

Internet Safety Precautions



Bruce Stephenson, DDS, FAGD



Josh Jacoby

Modern dental offices need the Internet. Its applications include online eligibility and benefits, free electronic claims submission and tracking, immediate nonrecourse third-party patient financing, patient newsletters, recare and appointment confirmations by e-mail, inexpensive or free Web sites, and a lot of unbiased information from other dentists about dental products, techniques, and the credibility of the latest dental gurus (Figure 1). (Note: Links to some of our favorite Web sites can be accessed from paperlessdentistry.com.)

The list of benefits is growing rapidly. Too many advantages and sources of information are simply unavailable any other way. Saying "I don't need the Internet" is like saying "I don't need electricity." Stop doing things the hard way. The biggest mistake a dental office can make concerning the Internet is not to use it! But, as with electricity, you want to use it safely (Figure 2).

Dental computers are no longer do-it-yourself projects. They are sophisticated business systems that interact with everyone and every

Saying "I don't need the Internet" is like saying "I don't need electricity." Stop doing things the hard way. The biggest mistake a dental office can make concerning the Internet is not to use it!

other system in a practice. Because an Internet connection potentially opens your office computers to every other Internet-connected computer in the whole world, you need some help with security. Dentists who try to do this themselves are like the dentists who try to fix their own teeth (Figures 3 and 4). We all know someone who tries, but it is not a very good idea. You need some competent, experienced help from an IT (information technology) person well versed in security. This is not a job for your spouse's uncle's friend who works in the mailroom of IBM. If your local IT person cannot give you references from very security-conscious clients such as banks, ask for a referral to someone who can. A parts and labor contract for a properly configured Internet

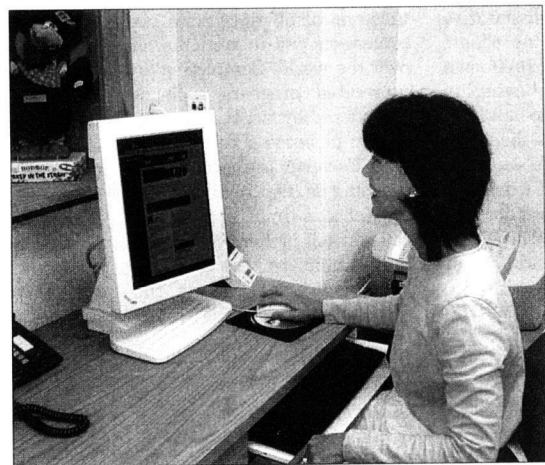


Figure 1. Efficient dental office operation now requires the Internet. Many dental insurance companies now have online patient benefits and some will take direct submissions of claims and pre-estimations.

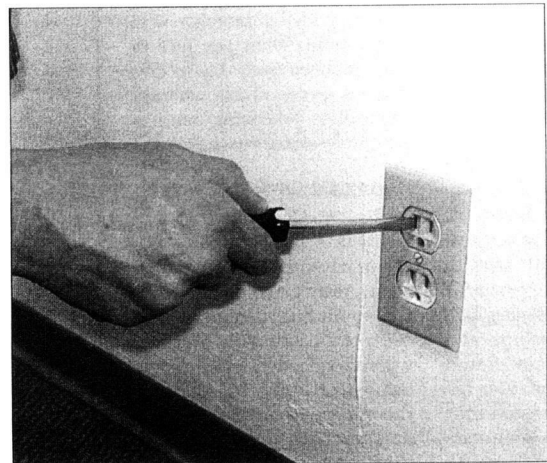


Figure 2. As valuable as it is, the Internet is not without hazards. Just as with the use of electricity, some precautions are necessary to avoid a very unpleasant experience!

continued on page 94

Internet Safety Precautions...*continued from page 92*

INTERNET SAFETY CHECK LIST

- ◆ Don't fix your own teeth: Get some qualified help from someone who does Internet security for a living. Connecting to the Internet is easy; protecting your computers and office from the Internet is much more difficult.

- ◆ Virus and spyware protection: There is no such thing as an absolutely "safe" computer connected to the Internet, but you can harden your system significantly with some awareness and planning. The entire computer system should be protected by antivirus software that is automatically updated at least once each week. Automatic updates for operating systems are also usually a good idea. You can check for and remove spyware with programs such as Adaware and Spybot.

- ◆ Software or hardware firewalls are mandatory for any computer that connects to the Internet. Windows XP has a software firewall built in but it is turned off by default. You can get some idea of your "Internet visibility" by visiting grc.com and having the site "probe your ports." (No, this is not some Internet version of a colonoscopy!)

- ◆ Content filters can block access to offensive Web sites. They can also be used to block access to nonbusiness-related sites that waste time in many dental offices providing unrestricted Internet access.

- ◆ Wireless networks provide great benefits for dentists but have their own security requirements. Passwords, WEP or WPA encryption, and MAC address restrictions should all be used. SSID broadcasting should be turned off.

- ◆ Broadband connections, when they are available, are usually inexpensive and much more convenient than dial-up connections. Often the cost of a DSL connection is less than you pay now for a separate phone line and the monthly fee to your ISP. Properly configured, they are not more dangerous than dial-up.

- ◆ Consider a "break room computer" for staff personal use that has unlimited Internet access (with the possible exception of offensive Web site blocking). But this "unsafe" computer should absolutely not be connected to your dental network. You can get a computer at Wal-Mart for about \$200 that runs a flavor of Linux, so it is somewhat virus-resistant and makes a great, cheap Web browser. This also is a great use for an "old" computer that still works.

- ◆ A written office policy should cover computer uses and include a section on the Internet and e-mail (including the admonition never to open e-mail attachments).

- ◆ Staff training in the rapidly changing field of dental computing should be a continuous process. Hardware and software without staff training is like a really expensive car with no engine!

- ◆ "Recare" is just as important for IT as it is for dental health. Two years ago, virus attaches were rare and no one was talking about spyware. Many IT companies now have inexpensive maintenance contracts available that cover these services.

Additional information on security and dental computing topics can be obtained from the authors. Mr. Jacoby can be reached at (916) 773-7222 or via e-mail at josh_jacoby@innovacrew.com. InnovaCrew's Web site is innovacrew.com. Dr. Stephenson can be reached at (510) 483-2788 or via e-mail at bruce@painlesscom.com. His Web site is paperlessdentistry.com.

connection will be anywhere from \$250 to \$1,000 or more, depending upon the number of computers on your network. But this is a bargain; your investment will be returned manyfold.

A GIANT OPEN-AIR MARKET

Think of the Internet as a giant open-air street fair and market with people from all over the world wandering around. Most of these people are nice, honest, helpful, law-abiding folks. But some of them are pickpockets. Some of them are robbers. And some of them would just as soon kill you as look at you. Unfortunately, there are very weird people in the world, and some of them are on the Internet. You need some help to protect yourself and your patients from some of these people to keep you and your staff safe from these malicious denizens of cyberspace. Figure 3 is a "clip-and-save" checklist to discuss with your Internet IT security person. The list is not all-inclusive, but it is an initial set of "talking points" when you plan your Internet connection.

Most computer users are now aware of the devastation caused by worms, viruses, and other forms of malicious software or "malware." But many users are not aware of how fast serious and expensive problems can happen. One dentist had just completed the installation of 10 new computers with fully integrated intraoral cameras, digital x-ray, clinical charting in all operatories...everything necessary for a paperless practice. This was an expensive and extensive system to set up. To save a little money, he decided to connect to the Internet himself. He had been told how easy it was and this proved to be true. He had no problem connecting and was soon "surfing" to some of the interesting Web sites he had heard about. No one knows just which of these Web sites was the culprit or exactly what he did to download the malware, but after about 30 minutes of surfing, all the computers on his network were infected with a very destructive worm that deleted many critical files on each of these computer's hard drives. This was akin to having your new car totaled as you drove it home

Figure 3. This is not meant to be an all-inclusive list of Internet safety considerations, but it provides topics you should be sure to discuss with your IT professional. The Internet is a "module," like data backup or digital radiography, of your total computer system.

from the car dealer. "Oops" doesn't begin to cover it! The hardware was undamaged, but—as with most complicated dental systems—the time spent in installing and configuring software is the more expensive part of the project. All the software, including the operating systems, had to be reinstalled and reconfigured.

It is uncommon to see problems this extensive happen this quickly. But they do occur...and they can be prevented. Get some competent help when you connect your business computer system to the Internet. This dentist "fixed his own teeth," and ended up needing a "full mouth reconstruction!"

Embracing the Internet, like using electricity, should be an interesting and rewarding experience, not a "shocking" one.

We don't yet have any such dental horror stories about HIPAA, "hackers," and "crackers," but you can be sure of some in the near future. Newspapers had a field day with the story of the 13-year-old boy who hacked into the personnel records of the state of California and made off with the governor's social security number and home address! Dentists have such information on their office computer systems, and many dentists have much more personal information such as medical alerts and credit card numbers. What if some 13-year-old hacked into your system just because it was an easy target on the Internet? What if he printed out your patients' social security numbers and distributed them at the local high school? You would probably not have to go to "HIPAA Jail," but I bet you sure would be embarrassed. And I bet you would have a few hopping mad patients to deal with! In California, if we discover such a computer break-in, we have a legal obligation to inform all those possibly affected (ie, all my patients)

that their personal information may be floating around somewhere. A real "practice builder!" And just wait until your local newspaper picks the story up. Maybe "60 Minutes" will be interested!

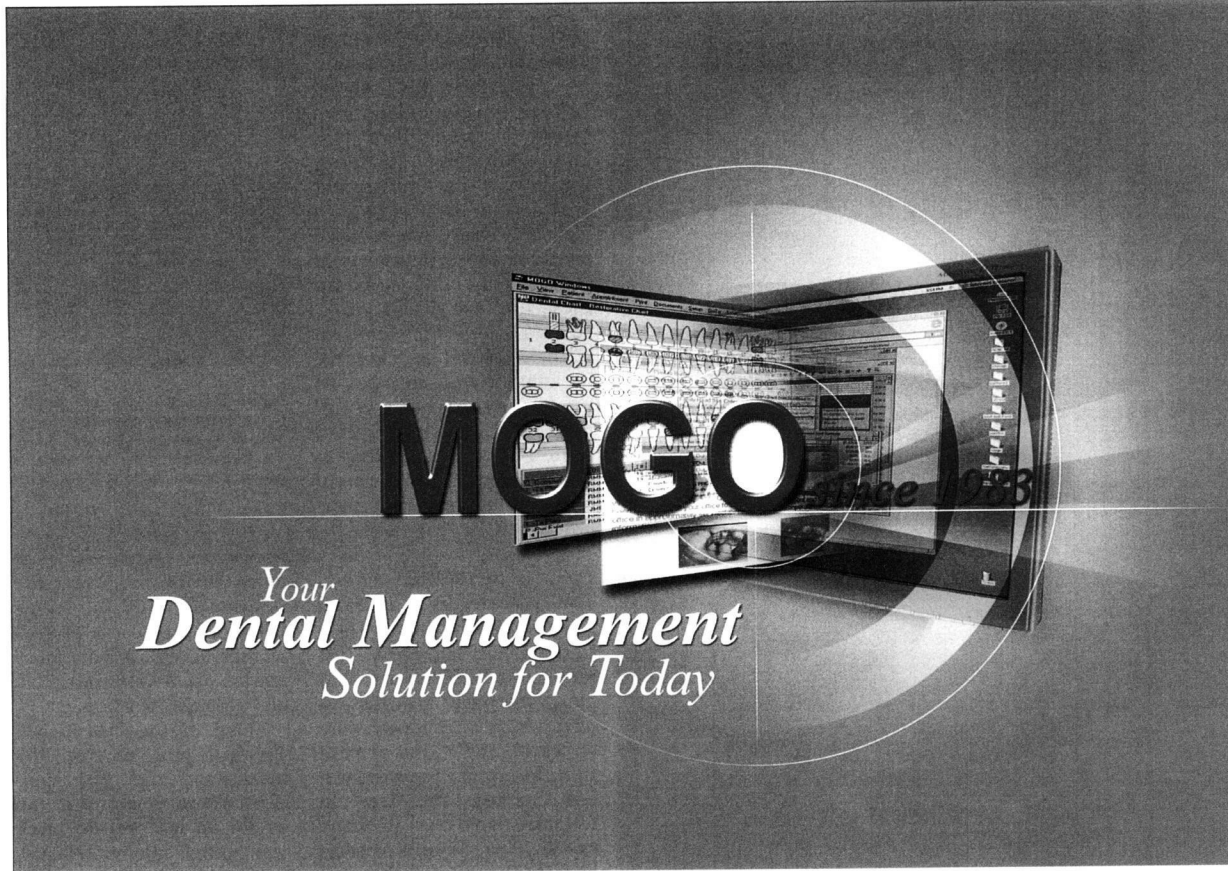
FIREWALLS

To prevent the above situation, you need a well-configured firewall. A firewall is either a hardware or software device that sits between your office computer system

and the Internet. It can "hide" your computers from those pesky 13-year-olds, but still allow you to access cyberspace. It may also offer some additional protection in the form of content filtering.

Parental controls are an example of content filters. They prevent computer users from accessing sites containing pornography, hate mon-

continued on page 96



*Your
Dental Management
Solution for Today*

All Modules Included

MOGO provides all modules for one low price including Appointment Monitor, Charting, Employee Time Clock, Instant Recall, Clinical Documentation, Business Analysis Report, and Budget Plans, as well as Real-Time Insurance Claim Tracking, at no extra charge.

Training

Over 20 hours of FREE multimedia training on CD-Rom is included. Your own personal trainer is available with a click of the mouse!

Technical Support

We want you to experience our high level of prompt, knowledgeable support. MOGO is the only dental software company that encourages you to call technical support while you are evaluating the program.

30 Day Free Trial

See for yourself why MOGO is consistently rated at the top when compared to other software programs. Try before you buy with our free 30 day evaluation cd at absolutely no obligation.

call toll free 1-800-944-MOGO (6646)



visit us at www.mogo.com

The Professional's Choice™

FREEinfo, circle 58 on card

Dentistry Today's Midwinter Product Showcase

February 2004 issue

Highlighting the profession's

newest products

to be featured at the

**Chicago Dental Society's
139th Midwinter Meeting**

Feb. 19 to Feb. 22

**at Chicago's
McCormick Place
convention facility.**

• Call •

Dentistry Today

**973-882-4700 - East
847-446-1095 - Midwest
415-721-0644 - West**

Internet Safety Precautions... *continued from page 95*

gering, and other categories of Web sites that might offend certain people and have essentially no business value for a dental practice.

A good firewall allows you or your designated IT person to set up "white lists" (the only sites your staff can access) or "black lists" (specific sites your staff is blocked from accessing). You can even subscribe to business services that set up and maintain these lists for you. If one of your staffers browsing an offensive Web site is observed by another staff member, as the business owner you are responsible. It is no different than allowing a staffer to display any other form of offensive material in your office.

SPYWARE

The last category of Internet intrusion I want to discuss is "adware" or "spyware." You may already be aware that most "freeware" also installs advertising tracking software (adware), and if you remove this adware, the freeware will not function. The "free" in freeware isn't true in many cases! This adware reports back to companies that are interested in where you go on the Internet and what you are interested in buying. Adware records this information and then sends it back to the Internet "motherhood" in the background (ie, unbeknownst to you) over your Internet connection. (There are lots of background tasks running while you are connected to the Internet. Most of them are beneficial, such as virus definition updates, but a few of them may have more nefarious intent.)

Most "legitimate" adware is installed with the user's consent but without the user's knowledge. The notice that this software will be installed on your computers is included in the software agreement you accept—but don't read—when you install the freeware. This adware tracking is not only legal but, adware folks argue, potentially beneficial to you as an Internet shopper. (Maybe

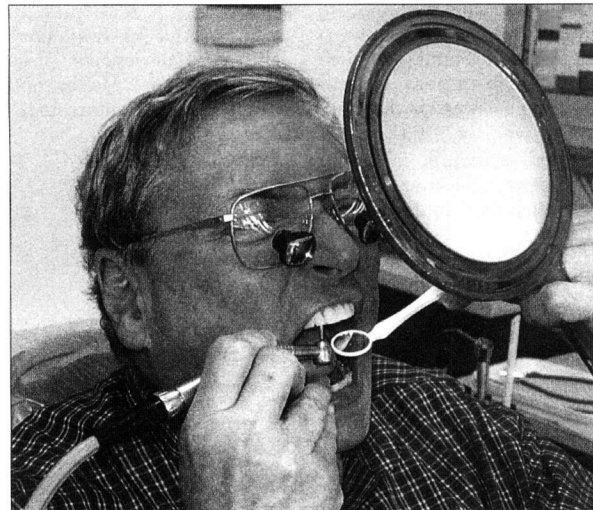


Figure 4. Don't fix your own teeth! Get some qualified help with the Internet. Computer systems are just too important to the operation of a practice to be "do-it-yourself" projects. A dentist's group of advisers, in addition to the traditional accountant, attorney, and insurance professionals, now needs to include an information technology (IT) professional.

they think you need even more Spam to stay truly informed!) But at some point, adware becomes spyware, as it records more information about you, your staff, and perhaps your family.

One of the best-known spyware programs on the market is the \$99 Win-WhatWhere program. It can be set up not only to track your online exploits but also to record everything you type, on or off the Internet. If you have a Web cam connected to your computer, it can also be set to take a picture at specific intervals, all "in the background." This information, including the pictures, is sent back to big brother by "stealthmail." This sounds like a really cool program, unless, of course, someone has installed it on your computer.

It gets even more exciting. Some of these adware/spyware programs have been implicated in spreading worms and other malware. You don't need to wait to download an e-mail attachment or go to a "bad" Web site; a worm or virus can be actively sought out and installed for you by one of these programs. Be sure to discuss with your IT security person the need to use such programs as Adaware or Spybot Search and Destroy to remove adware/spyware from your system.

CONCLUSION

The purpose of this article is not to scare dentists away from the Internet but to stress the need for adequate protection and safety precautions. Just as with electricity, the benefits far outweigh the disadvantages. Spending a little time and a little money to ensure a safe Internet connection is extremely cost-effective. Embracing the Internet, like using electricity, should be an interesting and rewarding experience, not a "shocking" one.♦

Dr. Stephenson practices restorative and paperless dentistry in San Leandro, Calif. He has been writing, lecturing, and consulting on dental computing since 1985. For a free copy of his dental computing newsletter, contact him at (510) 483-2788, e-mail bruce@painlesscom.com, or visit paperlessdentistry.com.

Mr. Jacoby is the founder of InnovaCrew, a computer and network support firm specializing in small businesses based in Sacramento, Calif. Clients include dentists, physicians, nonprofits, manufacturing, and financial service companies. Mr. Jacoby can be reached at (916) 773-7222, via e-mail to josh_jacoby@innovacrew.com, or by visiting innovacrew.com.