# Top 10 Small Business Cybersecurity Mistakes

GREEN MOUNTAIN IT SOLUTIONS

Professional IT for Vermont's Small Businesses

802-489-6948 | www.greenmtnit.com | Burlington, Vermont

## It happens here!

Just a couple years back, a Vermont retailer suffered a ransomware attack that cost them over $2 million in adjusted losses. Their systems were infected by a virus that encrypted their files and demanded a ransom payment to restore them. The company paid the ransom, but still lost months of work. They were lucky to stay in business.

The truth is, most cybersecurity attacks in small businesses take advantage of security issues that could have been easily fixed. Don't let your business be an easy target. Make sure you talk to your IT service provider about these ten common, easy-to-fix small business security mistakes.

## Security Mistake #1: Lack of Good Backups

Despite spending billions on security, even major players like Facebook or Google have suffered data breaches. No cybersecurity plan can be perfect, so it's essential to keep good backups. Research firm Gartner found that among companies without backups, "43 percent… were immediately put out of business by a major loss of computer records, and another 51 percent permanently closed their doors within two years." So, just 6% survived!

It's not enough to just *have* a backup, either. Make sure a copy of your backups are being stored off-site, such as in a cloud storage system. Also be sure that the backups are being monitored and tested regularly. A cyber-emergency is not the time to find out that your backups don't work.

## Security Mistake #2: Failing to Assess the Risks

Some business owners never stop to consider the potential impact of a security breach. Others tell themselves that their data is not important, or that they don't have the time or resources to improve security. These folks have never really considered the risks: besides data loss, there can be legal fees, recovery costs, lost productivity, and worst of all, permanent damage to your reputation.

A cyber-attack can cost your company millions of dollars, ruin your good name, and even put you out of business. Still, you'd be shocked how many small business think a cyber-attack can't happen to them—until it does.

Don't be caught off-guard. Talk to a trusted IT professional about your cybersecurity defense strategy.

## Security Mistake #3: Inadequately Trained Users

This could have been #1! According to SecurityMagazine.com, more than 99 percent of cyberattacks require a person to click something they shouldn't have. That means that someone clicked the wrong link, downloaded the wrong email attachment, or tried to install the wrong program.

Why would a hacker spend days on a sophisticated attack when they could trick your employees into helping them in a few minutes? Your employees are the most likely attack vector. In fact, many major cyber-attacks, including the recent one on Target stores, used simple tricks on staff members to gain access. You should ensure that all staff receive cyber-security awareness training. At Green Mountain IT Solutions, we offer FREE cybersecurity training for all our clients. Contact us today to find out more. Call 802-489-6948 or email info@greenmtnit.com

## Security Mistake #4: Being Careless with Email

Most viruses and cyber-attacks are spread through email. One type of email attack is *phishing*, a bogus imitation of a legitimate web site or service that steals your password when you mistake the fake site for the real thing. In recent years, we've also seen an uptick in *spear phishing*, where the attacker pretends to be someone you know.

Then there's email attachments and links. It only takes a click or two to open the wrong attachment or the wrong link and compromise your systems.

Green Mountain IT Solutions offers email filtering that stops malicious attachments and links from ever reaching your inbox. And again, security training is also vitally important to help your employees detect these attacks and stop them.

## Security Mistake #5: Poor Password Security

One of the worst things you can do is use the same password for everything. Do you do this? Come on, admit it! Imagine this: Facebook and Twitter both get hacked, and the attackers see that your password is the same for both. You can bet they're going to try that password for every bank and credit card site out there!

Another password mistake is using a password that's easy to guess, such as MyCompany123, Vermont802, GiantsF@n!, etc. Attackers today have programs that can automatically guess thousands of passwords in just a few minutes. If your password is weak, they'll guess it in no time.

You should also set up *Two-Factor Authentication* anywhere you can. You've probably used two-factor authentication before, maybe on your bank's website. Two-factor authentication means that after you enter your password on a site, you're sent a code by text message that you also must enter to sign in.

## Security Mistake #6: Using Out-of-Date Software and Not Updating

Updates, patches, and new releases—many of us find them to be a hassle, but it is critically important to stay up to date to avoid leaving security holes in your systems. Oftentimes, we want to keep our old QuickBooks 2005, or our old Windows 7 computer because we "just need it for that one thing." Avoid these temptations. They just aren't worth the risk.

Also be sure to install Windows and software updates as they are released. Updates are released to fix security issues that can be exploited by attackers if you don't update.

## Security Mistake #7: Letting Anyone and Anything on Your Network

We often run into a DIY "Guest Network" at a new client's office that turns out to be directly connected to the main network, with no wall between them. Another common issue we see is allowing employees to casually use personal laptops at work or allowing staff to install software and re-configure their PCs at will. If your employees have administrator accounts, they won't even have to ask before making whatever changes they want!

Obviously, this is a security nightmare. Be sure to lock down your network and only allow access to those who need it. Never grant anyone administrator access if you can help it. Also, consider physical security measures such as security cameras or alarms to keep attackers physically away from your network.

Green Mountain IT Solutions can configure a secure guest network and create a system that allows employees to securely use their own devices and work from home. Contact us today at 802-489-6948 or email info@greenmtnit.com to find out more.

## Security Mistake #8: Using Old or Misconfigured Equipment

We often run into network equipment such as switches, routers, or even printers that are well over 10 years old, or newer devices that just weren't set up securely. This also applies to gadgets like video doorbells or remote thermostats. Older equipment often has unpatched security flaws, while consumer devices may have intentional compromises installed by the manufacturer or even a foreign government (looking at you, China), or they're just poorly made.

Make sure your network has modern, business-class equipment installed and that it is kept up to date. Be sure to ask a professional for help with installing any new network devices.

## Security Mistake #9: Leaking Information Outside Official Channels

The most common type of data leak in small business is using personal email accounts like Gmail or Yahoo for work, or personal cloud storage like Dropbox. These services cannot be secured in the way business-class systems can, and they can make it difficult to know exactly who can access your data. As a business owner, you need to be in control of your company's information. Never let employees use personal accounts for work.

Sometimes, leaks are less technical. We all know someone who carries around a little notebook of passwords, or even has a sticky note right on their computer with their password on it! Be sure that all sensitive paper records are locked away and use a shredder to dispose of sensitive documents.

## Security Mistake #10: Relying on "Silver Bullets"

Cyber security is a complex and ever-changing field. New attacks (and defenses) emerge every single day. It can be easy to fall into the trap of thinking that because you've purchased anti-virus software or a firewall, you are safe forever. This couldn't be further from the truth. Strong security demands a layered, comprehensive approach.

Stay vigilant, and stay in touch with a trusted cyber security professional.

## Something FREE for You

Green Mountain IT Solutions is offering a free computer and network security checkup for local Vermont businesses. It's completely free, and there are no strings attached. There's no pushy sales pitch. We'll give you a free report that's yours to keep whether you hire us or not. And if you feel like we wasted your time, we'll even give you $100 to make it up to you!

To book your cybersecurity checkup, call 802-489-6948 or email info@greenmtnit.com.