The Top 10 Ways

Hackers Get Around Your Firewall and Antivirus To Rob You Blind

onestep
Secure IT Services

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.

Are You A Sitting Duck?

You, YES YOU, 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 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 not as big of a target as a J.P. Morgan or Home Depot? Think again. 82,000 NEW malware threats are being released every single day and HALF of the cyberattacks occurring are aimed at small to mid-sized businesses; you just don't hear about it because it's kept quiet for fear of attracting bad PR, lawsuits, data-breach fines and 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 this, it's critical that you protect your business from these **TOP 10 WAYS** that hackers get into your systems.

With locations in LA, Phoenix, NY, & Boston, we've got you covered.

By One Step Secure IT Services
Stop by www.onestepsecureit.com
Call us at (866) 617-8181
Say "HELLO" at hello@onestepsecureit.com

onestep
Secure IT Services

THE TOP 10 WAYS

Hackers Get Around Your Firewall & Antivirus To Rob You Blind

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 email (that's an email cleverly designed to look like a legitimate email from a website or vendor you trust). If they don't know how to spot infected emails 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 email. We strongly recommend putting a policy in place that limits the websites employees can access with work devices and Internet connectivity. Further, you have to enforce your policy with strict access configurations throughout your network. One Step Secure IT 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 their own personal devices to access company email and data.

If that employee is checking unregulated, personal email that infects their 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. You need to detail what an employee can or cannot do with that device, including circumventing security mechanisms you put in place.

3. They Take Advantage Of WEAK Password Policies. Passwords should be long, complex, and hard to guess. Any electronic device should require a password/code for entry to prevent that device from being compromised. Additionally, passwords should be regularly changed and never shared. These and other password best practices should be required as an integral part of your security efforts so employees don't put 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, 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 worse, intentionally!) deleting or overwriting files, natural disasters, hardware failures and a host of other data-erasing disasters. Again, your backups should be automated, tested, and monitored with a certain amount of retention built in. 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 an IT professional like One Step Secure IT as part of their regular, routine maintenance.

8. They Use Phishing Emails To Fool You Into Thinking That You're Visiting A Legitimate Website. A phishing email is a bogus email 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.

9. 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.

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 email 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.

"We've Got It Covered."

It's natural to think, "we've got it covered," when sadly, too many businesses are at serious risk for hacker attacks, data loss, and extended downtime. You've spent your entire career working hard to get where you are, earning 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.

Here are a list of questions to consider:

- 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? How long would it 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 unapproved sites, to look for other jobs and waste time shopping, or to check personal email and social media sites? You know some of this is going on right now, but do you know to what extent and how these actions put your company at risk?
- Are you accidentally violating any PCI, HIPAA or other data-privacy laws? New laws are put in place frequently and it's easy to violate one without even being aware; unfortunately, you'd still have to suffer the bad PR and fines.
- Is your firewall and antivirus configured properly and up-to-date?
- Have you changed all default passwords and regularly change passwords every 90 days?
- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup?

Need Help Ensuring That Your Company Has All 10 Of These Security Gaps Filled?

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

At no cost or obligation, we'll have one of our Security Consultants and a Senior Certified Technician conduct a **FREE IT Systems Security and Performance Assessment** of your

company's overall network health to review and validate a wide variety of different data-loss and security loopholes. We'll also look for common places where security and backups get overlooked, such as mobile devices, laptops, tablets and home PCs.

As previously stated above, it's natural to believe, "we've got it covered." Yet, I can almost guarantee we 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 businesses we have audited over the past 35 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 that 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, we'll report it to you.

You Are Under No Obligation To Do Or Buy Anything

Let's get this out of the way first. I want to be very clear that there are no expectations for you to do or buy anything if you choose to redeem our **Free IT Systems Security and Performance Assessment**. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy 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 will welcome the opportunity. But if not, we're still more than happy to give this free service to you.

Protect your business, your reputation, and your data.

Call us at **866-617-8181** for a quick **10 Minute Call** to talk about your business
or you can email me personally at **cheryl @onestepsecureit.com**.

Dedicated to serving you,

Cheryl Blasnek
VP of One Step Secure IT Services

Website: www.onestepsecureit.com
Email: cheryl@onestepsecureit.com

About One Step Secure IT

Our mission is to keep your business secure in an increasingly unsecure world. After 35 years, we know how to make technology work for your business, not against it. As technology continues to evolve, so do the threats to your business. Together, we'll work to eliminate vulnerabilities and protect your network from cyber attacks, data loss, and extended downtime.

We hope you enjoyed this report. If you would like to schedule a quick **10 minute call** to tell us about your IT challenges, please visit us **HERE.**

> "I would recommend One Step Secure IT to anyone that is looking to fix their IT infrastructure. I can't thank their team enough for all they have done for us at the marina."

Ken Runnels
Chief Administrator of Antelope Point Marina

onestep
Secure IT Services