ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

Direction de la Science, de la technologie et de l'industrie
Comité de la politique de l'information, de l'informatique et des communications

Orientations de l'OCDE pour les politiques sur le vol d'identité en ligne

Réunion Ministérielle de l'OCDE le futur de l'économie Internet

Séoul, Corée , 17 ~ 18 juin 2008

Accueillie par 방송통신위원회 KOREA COMMUNICATIONS COMMISSION

Orientations de l'OCDE pour les politiques sur le vol d'identité en ligne

I. Introduction

Le problème de l'usurpation (ou vol) d'identité, qui existe depuis toujours, s'est étendu à l'univers virtuel suite au développement de l'Internet et du commerce électronique. Si l'ampleur du phénomène apparaît limitée dans la plupart des pays, ses implications sont cependant considérables dans la mesure où l'usurpation d'identité numérique peut ébranler la confiance des consommateurs dans leur utilisation de l'Internet dans le cadre du commerce électronique. Les gouvernements ont pris des mesures pour lutter contre ce type de fraude – que ce soit en ou hors ligne, au niveau national comme international. Les *Lignes directrices de 1999 de l'OCDE pour la protection du consommateur dans le cadre du commerce électronique* (« les Lignes directrices de 1999 ») et les *Lignes directrices de 2003 de l'OCDE régissant la protection des consommateurs contre les pratiques commerciales frauduleuses et trompeuses* (« les Lignes directrices de 2003 »), comprennent, par exemple, des principes visant à renforcer les cadres institutionnels des pays membres pour lutter contre la fraude commise en et hors ligne. Outre les travaux de l'OCDE, des instruments internationaux tels que la *Convention contre la délinquance en ligne* du Conseil de l'Europe et la *Convention contre le crime organisé transnational* des Nations Unies ont été développés pour s'attaquer au problème (Annexe I).

Les principes énoncés dans les *Lignes directrices* de 1999 et de 2003 forment une base solide pour établir un cadre institutionnel de lutte contre l'usurpation d'identité en ligne et d'autres types de délinquance. L'objet du présent document est de décrire la manière dont les principes présentés dans ces instruments pourraient être étoffés de manière à renforcer et à développer des stratégies effectives dans les pays membres pour combattre l'usurpation d'identité en ligne. Ce document s'intéresse plus particulièrement à la manière dont l'éducation et la sensibilisation des parties prenantes pourraient être améliorées pour mieux lutter contre ce type de délits. Ces orientations s'appuient très largement sur les recherches et analyses contenues dans le *Document exploratoire sur le vol d'identité en ligne* qui a été examiné par le Comité de la politique à l'égard des consommateurs en 2007 (OCDE, 2008).

Définition de l'usurpation d'identité, formes et méthodes

L'usurpation d'identité se produit lorsqu'une personne acquiert, transfère, possède ou utilise sans autorisation des informations personnelles appartenant à une personne physique ou morale, dans l'intention de commettre, ou en relation avec, des actes de fraude ou autres actes de délinquance. Bien que cette définition

s'applique aux individus et aux personnes morales, les présentes orientations se limitent aux usurpations d'identité affectant les consommateurs.

Traditionnellement, l'usurpation d'identité consistait à accéder à des données trouvées dans des documents publics ou obtenues à l'occasion d'un vol d'effets personnels, de l'utilisation impropre de bases de données, de carte de crédit, de comptes bancaires ou d'épargne, et à faire un usage frauduleux de ces informations. Comme on le verra plus en détail dans l'Encadré 1 ci-dessous, les accès non autorisés à des données personnelles peuvent être réalisés par différents moyens, qui vont de la fouille de poubelles, au vol de cartes de paiement, en passant par l'invocation de faux prétextes, le coup d'œil par-dessus l'épaule d'une victime, le « skimming », ou le vol de documents comptables.

Encadré 1. Les moyens traditionnels d'accéder à des données personnelles pour le vol d'identité

Pêche dans les poubelles : dans ce cas de figure, les fraudeurs fouillent les poubelles à la recherche de pièces qui y auraient été jetées. C'est de cette manière que les voleurs d'identité obtiennent des copies de chèques de particuliers, de cartes de crédit ou de relevés bancaires, ou d'autres pièces contenant des informations personnelles.

Les prétextes : les « prétexteurs » contactent un établissement financier ou une compagnie de téléphone, en se faisant passer pour un client légitime, et en demandant des informations relatives au compte de ce client. Dans d'autres cas, le « prétexteur » fait partie de l'établissement financier, ou encore ouvre un compte en ligne au nom d'un client.

Le « shoulder surfing » : dans ce cas, le fraudeur regarde par-dessus l'épaule de sa victime ou depuis un point d'observation proche pendant que la victime saisit son code d'identification personnel (« PIN ») à un distributeur automatique de billets.

Le « skimming » : le fraudeur s'empare de données personnelles à partir des bandes magnétiques situées au dos des cartes de crédit ; les données sont alors transmises en un autre lieu ou elles sont ré-encodées pour fabriquer de fausses cartes de crédit.

Le vol de documents comptables : une personne vole des données appartenant à une entreprise (en s'emparant d'ordinateurs ou de fichiers) ou soudoie des personnes internes à l'entreprise pour obtenir ces informations détenues par l'entreprise ou l'organisation.

En ligne, il existe trois grandes méthodes pour obtenir des informations personnelles sur des victimes (voir encadré 2) : *i)* un logiciel conçu pour collecter des informations personnelles est secrètement installé sur un ordinateur ou un autre équipement (fixe ou mobile) appartenant à la victime potentielle (les « maliciels ») ; *ii)* des courriels ou des sites Internet mensongers sont rédigés pour inciter des personnes à révéler des informations personnelles les concernant (hameçonnage ; les courriels d'hameçonnage sont souvent distribués en masse par le biais de pourriels ; de plus en plus, ils vont de pair avec l'installation de maliciels sur les ordinateurs des destinataires.) ; et *iii)* le piratage ou tout autre type d'exploitation d'ordinateurs ou d'appareils mobiles en vue d'obtenir des données personnelles.

Encadré 2. Techniques en ligne pour voler des informations personnelles

Les maliciels : il s'agit d'un terme générique désignant un code ou un programme logiciel injecté dans un système d'informations dans le but de porter atteinte à ce système ou à d'autres systèmes, ou de les subvertir pour des usages autres que ceux prévus par leur propriétaire. On distingue plusieurs sortes de maliciels : les virus, les vers, les chevaux de Troie, les portes dérobées, les enregistreurs de clavier, les gratteurs d'écran, les rootkits, et les logiciels espions (voir les définitions de ces termes dans l'Annexe III).

Le pourriel (ou spam) : ce terme renvoie d'habitude aux messages non sollicités, non souhaités et pernicieux (OCDE, 2006c) ; le spam est de plus en plus considéré comme un vecteur de maliciels et d'escroqueries à base d'hameçonnage.

L'hameçonnage : il s'agit d'une tromperie qu'utilisent les voleurs pour « harponner » les informations personnelles d'identification d'internautes trop confiants, et ce au moyen de courriels et de sites Internet miroirs ressemblant à ceux d'entreprises existant véritablement – établissements financiers ou administrations, par exemple. Une attaque par hameçonnage se décomposera généralement comme suit :

- L'hameçonneur envoie à la victime un courriel qui semble provenir d'une société existante car reprenant les couleurs, les graphiques, les logos et la phraséologie de cette société.
- La victime, après avoir lu le courriel, envoie ses informations personnelles au hameçonneur, soit en répondant au courriel soit en remplissant, via un lien hypertexte, un formulaire qui semble provenir de la société en question.
- De cette manière, les informations personnelles de la victime sont transmises directement au fraudeur.

Le piratage : il consiste à exploiter les vulnérabilités de systèmes électroniques ou de certains logiciels afin de siphonner des données personnelles.

Prévalence

L'usurpation d'identité est un problème de plus en plus fréquent qui touche des individus de toutes les classes d'âge et de toutes les catégories sociales. L'encadré 3 donne une description des manières dont les voleurs d'identité abusent des informations personnelles des consommateurs, hors ligne et en ligne. L'usurpation d'identité en ligne a été reconnue comme une source de préoccupation croissante pour les consommateurs depuis quelques années, ayant un impact direct sur les transactions du commerce électronique et mobile (OCDE, 2006c, p. 21). Comme précisé dans l'*Eurobaromètre spécial de l'Union européenne (« UE ») de 2006* (Commission européenne, 2006, p. 12), l'utilisation de l'Internet pour acheter des biens et services en ligne n'est pas encore très répandue puisqu'elle ne concernait en 2005 que 27 % de la population de l'UE, et se limitait pour l'essentiel à des achats nationaux. Une telle limite s'explique en partie par une certaine défiance des consommateurs à l'égard du commerce électronique par crainte que leurs informations personnelles ne leur soient dérobées.[1]

1 En 2006, une enquête en ligne de l'Union Internationale des Télécommunications intitulée *Confiance et sensibilisation dans le domaine de la cybersécurité* (UIT, 2006) concluait que plus de 40 % des internautes ne procèderaient pas à des transactions en ligne pour cette raison.

Encadré 3. Utilisation frauduleuse d'informations personnelles : moyens classiques et techniques en ligne

Utilisation frauduleuse de comptes existants : les voleurs utilisent des comptes existants de leurs victimes : comptes de carte de crédit, comptes chèques, comptes téléphoniques (fixe et mobile), comptes de paiement sur Internet, courriel et autres comptes Internet, comptes d'assurance médicale.

Création de comptes nouveaux : Les voleurs utilisent des informations personnelles de leurs victimes pour ouvrir de nouveaux comptes, qui peuvent être des comptes téléphoniques (fixes et mobiles), des comptes de cartes de crédit, des comptes de crédit, des comptes chèques et comptes d'épargne, des comptes de paiement sur Internet, des comptes d'assurance automobile ou des comptes de paiements médicaux.

Autres actes frauduleux : les fraudeurs peuvent aussi donner à la police les données personnelles de victimes lorsqu'ils sont arrêtés ou accusés d'un acte de délinquance, ou s'en servir pour obtenir un traitement médical, des services, des fournitures, pour louer un logement, pour toucher des prestations sociales, ou dans le cadre de l'emploi.

La lutte contre l'usurpation d'identité

Ces dernières années, plusieurs pays membres ont mis en place des programmes de lutte contre l'usurpation d'identité (voir Annexe II). Ces programmes, qui font une large place à l'éducation et la sensibilisation, visent de larges publics : consommateurs, acteurs clés au sein des entreprises, des administrations et des forces de police. Une analyse des difficultés rencontrées fait apparaître que la lutte contre l'usurpation d'identité comporte trois aspects clés :

Prévention – ce que les parties prenantes peuvent faire pour réduire le risque de vol d'identités (améliorer la sécurité de l'identité ; détecter les tentatives et les instances de vol d'identité ; et limiter l'ampleur et la portée des incidents).

Dissuasion - ce que les parties prenantes peuvent faire pour dissuader des individus de se livrer à une usurpation d'identité (sanctions judiciaires, par exemple).

Récupération de l'identité et recours – ce que les parties prenantes peuvent faire pour faciliter la récupération de ce qui a été volé, et les recours des victimes pour les préjudices subis tels que financiers, les atteintes à la réputation ainsi que d'autres préjudices non monétaires.

Les présentes orientations portent principalement sur la prévention contre l'acquisition d'informations personnelles en ligne. La section II présente des idées sur la manière dont les parties prenantes peuvent utiliser l'éducation et la sensibilisation accrue pour *i)* aider les consommateurs à éviter d'être victimes d'usurpation d'identité et *ii)* aider les entreprises et les pouvoirs publics à lutter plus efficacement contre le problème. La section III porte spécifiquement sur les initiatives possibles pour faire connaître aux entreprises les moyens d'améliorer la sécurité des données, et la section IV se penche sur les problèmes liés à l'authentification de l'identité. La section V, enfin, examinera les domaines dans lesquels il serait utile d'approfondir les travaux sur les moyens de lutte contre l'usurpation d'identité en ligne. Si les présentes orientations sont axées sur l'usurpation d'identité en ligne, il convient de noter qu'un grand nombre des mesures suggérées sont également applicables à l'usurpation d'identité hors ligne.

II. Comment l'éducation et la sensibilisation pourraient être améliorées pour prévenir l'usurpation d'identité en ligne

Pour limiter les risques d'usurpation, l'éducation et la sensibilisation des consommateurs, des entreprises, des responsables publics et des médias à ce problème est indispensable. Diminuer ce risque renforcerait la confiance des consommateurs dans le commerce électronique. Comme le stipulent les *Lignes directrices* de 1999, « Les gouvernements, les entreprises et les représentants des consommateurs devraient collaborer en vue d'assurer l'éducation des consommateurs en matière de commerce électronique (…) et de sensibiliser davantage les entreprises et les consommateurs au cadre de protection des consommateurs qui s'applique à leurs activités en ligne » (OCDE, 1999, section VIII). Cette recommandation, laquelle figure également dans les *Principes directeurs de 2003* (OCDE, 2003, section II. F), s'applique directement à l'usurpation d'identité en ligne. L'usurpation d'identité en ligne est une activité frauduleuse de plus en plus complexe, qui utilise des méthodes technologiques sophistiquées en constante évolution. Pour s'y attaquer, une action concertée et coordonnée de toutes les parties prenantes (pouvoirs publics, entreprises et consommateurs) est indispensable. Éducation et sensibilisation sont donc nécessaires pour faire en sorte que les consommateurs, comme les entreprises, aient conscience de l'importance du problème et des formes sans cesse nouvelles qu'il peut prendre.

Structure des programmes d'éducation et de sensibilisation

Pour être efficaces, les programmes d'éducation et de sensibilisation nécessitent *i)* des documents de sensibilisation convaincants et informatifs et *ii)* des institutions et des canaux pour distribuer ces documents et dispenser l'éducation de manière efficace aux parties prenantes. De plus, la coopération et la coordination des initiatives entre parties peuvent donner lieu à des synergies intéressantes et rendre les efforts plus efficaces. L'implication des parties prenantes est donc essentielle en amont dans le cadre de développement des programmes ; les perspectives différentes permettent de mieux déterminer quels sont précisément les besoins en matière d'éducation et de sensibilisation, quels peuvent être les publics cibles et comment les atteindre.

La collecte d'informations pertinentes sur l'usurpation d'identité

La collecte et la diffusion d'informations de base sur la réalité du vol d'identité en ligne sont essentielles pour améliorer la sensibilisation et la connaissance de l'importance du problème et des moyens de le combattre. Cinq types d'information devraient être développés : *i*) des informations statistiques mettant en évidence les développements et les tendances ; *ii*) des informations sur les conséquences non économiques du vol d'identité ; *iii*) des éléments factuels sur les méthodes qu'utilisent les individus pour voler les identités, et *iv*) des recommandations générales pour protéger les identités, et notamment les instruments que peuvent utiliser les consommateurs et les entreprises pour bloquer les intrusions en ligne, et *v*) des recommandations sur les techniques qui permettent d'identifier ou de détecter les tentatives d'usage illicite de données d'identité.

i) Données statistiques mettant en évidence les développements et les tendances

Dans l'établissement et le maintien d'un cadre effectif visant à limiter l'incidence des pratiques frauduleuses contre les consommateurs, les *Lignes directrices* de 2003 appellent les pays membres à prévoir « des mécanismes efficaces pour rechercher, préserver, recueillir et échanger les informations et preuves pertinentes se rapportant à des cas de pratiques commerciales frauduleuses et trompeuses » (OCDE, 2003, section II. A. 2). La compréhension de la portée et de l'ampleur du problème est un élément clé des campagnes d'éducation. Pourtant, jusqu'à présent, l'information concernant l'évolution du phénomène du vol d'identité en ligne n'est en général pas accessible, en dépit de mises en garde dans les pays membres sur la recrudescence de ce phénomène. En outre, lorsque ces données existent, celles-ci rendent rarement compte en détail des formes que peut prendre l'usurpation d'identité en ligne (OCDE, 2008).

Il serait utile que les parties prenantes explorent les moyens d'améliorer l'élaboration d'informations statistiques qui rendent compte de l'évolution du phénomène du vol d'identité. Il serait bon également que ces informations comprennent des données spécifiques sur le vol d'identité en ligne. L'un des indicateurs fréquemment utilisés à cet égard est le nombre de plaintes déposées par des consommateurs. Il serait intéressant de voir quels autres types d'indicateurs pourraient être utiles.

Outre la mesure de l'ampleur du phénomène du vol d'identité, il pourrait être intéressant de déterminer son impact économique sur les individus et sur les pays. Cette information apporterait un éclairage nouveau et illustrerait l'ampleur du phénomène.

Des informations comparables d'un pays à l'autre et entre différentes sources au sein d'un même pays auraient un plus grand impact. Pour ce faire, celles-ci devraient être élaborées, dans la mesure du possible, à partir des efforts de groupes multilatéraux (publics comme privés) qui travaillent dans ce domaine. Des plateformes du secteur privé pourraient être utilisées pour réunir, analyser et diffuser les statistiques concernant l'hameçonnage, le pourriel et les virus à l'échelle mondiale. Parmi ces structures, citons : le Groupe de travail anti-hameçonnage "Anti-Phishing Working Group" (APWG, à www.antiphishing.org), qui travaille à l'élimination de la fraude et du vol d'identité lorsqu'elle passe par l'hameçonnage et par les usurpations d'identité en ligne ; le Groupe de travail "Messaging Anti-Abuse" (MAAWG, à www.maawg.org), dont l'objet est de préserver l'activité de messagerie électronique contre les « exploits » en ligne et les abus tels que l'hameçonnage de messageries, les attaques par maliciels et les autres formes d'abus ; et DigitalPhishNet (DPN, à www.digitalphishnet.org/default.aspx), un forum de collaboration au sein duquel des fournisseurs d'accès Internet, des sites d'enchères en ligne, des établissements financiers et des agents de la force publique mettent en commun leurs statistiques et leurs bonnes pratiques en temps réel pour s'attaquer à l'hameçonnage et aux autres menaces en ligne.

ii) Informations sur les effets indirects de l'usurpation d'identité

Outre ses coûts économiques, l'usurpation d'identité peut avoir d'autres incidences telsque le temps perdu par les victimes pour le rétablissement de leur réputation, les effets négatifs subis par leur réputation, et les difficultés qu'elles rencontrent par la suite pour rétablir leur crédibilité financière. La collecte d'informations sur ces aspects permettrait de dresser un état des lieux plus complet des implications du vol d'identité, contribuant ainsi à améliorer la sensibilisation.

iii) Éléments factuels sur les méthodes et techniques qu'utilisent les individus pour usurper les identités

L'identification des différentes techniques utilisées pour commettre les vols d'identité est essentielle si l'on veut pratiquer une dissuasion suffisante pour parer efficacement à la menace. Pour être utiles, les informations sur ces techniques doivent être collectées, analysées et actualisées régulièrement afin de suivre l'actualité. Lorsque c'est possible, il serait intéressant que ces informations soient traitées et partagées, non seulement entre les acteurs de la protection du consommateur, mais également avec d'autres organes chargés de l'application de la loi travaillant sur la question du vol d'identité. De fait, le vol d'identité soulève, dans de nombreux cas, des problèmes relevant de la sécurité, de la vie privée et du pourriel (Annexe I). Depuis quelques années, les voleurs d'identité font preuve d'une ingéniosité particulièrement impressionnante pour se procurer des informations personnelles. De plus en plus souvent, comme nous l'avons vu précédemment, les logiciels et les pourriels sont associés à l'hameçonnage.

Comme le montre l'encadré 4 ci-dessous, les attaques par hameçonnage sont de plus en plus sophistiquées, prenant des formes diverses et ciblant les appareils fixes comme les mobiles.

Encadré 4. Les variantes de l'hameçonnage

Le pharming : cette méthode, qui utilise les mêmes types d'identifiants usurpés qu'une attaque classique par hameçonnage, redirige les internautes depuis un site Internet authentique (celui d'une banque, par exemple) vers un site Internet frauduleux ressemblant en tout point à l'original. Lorsque le client connecte son ordinateur au serveur de sa banque, une recherche de correspondance du nom de l'hôte est effectuée pour traduire le nom de domaine de la banque (exemple banque.com) sous forme d'une adresse IP. C'est au cours de ce processus que l'adresse IP sera changée.

Le SmiShing : un utilisateur de téléphone mobile reçoit un SMS dans lequel une société confirme son inscription à un service de rencontre et l'informe que ce service lui sera facturé un certain montant par jour mais qu'il peut annuler sa commande en se rendant sur le site Internet de la société. Ce site Internet est évidemment frauduleux et sera utilisé pour voler des informations personnelles.

Le Vishing : dans un courriel frauduleux classique, qui ressemble à s'y méprendre à ceux d'une entreprise ou d'un établissement légitime, l'hameçonneur invite l'internaute à composer un numéro de téléphone. La victime appelle, tombe sur un répondeur automatique qui lui demande des informations personnelles – numéro de compte bancaire ou mot de passe – prétextant « des vérifications de sécurité ». Généralement, les victimes se méfient moins parce qu'elles ne doivent pas transmettre leurs informations personnelles sur un site Internet.

Il convient de noter que toutes les parties prenantes peuvent participer à l'élaboration et au partage des informations sur les méthodes et techniques employées. Pour exploiter au maximum les informations collectées, il est important que des mécanismes soient mis en place pour faciliter le partage des informations de manière efficace.

iv) Informations sur le niveau de sophistication des techniques de vol d'identité en ligne

Il ne suffit pas d'expliquer les différents procédés par lesquels le vol d'identité en ligne peut être commis ; les campagnes d'éducation doivent également alerter les consommateurs sur le fait que ces méthodes sont en perpétuelle évolution. Les messages d'hameçonnage étaient naguère assez naïfs et ne comportaient que du texte. Par exemple, la fameuse « escroquerie 419 » (aussi connue sous le nom de « arnaque nigériane » ou « lettre nigériane » dans sa version de courrier classique) ; les arnaqueurs tentaient de soutirer de l'argent à leurs victimes sous forme de virements bancaires. Généralement ils évoquaient d'importantes sommes d'argent qu'ils promettaient de partager avec leurs victimes si celles-ci les aidaient à les sortir du pays. Les victimes devaient alors avancer divers frais, droits ou taxes, pour permettre le déblocage des fonds. Mais, victime de son succès, cette arnaque est largement connue parmi les internautes et on ne la rencontre plus guère.

Ainsi, devant la nécessité de trouver des systèmes plus complexes, les hameçonneurs ont cherché et trouvé de nouveaux moyens pour obtenir des consommateurs qu'ils leur révèlent leur mot de passe, leurs numéros de comptes bancaires et autres données personnelles. De plus en plus, les systèmes d'hameçonnage utilisent des images et des logos réalisés avec soin imitant ceux d'établissements commerciaux légitimes. Les courriels sont également de plus en plus personnalisés, et peuvent même contenir les premiers chiffres du numéro de la carte de crédit de la cible – qui sont les mêmes dans toutes les cartes de crédit émises par une banque donnée – pour convaincre la victime potentielle que le message provient bien de sa banque. Comme les véritables offres commerciales, les messages d'hameçonnage contiennent de multiples sollicitations invitant la cible à révéler son mot de passe, son âge, son adresse, etc.

Alors que les hameçonneurs utilisaient auparavant des noms de domaine de niveau supérieur tels que « .com », « .biz », ou « .info », ils recourent maintenant à des noms de domaine de petits États insulaires pour éviter d'être détectés ; par exemple « .im » pour l'Île de Man (Royaume-Uni), que les filtres anti-pourriel ne repèrent souvent pas (McAfee, 2006, p. 15). Certains hameçonneurs vont jusqu'à utiliser des certificats auto-signés afin d'utiliser le protocole de sécurité « HTTPS » et de faire apparaître le cadenas de sécurité sur des sites Internet frauduleux.

Pour une meilleure prévention, il est essentiel que les consommateurs et les différentes parties prenantes soient tenus informés des nouveaux stratagèmes et des avatars des dispositifs connus.

v) Recommandations générales pour protéger son identité en ligne

Pour diminuer considérablement le risque de vol d'identité en ligne, voire le prévenir, il peut être utile de fournir aux parties prenantes des recommandations

pratiques sur les moyens de protéger leur identité (voir encadré 5). Un certain nombre d'organisations et de gouvernements ont élaboré des séries de recommandations dans ce domaine. L'une des initiatives les plus complètes et les plus ambitieuses est celle du gouvernement des États-Unis, qui a créé un site Internet réunissant des informations sur les moyens de protéger les informations personnelles et d'éviter les escroqueries sur Internet (http://onguardonline.gov/index.html), notamment le vol d'identité.

Encadré 5. Hameçonnage : conseils de prévention à l'intention des consommateurs, par OnGuardOnline.gov

- Installer des logiciels anti-virus et anti-logiciels espions, ainsi qu'un pare-feu sur votre appareil fixe ou mobile et veiller à ce qu'ils soient à jour.
- Ne pas cliquer sur les liens contenus dans les messages qui paraissent être du pourriel et ne jamais répondre aux courriels ou aux messages pop-up vous demandant des informations personnelles ou financières. Il faut aussi éviter de couper-coller un lien suspect dans la fenêtre de votre navigateur Internet. Les hameçonneurs peuvent créer des liens qui semblent aboutir à un site donné mais qui en réalité vous mènent sur un site « sosie ».
- Ne jamais communiquer son numéro de carte de crédit ou les numéros de sécurité en réponse à un message qui paraît être du pourriel. Si vous avez des doutes sur l'utilisation de votre compte, contacter l'établissement à l'aide d'un numéro de téléphone dont vous êtes certains de l'authenticité ou ouvrez une nouvelle session de navigateur et saisissez à la main l'adresse Internet correcte de la société.
- Faire suivre tout message d'hameçonnage aux autorités compétentes ou aux groupements professionnels tels que l'APWG, le DPN ou le MAAWG. Les messages d'hameçonnage peuvent également être communiqués à l'adresse spam@uce.gov. Outre les groupements professionnels et autorités compétentes, il peut également être utile d'adresser le courriel d'hameçonnage à l'établissement dont l'identité est usurpée.

Diffusion de l'information

Pour améliorer la prévention, il est essentiel de faire en sorte que les parties prenantes soient conscientes du phénomène de vol d'identité, et qu'elles aient facilement accès à des informations à ce sujet. Il faut à tout le moins que ces informations soient disponibles sur Internet. En outre, il serait utile d'organiser des sessions d'orientation ou de formation dans les établissements scolaires ou au sein de différents groupements. La radio et la télévision constituent également d'excellents vecteurs pour toucher le grand public, de même que les imprimés et les documents sur supports électroniques (CD et DVD). Enfin, les fournisseurs de services Internet et les sites Internet ayant une forte fréquentation comme les outils de recherche et les sites d'enchères, peuvent faire œuvre utile en attirant l'attention des consommateurs sur les informations mises à leur disposition par les gouvernements et les autres parties intéressées.

La coordination des initiatives de formation et de sensibilisation

La coordination des initiatives d'éducation et de sensibilisation est une bonne occasion d'améliorer leur efficacité, allant dans le sens d'une cohérence accrue et

d'une simplification des efforts. Cette coordination peut se faire entre les secteurs privé et public et à partir de plateformes locales, nationales et internationales. Cette coordination permettrait de mettre en évidence les pratiques les plus efficaces et d'en étendre l'utilisation. Les fournisseurs de services Internet par exemple, sont extrêmement bien placés pour souligner l'importance du vol d'identité en ligne, et pour orienter leurs abonnés vers des sources d'information.

Il convient de noter que les initiatives de formation et de sensibilisation revêtent plusieurs formes ; au sein des pouvoirs publics, par exemple, la formation des personnes responsables de l'application des lois couvrant le vol d'identité est un élément important du renforcement de la sensibilisation afin de limiter l'ampleur et la portée du vol d'identité. Un certain nombre de pays sont déjà actifs sur ce front.

Des réseaux internationaux d'autorités de répression tels que le Réseau International de Contrôle et de Protection des Consommateurs (« RICPC ») et le Plan d'Action de Londres pourraient être utilisés comme plateformes pour coordonner et diffuser des informations de sensibilisation à travers les pays membres de l'OCDE (OCDE, 2003, section III. D).

III. La sécurité des données

La sécurité des données doit également être au cœur de toute stratégie visant à lutter contre le vol d'identité. La violation de données peut avoir de nombreuses conséquences préjudiciables ; les consommateurs risquent d'être victimes d'un vol d'identité, l'entité dont le système a fait l'objet d'une effraction est exposée à des poursuites judiciaires pour n'avoir pas protégé les données, et le coût peut être élevé pour toutes les parties touchées. Il faut donc que les pays membres mettent au point et appliquent des normes de sécurité des données (lois et règlements, normes et lignes directrices sectorielles et dispositions contractuelles privées), pouvant aller le cas échéant, jusqu'au lancement d'enquêtes et de poursuites judiciaires contre les entités qui enfreindraient la législation en matière de sécurité des données.

Les pays membres doivent améliorer la sensibilisation du secteur privé sur la protection des données et inciter les organisations qui collectent et conservent des données sensibles sur les consommateurs à mettre en œuvre des mesures de sécurité concrètes pour protéger les données personnelles de ces consommateurs.

IV. Authentification électronique

L'authentification électronique est reconnue comme un processus utile, qui permet la vérification et la gestion des identités en ligne. Dans les *Orientations pour l'identification électronique* de l'OCDE (2006), dans lesquelles sont énoncés un certain nombre de principes opérationnels visant à aider les pays Membres à établir ou moderniser leurs méthodes d'identification, ce concept s'entend comme une fonction pour établir la validité et l'assurance de l'identité assumée par un utilisateur, un appareil ou un autre type d'entité dans un système d'information ou de communication. Elle peut donc constituer une dissuasion efficace contre le vol ou l'utilisation frauduleuse d'informations personnelles.

La sensibilisation aux bienfaits et aux bonnes utilisations de l'authentification sont des éléments essentiels pour la confiance des utilisateurs en ligne.

Comme le préconise la *Recommandation de l'OCDE sur l'authentification électronique de 2007*, qui invite les pays membres à établir des approches compatibles et non dépendantes des choix de technologie pour permettre l'authentification électronique des personnes physiques et morales à l'intérieur des frontières des pays et entre différents pays, les pays de l'OCDE doivent prendre des mesures pour aider tous les participants à prendre conscience des avantages de l'authentification électronique, aux niveaux tant national qu'international.

L'authentification électronique est actuellement considérée comme l'une des composantes du concept émergent de gestion des identités. Ce système global, dont l'objet serait de permettre aux utilisateurs d'interagir en livrant un minimum d'informations personnelles en ligne, fera l'objet de la plus grande attention par les pays de l'OCDE dans les années à venir.

V. Travaux ultérieurs

Comme nous l'avons vu dès le début de notre étude, trois aspects sont essentiels pour lutter contre le vol d'identité en ligne : *i)* la prévention, *ii)* la dissuasion et *iii)* la récupération de l'identité et les voies de recours. Le présent document s'intéresse principalement sur la prévention, et examine plus précisément les moyens de faire de la pédagogie auprès des consommateurs et des autres parties prenantes pour prévenir le vol d'identité en ligne. Il est toutefois urgent de s'occuper d'autres aspects de ce problème. Le Bureau des Nations Unies sur les Drogues et la Criminalité (UNODC) travaille en concertation avec la Commission des Nations Unies pour le Droit du Commerce International (CNUDCI) à l'élaboration de recommandations de bonnes pratiques pour la prévention, la dissuasion et la récupération des identités volées. La Commission européenne travaille à une définition harmonisée du concept et examine l'opportunité de faire du vol d'identité en ligne un délit pénal spécifique dans toute l'Union européenne. Comme le signale le *Document exploratoire sur le vol d'identité en ligne* (OCDE, 2008), un certain nombre d'agences gouvernementales et d'entreprises privées dans de nombreux pays étudient le problème.

Voici un certain nombre des aspects qui doivent être considérés aux niveaux national et international (par l'OCDE et par d'autres organismes internationaux) :

Aspects légaux

- Le vol d'identité doit-il être défini juridiquement en tant que délit spécifique ?
- Quelles sanctions dissuasives seraient appropriées (amende, confiscation, listes noires, *etc*.) ?
- Quelles devraient être les voies de recours pour les victimes ?
- La législation devrait-elle imposer aux entreprises de prendre davantage de mesures pour prévenir les vols d'identité ? Par exemple les entreprises devraient-elles être tenues de signaler les incidents de sécurité susceptibles d'affecter leurs clients lorsque ces incidents peuvent conduire à des vols d'identité, ou bien

d'améliorer l'authentification des consommateurs et des clients lorsqu'elles assurent des services ou qu'elles procèdent à des transactions ?

La coopération transnationale en matière de répression, entre autorités de protection des consommateurs d'une part et entre ces autorités et le secteur privé d'autre part.

- Comment la coopération transnationale entre autorités de répression peut-elle être renforcée dans les domaines suivants ?
  - Compétences en matière d'investigation et de partage de renseignements avec les autorités étrangères, les entreprises et le secteur privé, et les représentants des consommateurs.
  - Assistance, formation, et soutien aux efforts de répression des autres pays.
  - Mise en œuvre et échange de « bonnes pratiques » en matière d'éducation des consommateurs.

Récupération de l'identité et recours

- Quel type d'assistance les pouvoirs publics, les entreprises, et les ONG devraient-elles mettre en place pour aider les consommateurs à rétablir leur identité et à récupérer les sommes perdues et les pertes non monétaires résultant du vol de leur identité ?
- Des mécanismes de recours doivent-ils être proposés aux consommateurs, et dans l'affirmative, quelles entités doivent être responsables de ces recours ?
- De quels outils supplémentaires les victimes ont-elles besoin pour s'assurer du rétablissement effectif de leur identité et pour se remettre complètement de l'usurpation de leur identité ?

Appendice H.1 : Instruments multilatéraux concernant le vol d'identité en ligne

I. Instruments de l'OCDE sur le commerce électronique

OCDE (Organisation de coopération et de développement économiques) (1999), *Les lignes directrices de l'OCDE régissant la protection du consommateur dans le cadre du commerce électronique*, OCDE, Paris, http://www.oecd.org/document/51/0,3343,fr_2649_34267_1824435_1_1_1_1,00.html.

OCDE (2003), *Lignes directrices de l'OCDE régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses*, OCDE, Paris, www.oecd.org/sti/consumer-policy .

II. Instruments de l'OCDE concernant la sécurité, la vie privée et le pourriel

Sécurité :

OCDE (2002), *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information*, OCDE, Paris, www.oecd.org/dataoecd/16/22/15582260.pdf.

OCDE (2007), *Recommandation de l'OCDE sur l'authentification électronique et Orientations pour l'authentification électronique*, OCDE, Paris, www.oecd.org/dataoecd/32/45/38921342.pdf.

Vie privée :

OCDE (1980), *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel,* OCDE, Paris, www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

OCDE (2007), *Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée*, OCDE, Paris, www.oecd.org/dataoecd/43/28/38770483.pdf.

Pourriel :

OCDE (2006), *Boîte à outils anti-spam et politiques et mesures recommandées*, OCDE, Paris, www.oecd-antispam.org/.

III. Autres instruments internationaux

Conseil de l'Europe (2001), *Convention sur la cybercriminalité,* Budapest, 23 novembre 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

Organisation des Nations Unies (2001), *Convention des Nations Unies contre la criminalité transnationale organisée*, 8 janvier 2001, www.unodc.org/pdf/crime/a_res_55/res5525e.pdf.

Appendice H.2 : Les initiatives d'éducation en matière de vol d'identité dans les pays de l'OCDE

Initiatives des pouvoirs publics

États-Unis

En mai 2006, la Federal Trade Commission des États-Unis a lancé l'initiative « Deter, Detect, Defend », une campagne d'éducation qui a pour objet d'aider les consommateurs à prendre les mesures nécessaires pour réduire les risques de vol d'identité, pour contrôler la diffusion de leurs informations personnelles, et pour réagir rapidement lorsqu'ils soupçonnent qu'ils ont été victimes d'un vol d'identité. Cette campagne s'appuie notamment sur un support intitulé *the ID Theft Consumer Education Kit*, et permet aux organisations et aux différents groupements d'informer les consommateurs sur les moyens de réduire les risques de vol d'identité et sur les mesures à prendre lorsqu'on en a été victime. Ce kit se compose des éléments suivants :

- Un fascicule qui fournit des instructions détaillées et les outils pour contribuer à l'éducation des consommateurs.
- Une brochure.
- Un DVD contenant 10 minutes de vidéo – relatant des cas réels et montrant la manière dont les victimes de vol d'identité ont réagi.
- Un CD-ROM contenant tous les supports pédagogiques de manière à permettre une reproduction facile.
- Un guide plus approfondi destiné aux victimes de vol d'identité.

En avril 2007, une Task Force présidentielle spécialisée dans le vol d'identité a publié un rapport dans lequel est présenté un plan stratégique pour faire face aux problèmes posés par le vol d'identité (FTC, Département américain de la justice, 2007a). L'un des principaux axes de ce plan stratégique est d'éduquer les parties prenantes sur les moyens d'empêcher les données sensibles sur les consommateurs de tomber entre les mains de voleurs d'identité. Ce plan stratégique recommande une campagne d'éducation publique sur plusieurs années menée par les autorités fédérales des États et par les autorités locales. Les États-Unis ont aussi créé un site Internet d'information sur la Task Force, permettant de signaler les cas individuels et rappelant les droits des victimes (www.idtheft.gov).

Australie

Le gouvernement australien distribue un kit d'information intitulé, *How to prevent and respond to identity theft* (Comment prévenir le vol d'identité, comment réagir) (www.crimeprevention.gov.au), pour proposer au grand public des stratégies concrètes pour éviter d'être victime d'un vol d'identité. En 2007, il a publié une brochure, *ID Theft : Dealing with identity theft*, à l'occasion de la Semaine sur le vol d'identité de l'Australasian Consumer Taskforce, organisée dans le cadre de la campagne annuelle de sensibilisation à la fraude de la Task Force. Les pouvoirs publics distribuent également une brochure, *E-Crime - A Crime Prevention Kit for Small*

Business, qui indique aux petits entrepreneurs les moyens d'éviter d'être victime d'un acte de délinquance informatique. En juillet 2007, le gouvernement a introduit une série d'initiatives sur la sécurité informatique dans le cadre de l'E-Security National Agenda. Certaines de ces initiatives ont pour but d'améliorer la sensibilisation aux problèmes de sécurité informatique chez les particuliers et dans les petites entreprises et de généraliser le programme national et international d'exercice sur la sécurité informatique. Le site Internet du gouvernement consacré à la sécurité informatique, *Stay Smart Online* (www.staysmartonline.gov.au), donne aux internautes des conseils pratiques pour sécuriser un ordinateur personnel, effectuer des transactions en ligne, ainsi que des informations pour protéger les enfants et les jeunes sur l'Internet. Le groupe océanien (Australie et Nouvelle-Zélande) Australasian Consumer Fraud Taskforce a créé *ScamWatch* (www.scamwatch.gov.au), un site d'informations sur la fraude sur Internet destiné aux consommateurs et qui leur présente les différents types d'escroquerie, de systèmes et de fraudes. Il contient aussi un dispositif permettant de déclarer les cas de fraude.

Canada

Le Comité des mesures en matière de consommation (CMC), organisation qui représente les ministères fédéraux, provinciaux et territoriaux chargés de la consommation, a élaboré un kit d'information pour aider les consommateurs à se prémunir contre le vol d'identité et leur indiquer les procédures à engager s'ils en sont victimes. De plus, le CMC a préparé un document d'orientation à l'intention des entreprises, contenant des conseils pour protéger les informations personnelles de leurs clients (voir www.cmcweb.ca/idtheft). Un certain nombre d'autres initiatives en cours ont pour objet d'informer les consommateurs sur le vol d'identité en ligne. Citons le Forum de prévention de la fraude, qui regroupe des administrations, des autorités judiciaires et des représentants du secteur privé, qui organise le *Mois de sensibilisation à la fraude* tous les ans en mars, avec pour slogan *La fraude : Identifiez-la. Signalez-la. Enrayez-la.* Le vol d'identité, qui est une forme de fraude parmi d'autres, représente une part importante des informations présentées au public pendant le *Mois de sensibilisation à la fraude*.

Royaume-Uni

Au Royaume-Uni, le Comité directeur sur le vol d'identité au sein du Home Office a lancé un site Internet www.identity-theft.org.uk qui contient aussi des recommandations pour éviter les vols d'identité. En outre, le Bureau du Commissaire de l'Information a produit des supports pédagogiques sur le vol d'identité dans le cadre d'une boîte à outils d'information ; des spots télévisés ; un DVD de formation.

Mexique

Au Mexique, l'Université nationale autonome du Mexique (UNAM) (publique) a mis en place un certain nombre de sites Internet pour alerter les consommateurs et les internautes sur tous les risques qui pèsent sur la sécurité en ligne. Les internautes peuvent y puiser des conseils pour repérer les arnaques (www.seguridad.unam.mx/doc?ap=articulo&id=121), le pharming

(www.seguridad.unam.mx/usuario-casero/pharming.dsc), le phishing (www.seguridad.unam.mx/usuario-casero/phishing.dsc) et des trucs pour empêcher le piratage et les atteintes à la sécurité (www.seguridad.unam.mx/doc?ap=articulo&id=118).

Belgique

En Belgique, plusieurs campagnes sont en cours sur la sensibilisation aux risques Internet, dont fait partie le vol d'identité. Tous les supports sont utilisés : guides (Guide pour l'internaute), sites Internet (www.saferinternet.be, qui s'adresse aux enfants, http://economie.fgov.be du Service public fédéral Économie, qui contient des informations sur les droits des consommateurs en droit belge), communiqués de presse sur la fraude Internet destinés à attirer l'attention des consommateurs sur les pratiques frauduleuses sur l'Internet comme le phishing.

Japon

Au Japon, le Ministère des affaires intérieures et des télécommunications (MIC) a lancé un site Internet intitulé *Informations sur la sécurité à l'intention de l'ensemble des internautes* (www.soumu.go.jp/joho_tsusin/security/index.htm) qui contient des informations de base sur la sécurité des données et sur les mesures préventives de lutte contre les menaces en ligne telles que le vol d'identité.

Initiatives du secteur privé

Dans certains pays membres, le secteur privé participe également à des initiatives d'éducation.

Royaume-Uni

Au Royaume-Uni, un certain nombre d'associations de banques et de systèmes de paiement, telles que le British Banker Association (BBA) et le UK payments Association (APACS), se sont montrées particulièrement actives en menant des initiatives de sensibilisation auprès de leurs propres membres (banques et sociétés) comme de leurs clients ; on trouvera plus d'informations sur l'Internet sur le site *www.banksafeonline.org.uk* (OFCOM, 2006, p. 37).

Pays-Bas

Aux Pays-Bas, le *Nederlands Vereniging van Banken*, l'Association des banques néerlandaises, a lancé une campagne de sensibilisation en 2006 pour informer les consommateurs des risques de vol d'identité et pour leur expliquer les moyens de protéger leurs informations personnelles (INTERVICT, 2006, p. 24).

États-Unis

Aux États-Unis, un certain nombre de secteurs d'activité s'intéressent activement aux initiatives éducatives pour lutter contre le vol d'identité. Les établissements financiers, par exemple, qui peuvent être les principales victimes des attaques par

hameçonnage, sont de plus en plus nombreux à alerter leurs clients sur les nouveaux messages d'hameçonnage et les nouveaux risques qui pèsent sur la sécurité. Depuis 2004, les établissements financiers ont entrepris une action conjointe de sensibilisation par l'intermédiaire du Centre d'assistance sur le vol d'identité (Identity Theft Assistance Center), organisation nationale représentant certaines des plus grands banques des États-Unis ainsi que des agents de change et des sociétés financières. En outre, l'Association nationale des courtiers en valeurs mobilières a publié un guide intitulé « Phishing et autres types d'escroquerie basés sur le vol d'identité en ligne : ne mordez pas à l'hameçon ». Plus récemment, le groupe Identity Theft Prevention and Identity Management Standards Panel (IDSP), créé sous l'égide du Better Business Bureau (BBB) et de l'American National Standards Institute (ANSI) a lancé une nouvelle initiative portant sur l'ensemble du marché, dont l'objet est de contribuer à doter les entreprises et les autres entités des outils nécessaires pour lutter contre le vol d'identité en ligne et la fraude, et de protéger les consommateurs (et de se protéger elles-mêmes) contre les risques associés à ce type de délits : http://www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08.aspx?menuid=3. Ce rapport contient un catalogue des standards existants, des bonnes pratiques et des dispositifs d'application relatifs à cette question dans l'ensemble des secteurs et des activités, ainsi que des recommandations sur les autres domaines dans lesquels les pouvoirs publics et le secteur privé devraient élaborer des standards et des orientations. Il donne également un certain nombre de recommandations pour les initiatives de sensibilisation des consommateurs à des parades telles que le blocage des nouveaux crédits.

Australie

En Australie, l'Australian Bankers Association (ABA), l'Australian High Tech Crime Centre et l'Australian Securities and Investments Commission (ASIC), gèrent conjointement un site, *Protégez votre identité financière* (www.protectfinancialid.org.au) qui aide les individus à protéger leur identité financière et à limiter les dégâts si un problème survient. Il contient des conseils pratiques de prévention, des fiches d'information et un test interactif qui permet à chacun d'évaluer le niveau de sécurité de ses données personnelles.

Mexique

Au Mexique, quelques membres de l'Association de l'Internet mexicain (AMIPCI) ont créé un site Internet (consultable à l'adresse www.navegaprotegido.com.mx), qui contient des informations pour aider les consommateurs à mieux comprendre les risques liés au vol d'identité.

Coordination des initiatives d'éducation

États-Unis

Aux États-Unis par exemple, les services du Procureur général assistent à des séminaires de formation et un certain nombre d'organismes chargés du respect de la loi – parmi lesquels le Département de la justice des États-Unis, le Secret Service, la

FTC, et le FBI – de même que la American Association of Motor Vehicle Administrators ont conjointement organisé plus de 20 séminaires de formation d'une journée sur le vol d'identité à l'intention des autorités des États et des autorités locales de police du pays (US FTC, 2007a, Vol. II, p. 71 à 73).

Australie

En Australie et en Nouvelle-Zélande, le groupe Australasian Consumer Fraud Taskforce soutient une démarche coordonnée de sensibilisation et d'éducation. Ce groupe, formé en mars 2005, rassemble 18 agences de régulation et bureaux chargés de la protection du consommateur contre les escroqueries et les arnaques. Dans ses efforts d'amélioration de la sensibilisation aux risques d'arnaques, cette Taskforce a également pour partenaires un large éventail d'organisations communautaires, non gouvernementales et représentatives du secteur privé.

L'objet de la Taskforce est de favoriser la collaboration des pouvoirs publics pour :

- Donner plus d'efficacité aux efforts de répression de l'escroquerie et des arnaques menés par les autorités d'Australie et de Nouvelle-Zélande.
- Organiser une campagne annuelle coordonnée d'information des consommateurs : le Mois de sensibilisation à la fraude en février ou mars (pour coïncider avec le Mois de prévention de la fraude dans le monde).
- Inviter les entreprises à participer à la campagne d'information et les encourager à partager les informations qu'elles peuvent avoir sur les fraudes et les escroqueries.
- Susciter davantage d'intérêt pour la recherche sur les fraudes et les escroqueries touchant les consommateurs.

Mexique

Au Mexique, le groupe de travail eCrime, constitué d'entités publiques et privées, parmi lesquelles l'Association des banques mexicaines (ABM), la Chambre nationale des industries de transformation (Canacintra), la Banque nationale du Mexique (Banamex), la banque Bancomer, l'Association Internet du Mexique (AMIPCI), la police fédérale de prévention, la Commission fédérale des télécommunications (COFETEL), la Banque nationale du Mexique, la Commission nationale des banques et des marchés financiers (CNBV), Nic Mexico et l'Université publique UNAM, a été créé pour réunir des données sur le phénomène du phishing et pour neutraliser les noms de domaine associés à des usurpations d'identité.

Belgique

En Belgique, le Service public fédéral Économie, PME, travailleurs indépendants et énergie (FPS Économie), la Federal Computer Crime Unit (FCCU) et le Centre de recherche et d'information des organisations de consommateurs (CRIOC) organisent plusieurs campagnes d'information portant notamment sur le vol d'identité. Par exemple, la campagne de prévention de la fraude 2006 « Arnaqué, moi ? jamais ! » a été organisée sous l'égide de l'International Consumer Protection and Enforcement Network (ICPEN),

avec un ciblage spécifique sur l'usurpation d'identité et la fraude contre les consommateurs dans le cadre des services téléphoniques et la fraude liée à la consommation sur l'Internet. La diffusion emprunte plusieurs canaux : prospectus adressés par courrier ou distribués par les services sociaux des grandes villes et à la boutique d'information du FPS Économie (http://mineco.fgov.be/protection_consumer/fraud_prevention/home_fr_001.htm); spots radiodiffusés ; conférences de presse et publications dans des lettres d'information de partenaires externes et dans la presse ; en-tête des relevés de carte de crédit et des factures de téléphone. Cette campagne est financée par le FPS Économie et réalisée avec le soutien de partenaires externes (Belgacom, Loterie nationale, Proximus, Mobistar, Base, Diners Club, Citibank, American Express, Europabank, Les Maisons de justice, etc.).

Appendice H.3 : Terminologie

- *Les enregistreurs (mouchards) de clavier* : un enregistreur de clavier est un logiciel qui détecte et enregistre les touches frappées sur un clavier. Il existe deux types d'enregistreur de clavier : ceux qui nécessitent que l'attaquant récupère les données enregistrées sur le système compromis et ceux qui transmettent activement les données enregistrées.
- *Les rootkits* : un rootkit est un ensemble de programmes conçus pour masquer les atteintes faites à l'intégrité d'un logiciel au niveau le plus privilégié ou « root ». Comme la plupart des maliciels, les rootkits ont besoin d'un accès d'administrateur pour bien fonctionner ; une fois installés ils peuvent être quasiment indétectables.
- *Le pourriel* : il semble qu'il y ait une corrélation de plus en plus forte entre les maliciels, l'hameçonnage, et le pourriel. Le terme de pourriel (en anglais spam) couvre généralement les messages électroniques non sollicités, non souhaités et pernicieux.
- *Les chevaux de Troie* : un cheval de Troie est un logiciel informatique qui n'éveille pas les soupçons mais qui en réalité effectue des actions masquées pour contourner les mesures de sécurité et ouvrir la voie à des attaques. Généralement, un cheval de Troie pénètre dans le système d'un internaute en exploitant une vulnérabilité du navigateur ou une de ses fonctions.
- *Les virus* : un virus est un logiciel caché qui s'étend en infectant un autre programme et en insérant dans ce programme une copie de lui-même. Un virus a besoin d'un programme hôte pour fonctionner avant de devenir actif. Le terme de « virus » s'utilise de plus en plus au sens large pour décrire les virus et les vers.

BIBLIOGRAPHIE

ANSI (American National Standards Institute) et BBB (Better Business Bureau) (2008) Rapport final du panel ANSI-BBB « Identity Theft Prevention and Identity Management Standards « , 31 janvier 2008, www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08.aspx?menuid=3.

BWGCBMMF (2004), *Rapport sur le vol d'identité*. Rapport présenté à la ministre de la Sécurité publique et de la Protection civile du Canada et à l'Attorney General des États-Unis, Octobre 2004, http://www.ps-sp.gc.ca/prg/le/bs/report-fr.asp.

CE (Commission européenne) (2006), DG SANCO, Eurobaromètre spécial «Consumer protection in the Internal Market», septembre 2006, Bruxelles, http://ec.europa.eu/public_opinion/archives/ebs/ebs252_en.pdf.

FTC (Federal Trade Commission) et Département de la Justice (États-Unis) (2007a), Combating Identity Theft: A Strategic Plan (Lutte contre le vol d'identité : un plan stratégique), US Identity Theft Task Force du Président, 23 avril 2007, www.idtheft.gov.

FTC (2007b), Report on *Consumer Fraud and Identity Theft Complaint Data* (Rapport sur la fraude contre les consommateurs et les données concernant les plaintes pour vole d'identité), www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

INTERVICT (International Victimology Institute Tilburg) (2006), Le défi de la lutte contre le vol d'identité, Rapport commandé par le Programme national néerlandais sur la cyberdélinquance contre les infrastructures ("NICC"), 6 septembre 2006, www.tilburguniversity.nl/intervict/publications/NicolevanderMeulen.pdf.

McAfee (2006), *Rapport sur la délinquance virtuelle*, décembre 2006, www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_Criminology_Report_2006.pdf.

OCDE (Organisation de coopération et de développement économiques) (1999), *Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique*, OCDE, Paris, http://www.oecd.org/dataoecd/17/59/34023530.pdf.

OCDE (2003), *Les lignes directrices de l'OCDE régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses*, OCDE, Paris, http://www.oecd.org/dataoecd/24/33/2956464.pdf.

OCDE (2006a), *Rapport sur la mise en œuvre des Lignes Directrices de 2003 sur la Fraude Transfrontière*, OCDE, Paris, http://www.oecd.org/dataoecd/2/5/37133090.pdf.

OCDE (2006b), *Le commerce mobile*, DSTI/CP(2006)7/FINAL, Direction de la Science, de la Technologie et de l'Industrie, www.oecd.org/sti/consumer-policy.

OCDE (2006c), *Boîte à outils anti-spam: politiques et pratiques recommandées*, OCDE, Paris, http://www.oecd-antispam.org/sommaire.fr.php3.

OCDE (2007), *Recommandation sur le règlement des litiges de consommation et leur réparation*, OCDE, Paris, http://www.oecd.org/document/4/0,3343,fr_2649_201185_38960324_1_1_1_1,00.html.

OCDE (2008), *Document exploratoire sur le vol d'identité en ligne,* DSTI/CP(2007)3/FINAL, Direction de la Science, de la Technologie et de l'Industrie.

OFCOM (Office of Communications) (Royaume-Uni) (2006), *Protection en ligne : Enquête sur les consommateurs, les entreprises, et les systèmes et mécanismes de régulation*, 21 juin 2006, www.ofcom.org.uk/research/technology/onlineprotection/report.pdf.

UIT (Union Internationale des Télécommunications) (2006), *Enquête sur la confiance et la sensibilisation dans le domaine de la cybersécurité*, résultats au 17 mai 2006, www.itu.int/newsroom/wtd/2006/survey/charts/q_8.asp.