MASTER COMPUTING

Secure Connection

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

December 2020

Just The Facts

by
Justin Shelley
CEO, Master Computing

A CEO's Nightmare

The other night I woke up in a state of hysteria. You see, I'm a vivid dreamer. When I wake up from a dream it can take me several minutes to gather my senses enough to realize I was dreaming. That transitional state can be hell. This was one of those times.

Have you ever been asked, "What keeps you up at night?" It's a common question that gets asked in market research. When I'm putting together a marketing campaign, I want to make sure I'm speaking your language. I want to know that I'm addressing a real problem, and offering a real solution. This is why we post our Average Response Time right on the front page of our website. It's also why some of our prospects received a stopwatch in the mail a few weeks ago with a note that said, in effect, "Click start, call our helpdesk, and click stop when you are talking with a qualified technician". Because this is *your* language. With very few exceptions, when we pick up a new client one of their primary complaints is that their current IT provider doesn't respond quickly enough. It can take hours, sometimes days. I've heard horror stories of waiting a week or more to get a response to a technical crisis. You simply can't run an efficient business that way. You need the right solution, and you need it right now! Am I wrong?

But oddly enough, that isn't our primary deliverable. Don't get me wrong, we're damn good at responding quickly. That number on the website is real data, it's not a marketing number. We have bad days, we experience perfect storms, and sometimes our response time creeps up into the double digits. But we watch it like a hawk, and our target is 9 minutes or less. If you take me up on the stopwatch test you'll realize that it only takes a few seconds to reach one of our techs. But the average number we report on includes requests that come in through email, our web portal, etc. The phone is always answered live.

These quick response times are a product of internal processes. Now we're getting closer to our primary service deliverable. We are fanatics about process. We follow checklists

Continued on Page 2

Monthly Tech Tip

QR Codes

Anyone can create a QR Code and they are rapidly becoming increasingly popular. Scammers are taking advantage of this opportunity and are using QR codes as a tool to reach victims that may be unaware of the risks involved.

Cybercriminals can easily set up a webpage to be anything they want, fast and free. Victims can be tricked into thinking they are on a legitimate page only to realize that they have been tricked and shared personal information or downloaded a virus. To help reduce the risk of this happening, be sure to keep your personal devices updated with the latest software updates.

Not all QR Codes are scams. But, since they are growing in popularity, it is important to be cautious. Think twice before scanning, just like you would with a suspicious link. For physical QR codes, watch for tampering, such as a new code placed over the original.

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. **Contact us today. Sleep soundly tonight. Go to:**

MasterComputing.com/Discovery

MasterComputing.com
940-324-9400

Continued from Page 1

and Standard Operating Procedures (SOPs) for almost everything, and we're constantly reviewing them to look for possible improvements. When I look you in the eye and tell you that we will solve your technology problems before you even know you have them, I can prove it by slapping down a document detailing our procedure to do just that. Here again, this isn't marketing hype or a sneaky sales tactic. It's simply how we do business.

Still, not our primary deliverable. These standardized processes are something I'm quite proud of, and you'll love us for it as a client, and you might even *think* this is where we shine as a company. Semantics… Because we do shine here. And clearly I'm OK bragging about it. But what is our true deliverable?

We exist as an organization for the sole purpose of keeping you in business. Keeping your doors open. Our fanaticism around process and response times conveniently keeps your business running smoothly, keeps you efficient, keeps you profitable, and keeps you and your staff happy. This is the deliverable you'll notice. But here's what I never hear when I'm doing market research:

> ***But I am here to tell you that our #1 deliverable is keeping you in business****. Our deliverable is* ***preventing*** *my nightmare from becoming your reality.*

"I'm worried that we will get hit by a cyber-attack that will completely wipe out our organization, forcing us to close our doors forever. I'm worried I could lose this business I've built from the ground up. I'm worried I'll be looking for a job next week." I don't hear that. At best I'll hear: We need to be HIPAA compliant, NIST compliant, PCI compliant, etc. Or, "we're concerned about security". But I don't think many CEOs, practice managers, managing partners (insert your title here) truly understand the gravity of the *real* risk we face every day of our lives. We (and our organizations) are all one mistake away from complete collapse.

THIS is why I woke up in a state of hysteria the other night. In my very vivid dream my company was hit with a ransomware attack that left us completely crippled. Every computer, every server was locked. In my dream there was no path to recovery. In my dream, the backups were corrupted right along with the servers and workstations. When I woke up, the last line from my dream that was on repeat in my head was me yelling, "DO WE HAVE BACKUPS?!? DO WE HAVE BACKUPS?!?" I was asking it, but I knew the answer. And it wasn't pretty. In my transitional state between sleep and reality, the gig was up. I was looking for a job.

Thank God that was a dream. The true nightmarish element is that every part of that dream is perfectly plausible. Cyber-attacks are rampant. They are a daily occurrence. They are only getting worse. What makes this nightmare even worse is that it is *NOT* a primary concern for many of our prospects. Look at our website. We talk about response times, compliance, our processes, and we mention security. But there is zero mention of going out of business. Because market research doesn't support that verbiage. ***But I am here to tell you that our #1 deliverable is keeping you in business***. Our deliverable is ***preventing*** my nightmare from becoming your reality.

If someone asks me, "What keeps you up at night, Justin?" My answer 100% of the time will be: cyber-attacks. Because this is the world I live in. I see it on almost a daily basis. I truly lose sleep over this. I love that our response times are quick, I love our processes and procedures. But we *deliver* a good night's sleep.

We exist as an organization to keep you in business.

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.

Contact us today. Sleep soundly tonight.

Protect Your Information During the Online Holiday Shopping Season

Shop reliable websites, and get there safely. Don't be fooled by the lure of great discounts by less-than-reputable websites or fake companies. Use the sites of retailers you know and trust, and get to their sites by directly typing a known, trusted URL into the address bar instead of clicking on a link.

Beware of seasonal scams. Fake package tracking emails, fake e-cards, fake charity donation scams, and emails requesting that you confirm purchase information are particularly common this time of year. Use known, trusted URLs instead of clicking on links.

Always think twice before clicking on links or opening attachments -- even if they appear to be from people you know, legitimate organizations, your favorite retailers, or even your bank. Messages can easily be faked. Use known, trusted URLs instead of clicking on links. And only open known, expected attachments. **When in doubt, throw it out!**

Keep software up to date! Before searching for that perfect gift, be sure your device, apps, browser, and anti-virus/anti-malware software up to date.

Protect your passwords. Make them long and strong, never reveal them to anyone, and use multi-factor authentication whenever possible.

Check your credit card and bank statements regularly. These are often the first indicators that your account information or identity has been stolen. If there is a discrepancy, report it immediately.

Wi-Fi hotspots & public computers. Treat all Wi-Fi hotspots and public computers as compromised, even if they appear to be safe. Limit the type of business you conduct on them, including logging in to email and banking, and shopping. And set your devices to "ask" before joining new wireless networks so you don't unknowingly connect to an insecure or fraudulent hot spot.

Gift Cards. Be wary of anyone asking for payment with a gift card. Once paid, there is not a way to trace the funds and your money will be gone.

Cybercriminals Confess

The Top 3 Tricks And Sneaky Schemes They Use To Hack Your Computer Network That Can Put You Out Of Business

Cybercriminals and hackers are rarely shy about the methods they use to attack their victims. Many of them are more than happy to share how they broke into a business's network or how they walked away with thousands of dollars after successfully extorting a business owner whose company is now destroyed.

There are new stories out there to get your blood boiling as cybercriminals work to ruin people's lives and livelihoods. These criminals don't care what kind of damage they do. They only care about one thing: money. If they can get away with it – and many do – they'll keep on doing it.

It's up to the rest of us as business owners (and employees) to stay at least one step ahead of these cyberthugs. The single best way to do that is to **stay educated on the latest threats.** The second-best way is to **stay up-to-date with the latest technology designed to combat cyber-attacks.**

Here are three tricks of the trade cybercriminals are using right now in an attempt to get their hands on your money:

1. Ransomware. This is very common. It's a form of malware, and it can sneak onto your network and into your computers in a number of different ways:

— Ad Networks. These ads can appear on social media sites and on familiar websites. Someone clicks a compromised ad or pop-up, and it initiates a file download. It's quick and it can be confusing. This is where anti-malware and anti-ransomware come in very handy.

— Malicious Links. The cybercriminal sends you a legitimate-looking e-mail, supposedly from your bank or a familiar online store. It may even be disguised as an e-mail from a colleague. The e-mail contains a link or file. If you click the link or file, it installs the ransomware.

— Hidden Files On Thumb Drives. This happens way too often where someone brings a thumb drive from home. While the user doesn't know it, the drive has a malicious file on it. When the thumb drive is inserted into a networked machine, the file is installed.

No matter how the ransomware gets onto your devices, the result is basically the same. The ransomware goes to work and begins encrypting your files. Or it may completely block you from accessing your computer altogether. You'll get a full-screen message: *Pay up or never access your files again.* Some ransomware programs threaten to delete all of your files. Others say they will never restore access.

2. DDoS Extortion. Short for distributed denial of service, DDoS attacks are a relatively easy way for hackers to take down your business's online presence and wreak havoc on your network. These attacks mimic online users and essentially "flood" your network with access requests. Basically, it's as if millions of people were trying to access your website at once.

Your network simply can't handle that kind of traffic and, as a result, it goes down. The hackers can continue the attacks until you take action. That is to say, until you pay up. If you don't pay up, the hackers will do everything they can to keep you offline in an attempt to destroy your business. If you rely on Internet traffic, this can be devastating, which is why many businesses end up paying.

3. Direct Attacks. Some hackers like to do the dirty work themselves. While many cybercriminals rely on bots or malware to do the work for them, some hackers will see if they can break through your network security in a more direct way. If successful at breaking in, they can target specific files on your network, such as critical business or customer data.

Once they have the valuable data, they may let you know they have it. Sometimes they'll ask for money in return for the sensitive data. Sometimes they won't say anything and instead simply sell the data on the black market. Either way, you're in a bad position. A criminal has walked away with sensitive information, and there is nothing you can do about it.

Except, that last sentence isn't true at all! There *are* things you can do about it! The answer is preventative measures. It all comes around to these two all-important points:

- Stay educated on the latest threats
- Stay up-to-date with the latest technology designed to combat cyber-attacks

If you do these two things and work with an experienced IT services company, you can change the outcome. You can put the cybercriminals in their place and have a digital defense wall between your business and those who want to do your business harm.

HAPPY HOLIDAYS!

From everyone at Master Computing, we wish you a happy and healthy holiday season. 2020 was, to say the least, a challenge and we are thankful for the ongoing support and goodwill shared with our family and friends.

We look forward to 2021 and the possibilities it will bring.

Cheers!!

Business Security Podcast
"Stupid… or Just Irresponsible?" Ep. 11: Fire Alarms & Bookmarks"

Below are the show notes for Master Computing's Business Security Podcast, "Stupid...or Just Irresponsible?" Episode 11: Fire Alarms & Bookmarks. 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

SHOW NOTES:

Here's a sneaky trick used by many hackers: they purchase and set up a fraudulent website that is a close misspelling of a legitimate one. Example: www.faceboook.com (extra "o") or www.dropbox.net (net instead of .com). All you have to do is accidentally fat-finger ONE letter in the URL and up pops a very legitimate-looking fake copy of the site you were trying to get to – and the login and links are full of keylogger malware and virus landmines waiting for you to click on them. This is particularly important for any social networks you belong to.

Tip: Bookmark key sites you frequently visit. But even better, have us install a web gateway security product that BLOCKS sites that are suspicious and fraudulent. That way, even if you click on a link to a phishing site, get directed to an infected site or accidentally type in the wrong URL, the site will be blocked, protecting you and your employees.

We are going out of order today. Rather than end with our offer, we are going to start with it. The reason is, I feel over the last couple episodes I've gone soft. **[2:00]**

Justin asks Joe some questions:

What's the title of this podcast? Do you remember why we name it Stupid or Irresponsible?**[3:35]**

When I decided to call the podcast "Stupid or Irresponsible" I did it on purpose. To be inflammatory with the topic. I wanted to get people's attention, because this is one of those things we CAN'T take lightly. We can't just sit around and hope we don't get hit with ransomware, hope we don't get hacked by criminals in China and Russia.

Here's what's stupid: Putting fire alarms in your house AFTER having a fire. The most frequent sales of fire alarms are after people had a fire. **[5:10]**

When we are selling cybersecurity services, unless someone has had some sort of a cyber security event, they are very unlikely to buy.

What's STUPID is waiting for the event to happen and then taking preventive measure to prevent the event that just happened. **[5:25]**

If something doesn't cause emotional response in us, we don't take action. So yes, listeners, we are trying to scare you but trying to scare you in a way that will PREVENT something that is catastrophic. **[9:50]**

We are going in a little reverse order, before we even dig into our topic , we are going to talk about this offer for a free Security Assessment. **[11:10]**

How do I get my FREE Business Security Assessment?

Book a 10-Discovery call – jump on the phone, spend 10 minutes with Justin Shelley, CEO of Master Computing.

During this assessment, I will ask you some very *key questions*, and in just 10-minutes I can tell you what we need to do... A roadmap to success. 100% free.

What is a Key Question I will ask you in Discovery Call?

One of the very first questions I ask is if you are doing a regular consistent end-user education? Are your employees constantly going through some sort of cyber security program, and if they are, who is running it? When was the last time you went through an employee training program?

Go to MasterComputing.com/Discovery and book a 10-minute call before it's too late!

Justin gives Joe a POP QUIZ: **[13:00]**

How much does this Security Assessment I offer cost?

How many strings are attached?

Will we try to sell you something you don't need?

Does anyone ever complain about me, Justin, being a high-pressure salesperson?

What is stupid: Buying a fire alarm after your house is burned down. Guys don't wait. Please do not wait until you've been breached, hit with ransomware, until your business is vaporized. Because a lot of businesses aren't coming back from these attacks. They're brutal. **[32:55]**

A few simple measures. We can provide a roadmap that can protect you from 97% of this stuff.

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!