Health Information Compliance Alert

SECURITY TIP: PREPARE TO ACCEPT THESE IM SECURITY RISKS

Your firewall won't catch viruses sent via an instant message

Instant messaging can streamline your workflow, but any IM that crosses the 'Net could open a security hole.

Tackle these security danger zones before you use any rapid messaging system, advises **Tom Walsh**, a security expert at Tom Walsh Consulting in Overland Park, KS.

1. IMs use an unprotected port.

E-mails enter and leave your electronic network through a port in your firewall that scans all e-mails and their attachments for known viruses.

IMs, on the other hand, enter and leave your network through a completely different, unsecured port that does not scan any attachments.

2. You cannot verify IM users.

Any person using a commercial IM application can create a screen name that looks legitimate. It's almost impossible to verify that the person sending you an IM is who he or she claims to be.

Example: A remote user asks you through an IM to reset her password. You ask her to supply a piece of identifying information. She supplies several types of information, including the last four digits of her Social Security number. Why it's not enough: Though the user provided several pieces of hard-to-know data, a criminal could acquire all of it through social engineering or other form of data theft.

The Bottom Line

You must only send IMs across your closed, protected network. And any user needing tech support must use either telephone or e-mail to request help.