Rapport sur l’hameçonnage

Rapport au ministre de la Sécurité publique et de la Protection civile du Canada et au secrétaire américain à la Justice

Groupe de travail binational sur les fraudes transfrontalières par marketing de masse
Octobre 2006

Rapport sur l’hameçonnage

Rapport au ministre de la Sécurité et de la Protection civile du Canada et au secrétaire américain à la Justice

Contenu

Résumé 3
Introduction 5
Ce qu’est l’hameçonnage 5
Étendue de l’hameçonnage 6
Comment procèdent les spécialistes de l’hameçonnage 8
Variantes en matière d’hameçonnage 10
Conséquences de l’hameçonnage 13
Liste de contrôle à des fins de prévention et de signalement des procédés d’hameçonnage 14
Répliques à l’hameçonnage : pratiques actuelles et prometteuses 18
- Éducation du public 18
- Confirmation de l’authenticité 19
- Cadre législatif 19
- Application de la loi 20
- Coordination binationale et nationale 21

Conclusion 22

Annexe 1 : Bibliographie 23

Résumé

L'hameçonnage désigne les techniques de tromperie qu'utilisent les voleurs d'identité pour aller à la pêche de renseignements personnels dans un étang d'utilisateurs Internet sans méfiance. Il s'agit d'un terme général pour désigner la création et l'utilisation par des criminels de courriels et de sites Web conçus de manière à ressembler à ceux d'entreprises, d'institutions financières et d'organismes gouvernementaux bien connus, légitimes et auxquels les gens font confiance. Ces criminels amènent les utilisateurs d'Internet à fournir leurs renseignements bancaires et financiers, ainsi que d'autres données personnelles telles que des noms d'utilisateur et des mots de passe.

L'hameçonnage continue d'être une des principales catégories d'escroqueries de vol d'identité sur Internet et il cause des pertes à court terme et fait du tort à l'économie à long terme. En mai 2006, plus de 20 000 plaintes d'hameçonnage ont été déposées par des particuliers, ce qui représente un accroissement de plus de 34 % par rapport à l'année antérieure. Les données récentes laissent voir que les criminels réussissent à convaincre jusqu'à 5 % des destinataires de répondre à leurs courriels, de sorte qu'un nombre important de consommateurs ont été victimes de fraudes par cartes de crédit, de fraudes liées à l'identité et de pertes financières. Les pertes découlant d'attaques d'hameçonnage s'évaluent maintenant en milliards de dollars dans le monde.

Selon le type de fraude qu'un criminel commet à l'aide des données d'identification volées, les particuliers et les entreprises peuvent perdre des sommes pouvant aller de quelques centaines de dollars, à des dizaines de milliers de dollars et, les grandes banques, peuvent perdre souvent plus encore.

L'hameçonnage pose également un danger particulier, en ce que les techniques utilisées changent constamment. L'« hameçonnage vocal » est la technique selon laquelle les voleurs d'identité envoient un courriel conçu de la même façon qu'un courriel d'hameçonnage; cependant, au lieu d'un lien frauduleux sur lequel cliquer, le courriel fournit un numéro de service aux clients où la victime, si elle appelle, est invitée à « entrer dans le système » en utilisant son numéro de compte et son mot de passe. Les consommateurs peuvent aussi être appelés directement et informés qu'ils doivent immédiatement appeler à un certain numéro de service aux clients frauduleux, pour protéger leur compte.

Le « harponnage » est une technique où des courriels qui semblent authentiques sont envoyés à tous les employés ou tous les membres d'une société, d'un organisme gouvernemental, d'une organisation ou d'un groupe donné. À l'instar du courriel d'hameçonnage ordinaire, le message peut avoir l'air d'avoir été envoyé par un employeur ou un collègue s'adressant à tous dans la société, pour tenter d'obtenir des données de connexion. Les escroqueries de harponnage visent à avoir accès à l'ensemble du système informatique d'une société.

L'hameçonnage, comme le vol d'identité, ne connaît pas de limites frontalières. Le Canada et les États-Unis ont entrepris toute une gamme d'initiatives et de réformes législatives pour lutter contre l'hameçonnage. Bon nombre de ces initiatives sont multisectorielles, intergouvernementales et pluri-organismes et ont une portée allant au-delà des entités d'application de la loi.

Pour mieux comprendre la portée et l’ampleur de l’hameçonnage, ainsi que le concept plus vaste du vol d’identité, les gouvernements et les responsables de l’application de la loi ont établi, avec le concours du secteur privé, des mécanismes de signalement à la disposition du public.

Introduction

En octobre 2004, le Forum canado-américain sur la criminalité transfrontalière a publié un rapport rédigé conjointement par le département américain de la Justice et par Sécurité publique et Protection civile Canada (SPPCC) sur le vol d'identité. On y soulignait, entre autres méthodes de vol d'identité, l'utilisation croissante d'une technique appelée « hameçonnage » :

> Les consommateurs reçoivent des courriels « mystificateurs » (qui semblent provenir d'une entreprise légitime, par exemple une institution financière ou un site de vente aux enchères en ligne). En général, ces courriels redirigent les consommateurs vers un site « mystificateur » qui semble être celui de l'entreprise ou de l'entité en question. De nombreux consommateurs sont aussi la cible de scénarios selon lesquels une personne, se faisant passer pour le représentant d'une institution ou d'une entreprise légitime, lui demande des renseignements de nature personnelle. En fait, les criminels qui envoient les courriels, proposent des sites Web ou font ces appels téléphoniques n'ont aucun lien avec les entreprises qu'ils disent représenter. Leur seul objectif est d'obtenir les données personnelles du consommateur afin de les utiliser à toutes sortes de fins criminelles.[i]

Le Forum canado-américain sur la criminalité transfrontalière a jugé qu'il convenait de faire suivre le rapport sur le vol d'identité d'un rapport conjoint sur l'hameçonnage et ses incidences sur la criminalité transfrontalière. Le Forum a chargé le Groupe de travail canado-américain sur les fraudes transfrontalières par marketing de masse, qui fait rapport à chaque année au Forum, de préparer ce rapport. Produit conjointement par le département américain de la Justice et par Sécurité publique et Protection civile Canada (SPPCC), le rapport découle de documents produits par un grand nombre d'organismes et de particuliers des États-Unis et du Canada membres du Groupe de travail.

Le présent rapport vise à définir la nature, la portée et les conséquences de l'hameçonnage, à offrir au public de l'information sur la façon de réagir à des fraudes d'hameçonnage et à cerner les approches existantes, et d'autres approches prometteuses, permettant de lutter contre l'hameçonnage. Il inclut de l'information sur les tendances observées à cet égard, des statistiques et une analyse sommaire de sa principale utilisation qui explique pourquoi le phénomène de l'hameçonnage ne cesse de prendre de l'ampleur.

Ce qu'est l'hameçonnage

Le terme *hameçonnage* est un terme général pour désigner la création et l'utilisation par des criminels de courriels et de sites Web – conçus pour donner l'impression qu'ils appartiennent à des entreprises, des institutions financières et des organismes gouvernementaux bien connus, légitimes et auxquels les gens font confiance – dans le but de recueillir de l'information personnelle, financière et de nature délicate. Les criminels amènent les utilisateurs d'Internet à dévoiler leur information bancaire et financière ainsi que d'autres données personnelles telles que des noms d'utilisateurs et

des mots de passe, ou à télécharger involontairement un programme informatique malveillant qui peut permettre aux criminels d'avoir accès à ces ordinateurs ou aux comptes bancaires des utilisateurs[ii].

Bien que les termes hameçonnage, vol d'identité et fraude liée à l'identité soient souvent utilisés de façon interchangeable, certaines distinctions s'imposent. L'hameçonnage s'entend d'une méthode parmi d'autres permettant aux voleurs d'identité de « voler » de l'information par la tromperie – c'est-à-dire, en amenant des consommateurs non conscients du stratagème à donner involontairement des renseignements d'identification ou financiers, sous de faux prétextes ou en les amenant à donner aux criminels un accès non autorisé à leurs ordinateurs et leurs données personnelles. Les États-Unis et quelques autres pays utilisent le terme « vol d'identité »; le Royaume-Uni utilise souvent le terme « fraude liée à l'identité » pour désigner une pratique largement répandue qui consiste à obtenir et à utiliser à des fins frauduleuses des données d'identification d'autres personnes. La fraude liée à l'identité peut aussi désigner l'utilisation criminelle subséquente de données d'identification d'autres personnes pour obtenir des biens ou des services, ou l'utilisation de données d'identification fictives (non nécessairement associées à une personne réellement en vie) pour commettre un crime.

Le criminel se livre à l'hameçonnage pour obtenir de l'information de nature délicate et précieuse sur un consommateur, habituellement dans le but d'avoir accès de façon frauduleuse au compte bancaire ou à d'autres comptes financiers du consommateur. Il arrive souvent que les spécialistes de l'hameçonnage vendent des numéros de cartes de crédit ou de comptes à d'autres criminels, obtenant ainsi un bénéfice très important, moyennant un investissement technologique relativement modeste.

Étendue de l'hameçonnage

Il n'existe pas de statistiques complètes sur le nombre de personnes dont les renseignements personnels sont obtenus au moyen de procédés d'hameçonnage, ni sur les pertes totales en dollars attribuables à des fraudes liées à l'hameçonnage. Il apparaît cependant clairement que l'hameçonnage a crû substantiellement au cours des deux dernières années et qu'il est devenu sujet de préoccupation partout en Amérique du Nord, de même que dans d'autres régions du monde.

Une importante coalition multinationale d'entreprises qui se concentre sur l'hameçonnage, l'*Anti-Phishing Working Group* (APWG), publie régulièrement des rapports sur le volume et les types courants d'attaques d'hameçonnage. De récentes statistiques de l'APWG, soit pour août 2006, montrent la croissance et la diversité des attaques d'hameçonnage au cours de la dernière année et des années précédentes[iii]. Au cours du mois d'août 2006, à titre d'exemple :

- L'APWG a reçu 26 150 signalements différents d'hameçonnage (comparativement à 13 776 en août 2005 et à 6 957 en octobre 2004). Ce total se situe au deuxième rang du nombre total de signalements d'hameçonnage répertoriés par l'APWG au cours d'un seul mois.
- L'APWG a découvert 10 091 sites Web différents d'hameçonnage à travers le monde (comparativement à 5 259 en août 2005 et à 1 142 seulement, en octobre 2004[iv]).

- 148 marques d'entreprises différentes ont été « détournées » (utilisées à de mauvaises fins) au moyen de procédés d'hameçonnage (comparativement à 84 en août 2005[v]).
- Le secteur financier a été le secteur le plus fortement visé par les procédés d'hameçonnage, c.-à-d. par 92,6 % de l'ensemble des attaques d'hameçonnage (comparativement à 84,5 % en août 2005)[vi]. (À titre d'exemple, les principales institutions financières au Canada et aux États-Unis, de même que de plus petites institutions financières américaines telles que les sociétés de crédit mutuel, ont souvent été ciblées.)
- L'APWG a découvert 2 303 sites Web différents contenant des programmes d'« espionnage de clavier » -- c.-à-d. des programmes qui enregistrent les touches utilisées à un ordinateur donné, ce qui permet aux criminels d'obtenir les noms d'utilisateurs, les mots de passe et d'autres données précieuses appartenant à des tiers (comparativement à 958 sites Web semblables en août 2005 et à 260 sites Web équivalents en avril 2004[vii]). En comparaison, le nombre d'applications informatiques différentes qui incluent un programme malveillant tel qu'un logiciel d'espionnage de clavier est demeuré relativement constant (172 en août 2006, comparativement à 168 en août 2005).
- Les États-Unis sont le pays où l'on retrouve le pourcentage le plus élevé de sites d'hameçonnage dans le monde (27,7 %, comparativement à 27,9 % en août 2005), alors que le Canada occupe le neuvième rang (2,2 %, comparativement à 2,21 % en août 2005). La Chine demeure au deuxième rang des pays où l'on trouve ces sites Web (14 %, comparativement à 12,15 % en août 2005) et la Corée du Sud occupe le troisième rang (9,59 %, comparativement à 9,6 % en août 2005[viii]).

Dans le même ordre d'idées, le *Symantec Internet Security Threat Report*[1] pour septembre 2006 a signalé que, du 1er janvier au 30 juin 2006, on avait découvert 157 477 messages d'hameçonnage différents. Ce total représente une augmentation de 81 % par rapport aux 86 906 messages d'hameçonnage différents découverts dans les six mois précédents (30 juillet-31 décembre 2005) et une augmentation de 612 % par rapport aux 97 592 messages d'hameçonnage différents découverts dans les six premiers mois de 2005[ix]. Finalement, une étude d'AOL Canada aurait permis de découvrir que près du tiers des Canadiens interrogés avaient reçu un courriel d'une entreprise qui tentait de faire confirmer l'information sur leur compte[x].

De façon générale, les procédés d'hameçonnage ont consisté essentiellement à envoyer au hasard un très grand nombre de « courriels de pollupostage » sans tenir compte des caractéristiques démographiques des utilisateurs. Il n'en reste pas moins que certains procédés d'hameçonnage touchent probablement davantage certains segments de la population[xi]. En outre, certains procédés d'hameçonnage connus sous l'appellation « harponnage » tentent de viser de façon plus précise des groupes définis d'utilisateurs en ligne[xii]. (Voir la page suivante.)

[1] Symantec est une société internationale qui fournit des logiciels, des appareils et des services destinés à aider les consommateurs à assurer la sécurité, la disponibilité et l'intégrité de leurs ressources et leurs structures d'information. Le *Symantec Internet Security Threat Report* offre une analyse des activités représentant une menace sur une période de six mois. Il couvre les attaques sur Internet, les points de vulnérabilité, les programmes malveillants, l'hameçonnage, les pourriels, les risques pour la sécurité, et les prochaines menaces à prévoir.

À court terme, ces arnaques ont pour effet d'escroquer des particuliers et des institutions financières. Selon des données antérieures, dans certains procédés d'hameçonnage, les criminels ont été en mesure de convaincre jusqu'à 5 % des destinataires de répondre à leurs courriels, faisant un nombre important de victimes de fraudes par carte de crédit, de fraudes liées à l'identité, et de consommateurs ayant subi des pertes financières[xiii]. À long terme, l'hameçonnage peut miner la confiance du public en Internet pour les opérations bancaires en ligne et le commerce électronique.

Bien que les données sur l'hameçonnage puissent offrir d'importantes indications sur l'étendue du phénomène, plusieurs obstacles empêchent une mesure complète et exacte du problème. Tout d'abord, les victimes n'ont souvent aucune idée de la façon dont les criminels ont obtenu leurs données. Habituellement, les victimes fournissent leurs renseignements personnels aux spécialistes de l'hameçonnage précisément parce qu'ils croient avoir affaire à des personnes dignes de confiance. Des frais inexpliqués et inattendus apparaissent sur leurs relevés de carte de crédit souvent fort longtemps après la perpétration du méfait et ils ont trait à des articles qui n'ont aucun rapport avec l'objet des courriels et des sites Web utilisés pour l'hameçonnage, de sorte que les victimes n'ont aucune raison de faire le lien entre ces événements.

En deuxième lieu, les entreprises qui sont victimes de l'hameçonnage ne signalent pas toujours ces cas aux responsables de l'application de la loi. À la différence des autres types de crimes pouvant être commis sur Internet de façon clandestine, le piratage par exemple, l'hameçonnage, par nature, consiste en l'utilisation publique abusive des noms et des logos légitimes des entreprises et des organismes. Certaines sociétés peuvent hésiter à signaler ces cas aux représentants de la loi – en partie parce qu'elles craignent que, si le véritable volume de ces attaques d'hameçonnage était connu du public, il aurait pour effet de miner la confiance des consommateurs ou des titulaires de comptes à leur égard ou de les placer en position désavantageuse par rapport à leurs concurrents.

Comme le montrent les statistiques, l'hameçonnage est une forme de vol d'identité en ligne qui continue de croître rapidement et peut causer des pertes à court terme et faire du tort à l'économie à long terme. Dans un cas comme dans l'autre, les escroqueries d'hameçonnage et les autres crimes de vol d'identité entraînent des coûts importants qui devront peut-être par la suite être épongés par les consommateurs sous forme d'augmentations de frais des sociétés émettrices de cartes de crédit ou de prix chez les marchands acceptant le paiement par carte de crédit.

Comment procèdent les spécialistes de l'hameçonnage

Dans une fraude par hameçonnage typique, les criminels qui veulent obtenir les données personnelles des Internautes créent d'abord une réplique non autorisée (« usurpation de marque ») d'un site Web ou d'un courriel réel, habituellement, d'une institution financière ou une autre société qui traite de l'information financière, par exemple un commerçant en ligne. Le courriel est créé de façon à reproduire le style des courriels de l'entreprise ou de l'organisme légitime, en utilisant ses logos et ses slogans. La nature et la forme du principal langage de création des sites Web, le langage hypertexte, facilite énormément la copie d'images ou même de sites Web au complet. Bien que cette facilité de création des sites Web soit une des raisons pour lesquelles

Internet est devenu si populaire pour communiquer, elle permet aussi l'utilisation abusive des marques de commerce, des dénominations commerciales et des autres identificateurs d'entreprises sur lesquels les consommateurs comptent pour s'assurer d'être sur un site authentique.

Les spécialistes de l'hameçonnage, généralement, envoient des courriels d'« usurpation de marque » à autant de personnes que possible, pour arriver à en tromper un certain nombre. (Dans des attaques de « harponnage » [voir ci-dessous, la section sur le harponnage], des spécialistes de l'hameçonnage ont utilisé d'autres moyens illégaux pour obtenir de l'information sur des particuliers ou sur un groupe de personnes, puis ont ciblé un groupe précis, au moyen de courriels qui incluaient de l'information obtenue illégalement de façon à rendre ces courriels plus vraisemblables.) Ces courriels aiguillent les consommateurs vers un site Web d'usurpation de marque, qui semble appartenir à la même entreprise ou entité. Les criminels savent que, même si tous les destinataires n'ont pas nécessairement un compte auprès de l'entreprise ciblée, ou des liens avec elle, certains en auront, et ces derniers croiront plus volontiers que le courriel et les sites Web sont légitimes. Le concept sous-jacent à bon nombre d'attaques d'hameçonnage est similaire à celui des appels téléphoniques « à prétexte » (c.-à-d., des appels téléphoniques de personnes qui disent appartenir à des établissements ou des entreprises légitimes et qui demandent des renseignements personnels à leurs interlocuteurs). En réalité, les criminels derrière ces courriels, ces sites Web et ces appels téléphoniques n'ont aucun lien avec ces entreprises. Leur seul but est d'obtenir les données personnelles des consommateurs pour effectuer diverses manœuvres frauduleuses[2].

Généralement, les procédés d'hameçonnage reposent sur trois éléments. D'abord, les sollicitations par hameçonnage utilisent souvent des marques de commerce et des dénominations commerciales familières, de même que des noms et des logos d'organismes gouvernementaux reconnus. L'utilisation de telles marques de commerce fonctionne dans bon nombre de cas, parce que, étant donné que les marques sont bien connues des utilisateurs d'Internet, ces derniers risquent davantage de leur faire confiance sans les examiner très attentivement. En outre, les indicateurs qui sont fournis aux navigateurs du Web pour leur permettre d'évaluer la validité et la sécurité d'un site Web (p. ex., l'icône représentant un cadenas ou la barre d'adresse) peuvent tous faire l'objet d'une usurpation. Ce problème est aggravé par l'absence de protocoles normalisés entre les institutions financières sur la façon de communiquer avec leurs clients et sur l'information qu'elles exigeront sur Internet.

En deuxième lieu, les sollicitations contiennent systématiquement des avertissements destinés à amener les destinataires à se faire du souci au sujet de l'accès à un compte financier existant. Les escroqueries par hameçonnage inspirent généralement un sentiment d'urgence en avertissant les victimes qu'à défaut de se conformer aux instructions, leurs comptes seront fermés, des pénalités ou des frais seront imposés, ou qu'elles s'exposent à d'autres conséquences négatives. La crainte que suscitent de tels avertissements contribue à réduire la capacité qu'ont les consommateurs de juger si les messages sont authentiques. Même si un faible pourcentage seulement des personnes qui reçoivent ces avertissements frauduleux y répondent, la facilité avec laquelle de

[2] L'utilisation de prétextes n'a pas uniquement pour but de pousser plus loin l'hameçonnage ou d'autres formes de vol et de fraude liées à l'identité en ligne. Des rapports récents indiquent que l'utilisation de prétextes peut aussi servir à d'autres fins moralement contestables ou illégales.

telles sollicitations peuvent être distribuées à des millions de personnes permet malgré tout de faire un nombre assez important de victimes. (Il convient aussi de préciser que certains procédés malhonnêtes offrent plutôt des encouragements positifs, par exemple la promesse d'un paiement en retour de la participation à un sondage en ligne.)

Troisièmement, les sollicitations reposent sur deux faits liés à la confirmation de l'authenticité des courriels : 1) les consommateurs en ligne n'ont souvent pas les outils ni les connaissances techniques pour confirmer l'authenticité des messages des institutions financières et des entreprises de commerce électronique; et 2) les outils et les techniques disponibles ne permettent pas une confirmation fiable, ou ils peuvent faire l'objet d'une usurpation. Les criminels peuvent donc utiliser des techniques, par exemple la contrefaçon des en-têtes et des lignes de sujet des courriels, pour donner l'impression que les courriels viennent de sources dignes de confiance, sachant que bon nombre des destinataires n'auront aucune façon efficace d'en vérifier la provenance réelle.

Exemple – ***Les clients de la Banque Royale mordent à « l'hameçon »***

En juin 2004, la Banque Royale du Canada a avisé ses clients de l'existence de messages électroniques frauduleux dans lesquels une personne se faisant passer pour un représentant de la Banque Royale leur demandait de vérifier leurs numéros de compte et numéros d'identification personnelle (NIP) en utilisant un lien inclus dans le message électronique. Le message frauduleux indiquait que, si le destinataire ne cliquait pas sur le lien pour inscrire son numéro de carte et son code d'accès, il ne pourrait plus accéder à son compte. Les messages ont été envoyés une semaine après un problème électronique qui avait empêché la mise à jour des comptes des consommateurs. Le problème avait empêché le virement des salaires, et plusieurs consommateurs craignaient de ne pouvoir payer leur hypothèque, leur loyer ou d'autres dépenses. La Banque Royale croit que quelqu'un a tenté de profiter de la situation.

Variantes en matière d'hameçonnage

Dans la première génération des procédés d'hameçonnage, la plupart des attaques d'hameçonnage reposaient sur le jumelage de courriels frauduleux avec des liens menant à des sites Web frauduleux, pour obtenir l'information des utilisateurs d'Internet. Depuis deux ans, les criminels n'ont cessé de perfectionner leurs attaques d'hameçonnage en intégrant diverses autres techniques pour communiquer avec les victimes potentielles ou pour obtenir leurs renseignements.

« Harponnage »

Le « harponnage » est un terme familier pouvant servir à décrire toute attaque d'hameçonnage hautement ciblée. Les spécialistes du harponnage envoient de faux courriels qui semblent authentiques, à un groupe spécifiquement identifié d'utilisateurs Internet, tels que des utilisateurs d'un produit ou d'un service donné, les titulaires de comptes en ligne, les employés ou les membres d'une entreprise, d'un organisme gouvernemental, d'une association, d'un groupe ou d'un réseau social sur le Web. Tout comme dans le cas d'un courriel d'hameçonnage ordinaire, le message semble venir d'une source digne de confiance, par exemple un employeur ou un collègue susceptible

d'envoyer un message électronique à tous ou à un groupe sélectionné dans l'entreprise (p. ex., le chef des ressources humaines ou l'administrateur des systèmes informatiques). Comme la demande de données très utiles comme les noms d'utilisateurs ou les mots de passe vient d'une source connue ou digne de confiance, elle a plus de chances de sembler vraisemblable.

Tandis que les escroqueries d'hameçonnage ordinaires visent à voler de l'information auprès des particuliers, certaines escroqueries de harponnage peuvent faire intervenir aussi d'autres techniques, allant du piratage informatique, au recours à des « prétextes » (c.-à-d., l'obtention de renseignements personnels sous de fausses représentations), pour obtenir d'autres renseignements personnels servant à cibler un groupe donné ou à augmenter la vraisemblance des courriels destinés à l'hameçonnage. Essentiellement, certains criminels utilisent toute l'information qu'ils peuvent pour personnaliser le plus possible les fraudes d'hameçonnage en fonction d'un groupe précis[xiv].

Exemple – *Expédition d'hameçonnage au cœur du piratage informatique visant AT&T*

Dans une fraude récente, le système de vente d'AT&T, une importante entreprise de télécommunications, a été victime de pirates, ce qui a entraîné le vol d'informations liées aux commandes, notamment les noms et les adresses à domicile, les numéros de commandes et les numéros de cartes de crédit des clients. Les pirates informatiques ont ensuite envoyé à chaque consommateur un courriel hautement personnalisé indiquant qu'un problème était survenu au cours du traitement de leurs commandes et les dirigeant vers un autre site Web, d'usurpation, où ils ont été invités à entrer d'autres renseignements, dont leur date de naissance et leur numéro de sécurité sociale[xv].

Réacheminement et autres procédés malhonnêtes reposant sur des programmes malveillants

Une autre technique qu'utilisent les spécialistes de l'hameçonnage consiste à faire en sorte que des utilisateurs d'Internet ciblés téléchargent à leur insu certaines formes de programmes informatiques malveillants sur leur ordinateur au bureau ou à la maison. Un type de manœuvre d'hameçonnage qui utilise un programme malveillant est le « réacheminement ». De façon habituelle, lorsqu'un utilisateur d'Internet tape l'adresse d'un site Web en particulier (p. ex. *http://mavraiebanque.com*) sur le site d'un explorateur Internet, il est dirigé vers le bon site Web. Dans une manœuvre frauduleuse de réacheminement, le programme malveillant introduit par les spécialistes de l'hameçonnage change le code à l'intérieur de l'ordinateur de l'utilisateur de façon à ce que, lorsque l'utilisateur tente d'accéder à un site donné en tapant la bonne adresse, il est acheminé son insu à un site Web d'hameçonnage qui ressemble à s'y méprendre au site auquel il voulait accéder.

Un autre type de manœuvre d'hameçonnage liée à un programme malveillant concerne l'utilisation d'un logiciel d'espionnage de clavier ou « cheval de Troie » (c.-à-d., un programme qui permet aux criminels d'avoir accès à l'ordinateur de l'utilisateur à son insu). Lorsque le spécialiste de l'hameçonnage a réussi à faire en sorte qu'un utilisateur

d'Internet télécharge à son insu un programme malveillant qui inclut le logiciel d'espionnage de clavier, l'espion de clavier est généralement réglé pour ne fonctionner que lorsque l'utilisateur se sert du navigateur sur Internet pour avoir accès à un compte financier en ligne. En enregistrant les données sur les touches permettant d'entrer dans le système, puis en extrayant ces données, le spécialiste de l'hameçonnage peut par la suite utiliser cette information pour reproduire le nom de l'utilisateur et son mot de passe et avoir accès au compte de la victime pour y effectuer d'importants retraits. Le spécialiste de l'hameçonnage peut même utiliser un « cheval de Troie » pour effectuer une transaction directement à partir de l'ordinateur de l'utilisateur. Cette dernière technique est destinée à tromper le personnel de la sécurité de l'institution financière où la victime a un compte. L'utilisateur qui signale l'accès illégal à son compte a moins de chances d'être cru au tout début, si le personnel de la sécurité de l'institution financière retrouve la transaction non autorisée sur son ordinateur.

« Hameçonnage vocal »

Une technique d'hameçonnage qui a fait passablement parler d'elle récemment est l'« hameçonnage vocal », c.-à-d., au moyen de la voix. L'hameçonnage vocal peut se faire de deux façons. Dans une première version de la fraude, le consommateur reçoit un courriel conçu de la même façon que le sont les courriels d'hameçonnage, qui signale habituellement l'existence d'un problème relativement au compte. Plutôt que de fournir un lien frauduleux, le courriel fournit un numéro de service à la clientèle que le client doit composer et où il est invité à « entrer dans le système » au moyen du numéro de ses comptes et de ses mots de passe. L'autre version de la fraude consiste à appeler directement les consommateurs et à leur dire qu'ils doivent appeler immédiatement à un numéro de service à la clientèle frauduleux, afin de protéger leur compte. Les criminels peuvent aussi donner un sentiment de sécurité au consommateur en « confirmant » de l'information personnelle qu'ils possèdent déjà, telle que son nom complet, son adresse ou son numéro de carte de crédit[xvi].

L'hameçonnage vocal pose un problème particulier pour deux raisons. Tout d'abord, les criminels peuvent profiter des services d'appel sur Internet anonyme et bon marché qu'offre la téléphonie sur protocole Internet (voix sur IP), et il leur suffit d'utiliser un simple logiciel pour monter un service à la clientèle automatisé en ligne ayant toutes les apparences d'un service professionnel semblable à ceux qu'utilisent la plupart des grandes entreprises. Deuxièmement, contrairement à bon nombre d'attaques d'hameçonnage où les organismes légitimes ne se serviraient pas d'un courriel pour demander de l'information personnelle aux titulaires de comptes, l'hameçonnage vocal imite en fait un protocole bancaire typique suivant lequel les banques encouragent plutôt les clients à appeler et à confirmer l'authenticité de l'information[xvii].

Même si à l'occasion les banques appellent directement les clients et leur posent des questions pour vérifier leur identité, les consommateurs doivent se souvenir qu'une banque ne demandera jamais de NIP ou de mots de passe. Il est également important que les consommateurs ne fassent jamais confiance à un numéro de téléphone fourni dans un courriel, et qu'ils communiquent plutôt avec l'établissement au moyen d'un numéro qu'ils auront vérifié auprès d'une source indépendante ou qu'ils auront obtenu au moyen de l'assistance annuaire. Tel que susmentionné, il peut s'agir du numéro de téléphone ou du site Web fourni à l'endos de leurs cartes de crédit ou sur leurs relevés de compte mensuels.

Les consommateurs, les responsables de l'application de la loi et les entreprises doivent être conscients que plus le public devient plus averti relativement à l'hameçonnage, plus les criminels, eux, continuent d'utiliser des variantes, d'en mettre de nouvelles au point et de perfectionner leurs techniques.

Conséquences de l'hameçonnage

L'hameçonnage a quatre types distincts de conséquences, tant chez nous qu'à l'étranger, qui préoccupent les secteurs commerciaux et financiers, ainsi que les responsables de l'application de la loi dans les deux pays :

- *Perte financière directe*. Selon les types de fraude qu'un criminel commet au moyen des données d'identification volées, les consommateurs et les entreprises peuvent perdre des sommes allant de quelques centaines de dollars, à des dizaines de milliers de dollars. En fait, les petits commerces électroniques peuvent être particulièrement touchés par la fraude liée à l'identité. Par exemple, en raison des politiques pratiquées par les émetteurs de cartes de crédit, un commerçant en direct ayant accepté un numéro de carte de crédit qui se révèle avoir été acquis à la suite d'un vol d'identité risque de devoir assumer le plein montant des transactions frauduleuses faites au moyen de ce numéro.

- *Érosion de la confiance du public en Internet*. L'hameçonnage mine également la confiance qu'accorde le public à Internet. En amenant les consommateurs à douter de l'intégrité des sites Web commerciaux et financiers et même des systèmes d'adressage Internet, l'hameçonnage peut freiner l'utilisation d'Internet par ces clients, pour les transactions d'affaires. Si les gens ne peuvent avoir de certitude quant au site où ils se trouvent sur la Toile (*World Wide Web*), ils risquent d'utiliser moins la Toile pour leurs opérations commerciales et leurs communications légitimes[xviii].

  Ce risque est étayé par les résultats d'une étude de *Consumer Reports* menée en 2005, montrant que la confiance en la sécurité d'Internet diminue. Parmi les nombreuses conclusions que permet de tirer l'étude, on mentionnera le fait que neuf adultes américains utilisateurs d'Internet sur dix ont changé leurs habitudes relativement à Internet à cause du risque de vol d'identité et que, parmi ces utilisateurs, 30 % ont avoué avoir réduit de façon générale leur utilisation d'Internet. De plus, 25 % des répondants ont dit avoir cessé d'acheter en ligne, alors que 29 % de ceux qui le font toujours ont dit avoir diminué la fréquence de leurs achats[xix].

- *Casse-tête des enquêtes menées par les responsables de l'application de la loi*. Contrairement à certains autres types de vol d'identité pour lesquels les organismes d'application de la loi peuvent mener des enquêtes fructueuses dans un même secteur géographique (p. ex., les vols de portefeuilles, de sacs à main ou de courrier), l'hameçonnage – comme les autres types de crimes commis au moyen d'Internet – peut se faire à partir de n'importe quel endroit où des spécialistes de l'hameçonnage peuvent avoir un accès Internet. Un spécialiste de l'hameçonnage dans un pays peut s'emparer de façon électronique d'un ordinateur à l'étranger et s'en servir pour héberger son site Web d'hameçonnage

ou envoyer ses courriels d'hameçonnage à des résidents d'autres pays encore. De plus, au cours des dernières années, les activités criminelles en ligne ont souvent témoigné d'une répartition bien définie du travail. Par exemple, dans une fraude en ligne, les tâches de conception du programme, de repérage des sites hôtes pour l'hameçonnage, d'envoi des pourriels, et d'autres aspects de l'opération d'hameçonnage à grande échelle, peuvent être réparties entre des personnes se trouvant à divers endroits. Cela signifie que, dans certaines enquêtes sur l'hameçonnage, une collaboration en temps opportun entre les organismes d'application de la loi dans plusieurs pays peut être nécessaire pour repérer, identifier et arrêter les criminels complices de l'escroquerie.

- *Incitations pour les organisations criminelles à mener des opérations transfrontalières*. Les autorités responsables de l'application de la loi au Canada et aux États-Unis craignent que chacun des facteurs susmentionnés crée en outre des conditions incitant les membres de véritables organisations criminelles dans divers pays à mener des opérations d'hameçonnage systématiques. Les responsables de l'application de la loi ont déjà des indications selon lesquelles des groupes criminels en Europe embauchent des pirates informatiques, ou concluent avec eux des ententes, pour produire des courriels et des sites Web d'hameçonnage et pour mettre au point le programme malveillant dont ils se serviront pour les attaques d'hameçonnage.

Liste de contrôle à des fins de prévention et de signalement des procédés d'hameçonnage

Une des mesures les plus fondamentales que les gouvernements et les entreprises du secteur privé prennent pour protéger le public contre l'hameçonnage est la prestation de conseils précis sur la façon d'éviter les procédés d'hameçonnage, et de les signaler. Il est important de remarquer que, selon une étude récente sur l'hameçonnage, menée par des chercheurs de l'Université Harvard et de l'Université de la Californie à Berkeley, les bons sites Web d'hameçonnage dupent 90 % des participants, que près du quart d'entre eux ne vérifient pas l'existence de signaux visuels anti-hameçonnage (p. ex., des indicateurs de sécurité) et que certaines attaques au moyen de tromperies visuelles [hameçonnage] peuvent tromper même les utilisateurs les plus avertis[xx].

La liste de conseils au public qui suit – tirée de renseignements fournis par l'APWG, la *Federal Trade Commission* des États-Unis et le Centre d'appel antifraude du Canada (le centre national d'appel au Canada)[xxi] – se présente en quatre parties :

1. **Prévention : que faire**

- Protégez votre ordinateur au moyen d'un logiciel antivirus, de filtres de logiciels espions, de filtres pour courriels et de programmes pare-feu, et mettez-les à jour régulièrement.
    - Songez à installer une barre d'outils de navigateur Web pour vous protéger contre les faux sites Web d'hameçonnage (vérifiez auprès de votre fournisseur de navigateur Web ou de messagerie électronique où trouver de telles barres d'outils).

- Faites en sorte que votre navigateur Web sur Internet soit à jour et que les corrections de programme à des fins de sécurité aient été appliquées.
    - Si vous utilisez le navigateur Web *Microsoft Internet Explorer* en particulier, vous devriez vous rendre immédiatement à la page d'accueil de Microsoft Security -- http://www.microsoft.com/canada/french/default.aspx -- pour télécharger une correction de programme spéciale relative à certains procédés d'hameçonnage.

- Méfiez-vous des courriels comportant des demandes pressantes d'information financière personnelle ou des menaces de fermeture de comptes en ligne.
    - Les spécialistes de l'hameçonnage demandent généralement des renseignements tels que les noms d'utilisateurs, les mots de passe, les numéros de cartes de crédit, les numéros de sécurité sociale, etc.
    - Les courriels des spécialistes de l'hameçonnage ne sont habituellement pas personnalisés, alors que les messages authentiques d'une entreprise de commerce électronique le sont en règle générale.

- Lorsque vous communiquez avec votre institution financière, n'utilisez que les canaux dont des sources indépendantes ont confirmé la fiabilité (p. ex., information imprimée sur votre carte bancaire, sur la correspondance que vous envoie l'institution, votre relevé de compte mensuel) et ne vous fiez pas aux liens contenus dans des courriels, même si l'adresse Internet semble être exacte.

- Assurez-vous de toujours utiliser un site Web sécurisé lorsque vous fournissez votre numéro de carte de crédit ou d'autres renseignements de nature délicate sur votre navigateur Web.
    - Pour avoir la certitude d'utiliser un serveur Web sécurisé, vérifiez le début de l'adresse Web sur votre barre d'adresse de navigateur – cette adresse devrait être « https:// » plutôt qu'uniquement « http:// »

- Entrez régulièrement dans vos comptes en ligne.
    - Ne laissez pas s'écouler tout un mois avant de vérifier chaque compte.
- Vérifiez régulièrement vos relevés bancaires et vos relevés de cartes de crédit et de cartes de débit pour vous assurer que toutes les transactions sont légitimes.
    - S'il y a quelque chose de suspect, communiquez avec votre banque et avec les émetteurs de toutes vos cartes.

2. Prévention : ce qu'il faut éviter de faire

- Ne tenez pas pour acquis que vous pouvez identifier correctement un site Web en en vérifiant uniquement l'aspect général.

- N'utilisez pas les liens fournis dans un courriel pour atteindre une page Web, si vous soupçonnez que le message pourrait ne pas être authentique.
    - Appelez plutôt l'entreprise par téléphone ou rendez-vous sur le site Web directement en tapant l'adresse Web dans votre navigateur Web.

- Ne remplissez pas de formulaires dans des messages courriels ou des fenêtres éclairs non sollicitées où l'on vous demande de l'information financière personnelle.
    - Communiquez des renseignements tels que des numéros de cartes de crédit ou de l'information sur un compte, uniquement sur un site Web sécurisé ou au téléphone.

3. Signalement : courriels ou sites Web suspects

- Signalez toujours un courriel ou un site Web d'« hameçonnage » ou d'« usurpation de marque » aux groupes suivants, que vous ayez répondu ou non au courriel ou au site Web d'hameçonnage :
    - Acheminez le courriel, aux États-Unis à reportphishing@antiphishing.com, et au Canada à SEDDE.ca
    - Acheminez le courriel à l'entreprise visée par le courriel frauduleux, à son adresse destinée au signalement de fraude (p. ex., « usurpation@ebay.com »)
    - Aux États-Unis, acheminez le courriel à la *Federal Trade Commission* (FTC) à spam@uce.gov et avertissez l'Internet Crime Complaint Center (IC3) en portant plainte sur son site Web, http://www.ifccfbi.gov.
        - L'IC3 est un projet conjoint du FBI et d'un organisme sans but lucratif, le *National White Collar Crime Center* (NW3C) (centre national de la criminalité des cols blancs). Les personnes qui ont été victimes de criminalité par Internet, y compris de vols d'identité, peuvent signaler l'activité criminelle éventuelle sur le site Web d'IC3. Le personnel d'IC3 peut alors analyser les plaintes en essayant d'en dégager un modèle et d'établir le niveau possible de la criminalité et, s'il y a lieu, transmettre des dossiers d'enquête, comprenant des données sur les plaintes et d'autres renseignements, aux enquêteurs travaillant à l'échelle fédérale, d'un État ou d'une localité et aux procureurs de diverses régions métropolitaines des États-Unis. L'IC3 transmet aussi les données sur les plaintes relatives à un vol d'identité ou à une fraude informatique à la FTC, qui les intègre à son *Identity Theft Data Clearinghouse* (centre de données sur le vol d'identité).
        - La *Federal Trade Commission* a créé à la fin de l'année 1999 l'*Identity Theft Data Clearinghouse*, un centre national, dans le but de donner aux organismes d'application de la loi accès aux plaintes concernant le vol d'identité. Reposant sur le *Consumer Sentinel Network* de la FTC, le centre permet aux membres du réseau, qu'ils soient canadiens ou américains, d'accéder directement, en ligne et en toute sécurité, aux plaintes des consommateurs que la FTC a reçues au moyen de son formulaire en ligne http://www.consumer.gov/idtheft, d'une ligne d'information sans frais (877-IDTHEFT) ou des ententes sur le partage de données conclues avec d'autres organismes, par exemple le *Social Security Administration's Office*, qui relève de l'Inspector General. Les responsables de l'application de la loi peuvent faire des recherches dans les bases de données du centre en utilisant des données qui concernent l'endroit où se trouve un suspect, la victime, une entreprise impliquée dans l'utilisation frauduleuse de

l'identité ou de nombreux autres éléments clés relatifs au crime. À l'heure actuelle, plus de 1 000 organismes d'application de la loi peuvent accéder en ligne directement à près de 700 000 plaintes relatives à un vol d'identité dont les données sont conservées dans ce centre.

- Nota : Lorsque vous transférez des messages où l'identité a fait l'objet d'une usurpation, incluez toujours le courriel d'origine complet, muni de son en-tête intact.

4. Signalement : possibles divulgations à des spécialistes de l'hameçonnage

- Si vous croyez avoir divulgué de l'information en répondant à une fraude par hameçonnage, avertissez immédiatement les responsables de l'application de la loi.

  - Aux États-Unis, avertissez l'Internet Crime Complaint Center (IC3) en portant plainte sur son site Web, http://www.ifccfbi.gov.

  - Au Canada, avertissez la Gendarmerie royale du Canada en portant plainte sur le site Web du Signalement en direct des crimes économiques, à http://www.sedde.ca/ et obtenez de l'information sur la façon de faire face à un vol d'identité, en communiquant avec le Centre d'appel antifraude du Canada au http://www.phonebusters.com/.
    - Le Centre de signalement en direct des crimes économiques, un projet de partenariat intégré sur le Web auquel participent des organismes d'application de la loi provinciaux, fédéraux et internationaux ainsi que des organismes de réglementation et des organisations commerciales privées qui s'intéressent de façon légitime aux enquêtes et qui reçoivent une copie des plaintes relatives aux crimes économiques, dont le vol d'identité. Le Centre de signalement en direct des crimes économiques diffuse aussi des renseignements relatifs aux tendances et des informations sur l'éducation, la prévention et la sensibilisation des consommateurs aux crimes économiques.
    - Le Centre d'appel antifraude du Canada est dirigé à la fois par la Police provinciale de l'Ontario et par la Gendarmerie royale du Canada. Il recueille des informations sur la fraude par télémarketing, les lettres frauduleuses exigeant la perception préalable de frais et les plaintes touchant le vol d'identité. Même s'il est possible de déposer une plainte par courrier électronique, la plupart des victimes le font en téléphonant au Centre. L'information est transmise à l'organisme d'application de la loi compétent. En raison de l'augmentation constante du nombre de plaintes relatives au vol d'identité, le Centre a mis sur pied un projet pour le vol d'identité en 2002. Les données recueillies par le Centre sont utiles à qui veut évaluer les répercussions des divers types de fraude sur le public. [16] Le Centre d'appel antifraude du Canada joue un rôle clé en matière d'éducation du public puisqu'il fait connaître les scénarios utilisés pour la fraude par télémarketing. Le Centre joue aussi un rôle essentiel dans la collecte et la diffusion de données probantes concernant la victime, de statistiques et de documentation. Le premier mandat du Centre

consistait à entamer des poursuites judiciaires, en vertu du *Code criminel du Canada*, contre les individus impliqués dans la fraude par télémarketing en Ontario ou au Québec. Son mandat l'amène maintenant aussi à faciliter les poursuites judiciaires entamées par des organismes américains en favorisant l'extradition des coupables, et des procédures entamées par Industrie Canada en vertu de la *Loi sur la concurrence*. À l'automne de 2006, le Centre d'appel antifraude du Canada commencera à recueillir des statistiques et de l'information liées directement à l'hameçonnage, grâce à des occasions de signalement sur Internet, en conjonction avec le Centre de signalement en direct des crimes économiques.

- Nota : Une vaste gamme d'institutions financières régies par le fédéral aux États-Unis sont tenues de signaler au Financial Crimes Enforcement Network (FinCEN) du département du Trésor tous les cas où l'information recueillie leur permet de soupçonner un possible crime contre une institution financière. Les organismes américains d'application de la loi peuvent accéder à ces rapports aux fins de leurs enquêtes. Récemment, le nombre croissant de vols d'identité a justifié que l'on ajoute à rapports appellés *Suspicious Activity Reports* une case que l'institution financière peut cocher si elle croit que l'activité suspecte qu'elle signale implique une quelconque activité de vol d'identité. Cet ajout permet aux agents fédéraux de cerner plus facilement les crimes actuels ou récents liés au vol d'identité, touchant les institutions financières.

Répliques à l'hameçonnage : pratiques actuelles et prometteuses

Des entreprises du secteur privé et des organismes gouvernementaux au Canada et aux États-Unis ont entrepris un nombre croissant de mesures et d'initiatives diverses pour lutter contre l'hameçonnage. Comme cela a déjà été expliqué, bon nombre de ces mesures et de ces initiatives sont multisectorielles, intergouvernementales et pluri-organismes et ont une portée allant au-delà des entités d'application de la loi.

Éducation du public

Comme l'hameçonnage est une forme de vol d'identité qui diffère substantiellement d'autres techniques de vol d'identité faisant appel à des moyens physiques, le gouvernement et le secteur privé doivent faire en sorte que le public reçoive régulièrement de l'information à jour sur les dernières techniques d'hameçonnage et sur la façon de les reconnaître. À l'occasion du forum sur la criminalité transfrontalière de mai 2003, SPPCC (à l'époque, le ministère du Solliciteur général du Canada) et le département américain de la Justice ont émis conjointement deux alertes publiques sur les tendances observées et sur les derniers développements en matière de vol d'identité, l'une s'adressant aux consommateurs et l'autre aux détaillants. Les alertes mettaient l'accent sur certaines des formes les plus importantes de vol d'identité au Canada et aux États-Unis, en expliquant comment les reconnaître et comment y réagir. Depuis, divers organismes d'application de la loi au Canada et aux États-Unis ont diffusé à grande échelle de l'information sur l'hameçonnage, à l'intention du public. Par exemple, le département américain de la Justice a émis une alerte publique spéciale sur l'hameçonnage en 2004[xxii], la *Federal Trade Commission* des États-Unis a émis une

alerte à l'intention des consommateurs sur l'hameçonnage en 2005[xxiii], et la GRC a récemment affiché sur son site Web de l'information au sujet de l'hameçonnage et de l'hameçonnage vocal[xxiv].

Confirmation de l'authenticité

Bien que les programmes d'éducation des consommateurs soient une composante importante de la lutte contre l'hameçonnage et d'autres formes de vol d'identité impliquant la « manipulation des structures sociales », ils ne suffiront pas à assurer une protection adéquate du public, car les spécialistes de l'hameçonnage continuent de perfectionner leurs techniques d'attaque. Les entreprises du secteur privé doivent poursuivre leurs démarches, afin d'améliorer les techniques de confirmation de l'authenticité et déployer de multiples mesures de confirmation, s'il le faut, pour renforcer la confiance des utilisateurs d'Internet en la fiabilité et la provenance des messages en ligne qu'ils reçoivent. Il pourrait également être important que les entreprises tentent d'uniformiser davantage leur façon de communiquer avec leurs clients (p. ex., l'information qu'elles utilisent à des fins de confirmation de l'authenticité et les situations où elles demanderont cette information).

Cadre législatif

Un cadre législatif indéfectible est également fondamental pour arriver à lutter contre le vol d'identité et contre les mécanismes précis ou les méthodes utilisés à des fins telles que l'hameçonnage. Au Canada, le *Code criminel* ne prévoit aucune disposition interdisant directement l'hameçonnage ou d'autres méthodes d'obtention à des fins criminelles de renseignements sur l'identité. Si une attaque d'hameçonnage utilise de gros volumes de pourriels (courriels non sollicités) pouvant affecter le fonctionnement d'un système informatique ou si les pourriels utilisent des en-têtes trompeurs pour éviter les filtres de pourriels, alors certains articles du *Code criminel* concernant des infractions liées aux données informatiques peuvent s'appliquer. L'utilisation de renseignements sur l'identité ayant été obtenus par l'hameçonnage ou d'autres moyens, peut cependant correspondre à un certain nombre d'infractions criminelles, notamment l'usurpation de nom, la fraude ou l'utilisation illégale de données concernant des cartes de crédit. Le ministère de la Justice a entrepris, il y a plusieurs années, l'examen du *Code criminel* afin de déterminer sa pertinence face au problème croissant du vol d'identité. Le Ministère a commencé à élaborer des propositions pour pallier certaines des limites du droit pénal à cet égard, et à consulter les principaux intervenants afin d'obtenir leur précieuse contribution à des modifications législatives.

Une autre démarche récente au Canada concernant la législation entourant l'hameçonnage a été le lancement en 2004 par le gouvernement du Canada du *Plan d'action anti-pourriel pour le Canada* et l'établissement d'un groupe de travail réunissant des intervenants du gouvernement et du secteur privé pour surveiller et coordonner sa mise en œuvre. En 2005, ce groupe de travail a été chargé de produire un rapport sur la situation, et sur les progrès ayant été accomplis. Ce rapport, *Freinons le pourriel : Créer un Internet plus fort et plus sécuritaire*, a mis de l'avant 22 recommandations pour lutter contre les pourriels, sensibiliser davantage le public et rétablir la confiance en la messagerie électronique. Le groupe a également proposé des pratiques parmi les meilleures à l'intention des fournisseurs de services Internet et d'autres exploitants de réseaux, ainsi que pour le marketing par courriel. En outre, le groupe a recommandé

l'adoption d'une législation interdisant certaines formes de pourriels et d'autres nouvelles menaces pour la sécurité et la sûreté d'Internet (p. ex., l'hameçonnage) et la mise sur pied d'un organisme de coordination fédéral pour s'occuper de la question des pourriels de façon continue[xxv]. Cela est important du point de vue de l'hameçonnage, parce que l'hameçonnage se fait habituellement au moyen d'une technique de pourriels qui consiste à envoyer en lots des courriels non sollicités. Dans le cas de l'hameçonnage, le pourriel permet systématiquement aux criminels de distribuer leurs messages électroniques frauduleux à un grand nombre de consommateurs, à un coût minimum.

Aux États-Unis, depuis 1998, le fédéral ainsi que presque tous les États, ont adopté une législation pénale spécifique concernant le vol d'identité, qui peut s'appliquer à l'hameçonnage[xxvi]. En outre, les autorités fédérales peuvent porter des accusations de fraudes en vertu de la législation fédérale, notamment des fraudes en ligne[xxvii], et en vertu de la *CAN-SPAM Act*[xxviii], pour s'attaquer à la fois à l'envoi de courriels d'hameçonnage et à l'utilisation de courriels à en-têtes trompeurs et d'autres techniques typiques aux pourriels criminels. Actuellement, à la demande du président Bush, l'*Identity Theft Task Force* du Président prépare un plan stratégique pour lutter plus efficacement contre toutes les formes de vol d'identité, qui prévoit notamment des modifications à la législation, au besoin. On s'attend à ce que le plan soit présenté à la Maison-Blanche au début de novembre 2006[xxix].

Application de la loi

Pour que la réplique en vue d'identifier le vol exige soit efficace et complète, il faut faire enquête sur les cas impliquant des procédés d'hameçonnage et intenter des poursuites. Au cours de la dernière année, les États-Unis ont engagé un certain nombre de poursuites pénales fédérales contre des spécialistes de l'hameçonnage. À titre d'exemples :

- En août 2006, un résident de la Floride a été formellement accusé par un grand jury fédéral américain de fraude informatique liée à une manœuvre d'hameçonnage qui visait entre autres des personnes désireuses de faire des dons dans le cadre d'une campagne de secours aux sinistrés de l'ouragan Katrina. Le défendeur a créé et vendu des sites Web d'hameçonnage frauduleux. Les sites Web d'hameçonnage, présentés sous forme de « trousses d'hameçonnage », qui comportaient dans certains cas des témoignages en ligne de personnes demandant au public de faire des dons, étaient conçus de façon à faire croire aux visiteurs qu'ils fournissaient leurs renseignements personnels et financiers sur un site Web légitime. Parmi les sites Web frauduleux que le défendeur a censément créés, se trouvaient des sites analogues à celui des campagnes de secours aux sinistrés de l'ouragan Katrina de la Croix-Rouge américaine et de deux institutions financières canadiennes, la Banque Nationale et la Caisse de crédit Desjardins. L'homme a vendu les sites d'hameçonnage à deux fraudeurs en puissance pour environ 150 $ chacun. Un des sites, celui de la Banque Nationale, a reçu environ 8 500 « visites »[xxx].
- En mai 2006, un homme de l'État d'Iowa a été condamné à 21 mois de prison pour avoir exploité une manœuvre d'hameçonnage visant les consommateurs de MSN. Le défendeur a été condamné après avoir plaidé coupable à une fraude informatique et à des activités connexes liées à un appareillage d'accès. La peine incluait notamment l'obligation pour Harris de restituer la somme de

57 294,07 $. Le défendeur a admis avoir créé un faux site Web de MSN (une division de la société Microsoft), puis avoir envoyé des courriels aux clients de MSN pour leur demander de visiter le site Web et de mettre à jour l'information sur leur compte, en fournissant leur numéro de carte de crédit et d'autres renseignements personnels. Harris a trompé les clients de MSN en les amenant à croire que ce faisant, ils allaient se voir accorder un crédit de 50 % au regard de leur prochaine facture mensuelle. Lorsque les destinataires répondaient, l'information était acheminée à une adresse de courriel que Microsoft a pu retracer et qui était l'adresse du défendeur, à Davenport[xxxi].

- En janvier 2006, un Californien a été arrêté relativement à des accusations de fraude informatique et d'utilisation non autorisée d'un appareil d'accès (carte de crédit) relativement à une fraude d'hameçonnage visant les clients d'AOL. Le défendeur est accusé d'avoir envoyé des milliers de courriels à des utilisateurs d'*America Online* (AOL), qui semblent provenir du service de facturation d'AOL. Dans ces messages frauduleux, les abonnés étaient pressés de « mettre à jour » leur information aux fins de la facturation d'AOL, sous peine de perdre leur service sinon et ils étaient redirigés vers un des nombreux sites Web frauduleux pour entrer l'information sur eux-mêmes et sur leur compte financier. Le défendeur, qui est accusé d'avoir contrôlé ces sites Web, utilisait l'information obtenue frauduleusement pour porter des achats sur les cartes de crédit ou de débit des abonnés d'AOL trompés. Ce cas a fait l'objet d'une enquête des autorités américaines qui ont bénéficié d'une aide substantielle des services de police de l'Ontario et de l'État de la Californie.

Pour que les enquêtes et les poursuites relatives à l'hameçonnage soient fructueuses, il faut cependant que les responsables de l'application de la loi (incluant les enquêteurs et les procureurs) aient de la formation sur les procédés d'hameçonnage et les techniques d'enquête dans le cadre de leur formation sur le vol d'identité. Au Canada, la Police provinciale de l'Ontario a organisé trois conférences internationales sur le vol d'identité qui ont attiré des centaines d'enquêteurs de partout au Canada et aux États-Unis, ainsi que d'autres pays. Aux États-Unis, le département de la Justice, par l'intermédiaire de son *National Advocacy Center*, a donné de la formation sur l'hameçonnage et d'autres formes de vols d'identité aux agents et aux procureurs fédéraux. En outre l'Association canadienne des chefs de police et l'Association internationale des chefs de police ont des composantes qui ont pour mandat précis de se concentrer sur les questions concernant le vol d'identité et le cybercrime.

Coordination binationale et nationale

Les questions liées au vol d'identité, notamment l'hameçonnage, touchent toutes les compétences et concernent tous les paliers de gouvernement, l'ensemble des responsables de l'application de la loi et le secteur privé. Dans le but d'éviter de doubler les activités et d'assurer l'uniformité dans l'ensemble des compétences et des programmes, un certain nombre d'entités de coordination ont été mises sur pied aux échelons national, binational et multinational et elles se sont attaquées à différents aspects du vol d'identité. Vu leur intérêt pour le vol d'identité et leur mandat à cet égard, ces entités sont également bien placées pour faciliter la coordination binationale et nationale sur l'hameçonnage en particulier.

- **Groupe de travail binational sur les fraudes transfrontalières par marketing de masse / Forum sur la criminalité transfrontalière** – Depuis sa création, en 1997, le Groupe de travail binational sur les fraudes transfrontalières par marketing de masse s'est révélé un outil important pour la coordination et la coopération entre les deux pays, visant toutes sortes de problèmes liés à la fraude par marketing de masse. Le Groupe de travail, qui est en outre un sous-groupe du Forum sur la criminalité transfrontalière Canada--États-Unis, a déjà mis en relief le problème du vol d'identité, dans un rapport sur la fraude par marketing de masse publié en 2003, et en participant à la préparation d'alertes publiques conjointes sur le vol d'identité. Après l'annonce du plan stratégique du Groupe de travail sur le vol d'identité du Président, le Groupe de travail binational pourrait constituer un des instruments permettant des discussions précises sur la coordination binationale de l'éducation du public, la prévention et l'application de la loi relativement à l'hameçonnage et à d'autres formes de vol d'identité.
- **Groupe intergouvernemental d'experts chargé de réaliser une étude sur la fraude et l'abus et la falsification d'identité à des fins criminelles - Nations Unies**. Depuis 2005, sous la gouverne de la Commission des Nations Unies sur le crime, un Groupe intergouvernemental d'experts a étudié les problèmes liés à la fraude et à l'utilisation de l'identité à des fins criminelles. Le Groupe d'experts, dont font partie des participants du Canada et des États-Unis, prépare maintenant un rapport à l'intention de la Commission sur le crime dont on prévoit qu'il fournira une analyse portant précisément sur le vol d'identité en ligne, notamment l'hameçonnage, ainsi que des recommandations de pratiques exemplaires pour les gouvernements et le secteur privé.

Conclusion

L'hameçonnage est une forme de comportement criminel qui menace de plus en plus les consommateurs, les institutions financières et les entreprises commerciales au Canada, aux États-Unis, de même que dans d'autres pays. Étant donné que l'hameçonnage ne montre aucun signe d'affaiblissement et que, au contraire, il continuera probablement d'apparaître sous de nouvelles formes plus perfectionnées, les responsables de l'application de la loi, les organismes des autres gouvernements, ainsi que les intervenants du secteur privé des deux pays devront collaborer plus étroitement que jamais pour lutter contre l'hameçonnage, en améliorant l'éducation du public, la prévention, la confirmation de l'authenticité et les mesures nationales et binationales d'application de la loi.

Bien que l'hameçonnage soit une menace particulière en soi, il est aussi important de se rendre compte que les défis qu'il pose aux responsables des orientations politiques et aux têtes dirigeantes en matière d'application de la loi sont les mêmes que ceux qui se posent dans la problématique globale du vol d'identité.

Le rapport sur le vol d'identité présenté en octobre 2004 au Groupe de travail binational sur les fraudes transfrontalières par marketing de masse renferme des recommandations pour s'attaquer aux dangers que pose le vol d'identité, notamment la

coordination d'initiatives d'éducation du public, l'amélioration des mécanismes de signalement et de l'application de la loi, l'examen des cadres législatifs et l'amélioration de l'intégrité et de la sécurité des documents et des données[xxxii].

Les auteurs du rapport recommandent en outre de lutter globalement à la fois contre l'hameçonnage et le vol d'identité. En réponse à ces recommandations, les gouvernements des deux pays continuent de collaborer pour freiner l'hameçonnage et le vol d'identité.

[i] Rapport sur le vol d'identité, octobre 2004, disponible à http://www.psepc-sppcc.gc.ca/prg/le/bs/report-fr.asp.
[ii] Hameçonnage : une nouvelle forme de vol d'identité – Avis – *Forum sur la criminalité transfrontalière Canada – États-Unis*, octobre 2004 – http://www.psepc.gc.ca
[iii] Anti-Phishing Working Group, Phishing Activity Trends Report: August, 2006, *available at* http://www.antiphishing.org/reports/apwg_report_August_2006.pdf.
[iv] Anti-Phishing Working Group, Phishing Activity Trends Report: August, 2005, *available at* http://www.antiphishing.org/reports/apwg_phishing_activity_report_august_05.pdf.
[v] APWG, August 2005
[vi] APWG, August 2005
[vii] APWG, August 2005
[viii] APWG, August 2005
[ix] Symantec Corporation, Internet Security Threat Report at 22 (September 2006), *available at* http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf.
[x] See Dan Ferguson, Black Press, *Phishing warning Beware e-mails asking for personal info*, Peace Arch News, October 10, 2006, *available at* http://www.peacearchnews.com/portals-code/list.cgi?paper=44&cat=23&id=746625&more=.
[xi] Internet Scams Fraud Trends: January-December 2005, *National Consumers League*, *available at* Internet Scams Fraud Trends: January-December 2005, *National Consumers League*, *available at* http://www.fraud.org/internet/intstat.htm.
[xii] *See* Larry Greenemeier, Update: AT&T Hackers Devised Elaborate Phishing Scam To Dupe Customers, Information Week, September 1, 2006, *available at* http://informationweek.com/news/showArticle.jhtml?articleID=192501168.
[xiii] Phishing Activity Trends Report- January 2005, *The Anti-Phishing Working Group.*
[xiv] Spear hameçonnage: Highly Targeted Scams, *Microsoft*, December 9, 2005. Spear Phishing: Highly Targeted Scams, *Microsoft*, December 9, 2005. www.microsoft.com
[xv] Lazarus, David. Phishing expedition at heart of AT&T hacking, San Francisco Chronicle, September 1, 2006. www.sfgate.com
[xvi] L'ACFC met les consommateurs en garde contre une nouvelle forme d'hameçonnage, le « vishing », *Agence de la consommation en matière financière du Canada*, 19 juillet 2006.
[xvii] Schulman, Jay. Voice-over-IP Scams Set to Grow, *VoIP News*, July 21, 2006.
[xviii] Stevenson, Robert Louis B. Plugging the "Phishing" Hole: Legislation Versus Technology, 2005 Duke Law and Technology Review 0006.
[xix] Leap of Faith: Using the Internet Despite the Dangers, *Consumer Reports WebWatch*, October 2005. www.consumerwebwatch.org
[xx] *See* Rachna Dhamija, J.D. Tygar, and M. Hearst. Why Phishing Works paper presented at CHI 2006, April 22-27, 2006, Montréal, Quebec, *available at* http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf.
[xxi] See Anti-Phishing Working Group, Consumer Advice: How to Avoid Phishing Scams, available at http://www.antiphishing.org/consumer_recs.html; PhoneBusters, Comment savoir s'il s'agit d'une fraude : hameçonnage, disponible à http://www.phonebusters.com/francais/recognizeit_phishingemails.html.
[xxii] See Criminal Division, U.S. Department of Justice, Special Report on "Phishing" (2004), available at http://www.usdoj.gov/criminal/fraud/Phishing.pdf.
[xxiii] See FTC, Consumer Alert: How Not to Get Hooked by a ' Phishing' Scam, available at http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm.
[xxiv] Voir GRC, Hameçonnage, « phishing » ou usurpation de marque, disponible à http://www.rcmp-grc.gc.ca/scams/phishing_f.htm; GRC, Hameçonnage vocal, disponible à http://www.rcmp-grc.gc.ca/scams/vishing_f.htm.
[xxv] Freinons le pourriel : créer un Internet plus fort et plus sécuritaire, *Rapport du Groupe de travail sur le pourriel*, mai 2005
[xxvi] See 18 U.S.C. 1928(a)(&), 1028A(a).
[xxvii] See 18 U.S.C. 1343.
[xxviii] See 18 U.S.C. 1037.

[xxix] *See* Executive Order (May 10, 2006), *available at See* Executive Order (May 10, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html.

[xxx] See U.S. Attorney's Office, Western District of Pennsylvania, Press Release (August 16, 2006), available at http://www.usdoj.gov/katrina/Katrina_Fraud/pr/press_releases/2006/aug/08-16-06desirindict.pdf..

[xxxi] See U.S. Attorney's Office, Southern District of Iowa, Press Release (May 19, 2006), available at http://www.usdoj.gov/usao/ias/press_releases/051906a.html.

[xxxii] Rapport sur le vol d'identité, octobre 2004

Annexe 1 : Bibliographie

Consumer Advice: How to Avoid Phishing Scams. Anti-Phishing Working Group, *available at* http://www.antiphishing.org/consumer_recs.html.

Consumer Alert: How Not to Get Hooked by a "Phishing" Scam. FTC. June 2005, *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm.

Executive Order (May 10, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html.

L'ACFC met les consommateurs en garde contre une nouvelle forme d'hameçonnage, le « vishing », *Agence de la consommation en matière financière du Canada*, 19 juillet 2006.

Ferguson, Dan. Black Press. Phishing warning Beware e-mails asking for personal info, Peace Arch News, October 10, 2006, *available at* http://www.peacearchnews.com/portals-code/list.cgi?paper=44&cat=23&id=746625&more=.

Hameçonnage, « phishing » ou usurpation de marque. GRC, disponible à http://www.rcmp-grc.gc.ca/scams/phishing_f.htm

Internet Scams Fraud Trends: January-December 2005, *National Consumers League*, *available at* http://www.fraud.org/internet/intstat.htm.

Internet Security Threat Report: September 2006. *Symantec Corporation*.

Lazarus, David. Phishing expedition at heart of AT&T hacking, *San Francisco Chronicle*, September 1, 2006. www.sfgate.com

Leap of Faith: Using the Internet Despite the Dangers, *Consumer Reports WebWatch*, October 2005. www.consumerwebwatch.org

Le mois de mars est déclaré « Mois sur la prévention de la fraude » au Canada et partout dans le monde, *Bureau de la concurrence*, 1er mars 2006. www.competitionbureau.gc.ca

Hameçonnage : une nouvelle forme de vol d'identité – Avis – *Forum sur la criminalité transfrontalière Canada - États-Unis*, octobre 2004 – http://www.psepc.gc.ca

Phishing Activity Trends Report- January 2005, *The Anti-Phishing Working Group.* http://antiphishing.org

Phishing Activity Trends Report: August 2005. *The Anti-Phishing Working Group*.

Phishing Activity Trends Report- May 2006, *The Anti-Phishing Working Group*.

Phishing Activity Trends Report: August, 2006. *The Anti-Phishing Working Group.*

Comment savoir s'il s'agit d'une fraude : hameçonnage – *PhoneBusters*, www.phonebusters.com

Rapport sur le vol d'identité, octobre 2004

Schulman, Jay. Voice-over-IP Scams Set to Grow, *VoIP News*, July 21, 2006.

Spear Phishing: Highly Targeted Scams, *Microsoft*, December 9, 2005. www.microsoft.com

Special Report on "Phishing". Criminal Division, U.S. Department of Justice (2004), *available at* http://www.usdoj.gov/criminal/fraud/Phishing.pdf

Statistics on Phone Fraud: Identity Theft Complaints (2005) – *PhoneBusters,* Statistiques : vol d'identité - plaintes (2005) – *PhoneBusters,* http://www.phonebusters.com/francais/statistics_E05.html

Stevenson, Robert Louis B. Plugging the "Phishing" Hole: Legislation Versus Technology, 2005 Duke Law and Technology Review 0006.

Freinons le pourriel : créer un Internet plus fort et plus sécuritaire, *Rapport du Groupe de travail sur le pourriel,* mai 2005

Hameçonnage vocal, GRC, disponible à http://www.rcmp-grc.gc.ca/scams/vishing_f.htm.