TECHNOLOGY BYTES

Insider Tips to Make Your Business Run Faster, Easier & More Profitable

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! A true professional IT support team you can count on, available 24/7."

– Doug Johnson , CyberTrust IT Solutions
Contact us on: (949) 396-1100

Cyber-Attack Alert!

Are You A "Sitting Duck"?

To know,visit pg.2

What's Inside

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 make up 99.7% of employers in the United States, according to the Small Business Administration. It's these guys who are the biggest targets of cybercriminals.

In a nutshell, if you run a business, it is a potential target. It doesn't matter what industry you're in, what you sell or how popular you are. Cybercriminals go after every- body. In 2018, a cyber security survey by the Ponemon Institute, found that 67% of small and midsize businesses in the U.S. and U.K. 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 are able to extort money, steal sensitive information and ultimately profit off of destroying the property, prosperity and reputation of others.

Why do cybercriminals love to target small businesses? There are a handful of reasons why it makes sense to attack small businesses.

1. Small Businesses Are The Most Vulnerable. Business owners, entrepreneurs and executives aren't always up-to-date on network security, current cyberthreats or best practices in IT. They have a business to run and that's usually where their focus is. Unfortunately, that means cyber security 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's 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 invest in IT security. While this isn't always true (even big companies skimp on cyber security, 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 invest in 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 – it is not an 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 monitor your network 24/7 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.

"67% of small and medium-sized businesses in the US and UK were hit by a cyber-attack.

Shiny New Gadget Of The Month:

Weber Connect Smart Grilling Hub

Grilling can feel like guesswork. You throw the food on the grill and keep a close eye on it, hoping for the best. Say goodbye to guesswork and overcooked steaks with the Weber Connect Smart Grilling Hub.

The Weber Connect takes the thermometer and timer into the WiFi era. It monitors your food and sends updates to your smartphone. It lets you know when to flip the burgers or steaks – and then notifies you again when it's time to take them off the grill. You can even have the Weber Connect tell you when your meat of choice has reached your ideal level of doneness. It's great for those who are new to grilling or don't grill often, and it works with every grill! See more at **bit.ly/3eTL69Y!**

"There Are Only Two Types Of Companies: Those That Have Been Hacked, And Those That Will Be."...

- Robert Mueller

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 do) to eradicate entrepreneurial poverty. To make the world a better place for me, my family and my community.

Tip Of The Day!

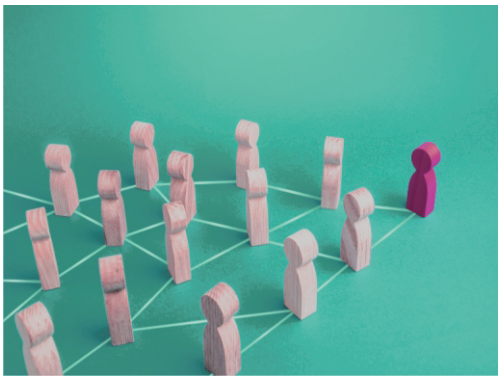
Stay Informed Of Current Cyber-Attack Event And Follow Precaution Measures

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/thebusinesshierarchy-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.

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.

Back To Basics

A lot of time is spent staying protected from the newest type of scam or the newest cybercrimes, 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 the 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 be reliably and regularly 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.

3 E-mail Productivity Tricks You Need To Know

Turn Off Notifications.

Every time you get a ping that you have a new e-mail, it pulls your attention away from what you were doing. It's a major distraction. Over the course of a day, you might get several pings, which can equal a lot of time wasted. Set aside a block of time for reading and responding to e-mails instead.

Use Filters.

Many e-mail programs can automatically sort incoming e-mails. You define the sources and keywords, and it does the rest. This helps prioritize which emails you need to respond to soonest and which are most relevant to you.

Keep It Short.

Most of us don't like to read e-mails so we don't. Or we quickly scan for relevant information. Your best bet is just to include the relevant info-ormation. Keep it concise and your recipients will appreciate it, and as a recipient, you'll appreciate it as well.
Small Business Trends, April 23, 2020

5 Easy Things You Should Do To Protect Your Business Now

Let's face it: no one likes to think about bad things happening to them, much less plan for them. But since **September is National Disaster Preparedness Month,** we want to give you a quick "brush-up" on some simple things you can (and should!) be doing to protect your business.

1. **Review Your Business Insurance Carefully.**

   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.

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.

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 in 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

Call us during the month of September and we'll give you a Disaster Recovery Business Assessment for FREE (a $297 value)!

Call: (949) 396-100