Secure Connection

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

Tech Tip

Secure Transportation

Taking work home has become a new way of life for many of us. While transporting equipment or paperwork may seem simple, there are many security precautions you should take in to account.

1) Before taking anything out of the office, get approval from your supervisor. Make a list of what you are taking and when you are taking it for your reference.
2) Prior to transport, make sure you are physically securing and locking devices. Keep them locked in the trunk of your car if possible.
3) Avoid making unnecessary stops when traveling with sensitive data. Leaving items unattended could leave them vulnerable to theft.
4) When you do make it to your final destination, continue maintaining physical security and keep devices locked whenever possible.

Key Point: Cybercriminals don't need any sophisticated hacking skills to steal items from a vehicle.

October 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

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 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

Continued on Page 2

Continued from Page 1

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! Master Computing is now offering new Managed Service programs to our clients. Think about how much time you spend taking care of your IT issues. These programs are designed to handle all of that for you by managing the day-to-day IT responsibilities and freeing up ***your*** time for running ***your*** business.

Master Computing will manage the training of your staff to make sure they are aware of the threats they may be exposed to daily. We will interface directly with your staff and share information, tips, and tests to make sure they are cybersecurity savvy. You can rest assured knowing that you are in compliance and that your office is more productive.

> ***"Master Computing will manage the training of your staff to make sure they are aware of the threats they may be exposed to daily."***

In addition to the Cybersecurity Training, we offer Managed Productivity Training in the MS Office Suite for Office 365 with both Mac and PC versions available. Available training includes, but is not limited to: Word, Excel, PowerPoint, Outlook, OneNote, SharePoint, OneDrive, and Teams.

We also offer "Done For You" IT Policies and Procedures. We handle the process and you can rest assured that you have up-to-date documentation in your files. The following polices and procedures are included: Disaster Recovery and Backup, Incident Response Plan, Data Disposal Procedure and Policy, Acceptable Use Policy, Vendor/3rd Party Management, Remote Access, Network Security and Access Control.

If you would like to find out more about the new Managed Services programs, please give us a call at **940-324-9400** or schedule a 10-minute discovery meeting at:

MasterComputing.com/Discovery

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

5 Easy Things You Should Do To Protect Your Business Now

1)Review Your Business Insurance. Most businesses carry some type of general liability insurance that would pay them if their building and the things in it were damaged. However, many businesses do not have enough coverage to replace all the computer equipment and devices, desks, art, supplies, and other things they've accumulated over the years that are housed in their office. Make sure you review your policy every year and keep in mind new additions and assets you've accumulated during that year.

2)Consider Cloud Computing. One of the biggest advantages of cloud computing is that your data and assets are stored off-site in a highly secure, high-availability data center, with failover and redundancy built in. That means that if your building was destroyed and you had to evacuate, or if your server melted down due to an unexpected hardware failure, everything you've worked so hard to create over the years is safe and not a sitting duck in your unsecured closet or server room.

3)Secure Your Data. Making sure that your data is protected from theft is a never-ending battle you don't want to lose. Companies that get hacked and expose sensitive client and employee data can face severe penalties, lawsuits, and massive loss of credibility in the marketplace. Make sure you never have to send an e-mail to your customers explaining the bad news that a hacker accessed their info through you. Further, if you keep any sensitive information (even passwords to portals containing sensitive information) on portable laptops, phones, and other devices, make sure you have a way of controlling and safeguarding that information.

4)Write A Simple Disaster Recovery Plan. The key word here is "simple." If your plan gets too complicated or difficult, you won't do it. But at a minimum, think of the disaster that is most likely to happen and that would have a severe and negative impact on your company's survival.

5)Review Your Employee Internet Policy. With so many people "addicted" to Facebook and Twitter, it's important that your employees know where the line is and what they can and can't post online. We also recommend content-filtering software to block content and web sites you don't want employees visiting during work hours.

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

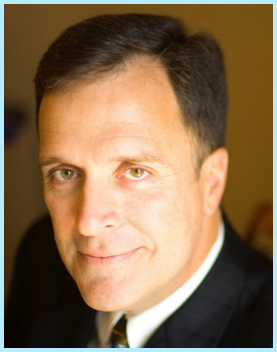
are invested wisely, the organization also achieves great success. By putting the time and expertise into your team members, you can motivate them to improve in their roles.

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, CSP, CPAE, is the President of Sanborn & Associates, Inc., an "idea studio" that seeks to motivate and develop leaders in and outside of business. He's the best-selling author of books like Fred Factor *and* The Potential Principle *and a noted expert on leadership, team building, customer service and company change. He holds the Certified Speaking Professional designation from the National Speakers Association and is a member of the Speaker Hall of Fame. Check out any of his excellent books, his video series "Team Building: How To Motivate And Manage People" or his website, marksanborn.com, to learn more.*

Business Security Podcast

"Stupid… or Just Irresponsible?" Ep. 6: 100% of Law Firms Targeted by Cyberattacks

Below are the show notes for Master Computing's Business Security Podcast, "Stupid...or Just Irresponsible?" Episode 6: 100% of Law Firms Targeted by Cyberattacks. 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

EPISODE SHOW NOTES:

Today's episode we talk about a security magazine study. In this study they show that 100% of law firms have been attacked or targeted between January - March of 2020. **[2:30]**

You are probably thinking "100%? That is B.S." right? In this study they are talking, specifically, that the Legal Industry is under attack. They make it sound like more so than anybody else. **[3:40]**

We **could do our own study and show that EVERYBODY is under attack 100% of the time** - *It is a matter of time before they get in,* that's the bigger point here.

Interesting statistics from this study: [4:07]

- **15%** of law firms were likely **compromised** (that's a lot)
- Nearly **HALF of law firms** had some other form of **suspicious activity on their network.**

The **problem we face in security** is that **it is just rampant**, the **attacks are everywhere**. They are **automated**. They are relatively **easy to pull off**. **[5:58]**

"**As a business owner** (*theoretically say I do not own an IT company or have any experience in IT)*. Maybe I own a law firm and I am the managing partner of the Law firm. Maybe I'm the primary doctor or physician at a local clinic. Maybe I own an accounting firm. I am the guy, I started it, I filed all the paperwork and my specialty is in my craft… **How do I prevent a cyber-attack, Joe?" [7:30]**

What To Look For In IT Support As A Business Owner: Businesses operate on some slim margins. So, when I'm out **looking for tech support** and 3 people show up at my door saying hey, we can all do the same thing, **how do I choose? [8:20]**

Cyber Security is more of a **specialty**. Whereas IT consultants are kind of generalist – think of your family physician.

As a business owner, as a managing partner at a law firm, as the practice manager who is responsible for the clinic. **When somebody gets hit, that falls on YOU.**

"The problem here like I said in the beginning, I don't know how to vet an IT company, and I sure as hell don't know how to vet a cyber security firm." **[13:07]**

Let's say, we **hired this firm to come protect our company.** If we were going to make sure they were doing their job properly, **what should we be looking for? [13:25]**

Let's go through a basic checklist of **what should be happening behind the scenes to protect a company.** Starting at the top: **[14:57]**

- We want to make sure they have strict **policy** on of use of company devices.
- **Procedures** – have a document in place
- Have regular **training**/education for employees for safest and best practices.
- **Ongoing education**
- **Letting the client know** if information has been compromised **immediately.**
- You SHOULD **have an incident response plan** for if and WHEN you get hit. What are the proper procedures?
- Constantly **updating security** and **hiring digital security firm** if needed.
- Like we mentioned earlier, if you have an IT guy that's great, but you **NEED a s*ecurity* guy.**
- You have got to have somebody or some entity that is looking out for security, that stays in on this, that is just living and breathing network security all the time. Like us!

If you were to be **compromised** there should be a ***policy*** and it should be ***enforced*****. [18:05]**

Quick point about Two Factor Authentication: If your IT guy if your security guy isn't talking to you and beating you up over Two Factor Authentication (2FA) then you probably better find a new one!

Here is a great litmus test: If you aren't annoyed as hell at your IT company for all the security stuff and hoops you are jumping through…you better find a different one! [20:40]

Justin's sign off: The stupid answer here is to not be prepared. To not be paying attention to this. To thinking that you are invulnerable. **To think that this isn't going to happen to you is *asinine,* I mean 100%.** It is rare that we can say 100% on anything, but the fact that you are being actively targeted right now is 100%. **[21:45]**

Go towww.MasterComputing.com/Discovery and book a 10 minute call, and we will talk about this, we will create an ACTION PLAN for you. If you're not ready to take that step then go to www.MasterComputing.com/live-webinars. **[22:30]**

Joe shares his final words of wisdom for our listening audience: **Change your passwords** - Everybody just go change your password real quick. Reset it. **[23:10]**

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!