Health Information Compliance Alert

READER QUESTIONS: PHISHING AND PHARMING--LEARN THE DIFFERENCE

Question: Our medical office has had problems with "phishing" scams on our Web site. Today, I happened to overhear the head of IT mention "pharming" in a conversation. This sounds so similar to "phishing" that it got me thinking--and worrying. What is "pharming," and do we have to safeguard our office Web site against it?

Tennessee subscriber

Answer: Unfortunately, "pharming" is very real--and potentially quite damaging to medical offices caught unawares.

Experts are warning medical offices that have their own Web sites about this scheme, which could severely compromise your patients' identities and health info.

Pharming might well be called "Phishing 2.0," because it represents a fairly new, and more devious, update to the concept of "phishing."

With phishing, your patients are sent an e-mail solicitation asking them to click on a URL that is supposed to send them to your Web site but routes them to a fake Web site instead. Your patients enter their logon information--giving the crooks access to valuable personal information.

Pharming kicks this concept up a notch. The attack still originates with an e-mail that tricks patients into clicking on an embedded URL. If they fall for the scam, they're providing confidential data to the ne'er-do-wells. But with pharming, the URL your patients click on is an exact match to your institution's URL, says Donna McIntire, product marketing manager with Postini E-mail Solutions in Austin, Texas.

In addition, with pharming, an embedded virus installs a code on patients' computers. The virus poisons each server the e-mail goes to in order to redirect patients to a criminal's Web site instead of your site, McIntire says.

If patients click on the URL in a pharming solicitation, and that code poisons whatever server they connected to, they'll be taken to the phony site without realizing it.

What's the difference? The false site is exactly the same as your site, with one crucial exception: When patients log on to your site, a "key" or "lock" symbol is viewable that indicates a secure session.

"If you go to the criminal's Web site, that's not the case," McIntire says.

Pharming affects only those Windows programs that came out before 2003. If you're running Windows software older than 2003, such as Windows 98, and not keeping up with the Microsoft patches for this threat, you're at risk, McIntire says.

Ask a techie for help: The only way to prevent phishing is to have your technical consultant do something about it.