Bulletin d'information e-Veille - Décembre 2009

Protéger son identité : un défi majeur à l'ère d'Internet

D'après la Chaire de recherche du Canada en sécurité, identité et technologie (2009), le vol de renseignements personnels « a frappé 6,7 % de la population adulte canadienne en 2008, ce qui représente environ 1,7 million de personnes » (Sproule et Archer, 2008). « Il a fait environ 340 000 victimes au Québec l'année précédente. [...] Le vol [de renseignements personnels][1]est l'un des crimes connaissant la plus forte croissance depuis quelques années » (Finkleaa, 2009).

Protéger son identité sur le réseau des réseaux n'est pas une mince affaire. Les éléments constituant l'identité – et pouvant être utilisés de façon frauduleuse – sont de divers ordres : sexe, nom, prénom, lieu et date de naissance, noms et prénoms des parents, et dans certains pays le numéro d'assurance sociale. S'y ajoutent également les données financières.

Selon l'Organisation de coopération et de développement économiques (OCDE), il s'avère difficile de donner une définition reconnue internationalement au vol de renseignements personnels relatifs à l'identité : chaque pays le définit différemment. Certains pays le voient comme un crime grave en soi, alors que d'autres le perçoivent comme un délit non criminel ou encore, comme une étape préliminaire à un crime de plus grande envergure. Néanmoins, tous s'entendent généralement pour dire qu'on parle de « vol d'identité », ou plus précisément de vol de renseignements personnels, lorsque « un individu acquiert, transfert, possède ou utilise les renseignements personnels d'une personne morale ou physique sans être autorisé à le faire dans l'intention de commettre un crime ou une fraude ou en lien avec un crime ou une fraude » (OCDE, 2009 : 16). Le vol de renseignements personnels représente donc une étape préliminaire avant de commettre un crime de plus grande envergure, soit l'usurpation d'identité.

Au Canada, le projet de loi S-4[2]modifiant le Code criminel et qui porte sur le vol d'identité et les inconduites connexes fait les mêmes distinctions dans la terminologie à employer. Selon ce projet de loi, le vol d'identité « représente les étapes préliminaires (comme la collecte et la possession de renseignements relatifs à l'identité) » – et réfère en fait au vol de renseignements personnels, alors que la fraude à l'identité ou l'usurpation d'identité « constitue l'usage trompeur subséquent des renseignements relatifs à l'identité d'une autre personne dans le cadre de diverses infractions (comme la supposition de personne, la fraude ou l'usage abusif des données de cartes de crédit) ».

Comment les fraudeurs s'y prennent-ils ?

Plusieurs techniques existent pour collecter frauduleusement des renseignements personnels, que ce soit par Internet ou non. Hors ligne, les fraudeurs peuvent tout simplement tenter de voler les renseignements personnels en espionnant les gens, en regardant par-dessus l'épaule des victimes pour relever leur mot de passe ou en écoutant les conversations pour obtenir des numéros de cartes de crédit. Certains

iront jusqu'à fouiller la cour ou même les rebuts pour débusquer une information, alors que d'autres utiliseront de fausses campagnes publicitaires ou de faux sondages par la poste ou par téléphone pour obtenir des renseignements personnels. Selon Dupont et Louis (2009) de la Chaire de recherche du Canada en sécurité, identité et technologie, l'acquisition frauduleuse de renseignements personnels hors ligne demeure plus répandue au Canada que la fraude en ligne. Sur Internet, les deux principales façons de voler des renseignements personnels consistent à propager un virus informatique ou un autre logiciel malveillant et à recourir à l'hameçonnage. D'ailleurs, d'après la Gendarmerie royale du Canada (GRC),

> [...] de plus en plus, les renseignements personnels sont échangés et vendus en ligne sur des sites Web restreints, par voie de messagerie instantanée et dans des salons de clavardage. [...] Les criminels ont tous accès à d'énormes volumes de renseignements personnels provenant de sources légitimes, ou du commerce criminel en ligne de données. Internet facilite l'anonymat des criminels, ainsi que la capacité de se faire passer pour légitime, comme le démontrent les cas d'hameçonnage. Internet fournit également aux criminels un accès à des centaines ou des milliers de victimes potentielles par voie d'escroquerie ou d'hameçonnage (GRC, 2007).

Même si les vols de renseignements personnels sont plus souvent commis hors ligne, c'est surtout Internet que les fraudeurs utilisent pour usurper l'identité. À quoi servent les renseignements personnels volés ? Selon les enquêtes réalisées par la GRC, la majorité de ces crimes sont commis pour générer des profits financiers. L'usurpation d'identité sert également au trafic de stupéfiants, aux infractions en matière d'immigration, ou encore à camoufler sa véritable identité (surtout dans le cas de criminels qui ont un lourd passé).

Toujours d'après la GRC, les fraudeurs viennent autant des villes que des milieux ruraux. Ils peuvent utiliser immédiatement les renseignements personnels volés, ou les conserver pour y recourir ultérieurement. Certains agissent seuls, alors que d'autres perpètrent la fraude en réseau. Le crime organisé international peut être également dans le coup.

Les Québécois et les Canadiens demeurent prudents

Des données publiées en juillet 2009, tirées de l'enquête NETendances du CEFRIO (Centre francophone d'informatisation des organisations), révèlent que « seulement 8,6 % des adultes québécois ont été victimes d'une fraude ou d'une tentative de fraude par courriel ou sur Internet au cours de la dernière année. En 2008, ils avaient été 12,4 % à avoir été victimes d'une fraude ou d'une tentative de fraude en ligne, ce qui représente une baisse de 31 % ». En fait, de plus en plus de Québécois reconnaissent l'importance de protéger leur ordinateur par un antivirus, un antiespiogiciel et un pare-feu, ce qui limite les cas de vol de renseignements personnels. En effet, la même étude souligne que « le tiers (32,9 %) des Québécois propriétaires d'ordinateur ont affirmé que leur ordinateur a été infecté par un virus, un ver, un trojan ou un espiogiciel au cours de la dernière année. En 2008, cette proportion atteignait 40,6 %, ce qui représente une baisse de près de 20 % entre juillet 2008 et juillet 2009 ! ».

En mars 2009, le Commissariat à la protection de la vie privée du Canada etles associés de recherche Ekos ont dévoilé les résultats d'une étude sur la fraude en ligne. Au Canada, une minorité d'adultes affirment avoir été victimes de ce type de fraude (16 %). C'est au Québec que le vol de renseignements personnels et l'usurpation d'identité ont fait le moins de victimes (10 %) et en Colombie-Britannique qu'on en trouve le plus (23 %). Selon cette étude, les Canadiens semblent extrêmement prudents quant à la protection de leurs renseignements personnels. En effet, 92 % d'entre eux vérifient leurs relevés bancaires et de cartes de crédit pour s'assurer qu'il ne s'y trouve pas d'achats faits à leur insu, 85 % disent qu'ils déchiquettent ou détruisent leurs documents qui renferment des renseignements personnels et près de la moitié de tous les Canadiens disent qu'ils évitent de transporter quotidiennement dans leur portefeuille ou sac à main des documents sensibles (comme leur carte d'assurance sociale ou leur passeport). Selon l'étude, les femmes et les aînés sont en général plus prudents.

Dupont et Louis (2009), chercheurs à la Chaire de recherche du Canada en sécurité, identité et technologie, mettent toutefois quelques bémols à ces résultats. Selon une étude qu'ils ont réalisée auprès d'internautes, les chercheurs ont constaté que plusieurs d'entre eux ne comprenaient pas exactement ce que signifient les termes « vol d'identité », « usurpation d'identité » ou « vol de renseignements

personnels ». De ce fait, les statistiques sous-estimeraient souvent le nombre de victimes de ce type de fraude.

Les jeunes de plus en plus visés

Les jeunes constituent une cible de choix pour les fraudeurs. Grands adeptes de la messagerie instantanée, du magasinage en ligne et des sites de réseautage personnel et d'autres médias sociaux, ils ont davantage d'occasions de partager leurs renseignements personnels, leurs photos, l'information sur leurs amis, leur date d'anniversaire, leur adresse, leur courriel, leurs goûts, leurs activités, etc. La GRC abonde également dans ce sens et ajoute que « les jeunes sont considérés comme un groupe émergent qui deviendra de plus en plus la cible de fraudes d'identité, cela en raison de dossiers de crédit vierges, de la prolifération des renseignements disponibles sur Internet et de la possession par les jeunes d'un nombre croissant de documents de sécurité » (GRC, 2007).

Plusieurs lois, politiques et programmes de prévention ont été mis en branle pour contrer ce fléau. Ce numéro d'*e-Veille* tentera de présenter quelques-unes des solutions mises en place dans différents pays partout dans le monde.

Rédactrice : Isabelle Vachon, chargée de projet et coordonnatrice du bureau de l'Abitibi-Témiscamingue, CEFRIO, avec la collaboration de Diane Charbonneau, chargée de veille, CEFRIO

Sources :

Identity theft blog, blogue.

CEFRIO. *NETendances*, résultats de juillet 2009.

CHAIRE DE RECHERCHE DU CANADA EN SECURITE, IDENTITE ET TECHNOLOGIE. Crimes-cyber, blogue.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE DU CANADA ETLES ASSOCIES DE RECHERCHE EKOS.*Les Canadiens et la vie privée*, mars 2009.

Dupont, B. et G. Louis. Chaire de recherche du Canada en sécurité, identité et technologie. *Les voleurs d'identité: Profil d'une délinquance ordinaire*, note de recherche no. 2, 22 juin 2009.

DUPONT, Benoît. *Résultats du premier sondage sur le vol d'identité et la cybercriminalité au Québec*, septembre 2008.

GENDARMERIE ROYALE DU CANADA. *Fraude d'identité au Canada — juillet 2007*, juillet 2007.

GOUVERNEMENT DES ÉTATS-UNIS. GOVERNMENT ACCOUNTABILITY OFFICE. *Identity Theft : Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain*, 17 juin 2009.

GOUVERNEMENT DES ÉTATS-UNIS. UNITED STATES DEPARTMENT OF JUSTICE. *Identity Theft and Identity Fraud*, 2009.

Tous les moyens sont bons pour protéger l'identité des jeunes en ligne

Du 9 au 27 novembre dernier, se déroulait, au Québec, la 3e campagne de sensibilisation à la sécurité de l'informatique et à la protection des renseignements personnels. Organisée par le ministère des Services gouvernementaux (MSG), en partenariat avec l'Institut de sécurité de l'information du Québec (ISIQ) et avec l'appui d'autres organismes et entreprises, la campagne s'intitulait « Je protège mon identité sur Internet ». Elle visait à sensibiliser les internautes aux bonnes pratiques à adopter lorsqu'ils naviguent et font des transactions sur Internet. Formation en ligne, jeux virtuels, blogue, liste des ressources disponibles, concours de vidéos amateurs sur le thème du hameçonnage comptent parmi la panoplie de moyens utilisés pour informer et sensibiliser les internautes sur la protection de leurs renseignements personnels en ligne.

Alors que cette campagne visait l'ensemble des internautes, qu'en est-il des moyens déployés par les administrations publiques et qui visent principalement les jeunes ? Plusieurs initiatives fort innovantes et inspirantes ont été réalisées dans divers pays partout dans le monde.

Australie : Stay smart online et Cybersmart

À l'intérieur de son plan numérique lancé au début de 2009, le gouvernement

australien accorde une attention particulière à la prévention en matière de sécurité informatique. Divers outils de sensibilisation ont d'ailleurs été déployés à cet effet.

L'initiative Cybersmart, promulguée par l'Australian Communications and Media Authority (ACMA), propose plusieurs activités, conseils, renseignements sur le Web pour les parents et leurs enfants. Ce programme innove par son degré d'interactivité et ses divers programmes adaptés à chacun des groupes d'âge visés :

- Pour les plus jeunes enfants, âgés de 5 à 7 ans, on trouve entre autres un jeu virtuel appelé « le monde d'Hector » et des casse-tête virtuels sur le sujet.
- Pour les enfants un peu plus âgés, Cybersmart présente des jeux-questionnaires et des jeux en ligne un peu plus élaborés.
- Enfin, pour les adolescents, on trouve des jeux-questionnaires, un blogue, des clips vidéo d'information et d'autres activités interactives.

Les parents, les écoles et les bibliothèques scolaires bénéficient aussi de trousses pédagogiques et de documents d'information sur la sécurité informatique et le cyberharcèlement. L'ACMA a récemment dévoilé les gagnants d'un concours de création vidéo sur le thème de la sécurité informatique. Des jeunes ont remporté des prix pour leur clip vidéo portant sur les enjeux des relations virtuelles, notamment le cyberharcèlement et les fraudes reliées à l'identité en ligne.

Le gouvernement australien a également mis à la disposition des jeunes un jeu en ligne appelé « Budd:e ». Ce jeu permet aux élèves du primaire et du secondaire de mieux connaître les risques inhérents au vol de renseignements personnels en simulant divers événements qui peuvent se produire sur Internet et en indiquant les meilleures façons de se protéger de la fraude. Le tout se déroule dans un environnement virtuel au design attrayant pour les jeunes et en utilisant leurs expressions.

Norvège : Campagne « C'est toi qui décides... »

Le gouvernement norvégien a misé, pour sa part, sur des clips humoristiques qui visent à faire connaître les conséquences des gestes faits sur Internet. Ainsi, des dessins animés (pour les 9-13 ans) et des vidéos (pour les 13-17 ans) mettent en scène des jeunes à qui des incidents arrivent (un clip vidéo tourné entre amis se retrouve diffusé partout sur la planète ; une jeune fille pense qu'elle se fait courtiser par un séduisant jeune garçon, alors qu'il s'agit de son frère qui se moque d'elle ; etc.)… et la conclusion de chaque épisode se termine sur le slogan « C'est toi qui décides ». Par la campagne « You decide… », le gouvernement norvégien souhaite faire réfléchir les jeunes sur les risques liés à la divulgation de renseignements personnels sur le Web et susciter des débats sur ces enjeux dans les écoles.

Cette initiative a été mise au point par le Norwegian Board of Technology, le Norwegian Data Inspectorate et le Norwegian Directorate for Education and Training, et elle s'adresse aux jeunes âgés de 9 à 17 ans. Deux trousses pédagogiques ont été conçues pour les enseignants qui accompagnent les élèves du primaire ou du secondaire dans leur réflexion et dans des activités de débats en classe. Les activités ont pour objectifs de présenter les différents choix devant lesquels sont placés les jeunes dans leur usage quotidien d'Internet et du téléphone cellulaire, et de les amener à définir leurs limites en relation avec les conséquences possibles de leurs comportements. Plutôt que de leur présenter une liste de règles à suivre, le gouvernement norvégien mise sur approche constructiviste, qui met l'apprenant en action plutôt que de tenter de lui inculquer des règles de conduite.

Royaume-Uni : Kidsmart

De son côté, le gouvernement du Royaume-Uni met à la disposition des jeunes un site très interactif et dynamique pour les informer et les sensibiliser à la sécurité sur Internet. Kidsmart utilise divers outils, dont un jeu de simulation virtuel, des jeux-questionnaires, des clips vidéo mettant en scène des jeunes, un concours de composition de paroles et de chansons sur la sécurité en ligne, un espace de clavardage, etc. Divers thèmes sont abordés, que ce soit la protection des renseignements personnels sur les sites de réseautage, les dangers du partage de fichiers musicaux, les risques des jeux en réseau et de la messagerie texte sur les téléphones cellulaires ou le cyberharcèlement. Des sections pour les parents et pour

les enseignants fournissent des activités pédagogiques et de l'information complémentaire. Kidsmart répertorie également toutes les ressources offertes aux jeunes sur ces questions et agit ainsi comme un portail d'information nationale.

France: Internet sans crainte

En France, le programme Internet sans crainte offre, par l'entremise d'un site Web dynamique et coloré, une variété d'outils de sensibilisation à la protection des renseignements personnels et à la sécurité en ligne. Blogue, information, ressources pour les parents, ligne d'aide Net Écoute comptent parmi les ressources offertes. Le coin des juniors, une section réservée aux enfants de 7 à 12 ans, présente les dessins animés « Vinz et Lou », qui vivent plein d'aventures en relation avec la sécurité de l'information. Chaque épisode est accompagné de « défis interactifs », c'est-à-dire des jeux-questionnaires pour valider la compréhension du dessin animé. Les enseignants disposent aussi de fiches pédagogiques, soit des guides pour l'organisation d'un atelier autour du dessin animé. Pour les adolescents, un « Espace jeunes » propose, entre autres, un concours de création vidéo qui leur permet de s'exprimer sur leur vision d'Internet en 2025. Cette initiative est soutenue par l'Union européenne et fait partie du programme européen Insafe (Safe Internet Action Plan). Elle a été mise sur pied dans un partenariat entre le ministère français de l'Enseignement supérieur et de la Recherche et des organismes préoccupés par la protection de l'identité des jeunes sur Internet.

États-Unis : Netsmartz, OnguardOnline et autres

Aux États-Unis, le site Netsmartz workshop propose, dans un environnement haut en couleur, des ateliers, des jeux, des vidéos d'information et des clips musicaux destinés aux enfants et aux adolescents, ainsi qu'à leurs parents, à leurs enseignants et aux membres des forces de l'ordre. Le site fait valoir des expériences réalisées dans diverses écoles aux États-Unis par des reportages vidéo diffusés sur le blogue. Cette initiative est née d'une collaboration entre le National Center for Missing & Exploited Children, le Boys & Girls Clubs of America, le CyberTipline Report et l'Internet Content Rating Association du Family Online Safety Institute.

Plusieurs autres ressources existent aux États-Unis, notamment le Identity Theft Ressources Center qui rend publics des conseils pour les jeunes dans son « Teen Space » et qui dispose d'une ligne gratuite de dénonciation des fraudes d'identité. Le site OnguardOnline.gov propose également des jeux en ligne et une gamme de matériel pédagogique destinés aux jeunes.

En conclusion : qu'en est-il au Canada ?

On constate, à la lumière des divers cas présentés, que les administrations de plusieurs pays dans le monde consentent beaucoup d'efforts à la prévention du vol de renseignements personnels chez les jeunes. Le Canada n'est pas en reste. En effet, diverses initiatives ont été mises en branle pour sensibiliser et informer les jeunes sur les risques de la navigation sur Internet et sur la protection de leurs renseignements personnels.

Premièrement, le Commissariat à la protection de la vie privée a mis en ligne un site et un blogue intitulés « Vie privée des jeunes » et qui ont pour mission d'« encourager les jeunes Canadiennes et Canadiens à discuter des effets des nouvelles technologies sur la protection de leur vie privée et les aider à apprendre à se construire une identité en ligne en toute sécurité, ce qui veut dire réfléchir aux renseignements qu'ils souhaitent afficher sur le Web avant de le faire ». Le blogue offre de l'information sur la protection de l'identité en ligne dans diverses situations, notamment sur les sites de réseautage. Deux éditions d'un concours de création vidéo visant la protection des renseignements personnels ont été organisées en 2008 et en 2009. Des jeunes de diverses provinces y ont participé en grand nombre.

Deuxièmement, Sécurité Canada met à la disposition des internautes canadiens une panoplie d'informations sur le vol de renseignements personnels sur son site.

Troisièmement, le gouvernement canadien dispose aussi d'un centre d'appels antifraude – PhoneBusters – qui « réunit et collige les renseignements sur les plaintes relatives au marketing de masse, aux lettres de fraude sur les frais payables d'avance (lettres du Nigéria) et recense les plaintes pour vol ». Il s'agit d'un service qui permet aux citoyens et aux organismes de dénoncer un acte frauduleux dont ils ont été victimes. Le centre d'appels est sous la responsabilité de

la Police provinciale de l'Ontario (OPP) et est géré en partenariat avec la Gendarmerie royale du Canada (GRC) et le Bureau de la concurrence. Selon PhoneBusters, 10 845 Canadiens auraient été victimes de vol de renseignements personnels et d'usurpation d'identité entre le 1er janvier et le 30 novembre 2009, pour un montant de près de 10 millions de dollars. Seulement en novembre 2009, au Canada, 282 personnes ont été victimes de ce type de fraude pour un montant de plus de 560 000 $.

Quatrièmement, le Réseau Éducation-Médias a récemment lancé un jeu interactif en ligne pour les élèves de la 4e année du primaire à la 2e année du secondaire. Intitulé « Passeport pour Internet », l'environnement virtuel simule une expérience avec Internet dans le but d'amener les élèves à développer leurs compétences en matière de protection de leurs renseignements personnels, en gestion de leurs relations en ligne et en sécurité informatique. Par ce tutoriel, l'organisme souhaite amener les élèves « à développer une pensée critique face à leurs expériences en ligne afin qu'ils puissent utiliser le plein potentiel des sites Web et des outils offerts sur Internet de manière sécuritaire et éthique ».

Enfin, dans le but de sensibiliser les jeunes et la population en général à ce type de fraude, la GRC a également publié en 2007 un guide sur la protection des renseignements personnels pour les étudiants et elle organise chaque année le mois de la prévention de la fraude.

Rédactrice : Isabelle Vachon, chargée de projet et coordonnatrice du bureau de l'Abitibi-Témiscamingue, CEFRIO

Sources : Les références utilisées sont insérées directement dans le texte de l'article.

Vie privée et sites de réseautage peuvent-ils faire bon ménage ?

Au cours des derniers mois, les médias ont rapporté plusieurs cas d'artistes, d'athlètes et d'autres personnalités publiques – dont Guy Laliberté, fondateur du Cirque du soleil – qui ont été victimes d'usurpation d'identité sur des sites de réseautage. Facebook, le plus populaire d'entre eux, compte aujourd'hui plus de 350 millions de membres. Quels sont les risques de faire partie de ce réseau ? Les jeunes sont-ils plus insouciants que les autres internautes à ce sujet ?

Le Canada fait avancer la cause

Après plusieurs plaintes concernant le manque de contrôle des usagers sur les renseignements personnels divulgués sur la plateforme, le numéro un des médias sociaux a dû réajuster le tir. Parmi ces plaintes, celle du Commissariat à la protection de la vie privée du Canada (CPVPC) a semblé avoir le plus d'effet sur la volte-face de Facebook.

Dans une lettre datée du 30 mai 2008, des représentants de la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) ont déposé une plainte contre Facebook Inc. Celle-ci portait sur plusieurs aspects du réseau social en ligne, comme « les paramètres de confidentialité par défaut, la collecte et l'utilisation des renseignements personnels des utilisateurs à des fins publicitaires, la communication des renseignements personnels des utilisateurs aux tiers développeurs d'applications, et la collecte et l'utilisation des renseignements personnels des non-utilisateurs » (CPVPC, 16 juillet 2009 : 3). Trois principaux enjeux se trouvaient au cœur de la plainte :

1. le degré de connaissance et le véritable consentement des usagers sur la collecte et l'utilisation de leurs renseignements personnels ;
2. la conservation des données recueillies par le réseau social à la fermeture des comptes ;
3. les mesures de sécurité des renseignements personnels reliées aux applications de tiers (différents jeux et jeux-questionnaires proposés par des entreprises externes pour rendre l'expérience de Facebook plus ludique et dynamique. Ces promoteurs ont ainsi accès au contenu des comptes des usagers et donc à leurs renseignements personnels) (CPVPC, 16 juillet 2009 : 3).

Le 27 mars 2009, le Commissariat a remis à Facebook un rapport préliminaire,

comprenant 20 recommandations. Deux rencontres se sont ensuite tenues en avril et en mai 2009 avec les représentants des deux parties.

Depuis ces actions menées par le Commissariat, le célèbre réseau social a apporté plusieurs modifications pour une meilleure protection des renseignements personnels des usagers. En effet, Facebook a tenté au cours de l'année 2009 d'ajouter de nouvelles options à sa plateforme et offre maintenant la possibilité à ses adhérents de contrôler l'information publiée ; de choisir quels contenus sont visibles et pour qui ils le sont ; et de bloquer l'accès aux renseignements personnels de base à certaines personnes. Un autre problème résolu par les propriétaires de Facebook aura été de bien indiquer aux membres le risque associé à l'ajout d'applications ludiques – développées par d'autres entreprises – quant à la protection des renseignements personnels.

La commissaire Jennifer Stoddart ne condamne pas le recours aux réseaux sociaux pour autant, mais souhaite que les internautes soient conscients des risques qu'ils encourent sur Internet et que les plateformes de réseautage leur permettent de contrôler la collecte et la diffusion de leurs renseignements personnels. Selon elle,

> à une époque où tout le monde semble laisser l'empreinte numérique de ses points de vue, photos, croyances et parfois même de ses aléas amoureux, notre notion du contrôle de ses propres renseignements personnels — qui constitue le fondement de la *Loi sur la protection des renseignements personnels et les documents électroniques* — se trouve sérieusement ébranlée. De notre point de vue d'organisme de réglementation, les sites de réseautage social comme Facebook posent un défi intéressant (CPVPC, 16 juillet 2009 : 6).

Autre génération, autre vision de la vie privée en ligne

Des chercheurs de la Ryerson University se sont intéressés à la vision qu'ont les jeunes de la protection de leur vie privée sur les réseaux sociaux. L'étude menée en 2008 auprès de 2 000 jeunes Canadiens membres de sites de réseautage révèle que les jeunes n'auraient pas la même définition de la vie privée et ne partageraient pas les mêmes soucis quant à la protection de leur vie privée sur ces sites. Ainsi, ils considèrent comme privés les réseaux qui ne sont ouverts qu'à leurs amis ou aux personnes qu'ils autorisent. Pour eux, l'information publiée sur leur réseau de contact privé ne constitue pas de l'information publique, ouverte à tous, contrairement à ce que la génération d'internautes plus âgés croit souvent. Il y aurait alors, selon les chercheurs, un fossé entre la perception des jeunes de la protection de la vie privée et celle de leurs aînés. Les résultats de cette recherche indiquent que la majorité d'entre eux sont conscients des risques d'échanger en ligne et tentent autant que possible de limiter la diffusion de leurs renseignements personnels sur Internet. Les chercheurs soulignent toutefois que les organisations privées et publiques qui embauchent ces jeunes ne se sont pas adaptées à l'usage de ces médias sociaux. Ils recommandent aux employeurs de mettre en place des politiques sur l'usage de ces outils au travail, sans en bloquer totalement l'accès.

Bien d'autres médias sociaux constituent des portes ouvertes sur la vie privée des internautes et se basent sur le partage de renseignements personnels sur la Toile. Twitter, Flickr, YouTube, MySpace sont autant de vitrines qu'il faudra surveiller de près pour éviter que d'autres cas d'usurpation d'identité se produisent. Pour ce faire, la sensibilisation des jeunes et moins jeunes internautes doit aller de pair avec une protection accrue de la vie privée par les promoteurs de ces médias.

Rédactrice : Isabelle Vachon, chargée de projet et coordonnatrice du bureau de l'Abitibi-Témiscamigue, CEFRIO

Sources :

« Facebook breaches Canadian privacy law: commissioner », *CBC News, 16 juillet 2009.*

« Fears of impostors increase on Facebook », *CNN*, février 2009.

Commissariat à la protection de la vie privée du Canada, blogue.

Commissariat à la protection de la vie privée du Canada. *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques*, 16 juillet 2009.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE DU CANADA. *Le réseautage personnel*, 2009.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE DU CANADA. *Le vol d'identité : qu'est-ce*

que c'est, et quoi faire, 2009.

HERZOG, Ari. « How Your Facebook Experience Changes Today », Ari Writer blog, 9 décembre 2009.

LEVIN, Avner etautres. *The Next Digital Divide: Online Social Network Privacy*, Privacy and Cyber Crime Institute. Ted Rogers School of Management. Ryerson University, mars 2008, 94 p.

STANTON, Jim. « Social Media Fraud On the Increase », *Digital Communities Blogs*, 8 juin 2009,

VIJAYAN, Jaikumar. « Lawsuit seeks info on surveillance of social networking site », *Computerworld*, 3 décembre 2009.

OCDE : état des travaux sur le vol de renseignements personnels

Le vol de renseignements personnels dans le but d'usurper l'identité est un souci majeur pour les pays de l'Organisation de coopération et de développement économiques (OCDE) car la protection de l'identité des personnes en ligne est vitale pour l'avenir de l'économie d'Internet, indispensable aux consommateurs et aux services publics.

Définition du vol d'identité par l'OCDE

Le « vol de renseignements personnels », souvent appelé dans la littérature « vol d'identité », n'a pas, à ce jour, fait l'objet d'une définition harmonisée à l'échelle nationale ou internationale. En l'absence d'une définition internationalement admise, l'OCDE le définit de la façon suivante : un acte qui « consiste en l'acquisition, le transfert, la possession ou l'utilisation non autorisés des informations personnelles d'une personne physique ou morale dans l'intention de commettre, ou en relation avec, des actes frauduleux ou autres délits ».

Historique des travaux de l'OCDE

En 1998, à l'occasion de la conférence ministérielle de l'OCDE sur le commerce électronique tenue à Ottawa, l'OCDE a souligné, à ses pays membres, l'émergence de nouveaux types de menaces en ligne au détriment des consommateurs et la nécessité de sécuriser les transactions électroniques à l'échelle mondiale.

En octobre 2005, le Comité de la politique de l'information, de l'informatique et des communications de l'OCDE a convenu de réaliser des travaux d'analyse sur les tendances et politiques de l'économie Internet et d'en présenter les résultats à la conférence ministérielle de juin 2008 sur le futur de l'économie Internet, à Séoul, en Corée.

En octobre 2006, le Comité de la politique à l'égard des consommateurs de l'OCDE a convenu de contribuer à ce projet, en réalisant une analyse sur le vol de renseignements personnels en ligne. Cette analyse a fait l'objet d'un rapport intitulé *Document exploratoire sur le vol d'identité en ligne*. Ce rapport a été rédigé par Brigitte Acoca, avocate, du Secrétariat de l'OCDE, sur la base de recherches indépendantes et de contributions des pays membres. Le document a été approuvé à la conférence de Séoul en 2008. Il constitue, en quelque sorte, les orientations pour l'OCDE à l'égard du vol de renseignements personnels relatifs à l'identité.

Portée de la politique de l'OCDE concernant le vol de renseignements personnels

La portée de l'analyse de l'OCDE, présentée dans son rapport *Document exploratoire sur le vol d'identité en ligne*, se limite au vol de renseignements personnels affectant les consommateurs et couvre les aspects suivants :

- les caractéristiques du vol de renseignements personnels et les approches juridiques adoptées par les pays membres de l'OCDE en matière de législation et d'infraction spécifique ;
- les méthodes utilisées par les fraudeurs pour obtenir les informations personnelles de leurs victimes ;
- les formes et l'ampleur du vol de renseignements personnels, ainsi que le profil des victimes de ce type de fraude basé sur les statistiques disponibles

concernant les plaintes de victimes et les dommages subis ;

- les efforts menés par les pays membres de l'OCDE à l'échelle nationale et internationale pour réprimer ce type de fraude en ligne.

Des caractéristiques et des qualifications juridiques différentes selon les pays

Le vol de renseignements personnels relatifs à l'identité est une activité illicite aux multiples aspects. Il s'inscrit généralement dans une chaîne d'infractions ou de délits plus large. Plus précisément, il se réalise en différentes étapes.
Cette complexité a ouvert la voie à différentes catégorisations juridiques de ce concept dans les pays membres de l'OCDE, qui font du vol de renseignements personnels relatifs à l'identité, un délit pénal spécifique, un délit civil ou, bien encore, le considèrent comme une étape préparatoire dans la perpétration d'autres infractions comme la fraude, la falsification, le terrorisme ou le blanchiment d'argent.

Par exemple, au Canada et aux États-Unis, le vol de renseignements personnels est une infraction pénale spécifique. En Australie, cet acte n'est pas une infraction distincte. Dans les États membres de l'Union européenne, hormis le Royaume-Uni, il ne représente qu'une fraude.

Cette différenciation de nature juridique apporte également des régimes différents de prévention, de poursuites et de sanctions dans les pays de l'OCDE.

Méthodes pour commettre des vols d'identité examinées par l'OCDE

Les techniques des voleurs conçues pour tromper les personnes et les amener à révéler leurs informations personnelles ne cessent d'évoluer.

En plus de l'activation de maliciels (*Malware*), logiciels malveillants installés sur un ordinateur afin d'y causer des dommages, l'étude souligne que les pays membres ont déclaré être aux prises avec les diverses techniques d'hameçonnage suivantes :

- par courrier électronique trompeur ;
- par l'utilisation de sites Web factices imitant des institutions bien connues ;
- par attaques massives de pourriels pour installer des maliciels dans les ordinateurs des destinataires ;
- par clonage de serveur qui redirige les utilisateurs d'un site Web authentique vers un site frauduleux ;
- par téléphonie sur protocole Internet par lequel on invite le destinataire à appeler un numéro de répondeur qui lui demande de saisir des informations personnelles ;
- par message SMS de téléphonie mobile qui incite l'utilisateur à se connecter à un site Web piégé.

L'ampleur du phénomène

Les principales formes de vol de renseignements personnels relatifs à l'identité dans les pays de l'OCDE sont l'utilisation frauduleuse de comptes existants ou l'ouverture de nouveaux comptes, le négoce de données personnelles et l'obtention frauduleuse de services, d'allocations ou de documents des administrations publiques.

Malheureusement, selon le rapport, l'ampleur véritable de ce phénomène et le profil des victimes sont difficiles à mesurer pour les raisons suivantes :

- les statistiques disponibles ne sont pas homogènes d'un pays à l'autre, et ne couvrent pas tous les pays membres de l'OCDE, ce qui complique les comparaisons internationales ;
- les statistiques réunies par les autorités publiques pour les besoins de l'action gouvernementale sont différentes de celles que collectent les entreprises privées à des fins commerciales ;
- la plupart des données reposent sur les plaintes des consommateurs, mais beaucoup de victimes ne se signalent pas aux autorités ;

- les statistiques ne mesurent pas les mêmes types de fraudes ou délits et ainsi ne permettent pas de comparaisons ;
- les données sur les dommages directs et indirects ne couvrent pas toutes les victimes ni tous les types de vol de renseignements personnels.

Efforts préconisés par les pays membres de l'OCDE au niveau national et international

Plusieurs mesures sont présentement examinées par les pays de l'OCDE pour réprimer le vol de renseignements personnels en ligne, notamment :

- l'information du public par l'entremise de sites Web, de vidéos, de brochures et de trousses d'information générale ;
- l'information des entreprises par l'usage de trousses d'information pour leur apprendre à réduire les dangers qui menacent les informations personnelles des consommateurs et à réagir en cas de vol d'identité ;
- le renforcement de la coopération transfrontière pour assurer le respect des lois ;
- l'élaboration d'un concept universellement accepté par les membres de l'OCDE pour faciliter la mise en œuvre de sanctions dissuasives ;
- l'obligation d'astreindre les entreprises à révéler les atteintes à la sécurité touchant les informations personnelles de leurs clients ;
- l'utilisation d'outils d'authentification électronique pour protéger les données personnelles ;
- l'instauration de cadres de coopération internationaux, bilatéraux et régionaux pour l'application de la loi entre les multiples parties prenantes du secteur public et privé.

En conclusion

Il n'y a pas, à ce jour, de politique établie et approuvée de la part de l'OCDE en matière de vol de renseignements personnels relatifs à l'identité. Il n'y a présentement que des orientations sur la nature et la portée des travaux à réaliser. Le progrès des travaux de l'OCDE sur ce dossier reste donc à suivre au cours des prochains mois.

Rédactrice : Diane Charbonneau, chargée de veille, CEFRIO

Sources :

OCDE. *Online Identity Theft*, 31 mars 2009, 142 p.

OCDE. Direction de la science, de la technologie et de l'industrie. Comité de la politique de l'information de l'informatique et des communications. *Document exploratoire sur le vol d'identité en ligne*, 19 février 2008, 78 p.

---

1. Le terme « vol d'identité » est utilisé habituellement dans la littérature sur la sécurité de l'information, mais signifie en fait « vol de renseignements personnels » et se distingue de l'usurpation d'identité. Retour au texte

2. Le projet de loi S-4 a reçu la sanction royale le 27 octobre 2009. Conséquemment, deux nouvelles infractions, assujetties à une peine maximale de cinq ans, sont créées dans la nouvelle section « Vol d'identité et fraude à l'identité » du Code criminel canadien :

   - 402.2 (1) Commet une infraction quiconque, sciemment, obtient ou a en sa possession des renseignements identificateurs sur une autre personne dans des circonstances qui permettent de conclure raisonnablement qu'ils seront utilisés dans l'intention de commettre un acte criminel dont l'un des éléments constitutifs est la fraude, la supercherie ou le mensonge.
   - (2) Commet une infraction quiconque transmet, rend accessible, distribue, vend ou offre en vente, ou a en sa possession à une telle fin, des renseignements identificateurs sur une autre personne sachant qu'ils seront utilisés pour commettre un acte criminel dont l'un des éléments constitutifs est la fraude, la supercherie ou le mensonge ou ne se souciant pas de savoir si tel sera le cas. Retour au texte

---

Le bulletin *e-Veille* est produit sous la coordination du ministère des Services gouvernementaux, en collaboration avec le CEFRIO.

Direction des politiques
Ministère des Services gouvernementaux
Québec (Québec) G1R 5H6
Téléphone : 418 646-9121
Télécopieur : 418 646-9093

Gestion et supervision
Stéphanie Sauvageau, chargée de projet, Direction des politiques, ministère des Services gouvernementaux
Mireille Lacasse, directrice de projet, CEFRIO

Réalisation et rédaction
Isabelle Vachon, chargée de projet et coordonnatrice du bureau de l'Abitibi-Témiscamingue, CEFRIO

Collaboration à la rédaction:
Diane Charbonneau, chargée de veille, CEFRIO

Édition Web
Sébastien Racine, technicien en informatique, CEFRIO
Direction des affaires publiques et des communications, ministère des Services gouvernementaux

Recherche documentaire
Isabelle Poulin, chargée de veille, CEFRIO

Dernière modification de cette page : 2010-01-06

Québec