

## Les meilleures pratiques

En sécurité informatique, l'expression « les meilleures pratiques » décrit les habitudes et les méthodes que les internautes devraient employer pour contrer les attaques et les menaces communes à l'égard des données.

### Les pièces jointes au courriel

On ne peut trop insister sur la « meilleure pratique » ou les précautions à prendre au moment d'ouvrir les documents annexés aux courriels. Ils existent de nombreux virus, plus particulièrement, des vers informatiques dans la catégorie du pollupostage. Comme le laisse entendre le terme, ces vers s'infiltrent dans les carnets d'adresses et se propagent dans toutes les adresses ainsi repérées. Si vous recevez un tel courriel, informer l'expéditeur sur-le-champ afin qu'il prenne des mesures immédiates pour prévenir tout autre dommage.



### Évitez les logiciels espions / publicitaires

Prenez garde de télécharger par inadvertance des logiciels gratuits ou des logiciels sur Internet. Malgré utilité, renseignez-vous sur les logiciels que vous désirez télécharger et installer. Il se peut fort bien qu'ils contiennent des logiciels mouchards ou de la publicité; l'information à ce sujet sera affichée à de nombreux endroits sur l'Internet. Certains systèmes d'exploitation n'autorisent pas les employés à installer quelque logiciel que ce soit. Il importe également de toujours lire les messages de sécurité affichés. Soyez prudent avant de cliquer sur « autoriser » ou « oui ».

### Changez vos mots de passe

Une « meilleure pratique » souvent négligée est le changement des mots de passe sur une base régulière. Il faut également s'assurer que ce ne sont pas des noms ou des mots du dictionnaire. Il est préférable d'utiliser des mots de passe complètement différents pour chaque service; ainsi, si quelqu'un pirate le mot de passe de votre compte courriel, il n'aura pas automatiquement accès à votre compte de banque en ligne. Il vaut mieux ne pas écrire vos mots de passe mais, si vous devez le faire, assurez-vous qu'ils se trouvent dans un endroit sûr dont l'accès vous est réservé.



### Logiciels à jour!

La plus importante des meilleures pratiques consiste à tenir vos logiciels à jour. Assurez-vous de télécharger les mises à jour des systèmes suivants : système d'exploitation, navigateur, logiciel de courrier électronique client et logiciel antivirus

# L'essentiel sur la sécurité informatique pour les petites entreprises et les professionnelles



Créé par

## CEONET

Communities of Eastern Ontario Network

Le réseau des communautés de l'est de l'Ontario

Tél: 613 525-2151 Télécopieur: 613 525-2417

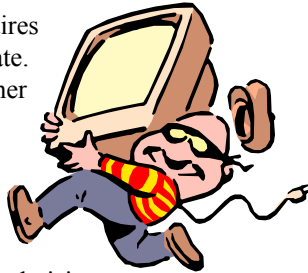
info@ceonet.on.ca www.ceonet.on.ca

## Les risques et menaces

Tout dépendant de la sensibilité des données avec lesquelles vous travaillez couramment, les risques pourraient être assez élevés si vous ne tenez pas compte de la sécurité de ces données. Ces risques sont les mêmes auxquels sont confrontés les utilisateurs à domicile; toutefois, les conséquences sont beaucoup plus graves. La compromission de l'information au sein d'une entreprise peut entraîner des coûts assez considérables quant à la perte de données, la violation de la confidentialité avec les clients, et le risque de responsabilité légale.

### L'intrusion au niveau du réseau

Une connexion Internet est grandement utile pour les affaires mais elle peut s'avérer dangereuse sans protection adéquate. En effet, quiconque a les habiletés requises peut se brancher sur un ordinateur ou un réseau en ligne. Certains pirates informatiques sont tout simplement curieux et ne veulent causer aucun dommage, tandis que d'autres sont vindicatifs et ont l'intention de voler ou détruire autant d'information que possible. Ce qui porte à confusion c'est que parfois un ordinateur ou réseau semble avoir été choisi au hasard pour ce type d'attaque, voire par un étranger d'un autre continent.



### Les virus, les vers et les chevaux de Troie



Alors que certains internautes malveillants désirent voler ou exploiter vos données, d'autres se plaisent à créer des virus pour les détruire, des vers pour les infecter et propager l'infection, ou des chevaux de Troie visant à rendre votre système vulnérable à une intrusion dérobée.

### Les logiciels espions / publicitaires

Les logiciels espions visent à enregistrer ce que vous faites à l'ordinateur. Par exemple, les sites Web que vous visitez peuvent transmettre à une tierce partie aux fins d'étude du marché ou de publicité ciblée.

Les logiciels publicitaires servent à afficher vos publicités sur Internet, soit par téléchargement ou de façon instantanée. Ces publicités sont à l'avantage financier de l'auteur.



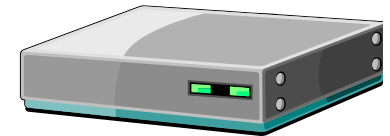
Toutefois la répétition des messages peut entraîner un risque, à savoir que le logiciel peut être en communication constante avec une tierce partie utilisant votre connexion Internet. Il ne faut surtout pas présumer que votre confidentialité est assurée durant une connexion Internet sur DSL, SMDM ou un autre service toujours en ligne.

## Les mesures préventives et de rétablissement

Les petits bureaux sont souvent à court de personnel formé en sécurité informatique. Heureusement, il existe des solutions faciles sur le marché. Même si les produits disponibles exigent une connaissance pratique de certains fondements, la protection du réseau local de votre bureau est maintenant assez à administrer.

### Les routeurs / commutateurs

La façon la plus simple de protéger un réseau local contre toute intrusion est l'installation d'un routeur / commutateur peu coûteux. Un tel appareil sécurise les ordinateurs, les autres dispositifs de réseau et la connexion à l'Internet. La barrière de sécurité du routeur peut être configurée au moyen d'un navigateur sur un ordinateur personnel branché ou peut empêcher certaines données d'entrer dans votre réseau ou d'en sortir.



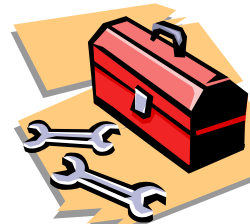
### Les logiciels antivirus



En plus des meilleures pratiques, la meilleure protection contre les virus, les vers et autres programmes semblables est l'exploitation de logiciels antivirus de pointe sur chaque ordinateur personnel, avec le téléchargement des mises à jour sur une base régulière. En plus de protéger chaque ordinateur sur lequel il est installé, le logiciel antivirus peut assez facilement supprimer les contaminations qui peuvent se glisser.

### Les outils de suppression des logiciels espions / publicitaires

La meilleure façon de se débarrasser des logiciels espions ou publicitaires est d'éviter de les installer au départ sur votre ordinateur puisqu'il n'est pas toujours simple de les supprimer. Il existe des outils à téléchargement gratuit qui peuvent vous aider à garder la situation sous contrôle. Deux outils fortement recommandés sont Spybot Search & Destroy et HijackThis. Détails, qu'on peut trouver en ligne.



AdAware - [www.lavasoft.de](http://www.lavasoft.de)

HijackThis - [www.hijackthis.nl](http://www.hijackthis.nl)

SpyBot Search & Destroy - [www.safer-networking.org](http://www.safer-networking.org)