The Top 10 Ways Hackers Get Around Your Firewall And Anti-Virus To Rob You Blind

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit." Don't be their next victim! This report reveals the most common ways that hackers get in and how to protect yourself today.

Provided By:
Joseph Martin
President & CEO
Carolina IT Group
(252) 227-0491
www.carolinaitg.com

Are You A Sitting Duck?

You, the CEO of a small business, are under attack. Right now, extremely dangerous and well-funded cybercrime rings in China, Russia and the Ukraine are using sophisticated software systems to hack into thousands of small businesses like yours to steal credit cards, client information, and swindle money directly out of your bank account. Some are even being funded by their own government to attack American businesses.

Don't think you're in danger because you're "small" and not a big target like a J.P. Morgan or Home Depot? Think again. 82,000 NEW malware threats are being released every single day and HALF of the cyber-attacks occurring are aimed at small businesses; you just don't hear about it because it's kept quiet for fear of attracting bad PR, lawsuits, data-breach fines and out of sheer embarrassment.

In fact, the National Cyber Security Alliance reports that one in five small businesses have been victims of cybercrime in the last year – and that number is growing rapidly as more businesses utilize cloud computing, mobile devices and store more information online. You can't turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity. **Because of all of this, it's critical that you protect your business from these top 10 ways that hackers get into your systems.**

1. **They Take Advantage Of Poorly Trained Employees.** The #1 vulnerability for business networks are the employees using them. It's extremely common for an employee to infect an entire network by opening and clicking a phishing e-mail (that's an e-mail cleverly designed to look like a legitimate e-mail from a web site or vendor you trust). If they don't know how to spot infected e-mails or online scams, they could compromise your entire network.

2. **They Exploit Device Usage Outside Of Company Business.** You must maintain an Acceptable Use Policy that outlines how employees are permitted to use company-owned PCs, devices, software, Internet access and e-mail. We strongly recommend putting a policy in place that limits the web sites employees can access with work devices and Internet connectivity. Further, you have to enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what web sites your employee's access and what they do online during company hours and with company-owned devices, giving certain users more "freedom" than others.

Having this type of policy is particularly important if your employees are using their own personal devices to access company e-mail and data.

If that employee is checking unregulated, personal e-mail on their own laptop that infects that laptop, it can be a gateway for a hacker to enter YOUR network. If that employee leaves, are you allowed to erase company data from their phone? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos, texts, etc. – to ensure YOUR clients' information isn't compromised?

Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured; but that doesn't mean an employee might not innocently "take work home." If it's a company-owned device, you need to detail what an employee can or cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

3. **They Take Advantage Of WEAK Password Policies.** Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. Again, this can be ENFORCED by your network administrator so employees don't get lazy and choose easy-to-guess passwords, putting your organization at risk.

4. **They Attack Networks That Are Not Properly Patched With The Latest Security Updates.** New vulnerabilities are frequently found in common software programs you are using, such as Microsoft Office; therefore it's critical you patch and update your systems frequently. If you're under a managed IT plan, this can all be automated for you so you don't have to worry about missing an important update.

5. **They Attack Networks With No Backups Or Simple Single Location Backups.** Simply having a solid, reliable backup can foil some of the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be AUTOMATED and monitored; the

worst time to test your backup is when you desperately need it to work!

6. **They Exploit Networks With Employee Installed Software.** One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games or other "innocent"-looking apps. This can largely be prevented with a good firewall and employee training and monitoring.

7. **They Attack Inadequate Firewalls.** A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. But all firewalls need monitoring and maintenance, just like all devices on your network. This too should be done by your IT person or company as part of their regular, routine maintenance.

8. **They Attack Your Devices When You're Off The Office Network.** It's not uncommon for hackers to set up fake clones of public WiFi access points to try and get you to connect to THEIR WiFi over the legitimate, safe public one being made available to you. Before connecting, check with an employee of the store or location to verify the name of the WiFi they are providing. Next, NEVER access financial, medical or other sensitive data while on public WiFi. Also, don't shop online and enter your credit card information unless you're absolutely certain the connection point you're on is safe and secure.

9. **They Use Phishing E-mails To Fool You Into Thinking That You're Visiting A Legitimate Web Site.** A phishing e-mail is a bogus e-mail that is carefully designed to look like a legitimate request (or attached file) from a site you trust in an effort to get you to willingly give up your login information to a particular web site or to click and download a virus.

   Often these e-mails look 100% legitimate and show up in the form of a PDF (scanned document) or a UPS or FedEx tracking number, bank letter, Facebook alert, bank notification, etc. That's what makes these so dangerous – they LOOK exactly like a legitimate e-mail.

10. **They Use Social Engineering And Pretend To Be You.** This is a basic 21st-century tactic. Hackers pretend to be you to reset your passwords. In 2009, social engineers posed as Coca-Cola's CEO, persuading an exec to open an e-mail with software that infiltrated the network. In another scenario, hackers pretended to be a popular online blogger and got Apple to reset the author's iCloud password.

Want Help Ensuring That Your Company Has All 10 Of These Holes Plugged?

If you are concerned about employees and the dangers of cybercriminals gaining access to your network, then call us about how we can implement a managed security plan for your business.

At no cost or obligation, we'll send one of our security consultants and a senior, certified technician to your office to conduct a free **Cyber Security Audit** of your company's overall network health to review and validate different data-loss and security loopholes, including small-print weasel clauses used by all third-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs. At the end of this free audit, you'll know:

- Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?

- Is your data backup TRULY backing up ALL the important files and data you would never want to lose – and (more importantly) how FAST could you get your IT systems back online if hit with ransomware? We'll reveal exactly how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).

Are your employees freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check personal e-mail and social media sites? You know some of this is going on right now, but do you know to what extent? Are they downloading illegal files (music and video) and exposing you, as happened with LabMD?

- Are you accidentally violating any PCI, HIPAA or other data-privacy laws? New laws are being put in place frequently, and it's easy to violate one without even being aware; however, you'd still have to suffer the bad PR and fines if a breach happens and the investigation reveals YOU didn't take necessary precautions – and ignorance is not an acceptable excuse that will get you out of a lawsuit.

- Is your firewall and antivirus configured properly and up-to-date? No security device is "set and forget." It needs to be constantly monitored and updated – is yours? Is your IT Company giving you the assurances that it is?

- Are your employees storing confidential and important information on unprotected cloud apps like Google Drive or Dropbox that are OUTSIDE of your backup? Could they walk off the job with a list of all your clients and go work for a competitor?

I know it's natural to want to think, "We've got it covered." **Yet I can practically guarantee my team will find one or more ways your business is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the many businesses we've audited over the years.**

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a third party to validate nothing was overlooked. I have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, I'll report it to you.

You Are Under No Obligation To Do Or Buy Anything

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our **Free Cyber Security Audit**. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson, because I don't appreciate heavy sales pressure any more than you do.

Whether or not we're a right fit for you remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to give this free service to you.

You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, your reputation and your data are protected. Call us at (252) 227-0491 or you can e-mail me personally at joseph@carolinaitg.com.

Dedicated to serving you,

Joseph Martin

How To Request Your FREE Cyber Security Audit:

You can visit our website and complete the request form at:
https://carolinaitg.com/cyber-audit - or call us at (252) 227-0491.

Here's What A Few Of Our Clients Have Said:

Dr. Brian Kean
President of The
Robert Taylor Group

We have been using Carolina IT Group for over 10 years. Prior to using them, we used various local computer companies and other people. They managed to get the job done and our systems working, but we were always oblivious when it came to maintenance care and monitoring. The inconsistencies in their service slowed down our production and reflected upon us negatively due to long wait times for service. This, in turn left us without the tools needed to properly care for our patients.

We rest easier at nights knowing that all of our important and private patient information is safe, secure and there is someone on the other end monitoring and ready to act if ever needed. The implementation of our new office server took us light years ahead of the competition and has increased our ability to service a great number of patients daily. With peace of mind and confidence that our systems are working appropriately, we can put our focus on our main priority of patient care.

He has assisted us with so many aspects of the business. From computer repair, to software advice and installs, we are never let down. I always enjoy their knowledgeable team visiting and talking with them over the phone. They are always willing to go the extra mile and explain the process of things as well as teach me and our staff ways to help avoid issues in the future. That alone is priceless.

All our issues seem to take high priority with Carolina IT Group. While I know they have several high-profile customers, they always take our concern seriously and immediately respond. We could not have a better or more dependable company to work with for all our IT needs.

Carolina IT Group has given us confidence in our systems. With the ever-changing world of computers, it is refreshing to know that an answer is only a phone call away.

I would tell people, and I have told them, that there is no other company to call in Eastern NC but Carolina IT Group. I believe that a good company stands behind its product, treats others with respect, does as it says it's going to, and does not take advantage financially of

those that may not know better, Carolina IT Group is certainly a wonderful representation of all those qualities and more.

The Robert Taylor Group

"Good folks that do a great job for a fair price"

Ken Lang
President of The Robert Taylor Group

I have been using Carolina IT Group for several years. The company we used before was very spotty but now that we use Carolina IT Group our service is very good.

Whenever we have an issue it is very easy to get up with them to handle our problem and they handle it on a very timely bases. They are **very helpful about suggesting new ideas** to help us out. They are good folks that do a great job for a fair price.

ACF Insurance Services, Inc.

"They are so nice to deal with, so it is a no brainer for us"

Matt Alala
President of ACF Insurance Services, Inc.
www.acfinsurance.com

I have been using Carolina IT Group for 4 years. The provider we had before was good, but now that we use Carolina IT Group it's even better than before! Whenever we have any issues or emergencies it is very easy to get assistance and the issues get resolved very quickly. I am very glad I switched too!

Carolina IT Group helps us stay up with technology and changes so that we have secure and reliable systems. They are so nice to deal with, so it is a no brainer for us as to why we chose them. Plus, **I would refer my best friend in a second** to use Carolina IT Group.

The Appraisal Advantage

"Switching to Carolina IT Group was one of the best business decisions"

Ashley Barker
Owner of The Appraisal Advantage

We have been using Carolina IT Group for 10+ years. The service from other IT companies was erratic and undependable at best. However, **now our service is quick, reliable, and personable.** Whenever I have an IT issue, help is just a phone call away. All of my IT issues get resolved quickly, which is very important to minimize my office downtime.

Switching to Carolina IT Group was one of the best business decisions that I have made. They give me the peace of mind in knowing that if I do have an IT issue, it will be resolved within a very short period of time and my office will be back up and running.

I have recommended Carolina IT Group to several of my friends for their businesses and will continue to do so!