Health Information Compliance Alert

Security Tips: Create A Failsafe Procedure To Protect Office From Leaks, Viruses

Train staff to recognize and eradicate Internet scams

Staying on top of viruses and hoaxes as they appear and keeping staff informed about handling them will go a long way to protect your office's confidential information--from sensitive financial records to patients' protected health information.

Follow our experts' advice for designing a policy and procedure to protect your staffers--and sensitive information--from even the trickiest Internet scams.

Appoint A 'DSO'

Someone in your office must be aware of what scams are circulating the Internet, says **William Hubbartt**, president of Hubbartt & Associates, a privacy and security consulting practice in St. Charles, IL. Your office may have a designated security officer (DSO) to keep tabs on the Internet, but most smaller offices do not have a full-time DSO.

Part of the DSO's job should be spending a certain amount of time visiting security Web sites and reading how the newest viruses or scams can be detected and prevented. Constantly checking for software and anti-virus updates is an important part of this process, Hubbartt stresses.

And, as your DSO develops new ways to fend off e-mail and Internet attacks, he or she should update your policies and procedures to reflect all new approaches.

Educate All Employees

An office's best-laid plans to ward off leaks and viruses will be foiled if just one staff member opens the wrong e-mail or visits the wrong Web site, points out **Chad Markham**, information security officer for Mercy Medical Center in Sioux City, IA.

Solution: Markham sets up regular security training sessions with his staffers to remind them about Mercy Medical Center's policies and procedures. He also uses this time to educate his personnel on the latest happenings in e-mail and Internet hoaxes.

Between training sessions, Markham uses newsletters and e-mail reminders to keep his staff members on their toes about the dangers of e-mail and the Internet. The following sample scripts are email messages that Markham has sent out to staffers in the past:

Sample script 1: "Immediately delete an e-mail if the subject line, punctuation or attachment extension looks suspicious. Some examples of this are: !HATNow!!, iloveyou, or File.mp3.exe. If you are unsure about an attachment, send it to the IT team without opening it."

Sample script 2: "Never respond to an e-mail asking you for financial, medical or other confidential information. If the sender looks familiar to you (such as an e-mail from the medical center's or your bank's domain), pick up the phone and call to verify that they need the information--then give it to them over the phone. However, in 99.9percent of these cases, the e-mail is a scam."

Codify
BY AAPC