vector choice

2180 Satellite Blvd
Suite 400
Duluth, GA 30097

Office: 877.468.1230

VectorChoice.com

TOP 7 THINGS TO DO SO YOU DON'T GET HACKED WHEN SHOPPING ONLINE

1. Verify the URL is safe. Many browsers have a little padlock in the URL bar. If the padlock is closed, the URL is safe. If it's open, you may want to avoid the site.

2. Verify the URL is accurate. Many scammers register fake websites using misspelled URLs or extra numbers to look like the real deal. If the URL looks odd, it's probably a scam.

3. Use a secure web browser. Firefox and Chrome, for example, always navigate to HTTPS (Hypertext Transfer Protocol Secure) websites. These websites are more secure than their HTTP counterparts.

4. Don't click suspicious links or attachments. Never click a link if you can't verify it first. In fact, it's better to delete any email you don't recognize.

5. Always bookmark authentic websites. When you bookmark real websites, you never have to worry about mistyping or clicking scam links.

6. Rely on a password manager. It's hard to remember strong passwords, but with a password manager, you don't have to. Never use a bad password again!

7. Use the official mobile apps for online stores. If you download the official app of your favorite online stores, such as Amazon or eBay, you don't have to worry about accidentally navigating to a scam website. Just make sure the app is verified by Google or Apple. *Lifehacker, Nov. 19, 2019.*

TIP TIPS FOR SCALING SECURITY FOR YOUR SMALL BUSINESS

PUT A GREATER EMPHASIS ON PASSWORDS.

As businesses grow and adopt more technologies, such as cloud-based apps and mobile apps, they also have to deal with more passwords. The more passwords employees have to remember, the less likely they are to have strong passwords and the more likely they will use the same password for everything. Another problem is password sharing. A team of people may share a single license for a piece of software which means they share a single password. Password managers like LastPass can save a lot of hassle while still protecting your accounts and many passwords managers are scalable.

RELY ON MULTI-FACTOR AUTHENTICATION (MFA).

MFA adds another layer of security on top of firewalls and malware protection. It's like adding an extra password on top of your existing password, though only you can enter it. However, some employees skip MFA because it adds extra steps to the login process. But an extra 15 seconds to log in is worth it for the security. There are many MFA options available for different-sized businesses. Make it a part of your cyber security policy. *Small Business Trends, Nov. 1, 2019.*

Published by The Newsletter Pro . www.TheNewsletterPro.com

THE VECTOR CHOICE

TECHNOLOGY TIMES

INSIDER TIPS TO HELP YOUR BUSINESS RUN FASTER, MORE EFFICIENTLY, AND ULTIMATELY, MORE PROFITABLY

FEBRUARY 2020

IF YOU THINK THAT YOUR BUSINESS IS TOO SMALL TO BE HACKED ... YOU'RE A CYBERCRIMINALS #1 TARGET

"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 Nolan
Founder & CEO
Vector Choice

Many cybercriminals look at small businesses as blank checks. More often than not, small businesses just don't put money into their cyber security, and hackers and cybercriminals love those odds. They can target small businesses at random, and they are all but guaranteed to find a business that has no IT security – or the business does have some security but it isn't set up correctly.

At the same time, cybercriminals send e-mails to businesses (and all the employees) with links to phishing websites (websites designed to look like familiar and legitimate websites) or links to malware. They hope employees will click on the links and give the criminals the information they want. All it takes is ONE employee to make the click.

Or, if the business doesn't have any security in place, cybercriminals may be able to steal all the data they want. If you have computers connected to the Internet and those computers house sensitive business or customer data – and you have NO security – cybercriminals have tools to access these computers and walk away with that sensitive data.

It gets worse! There are cybercriminals who have the capability of locking you out of your computer system and holding your data hostage. They may send along a link to ransomware, and if you or an employee click the link or download a file, your business could be in big trouble. The criminal may request a sum of money in exchange for restoring your PCs or data.

However, as some businesses have learned, it's not always that simple. There are businesses that have paid the ransom, only for the cybercriminal to delete all of their data anyway. The criminal walks away with the money and the business is left to die.

And that's not an understatement! Once cybercriminals have your data and money,

CONTINUED ON PAGE 2

INSIDE THIS ISSUE

Published by The Newsletter Pro . www.TheNewsletterPro.com

CONTINUED FROM COVER...

or both, they don't care what happens to you. Cybercriminals cannot only do major damage to small businesses, their actions can literally destroy a business! We're talking about the costs of repairing the damage and the cost of losing customers who no longer want to do business with you. You're looking at a public relations nightmare!

> **"Cybercriminals cannot only do major damage to small businesses; their actions can literally destroy a business! "**

This goes to show just how critical good IT security really is, but business owners still don't take it seriously. Even as we enter 2020, there are business owners who don't consider cyber security a high priority – or a priority at all. It's a mindset that comes from before the age of the Internet, when businesses didn't face these kinds of threats. And many business owners fall into the habit of complacency. In other words, "It hasn't happened yet, so it probably isn't going to happen." Or, "My business isn't worth attacking."

Cybercriminals don't think that way. For them, it's a numbers game and only a matter of time. Business owners need to adapt to today's online landscape where just about everything is connected to the Internet. And if something is connected to the Internet, there is always going to be some level of vulnerability.

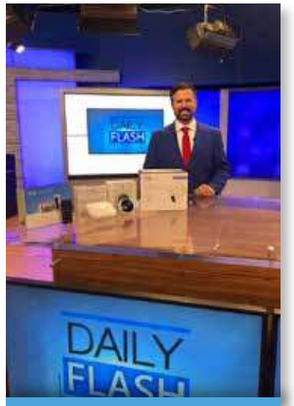
But you can control your level of vulnerability! You can be cheap or complacent and do the bare minimum, which will put your business and customers at risk. Or you can take it seriously and put IT security measures in place – firewalls, malware protection, secure modems and routers, cyber security insurance and working with a dedicated IT security company. There are so many options available to secure your business.

The reality is that cyber security should be a normal, everyday part of any business. And anyone thinking about starting a business should have the cyber security discussion right from the very beginning: "What are we going to do to protect our business and our customers from outside cyberthreats?"

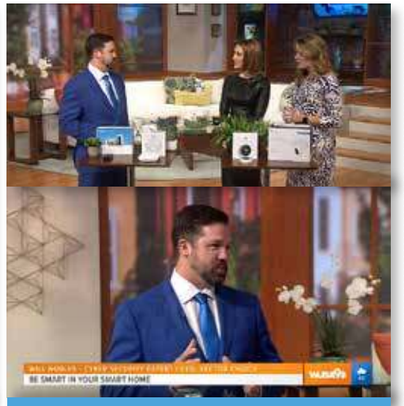
When it comes down to it, not only do you need good cyber security, but you also need a good cyber security policy to go along with it. It's something you share with your team, customers, vendors, investors and anyone else who puts their trust in your business. Transparency about your cyber security is a great way to build and maintain trust with these people. If you don't have IT security in place, why should anyone trust you?

Think about that question and think about the security you have in place right now. How can you make it better? If you need to reach out to an IT security firm, do it! It will only make your business better and prepare you for the threats that are looming right now. No business is too small or too obscure to be hacked.

VECTOR CHOICE NEWS



Our CEO Will Nobles had a great time as a special guest on the Daily Flash Orlando!



Will during his TV segment, Be Smart In Your Smart Home, on CBS - Great Day Washington!

TRIVIA

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!

One of the most profound technology inventions to affect our lives in the 20th century and beyond has been the internet. The internet infrastructure (usually considered to be TCP-IP) had been used by various research projects and organizations but the advent of the World Wide Web as an application enabled the interconnectivity between various systems that we today take for granted. Who is the computer scientist and MIT Professor credited with inventing the World Wide Web?

A. Bill Gates
B. Gordon Moore
C. Charles Babbage
D. Sir Tim Berners-Lee

Ready? Call us right now with your answer!
877.468.1230

SHINY NEW GADGET OF THE MONTH: M&R DIGITAL COUNTING COIN BANK

Many of us still keep a coin jar to toss in our spare change. Even with the growing popularity of apps like Apple Pay and Google Pay, coins remain a big part of our lives. Of course, when you're tossing coins into a jar at the end of the day, you have no idea how much you've collected until you count it or take it to a Coinstar.

The M&R Digital Counting Coin Bank solves this problem. You never have to count change again. Every time you drop coins into the bank, it counts and adds them to the total. The digital readout keeps you updated on how much you've saved. It's a remarkably simple piece of technology that eliminates the hassle of keeping track of change.

How To Market To Gen Z

Generation Z is quickly becoming a major segment of the consumer space. Businesses must start marketing to this generation. They are tech-savvy, and they grew up with social media, so their phones and social connections mean everything. Here are three things to keep in mind when marketing to Gen Z.

Go to them. They aren't going to seek you out. They respond best to social media and mobile marketing. Don't pander, be personal and speak to what they get out of it.

Don't waste their time. Gen Z has a short attention span and skips walls of text and 30-second videos. Be fast and efficient. What are you selling and what are the benefits?

Avoid labels. Gen Z hates labels (including the label "Gen Z"). They don't want to be grouped with others or generalized. They value individuality immensely, so your marketing must reflect that.

THE FIRST MISTAKE BAD LEADERS MAKE IN A NEW JOB

The first mistake bad leaders make in a new job is subtle, common and avoidable: they come into an organization and they don't narrow the priority list.

In our research for *Power Score*, we found that only 24% of leaders are good at prioritizing. And when a leader is bad at prioritizing, 90% of the time it's because they let too many priorities stay alive.

In short, great leaders **prune priorities**.

What does priority pruning look like?

It looks like taking a weed whacker to the overgrown mass of useless priorities that grow inside organizations.

It looks like what Steve Jobs did when he returned to Apple and trimmed the number of products from hundreds to under 10.

It looks like what In-N-Out Burger (for those of you who have enjoyed this delicious West Coast treat) does in only giving you a menu of burger, fries and a drink.

It looks like what Scott Cook, founder of Intuit, did in making QuickBooks as easy as using your checkbook.

There are so many leaders I see who lack the analytical horsepower, the courage or the decisiveness to prune priorities, so they just let dozens, hundreds or even thousands of priorities live on in their organizations and distract people away from the small set of things that matter most.

If you want a simple way to prune priorities, use this one-page discussion guide straight out of our *Power Score* book (find that at **geoffsmart.com/books/power-score-your-formula-for-leadership-success**). Have your team rate your priorities 1–10. If you are scoring a nine or 10, keep doing what you are doing. If you score less than a nine, then it's time to get out the weed whacker!

Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times *best-selling book,* Who: A Method For Hiring, *and the author of the No. 1* Wall Street Journal *best seller* Leadocracy: Hiring More Great Leaders (Like You) Into Government. *Geoff co-created the Topgrading brand of talent management. He is the founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in Economics with honors from Northwestern University, and an MA and PhD in Psychology from Claremont Graduate University.*