Commissaire à l'information et à la protection de la vie privée/Ontario

Vol d'identité:
Qui se sert de votre nom?

Ann Cavoukian, Ph. D.
Commissaire
Juin 1997

Commissaire à l'information et à la protection de la vie privée/Ontario

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site web : www.ipc.on.ca

La commissaire à l'information et à la protection de la vie privée/Ontario souligne la contribution de Peony Gandolfi à la préparation du présent document.

Cette publication est aussi disponible sur le site web du Bureau du commissaire.

This publication is also available in English.

Table des matières

Introduction

Vous n'avez pas reçu la nouvelle carte de crédit que l'on vous avait envoyée par la poste. Des mois passent, puis vous commencez à recevoir des appels téléphoniques répétés de créanciers réclamant le paiement d'articles que vous n'avez jamais achetés. Vos antécédents en matière de crédit ont toujours été sans tache, mais voilà qu'on vous refuse le financement demandé à cause de nombreuses défaillances qui figurent dans votre rapport de solvabilité. Est-ce possible? Malheureusement, oui; c'est même arrivé à des milliers de victimes d'un crime que l'on a baptisé «vol d'identité».

Dans le cadre de son mandat, le Commissaire à l'information et à la protection de la vie privée fait des recherches et des observations sur les questions et les tendances se rapportant à la protection de la vie privée. Le vol d'identité, un crime qui consiste en l'appropriation et l'utilisation illicites de renseignements personnels, est un problème sociétal croissant qui mérite notre attention. Dans le présent rapport, nous examinerons ce qui constitue le vol d'identité, comment il se produit, pourquoi il faut s'en préoccuper et comment les particuliers et les sociétés peuvent s'y prendre pour réduire le risque de s'en trouver victimes. Nous examinerons en particulier les moyens technologiques de protéger nos renseignements personnels.

Un grand thème sur lequel s'appuiera ce document sera que le vol d'identité pourrait être considérablement réduit si un plus grand nombre d'organisations adoptaient des pratiques équitables en matière de renseignements[1].

Qu'est-ce que le vol d'identité?

Le vol d'identité consiste à acquérir des renseignements signalétiques sur un particulier dans le but d'usurper son identité et de s'en servir à des fins criminelles. En plus de renseignements tels que le nom, l'adresse et le numéro de téléphone, les voleurs d'identité s'intéressent aux numéros d'assurance sociale, aux numéro de permis de conduire, de cartes de crédit et de comptes bancaires, ainsi qu'aux cartes bancaires, aux cartes d'appels des compagnies de téléphone, aux certificats de naissance et aux passeports. Ces renseignements permettent au voleur d'identité de commettre diverses formes de fraudes : faire de folles dépenses en se servant du nom de la victime, assumer les comptes financiers de la victime, ouvrir de nouveaux comptes, rediriger le courrier de nature financière de la victime à l'adresse du voleur, faire des demandes de crédit, de cartes de crédit, de prestations d'aide sociale, louer des appartements, s'abonner aux services de sociétés de services publics, etc.

Pourquoi devrais-je m'en préoccuper?

Chaque année, des milliers de personnes sont victimes de voleurs d'identité qui volent des millions de dollars des banques, des détaillants et d'autres créanciers. Par exemple, aux États-Unis, les pertes des banques attribuables aux vols d'identité ont atteint près de 90 millions de dollars en 1995[2]. Éventuellement, c'est chacun d'entre nous qui doit payer, sous la forme de taux d'intérêt ou de frais de service plus élevés. Aux États-Unis, des porte-parole décrivent le vol d'identité comme la «forme de délit qui connaît la croissance la plus rapide au pays», ayant été reconnue comme la «principale forme de fraude dans le secteur de la consommation[3].»

La victime d'un vol d'identité peut se retrouver avec une mauvaise cote de crédit et une réputation ternie, et il faudra peut-être des mois, voire des années pour corriger la situation. Entre-temps, à cause de ses supposés mauvais antécédents en matière de crédit, il se peut qu'on lui refuse des emplois, des emprunts, le droit de tirer des chèques ou le droit de louer ou d'acheter un logement. Elle risque même qu'on l'arrête illégalement ou qu'on ne la croie pas.

Les pertes financières d'une victime de vol d'identité peuvent atteindre 36 000 dollars. Cela comprend les appels téléphoniques, les déclarations sous serment, les emprunts, les frais de counselling et le salaire perdu à cause du temps qu'il a fallu pour s'occuper du problème. Le chiffre ne comprend pas les pertes reliées au paiement des factures du voleur ou au refus d'emplois[4].

En outre, les victimes sont souvent surprises du manque de collaboration de la part de ceux dont ils ont demandé l'aide. Il est arrivé que la police ait refusé de croire qu'elles étaient des victimes et même, les ait arrêtées pour des délits commis par le voleur. Les créanciers et les bureaux de crédit ont accusé les victimes de mentir et d'essayer de se soustraire à leurs propres dettes. Des bureaux de crédit ont refusé de retirer les données erronées des dossiers des victimes. En d'autres termes, celui à qui l'on vole l'identité sera presque laissé à ses propres ressources pour régler la situation.

Pis encore, nombre de voleurs d'identité ne sont jamais appréhendés et sont donc libres de répéter ce genre de fraude autant de fois qu'ils veulent. Mais, ce qui est vraiment effrayant, c'est la facilité avec laquelle on peut voler l'identité de quelqu'un.

Comment peut-on voler mon identité?

De nos jours, les voleurs d'identité s'approprient des renseignements signalétiques sur les gens par des moyens beaucoup plus sophistiqués que le vol de portefeuilles[5]. Par exemple,

- en rôdant autour des guichets automatiques et des cabines téléphoniques pour tâcher de capter les numéros d'identification personnel (NIP) (en se servant de lunettes d'approche pour lire les numéros que l'usager entre ou, tout simplement, en essayant de lire par-dessus son épaule). Les voyageurs font une cible particulièrement facile;

- en volant le courrier des boîtes aux lettres ou en le réacheminant pour tâcher d'obtenir des cartes de crédit, des relevés de comptes bancaires, de comptes de crédit, des offres de crédit autorisé, des renseignements sur l'impôt ou tout autre renseignement personnel. La revue *Privacy Journal* a également fait remarquer que les bureaux de crédit automatisé acceptent normalement un changement d'adresse sans le vérifier auprès de l'abonné et sans l'en informer. Un imposteur qui s'approprie illicitement l'identité d'un consommateur peut facilement demander à un détaillant d'entrer un changement d'adresse, et c'est ce que font des milliers de fraudeurs du crédit...[6]»;

- en obtenant illégalement des rapports de solvabilité;

- en ayant recours au telemarketing pour soutirer les numéros de compte de consommateurs crédules;

- en gagnant l'accès à des renseignements personnels envoyés accidentellement au mauvais numéro de télécopieur, à la mauvaise adresse électronique ou boîte vocale;

- en fouillant dans les vidanges à la recherche de demandes de cartes de crédit, de demandes d'emprunt, des dossiers de l'employeur et de données d'identification ou d'authentification telles que les identificateurs d'entrée en communication et les mots de passe. De même, les voleurs peuvent rechercher sur les disques effacés, les données récupérables;

- en envoyant sur Internet de faux messages (espionnage) dans le but de recueillir des renseignements privés. Par exemple, en prétendant être un agent de voyages ou un autre fournisseur de services, un voleur d'identité aura le numéro de carte de crédit dont on s'est servi pour acheter le billet ou le service;

- en envoyant un message par courrier électronique en se servant de l'ordinateur d'une autre personne ou de son adresse de courrier électronique[7];

- en se servant de différents logiciels tels que l'analyseur de signaux et le renifleur pour intercepter les données financières, les mots de passe, les adresses et autres renseignements personnels envoyés sur les réseaux;

- en perçant les systèmes informatiques pour avoir accès aux renseignements personnels. Par exemple, les noms, adresses et numéros de cartes de crédit, d'assurance sociale et de sécurité sociale emmagasinés dans les bases de données des gouvernements, des institutions financières, des employeurs, des créanciers et des bureaux de crédit peuvent être téléchargés par les employés, les anciens employés ou des pirates informatiques de l'extérieur. Ces derniers peuvent ensuite vendre l'information ou s'en servir pour ouvrir des comptes frauduleusement.

Un spécialiste en sécurité a constaté que près de 70 pour 100 des sites web qu'il a examinés au mois de décembre 1996 comportaient des «lacunes sur le plan de la sécurité». Parmi les sites examinés, il y avait des banques, des caisses populaires et des organismes gouvernementaux[8]. Plus récemment, un garçonnet de 14 ans a fait face à des accusations multiples après avoir fait des achats frauduleux en se servant d'une série de numéros de cartes de débit qu'il avait téléchargés d'Internet[9].

Dossiers de cas de vol d'identité

Pour que les lecteurs sachent bien le genre de tension, d'irritation que connaissent les victimes de vols d'identité, nous présentons ici plusieurs dossiers de cas de vol.

- Une jeune secrétaire a passé de nombreuses années à rétablir sa réputation après qu'une fraudeuse fiscale ait mis la main sur sa carte d'assurance sociale, qu'elle n'avait jamais reçue. L'imposteur s'était servi du nom de la secrétaire et de son numéro d'assurance sociale pour passer d'un emploi à l'autre et recevoir des prestations d'assurance-chômage, des prestations d'assurance-maladie et des prestations de maternité, toujours sans payer d'impôts. La secrétaire était continuellement harcelée par le gouvernement pour régler «ses» impôts non payés. Revenu Canada avait même obtenu la saisie-arrêt de son compte bancaire et de ses revenus. La victime a dû se rendre chez chacun des six anciens employeurs de la voleuse pour réclamer des déclarations afin de démontrer aux fonctionnaires de l'impôt qu'elle-même n'avait jamais travaillé pour eux[10].

- Se servant du certificat de naissance et de la carte d'assurance sociale de quelqu'un d'autre, un homme de Vancouver a réussi à se procurer une carte d'identité avec photographie, du gouvernement de la Colombie-Britannique. Il s'est ensuite servi de ces trois pièces d'identité pour ouvrir des comptes bancaires frauduleusement. Il a ensuite volé plus de 170 000 dollars de plusieurs banques, en s'y prenant de la façon suivante. Il déposait des faux chèques dans les comptes et allait immédiatement retirer l'argent aux guichets automatiques[11].

- Une parisienne dont la carte d'identité avait été volée a découvert plus tard, à sa grande surprise, qu'elle avait été «mariée» durant quatre ans, à un homme qu'elle n'avait jamais rencontré. Une fois que son «mari» eut obtenu la citoyenneté française, il la divorça[12].

- Dans un cas de fraude à plusieurs victimes, un enseignant a ouvert frauduleusement plusieurs comptes de crédit et a volé pour 43 000 dollars de marchandises, se servant des noms et des numéros de sécurité sociale de ses élèves et collègues. Le voleur a tiré les renseignements personnels d'une liste d'étudiants et des talons de chèques de paye qu'il a volés dans les boîtes aux lettres du campus. Les victimes ont dû persuader les trois bureaux nationaux du crédit d'effacer, de façon permanente, les données se rapportant à la fraude de leurs rapports de solvabilité. Ils ont également demandé que les créanciers prennent soin de ne pas accorder de crédit en leur nom avant de vérifier auprès d'eux qu'ils en avaient fait la demande[13].

- Quand une télétravailleuse handicapée reçut son rapport de solvabilité de TRW[14], elle constata qu'il comportait sept pages et plus de 15 comptes frauduleux en souffrance. Il y figurait même un jugement d'éviction d'un appartement contre elle. Plus tard, elle reçut en outre un avis de défaut de paiement d'un prêt. Lorsqu'elle se rendit chez le shérif pour porter des accusations contre son voleur d'identité, on l'informa qu'on n'examinerait sans doute jamais son cas, parce qu'il n'y avait que deux détectives et que «ce n'était pas aussi important qu'un meurtre.» TRW exigea qu'elle démontre elle-même aux 15 créanciers qu'elle avait porté des accusations en leur faisant parvenir des déclarations sous serment (au coût de 10 dollars chacune). Toutefois, aucun des créanciers ne poursuivit le voleur, disant que financièrement cela n'en valait pas la peine[15].

- Un an après qu'on lui eut volé son numéro de sécurité sociale, une ancienne californienne se vit refuser une hypothèque parce qu'il y avait plusieurs comptes en souffrance sur ses rapports de solvabilité. Après des mois, elle réussit à faire effacer les renseignements erronés de son dossier par TRW, mais ils réapparurent, six mois plus tard. Equifax et Trans Union ont égaré ses dossiers et neuf des 12 données erronées originales n'ont jamais été effacées. Pour ajouter encore à l'insulte, Trans Union a même insinué que c'était la victime elle-même qui avait commis le crime.

  Le mauvais rapport de solvabilité de la victime a également affecté son mari dont on ne renouvela pas la carte Visa. À la fin, elle poursuivit les trois bureaux de crédit pour leurs pratiques abusives, témoignant en cour qu'ils lui téléphonaient «à toutes heures du jour et de la nuit» et que leurs appels ne cessèrent que lorsqu'elle déménagea dans un autre état. Trans Union fit valoir que l'amélioration du système pour garantir le maximum d'exactitude était coûteux et que les bureaux de crédit n'avaient aucun moyen de différencier les victimes authentiques des consommateurs eux-mêmes auteurs de fraudes[16].

- Après des années d'ennuis, un couple du Texas a gagné le procès de 1,45 million de dollars qu'il avait intenté contre un voleur d'identité pour atteinte à la vie privée, diffamation et une foule d'autres accusations. Toutefois, étant donné le peu d'avoirs de l'auteur de l'infraction, c'est une fausse victoire. Ce dernier, un ancien agent de prêts, s'était servi de l'ordinateur de la banque pour obtenir des renseignements personnels sur le couple et avoir accès à leur rapport de solvabilité. Se servant de leurs numéros de sécurité sociale, de leur adresse et des renseignements sur leurs comptes financiers, le voleur a ouvert 21 comptes financiers, comptes d'essence et autres comptes de crédit pour un total d'environ 50 000 dollars. Dans une autre poursuite, le couple a également poursuivi 13 bureaux de crédit, agences de recouvrement, banques, magasins et autres créanciers mêlés à l'affaire pour atteinte à la vie privée, diffamation et autres accusations[17].

- Après que sa cote de sécurité militaire fut soudainement révoquée, une employée de l'armée découvrit qu'une parente avait volé son identité et ouvert plusieurs comptes frauduleux. Tentant de se disculper, elle paya les dettes frauduleuses de 30 000 dollars. Elle quitta ensuite son emploi pour en prendre un autre à 30 000 dollars par année, mais l'offre fut par la suite retirée, le nouvel employeur ayant vu son rapport de solvabilité. Par conséquent, elle se retrouva sans emploi et incapable de garder son appartement. En outre, elle ne réussit à obtenir aucune aide du gouvernement, ni aucune aide financière du bureau de crédit. Éventuellement, elle dut quitter le pays, le seul emploi qu'elle pouvait trouver étant en Corée[18].

- Quant au vol d'identité dans les entreprises, dans une cause de 1994, plus de 300 000 dollars ont été volés d'institutions financières à l'aide de signatures et autres renseignements personnels obtenus dans les vidanges de la banque. Il a également été découvert que la plupart des intrusions dans les bases de données des rapports de solvabilité sont commises à des terminaux autorisés, et non pas par des pirates informatiques de l'extérieur[19].

Ne soyes pas une cible facile

Les renseignements personnels sont maintenant si facilement accessibles dans notre monde réseauté qu'il est sans doute impossible d'enrayer totalement les vols d'identité. Une réforme plus générale du système et des lois et la collaboration de nombre d'intéressés dont les créanciers, les bureaux de crédit, les organismes d'application de la loi et le gouvernement seront essentielles pour combattre le problème. Entretemps, toutefois, il existe de nombreux moyens de prévention, qui peuvent aider à ne pas nous retrouver victimes[20]. On en parle ci-dessous.

Moyens simples

- Toujours conserver les cartes et les documents renfermant des renseignements personnels de nature délicate dans un endroit sûr. Les données de nature délicate peuvent comprendre : les cartes de crédit, les numéros d'assurance sociale, les permis de conduire, les numéros de comptes bancaires, les formulaires de crédit préautorisé, l'adresse, la date de naissance, les dossiers d'impôt, les passeports, les factures de services publics et de téléphone. Déchiqueter (ou déchirer) tous les documents de ce genre avant de les jeter. Songez à installer une boîte aux lettres sûre.

- Obtenir un exemplaire de son rapport de solvabilité régulièrement pour vérifier s'il y a des comptes frauduleux, de faux changements d'adresse ou autres renseignements frauduleux. Signaler toutes les erreurs au bureau de crédit et demander qu'on les corrige sans tarder.

- Conserver et avoir sur soi le moins de cartes possible. Après avoir porté une transaction sur une carte de crédit, vérifier que la carte qu'on vous remet est bien la vôtre. Jeter les copies sur papier carbone. Annuler tous les comptes de crédit dont on ne se sert pas.

- Vérifier soigneusement tous les relevés bancaires et les relevés de comptes de crédit, les chèques payés, les factures des compagnies de téléphone et de services publics dès qu'ils arrivent. Signaler tout écart sans tarder. Si des relevés attendus n'arrivent pas à temps, communiquer avec le bureau de poste et avec les créanciers pour être certain que le courrier n'est pas réacheminé vers un autre endroit.

- Si la nouvelle carte de crédit demandée n'arrive pas dans les délais, téléphoner à la banque ou à la compagnie de crédit concernée. Signaler sans tarder tout vol ou perte de cartes.

- Ne pas donner son adresse en payant par carte de crédit. Veiller à ce que son numéro de permis de conduire ne soit jamais préimprimé sur ses chèques. En outre, éviter d'écrire son numéro de carte de crédit, d'assurance sociale ou de sécurité sociale sur ses chèques, à moins d'y être légalement tenu.

- Éviter de donner son numéro de carte de crédit ou tout autre renseignement personnel au téléphone, à moins d'avoir toute confiance en l'entreprise avec laquelle on fait affaire et de lui avoir téléphoné soi-même. Tout particulièrement, ne pas donner de renseignements personnels par des moyens de communication sans fil non chiffrés tels que des téléphones sans fil ou cellulaires. (Même les appareils de surveillance de chambres de bébé peuvent permettre aux oreilles indiscrètes d'écouter vos communications personnelles.)

- Certains émetteurs de cartes téléphonent aux clients s'ils constatent des débits inhabituels sur leurs cartes. On ne doit jamais donner de renseignements au sujet de son compte au téléphone, sauf pour confirmer ce qui est déjà fait. En cas de doute, raccrocher et communiquer directement avec l'émetteur de la carte. De même, ne pas fournir de renseignements personnels à des personnes que vous ne connaissez pas et qui disent représenter votre institution financière ou votre courtier. Demander le nom de la personne, raccrocher, puis la rappeler vous-même[21].

- Il ne faut **jamais** écrire ses NIP ni les révéler à **personne**. Les choisir pour qu'ils soient difficiles à deviner et les changer fréquemment. En faisant des transactions bancaires ou des transactions de placement au téléphone, veiller à ce que personne ne puisse vous entendre ou ne soit en mesure de déceler votre NIP ou votre mot de passe quand vous l'entrez.

- Advenant que des renseignements personnels sur soi figurent dans un répertoire de consultation en direct ou dans une base de données de recherche, il faut tenter de les faire enlever. Par exemple, un important exploitant de bases de données américain vend des noms, adresses, numéros de téléphone non inscrits et autres données sur des millions de personnes, par Internet. Même les numéros de sécurité sociale étaient offerts au début, jusqu'à ce que des centaines de personnes se plaignent[22].

- Ne pas créer en direct de profil contenant vos renseignements personnels — quelqu'un pourrait s'en servir pour usurper votre identité.

- Se méfier de logiciels de démarrage qui demandent des données d'enregistrement comme un numéro de carte de crédit, d'assurance sociale ou de sécurité sociale pour «fins de facturation» au téléchargement.

Moyens de haute technologie : confidentialité améliorée

L'infrastructure électronique qui prend de l'ampleur dans le monde a permis à la fraude de croître exponentiellement. Dans notre monde de plus en plus dépendant de la technologie, le recours à des technologies qui rehaussent la confidentialité peut être un élément important des pratiques sécuritaires décrites plus haut. Les technologies qui protègent la confidentialité sont celles qui tansmettent les renseignements personnels sous forme de chiffres ou qui permettent de faire des transactions électroniques de façon anonyme en minimisant ou éliminant le besoin de fournir des données d'identification personnelles. Le chiffrement est le processus mathématique par lequel les renseignements sont codés de sorte qu'ils ne puissent être lus sans la «clé» qui permet de les décoder.

En transmettant des renseignements sur un réseau de communications, il faut présumer que la communication n'est pas privée, à moins que l'information ne soit chiffrée[23]. Sans une bonne méthode de chiffrement, les transactions bancaires par ordinateur personnel, les transactions de placement et les achats en direct, l'envoi et la réception de courrier électronique et les demandes de crédit commercial ou autre par Internet peuvent mener à la divulgation non-autorisée, au vol ou à l'altération de renseignements personnels.

Internet a la réputation d'être le moyen de vol d'identité dont l'usage croît le plus rapidement[24]. Cela n'a rien de surprenant, étant donné les possibilités qu'il offre pour la collecte (et l'utilisation illicite) de renseignements personnels, à un niveau impossible jusqu'à présent. On a prédit que d'ici à l'an 2000, en Amérique du Nord, 30 pour 100 de toutes les transactions commerciales se feront dans le cyberespace et que dans le commerce mondial, les revenus par Internet atteindront 200 milliards de dollars américains[25]. Aussi, les possibilités de vol d'identité ne cesseront de croître.

Un grand nombre de technologies qui rehaussent la confidentialité existent de nos jours. On parlera des principales d'entre elles dans la partie qui suit. En joignant à ces technologies d'autres caractéristiques de sécurité telles que les mots de passe et le chiffrement, on augmentera encore davantage la sécurité et la confidentialité.

Protecteurs d'identité

Les protecteurs d'identité tels que les signatures aveugles et les pseudonymes numériques sont des séries de chiffres basées sur les techniques de chiffrement qui permettent aux usagers de faire des transactions électroniques de façon anonyme, tout en permettant au fournisseur de service de vérifier l'authenticité de l'usager et son admissibilité aux prestations et aux services.

Les **signatures numériques** sont l'équivalent de signatures manuscrites. Comme les signatures manuscrites permettent d'authentifier les documents, les signatures numériques permettent d'authentifier les documents électroniques. Les signatures numériques peuvent protéger contre la mystification et les faux, mais elles protègent peu la confidentialité, étant conçues pour reconnaître l'expéditeur. Les **signatures «aveugles»**, créées par David Chaum de DigiCash[26], font mieux puisqu'en plus de permettre d'authentifier un document comme le font les signatures numériques, elles ne révèlent pas l'identité de l'expéditeur. L'avantage d'un tel système est qu'il permet l'authentification tout en protégeant la vie privée.

Un **pseudonyme numérique** est une autre identité qu'un usager peut adopter pour faire anonymement des transactions, communications ou autres services. On peut se servir d'un pseudonyme différent pour chaque fournisseur de service, ou pour chaque service.

Pour une étude de ces moyens de haute technologie et autres, les lecteurs peuvent se référer au rapport mixte de Bureau du commissaire et du Netherlands Data Protection Authority, intitulé *Privacy-Enhancing Technologies : The Path to Anonymity*. Publiée à l'automne de 1995, cette étude donne une analyse détaillée des techniques de chiffrement de pointe qui permettent d'authentifier les transactions, même anonymes, telles que les signatures numériques, les signatures aveugles, les pseudonymes numériques et les tierces parties de confiance.

Chiffrement des données

De nombreux logiciels de chiffrement puissants sont déjà disponibles sans frais par l'entremise des fournisseurs de service Internet sous la forme de logiciels autonomes ou d'ensembles pour le chiffrement de fichiers ou de courrier électronique et de signatures numériques. Par exemple, un système puissant de chiffrement à clé révélée, «intimité plutôt bonne» (PGP) mis au point par Philip Zimmermann[27], peut être utilisé pour chiffrer le courrier électronique ou les fichiers informatiques.

Une alternative au PGP est le système d'authentification Kerberos, qui peut être utilisé pour assurer la sécurité de messages spécifiques ou pour protéger le niveau de protocole du serveur. Le protocole PEM peut aussi être utilisé pour chiffrer les données sensibles avant de les envoyer par Internet.

On met présentement au point diverses technologies de chiffrement des numéros de cartes de crédit pour les paiements par Internet, telles que Secure Electronic Transaction (SET). Les communications et les transactions par Internet peuvent également être chiffrées à l'aide du protocole S-HTTP et Secure Sockets Layer (SSL).

Envois anonymes

Lorsqu'il envoie une lettre par le courrier régulier, l'expéditeur peut facilement demeurer anonyme en n'indiquant pas d'adresse de retour sur l'enveloppe. Sur Internet, toutefois, l'adresse de retour est envoyée automatiquement à moins que l'expéditeur ne prenne les moyens d'acheminer son envoi anonymement. Ce service permet d'enlever l'identification d'en-tête du courrier électronique avant de l'envoyer. Pour connaître les services anonymes offerts sur Internet, veuillez consulter www.anonymizer.com.

Mécanismes de paiement anonyme

Les paiements électroniques peuvent se faire de façon anonyme à l'aide de cartes à mémoire telles que les cartes à valeur emmagasinée, de transpondeurs à prépaiement pour les routes à péage électronique ou de monnaie électronique, argent à codage numérique. Mis au point pour servir d'équivalent électronique à la monnaie, les systèmes de monnaie codée sont conçus pour qu'il soit impossible de retracer la transaction à l'acheteur tout en assurant le bénéficiaire de l'authenticité du paiement.

Autres technologies qui rehaussent la confidentialité

- Il existe des matériels et logiciels de sécurité informatique tels que les logiciels et programmes de contrôle d'accès qui empêchent l'accès non-autorisé à un ordinateur. Un logiciel qui peut transformer un ordinateur personnel en téléphone confidentiel peut être téléchargé gratuitement d'Internet.

- les jetons sont des chaînes d'identification qui peuvent être mémorisées dans les cartes à mémoire. Ils peuvent être utilisés conjointement avec les mots de passe, numéros d'identification personnels, lecteurs de cartes et parfois, le chiffrement.

- Des imprimantes qui rehaussent la confidentialité ont des boîtes aux lettres et des interclasseuses et plusieurs tiroirs à clé, chacun ayant son propre mot de passe. Chaque utilisateur peut envoyer son travail à son propre tiroir.

- D'autres technologies qui rehaussent la confidentialité comprennent la signature à usage unique, le mot de passe protégé, le mot de passe à usage unique, les paliers d'entrée, l'accès à partitions selon la sensibilité du fichier, et le blocage d'appels. Un fournisseur de service Internet offre même gratuitement des comptes Internet anonymes, des serveurs pseudonymes et des services d'anonymat qui permettent aux navigateurs du W3 de naviguer dans la plus grande anonymité[28].

Bien qu'il existe de nos jours des technologies qui rehaussent la confidentialité et qu'il y en ait de nouvelles chaque jour, on les connaît et on les utilise peu. Leur généralisation par les entreprises, le gouvernement et le secteur privé ne se fera qu'à l'insistance des consommateurs. En faisant connaître ce que vous en pensez, vous pouvez aider à créer un avenir électronique davantage axé sur la confidentialité pour chacun d'entre nous.

Ce que les organismes peuvent faire

Le rôle des organismes pour empêcher les vols d'identité est aussi important que celui des consommateurs, sinon plus. Dans la revue *Privacy Times* on écrivait «les cas de vol d'identité sont l'effet direct de l'intérêt croissant des criminels à tirer parti de la sécurité inadéquate des données financières des particuliers dans les bases de données des bureaux de crédit et autres bases de données importantes[29].» Nous faisons donc les recommandations qui suivent, qui sont particulièrement applicables aux organismes du secteur financier et du secteur public :

- Lors de la conception ou de la mise à jour de systèmes informatiques, veiller à la meilleure façon de protéger la confidentialité de l'utilisateur. Explorer la mise en oeuvre de moyens technologiques qui rehaussent la confidentialitée et veiller à ce que des mesures de sécurité appropriées soient prises. Demander : Combien de renseignements d'identité personnels sont vraiment nécessaires pour que ce système fonctionne? Une fois ce besoin déterminé, ne recueillir et retenir que le minimum nécessaire.

- Comme la législation n'existe pas, adopter une politique pour la protection de la vie privée dans votre organisation et enseigner à tous les employés des méthodes responsables de traiter l'information. Le Code type sur la protection des renseignements personnels (CAN/CSA Q830-96) de l'Association canadienne de normalisation (CSA) est un excellent code pour les organismes du secteur privé.

- Lors de la collecte, de l'utilisation et de la divulgation de numéros d'assurance sociale ou de sécurité sociale, faire preuve de la plus grande circonspection. Ne pas demander ces renseignements sauf si la loi l'exige. Le vol de ces numéros est responsable de milliers de cas de vol d'identité de crédit chaque mois. Les personnes qui n'ont pas les documents nécessaires peuvent voler ces numéros et s'en servir pour acquérir une identité légale. Un numéro d'assurance sociale ou de sécurité sociale peut également permettre d'usurper l'identité de quelqu'un au téléphone ou en direct pour soutirer des renseignements personnels sur le particulier tels que des renseignements sur l'impôt. Éviter d'utiliser les numéros d'assurance sociale ou de sécurité sociale comme identificateurs des clients, employés ou étudiants.

- Songer à emmagasiner séparément la partie texte d'un dossier (par exemple, les renseignements sur une visite qui se trouvent dans le dossier médical), sans identificateurs personnels; conserver les renseignements d'identification (nom, numéro d'assurance sociale, adresse, date de naissance) dans une base de données distincte, préférablement sous forme chiffrée. Les organismes peuvent également séparer le cheminement des données sur les renseignements personnels, de celui des autres données de transactions dans leurs systèmes informatiques.

- Si vous êtes un bureau de crédit, fournir chaque année gratuitement, sur demande, un rapport de solvabilité à vos clients et informer vos clients chaque fois que leurs rapports de solvabilité sont interrogés.
- Demander une preuve d'identité et la vérifier soigneusement lorsqu'un client présente une demande de crédit ou un changement d'adresses. Les bureaux de crédit ne devraient pas accepter de changements d'adresses des créanciers sans d'abord les vérifier auprès du consommateur intéressé.
- Utiliser les logiciels d'intelligence artificielle pour reconnaître les formes de fraude qui reviennent et informer les consommateurs de toute activité suspecte. Les créanciers sont tenus de porter à l'attention de la police les comptes de fraude et de les effacer du dossier d'un client légitime.
- Ne pas se servir des renseignements personnels d'un client à des fins «secondaires», par exemple pour une liste d'envoi ni les vendre ou les louer à des tiers sans le consentement explicite de l'intéressé.
- Emmagasiner et utiliser les renseignements personnels correctement, dans la plus grande confidentialité, surtout les formulaires de demande de crédit et de prêt.
- Éviter d'utiliser la date de naissance ou le nom de famille de la mère comme mots de passe pour des comptes financiers. Ce genre de renseignement est souvent très facile à acquérir par les autres.
- Ne pas introduire les signatures obtenues par balayage dans le site web de votre organisme.

Que faire si cela m'arrive?

Le vol d'identité est un problème à plusieurs volets qui n'est pas sur le point de disparaître. Si vous en devenez victime, vous devrez réagir sans tarder[30].

- Informez immédiatement la police, les banques et les créanciers. Obtenez une copie du rapport de police (qui servira de preuve de la fraude). Annulez toutes les cartes de crédit existantes, les comptes, les mots de passe et les numéros d'identité personnels, et remplacez-les par de nouveaux.

- Téléphonez à tous les bureaux de crédit et demandez à chacun d'attacher un avis de fraude et une déclaration de victime à votre rapport. Demandez aux créanciers de communiquer avec vous avant d'ajouter quoi que ce soit à votre rapport. Faites parvenir les corrections à tous ceux qui ont reçu votre rapport de solvabilité au cours des deux dernières années. Demandez une copie gratuite de votre rapport après trois mois.

- Communiquez avec le bureau de poste, si vous soupçonnez qu'un voleur d'identité a rempli un changement d'adresse en se servant de votre nom pour faire réacheminer votre courrier.

- Informez toutes les compagnies de services publics que quelqu'un s'est servi de votre identité frauduleusement et informez les autorités compétentes qu'il se peut que quelqu'un utilise illicitement vos numéros d'assurance sociale et de permis de conduire.

- Prenez les mesures qu'il faut pour faire rayer de façon permanente de vos dossiers tous les jugements en cours civile ou criminelle résultant d'actes commis par votre voleur d'identité.

- Conservez un registre de toutes vos communications et faites des copies de tous les documents. Vous voudrez peut-être communiquer avec un organisme de protection de la vie privée ou de protection du consommateur[31].

- Dans certains cas, il peut être conseillé de consulter un avocat.

Conclusion

Le vol d'identité peut constituer une menace grave à la vie privée de la victime et lui rendre la vie très difficile. Dans cette étude, nous avons examiné brièvement certains des facteurs qui contribuent à ce crime, des moyens de l'empêcher ou, éventuellement d'y remédier.

Il faut attaquer le problème du vol d'identité sur plusieurs fronts. Le recours à des méthodes d'information équitables est un bon point de départ. En outre, comme les ordinateurs et les réseaux rendent de plus en plus facile de recueillir des renseignements personnels, les méthodes technologiques pour protéger la vie privée prendront de plus en plus d'importance. Les organismes qui peuvent offrir à leurs clients une plus grande confidentialité de leurs renseignements personnels auront sans doute un avantage sur leur concurrence. Si un plus grand nombre de personnes l'exigent, il se peut qu'à l'avenir les transactions anonymes (qui authenfient l'identité de façon anonyme) deviennent la norme, à l'encontre des transactions identifiables que l'on connaît aujourd'hui. La désidentification des renseignements représente sans doute l'avenir, en matière de protection de la vie privée.

Références

1. En 1980, l'OCDE (Organisation de coopération ou de développement économiques) a mis au point les principes reconnus à l'échelle mondiale pour le traitement responsable des renseignements personnels communément appelé le Code de pratiques équitables en matière d'emploi. Le Code établit diverses limitations et nombres concernant la cueillette, le stockage, l'utilisation, la divulgation et la sécurité des renseignements personnels. Plus récemment, l'Association canadienne de normalisation a mis à jour le Code type sur la protection des renseignements personnels.

   OCDE, *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, septembre 1980.

   Association canadienne de normalisation, CAN/CSA-Q830-96 *Code canadien de protection des renseignements personnels*. Une norme nationale du Canada, mars 1996.

2. U.S. Public Interest Research Group, *Theft of Identity : The Consumer X-Files*, août 1996, pp. 14-15.

3. Idem, p. 14.

   Article intitulé «Scam Artists Await Unwary Travellers», *Toronto Star*, 2 décembre 1995, p. F19.

4. U.S. Public Interest Research Group, *Theft of Identity : The Consumer X-Files*, août 1996, p. 15-16.

5. U.S. Public Interest Research Group, *Theft of Identity : The Consumer X-Files*, août 1996.

   Privacy Rights Clearinghouse «Coping with Identity Theft : What to Do When an Imposter Strikes», Bulletin n° 17, mai 1995.

6. «Fraud Happens : Here's How», *Privacy Journal*, juillet 1996, pp. 5-6.

7. Marta Gold, «Easy E-Mail Easy to Open — PC Privacy Just an Illusion», *Southam Newspapers*, 15 février 1997.

8. «Web Security Studied», *Globe & Mail*, 1er janvier 1997, p. B6.

9. «Cops Bust Kid Who Found Credit Numbers on Net Site», *Privacy Times*, 16 janvier 1997, p. 3.

10. Geoff Baker, «Imposter Makes Life Hell for Secretary», *The Gazette* (Montréal), 5 novembre 1992, p. A1.

11. Bob Stall, «He Conned His Way Into Hearts», *The Province* (Vancouver), 5 novembre 1995, p. A8.

12. «Marriage Was Surprise to Her : Married 4 Years to Unknown Man», *The Province* (Vancouver), 10 novembre 1995, p. A43.

13. «Theft of Identity Rises to Thousands a Day», *Privacy Journal*, février 1996, pp. 1, 4.

14. TRW est un des trois principaux bureaux de crédit aux États-Unis (les deux autres sont Equifax et Trans Union). TRW a changé son nom à Experian à l'été de 1996. Lire Robert Ellis Smith dans «Privacy : The Untold Stories», *Wired,* février 1997, p. 96.

15. U.S. Public Interest Research Group, «Theft of Identity : The Consumer X-Files», août 1996, pp. 3-5.

16. «Going Against All Three», *Privacy Journal*, mai 1996, pp. 4-5.

    «L. A. Jury Identifies With Theft of Identity Victim», *Privacy Journal*, août 1996, pp. 1, 4.

17. «Biggest Yet! Texas Couple Wins $1.45 Million for ID Theft», *Privacy Times*, 5 octobre 1995, pp. 1-3.

18. The Consumer X-Files, pp. 6-7.

19. «Flap Forces Connecticut Banks to Review Data Security Policies», *Privacy Times*, 20 juillet 1995, p. 2.

    U.S. Public Interest Research Group, *Theft of Identity : The Consumer X-Files*, août 1996, p. 31.

20. Privacy Rights Clearinghouse : «Coping with Identity Theft : What to Do When an Imposter Strikes», Bulletin n° 17, mai 1995.

    Privacy Rights Clearinghouse : «What to Do When Your Wallet is Stolen», Bulletin, n° 13, juin 1994.

    PIRG Consumer Watchdog Fact Sheet : «What Can Consumers Do to Avoid Becoming Theft of Identity Victims?»

21. Royal Bank Consumer Information brochure : «Straight Talk About Safeguarding Against Financial Fraud».

    Un usurpateur d'identité peut également causer des problèmes en envoyant des messages en se servant de l'adresse de courrier électronique de quelqu'un d'autre. C'est une bonne idée de confirmer les envois de courrier électronique en répondant pour s'assurer d'abord de leur authenticité.

22. «SSNs For Sale On-Line», *Privacy Journal*, juin 1996, p. 4.

    «Lexis-Nexis Spin : Did it Work?», *Privacy Journal*, septembre 1996, p. 7.

23. Ne pas oublier que, même si le chiffrement peut rehausser considérablement la sécurité et la confidentialité, il ne peut pas la garantir.

24. Article intitulé : «Scam Artists Await Unwary Travellers», *Toronto Star,* 2 décembre 1995, p. F19.

25. Patrick Brethour, «Is This the Year for Internet Commerce?» *Globe and Mail*, janvier 1997, p. B12.

26. David Chaum : «Achieving Electronic Privacy», *Scientific American*, août 1992.

27. Steven Levy, «Crypto Rebels», *Wired*, mai-juin 1993.

28. Sandy Sandfort, «Making Privacy Pay», *Wired*, janvier 1997.

29. «Biggest Yet! Texas Couple Wins $1.45 Million for ID Theft», *Privacy Times*, 5 octobre 1995, pp. 2.

30. PIRG Consumer Watchdog Fact Sheet : «A Checklist For Theft of Identity Victims».

    Privacy Rights Clearinghouse : «Coping with Identity Theft : What to Do When an Imposter Strikes», Bulletin n° 17, mai 1995.

31. Par exemple, Privacy Rights Clearinghouse de Californie (619-298-3396) ou Public Interest Research Group (310-397-3404).