How do I protect my business from hackers or cyberattacks? Watch out for phishing and spear phishing

Small and medium-sized businesses are an attractive target for cyber criminals. What are the best ways to protect your business from hackers or cyber attacks? Along with setting up defenses such as firewalls or anti-malware software, don't overlook the threat posed by different forms of impersonation, particularly phishing.

The continued threat of phishing and spear phishing

Phishing is a type of scam involving emails that look legitimate. For example, an email that seems to come from a bank may request log-in credentials or credit card numbers, or maybe prompt you to click on a link to fill out a form. If you aren't sufficiently wary, these emails can trick you into revealing sensitive information or infecting your system with malware.

Spear phishing is a more personalized version of this scam. The email may look as if it comes from your boss, colleague, employee, or business partner, or even a close friend or family member. Ordinary phishing emails may get sent out to hundreds of people. In contrast, a spear phishing scam can get individually tailored to you or to one of your employees.

How can you reduce the chances of falling for these scams?

A recent article from *Dark Reading* points out that cyber criminals often research content for spear phishing emails by studying social media accounts. They can make their emails sound more authentic by referencing anything from travel plans to recent restaurants you've eaten at. Limiting information shared publicly on social media sites reduces the chances of successful spear phishing scams.

However, it isn't practical to expect that everyone you know will stop sharing personal information online. Protecting against phishing and spear phishing depends in large part on training employees to act with greater vigilance and awareness:

- They'll need to refrain from automatically responding to emails or clicking on links or files.
- If they have suspicions about an email, they'll need to know what steps to take next, such as who to report it to.
- Establishing clear policies at your business will help. For example, if you absolutely forbid sharing passwords and other sensitive information via email, any scam emails that ask for such information - even if they seem to come from a co-worker - will be regarded with greater suspicion.
- Verification procedures also help. If employees receive an email that seems to come from you and requests a financial document or other confidential information, they can call you to verify that you sent the request.

Even though sophisticated anti-malware programs can detect emails containing malicious links, don't rely on technological solutions alone to combat phishing. Vigilance and training are key to protecting your business from these potentially devastating scams. Please contact us for more information about strengthening cyber security at your business.

CST
Combined Systems Technology
800-944-2966 515-270-5300
www.cstoncall.com info@cstoncall.com