Matt Duray
President

Connect Telephone & Computer Group Leverages State-of-the-Art Cybersecurity Techniques and Tools to Protect Customers

Leading Expert in Cybersecurity Secures SMB Networks

Billings, MT – December 19, 2016 - Connect Telephone & Computer Group a leading provider of unified communications, announced today that the company is leveraging state-of-the-art cyber security techniques and tools to protect customers from cyber attacks that have become a daily occurrence in the small to mid-sized business marketplace. The company has been at the forefront of cybersecurity for many years and has taken their expertise to an entirely new level, well beyond their competition. Connect Telephone & Computer Group protects businesses from several key cybersecurity threats.

The first threat facing organizations is phishing. Phishing is essentially, using fake links to lure users into offering up sensitive information, by posing as an authority. Hackers can embed malicious links into emails, attachments or images, which usually lead to another page that requests the sensitive information, which will later be used against the user. One of the most creative ways hackers have found to attack SMBs is to call in and impersonate IT staff or Network Administrators, asking for specific information off the employee's computer to resolve a potential "virus." The employee will usually comply and supply the information, giving the hacker the exact keys they need to infiltrate the system.

The next area of concern is mobile security. As web traffic continues to migrate from PC to mobile, hackers have followed suit by redirecting their efforts to mobile attacks, as well. At an organization, whereby users are encouraged to BYOD (bring-your-own-device) to the network, this increases the exposure for network attack exponentially. SMBs need to be on the lookout for attacks from third party apps, mobile malware and unsecured public Wi-Fi locations. For example, employees will use their phone at an unsecured Wi-Fi hotspot to work but they won't realize that the network is rigged to enable hackers with easy access to sensitive apps, data and information on any phones connected to that particular unsecured Wi-Fi hotspot. In many cases, users will be attacked without even realizing that the attack has happened.

The last area for an SMB to monitor is malvertising. This threat is where hackers embed malware within advertisements, landing pages or even directly on reputable websites. Sites that offer advertising on a massive scale, such as Facebook, have a tough time regulating online security throughout the buying process. Facebook can do its best to ensure that the links on Facebook aren't malicious; however, they have no access to monitoring the pages that those advertisements lead to, once the user has left Facebook. Malvertisers can embed a code on an advertisement which leads to a dummy checkout page or a fake application page, which phishes all of the sensitive information that the hacker needs to launch an attack.

"These threats all point to the importance of SMBs consulting with an expert in the cybersecurity field," stated Matt Duray, President at Connect Telephone & Computer Group. "We are well-equipped to deal with threats like these, in addition to the new threats that will undoubtedly arise over the coming years. For any business that leverages technology as one of its key productivity drivers, it pays to have a team like Connect Telephone & Computer Group to face the hackers of the world."

About Connect Telephone & Computer Group

Connect Telephone & Computer Group is Montana's premier telephone and data communications group. Connect provides industry-leading products, serviced by the most certified technicians in the region. The company's local dispatch center delivers round-the-clock service to ensure system reliability. The Connect Group also offers comprehensive service 24 hours a day, 7 days a week and emergency service guaranteed within 4 hours.