



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: Professional Computer Management Inc.
Author: Ed VanderLaan
220-1100 South Service Rd.
Stoney Creek, ON L8E 0C5
289-656-1100
www.pcm.ca

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 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 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 **Security And Backup Audit** of your company's overall network health to review and validate as many as 27 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 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? 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, PIPEDA 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.
- Is 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 50 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 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 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 289-656-1100 or you can e-mail me personally at evanderlaan@pcm.ca.

Dedicated to serving you,

Ed VanderLaan

Web: www.pcm.ca

E-mail: evanderlaan@pcm.ca

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

Save Time And Money While Gaining Peace Of Mind



Susan McLeod
Operations
Administrator
Allied Track
Services
Grimsby

Security has become an increasing problem in today's world. It is very hard to keep ahead of all the hackers, scammers, etc. that are out to destroy companies and people. **Putting the proper security measures in place is very important** to stop these attempts. Better to be safe than sorry is a very true comment here.

Professional Computer Management **saves us time, effort, and money**, and they give us the **comfort and peace of mind** that we can come into work and our system will not have problems because we know everything is in place that should be there (i.e. Security, Backups, Computer/Server Monitoring, Remote Access, etc.).

PCM is very reliable, knowledgeable, and not as expensive as some of the IT companies that are currently out there. We are definitely getting great service for our money!

I recommend PCM to any company who values their technology and security needs.

Save On IT Staff And Gain Better Security



Joel DeGroat
Managing Director
ServiceMaster of
Canada Limited
Mississauga

Using Professional Computer Management provides the expertise necessary to not only **eliminate an IT person on staff** but has also provided **fantastic executive reports that prove all the services are working** right down to the number of help desk calls and time to resolve the issues. Our company is not the cheapest in the market, so we appreciate that great quality, service and knowledge comes at a premium.

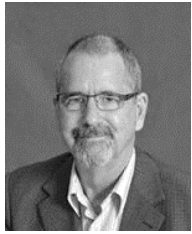
Security monitoring is critical to us, like insurance, it is something you buy hoping you never have to use it. Should a breach ever occur not only is your internal information at risk but so is the information of your customers. For us it is not just the question of how much it would cost to start up from scratch, but what if there is a ransom involved or worse if the data is destroyed.

Another serious consideration is if customer or employee information is exposed, now we would have bad press and lawsuits where **we would not be able to stand in front of a judge and claim that we did our due diligence and were responsible with our data.** This would be extremely expensive.

Lastly some of our larger commercial and institutional customers are demanding that we do it or we would lose them as customers.

Having PCM as part of our organization **gives us the resources we need** to ensure all aspects of technology are properly maintained, and industry best practices are reviewed in the ever changing technology field.

Highly Responsive Team That Cares About Our Mission



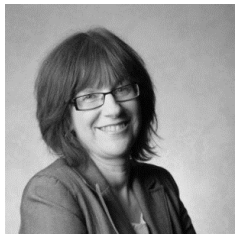
Wayne de Jong
CFO/Director of
Finance
Mission Services of
Hamilton

Professional Computer Management has been taking care of our technology needs for over 11 years. The cost of their Sentinel Managed IT Service is **extremely reasonable**, given the **high quality of detailed support**. For us this is far cheaper, and much less stressful, than doing IT in-house. PCM's rock-solid support and risk-free business continuity services continue to serve our needs well. **The team is very responsive and highly dedicated**, even available 24/7 if needed.

We continue to benefit from their **constant monitoring of network health** and detailed monthly reports. All our locations have the servers being backed up on an hourly basis with daily off-site copies. We also value how **highly responsive the team** is at all times, and how they are able to come **on-site in a flash** whenever necessary.

Having the PCM team as part of our organization allows us to focus on our mission while ensuring that our **donor and client data is properly protected**. We also appreciate the regular reviews and recommendations to keep up with industry best practices and our evolving technology needs.

A Reliable, Quality Team That Keeps Us Safe



Randi Glass
Executive Director
Canadian Defence
Lawyers
Toronto

I'm a firm believer in "you get what you pay for". Professional Computer Management is not the cheapest in town, but **their reliability and quality of their team makes that extra expense worthwhile**. We would rather pay more and have any **problems solved quickly and professionally**. The risk of potential IT "down time" is much more costly than the marginally greater monthly retainer fee we pay to PCM.

Cyberhealth is so very important now and having an expert team maintaining all technology is critical. We also carry a cyber insurance policy and have for several years. Scams, viruses, ransomware, etc. are all getting so sophisticated that even the savviest employees could be fooled and risk the whole network. PCM's regular monitoring and continuous backup provide the **comfort level we need to focus on our jobs**, and not worry about breaches to our database, financial management and internal files.