

L'Internet pour les dentistes

LA SÉCURITÉ SUR INTERNET

© J Can Dent Assoc 2000; 66:239

La plupart des gens n'auraient jamais l'idée de partir de chez eux sans verrouiller leur porte d'entrée. Certains même installent des systèmes de sécurité pour se protéger contre les intrus. Comme votre maison, votre ordinateur a besoin d'être protégé contre ceux qu'on appelle les pirates. Avant l'avènement de l'Internet, c'est-à-dire quand on accédait aux ordinateurs principalement par souris et clavier, on ne craignait guère les pirates. Aujourd'hui, il est important de vous rendre compte que les pirates peuvent accéder à votre ordinateur personnel sans autorisation grâce à l'Internet. Des logiciels sophistiqués sont maintenant vendus qui leur permettent de s'aventurer dans votre système et éventuellement de porter atteinte à la sécurité de celui-ci. Ils peuvent même être sur votre système en même temps que vous sans que vous le sachiez.

Les pirates ont tendance à fureter pour plusieurs raisons. Certains veulent prouver qu'ils peuvent s'infiltrer, d'autres ont une raison politique et d'autres cherchent des renseignements personnels pour en tirer des gains financiers. Peu importe la raison, il est important de reconnaître que les pirates sont bien en vie sur Internet. Et les cabinets dentaires sont pour eux une cible parfaite.

La plupart des cabinets dentaires ont un réseau local relativement petit de moins de 20 ordinateurs. Si un pirate s'infiltré dans l'un des ordinateurs, tous les autres sont à sa portée. Pourquoi un pirate accéderait-il à un cabinet dentaire, me

demandez-vous? Pensez aux précieuses données sur les cartes de crédit que votre système renferme. Peut-être que l'employé mécontent que vous venez de renvoyer est aussi un pirate. Peut-être que vous venez de placer un pont à six unités dans la bouche d'un pirate qui aimerait effacer les données de votre registre! Pour une raison ou pour une autre, votre cabinet n'est pas à l'abri.

Les pirates accèdent à votre ordinateur de différentes façons. Quand vous êtes sur Internet, vous utilisez ce qu'on appelle une adresse IP qui permet à d'autres ordinateurs de vous localiser. Cette adresse change à chaque fois que vous accédez à l'Internet, mais reste la même quand vous gardez la même connexion. Les pirates peuvent trouver cette adresse en utilisant des programmes spécialement conçus à cet effet. Une fois qu'ils connaissent votre adresse IP, ils décodent votre mot de passe pour accéder à votre réseau. Si votre cabinet est continuellement branché sur Internet, il se peut que vous laissiez la porte arrière ouverte aux intrus.

Les pare-feux

Une façon de protéger votre réseau est d'utiliser des pare-feux, c'est-à-dire des matériels et logiciels qui empêchent les pirates d'accéder à vos données personnelles. En d'autres termes, ils fonctionnent comme un système de sécurité. Ils peuvent être installés sur le serveur du réseau ou un ordinateur autonome qui est réservé à la sécurité sur Internet. Si vous avez une connexion rapide et continue à l'Internet, vous devriez désigner un ordinateur comme pare-feu, dont la seule fonction est de vérifier qu'il n'y a pas d'intrus. Les pare-feux sont branchés aux autres ordinateurs du réseau par le noeud central, ce qui augmente la sécurité de votre réseau sans en compromettre la rapidité.

Certains des principaux fournisseurs Internet vantent au public le fait que leurs réseaux sont munis de pare-feux. Or, ceux-ci ne se trouvent pas à l'endroit idéal pour protéger votre cabinet. En effet, à quoi bon verrouiller vos portes si l'intrus

est déjà à l'intérieur? Les pare-feux doivent être directement branchés sur votre point d'accès au réseau pour vous protéger contre les pirates qui, comme vous, se trouvent à l'intérieur. La plupart des logiciels dentaires nécessitent que le serveur partage les dossiers sur réseau. Les renseignements comme l'adresse, le traitement et les comptes sont ainsi partagés par tous les ordinateurs, ce qui permet non seulement à tous les membres du cabinet de maintenir les dossiers à jour, mais aussi aux intrus d'accéder plus facilement aux dossiers. Si vous accédez à l'Internet de votre serveur, vous devriez avoir un pare-feu qui empêche les intrus de pirater les fichiers qui sont partagés latéralement. Pour obtenir un logiciel pare-feu gratuit, consultez le site <http://www.zonealarm.com/>.

Mots de passe

Beaucoup de cabinets utilisent des logiciels comme PCAnywhere pour accéder au bureau depuis la maison ou permettre à l'équipe de soutien informatique d'accéder au réseau. Assurez-vous d'utiliser un mot de passe de sécurité pour empêcher l'accès à cet endroit. Le mot de passe devrait être alphanumérique. Les pirates ont des programmes qui peuvent rapidement passer en revue un dictionnaire de mots, de noms et de dates de naissance pour décoder votre mot de passe. Si vous utilisez une combinaison de chiffres et de lettres (certaines devraient être en majuscule, c.-à-d. 2motPasse), le pirate aura beaucoup de mal à le décoder.

Comme ma mère me rappelait quand j'étais enfant, «N'oublie pas de verrouiller toutes les portes!» ♦

*Le Dr Scott MacLean exerce dans un cabinet privé à Halifax (Nouvelle-Écosse).
Courriel : maclean@ns.sympatico.ca.*

Les vues exprimées sont celles de l'auteur et ne reflètent pas nécessairement les opinions et les politiques officielles de l'Association dentaire canadienne.

(La version électronique de L'Internet pour les dentistes contient des liens activés qui permettent aux lecteurs de se rendre directement aux sites Web référés dans l'article.)
