HealthManagement
Promoting Management and Leadership

Check! Don’t get hooked!

Phishing attacks are increasing and have become a significant risk to the health-care industry. “Phishing” is the current weapon of choice for cyber attackers.

Phishing is one of the more popular methods used by scammers to access secure data. A phishing attack is when someone is tricked into providing access credentials or visiting a fake website that installs malware. Hospitals are particularly vulnerable to phishing schemes, according to experts, who note that many ransomware programs have been created specifically to target healthcare facilities and the sensitive info stored in their systems.

You might also like: Part 2: How to be 1 step ahead of healthcare cyber hackers

Here are five simple steps to help reduce your facility's risk from this form of security threat.

1. Determine which employees are most vulnerable. Sending out fake phishing emails can show you which staff members are most susceptible to downloading unknown files or visiting suspect websites. With this knowledge, you can target training directly to those employees and monitor improvement. To avoid problems, you may want to limit their access to confidential data – or their access to a computer altogether.

2. Implement multifactor authentication. Many companies already use this as a security measure, and it can work for your hospital, too. How it works: Once someone enters their username and password, they have to put in an additional code sent to another device, like a smartphone, before they can log in. This can boost the security of your electronic health records (EHR) system and prevent unauthorised access.

3. Discuss extra security. Talk to your IT department or EHR vendors who may be able to suggest other security steps you can take, and offer advice on how to train employees and get them to buy in to any changes.

4. Stress safety’s importance. There may be resistance from some staff members who don’t want to take extra steps to log in or don’t want to spend time learning a new system. It will help by making them aware of the importance of implementing such advanced safety features.

5. Plan your budget. Instituting some of these security steps can be expensive, but keep in mind that a data breach could be much more costly and difficult to deal with. Weigh your options accordingly, and allocate a budget that best fits your hospital’s cyber security requirements.

Source: Healthcare Business & Technology

Published on : Tue, 23 Apr 2019