

TECHNOLOGY TODAY

Tick - Tock...

Time is running out for Windows 7 security support. After this coming January, W7 becomes like an open or broken window through which cyber crooks can crawl into your system with ease.

Do you really know the state of your network? What's really in there? A network needs to be kept current. The weak link not only slows things down, but it's the vulnerable point.

Get a 3rd party opinion as to how well protected your system is. If you are in the L.A. area, with at least 10 computers and a server, we offer to show you your weak spots absolutely FREE.

Call us at 818-797-5300 or visit us at www.itsupportla.com/free-stuff/free-network-security-assessment/

September 2019



This monthly publication provided courtesy of Yuri Aberfeld, CEO of IT Support LA.

IT Support LA creates the possibility of focusing on business goals and priorities by providing a trusted technology partnership to small businesses.



Cybercriminals Are Plotting To Hack Your Network RIGHT NOW...And What You Can Do To Prevent It

Did you know that small businesses are more likely to be targeted by cybercriminals than any other business or organization? It's true! While we hear about major breaches on the news, we don't get to hear the stories of the businesses that struggle with hacking attempts and cyber-attacks.

Hackers love to go after small businesses for one very big reason: small businesses are less likely to invest in top-notch (or even worthwhile) cyber security. Hackers love this vulnerability.

According to the Verizon 2019 Data Breach Investigations Report, 43% of cyber-attacks hit small businesses. The reason comes down to many factors, but there are two in particular that hackers really dig into when going after targets: lack of resources and lack

of knowledge. Of course, there's more to this story, as hackers also look at a business's customer base and the type of data the business shares online.

A lot of small businesses are also relying more on the cloud (and this is the trend moving forward), but then they do little to keep their line of communication with the cloud storage, or just the cloud storage itself, secure. According to Symantec, a lot of businesses that rely on the cloud also fail to rely on strong encryption software. They just share their data to the cloud and let that be that.

Hackers attack small businesses because they want money. Hackers go after targets they can profit from, whether they hold a business's data hostage and demand a ransom (and get that ransom – hackers got \$460,000 from

Continued on pg.2

Get More Free Tips, Tools and Services At Our Website: www.itsupportla.com
(818) 797-5300

Continued from pg.1

Lake City, Florida, officials after a ransomware attack on government computers, and that wasn't the only Florida city to pay!), or by stealing customer data and either selling it on the dark web or black market, or using it for themselves.

The Verizon report also looked at the types of businesses that are targeted. The top three are:

- Public administration (23,399 reported incidents and 330 confirmed data disclosure)
- Information services (1,094 reported incidents and 155 confirmed data disclosure)
- Financial and insurance (927 reported incidents and 207 confirmed data disclosure)

They go after these types of businesses because this is where they can make their money – and it's where they've discovered the most vulnerability. However, while these types of businesses represent the top three, there are *many* more. *Every* type of business is targeted. Some businesses make it past the attack unscathed, but many don't. Their data is compromised in one way or another.

Why are small businesses targeted so much? It's a numbers game. Hackers know most small businesses lack good cyber security. This makes these businesses easier targets. Target

"First and foremost, you have to realize YOU are a target. It doesn't matter if you've never been hacked before."

enough of them, and you're going to make some serious money (from selling stolen data or paid ransoms).

So, what can you do about this? How can you protect your network? First and foremost, you have to realize YOU are a target. It doesn't matter if you've never been hacked before. It just means the hackers haven't gotten to you yet. Once you realize this, you can go to work and get your business ready for the eventual attack.

This is where a risk assessment can do a lot of good. You may already have some security measures in place, but do you know how effective those measures are? You need to know where your holes are so you can plug them and then reinforce them. You don't want just a wall around your business, you want an entire ocean.

But it doesn't end there. One of the most powerful tools against hackers and cybercriminals is knowledge. Next to securing your business, the best thing you can do is train your employees on understanding cyber security and the threats that exist to harm the business they work for. Your team **MUST** know how to identify phishing schemes, fraudulent websites and virus scams, then stay regularly updated on the threats out there. (And don't forget using complex passwords that are locked away in a password vault or manager to add another layer of security).

On top of this, work with an IT team who knows what they're doing. It's one thing to tackle this all by yourself, as many businesses do, but it's another to work with an experienced IT security firm. If you go it alone, you might miss something or you might not fully understand the security you have in place. Having an outsourced team of pros means you're one step ahead of the hackers.

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

PROTECT YOUR NETWORK

"What Every Business Owner Must Know About Protecting and Preserving Their Network"



Don't Trust Your Company's Critical Data And Operations To Just Anyone!

This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
www.itsupportla.com/protect
or call our office at (818) 797-5300.

Get More Free Tips, Tools and Services At Our Website: www.itsupportla.com
(818) 797-5300

They're Back!

More appropriately: They never left, they just slacked off. But now there's Good News and there's Bad News to report:

The Good News is that ransomware attacks are dwindling against consumers, where crooks would typically hit smart phones and home computers for a few hundred bucks, but small fish like these entry level cyber criminals outgrow their pond and want to be bigger fish.

The Bad News is a new, incredible surge in attacks on small and mid-sized businesses (SMBs). These attacks had levelled off, due in part to the uptick of hackers breaking in quietly to use their victim's computing power to mine for Bitcoins and other online currencies, but now they are back with a ferocity. By midway through 2019, there were more Ransomware attacks than in all of 2018, and they're growing exponentially.

Just like many entrepreneurs, Cyber crooks try new things, but the sad fact is that SMBs have always been their bread and butter. They have armies of free-lance spotters who scour a multitude of businesses for ways to get in by mining for employee information. Once they secure this data, they sell it up the food chain to the actual hackers, who attack your network using a variety of methods. The most common is Phishing.

But these aren't just Phishermen. They are hungry predatory sharks, and the weaknesses in your system, including a lack of user training, is chum in the water.

We still talk to business owners ever day – smart men and women who have built their companies up from nothing by using their brains and will. YET, so many of these intelligent businesspeople continue to think they won't be hit by hackers. How many times have we heard, "We're too small. They wouldn't bother with us."

YES, THEY WILL... THEY DO.

Are you protected? We will provide you with a FREE network and report of your system, and we rarely find a system that is well protected. Call us at 818-797-5300. Be ready.

5 Ways Smart People Blow The Close

The weirdest thing happens when it's time to close a deal. Smart people turn to mush! I've seen it a hundred times. Here are some common ways smart people blow the close.

1. HIT MUTE

I was with a colleague in the boardroom of a billionaire CEO of the #1 company in his industry. Right after the CEO talked about the ways he wanted our help, my colleague had the chance to close the deal and help this great entrepreneur achieve his vision. Rather than bring it to a close, my colleague's mind hit Mute. Silence. Twenty seconds of silence while the client expected to wrap up the conversation and close this deal! My colleague recovered, and we ended up with a happy outcome. Clients want help wrapping up a conversation and turning to an action plan. Don't just sit there! Close the deal!

2. DON'T IMPOSE

I was in another boardroom with another colleague late in the day. My colleague did an amazing job of using reflective listening techniques to help the CEO identify his biggest leadership challenges. And then my colleague let the meeting end with no next steps. Afterward, I asked, "Why didn't you close him on the next step you want to take to solve the problems you just identified?" My colleague said, "I didn't want to impose! I didn't want to turn it into a sales call." I was like, "Impose? How is helping a CEO solve his #1 problem imposing!" That one didn't turn out well for us.

3. DAZZLE WITH COMPLEXITY

One of my other colleagues is a ninja at turning a trusted advising conversation into an actual project. But she was not always this good! In the early days, she talked at 90 mph, offering complex, nuanced analyses sprinkled with long, multipart questions. Her intent was to show how smart she was and dazzle clients into hiring us, but clients felt they couldn't get a word in edgewise. This is a common pitfall for smart people who come out of consulting backgrounds.



4. WIN THE ARGUMENT

One of my colleagues put his hand up like a "stop" gesture in the face of our client. The consultant said, "Let me stop you there. I think your logic doesn't hold. The data tell a different story. Here is why ..." The client was not impressed with the posture. Serving clients is not about winning arguments; it's about understanding the client and figuring out how to get them what they want. You are on the same team. If you forget this, you may win the argument but lose the deal.

5. STAY SAFELY VAGUE

When I was hiring a law firm many years ago, I had a specific goal of designing an employee stock purchase program. I wanted to know the steps in drafting the plan, how long it would likely take and how much it would likely cost. The bad lawyers stayed "safely vague": "Well, that all depends." I felt like saying, "Well, no kidding, but I'm trying to get a rough estimate of the time and cost of designing this plan." The good lawyers said things like, "I'm going to ask a few questions, and I'm happy to give you an estimate for how long this project might take, how much it's likely to cost, and I'll tell you the things that will affect the time and cost." Be specific. Clients like it when you offer specifics that will help them achieve their goals.



Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times best-selling book, Who: A Method For Hiring, and the author of the No. 1 Wall Street Journal best seller Leadocracy: Hiring More Great Leaders (Like You) Into Government. Geoff co-created the Topgrading brand of talent management. He is the founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in Economics with honors from Northwestern University, and an MA and PhD in Psychology from Claremont Graduate University.

■ 5 Technology Trends You CANNOT Ignore

Internet of Things (IoT) - From WiFi-connected thermostats to smart locks, we're surrounded by IoT devices. Smart locks, for instance, can track who comes and goes with zero oversight.

Artificial Intelligence (AI) - AI can enhance consumer experience by delivering personalized experiences to customers. Automate more of what you do on social media with the help of AI.

Telecommuting - Working between home and office is easier than ever. As cloud collaboration has become simpler and more user-friendly, more employees are opting to use their own devices, saving the company big dollars.

Customer-Relationship Management (CRM) Software - It's all about building and managing customer relationships.

CRM is crucial in tracking prospects, logging e-mails and phone calls and more.

Voice Search - More people are using assistants like Alexa and Siri to access information. Optimize your SEO to get the most out of voice-search technologies. *TechRepublic, 5/21/2019*

■ Implement These 2 Steps Now To Prevent Fraud In Your Bank Account

Did you know your company's bank account doesn't enjoy the same protections as a personal bank account when it comes to fraud? If a hacker takes money from your business account, the bank is NOT responsible for replacing funds. Ask your bank what their policy is on refunding money stolen from your account. Many people erroneously believe the FDIC protects you from fraud. It does not; it only protects you from bank insolvency.

Tip: Step 1: Invest in insurance to protect you from fraud. Step 2: Set up e-mail alerts to receive notifications any time money is withdrawn from your account. The faster you catch fraudulent activity, the better your chances are of keeping your money. If you contact the bank immediately after any money is taken out, you have a very high probability of stopping hackers from robbing you.

■ 4 Proven Techniques To Improve Project Management In Your Business

1. Know the project's purpose/scope/goal. This is how you get focused. When you know your purpose, you can tackle the project one step at a time and not take a scattershot approach.
2. Set deadlines and budgets for every step. Give yourself a timeline for every step of the project to keep things moving. A budget can also help you delegate and spend accordingly. Deadlines and budgets can also increase accountability.
3. Keep everyone looped in. Everyone on the project needs to know exactly what is going on, from tasking to status updates and any scheduling. When you're all on the same page, things move along much easier. Even better, use a web app to keep everything in one place.
4. Review the project. Examine what went well and what didn't. You can adjust the next project and hammer down what worked while avoiding the same mistakes. *Small Business Trends, 6/18/2019*

