

## Articles du 17 octobre 2003

Dans cette édition :

1. Prenez garde : des logiciels vous espionnent!
2. Publicité ou pourriel? Évitez les pièges en posant les bonnes questions
3. Quand les TI se font anges gardiens
4. Bromont : première ville à se mériter le label « Ville Internet » à l'extérieur de l'hexagone

**1. Prenez garde : des logiciels vous espionnent!** - Ils s'installent sournoisement sur votre ordinateur, collecte des données sur la configuration de votre ordinateur et vos habitudes d'internaute, puis transmettent le tout à des firmes de marketing : les logiciels espions s'immiscent dans votre vie à votre insu et peuvent divulguer vos renseignements les plus intimes.

On entend par « logiciels espions » – *spyware* en anglais ou encore *espiogiciels* pour les avides de néologismes – des petits programmes informatiques qui s'installent sur votre ordinateur sans que vous ne le sachiez. On les retrouve intégrés en complément d'un logiciel principal, le plus souvent des gratuits et des applications pour le poste-à-poste (P2P) comme Kazaa. Ils collectent et conservent des données, entre autres, sur votre comportement d'internaute, sur la configuration de votre ordinateur ou la liste des sites Web que vous avez visités. Ils iront parfois même jusqu'à tenir un registre du contenu de votre disque dur ou à le balayer à la recherche de mots de passe ou de courriels.

Les données ainsi récoltées sont ensuite envoyées par Internet à leur auteur, soit habituellement un concepteur de gratuits qui souhaite arrondir ses fins de mois en vendant vos données personnelles à une firme de marketing. Gare ensuite aux pourriels, aux fenêtres-pubs d'entrée (pop-ups) qui apparaissent sans cesse dans votre messagerie instantanée et autres désagréments! En plus de vous envahir de publicités non sollicitées, ils accaparent votre bande passante, votre mémoire vive et votre disque dur. Le pire dans tout ça : leur légalité. En effet, sous le couvert d'une volonté d'offrir un bon service aux clients par la mise à jour de leurs logiciels ou la correction des erreurs rencontrées par leurs clients, les concepteurs de logiciels ont le droit d'utiliser les *espiogiciels* avec le consentement de l'utilisateur. Encore faut-il que les clients lisent les politiques d'utilisation en petits caractères avant de les télécharger, ce qui n'est malheureusement pas toujours le cas.

Comment s'en protéger ou s'en débarrasser? Les antivirus et les coupe-feux ne suffisent souvent pas à la tâche. Les *espiogiciels* ont plus d'un tour dans leur sac : ils se modifient et se déplacent sur votre ordinateur à chaque semaine, voire parfois même à chaque jour. Une panoplie de logiciels spécialisés, gratuits ou non, permettent de les enrayer. Certains les empêchent d'envoyer les données à des serveurs externes, d'autres bloquent leur installation ou les détectent et les suppriment sur votre ordinateur infecté. Les plus

sophistiqués offrent toutes ces options à la fois et fournissent même une liste des logiciels espions installés sur votre ordinateur, leur localisation et leurs fonctions.

Malgré tous ces logiciels disponibles, il n'en demeure pas moins qu'une prudence élémentaire de l'internaute s'avère le meilleur moyen de contrecarrer ces nuisances. Lire les petits caractères des contrats d'installation des logiciels avant de les installer et demeurer à l'affût des logiciels espions en cours sur le marché devraient vous garder à l'abri de leur intrusion.

Rédactrice : Isabelle Vachon, analyste-conseil en veille stratégique et enquêtes, CEFRIO  
Sources :

Isabelle Falque-Pierrotin, 2003, «Est-il vrai que lorsque l'on télécharge certains logiciels, des programmes espions s'installent sans que l'on en soit informé ? », *Droit du Net.fr*.  
[http://www.droitdunet.fr/par\\_profils/lecture.phtml?type=profil\\_internaute&it=6&id=72](http://www.droitdunet.fr/par_profils/lecture.phtml?type=profil_internaute&it=6&id=72)

Richard Koontz, 13 octobre 2003, "Spyware Removal Tools Stop Snoopers", *E-Commerce News*.  
<http://www.ecommercetimes.com/perl/story/31833.html>

Vincent Ryan, 7 octobre 2003, "Internet Sleuths for Hire : Defeating Spyware", *NewsFactor*.  
<http://www.newsfactor.com/perl/printer/22432/>

**2. Publicité ou pourriel? Évitez les pièges en posant les bonnes questions** - Une boîte de réception remplie de courriels gênants, dans tous les sens du terme, ça vous dit quelque chose? Les pourriels (*spam*), qui promettent mer et monde, constituent un irritant quotidien pour bien des internautes. Et pourtant, pour plusieurs entreprises le marketing par courriel demeure un outil promotionnel très efficace.

Certes, la meilleure option du marketing par courriel demeure la conception de sa propre liste de prospects en offrant aux internautes la possibilité de s'y inscrire. Cependant, certains peuvent être tentés par l'option plus facile que constitue l'achat d'une liste compilée par un tiers.

Afin d'éviter les pièges du pourriel, voici les questions clés à poser au fournisseur d'une telle liste :

- **Comment et quand le consentement des individus a été vérifié?** Revoir le processus de collecte d'autorisation d'utilisation des adresses pour s'assurer de l'aval de leur propriétaire. Dans les cas québécois et canadiens, tout doit être conforme à la **Loi sur la protection des renseignements personnels** qui stipule que la vente de renseignements personnels ne peut se faire sans le consentement de la personne concernée.
- **À quelle fréquence les individus reçoivent-ils les messages?** S'assurer que les courriels ne sont pas trop rapprochés en matière de temps. Si un fournisseur ne peut pas fournir ce détail, il faut changer de fournisseur.
- **Est-ce que de nouveaux noms sont ajoutés fréquemment? Est-ce que les adresses qui annulent leur abonnement sont retirées rapidement?** Cette dernière question est capitale pour éviter d'être associé aux pourriels par les individus qui ont exprimé leur volonté de ne plus faire partie de la liste.

- **Est-ce que la liste est exclusive à ce fournisseur?** Si elle ne l'est pas, elle risque d'être employée plus fréquemment et ce, peut-être, par des concurrents.
- **Qu'est-il écrit dans l'en-tête et le bas de page des courriels?** Le texte doit clairement expliquer pourquoi les destinataires reçoivent le courriel et comment ils peuvent mettre à jour leur profil ou, encore, comment ils peuvent se désabonner.
- **À quoi ressemble le texte d'identification de l'expéditeur du courriel (sender line)?** Très importante question à poser puisque les destinataires détruisent les courriels dont ils ne connaissent pas l'origine.
- **Comment le fournisseur s'assure-t-il de réellement envoyer les courriels? Quel est le taux de courriels non envoyés?** S'assurer que le fournisseur peut garantir que les courriels ne seront pas filtrés comme des pourriels.
- **Est-ce qu'il y a des limites à la créativité?** Les fournisseurs doivent surveiller le contenu des courriels et fournir des conseils pour qu'ils passent au travers des filtres. Par exemple, certains filtres n'acceptent pas les messages qui sont en HTML.
- **Quel est le degré de réceptivité des destinataires de la liste?** Est-ce que la liste est composée d'individus qui ont manifesté leur intérêt pour le produit ou service vanté par le courriel? Si oui, le courriel doit en tenir compte, sinon il doit en tenir compte également.
- **Combien ça coûte, pourquoi et pour combien de temps? Est-ce qu'une politique garantit que les courriels seront correctement envoyés? Y a-t-il des conditions spécifiques? Y a-t-il un service après-vente?** Connaître tous ces détails permet de mieux gérer la campagne et de s'assurer un meilleur retour sur l'investissement.

Avec les bonnes questions et les bonnes réponses, le recours à de telles listes peut offrir une alternative intéressante aux « listes maison » et permettre un certain succès à une campagne de marketing par courriel.

Rédactrice : Caroline Jacob, analyste-conseil en veille stratégique, CEFRIO  
 Source : Al DiGuido, « Questions to Ask Before Renting a List », Small Business Computing.com, 21 août 2003.  
<http://www.smallbusinesscomputing.com/emarketing/article.php/3066681>

**3. Quand les TI se font anges gardiens** - Le pire cauchemar des parents est sans aucun doute de voir leurs enfants harcelés, agressés ou pire encore, enlevés. Or, si une sensibilisation des jeunes aux dangers qui les guettent demeure sans conteste l'une de leurs meilleures armes, la technologie peut cependant elle aussi – et de plus en plus - renforcer la sécurité des petits comme des plus grands et partant, diminuer l'angoisse des parents.

Les dispositifs de sécurité personnelle prennent en effet depuis quelques temps déjà la forme de divers produits destinés à la protection des enfants. Ayant le grand avantage d'être littéralement fixés à l'enfant, ces dispositifs sont de plus en plus populaires. Ils se présentent selon un vaste éventail, de la simple alarme qui, une fois déclenchée, émet un son à briser les tympans, au nec plus ultra des systèmes de protection, une unité qui ressemble à s'y méprendre à un inoffensif bracelet-montre, à la grande différence près cependant que le dispositif est verrouillé au poignet de l'enfant et connecté à un système de localisation par satellite basé sur la technologie GPS. Certainement le plus sophistiqué d'entre tous, ce système rend compte de la position et des mouvements de son utilisateur,

permettant ainsi aux parents de localiser leur progéniture. Encore faut-il toutefois avoir les moyens d'en munir son bambin – le fameux bracelet-montre coûte tout de même environ 200 \$US – et habiter aux États-Unis, dans une région desservie par des réseaux de satellites appropriés.

Mais si les jeunes doivent être prémunis contre les dangers de la rue, ils doivent aussi, et dans la très grande majorité des cas (1), savoir reconnaître les menaces de l'univers virtuel. Et entre tous les risques que comporte Internet, la rencontre de personnages peu recommandables lors de sessions de clavardage est certainement l'un des plus inquiétants.

C'est à partir de ce constat et pour enseigner aux enfants les rudiments de la sécurité en ligne, qu'une petite entreprise de logiciels éducatifs basée à Vancouver (Live Wires) a développé il y a quelques années déjà le jeu sur ordinateur Missing. Ayant fait son apparition en février 2000 au Canada, le logiciel connaîtra sous peu un nouvel essor chez nos voisins du Sud, puisque des représentants du congrès américain, d'organismes chargés de l'application de la loi et de grands de l'industrie du jeu sur ordinateur, propulseront sa distribution dans 25 États supplémentaires.

Destiné à mettre les enfants au courant des dangers et des tactiques des prédateurs du Net, Missing est basé sur une histoire vraie : Zack, un adolescent canadien, est leurré par un homme éminemment sympathique, mais pédophile à ses heures, qui le persuade de faire une fugue et de l'accompagner à l'étranger. Le but du jeu : agir en véritable limier et retrouver Zack avant que le plan du prédateur n'ait totalement réussi. À noter que Missing a par ailleurs aidé les autorités américaines à appréhender de véritables pédophiles, les policiers ayant bénéficié d'indices fournis par des adolescents inspirés par leur expérience du logiciel.

Fort du succès de Missing, Live Wires compte en outre lancer sous peu Mirror Image, une vidéo interactive qui présente toujours les dangers reliés aux prédateurs du Net, mais qui vise cette fois les adolescents.

Les TI, on le voit, peuvent contribuer à rassurer les parents et les aider à sensibiliser leurs jeunes aux périls d'Internet. Il n'en tient en fait qu'à nous de repousser leurs limites pour encore mieux les mettre au service de la sécurité des enfants.

Note :

1- Selon l'enquête NetAdos menée en 2003 par le CEFRIO, 99 % des jeunes Québécois de 12-17 utilisent en effet Internet. Pour plus d'information, veuillez noter que le rapport complet de l'enquête et la brochure qui en présente les principaux résultats sont disponibles tout à fait gratuitement sur le site du CEFRIO aux adresses :

<http://www.cefrio.qc.ca/rapports/NetAdos-2003-rapp.pdf>

[http://www.cefrio.qc.ca/rapports/Net\\_Ados\\_2003.pdf](http://www.cefrio.qc.ca/rapports/Net_Ados_2003.pdf)

Rédactrice : Catherine Lamy, analyste-conseil en veille stratégique, CEFRIO

Sources :

David Porter, « Child security devices becoming more common », Canada.com News, 13 octobre 2003 (page consultée le 15 octobre 2003)

<http://www.canada.com/technology/wires/story.html?id=2C2C400A-4839-4B1C-8C8B-9710F2381B5D>

Paul Koring, « New software teaches kids Internet safety », The Globe and Mail, 1er octobre 2003 (page consultée le 15 octobre 2003)

<http://globeandmail.workopolis.com/servlet/Content/fasttrack/20031001/UCOMPM?section=Dot-com>

Life Wires Design Ltd (page consultée le 16 octobre 2003)

<http://www.livewwwires.com/>

**4. Bromont : première ville à se mériter le label « Ville Internet » à l'extérieur de l'hexagone** - Le 14 octobre 2003, à l'occasion de la cérémonie de remise des labels 2003 «Ville Internet», monsieur Jean-Yves Beaudoin, directeur du projet Bromont ville branchée, s'est vu décerner au nom de la Ville de Bromont le prestigieux label par monsieur Jean-Louis Borloo, ministre délégué à la Ville et à la Rénovation urbaine, madame Claudie Haigneré, ministre déléguée à la Recherche et aux Nouvelles technologies, monsieur Francis Mayer, directeur général de la Caisse des dépôts et consignations et monsieur Emmanuel Eveno, président de l'Association Villes Internet et du jury du Label Ville Internet. Bromont est ainsi la toute première ville à l'extérieur de la France à se mériter un tel honneur.

Le label « Ville Internet » reconnaît les cités qui valorisent, développent et diffusent l'usage des TI auprès de leurs citoyens et est illustré par l'octroi d'une à cinq arobases. Cette année, 252 villes et communes se sont méritées le label. À l'instar de treize localités françaises, Bromont a reçu 4 arobases, tandis que seulement trois villes ont vu leurs efforts récompensés par 5 arobases.

Félicitations à toute l'équipe du projet Bromont, ville branchée, partenaire du CEFRIO dans le cadre du projet Développement des collectivités locales et régionales par les TI.

Rédactrice : Catherine Lamy, analyste-conseil en veille stratégique, CEFRIO

Sources :

Communiqué de presse, « Bromont ville branchée reçoit 4 arobases au «Label Ville Internet 2003» de France », 14 octobre 2003

[http://www.bromont.net/index\\_ie\\_new1.htm](http://www.bromont.net/index_ie_new1.htm)

Site du réseau Villes Internet, <http://www.villes-internet.net/>

---

Ce bulletin est préparé par le CEFRIO :

Pour consulter les archives du bulletin : [http://www.cefrio.qc.ca/pub\\_bul.cfm](http://www.cefrio.qc.ca/pub_bul.cfm)

Reproduction: les nouvelles du bulletin SISTech peuvent être reproduites à des fins non commerciales à la condition expresse d'indiquer la mention suivante: Bulletin SISTech, CEFRIO et de créer un hyperlien à l'adresse : <http://www.infometre.cefrio.qc.ca>