Alberta Doctors' Digest

Cyber security now

Cyber attacks on Canadian health care organizations, ranging from individual physicians to large health care institutions, have been increasing at an alarming rate. Successful attacks on large hospitals and regional authorities have made headlines, while clinics across Canada fell victim to attacks resulting in exposure of thousands of patient records. In fact, nearly 50% of breaches in Canada in 2019 occurred in the health care sector.

Taking advantage of the pandemic

To add to this growing threat, cyber criminals are aggressively taking advantage of the current COVID-19 crisis. The increased volume of communications and updates sent to health care professionals, along with a sudden move to virtual care, has further increased the risk of cyber attacks. COVID-19 provides a perfect cover for emails disguised as official notices that contain malicious links to fake websites impersonating official organizations. The Canadian Centre for Cyber Security has identified over 1,500 websites posing as Government of Canada COVID-19 pages designed to scam Canadians. In late May, CCCS warned Canada's health care and medical research sectors that they are of particular interest to cyber criminals, particularly state-sponsored ones.

There has been a dramatic surge in cyber attacks against physicians, clinics, health care professionals and hospitals stretched by the crisis. Since the COVID-19 outbreak, there has been a 150% increase in cyberattacks in the health care sector.

COVID-19 provides the perfect environment for socially engineered cyber attacks (photo credit: Darwin Laganzon, Pixabay.com)

Targeting busy health care professionals

COVID-19 provides the perfect environment for socially engineered cyber attacks. Cyber criminals use social engineering to exploit natural human vulnerability and to deceive and hack busy health care workers. The most common form of social engineering is phishing, which is an attempt to trick recipients into clicking on a link or downloading an infected file. Successful phishing can lead to encrypted files, such as patients' personal health information. Cyber criminals then demand a ransom payment to restore access to the files.

"The doctors are under attack," says Dr. Dennis Desai, a physician advisor at the Canadian Medical Protective Association. "We are getting physicians on a regular basis saying, 'I have a computer; I got locked out; I have ransomware.'"

Cyber criminals often consider the human element to be the weakest link in a health care organization's security. Physicians and health care workers are one click away from unknowingly infecting their entire organization's IT systems with malware and other viruses. Cyber criminals are skilled at exploiting basic human psychology and tapping into fear, curiosity and the desire to help. The email content is designed to manipulate employees into clicking before verifying the link is safe.

Safeguarding against social engineering

While a modern and robust IT network can be highly effective at preventing some cyber attacks, technology is only one component of a strong cyber defence. A knowledgeable and aware "human defence" is critical.

Clinics may not know that awareness resources and affordable education programs designed specifically for health care teams are available to them. Training the health care team on cyber security and privacy best practices is vital. Phishing and malware attacks can lead to locked-down institutions, health systems and encrypted electronic patient records; the need to provide information on avoiding such a breach is urgent. An effective cyber security and privacy education program is crucial. Engaging the entire health care team in ongoing, evidence-based, and health care-specific training helps the team avoid a breach and identify and react appropriately if a breach should occur.

Banner image credit: Darwin Laganzon, Pixabay.com