3 Must-Knows for Small Business Security

You probably don't spend a lot of your day thinking about network security in Minneapolis-St. Paul. In fact, you may not think of it at all unless something goes wrong. However, if you're the owner of a small- to medium-sized business, you're gambling with your livelihood. The incidence of cyberattacks targeted at smaller businesses in on the rise. In fact, the majority of attacks within the past few years have been on small businesses! Everything in today's business world is interconnected. There's rarely a business that doesn't use some sort of technology in daily operation. As a result, everyone is at risk of a cyberattack. Knowing what to protect yourself against is the first step in making your business more secure. While you should have a trusted IT partner to take care of the details, educating yourself on some basics is crucial.

Here are three things you must know about small business network security in Minneapolis-St. Paul.

1. **Knowledge is power.** One of the most dangerous things threatening your business is your own staff. Human

error accounts for much of cyberattacks. Simple things like failing to practice strong password protocol to accidentally downloading infected files or giving up information to phishing scams can all cause serious damage to your business. Educating yourself and your employees is the first step in protecting your business. Learn how to spot the signs of a nefarious email or attachment. Make sure everyone understands all the forms that cyber attacks can take including malware, phishing, and the like. Let them know how important it is to keep their software and machines updated instead of putting them off over and over again. Enforce strong password protocol for all accounts and devices. Make sure all of this information is also posted throughout the office so that it's top of mind for all employees.

2. **VPNs are important.** Does your business use a virtual private network (VPN)? These can provide an extra layer of network security in Minneapolis-St. Paul. If you have remote employees, you should mandate that they use a VPN for work, but it can also help for those in-house. VPNs route data through their own servers then mask IP addresses and encrypt data which keeps things private. This way, you can reduce the risk of having any information stolen (like passwords or business files) when remote workers access business accounts over an unsecured network. Many big-name corporations have their own VPNs, but small businesses can also take advantage of the technology through VPN service providers. It may be worth looking into for your business.

3. **Updates are crucial.** As noted above, updates are crucial. Many businesses are operating on outdated software which can put your entire network at risk. Everything you run for your business should always be kept up to date including operating systems, antivirus software, CRMs, and more. When systems aren't kept up to date, they're easier to hack. Updates provide security patches that shore up any vulnerabilities that hackers have discovered. If you find you're running a software system or piece of hardware that can no longer be updated, then you need to replace it.

If you're looking for help with network security in Minneapolis-St. Paul, let CMIT Solutions help. We'll right-size a plan to fit your needs and budget. With us, you get an entire nationwide network of IT professionals to support your business.

See Original Post Here