



NNEDV

Qui vous espionne lorsque vous utilisez votre ordinateur?

AVERTISSEMENT DE SÉCURITÉ: Il y a longtemps que le harcèlement existe, mais il est plus facile que jamais pour les auteurs de ce crime de harceler, de suivre et de surveiller leur victime. Les gens qui se livrent à la violence, au harcèlement ou à d'autres crimes peuvent maintenant utiliser un logiciel espion pour surveiller ce que fait une personne lorsqu'elle utilise son ordinateur ou un appareil portable, par exemple un téléphone cellulaire, sans qu'elle le sache. Si vous pensez que quelqu'un vous surveille ou si vous vous sentez traqué, vous devez savoir les choses suivantes:

- il pourrait être dangereux pour vous d'essayer de détecter un logiciel espion installé sur votre ordinateur, appareil portable ou téléphone cellulaire, parce que la personne qui vous surveille peut savoir immédiatement que vous effectuez des recherches en ce sens;
- vous devez utiliser un ordinateur ou un appareil portable sécuritaire (un appareil auquel la personne qui vous surveille n'a pas accès directement ou à distance) pour effectuer des recherches dans Internet ou pour envoyer des courriels que vous ne voulez pas que la personne puisse lire;
- si vous voulez conserver des preuves de l'installation d'un logiciel espion dans votre ordinateur, veuillez communiquer avec le service de police de votre ville.

Pour consulter des listes de logiciels et d'appareils espions qui sont faciles à installer dans un ordinateur et qui peuvent être utilisés pour espionner un amant, une petite amie, un petit ami, un partenaire, un mari ou une femme et pour surveiller en secret l'utilisation que fait une épouse infidèle de son ordinateur, il suffit de taper « espionner sa femme » dans n'importe quel moteur de recherche.

QU'EST-CE QU'UN LOGICIEL ESPION?

Un logiciel espion est un logiciel informatique ou un appareil qui permet à une personne (mal intentionnée) de surveiller en secret l'utilisation qu'une autre personne fait de son ordinateur et de recueillir des renseignements de cette façon, sans y être autorisée.

Il existe de nombreux types de logiciels informatiques et d'appareils qu'on peut installer dans un ordinateur pour surveiller l'utilisation qui en est faite. Quelqu'un peut installer ces appareils ou logiciels dans votre ordinateur sans que vous le sachiez, sans même nécessairement avoir directement accès à votre ordinateur. La surveillance informatique est légale dans certains États, illégale dans d'autres, et cela dépend aussi du contexte dans lequel le logiciel ou l'appareil est installé et utilisé. Dans tous les cas, les logiciels espions sont importuns, envahissants et peuvent représenter un grand danger pour les victimes.

Les logiciels espions sont parfois présentés par les entreprises qui les vendent comme le moyen de surveiller des enfants ou des employés. Si vous êtes un employeur, vous devriez demander à vos employés de lire et de signer une politique d'utilisation des outils technologiques. Cette politique devrait expliquer les utilisations permises des biens de l'entreprise, définir les attentes quant aux gestes qui peuvent être posés en ligne, et en INFORMER les employés lorsque leur ordinateur fait l'objet d'une surveillance. En outre, vous devriez choisir un progiciel qui affiche une icône rappelant aux employés qu'ils sont surveillés. (*Voir aussi la remarque à l'intention des parents à la fin du présent texte.)

Il existe certaines ressemblances et différences entre les logiciels espions et les logiciels connexes. Voici quelques exemples:

- **Logiciel publicitaire:** Il s'agit de logiciels de marketing cachés qui affichent des publicités sur les écrans des consommateurs, qui peuvent aussi servir à établir le profil des utilisateurs d'Internet quant à leurs habitudes de navigation et de magasinage. Les logiciels publicitaires sont souvent cachés dans un autre logiciel téléchargé par un utilisateur, ou encore en font partie. La plupart des ordinateurs ordinaires sont touchés par les logiciels publicitaires assez régulièrement, et les signes courants sont notamment le ralentissement du système et beaucoup de fenêtres flash publicitaires.
- **Logiciel malveillant:** Il s'agit de tout programme qui tente de s'installer dans un système informatique de lui-même ou de l'endommager sans le consentement du propriétaire. Ce sont notamment des virus, des vers, des logiciels espions et des logiciels publicitaires.

Pour de plus amples renseignements sur les logiciels publicitaires et malveillants, veuillez consulter le document intitulé « Protecting Your Computer » à l'adresse suivante (en anglais seulement):

<http://www.antispywarecoalition.org/documents/documents/ProtectingYourComputerflyerletter.pdf>.

COMMENT LES LOGICIELS ESPIONS FONCTIONNENT-ILS?

Les logiciels espions permettent de surveiller tout ce que vous saisissez au clavier, toute utilisation d'une application logicielle que vous faites, tous les sites Web que vous visitez, toutes les séances de clavardage auxquelles vous participez, tous les messages instantanés que vous envoyez, tous les documents que vous ouvrez et tout ce que vous imprimez. Certains logiciels espions permettent à la personne qui l'utilise de geler votre ordinateur, de l'éteindre ou de le redémarrer. Certaines versions de ces logiciels permettent même d'activer votre caméra Web à distance ou de faire parler votre ordinateur.

Une fois qu'un logiciel espion est installé, il peut fonctionner en mode furtif et être difficile à détecter ou à désinstaller. Si la personne qui l'a installé a directement accès à votre ordinateur, elle peut utiliser une combinaison de touches particulières pour faire afficher un écran d'ouverture de session. En saisissant le mot de passe, elle fait ensuite afficher une fenêtre qui lui permet de prendre connaissance de tout ce que vous avez fait avec votre ordinateur depuis la dernière session, notamment les courriels que vous avez envoyés, les documents que vous avez imprimés, les sites Web que vous avez visités, etc. Si la personne n'a pas directement accès à votre ordinateur, elle peut demander au logiciel espion d'effectuer des saisies de votre écran à intervalles de quelques secondes et de les lui envoyer par Internet sans que vous le sachiez.



COMMENT UN LOGICIEL ESPION PEUT-IL SE RETROUVER DANS MON ORDINATEUR?

La personne qui veut vous surveiller peut installer un logiciel espion dans votre ordinateur ou un appareil portatif que vous possédez si elle y a directement accès ou si elle y a accès par Internet. Certaines personnes peuvent accéder à votre ordinateur à distance par Internet. Il se peut aussi qu'on vous envoie un logiciel espion comme pièce jointe qui s'installe automatiquement lorsque vous ouvrez le courriel ou que vous l'affichez dans une fenêtre d'aperçu. Autre possibilité: on peut vous faire parvenir par courriel ou par message instantané une carte de souhait ou un jeu, ou encore utiliser une autre tactique pour vous inciter à ouvrir une pièce jointe ou à cliquer sur un lien, ou encore inciter vos enfants à le faire. Une fois ouvert, le programme installe automatiquement un logiciel espion dans l'ordinateur de la victime, en mode furtif, sans avis ou sans le consentement de la victime, et le logiciel espion peut ensuite envoyer des rapports électroniques à la personne qui en est à l'origine par Internet.

La plupart des outils d'espionnage informatique sont des logiciels (il s'agit de programmes qu'on installe dans un ordinateur), mais il y a aussi des appareils qui remplissent la même fonction et qu'on appelle des enregistreurs de frappe. Ces petits appareils qui enregistrent la frappe peuvent sembler faire partie de l'ordinateur. Cependant, lorsque l'appareil est branché à votre ordinateur, il est en mesure d'enregistrer sur un petit disque dur ce que vous saisissez au clavier, tous les mots de passe, numéros d'identification personnels (NIP), tous les sites Web que vous visitez et tous les courriels que vous envoyez. Il existe en outre des claviers qui permettent d'enregistrer la frappe.

Remarque: N'oubliez pas que de nombreux appareils portatifs sont de mini-ordinateurs. Il existe maintenant des logiciels espions pour les téléphones cellulaires et les autres appareils portatifs, qui permettent à une personne de surveiller les messages-textes que vous envoyez et les numéros de téléphone que vous composez. *(Remarque: Il est aussi possible d'obtenir le registre d'appels autrement qu'à l'aide d'un logiciel espion, par exemple en devinant votre mot de passe et en accédant à votre compte de services téléphoniques sur le site Web du fournisseur, ou encore en consultant l'historique d'appels de votre téléphone.)*

COMMENT FAIRE POUR SAVOIR SI UN LOGICIEL ESPION EST INSTALLÉ DANS MON ORDINATEUR?

- Si votre ordinateur est actuellement sous surveillance, il peut être dangereux pour vous d'essayer de détecter un logiciel espion ou d'utiliser un logiciel qui sert à repérer les logiciels espions. Si votre ordinateur est touché, le logiciel espion enregistre toutes vos tentatives de recherche et alerte la personne qui vous surveille.
- Si vous pensez que quelqu'un a installé un logiciel espion pour surveiller vos activités, consultez un défenseur des droits des victimes avant d'essayer de désinstaller le logiciel espion. La police ou encore un expert judiciaire en informatique pourront peut-être vous aider si vous souhaitez conserver des preuves qui pourraient être nécessaires dans le cadre d'une enquête criminelle.

En général, les logiciels espions fonctionnent en mode furtif et utilisent des noms de fichiers fictifs, ce qui fait qu'il est extrêmement difficile de détecter ces logiciels lorsqu'ils sont installés dans un ordinateur.

Si un logiciel espion est installé dans votre ordinateur et surveille votre utilisation de celui-ci, il se peut que vous ne remarquiez aucun changement dans le fonctionnement de l'ordinateur (c.-à-d. que l'ordinateur ne va pas nécessairement ralentir ou geler). Par ailleurs, tout comme dans le cas des virus informatiques, il existe des centaines de logiciels espions différents. Ainsi, certains logiciels sont créés par de grandes entreprises de logiciels, mais d'autres le sont par des « pirates informatiques ».

Il y a sur le marché toutes sortes de logiciels qui servent à détecter les logiciels espions, mais ceux-ci servent surtout à détecter les logiciels publicitaires et les logiciels malveillants, sans pour autant nécessairement permettre de découvrir un logiciel espion utilisé pour surveiller quelqu'un. En outre, les logiciels de détection des logiciels espions ne permettent généralement pas de détecter les appareils comme les enregistreurs de frappe.

Si vous pensez qu'un logiciel espion est installé dans votre ordinateur, les conseils qui suivent s'adressent à vous.

CONSEILS POUR LES SURVIVANTS

- Si vous utilisez l'ordinateur sous surveillance pour essayer de détecter les logiciels espions installés dans celui-ci ou pour essayer de télécharger un logiciel de détection de logiciels espions, le logiciel espion consignera toutes vos activités et alertera la personne qui vous surveille, ce qui peut être dangereux.
- Vous devriez chercher à utiliser un ordinateur sécuritaire lorsque vous consultez des ressources sur la violence conjugale ou sexuelle. Il serait plus sûr que vous utilisiez un ordinateur dans une bibliothèque publique, un centre communautaire ou un cybercafé.
- Si vous pensez qu'une personne mal intentionnée a accès à vos courriels ou à votre service de messagerie instantanée (MI), vous devriez envisager de créer de nouveaux comptes de courriel/de MI à partir d'un ordinateur sécuritaire. N'ouvrez pas de nouveaux comptes et ne prenez pas de messages à partir d'un ordinateur si vous pensez qu'il peut être sous surveillance. Privilégiez les comptes de courriel Web et les noms et renseignements sur votre compte qui ne permettent pas de vous identifier, (p. ex., chatbleu@courriel.com et non votrevrainom@courriel.com). Par ailleurs, assurez-vous de bien lire le contenu des écrans d'inscription, de façon à pouvoir choisir d'exclure votre nom des répertoires en ligne.
- Méfiez-vous si une personne ayant un comportement violent a installé un nouveau clavier, un nouveau câble ou un nouveau logiciel, ou encore a récemment réparé votre ordinateur et que cela coïncide avec une surveillance ou une impression d'être traqué plus importante qu'auparavant.
- Si vous songez faire l'acquisition d'un nouvel ordinateur, il y a des mesures que vous pouvez prendre pour réduire le risque qu'un logiciel espion soit installé dans votre nouvel ordinateur, même s'il est impossible d'éliminer totalement les risques.
 - Installez un pare-feu et activez-le. Il existe des pare-feu sous forme de logiciels et d'appareils. Si votre ordinateur n'est pas muni d'un pare-feu intégré, vous pouvez télécharger un logiciel à l'adresse suivante: <http://www.zonealarm.com>.
 - Installez au moins un logiciel antivirus dans votre ordinateur afin qu'il cherche activement des virus qui peuvent être dans votre ordinateur et assurez-vous que les définitions de virus du logiciel sont à jour, puisque de nouveaux virus dangereux sont libérés quotidiennement. Il se peut que vous deviez demander à votre ordinateur d'effectuer de façon automatique les mises à jour des définitions de virus et d'effectuer des recherches de virus quotidiennes. Assurez-vous de renouveler votre abonnement au logiciel antivirus tous les ans.
 - Installez des logiciels servant à détecter des logiciels espions avant même d'effectuer une connexion à Internet et assurez-vous que les définitions de logiciels espions de ces logiciels sont mises à jour de façon automatique et régulière.
- Fiez-vous à votre intuition et cherchez à détecter des régularités. Si la personne qui vous surveille sait des choses que vous n'avez dites qu'à des gens par courriel ou par messagerie instantanée, votre ordinateur est peut-être infecté par un logiciel espion. Si vous pensez qu'une personne vous surveille, c'est probablement parce que c'est le cas.

Pourquoi ne puis-je me contenter de « supprimer » mon historique de navigation?

- Il est impossible d'effacer toute trace de navigation dans votre ordinateur, surtout parce que les logiciels espions enregistrent toutes vos tentatives de suppression des nombreux historiques qui figurent dans votre ordinateur. En réalité, il y a des centaines d'historiques cachés dans votre ordinateur. Par ailleurs, la personne qui vous surveille peut se méfier et vous surveiller de plus près si elle suit vos activités et votre historique depuis un moment et s'aperçoit tout à coup que vos historiques de navigation sont vides.
- Les logiciels espions enregistrent tout ce que vous faites avec votre ordinateur ou avec votre appareil, puis enregistrent toutes vos tentatives de suppression des traces de vos activités. Dans certains cas, les logiciels espions sont impossibles à détecter à moins de demander à un spécialiste d'effectuer un examen de votre disque dur et à moins de connaître le mot de passe et la combinaison de touches que la personne qui vous surveille utilise pour visualiser les saisies d'écran effectuées pour surveiller votre ordinateur.
- Il peut être dangereux pour vous de tenter d'effacer vos historiques, d'essayer de déterminer si un logiciel espion est installé dans votre ordinateur ou d'essayer d'obtenir de l'aide en consultant une page Web sur la violence conjugale, si vous utilisez un ordinateur surveillé par une personne mal intentionnée.

Affichez un avertissement de sécurité sur toutes les pages de votre site Web

- Vous pouvez aider les victimes à prendre conscience des risques en affichant un avertissement de sécurité clair, mais bref, dans votre site Web (p. ex.: « Il se peut que vous soyez incapable de supprimer les traces d'utilisation de votre ordinateur. Si vous pensez que quelqu'un vous surveille, utilisez un ordinateur sécuritaire ou composez le numéro d'une ligne d'aide pour obtenir de plus amples renseignements. »)

Prenez des mesures pour sécuriser les données qui sont en possession de votre organisation

- Les organisations devraient protéger tout renseignement personnel sur une victime qui permet de l'identifier, puisqu'une fuite ou une brèche dans la protection des données pourrait engendrer des conséquences graves pour cette personne. Pour des raisons de sécurité, nous recommandons aux organisations de ne pas conserver de renseignements confidentiels ou qui permettent d'identifier une victime dans les ordinateurs branchés à Internet. Avec les ordinateurs qui ne sont pas connectés à Internet, le risque qu'une personne mal intentionnée s'infilte et accède aux données de votre organisation, ou encore qu'un virus infecte l'ordinateur et envoie à l'extérieur des fichiers confidentiels par courriel de façon automatique, est beaucoup moins important.
- Il est important que l'organisation établisse des politiques sur les pratiques relatives à l'information en format électronique ou papier, notamment en ce qui concerne les personnes autorisées à accéder à telle ou telle donnée, la façon sécuritaire de se débarrasser des documents confidentiels, des disques durs d'ordinateurs et d'autres outils électroniques (p. ex., les disques durs externes ou les clés USB) qui contiennent des données sur les victimes. Veuillez consulter la liste de vérification de la sécurité des données à l'adresse suivante (en anglais seulement):
http://www.nnedv.org/SafetyNet/Publications/NNEDV_DataSecurityHandout.pdf.

Assurez-vous de régler les questions relatives à la sécurité informatique avant d'envisager d'offrir des services dans Internet

- Prenez connaissance des faits: de 60 à 80 p. 100 des ordinateurs sont infectés par des virus, des logiciels publicitaires ou d'autres logiciels malveillants qui peuvent compromettre la sécurité à la fois des victimes/des survivants et des ordinateurs de votre organisation. (www.pewinternet.org)
- Prenez conscience du fait que vous ne pouvez garantir la sécurité des ordinateurs de toutes les personnes qui utilisent vos services. Informez bien et dès le départ les utilisateurs de vos services au sujet des questions de sécurité, de confidentialité et de capacité, de façon qu'ils puissent prendre des décisions éclairées et réalistes avant d'utiliser vos services.
- Fournissez des renseignements sur les limites des outils technologiques, de la confidentialité et de la sécurité qu'offrent les services en ligne, notamment en ce qui concerne les différences d'accès aux outils technologiques, les différentes connexions à Internet (rapidité) et les pannes de connexion.
- Discutez, au sein de votre organisation, du préjudice que peuvent subir les victimes dans le cas où la personne qui leur veut du mal sait exactement comment la victime prévoit lui échapper, parce que celle-ci en a discuté dans le cadre de services en ligne.

Utilisez des pare-feu et assurez-vous de mettre à jour les définitions de virus et de logiciels espions

- Évidemment, la première chose à faire pour se protéger des logiciels malveillants et des logiciels publicitaires est de mettre à jour ses logiciels de protection. Cependant, ces programmes offriront une protection limitée contre les logiciels utilisés pour la surveillance, puisque ceux-ci peuvent passer pour des produits légitimes et ne pas être repérés par des logiciels de détection. Même si l'utilisateur prend des précautions, le logiciel espion permet à la personne qui lui veut du mal de le surveiller lorsqu'il utilise son ordinateur et navigue dans Internet, ce qui lui permet de savoir ce que sa victime fait pour essayer de lui échapper ou d'obtenir de l'aide.

Sécurisez vos ordinateurs

- Assurez-vous que l'ouverture d'une session sur tous les ordinateurs de votre organisation exige un mot de passe alphanumérique offrant un haut niveau de sécurité. Chaque utilisateur devrait avoir un mot de passe qui lui est propre, et les utilisateurs ne devraient pas utiliser à cette fin le nom de votre organisation, votre adresse ou des renseignements du genre.
- Si vous avez des ordinateurs publics, envisagez de bloquer le téléchargement de logiciels par les utilisateurs.

CONSEILS POUR LES PARENTS

- Après vous être renseigné sur Internet et sur les ordinateurs, discutez avec vos enfants des avantages qu'offre Internet et des risques qui existent. Avec les membres de votre famille, établissez un ensemble de règles de sécurité pour la navigation dans Internet. Si vos enfants participent à la création des règles, ils seront plus susceptibles de les respecter.
- Placez l'ordinateur familial dans un espace partagé, par exemple dans la pièce familiale ou le salon. Si vos enfants savent que vous pouvez passer devant l'ordinateur à tout moment, ils seront beaucoup moins susceptibles d'enfreindre les règles établies.
- Si vous décidez d'utiliser le logiciel de surveillance parentale, DITES à vos enfants que vous allez le faire et expliquez-leur pourquoi. Il est extrêmement important que vous permettiez l'utilisation de l'ordinateur dans un climat de confiance et de respect, de façon que vos enfants soient à l'aise de vous faire part de tout problème qui pourrait survenir. Par ailleurs, vous devriez utiliser un logiciel qui affiche une icône à l'écran lorsqu'il est activé. Ainsi, vos enfants se rappelleront qu'ils sont surveillés, et cela va les encourager à respecter les règles de sécurité pour la navigation dans Internet.