BERTIGROUP
MANAGED IT SERVICES

BERTIBRIEF

Issue #26- September 2020

In This Issue

Why Your Business Is The PERFECT Target For Hackers …And What You Need To Do NOW To Protect Yourself

Everybody gets hacked, but not everything makes the evening news. We hear about big companies like Target, Home Depot, Capital One and Facebook getting hacked. What we rarely hear about are the little guys – the small businesses that makeup 97.9% of employers in Canada (https://www.ic.gc.ca/eic/site/061.nsf/eng/h_03090.html#point1-1). It's these guys who are the biggest targets of cybercriminals.

If you run a business, that business is a potential target. It doesn't matter what industry you're in, what you sell or how popular you are. Cybercriminals go after everybody. In 2018, a cybersecurity survey by the Ponemon Institute found that 67% of small and mid-size businesses in North America and the UK were hit by a cyber-attack.

For the cybercriminal, casting a wide net makes the most sense because it gets results. It puts them in a position where they can extort money, steal sensitive information and ultimately profit off of destroying the property, prosperity and reputation of others. So,Why do cybercriminals love to target small businesses? There are a handful of reasons why small businesses make sense to attack. Cont'd pg. 3

Back To Basics

A lot of time is spent staying protected from the newest type of scam or the newest cyber crimes, but as is true with many things, remembering the basics is the entire foundation of making sure you, your company and your clients remain safe.

Everyone in the company or organization should know basic security principles. Security principles and policies should be documented and part of every new employee training. Strong password requirements, Internet usage guidelines and only connecting remotely over VPN are examples of some common security policy items. Strict penalties for violating security policies should be detailed.

It's not a good habit to save files onto your computer if there is a location on the network or on your server where they can live. They're much less likely to be backed up on your computer, whereas they'll reliably and regularly be backed up if they are saved on the server.

If you use websites or software that do not require regular password changes, set a calendar reminder to change the password yourself every other month.

As with other things, a little prevention goes a long way – remembering the security basics, and asking about them if you don't know what they are, is the single best thing you can do to protect yourself and protect the company.

MAKE AN IMPACT

Why did you decide to start your own company? When I ask business owners and entrepreneurs this question, they most often answer, "I wanted to make a positive impact in the world."

The same is true for me. Yes, sure, I wanted to be my own boss, do work that brings me joy, create my own systems, have financial freedom … but the endgame was that I wanted to make things better through my business. I wanted (and still want) to eradicate entrepreneurial poverty. To make the world a better place for me, my family and my community.

I know – with the current state of things, you may be feeling as though your dreams are too lofty and need to take a back seat. Your business has a crisis to survive, after all. But you can accomplish both surviving (heck, thriving) and making an impact – even during a pandemic.You are closer to your dreams than you may feel right now. They don't have to fall by the wayside.

The biggest impact you can make right now is through HOW you serve your clients and community in the face of one of the biggest challenges in our lifetime.But you can't do that if you don't have a solid foundation in your business.

So let's recap what I have been posting about: The Business Hierarchy Of Needs (mikemichalowicz.com/the-businesshierarchy-of-needs) is the key to your business's success right now.The needs of your customers and clients have likely changed over the last few months and you may feel stuck in, say, the sales level of the Hierarchy. This is why I created the Recession Response (mikemichalowicz.com/recession response), which addresses the HOW – how to take steps to ensure your first three levels of The Business Hierarchy Of Needs are in place, so you can go ahead and make your impact in the world. Cont'd pg. 4

1. Small Businesses Are The Most Vulnerable. Business owners, entrepreneurs and executives aren't always up-to-date on network security, current cyber threats or best practices in IT. They have a business to run and that's usually where their focus is. Unfortunately, that means cybersecurity can take a back seat to other things, like marketing or customer support. This also means they might not be investing in good network security or any IT security at all. It's just not top of mind or they may feel that because it's never happened to them, it never will (which is a dangerous way of thinking).

2. Small Businesses Don't Take IT Security Seriously. Coming off that last point, it is true that many businesses don't properly secure their network because they feel that they aren't vulnerable. They have the mindset of "It hasn't happened to me, so it won't." Along those same lines, they might not even take password security seriously. According to research conducted by Trace Security, upward of 80% of ALL breaches come down to one vulnerability: weak passwords! Even in 2020, people are still using passwords like "12345" and "password" to protect sensitive data such as banking information and customer records. Secure passwords that are changed regularly can protect your business!

3. Small Businesses Don't Have The Resources They Need. Generally speaking, medium to large companies have more resources to put into IT security. While this isn't always true (even big companies skimp on cybersecurity, as the headlines remind us), hackers spend less time focused on big targets because they assume it will take more of their own resources (time and effort) to get what they want (money and sensitive data). Many small businesses lack the resources like capital and personnel to put toward IT security, so hackers are more confident in attacking these businesses.

Just because you haven't had any major problems for years – or at all – is a bad excuse for not maintaining your computer systems. Threats are growing in number by the day. While many small businesses might think, "I don't have the time or resources for good security," that's not true! You don't need to hire IT staff to take care of your security needs. You don't need to spend an arm and a leg securing your network. IT security has come a LONG way in just the last five years alone. You can now rely on IT security firms to handle all the heavy lifting. They can monitor your network 24/7. They can provide you with IT support 24/7.

That's the great thing about technology today – while many hackers are doing everything, they can to use technology against us, you can use it against them too. Work with a dedicated and experienced IT security firm.Tell them your business's network security needs and they'll go to work fighting the good fight against the bad guys.

THREE EMAIL PRODUCTIVITY TRICKS YOU NEED TO KNOW

1. **Turn Off Notifications.** Every time you get a ping that you have a new email, it pulls your attention away from what you were doing. It can be very distracting. During the workday, you might get several pings, which equals to a lot of wasted time. Set aside a block of time for reading and responding to emails instead, and utilize the time to go through emails and sort them if required to plan your day.

2. **Use Filters**. Many email programs can automatically sort incoming emails. You define the sources and keywords, and it does the rest. Sorting helps to prioritize emails you need to respond to sooner and which are most relevant to you.

3. **Keep It Short.** Most of us do not like to read long-winded emails so we try to avoid emails that tend to be long-winded. We usually scan relevant information to get a general idea of what does the email indicates. It is a best practice to include short and relevant information. Your recipients will appreciate if you keep the information concise.

Small Business Trends, April 23, 2020

Did You Experience a Spike In Spam Emails Lately ?

If yes, we have four simple preventative measures you can take to reduce the chances of your e-mail address getting on a spammers list.

1. Use a disposable e-mail address. To avoid your primary e-mail address becoming a spam dump, set up a free Internet e-mail address with Gmail or Hotmail and use it when buying or opting into online newsletters. You can also use a throwaway e-mail address when making purchases or subscribing to newsletters (see #4 below).

2. Pay attention to checkboxes that automatically opt you in. Be very watchful of small, pre-checked boxes that say, "Yes! I want to receive offers from third-party companies." If you do not uncheck the box to opt-out, your e-mail address is likely to be sold to every online advertiser.

3. Don't post your primary e-mail address on your website, web forums, or newsgroups. Spammers have special programs that can glean e-mail addresses from websites without your permission. If you are posting to a web forum or newsgroup, use your disposable e-mail address instead of your primary e-mail address.

4. Don't open, reply to or try to opt-out of any overtly obvious spam e-mails. Opening, replying, or even clicking a bogus opt-out link in a spam e-mail signal that your e-mail address is active, and more spam will follow.

I invite you to visit the Recession Response for tips and tangible, actionable resources to help you maintain your SALES, PROFIT and ORDER levels of The Business Hierarchy Of Needs, because you can still achieve your dream and impact your community in a positive way. You were put on this earth to have an impact. And that impact is not achieved by sacrificing yourself, or your business. Nail the first three levels of sales, profit and order. Then you can give back to the world and make your impact.

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!" For more information, visit MikeMichalowicz.com.

Are Your Employees Leaving This Back Door Wide Open?

Chances are your employees have wireless networks set up in their homes. Unfortunately, unlike in well-managed office environments, many home users are very lax about the security of their wireless networks leaving a back door open to hackers. Wi-Fi signals often broadcast far beyond the home of your employee and out into the streets, leading to an epidemic of drive-by hacking among cybercriminals. We have FIVE simple tips for securing home Wi-Fi networks for your employees:

1. Use stern encryption (WPA2) and more complex passwords
2. Hide your wireless network's name
3. Ensure that they have a VPN to access sensitive documents
4. Designate a Wi-Fi connection for work that doesn't compete with your home use Wi-Fi
5. Use a firewall or a threat protection filter

These security measures are easy to set up but can have a massive impact on your remote team's security. If you need help setting up a Work From Home solution or have any other technology questions, please call us at (403)800-3105 or email us at ask@bertigroup.com, one of our network specialists will be happy to assist.