5 Ways To Detect A Cyber Attack

This article was originally published on Huffington Post Canada.

Businesses aren't reacting fast enough to malicious network activity. In fact, the industry average for detecting threats is 100-200 days and that's not nearly fast enough, according to the 2016 Cisco Midyear Cybersecurity Report. Having an effective cyber security plan is becoming increasingly important for all businesses to counter the ever-evolving security risks they face. The plan must implement strong IT security tools, have a strategy for emerging threats and consider education programs for staff since most attacks are caused by human error. Cybersecurity is a shared responsibility. Become a part of the detection process by looking out for these five signs of a cyber attack, presented in partnership with Cisco.

Identify mysterious emails

Email phishing refers to a method used by malicious actors to access sensitive business information by pretending to be a trusted organization or website. Phishing attempts are growing in number and it would be an understatement to note that employees need to practice safe email protocol and should be careful when clicking on online links from unknown sources or opening email attachments. And it almost goes without saying that employees should never respond to such emails as any response validates the recipient email address which might lead to continued attacks.

Note unusual password activity

If an employee is locked out of their system and/or receives an email stating that a password has been changed, it is a potential sign that the password is compromised if they did not initiate any of this action. A good security best practice is to ensure that all employees create a strong password for email and the network that's updated every six months.

Identify suspicious pop-ups

Increased security awareness in a business environment also means safe web browsing. Employee should avoid clicking on web pop-up windows, even to close them. Unknown pop-ups can be infected with malware or spyware that can compromise the network.

Report a slower-than-normal network

A hacking attempt or malware outbreak often results in spikes in network traffic that can reduce internet speed. Employees should inform the IT security department when they face substantially slower than normal network speeds.

Keep software up-to-date

While human error is often the cause for a network breach, ensuring that the IT software environment is current can help reduce the likelihood of malware attacks. This involves ensuring that regular patches and updates are implemented and all desktops, laptops and mobile devices are locked down with the latest cybersecurity tools. That ensures that staff are more safe and in a better position to detect and identify when a potential security attack is in progress.

The threat of a cyberattack on your business is real. Protecting the business network comes down to ensuring security controls are in place across the organization. Cisco offers security solutions that are simple, open and automated to allow organizations the freedom to focus on their core business so that they are better poised to take advantage of a new world of digital business opportunities.