EBOOK

Logicspeak℠

PROTECT YOUR SMB FROM CYBERATTACKS

Train Your Employees – They're Your First Line of Defense.

If you think your small business isn't a target for cyberattacks because of its size, or because you don't have anything worth stealing, you're wrong! Cybercrime is growing exponentially, and your small-to-midsized business (SMB) is a prime target!

DID YOU KNOW?

- In 2015, **43% of Cyberattacks** Targeted Small Businesses?
- A 2014 survey conducted by the National Small Business Association underscores just how serious a threat cybercrime poses to SMBs. According to the survey, **half of all SMBs surveyed** reported being the target of a cyberattack – This was a 14 percent increase over the previous year.
- **44% of small businesses** reported being the victim of a cyberattack, with an average cost of approximately $9,000 per attack.
- In 2016, **80% of U.S. companies** suffered a cyberattack, and 47% of these were due to ransomware.
- **Nearly 50% of U.S. SMBs** don't have a contingency plan that outlines procedures for responding to and reporting data-breach losses.

Juniper Research estimates that cybercrime will cost businesses **$2.1 trillion globally by 2019,** an increase of almost 4X the cost of breaches in 2015! Many SMBs aren't prepared to deal with security threats, often due to inadequate resources and interest. This is another reason why SMBs are a prime target for cybercrime.

YOUR FIRST LINE OF DEFENSE IS TRAINING FOR YOUR EMPLOYEES SO THEY CAN RECOGNIZE TACTICS HACKERS USE, AND MITIGATE ATTACKS.

The lack of employees' cybersecurity awareness is the leading cause of successful ransomware attacks. This is the easiest way for cybercriminals to obtain access to your private data.

Phishing: This is the most popular tactic used by today's ransomware hackers. They deliver malware in the form of an email, chat, web ad or website, and design it to impersonate a real person or organization. They send a message with a sense of urgency and importance, from a government agency or a major corporation, to trick your employees.

Baiting: This is similar to phishing, and typically involves offering something enticing to an employee in exchange for private data. The "bait" could come as a digital file, such as a music or movie download; or a fake link in an email saying "check out our new employee policies." Once they go for the bait, the malware is free to infect their computer, and your network.

Make sure your employees are aware of emails containing attachments that they aren't expecting. Before clicking on anything, they should confirm who the sender is via a phone call, text message, or by sending a separate email.

Quid Pro Quo: Quid pro quo is a request for the exchange of private data for a free service. In some cases, the hacker poses at a technology expert offering something for free to an employee, in exchange for their login credentials.

Tailgating: This is a physical intrusion where an unauthorized person follows one of your employees into your premises. The criminal asks the employee to hold the door open for them, claiming they've forgotten their entry card. Or they may ask one of your employees to "borrow" their company laptop for just a few minutes. They then quickly steal data or install malware.

Pretexting: This is when a cybercriminal develops a trust between themselves and an employee by impersonating a co-worker or other authority. When this is done, they convince the employee to share your company data. For example, they send an email posing as the head of a department asking for access to a file. Or they'll get a pop-up message that claims their computer has been locked by the FBI because it was used to access illegal material such as child pornography. They are warned that they must click a link to pay a fine. Believe it or not, people are fooled by this.

Teach your employees to recognize cyber scams designed to prey upon their fear of breaking the law. Be sure to tell them NOT to click anything.

Malicious Websites and Malvertisements: These are designed to look like a legitimate webpage or website. Cybercriminals can make them look incredibly real by display branding and logos from actual organizations (such as banks). The hackers then insert a code into a legitimate site which redirects unsuspecting users to their malicious site.

Teach your employees how to check URLs by hovering their mouse over the link to reveal the complete URL in the status bar at the bottom of the browser.

ONLY WITH ONGOING STAFF TRAINING ABOUT CYBERCRIME CAN YOU DECREASE THE LIKELIHOOD THAT YOUR DATA WILL BE BREACHED DUE TO EMPLOYEE ERRORS.

Logicspeak will take the stress out of technology for you and your business. Contact us at (678) 990-0068 to talk about how we can help.

Logicspeak℠

WWW.LOGICSPEAK.COM