HealthManagement
Promoting Management and Leadership

## Staff Training to Prevent Hacking Attacks


Insider-caused breaches have proved to be costly for a number of companies, according to a report from cybersecurity firm Forcepoint. Tech experts suggest some training strategies to help your staff from causing data loss or leak.

Technology can do its part in protecting against cyberattacks, but user education is key to bolstering the human factor. There are different ways to look at user education and different ways to train during the educational process, some experts point out.

“Healthcare organisations should look at insiders on a spectrum; essentially, users fall into a category – accidental, compromised or malicious – but can fluidly move along this continuum based on external factors such as job satisfaction, training or fatigue,” said Bob Hansmann, director of security technologies at Forcepoint. “The key here is that the way that each type of insider interacts with data, like patient records, and their intentions or motivations behind that interaction vary."

For Hansmann, knowing the types of insiders can help in designing the appropriate types of education and solutions to prevent insider-caused data hacks.

**Accidental insiders.** They can be inadvertent actors or convenience seekers – both make unintentional mistakes whether the intent was due to negligence or simply attempting to do their job, but not following the process, Hansmann said. These insiders require a focus on education, awareness and best practices for completing tasks safely and effectively, he added.

**Compromised insiders.** They can be malware victims or impersonated users – in both cases, the malware is attempting to act as the user. Since credentials are often stolen through social engineering, these users should be keenly aware of what they are clicking on or information they are providing to unknown sources, Hansmann said. "Ensuring you have proper web and e-mail solutions in place also can help limit these users' interactions with potentially malicious content.”

**Malicious insiders.** They include rogue employees or criminal actor employees, who typically comprise the smallest portion of insider threats in a given network. Having a strong data loss prevention solution and insider threat programme often will lead to the discovery of such users, Hansmann said.

Moreover, it’s important to have awareness training about the proper tools to accomplish various business tasks, Hansmann added.

“This all rests on the idea of looking at the point where healthcare workers interact with sensitive data,” he said. “Many mistakes happen when a user creates a workaround simply because they do not understand the official process available. And on another note, general education about the organisation’s ability to monitor for abusive activity can help prevent incidence of opportunity. There are many case studies of this that draw on the use of cameras to help reduce crime because people are afraid they might be caught.”

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 4 Jul 2017