

Inside This Issue

Cybercriminals Are Plotting To Hack Your Network
RIGHT NOW... And What You Can Do To Prevent It | 1

Security Byte: Mobile Device Management | 2

5 Ways Smart People Blow The Close | 3

5 Technology Trends You CANNOT Ignore

Internet of Things (IoT) - From WiFi-connected thermostats to smart locks, we're surrounded by IoT devices. Smart locks, for instance, can track who comes and goes with zero oversight.

Artificial Intelligence (AI) - AI can enhance consumer experience by delivering personalized experiences to customers. Automate more of what you do on social media with the help of AI.

Telecommuting - Working between home and office is easier than ever. As cloud collaboration has become simpler and more user-friendly, more employees are opting to use their own devices, saving the company big dollars.

Customer-Relationship Management (CRM) Software - It's all about building and managing customer relationships. CRM is crucial in

tracking prospects, logging e-mails and phone calls and more.

Voice Search - More people are using assistants like Alexa and Siri to access information. Optimize your SEO to get the most out of voice-search technologies. *TechRepublic, 5/21/2019*

IMPLEMENT THESE 2 STEPS NOW TO PREVENT FRAUD IN YOUR BANK ACCOUNT

Did you know your company's bank account doesn't enjoy the same protections as a personal bank account when it comes to fraud? If a hacker takes money from your business account, the bank is NOT responsible for replacing funds. Ask your bank what *their* policy is on refunding money stolen from your

account. Many people erroneously believe the FDIC protects you from fraud. It does not; it only protects you from bank insolvency.


Tip: Step 1: Invest in insurance to protect you from fraud. **Step 2:** Set up e-mail alerts to receive notifications any time money is withdrawn from your account. The faster you catch fraudulent activity, the better your chances are of keeping your money. If you contact the bank immediately after any money is taken out, you have a very high probability of stopping hackers from robbing you.

4 PROVEN TECHNIQUES TO IMPROVE PROJECT MANAGEMENT IN YOUR BUSINESS

1. Know the project's purpose/scope/goal. This is how you get focused. When you know

Continued on page 3

The Tech Chronicle

Brought to you by  **bridge**
IT SUPPORT

Insider Tips To Make
Your Business Run
Faster, Easier And More
Profitably

What's New in September

Congratulations to Michael on celebrating his first full year with us!

He came to us with a few years of IT support experience, and has quickly grown to be an indispensable part of our team. His current position as a Technical Specialist allows him to interact with our clients every day. One of the things our clients like best about Michael is his calm, understanding demeanor that allows him to fully understand a computer issue before diving in for the fix.



Outside of his career, Michael likes to work on his house, rebuilding a '68 Chevy truck, and hopes to get to his race car that is buried in the back of the garage someday! Good luck with that one, Michael!



Cybercriminals Are Plotting To Hack Your Network RIGHT NOW ... And What You Can Do To Prevent It

September 2019



This monthly publication provided courtesy of Mark VanderWal, President of Bridge IT Support.

Our Mission:

To positively influence the quality of life in West Michigan by directing our God-given talent of fixing and maintaining computer systems to our loyal clients so they can deliver the same to their clients.

Did you know that small businesses are more likely to be targeted by cybercriminals than any other business or organization? It's true! While we hear about major breaches on the news, we don't get to hear the stories of the businesses that struggle with hacking attempts and cyber-attacks.

Hackers love to go after small businesses for one very big reason: small businesses are less likely to invest in top-notch (or even worthwhile) cyber security. Hackers love this vulnerability.

According to the Verizon 2019 Data Breach Investigations Report, 43% of cyber-attacks

hit small businesses. The reason comes down to many factors, but there are two in particular that hackers really dig into when going after targets: lack of resources and lack of knowledge. Of course, there's more to this story, as hackers also look at a business's customer base and the type of data the business shares online.

A lot of small businesses are also relying more on the cloud (and this is the trend moving forward), but then they do little to keep their line of communication with the cloud storage, or just the cloud storage itself, secure.

According to Symantec, a lot of businesses

Continued on page 2

that rely on the cloud also fail to rely on strong encryption software. They just share their data to the cloud and let that be that.

Hackers attack small businesses because they want money. Hackers go after targets they can profit from, whether they hold a business's data hostage and demand a ransom (and get that ransom – hackers got \$460,000 from Lake City, Florida, officials after a ransomware attack on government computers, and that wasn't the only Florida city to pay!), or by stealing customer data and either selling it on the dark web or black market, or using it for themselves.

The Verizon report also looked at the types of businesses that are targeting. The top three are:

- Public administration (23,399 reported incidents and 330 confirmed data disclosure)
- Information services (1,094 reported incidents and 155 confirmed data disclosure)
- Financial and insurance (927 reported incidents and 207 confirmed data disclosure)

They go after these types of businesses because this is where they can make their money – and it's where they've discovered the most vulnerability. However, while these types of businesses represent the top three, there are *many* more.

Every type of business is targeted. Some businesses make it past the attack unscathed, but many don't. Their data is compromised in one way or another.

Why are small businesses are targeted so much? It's a numbers game. Hackers know most small businesses lack good cyber security. This makes these businesses easier targets. Target enough of them, and you're going to make some serious money (from selling stolen data or paid ransoms).

So, what can you do about this? How can you protect your network? First and foremost, you have to realize YOU are a target. It doesn't matter if you've never been hacked before. It just means the hackers haven't gotten to you yet. Once you realize this, you can go to work and get your business ready for the eventual attack.

This is where a risk assessment can do a lot of good. You may already have some security measures in place, but do you know how effective those measures are? You need to know where your holes are so you can plug them and then reinforce them. You don't want just a wall around your business, you want an entire ocean.

But it doesn't end there. One of the most powerful tools against hackers and cybercriminals is knowledge. Next to securing your business, the best thing you can do is train your employees

on understanding cyber security and the threats that exist to harm the business they work for. Your team MUST know how to identify phishing

“First and foremost, you have to realize YOU are a target. It doesn't matter if you've never been hacked before.”

schemes, fraudulent websites and virus scams, then stay regularly updated on the threats out there. (And don't forget using complex passwords that are locked away in a password vault or manager to add another layer of security).

On top of this, work with an IT team who knows what they're doing. It's one thing to tackle this all by yourself, as many businesses do, but it's another to work with an experienced IT security firm. If you go it alone, you might miss something or you might not fully understand the security you have in place. Having an outsourced team of pros means you're one step ahead of the hackers.

... continued from page 4

your purpose, you can tackle the project one step at a time and not take a scattershot approach.

2. Set deadlines and budgets for every step. Give yourself a timeline for every step of the project to keep things moving. A budget can also help you delegate and spend accordingly. Deadlines and budgets can also increase accountability.

3. Keep everyone looped in. Everyone on the project needs to know exactly what is going on, from tasking to status updates and any scheduling. When you're all on the same page, things move along much easier. Even better, use a web app to keep everything in one place.

4. Review the project. Examine what went well and what didn't. You can adjust the next project and hammer down what worked while avoiding the same mistakes. *Small Business Trends*, 6/18/2019



Do This First.

Many entrepreneurs will have written a book at some point in their lives. It's a great way to connect with prospects and clients and to grow your business. But you need

to ask yourself a few questions before you sit down to hash out your story.

Why are you writing this book? You need to understand what you're trying to accomplish. When you answer "why," it helps you hone in on what you're trying to say, saving you countless words in the process.

Who is this book for? You're writing what you know for people you want to share that knowledge with. If you don't know your audience (e.g., prospects with limited knowledge of your industry), your message could be lost in translation.

Do you need help writing? Not all of us are authors (or have time). This is where ghostwriters come in. Many entrepreneurs rely on experienced ghostwriters to get their message across while capturing your voice and delivering your message.

5 Ways Smart People Blow The Close



The weirdest thing happens when it's time to close a deal. Smart people turn to mush! I've seen it a hundred times. Here are some common ways smart people blow the close.

1. HIT MUTE

I was with a colleague in the boardroom of a billionaire CEO of the #1 company in his industry. Right after the CEO talked about the ways he wanted our help, my colleague had the chance to close the deal and help this great entrepreneur achieve his vision. Rather than bring it to a close, my colleague's mind hit Mute. Silence. Twenty seconds of silence while the client expected to wrap up the conversation and close this deal! My colleague recovered, and we ended up with a happy outcome. Clients want help wrapping up a conversation and turning to an action plan. Don't just sit there! Close the deal!

2. DON'T IMPOSE

I was in another boardroom with another colleague late in the day. My colleague did an amazing job of using reflective listening techniques to help the CEO identify his biggest leadership challenges. And then my colleague let the meeting end with no next steps. Afterward, I asked, "Why didn't you close him on the next step you want to take to solve the problems you just identified?" My colleague said, "I didn't want to impose! I didn't want to turn it into a sales call." I was like, "Impose? How is helping a CEO solve his #1 problem imposing!" That one didn't turn out well for us.

3. DAZZLE WITH COMPLEXITY

One of my other colleagues is a ninja at turning a trusted advising conversation into an actual project. But she was not always this good! In the early days, she talked at 90 mph, offering complex, nuanced analyses sprinkled with long, multipart questions. Her intent was to show how smart she was and dazzle clients

into hiring us, but clients felt they couldn't get a word in edgewise. This is a common pitfall for smart people who come out of consulting backgrounds.

4. WIN THE ARGUMENT

One of my colleagues put his hand up like a "stop" gesture in the face of our client. The consultant said, "Let me stop you there. I think your logic doesn't hold. The data tell a different story. Here is why ..." The client was not impressed with the posture. Serving clients is not about winning arguments; it's about understanding the client and figuring out how to get them what they want. You are on the same team. If you forget this, you may win the argument but lose the deal.

5. STAY SAFELY VAGUE

When I was hiring a law firm many years ago, I had a specific goal of designing an employee stock purchase program. I wanted to know the steps in drafting the plan, how long it would likely take and how much it would likely cost. The bad lawyers stayed "safely vague": "Well, that all depends." I felt like saying, "Well, no kidding, but I'm trying to get a rough estimate of the time and cost of designing this plan." The good lawyers said things like, "I'm going to ask a few questions, and I'm happy to give you an estimate for how long this project might take, how much it's likely to cost, and I'll tell you the things that will affect the time and cost." Be specific. Clients like it when you offer specifics that will help them achieve their goals.



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.

Cartoon Of The Month

www.audifreedom.com

"So, Tom, how goes the growth hacking?"

Security Bite: Mobile Device Management

If you use a cell phone, tablet, or laptop for work, does it contain information that could be harmful if it got out, such as passwords, emails, bank accounts, etc.? Does it potentially contain or have access to Protected Health Information? If so, it should be protected with Mobile Device Management, also known as MDM. This allows us to locate your device if it is lost, and remotely wipe off all the data if it falls into the wrong hands.



As a general rule, mobile devices should also be encrypted; all modern Androids and iPhones can be encrypted. You should also have a strong passcode; no "0000" or "1234."