Health Information Compliance Alert

Clip 'N' Save: Use These Guidelines to Safeguard Against 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? Think again. You must educate your staff members on 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 similar to the one below to all your regular e-mail or Web users. Tell them to refer to the sheet each time they spot a suspicious e-mail or are contacted by companies claiming to need personal data, advises **Elisabeth Derwin,** an information technology specialist with Bennet Health System in San Francisco.

Internet Safety Dos & Donts

1. If you don't recognize the sender, don't open the email or attachments. Before you open the attachment, try to determine if it's legitimate by scanning the e-mail. Does it contain a phone number you can call to double check that the attachment is not a virus? If a friend or co-worker sent the attachment, call or e-mail that person to make sure they meant you to receive the file. But, if the body of the e-mail is empty or contains text that makes no sense to you, your best bet is to delete the e-mail without opening the attachment.

When in doubt, 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 (e.g.,). You can also build your passwords from slogans or phrases that you encounter every day.

Best: Think of a phrase or your favorite song lyric. Then shorten the line to the first letters of each word to come up with your password. Remember to swap out at least one letter for a number and one letter for a symbol, and make at least one letter uppercase.

Example: You can shorten "All the world needs is love" to "ATWNIL." Then swap out a few characters to create "@TWN1L." Next make some of those letters lowercase: "@tWn1L." Now you'll need to add two characters to lengthen the code to eight characters: "&@tWn1L&."

Remember to make your passwords at least eight characters long. And, you should create multiple passwords for each site that requires you to login.

4. Do connect to the Internet when you need something and disconnect when you're through. The Internet sends and receives information the entire time you are connected to it. By disconnecting when you're not using the Internet, you lessen the chance you'll receive something malicious.

5. 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. That means they'll just keep on spamming you. And any of those spam e-mails could be the one that contains a virus.

6. **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.

Strategy: Beat data thieves at their own game by deleting these e-mails immediately and then calling the institution they were supposedly from. Never share your financial or other confidential information via e-mail even if you are positive the sender is legitimate.