MASTER COMPUTING

Secure Connection

"Insider Tips To Make Your Business Run Safer, Faster, Easier and Profitably"

Tech Tip

Home Office Security

It may come as a surprise, but working remotely can be just as (or more) secure than working in the office. If done right.

Those are the three operating words: if done right. This takes effort on the part of both the business and the remote employee. Here are a few MUST-HAVES for a secure work-from-home experience:

Secure networks. This is non-negotiable. Every remote employee should be connecting to a secure network (at home, it should be WPA2 encrypted), and they should be doing so with a VPN.

Secure devices. All devices used for work should be equipped with endpoint security – antivirus, anti-malware, anti-ransomware and firewall protection. Employees should also only use employee-provided or approved devices for work-related activity.

Secure passwords. If employees need to log in to employer-issued programs, strong passwords that are routinely updated should be required. Of course, strong passwords should be the norm across the board. *Entrepreneur, June 17, 2020*

November 2020

MC University

97%

of Cybercrime could have been prevented with basic security measures. We'll give you the formula and coach you through the implementation.
Register now for our Upcoming Live Webinar at:

MasterComputing.com/Live-Webinars

Just The Facts

by
Justin Shelley
CEO, Master Computing

4 Questions Your IT Services Company Should Be Able To Say "Yes" To

Out with the old and in with the new! For far too long, small businesses have taken an old-school approach to IT services and security. In other words, they wait until something goes wrong before they call an IT services company and request help.

Back in the day (think 1990s and 2000s), this approach worked, more or less. External threats, such as hackers and viruses, were still few and far between. A data breach wasn't on anyone's mind. So, it made sense to wait until something went wrong before taking action.

In IT circles, this is known as the "break-fix" approach. Something breaks, so someone has to come in to fix it. And they charge for their services accordingly. If something small breaks and it takes a short time to fix, you could expect a smaller bill. If something big breaks, well, you can expect a pretty hefty bill.

The break-fix approach is 100% reactive. As many businesses have learned, especially in more recent years, as the number of threats have skyrocketed, it can get very expensive. IT specialists are an in-demand field. With just about every business relying on the Internet and Internet-connected devices in order to operate, there's a lot of opportunity for something to go wrong.

This is exactly why you can't rely on the reactive break-fix model anymore. If you do, you could be putting your business at serious risk. In some cases, the mounting costs and damages done could put you out of business.

If you're hit by a data breach or if a hacker infiltrates your network (which is a common occurrence), what's next? You call your IT services partner – if you have a partner – and tell them you need help. They might be able to restore lost or stolen data. That is, if you routinely backed up that data. You don't want to find yourself in this position.

And you don't have to.

Continued on Page 2

Continued from Page 1

Instead, take a proactive approach to your IT support and security. This is the new way of doing things! It's also known as managed services – and it's a far cry from the break-fix approach.

If you work with an IT services company that only comes out when something breaks, it's time to get them on the phone to ask them four big questions. These are questions they absolutely need to say "yes" to.

1. **Can you monitor our network and devices for threats 24/7?**
2. **Can you access my network remotely to provide on-the-spot IT support to my team?**
3. **Can you make sure all our data is backed up AND secure?**
4. **Can you keep our network protected with up-to-date malware solutions, firewalls and web filtering?**

If your IT services partner says "no" to any or all of these questions, it might be time to look for a new IT services partner.

"When things go wrong, and these days, things will go wrong, you'll be left with the bill – and be left wishing you had been more proactive!"

If they say "yes" (or, even better, give you an emphatic "yes"), it's time to reevaluate your relationship with this company. You want to tell them you're ready to take a proactive approach to your IT support, and you'll be happy to have them onboard.

Far too many small businesses don't bother with proactive support because they don't like the ongoing cost (think of it as a subscription for ongoing support and security). They would rather pay for things as they break. But these break-fix services are more expensive than ever before. When things go wrong, and these days, things will go wrong, you'll be left with the bill – and be left wishing you had been more proactive!

Don't be that person. Make the call and tell your IT services provider you want proactive protection for your business. Ask them how they can help and how you can work together to avoid disaster!

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To get started and claim your free assessment now, call our office at (940) 324-9400

Top Tips On How To Prevent Your Smart Cameras From Being Hacked

Smart cameras have been under attack from hackers for years. In fact, one popular smart camera system (the Amazon Ring) had a security flaw that allowed hackers to get into homeowners' networks. That issue has since been patched, but the risk of being hacked still exists. Here are three ways to keep your camera (and your network) safe from hackers:

1. Regularly update your passwords. Yes, passwords. This includes your smart camera password, your WiFi network password, your Amazon password – you name it. Changing your passwords every three months is an excellent way to stay secure. Every password should be long and complicated.

2. Say no to sharing. Never share your smart camera's login info with anybody. If you need to share access with someone (such as a family member or roommate), many smart camera systems let you add a "shared user." This will let them access the camera, without the ability to access the camera's configuration or network tools.

3. Connect the camera to a SECURE network. Your smart camera should only be connected to a secure WPA2 encrypted, firewalled WiFi network. The more protection you put between the camera and the rest of the digital world, the better. *Digital Trends, May 7, 2020*

4 Steps To Move Your Business From Defense To Offense During Times Of Disruption

"Everyone has a plan until they get punched in the mouth." –Mike Tyson

As business leaders, we've all been punched in the mouth recently. What's your new game plan? Since COVID-19, the annual or quarterly one you had is now likely irrelevant. You have two options:

1. Sit and wait for the world to go back to the way it was, a place where your plan may have worked (and let's face it, that's not happening).
2. Create and act upon a new game plan. One that's built to overcome disruption and transform your business into something better and stronger.

Option Two is the correct answer! AND, we at Petra Coach can help.

At Petra Coach, we help companies across the globe create and execute plans to propel their teams and businesses forward. When disruption hit, we created a new system of planning that focuses on identifying your business's short-term strengths, weaknesses, opportunities and threats and then creates an actionable 30-, 60- and 90-day plan around those findings.

It's our DSRO pivot planning process. DSRO stands for Defense, Stabilize, Reset and Offense. It's a four-step process for mitigating loss in your business and planning for intentional action that will ensure your business overcomes the disruption and prepares for the upturn — better and stronger than before.

Here's a shallow dive into what it looks like.

Defense: A powerful offensive strategy that hinges on a strong defense. Identify actionable safeguards you can put in place. The right safeguards act as the backbone of your company, giving you a foundation you can count on.

Stabilize: The secret to stabilization is relentless communication with everyone. That includes internally with your teams AND externally with your customers. Streamline communication and eliminate bottlenecks through a visual dashboard.

Reset: By completing the first two steps, you'll gain the freedom to re-prioritize and focus your efforts on the most viable opportunities for growth.

Offense: Don't leave your cards in the hands of fate. Shifting to offense mode gives you the power to define the future of your business. Equip yourself with the tools and knowledge to outlast any storm.

Interested in a deep dive where a certified business coach will take you (and up to three members from your team) through this process? Attend Petra's DSRO pivot planning half-day virtual group workshop. (We've never offered this format to non-members. During this disruptive time, we've opened up our coaching sessions to the public. Don't miss out!)

When you call a time-out and take in this session, you'll leave with:

- An actionable game plan for the next 30, 60 and 90 days with associated and assigned KPIs
- Effective meeting rhythms that will ensure alignment and accountability
- Essential and tested communication protocols to ensure your plan is acted upon

I'll leave you with this statement from top leadership thinker John C. Maxwell. It's a quote that always rings true but is crystal clear in today's landscape: "Change is inevitable. Growth is optional."

Let that sink in.

Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multimillion-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational BS faster than a hot knife through butter.

Business Security Podcast

"Stupid… or Just Irresponsible?" Ep. 8: How To Protect Against Ransomware

Below are the show notes for Master Computing's Business Security Podcast, "Stupid...or Just Irresponsible?" Episode 8: How To Protect Against Ransomware. You can hear the live version on our website: MasterComputing.com/Podcasts. You can also subscribe and listen on your favorite streaming platform: Spotify | Apple Products | Google Podcasts

In this episode we cover:

- What NOT to do if you want any hope at protecting against ransomware.
- The background story of this virus (P.S. this is almost as interesting as the actual exploit itself)
- How ransomware works - paralyzing machines and demanding bitcoin ransom, WannaCry jumping from one machine to the next
- The 5 different stages of this malware spread

Why cybersecurity researchers named the worm "WannaCry"

Not too long ago, the WannaCry ransomware attack was all over the news, infecting over 400,000 computers. The threat was straightforward: Pay us or we'll erase your files.

Ransomware, like the WannaCry attack, works by encrypting your files to prevent you from using or accessing them. After your files are compromised, the hackers behind the attack then pop up a demand screen asking for payment within a set time frame (e.g., 72 hours, three days, etc.) in order to get the key to decrypt your files. WannaCry forced many business owners to lose data or pay up since there was no other way to decrypt the files – and many paid without getting their files back.

Obviously, the best way to foil a ransomware attack is to be incredibly diligent about IT security; but with hundreds of thousands of new attacks being created daily, there are no guarantees that you won't get infected. Therefore, it's critical to maintain a full, daily backup of your data so you never have to pay the ransom – AND your backup needs to be a professional-grade backup that is impervious to ransomware since hackers write their attacks to infect BOTH your PC/server AND your backups.

SHOW NOTES:

- Joe tells the story of WannaCry Ransomware **(5:00)**
- How did this worm get the name "WannaCry"? **(5:50)**
- The background story of this virus **(6:10)**
- How did this virus start? (Hint: your employees are your weakest security link!) **(6:25)**
- The different stages of ransomware: **(6:50)**
  1. Initial access
  2. Execution
  3. Escalation
  4. Defense evasion – hiding around from your antivirus
  5. Then the exploit, the impact
- **Stupid:** When it comes to cyber security stupid is thinking you can DIY. Thinking you can protect your business from these hackers by yourself. *"Thinking you can do this yourself, that cyber security is a DIY type activity is flat stupid"* **(16:00)**
- **Irresponsible**: Is trusting your IT company / cyber security firm WITHOUT VERIFYING. **(16:55)**
- **The DIY approach to security** - we are going to talk about DIY first to make the point we are giving this formula NOT as a formula to do it yourself, but to rate your current support system. Then, if these things aren't happening you know you've got to do something different now! **(20:00)**

If you can't *easily* answer these questions about the things happening in your company, *you have a problem*! **(20:17)**

- **Top 9 ways to protect against ransomware: (21:40)**

Book A 10-Minute Discovery Call: Please take a second and go to mastercomputing.com/discovery, book a 10-Minute call and we'll make sure you are properly protected and have a plan in place.

DISCOVERY CALL

We'll take 10 minutes to ask some key questions and answer any of yours, to find out if we're a good fit.

ASSESSMENT

Our 27-point network health and security assessment will help us build the perfect technology roadmap for your organization.

ROADMAP

Buy it from us, or buy it from somewhere else, but this is the path to success. We put all our cards on the table.

ACCOUNTABILITY

Through our live-data portal, regular meetings, and complete transparency, you will always know we deliver on our promises.

Don't wait, go to MasterComputing.com/Discovery to book your 10-minute discovery call today!