



The Top 10 Ways Hackers Get Around Your Firewall and Anti-Virus to Rob You Blind

Don't be their next victim! This report reveals the most common ways that hackers get in and how to protect yourself today.



James Moore
Technology Solutions Consultants

*Technology Solutions That Allow Business Owners
MOORE Time to Focus on Running Their Business.*



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 card and client information and get 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 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 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 online information storage. You can't turn on the TV or read a newspaper without learning about the latest 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 the top 10 ways that hackers get into your systems.**

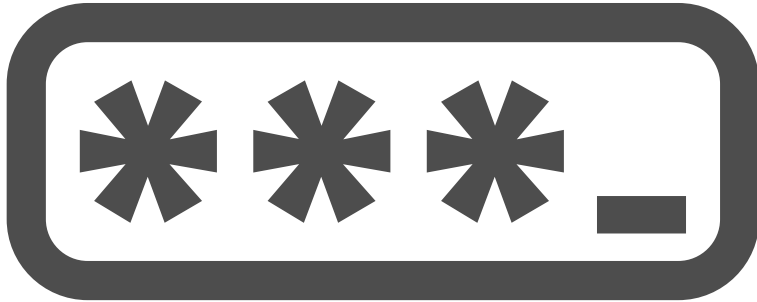
1.

They exploit device usage outside of company business. You must maintain an acceptable use policy (AUP) 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 content-filtering software and firewalls. We can set up permissions and rules that will regulate the websites your employees access and their online activity during company hours and with company-owned devices (allowing certain users more liberties with this use if desired).

An AUP is particularly important if your employees are using personal devices to access company email and data. If an employee's laptop is compromised by a virus or malware when checking personal email or visiting websites, that laptop becomes a gateway for a hacker to enter YOUR network. Your AUP must address the use of employee-owned laptops for company work. Additionally, if an employee's phone is lost or stolen, your clients' information falls into the hands of strangers. Your AUP should have provisions allowing you to remotely wipe the phone – which would also delete all of that employee's photos, videos, texts, etc. – to ensure your clients' information isn't compromised. It should also give you the ability to erase work data from the personal devices of employees who leave your company.

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.

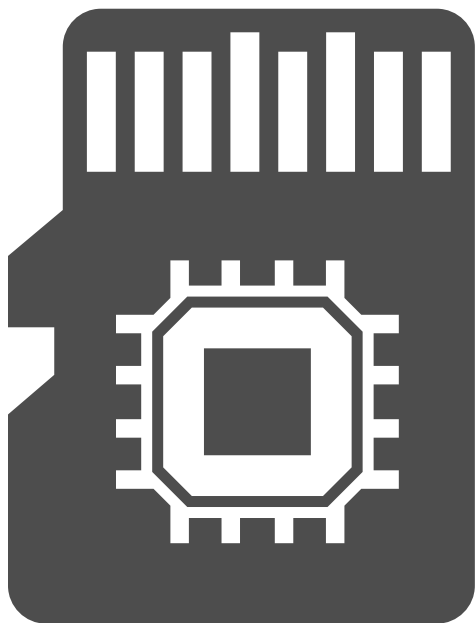




- 2.** **They take advantage of weak password policies.** Passwords should be at least eight characters and contain lowercase and uppercase letters, symbols and at least one number. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. Again, this can be enforced by your network administrator so employees don't get lazy and choose easy-to-guess passwords that put your organization at risk.

- 3.** **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. So it's critical that you patch and update your systems frequently. If you're under a James Moore ProActive Services plan, we take care of this for you – so you don't have to worry about missing an important update.



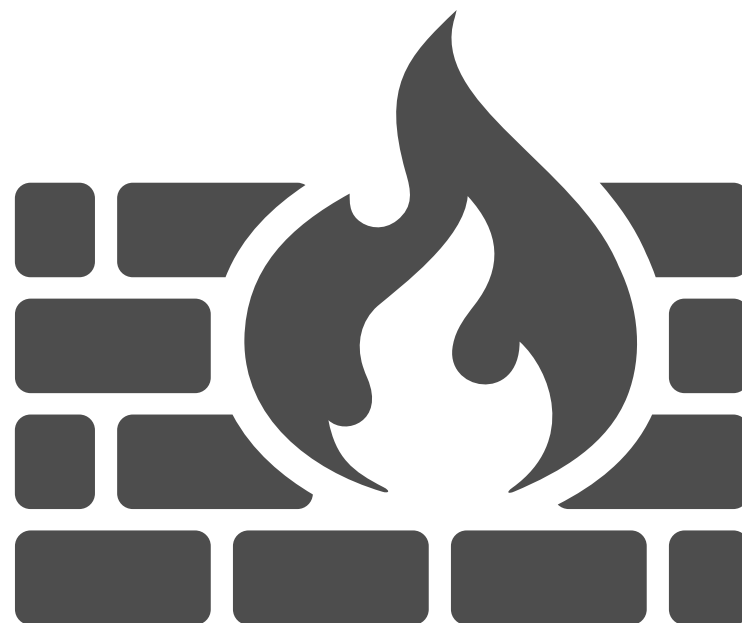


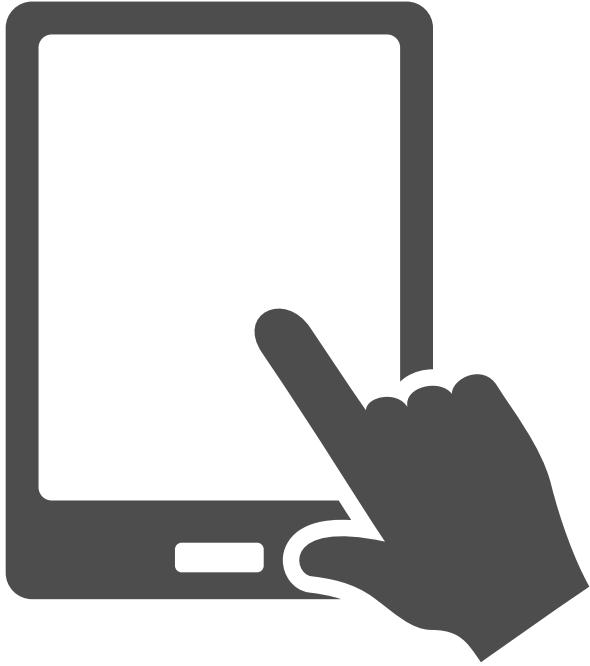
4.

They attack networks with no backups or simple single location backups. Just having a solid, reliable backup can foil some of the new and most aggressive ransomware attacks (in which 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 events. Again, your backups should be AUTOMATED, monitored and tested regularly; the worst time to test your backup is when you desperately need it to work!

5.

They exploit networks where employees can install 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, computer security policies and employee training.





6.

They attack inadequate or unmanaged firewalls. A firewall acts as the front line of defense against hackers by blocking everything you haven't specifically allowed to enter (or leave) your computer network. Firewalls can be basic filters or they can have advanced technologies built in that provide exceptional protections from diverse threats. 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 routine maintenance (and is included as part of James Moore's ProActive Services plan).

7.

They attack your devices when you're off the office network. It's not uncommon for hackers to set up clones of public Wi-Fi access points to get you to use their Wi-Fi instead of the legitimate, safe public one 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 absolutely certain the connection point you're on is safe and secure. Many cell phone carriers allow you to enable a Wi-Fi hotspot from your mobile device. If you must shop online or access sensitive information, use your own hotspot to do it.





8.

They use phishing emails to fool you into thinking that you're visiting a legitimate website. 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 website or to click and download a virus. Please take a minute and review our whitepaper on Cyber Security and Identity theft located at:

<http://www.jmco.com/media/Identity-Theft.pdf>


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

9.

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 and persuaded an executive to open an email with software that infiltrated the company's network. In another scenario, hackers pretended to be a popular online blogger and got Apple to reset the author's iCloud password.

10.

They take advantage of poorly trained employees. The #1 vulnerability of business networks is the employees using them. It's extremely common for an employee to infect an entire network by opening and clicking links or attachments from a phishing email or a nefarious website. If they don't know how to spot infected e-mails or online scams, they could compromise your company's entire network.



Cybercrime is at an all-time high,
and hackers are setting their sights
on small and medium businesses.
Don't be their next victim!

At James Moore, we understand and
are here to help. As your trusted
business advisor, we can assist
with all of your technology needs,
including firewall and anti-virus
protection. Contact us today at 800-
455-5676 to see how our technical
staff can help you.