Résultats du premier sondage sur le vol d'identité et la cybercriminalité au Québec

Septembre 2008

Québec

Conception et analyse:
Benoît Dupont
Titulaire de la Chaire de recherche du Canada en sécurité, identité et technologie

Révision linguistique:
Direction des communications

Pour obtenir une copie du présent document, veuillez vous adresser au:
Ministère de la Sécurité publique
Direction de la prévention et de la lutte contre la criminalité
2525, boul. Laurier, 4e étage
Québec (Québec) G1V 2L2
Courriel: infodplc@msp.gouv.qc.ca
Téléphone: 418-646-6708
Télécopieur: 418-646-3564

Le document est aussi disponible sur le site Internet du ministère de la Sécurité publique
à l'adresse suivante: www.msp.gouv.qc.ca

Comme le document fait mention d'estimations, précisons que les propos de l'auteur sont personnels et ne reflètent pas nécessairement ceux du ministère de la Sécurité publique. Il y a donc lieu d'interpréter les données présentées avec prudence.

Dépôt légal – Bibliothèque et Archives nationales du Québec, 2008
ISSN: 1913-1542

Table des matières

Faits saillants

- Le premier sondage québécois sur le vol d'identité et la cybercriminalité a été administré par la firme *D2 Communication Marketing* du 17 au 30 septembre 2007 auprès d'un échantillon de 1 100 personnes choisies au hasard partout au Québec, ce qui correspond à une marge d'erreur de 2,95 %, pour un intervalle de confiance de 95 %.

- Le questionnaire a été élaboré conjointement par Benoît Dupont, titulaire de la Chaire de recherche du Canada en sécurité, identité et technologies et la Direction de la prévention et de la lutte contre la criminalité du ministère de la Sécurité publique (MSP). Il comprenait 36 questions.

Résultats :

- 877 600 incidents de vol d'identité et de cybercriminalité touchent chaque année la population québécoise en âge de posséder une carte de crédit depuis au moins 12 mois (19 ans et plus).

- 3,2 % des répondants n'associent pas la fraude dont ils ont été victimes à un vol d'identité, malgré la présence de tous les critères requis par les experts dans ce domaine. Une telle méconnaissance de ce que désigne le terme « vol d'identité » risque de s'avérer problématique lors de la promotion de programmes de prévention auprès du grand public.

- 5,7 % de la population québécoise a été victime au cours des 12 derniers mois d'un vol d'identité avec préjudice financier, ce qui correspond à un nombre estimé de 338 000 incidents pour 2006-2007.

- Le type de vol d'identité qui se détache nettement de notre échantillon est l'utilisation frauduleuse de cartes de débit ou de crédit, avec 3 % de victimes parmi la population québécoise au cours des 12 derniers mois.

- L'unique variable sociodémographique semblant être associée à la victimisation vis-à-vis du vol d'identité est le niveau de revenus du foyer : des revenus élevés sont associés à des risques accrus d'être victime d'un vol d'identité.

- 52 % des victimes d'un vol d'identité sont capables d'indiquer comment, selon elles, les fraudeurs se sont approprié leurs données personnelles.

- Le clonage de cartes de débit et de crédit semble représenter à l'heure actuelle le problème principal en matière d'acquisition frauduleuse des données personnelles.

- Les préjudices financiers individuels sont relativement faibles, puisque un peu plus de la moitié des victimes (58,7 %) ont déclaré un préjudice financier inférieur à 100 $.

- La majorité (57,1 %) ont pu obtenir un remboursement intégral de leur préjudice financier mais, contrairement à ce que l'on peut penser, un nombre non négligeable de victimes (39,7 %) ont dû assumer l'intégralité des pertes subies.

- Parmi les victimes de vol d'identité (n = 63) seulement 21,9 % ont déclaré celui-ci à la police.

- La satisfaction des victimes est très forte à l'égard des institutions financières, puisque 77,8 % d'entre elles se déclarent très ou assez satisfaites de la manière dont leur banque ou organisme de crédit les a aidées à résoudre le problème.

- 4,5 % des répondants sont victimes d'intrusions ou de piratage informatiques chaque année au Québec, ce qui correspond à 267 000 incidents parmi les particuliers.

- La fraude sur Internet (fraude sur les sites d'encan, fraude nigériane, fraude par loterie) représentait 94 900 incidents en 2006-2007.

- 0,5 % des répondants ont déclaré avoir fait l'objet de harcèlement ou avoir reçu des menaces par Internet au cours des 12 derniers mois, ce qui représente 29 700 personnes au Québec.

- Les trois principales institutions qui bénéficient de la confiance du public en matière de contrôle de la cybercriminalité sont respectivement les institutions financières (68,5 %), la police (66,5 %) et les organismes de protection des consommateurs (66 %).

Introduction

La cybercriminalité et le vol d'identité figurent parmi les formes de criminalité émergentes qui semblent inquiéter le plus la population, au Québec comme dans le reste du Canada. Dès 2005, un sondage commandé par l'entreprise AOL Canada à Maritz Research faisait apparaître que le vol d'identité représentait la première préoccupation des internautes en matière de sécurité des échanges en ligne (39 %), devant l'exposition à des virus informatiques (31 %), l'utilisation de logiciels espions (16 %) ou la prolifération des pourriels (9 %).

Simultanément, la presse généraliste et informatique nord-américaine a relayé auprès de l'opinion publique les résultats alarmants d'enquêtes et de sondages menés aux États-Unis par des organismes gouvernementaux ou parapublics comme la Federal Trade Commission, le Better Business Bureau, l'Internet Crime Complaint Center ou l'Anti-Phishing Working Group, pour ne citer que les principaux. Les résultats de ces sondages en règle générale révèlent des taux de victimisation annuels relatifs à la cybercriminalité et au vol d'identité qui oscillent entre 5 et 10 % de la population, selon la méthodologie employée et le phénomène étudié.

La forte médiatisation des résultats de ces sondages est attribuable en grande partie à l'absence de statistiques officielles sur ce phénomène, puisque les services de police n'enregistrent pas de manière uniforme ces deux types de crimes et que les taux de déclaration à la police sont très bas. Il n'en demeure pas moins qu'une proportion significative de la population adulte est exposée aux États-Unis à cette nouvelle forme de criminalité.

Au Canada, puisque les données accessibles restent très fragmentaires, nous sommes obligés d'extrapoler à partir des statistiques des États-Unis, ce qui s'avère très insatisfaisant, aussi bien d'un point de vue empirique que d'un point de vue théorique. Quelques sondages ont été rendus publics au cours des dernières années, mais tous étaient commandés par des entreprises privées, dont les motivations mercantiles doivent être soulignées. La seule exception notable à ce déficit de données concerne un sondage réalisé en mai 2007 pour l'Institut de la sécurité de l'information du Québec (ISIQ) par Léger Marketing qui, dans une enquête menée auprès des internautes québécois, a posé quelques questions d'ordre général sur le vol d'identité et le harcèlement en ligne. Cette étude portait cependant principalement sur les comportements des internautes québécois en matière de sécurité, mettant l'accent sur les mécanismes de prévention et de protection adoptés plutôt que sur les actes criminels.

À la suite de l'identification par le premier ministre du Québec, M. Jean Charest, de la lutte contre la cybercriminalité comme une priorité gouvernementale lors de son assermentation le 18 avril 2007, il devenait primordial de constituer une base de connaissances sur l'ampleur du phénomène au Québec afin que la politique à mettre en oeuvre cible les besoins prioritaires de la population. Au cours de l'été 2007, une entente était donc conclue par la Direction de la prévention et de la lutte contre la criminalité du MSP avec l'auteur du présent rapport afin de concevoir, de faire administrer et d'analyser les résultats d'un sondage sur le vol d'identité et la cybercriminalité. L'administration du sondage téléphonique et la constitution de la base de données ont été réalisées par *D2 Communication Marketing* de Bromont.

Les objectifs de ce sondage étaient multiples :

- Le premier objectif consistait à **tester la connaissance du terme « vol d'identité »** parmi la population québécoise. En effet, nos recherches préliminaires ont fait apparaître que celui-ci est utilisé par les médias, les enquêteurs policiers et les praticiens de la sécurité de l'information pour désigner plusieurs pratiques très différentes les unes des autres, ce qui a pour effet de limiter sa compréhension au sein du public. Si l'on souhaite que les campagnes de prévention soient efficaces, il est indispensable que la terminologie employée soit sans ambiguïté pour le public auquel elles s'adressent.

- Le deuxième objectif du sondage était de **mesurer la prévalence du vol d'identité et de plusieurs formes spécifiques de comportements déviants ou illégaux ayant pour support Internet**, en se basant sur l'expérience des victimes, y compris celles n'ayant pas déclaré ces comportements à la police. L'intérêt de cette méthode, connue sous le nom de « sondage de victimisation », est qu'elle permet de mesurer le chiffre noir de la délinquance, c'est-à-dire les crimes qui échappent aux statistiques policières et qui, dans le domaine de la cybercriminalité, représentent la majorité des événements.

- Si la majorité des victimes ne déclarent pas ces faits à la police, elles se tournent néanmoins vers d'autres organisations qui les aideront à résoudre les problèmes qui en découlent. Pensons notamment ici – mais pas seulement – aux institutions financières. Dans cette perspective, le troisième objectif du sondage consistait à **évaluer la satisfaction des victimes de vol d'identité vis-à-vis des institutions avec qui elles doivent transiger pour réparer le préjudice qu'elles ont subi**.

- Le quatrième et dernier objectif du sondage était de **comparer les niveaux de confiance de la population envers diverses institutions publiques et privées** quant à la protection que celles-ci pouvaient lui fournir contre le vol d'identité et la cybercriminalité.

Ce rapport est par conséquent organisé en quatre parties : une fois la méthodologie du sondage présentée dans la première partie, la problématique du vol d'identité est abordée dans la deuxième partie; la troisième est consacrée aux autres formes de comportements illégaux enregistrés sur Internet; enfin, la quatrième partie traite de la confiance générale du public vis-à-vis des principales institutions responsables de la sécurité de l'information.

1. Méthodologie

Le sondage a été administré par la firme *D2 Communication Marketing* du 17 au 30 septembre 2007 au moyen d'entretiens téléphoniques. Le choix du sondage téléphonique plutôt que du sondage par Internet, qui pourrait sembler plus approprié dans ce domaine, est justifié par la volonté de réduire les biais d'autosélection qui découlent du second. En effet, les sondages par Internet ont recours à des listes préétablies de répondants qui acceptent d'être sollicités à cette fin, et qui obtiennent en échange de leur participation des points de récompense leur permettant de se procurer des biens ou des services. Si les sociétés de sondage veillent à ce que les échantillons restent le plus représentatifs possible et tentent de limiter la fréquence des participations à un nombre raisonnable, il n'en demeure pas moins qu'il est difficile d'interroger par ce moyen les personnes qui n'utilisent pas (ou peu) Internet, mais qui ont pu néanmoins être victimes de vol d'identité. Les personnes à hauts revenus sont également peu susceptibles de participer à de tels exercices, les bénéfices financiers à en tirer ne constituant pas pour elles des incitatifs suffisants. Il en va de même des personnes qui se méfient des transactions effectuées sur Internet, y compris celles de nature non marchande ou de celles qui tiennent particulièrement à protéger leur vie privée. Même s'ils ne peuvent être totalement éliminés par la technique du sondage téléphonique, ces biais sont considérablement réduits, dans la mesure où la dimension aléatoire de l'échantillonnage est beaucoup plus forte.

Échantillonnage

La taille de l'échantillon était de 1 100 personnes choisies au hasard au Québec à partir d'un CD-ROM de la société InfoCanada, qui contient de l'information détaillée sur 12 millions de Canadiens. Cette méthode d'échantillonnage est la plus couramment utilisée, puisqu'elle est à la fois simple à mettre en œuvre et qu'elle permet à chaque membre de la population de référence à partir de laquelle l'échantillon est constitué d'avoir une chance égale d'être inclus dans celui-ci. Afin de renforcer ce critère, les entrevues téléphoniques ont été menées entre 17 h et 21 h, pour pouvoir aussi bien cibler les salariés que les travailleurs autonomes ou les personnes sans emploi.

Le seul critère de sélection appliqué à cet échantillon était celui de l'âge. Pour pouvoir répondre au questionnaire, les répondants devaient avoir plus de 19 ans; ainsi, ils étaient admissibles à la possession d'une carte de crédit.

La marge d'erreur de 2,95 %, pour un intervalle de confiance de 95 % (niveau le plus répandu dans les sondages), est considérée comme très satisfaisante et fiable pour un sondage de cette nature.

Caractéristiques des répondants

Les paragraphes qui suivent décrivent les caractéristiques sociodémographiques significatives de l'échantillon et leur impact sur les résultats.

La distribution des répondants par sexe donne lieu à une légère surreprésentation des femmes, qui constituent 63 % de notre échantillon, alors qu'elles comptaient pour 51 % de la population du Québec en 2006[1]. Cette variation significative est fréquemment constatée dans les sondages téléphoniques, et est souvent attribuable à un plus fort taux de participation des femmes. On tiendra donc compte de cette surreprésentation dans les analyses.

La distribution de l'échantillon du sondage par groupe d'âge diffère de manière significative de celle de la population québécoise en 2006. On note particulièrement la non-représentation des jeunes de moins de 19 ans, inhérente à ce type de sondage, et une surreprésentation notable des 45 ans et plus.

	Échantillon (2007)	**Statistiques québécoises de 2006**
0-18 ans	Sans objet	22,3 %
19-24 ans	4,4 %	6,4 %
25-44 ans	32,5 %	28,7 %
45-64 ans	40,9 %	28,4 %
65 ans et plus	21,1 %	14,2 %
Refus	1,1 %	Sans objet

Cette différence entre l'échantillon et la population québécoise est susceptible d'avoir des répercussions sur les résultats, puisque certaines formes de comportements problématiques, comme le harcèlement ou la cyberintimidation, semblent plus répandus parmi les jeunes internautes que les autres usagers d'Internet (Erin Research 2005).

Afin de pouvoir mener des analyses plus poussées sur l'influence que des variables sociodémographiques peuvent avoir sur la victimisation des répondants au vol d'identité et à la cybercriminalité, nous avons également recueilli des données sur le niveau de revenu familial brut, le niveau de scolarité ainsi que les habitudes d'utilisation d'Internet pour des raisons personnelles et professionnelles. Les variations attribuables à ces facteurs spécifiques seront mises en évidence lorsque cela s'avérera pertinent.

1 D'après les chiffres de l'Institut de la statistique du Québec.

Description du questionnaire

Le questionnaire, élaboré conjointement par l'auteur du présent rapport et la Direction de la prévention et de la lutte contre la criminalité du MSP, comprenait 36 questions réparties en 4 groupes :

- Une série de 12 questions sur les types d'incidents de vol d'identité et de cybercriminalité dont les répondants ont été victimes au cours des 12 derniers mois;
- Une série de 7 questions sur les caractéristiques de ces incidents (délai entre la survenance et la découverte, méthode de compromission de l'information personnelle (si connue), montant des préjudices financiers subis et des remboursements consentis par les institutions bancaires);
- Une série de 10 questions portant sur la satisfaction et la confiance à l'égard des organisations publiques et privées exerce un contrôle sur ces comportements;
- Une série de 7 questions sur les caractéristiques sociodémographiques des répondants et leurs habitudes d'utilisation d'Internet.

Limites de l'étude

Bien que ce sondage constitue un outil relativement fiable permettant d'évaluer l'ampleur des phénomènes de vol d'identité et de cybercriminalité au Québec, certaines limites doivent être signalées.

Tout d'abord, le sondage ne permet pas de connaître le nombre de **cybercrimes dont les victimes sont des entreprises** et non des particuliers. Ainsi, une étude menée par ID Analytics (2007) tendrait à démontrer que plus de 88 % des vols d'identité commis aux États-Unis concernent des identités « synthétiques ». Ces identités sont entièrement ou partiellement fictives et ne correspondent par conséquent pas à des personnes. Elles sont utilisées principalement pour ouvrir de nouveaux comptes bancaires ou obtenir des cartes de crédit, qui seront ensuite utilisés intensivement sans aucune intention de remboursement. Puisque ce type de fraude touche exclusivement des entreprises, elle n'apparaîtra pas dans les résultats du sondage. Il serait toutefois utile de connaître la proportion de vols d'identité commis au Québec qui correspondent à ce mode opératoire plus organisé, par comparaison avec les vols d'identité « traditionnels ».

Selon la même logique, les données personnelles compromises par les entreprises (perte ou vol de base de données contenant de l'information personnelle, piratage de réseaux sans fil, etc.) sans qu'une fraude subséquente ait lieu ou que les victimes aient été averties ne sont pas prises en compte, même si les données ont été vendues sur le marché clandestin pour être utilisées au cours des prochains mois. Cette **limite temporelle** inclut également les victimes qui n'ont pas encore réalisé qu'elles avaient fait l'objet d'une fraude, soit parce que les délinquants n'ont pas encore monnayé les données personnelles acquises frauduleusement, soit parce que la nature de la fraude retarde sa détection.

La troisième **limite** est de nature **géographique**. En effet, ce sondage ne comprend que des répondants québécois, ce qui implique que les crimes commis à partir du Québec à l'endroit de victimes du reste du Canada ou des États-Unis ne sont pas pris en compte. De la même façon, un certain nombre de victimes québécoises peuvent avoir fait l'objet de fraudes perpétrées par des délinquants du monde entier. Les cybercrimes peuvent par définition être commis sans que la victime se trouve en aucun moment en présence du fraudeur, ce qui rend l'estimation du nombre d'incidents commis sur un territoire déterminé difficile à établir avec certitude.

La dernière limite concerne la **représentativité spécifique de l'échantillon** pour certaines questions qui ne s'adressaient par définition qu'à un sous-groupe. Ainsi, seulement 14 personnes ont répondu à la question relative à la satisfaction vis-à-vis de l'assistance offerte par la police en matière de vol d'identité. Cette situation s'explique par le fait que seulement 63 personnes appartenant à notre échantillon ont été victimes d'un vol d'identité au cours des 12 derniers mois, et que le taux de déclaration à la police (une condition nécessaire à l'émission d'un jugement informé) est inférieur à 25 %. Si un échantillon de 1 100 personnes nous permet de tirer des conclusions statistiquement significatives sur de nombreux aspects du sondage, les questions qui ne concernent que quelques dizaines de répondants doivent être interprétées avec la plus grande prudence. Le tableau ci-dessous récapitule le degré de robustesse des données en notre possession en fonction du nombre de répondants aux principales questions du sondage.

Nombre de répondants	Nature des questions	Degré de robustesse statistique
1 100 (échantillon complet)	Taux de victimisation selon les différents types de vol d'identité ou de cybercrimes	Fort
	Degré de confiance envers les institutions	Fort
63 (victimes d'un vol d'identité)	Taux de déclaration à la police	Moyen
	Montant des pertes financières subies	Moyen
	Pourcentage des préjudices financiers remboursés par les institutions financières	Moyen
	Satisfaction envers l'assistance fournie par les institutions bancaires	Moyen
33 (victimes d'un vol d'identité possédant de l'information sur le fraudeur)	Connaissance de la méthode compromission de leurs données personnelles	Faible
14 (victimes ayant déclaré le vol d'identité à la police)	Satisfaction envers l'assistance fournie par la police	Faible

2. Le vol d'identité

Comme nous l'avons précisé dans l'introduction, un des objectifs de ce sondage était d'établir le degré de connaissance de l'expression « vol d'identité » au sein de la population québécoise et son association avec certains types de comportements frauduleux expressément désignés comme tels par les spécialistes en sécurité publique et privée. Nous avons également cherché à améliorer notre connaissance de l'ampleur du phénomène du vol d'identité au Québec, ainsi que les caractéristiques des victimes, des méthodes employées par les fraudeurs et de la qualité de l'assistance fournie aux victimes par les services de police et les banques.

L'ambiguïté du « vol d'identité »

Afin de déterminer le degré de spécificité de l'expression « vol d'identité », qui a fait son entrée dans l'usage courant médiatique au cours des dernières années, une question générale correspondant à celle habituellement posée dans les autres sondages portant sur le sujet a été soumise aux répondants :

> Au cours des 12 derniers mois, avez-vous été victime d'un vol d'identité?

Cette question était posée après la définition suivante : « Fraude qui consiste à collecter et à utiliser des renseignements personnels à l'insu et sans l'autorisation de la victime, et ce, à des fins généralement criminelles. »

Cinq cas spécifiques de vol d'identité étaient ensuite présentés aux répondants, qui devaient indiquer pour chacun d'entre eux s'ils en avaient été victimes au cours des 12 derniers mois :

1. Quelqu'un a-t-il utilisé votre carte de débit ou de crédit (ou son numéro) pour faire des achats que vous n'aviez pas autorisés?
2. Quelqu'un a-t-il utilisé frauduleusement des renseignements personnels vous concernant afin d'obtenir de nouvelles cartes de crédit ou des prêts bancaires à votre nom sans votre autorisation?
3. Quelqu'un a-t-il pu accéder à votre compte bancaire et effectuer des virements de fonds ou payer des factures sans votre autorisation?
4. Quelqu'un a-t-il utilisé des renseignements personnels vous concernant afin d'obtenir des services téléphoniques, hydroélectriques ou autres à votre nom sans votre autorisation?

5. Quelqu'un a-t-il eu accès de manière frauduleuse à de l'information personnelle vous concernant, même si cette information n'a pas encore été utilisée pour commettre des fraudes ou des crimes? (Par exemple, votre banque vous a-t-elle averti de ne plus utiliser votre carte de débit ou de crédit, ou vos données personnelles ont-elles été volées à un organisme ou à une entreprise avec qui vous avez fait affaire?)[2]

Alors que 2,5 % des répondants se déclaraient victimes de vol d'identité lorsque la question générale était posée, l'addition des réponses positives aux questions spécifiques portant sur cinq cas concrets de vol d'identité donne un résultat considérablement plus important, avec 5,7 % de victimes. Cette différence notable peut être résumée de la manière suivante :

> **3,2 % des répondants n'associent pas la fraude dont ils ont été victimes à un vol d'identité, malgré la présence de tous les critères requis par les experts dans ce domaine.**

Cette différence qui change du simple au double le nombre de victimes indique clairement qu'à l'heure actuelle la population québécoise semble mal informée des phénomènes précis que désigne l'expression « vol d'identité ». Les conséquences de cette situation sont multiples.

- D'abord, les sondages ne comportant comme seul indicateur qu'une question générale risquent de sous-estimer l'ampleur du phénomène;
- Ensuite, les campagnes de prévention qui utilisent la terminologie du vol d'identité sans expliquer clairement aux destinataires quels phénomènes particuliers sont ciblés risquent de manquer leur cible, puisque de nombreuses victimes ne considéreront pas ces messages comme étant pertinents par rapport à leur situation personnelle;
- Enfin, une définition commune de ce qui constitue ou non un vol d'identité devrait être formulée par les organismes responsables de la prévention et de la répression dans ce domaine, afin de limiter au minimum les divergences d'interprétation qui ne peuvent que renforcer la perplexité du public.

2 Bien que ce cas de figure ne représente pas une fraude au sens littéral du Code criminel (dans son énoncé actuel), il concerne néanmoins la première étape du mode opératoire des voleurs d'identité, qui consiste à acquérir l'information personnelle de leurs victimes. Il arrive que les mécanismes de détection de la fraude déployés par les institutions bancaires et d'autres organisations soient capables de déceler de telles tentatives avant que les fraudeurs puissent monnayer cette information. Les procédures de remplacement de cartes de débit ou de crédit qui sont mises en œuvre sont alors en mesure d'alerter les usagers sur ces tentatives.

La prévalence des diverses formes de vol d'identité

Comme nous l'avons indiqué précédemment, nous avons mesuré la prévalence de cinq types de vol d'identité commis au Québec entre septembre 2006 et septembre 2007. De manière à simplifier la suite des analyses, les cinq catégories peuvent être désignées comme suit :

- Utilisation frauduleuse de la carte de débit ou de crédit de la victime (ou de son numéro);
- Obtention frauduleuse d'une nouvelle carte de débit ou de crédit ou d'un prêt financier grâce à de l'information personnelle de la victime;
- Accès frauduleux à un compte bancaire appartenant à la victime;
- Obtention frauduleuse de services téléphoniques, d'électricité ou autres grâce à l'information de la victime;
- Information personnelle compromise sans fraude subséquente (au moment du sondage).

Le tableau suivant présente les pourcentages de répondants victimisés selon les cinq catégories de vol d'identité, classés de manière décroissante.

Catégorie de vol d'identité	**Pourcentage de victimisation**
Utilisation de carte de débit ou crédit	3,0 %
Informations personnelles compromises sans fraude	2,5 %
Accès comptes bancaires	1,0 %
Services de téléphonie, d'électricité ou autres	0,9 %
Obtention de carte de crédit ou prêt	0,8 %

Le pourcentage de victimisation est calculé en fonction de chaque type de crime, mais on ne peut pas obtenir le pourcentage global de victimes par une simple addition, puisqu'une même personne peut être victime de plusieurs fraudes. Ainsi, dans notre échantillon de 1 100 répondants, 63 victimes ont subi 90 incidents, soit une **moyenne annuelle de 1,4 incident par victime.**

Il serait donc préférable que les programmes de prévention soient axés sur les victimes d'un premier vol d'identité, dans la mesure où elles risquent plus que les autres personnes d'être de nouveau touchées par ce phénomène dans les 12 mois suivant l'incident initial.

Si l'on projette les données de notre échantillon sur l'ensemble de la population en âge de posséder une carte de paiement, en faisant abstraction de l'information personnelle compromise sans qu'un préjudice financier subséquent ait été observé, on peut conclure que **le nombre estimé de vols d'identité était de 338 000 en 2006-2007 au Québec, pour un peu plus de 240 000 victimes**.

Le type de vol d'identité qui se détache nettement de notre échantillon est l'utilisation frauduleuse de cartes de débit ou de crédit. Cette situation peut s'expliquer par la facilité technologique avec laquelle l'information personnelle stockée sur les pistes magnétiques des cartes actuelles peut être copiée par les délinquants (par procédé de « clonage ») et la difficulté de repérer dans les points de vente les cartes douteuses dans un contexte où des millions de transactions sont effectuées chaque jour.

Facteurs de risque

Bien que l'on puisse s'attendre à ce que les Québécois soient exposés de manière différentielle au risque d'être victimes d'un vol d'identité selon leurs caractéristiques sociodémographiques ou leurs habitudes de vie, les données du sondage ne nous permettent pas d'établir des profils particuliers de victimes en raison de l'insuffisance des cas recensés (63).

L'unique variable sociodémographique semblant être associée à des risques plus élevés d'être victime d'un vol d'identité est le niveau de revenus du foyer. En effet, les Québécois dont les revenus bruts annuels sont supérieurs à 80 000 $ sont surreprésentés dans notre échantillon de victimes pour trois modes opératoires particuliers. En effet, alors qu'ils ne représentent que 12,5 % de notre échantillon, ces répondants à revenus élevés comptent pour 33,3 % des victimes d'usage frauduleux de cartes de débit ou de crédit, pour 40 % des victimes d'obtention frauduleuse de services (hydroélectricité, télécommunications, etc.) et pour 48,1 % des personnes convaincues que leurs données personnelles ont été acquises frauduleusement, même si aucune fraude n'a encore été commise.

Il est difficile d'établir à l'aide des données à notre disposition si cette surreprésentation doit être attribuée à la prédilection des délinquants pour des victimes plus « rentables » ou au manque de précautions dont peuvent faire preuve ce groupe de répondants. Dans le cas d'usage frauduleux des cartes de débit et de crédit, le marquage distinctif des cartes associées à des comptes « privilégiés » constitue par exemple un moyen rapide et aisé d'identification des victimes potentiellement plus lucratives par les fraudeurs. On peut aussi imaginer que les habitudes d'utilisation de services financiers des Québécois aux revenus les plus élevés les exposent statistiquement plus fréquemment à des « rencontres » avec les fraudeurs.

Afin d'approfondir notre connaissance du profil des victimes, il serait intéressant de réaliser un sondage dont l'échantillon serait exclusivement constitué de répondants ayant été victimes d'un vol d'identité. Étant donné notre estimation de 240 000 victimes en 2006-2007, un échantillon de 1 062 victimes sélectionnées au hasard à partir des dossiers d'institutions financières et de services de police pourrait nous donner une image relativement fiable de la situation, avec une marge d'erreur acceptable de 3 % (19 fois sur 20).

Une autre conclusion à tirer des données parcellaires à notre disposition est de s'assurer que les campagnes de prévention atteignent bien cette catégorie particulière de victimes, qui pourrait à tort s'estimer protégée contre ce phénomène en raison de son statut économique élevé ou qui possède certainement des habitudes de consultation des médias de masse (télévision, radio, presse) différentes des segments à revenus plus bas de la population québécoise.

Modes opératoires

Seulement **52 % des victimes d'un vol d'identité sont capables d'indiquer comment (selon elles) les fraudeurs se sont approprié leurs données personnelles**. Ce faible taux de connaissance des moyens et des stratégies employés par les délinquants rend d'autant plus difficile la détection précoce par les victimes de ce type de fraude.

Le tableau ci-dessous illustre la distribution des techniques employées par les fraudeurs :

Techniques d'acquisition des données personnelles utilisées par les fraudeurs (d'après les victimes)	**Pourcentage (N = 33)**
Clonage ou écrémage électronique de cartes	39,4 % (N = 13)
Employés corrompus au sein d'une organisation publique ou privée	15,2 % (N = 5)
Vol ou piratage d'une base de données appartenant à une organisation publique ou privée	12,1 % (N = 4)
Perte ou vol de sac à main ou de porte-monnaie	9,1 % (N = 3)
Piratage de l'ordinateur personnel ou professionnel de la victime	6,1 % (N = 2)
Données volées par des personnes provenant de l'entourage de la victime	3,0 % (N = 1)
Hameçonnage	3,0 % (N = 1)
Télémarketing frauduleux	3,0 % (N = 1)
Autre	9,1 % (N = 3)

Même si ces chiffres sont trop minimes pour que nous puissions en tirer des conclusions définitives concernant les modes opératoires privilégiés par les fraudeurs, quelques remarques s'imposent :

- Le clonage, qui implique un contact physique avec la carte originale de la victime, semble représenter, à l'heure actuelle, le problème le plus pressant en matière de capture des données personnelles et devrait certainement constituer la priorité des programmes de prévention et de répression du vol d'identité;
- Les deux méthodes suivantes les plus fréquemment utilisées impliquent la vigilance des organisations publiques et privées, qui semblent être confrontées à des infiltrations de la part de fraudeurs, ou à des attaques ciblées de leurs bases de données. À ce titre, des campagnes de prévention destinées aux particuliers n'auraient que peu d'effet sur ces stratégies, et des initiatives spécifiquement conçues pour les entreprises et les organismes gouvernementaux devraient être envisagées;
- Les techniques frauduleuses les plus souvent mentionnées dans la littérature nord-américaine sur le vol d'identité, qu'il s'agisse de l'acquisition des données par des proches de la victime ou de l'hameçonnage, ne figurent que de manière anecdotique dans les résultats du sondage. Cette situation doit nous amener à nous questionner sur le transfert de programmes et de conseils de prévention provenant de territoires qui sont confrontés à des réalités très différentes de la situation québécoise.

Les **délais de découverte de la fraude** sont par ailleurs inférieurs à ceux observés dans d'autres sondages nord-américains. Ainsi, le tiers des fraudes sont découvertes dans les 24 heures de leur réalisation, et un autre tiers dans des délais inférieurs à une semaine. Alors que seulement 43 % des vols d'identité étaient découverts dans un délai inférieur à un mois aux États-Unis en 2005, selon un sondage de l'Identity Theft Data Clearinghouse (2006), le sondage québécois estime plutôt la proportion de ces détections précoces à plus de 81 % des affaires déclarées. Par contraste, alors que 24 % des vols d'identité étaient découverts plus de un an après avoir été commis aux États-Unis, la proportion de détections tardives de notre sondage n'est que de 3,1 %. Cette différence significative pourrait expliquer, en grande partie, pourquoi le préjudice financier est considérablement moins élevé au Québec qu'aux États-Unis, la détection rapide combinée des victimes et des institutions bancaires réduisant la fenêtre temporelle pendant laquelle les fraudeurs peuvent monnayer l'information personnelle dérobée.

Préjudices financiers

Étonnamment, **plus de la moitié des victimes (58,7 %) ont déclaré un préjudice financier inférieur à 100 $**, et 22,2 % de plus ont vu leurs pertes ne pas dépasser 500 $. Seulement 6,3 % des victimes ont enregistré des pertes supérieures à 5 000 $. Cette limitation du préjudice financier des victimes semble confirmer les données statistiques les plus importantes disponibles à ce jour, puisqu'un sondage américain mené en 2004 par le National Institute of Justice (2006) auprès d'un échantillon beaucoup plus important (77 000 foyers) révèle que plus de la moitié des victimes avaient subi un préjudice financier inférieur à 500 $, et que seulement 5 % avaient perdu plus de 5 000 $.

Il ne s'agit pas de minimiser l'impact du vol d'identité sur les victimes, puisque notre sondage ne permet pas de quantifier le temps consacré par celles-ci à obtenir une compensation, à renouveler leurs documents ou à prouver leur innocence. Ces tâches peuvent mobiliser l'énergie des victimes pendant plusieurs jours, voire plusieurs semaines. Par ailleurs, les pertes assumées par les institutions financières ou les organisations impliquées dans de tels incidents ne sont pas prises en considération.

Cependant, il semble que, si on considère chaque affaire séparément, les sommes dérobées par les délinquants sont relativement limitées, même si les profits globaux découlant de ce type de fraude sont considérables. Il s'agit par conséquent d'un type de crime à fort volume et à faible impact contre lequel les moyens traditionnels de répression semblent mal adaptés. Par contre, on peut imaginer que le déploiement par les institutions bancaires de systèmes informatisés de veille et d'analyse des transactions frauduleuses joue un rôle important dans la détection précoce des vols d'identité et dans la limitation des préjudices financiers.

Plus de la moitié des victimes (57,1%) ont pu obtenir un remboursement intégral de leur préjudice financier mais, contrairement à ce que l'on peut penser, un nombre non négligeable de victimes (39,7 %) ont dû assumer l'intégralité des pertes subies. Comme on le verra plus loin, cette politique non systématique de remboursement ne semble pas influencer la satisfaction des victimes à l'égard de leur institution financière.

Déclaration à la police

Parmi les victimes d'un vol d'identité, seule une victime de vol d'identité sur cinq a déclaré celui-ci à la police. Aucune variable sociodémographique ne semble influencer le taux de déclaration. Ce chiffre relativement bas s'explique par la politique de remboursement des institutions financières, ainsi que par les faibles sommes en cause dans la majorité des affaires et, peut-être aussi, par le faible intérêt des organisations policières pour ce type d'incidents, sauf si les pertes représentent plusieurs milliers de dollars.

Ce faible taux de déclaration a cependant comme inconvénient majeur d'empêcher la collecte systématique de données, puisque celles dont dispose la police sont incomplètes et que celles qui sont dispersées parmi les organismes publics et privés sont rarement partagées avec les organismes chargés d'élaborer les politiques de prévention et de lutte contre le vol d'identité. La question d'une **obligation de déclaration** annuelle de la part des institutions financières et des autres organismes doit donc être posée. D'autres juridictions ont également mis en place des sites Internet destinés à recueillir les plaintes du public et à les réacheminer aux autorités responsables, à l'instar de l'Internet Crime Complaint Center du FBI (www.ic3.gov) ou du Centre de signalement en ligne des délits économiques de la Gendarmerie royale du Canada (www.recol.ca). S'il est fort peu probable que toutes les victimes signalent sur ces sites les vols d'identité qu'elles ont subis, leur facilité de déclaration pourrait améliorer significativement la qualité des données accessibles, afin de mieux adapter les réponses répressives et préventives.

La satisfaction des victimes à l'égard de la police et des institutions financières

Comme nous l'avons signalé précédemment, **la satisfaction des victimes est très élevée à l'égard des institutions financières, puisque 77,8 % d'entre elles se déclarent très ou assez satisfaites de la manière dont leur banque ou organisme de crédit les a aidées à résoudre le problème**. Seulement 15,8 % des victimes émettent un avis assez ou très négatif sur le traitement dont elles ont fait l'objet de la part de leur institution financière. Cette opinion très favorable de la part des victimes contraste avec la satisfaction plus mitigée à l'égard de la police.

En effet, même si une majorité (57 %) des victimes ayant fait une déclaration à la police se disent assez ou très satisfaites, un peu plus d'**un tiers des répondants à cette question se déclarent très insatisfaits (35,8 %) de l'assistance offerte par la police**. Il faut cependant rappeler que le faible nombre de personnes ayant répondu à cette question nous empêche de tirer des conclusions statistiquement significatives des réponses recueillies. Malgré cette mise en garde, ces chiffres laissent penser que des efforts importants doivent être consentis par les organisations policières pour prendre en charge de manière plus satisfaisante les plaintes des victimes de vol d'identité.

3. Les autres formes de cybercriminalité

Bien que ce sondage ait eu pour thème principal le vol d'identité, une série de questions étaient consacrées à d'autres formes de cybercriminalité, qu'il s'agisse de piratage et d'intrusions informatiques, de fraude ou de harcèlement en ligne.

Intrusions et piratage informatiques

Les intrusions et le piratage informatiques portent atteinte à l'intégrité des machines et des équipements utilisés pour accéder aux services en ligne ou pour stocker des données personnelles sur un support électronique. Les objectifs poursuivis par les délinquants responsables de ces actes sont multiples : dans certains cas, on cherche à détruire les données ou à rendre l'équipement inutilisable. La plupart du temps, cependant, les auteurs souhaitent plutôt obtenir les données personnelles des utilisateurs afin de commettre eux-mêmes des fraudes ou de les revendre à des fraudeurs sur les marchés clandestins en ligne. Un troisième objectif peut être d'implanter un programme qui permettra au délinquant la prise de contrôle de milliers (ou parfois de millions) d'ordinateurs à l'insu de leurs propriétaires afin de relayer des pourriels ou de lancer des attaques concertées contre des réseaux informatiques (attaques distribuées par déni de service ou DDOS). On appelle ces réseaux malveillants d'ordinateurs compromis des «zombinets», et les machines qui les composent des «zombies».

La question du sondage relative au piratage portait spécifiquement sur l'équipement informatique personnel du répondant.

Les résultats révèlent que **4,5 % des répondants sont victimes de ce phénomène chaque année au Québec, ce qui correspond à 267 000 incidents de piratage ou d'intrusions chez des particuliers**.

Tous les internautes ne semblent pas exposés aux mêmes risques : en effet, les facteurs tels que l'âge, le sexe et la fréquence d'utilisation influencent fortement les probabilités d'être victime d'un acte de piratage ou d'une intrusion informatique. Les Québécois de **moins de 35 ans**, qui représentent 17,6 % de notre échantillon, comptent pour 30 % des victimes, alors que les plus de 55 ans, qui représentent 38,6 % de notre échantillon, ne dépassent pas 16 % des victimes.

De même, les répondants qui passent **plus de 10 heures par semaine sur Internet pour des raisons personnelles** (9,9 % de l'échantillon) sont surreprésentés parmi les victimes (26 %), comparativement aux usagers épisodiques qui consacrent moins de 5 heures par semaine à cette activité (74,8 % des répondants, mais seulement 54 % des victimes).

Enfin, le sexe semble être un facteur discriminant pour l'exposition à ce type de risques. En effet, les 37,3 % d'**hommes** ayant répondu à ce sondage représentent 56 % des victimes.

Ces trois observations semblent démontrer que **le fait d'être un usager régulier et aguerri des nouvelles technologies de l'information ne protège absolument pas contre les tentatives de piratage ou d'intrusion**, puisque les personnes pouvant être décrites comme celles qui ont les connaissances les plus approfondies de ces outils sont aussi celles qui sont le plus susceptibles d'être confrontées à ce type d'incident. Il est toutefois nécessaire de rappeler que cette affirmation s'appuie sur des données très incomplètes, et qu'on pourrait également supposer que c'est justement cette expertise qui permet aux répondants de déceler des incidents de piratage ou d'intrusion là où des usagers plus novices sont moins conscients des menaces ayant atteint leur équipement.

Les fraudes sur Internet

Les fraudeurs utilisent de manière croissante Internet pour identifier et contacter des cibles potentielles, qui vont alors être persuadées de manière plus ou moins élaborée de se départir de sommes d'argent parfois considérables en échange d'un bénéfice qui ne se matérialisera jamais. Plusieurs types de fraudes ont cours sur Internet :

- La **fraude sur les sites d'encan en ligne** (eBay, Kijiji, etc.) ou les sites de petites annonces (LesPAC) consiste pour le fraudeur à promettre à sa victime la livraison d'un bien à un prix défiant toute concurrence. Une fois le paiement reçu par le fraudeur, celui-ci disparaît ou fait parvenir à sa victime un produit ne correspondant pas aux spécifications initiales. Afin de faciliter ce type de fraude, les délinquants peuvent avoir recours au piratage de comptes légitimes pour bénéficier de la bonne réputation de leurs détenteurs. Ce type de fraude est le plus répandu aux États-Unis, puisqu'il représente 12 % des affaires analysées en 2005 par l'Identity Theft Data Clearinghouse (2006), et 44,9 % des plaintes reçues par l'Internet Crime Complaint Center (2007) pour 2006. Au Québec cependant, ce type de fraude ne concerne que **0,7 % de la population. Le facteur de la langue pourrait constituer** une explication à ce nombre réduit, étant donné que les sites les plus fréquentés sont principalement destinés à une clientèle anglophone.
- La **fraude nigériane**, aussi connue sous le nom de fraude 419, consiste à faire croire au destinataire d'un courriel que l'expéditeur est en possession de fonds importants (héritage, compte bancaire « oublié », investissement à réaliser à l'étranger afin d'échapper à un contexte politique instable, etc.) auquel il ne peut accéder sans son assistance. Le fraudeur propose à la victime de toucher un pourcentage de ces fonds en échange de son aide. La fraude repose sur des demandes répétées d'avances de fonds du fraudeur à la victime afin de couvrir des frais administratifs qui permettront de finaliser le transfert. Ce dernier n'a bien évidemment jamais lieu, puisque toute l'affaire est fictive. Seulement **0,4 % de notre échantillon** a répondu positivement à une telle demande en envoyant une somme d'argent aux fraudeurs, ce qui représente **23 700 incidents annuels**. Il semble que les campagnes de mise en garde menées au cours des dernières années dans les médias aient porté leurs fruits.

- Une variante de la fraude nigériane est la **fraude par loterie ou par concours. Dans ce cas,** la victime reçoit un courriel lui annonçant qu'elle a gagné un prix important, mais qu'elle doit acquitter des frais juridiques ou fiscaux pour permettre le versement des fonds. Une fois l'avance de fonds consentie par la victime, les fraudeurs disparaissent. Ce type de fraude a touché **0,5 % de notre échantillon**, ce qui équivaut à **29 700 incidents annuels** au Québec. Bien que ce type de courriel soit le plus fréquemment rédigé en anglais, on assiste à une recrudescence des propositions rédigées en français.

- La **fraude boursière** connue sous l'expression *pump and dump* consiste à convaincre le destinataire d'un courriel d'acheter une action de très faible valeur (habituellement quelques cents) en lui faisant miroiter une augmentation spectaculaire de son cours à la suite d'une découverte scientifique, minière ou de la signature d'un contrat qui sont seulement connus des initiés. Les fraudeurs se sont préalablement portés acquéreurs de quantités importantes de cette action, et l'achat concerté des victimes provoque un gonflement artificiel des cours qui est mis à profit par les premiers pour réaliser des profits ne reposant sur aucune réalité économique. Les victimes se retrouvent alors propriétaires d'actions sans aucune valeur. **Aucun des répondants de notre sondage n'a déclaré avoir été victime d'une telle fraude au cours des 12 derniers mois**. Ce constat semble confirmer les résultats d'un sondage mené pour les Autorités canadiennes en valeurs mobilières (Innovative Research Group 2007), qui montre que les Québécois sont beaucoup moins sollicités que les résidents des autres provinces canadiennes par les fraudeurs, la langue jouant, là encore, certainement un rôle important.

Les montants des préjudices financiers découlant des quatre types de fraude mentionnés précédemment sont relativement limités, puisque **75 % des victimes ont déclaré des pertes inférieures à 100 $**, et que les 25 % qui restent ont vu leur préjudice limité à moins de 500 $. Même si les chiffres à notre disposition sont trop incomplets pour pouvoir en tirer des conclusions statistiquement significatives, il semblerait que les fraudes ayant pour support Internet ne produisent pas de préjudices financiers considérables et que l'impact qui en découle pour les victimes est relativement bénin.

Le harcèlement et les menaces en ligne

Une dernière forme de conduite illégale en ligne faisait l'objet d'une question dans notre sondage. Il s'agit des menaces et du harcèlement qui utilisent Internet comme support, que ce soit par l'intermédiaire d'un courrier électronique, de sites de réseaux sociaux (*Facebook, Myspace*…), de forums de clavardage ou de sites traditionnels. Les manifestations de ce type semblent peu fréquentes au Québec, puisque seulement **0,5 % de notre échantillon** a déclaré y avoir été confronté au cours des 12 derniers mois, ce qui correspond à **29 700 incidents annuels** au Québec. Ce chiffre relativement bas semble indiquer qu'au Québec Internet est plutôt caractérisé par des relations de civilité et de respect entre ses usagers, du moins en ce qui concerne ceux de plus de 19 ans.

4. La confiance du public

Nous avons vu l'ampleur des principales formes de cybercriminalité et de vol d'identité au Québec. Afin de pouvoir mettre en œuvre des programmes de prévention et de répression efficaces, qui puissent bénéficier d'une collaboration optimale de la population, il est nécessaire de connaître le degré de confiance de cette dernière vis-à-vis des diverses institutions qui exercent des responsabilités dans ce domaine.

Le sondage comprenait des questions relatives à la confiance du public dans la capacité de prévenir et de contrôler la cybercriminalité et le vol d'identité portant sur huit types d'institutions. Le tableau ci-dessous présente les résultats obtenus par ordre décroissant de confiance :

Organisation	Degré de confiance
Institutions financières	68,5 %
Police	66,5 %
Organismes de protection des consommateurs	66,0 %
Tribunaux	56,3 %
Services gouvernementaux	55,7 %
Fabricants d'équipement informatique et de logiciels	40,5 %
Fournisseurs d'accès à Internet	37,6 %
Entreprises offrant des biens et des services sur Internet	22,2 %

Ces résultats laissent entrevoir une **hiérarchie informelle inattendue qui place les institutions financières au premier rang des organisations ayant la confiance du public contre la cybercriminalité et le vol d'identité.** La police et les organismes de protection des consommateurs arrivent respectivement en deuxième et troisième position avec plus de 65 % de confiance. En dernier rang, on trouve des entreprises qui fournissent les infrastructures nécessaires au bon fonctionnement d'Internet ou dont les activités économiques reposent principalement sur le réseau. Ce manque de confiance reflète certainement la perception du manque d'intérêt des entreprises concernées pour les questions de sécurité, par contraste avec les institutions financières qui semblent déployer des systèmes de lutte contre la fraude plus performants et qui disposent de politiques de compensations financières relativement généreuses.

Il faut toutefois préciser que la confiance dans ces institutions ne se répartit pas de manière identique parmi tous les groupes de la population. Ainsi, les **répondants ayant des revenus annuels de plus de 80 000 $** font moins confiance à la police (-5,2 %) et aux tribunaux (-7,4 %) que le reste de l'échantillon, mais semblent par contre plus confiants envers les fournisseurs d'accès à Internet (+6,2 %) ou les fabricants d'équipements et de logiciels (+15 %). **Les jeunes de 19 à 24 ans** semblent également accorder une confiance plus importante que les autres répondants aux fournisseurs d'accès à Internet (+8,2 %), aux entreprises qui offrent des services et des biens sur Internet (+11,1 %), ainsi qu'aux fabricants d'équipement informatique et de logiciels (+17,8 %). Pour leur part, les **utilisateurs fréquents d'Internet** (plus de 20 heures par semaine pour un usage personnel) font moins confiance à la police (-16,5 %) que leurs concitoyens, alors qu'ils semblent accorder plus de crédit aux fournisseurs d'accès (+7,4 %), aux entreprises offrant des biens et des services (+10,3 %) et aux fabricants d'équipement informatique et de logiciels (+22 %).

Ces variations suggèrent que **la perception des capacités des principales institutions et entreprises en matière de contrôle de la cybercriminalité varie au sein de la population**, selon des variables sociodémographiques qui correspondent assez étroitement à celles associées à des risques accrus de victimisation. Dès lors, il serait intéressant de poursuivre la réflexion afin de vérifier si une confiance excessive dans certaines organisations ne pousserait pas certains usagers à adopter des comportements à risque dans leur utilisation d'Internet. Ces variations devront également être prises en compte lors de la conception de programmes de prévention et de contrôle de la cybercriminalité, aussi bien à l'étape de la définition des objectifs (en incluant des mesures destinées à faire connaître les capacités d'intervention de la police, par exemple) qu'à celle du choix des moyens à mettre en œuvre afin de mobiliser les institutions qui sont le plus susceptibles d'avoir un impact sur les usagers.

Conclusion

Le sondage mené en septembre 2007 offre pour la première fois une estimation de l'ampleur du vol d'identité et de la cybercriminalité qui touchent les particuliers au Québec. Les statistiques recueillies nous permettent d'estimer que, chaque année, 877 600 incidents associés à ces deux phénomènes touchent la population adulte de plus de 19 ans, causant un préjudice financier de plusieurs dizaines de millions de dollars en plus d'un préjudice moral difficile à mesurer.

Type d'incident	**Nombre estimé annuel d'événements au Québec**[3]
Vol d'identité (avec préjudice financier)	338 000
Vol d'identité (sans préjudice financier immédiat)	148 000
Intrusions et piratage informatiques	267 000
Fraude sur Internet	94 900
Harcèlement et menaces au moyen d'Internet	29 700
Total	**877 600**

Ce sondage nous a également permis de mesurer la satisfaction des victimes de vols d'identité à l'égard des institutions financières et des organisations policières, les premières obtenant des résultats élevés inattendus confirmés par la confiance qui leur est accordée par la population pour contrôler la cybercriminalité.

Parmi les différents types de cybercriminalité ayant fait l'objet de questions, les intrusions et le piratage représentent à l'heure actuelle la principale menace en volume, suivis par les diverses formes de fraude financière qui utilisent Internet comme moyen privilégié de communication avec les victimes.

Les questions sur la confiance des Québécois envers les diverses institutions et organisations responsables du contrôle de la cybercriminalité ont également fait apparaître la prééminence de trois acteurs : les institutions financières, la police et les organismes de protection des consommateurs. Ainsi, toute politique de prévention devra intégrer ces derniers et des efforts considérables devront également être consentis par les principales entreprises de la cyberéconomie, dont les performances ne semblent pas inspirer confiance à la population, à l'exception de certains groupes qui présentent les risques les plus élevés d'être victimisés.

3 Arrondi à la centaine la plus proche.

Enfin, il est souhaitable que les données de ce sondage soient considérées comme un **premier point de référence** à partir duquel on pourra évaluer l'évolution du phénomène et des réponses qui y seront apportées au cours des prochaines années. Il est à ce titre impératif que les résultats (et la méthodologie utilisée) soient diffusés aussi largement que possible auprès des divers partenaires et du public, afin que ceux-ci puissent débattre de leur utilité et suggérer des améliorations, en perspective d'une administration régulière qui pourrait se faire sur une base annuelle ou bisannuelle. Cette approche aurait pour intérêt principal de **normaliser les définitions** des phénomènes relatifs à la cybercriminalité et au vol d'identité, en plus de constituer une **base de connaissances communes** produite et mise à jour de manière transparente et selon des critères scientifiques.

Références

Baum, Katrina (2006), *Identity theft 2004: First estimates from the National crime victimization survey*, Washington DC: Bureau of Justice Statistics.

Erin Research (2005), *Young Canadians in a wired world phase II*, Ottawa: Réseau education médias.

ID Analytics (2007), *National fraud ring analysis: Understanding behavioral patterns*, San Diego: ID Analytics.

Identity Theft Data Clearinghouse (2006), *Identity theft complaint data figures and trends January 1-December 31 2005*, Washington DC: Federal Trade Commission.

Innovative Research Group (2007), *2007 CSA investor study: Understanding the social impact of investment fraud*, Montréal: CSA-ACVM.

Internet Crime Complaint Center (2007), *Internet crime report January 1st, 2006 – December 31st, 2006*, Washington DC: FBI & National White Collar Crime Center.

Weisel, Deborah Lamm (2005), *Analysing repeat victimization*, Washington DC: Center for Problem-Oriented Policing.