PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions December 2019

A Note of Gratitude:

Our clients are the BEST part of our work. We thank you for another great year.

Happy Holidays to you and yours from our team at PalmTech Computer Solutions!

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.

Cybercriminals Are Taking Aim At Your Business … Is Your Network Protected?

Cybercriminals love to test your defenses. They love to see how far they can get into the networks of businesses all over the globe. Cybercriminals really love going after small businesses because they can all too often sneak onto a network, copy data and move on. Through the use of ransomware, they can hold your data hostage and refuse to cooperate until you pay them some amount of dollars – and if you don't pay up, they threaten to delete all your data.

But protecting yourself is not as hard as you might think. While cybercriminals and hackers are an everyday threat to businesses, you can take steps to significantly reduce that threat and take that target off your back.

The first thing you need to do is understand why cybercriminals target small businesses and what makes your particular business vulnerable. There are many things small businesses do and don't do that open them to attack and data theft. These may include not having enough (or any) security in place or not training employees on security protocols.

Realistically speaking, the biggest threat to your business does, in fact, come from your own employees. This doesn't mean they are intentionally

continued on page 2

harming your business or leaving your network exposed to outside threats. It means they don't have the proper training and knowledge to protect your business from a cyberthreat.

For instance, your team needs to be trained to use strong passwords, and those passwords *must* be changed periodically (every three months is a good rule of thumb). A lot of people push back on strong, complicated passwords or use the same password for everything, but this is just asking for trouble and should not be allowed at your company.

Once strong passwords are in place, enable two-factor authentication (2FA) on everything you possibly can, from network access to every account you and your employees use. This is an additional layer of security on top of standard password protection. This feature is generally tied to a mobile number or secondary e-mail, or it may be in the form of a PIN. For example, when 2FA is enabled, after you've put in your password, you will be prompted for your PIN for the associated account.

Another thing you must do to get that target off your back is to get anti-malware software installed. Every workstation or device should have some form of this protection. Not sure what to use? This is when working with a dedicated IT company can come in handy. They can help you get the right software that will meet your specific needs without slowing you down. They will install software that is compatible with your PCs and other networked equipment. Plus, they will make sure anti-malware software is working and is regularly updated.

> **"You can take steps to significantly reduce that threat and take that target off your back."**

On top of this, you want to have an active firewall in place. Every business should have its network protected by a firewall; like anti-malware software, firewall security comes with a number of different settings, and you can customize it to fit the needs of your network. Firewalls help keep attackers and malicious software off your network. When paired with a good anti-malware software, your layers of security are multiplied. The more layers, the better protected you are.

Finally, with all of this in place, your employees need to know what it all means. Keep your team up-to-date on your business's security protocols. This includes items like your password policy, malware protection policy and proper e-mail and web-surfing etiquette. The bad guys are never going to stop attacking, but you have the power to protect your business from those attacks.

Your staff is your first line of defense. Call us for assistance regarding our cybersecurity awareness training to ensure your employees are educated on the security risks that exist **(561)969-1616**.

Shiny New Gadget: HD Mask Surveillance Camera USB Spy Cam

Sometimes, you don't want security cameras in plain sight or you don't even want to go to the trouble of installing cameras. Meet the HD Mask Surveillance Camera USB Spy Cam. This device makes video monitoring easier than ever.

The HD Mask is a tiny camera disguised as a USB charger. At a glance, you would have no idea it was a camera. Even better, it actually works as a USB phone charger, which really sells the disguise. It records as soon as it's activated with motion and has many practical purposes, from keeping an eye on pets to monitoring certain areas of your office for security purposes. You can access the footage right on your smartphone and watch in real time. Learn more at HDMask.com.

What A Football Coach Can Teach You About Getting Better

Woody Hayes spent 28 seasons as the head football coach at Ohio State University, and then he was fired after a now-infamous incident in the 1978 Gator Bowl.

With time running down in the fourth quarter and the Buckeyes already in a position to try a game-winning field goal, Hayes called a pass play. A Clemson player intercepted the pass and was knocked out of bounds along the Ohio State sideline, securing the victory for the Tigers.

Frustrated by the play and the opponent's celebration among his troops, Hayes lost his temper and hit the Clemson player.

For most Ohio State fans, however, that's not the legacy of Woody Hayes. Some, naturally, see his legacy in his coaching record – 238 wins, 72 loses, 10 ties, 13 Big Ten titles, and three National Championships. That proved more than enough to land Hayes in college football's Hall of Fame. The OSU Woody Hayes Athletic Center is also named in his honor.

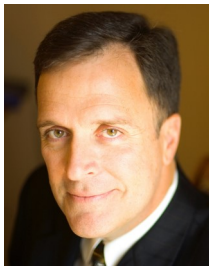
Others, however, see his legacy in a chair – the Wayne Woodrow Hayes Chair in National Security Studies. In keeping with his wishes, donations made in his honor following his death in 1987 were directed toward academics, which led to the creation of the chair. Hayes, who once grilled Richard Nixon about foreign policy, always took academics as seriously as he did football.

I remember Hayes for all of those things, but I remember him most for something he said during a pep rally when I was a student on the Columbus campus: "You're either getting better or you're getting worse," he told the crowd. "Status quo is a myth."

I used to think that was coach talk, but time and experience taught me the truth in what he meant. In a competitive world, if you stay the same, you get passed by. It highlights the incredible importance of the "innovation imperative": keep making your value better, because your competition keeps getting better.

Regardless of how good you've become, you can't afford to stay the same because status quo is a myth.

About The Author: Mark Sanborn



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 best-selling 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.*

Yet Another Ransomware Attack...

A cyberattack slammed Pensacola's computer system on December 7th. A city spokesperson reported that the hackers were seeking $1 million to return the documents compromised in the attack, a city spokesperson said.

At least seven other cities nationwide have been hit by similar attacks, and two in Florida have paid out large ransoms.

Lake City paid out $426,000 worth of bitcoin, and Riviera Beach paid out $600,000 to hackers.

The city of Stuart also was hacked, but managed to shut down the attack — which involved hackers encrypting city data, in effect locking the files so they couldn't be used without an encryption key, which the hackers typically provide once the ransom has been paid.

In Stuart, an IT employee putting in weekend overtime spotted the attack and disrupted it. No such luck for Pensacola, where online payment systems were down and the Florida Department of Law Enforcement said the attack seemed similar to one launched against Allied Universal, a California-based company with offices in Pensacola.

Just a few days ago, New Orleans declared a state of emergency and shut down its computers after a cyberattack.

Hackers will continue to step up their game, however, security pros can take decisive action to minimize the impact of ransomware.

The first line of defense is always a good offense. To prevent an attacker from establishing a foothold in an organization's network, organizations should put the following in place:

- **Best practices** such as strong patching policies, regular system backups, multifactor authentication, application whitelisting, and restrictions of local administrator rights and privileges
- **Awareness programs** to educate users about phishing and other forms of social engineering
- **Security tools** that provide spam filtering, link filtering, domain name system blocking/filtering, virus detection, and intrusion detection and prevention
- **A zero-trust framework** to identify, authenticate, and monitor every connection, login, and use of resources
- **Least privilege policies** to restrict users' permissions to install and run software applications

Minimizing the impacts of ransomware is about more than just defending systems against attack. It also involves taking action to minimize the impact of breaches as they happen. This is critical, since all systems can be breached by attackers who have sufficient time and resources. Call PalmTech Computer Solutions for assistance in ensuring your organization is secure and following best practices - (561)969-1616.

Are Your Employees' Credentials For Sale On The Dark Web?

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