The **Top 10** Ways Hackers Bypass Your Firewall, Dismantle Your Anti-Virus, and *Rob You Blind*

Cybercrime is at an all-time high, and hackers set their sights on small and medium businesses that 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: Choose Networks, Inc.
Author: Chris Hoose, President & CEO
1300 E Central Ave, Wichita, Kansas 67214
[www.chosennetworks.com](http://www.chosennetworks.com)
316-928-8810
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 thousands of small businesses like yours. They’re stealing your credit cards, client information and money directly out of your bank account. Some are even funded by their own government to attack American businesses.

Do you think you’re not 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 these cyber-attacks are aimed at small businesses—you just don’t hear about it. They’re kept quiet in fear of 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.

1. **They Take Advantage Of Poorly Trained Employees.** The #1 vulnerability for business networks is the employees that use them. It’s extremely common for an employee to infect an entire network by opening a phishing e-mail—an e-mail 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 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 regulate the web sites your employees access, 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 an employee checks unregulated, personal e-mail on 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 and financial information—you may not be legally permitted to allow employees to access it on unsecure devices; 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 in preventing a stolen device from being compromised. Your network administrator can ENFORCE this 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. 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.** 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. 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.** Cybercriminals access networks by duping unsuspecting users to willfully download malicious software. They do this by embedding it within downloadable files, games or other “innocent”-looking apps. This can 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 firewalls need monitoring and maintenance, just like all devices on your network. Your IT person should do this as part of their regular, routine maintenance.

8. **They Attack Your Devices When You’re Off The Office Network.** Hackers set up fake WiFi access points to trick you into connecting to THEIR WiFi over the safe public one that’s available to you. Before connecting, check with an employee of the store or location to verify the WiFi they are providing. Next, NEVER access financial, medical or other sensitive data while on public WiFi. Don’t shop online and enter your credit card information unless you’re certain the connection point is safe and secure.

9. **They Use Phishing E-mails To Fool You Into Thinking 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. They aim to get you to willingly give up your login information to a particular web site or to click and download a virus.

   These e-mails often 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 accessing to your network, call us to learn 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 Audit of your company’s overall network health. We’ll review and validate 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 audit, you’ll know:

- Is your network really secured against the most devious cybercriminals? And if not, what do you need to do 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 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.

- Is your firewall and antivirus configured properly and up-to-date?
• Are your employees storing confidential and important information on unprotected cloud apps 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 see it all too often in the businesses we’ve audited over the years.

Even if you do have a trusted IT person or company in place, it never hurts to get a 3rd party validation 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, 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 for you to do or buy anything when you take us up on our [Free Security And Backup 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 that your business, reputation and data are protected. Call us at 316-928-8810 or you can e-mail me personally at choose@choosenetworks.com.

Dedicated to serving you,

Chris Hoose
Web: www.choosenetworks.com
E-mail: choose@choosenetworks.com
Here’s what a few of our clients have said:

Choose Networks Fixed Our Problem Remotely In 15 Minutes!
“Choose Networks is always quick to respond to our technical emergencies. We recently lost all connection to our e-mail services on a busy Saturday morning. After connecting with an on-call team member, they remotely got into our system, and had us running again within 15 minutes of our original call. It’s comforting to know we have a technology partner that will keep us going!” — Allison Walden, Office Manager at Downing and Lahey Mortuaries

Choose Networks Is An Affordable IT Company
“Our company is now dependent on an IT company that we can afford. Our managers are able to spend more time on business, instead of wasting time trying to solve problems in an area that we are not experts in. This allows us to provide better member service, and not have to deal with IT disruptions.” — Gary Torres, President at EquiShare Credit Union

Choose Networks Provides Stability, Security and Room To Grow!
The staff and technicians at Choose Networks are great! Whether it’s an order, repair or crisis situation, they are always there to help and continuously prove to do so in a timely—and very knowledgeable—manner. They successfully rebuilt our infrastructure from the ground up, providing our company with more stability, security and room to grow.” — Paula Cheatum, IT Administrator at South Central Mental Health Counseling Center

Choose Networks Sends Above-and-Beyond Support!
“Choose Networks always sends a technician that goes above and beyond. One of our calls to Choose was in reference to a non-functioning printer. Jake provided a diagnosis of the problem and advised us on all options to consider before making a recommendation. Without his help, we would have spent countless hours researching and seeking a solution. Thanks for the stand out service, Jake!” — Julie Oetting, Assistant Manager at Valley Floral Company