

La fraude via les médias sociaux

Nancy Ryan, Pierre-Eric Lavoie, Benoit Dupont
& Francis Fortin

Note de recherche no. 13



Benoît Dupont, Ph.D.

Titulaire de la Chaire de recherche du Canada en sécurité, identité et technologie,
Université de Montréal

Francis Fortin, M.Sc.

Direction du renseignement et des enquêtes criminelles, Division de l'analyse
stratégique, Sûreté du Québec

Pierre-Eric Lavoie, Candidat à la Maîtrise

École de criminologie, Université de Montréal

Nancy Ryan, Candidat à la Maîtrise

École de criminologie, Université de Montréal

Cette recherche a été entreprise grâce au soutien financier du Conseil de Recherches en Sciences Humaines du Canada et du Programme des chaires de recherche du Canada, ainsi qu'en partenariat avec la Sûreté du Québec.

La Chaire de recherche du Canada en sécurité, identité et technologie de l'Université de Montréal mène des études sur les pratiques délinquantes associées au développement des technologies de l'information, ainsi que sur les mécanismes de contrôle et de régulation permettant d'assurer la sécurité des usagers. Elle collabore pour cela avec des organismes gouvernementaux et des entreprises.

Prof. Benoît Dupont

Centre International de Criminologie Comparée (CICC)

Université de Montréal

CP 6128 Succursale Centre-ville

Montréal QC H3C 3J7 - Canada

benoit.dupont@umontreal.ca

www.benoitdupont.net

Fax : +1-514-343-2269

© Chaire de recherche du Canada en sécurité, identité et technologie 2011

Faits saillants

Les médias sociaux ont connu ces dernières années une croissance exponentielle. Facebook, le plus populaire d'entre eux, revendiquait ainsi plus de 500 millions de membres au début de l'année 2011.

Tout comme les autres innovations technologiques survenues avant lui, les médias sociaux présentent des opportunités intéressantes pour les fraudeurs qui peuvent exploiter la confiance liant les usagers de ces services en ligne.

Afin de mieux comprendre la nature et la structure de ces risques, une base de données d'incidents criminels associés à des sites de socialisation en ligne a été constituée à partir de comptes-rendus médiatiques.

L'échantillon global comprend 1301 cas recueillis sur une période de vingt-quatre mois (octobre 2008 à septembre 2010), dont 10,1% (131 cas) concernent des affaires de fraude.

Il est possible de classer celles-ci en deux grandes catégories : les fraudes élaborées qui se divisent en quatre sous-catégories (la fraude par abus de confiance, la fraude de location immobilière, la fraude par usage de faux et l'offre de services sans permis) et le vol d'identité.

Les fraudes élaborées (76,3%) représentent un volume trois fois plus important d'affaires dans notre échantillon que les vols d'identité (23,7%). À eux seuls, les abus de confiance (29,8%) et les locations immobilières fictives (24,4%) sont responsables de plus de la moitié des fraudes perpétrées par le biais des médias sociaux.

La grande majorité des incidents rapportés par les médias se sont produits sur Craigslist (77,9%) alors qu'une minorité d'entre eux sont survenus sur Facebook (13%). Presque tous les événements de fraude élaborée se sont déroulés sur des sites d'annonces classées (93%) alors que les vols d'identité se commettent majoritairement sur les sites de réseautage social (71%).

Concernant l'âge des suspects et des victimes, les résultats montrent que les fraudeurs sont un peu plus jeunes en moyenne (29,7 ans) que les victimes (33,3 ans). De plus, les fraudeurs élaborés (34,6 ans) seraient plus âgés que les voleurs d'identité (24 ans).

Comme pour la majorité des crimes commis sur le web 2.0, les suspects de fraudes sont presque tous de sexe masculin (80%). Il faut toutefois noter que le vol d'identité semble attirer une plus forte proportion de suspects de sexe féminin (26,3%) que les fraudes élaborées (17,1%).

Les résultats montrent également que les victimes de fraudes commises sur le web 2.0 sont réparties plutôt également selon le sexe. En effet, sur les 71 victimes identifiées, 49,3% sont de sexe masculin.

L'ingénierie sociale est la technique de prédilection des fraudeurs sur les médias sociaux, devant les compétences informatiques, ce qui limite l'efficacité des solutions technologiques pour prévenir ce type de délinquance.

Introduction

La fraude est un crime qui se présente sous divers aspects. Il s'agit d'un terme large qui englobe tout acte illégal qui utilise la tromperie, la falsification ou l'imposture, afin de se procurer des biens, des bénéfices financiers, ou des privilèges au dépend d'individus ou d'organisations privées ou publiques. La fraude existe sous différentes formes : contrefaçon, vol d'identité, abus de confiance, détournement de fonds, réclamation mensongère aux assurances, fraude pyramidale ou encore évasion fiscale.

Avec le développement des moyens de communication en ligne, les fraudeurs ont accès à un bassin de victimes toujours plus grand. La démocratisation de l'Internet s'est accompagnée de diverses formes de fraudes comme les lettres nigérianes, l'hameçonnage, les fraudes impliquant la vente fictive d'une automobile, les combines offrant des opportunités d'affaires ou la possibilité de travailler à domicile, les fraudes d'avances de fonds et les arnaques romantiques. Il est donc peu surprenant que le passage vers une deuxième génération d'applications Internet présente de nouvelles opportunités pour les fraudeurs.

Cette note explorera la fraude associée au web 2.0. Les données utilisées furent recueillies dans le cadre d'une vigie médiatique qui compile, depuis octobre 2008, différents articles de presse concernant des comportements déviant impliquant une interaction avec le web 2.0. Ces données furent recueillies à l'aide du logiciel Yahoo! Pipes qui met à la disposition de l'utilisateur des outils permettant de filtrer et de structurer de grandes quantités d'informations. En éliminant le tri manuel, Yahoo! Pipes permet de couvrir quotidiennement 87 sources médiatiques (Dupont, Lavoie et Fortin, 2010). En date du 9 mars 2011, l'échantillon comportait 1301 cas, permettant l'identification de 1087 suspects et de 670 victimes de crimes commis sur le web 2.0.

La fraude observée sur le web 2.0

Tout comme les outils de communication qui l'ont précédé, le web 2.0 présente des opportunités intéressantes pour les fraudeurs. D'une part, le web 2.0 ouvre la porte aux fraudes reposant sur des abus de confiance. En effet, les informations diffusées par le biais des médias sociaux ne proviennent généralement pas des fournisseurs de services tels que Facebook ou Twitter, mais plutôt des autres utilisateurs avec qui la victime partage des intérêts ou entretient des liens d'amitié. L'utilisateur du web 2.0 postule donc par défaut la bonne foi de la personne à l'origine des informations, sur la base d'interactions préalables. Cette confiance est toutefois exploitée par les fraudeurs qui vont par exemple prendre illégalement le contrôle d'un compte Facebook et personifier l'ami de l'utilisateur afin de soutirer de l'argent à ce dernier. Un autre peut adopter l'identité d'un individu célèbre sur Twitter et émettre des messages qui vont profiter de la réputation de la victime pour recruter des victimes potentielles. Le

vendeur sur Craigslist, un site gratuit de petites annonces, fera miroiter aux chasseurs d'aubaines des transactions à des tarifs très avantageux qui se révéleront irréalistes.

Les résultats de l'analyse des 1301 affaires de délinquance associées à des médias sociaux démontrent que la fraude constitue 10,1% (n=131) des cas composant notre échantillon, ce qui semble peu pour un tel type d'activité délinquante et est certainement partiellement attribuable à sa sous-représentation médiatique. Il est possible de classer les affaires de fraude en deux grandes catégories : les fraudes élaborées et le vol d'identité. Les fraudes élaborées se divisent en quatre sous-catégories : la fraude par abus de confiance, la fraude de location immobilière, la fraude par usage de faux et l'offre de service sans permis.

Distribution des fraudes

| Types de fraudes | Fréquence | Pourcentage |
|--------------------------------|-----------|-------------|
| Fraudes élaborées | 100 | 76,3% |
| Fraude par abus de confiance | 39 | 29,8% |
| Fraude de location immobilière | 32 | 24,4% |
| Fraude par usage de faux | 23 | 17,6% |
| Offre de service sans permis | 6 | 4,6% |
| Vol d'identité | 31 | 23,7% |
| Total | 131 | 100% |

Il ressort de ces résultats que les fraudes élaborées sont plus fréquemment présentes dans les médias que les vols d'identité. En effet, alors que les fraudes élaborées constituent 76,3% (n=100) des nouvelles portant sur la fraude, seulement 23,7% (n=31) relèvent du vol d'identité. Il nous est impossible de savoir si cette faible présence du vol d'identité reflète une sous-représentation attribuable à un biais médiatique (en raison par exemple de la prolifération de telles affaires ou des faibles montants financiers extorqués aux victimes), ou si les fraudeurs négligent effectivement le vol d'identité pour se focaliser sur des pratiques frauduleuses plus rentables et exigeant moins d'efforts. Le type de fraude élaborée le plus commun dans les médias est la fraude par abus de confiance, suivi de la fraude de location immobilière. Les résultats montrent effectivement que 29,8% (n=39) des affaires de fraude constituent de la fraude par abus de confiance et que 24,4% (n=32) impliquent de la location immobilière.

Les différentes formes de fraudes commises à l'aide du web 2.0

La fraude élaborée

La fraude élaborée constitue un acte de tromperie commis dans le but de réaliser un gain, et ce, sans vol d'identité. La fraude élaborée serait plutôt commise par des suspects de sexe masculin. En effet, 82,9% des suspects identifiés seraient des hommes. Les victimes de fraudes élaborées sont également réparties entre les hommes et les femmes (n=50).

Fraude par abus de confiance

Ce type de fraude implique que l'arnaqueur abuse de la confiance accordée par un acheteur dans un contexte de transaction réalisée en ligne, en ne donnant pas le bien ou le service attendu après avoir été payé. Les fraudes par abus de confiance se produisent généralement selon l'un ou l'autre des scénarios suivants. D'une part, un individu peut offrir un service en ligne en exigeant une avance d'argent pour ensuite ne pas livrer celui-ci. Un article rapporte ainsi qu'une annonce d'une agence de casting diffusée sur Craigslist indiquait qu'elle était à la recherche d'individus pour participer à la prochaine saison d'une émission populaire de télé-réalité (Moylan, 2010). Une journaliste décide d'enquêter. Lorsqu'elle contacte la supposée agence de casting par téléphone, un individu prend en note quelques informations personnelles, la réfère à un site web sur lequel les individus intéressés peuvent transférer leur photographie et lui demande son numéro de carte de crédit pour payer des frais de traitement de 98\$. Or, après vérifications, la journaliste constata que l'agence de casting était fautive et qu'elle tentait de frauder des individus en quête de célébrité.

D'autre part, un vendeur en ligne peut tout simplement recevoir le paiement d'un acheteur et ne pas envoyer le bien pour lequel le paiement a été envoyé. Parfois, le bien est envoyé, mais celui-ci ne correspond pas au produit initialement offert ou est une contrefaçon. Un exemple d'un tel stratagème est la vente de faux billets pour des événements sportifs ou musicaux. Un individu de l'État de l'Illinois avait répondu à une annonce pour acheter sur Craigslist les billets de saison très convoités d'une équipe de football professionnel (Rusin, 2010). Il expédia au vendeur un chèque de 4700\$ en lui promettant de payer le solde plus tard. Or, ce ne fut pas l'acheteur qui fraudait le vendeur en ne payant pas le montant restant, mais plutôt le vendeur qui lui fournit de faux billets.

Fraude de location immobilière

La fraude de location immobilière est similaire à la fraude par abus de confiance puisque l'arnaqueur obtient un paiement pour un service qu'il n'a pas l'intention d'offrir. Par

contre, elle implique spécifiquement le domaine de l'immobilier et est généralement plus élaborée que les fraudes précédentes. Le fraudeur trouve une annonce pour une maison ou un appartement en vente sur Internet et utilise les photos qui accompagnent cette dernière afin de créer une annonce qui indique que la maison est à louer à l'année ou pour de courts séjours touristiques. Ensuite, il donne pour excuse de ne pas pouvoir faire visiter la maison ou l'appartement parce qu'il réside sur un autre continent, généralement en Afrique. Puisque le loyer est généralement considéré comme une aubaine par les futurs locataires, ceux-ci ne protestent pas. Le fraudeur demande alors aux locataires intéressés d'envoyer le montant du dépôt par la poste et affirme qu'il va leur renvoyer la clé par retour du courrier une fois l'argent reçu, ce qui ne se produit évidemment jamais (Herald-Tribune, 2009).

Fraude par usage de faux

La fraude par usage de faux diffère de la fraude par abus de confiance par le fait que le fraudeur est un acheteur plutôt qu'un vendeur. Dans ce cas-ci, l'acheteur fraudeur donne l'illusion initiale au vendeur victime que la transaction a bel et bien été réalisée équitablement, jusqu'à ce que ce dernier réalise que le mode de paiement était contrefait. Un exemple typique de fraude par usage de faux est le fait pour un acheteur de donner un faux chèque en guise de paiement pour un bien. Le but du fraudeur semble être de se procurer le bien gratuitement, mais il lui arrive parfois d'envoyer un chèque d'un montant plus élevé que le prix du bien en s'excusant de son erreur au vendeur et en lui demandant de lui renvoyer un mandat poste pour compenser une partie de la différence. Un tel cas est survenu dans l'État de New York (Lockport Union-Sun & Journal, 2009). Un individu avait mis une annonce sur Craigslist afin de vendre une pièce mécanique de camion pour 50\$. Quelques jours plus tard, il reçut l'appel d'un homme qui lui dit qu'il était intéressé par le silencieux et qu'il allait payer par mandat poste. Le lendemain, le vendeur reçut un mandat poste d'un montant de 950\$ et se fit appeler par l'acheteur qui lui dit que son comptable avait fait une erreur et envoyé trop d'argent. L'acheteur donna pour instruction au vendeur de lui transférer la différence par Western Union à une adresse à Londres en Angleterre et d'encaisser le mandat poste. Le vendeur, suspicieux des demandes de l'acheteur, contacta les autorités et eut la confirmation que le mandat poste était contrefait.

Offre de service sans permis

Le fraudeur qui effectue une offre de service sans permis crée une annonce en ligne offrant un service pour lequel il n'a pas les qualifications ou les autorisations légales nécessaires. L'offre de service sans permis ne constitue pas un vol d'identité, même si elle constitue une personification, puisque le fraudeur ne prend pas l'identité d'un individu spécifique. Un exemple concerne des déménageurs publiant une annonce sur Craigslist et opérant sans les assurances ni le permis requis par la juridiction commerciale dans laquelle ils offrent leurs services (Burke, 2009). Il faut également

noter que le recours à de tels stratagèmes n'est pas toujours dicté par la recherche d'un gain monétaire. Ainsi, Jon Glasure, un délinquant sexuel enregistré se faisait passer pour un massothérapeute et offrait ses services sur Craigslist à prix modique dans le but d'assouvir ses pulsions (CBS, 2009).

Le vol d'identité

Le vol d'identité constitue la collecte et l'utilisation non autorisées des renseignements personnels d'un individu, habituellement à des fins criminelles. Sur les 19 suspects de vol d'identité identifiés, un peu plus du quart (26,3%) sont de sexe féminin, mais plus de la moitié des victimes sont de sexe féminin sur les 21 victimes identifiées. L'âge moyen des voleurs d'identité est de 24 ans (n=12). L'analyse de l'échantillon a permis de discerner quatre principaux scénarios de vol d'identité.

Le premier est la personnification d'un individu. Le voleur d'identité crée d'abord un profil ou une annonce Internet, ou bien pirate le profil d'un individu. Par la suite, il se fait passer pour cet individu dans le but de l'humilier ou de lui transférer la responsabilité de ses actions. Dans un cas, les services secrets américains ont arrêté Neil Allan Thomas après que celui-ci ait utilisé un compte MySpace à l'insu de son propriétaire dans le but de menacer d'assassiner le président américain et de faire exploser une caserne de pompier (WMCTV, 2008). Dans un autre événement, une femme fut arrêtée pour avoir assumé l'identité de son ex-petit ami sur le site Craigslist. Elle avait publié une annonce sous le nom de ce dernier, offrant aux usagers d'appeler un numéro pour discussion érotique. Le numéro correspondait en réalité au lieu de travail de la victime (The Smoking Gun, 2009).

Le second scénario consiste à personnifier une célébrité. Le voleur d'identité se fait passer pour une personne connue et se crée un profil Internet sous cette identité. En effet, les comptes appartenant aux célébrités sont généralement fort populaires et certains chercheront à tirer profit de cette notoriété pour arriver à diverses fins, qu'il s'agisse de nuire à la personne visée, de s'immerger dans son quotidien, d'obtenir des gains personnels ou de simplement s'amuser. Deux méthodes de personnification de célébrités existent. D'abord, le pirate peut créer une fausse page ou un faux profil qui utilise les éléments identificateurs en général relativement connus de la victime. En guise d'illustration, un joueur de soccer italien, Alessandro del Piero, eut la mauvaise surprise de découvrir qu'une page à son nom existait sur Facebook et que son contenu incitait à la controverse. L'athlète intenta une poursuite contre le site Facebook, alléguant que ce faux profil ternissait son image (Rodrigue, 2009). L'autre méthode est le piratage de comptes appartenant réellement à des personnalités publiques. Dans ces situations, les pirates informatiques tirent avantage du grand nombre d'amis ou de fans dont disposent ces individus. Dans un cas, l'usurpateur avait acquis plusieurs comptes de célébrités et les utilisa pour distribuer des pourriels (Leydon, 2009). L'usurpation d'un compte utilisé par une célébrité peut également servir à diffuser des messages diffamatoires à une grande quantité de destinataires, comme ce fut le cas du compte

Twitter de Fox News qui après être tombé sous le contrôle d'un pirate, afficha un message affirmant que l'un de ses animateurs vedettes les plus conservateurs était homosexuel (Zetter, 2009).

Le troisième scénario concerne la personnification d'autrui dans le but d'en tirer un gain financier. L'individu réussit à pirater le profil Facebook d'un individu et s'adresse aux proches de celui-ci en leur demandant de lui envoyer un mandat-poste en affirmant généralement qu'il est en voyage dans un pays lointain et qu'il a été victime de vol. Ce mode opératoire est associé aux fraudes nigérianes. Elles se distinguent toutefois par des contenus qui contiennent des informations personnelles, ce qui peut accroître les chances de succès des fraudeurs. Beny Rubinstein est l'un de ceux qui tomba dans ce piège (Sutter et Carroll, 2009). Après avoir reçu le message « Bryan NEEDS HELP URGENTLY!!! » sur Facebook, l'homme questionna son ami via la messagerie intégrée à ce service sur les raisons de cette urgence. « Bryan » répondit qu'il s'était fait dérober tous ses effets personnels à Londres et qu'il avait besoin d'argent pour rentrer chez lui. Pour venir en aide à son ami, qui lui avait promis de rembourser l'argent dès son retour, Rubinstein transféra 1 143 \$ à celui qu'il croyait être Bryan. Or, le véritable Bryan n'avait jamais quitté le pays pour Londres et s'était tout simplement fait pirater son compte Facebook. Un simple coup de téléphone aurait certainement pu éviter une telle méprise.

Le dernier scénario est le vol d'identité par abus de confiance, qui s'apparente à l'hameçonnage (aussi connu sous le nom de *phishing*). L'individu crée une annonce sur Internet visant à attirer des chercheurs d'emplois ou de potentiels locataires. Le voleur d'identité précise alors à ces individus que pour obtenir l'emploi ou l'appartement convoité, ils doivent fournir des informations personnelles ou fournir un rapport de crédit. Il se sert alors des informations personnelles recueillies pour faire émettre des cartes de crédit au nom de ces individus. Un exemple de nouvelle médiatique mettant en scène un tel scénario a été publié dans un journal du Nevada (Tahoe Daily Tribune, 2009). Une offre d'emploi dans une société financière fut diffusée sur Craigslist. Les individus intéressés par l'emploi ont été invités, s'ils voulaient une entrevue, à obtenir une vérification de crédit en cliquant directement sur un lien dans le courriel qui leur était envoyé. Les victimes étaient en fait dirigées vers un faux questionnaire comportant des questions d'ordre personnel et financier. Une fois les informations envoyées et après un long silence des supposés employeurs, les chercheurs d'emploi réalisèrent alors qu'ils avaient été floués et que ni l'emploi promis ni l'entreprise recruteuse n'avaient d'existence légale.

La distribution des événements selon les sites du web 2.0 impliqués

Une façon de prolonger l'analyse est de distribuer les événements de fraude selon les sites du web 2.0 sur lesquels ils surviennent. La grande majorité des incidents rapportés par les médias se sont produits sur Craigslist (77,9%) alors qu'une minorité d'entre eux sont survenus sur Facebook (13%). Cette analyse a également permis de faire ressortir deux tendances. Il apparaît tout d'abord que la forte majorité des fraudes élaborées (93%) se commettent sur Craigslist, un site d'annonces classées. En fait, la seule catégorie de fraude élaborée se produisant à la fois dans des sites d'annonces classées et dans un site de réseautage social tel que Facebook est la fraude par abus de confiance. De leur côté, les vols d'identité s'effectueraient à la fois sur Craigslist (29,0%) et sur les sites de réseautage social, en particulier sur Facebook (41,9%). Quant au site de microblogage Twitter, il apparaît tout à fait marginal en dépit de sa popularité croissante.

Répartition des fraudes selon le site

| | Craigslist | Kijiji | MySpace | Facebook | Twitter | Autre | Total |
|--------------------------------|------------|--------|---------|----------|---------|-------|-------|
| Fraude élaborée | 93% | 2% | 0% | 4% | 0% | 1% | n=100 |
| Fraude par abus de confiance | 84,6% | 2,6% | 0% | 10,3% | 0% | 2,6% | n=39 |
| Fraude de location immobilière | 100% | 0% | 0% | 0% | 0% | 0% | n=32 |
| Fraude par usage de faux | 95,6% | 4,3% | 0% | 0% | 0% | 0% | n=23 |
| Offre de service sans permis | 100% | 0% | 0% | 0% | 0% | 0% | n=6 |
| Vol d'identité | 29,0% | 0% | 19,4% | 41,9% | 6,5% | 3,2% | n=31 |
| Total | 77,9% | 1,5% | 4,6% | 13% | 1,5% | 1,5% | n=131 |

La fraude élaborée se commet principalement dans des sites d'annonces classées parce qu'elle vise généralement le gain personnel et que les sites de réseautage social sont (pour l'instant) davantage utilisés pour communiquer avec des amis que pour réaliser des transactions commerciales. Par contre, les voleurs d'identité privilégient les sites de réseautage social où ils personnifient les amis de leurs victimes et exploitent les liens amicaux qui unissent ces deux individus afin de réaliser leurs gains. En ce qui concerne les vols d'identité commis sur les sites d'annonces classées, ils ne viseraient généralement pas un gain personnel mais plutôt le désir de diffamation d'autrui puisque ces sites sont fréquemment utilisés pour offrir des services de prostitution.

Le profil démographique des suspects et des victimes

On recense parmi les 131 affaires de fraude 60 suspects et 71 victimes. La faible proportion de suspects rapportée au nombre d'affaires identifiées dans les médias laisse sous-entendre que les auteurs de fraudes sur le web 2.0 sont rarement détectés et arrêtés.

Comme pour la majorité des crimes commis sur le web 2.0, les suspects de fraudes sont presque tous de sexe masculin (80%). Il faut toutefois noter que les vols d'identité ont une plus grande proportion de suspects de sexe féminin que les fraudes élaborées. En effet, alors que les femmes constituent seulement 17,1% des suspects de fraudes élaborées, elles constituent toutefois plus du quart (26,3%) des suspects de vols d'identité.

Distribution des suspects de fraudes par sexe

| Type de fraude | Féminin | Masculin | Total |
|--------------------------------|------------|------------|-------------|
| Fraudes élaborées | 17,1% | 82,9% | n=41 |
| Fraude par abus de confiance | 21,1% | 78,9% | n=19 |
| Fraude de location immobilière | 25% | 75% | n=8 |
| Fraude par usage de faux | 10% | 90% | n=10 |
| Offre de service sans permis | 0% | 100% | n=4 |
| Vol d'identité | 26,3% | 73,7% | n=19 |
| Total | 20% | 80% | n=60 |

Il est difficile de statuer sur les raisons qui expliquent cette plus grande proportion de femmes observée dans la catégorie des vols d'identité, mais on observe là une tendance déjà mise en lumière pour les vols d'identité commis de manière « traditionnelle » (Dupont et Louis 2009).

Distribution des victimes de fraude par sexe

| Type de fraude | Féminin | Masculin | Total |
|--------------------------------|--------------|--------------|-------------|
| Fraudes élaborées | 50% | 50% | n=50 |
| Fraude par abus de confiance | 53,3% | 46,7% | n=15 |
| Fraude de location immobilière | 56,3% | 43,7% | n=16 |
| Fraude par usage de faux | 42,1% | 57,9% | n=19 |
| Offre de service sans permis | 0% | 0% | n=0 |
| Vol d'identité | 52,4% | 47,6% | n=21 |
| Total | 50,7% | 49,3% | n=71 |

Les résultats montrent que les victimes de fraudes commises sur le web 2.0 sont réparties plutôt également selon le sexe. En effet, sur les 71 victimes dont le sexe est identifiable, 49,3% sont de sexe masculin. Il semble donc que le choix des victimes soit peu influencé par le sexe de celles-ci. Selon Pratt, Holtfreter et Reisig (2010), ceci s'expliquerait par le fait que les attributs démographiques ne peuvent pas toujours être observés en ligne et que la plupart des fraudeurs en ligne choisiront leurs victimes dans le cadre de leurs activités routinières sur Internet.

Répartition des suspects de fraude selon le site et le sexe

| Sites du Web 2.0 | Féminin | Masculin | Total |
|---|---------|----------|-------|
| Sites d'annonces classées (Craigslist et Kijiji) | 25% | 75% | n=48 |
| Sites de réseautage social (Facebook, MySpace et Twitter) | 0% | 100% | n=12 |

Les résultats de la répartition des suspects de fraudes selon le site et le sexe montrent que les fraudeurs de sexe féminin agissent tous sur les sites d'annonces classées et que seuls les hommes feraient de la fraude sur les sites de réseautage social. Ces résultats s'expliqueraient par le fait que les fraudes sur les sites de réseautage social impliquent dans certaines circonstances du piratage et que les femmes seraient moins portées à commettre un tel type de geste que les hommes (Adam, 2004).

Répartition des victimes de fraude selon le site et le sexe

| Sites du Web 2.0 | Féminin | Masculin | Total |
|---|---------|----------|-------|
| Sites d'annonces classées (Craigslist et Kijiji) | 52,7% | 47,3% | n=55 |
| Sites de réseautage social (Facebook, MySpace et Twitter) | 43,8% | 56,2% | n=16 |

Contrairement aux suspects de fraude, il semble que le type de site sur lequel survient la fraude n'affecte pas significativement la répartition des victimes selon le sexe. En effet, bien que les femmes soient davantage victimes que les hommes sur les sites d'annonces classées (52,7%) et que les hommes soient davantage victimes sur les sites de réseautage social (56,2%), la différence est plutôt faible et pourrait être attribuable au hasard. Il est également probable que ces deux faibles majorités soient attribuables au fait que les suspects de sexe féminin utilisent tous les sites d'annonces classées pour commettre leurs gestes et que ceux-ci soient moins susceptibles de frauder quelqu'un du sexe opposé par peur de représailles.

Concernant l'âge des suspects et des victimes, les résultats montrent que les fraudeurs sont un peu plus jeunes en moyenne (29,7 ans; n=30) que les victimes (33,3 ans; n=19). De plus, les fraudeurs élaborés (34,6 ans; n=17) seraient plus âgés que les voleurs d'identité (24 ans; n=12). Il est probable que les voleurs d'identité soient plus jeunes en raison du fait que du piratage soit requis dans certains cas et que les pirates informatiques seraient plus jeunes en moyenne que les fraudeurs généralistes.

Conclusion

L'objectif de cette note de recherche était de décrire la fraude en lien avec les plateformes du web 2.0 à l'aide de données tirées des médias. Il ressort principalement des résultats obtenus que les fraudes ne constituent qu'une faible minorité des affaires de déviances observées sur le web 2.0 qui sont rapportées par les médias, et que les fraudes élaborées sont plus communément médiatisées que les vols d'identité. La grande majorité des incidents rapportés par les médias se sont produits sur les sites d'annonces classées. Presque tous les cas survenus sur Facebook sont des vols d'identité, alors que la grande majorité des cas de fraude élaborée rapportés par les médias ont eu lieu sur Craigslist. Il semble que, comparativement aux fraudeurs élaborés, les voleurs d'identité soient plus jeunes et plus communément de sexe féminin. Les femmes privilégieraient les sites d'annonces classées plutôt que les sites de réseautage social. Les résultats montrent également que les victimes de fraudes commises sur le web 2.0 seraient réparties plutôt également selon le sexe.

La nouvelle génération d'applications Internet ne semble pas être à l'origine d'une véritable révolution de la fraude en ligne. Elle constitue plutôt un support pour celle-ci permettant l'emploi d'anciennes méthodes dans un contexte renouvelé. Dans cet environnement en constante évolution, les fraudeurs apprennent à personnaliser leurs attaques, à utiliser la confiance des utilisateurs envers les autres utilisateurs comme levier pour les amener à commettre des erreurs de jugement et à exploiter la prolifération des données personnelles pour commettre des vols d'identité qui ne sont pas exclusivement motivés par l'appât du gain.

Puisque l'ingénierie sociale semble privilégiée par les fraudeurs du web 2.0 qui n'ont pas recours à des compétences technologiques très avancées, la clé pour prévenir la fraude en ligne semble être l'éducation et la sensibilisation des usagers. Une des principales leçons à tirer de la présente note, que tout acheteur ou vendeur de biens et services sur le web 2.0 devrait retenir, est que les offres trop belles pour être vraies cachent souvent des intentions malveillantes. Tant et aussi longtemps que cette leçon élémentaire n'aura pas été assimilée par les utilisateurs des médias sociaux, les fraudeurs continueront à trouver dans cette technologie un terrain favorable qui les expose à des risques de détection très faibles. Par ailleurs, on recommande également aux personnes qui réalisent des transactions à l'aide du web 2.0 ou qui reçoivent des invitations pressantes à aider financièrement leurs « amis » à utiliser des canaux d'information complémentaires (courrier électronique, téléphone, fax, visite en personne...) afin de valider autant que possible les informations sur lesquelles ils basent leurs décisions.

Références

Adam, A. E. (2004): "Hacking into Hacking: Gender and the Hacker Phenomenon," *ACM SIGCAS Computers and Society*, 32(7).

Burke, A. (2009). « Sting nets unlicensed movers », *Mail Tribune*, 20 février, <http://www.mailtribune.com/apps/pbcs.dll/article?AID=/20090220/NEWS/902200330>. (page consultée le 18 avril 2011).

CBS. (2009). « Sex offender arrested for giving "messages" at home », *CBS*, 7 mai, <http://www.cbs12.com/news/glasure-4717619-massages-offender.html>, (page consultée le 18 avril 2011).

Dupont, B., Lavoie, P-E. et Fortin, F. (2010), « Les crimes sur le web 2.0 : Une recherche exploratoire », <http://www.benoitdupont.net/sites/default/files/Dupont%20Lavoie%20Fortin%20crimes%20web%202%200.pdf>, page consultée le 9 mars 2011.

Dupont, B. et Louis, G. (2009), « Les voleurs d'identité : Profil d'une délinquance ordinaire », <http://www.benoitdupont.net/sites/www.benoitdupont.net/files/DupontLouisprofilvid.pdf>, page consultée le 6 juin 2011.

Herald-Tribune (2009). « Manatee couple lose money via Craigslist », *Herald-Tribune*, 24 avril, <http://www.heraldtribune.com/article/20090424/ARTICLE/904249995/-1/NEWSITEMAP> (page consultée le 18 avril 2011).

Leydon, J. «Miley Cyrus hacker in MySpace spam ringtone scam ». *The Register* [En ligne]. (26 février 2009). http://www.theregister.co.uk/2009/02/26/myspace_spam_ringtone_scam/ (page consultée le 29 juillet 2009).

Lockport Union-Sun & Journal. (2009). « CRIME : Two residents report fraud involving Craigslist », *Lockport Union-Sun & Journal Online*, 13 mars, <http://lockportjournal.com/crime/x212290665/CRIME-Two-residents-report-fraud-involving-Craigslist>

Moylan, B. (2010). A Public Service Announcement for Anyone Looking to Be Cast on Jersey Shore, *Gawker*, 11 février, <http://gawker.com/#!5469742/a-public-service-announcement-for-anyone-looking-to-be-cast-on-jersey-shore> (page consultée le 18 avril 2011)

Pratt T.C., Holtfreter K., Reisig M.D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory, *Journal of Research in Crime and Delinquency*, 47 (3), pp. 267-296.

Rodrigue, G. «Faux profil sur Facebook: un Italien compte poursuivre ». *Techno Branchez-vous* [En ligne]. (7 février 2009). http://techno.branchez-vous.com/actualite/2009/02/faux_profil_sur_facebook_un_it_1.html (page consultée le 29 juillet 2009).

Rusin (2010). « Police: Huntley man sold bogus Cubs tickets on Craigslist », *Chicago Breaking News Center*, 1^{er} février, <http://archive.chicagobreakingnews.com/2010/02/police-huntley-man-sold-bogus-cubs-tickets-on-craigslist.html>, (page consultée le 18 avril 2011).

Sutter, J. et Carroll, J. (2009). « Fears of impostors increase on Facebook », *CNN.com*, 6 février, <http://www.cnn.com/2009/TECH/02/05/facebook.impostors/>, consulté le 7 avril 2011.

Tahoe Daily Tribune (2009). « Job seekers victimized through Craigslist.org », *Tahoe Daily Tribune*, 23 juin, <http://www.tahodailytribune.com/article/20090623/NEWS/906239998/1056/rss04>, (page consultée le 18 avril 2011).

The Smoking Gun. «Felony Charge For Craigslist Prank ». *TheSmokingGun.com* [En ligne]. (5 mars 2009). <http://www.thesmokinggun.com/archive/years/2009/0305094eau1.html> (page consultée le 29 juillet 2009).

WMCTV. «Miss. man accused of threat against Bush remains in jail ». *WMCTV.com* [En ligne]. (7 décembre 2008). <http://www.wmctv.com/global/story.asp?s=9472774> (page consultée le 29 juillet 2009).

Zetter, Kim. «Britney, Obama Twitter Feeds Hijacked Following Phishing Attack ». *Wired, Threat Level* [En ligne]. (5 janvier 2009). <http://www.wired.com/threatlevel/2009/01/twits-get-phish/> (page consultée le 29 juillet 2009).