HealthManagement
Promoting Management and Leadership

Visual Hacking Threats: Expert Tips for Healthcare

The HIPAA does not stipulate the need to train employees to protect against the visual hacking but healthcare CISOs and CIOs should not let this practice fly under the radar says a IT security expert.

Kate Borden of the Visual Privacy Advisory Council says that the low-tech nature of visual hacking means it is often overlooked in the drive for IT security

“It starts with awareness,” Borten said in a HealthcareITNews interview. “Visual hacking flies under the radar and tends to be overlooked.”

The 2016 Ponemon Institute report, *Global Visual Hacking Experiment*, showed 91 percent of visual hacking attempts were successful.

Visual hacking is related to spying on physical items, such as a desktop, a computer screen or a mobile device. Such attacks happen swiftly and are difficult to detect and trace.

See Also: Departmental Reorganisation for Better ITSecurity

Morten says the problem is CISOs and CIOs are usually focused purely on routes into IT security breaches rather than alternative routes such as visual hacking.

However, simple adjustments can help healthcare leaders improve protection against the visual hacking threat.

A common mistake in healthcare include:

- leaving important papers in stacks on desks and around recycling bins;
- risky fax machine placement in high traffic areas;
- poor computer monitor placement and angling.

Morten also suggests better walk-around checks where privacy officers work to a checklist of ways of fighting visual hacking and monitor staff implementation of security measures.

Putting such measures in place can also help an organisation in the event of a security breach says Morten. “The organisation can demonstrate it was taking the steps needed to protect information.”

Also, visual hacking of healthcare data isn’t confined to the four-walls of a hospital. Borten stressed that mobile devices have increased the risk of hacking. While many organizations consider privacy filters for log-ons for workplace screens, these filters should be required on all devices.

“This is a pervasive thing and healthcare providers in particular are in a sticky situation because they’re essentially open to the public,” Borten said. “Anyone can walk in and the exposures really do create a risk.”

Source: HealthCareITNews
Image Credit: Pixabay

Published on : Mon, 12 Sep 2016