Cybercrime is at an all-time high. Hackers have set their sights on small and medium sized businesses. Don’t be their next victim! This report reveals the most common ways that hackers get in and how to protect yourself today.
Cybercrime is at an all-time high. Hackers have set their sights on small and medium sized businesses. 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: Acutech Network Services
Authors: Patrick Sullivan & Tristen Cooper
2328 North Batavia Street
Suite 114
Orange, CA 92865
www.acutech.net
(714) 279-3901
Are You A Sitting Duck?

**You, the CEO of a small business, are under attack.** Right now, dangerous, well-funded cyber crime rings in China, Russia, Iran, and North Korea are using sophisticated software and techniques to hack thousands of small businesses like yours. They steal credit cards, client information, intellectual property, and even money directly out of bank accounts. Some governments even funded these groups 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, on average, over 356,000\(^1\) NEW malware threats were released every single day in 2016 and over HALF of the cyber-attacks occurring are aimed at small businesses; hackers and cyber criminals rely on businesses’ fear of attracting bad PR, lawsuits, data breach fines, and sheer embarrassment to keep them from reporting incidents.

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 businesses utilize aging software, increase their use of mobile devices, and store more information online. The media consistently reports on the latest online data breach, government fines, and regulatory agencies, and the reports are growing in number and severity. **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.** A businesses’ employees pose the greatest threat to its network. Hackers most commonly enter a network by tricking employees into opening attachments in phishing e-mails (e-mails cleverly designed to look like a legitimate e-mail from a website or vendor you trust). If employees don’t know how to spot infected e-mails or online scams, they run a greater risk of compromising your entire network.

2. **They Exploit Devices Used Outside of Company Business.** Hackers exploit companies who fail to implement and enforce Acceptable Use Policies. Acceptable Use Policies outline how employees are permitted to use company-owned PCs, devices, software, Internet access, and e-mail. We strongly recommend implementing a policy that limits the websites employees can access with company devices and networks.

   Further, you have to enforce your policy with content-filtering software and business-class firewalls. We can set up rules that regulate what websites employees access during company hours and with company-owned devices, giving certain users more “freedom” than others if needed.

   If the data in your organization is highly sensitive, such as patient records, credit card

---

1 According to statistics provided by the AV-Test, an independent IT-Security Institute.  https://www.av-test.org/en/statistics/malware/
information, financial information and the like, the law may bar employees from access company data on insecure devices or networks. An Acceptable Use Policy clearly details detail what an employee can or cannot do with company devices, including “rooting” or “jailbreaking” the device to circumvent security mechanisms.

If employees use their own personal devices to access company e-mail and data, your company requires a more robust policy. If hackers infect an employee’s personal laptop or phone through their unregulated, personal e-mail, the device can acts as a gateway for hackers to enter YOUR network. If that employee leaves, are you allowed to erase company data from their device? If their device is lost or stolen, are you permitted to remotely wipe it – which would delete all of that employee’s photos, videos, texts, etc. – to ensure YOUR clients’ information isn’t compromised?

3. **They Take Advantage of WEAK Password Policies.** Password policies help to strengthen perimeter security by building in complexity and variation. Passwords should be at least eight characters and contain lowercase and uppercase letters, symbols, numbers, and be required to change specific intervals. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. You should systematically ENFORCE your Password policy to keep employees from putting your organization at risk by forgetting or choosing easy-to-guess passwords.

4. **They Attack Unpatched Networks and Devices.** The vulnerabilities found by the hacker, security, and software communities in everyday software pose an ever-evolving threat to your network. Patching software like Java, Microsoft Windows and Office, Adobe Acrobat, and others offers the best option for mitigating this omnipresent threat. 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. **Their Attacks Devastate Networks with No Backups or Simple Single Location Backups.** Having a solid, reliable backup foils some of the latest, and most aggressive ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If you back up your files, you don’t have to pay the attacker to get them back. A good backup also protects 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, monitored, and tested; the worst time to test your backups is when you desperately need them to work!

6. **They Attack Inadequate Firewalls.** A firewall acts as the border defense against hackers, blocking everything you haven’t specifically allowed to enter (or leave) your computer network. While firewalls are great tools, they need monitoring and maintenance, just like all devices on your network. This too should be done by your IT team or company as part of their regular maintenance.

7. **They Attack Your Devices When You’re Outside the Office Network.** It’s not uncommon for hackers to set up clones of public WiFi access points to trick users into connect to THEIR
WiFi over the legitimate network 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. Similarly, don’t shop online or enter your credit card information unless you’re certain the network you’re on is safe and secure.

8. **They Use Phishing E-mails to Penetrate Your Defenses.** A phishing e-mail is a malicious e-mail, carefully designed to look like a legitimate request (or attached file) from a person or organization you trust to penetrate your network.

Often these e-mails look 100% legitimate and show up in the form of a PDF (scanned document), UPS or FedEx tracking number, bank letter, Facebook alert, bank notification, and so on. That’s what makes these so dangerous – they LOOK exactly like a legitimate e-mail.

By clicking the link or opening the attachment, the user inadvertently loads the hacker's malicious software on their computer. After the software silently installs, they can start exfiltrating YOUR data and intellectual property.

9. **They Use Social Engineering and Pretend to be You.** Hackers take advantage of people's good nature, and lack of vigilance to convince people they are someone else, including you. Hackers pretending to be you can do things like resetting your passwords, transfer money, and so on. In 2009, a hacker breached Coca-Cola’s network by pretending to be the CEO and persuading another exec to open an e-mail attachment with malicious software embedded inside. In another scenario, a hacker pretended to be a popular online blogger and convinced Apple to reset the author’s iCloud password.

10. **Their Attacks are Devastating Against Networks Without Up-to-Date Anti-virus.** Updated anti-virus, anti-malware, and anti-ransomware software help to notify users of the existence of attack software, often stopping it from running on their machine. Having a robust suite of anti-virus, anti-malware, and anti-ransomware software provides a second line defense against attacks that make it passed your users and firewall.

Want Help Ensuring That Your Company Has All 10 of These Holes Plugged?

If you are concerned about cyber security and the dangers of cybercriminals gaining access to your network, call us to discuss 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 30 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?

- Are your data backups 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 or porn sites, to look for other jobs, 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.

- 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?

It’s natural to think, “We’ve got it covered, we haven’t been hit yet.” With cyber-attacks on the rise, can you afford to rely on luck and the unknown? Taking advantage of a no-cost security assessment arms your business with knowledge of your security environment and potential weaknesses hackers might leverage to steal your data, intellectual property, and money, both by fraud and theft, and extended bills associated with downtime.

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 or out-of-date. We can provide you with a professional, timely, and accurate reporting of your cyber security defenses.

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 service to you for free.

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 714-279-3901 or you can e-mail me personally at psullivan@acutech.net.
Dedicated to serving you,

Patrick Sullivan
Web: www.acutech.net
E-mail: psullivan@acutech.net