

5 Ways to Protect Your Business from Cyber Threats



You probably don't think about [network security](#) in the Twin Cities that often. Unless something goes wrong, most people don't think about systems that are working as they should. However, more and more [small- to medium-sized businesses are becoming victims of cyberattacks](#) every day. Many small business owners don't realize that they need to be as vigilant as their larger counterparts in ensuring their network and systems are protected, but they do! A majority of cyberattacks are targeted toward small businesses. Simply put, hackers know that small businesses have less resources to devote to network security, which makes them easy targets. Here are some things that you need to focus on to protect your business from mounting cyber threats.

1. **Back up your data.** Cyber criminals are after your data. It's as good as gold and hackers start with low-hanging fruit like small businesses that are unprotected. The first step in protecting yourself from threats is to back up your data. What would happen if a hacker took control of your systems or brought your network down? Where would your data go? Don't leave yourself vulnerable to losing everything you have in the event of a cyberattack. It is crucial that you regularly back up your data including financial records, client information, proprietary documents, and more. Simply putting a backup of your data on the cloud can avoid disaster.

2. **Secure devices.** This sounds simple and it is – secure all your devices. Some of the most frequent types of attacks are through malware and viruses, which infect devices. By installing security software with anti-virus and anti-spam filters, you're securing your devices against these destructive programs. Set up firewalls, too, and always make sure they're installed on portable devices.
3. **Mandate passwords.** Network security in the Twin Cities doesn't have to be overly complicated. Something as simple as mandating strong passwords in your organization can go a long way. Create a password protocol and ensure your employees adhere to it. Be vigilant, especially with administrator-level accounts where hackers can gain access to everything. Make a policy to change passwords frequently, too.
4. **Educate yourself.** One of the biggest threats to network security is [you and your employees](#). Many of the viruses and malware that infects businesses each year are introduced by unwitting employees through opening infected emails, downloaded infected attachments, or clicking suspicious links. Educate yourself and your employees on best practices when it comes to being safe online as the first line of defense.
5. **Get help.** Dealing with network security in the Twin Cities can be time consuming if done thoroughly and properly. As a small business, you may simply not have the resources or time to dedicate to efficiently protecting your business. If that's the case, bring in the professionals to help. The cost of hiring an outsourced IT team pales in comparison to the money that you'll lose through an unprotected network.

If you're looking for help with network security in the Twin Cities, let CMIT Solutions help. Our trained and talented IT team can take care of the small stuff that could end up being big stuff if the wrong person gets a hold of your information. [Contact us today](#) to find out more.

[See Original Post Here](#)