Health Information Compliance Alert

Internet Safety Tip: Be On the Lookout for This Sinister Scam

You have every reason to worry that your patients could be tricked into divulging their information to ID thieves. A new hoax-called "pharming" could be extremely damaging to your patients' identities.

Pharming kicks the concept of phishing up a notch. Phishing: Your patients are sent an e-mail with an embedded link that appears to be from your organization. When users click on the link, they are sent to a crook's Web site instead.

The difference: A pharming scam asks your patients to click on a URL that is an exact match to your institution's URL, says **Donna McIntire**, product marketing manager with Postini Email Solutions in Austin, TX.

Problem: 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 notes.

The bottom line: You can help your patients avoid this scam by advising them to always search for the secure session indicator. And, remind them that if they aren't sure about whether an e-mail is legitimate, they should pick up the phone and investigate.

Editor's note: Don't wait for a patient or employee to bring a pharming attempt to your attention. Alert them now so that they can spot and squash crooks' attempts to hi-jack confidential information.