



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, only connecting remotely over VPN, and Internet usage guidelines 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 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.



## 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 clients can automatically sort incoming e-mails. You define the sources and keywords and it does the rest. This helps prioritize which e-mails 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 – and so we don't. Or we quickly scan for relevant information. Your best bet is to just include the relevant information. 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*

## WHY YOUR BUSINESS IS THE PERFECT TARGET FOR HACKERS ...



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.

Basically, 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 cyber security survey by the Ponemon Institute found that 67% of small and medium-sized 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 cyber crooks love to target small businesses? There are a handful of reasons why small businesses make sense to attack.

**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 backseat 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).

CONTINUED ON PAGE 2

"As a business owner, you don't have time to waste on technical and operational issues. That's where we come in! Call us and put an end to your IT problems finally and forever!"



Will Nathan  
Founder & CEO  
Vector Choice

## INSIDE THIS ISSUE

Why Your Business Is The PERFECT Target For Hackers ...

PAGE 1

Vector Choice News

PAGE 2

Check Out This Month's Shiny New Gadget: Weber Connect Smart Grilling Hub

PAGE 3

Make An Impact

PAGE 3

Back To Basics

PAGE 4

CONTINUED FROM COVER...

**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:

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

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 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 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 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.

## 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!](http://bit.ly/3eTL69Y)



## MAKE AN IMPACT

Why did you decide to start your own company? When I ask business owners and entrepreneurs this question, it is most often answered, "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.

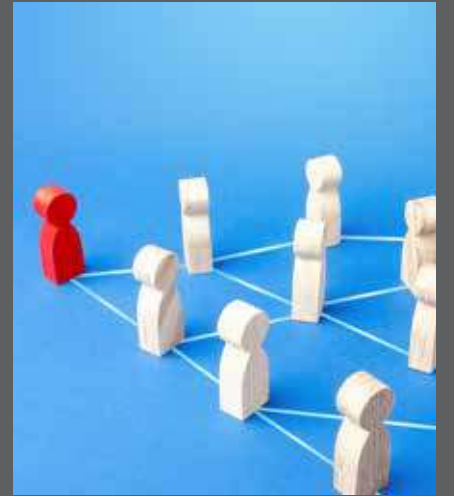
I know – with the current state of things you may be feeling as though your dreams are too lofty and need to take a backseat. Your business has a crisis to survive, after all. But you can accomplish both surviving (heck, thriving) and making an impact – even during a pandemic.

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-business-hierarchy-of-needs](http://mikemichalowicz.com/the-business-hierarchy-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](http://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.



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 multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Proventus 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](http://MikeMichalowicz.com).

## VECTOR CHOICE NEWS

## TRIVIA



Vector Choice has made the Inc. 5000 list, a ranking of the nation's fastest-growing private companies, for the 2nd year in a row!



**CEO Will Nobles speaking at AT&T to a socially distanced group.**

### Who wants to win a \$25 gift card?

You can be the winner of this month's trivia challenge quiz! Just be the first person to correctly answer this month's trivia question and receive a \$25 Amazon gift card!

Who designed the 'first' small computer for home use?

- A. John Blankenbaker
- B. Steve Wozniak
- C. Chuck Peddle
- D. Steve Leininger

Ready? Call us right now with your answer! **877.468.1230**

### It May Be Time For A Smartphone App Permissions Audit



Every smartphone app requests permissions in order to operate. The basic "phone" app needs permission to use the microphone and contacts. This makes sense and you would never think twice about it.

Other apps can pose problems. Many apps want access to your location, camera, or Bluetooth, for example. For some apps, some permissions make sense. For others, they're a red flag. This is why you need to do an app audit.

On an iPhone, check app permissions in *Settings > Privacy*. You can view the permissions of every app you have installed and change them, if needed.

On Android devices, app permissions are in *Settings > Apps & Notifications* (it may be under *Apps* on older devices). Tap on the app for permission details.