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

2022

Cybercrime Report

THE PROBLEM

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses, considering them "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.

WHO WE ARE

Holly Fullingim
CEO

Quick Compute

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 Ukraine are using sophisticated software systems to hack into thousands of small businesses like 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 through online news articles without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity. **Because of all this, it's critical that you protect your business from these 10 ways that hackers get into your systems.**

1. **They Take Advantage Of Poorly Trained Employees.**
   The # 1 vulnerability for business networks is 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 email cleverly designed to look like a legitimate e-mail from a website 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 websites employees can access with work devices and Internet connectivity. Further, you must enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what websites your employees 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 personal devices to access company e-mail and data. If that employee is checking unregulated, personal e-mail on a personal 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 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, 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 Wi-Fi access points to try and get you to connect to THEIR Wi-Fi 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 Wi-Fi they are providing. Next, NEVER access financial, medical, or other sensitive data while on public Wi-Fi. Also, don't shop online and enter your credit card information unless you're certain the connection 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, trying to get you to willingly give up your login information to a particular website or to click and download a virus.

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 Security And Backup Review of your company's overall network health to review and validate many different data-loss and security loopholes, including small-print weasel clauses used by all 3rd-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 review, 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? We'll also 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 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.

Are your firewall and antivirus configured properly and up to date?
Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup?

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 hundreds of businesses we've assessed 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 3rd 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 Security And Backup Assessment. I will give you a 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 956-428-7777 or you can e-mail me personally at holly@quickcompute.com

Dedicated to serving you,

Holly Fullingim
CEO, Quick Compute, Inc.
HIPAA Certified Privacy and Security Expert
(956)428-7777 holly@quickcompute.com

Please continue reading to hear what a few of our clients have to say about us.

We Fell Victim to CryptoWall – 100% Recovery Success

"Our organization was one of the unlucky ones who fell victim to a CryptoWall attack within 2 months of its first release. Fortunately for us, we have excellent IT Support in Quick Compute and we weren't the first in the Rio Grande Valley that had experienced issues of files that were reported as corrupt. As soon as we contacted Quick Compute they knew right away what was wrong and jumped into action to block and stop further spreading of the encryption of our files. Because of the excellent planning and maintenance of our IT systems, our backup was totally up-to-date, and all of our affected files were fully recoverable within a couple of hours.

Since that time Quick Compute implemented their Cybersecurity Plus Plan and helped us to provide better and safer internet and email usage across our organization. To date, we have not had any further issues with Ransomware attacks or any other virus or malware attacks. We have the peace of mind knowing that our full IT protection is modern and up-to-date."

Jesus A. Sanchez
Executive Director
Children's Advocacy Center of Hidalgo & Starr Counties, Inc.

"We Have So Few Problems Now Because Our Systems Are Being Maintained And Monitored Daily."

"Our companies transitioned from being part of a very sophisticated corporate network system to a standalone system for just our companies. After extensive planning for the switchover by Quick Compute and our staff, the migration went exactly as planned, on time, and on budget with minimal business interruption. We were so surprised to have such a seamless transition! We now have an information and data system that will rival any corporate system at a greatly reduced price.

The monitoring that is being done is behind the scenes, so we really don't feel it, nor do we have issues with virus or time outs, etc. I believe that we have so few problems because our systems are being maintained and monitored daily.

Price was not the most important factor for us in choosing our IT Service Company. We wanted to have access to a team that would be quick to answer calls and respond to problems. The continuous service and the quick response when we have experienced problems has been very important to us. We appreciate how they've been handled thoroughly and quickly."

Judy Quisenberry
Executive Director
Valley Baptist Legacy Foundation