

What's New

Have I been hacked?

Before now I had to answer "It depends" as you really didn't know unless you spent five figures to forensic IT experts to know for sure. Now, we have a new weapon, Huntress, from an ex-NSA 'good guy hacker' which detects a hacker creating a foothold in your network as it happens.

Once we set up Huntress on your network, the answer to the question above will then be a very simple, **"NO, you haven't."** and your business can easily afford it. Call us to learn more, **(317) 290-8702**.

May 2019



This monthly publication is provided courtesy of Rick Rusch, CEO of Secure ERP, Inc. Secure ERP is a network security & ERP integration specialist in central

Indiana with over 25 years of experience supporting small to medium sized businesses. Founded by a CPA and Cybersecurity Evangelist, Secure ERP is dedicated to protecting our clients' data and supporting their people and growth.



Are YOU Prepared For The End Of Windows 7?

If you're one of the estimated 40%+ of businesses still on the outdated Windows 7 platform, consider this your wake-up call: time is nearly up for your trusty, tried-and-true operating system. On January 14, 2020, Microsoft will end support for Windows 7. That means no more updates, security or otherwise, will be offered by the company from that date forward.

The clock's been ticking on Windows 7 ever since Microsoft ended mainstream support back in 2015, and its time will soon be up. While it's important to note that Windows 7 will still technically be usable after next January, this upcoming shift will spell trouble for users who've stuck it out to the platform's bitter end. Not only will Windows 7 become progressively more unstable as modern hardware outpaces the software, but cybercriminals are certain to flock to the operating system after support shuts down, eager to pick off easy targets left

vulnerable by the lack of ongoing security updates.

If you're running a business, this is a risk you can't afford. It's time to contact your IT provider and make preparations to upgrade, preferably well in advance of the January 14 deadline. Whether you're planning on seamlessly transitioning to Windows 10 or moving on to an alternative operating system, this is a task that needs to be at the top of your list.

DON'T LEAVE YOURSELF VULNERABLE

Since Windows 7 will continue to work after January 14, you may wonder why you can't just stick it out and keep using the platform. The answer is you *can* – but you absolutely shouldn't. In fact, the risks and problems this decision would pose to your business make an upgrade less of a decision and more of an eventuality.

Modern software is no longer designed

Continued on pg.2

Our passion is your cyber protection, worry free tech is what we deliver.

www.secureerpinc.com • (317) 290-8702

Continued from pg.1

with Windows 7 in mind. This includes old software that's been upgraded since the world moved on from the operating system. As technological progress continues at breakneck speed, more and more key programs will become unusable in Windows 7.

The same goes for hardware. Tech equipment advances exponentially year by year. In order to take advantage of these massive improvements, you need an operating system equipped to handle these new capabilities and features. What's more, as the hardware progresses, it may become incompatible with Windows 7 altogether.

However, these are small concerns when compared to the future security of your network. As time goes on, new vulnerabilities are discovered in even the most well-designed operating systems. To fight against hackers, developers continuously search for ways to remove these security gaps and release them in the form of patches. With every annoying update you're forced to install on your machine, you're staving off would-be opportunists on the

hunt for their next victim.

After Windows 7's end of life, these updates will dry up. That means that any users still on the platform – and there will be a lot of them – will be exposed to the increasingly crafty exploits used by hackers. Cybercriminals, attracted to the lowest-hanging fruit, will come in droves for Windows 7 users, eager to pick at the scraps.

Staying on an operating system after it's no longer supported is like leaving the digital door open on your business. Don't do it.

TIME IS RUNNING OUT

Of course, we're still at least six months out from the Windows 7 end-of-life date. That may seem like a lot of time. When it comes time to actually make the transition, though, you'll need all the time you can get. Upgrading dozens, hundreds or even thousands of PCs is more laborious than you probably realize. And with so many other companies scrambling to do the same toward the end of the year, IT providers are likely to get bogged down with service requests.


Instead of putting it off to the last minute and potentially leaving yourself vulnerable, contact your IT provider as soon as possible to initiate the upgrade process. You'll leave yourself ample time to iron out any issues as they arise without the added pressure of an imminent deadline.

When your business is on the line, it just doesn't make sense to delay. Don't risk losing everything you've worked so hard to build. Make preparations to leave Windows 7 behind today!

“Cybercriminals are certain to flock to the operating system after support shuts down, eager to pick off easy targets left vulnerable by the lack of ongoing security updates ...”

Cyber Threats & Solutions Webinar Series

Thursday, May 23 @ 11am EDT—Protection Technology



Who Should Attend? C-Level executives & managers who are concerned about lost or stolen devices; privacy of confidential information; employment litigation introduced when employees use personal devices to access company data; and reputational damage along with State & Federal laws that carry heavy fines for lost or stolen customer/employee data. Of particular importance for those organizations that handle ANY sensitive data, medical records (or serve clients who have such records) or that want to avoid having their bank account wiped out due to a cyber-attack or ransomware.

The proper tools will keep you from being “an easy target.”

**Register online: <https://www.secureerpinc.com/may23web>
or call our office at (317) 290-8702.**

Our passion is your cyber protection, worry free tech is what we deliver.
www.secureerpinc.com • (317) 290-8702

Cyber Security TIPS



Did you know your COMPANY'S bank account doesn't enjoy the same protections as a personal bank account? For example, if a hacker takes money from your business account, the bank is NOT responsible for getting your money back. Don't believe me? Go ask your bank what their policy is on refunding you money stolen from your account! Many people think FDIC protects you from fraud; it doesn't. It protects you from bank insolvency, NOT fraud.

One way to thwart these frauds is to implement **Positive Pay** with your bank. There is a fee for this, but as a CPA, I highly recommend it as part of finance "best practices."

Here's an FBI alert about bank fraud related to wire transfers from July, 2018. I recommend your financial team reads it:

<https://www.ic3.gov/media/2018/180712.aspx>

(You may need to copy and paste the above link for it to work properly.) Stay Protected! - R²

What Keeps Them Coming Back?



In this era of intense competition and global communication, it's more essential than ever that your company makes figuring out what your customers want, need, desire and expect your #1 priority. Everything should start with a definition of how you want your company to be remembered in the eyes of your customers. Once that's in place, ensure that everyone in your organization understands and strives to make that definition a reality.

Lauren Freedman, president of the e-tailing group, once said, "Always keep in mind the old retail adage: Customers remember the service a lot longer than they remember the price." The human side of doing business is of paramount importance, especially in this age of advanced technology and e-commerce. Consider it an enormous opportunity for any company wishing to enlarge their market share. After all, only one company can be the cheapest, so all others must do something else to attract their customers. With that in mind, raising your level of customer service will boost your revenue and dominate your market.

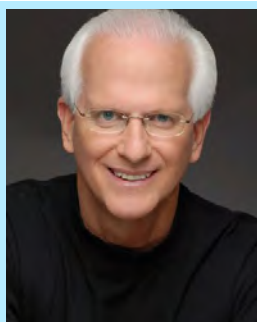
It seems to me that many companies fight their competitors the wrong way. They spend enormous sums on advertising, desperate to establish their brand presence in the marketplace, rather than simply *doing more* than their competitors. They overlook the principal factor that will drive customers to tell their friends and family about what a great company they are. Take a look at the demographics: millennials are now the largest group in America, and Gen Z

will take that title by 2020. And what do more than half of these individuals cite as the most influential factor on their purchase? Comments on social media.

Disappointed, displeased, unsatisfied and unhappy customers all happen because of one word: *less*. The company or service person delivers "less" than expected, "less" than required, "less" than promised. "Less" is a disease caused by poor corporate culture, and eventually, it will kill any company, no matter how much they pour into advertising.

If you want to succeed, you better fully understand what it is your customers expect and do everything in your power to never deliver less than that or less than what your competitors deliver. When you turn your customers' expectations into reality, everyone wins.

One of the most powerful statistics I've ever come across comes from a study conducted by the global consulting firm Bain & Company, in which they state, "eighty percent of companies believe they deliver superior customer service, but only 8 percent of their customers say they do." With that in mind, go back to my first statement in this article: identify what your customers want, need, desire and expect; define how you want your company to be remembered; and make sure everyone in your organization is dedicated to making that definition happen.



Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys and 52 Essential Habits For Success, he's shared the podium with esteemed figures from across the country, including former President George H.W. Bush, former Secretary of State Colin Powell, Anthony Robbins, Tom Peters and Steven Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.

3 Ways To Protect Your Remote Employees From Being Hacked

Remote work is a staple of any truly modern office, but it opens your employees up to some unique security risks. To minimize the vulnerability of your team and the precious data of your organization, it's essential that you implement a few simple guidelines.

First, avoid using public, unsecured WiFi. Tons of people work from the comfort of a coffee shop, but this is actually a pretty big security risk. Hackers can spoof free WiFi networks to boost company data or spread malware throughout unprotected networks. It's hard to ban this one outright, but it's important to at least be aware of the risks, and at the very least, never log in to a network that isn't password-protected.

As always, the weakest link in any

security plan is the people behind it. Teach your team about the warning signs of malicious cyber-tactics, like phishing, and the importance of implementing tech best practices while they work, such as strong passwords. With a little foresight, you can reduce your employees' exposure and teach them to be responsible with company data out in the wild. *Inc.com, 2/12/2019*

Don't Use These E-mail Accounts for Business

Here's an opinion that's sure to be unpopular: you shouldn't be using Gmail, Yahoo, Hotmail or any other popular free email service for your business accounts. Without a proprietary e-mail address specific to your business to lend your e-mails legitimacy, prospects are likely to ignore them outright or even assume they're spam. What's more, cloud-based e-mail platforms can be quite vulnerable. It's pretty easy to set

up a company e-mail, and once you do, you'll never look back. *ConversionPipeline.com*

4 Insurance Plans You Should Carry TODAY

1. Cyber security insurance. As data breaches against small businesses skyrocket year after year, it's practically a no-brainer to invest in insurance that keeps you protected, especially if you collect sensitive data from your customers.

2. Sexual harassment insurance. It's vital to hold accountable those acting inappropriately in the workplace and to make the global working environment comfortable for everyone. But unfortunately, you can't always prevent the bad behavior of insidious assaulters, making sexual harassment claims a constant risk.

3. Flood insurance. Floods have been steadily worsening countrywide over the past few years. Forty percent of businesses that face damage from natural disasters never reopen – do you want to be one of them?

4. Umbrella insurance. For every potential liability issue not specifically covered under another policy, it's good to have your bases covered. This isn't for every business, but if you're concerned about things like rental-vehicle accidents, slander or defamation-of-character claims, it's a good idea to invest in the added protection. *SmallBizTrends.com, 2/18/2019*

