The Internet for Dentists

INTERNET SECURITY

© J Can Dent Assoc 2000; 66:239

Most people would never think of leaving their front door unlocked when they are not home. Besides locking the door, some people also install a security system to protect themselves against unwanted visitors. Like your home, your computer must also be protected against intruders (known as hackers). Before the advent of the Internet, when computers were accessed mainly through the keyboard and mouse, the fear of hackers was not a big issue. Today it is important to realize that hackers can get into your private computer without authorization via the Internet. Sophisticated software is now available that allows hackers to find paths into your system and cause potential security breaches. They can even be on your computer at the same time you are and you won't know it.

Hackers tend to snoop around for a number of reasons. Some want to prove they can break in, some have a political agenda, still others are looking for private information they can use for financial benefit. Regardless of the reason, it is important to acknowledge that hackers are alive and well on the Internet. The dental office is a perfect target for hackers.

Most dental offices have a relatively small local area network (LAN) of less than 20 computers. If a hacker penetrates one of the computers, then all the others can be accessed. Why would a hacker break into your dental office? Think of the valuable credit card information that is stored on your computers. Maybe you just fired a disgruntled staff who is also a hacker. Perhaps you just placed a six-unit bridge on a hacker who would like to delete the book entry! Regardless of the reason, your office is a potential target.

Hackers use different ways to break in. When you are on the Internet you use a number called an IP address that allows other computers to know where you are. This IP address changes each time you connect or remains the same when you are using a continuous connection. Hackers can find this address using programs called "IP sniffers." Once they know your IP address, hackers use password crackers to access your network. The longer you are connected to the Internet, the greater the risk of an intrusion. If your office has a continuous connection, then you may be leaving your back door open to unwanted visitors.

Firewalls

One way to protect your office network against unwanted visitors is to use a firewall. Firewalls are hardware and software programs that prevent hackers from accessing your private data. In other words, firewalls work like a security system. You can have firewall software installed on the network server or on a stand-alone computer that is dedicated to Internet security. If you have a high-speed continuous connection to the Internet, it is recommended that you use a dedicated computer as a firewall whose sole task will be to check for intruders. The firewall is attached to the other computers on the network via the central hub, which maximizes the security protection on your network without slowing its performance down.

Some of the larger Internet provider companies publicize the fact that they have firewall protection on their networks; however, this firewall is not ideally located to protect your office. Think of it this way: What's the point of locking your doors if the intruder is inside the house already? The firewall must be directly on your point of access to the network to protect against hackers that are inside the firewall with you. Most dental software require that the server share files on the network. Information such as patient addresses, treatment, accounts, etc., is thus shared by all the computers. Sharing files allows everyone in the office to maintain and update one record; however, it also makes it easier for intruders to access these files. If you are accessing the Internet from your server then you should have a firewall to protect intruders from laterally hacking into your shared files. For free firewall software, visit http://www.zonealarm.com/.

Passwords

Many offices use remote software programs like PCAnywhere to access the office from their home computer and to allow the software support team access to the network. Make sure that you use a security password to prevent access via this location. The password should be alphanumeric. Hackers have password cracker programs that can quickly go through a dictionary of words, names, and birth dates. If you use a password with a combination of numbers and letters (some of which should be capitalized, i.e., 2passWord), then you will make it extremely difficult for the hacker to succeed.

As my Mom used to remind me when I was growing up, "Remember to lock both the front and back doors!" ◆

Dr. Scott MacLean maintains a private practice in Halifax, Nova Scotia. His e-mail address is maclean@ns.sympatico.ca.

The views expressed are those of the author and do not necessarily reflect the opinion or official policies of the Canadian Dental Association.

(The online version of The Internet for Dentists contains active links that allow readers to go directly to the Web sites mentioned in the article.)