Email security revisited

In the Aug. 1 issue of *CMAJ* (157:310) I discussed the threat inherent in sending confidential information via email over the Internet. I mentioned that public-key encryption schemes, which are included with new versions of Microsoft Outlook Express and Netscape Communicator, can protect email contents from prying eyes.

I failed to note that version 5.0 of Phil Zimmerman's encryption utility called PGP (Pretty Good Privacy) has been released and features seamless integration with Microsoft Outlook for Windows 95, Microsoft Exchange 4.0, Eudora Pro for Windows 95/NT and Macintosh, and Claris E-mailer for Macintosh. A 30-day evaluation copy is available (**www.pgp.com**).
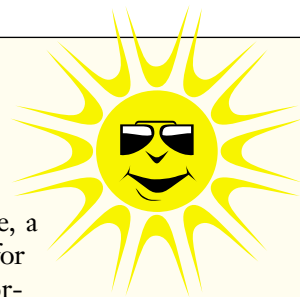
In this column I want to discuss security on the World Wide Web and the streetproofing of cyber citizens. Like email, much of the information that is on the World Wide Web is unencrypted. Back when information could only move in 1 direction, from a Web site to your browser, security wasn't a major concern. However, when the capability to send information back to other computers on the Web was developed, the information you transmit became vulnerable to interception.

For example, whenever you fill out a form using your Web browser on an insecure Web site, a third party can intercept the information transmitted back to the server. From a computer criminal's perspective, it is child's play to write a program that sifts through the unencrypted traffic on the Web and captures all strings of 13 integers that begin with the numbers 4 and 5, as certain credit cards do. Fortunately, most new Internet browsers such as Microsoft Internet Explorer 3.0 (**www.microsoft.com**) and Netscape Navigator and Communicator

(**www.netscape.com**) support security protocols that make Web sites safe from third-party interception.

You can tell if a site is secure because secure-capable browsers display an image of a closed lock on your computer screen's status bar. This indicates that the browser can send and receive encrypted communications involving that site. The lock indicates that you can safely enter sensitive information such as your credit-card number.

When information is sent to a secure site, secure browsers serve 2 purposes: they encrypt the information and they verify that you are sending the information to the correct Web site and not to an impostor's site. These security features provide end-to-end encryption of transactions involving reputable online merchants, while denying criminals the opportunity to intercept your credit-card information. VISA has already published several detailed articles on secure electronic commerce at its Web site (**www.visa.com**).

The other main problem involving the Web is personal privacy. If a site wants additional personal information such as your address, current income or number of teenagers living under

your roof, check carefully for a notice indicating that this personal information will not be used for marketing purposes. If the notice is absent, prepare to receive lots of junk mail.

Personal security in cyberspace, like security in the real world, should not be taken lightly. However, as in the real world, netizens who take adequate precautions and avoid unnecessary risks will face few threats. — *Warren Lampitt*, information systems manager, Gretmar Communications (**warren@gretmar.com**)

Highlights from *CMA Online*

MD Management's Practice Management (**www.cma.ca/mdmgmt/pratmngt.htm** [**pratmn_f.htm** — French]) is a new addition to *CMA Online* and will appeal to physicians with an interest in the business side of medical practice. The site provides practical information on practice management from experts at MD Management, and explains how doctors can learn on their own time with the *Guide for Practice Productivity*. It also provides details on a special program for medical students and residents. — *Dawna Ramsay*

Cool site

www.virtualkamloops.com/cloughs/orth-link.html

Myles Clough, an orthopedic surgeon in Kamloops, BC, manages the Orthopaedic Links Page, a collection of evaluated links intended primarily for health care professionals. Extensive patient information and handouts are also available. Clough and colleagues who manage orthopedic links pages in other countries have begun annotating their links and combining their collections in hope of creating an authoritative resource (Orthopaedic Web Links) that is accessible from each manager's site. "The task of finding and evaluating the information available to orthopedic surgeons and patients is far greater than an individual or organization can undertake," notes Clough. He invites enquiries from potential contributors (**cloughs@mail.netshop.net**). — *Ann Bolster*