L’IDENTITÉ À L’ÈRE DU NUMÉRIQUE

ATELIER D’ÉCHANGES SUR LES PRATIQUES ET LES ENJEUX LIÉS À L’IDENTITÉ EN LIGNE

1. Définition

L'identité numérique (IN) est l'image qu'on peut se faire d'une personne, d'un groupe, d'une organisation, ou d'une entité x (par exemple, un quartier) à partir de l'information numérisée qui existe à son sujet. L'identité web est une sous-section de l'identité numérique. Quand on parle d'identité numérique, on parle en fait de deux choses :

- celle d'ordre administratif;
- elle de l'ordre de la personnalité.

Ces deux types d'identité peuvent être abordés séparément ainsi qu'en lien l'une avec l'autre. Cependant, il faut garder à l'esprit qu'il s'agit de deux notions distinctes.

Alors qu'il y a quelques années on parlait de l'impermanence du matériel sur le Web par rapport à la permanence de l'imprimé, on parle pour l'identité Web de traces qui demeurent au fil du temps et qui sont susceptibles d'être diffusées rapidement et largement.

Lieux de l'identité numérique

Partout où on a un login et partout où on produit du contenu tel que
- Les blogues (en tant qu'auteur ou commentateur)
- Les forums de discussion
- La présentation de soi sur un site de réseautage social
- Participation à un média social (par exemple, Wikipedia)

On peut partir du bottin de téléphone, au bottin de téléphone inversé, à la recherche de courriel pour une personne, à la recherche d'information sur une personne avec son adresse de courriel. Info sur le web mais aussi dans les bases de données publiques.

Nous aborderons ici surtout l'IN d'une personne, celle-ci semblant la plus susceptible de donner lieu à une formation aux personnes participant aux activités de Communautique et à la population en général.

L'identité numérique d'ordre administratif

L'IN administrative est basée sur des informations telles l'adresse, le numéro de téléphone, le numéro d'assurance sociale, un numéro de compte bancaire ou de carte de crédit et autres renseignements personnels. Elle peut aussi être basée sur de l'information apparaissant dans des documents officiels – certificat de naissance, de mariage ou d'adoption, dossier de crédit, dossier criminel, titres de propriété, dossier médical, etc. Si cette information est généralement de type textuel ou numérique, elle peut aussi être d'ordre graphique (photographie,

radiographie, empreinte digitale ou rétinienne), vidéo (surveillance) ou encore géomatique. Dans les cas énumérés jusqu'ici, elle est associée le plus souvent au nom légal de la personne dans une relation non équivoque et avérée, qui ne donne pas lieu à l'interprétation. On peut bien entendu interpréter le contenu d'un dossier criminel ou médical. Cela dit, la nature du lien d'appartenance du dossier à la personne ne donne pas lieu à interprétation. Si le lien n'est pas véridique, c'est qu'il y a erreur, falsification ou fraude.

Ce type d'information réside généralement dans des banques de données qui ne sont pas nécessairement d'emblée disponibles via le Web. Cependant, d'une part, la nature numérique des informations les rend plus susceptibles à des accès élargis, par des canaux administratifs ou criminels, et à une diffusion plus aisée. D'autre part, les internautes peuvent choisir d'utiliser certaines de ces informations au fil de leurs activités sur le web.

Il existe des informations de type administratif qui sont propres au Web. On pense ici aux adresses IP et autres informations nécessaires au fonctionnement même du web. Enfin il y a le couple « nom d'utilisateur » et « mot de passe » (ou numéro d'identification personnel) qui sert à accéder à des services sur le web, qu'il s'agisse d'une institution bancaire, d'un service de courriel, d'un réseau de socialisation, d'une plateforme de jeu, d'un blogue, d'un forum, etc. Cette information peut être associée au nom légal de la personne ou à un pseudonyme.

L'identité numérique de l'ordre de la personnalité

L'identité de l'ordre de la personnalité est basée sur de l'information qui révèle les goûts, les opinions, les attitudes, les valeurs, les activités et les relations d'une personne. Ces informations sont constituées des traces que l'internaute laisse sur le web au cours de ses activités en ligne. Ces traces peuvent être de divers ordres. Celles auxquelles on pense en premier sont les traces textuelles, photographiques ou vidéo que les internautes produisent et mettent en ligne. Ensuite, il y a les traces qui sont dérivées de l'appartenance de l'internaute à tel groupe, tel service, tel réseau. Un type de trace qui est de plus en plus mis en valeur est celle des relations déclarées entre des individus. Le cas le plus connu est celui des « amis » sur des réseaux de socialisation tels Facebook. Il existe plusieurs autres cas qui peuvent permettent de déceler les relations sociales possibles d'un individu comme le suivi des signets, des photographies, des vidéos, des « tweets » ou d'autres productions mises en ligne par un internaute.

Ces traces relatives à la personnalité peuvent être interprétées dans les limites d'un service particulier. On observera alors le comportement d'un individu à 'intérieur d'un réseau social. Elles peuvent être considérées dans un contexte plus global en considérant l'ensemble des activités en ligne d'un internaute. La procédure type pour ce faire est de « googler » le nom d'une personne et d'examiner le contenu des résultats de recherche ainsi obtenus.

2. Questions suscitées par l'identité numérique

Les grandes lignes:

- l'IN d'ordre administratif soulève principalement la problématique de la confidentialité des renseignements personnels dépendante de la sécurité de l'information;
- l'IN de l'ordre de la personnalité soulève des questions relatives aux impacts du degré et de la qualité de dévoilement personnel souhaitable sur le web;
- il existe aussi la problématique du croisement entre les renseignements administratifs et les informations sur la personnalité.

Enjeux de l'IN d'ordre administratif

Le principal enjeu de l'IN administrative est celui des dangers de l'usurpation d'identité qui peut donner lieu à des fraudes. Par exemple, un tiers peut voler ou falsifier des renseignements personnels pour

- obtenir un prêt bancaire, des cartes de crédit, ouvrir un compte bancaire (marge de crédit), détourner des fonds;
- obtenir documents officiels (gouvernementaux) : permis de conduite, carte d'assurance sociale, passeport;
- en lien avec les informations sur la personnalité, entacher la réputation d'une personne.

La confidentialité, l'accès et l'utilisation des renseignements personnels faisaient avant le numérique l'objet de protection législative. Depuis le numérique, ces lois ont été adaptées au nouveau contexte.

Enjeux de l'IN de l'ordre de la personnalité

- la réputation de l'individu, question particulièrement sensible au moment de la recherche d'emploi ou d'un partenaire amoureux;
- la qualité des rapports sociaux aux plans des intérêts, des opinions et des attitudes;

Enjeux du croisement de l'IN administrative et de celle de la personnalité

- vulnérabilité à des prédateurs

3. La gestion de l'IN

La volonté de gérer son identité en ligne est plus une question de choix que d'obligation et est influencée par divers facteurs (valeurs, objectifs, attitudes,

connaissances des enjeux). On peut donner en exemple quelques "profils" de comportements par rapport à l'identité en ligne:

- l'individu précautionneux qui n'utilise les services d'identification en ligne qu'après avoir examiné minutieusement que ses informations demeurent confidentielles et qui s'exprime peu en ligne;
- l'individu nonchalant qui fait un usage confiant des dispositifs en ligne, qui laisse des traces un peu partout au hasard de ses activités d'internaute en faisant modérément attention;
- l'exhibitionniste qui relate sa vie en détail sur le web;
- l'individu qui soigne son image web pour soutenir de bonnes relations sociales ou de travail, ou pour favoriser la recherche d'emploi

On peut ne pas gérer son IN, la gérer avec des précautions de base, ou la gérer de manière stratégique. Ainsi, il existe dorénavant des services de gestion de l'image web que l'on projète dont les principes sont dérivés du « branding » commercial. Il existe aussi des articles proposant les mesures à prendre pour gérer son image en ligne. Les points traités par la gestion pro active de l'image Web sont la réputation, la production d'une image conforme à nos objectifs, le monitoring de la réputation et de l'image. Notons qu'une gestion proactive de l'image web représente un travail considérable et exige qu'on ait beaucoup de temps à y consacrer. La « clientèle » de la gestion proactive de l'image web est surtout celle des professionnels, des chercheurs d'emploi et des afficionado du web.

4. Quelques ressources pour en savoir plus

Aspects sécuritaires

Mon identité (monidentite.isiq.ca)
Portail du Gouvernement du Québec dédié aux questions de sécurité qui entourent l'identité numérique tel que le vol d'identité , les mesures préventives, la sécurisation de l'ordinateur, savoir débusquer les menaces . Une section est consacrée aux réseaux sociaux menant à des guides pratiques sur les comportements sécuritaires à adopter pour le réseautage social tel que le document *Comprendre et configurer votre compte Facebook* (monidentite.isiq.ca/documents/guide_facebook2009.pdf)

Comment protéger vos renseignements personnels en ligne
(www.priv.gc.ca/resource/ii_5_01_f.cfm)
Site du commissariat à la protection de la vie privée du Canada. Plusieurs documents (textes, vidéo, discours) sur les sites de réseautage et la vie privée. Un document "L'identité en ligne: entre la vie privée et les profils virtuels"

Dont Track Us (donttrack.us)
Ce site explique le fonctionnement du « Ad-Tracking », mécanisme utilisé par les

moteurs de recherche tel que Google lorsque l'on effectue nos recherche. Le Ad-tracking consiste à transmettre aux sites suggérées par Google que vous visitez, les mots-clés utilisés pour vos requêtes. Quelques applications sont proposées afin de contrer cette mécanique intrusive.

Gestion de son image

Identité Web (www.identiteweb.fr)
Le site Identiteweb.fr est un blog dédié à la gestion pro-active de son identité numérique et à la « mise en marché personnelle » (personal branding).

La section *Astuces* contient des articles sur des techniques pour maîtriser ses traces laissés sur le web ainsi que des conseils sur la maîtrise de son identité en ligne (*Les 7 étapes pour gérer sa réputation en ligne* et *Contrôlez votre identité numérique, configurez votre Facebook* !)

5. CAPSULES PRATIQUES

a) La recherche de contenu sur Internet

Quand je fais une recherche sur Internet, il y a des chances que le moteur de recherche stocke ensemble dans ses bases de données

- les mots de ma recherche
- l'adresse de mon ordinateur
- le type de fureteur que j'utilise
- Comme il a ces mêmes informations sur les recherches que j'ai faites dans le passé, il possède un historique de mes recherches, ce qui constitue mon profil
- En plus, le moteur de recherche va stocker les adresses des sites que j'ai visité à partir des liens des résultats de ma recherche
- Plusieurs moteurs de recherche vont envoyer les informations de ma recherche aux sites que je visite à partir de la liste des résultats qui eux aussi bâtiront mon profil

Enjeux et conséquences

- plusieurs personnes connaissent à mon insu beaucoup de choses sur moi
- mon profil de recherche peut éventuellement être retracé jusqu'à moi
- je peux faire l'objet d'un marketing plus ciblé, qu'il soit adéquat ou non, que je le veuille ou non
- ces informations potentiellement sensibles peuvent tomber dans les mauvaises mains et me nuire (enquêtes de crédit, enquêtes pour assurance santé, autres)

Choix et contrôles possibles

- utiliser un moteur de recherche qui ne stocke pas de données sur mes activités, par exemple DuckDuckGo.com qui utilise en plus un système d'encryption, comme le dénote le https en début d'adresse
- utiliser des services qui servent à brouiller les pistes de la provenance des recherches. Le principe en est qu'un serveur intermédiaire fait la requête pour vous, ce qui fait que votre adresse IP n'est pas révélée au moteur de recherche. Plusieurs services de ce type sont proposés en bas de page du site Don't Track Us (donttrack.us), ou encore visitez le site Google Sharing (googlesharing.net) ou FreeNet (freenetproject.org/fr

b) Naviguer dans un site web

Quand je navigue sur un site web, je clique sur des liens, je passe plus ou moins de temps sur certaines pages et éventuellement je quitte le site. Je peux aussi peut-être y télécharger des fichiers, répondre à un sondage, laisser un commentaire, poser une questions dans la section appropriée (ou non!), etc. Chacune de ces actions déclenche une requête au serveur qui est consignée dans le « journal du serveur ». Ce journal contient ainsi plusieurs informations qui peuvent être utiles au propriétaire du site. Par exemple :

Actions du visiteur	Heure	Informations dérivées
Arrive sur le site	15:34	Avec les données de plusieurs utilisateurs, connaître le moment où il y a le plus d'achalandage sur le site.
Clique sur « français »	15:37	Connaître la langue de préférence du ou des utilisateurs. Savoir que l'internaute consulte la page d'accueil en français.
Clique sur le lien du produit *a*	15:39	Savoir combien de temps le ou les utilisateurs passent sur la page d'accueil en français. Savoir que le ou les utilisateurs s'intéressent au produit *a*.
Clique sur le lien vers les prix	15:42	Savoir combien de temps le ou les utilisateurs prennent à lire la page sur le produit *a*. Savoir que l'utilisateur s'intéresse au prix du produit *a*.
Retourne à la page du produit *a*	15:43	Savoir combien de temps l'utilisateur s'est intéressé au prix. Savoir que l'utilisateur s'intéresse encore au produit *a*.
Télécharge le document de présentation détaillée du produit *a*	15:44	Savoir que l'utilisateur s'intéresse suffisamment au produit *a* pour en télécharger le document de description détaillée.
Quitte le site	15:45	Donne une idée du temps passé sur le site.

Les informations obtenues peuvent servir à

- obtenir des statistiques sur ce que les visiteurs font sur le site pour
- améliorer la structure du site, son ergonomie
- avoir une meilleure idée des produits et services qui intéressent les visiteurs dans leur ensemble, ce qui peut servir à orienter les activités de l'organisation ou à améliorer sa stratégie globale de marketing.
- produire un profil persistant de l'utilisateur pour personnaliser ce qu'on lui offre, par exemple, des publicités ciblées à ses intérêts indiqués selon son parcours.

Ces informations peuvent être construites à partir de traces qui se trouvent à plusieurs endroits :
- le journal du site visité
- sur mon ordinateur (cookies, adresse IP, caractéristiques de mon navigateur)
- les informations de mon compte d'utilisateur

On peut apprécier la personnalisation que peut procurer le développement de notre profil de navigation. Par exemple, je suis contentE que lorsque je reviens sur le site, on me présente d'emblée la section en français et des nouvelles qui concernent le produit *a* ou des éléments d'intérêts qui lui sont similaires.

On peut ne pas apprécier qu'on nous montre seulement les éléments déduits de notre profil de navigation. Je m'intéresse aussi à autre chose et je veux avoir le plus de choix possible dans ce qui m'est offert.

Je peux ne pas vouloir qu'on connaisse mes préférences. Dans ce cas que je peux
- rejeter les cookies d'emblée, ou
- les effacer de mon fureteur après avoir visité le site.
- utiliser des plugiciels qui brouillent les traces,
- utiliser des outils qui préviennent les cookies menant à une publicité ciblée (utiliser le service du Network Advertising Initiative et se désabonner de DoubleClick)
- utiliser des logiciels d'anonymisation

Voici quelques lien qui vous présenteront plus en détail les considération des traces qu'on laisse et les moyens qui existent pour les minimiser si tel est notre souhait ;

- Vos traces sur Internet, ce n'est pas virtuel (CNIL)- www.cnil.fr/vos-libertes/vos-traces/

- Surfer anonymement (commentcamarche.net) - www.commentcamarche.net/faq/5351-surfer-anonymement

- Netscop - www.netscop.net/

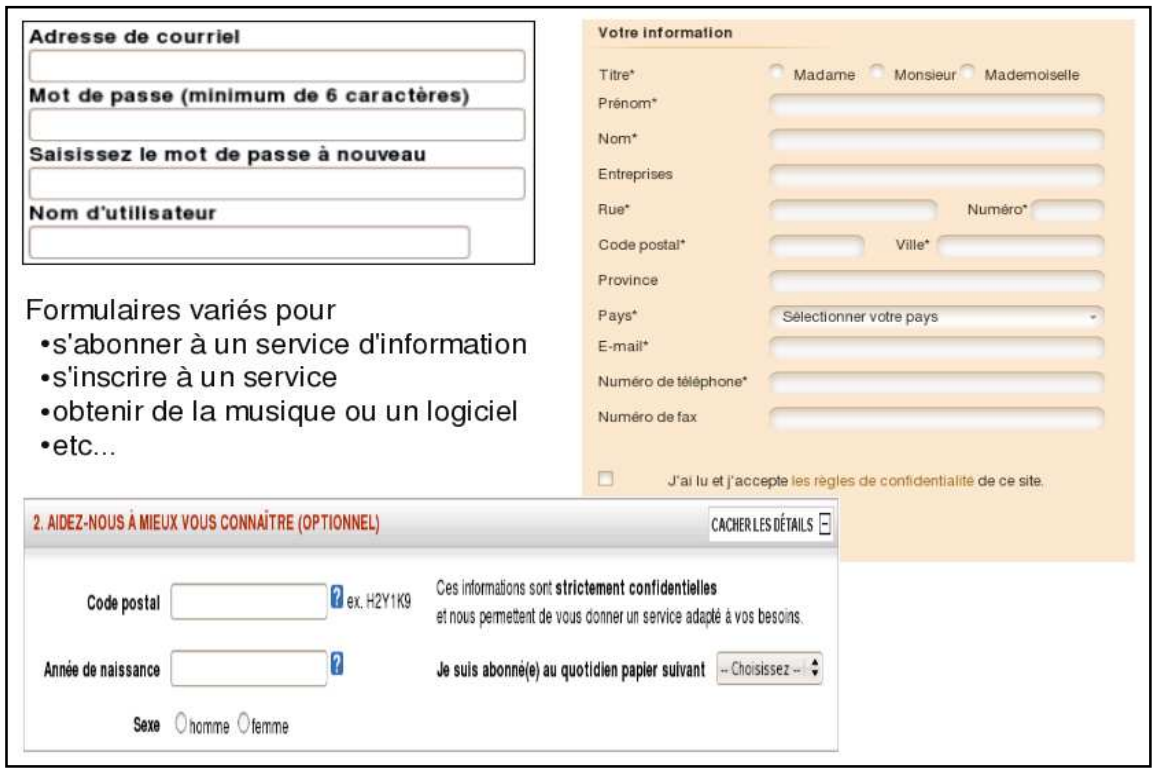
- Outils pour naviguer de manière anonyme

    - Service de désactivation de multiples cookies publicitaires par le service du Network Advertising Initiative - www.networkadvertising.org/managing/opt_out_intl.asp?lang=fren
    - Plugin de désactivation du cookie publicitaire de Google - www.google.com/ads/preferences/plugin/index.html?hl=fr&lr=all

c) Se procurer des services

Je vais sur Internet pour
- télécharger un logiciel
- m'abonner à un site d'intérêt x
- m'abonner à un service

S'il ne s'agit pas d'une visite ou d'un téléchargement direct, on me demandera des informations pour obtenir le service ou le bien qui m'intéresse. L'information qu'on me demande peut être plus ou moins détaillée comme le montrent les exemples suivants :



Il se peut que l'on demande certaines informations à titre optionnel et d'autres de manière obligée, sans quoi le service est refusé.

Certaines de ces informations seront nécessaires au fonctionnement du service lui-même. C'est souvent le cas du nom d'utilisateur, du mot de passe, et de l'adresse courriel.

Les informations qui ne sont pas strictement nécessaires au fonctionnement du service vont généralement servir à

- dresser un portrait de l'ensemble des utilisateurs du service à des fins de mise en marché
- dresser un portrait de l'utilisateur individuel pour personnaliser les services qu'on lui offre
- compiler une liste d'envoi pour du matériel promotionnel ou de mise à jour.

Les risques encourus lors du dévoilement de nos informations au moment de demander un service sont généralement de l'ordre de la sollicitation non désirée sous forme de pourriel ou de bandes annonces sur le site. Dans certains cas, plus rares, il peut y avoir risque de fraude. Pour minimiser ces risques, on pourra choisir quelle information on accepte de donner ou pas selon

- qu'on désire absolument ou non le service ;
- qu'on veuille ou non que nos informations enrichissent les bases de données des fournisseurs de service ;
- à quel point les publicités nous dérangent ou non ;
- qu'on soit attiré ou non par un service plus personnalisé ;
- qu'on fasse confiance ou non au fournisseur de service.

d) Le réseautage social

Il y a une véritable pluie de kits de consignes pour la protection des renseignements personnels sur Internet. Il en existe de plus spécifiques aux sites de réseautage social qui correspondent aux consignes qui sont données pour les blogues, les forums et autres dispositifs en ligne semblables. Pour les réseaux sociaux, ça revient généralement à

- Se renseigner sur le réseau social auquel on veut s'inscrire
- Bien prendre connaissance des politiques de confidentialité du service
- Régler les paramètres de sécurité de son profil au maximum
- Toujours se demander si l'information qu'on publie pourrait être utilisée contre nous ou contre une autre personne
- Se tenir au courant de ce que nos parents, amis et connaissances publient sur nous
- Protéger son mot de passe
- Prendre les mesures de sécurité appropriées lorsqu'on accède au réseau depuis un poste informatique public
- Savoir qu'il n'y a pas de protection parfaite lorsqu'il est question de documents numériques.

Le réseau le plus connu ici, Facebook, se distingue par la complexité des modalités de gestion de la confidentialité et sa morale douteuse au plan de l'appropriation par l'entreprise des informations produite par les membres du réseau.

Quelques enjeux à considérer pour une participation éclairée dans les médias sociaux

- La démarcation entre le public et le privé
- La sécurité des renseignements personnels
- La réputation
- L'employabilité
- La popularité et ou la discrimination

La vulnérabilité à problèmes d'aspects sociaux et psychologiques

e) Activités citoyennes

Internet offre la possibilité de s'exprimer et d'échanger de manière publique sur diverses questions citoyennes ou politiques. Par exemple

- Je réponds à un commentaire sur un article de blogue qui traite de l'action de GreenPeace après le naufrage d'un pétrolier
- Dans un quotidien en ligne, je commente un article qui traite de la hausse des taxes
- Dans un forum, je discute de la question des soins médicaux en fin de vie et de l'euthanasie
- Dans mon blogue, j'argumente en faveur de tel ou tel parti politique pour les prochaines élections
- Depuis FaceBook et Twitter, je contribue à l'organisation ou à la publicité concernant une manifestation en appui à un soulèvement populaire pour la démocratie dans une dictature du monde arabe
- Je signe une pétition contre l'augmentation des frais de scolarité
- Dans le cadre d'une consultation publique, sur le site du gouvernment du Québec, je réponds au questionnnaire associé sur le nettoyage du fleuve Saint-Laurent

Dans chacun de ces cas, j'énonce une opinion d'ordre citoyen ou politique. Je peux exprimer ces opinions en utilisant soit mon nom soit un pseudonyme, selon les circonstances et mes préférences.
Par exemple :

- si je crains que mes opinions politiques m'exposent à des représailles maintenant ou dans le futur, j'utilise un pseudonyme secret
- si je veux que tous connaissent mes opinions - amis, famille, employeurs, collègues, etc. - j'utilise mon nom

- si je veux que seulement certaines personnes puissent m'associer aux opinions que j'exprime, je peux utiliser un pseudonyme qui n'est connu que de certaines personnes. Ainsi, seulement les personnes à qui je choisis de dévoiler mon pseudonyme sauront que ces opinions m'appartiennent.

Le fait de choisir d'utiliser son nom ou un pseudonyme lors de l'expression d'opinions citoyennes peut soulever des questions d'impact et d'intégrité. Ainsi, certains accorderont plus de valeur à une opinion si elle est revendiquée par la personne en son propre nom. Cette valeur peut se trouver encore augmentée si la personne qui exprime son opinion est reconnue comme ayant des connaissances ou des compétences particulières concernant l'objet de discussion.

Dans certains cas, l'utilisation d'un pseudonyme peut soulever des questionnements sur l'intégrité de son utilisateur. Prenons le cas d'un membre du personnel d'un parti politique qui, sous un pseudonyme, tient des propos en faveur de son parti. Le pseudonyme porte à croire que l'opinion énoncée vient d'un citoyen indépendant, ce qui lui donne un poids différent que si on connaissait l'identité de son auteur. On peut dans ce cas considérer qu'il y a fausse représentation. De même, signer plusieurs fois une pétition en utilisant différents noms ou pseudonymes met en péril la crédibilité de la pétition en question.

Annexe : Adopter des pratiques sécuritaires sur Internet

Tiré de la section « Adoptez de bonnes pratique » du site « Je protège mon identité sur Internet » Ministère des Services gouvernementaux (MSG) et Institut de sécurité de l'information du Québec (ISIQ)

1) Soyez prudent lorsque vous donnez vos renseignements personnels sur Internet

Le vol d'identité

Le vol d'identité survient lorsqu'une personne prend possession de vos renseignements personnels sans vous avertir ou sans demander votre permission, généralement en vue de commettre un crime comme une fraude ou un vol.

Un renseignement personnel

Tout renseignement qui concerne une personne et permet de l'identifier, tel que :
- le numéro d'assurance sociale (NAS)
- le numéro de permis de conduire
- le numéro de carte de crédit
- le numéro de compte bancaire et numéro d'identification personnel (NIP)
- le nom, la date de naissance, l'adresse et le numéro de téléphone

Votre date de naissance en soi n'est pas un renseignement personnel car plusieurs personnes ont la même date de naissance. Mais combiné à votre nom et à votre adresse, par exemple, elle devient un renseignement qui pourrait permettre à un fraudeur d'usurper votre identité.

Les renseignements vous identifiant en tant qu'employé d'une entreprise, tels que votre titre, votre adresse et votre numéro de téléphone, ne sont pas considérés comme étant des renseignements personnels au sens de la loi.

À quoi servent les renseignements personnels ?

En général, les renseignements personnels permettent aux organisations de vous identifier afin que vous puissiez , par exemple :
- demander des prêts ou des cartes de crédit
- ouvrir un compte bancaire
- obtenir des documents du gouvernement comme un permis de conduire et une carte d'assurance sociale
- obtenir un passeport
- louer un appartement
- faire des achats

Comment un fraudeur peut-il se servir de vos renseignements personnels?

- Faire une demande de carte de crédit à votre nom mais à son adresse ou tout simplement faire rediriger votre compte existant à son adresse
- Utiliser votre nom pour ouvrir un compte de téléphone cellulaire ou d'autres commodités
- Créer de faux chèques utilisant votre nom et votre numéro de compte bancaire
- Ouvrir un nouveau compte bancaire à votre nom et obtenir des chèques
- Faire une demande de prêt en votre nom
- Obtenir un permis de conduire ou un autre document officiel avec votre nom mais sa photo
- Utiliser votre nom et NAS pour obtenir des avantages sociaux du gouvernement
- Remplir un rapport d'impôt frauduleux avec vos renseignements
- Obtenir un emploi
- Louer un appartement

Donner vos renseignements s'il est arrêté par la police afin que ce soit vous qui soyez poursuivi lorsqu'il ne se présentera pas en cour

2) Gérer son identité numérique

« Gérer son identité numérique » signifie surveiller l'utilisation des éléments constituant notre identité numérique c'est –à-dire l'ensemble des renseignements et des données qui se rapportent spécifiquement à un individu sur Internet.
.
Les éléments composant votre identité numérique pourraient être utilisés à des fins possiblement dommageables. Par exemple :

- vos photos, textes, etc. sont utilisés sans votre consentement et dans un contexte que vous n'approuvez pas
- vos données personnelles sont collectées par des entreprises à votre insu
- votre identité numérique est utilisée pour porter atteinte à votre réputation
- vos renseignements et données sont utilisés par un fraudeur

Plus spécifiquement, un fraudeur pourrait :

- épier vos échanges pour obtenir des renseignements personnels et usurper votre identité
- utiliser les renseignements que vous affichez en ligne pour deviner votre mot de passe et accéder à votre ordinateur

Comment vous protéger?

- Soyez conscient de votre identité numérique
- Soyez conscient qu'une fois un élément de votre identité numérique est affiché sur le Web, vous en perdez le contrôle
- N'affichez aucun renseignement personnel sur Internet

- Si vous devez créer un profil d'utilisateur, utilisez toujours un pseudonyme
- Faites la gestion de vos profils afin de savoir quelles traces vous avez laissées à quels endroits
- Créez des mots de passe sécuritaires

3) Utilisation prudente de certains services Internet afin de déjouer les fraudes

Messagerie instantanée

La messagerie instantanée ou clavardage est un moyen de communication sur Internet permettant d'échanger en temps réel avec une ou plusieurs personnes

Un fraudeur pourrait :

- se faire passer pour quelqu'un d'autre pour gagner votre confiance et vous harceler ou porter atteinte à votre réputation
- épier vos échanges pour obtenir des renseignements personnels et usurper votre identité
- vous transmettre des vers informatiques, des chevaux de Troie, des logiciels espions ou tout autre logiciel malveillant

Comment se protéger

- Utilisez toujours un pseudonyme
- N'affichez aucun renseignement personnel dans votre profil
- Ne donnez aucun renseignement personnel lors de vos conversations
- Protégez la confidentialité de vos parents et de vos amis en ne donnant pas de renseignements personnels à leur sujet
- Méfiez-vous des inconnus
- Méfiez-vous des fichiers et des liens reçus de source inconnue
- Ne cliquez pas sur un lien reçu avec un message publicitaire, même si le message provient d'un contact que vous connaissez
- Assurez-vous que votre logiciel de messagerie instantanée est mis à jour régulièrement

Réseaux sociaux

En ligne, les réseaux sociaux sont des communautés virtuelles qui relient des individus désirant partager leurs intérêts, leurs activités et certains renseignements. C'est un lieu de rencontre virtuel qui permet aux personnes de communiquer entre elles à l'aide de différents outils en ligne tels que la messagerie instantanée et les blogues et les forums de discussion.

Un fraudeur pourrait :

- se faire passer pour quelqu'un d'autre pour gagner votre confiance et vous harceler ou porter atteinte à votre réputation
- épier vos échanges pour obtenir des renseignements personnels et usurper votre identité
- transmettre à votre ordinateur des logiciels malveillants

Comment vous protéger?

- N'affichez aucun renseignement personnel dans votre profil
- Ne donnez aucun renseignement personnel lors de vos échanges
- Protégez la confidentialité de vos parents et de vos amis en ne donnant pas de renseignements personnels à leur sujet
- Méfiez-vous des inconnus
- Protégez-vous des vers informatiques, des chevaux de Troie, des logiciels espions et autre logiciels malveillants
- Utilisez prudemment la messagerie instantanée
- Utilisez prudemment les blogues et les forums de discussion
- Lisez attentivement la politique du site à propos de la protection des renseignements personnels et assurez-vous de bien la comprendre
- Prenez connaissance des paramètres de sécurité par défaut du site de réseautage social

Systèmes de gestion de contenu

Les systèmes de gestion de contenu (SGC) sont des logiciels de conception et de mise à jour de contenu de sites Web. Certains types sont disponibles au grand public et permettent à plusieurs utilisateurs d'alimenter le contenu et de travailler à plusieurs (wikis) et apporter vos commentaires (blogues, forums de discussion en ligne).

Un fraudeur pourrait :

utiliser les renseignements que vous affichez en ligne pour deviner votre mot de passe et accéder à votre ordinateur ou même usurper votre identité
transmettre à votre ordinateur des logiciels malveillants

Comment vous protéger?

- N'affichez aucun renseignement personnel sur Internet
- Si vous devez créer un profil d'utilisateur, utilisez toujours un pseudonyme
- Créez des mots de passe sécuritaires