



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.

ITSUPPORTLA

Provided by: IT Support LA
Author: Igor Pinchevskiy
6047 Tampa Ave, Suite 308
Tarzana, CA 91356

818-797-5300
www.itsupportla.com

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

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 7 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, 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?

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 hundreds 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 818-805-0909 or you can e-mail me personally at igorp@itsupportla.com

Dedicated to serving you,



Igor Pinchevskiy, CEO
IT Support LA

Web: www.itsupportla.com

E-mail: igorp@itsupportla.com

See What Other Los Angeles Business Owners Are Saying:



“I had some Network issues and I grew tired of having my IT guy coming and check any issue after a week of annoyance, and then having him nickel and dime me for anything he does. I was referred to IT Support LA by another colleague who told me only good things about them and they had this amazing offer of 2 hours free IT consultancy which I took and what I like the most was that they were listening to my issues and suggesting solutions that I actually

understood, using a language I actually understood and not that computer jargon some people are using.

They respond to all my issues within 60 minutes and solve all my issues same day and after they do, they even explain and educate me what I did wrong or what happened so that I will be aware of that issues next time. I appreciate all the help and expertise!” - **Alex Mirzaian**, *Epic Auto Leasing*



“IT Support LA will jump through any hoops to get you what you need and the service offered by IT Support LA is unmatched by any provider I’ve dealt with in the past. Using IT Support LA just once will have them doing whatever they can to beat prices, offer service and value to ensure they get your return business.” - **Marco Belmonte**, *Ria Financial*



“IT Support LA has helped me to lay down the IT foundations I needed for my growing business.

Now that my practice accelerates and we need to make sure everything is backed up and running well, their design at early stage really helped us transition to bigger and more complex infrastructure without us suffering from any lack of process or design flaws.

IT Support LA has been crucial to my growing business and I really don’t think I would be relaxed about growing my business if I didn’t have them and had to “figure out things” on the fly like others have to do. I truly cherish their expertise and everything they have done for my practice.” - **Matthew Kanin**, *Law Office of Matthew Kanin*



“In our line of work, we need to have very good data security and data backup to protect our clients’ data. Now that IT Support LA has set up my backup, I have complete peace of mind that it’s all safe and secure – and it’s great not having to worry about my clients’ data. I feel that it’s much better to have a total backup solution that you just don’t need to worry about.” – **Dr. Ogden Page**, *President, Ogden Page Accountancy Corp.*



“WOW! That is all I can say about Igor and the team at IT Support LA! It’s so nice to know that our entire network is handled so I have one less crisis to deal with in my already crazy-busy schedule. I’ve worked with a number of other computer consultants in the past and no one can touch their level of service or expertise.” – **Dianne Pesgado**, *Office Manager, ABR Inc.*



“I like being able to call for IT help and get a near-immediate response. Recently I arrived at my office to find that I was unable to access documents on the network server from my workstation. I was under a court deadline and needed immediate access to the documents. I called IT SUPPORT LA for help. Within 60 minutes I had a tech working on the problem. I don’t spend valuable (billable) time solving IT problems. Also, having IT SUPPORT LA do the IT work has provided invaluable continuity of the IT solutions used in my law firm. Thanks!” – **Edward W. Pilot**, *Edward Pilot Law A Professional Corporation.*



“Before hiring IT Support LA, our network would go down regularly, run slow, and even run into the occasional virus. Since signing up for their network maintenance plan, we haven’t had one single issue. I’m VERY glad we hired these guys to support our network.” – **Ella V. Realtor**

The Top 7 Reasons Why You'll Want To Outsource Your IT Support To Us:

1. **We Respond Within 5 Minutes Or Less.** The average amount of time it takes for one of our clients to get on the phone with a technician who can start working on resolving their problem is 3.5 minutes. We know you're busy and have made a sincere commitment to making sure your computer problems get fixed FAST. And since most repairs can be done remotely using our secure management tools, you don't have to wait around for a technician to show up.
2. **No Geek-Speak.** You deserve to get answers to your questions in PLAIN ENGLISH, not in confusing technical terms. Our technicians will also not talk down to you or make you feel stupid because you don't understand how all this "technology" works. That's our job!
3. **100% No-Small-Print Satisfaction Guarantee.** Quite simply, if you are not happy with our work, we'll do whatever it takes to make it right to YOUR standards without charging you for it. And if we can't make it right, the service is free.
4. **All Projects Are Completed On Time And On Budget.** When you hire us to complete a project for you, we won't nickel-and-dime you with unforeseen or unexpected charges or delays. We guarantee to deliver precisely what we promised to deliver, on time and on budget, with no excuses.
5. **Lower Costs, Waste And Complexity With Cloud Solutions.** By utilizing cloud computing and other advanced technologies, we can eliminate the cost, complexity and problems of managing your own in-house server while giving you more freedom, lowered costs, tighter security and instant disaster recovery.
6. **We Won't Hold You Hostage.** Many IT companies do NOT provide their clients with simple and easy-to-understand documentation that outlines key network resources, passwords, licenses, etc. By keeping that to themselves, IT companies hold their clients "hostage" to scare them away from hiring someone else. This is both unethical and unprofessional. As a client of ours, we'll provide you with full, written documentation of your network and all the resources, software licenses, passwords, hardware, etc., in simple terms so YOU can understand it. We keep our clients by delivering exceptional service — not by keeping them in the dark.
7. **Peace Of Mind.** Because we monitor all of our clients' networks 24/7/365, you never have to worry that a virus has spread, a hacker has broken in or a backup has failed to perform. We watch over your entire network, taking the management and hassle of maintaining it off your hands. This frees you to focus on your customers and running your business, not on your IT systems, security and backups.