



## **Amorce 1 - Navigation ou surveillance ?**

Les nouvelles technologies sont en mesure de « surveiller » et de recueillir votre information personnelle et ce, de maintes façons.

### **Adresses IP (ou adresse numérique Internet)**

Lorsque vous visitez un site Web, on accumule des renseignements sur vous. On obtient votre information personnelle lorsque vous acceptez de signer une entente pour obtenir un service, de vous inscrire à un concours, une promotion ou de participer à un sondage. Mais il arrive parfois que vous donniez ces renseignements à votre insu. Certains sites obtiennent cette information en enregistrant votre adresse IP – une adresse numérique unique et rattachée à votre ordinateur, qui permet de vous retracer aisément. S'il est vrai que plusieurs sites n'utilisent pas votre information personnelle pour surveiller vos allées et venues sur Internet, d'autres par contre l'emploient pour vous suivre à la trace et prendre note de tous les sites Web que vous aurez visités.

### **Courrier électronique (ou courriel)**

Le courrier électronique, voilà un moyen facile, amusant et rapide de communiquer avec vos amis. Vous croyez sans doute que vos courriels sont des messages tout à fait privés – il est vrai que votre adresse de courriel et le contenu de vos messages électroniques sont riches en information personnelle et privée. Toutefois, sachez qu'envoyer un courriel c'est comme écrire votre message sur une carte postale – sans enveloppe – et de la mettre à la poste. Avant qu'elle ne parvienne au destinataire, votre carte postale peut être interceptée et lue par n'importe qui.

De plus, le courriel est fort tenace ! Une fois envoyé, le courriel ne disparaît jamais complètement et ce, même si vous l'avez supprimé de votre boîte d'envoi ou de réception. Il laisse une empreinte sur le disque dur des deux ordinateurs – expéditeur et destinataire – et l'utilisateur ne peut contrôler cet état de fait. Il est rare qu'une personne consulte ces empreintes laissées sur le disque dur mais elles sont toujours accessibles et peuvent être retracées par l'administration de l'école, vos professeurs et même vos parents.

### **Pourriel**

Les pourriels sont des messages électroniques non sollicités et envoyés massivement de manière envahissante. La protection de notre vie privée est de plus en plus menacée par cette pratique courante, c'est-à-dire retracer, employer et publiciser votre adresse de courriel sans votre consentement. Le texte de ces messages vous font croire que l'expéditeur vous « connaît » - il cite votre nom ou fait référence à un nom tiré de votre liste d'envoi ou, mieux, vous parle de vos intérêts personnels. C'est la preuve que l'expéditeur de ce pourriel a déjà recueilli une foule de renseignements sur vous. Il a fait une recherche, recueilli des données et créé votre profil – souvent bien avant l'envoi de ce premier message que vous venez de recevoir. Ce pourriel peut poursuivre divers objectifs. Parfois, il sert simplement à vérifier si votre adresse de courriel est encore valide...attention ! vous leur donnez la confirmation tant attendue simplement en cliquant sur l'un des liens contenus dans

le pourriel. Si l'expéditeur n'utilise pas votre profil qu'il a créé, il peut le vendre à des agences de marketing sans votre consentement. La plupart du temps, vous n'en saurez rien. Quelle est la meilleure façon de vous protéger? Jetez ce pourriel à la corbeille sans l'ouvrir et surtout n'y répondez jamais.

### **Pixel espion (ou pourriel invisible)**

Le pixel espion se cache dans un courriel qui, une fois ouvert, transmet de l'information à l'expéditeur. Il peut enregistrer le temps que vous mettez à lire ce courriel, la durée pendant laquelle ce courriel est demeuré ouvert dans votre ordinateur ou confirmer la validité de votre adresse électronique. D'autres pixels espions peuvent recueillir des renseignements personnels figurant dans votre ordinateur et même installer des témoins (cookies) et des fenêtres publicitaires intempestives ( pop-ups) dans votre ordinateur.

### **Hameçonnage**

Avez-vous déjà reçu un courriel vous annonçant que vous aviez gagné à la loterie ? C'est ce qu'on appelle de l'hameçonnage, une tentative de fraude et d'usurpation de votre identité par courriel. Il s'agit d'un faux courriel, apparemment authentique, qui emprunte l'identité d'une compagnie ou d'une banque par exemple et dans lequel on vous annonce qu'on doit résoudre un problème relié à votre compte ou qu'on doit y faire un dépôt. L'expéditeur vous demande donc de lui fournir des renseignements personnels et confidentiels comme votre numéro de compte bancaire ou autre. Il vaut mieux ignorer et jeter à la corbeille ces courriels...et ne pas mordre à l'hameçon !

### **Virus**

Dans le pire des cas, un message électronique peut contenir des virus en tous genres (de type worms et trojans par exemple) et infecter votre ordinateur. Des pièces jointes peuvent contenir des codes malicieux et corrompre vos dossiers ou de pirater votre page d'accueil ou votre connexion à Internet. Ce code peut se transmettre à d'autres ordinateurs par l'entremise de votre carnet d'adresses. Il peut installer des systèmes de surveillance à distance afin de noter et de divulguer vos habitudes de navigation sur le Net, d'enregistrer vos saisies sur clavier ou encore d'ouvrir des portes dérobées de votre système afin de permettre aux pirates informatiques d'en prendre le contrôle à distance.

### **Des solutions pratiques**

- Avant de transmettre votre adresse électronique, assurez-vous que vous transigez réellement avec la compagnie visée et non une compagnie bidon.
- Créez et utilisez une adresse de courriel spécifiquement pour les concours, les listes d'envoi, etc.
- Lisez tous vos messages électroniques hors connexion. Si possible, faites cette lecture uniquement en format texte.
- Ne répondez jamais et d'aucune façon aux pourriels. Lorsque vous faites des transactions monétaires sur Internet, soyez brefs et quittez le site le plus rapidement possible.
- Installez sur votre ordinateur et utilisez des logiciels de protection antivirus, anti-espion, coupe-feu et autres et gardez-les à jour. À partir de votre

- système d'opération, téléchargez et installez les mises à jour automatiques de sécurité.
- Prenez soin de crypter vos messages très personnels avant de les envoyer par courriel.
  - N'ouvrez jamais les pièces jointes d'un message envoyé par un expéditeur inconnu.
  - Modifiez régulièrement le mot de passe de vos comptes de messagerie électronique.
  - Avant de transférer un courriel à un tiers, supprimez les adresses électroniques des premiers destinataires ayant reçu ce message.

Pour de plus amples informations, voir le chapitre 4 du recueil intitulé *Techno-tonomy* (disponible seulement en anglais).

© Alberta Civil Liberties Research Centre, 2006. Reproduit avec la permission.