

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 Advance Security: Move beyond outdated antivirus tools of the past.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



If You Think Your Business Is Too Small To Be Hacked ... You're A Cybercriminal's #1 Target

Many cybercriminals look at small businesses like blank checks. More often than not, small businesses just don't put money into their cyber security, and hackers and cybercriminals love those odds. They can target small businesses at random, and they are all but guaranteed to find a business that has no IT security - or the business does have some security but it isn't set up correctly.

At the same time, cybercriminals send e-mails to businesses (and all the employees) with links to phishing websites (websites designed to look like familiar and legitimate websites) or links to malware. They hope employees will click on the links and give the criminals the information they want. All it takes is ONE employee to make the click.

Or, if the business doesn't have any

security in place, a cybercriminal may be able to steal all the data they want. If you have computers connected to the Internet and those computers house sensitive business or customer data - and you have NO security - cybercriminals have tools to access these computers and walk away with sensitive data.

It gets worse! There are cybercriminals who have the capability to lock you out of your computer system and hold your data hostage. They may send along a link to ransomware, and if you or an employee clicks the link or downloads a file, your business could be in big trouble. The criminal may request a sum of money in exchange for restoring your PCs or data.

However, as some businesses have

Continued on pg.2



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

learned, it's not always that simple. There are businesses that have paid the ransom only for the cybercriminal to delete all of their data anyway. The criminal walks away with the money and the business is left to die.

And that's not an understatement! Once cybercriminals have your data and money, or both, they don't care what happens to you. Cybercriminals can do more than just major damage to small businesses; their actions can literally destroy a business! We're talking about the costs of repairing the damage and the cost of losing customers who no longer want to do business with you. You're looking at a public relations nightmare!

This goes to show just how critical good IT security really is, but business owners still don't take it seriously. Even as we enter 2020, there are business owners who don't consider cyber security a high priority – or a priority at all. It's a mindset that comes from before the age of the Internet, when businesses didn't face these kinds of threats. And many business owners fall into the habit of complacency. In other words, "It hasn't happened yet, so it probably isn't going to happen." Or "My business isn't worth attacking."

Cybercriminals don't think like this. It's a numbers game and only a matter of time. Business owners need to adapt to today's online landscape where just about everything is

connected to the Internet. And if something is connected to the Internet, there is always going to be some level of vulnerability.

But you can control your level of vulnerability! You can be cheap or complacent and do the bare minimum, which will put your business and customers at risk. Or you can take it seriously and put IT security measures in place – firewalls, malware protection, secure modems and routers, cyber security insurance and working with a dedicated IT security company. There are so many options available to secure your business.

The reality is that cyber security should be a normal, everyday part of any business. And anyone thinking about starting a business should be having the cyber security talk right from the very beginning: "What are we going to do to protect our business and our customers from outside cyberthreats?"

When it comes down to it, not only do you need good cyber security, but you also need a good cyber security policy to go along with it. It's something you share with your team, customers, vendors, investors and anyone else who puts their trust in your business. Transparency about your cyber security is a great way to build and maintain trust with these people. If you don't have IT security in place, why should anyone trust you?

Think about that question and think about the security you have in place right now. How can you make it better? If you need to reach out to an IT security firm, do it! It will only make your business better and prepare you for the threats that are looming right now. No business is too small or too obscure to be hacked.

"The reality is that cyber security should be a normal, everyday part of any business."

Free Report Download:

The Business Owner's Guide To IT Support Services And Fees

You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

IT BUYERS GUIDE

What Every Business Owner MUST Know About IT Support Services And Fees



What You Should Expect To Pay For IT Support For Your Business And How To Get Exactly What You Need

Claim your FREE copy today at

www.pcplustnetworks.com/ITbuyersguide

Get More Free Tips, Tools and Services At Our Website: www.PcPlusNetworks.com

(678) 523-5599

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.

3 Reasons Why Recessions Are Awesome For Great Companies

It may be jarring to read the words "recession" and "awesome" in the same sentence. Recessions are bad for most people. I will not make light of how horrible recessions are for the vast majority of companies and their employees, (as well as for not-for-profit organizations and governments).

For most companies, recessions mean increased stress at work, stalled career progression or even layoffs, uncertainty, increased board and shareholder pressure, increased financial strain and a feeling of looming danger in the pit of your stomach, which is no fun to wake up to every day!

But for great companies, recessions can be awesome.

What are great companies?

Great companies make great products or deliver great services to customers. They provide a wonderful work culture that attracts and retains talented people. And because they take great care of customers and employees, great companies don't have a dangerous debt burden. They are profitable and able to pay their bills to suppliers while delivering an attractive return to investors in dividends and equity appreciation.

How are recessions awesome for great companies?

Recessions allow great companies an opportunity to do the following:

1. Shake loose the cobwebs of complacency. "Success breeds complacency," said Andy Grove, the legendary CEO of Intel. And while I'm not here to suggest everybody embrace full-on "paranoia" in the workplace (*Only The Paranoid Survive*), I am here to suggest that great companies have to keep hustling to stay great. A recession provides an opportunity for a wake-up



call to great companies that may start to coast on past greatness and help them get back on track.

2. Take customers and colleagues away from lesser companies that don't deserve them.

As lesser companies stumble during a recession (e.g., shutting locations, letting service and quality drop, highlighting dysfunction in the culture, etc.), it's the perfect time for great companies to pick up more customers and talented people. I remember when a successful business services company with 70 locations around North America entered the '08 recession. Lesser competitors were closing branches and laying off people, and service was slipping. But the CEO of the successful company was not fearful about the recession. Instead, he sensed the opportunity to win more customers with better service and poach some top talent away from the struggling competitors. The recession allowed this great company to gain market share and build a stronger leadership talent pipeline.

3. Increase the rate of learning of your leaders.

Time seems to move more quickly for me during harder times than during easy times. This can improve the learning curve of your up-and-coming leaders. Just remember to not make too many decisions for them; that will stunt their growth. Allow your leaders to come to you with problems and solutions, and coach and support them. Let them test and learn various approaches to leading through uncertain times. ~Geoff Smart

IT Security Tip: Don't Just Throw Out That Old Computer

Getting rid of old computers or servers? Did you know that the components used in technology equipment are not landfill-safe? On top of the environmental hazards, unprotected e-waste typically contains a lot of confidential and private information in the form of saved passwords, Internet history and files left on the retired computer or server.

As a first prevention step, find a local recycling facility where e-waste can be safely disposed of. And make sure to take the following #1 security precaution before you haul it off: remove and destroy the hard drives. A drill and hammer usually do the trick just fine. Alternatively, many companies that shred paper documents will also destroy your hard drives.

Don't forget other e-waste such as mobile phones, copy machines and any other device that ever touched your company data. Give serious thought to what data is on any device before you recycle it.



1010 Lakes Pkwy
Lawrenceville, GA 30043

Inside This Issue

If You Think Your Business is Too Small To Be Hacked...You're A Cybercriminal's #1 Target

3 Reasons Why Recessions Are Awesome For Great Companies

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.