pcplus networks
better People, better Solutions

Real World Tech Tips

making your business IT reliable & more secure than ever

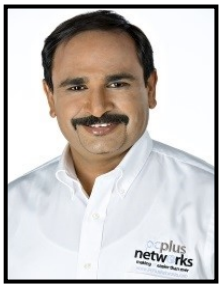
## Did You Know?

**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 Advance Security: Move beyond outdated antivirus tools of the past.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 at (678) 523-5599!

## October 2020



**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 to put an end to your IT problems finally and forever."


# Employees Are Letting Hackers Into Your Network ...

## What You Can Do To Stop It

Cyberthreats are everywhere these days. Hackers, scammers and cybercriminals are working overtime to break into your network – and the network of just about every business out there. They have a huge arsenal of tools at their disposal, from automated bots to malicious advertising networks, to make it possible.

But there is one "tool" that *you* may be putting directly into their hands: your employees. Specifically, **your employees' lack of IT security training**.

While most of us expect hackers to attack from the outside using malware or brute-force attacks (hacking, in a more traditional sense), the truth is that most hackers love it when they can get others to do their work for them.

In other words, if they can fool your employees into clicking on a link in an e-mail or downloading unapproved software onto a company device, all the hackers have to do is sit back while your employees wreak havoc. The worst part is that your employees may not even realize that their actions are compromising your network. And that's a problem.

Even if you have other forms of network security in place – malware protection, firewalls, secure cloud backup, etc. – it won't be enough if your employees lack good IT security training. In fact, a lack of training is the single biggest threat to your network!

It's time to do something about it. Comprehensive network security training accomplishes several things, including:

**1. Identifying Phishing E-Mails** Phishing e-mails are constantly evolving. It used to be that the average phishing e-mail included a message littered with bad grammar and misspelled words. Plus, it was generally from someone you'd never heard of.

These days, phishing e-mails are a lot more clever. Hackers can spoof legitimate e-mail addresses and websites and make

*Continued on pg.2*

*Continued from pg.1*

their e-mails look like they're coming from a sender you actually know. They can disguise these e-mails as messages from your bank or other employees within your business.

You can still identify these fake e-mails by paying attention to little details that give them away, such as inconsistencies in URLs in the body of the e-mail. Inconsistencies can include odd strings of numbers in the web address or links to YourBank.**net** instead of YourBank.**com**. Good training can help your employees recognize these types of red flags.

**2. Avoiding Malware Or Ransomware Attacks** One reason why malware attacks work is because an employee clicks a link or downloads a program they shouldn't. They might think they're about to download a useful new program to their company computer, but the reality is very different.

Malware comes from many different sources. It can come from phishing e-mails, but it also comes from malicious ads on the Internet or by connecting an infected device to your network. For example, an employee might be using their USB thumb drive from home to transfer files (don't let this happen!), and that thumb drive happens to be carrying a virus. The next thing you know, it's on your network and spreading.

This is why endpoint protection across the board is so important. Every device on your network should be firewalled and have updated malware and ransomware protection in place. If you have remote employees, they should only use verified and protected devices to connect to your network. (They should also be using a VPN, or virtual private network, for even more security.) But more importantly, your employees should be trained on this security. They should understand why it's in place and why they should only connect to your network using secured devices.

**3. Updating Poor Or Outdated Passwords** If you want to make a hacker's job easier than ever, all you have to do is never change your password. Or use a weak password, like "QWERTY" or "PASSWORD." Even in enterprise, people still use bad passwords that never get changed. Don't let this be you!

A good IT security training program stresses the importance of updating passwords regularly. Even better, it shows employees the best practices in updating the passwords and in choosing secure passwords that will offer an extra layer of protection between your business and the outside world.

If you or your employees haven't updated their passwords recently, a good rule of thumb is to consider all current passwords compromised. When hackers attack your network, two of the big things they look for are usernames and passwords. It doesn't matter what they're for – hackers just want this information. Why? Because most people do not change their passwords regularly, and because many people are in the habit of reusing passwords for multiple applications, hackers will try to use these passwords in other places, including bank accounts.

Don't let your employees become your biggest liability. These are just a few examples of how comprehensive IT and network security training can give your employees the knowledge and resources they need to help protect themselves and your business. **Just remember, you do not have to do this by yourself! Good IT training programs are hard to find, and we are here to help.**

> **"Every device on your network should be firewalled and have updated malware and ransomware protection in place."**

## Free Report Download: If You Are Considering Cloud Computing For Your Company, DON'T, Until You Read This…


If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report: **"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."**

This report discusses in simple, nontechnical terms the pros and cons of cloud computing, data security, how to choose a cloud provider and three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated. **Even if you aren't ready to move to the cloud yet**, this report will give you the right information and questions to ask when the time comes.

**Get your FREE copy today:**
**www.PcPlusNetworks.com.com/cloudreport**

## Shiny New Gadget Of The Month:


### Ovo Portable Steam Iron And Garment Steamer

The **Ovo Portable Steam Iron And Garment Steamer** is much smaller than your average iron and yet capable of so much more. It's an iron *and* a steamer and the perfect companion for when you're traveling and want to look sharp. Or keep the Ovo at home to save space!

The Ovo fits easily in your hand. It's lightweight and won't take up much space in your luggage. Plus, it holds enough water to create up to 10 minutes of steam. You can quickly switch from the metal ironing plate to the brush attachment to add finishing touches to delicate fabrics (and remove any lint or pet hair). It even comes with a heat-resistant travel case. Learn more about this mini-marvel at **bit.ly/2CgQzJG**!

# The Leader's Most Important Job

Can you guess what the most important trait is for effective leaders? You can probably guess all sorts of things: relationship building, communication, awareness, positivity, innovation … The list goes on. And you probably do a lot of those things too.

When I speak with leaders, I emphasize that a person's success as a leader doesn't come from what they do or how they do it — it's about *how often they do these important things*.

**The Most Important Thing For Leaders: Focus Your Team**

A leader's most important job is taking the time and effort to focus their team. Leaders must help their team members focus their time and expertise to complete the organization's most important work.

The most successful businesses are driven by **profit, innovation, efficiency and effectiveness.**

Your team's revenue and results are all driven by how people spend their time (effort) and expertise (knowledge and skills), and these are the keys to elevating your team's success. By doing these things and being a role model for your team, you can experience amazing results.

**How To Elevate Your Team**

**1. Passion** Creating a vision requires passion. This passion elevates your own commitment and helps both you and your team be productive. It's unlikely that a leader will be fully immersed in their role, their organization or their team if they are not passionate about what they are doing.

**2. Time, Expertise And Motivation** Everything is the by-product of time and expertise. When a leader invests both time and expertise into their team, the team grows. When time and expertise are invested wisely, the organization also achieves great success. By putting the time and expertise into your team members, you can motivate them to improve in their roles.

**3. Focus** This goes hand in hand with time and expertise. By focusing on the strengths (and weaknesses) of a team and learning how to constantly improve and grow, an organization can produce positive results. When a leader doesn't have this focus, the organization suffers. Mediocrity becomes the norm.

A great deal of time and expertise is wasted in companies where employees are doing low-priority work or work that shouldn't be done at all. When a team lacks an effective leader, it is difficult for them to know what they should be doing instead.

When a leader takes the time to show their team the importance of their work and how their work will achieve success, the whole organization grows. This commitment is what creates remarkable performances. You can learn more about this in my book *The Encore Effect: How To Achieve Remarkable Performance In Anything You Do*.

At the end of the day, it's most important for leaders to regularly take the time to focus on and elevate their team. Just as a conductor makes sure members of an orchestra are all playing the right music to the best of their ability, so does an effective leader do their job.

*~Mark Sanborn*

### IT Security Tip: New quarter, new password

It's a wise idea to follow the calendar year when changing passwords to your online sites, financial/banking sites and computer systems. We recommend you change these passwords at least once every three months. It's also important you don't reuse passwords or use the same passwords for two different resources.

If your social media account gets hacked, you don't want the attacker to also be able to gain access to your Amazon.com and banking accounts simply because you used the same password for both sites. Maintaining separate passwords is a lot of work – but the cybersociety we live in demands it.
A good password will be composed of both lowercase and CAPITAL letters, numbers and !@#$% ^ (symbols). Passwords for various sites should always be different, but they can be similar. You may use J@nu@ry1! for site A and J@nu@ry1@ for site B.

Need help in developing strong password policies? Give us a call and we'll be happy to help.

pcplus networks
better people, better solutions

1010 Lakes Pkwy
Lawrenceville, GA 30043

## Inside This Issue:

Employees Are Letting Hackers Into Your Network … What You Can Do To Stop It

The Leader's Most Important Job

### Do These Things To Protect Your Business From Getting Hacked

**1. Train Employees.** Your team needs to know how to identify and handle today's IT security threats. Cybercriminals often rely on your employees' lack of training to break into your network. Ongoing training gives employees tools and resources to overcome this and many other IT security challenges. Make training a top priority!

**2. Hold Employees (And Yourself) Accountable.** Training and company guidelines don't mean much without accountability. When you set rules, follow them, just as you follow industry and government rules and regulations when operating your business. Be willing to hold anyone who does not accountable.

**3. Have A Disaster Recovery Plan.** Things happen. When you store sensitive data, you need to have a plan in place to recover and restore that data should anything happen. This doesn't just include data loss from malicious attacks but other types of disasters, including hardware failure, fire and flood. How is your data being backed up and saved? Who do you notify in the event of a breach? Who do your employees call in the event of disaster? *SmallBiz Technology, Dec. 26, 2019*

### 4 Tips To Get Projects Done On Time With A Small Team

**1. Give Them The Tools And Resources They Need**
We all need tools to get things done – project management software, content creation tools, messaging apps, virtual private network access and more. Have a conversation about what each team member needs to maximize productivity and work closely with them to meet that need.

**2. Set Aside Time For Proper Research**
Don't jump headfirst into a project without jumping into research first. Information is a powerful tool to get things done efficiently and effectively.

**3. Assign Accordingly**
Before the team goes to work, make sure assignments or responsibilities are delegated properly and check in with everyone on a regular basis to make sure things are going smoothly (or to see if they need help).

**4. Plan And Plan Again**
Plan out the project before you set to work. Give yourself and your team a map to follow as you work through the project. As with any project, expect obstacles along the way and be willing to update your map accordingly. *Small Business Trends, July 4, 2020*