BERTIGROUP
MANAGED IT SERVICES

BERTIBRIEF

April 2020, Issue #21

In This Issue

P. 1 Employees Are Letting Hackers Into Your Network By Doing These 5 Things…Here Is What You Can Do To Stop It !

P. 2 4 Cyber Security Myths Business Owners Need To Know

P. 2 Top Tips For Making The Most of Your Small-Business Technology

P. 2 3 Things Mentally Strong People Don't Waste Doing

P. 3 Anticipating Customer Needs

P. 3 Benefits of A Mastermind Group

P. 3 How To Spot Phishing Email

P. 4 Anticipating Customer Needs Cont'd

P. 4 Employees Are Letting Hackers Into Your Network Cont'd

"Well, it's not the worst I've seen."

Employees Are Letting Hackers Into Your Network By Doing These 5 Things … Here Is What You Can Do To Stop It !

If you run a small business, you are a target for cybercriminals. At this point, it's just a fact of life. Hackers, scammers and cybercriminals of all kinds target small businesses because they are plentiful, and more often than not, they lack good cyber security (if they have any at all). Here's the kicker: these criminals don't need to use malicious code or advanced hacking skills to get what they want. In reality, many of them target your biggest vulnerability: your own employees.

It's a sad truth, but every day, employees of small businesses let hackers right in because they don't know better. They see an email from the boss, open it and click the link inside. By the time they realize they've made a mistake, they're too embarrassed to say anything. From there, the problem gets worse. Actions like this can end in DISASTER for your business.

The problem is that most employees don't have the training to identify and report IT security issues. They aren't familiar with today's threats or they don't know to not click that email link. There are many things employees are doing – or not doing – that cause serious problems for small-business owners. Here are five things people do that allow hackers to waltz in through your front door. Cont'd pg. 4

4 CYBER SECURITY MYTHS BUSINESS OWNERS NEED TO KNOW

Myth:Cyber-attacks only come from external sources.

Reality: Upward of 60% of data breaches can be traced back to employee error. They may leave sensitive data on unsecured hardware rather than behind digital walls. They may open malicious files that copy and send data to an external location. Employee IT security training goes a long way to fix this.

Myth: Simple antivirus software or firewalls are enough to protect your business.

Reality: Cybercriminals use sophisticated tools to get what they want. The fewer security solutions you have in place, the easier it is. Antivirus software can't do anything to stop a motivated hacker, and firewalls should never be considered a primary line of defence. Web scanning and malware detection software can give you more protection on top of these.

Myth: Your business is too small or niche to be a target.

Reality: Cybercriminals don't care about the size or type of your business. They target everyone because they know they'll eventually break through somewhere. Small businesses are more appealing because they often lack serious cyber security solutions.

Myth: You don't collect payment or financial data, so you aren't worth targeting.

Reality: They aren't just looking for credit card details. They want usernames, passwords, email addresses and other personal identifying information they may be able to use elsewhere because people have a bad habit of reusing passwords for other accounts, including online banking.

Inc., Dec. 16, 2019

TOP TIPS FOR MAKING THE MOST OF YOUR SMALL-BUSINESS TECHNOLOGY

Embrace mobile. Your customers use mobile, so your business needs to work in the mobile space too. Optimize your website for a better mobile experience.

Good copy goes far. From blogs to social media posts, compelling, well-written copy can go a long way. Share personal stories and success stories and create a narrative for your business online.

Instagram it. If your business isn't on Instagram, it should be. Many of your current and future customers are there. It's a great place to share photos, tell stories and foster connections.

Get more out of SEO. Good header tags, for instance, are a must for good overall SEO. Learn how to get more out of headers and you'll be able to drive more traffic to your website or related web pages. *Small Business*

Trends, Dec. 1, 2019

3 THINGS MENTALLY STRONG PEOPLE DON'T WASTE TIME DOING

Overthinking – They look at their situation and take decisive actions. Some look at all the available information and go. Others rely more on their gut. Either way, they keep things moving forward.

Regretting – It's natural to want a different outcome than the one you got or to think, "I should have done X instead of Y." But these thoughts can hold you back and lead to second-guessing yourself later.

Complaining – It can be healthy to complain. It gets your thoughts into the open where they can be discussed. But you have to discuss and arrive at solutions. Complaining for the sake of complaining – or complaining to people who can't help – is unproductive.

Embrace the unexpected - Life and work can be stressful. But focusing on the negative that we deserve better will not add to the solution.Mentally strong people take a positive approach to find always the bright side of life. Victimizing our own self will only make it worse, so instead of finding culprits, comparing miseries they choose to grow with adversity. This helps them overcome obstacles and turn them to their advantage. Being flexible enough and resilient to change is the key to grow while working towards the 'bigger' goals of life.

Business Insider, Dec. 17, 2019

Anticipating Customer Needs

What is the best way to create a loyal customer base and, therefore, a more profitable business?

Anticipate Customer Needs.

Anticipating needs is the best way to let your customers know that their success is your priority. When you deliver something customers need without asking, you create a sense of ease and let them know you have their best interests in mind – a proverbial "I have your back."

The most effective way to anticipate the needs of your customers is to know them well. How else will you know what their expectations are? You have to create a relationship with them to identify what their demands are and fulfill them before they even know what they wanted. So, how do we go about this? Here are just a few examples.

Establish A Relationship.

In most of my books, I have a call to action. I ask readers to email me to make their commitment to improving their businesses. Developing this dialogue with readers is an act of accountability on both of our parts. Moreover, it is a big leap of faith for some, and I am honoured they trust me. They tell me why they are committed, and I let them know I am here and interested in helping them succeed. My hope is that they feel less alone in their struggles as business owners and more motivated to make the necessary changes they need for a successful business.

Exceed Expectations.

The responses from readers when they receive emails or videos from me has been overwhelmingly positive. Cont'd pg. 4

The Benefits of Mastermind Group

I believe no man is an island. So, I offer this tip: if you're an entrepreneur, you need to be in a mastermind. Being in a mastermind group is one of the most powerful tools to help you increase profitability in your business.

1. What is a mastermind group? If you aren't familiar with them, a mastermind is a group in which entrepreneurs can mentor each other and help each other grow their businesses. It can be an important catalyst for growth and shaping your business. The mastermind I run is called the Edison Collective. We get together face-to-face every quarter to expand our business (and occasional musical) knowledge. We share our ideas, solutions, best practices, successes and challenges as entrepreneurs. Most of all, we motivate and inspire each other.

2. What are the benefits of belonging to a mastermind? While some mastermind groups run on a digital platform, face-to-face meetings are important if they're an option. What I love about being in a mastermind is the connection. We are truly there to learn from each other. No one walks in with their ego. We gather to benefit ourselves and each other by sharing and learning from other entrepreneurial experiences.

3. To benefit from a mastermind, you must be willing to collaborate, share and learn from each other. And remember, trust is imperative. There is total confidentiality, so feel free to not be a boss for a bit. Who can be in a mastermind? The beautiful thing is that you don't have to join an established mastermind. You can start your own. Find like-minded entrepreneurs who are driven to achieve the same goals and vision you are. Get Together once a quarter face-to-face, have open discussions about your business and get your insights from each other. That right there ? Priceless!

How to Spot Phishing Email ?

It's the perfect time for hackers to send e-mails with dangerous malware and viruses. Right now, your inbox is probably filled with "COVID-19" subject lines and coronavirus-focused e-mails.

Hackers are even using a fake cdc-gov e-mail address that's not legitimate and spamming inboxes.How can you tell a phishing e-mail from a legitimate one? Here's a few telltale signs:

1. Look closely at the e-mail address to make sure it's spelled correctly.
2. Hover over any links in the e-mail (but DON'T CLICK) to see the ACTUAL website you'll be directed to.If there's a mismatched or suspicious URL, delete the e-mail immediately.
3. Watch for poor grammar and spelling errors.
4. Never download an attachment unless you know who sent it and what it is.
5. When in doubt, call the person who supposedly sent the e-mail on the phone to verify it's legitimate.

It seems that most assume their emails will go into a black hole, never to be answered. Not only do I answer, but I also include a ton of resources that basically equal free coaching. There is an FAQ, links to my Entrepreneurship Elevated podcast, links to find a Profit First Professional and become a Profit First. And while it could be interpreted as marketing, anyone who knows me knows I am out to empower others and help their businesses become more profitable. I often get emails from readers who are pleasantly surprised – they are getting answers to questions before they even knew they had them.

See? Anticipating needs! Professional, links to Clockwork resources, links to Pumpkin Plan resources … You get my drift.

Ask For Feedback.

I often request reviews of my books. Is this because I want to hear how great they are? No. I ask for reviews because I want that honest feedback. How the heck else will I know what to write next? How will I know what problems need solving and what business solutions entrepreneurs are seeking if I don't ask? Getting reviews enables me to focus on these key areas where business owners are trying to improve.

MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford – a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multi-million-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group. He is also a former small-business columnist for The Wall Street Journal, MSNBC's business makeover expert, a keynote speaker on entrepreneurship and the author of the cult classic book The Toilet Paper Entrepreneur. His newest book, The Pumpkin Plan, has already been called "the next E-Myth!" MikeMichalowicz.com.

- **They don't know better.** Many people have never been trained in cyber security best practices. While some of us may know how to protect our network, safely browse the web and access email, many people don't. Believe it or not, people do click on ads on the Internet or links in their email without verifying the source.This can be fixed with regular cyber security training. At Berti Group you have an option to learn about best practices, current threats and how to safely deal with such issues

- **They use bad passwords.** Many people still use bad passwords like "12345" and "qwerty." Simple passwords are golden tickets for hackers. Once they have a username (which is often just a person's actual name in a business setting), if they can guess the password, they can let themselves into your network. Many security experts suggest having a policy that requires employees to use strong passwords. Passwords should be a mix of letters (uppercase and lowercase), numbers and symbols. The more characters, the better. On top of that, passwords need to be changed every three months, and employees should use a different password for every account. Employees may groan, but your network security is on the line

- **They don't practice good security at home.** These days, many businesses rely on "bring your own device" (BYOD) policies. Employees use the same devices at home and at work, and if they have poor security at home, they could be opening up your business to major outside threats.How do you fix this? Define a security policy that covers personal devices used in the workplace, including laptops, smart phones and more. Have a list of approved devices and approved anti-malware software. In current pandemic environment it is essential to have this policy at Berti Group we have resources to help you put together a solid BYOD security policy.

- **They don't communicate problems.** If an employee opens a strange file in an email, they might not say anything. They might be embarrassed or worry that they'll get in trouble. But by not saying anything, they put your business at huge risk. If the file was malware, it could infect your entire network.Employees must be trained to communicate potential security threats immediately. If they see something odd in their inbox, they should tell their direct supervisor, manager or you. The lines of communication should be open and safe. When your team is willing to ask questions and verify, they protect your business

- **They fall for phishing scams.** One of the most common scams today is the phishing scam. Cybercriminals can spoof email addresses to trick people into thinking the message is legitimate. Scammers often use fake CEO or manager emails to get lower-level employees to open the message. Criminals will do anything to trick people into opening fraudulent emails. Again, it's all about asking questions and verifying. If someone isn't sure if an email is legit, they should always ask.