HealthManagement
Promoting Management and Leadership

Hackers Target Junior Staff

Cybercriminals are adjusting their social engineering tactics to focus on the more vulnerable members of an organisation: the junior staff. While top executives who usually have wide-ranging digital access can be considered as prime targets, they also are likely more capable of protecting themselves and their assets against possible phishing attacks.

Because of their positions and key digital access, C-suite level executives often receive high-quality cybersecurity education. In fact, a new study shows that the higher an employee's annual income, the more likely it is that employee has received cybersecurity training at their organisation. The "Cybersecurity Training in the Workplace" survey was conducted by cybersecurity vendor ESET.

It's no wonder that spear-phishing hackers are targeting lower-level employees -- smaller fish who nonetheless have key access. CIOs and CISOs need to be aware of this tactic and protect junior staff as well as they do senior executives.

"CXOs may be protected by extensive cybersecurity training; on the other hand, gatekeepers, such as administrative assistants, who screen and filter through incoming requests, calls and e-mails before escalating to the top, often are moving quickly and have not received the security education required to filter out phishing attacks on their own," said Asaf Cidon, vice president of content security services at cybersecurity vendor Barracuda Networks, which has observed more junior staff members being spear-phished.

For example, admin assistants are a first point of contact for a CXO and they open most emails. In an impersonation scam, a frequent social engineering tactic, a phisher could masquerade as an internal member of an organisation and target admins to obtain personal information and credentials for further network access, Cidon explained.

Another social engineering tactic used to target and interact with members within an organisation is through social media scams, where it can be easy to determine where an individual falls in an organisation chart.

"This can be a request for a connection on LinkedIn, or an impersonation on collaboration tools like Slack or Mattermost," Cidon said. "Once the connection is made on social media, an attacker can pose as a non-threatening actor, or leverage the relationship to conduct more in-depth research on a target. Because of the personal nature of these initial attacks, and the fact that most of them do not contain malicious files or links, traditional email security solutions can't stop these attacks."

Healthcare CIOs and CISOs have an even greater responsibility when combating phishing. This is because a health system can span multiple hospitals and include hundreds and sometimes thousands of staff members, all of whom have access of some kind to the network, and access to patient information, Cidon points out. To protect patient data, IT teams should install appropriate software defences, such as e-mail filters, firewalls and threat detection systems, Cidon adds.

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Wed, 28 Jun 2017