PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions | February 2019

End of Life for Windows Server and Windows 7

Did you know that Microsoft will no longer be offering support for Windows 7 and Windows Server 2008 after January 2020? This means that all security updates will no longer be offered and support will not be provided after this date.

Make plans soon! Contact us at (561)969-1616 for more information and we will ensure that the upgrade runs smoothly!

This monthly publication provided courtesy of Chuck Poole, President of PalmTech Computer Solutions.

Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.

Sneaky Ways Cybercriminals Access Your Network

And What You Can Do To Prevent It TODAY

Hackers prefer the little guy. The high-profile data breaches you read about in the news — your Facebooks and Equifaxes and T-Mobiles — are only the tip of the iceberg when it comes to the digital crimes being perpetrated

day after day, especially against small businesses. Today, according to a report by the National Cyber Security Alliance, 70 percent of hackers specifically target small businesses. Attracted by the prospect of easy money, they search for those organizations who underspend on protection, who have employees untrained to spot security risks, and who subscribe to woefully out-of-date practices to protect their data. As a result, more than 50 percent of small businesses have been hacked, while 60 percent of companies breached are forced to close their doors within six months.

Most business owners have no idea the danger they're putting their livelihood in by leaving cyber security up to chance. According to a survey conducted by Paychex, 68 percent of small-business owners aren't concerned about their current cyber security standards, despite the fact that around 70 percent of them aren't adequately protected. In the face of an imminent, global threat to the very existence of small businesses everywhere, most CEOs offer up a collective shrug.

The tactics and software available to hackers become more sophisticated by the day, but with so many unwitting victims, most criminals don't even need to work that hard to net a six-figure income. By sticking to two tried-and-

continued on page 2

tested tools of the trade — phishing, ransomware and the subtle art of guessing users' passwords — they leech comfortably off the earnest efforts of small businesses all over the world.

So, what's to be done? Well, first things first: You need to educate yourself and your team. Protect your organization against phishing by fostering a healthy skepticism of any email that enters your inbox. Make it a habit of hovering over hyperlinks to check their actual destination before you click. If an email is coming from someone you know, but the email address is different, verify it with the other party. And never, ever send passwords or personal details to anyone over the internet if you can avoid it.

Speaking of passwords, you probably need to upgrade yours. The majority of folks use the same password for everything from their Facebook account to their business email. The fact that this includes your employees should make you shudder. It may not seem like a big deal — who's going to take the time to guess SoCcErMoM666? — but aside from the fact that simple software enables hackers to guess even complicated

passwords in minutes, that's not even usually necessary. Instead, they can just look at the data dumps from a recent more high-profile breach — think the Equifax fiasco — pull your old website from there and type it into whatever profile they want to access. If you keep all your passwords the same across sites, it won't take them long to dig into your most precious assets. To avoid this, implement a strict set of password regulations for your business, preferably incorporating two-factor authentication and mandatory password changes every few weeks.

> **"In the face of an imminent global threat to the very existence of small businesses everywhere, most CEOs offer up a collective shrug."**

Of course, you can read up on hacking techniques and teach them to your team until you're blue in the face, and a data breach can still occur. Cybercrime is constantly evolving, and staying abreast of its breakneck pace takes a dedicated awareness of the latest protective tools and measures. That's why your single best weapon to defend you against the hackers at your door is to find a managed service provider (MSP) with a background in defending against digital threats to partner with your organization. These companies not only regularly monitor your network, they also keep it updated with the latest patches and measures to prevent the worst. And if crisis somehow still strikes, they'll be able to get your network back up in minutes rather than days, equipped with an expert knowledge of your systems and years of experience in the field.

In today's digital world, leaving your cyber security up to a subpar antivirus and some wishful thinking is more than irresponsible — it's an existential threat to your company. But with a little savvy, a bit of investment and a second opinion on the circumstances of your company's security, you can rest easy knowing that no matter what comes, you're protected. Cal us at 561.969.1616 to discuss how we can protect you and your organization.

Shiny New Gadget Of The Month: The Movi

Sure, your big honking iPhone or massive Android is impressive, but does it have a screen the size of an entire wall?

The Movi is the first smartphone to integrate a built-in pico projector into its design, allowing users to project 720p images up to 200 inches in size wherever they are. At only $599, it's a bargain when compared to other comparable projectors.

However, there are caveats: the Movi's FHD phone screen can't compare to its higher-end OLED competitors, and its camera leaves something to be desired. But if you're an avid video buff with a mind for convenience, the Movi may be just what you're looking for.

Watch Your Doors

When was the last time you looked at the doors to your business? It isn't just about who comes in; it's also about how.

Let me give an example. A new restaurant opened near my office. It's been very successful, and I eat there regularly. The only problem is the horrendous door you have to go through to get in. Opening it causes an obnoxious grating sound, not unlike a few metal tomcats duking it out in an alley. The pull is hard and inconsistent. At first I thought they'd fix it, but since it hasn't been dealt with in months, it's clear to me that the owners don't give much thought to the first impression it creates.

Actual doors are important, but the metaphorical doors to your business are even more important. These "doors" are entry points, drawing people in or keeping them out. They can welcome or they can warn.

What about the doors to your business?

Your website is your online door. Is it aesthetically pleasing? Easy to navigate? Up-to-date? Can a visitor quickly find contact information? Does it just advertise, or does it make it easy for visitors to actually take action?

Your phone is a door too. Whether answered by a person or a recorded message, it speaks volumes about your professionalism and punctuality.

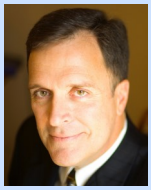
The way you handle service and support is yet another door. How easy is it for a customer to schedule a repair? Do techs arrive when promised? Are they professional in appearance and friendly in demeanor?

Then there's your social media accounts. What image do your various platforms convey? Does your social media support or detract from your brand?

Your office environment is another. Is it a place customers enjoy or endure? If you serve coffee, how good is it?

Gordon Hinckley said, "Eternal vigilance is the price of eternal development." Paying attention consistently will allow you to develop and achieve success. Ignoring the doors, literal and metaphorical, can be costly.

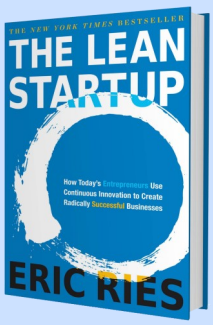
A good door makes it easy for customers to enter. A great door invites them in and sets the tone for what follows. Make sure yours immediately conveys everything you want others to know about your business.



Mark Sanborn, CSP, CPAE, is the president of Sanborn & Associates, Inc., an "idea studio" that seeks to motivate and develop leaders in and outside of business. He's the bestselling author of books like Fred Factor and The Potential Principle and a noted expert on leadership, team building, customer service and company change. He holds the Certified Speaking Professional designation from the National Speakers Association and is a member of the Speaker Hall of Fame. Check out any of his excellent books, his video series, "Team Building: How to Motivate and Manage People," or his website, marksanborn.com, to learn more.

The Lean Startup By Eric Reis

The list of start-ups that come up with a seemingly brilliant idea, rush into business and promptly crash and burn is infinitely long. But the fact is most of this failure isn't a product of fickle consumer interest or some external factor, and it's actually totally preventable. The key is to not succumb to conventional management strategies. In his book, The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation To Create Radically Successful Businesses, Eric Ries outlines an approach that empowers companies of all sizes to be more efficient, nimble and successful for the long term. Through continuous testing and constant adaptation, even the clunkiest organizations can slim down and stay abreast of their competitors.



The Dangers Of The Web And How To Stay Safe

You probably go to great lengths to keep yourself safe, whether at home or in public. But what happens when you get online? Learn more about how you could be exposing yourself and your personal information over the internet so you can stay safe.

With the headlines about data breaches and cyberattacks greeting you every time you go online, it seems impossible to have a surefire, foolproof way to keep your information secure. Sometimes cyber predators are relatively harmless, but oftentimes, their goal is to steal identities and financial information. Virus scanners and firewalls can definitely help, but here's an added layer of protection when you go online.

What is private browsing?

Your web browser — whether it be Chrome, Edge, Firefox, Safari, or Opera — stores the addresses of the sites you visit, cookies that track your activity, passwords you've used, and temporary files you've downloaded. This can be convenient if you frequently visit certain pages, can't remember your login details, or if you're trying to recall a website you visited a few days ago. But if someone else uses or gains access to your computer, your most private (and embarrassing) internet activities are exposed for anyone to see.

With private browsing — also called Incognito Mode in Chrome and InPrivate Browsing in Edge — all the information listed above does not get recorded. In fact, all the websites and information you accessed during a private browsing session is discarded without a trace as soon as you close the browser. This can come in handy when you're using a public computer because you're instantly logged out of all the accounts after closing the window.

Private browsing also prevents cookies from being stored on your computer. In a normal browsing session, sites like Facebook will inundate you with highly targeted ads based on the sites and pages you've visited. But in private browsing mode, your internet activity won't be used against you by marketing companies.

Another benefit of private browsing is you can use it to log in to several accounts on the same site, which is useful if you need to log in to two different Google accounts at the same time.

Limitations of private browsing

Although private browsing does prevent your web browser from storing your data, it doesn't keep your online activities 100% private. If your computer is connected to the company network, system administrators can still keep track of what you're browsing, even if you're in Incognito Mode. Also, if spyware or keylogger malware is installed on your computer, hackers will still be able to see what you're doing online.

A keylogger malware records every key you punched in and may send this information to a predefined email address without you knowing. This means passwords, answers to verification questions, account numbers, credit card details, or even the words you type in a chat can be emailed to someone spying on your online activities.

Even though private browsing has quite a few benefits, you shouldn't solely depend on it for online privacy. Your computers and mobile devices must be equipped with Virtual Private Networks that encrypt your internet connection and prevent anyone from intercepting your data. And don't forget to scan your computer for viruses with a strong anti-malware program to keep spyware and other malicious web monitoring software at bay.

Call us at (561)969-1616 to learn how we can protect your organization.

Are Your Credentials For Sale On The Dark Web?

Visit www.palmtech.net/darkweb/ For A Free Scan!