

## What's New

### 9 Ways to prevent Disaster.

1. Spam Emails: Secure your email  
Most attacks happen through Email.
2. Passwords: Apply Security Policies.
3. Computer Updates: Keep Microsoft, Adobe and JAVA products updated.
4. Training: Train your users - Often!  
Teach them about data security, Email attacks, policies and procedures.
5. Advance Security: Move beyond outdated antivirus tools of the past.
6. Firewall: Turn on Intrusion Detection & Intrusion prevention features.
7. Encryption: Whenever possible, the goal is to encrypt files at rest and in motion.
8. Two Factor Authentication.
9. The Most important is Backup: Local (BDR Appliance) & to the cloud, test your backups often.

If you need help to implement any of these, call us today!



## 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.

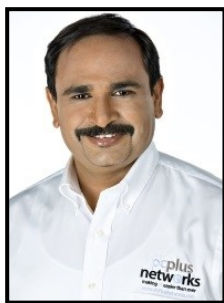
But protecting yourself is not as hard as you might think. While cybercriminals and hackers are an everyday threat to businesses, you can take steps to significantly reduce that threat and take that target off your back.

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 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.

*Continued on pg.2*

## December 2019



**This monthly publication provided courtesy of Shan Dholaria, CTO of PCPlus Networks.**

"As a business owner, you don't have time to waste on technical and operational issues plus security is a BIG concern too. That's where we shine! Call us and put an end to your IT problems finally and forever!"

Continued from pg.1

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.

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.

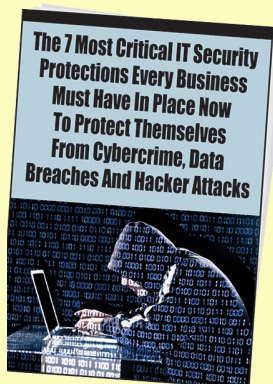
Finally, with all of this in place, your employees need to know what it all means. Keep your team up-to-date on your business's security protocols. This includes items like your password policy, malware protection policy and proper e-mail and web-surfing etiquette. The bad guys are never going to stop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

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

## **FREE Report: The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks**

Eighty-two thousand NEW malware threats are being released every day, and businesses (and their bank accounts) are the No. 1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious damage to reputation, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack, you **MUST** read this report and act on the information we're providing.

**Claim your FREE copy today at  
[www.pcplusnetworks.com/cybercrime](http://www.pcplusnetworks.com/cybercrime)**



## Services We Offer

PCPlus Networks connects you to maximum return on your IT investment with top notch business continuity solutions. As your partner we'll deliver speed, value, and quality from start to finish - using expert Engineers & project managers to keep everything running smoothly. We work with you every step of the way, from consulting to design, project management, installation and ongoing support. We even back it all up with a long lasting warranty.

### IT Services includes:

Managed Cyber Security  
IT Infrastructure Management.  
Network Support  
Managed IT Services  
Cloud Integration  
IT Consulting.  
Hardware/Software  
Backup & Disaster Recovery  
Network Storage Solutions  
VOIP / Virtualization  
Wireless / Wi-Fi Solutions  
Virus/Malware Protection  
Email / Spam Protection.  
Business Continuity Solutions  
IP Video Surveillance.  
Network Wiring/Cabling

Give us a call today at  
(678) 523-5599 to  
discuss your needs.

# 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 losses, 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. . . ~Mark Sanborn

### **IT Security Tip:** Do you enter your PIN when you use your debit card?

We live in a mostly cashless society these days. Our parents wouldn't have ever thought to pay for a \$1.50 cup of coffee with plastic; now it's commonplace. How you swipe that plastic, though, makes a big difference in how you are protected from your neighborhood cyberthief.

If you enter your PIN when you run a debit card transaction, STOP! Run the card as credit. Not only will you not have to enter the PIN, you'll almost always get more anti-fraud protection should you have a problem with a purchase or if the card number is stolen. In addition, always use the card as credit when shopping online, out of town on vacation or business, or when making large purchases.

Running your transaction through the credit card network instead of the bank network offers these additional protections - plus it's faster!



1010 Lakes Pkwy  
Lawrenceville, GA 30043

## Inside This Issue

**Cyber Criminals Are Taking Aim At Your Business. Is Your Network Protected?**

**What A Football Coach Can Teach You About Getting Better**

### **Do You Have These 3 Things Every Business Needs To Be Successful?**

You have a solid team. People are everything in business – that includes your employees. You strive to hire the best team (who match your core values and company culture and who bring top-notch skills to the table) and you train them well (they understand your systems and processes). On top of that, they're happy!

You have purpose behind what you do. We all need purpose to not only be happy but also to thrive. When your team knows what they're working toward and understand the value of their work, that gives them purpose. You've clearly laid out the objectives and everyone is on the same page. When your employees know why they do what they do, they're happier and more productive for it.

You are passionate. You don't just love what you do, you love the people you work with and you love the difference your business makes in the community or the world. When you have passion, it's infectious. It inspires people around you. When your team is inspired, they'll go the extra mile and your business will find success likes it's never found before.

*Inc.com, 5/20/2019*

### **What The Heck Is An AUP ... And Why Do You Want It?**

With so many access points, from cell phones to laptops and home computers, how can anyone hope to keep their network safe from hackers, viruses and other unintentional security breaches? The answer is not "one thing" but a series of things you have to implement and constantly be vigilant about, such as installing and constantly updating your firewall, antivirus, spam-filtering software and backups. This is why clients hire us – it's a full-time job for someone with specific expertise (which we have!).

Once that basic foundation is in place, the next most important thing you can do is create an Acceptable Use Policy (AUP) and train your employees on how to use company devices and other security protocols, such as never accessing company e-mail, data or applications with unprotected home PCs and devices (for example). Also, how to create good passwords, how to recognize a phishing e-mail, what websites to never access, etc. NEVER assume your employees know everything they need to know about IT security. Threats are ever-evolving and attacks are getting more sophisticated and cleverer by the minute.

If you'd like our help in creating an AUP for your company, based on best practices, call us. You'll be glad you did.