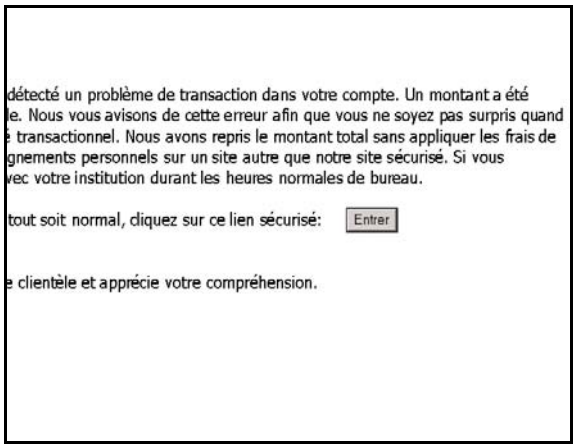
GENDARMERIE ROYALE DU CANADA

La Fraude

Identifiez-la.
Signalez-la.
Enrayez-la.

Protection des renseignements personnels et protection contre l'escroquerie

Guide pratique de l'étudiant



Gendarmerie royale du Canada | Royal Canadian Mounted Police

Canada

Version 1.3

Présenté au :
Directeur, sous-direction des délits commerciaux
Gendarmerie royale du Canada

Rédigé par :
Mélanie Waite, étudiante en sciences biomedicales et criminologie
en collaboration avec la sous-direction des délits commerciaux
de la GRC

Le 1 Mars 2006
Révisé le 23 avril 2007
Ottawa (Ontario)

Préface

La fraude d'identité, c'est-à-dire le vol et l'utilisation de données personnelles à des fins criminelles, est l'une des infractions qui connaît la plus forte croissance au pays. Tous les Canadiens doivent être sensibilisés à la nécessité de bien protéger leurs données personnelles et veiller à maintenir l'intégrité de leur identité et de leurs finances.

À notre époque, la prévention criminelle exige une intégration et une coopération entre les forces policières et les organismes publics et privés. De ces partenariats, on pourra créer des outils permettant de sensibiliser les gens à la fraude et à certaines des pratiques malhonnêtes les plus courantes auxquelles ont recours les criminels pour obtenir leurs données personnelles.

Le présent guide a été conçu par un étudiant pour les étudiants en collaboration avec la Sous-direction des infractions commerciales de la GRC et l'Université d'Ottawa.

Wayne Watson, surintendant principal
Directeur, Infractions commerciales
Gendarmerie royale du Canada
Ottawa (Ontario)

Table des matières

« J'avais lu beaucoup d'histoires, mais je ne croyais jamais que cela pourrait m'arriver... Hou la! Cela peut vraiment arriver. N'importe qui pourrait se faire passer pour vous. » *Ottawa Citizen*, octobre 2005, victime d'une fraude d'identité.

Dans notre société fondée sur l'information, nous pouvons vivre et vaquer à nos activités quotidiennes relativement aisément, parce que nous avons confiance dans les systèmes, les organisations et les gens qui sauvegardent les renseignements qui nous concernent. Chaque citoyen ou consommateur est en fin de compte responsable de sa propre sécurité hors ligne et en direct ainsi que de sa propre éducation ou sensibilisation. Nous disposons pour la plupart de l'information dont nous avons besoin pour nous protéger et pour protéger nos biens contre les crimes classiques. Toutefois, en raison des menaces de plus en plus sophistiquées, les gens doivent régulièrement s'efforcer à l'auto-éducation. Dans l'environnement technologique d'aujourd'hui, c'est dans votre meilleur intérêt de le faire. Ce document a été conçu pour fournir une approche holistique en se renseignant sur la fraude d'identité et les escroqueries en général. Ce document évoluera pour produire de nouvelles versions avec le temps. Il contient les informations de base et les outils pertinents que tout Canadien peut utiliser afin d'enrichir ses connaissances sur la plupart des escroqueries.

« Si la connaissance peut créer des problèmes, ce n'est pas l'ignorance qui peut les résoudre ».
Isaac Asimov (1920-1992)

Les renseignements personnels sont devenus des produits très précieux pour les criminels. Un peu comme les produits qui sont vendus à la bourse des valeurs mobilières tous les jours, de grandes quantités de renseignements personnels changent de main du côté obscur du cyberespace. Vos renseignements personnels peuvent avoir été compromis, vendus, utilisés ou stockés dans une base de données à votre insu pour être utilisés plus tard. Personne n'est à l'abri de ce type de crime.

La Gendarmerie royale du Canada (GRC) définit la fraude d'identité comme l'acquisition, la possession ou le commerce illicite de renseignements personnels ou l'utilisation non autorisée de ces renseignements dans le but de créer une identité fictive ou d'emprunter une identité existante ou d'en prendre le contrôle afin d'obtenir des profits financiers, des biens ou des services ou de dissimuler des activités criminelles. Votre numéro d'assurance sociale (NAS), votre certificat de naissance, votre passeport et votre permis de conduire sont les principaux renseignements ciblés par les criminels. **Ne gardez jamais les trois premiers documents dans votre portefeuille ou votre sac à main** à moins d'en avoir besoin à des fins précises le jour même.

Selon un sondage effectué par Ipsos-Reid en 2006, 73% des adultes canadiens sont inquiets de devenir des victimes de fraude d'identité. Seulement 33% des Canadiens croient qu'ils sont bien éduqués au sujet de la protection d'information personnelle et de la fraude d'identité.

Lorsque de nouvelles menaces apparaîtront, la GRC publiera des versions mises à jour du présent document. Assurez-vous de surveiller les mises à jour. La GRC sait qui est le meilleur expert en la matière, pour ce qui est de l'éducation et de la sensibilisation relatives à la fraude. C'est vous. Servez-vous du présent guide pour vous sensibiliser davantage et ainsi être prêt lorsque la fraude abattra ses filets sur vous. Utilisez ces connaissances pour éduquer votre famille, vos amis et vos connaissances. Informez-vous et restez informé.

PhoneBusters, le centre d'appel antifraude du Canada, est administré conjointement par la Gendarmerie royale du Canada, la Police provinciale de l'Ontario et le Bureau de la concurrence. PhoneBusters joue un rôle clé en renseignant le public sur les pratiques frauduleuses des télévendeurs. Le centre joue également un rôle essentiel dans la collecte et la diffusion des témoignages des victimes, de la documentation, des statistiques et des enregistrements sur bandes magnétiques, qu'il met à la disposition de divers organismes d'application de la loi.

Vous pouvez contacter PhoneBusters en composant le numéro sans frais 1(888) 495-8501 ou www.phonebusters.com .

Signalement en direct des délits économiques (Centre SEDDE) est une initiative qui fait appel à un partenariat intégré entre des organismes d'application de la loi internationaux, fédéraux et provinciaux ainsi que des organismes de réglementation qui désirent à bon droit recevoir, à des fins d'enquête, une copie des plaintes relatives à des délits économiques. Le Centre SEDDE recommandera au besoin aux services de police, à l'organisme de réglementation ou à l'organisation commerciale privée de mener une enquête. Vous pouvez déposer une plainte au Centre SEDDE à l'adresse www.sedde.ca .

1. Escroqueries

La présente section décrit diverses escroqueries en les classant selon la façon dont elles se produisent le plus couramment. Cette section du Guide canadien est donc divisée en cinq environnements distincts. Bien qu'il soit impossible de prévenir certaines escroqueries, on peut, dans la plupart des cas, réduire au minimum les risques d'en être la victime. Notre objectif est de vous apprendre à déceler les risques en déclenchant des signaux d'alarme et en proposant la ligne de conduite la plus sûre.

Les consommateurs doivent adopter certains comportements sécuritaires en matière d'achat en ligne afin de réduire au minimum les risques d'être victimes d'une fraude en ligne. Vérifiez toujours les politiques du commerçant en matière de protection des renseignements personnels, de remboursement et de retour, de même que les conditions légales avant de donner des renseignements personnels et financiers. Conservez une copie de la page de confirmation et de la correspondance échangée avec le commerçant ou le fournisseur en ligne. La façon la plus sûre de payer ses achats en ligne consiste à utiliser une carte de crédit quand le client est protégé par une politique de responsabilité zéro. Informez-vous au sujet de cette option auprès de la société qui a émis votre carte de crédit.

1.1 En direct

En direct

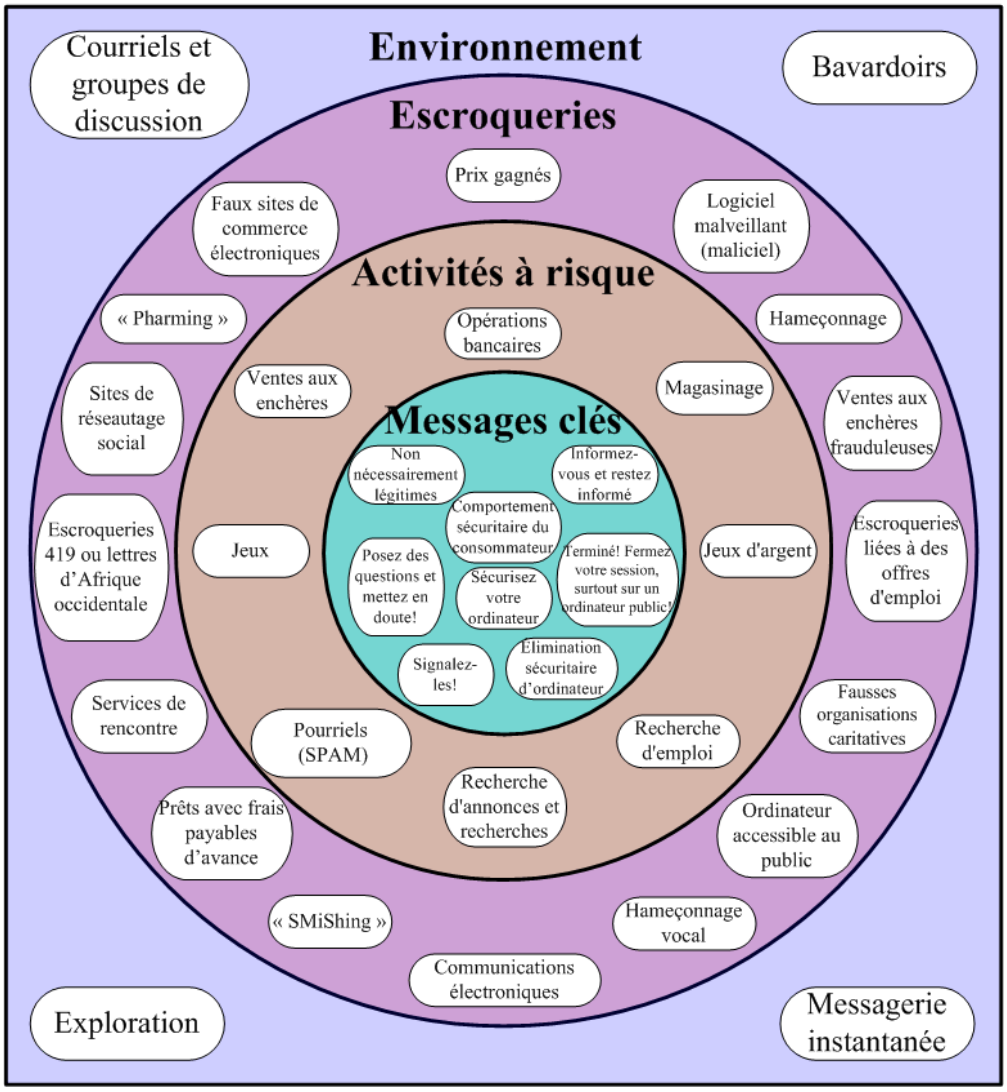


Figure 1 : Messages clés pour éviter les escroqueries en direct qu'on trouve dans divers environnements

De nombreuses activités peuvent être exécutées en direct, telles que le magasinage, la recherche d'annonces, des recherches, la vente aux enchères, des opérations bancaires, les communications, la recherche d'un emploi et les jeux, entre autres. Comme c'est le cas pour les crimes classiques, la clé de la réduction du risque d'être victime d'un crime réside dans la compréhension de base de ces crimes.

La présente section peut comprendre une terminologie avec laquelle vous n'êtes pas familier. Pour enrichir votre terminologie technologique, vous trouverez des descriptions et des définitions fondamentales dans les pages Web appelées « abécédaires ».

1.1.1 Faux sites Web de commerce électronique

Soyez prudent face à des offres « trop belles pour être vraies ». Certains sites Web de commerce électronique sont mis créés dans le but de dérober vos renseignements personnels. Ils seront ouverts pendant quelques semaines, puis ils disparaîtront. Les escrocs qui parviennent à leurs fins ont toujours des raisonnements auxquels les victimes potentielles ne demandent qu'à croire. Internet regorge aussi d'entreprises légitimes qui prétendent vous faire de bonnes affaires. Faites preuve d'intelligence et prenez le temps nécessaire pour faire des recherches. Parfois, il est tout simplement plus prudent de laisser passer une bonne affaire quand on ne peut pas la valider.

1.1.2 Hameçonnage

L'inondation-réseau (SPAM) désigne la transmission de grandes quantités de messages électroniques non sollicités. Tout comme dans le cas d'inondation-réseau, l'hameçonnage tente d'obtenir les informations personnelles d'un grand nombre d'individus en les dirigeant à leur insu vers une copie frauduleuse d'un site Web légitime. Ces messages font appel à la peur et à un sentiment d'urgence pour déclencher une réaction impulsive chez le lecteur. Parfois, ces criminels iront jusqu'à vous dire que vous risquez d'être victime d'un vol d'identité si vous ne suivez pas le lien prévu. Ils utiliseront vos renseignements personnels pour faire des profits financiers ou cacher leurs activités criminelles en se servant de votre bonne réputation. Vous pouvez les déjouer en ne sélectionnant jamais aucun des liens prévus et en supprimant immédiatement le message. Si vous avez encore des préoccupations, prenez l'annuaire téléphonique, appelez l'entreprise véritable et informez-vous.

Il n'y a pas de façon infaillible d'identifier un courriel ou un site Web d'hameçonnage. Lisez et comprenez les indicateurs contenus dans les tableaux 1.1 et 1.2. La présence d'un ou plusieurs indicateurs n'est pas nécessairement une preuve d'hameçonnage. Cela signifie seulement que vous devez faire preuve de plus de prudence.

Tableau 1.1 : Comparaison entre un courriel légitime et un courriel d'hameçonnage

Indicateur	**Légitime**	**Hameçonnage**
Salutation	Généralement personnalisée	Les salutations peuvent être étranges ou ne pas être personnalisées.
Orthographe	Ne contient généralement pas de fautes d'orthographe.	Il peut contenir des fautes d'orthographe.
Urgence	Vous laisse le temps de réfléchir à l'offre.	On utilise des déclarations dérangeantes ou emphatiques afin de provoquer une réaction impulsive et immédiate.
Lien intégré ou caché	Aucune tromperie.	Le lien visible semble légitime, mais la destination actuelle peut être frauduleuse.
Demande de renseignements personnels	Ces renseignements ne sont généralement pas demandés.	Ils peuvent être demandés ou on peut vous amener sur un site où on les demande.
Expéditeur	L'adresse électronique correspond à l'identité et au pays de l'expéditeur.	L'adresse électronique peut ne pas correspondre à l'identité ou au pays de l'expéditeur
Utilisation du courrier électronique par l'entreprise	Les organisations légitimes évitent de demander des renseignements personnels aux clients par courrier électronique.	On utilise le nom et la réputation d'une organisation légitime pour communiquer avec un grand nombre de consommateurs et des renseignements personnels peuvent être demandés.
Texte	Il est peu probable qu'il contienne du texte incompréhensible.	Il peut contenir du texte de camouflage composé au hasard.

Tableau 1.2 : Comparaison entre un site Web légitime et un site Web d'hameçonnage

Indicateur	Légitime	Hameçonnage
Indicateurs de la sécurité du site	Il y aura "https://" dans la barre d'adresse et un cadenas dans la barre d'état.	Il peut contenir des irrégularités ou être dépourvu de tout indicateur de la sécurité.
Fonctionnalité	Il est entièrement fonctionnel.	Il peut ne pas être pleinement fonctionnel ou peut mener vers certaines fonctionnalités du site légitime.
Demande de renseignements personnels	On n'y demandera aucun renseignement personnel qu'on possède déjà.	On demandera des renseignements personnels.
Nom de domaine	On utilisera et affichera le bon nom de domaine.	La barre d'adresse ou d'état peut découler d'une mystification ou contenir un nom de domaine qui semble similaire, ou ne pas avoir de barre d'adresse.
Erreur dans la barre d'état du navigateur	Il ne contiendra généralement pas d'erreur.	Il peut contenir des erreurs au moment de charger la page Web.
Procédure d'entrée en communication	Il ne sera accessible qu'avec un mot de passe valide.	Un nom de connexion et un mot de passe bidon peuvent fonctionner.

Internet est structuré autour d'un protocole numérique appelé protocole Internet ou IP. L'Internet utilise maintenant la version 4 qui se compose essentiellement de quatre chiffres qui vont de 0 à 255, séparés par un point. Par exemple, 198.103.98.139 est l'adresse IP du site Web de la GRC. Il est tout simplement plus difficile à retenir qu'une adresse comme « grc.ca ». Les criminels sont devenu très malins lorsqu'il s'agit de créer des noms de domaine qui ressemblent à s'y méprendre au site original. Ces noms de domaine peuvent être difficiles à remarquer si vous ne savez pas comment les lire. Dans la présente section, nous vous montrerons comment lire les noms de domaine.

On lit les noms de domaine de droite à gauche. Observez le nom de domaine en rouge dans l'adresse Web suivante :

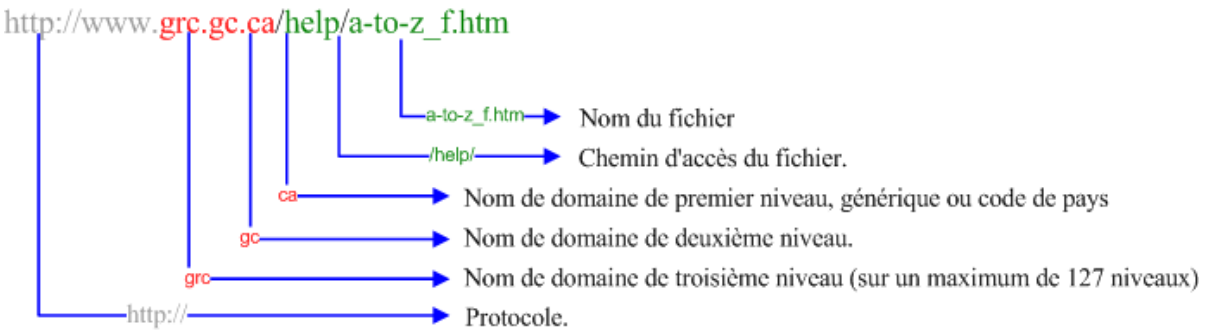


Figure 2 : Décomposition complète de l'adresse d'un site Web

Cette adresse dira à votre navigateur que vous cherchez la page Web (http://) a-to-z_f.htm, située dans le nom de domaine grc.gc.ca, en suivant le chemin d'accès /help/. Le caractères "www" à la suite de l'identificateur du protocole (http://) n'ont aucune signification dans nom du domaine. Votre navigateur enverra ce nom de domaine à un serveur spécial afin de vérifier si de tels noms de domaine de premier, deuxième et troisième niveau existent. Si c'est le cas, l'adresse Internet correspondante est le 198.103.98.139. Après avoir identifié le nom du domaine, vous pouvez trouver de plus amples renseignements à ce propos en utilisant le bottin Internet, ou le site "WHOIS" (se reporter à l'annexe 1). Ce site vous permettra de voir si les renseignements sur l'enregistrement du domaine sont incomplets ou s'il sont incompatible avec l'organisation correspondante.

Dans les escroqueries d'hameçonnage, on utilisera souvent des variations du nom légitime pour tromper l'utilisateur. Portez une attention particulière aux changements apportés dans l'emplacement des points ou des barres obliques et à la présence de caractères spéciaux et de variations dans le nom de domaine. Par exemple, si vous deviez remplacer la lettre minuscule « l » dans le site Web suivant, www.ghijklmnop.com, par le chiffre 1, vous seriez amené à vous rendre sur le site bidon suivant : www.ghijk1mnop.com Cette variation subtile passera inaperçue si l'internaute n'examine pas attentivement ce qu'il y a dans la barre d'adresse. Dans une autre variation d'une escroquerie d'hameçonnage, on changerait l'adresse du site Web en ajoutant un niveau subtil au nom de domaine. Cet ajout d'un niveau au nom d'un domaine changerait donc la position de tous les niveaux de nom de domaine suivants et tromperait l'utilisateur en l'amenant sur un site différent de celui auquel il s'attendait. Prenons le premier exemple : si l'on ajoute « .ca » devant le vrai nom de domaine, on se retrouve avec l'adresse www.ghijklmnop.ca.com, qui devient un nouveau nom de domaine totalement différent.

Il n'existe aucune façon infaillible de déterminer la légitimité d'un site web. Il y a toujours la possibilité qu'un logiciel espion infecte l'ordinateur de l'utilisateur ou son DNS. Vérifiez toujours l'existence de modèles inhabituels et de toute irrégularité dans l'adresse du site web ou sa page web. Si vous doutez de la légitimité du site, utilisez un nom de connexion et un mot de passe bidon aléatoire. Vous pourrez ainsi minimiser votre risque en observant si ce site accepte un nom de connexion et un mot de passe invalide. Il est important de toujours faire attention aux messages d'avertissement qui apparaissent sur l'écran. Vous devez bien lire et comprendre le message avant de sélectionner quoi que ce soit. Une des meilleures façons de minimiser les chances de devenir une victime d'hameçonnage est d'effacer les pourriels.

1.1.3 "Pharming" (Empoisonnement du système du nom de domaine)

La contamination, également connu sous le nom d'empoisonnement du système du nom de domaine (DNS), ressemble de près à l'hameçonnage, sauf qu'il n'y a pas de message électronique comme appât. Ce type d'escroquerie est causé par une corruption délibérée des ordinateurs spéciaux dans Internet qui dirigent l'utilisateur vers le site Web qu'il a demandé. Cela permet au pirate informatique de rediriger les utilisateurs d'un site Web légitime vers un site Web corrompu. Par conséquent, même si l'utilisateur tape le bon URL (adresse Web), le pirate informatique peut quand même rediriger l'utilisateur, à son insu et sans son consentement, vers un site bidon.

1.1.4 « SMiShing » ou hameçonnage par SMS

Le « SMiShing », qu'on appelle également hameçonnage par SMS (Short message service ou service d'envoi de messages courts), est une nouvelle menace émergente. Cette variante de l'escroquerie par hameçonnage fait appel à la technologie de la messagerie texte des téléphones cellulaires. Le propriétaire d'un téléphone cellulaire reçoit un message texte portant une adresse URL. Comme c'est le cas pour une escroquerie par hameçonnage, vous ne devez pas sélectionner l'adresse URL parce que vous pourriez télécharger un cheval de Troie. Ne prenez pas de risques et supprimez immédiatement ces messages texte de la boîte de message de votre téléphone cellulaire.

1.1.5 Hameçonnage vocal

Alors que les utilisateurs du Web se protègent de plus en plus contre l'hameçonnage, les fraudeurs s'adaptent. Ils fournissent dorénavant à leur victime un numéro de téléphone au lieu d'une adresse Internet dans le courriel hameçon qu'ils lui envoient. Il importe de savoir que ces numéros de téléphone utilisent la technologie peu coûteuse du protocole Voix sur IP (téléphonie Internet), qui donne au fraudeur la possibilité de reconnaître les frappes sur le clavier du téléphone et lui permet en outre d'être situé n'importe où dans le monde. Lorsque la personne appelle, un message enregistré lui demande d'entrer des renseignements numériques personnels au moyen du clavier de son téléphone aux fins de la vérification de son identité. Ne faites jamais confiance aux données d'identification de l'appelant sur votre téléphone

parce que celles-ci peuvent avoir été modifiées. Si vous êtes inquiet, communiquez avec l'organisation légitime en utilisant un numéro de téléphone que vous savez sûr. Par exemple, utilisez le numéro de téléphone figurant à l'endos de votre carte de crédit pour communiquer avec la société émettrice.

Les criminels peuvent également cibler d'autres pièces d'identification personnelle ou financière comme votre permis de conduire, votre passeport, votre carte bancaire et votre NIP, ainsi que votre carte d'assurance-maladie.

1.1.6 Prix gagnés

Un consommateur peut être l'objet d'une arnaque au prix gagné par courrier électronique, par téléphone ou par la poste. Il s'agit habituellement d'un avis informant le consommateur qu'il a gagné un prix. On fait croire à ce dernier que, pour pouvoir recevoir ou percevoir son prix, il doit payer des taxes ou des frais fictifs divers. Dans une variante de ce stratagème, on demande au consommateur d'acheter un produit ou un service pour recevoir le prix. Il est important que les consommateurs sachent qu'au Canada, quand on gagne un prix légitime, il n'y a pas de taxe ou de frais à payer pour l'obtenir.

Le stratagème du recouvrement d'argent est une variante de l'arnaque au prix gagné. Si vous avez été victime d'une telle escroquerie, il se peut fort bien que vous receviez un courriel ou un téléphone d'une personne qui vous promettra de recouvrer votre prix ou votre argent moyennant une petite somme. Cette personne se fera probablement passer pour un agent de police, un employé du ministère du Revenu, un agent de douane ou un employé d'une entreprise légitime.

1.1.7 Ventes aux enchères frauduleuses

Les ventes aux enchères en direct consistent en une sélection d'articles à vendre qui peuvent être achetés en se portant acheteur des articles. Les ventes aux enchères frauduleuses comprennent des fraudes telles que l'information trompeuse sur un article, la non-livraison de biens et de services et le non-paiement de biens livrés.

De nombreux consommateurs se font souvent arnaqués quand ils font affaire avec des maisons de vente aux enchères en ligne parce qu'ils ne connaissent pas ou encore ne suivent pas les bonnes procédures d'achat et de vente. La plupart des maisons de vente aux enchères en ligne offrent un guide d'apprentissage et des conseils de sécurité en ligne qui renferment des renseignements portant par exemple sur les systèmes et les modalités appropriés de paiement en ligne et sur les précautions à prendre dans ce domaine. Ces systèmes de paiement sont très sûrs et, lorsqu'ils sont utilisés, ils peuvent réduire au minimum les risques d'être victime de fraude et ils peuvent en outre offrir une protection des achats. Ne vous laissez pas convaincre de passer à d'autres modes de paiement en envoyant de l'argent ou des mandats ou en effectuant un transfert de fonds. La façon la plus sûre consiste à payer avec votre carte de crédit au moyen du système adéquat de paiement en ligne.

On recourt habituellement à des services d'entiercement quand des articles à prix élevé comme des automobiles, des bijoux et du matériel informatique spécialisé sont achetés sur des sites de vente aux enchères en ligne. Le tiers ou dépositaire offre un service consistant à retenir le paiement de l'acheteur jusqu'à ce qu'il soit avisé que les marchandises ou les services ont été livrés. Il verse alors le paiement au vendeur ou au fournisseur.

Malheureusement, les criminels créent des sites de services d'entiercement frauduleux en piratant des sites légitimes ou en inventant des entités entièrement fictives pour s'approprier l'argent des victimes qui s'en remettent à eux en toute confiance. Faites également des recherches pour vérifier la crédibilité du service d'entiercement approuvé par le fournisseur de services de vente aux enchères en ligne. Signalez sans attendre toute activité suspecte au service de sécurité de la maison de vente aux enchères en ligne.

1.1.8 Logiciel malveillant (maliciel)

Le logiciel malveillant est conçu pour altérer le comportement d'un ordinateur à l'insu de son utilisateur. Il se présente sous différentes formes, par exemple des virus, des vers, des programmes de cheval de Troie, des espiogiciels et des publiciels. Les ordinateurs peuvent être infectés par des logiciels malveillants quand leur utilisateur ouvre un courriel, accède à un site Web, utilise des supports contaminés ou télécharge des programmes infectés tels que des jeux. Un code malveillant peut s'emparer des renseignements personnels à partir de votre ordinateur ou de votre clavier et les transmettre à une autre personne. Comme les renseignements peuvent être interceptés dans leur forme déchiffrée à partir de votre ordinateur, vous ne devriez pas vous fier uniquement au chiffrement.

Protégez donc adéquatement votre ordinateur en tenant votre système d'exploitation et vos progiciels à jour. Utilisez également des versions à jour de logiciels comme des antivirus, des pare-feux, des anti-espiogiciels et des anti-publiciels pour protéger votre ordinateur. Si vous ne mettez pas à jour vos progiciels, vous augmentez les risques d'atteinte à l'intégrité de votre ordinateur. Sachez qu'un code malveillant peut être camouflé en n'importe quel genre de fichier informatique et qu'un appareil bien protégé peut quand même être vulnérable. Méfiez-vous des logiciels gratuits.

1.1.9 Communications électroniques

Toute information qui voyage par la voie des airs risquerait d'être interceptée. Comme pratique sécuritaire, évitez de transmettre ou de stocker des renseignements personnels sous forme de données électroniques ou vocales lorsque vous utilisez les voies suivantes : téléphones cellulaires, combinés téléphoniques portables, courriels non chiffrés, messagerie instantanée non chiffrée, site de bavardage, forums, pages Web et connexions à un réseau sans fil.

Au cours des dernières années, les avantages des réseaux sans fil (Wi-Fi) ont fait grimper leur popularité de façon spectaculaire auprès des consommateurs. De nouveaux produits intégrant des capacités Wi-Fi apparaissent sur le marché. Pour éviter d'exposer accidentellement vos renseignements, débranchez ou désactivez votre carte Wi-Fi lorsque vous ne l'utilisez pas, utilisez uniquement le mode Wi-Fi pour des activités de nature non délicate, comme la navigation sur le Net, désactivez la fonction automatique de recherche de points d'accès ou d'ouverture de session, vérifiez vos paramètres concernant le partage de fichiers informatiques et utilisez un mot de passe difficile à trouver. Avant d'ouvrir une session Wi-Fi, utilisez une combinaison composée d'un nom d'utilisateur et d'un mot de passe invalides. Ne vous servez pas de la connexion si vous êtes capable d'ouvrir une session avec de l'information invalide concernant votre compte.

Le problème avec les réseaux sans fil, c'est qu'ils peuvent être l'objet de tentatives d'hameçonnage au point d'accès sans fil (« Evil Twin » ou « Wi-phishing »). Dans ce cas, un point d'accès légitime est piraté et les utilisateurs, qui ne se doutent de rien, sont redirigés vers un point d'accès illégitime. Les données et les fichiers de votre portable ou de votre appareil sans fil peuvent donc être dérobés par l'attaquant « Evil Twin ».

Tableau 2 : Conseils relatifs aux réseaux sans fil (Wi-Fi)

Pratique	**Conseil**
Utiliser un point d'accès ouvert ou non sécurisé.	Toute l'information que vous envoyez ou que vous recevez est transmise sous forme de signal radio et il peut être interceptée par tout le monde et par le responsable du point d'accès. Cela comprend vos renseignements personnels contenus dans les paramètres de votre navigateur.
Utiliser un point d'accès sécurisé.	Du point de vue technique, l'administrateur du point d'accès est capable de contrôler votre information, mais les autres ne le peuvent pas. Le protocole WEP est reconnu comme étant plus faible; utilisez donc le WPA, qui est plus sûr.
Utiliser une session sécurisée (https:// pour une session d'opérations bancaires en ligne ou de commerce électronique par exemple) dans un point d'accès sécurisé.	Il est toujours préférable d'utiliser une connexion Internet régulière pour des sessions de ce type. Si le point d'accès est légitime, vos données seront entièrement chiffrées pour passer de votre ordinateur au site sécurisé.
Utiliser et configurer un routeur ou appareil Wi-Fi domestique.	Sachez que des criminels peuvent scruter votre quartier pour trouver un accès à votre réseau ou à vos ordinateurs. - Évitez d'acheter du matériel à prix d'aubaine. - Songez à éteindre ou à débrancher votre matériel, y compris vos routeurs, lorsque vous ne l'utilisez pas. - Utilisez un SSID (identificateur d'ensemble de services) différent de celui qui est fourni par défaut et ne le diffusez pas. - Utilisez une clé de chiffrement WPA au niveau maximal existant. - Changez le canal de votre appareil pour en choisir un autre que celui qui est déterminé par défaut. - N'utilisez pas la plage d'adresses IP par défaut ou le DHCP. - Envisagez le filtrage des adresses MAC.

1.1.10 Ordinateurs accessibles au public

Les bibliothèques publiques, les cafés Internet, les campus, les hôtels et même les terrains de camping mettent des ordinateurs à la disposition du public. Évitez d'utiliser des ordinateurs accessibles au public pour effectuer des opérations bancaires en ligne, pour envoyer des courriels contenant des renseignements personnels ou pour payer des achats en ligne au moyen de vos cartes de paiement. Si vous devez vous servir de ces ordinateurs, exécutez la procédure de fin de traitement pour sortir de vos comptes en ligne, videz la mémoire cache de votre navigateur, supprimez les témoins, supprimez l'historique et fermez le navigateur. Pour obtenir des instructions applicables à la marque et à la version de votre navigateur, rendez-vous sur le site Web du concepteur et recherchez les expressions suivantes : « vider le cache du navigateur », « supprimer les témoins » et « supprimer l'historique du navigateur ».

Votre bon sens peut également vous aider à réduire les risques que vos renseignements personnels soient dérobés quand vous utilisez un ordinateur accessible au public. Des trucs simples, comme ne pas laisser l'ordinateur sans surveillance ou dissimuler son mot de passe au moment de la saisie, vous aideront à réduire les risques. Soulignons en outre que les ordinateurs accessibles au public sont habituellement sûrs, mais il est impossible pour l'utilisateur d'en être tout à fait certain.

1.1.11 Sites de réseautage social

Un réseau social en ligne consiste en des applications Internet qui créent une structure sociale en ligne facilitant la connectivité entre les individus. Les réseaux sociaux peuvent également indiquer la nature de la relation que des personnes entretiennent entre elles. Les réseaux sociaux en ligne offrent des services tels que la messagerie instantanée, et ils peuvent permettre aux utilisateurs de tenir des blogues ou des fichiers messagerie. Un blogue ou blog, terme né de la contraction de weblog (carnet de bord sur le Web), est la publication en ligne d'articles périodiques portant généralement sur un seul sujet. Mais depuis peu, les blogues sont utilisés comme un journal personnel sur le Web et contiennent du texte, des images et des liens vers d'autres blogues ou d'autres pages Web.

Lorsque vous affichez des renseignements à votre sujet sur le Net, vous devriez réduire au minimum les risques auxquels vos renseignements personnels sont exposés. On recommande, lorsque c'est possible, de ne pas entrer de renseignements tels que votre nom complet, votre date de naissance, votre adresse résidentielle, votre numéro de téléphone, votre numéro d'assurance sociale et tout renseignement qui pourrait présenter de l'intérêt pour un prédateur financier ou un prédateur sexuel. Veuillez également prendre note que l'affichage de vos intérêts personnels et de vos passe-temps dans votre profil ou votre blogue pourrait servir de tremplin pour l'ingénierie sociale. Lisez et comprenez bien les dispositions de l'entente et la politique de protection des renseignements personnels pour vous assurer que vos renseignements seront correctement utilisés et stockés. Prenez connaissance des paramètres de sécurité par défaut du site de réseautage social. Certains de ces paramètres implicites permettront aux autres de visualiser vos renseignements personnels.

Lorsque vous utilisez la technologie amusante et utile des réseaux sociaux en ligne, suivez les dix étapes suivantes en matière de sécurité pour réduire au minimum les risques d'être victime d'une usurpation d'identité.

Tableau 3 : Les dix étapes à suivre pour le réseautage social en ligne sans risques

Étape 1	Faites les recherches qui s'imposent. Renseignez-vous avec soin sur le réseau social en ligne auquel vous voulez adhérer. N'utilisez que les services en ligne bien connus.
Étape 2	Une fois que vous avez choisi un service, lisez attentivement et comprenez clairement les modalités d'utilisation.
Étape 3	Lisez attentivement et comprenez clairement la politique du site sur la protection des renseignements personnels. Évitez d'utiliser les services qui partageront vos renseignements avec d'autres entreprises.
Étape 4	Ne vous attendez jamais à une protection parfaite de vos renseignements personnels! Créez votre compte sans fournir de renseignements personnels délicats. Ne fournissez jamais de renseignements délicats valides comme votre date de naissance, votre nom au complet, votre numéro d'assurance sociale ou votre adresse.
Étape 5	Protégez le profil de votre compte en établissant les paramètres de sécurité les plus élevés et les plus restrictifs.
Étape 6	Créez votre profil. Pour chaque élément d'information que vous donnez, posez-vous la question suivante : « Un prédateur financier ou sexuel pourrait-il tirer parti de cette information? »
Étape 7	Vous contrôlez votre environnement en ligne. Ne permettez pas à des étrangers d'accéder à votre profil.
Étape 8	Protégez vos amis. Faites attention à ce que vous affichez sur Internet à leur sujet.
Étape 9	Surveillez dans votre page les renseignements personnels donnés par des amis dans leurs messages. Surveillez également vos propres renseignements personnels qui s'afficheront dans les pages de vos amis. Un simple commentaire ou une photographie peut révéler votre date de naissance ou donner des renseignements qui pourraient être utiles aux prédateurs.
Étape 10	Soyez créatif, soyez prudent et amusez-vous!

1.1.12 Services de rencontre

Un service de rencontre en ligne permet à des personnes et à des groupes de se rencontrer sur le Net dans l'espoir d'établir une relation amoureuse. Les escrocs se servent des services de rencontre en ligne. Ils donnent de faux renseignements dans leurs profils en ligne, de même que dans leurs communications avec leurs victimes potentielles. Ils se font souvent passer pour des étrangers. Ils gagnent votre confiance en envoyant des messages touchants par courriel, par téléphone et par messagerie instantanée. Quand vous vous sentirez à l'aise dans cette nouvelle relation, la personne vous demandera si elle peut vous rendre visite dans le but peut-être de vous demander en mariage, de fuir son pays ou de finalement vous rencontrer. Elle vous demandera fort probablement de payer le prix du voyage en avion, les frais de passeport et d'autres coûts liés au voyage. Quand vous aurez envoyé l'argent nécessaire à cette personne, il y a fort à parier que vous ne la rencontriez jamais ou que vous n'entendiez plus jamais parler d'elle. Vous ne récupérerez pas non plus votre argent.

Souvenez-vous qu'avec le temps et la pratique, les arnaqueurs qui parviennent à leurs fins deviennent très forts quand il s'agit de jouer avec les sentiments des autres. Rappelez-vous donc toujours que la personne que vous rencontrez en ligne pourrait ne pas être celle qu'elle prétend être. Même si la personne a une photo dans son profil et semble très sincère, vous pourriez avoir affaire à une personne qui utilise une fausse identité pour s'emparer de votre argent. Signalez sans tarder toute activité suspecte à www.sedde.ca ou à PhoneBusters au 1 (888) 495-8501 ou au www.phonebusters.com.

1.1.13 Prêts avec paiement de frais à l'avance

Des prêts moyennant des frais payables d'avance sont couramment offerts dans les annonces classées des journaux, des revues et des tabloïdes. On en trouve également dans Internet. Ces annonces garantissent un prêt sans égard aux antécédents du demandeur en matière de crédit, mais ce dernier doit payer des frais à l'avance. Il va sans dire que le demandeur n'obtient jamais le prêt et qu'il perd la somme payée d'avance. Les sociétés de financement légitimes ne demandent jamais le paiement de frais à l'avance. Cette pratique est illégale au Canada et aux États-Unis.

N'acceptez pas de payer des frais pour obtenir un prêt. Ne croyez pas les promesses selon lesquelles votre prêt sera automatiquement accepté, surtout si votre cote de crédit n'est pas bonne ou si vous n'avez pas d'antécédents en matière de crédit. En cas de doute, consultez des spécialistes d'un établissement financier légitime connu. Signalez sans tarder une activité suspecte à www.sedde.ca ou à Phonebusters, au 1 (888) 495-8501 ou au www.phonebusters.com,et le département de sécurité de l'établissement financier concerné.

1.1.14 Escroqueries liées à des offres d'emploi

Faites attention aux escroqueries liées à des offres d'emploi lorsque vous cherchez du travail. Il est important que votre résumé en direct anonyme et laisser seulement un adresse électronique comme moyen de communication. Ne donne pas trop d'information personnel à un nouveau employeur. Cela comprend le fait de donner trop d'information à un employeur potentiel ou à un nouvel employeur. Ne divulguez pas votre numéro de compte de banque ou de carte de crédit, ni le nom d'utilisateur et le mot de passe de vos comptes en direct. Il n'est pas nécessaire de fournir son numéro d'assurance sociale (NAS) lorsqu'on remplit une demande d'emploi. L'employeur n'en aura besoin que lorsqu'il vous aura embauché. Soyez prudent lorsque vous faites une demande d'emploi liée à une offre d'emploi trouvée dans les annonces classées, dans les journaux, sur un babillard ou dans Internet qui concerne l'envoi de colis, le transferts de fonds, le virement électronique de fonds ou à des emplois de télémarketing bien payés. Vous pouvez finir par participer à des activités criminelles. Signalez les activités suspectes.

1.1.15 Fausses organisations caritatives

Les fausses organisations caritatives exploitent la nature généreuse d'une personne pour les tromper et les amener à faire un don. Elles auront souvent recours à des histoires touchantes et patriotiques. Ces histoires peuvent porter principalement sur des événements catastrophiques récents. Les pseudo-organisations caritatives porteront souvent un nom qui ressemble à celui d'une organisation caritative légitime, auquel on a ajouté un mot ou dont on a modifié un mot. Vous pouvez faire plusieurs choses pour éviter de devenir une victime de fausses organisations caritatives. D'abord, soyez prudent face aux courriels ou aux appels que vous recevez, car ils pourraient provenir d'une organisation qui se fait passer pour une organisation caritative légitime. De plus, soyez prudent avec les noms d'organisations caritatives qui se ressemblent. En cas de doute sur la légitimité d'un site, consultez le site Web officiel de l'organisation ou appelez cette organisation. N'utilisez pas l'adresse Web et le numéro de téléphone fournis par l'organisation caritative en question.

1.1.16 Escroqueries 419 ou lettres d'Afrique occidentale

L'escroquerie 419, ou lettres frauduleuses provenant d'Afrique occidentale, également connue sous le nom de lettres frauduleuses sur les paiements de frais à l'avance, désigne des lettres envoyées à des personnes ou à des entreprises dans lesquelles on leur demande d'effectuer un transfert de fonds étrangers en échange de la remise d'un pourcentage de la somme transférée. Ces lettres, envoyées par courrier électronique, par courrier ou par télécopieur, insistent sur le fait que la confiance et l'honnêteté sont des aspects importants de cette opération commerciale confidentielle. L'auteur de la lettre se présentera vraisemblablement comme un médecin, un représentant important d'une entreprise, généralement la Nigerian National Petroleum Corporation ou une personne qui fait partie du gouvernement du Nigéria, d'un autre pays africain ou de militaires. Le même scénario peut s'appliquer à d'autres organisations et pays étrangers.

Si la victime communique avec l'auteur par courrier électronique, courrier ou téléphone, on lui demandera d'assumer diverses dépenses, comme des pots-de-vin, des taxes, des frais d'inscription et des frais de mandataire payables à l'avance. Cela peut se poursuivre pendant longtemps et être conditionnel à l'exécution du transfert de fonds. Évidemment, la victime ne recevra jamais d'argent. Ne répondez pas à ce type de lettre. Envoyez-en une copie à Phonebusters au wafl@phonebusters.com ou par télécopieur au 1(888) 654-9426.

1.2 Public, amis et connaissances

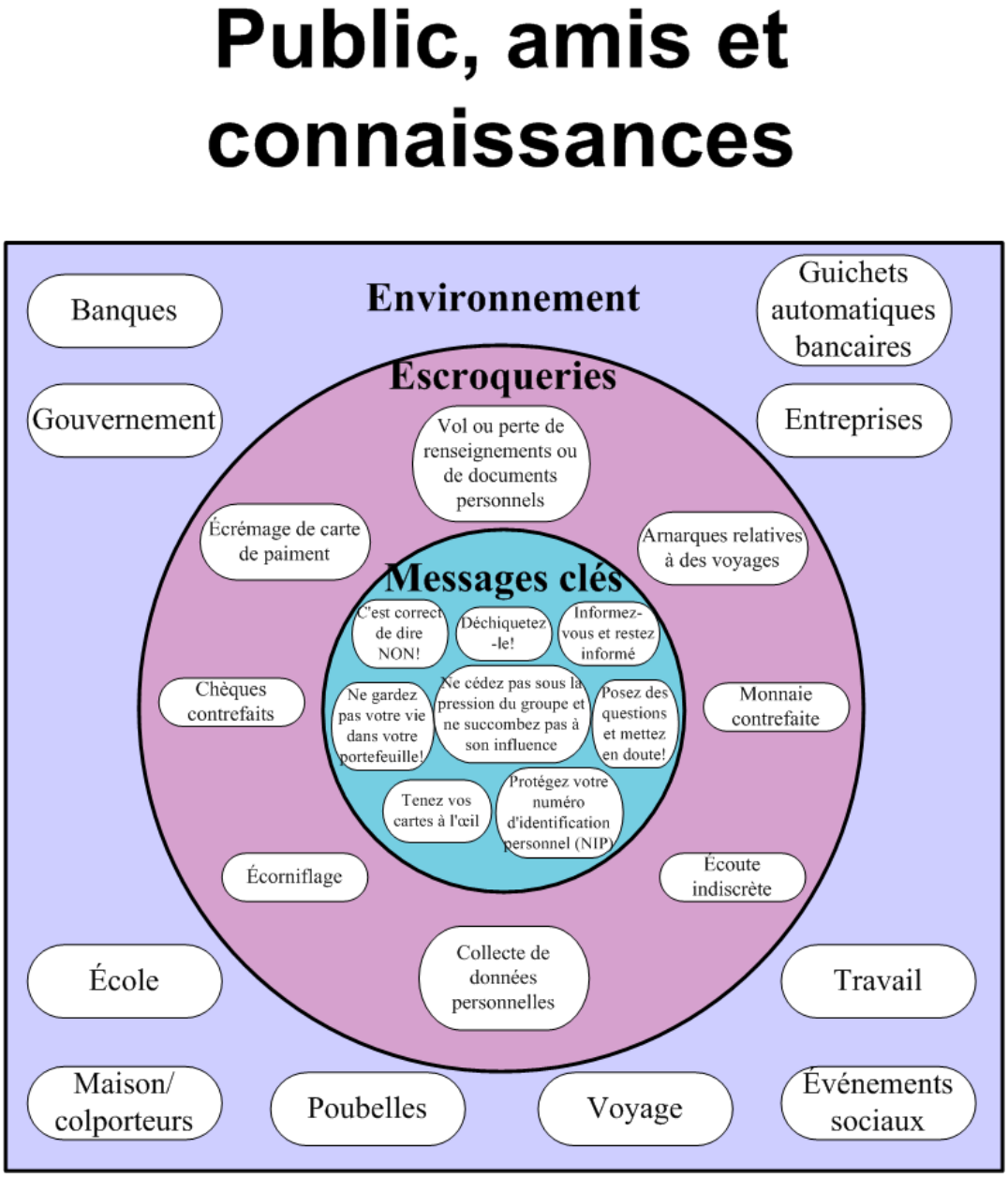


Figure 3 : Messages clés pour éviter les escroqueries publiques qu'on trouve dans divers environnements

Vous menez une vie active et voyagez constamment entre la maison, l'école et le travail. Ces activités vous mettent en contact avec un grand nombre de personnes et d'organisations. Dans la présente section, on traite d'escroqueries telles que le vol de portefeuille, écrémage de carte de paiement, la monnaie contrefaite, la fouille de poubelles et l'écoute clandestine.

1.2.1 Vol ou perte de renseignements ou de documents personnels

Ne gardez pas votre vie dans votre portefeuille ou dans votre voiture. Ne portez avec vous que les documents dont vous avez besoin dans vos activités courantes. Ne transportez pas sur vous votre carte d'assurance sociale, votre certificat de naissance, votre passeport ou tout autre document contenant le même genre de renseignements. Les documents comme les vieilles cartes d'hôpital peuvent contenir plus de renseignements que vous ne le pensez. Examinez donc le contenu de votre sac à main ou de votre portefeuille. Rangez ces documents et ces cartes dans un endroit sûr, comme une armoire ou un tiroir fermé à clé ou un coffre-fort. Déchiquetez les documents inutiles.

1.2.2 Chèques contrefaits

Les chèques contrefaits sont des chèques modifiés ou des chèques fabriqués. Ils sont couramment associés à des occasions « trop belles pour être vraies ». On les retrouve dans les arnaques au prix gagné et aux frais d'emprunt payables à l'avance, dans les loteries frauduleuses, dans les arnaques dans le domaine de l'emploi et dans la vente aux enchères en ligne. Dans un scénario typique, la victime potentielle se voit offrir, en échange de biens ou de services, un chèque que l'acheteur aurait déjà en sa possession. Le montant du chèque est supérieur à la somme due et la victime est priée d'accepter le chèque contrefait et de rembourser la différence. Cette fraude mise sur les délais de traitement des chèques. La banque tiendra la victime responsable du chèque contrefait. N'acceptez jamais de chèque d'un montant plus élevé que la valeur de l'opération et attendez toujours que le chèque soit entièrement compensé avant de livrer les biens ou de fournir les services. Si ça semble trop beau pour être vrai, c'est que ça l'est tout simplement. Caveat Emptor! (Acheteurs, soyez vigilants!)

1.2.3 Monnaie contrefaite

Les billets de banque canadiens sont émis par la Banque du Canada. La Banque a la charge du remplacement des billets de banque authentiques qui sont abîmés, mais elle n'assume pas la responsabilité de rembourser les victimes de billets de banque contrefaits. Faire une habitude de régulièrement vérifier l'authenticité les billets de banque est la meilleure façon de se protéger.

Les billets de banque canadiens comportent plusieurs éléments de sécurité qu'y sont facile et rapide à utiliser. La Banque du Canada fait savoir que vous devriez toujours vérifier l'authenticité de votre billet de banque en le touchant, en l'inclinant, en l'examinant et en le regardant à contre-jour. Pour obtenir de l'information sur la façon de vérifier la légitimité d'un billet de banque, veuillez consulter le site Web de la Banque du Canada à l'adresse suivante: http://www.bankofcanada.ca/fr/banknotes/counterfeit/security_features.html.

En vue de réduire au minimum les risques de posséder un billet de banque contrefait, prenez le temps de vérifier la plupart de ces éléments. Vérifiez plus d'un élément de sécurité au cours d'une transaction afin de déterminer s'il est légitime. Vous pouvez demander au marchand de vous donner un billet de banque différent, si vous vous sentez mal à l'aise en raison de celui qu'il vous a remis.

Si vous recevez un billet contrefait ou que vous soupçonnez être contrefait, arrêtez la transaction et demandez un billet de banque différent. Vous avez la responsabilité de remettre à une autorité compétente, telle que la police locale ou un caissier de banque, les billets contrefaits provenant d'un guichet automatique bancaire (GAB) de la banque. On ne vous remboursera pas votre billet de banque contrefait. Et surtout, vous ne devriez pas essayer de le donner à quelqu'un en sachant qu'il est contrefait. Vous pourriez faire face à des accusations au criminel.

1.2.4 Collecte de données personnelles

Il est important d'être prudent lorsqu'on remplit une formule d'inscription au tirage de prix dans les centres commerciaux, les expositions sportives et les conventions. Vos renseignements personnels peuvent être utilisés par la suite par des tiers qui communiquent avec vous par téléphone ou vous envoient des pourriels afin de vous amener, par l'escroquerie, à leur donner plus de renseignements personnels ou accéder vos comptes bancaires. Certaines organisations frauduleuses analyseront même l'écriture qui figure sur le formulaire d'inscription afin de trouver des victimes potentielles pour leurs escroqueries.

1.2.5 Arnaques relatives à des voyages

Les sollicitations concernant des vacances affluent à longueur d'année, mais elles sont généralement plus fréquentes au cours de la saison des voyages. Accueillez toujours avec une bonne dose de scepticisme ces sollicitations, que vous les receviez par courriel, par télécopieur ou par téléphone. Surtout lorsqu'une entreprise que vous ne connaissez pas vous félicite d'avoir gagné un séjour gratuit ou bon marché dans un endroit de villégiature ou à bord d'une croisière. Il est fort probable que ce genre de sollicitation soit une arnaque. Ces entreprises de voyages illégitimes vous demanderont le numéro de votre carte de crédit et certains renseignements personnels, ce qui pourrait porter atteinte à votre identité et à vos finances. Un autre risque, c'est la pratique trompeuse qu'utilisent les agences de voyage malhonnêtes pour attirer une victime vers une lointaine destination et lui exiger des frais supplémentaires pour des caractéristiques et des services qui étaient censés être inclus dans le forfait voyage initial. Vos vacances de rêve deviennent alors une expérience des plus éprouvantes. Il est plus prudent de faire affaire avec des agents de voyage bien établis et dignes de confiance.

Vous devez demeurer à l'affût de la fraude quand vous êtes en vacances ou en voyage. Si vous voyagez à l'étranger, planifiez soigneusement votre voyage en visitant le site d'information sur les voyages d'Affaires étrangères et Commerce international à l'adresse http://www.voyage.gc.ca. Un peu de prévention facilite bien des choses. N'oubliez pas d'emporter avec vous un exemplaire de la brochure « Bon Voyage, mais ... ».

Portez une attention particulière aux documents qui contiennent vos renseignements personnels. N'apportez que les documents nécessaires et portez-les sur vous en toutes circonstances. Ne laissez jamais vos renseignements personnels sans surveillance dans une chambre d'hôtel ou à tout autre endroit.

1.2.6 Écrémage de carte de paiement

Ne perdez jamais de vue votre carte de crédit ou de débit lorsque vous l'utilisez pour faire un achat. Ne permettez pas à un commis de partir avec votre carte. Dans cette combine qu'on appelle le clonage de cartes, l'employé glisse à votre insu votre carte dans un petit appareil qui lit et emmagasine l'information contenue dans la bande magnétique de votre carte. Cette information peut être utilisée pour dupliquer votre carte. Assurez-vous de cacher votre NIP avec votre main lorsque vous le saisissez sur le clavier. Vous risquez ainsi moins qu'une personne qui vous surveille lorgne votre NIP ou qu'une caméra cachée l'enregistre.

Sur la plage de signature de votre carte de crédit ou à proximité de celle-ci se trouve un code de trois chiffres appelé le code de vérification de carte ou la valeur de vérification de carte. Ce code permet aux commerçants de confirmer que le consommateur a la carte en sa possession quand il effectue une opération sur Internet ou par téléphone. Il s'agit d'un autre élément d'information que vous ne devez dévoiler à personne, sauf si vous effectuez ce genre d'opération ou quand vous communiquez avec la société qui a émis votre carte de crédit.

Dans une variante de cette arnaque, apparue récemment, des employés malhonnêtes ou des fraudeurs habiles remplacent par un autre le clavier numérique du terminal de paiement. Bien que ce clavier puisse sembler identique à première vue, il a été modifié par l'ajout d'un deuxième mécanisme de lecture dans la fente de lecture de la carte et d'une mémoire connectée au clavier. Les criminels peuvent ainsi stocker les données de la bande magnétique de votre carte et votre NIP. Les données sont par la suite téléchargées, des cartes frauduleuses sont fabriquées et les criminels sont prêts à faire du magasinage avec un clone de votre carte et votre NIP.

Tableau 4 : Indices de trafiquage du terminal de paiement

Indice	**Légitime**	**Contrefait**
Boîtier du terminal	Le boîtier ne porte aucun signe d'altération, les pièces s'emboîtent parfaitement sans laisser de fissures ou de joints ouverts. L'endos du boîtier est fermé au moyen de rivets permanents ou de boulons exclusifs (spéciaux) ou le dispositif de fermeture est dissimulé à l'intérieur du boîtier. Des fils ne sont jamais visibles par les orifices de ventilation à l'endos.	Le boîtier peut présenter des signes d'altération, des fissures ou des joints ouverts, ou encore peut être mal assemblé. L'endos du boîtier peut être fermé au moyen de boulons ordinaires. Des fils peuvent être visibles par les orifices de ventilation.
Mécanisme de lecture	Seule une tête de lecture est visible par la fente d'insertion de la carte du terminal de paiement.	Deux têtes de lecture ou des signes d'altération peuvent être visibles par la fente d'insertion de la carte.

Communiquez avec le service de police local lorsque vous avez l'impression qu'un terminal de paiement a été contrefait. Sachez également que les dispositifs de paiement par carte des pompes à essence peuvent à l'occasion être trafiqués eux aussi. Privilégiez l'utilisation de cartes de crédit plutôt que de cartes de débit dans ces dispositifs parce qu'elles vous offrent une meilleure protection.

1.2.7 Écorniflage et écoute indiscrète

Il est vrai que par soi-même, ces deux activités ne sont pas des fraudes, mais elles sont utilisées en conjonction avec une multitude de fraudes. L'écorniflage et l'écoute indiscrète sont utilisés pour collectionner de l'information et de la documentation personnelle telles que des codes d'accès d'édifice, des combinaisons d'alarme de sécurité, des NIPs, des noms d'utilisateur/mots de passe et de l'information de cartes de crédit. Il est important de toujours cacher avec votre corps ou votre main les claviers numériques sur lesquels vous rentrez de l'information personnelle pour minimiser le risque que quelqu'un vous observe pour capturer votre information. Il est aussi important de faire certain que personne ne puisse vous entendre lorsque vous devez donner cette information à quelqu'un au téléphone. N'utilisez pas des réseaux sans fils pour communiquer cette information.

1.3 Téléphone

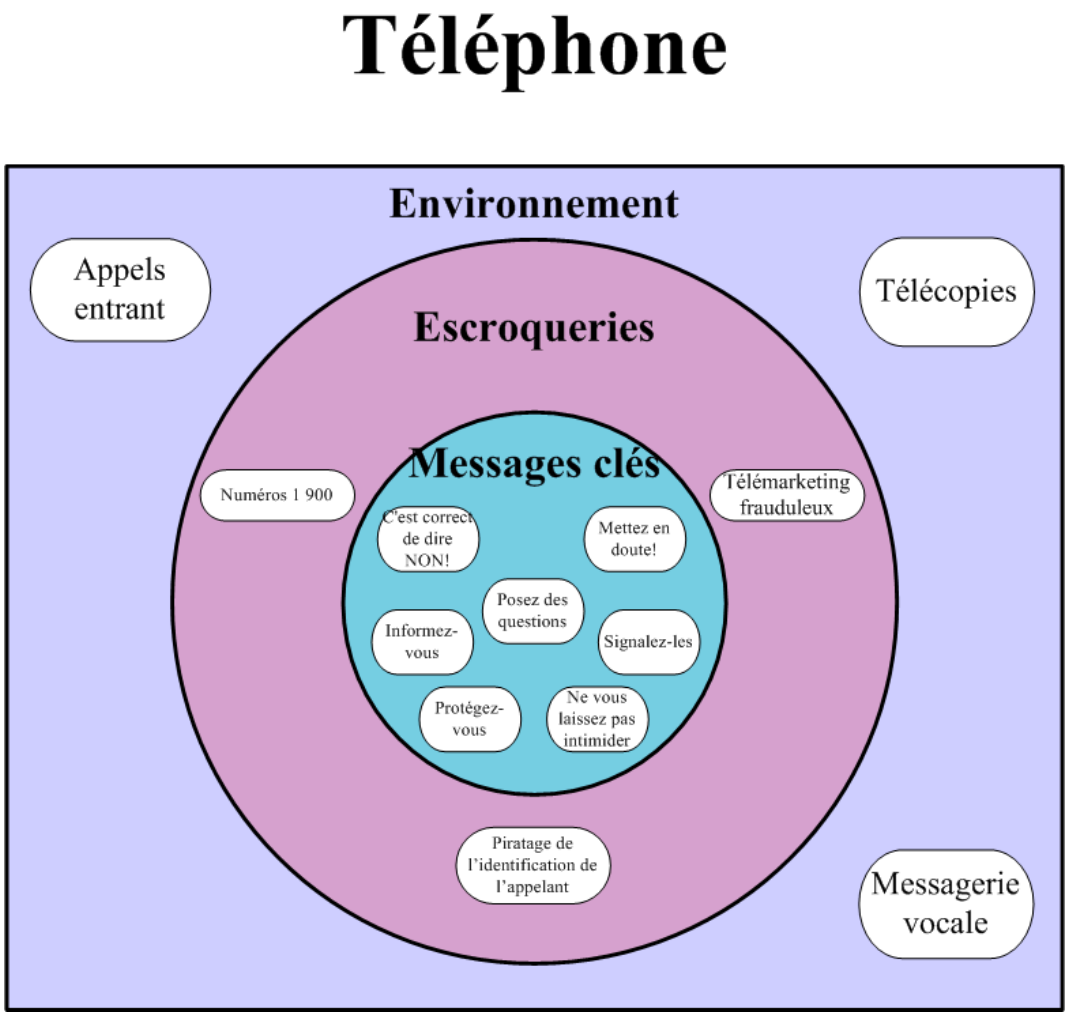


Figure 4 : Messages clés pour vous aider à éviter les escroqueries téléphoniques qu'on trouve dans divers environnements

L'identification de l'appelant est un service qui permet d'identifier le numéro et le nom de la personne ou de l'organisation qui appelle. Il est à noter qu'il ne faut pas complètement se fier à ce service pour connaître l'identité de l'appelant. Il existe d'autres services qui permettent le piratage de l'identification de l'appelant. Ceci est fait en falsifiant le numéro et le nom qui apparaissent sur l'écran. Les fraudeurs utilisent cette technologie pour vous truquer à partager votre information personnelle et financière. Rappelez-vous de ne jamais donner cette information lorsque quelqu'un vous appelle.

1.3.1 Télémarketing frauduleux

Le télémarketing permet à des entreprises légitimes d'annoncer et de vendre leurs produits et leurs services par téléphone. Malheureusement, des criminels utilisent aussi les mêmes techniques de télémarketing pour commettre des fraudes au détriment des gens. Vous devriez donc être prudent lorsque vous recevez un appel dont le but est de vous parler d'une promotion stupéfiante ou de prix à gagner. Méfiez-vous également des organisations que vous ne connaissez pas et ne vous laissez pas avoir par leurs promesses extravagantes. N'ayez pas peur de dire non et de raccrocher. Souvenez-vous qu'il ne faut pas divulguer de renseignements personnels ou financiers au cours d'un appel entrant. L'erreur que font

bien souvent les consommateurs est d'associer les numéros 1-800 à des entreprises de télémarketing légitimes. Ce n'est pas toujours le cas. Ne vous fiez donc pas à ce signe pour distinguer les entreprises de télémarketing légitimes des entreprises frauduleuses. Si vous désirez signaler des appels téléphoniques suspects, communiquez avec PhoneBusters au 1(888) 495-8501 ou au www.phonebusters.com.

Tableau 5 : Comparaison entre le marketing de masse légitime et frauduleux

Indicateurs	**Légitime**	**Frauduleux**
Enthousiasme	L'appelant peut être très enthousiaste.	L'appelant est plus excité que vous.
Gentillesse	L'appelant peut agir avec une gentillesse exagérée.	On veut créer un contact personnel pour éventuellement miser dessus par la suite.
Pression	Cela peut être une technique légitime pour conclure une affaire, mais on n'aura pas normalement recours à la violence verbale.	On veut vous forcer à fournir ce qu'on vous demande et on pourrait avoir recours à la violence verbale.
Urgence	Vous pouvez prendre le temps de réfléchir à l'offre.	On exercera une pression afin de vous faire prendre une décision si vous n'agissez pas maintenant. On peut exiger que vous répondiez immédiatement.
Empressement à fournir des références complètes	Ce n'est généralement pas un problème et on fournira les références complète.	On peut rechigner davantage ou consentir à fournir de l'information limitée, telle qu'un numéro de téléphone.
Mode de paiement	De nombreuses options sont généralement disponibles.	On se limite aux messageries et aux services télégraphiques.
Prix	Il a une valeur marchande.	Le prix est bas de manière déraisonnable et il y a une explication non réaliste pour ce prix.
Avantages	Les avantages et la valeur des primes sont réalistes et permettent la réalisation d'un profit.	La valeur des primes ou des avantages n'est pas raisonnable, car elle sont très élevée et les explications fournies ne sont pas réalistes. C'est trop beau pour être vrai.
Offres de crédit	Elles sont généralement fixées selon votre cote de solvabilité.	On vous fait des offres sans tenir compte de votre cote de solvabilité.
Sondages	Votre information servira aux fins prévues.	Votre information peut servir à des fins criminelles.
Explications	Lorsque vous mettez en doute quelque chose, on vous fournit généralement des explications claires et sensées.	Les explications vous semblent compliquées, diffuses et déroutantes.
Ingénierie sociale	Elle pourrait servir d'aide à la vente.	Elle peut servir à profiter de la victime sur le plan psychologique et à l'amener par la ruse à fournir des renseignements personnels.

1.3.2 Escroqueries utilisant le numéro « 900 »

Les escroqueries utilisant le numéro « 900 » ressemblent aux escroqueries de prix gagnés. Les consommateurs recevront généralement une offre par la poste dans laquelle on les persuade de composer un numéro 1 900 afin pour apprendre le type de prix qu'ils ont gagné ou la valeur de ce prix. Le problème, c'est que cet appel durera normalement plusieurs minutes avant que l'appelant découvre que la valeur du prix est très modeste. Dans le cas de certains numéros 1 900, on annoncera qu'on vous donne un cadeau gratuit si vous appelez. Mais, c`est vous qui payer en utilisant le numéro 1 900. Rappelez-vous

que les numéros 1 900 ont un tarif d'utilisation à la minute. Si un numéro 1 900 soulève des préoccupations, communiquez immédiatement avec Phonebusters 1(888) 495-8501 ou au www.phonebusters.com.

1.3.3 Piratage de l'identification de l'appelant

L'identification de l'appelant est une fonction commode. Toutefois, l'information qui s'affiche peut être falsifié par des criminels. Ne vous servez jamais uniquement de l'information affichée pour confirmer l'identité de l'appelant, qu'il s'agisse d'un individu, d'une entreprise ou d'une organisation.

1.4 Documents imprimés

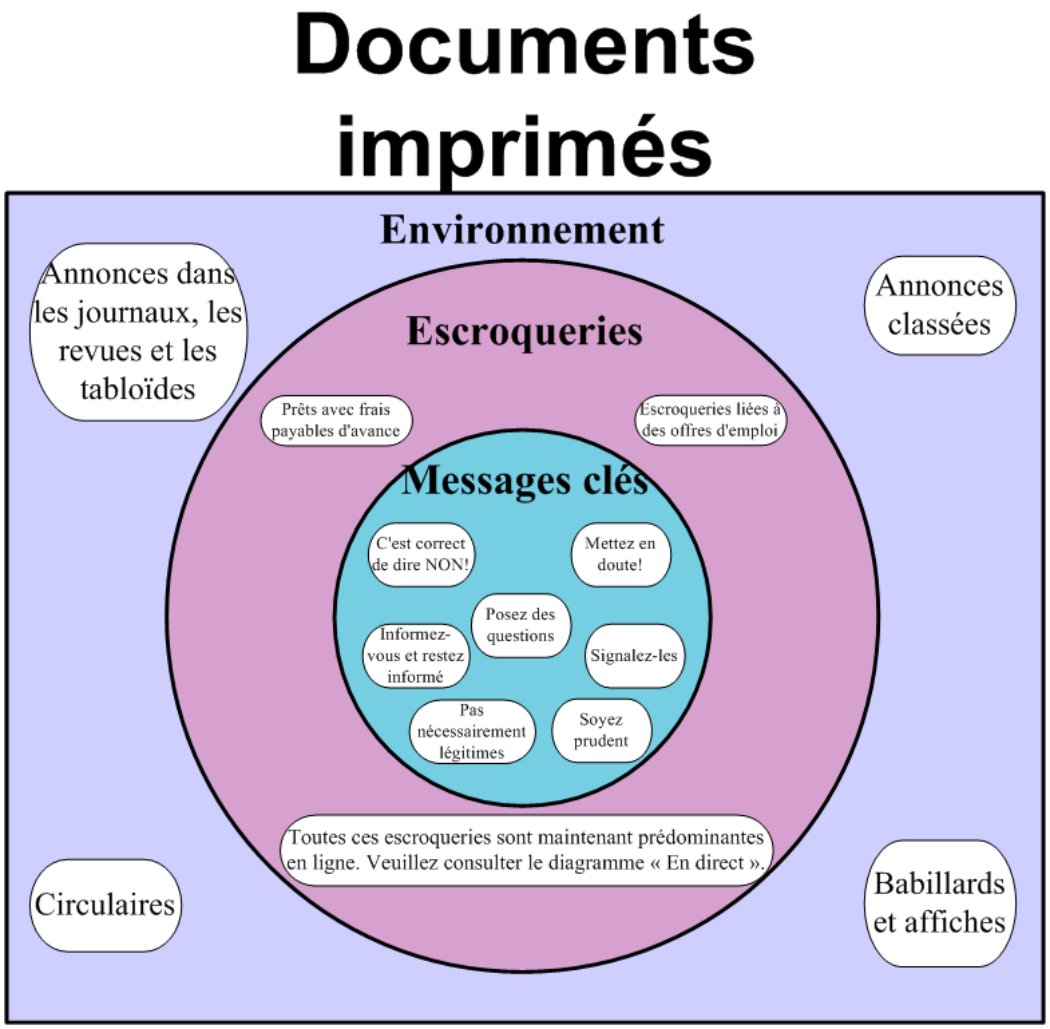


Figure 5 : Messages clés pour vous aider à éviter d'être victime d'escroqueries liées à des documents imprimés qu'on trouve dans divers environnement

On peut trouver des annonces relatives aux offres d'emploi, aux prêts avec paiement de frais à l'avance, aux tirages, aux loteries et aux marchandises précieuses dans les journaux, les revues, les tabloïdes, les annonces classées et les circulaires ou sur les babillards et les affiches. Certaines de ces annonces pourraient être des escroqueries destinées à obtenir vos renseignements personnels et financiers ou simplement à voler votre argent. Soyez prudent lorsque vous répondez à ces annonces imprimées. Rappelez-vous que les annonces publiées dans un journal local, une revue populaire ou affichées sur un babillard ne sont pas nécessairement légitimes. Vous devez prendre certaines précautions, telles que vérifier la crédibilité de l'entreprise et appeler cette entreprise afin de vous assurer qu'elle a bien fait publier l'annonce. Vous pouvez transmettre l'article suspect à Phonebusters par télécopieur, en composant le 1 (888) 654-9426.

Dans des provinces et des territoires, une grande quantité de renseignements personnels est imprimée sur l'étiquette des bouteilles d'ordonnance et sur les reçus qui s'y rattachent délivrés par les pharmacies et les hôpitaux. Avant de recycler ou de jeter ces articles, vous devriez déchiqueter toutes les étiquettes ou documents portant des renseignements personnels

1.5 Courrier

Courrier

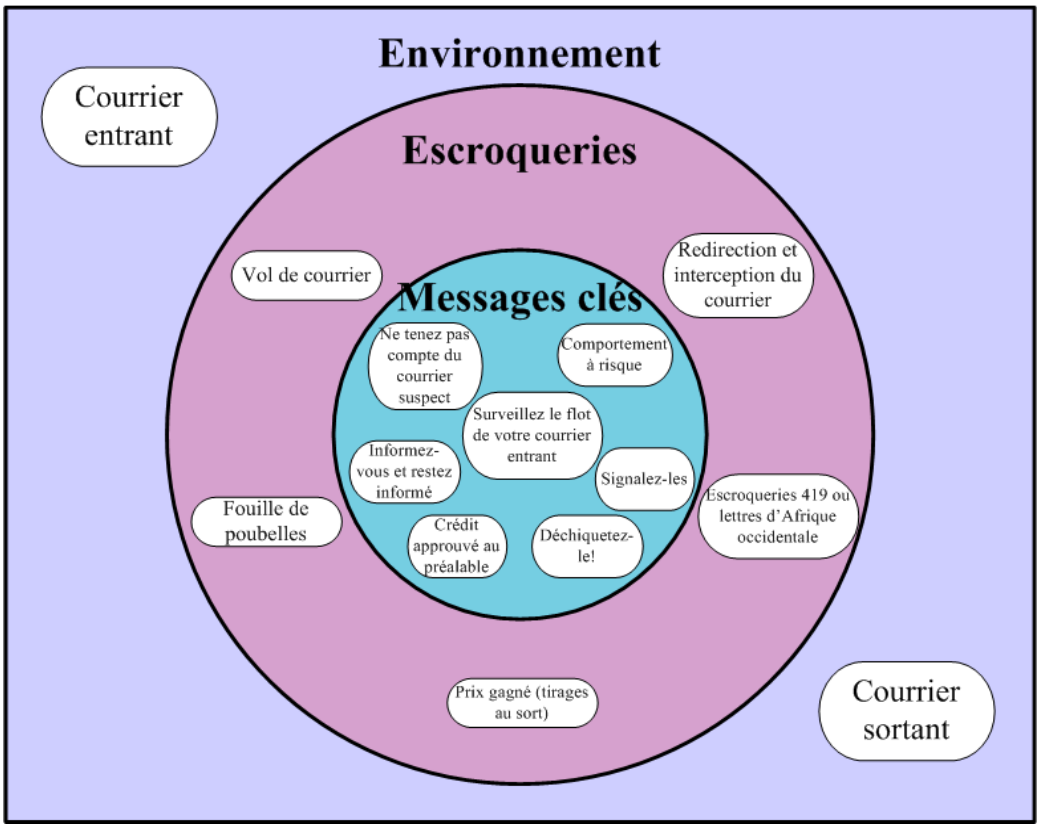


Figure 6 : Messages clés pour vous aider à éviter les escroqueries liées au courrier qu'on trouve dans divers environnements

Vous avez sans aucun doute déjà reçu du courrier dans lequel on vous annonçait que vous aviez gagné des prix, des vacances ou des services. Beaucoup de ces sollicitations pourraient ne pas être légitimes. Ce sont des variantes ou des imitations d'escroqueries comme celles des frais d'emprunt payables d'avance, des prix gagnés, des lettres frauduleuses provenant d'Afrique occidentale et des faux organismes de bienfaisance. Ces sollicitations peuvent prendre la forme de cartes postales, de certificats, de chèques non sollicités, de lettres de félicitations concernant des prix gagnés ou des gains de loterie, d'abonnements gratuits à des revues, de cartes de crédit approuvés et d'offres de prêt. Examinez soigneusement tout votre courrier quand il arrive. Par exemple, si vous recevez une carte de crédit préapprouvée par la poste et que vous décidez de ne pas y donner suite, assurez-vous de la déchiqueter avant de la mettre aux ordures. On ne sait jamais, elle pourrait être récupérée par un pêcheur de poubelles.

Le courrier présente d’autres menaces qui pourraient entraîner le vol de vos renseignements personnels, comme le vol, l’interception et le réacheminement du courrier. Disposer d’une boîte aux lettres fermée à clé et sécurisée est la première mesure à prendre pour assurer la sécurité de son courrier et de son contenu. De plus, vous ne devriez déposer votre courrier que dans les boîtes postales du bureau de poste ou à votre bureau de poste local. Connaître son cycle de facturation et vérifier régulièrement son courrier constituent de bonnes habitudes à prendre qui aident à découvrir si le courrier est intercepté ou réacheminé. En outre, si vous déménagez, vous devriez prendre soin de faire votre changement d’adresse. Assurez-vous que tous les fournisseurs de services sont informés de votre déménagement. Vous pourrez ainsi vous assurer que votre cycle de facturation n’est pas interrompu.

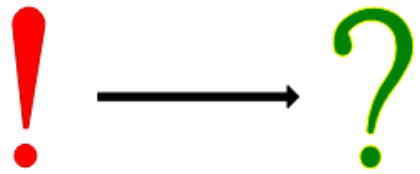
2. Signaux d'alarme

Signaux d'alarme

Aucune méthode ne peut garantir que vous savez si vous êtes exposé à la fraude. Lisez les 14 indicateurs suivants et appliquez-les dans votre vie quotidienne. Rappelez-vous qu'une situation dans laquelle apparaît au moins un signal d'alarme n'en fait pas automatiquement un cas de fraude. Elle signifie que vous devriez être prudent, faire des recherches et poser les bonnes questions. Si les réponses fournies ou si vos recherches ne dissipent pas ces signaux d'alarme, laissez tomber, tout simplement.

La Fraude

Identifiez-la.
Signalez-la.
Enrayez-la.



Indicateurs

1. À qui ai-je vraiment affaire?
2. Pourquoi cette personne demande-t-elle plus de renseignements que ce dont elle a vraiment besoin?
3. Est-ce qu'on me presse ou me pousse à prendre une décision impulsive?
4. Cette personne est-elle exagérément enthousiaste?
5. Est-ce trop beau pour être vrai?
6. Ce guichet automatique bancaire (GAB) a-t-il quelque chose d'inhabituel?
7. Y a-t-il un appareil photo intégré dans un téléphone cellulaire dissimulé ou une personne cachée qui lit mon NIP?
8. S'agit-il d'une offre d'emploi légitime?
9. Ce site Web est-il digne de confiance et légitime?
10. Cette organisation ou cet employeur protégeront-ils mes renseignements personnels?
11. Pourquoi me demandent-ils de payer des frais de traitement pour m'accorder un prêt?
12. Comment ont-ils obtenu l'information personne-ressource qui me concerne?
13. Suis-je en train de diffuser mes renseignements personnels par fréquence radio?
14. Pourquoi cet étranger veut-il soudainement devenir mon meilleur ami?

3. Scénarios

Hameçonnage :

Vous avez reçu un courriel de votre banque dans lequel elle vous informe qu'elle a mis à niveau ses mesures de sécurité pour vous protéger contre le vol d'identité. Elle vous demande de toute urgence d'ouvrir une session sur son site et, comme par hasard, elle fournit le lien pour ce faire. Vous êtes un client de longue date de cette banque, vous lui faites confiance et vous savez qu'elle protège votre information. Mais vous êtes inquiet. Que devriez-vous faire?

Les banques ne font tout simplement pas cela. Votre banque dispose déjà de tous vos renseignements personnels! Il n'est pas crédible qu'elle communique avec vous pour les obtenir de nouveau, n'est-ce pas? Pourquoi enverrait-elle un courriel pour vous demander vos renseignements personnels alors qu'elle travaille durement pour vous protéger contre l'hameçonnage? L'auteur de ce courriel pourrait également prétendre être un représentant d'un organisme gouvernemental ou d'une compagnie prétrolière en direct. Faites preuve de bon sens, détruisez ces messages, n'y répondez pas, ne suivez aucun lien fourni et ne composez aucun numéro de téléphone.

Disposition d'un ordinateur personnel :

Vous savez que vous devez protéger vos renseignements personnels. Avant de vendre votre vieil ordinateur, vous effacez tous les fichiers dans lesquels vous avez stocké toute votre information. Vous devriez vous sentir en sécurité maintenant, n'est-ce pas?

Lorsque vous effacez vos renseignements dans un ordinateur, l'ordinateur ne les efface pas physiquement, en fait. Il les cache simplement hors du système de fichiers actifs. Si l'espace disque libéré n'a pas par la suite été écrasé par un nouveau fichier, l'information sera encore lisible et pourra le rester pendant très longtemps. Avant de disposer d'un disque dur, envisagez les deux solutions de rechange sécuritaires suivantes : 1) reformattez le disque dur et réinstallez le système d'exploitation (Windows, MacOS) et « essuyez » l'espace non utilisé à l'aide d'un logiciel spécialisé ou 2) détruisez physiquement le disque dur.

Écrémage de carte de paiement :

Brian s'arrête à une station-service libre-service locale. Tout en payant avec sa carte de débit, il bavarde avec le commis qui est très amical. Brian est tellement absorbé par la conversation qu'il ne remarque pas la caméra cachée et le fait que sa carte a été glissée à travers une deuxième machine? Aurait-il fallu que Brain soit plus attentif?

Oui, puisque deux semaines plus tard, Brian remarque plusieurs gros retraits de son compte de banque qu'il n'a pas faits. Brian aurait pu éviter ce scénario. Il aurait dû simplement garder un œil sur sa carte et protéger son numéro d'identification personnel (NIP).

Fouille de poubelles :

Dans un grand ensemble d'habitations collectives, Michel le concierge a trouvé un nouveau passe-temps payant. Il recycle les rebuts. Paul, un ami d'un ami, donne à Michel beaucoup d'argent pour obtenir de la paperasserie inutile, comme des demandes de crédit approuvées au préalable. En fait, Paul paiera même pour tout rebut qui contient des renseignements personnels. Michel est un gars honnête et il n'y a rien de mal à vendre les rebuts inutiles, n'est-ce pas?

Non. Michel est peut-être un homme honnête mais Paul utilise cette information des locataires pour appliquer et par la suite recevoir des cartes de crédit sous leur nom. Donc plusieurs grands achats ont été faits. En conséquence, les cotes de crédits des locataires sont affectées. Les locataires négligents risquent de perdre beaucoup de temps et d'argent pour rétablir leur réputation. Déchiquetez vos renseignements personnels avant de les jeter.

Intrusion dans l'espace personnel :

Après une partie de water polo à la piscine de l'université, les joueurs retournent au vestiaire pour découvrir que tous les cadenas ont été coupés. La plupart des portefeuilles ont disparu. Les joueurs s'entendent tous pour signaler le vol à la police, et toutes les cartes peuvent être remplacées.

Ne transportez pas votre vie dans votre portefeuille. Gardez votre carte de NAS, votre certificat de naissance et votre passeport sous clé, dans un endroit sûr. Si la confidentialité des renseignements personnels a été compromise, signalez-le aux bureaux de crédit et demandez-leur d'inscrire une alerte à la fraude dans votre dossier. Signalez l'incident à la police et à Phonebusters au 1(888) 495-8501 ou au www.phonebusters.com ou www.sedde.ca.

Écoute clandestine :

Tout en déjeunant à la cafétéria, Diane se rend compte qu'elle a oublié de vérifier le solde de son compte. Elle prend son téléphone cellulaire et accède à cette information.

En fait, Diane diffuse l'information sur sa banque, son identificateur de compte et son NIP par fréquence radio. La situation serait la même si elle utilisait un réseau ou un téléphone sans fil. Dans les limites de diffusion de l'appareil, des criminels pourraient surveiller les communications et saisir les numéros qu'elle a tapés ou l'information vocale qu'elle a donnée. Son compte pourrait maintenant être à risque. Faites également attention aux gens qui peuvent entendre ce que vous dites ou lire sur vos lèvres, par hasard, dans un endroit public.

Écorniflage :

Vous êtes pressé d'obtenir de l'argent comptant au GAB du campus. Alors, vous ne prenez pas la peine de bien protéger votre NIP avec votre main et votre corps. Ceci permet que la prochaine personne en ligne puisse voir votre NIP.

Vous vous faites attaquer par l'individu qui était derrière vous en ligne au GAB. Cet individu a pu mémoriser votre NIP et a pris votre carte de débit. Maintenant qu'il a votre carte de débit, il peut aller vider votre compte de banque avant que vous puissiez avertir la police.

Téléphone :

Benoît reçoit un appel de Robert Couture, du magasin de meubles local Prix modique, où la plupart des étudiants achètent leurs meubles. M. Couture lui fait savoir que sa commande de sofa payée avec sa carte VISA est en souffrance. Benoît dit qu'il n'a jamais commandé ce sofa et qu'il ne le paiera pas. L'employé s'excuse et demande le numéro de la carte de crédit de Benoît aux fins de remboursement. Benoît devrait-il fournir cette information?

Certainement pas au téléphone sans avoir validé l'identité de cette personne. Rendez-vous au magasin et demandez à voir les factures. Vous pouvez appeler au magasin à l'aide du numéro de téléphone qui figure dans l'annuaire téléphonique. Appelez l'émetteur de la carte si ce n'est pas possible de le faire. Ne vous laissez pas avoir!

Offre de crédit frauduleuse :

Vous trouvez une offre incroyable de carte de crédit faite par un établissement de crédit important à la galerie marchande. Elle n'est assortie de presqu'aucune obligation et son taux d'intérêt est bien moindre que celui de la concurrence. Vous êtes intéressé mais que devriez-vous faire?

Communiquez avec cette compagnie émettrice de carte de crédit en utilisant un numéro de téléphone publié et posez-leur des questions sur cette offre. S'il s'agit d'une offre frauduleuse, fournissez tous les détails à la compagnie émettrice de la carte de crédit, communiquez avec la police locale et signalez l'offre par voie électronique à www.sedde.ca ou par téléphone à Phonebusters 1 (888) 495-8501 ou www.phonebusters.com.

Escroquerie liée à des offres d'emploi :

Vous trouvez un emploi de télémarketing à temps partiel, très payant, sur le babillard de votre campus universitaire. Aucune expérience n'est exigée. Vous les appelez, passez une entrevue et obtenez l'emploi la journée même. Vous commencez à travailler avec 10 autres personnes de votre âge. Quelques jours plus tard, votre patron commence à faire pression sur vous, pour que vous fassiez de meilleures ventes, mais la vente de ces « trousses de rétablissement de crédit » vous rend de plus en plus mal à l'aise . Vous entendez des collègues de travail essayer de se convaincre qu'il n'y a rien de mal à mentir pour conclure une vente. Il n'y a rien de mal, n'est-ce pas?

Votre petite voix intérieure a vraisemblablement raison. Il devient évident que vous avez été amené, par la ruse, à commettre des fraudes au détriment des autres. Le fait que vous ayez également fourni vos renseignements personnels à des criminels est moins évident. Ils peuvent décider de les utiliser des mois ou des années plus tard. Vous en savez maintenant assez pour comprendre que vous participiez à une infraction à votre insu. Continuer à y participer en connaissance de cause vous ferait prendre part à cette infraction. Démissionnez, suivez les conseils de prévention contre le vol d'identité inclus dans le présent guide et signalez l'incident par voie électronique à www.sedde.ca ou par téléphone à Phonebusters au 1(888) 495-8501 ou www.phonebusters.com. Appelez également la police pour signaler l'escroquerie. Une autre version de l'escroquerie liée à des offres d'emploi concerne des manœuvres frauduleuses de réexpédition à la maison, pour lesquelles on n'exige aucune expérience.

Accès sans fil à Internet :

Vous êtes très occupé au bureau et vous adorez la connectivité spontanée que votre ordinateur portatif Wi-Fi vous offre. De nouveaux points de contrôle d'accès Wi-Fi apparaissent continuellement et certains sont mêmes gratuits. Vous en êtes maintenant rendu à utiliser le Wi-Fi pour la plupart de vos transactions et communications dans Internet. Cela ne pose pas de problème, n'est-ce pas?

Il n'y a rien de mal à utiliser le Wi-Fi. Seulement, soyez conscient que ce type d'accès utilise des fréquences radio et que vos données pourraient être interceptées ou si ton point d'accès favoris peut-être détourné par un "Evil Twin". Ceci est un point d'accès falsifié qui est contrôlé par un individu assis dans une camionnette de l'autre côté de la rue ou à quelques tables plus loin dans un ordinateur portatif dans un sac à dos, piratait vos points d'accès Wi-Fi préférés. Lorsque vous avez le choix, utilisez une connexion Internet ordinaire, utilisez un mot de passe et chiffrez vos sessions lorsque vous êtes connecté à un point d'accès Wi–Fi.Utilisez un mot de passe invalide la première fois que vous essayez d'ouvrir une session. Soupçonnez qu'il y a un problème si vous pouvez vous connecter avec un mot de passe invalide.

Ordinateurs à accès public :

Vous n'avez pas votre propre ordinateur et vous profitez au maximum des ordinateurs à accès public pour rester branché. Il ne devrait pas y avoir de problème, n'est-ce pas?

Soyez conscient qu'on peut avoir installé des enregistreurs de frappes sur les ordinateurs à accès public. L'intégrité de ceux-ci également être compromise par un logiciel espion. Il est préférable de ne pas utiliser les sites web sécurisés sur les ordinateurs à accès public. Soyez certain de bien fermer votre session. Il est possible que certains navigateurs copient de l'information sur le disque dure et qui pourrait être par la suite visible aux autres utilisateurs. Donc, il est important de savoir comment bien « vider le cache du navigateur », « supprimer les témoins » et « supprimer l'historique du navigateur ».

Ventes aux enchères frauduleuses :

Vous voulez vendre votre voiture et vous décidez d'essayer de la vendre sur un site de ventes aux enchères. Vous décidez de la mettre en vente aux enchères en direct dans votre site préféré. Peu après, vous recevez un message d'une personne vivant aux États-Unis qui vous offre beaucoup plus que la valeur réelle de votre bien, si vous arrêtez votre vente aux enchères. Il vous raconte une histoire compliquée que vous ne vous souciez pas vraiment de comprendre. Comme dernier détail, il a un chèque d'une banque du Texas dont la valeur dépasse de quelque 1 000 $US ce qu'il vous offre pour votre voiture. Comme vous êtes Canadien, il est confiant de récupérer son argent.

Cela semble trop beau pour être vrai. Et effectivement, ce n'est probablement pas vrai. Le chèque est probablement contrefait. Cette personne veut vraisemblablement tirer profit du temps de traitement des chèques.

Prêts avec paiement de frais à l'avance :

En lisant le journal local, vous remarquez une annonce de prêt d'une petite somme dans laquelle on vous garantit pratiquement que n'importe qui peut avoir un prêt, sans égard à la bonne ou à la mauvaise cote de crédit ni au fait que vous avez déjà fait faillite. Comme la plupart des étudiants, vous manquez d'argent ce mois-ci et décidez de composer le numéro sans frais. Vous recevez des formulaires que vous remplissez en y inscrivant vos renseignements personnels. Quelques jours plus tard, on vous appelle pour vous dire que votre demande de crédit a été approuvée et qu'il faut que vous fassiez un virement électronique pour payer les frais d'assurance et de traitement avant de recevoir le prêt. Devriez-vous envoyer cet argent?

Non. D'abord, vérifiez qu'il s'agit d'une annonce valide publiée par une banque canadienne valide. Les banques canadiennes valides figurent sur une liste de l'Association des banquiers canadiens, soit les listes de banques des annexes I, II ou III. Veuillez vous reporter à l'annexe sur les liens utiles incluse à la fin du présent document. Appelez la banque correspondante et informez-vous sur sa promotion. Si la banque ne figure pas sur la liste ou si elle n'est pas au courant de cette promotion, signalez l'incident!

Sites de réseautage social :

Vous décidez de créer votre premier profil en ligne sur un site populaire de réseautage social. Pour impressionner vos amies, vous remplissez de façon très détaillée la section des renseignements. Vous avez mis votre date de naissance, votre numéro de téléphone, votre adresse, votre école et vos équipes de sport. Vous ajoutez des photos de votre voyage fait avec vos amis au cours de l'été. Tout cela semble inoffensif, n'est-ce-pas?

Faux! Avant que vous créez votre premier profil en ligne, assurez-vous de bien comprendre que certains renseignements personnels ne doivent pas apparaître dans votre profil. Vous devez connaître les conséquences négatives qui peuvent résulter de l'affichage de certains renseignements en ligne. Vous ne devez jamais entrer votre date de naissance, votre adresse et l'adresse de votre école. Même des photos peuvent révéler trop d'éléments d'information qui pourraient être utilisés par un escroc pour en obtenir encore plus. Choisissez les paramètres de sécurité adéquats pour assurer la protection maximale de votre information.

Services de rencontre :

Une femme de l'étranger communique avec Greg par l'entremise d'un site de rencontre. Ils commencent à bavarder en ligne et s'échangent leurs numéros de téléphone. Après quelques semaines, la femme a gagné l'entière confiance de Greg. Elle lui explique qu'elle veut le rencontrer en personne, mais qu'elle a besoin d'argent pour acquitter ses frais de voyage, p. ex. pour la nourriture, le billet d'avion et un passeport. Elle pourra le rembourser quand ils se rencontreront étant donné qu'elle a un oncle fortuné qui vient tout juste de décéder au Canada, et que pour accéder à l'argent, elle doit venir au Canada. Greg devrait-il lui envoyer de l'argent?

Non, parce que Greg n'en reverra probablement jamais la couleur. Soyez très prudent quand vous rencontrez quelqu'un dans le cyberespace. Bien que l'autre puisse vous sembler tout à fait sincère et digne de confiance, vous ne savez pas vraiment à qui vous avez affaire.

Ne sous-estimez pas l'importance de vos renseignements personnels. Une identité volée, c'est la clé pour obtenir vos antécédents en matière de crédit et votre argent. Elle peut également être utilisée à des fins criminelles. Il faut consacrer beaucoup d'efforts, de temps et d'argent pour régler ses problèmes de crédit et récupérer son argent. Rappelez-vous qu'il n'est pas toujours possible de complètement régler ces problèmes. Suivez les conseils destinés à vous aider à éviter de devenir une victime de la fraude d'identité qu'on mentionne dans le présent guide. L'importance de votre contribution au contrôle des renseignements personnels et au problème de la protection contre l'escroquerie n'est généralement pas suffisamment reconnue. Dans votre cercle de connaissances, vous avez le pouvoir d'éduquer les autres. Au cours de vos activités quotidiennes, prenez quelques minutes pour transmettre, à votre famille, à vos amis et à vos collègues, des connaissances que vous venez d'acquérir. Plus précisément, transmettez les meilleures pratiques de manipulation de l'argent et des cartes de crédit ou de débit lorsque vous êtes en public ou les meilleures pratiques de sécurité en direct. La meilleure façon de réduire au minimum les risques d'être la victime d'une fraude, c'est de s'informer sur les nouvelles escroqueries et techniques frauduleuses et de rester informé.

La Fraude

Identifiez-la.
Signalez-la.
Enrayez-la.

La police a besoin de votre soutien pour être en mesure de trouver les criminels qui utilisent cette information à leur avantage. Signalez toute information relative à une escroquerie :

- à l'adresse www.sedde.ca ou
- au centre d'appel canadien pour combattre la fraude, au 1 (888) 495-8501 ou à www.phonebusters.com.

Veuillez noter que l'information qui a été utilisé pour compiler ce guide a été obtenu de plusieurs organisations retrouvées dans la section de Liens Utiles.

Annexe 1 - Liens utiles

Sensibilisation des consommateurs et gouvernement	
Comité des mesures en matière de consommation - Protégez votre identité	http://cmcweb.ca/epic/internet/incmc-cmc.nsf/fr/fe00088f.html
Passerelle d'information pour le consommateur canadien	http://www.consumerinformation.ca/
Conseil canadien des bureaux d'éthique commerciale	http://www.ccbbb.ca/francais/
Agence de la consommation en matière financière du Canada	http://www.fcac.gc.ca/fra/consumers/default.asp
Gouvernement de la Colombie-Britannique - Protection des renseignements personnels (en anglais seulement)	http://www.mser.gov.bc.ca/privacyaccess/Privacy/
Gouvernement de l'Ontario - Les consommateurs avisés font de bonnes affaires	http://www.cbs.gov.on.ca/mcbs/francais/info_consomm.htm
Gouvernement du Québec - OPC Jeunesse (en français seulement)	http://www.opc.gouv.qc.ca/jeunesse/accueil/affiche.asp?page=18plus
Contrefaçon	
Éléments de sécurité des billets de banque	http://www.banqueducanada.ca/fr/billets/contrefacon/securite_elements.html
Bureaux de crédit	
Equifax Canada	http://www.equifax.com/EFX_Canada/index_f.html
Trans-Union Canada	http://www.tuc.ca/TUCorp/french/home.asp
Les Bureaux de crédit du Nord Inc.	http://www.creditbureau.ca/
Noms de domaine	
Autorité canadienne pour les enregistrements Internet	http://www.cira.ca
Internet Assigned Numbers Authority (en anglais seulement)	Codes de pays - http://www.iana.org/cctld/cctld-whois.htm Domaines génériques de premier niveau - http://www.iana.org/gtld/gtld.htm Domaine de premier niveau de l'infrastructure - http://www.iana.org/arpa-dom/ Service -WHOIS http://whois.iana.org/ Regional Internet Registries - http://www.iana.org/ipaddress/ip-addresses.htm
SamSpade.org - WHOIS (en anglais seulement)	http://www.samspade.org/
Source WHOIS -WHOIS (en anglais seulement)	http://www.whois.sc/

Sécurité des comptes de banque personnels	
Association des banquiers canadiens Banques de l'annexe I Banques de l'annexe II Banques de l'annexe III 10 bons moyens de protéger vos cartes de crédit	http://www.cba.ca/fr/section.asp?fl=3&sl=308&tl=&docid= http://www.cba.ca/fr/viewdocument.asp?fl=2&sl=204&tl=160&docid=354 http://www.cba.ca/fr/viewdocument.asp?fl=2&sl=204&tl=161&docid=350 http://www.cba.ca/fr/viewdocument.asp?fl=2&sl=204&tl=162&docid=353 http://www.cba.ca/fr/viewdocument.asp?fl=3&sl=11&tl=129&docid=257&pg=1
Protéger son argent et se protéger	http://www.yourmoney.cba.ca/fr/tsamprogram/protecting/index.cfm
GRC/CHOIX : Comment bien utiliser les bouts de plastique	http://www.deal.org/content/index.php?option=com_content&task=view&id=565&Itemid=32&lang=fr
Interac - Protégez votre NIP	http://www.interac.org/fr_n1_50_protectyourpin.html
Hameçonnage	
The Anti-Phishing Working Group (en anglais seulement)	http://www.antiphishing.org
Sécurité publique	
Sécurité publique et Protection civile Canada - Vol d'identité – Questions et réponses	http://www.securitecanada.ca/identitytheft_f.asp
Jeux-questionnaires	
Industrie Canada - Consommateur Connexion - Questionnaire sur la fraude	http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/fr/ca01960f.html
SonicWall Phishing IQ Test II (en anglais seulement)	http://www.sonicwall.com/phishing/
Signalisation des fraudes au Canada	
Phonebusters	http://www.phonebusters.com
Signalement en direct des délits économiques (Centre Sedde)	http://www.sedde.ca
Pourriels (SPAM), logiciel espion	
Industrie Canada - Arrêter le pollupostage	http://arretezlepourrielici.ca/
Anti-Spyware Coalition (en anglais seulement)	http://www.antispywarecoalition.org/index.htm
Terminologie et encyclopédie	
CERT.ORG - Home Computer Security (en anglais seulement)	http://www.cert.org/homeusers/HomeComputerSecurity/
How Stuff Works (en anglais seulement)	http://www.howstuffworks.com/
Wikipedia	http://fr.wikipedia.org/wiki/Accueil

Éducation, sensibilisation et assistance	
Forum de prévention de la fraude	http://www.competitionbureau.gc.ca/internet/index.cfm?itemID=122&lg=f
US Federal Trade Commission (en anglais seulement)	http://www.ftc.gov/bcp/edu/microsites/idtheft/
Ressources humaines et Développement des compétences - Carte de numéro d'assurance sociale (NAS) perdue ou volée	http://www.rhdcc.gc.ca/asp/passerelle.asp?hr=fr/sm/nas/130.shtml&hs=sxn http://www.rhdsc.gc.ca/fr/sm/nas/0300/0300_in125.shtml
Commissariat à la protection de la vie privée du Canada	NAS - http://www.privcom.gc.ca/fs-fi/02_05_d_02_f.asp Vol d'identité - http://www.privcom.gc.ca/fs-fi/02_05_d_10_f.asp
Service Canada - Perte du portefeuille	http://www.servicecanada.gc.ca/fr/vie/portefeuille.shtml

Glossaire

Adresse IP (protocole Internet)

Numéro unique que les machines utilisent dans le but d'identifier les autres machines et communiquer entre elles dans un réseau à l'aide de la norme de protocole Internet.

Cache navigateur

C'est des données qui sont copiées pour optimiser la performance de l'application de l'ordinateur.

Cookies HTTP

Les cookies HTTP sont des parties d'information qui sont envoyées au serveur et renvoyées par le serveur. Ces parties d'information sont employées pour tracer et garder l'information des habitudes en direct de l'utilisateur. Ces habitudes peuvent inclure les sites Web préférés de l'utilisateur ainsi que la fréquence d'utilisation de ces sites Web.

DNS

DNS est l'abréviation anglaise pour « système de nom de domaine ». Fonction Internet qui trouve et traduit immédiatement les noms de domaine en adresse de protocole Internet (adresse IP).

Enregistreur de frappe

C'est un logiciel malveillant (maliciel) qui capture, stock et envoi les touches frappées sur le clavier de l'utilisateur à un autre ordinateur. Ce type de logiciel enregistre tout l'information tapée par l'utilisateur.

Fraude

Dépossession malhonnête des intérêts économiques de quelqu'un.

Fraude d'identité

Définition de la GRC. Acquisition, possession ou commerce non autorisés de renseignements personnels ou utilisation non autorisée de ces renseignements pour créer une identité fictive ou emprunter une identité existante ou en prendre le contrôle afin d'obtenir des profits financiers, des biens ou des services ou de dissimuler des activités criminelles.

Fraudeur

Personne qui commet la fraude.

Hameçonnage

Utilisation de l'ingénierie sociale dans des messages électroniques afin de provoquer une réaction impulsive immédiate chez des personnes et les amener vers des sites Web frauduleux. Le but ultime consiste à acquérir des renseignements personnels ou de nature délicate.

Information personnelle

Dans ce document, l'information personnelle désigne tout élément ou combination d'éléments pouvant être utilisés pour identifier positivement un individu aux fins de livraison de biens et services, services gouvernementaux ou d'application de la loi. Peux aussi désigner toute combinaison d'information pouvant être utilisé afin d'obtenir de l'information additionnelle sur un individu.

Ingénierie sociale

Pratique qui consiste à manipuler la confiance d'une personne afin d'en tirer des avantages.

Logiciel malveillant (Malware)

Programme délibérément conçu pour saisir, modifier, endommager ou changer des données ou modifier le comportement d'un ordinateur sans que l'utilisateur en ait connaissance ou l'intention explicite. Parmi les logiciels malveillants, on trouve des chevaux de Troie, des logiciels espions (espiogiciels), des virus et des vers.

Mystification (Spoofing)

Modification de l'information relative à l'identité ou à l'authentification afin de tromper le lecteur sur l'identité véritable de l'expéditeur.

NIP - Numéro d'identification personnel

Code de sécurité utilisé afin d'accéder à des données et à des comptes personnels.

Nom de domaine

Un nom est plus facile à mémoriser qu'un adresse numérique, ceci est un équivalent plus significatif d'une adresse IP numérique.

"Pharming"

Code malveillant installé dans un ordinateur ou un serveur personnel pour détourner les utilisateurs vers des sites frauduleux à leur insu ou sans leur consentement.

Pourriels/pollupostage (SPAM)

Pratique qui consiste à envoyer à tort et à travers des messages électroniques non sollicités, non désirés ou inappropriés en grande quantité.

Protocole

Norme industrielle ou internationale qui consiste en un ensemble particulier de règles conçues en vue de gérer les communications.

Racleur d'écran

C'est un logiciel malveillant (maliciel) qui permet que quelqu'un d'autre puisse voir ce qui est sur ton écran. Ce type de logiciel prend une photo de ton écran et l'envoi à un autre ordinateur.

URL

Abréviation anglaise de « localisateur de ressources uniformes » (Uniform Resource Locator). Adresse unique d'un fichier accessible dans Internet.

WEP

Abréviation de « Wired Equivalent Privacy », il s'agit d'une norme de réseau pour les réseaux sans fil. Comme son nom l'indique, il vise à offrir aux réseaux sans fil une confidentialité et une sécurité équivalentes à celles des réseaux cablés.

WPA

Abréviation de « Wi-Fi Protected Access », il s'agit d'une norme de réseau sans fil visant à renforcer la sécurité offerte par la norme WEP.