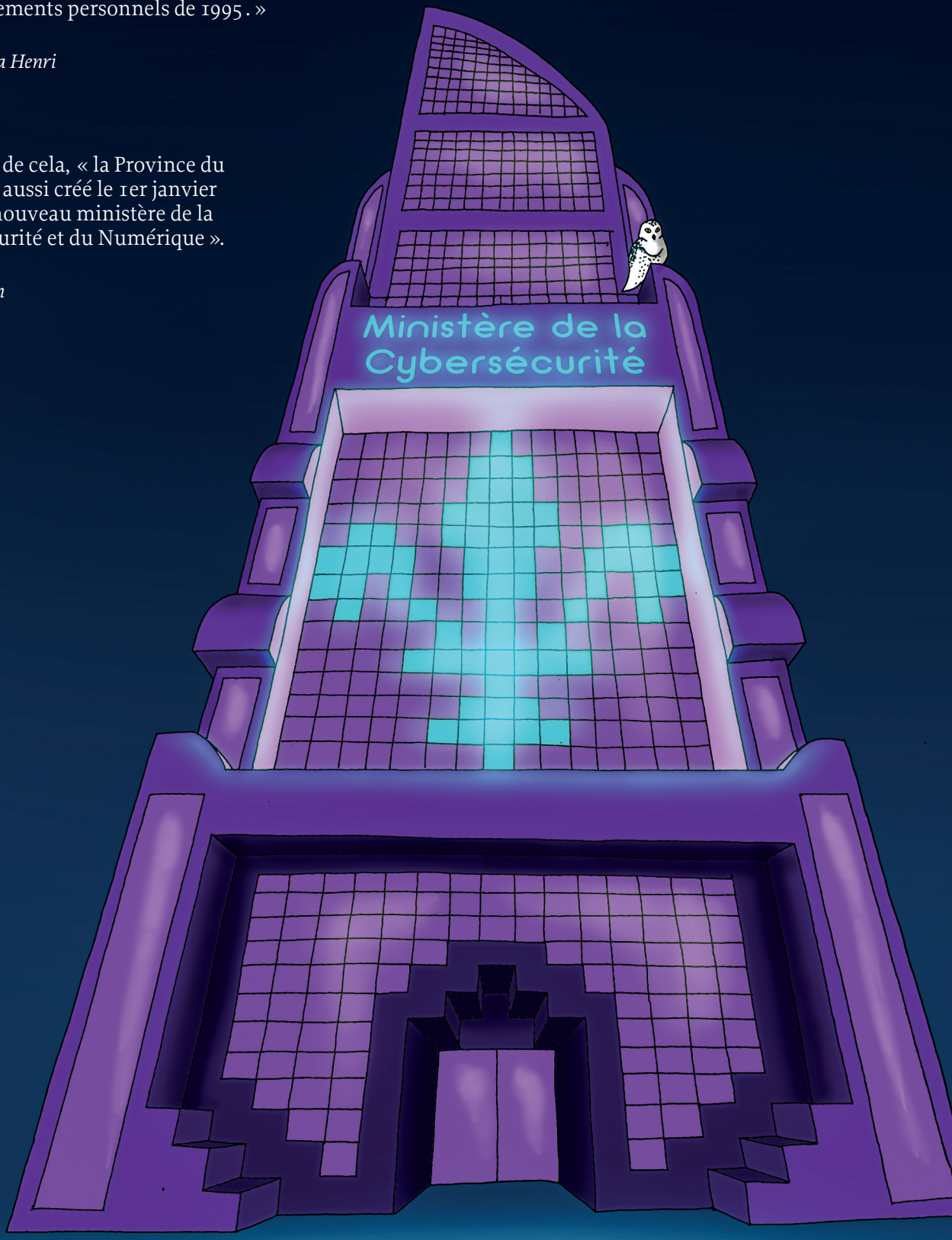
Photo : Gracieuseté

« Le 21 septembre 2021, pour préserver ses relations avec la France, le Québec a adopté le projet de loi C-64 qui modifiait la Loi 25 modernisant des dispositions législatives en matière de protection des renseignements personnels de 1995 . »

Me Vanessa Henri

À la suite de cela, « la Province du Québec a aussi créé le 1er janvier 2022 un nouveau ministère de la Cybersécurité et du Numérique ».

Bob Gordon



Des lois et des stratégies variables

En matière de cybercriminalité au Canada, dix des 13 provinces et territoires suivent la loi fédérale et trois provinces, le Québec, l'Alberta et la Colombie-Britannique, ont adopté leur propre loi provinciale.

Écrit par **Camille HARPER**

Les provinces et territoires canadiens ne sont pas tous égaux en matière de cybercriminalité. Par exemple, certaines provinces ont choisi d'adopter leurs propres lois en complément des lois fédérales. C'est le cas du Québec, de l'Alberta et de la Colombie-Britannique.

Les articles 91 et 92 de la *Loi constitutionnelle* définissent les champs de compétences fédérale et provinciale, mais la question de la cybersécurité reste floue. Le professeur de droit à l'Université de Montréal, Me Vermeys, en explique la raison : « En 1867 quand la *Loi constitutionnelle* a été écrite, il n'y avait pas de notion de cybercriminalité ni de protection des données personnelles.

« Quand la loi ne le précise pas, c'est le plus souvent considéré comme une compétence fédérale, mais cette question de la protection des renseignements personnels fait débat. C'est pourquoi certaines provinces ont adopté une loi provinciale, et d'autres non. »

Au Manitoba

Pour sa part, le Manitoba est principalement régi par les lois fédérales en matière de cybercriminalité et de cybersécurité.

On peut cependant souligner quelques lois manitobaines pertinentes pour renforcer la cybersécurité des particuliers : la *Loi modifiant la Loi sur l'accès à l'information et la protection de la vie privée*, entrée en vigueur le 1er janvier 2022, qui réglemente la façon dont les organismes publics gèrent les renseignements personnels, ou encore la *Loi sur les renseignements médicaux personnels* entrée en vigueur le 1er juin 2022.

Ailleurs au Canada

Tout comme le Manitoba, l'Ontario, la Saskatchewan et l'Île-du-Prince-Édouard n'ont pas de loi provinciale sur la cybersécurité.

« Plutôt que de toutes passer par un même long processus de création d'une nouvelle loi de toutes pièces, ces provinces ont voté que chez elles, la loi fédérale s'appliquerait aussi à ce qui relève de la juridiction provinciale », explique Bob Gordon, conseiller stratégique de l'Échange canadien des cybermenaces (Canadian Cyber Threat Exchange - CCTX).

Toutefois, l'Ontario a lancé en 2019 sa toute première Stratégie pour la cybersécurité. Et en 2020, la Province a mis sur pied un panel d'experts sur la cybersécurité, qui a analysé l'état de la cybersécurité dans la province et rendu son rapport avec recommandations à l'automne 2022.


Bob Gordon

Pour sa part, le Nouveau-Brunswick a une loi provinciale, mais elle est spécifique au secteur de la santé et complémentaire de la *Loi fédérale sur la protection des renseignements personnels et les documents électroniques*. Les deux lois s'appliquent donc.

Quant au Québec, à l'Alberta et à la Colombie-Britannique, elles ont chacune adopté leurs propres lois provinciales en matière de cybersécurité. Ce sont elles qui s'appliquent dans leurs provinces respectives.

Le cas du Québec

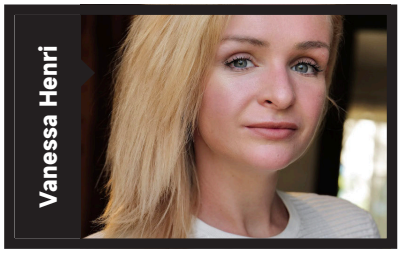
En matière de cybersécurité, le Québec n'a pas attendu le fédéral

Illustration : RIENNEPRESS - Tanguy Maerten — Photo : Gracieuseté

pour agir. Me Vanessa Henri, avocate québécoise spécialiste en cybersécurité et gouvernance des données, explique que « le 21 septembre 2021, pour préserver ses relations avec la France, le Québec a adopté le projet de loi C-64 qui modifiait la *Loi 25 modernisant des dispositions législatives en matière de protection des renseignements personnels* de 1995 ».

À la suite de cela, « la Province du Québec a aussi créé le 1er janvier 2022 un nouveau ministère de la Cybersécurité et du Numérique », une première au pays, ajoute Bob Gordon.

Avec la modernisation de la loi, la Commission d'accès à l'information du Québec a notamment plus de pouvoirs : l'un d'entre eux sera d'élaborer des lignes directrices pour faciliter l'application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, et de la *Loi sur la protection des renseignements personnels dans le secteur privé*, mais aussi d'imposer des amendes aux contrevenants.



Me Vanessa Henri poursuit : « Les responsabilités des directeurs d'entreprises, des organismes et des partis politiques québécois sont renforcées. » Ces derniers devront notamment mettre en place des mesures pour atténuer les risques d'atteinte au droit à la vie privée, et ce progressivement jusqu'à septembre 2024. Tout incident de confidentialité devra de plus être signalé à la Commission d'accès à l'information.

Plus précisément, les chefs d'entreprises devront désigner une personne responsable de la protection des renseignements personnels, qui sera en charge de veiller à ce que la loi soit bien appliquée, et que les pratiques de collecte, traitement et communication de données personnelles soient optimales.

Ils devront également établir un plan de gouvernance en matière de protection des renseignements personnels, qui définira de façon transparente et publique, les pratiques de l'entreprise relatives à la collecte, la conservation puis la destruction de données, les rôles et responsabilités de chaque personne impliquée dans ce processus, ainsi que le processus de réception et traitement des plaintes.

D'ailleurs, toute personne concernée par une collecte de ses données devra clairement donner son consentement à une telle collecte. C'est une nouvelle obligation légale pour les entreprises de demander ce consentement et de fournir toutes les informations nécessaires pour qu'il soit éclairé. De même, si la collecte permet une localisation ou un profilage de la personne, celle-ci doit être mise au courant à l'avance et se voir offrir l'option de désactiver ces fonctions.

« La loi donne aussi plus de clarté sur la durée pendant laquelle on peut garder des données. C'est important car un grand nombre de cyberattaques ont lieu sur des données que les entreprises n'auraient plus dû avoir », a constaté Me Vanessa Henri dans sa pratique.

En résumé, « cette loi modernisée a beaucoup plus de dents qu'avant, se réjouit l'avocate. On est passé d'une loi réactive à une loi proactive ».

Quels moyens ?

Du côté des juristes, les ressources qualifiées manquent à l'appel. Selon la Fédération des ordres professionnels de juristes du Canada, le pays compte plus de 136 000 avocats, et parmi eux, le professeur adjoint de droit à l'Université du Manitoba, Me Brandon Trask, estime qu' « une cinquantaine à une centaine sont spécialisés en cybercriminologie. C'est très peu ».

Me Ruphine Djuissi, avocate manitobaine, annonce cependant qu'au Manitoba, « le Barreau a récemment pris des dispositions pour que tous ses membres suivent une formation obligatoire sur la cybercriminalité ».

Du côté technique, une question que la plupart des Provinces se posent en effet est : *Comment créer la main-d'œuvre suffisante, avec l'expertise nécessaire, pour résoudre adéquatement la question de la cybersécurité ?*

Bob Gordon rapporte que « la majorité des provinces mettent en place une variété d'initiatives dans ce sens. En Ontario par exemple, on a le Rogers Cybersecure Catalyst à la Toronto Metropolitan University. Et au Manitoba, début 2020, le Centre d'excellence technique sur la cybersécurité (Cyber Security Technical Centre of Excellence) a ouvert ses portes au Manitoba Institute of Trades and Technology ».

Photo : Gracieuseté

Pourquoi le Canada repense sa politique en cybersécurité

De l'avis du professeur à l'École nationale de l'administration publique, Stéphane Roussel, expert en stratégie et défense, il était devenu « urgent » pour le Canada de sécuriser ses infrastructures essentielles, en optant pour l'amendement de la Loi sur les télécommunications. Les informations obtenues par La Liberté auprès du Centre canadien pour la cybersécurité en disent long.

Écrit par **Mehdi MEHENNI**

À l'heure où la scène géopolitique mondiale connaît des bouleversements majeurs, avec notamment la guerre en Ukraine et les tensions grandissantes entre l'Amérique du Nord et la Chine, le Canada revoit sa politique en matière de cybersécurité. C'est dans cet esprit que le gouvernement fédéral a décidé de réformer la *Loi sur les télécommunications* pour protéger ses infrastructures essentielles, liées notamment aux secteurs de l'énergie, des finances, de la santé et du transport, contre les cyberattaques.

En déposant, le 14 juin 2022 à la Chambre des Communes, le projet de loi C-26 portant sur la cybersécurité, toujours en attente - à l'heure de passer sous presse - d'adoption au niveau du parlement, le ministre de la Sécurité publique, Marco Mendicino, désignait la sécurité numérique comme étant, désormais, un "objectif politique". « Le gouvernement aura une autorité claire d'imposer toute action pour sécuriser les systèmes de télécommunication, y compris d'interdire aux entreprises d'utiliser des produits et des services de fournisseurs à haut risque », lit-on dans un communiqué du ministère de la Sécurité publique diffusé à l'occasion.


Stéphane Roussel

Ces mesures, qui peuvent être considérées par certaines parties comme restrictives en matière de liberté d'entreprendre, revêtent cependant un caractère "urgent" aux yeux de Stéphane Roussel, professeur titulaire à l'École nationale de l'administration publique (ENAP).

« Avec les attaques qui ont ciblé, récemment, de grandes entreprises comme Bombardier produits réactifs (BRP), il était devenu urgent de protéger les infrastructures qui peuvent avoir un impact sur la vie économique ou la sécurité des citoyens », soutient celui qui est également titulaire de la Chaire de recherche en politiques étrangère et de défense canadiennes.

L'universitaire pense particulièrement aux hôpitaux, dans le cas où une cyberattaque venait à paralyser le système de santé du Canada. « Ce sont des milliers de patients qui verraient leurs rendez-vous retardés, et d'autres leurs opérations chirurgicales déprogrammées. Ce serait une catastrophe pour la population », estime -t-il.

Une crainte d'autant plus légitime que la Grande-Bretagne, pays allié du Canada, a vu en 2017 son service public de santé (NHS) paralysé. Pour rappel, des pirates informatiques avaient bloqué l'accès aux fichiers des utilisateurs de centaines de structures hospitalières, via un logiciel malveillant appelé "Wannacry".

Photo : Gracieuseté de l'École nationale de l'administration publique (ENAP)

Insécurité générale

Si Stéphane Roussel redoute un tel scénario, c'est que le contexte est marqué par « une Russie devenue subitement très menaçante » et que « la participation du Canada et son aide à l'Ukraine en font une cible ».

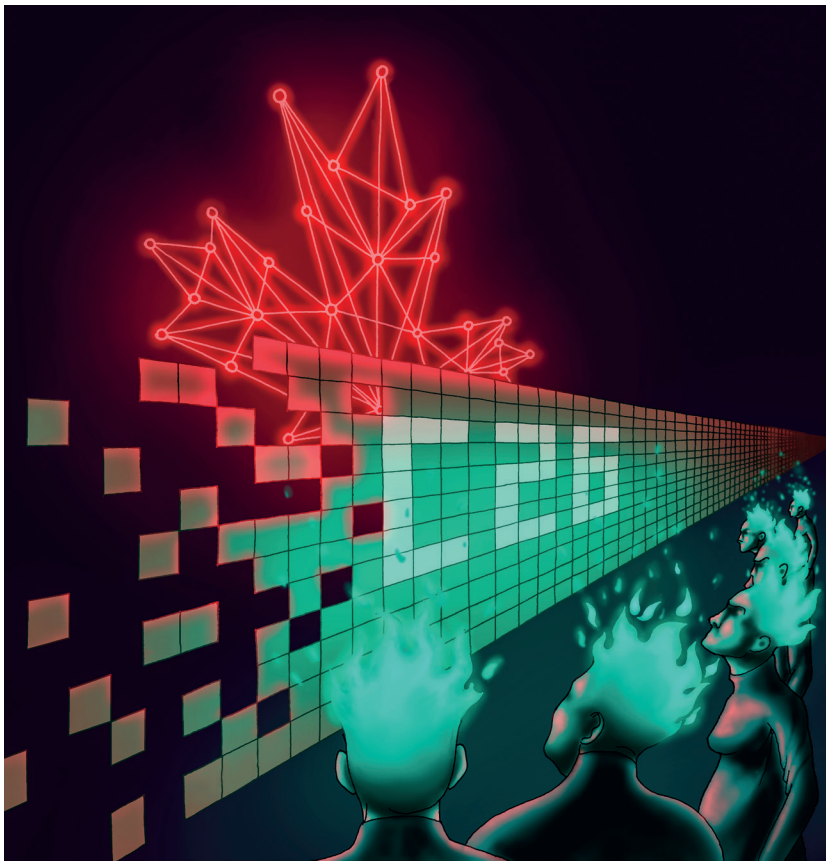
« Le niveau d'insécurité générale a été rehaussé, que ce soit pour la sécurité physique, la cybersécurité ou la sécurité économique et financière. Tout cela est lié à la guerre en Ukraine », estime-t-il.

À cette situation s'ajoute les tensions avec la Chine, devenue aujourd'hui une grande puissance dans le domaine des technologies de l'information. « Le Canada a eu de très mauvaises expériences avec la Chine durant les dernières années. Je pense que ça va devenir un sujet de préoccupation », prévient le professeur à l'ENAP.

Pour preuve, le Centre canadien pour la cybersécurité a publié, durant les derniers mois, plusieurs bulletins, rapports et conseils sur les cybermenaces sur le site cyber.gc.ca.

Il est explicitement demandé à la collectivité canadienne de la cybersécurité, tout particulièrement aux responsables de la défense des réseaux des infrastructures essentielles, de renforcer leur sensibilisation et leur protection contre les cybermenaces d'envergure.

« On invite tous les secteurs des infrastructures essentielles du Canada à faire preuve de vigilance et à tenir compte de la possibilité d'une augmentation des activités de cybermenace », déclare Evan Koronewski, porte-parole au Centre de la sécurité des télécommunications (CST), organisme duquel dépend le Centre canadien pour la cybersécurité.



Les rapports du gouvernement

En 2021, le Centre canadien pour la cybersécurité avait d'ailleurs détecté 304 attaques par rançongiciel qui ont ciblé des Canadiens et Canadiennes. La moitié des victimes avait un lien avec des infrastructures essentielles.

« Il est important de se rappeler que nous formulons ces avertissements en raison de l'augmentation des risques liés aux cybermenaces. Ces avertissements sont basés sur les rapports de renseignement du gouvernement », explique Evan Koronewski.

Le message est on ne peut plus clair. Raison pour laquelle le porte-parole du CST recommande aux partenaires des infrastructures essentielles du Canada de « prendre les mesures nécessaires pour protéger leurs systèmes d'importance, notamment en menant des activités préventives de surveillance des réseaux et en prenant des mesures d'atténuation immédiates ».

Enfin, et attendant un débat national sur le projet de loi C-26, le professeur Stéphane Roussel considère qu'il était important d'envoyer un signal fort aux partenaires du Canada, pour les rassurer sur la viabilité des systèmes de défense du pays.

Illustration : RIENNEPRESS - Tanguy Maerten

Une **loi avec des dents** pour mieux **protéger** les **citoyens**

Déposé à la Chambre des communes en juin 2022, le projet de loi C-27 vise à mettre à jour la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE).

Écrit par **Camille HARPER**

Me Ruphine Djuissi, avocate d'Infojustice au Manitoba, explique les raisons du dépôt en chambre du projet de loi C-27 : « C'est important de protéger la vie privée des consommateurs et de s'assurer que leurs données sont bien protégées, car les Canadiens et Canadiennes font de plus en plus d'achats en ligne. »

Le projet de loi prévoit entre autres la mise sur pied d'un Tribunal de la protection des renseignements personnels et des données, qui entendra les appels des décisions du Commissaire à la protection de la vie privée et qui pourrait infliger jusqu'à plusieurs millions $ d'amende en cas de contravention à la loi.

« Avec un tribunal spécifique, les consommateurs seront plus rassurés, anticipe Me Djuissi. Ce sera plus direct, et le tribunal pourra frapper plus fort. Pour le moment, il n'y a que l'ombudsman, qui n'est que médiateur et fait seulement des recommandations. »

De plus, « de nouveaux pouvoirs d'enquête sont attribués au Commissaire à la protection de la vie privée. Il avait déjà le pouvoir d'examiner les plaintes, il pourra aussi, si ce projet de loi est adopté, imposer des mesures et faire des accords avec les entreprises contrevenantes ».

Enfin, le projet de loi C-27 veut créer la première *Loi canadienne sur l'intelligence artificielle et les données*. Ce serait la première fois que l'intelligence artificielle est inscrite dans la loi.

Un projet de loi avec des dents

Me David Davis, avocat winnipégois dans le domaine de la cybersécurité, se réjouit tout autant du dépôt en Chambre du projet de loi C-27.

« S'il est adopté, le projet de loi C-27 donnera plus de dents à la Loi. Ce sera notamment la responsabilité des entreprises de rapporter les cyberattaques dont elles sont victimes et si elles ne le font pas, elles pourraient payer des amendes de plusieurs millions de dollars ou 5 % de leur revenu global, selon la somme la plus élevée des deux. Ce sont des sanctions très sévères, en particulier comparé à ce qui existe dans la législation actuelle, c'est-à-dire aucune sanction pécuniaire réelle, et ceci va certainement renforcer l'intérêt des entreprises à bien suivre la loi ! »

Il entrevoit toutefois un potentiel problème éthique autour de la définition d'un incident de cybersécurité. « Puisque la technologie et les techniques des cybercriminels évoluent constamment, la définition d'un cyberincident est elle aussi, par conséquent, évolutive.

« Le projet de loi C-27 impose aux entreprises de rapporter toute cybermenace qui les touche. À partir de quand une entreprise devrait-elle considérer un incident comme digne d'être rapporté aux autorités ? Ne risque-t-on pas de créer une peur inutile dans la société ? Les entreprises ont-elles droit à un

Photo : Gracieuseté

temps d'investigation en cas de suspicion de problème ? »

Des juristes majoritairement optimistes

Un projet de loi similaire était mort au feuilleton en 2019-2020, en raison des élections fédérales. Me Ruphine Djuissi reste optimiste : « C-27 a beaucoup de chances de passer car c'est dans l'intérêt du Canada de mieux protéger les Canadiens et Canadiennes. Avoir un e-commerce fiable et sécuritaire va permettre de rehausser notre pouvoir économique. »

Même son de cloche chez Me David Davis. « Je pense vraiment que le projet de loi C-27 sera adopté. Certes, cela pourrait prendre du temps et beaucoup de discussions car c'est un projet de loi très important et essentiel dans le monde actuel, et tous les partis politiques voudront avoir leur mot à dire dedans, mais tous s'accordent sur le fait que c'est nécessaire et dans l'intérêt de toutes et tous de faire ce travail et d'amender au plus vite la législation actuelle. J'imagine que le projet de loi sera adopté d'ici la fin 2023. »

En revanche, Me Vanessa Henri, du cabinet québécois Henri & Wolf, s'avance beaucoup moins : « Le projet de loi C-27 crée un tribunal de données et ajoute à la loi une partie sur l'intelligence artificielle. C'est très ambitieux. À mon avis, ça risque de ne pas passer. »

Selon Bob Gordon, conseiller stratégique de l'Échange canadien des cybermenaces (Canadian Cyber Threat Exchange - CCTX), « une fois que le projet de loi en sera à l'étape des comités parlementaires, on aura une meilleure idée des points de contention et de son avenir.

« Mais ce qui est sûr, c'est que tout le monde s'accorde à dire que la cybercriminalité est un problème et qu'il faut trouver des solutions pour le résoudre. Et que tous, même le Commissaire à la protection de la vie privée, estiment que la LPRPDE actuelle doit être modernisée car elle est difficile à appliquer au contexte d'aujourd'hui. »

Illustration : RIENNEPRESS - Tanguy Maerten

CONSEILS PRATIQUES

Sur les conseils de William Georges Khouri, architecte en cybersécurité au sein d'une compagnie spécialisée en cyberintelligence au Québec, la rédaction vous donne quelques astuces pour utiliser Internet de la façon la plus sécuritaire possible.

À FAIRE	À NE PAS FAIRE
LES MOTS DE PASSE : • un mot de passe long, composé d'au moins 12 caractères, mêlant majuscules, minuscules, caractères spéciaux et chiffres. Idéalement, une phrase dont vous vous rappellerez suivie d'une date. • Avoir un mot de passe différent pour chaque site web ou réseau social • Pour se faciliter la vie, utiliser un gestionnaire de mots de passe. • Multiplier les facteurs d'identification quand c'est possible : applications d'authentification, données biométriques etc.	**LES MOTS DE PASSE :** • Communiquer son mot de passe à autrui. • Composer son mot de passe avec des informations qui sont disponibles sur vos réseaux sociaux : date de naissance, prénoms de vos enfants ou de vos animaux de compagnie, etc. • Enregistrer vos mots de passe et utiliser la fonction de remplissage automatique de Google. En effet, les mots de passe enregistrés par Google ne sont pas protégés.
À PROPOS DES COURRIELS : • Être prudent, même lorsque l'on connaît l'expéditeur, car il pourrait lui-même être compromis sans le savoir. • Se méfier des courriels à caractère urgent ou confidentiel. • Tenir à jour ses applications de messagerie.	**À PROPOS DES COURRIELS :** • Ouvrir une pièce jointe ou cliquer sur un lien URL que vous n'attendez pas. • Communiquer ses informations personnelles. Même votre banquier ne peut pas vous demander vos codes par courriel ou par téléphone.
SUR LE WEB : • Vérifier la fiabilité des sites avant de les visiter, en tapant par exemple : Nom du site + Avis ou review, en utilisant l'outil ScamDoc, ou en consultant Fraude-Alerte.ca. • Se méfier des sites sponsorisés par Facebook, Instagram, etc. Ces derniers ne vérifient pas l'authenticité de ces sites-là. • Tenir à jour son navigateur et son antivirus. • Utiliser un RPV. Aussi appelé VPN, ce logiciel permet de chiffrer vos données personnelles et de prévenir ainsi le risque qu'elles soient volées. Le RPV permet notamment de naviguer sur internet de manière anonyme.	**SUR LE WEB :** • Accepter les cookies sur les sites non-encryptés. Avant d'accepter des cookies, vérifiez qu'une icône de cadenas se trouve à la gauche de l'URL. • Utiliser le Wi-Fi public sans prendre de précautions (pour accéder à ses comptes, faire des achats, etc.) • Partager ses informations ouvertement avec le monde entier.
LORS D'UNE TRANSACTION EN LIGNE : • Se renseigner sur l'entreprise auprès de laquelle vous faites vos achats. • Faire vos achats à partir d'une connexion et d'un endroit sécurisé. Éviter les réseaux Wi-Fi publics. • S'assurer que la page de transaction est encryptée (icône cadenas à gauche de l'URL). • Utiliser l'option "invité" au lieu de se créer un compte. • S'assurer de ne partager que les informations nécessaires à l'achat de vos produits.	**LORS D'UNE TRANSACTION EN LIGNE :** • Enregistrer ses informations de paiement lorsqu'on vous le propose. Même si c'est Amazon. • Utiliser un autre moyen de paiement que sa carte de crédit ou PayPal. • Sauter sur les offres "trop belles pour être vraies" par peur de manquer l'aubaine du siècle.

Si vous soupçonnez qu'un message est frauduleux, ne pas y répondre est la meilleure solution pour votre sécurité et celle de votre famille.
En effet, quand vous pensez avoir détecté une tentative de fraude, même si votre curiosité, votre témérité ou votre âme d'enquêteur naturel vous pousse à tester les réflexes et l'intelligence du criminel, vous passerez alors dans les mains d'un deuxième, voire un troisième niveau de criminalité pour lequel vous n'êtes ni outillé, ni professionnel.
Même si la supercherie vous paraît simpliste, répondre qualifie votre adresse courriel, votre numéro de téléphone ou votre messagerie SMS comme valide et propice à répondre.

MA·LOI·25

Vous avez besoin d'aide pour protéger vos renseignements personnels?

In search of help to protect your personal data?

À la demande du Gouvernement du Québec, **In-Sec-M** – *la grappe nationale de la cybersécurité* – a conçu le programme **MaLoi25** pour accompagner les PMO dans l'**identification de leurs failles** et l'**adoption de meilleures pratiques** en matière de protection des données personnelles.

At the request of the Quebec Government, In-Sec-M – *the national cybersecurity cluster* – has designed the **MaLoi25** program to help SMO **identify their flaws** and **adopt best best practices in the protection of personal data**.

Pour accéder à notre outil d'autodiagnostic et vous inscrire à nos formations
To access our self-diagnosis tool and subscribe for our training courses.

Rendez-vous sur le site MaLoi25.ca

MALOI25.CA

Visit Maloi25.ca

En collaboration avec

Québec

IN·SEC·M