IT: SÉCUR-IT

Ici, il y a des DRAGONS

Lorsque les fidèles lecteurs de *Connexions* recevront ce numéro, le Ministère aura élargi l'accès assuré à Internet par l'intermédiaire du pare-feu, et aboli l'obligation de posséder un compte et un numéro d'utilisateur pour pouvoir y accéder. De façon concrète, cela signifie que les employés pourront désormais utiliser leur explorateur favori autant qu'il leur plaira pour parcourir les vastes étendues du WWW.

Dans des articles parus antérieurement sur la sécurité des technologies de l'information, nous avons fait porter nos efforts sur des menaces précises inhérentes au monde « branché » : virus, logiciels pernicieux, piratage informatique et autres. Il faut toutefois aussi se méfier de certains dangers à l'aspect inoffensif, et qui ne sont d'ailleurs pas le fait de mauvaises intentions.

Mentionnons, par exemple, le cas d'un utilisateur du Ministère qui, récemment, s'est servi de son explorateur pour gagner le site Web d'une entreprise et s'y procurer le dernier exemplaire d'évaluation de son logiciel. En installant ce dernier, il a effacé son disque dur et perdu toutes les données qui s'y trouvaient enregistrées. Cela s'est-il produit en raison de la présence d'un virus? Non. Le logiciel était-il pernicieux? Pas de l'avis de ses fabricants. A-t-on pu imputer cet incident à un acte de piratage informatique alors? Pas davantage. L'incident a-t-il fait intervenir un geste normalement considéré comme une menace pour nos biens (aussi bien physiques, si l'on songe au disque dur, qu'intellectuels, si l'on considère les données contenues sur ce dernier)? Euh, maintenant que vous mentionnez la chose... eh bien... oui.

Lors de cet incident, le Ministère a perdu des biens - le fait qu'il s'agisse de biens intellectuels plutôt que de biens matériels qui nous semblent plus tangibles, comme un bureau, ne change rien à l'affaire. Vous avez, en tant qu'employé du Ministère, la responsabilité de protéger les biens ministériels qui sont confiés à votre garde. Cela englobe les fichiers enregistrés sur votre disque dur, sur disquettes, dans les dossiers de votre messagerie électronique, etc. Vous avez le devoir de prendre des mesures raisonnables pour protéger leur intégrité.

Voici donc quelques points à garder en mémoire en vue de vos déplacements cyberdiplomatiques :

- Si vous avez besoin de logiciels autres que ceux fournis par le Ministère à titre standard, assurez-vous d'utiliser des exemplaires sous licence achetés conformément aux politiques d'acquisition en vigueur.

- Manipulez avec des précautions raisonnables tout ce que vous obtenez par l'intermédiaire d'Internet - et vérifiez les logiciels au moyen d'un programme de détection des virus avant de les installer et de les utiliser.

- Si vous n'êtes pas raisonnablement familier avec le processus d'installation de logiciels, demandez de l'aide. Dans la mesure où ils en seront capables et où ils disposeront de suffisamment de temps pour ce faire, les gestionnaires des systèmes SIGNET pourront vous prêter main forte. Soyez toutefois conscients du fait que rien ne les oblige à fournir un appui lorsqu'il ne s'agit pas de logiciels standard exploités par le Ministère, et que souvent même ils ne seront pas en mesure de vous aider.

- Soyez prudents et vigilants lorsque vous naviguez sur Internet, compte tenu du fait que tout ce que vous y exprimerez sera considéré par les internautes du monde entier comme émanant d'un employé du Ministère (votre adresse ministérielle sera en tous cas communiquée à tous les sites que vous visiterez et à chacun des sites empruntés pour y parvenir). Assurez-vous d'indiquer que les propos que vous tenez représentent votre opinion personnelle, à moins que vous n'ayez obtenu l'autorisation expresse de représenter le Ministère.

Autrefois, à l'époque des grandes explorations maritimes, les cartographes européens portaient sur les cartes, à l'emplacement des mers inexplorées, une mise en garde indiquant : « Ici, il y a des dragons ». Si vous entreprenez vos pérégrinations avec un grain de sel et un gramme ou deux de bon sens, il n'y a pas de raison pour que vous ne puissiez éviter les dragons qui hantent ces eaux.

CONNEXIONS est publié une fois par mois par la Direction des services à la clientèle (SXC) et diffusé au Canada et dans les missions à l'étranger à tous les fonctionnaires du ministère des Affaires étrangères et du Commerce international. Il est disponible via l'Intranet sous « Quoi de neuf ?».

Les unités qui veulent faire paraître un avis dans *CONNEXIONS* sont priées de faire parvenir le texte à SXC accompagné d'une note de service signée par leur directeur. Tous les lecteurs sont invités par ailleurs à envoyer, par ICONDESK (Suggestions), les ébauches d'articles qu'ils désirent faire publier.