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 Advance Security: Move beyond outdated antivirus tools of the past.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

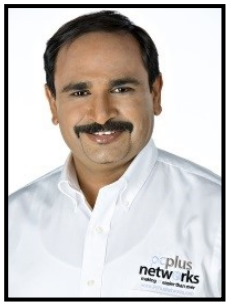
7. Encryption: Whenever possible, the goal is to encrypt files at rest and in motion.

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 anything of these, call us today!

October 2018



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!"

How To Make Sure You Never Fall Victim To Ransomware

Late last March, the infrastructure of Atlanta was brought to its knees. More than a third of 424 programs used nearly every day by city officials of all types, including everyone from police officers to trash collectors to water management employees, were knocked out of commission. What's worse, close to 30% of these programs were considered "mission critical," according to Atlanta's Information Management head, Daphne Rackley.

The culprit wasn't some horrific natural disaster or mechanical collapse; it was a small package of code called SAMSAM, a virus that managed to penetrate the networks of a $371 billion city economy and wreak havoc on its systems. After the malicious software wormed its way into the network, locking hundreds of city employees out of their computers, hackers demanded a $50,000 Bitcoin ransom to release their grip on the data. While officials remain quiet about the entry point of SAMSAM or their response to the ransom, within two weeks of the attack, total recovery costs already exceeded $2.6 million, and Rackley estimates they'll climb at least another $9.5 million over the coming year.

It's a disturbing cautionary tale not only for other city governments, but for organizations of all sizes with assets to protect. Atlanta wasn't the only entity to buckle under the siege of SAMSAM. According to a report from security software firm Sophos, SAMSAM has snatched almost $6 million since 2015, casting a wide net over more than 233 victims of all types. And, of course, SAMSAM is far from the only ransomware that can bring calamity to an organization.

If you're a business owner, these numbers should serve as a wake-up call. It's very simple: in 2018, lax, underfunded cyber security will not cut it. When hackers are

Continued on pg.2

Continued from pg.1

ganging up on city governments like villains in an action movie, that's your cue to batten down the hatches and protect your livelihood.

The question is, how? When ransomware is so abundant and pernicious, what's the best way to keep it from swallowing your organization whole?

1. BACK UP YOUR STUFF

If you've ever talked to anyone with even the slightest bit of IT knowledge, you've probably heard how vital it is that you regularly back up everything in your system, but it's true. If you don't have a real-time or file-sync backup strategy, one that will actually allow you to roll back everything in your network to before the infection happened, then once ransomware hits and encrypts your files, you're basically sunk. Preferably, you'll maintain several different copies of backup files in multiple locations, on different media that malware can't spread to from your primary network. Then, if it breaches your defenses, you can pinpoint the malware, delete it, then restore your network to a pre-virus state, drastically minimizing the damage and totally circumventing paying out a hefty ransom.

2. GET EDUCATED

We've written before that the biggest security flaw to your business

isn't that free, outdated antivirus you've installed, but the hapless employees who sit down at their workstations each day. Ransomware can take on some extremely tricky forms to hoodwink its way into your network, but if your team can easily recognize social engineering strategies, shady clickbait links and the dangers of unvetted attachments, it will be much, much more difficult for ransomware to find a foothold. These are by far the most common ways that malware finds it way in.

3. LOCK IT DOWN

By whitelisting applications, keeping everything updated with the latest patches and restricting administrative privileges for most users, you can drastically reduce the risk and impact of ransomware. But it's difficult to do this without an entire team on the case day by day. That's where a managed services provider becomes essential, proactively managing your network to plug up any security holes long before hackers can sniff them out.

The bad news is that ransomware is everywhere. The good news is that with a few fairly simple steps, you can secure your business against the large majority of threats.

> **"The question is, how? When ransomware is so abundant and pernicious, what's the best way to keep it from swallowing your organization whole?"**

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This report will outline in plain, nontechnical English common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
www.PcPlusNetworks.com/protect
or call our office at (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.

4 Ways To Keep Your Team Inspired

Entrepreneurs and business leaders often find that motivating team members is one of the most challenging parts of the job. Leaders seldom lack self-motivation — it's so second nature to them that they get frustrated when a team member doesn't appear to have the same level of drive and ambition.

One of the most frequently asked questions I hear from business leaders is "How can I motivate my team?" Imagine their surprise when I tell them, "You can't." My responsibility as a coach is to help company leaders grasp the underlying reasons for their own motivation and ensure that those reasons are consistent with the goals and objectives of their business. In the same way, leaders need to stop looking for ways to motivate and instead find ways to inspire team members to seek out their own motivation.

Business leaders must understand that team members will not always share their outlook or passion. Instead of forcing your will on others, use these four approaches to inspire motivation in your team.

1 Lead by example.
Show your team members how it's done, and dedicate yourself to showing your passion and motivation in everything you do. When your team members see your genuine excitement and enthusiasm, they'll be much more likely to increase their energy levels and get on board.

2 Honesty is the best policy.
It's vital that you be open and honest about the task at hand. You must get your team members to understand why the task is so important to you personally and to the company as a whole. Not every goal, task, or objective will foster the same amount of excitement and teamwork. If what you want is challenging or risky, let your team know. They'll respect your transparency and be more likely to trust you and your leadership.

3 Find balance.
There are two surefire ways to destroy motivation among team members. The first is micromanaging, and the second is being so hands-off that your team doesn't know what to do when problems arise. Give your team the freedom they need to feel empowered, but stay involved so that you can provide the necessary guidance when team members get discouraged.

4 Expect results and celebrate victories.
Before you give your team their marching orders, let them know you have confidence in their abilities. Take time to explain why a successful outcome is important to you and the business. They'll be more likely to meet your expectations, not because they're doing it for your sake, but because they're working harder for the benefit of the team as a whole.

It's crucial to celebrate wins with the team and to express your appreciation. An individual reward can be a great motivational tool, but it's just as important that you celebrate as a team.

~ Andy Bailey is the founder, CEO and lead business coach at Petra

IT Security Tip: Never use **PERSONAL** devices to connect to **COMPANY** data

You're a hardworking team player who likes to check e-mail and get a few things done after hours – all good! But here's something you might not know: you should never access company data, file servers or applications through personal devices and home PCs that are not properly monitored by us. Why? If you and your kids are using a home PC to play games, access Facebook and surf the web **AND** you're not diligently updating and monitoring the antivirus software, firewall and security patches on the machine (and who does, honestly?), then there's a high probability you're infected with spyware or malware. Since most malware is designed to operate in total stealth mode undetected, you won't know that some hacker is watching you log in to your company's file server or key cloud application containing critical, sensitive data and capturing your login with a key logger. Bottom line, **ONLY** use company-approved devices that are properly protected and monitored to access company data; and if you just can't help but take work home, let us know so we can set you up with a **SECURE** way to work remote or from home.

pcplus networks
better people, better solutions

2775 Cruse Rd. Suite 2203
Lawrenceville, GA 30044

Inside This Issue

2 Sneaky Ways Hackers Will Rob You Blind

We've said it before and we'll say it again: cyber-attacks aren't limited to big corporations and government organizations. Verizon's 2018 Data Breach Investigations Report states that 58%of data breaches in 2017 occurred at small businesses. And according to Verizon's data, there are two specific hacking techniques on the rise today that small businesses should know about.

The first technique is point-of-sale (POS) system hacking. If you're in the hospitality industry, this should definitely be on your radar. Verizon recorded 368 POS incidents in 2017, most instigated by hackers penetrating the system rather than employees making mistakes that opened up vulnerabilities. Usually, hackers will steal credentials directly from a POS service provider, which enables them to exploit the POS systems used by that provider's customers.

The second is called financial pretexting. Instead of phishing a business and installing malware, attackers impersonate a high-level employee within an organization — often using a legitimate but compromised e-mail account — to steal funds or sensitive information from the company's finance or HR department. As always, forewarned is forearmed. Equip your teams with the know-how to avoid these scams and you will be ahead of the game. *SmallBizTrends.com, 5/1/2018*

Top Training Tips To Improve Your Team's Customer Satisfaction Skills

When customers leave dissatisfied after interactions with your business, the problem is likely more systemic than you realize. It can be hard to get a handle on poor customer satisfaction, but one of the best ways to address it is through comprehensive onboarding and training programs for your employees.

Don't make training a grueling info dump — the human mind can take in only so much data at once. It's best to split up your training programs into manageable chunks to ensure all the information gets absorbed. And give employees the tools to manage their own training. The ability to dip in and out of training modules allows them to move at their own pace, which greatly increases retention rates. Most importantly, don't waste your employees' time with big, clunky meetings, when individually tailored programs will suffice. *SmallBiztrends.com, 7/20/ 2018*