Optometry Coding & Billing Alert

HIPAA Corner: Use 5 Guidelines to Prevent Internet Attacks

Send e-mail scams to the recycling bin with these tips

Think your employees know how to stop an Internet scam in its tracks? Educate your staff so they know how to react to even the simplest virus or hoax--or risk leaking your patients- PHI to hackers and identity thieves.

Strategy: Distribute a -Do's & Don-ts- tip sheet containing Internet safety strategies similar to the ones below, says **Elisabeth Derwin,** an information technology specialist with Bennet Health System in San Francisco.

Internet Safety Do's & Don-ts

1. If you don't recognize the sender, don't open the e-mail or attachments. Check for these common signs of an e-mail virus: 1) The e-mail's subject line is suspicious (e.g., -iloveyou- or -Anna Kournikova-); 2) it was sent in the middle of the night; and 3) there are multiple messages containing attachments from the same sender.

2. Do use hard-to-guess, frequently changed passwords. The strongest passwords mix upper case, lower case, numbers and symbols to create a code not found in the dictionary. Remember to make your passwords at least eight characters long and create multiple passwords for each site that requires you to log in.

3. Do connect to the Internet when you need something and disconnect when you don-t. The Internet sends and receives information the entire time you are connected to it. To lessen your risk, disconnect when you-re not using the Internet.

4. Don't use the -Unsubscribe- feature on spam e-mails. Spammers have no clue how many of the e-mail addresses on their lists are valid. But, as soon as you send an -Unsubscribe- reply to their message or go to their Web site to unsubscribe, you-ve confirmed that your e-mail address works.

5. Don't reply to e-mails asking for your credit card number or other personal information. Many high-tech scams deceive consumers into sharing their confidential information. Never confide your financial or other personal information via e-mail--even if you are positive the sender is legitimate.