

Diapo 25 (2005) Conclusion

Visitez : Le site Web du Commissariat à la protection de la vie privée du Canada

http://www.privcom.gc.ca/fs-fi/02_05_d_13_f.asp

Protégez votre vie privée sur l'Internet

Sur le Web Ce qui peut arriver :

Beaucoup de sites Web recueillent des renseignements personnels : certains le font simplement de façon plus évidente.

Certains sites Web demandent de fournir des renseignements personnels avant de donner accès au contenu du site. On peut vous demander votre nom complet, votre âge, votre adresse, votre numéro de téléphone, voire des renseignements sur vos préférences personnelles.

D'autres sites recueillent de l'information de façon plus subtile : ils enregistrent votre adresse Internet et les pages que vous consultez.

Cela passe par l'installation d'un ou plusieurs « [témoins](#) » (cookies) sur le disque dur de votre ordinateur. Les « [témoins](#) » sont de petits fichiers-textes qui peuvent recueillir et stocker divers renseignements dont les suivants :

- L'adresse Internet de votre ordinateur.
- Le nombre de fois que vous avez consulté le site.
- Vos préférences (ex. : langue de communication).
- Votre nom d'utilisateur et votre mot de passe.
- Les articles de votre « panier ».
- Les sites Web que vous avez consultés.
- Des renseignements comme votre nom.
- Tout lien alphanumérique unique qui peut être associé aux renseignements personnels qui vous concernent.

Ces renseignements permettent aux sites Web de vous identifier lorsque vous les consultez de nouveau. Cela vous évite de vous identifier chaque fois que vous consultez le site et permet au site de vous fournir de l'information sur mesure, par exemple les résultats de vos équipes sportives préférées.

Cependant, les [témoins](#) permettent également aux sites Web ou aux réseaux de marketing de créer un profil à partir de renseignements que vous avez fournis et de déterminer vos habitudes de navigation, souvent à des fins publicitaires.

Ce profil peut être communiqué à un annonceur qui choisira, en fonction de vos préférences, les annonces publicitaires qui apparaîtront sur votre écran. Les annonceurs peuvent également utiliser ces renseignements pour envoyer des messages électroniques à caractère publicitaire pour vous proposer des biens et services susceptibles de vous plaire.

Une fois les renseignements recueillis, ils peuvent être utilisés, partagés – et éventuellement faire l’objet d’abus – de toutes sortes de manières. Il peut être difficile de déterminer ce qui arrive aux renseignements personnels qui circulent sur Internet. Les reportages des médias sur les pirates informatiques ayant obtenu l’accès à des sites qui sont en principe protégés et obtenu des numéros de carte de crédit et d’autres renseignements personnels donnent à penser que peu de sites Web, s’il en est, sont vraiment sûrs. Des pratiques médiocres de gestion de l’information et de contrôle de la sécurité peuvent menacer votre vie privée en laissant place à un accès non autorisé. La menace peut également venir d’un initié malhonnête ou mécontent qui a légitimement accès aux renseignements personnels qui vous concernent, mais qui les utilise à des fins frauduleuses.

Il est évident que le meilleur moyen de protéger le caractère confidentiel des renseignements personnels qui vous concernent est de ne jamais les communiquer à un site Web, mais ce n’est pas toujours pratique. Il est commode et utile pour beaucoup de gens de faire de emplettes et d’obtenir des services et des renseignements par le biais d’Internet. Ces activités peuvent exiger la communication de renseignements personnels.

Le meilleur moyen consiste à réduire au minimum la possibilité de recueillir, d’utiliser et de communiquer les renseignements personnels que vous fournissez et à veiller à ce qu’ils soient gérés selon des principes équitables de gestion de l’information. Les politiques de protection des renseignements personnels affichées par les sites Web sont un bon point de départ. Les « sceaux d’attestation » de la protection des renseignements personnels sont une autre garantie pour les utilisateurs de services en ligne. Les lois et règlements du Canada sur la protection des renseignements personnels sont une garantie de plus.

Les organisations assujetties à la [Loi sur la protection des renseignements personnels et les documents électroniques](#) sont tenues de vous informer pleinement et précisément des renseignements personnels qu’elles recueillent à votre sujet, des fins auxquelles elles le font, de ce qu’elles ont l’intention d’en faire et de la manière dont elles les protègent. Ces organisations doivent en tout temps obtenir votre consentement avant de recueillir, utiliser ou communiquer les renseignements personnels qui vous concernent et elles sont tenues de vous proposer divers moyens d’accès à cette information et de régler les problèmes et plaintes éventuels concernant la protection de ces renseignements.

Dans un monde idéal, les entreprises protègeraient en tout temps les renseignements personnels qui vous concernent, mais, malheureusement, ce n’est pas le cas. Voici quelques conseils utiles pour vous protéger vous-même.

Ce que vous pouvez faire

- Lisez toujours les politiques ou les déclarations formulées sur les sites Web concernant la protection des renseignements personnels avant d’en fournir, notamment s’il s’agit de renseignements de nature délicate à caractère financier ou médical. Si vous ne comprenez pas clairement une partie quelconque de cette politique, demandez des éclaircissements. Ne consentez jamais à quelque chose que vous ne comprenez pas.
- Refusez certains ou la totalité des témoins que vous offrent les sites Web. Ils peuvent utiliser ces renseignements à des fins de marketing. Réduisez le volume de renseignements personnels que vous fournissez et ne donnez pas de renseignements qui ne vous sont pas demandés.

Vérifiez les dispositions de non-participation qui permettent de limiter l'usage des renseignements que vous fournissez.

- Naviguez de façon anonyme en utilisant le logiciel d'un tiers qui dissimule votre adresse Internet réelle.
- Employez une adresse électronique jetable au lieu de la vôtre lorsque vous fournissez vos coordonnées à des parties non connues de vous sur Internet.
- Insistez toujours sur l'utilisation de connexions sûres et chiffrées lorsque vous devez communiquer des renseignements confidentiels, par exemple lorsque vous faites des achats ou des opérations bancaires en ligne.

Groupes de clavardage/discussion et forums Ce qui peut arriver :

Si vous participez à des [groupes de clavardage](#) et autres forums en ligne, il se peut que vous affichiez des messages sur un site public que tout le monde peut lire. N'importe qui, du simple curieux aux employés éventuels, peut chercher des exemplaires de vos messages, lesquels peuvent être conservés indéfiniment. Il est possible de trouver les noms des groupes de clavardage ou de discussion auxquels vous participez et les noms des forums auxquels vous êtes abonné. Les noms de ces groupes, à eux seuls, peuvent en dire long sur vous.

Ce que vous pouvez faire :

- Participez à des [groupes de clavardage ou de discussion](#) sous un pseudonyme.
- Soyez discret. Ne fournissez pas de renseignements personnels à moins que ce ne soit absolument nécessaire.
- Utilisez une adresse électronique dont vous pourrez vous débarrasser.
- Certains groupes vous offrent le moyen de supprimer complètement les vieux messages qu'ils conservent : faites-le!

Le courrier électronique Ce qui peut arriver :

Le courriel est un moyen commode et économique de communiquer. Votre adresse électronique ainsi que le contenu de vos messages personnels constituent des renseignements personnels. Soyez toujours attentif aux nombreux risques associés au courriel et sachez comment les réduire.

Les messages non sollicités ou importuns, ce qu'on appelle des pourriels, encrassent les boîtes de courriel de façons de plus en plus agressives et envahissantes. La collecte, l'utilisation et la

communication des adresses électroniques sans le consentement des intéressés est une préoccupation grave et de plus en plus pressante. Il peut également s'agir d'activités frauduleuses ou criminelles.

Certains des messages électroniques non sollicités que vous recevez peuvent sembler « savoir des choses » sur vous et s'adresser précisément à ce qui vous intéresse. Dans ce cas, il se peut que l'on ait dressé un profil à partir d'autres renseignements personnels associés à votre adresse électronique. Si vous avez répondu à une enquête en ligne, participé à un concours, vous êtes inscrit sur une liste d'envoi, avez demandé des renseignements ou avez fait des achats et, par conséquent, fourni votre adresse électronique, vous avez probablement fait l'objet d'un profil. Le profilage est une tactique courante dans le domaine de la publicité et du marketing direct, où il est indispensable de rejoindre un certain type de consommateurs pour réussir.

Les annonceurs et les spécialistes du marketing font tout pour personnaliser leurs messages électroniques et mesurer le taux de réponse aux campagnes de marketing direct. Si vous cliquez sur un lien fourni dans un message, cette manœuvre peut être enregistrée et associée à votre profil. Certains « inondeurs » peuvent même inclure de faux liens de non-participation dans leurs messages : il suffit de cliquer sur un lien quelconque pour confirmer que votre adresse électronique est « active » et qu'elle correspond au profil de quelqu'un qui répond aux messages de marketing direct. Tout mode de réponse mesurable peut être associé à votre profil. Ce profil vaut de l'or. Il peut être vendu des dizaines de fois à travers le monde, à votre insu et sans votre consentement, ce qui donne lieu à d'autres pourriels et à un grave problème de protection de la vie privée.

Autre méthode : l'enchâssement de « pixels espions » dans les messages électroniques, qui renvoient un message à l'expéditeur lorsque le destinataire consulte ou ouvre son courriel. Ces pixels mesurent la consultation du courriel, confirment les adresses électroniques valides et peuvent recueillir des renseignements comportementaux et informatiques sur le sujet. Un pixel espion peut également placer un témoin sur le disque dur de votre ordinateur et fournir une adresse Internet pour les annonces publicitaires incrustées.

Il existe un nouveau type de manœuvre frauduleuse au caractère inquiétant : c'est ce qu'on appelle le « *phishing* » (pêche aux données personnelles). Un artiste de la fraude vous envoie un message électronique qui semble venir d'une entreprise de bonne réputation. Il vous signale un problème concernant votre compte et vous demande de préciser vos numéros de compte et de fournir d'autres renseignements personnels pour « corriger » votre dossier. Ces renseignements serviront ensuite à voler votre identité et à commettre des actes frauduleux.

Certains messages électroniques introduisent des virus, des vers et des chevaux de Troie dans votre ordinateur. Ces messages peuvent être accompagnés de pièces jointes contenant un code malveillant dans votre ordinateur pour corrompre ou pirater votre page d'accueil ou votre modem. Ce code peut se répandre dans d'autres ordinateurs à l'aide de votre liste d'adresses électroniques. Il est possible d'installer des instruments de surveillance à distance qui suivent et transmettent votre comportement en ligne, enregistrent vos habitudes de clavier ou ouvrent des accès dissimulés à votre ordinateur, de sorte que des pirates peuvent effectivement prendre le contrôle de votre ordinateur à distance.

Nous sommes pour la plupart convaincus que l'envoi de messages électroniques est une manœuvre protégée, mais, en réalité, l'envoi d'un message électronique ressemble à l'envoi d'une carte postale. Il n'est pas difficile, techniquement, d'en faire une copie durant sa transmission. Et, lorsque le message est envoyé, vous perdez le contrôle de son acheminement et de son contenu. Dans ce monde de réseaux

électroniques et de communications instantanées, vos messages « personnels » peuvent passer par un forum public et être accessibles au monde entier d'un simple clic. Qu'ils appartiennent ou non au domaine public, les messages électroniques sont souvent archivés et répertoriés de façon permanente. L'une des pires violations de la vie privée en la matière est peut-être ce qui se passe lorsque quelqu'un d'autre utilise votre nom d'utilisateur et votre mot de passe. Grâce à ces renseignements, vos messages peuvent être téléchargés et lus par d'autres pendant des années, à votre insu.

Ce que vous pouvez faire :

- Soyez prudent lorsque vous donnez votre adresse électronique en ligne. Lisez toujours la note relative à la protection des renseignements personnels et assurez-vous que vous avez affaire à une entité licite. À titre de principe, ne donnez pas l'adresse électronique de quelqu'un d'autre en ligne.
- Utilisez des adresses dont vous pourrez vous débarrasser pour vous inscrire à des listes d'envoi, participer à des concours, etc.
- Lisez tous vos messages électroniques hors connexion. Autant que possible, lisez-les en format texte seulement.
- Ne répondez jamais aux pourriels. S'il s'agit d'entreprises licites, choisissez l'option de non-participation dès que possible.
- Installez et utilisez des systèmes anti-pourriel, des pare-feux, des antivirus et autres logiciels de protection des renseignements personnels et de sécurité et tenez-les à jour. Téléchargez et installez des programmes de correction.
- Chiffrez vos messages particulièrement confidentiels.
- N'ouvrez pas les pièces jointes accompagnant les messages d'expéditeurs inconnus.
- Changez régulièrement votre mot de passe pour accéder à votre compte de courriel.
- Lorsque vous retransmettez des messages, supprimez les adresses des destinataires antérieurs.