pcplus networks
better People, better Solutions

Real World Tech Tips

making your business IT reliable & more secure than ever

Stop Failures!

9 Ways to prevent Disaster.

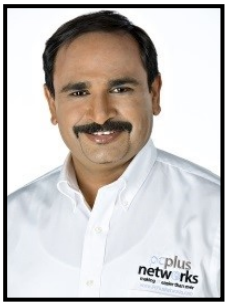
1. Spam Emails: Secure your email

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 Advance Security: Move beyond outdated antivirus tools of the past.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!

November 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!"

4 Things You Should Absolutely Demand From Your IT Services Firm

How much do you rely on your IT services provider? It's startling to think that a lot of small businesses outsource their IT (which is a good thing), only to get little to nothing out of that relationship.

Why is that?

Well, some businesses just aren't proactive. They only rely on their IT services company when something goes horribly wrong. If there's a network failure or their website gets hacked, they'll make the call to their IT people, but that's the extent of the relationship.

On the other side of the same coin, there are a lot of IT companies that wait around for that phone call. They don't work with their clients as closely as they should. Both of these reasons are downright irresponsible.

First and foremost, business owners should work closely with their IT pros. They should have the staff and resources to not only address your IT emergencies but also to keep your business safe and secure to minimize those emergencies. Here are four things you should ask of your IT services provider.

"Keep my business safe!" Your IT company should make sure your network security, firewalls, malware protection, etc., are installed, operating and up-to-date. They should be working with you to do everything to keep your business's data secure and make sure it can be restored in the rare event that data loss does occur.

Continued on pg.2

Continued from pg.1

Keeping your customer data secure should be a top priority. Don't take unnecessary risks, because when you do, the consequences can be devastating.

"Help me keep costs down!" You outsourced your IT to save money. Hiring an internal IT person or staff is a massive expense (plus, many small businesses simply don't have the revenue to sustain IT personnel). However, your IT company should be working to maintain your network and associated hardware and software. They are there to help you avoid costly disasters like data loss or network downtime. If you do a lot of e-commerce, your IT company can be an invaluable asset. You literally pay them to save money.

"Help me stay proactive!" An experienced IT company can often spot an issue before it becomes an issue. They keep your network updated and maintained, and they can help you avoid unnecessary downtime. Working closely with your IT company means you aren't skimping on security, and this alone puts you ahead of so many other businesses that do. And make sure you have an open line of communication between your business and your IT team, even if that means scheduling regular calls. You should regularly talk about security and know about the issues that may impact your business, whether it's an equipment concern or a hacker threat. On top of that, tell your customers you care about the security of your business and their data. They will appreciate it – seriously!

"Waiting until something breaks is a dangerous – and costly – way to do business."

"Keep my network up-to-date!" This covers a lot of ground. Your outsourced IT should be keeping your security updated, from your firewall to your malware protection, but they should also be keeping your network tech updated too. Hackers look for weaknesses in network tech every day – weak spots that allow them to capture data from your network. Sometimes they exploit the firmware, and sometimes it's the hardware. Regardless, you should always rest assured that your IT company is doing everything they can within the budget you set to keep your network as updated as possible.

If your IT company isn't doing any of these things, you need to get on the phone with them NOW! Don't put your business at risk because you only make the call *after* the worst-case scenario has occurred. Waiting until something breaks is a dangerous – and costly – way to do business. It's time to be proactive and get the most out of the relationship you have with your IT company.

Help Us Out And We'll Give You A Brand-New Kindle Fire For Your Trouble

We love having you as a customer and, quite honestly, wish we had more like you! So instead of just wishing, we've decided to hold a special "refer a friend" event during the month of November.

Simply refer any company with 10 or more computers to our office to receive a FREE computer network assessment (a $499 value). Once we've completed our initial appointment with your referral, we'll rush YOU a free Kindle Fire of your choice as a thank-you (or donate $100 to your favorite charity ... your choice!).

Simply call us at 678-523-5599 or e-mail us at sales@pcplusnetworks.com with your referral's name and contact information today!

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.

1. MAKE YOURSELF INTO A PRODUCT.

Position yourself as the authority in your niche. Develop products like videos or books that share your secrets of success. The beauty of a book is that, once the hard work is over – it's written, edited and published – you simply collect proceeds while you move on to your next project.

2. DO FEWER THINGS.

It's impossible to automate aspects of your business if you do everything personally. Train staff to handle certain aspects of your business and simplify your output. Identify strengths and streamline your offerings, focusing on the items that you can train your staff to replicate.

3. CREATE CONTINUITY.

Billing for each service or product you supply is volatile. Your revenue and your client's expenses vary wildly. By selling a subscription at a flat rate, you create reliable income and provide clients with predictable expenses. Both parties are invested in maximum efficiency – maximizing quality and minimizing hassle.

4. SELL YOUR SYSTEM CHEAP AND MAKE MONEY ON THE REFILLS.

We're talking here primarily about businesses that produce tangible goods. The best two examples of this model are printers and Keurig coffee makers. The devices themselves are relatively cheap. The profit is in cartridges of ink or individual coffee refills. If your machine makes a great cup of coffee or great quality copies, once consumers own the device, you're guaranteed continued business.

5. BECOME THE MIDDLEMAN.

Find a way to broker business and let other folks do the work for you. Becoming an Amazon affiliate is a great example. You link to their site, they sell, and you make money. There's also a fortune to be made in consolidating and coordinating the transportation of goods.

6. BECOME A TEACHER.

Find ways to teach other entrepreneurs how to acquire the skills necessary for opening their own business modeled on yours. Say you own a successful pizza shop. You could write a book or create a series of instructional videos on your family's recipes, or you could market a consumable version of your plan for opening a profitable pizza shop. You can even generate greater consumer awareness for your business.

7. BECOME AN INVESTOR.

Money makes money, but it's important that you're careful about how you invest as an entrepreneur. Here's my tip: look at your clients and assess their needs. Find a company that addresses those needs and invest there. Not only will you be forging a bond between your company and others that focuses on enhancing client relationships, but you also cement your position in your customers' minds as the business that caters to their desires. Once you've done the groundwork, you're the good guy who makes money without effort. ~Mike Michalowicz

IT Security Tip : Do you allow guests to access your WiFi network?

Do you have guest access on your company WiFi network? Or do you simply give out the same password that your employees use? If you give out your password, you're practically opening the door for anyone to come in and steal private information, infect your private computers and even steal customer credit card data if you are processing them over the same internet connection.

The key to providing free guest WiFi access is in segregation and security. Your WiFi guests need to be completely isolated and segregated from your private network. Your guests should not be able to reach your internal computer network, credit card terminals or other network-connected devices. Don't know how to enable guest WiFi access? Give us a call and we'll help you out.

pcplus networks
better people, better solutions

1010 Lakes Pkwy
Lawrenceville, GA 30043

Inside This Issue

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.