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 October

We are moving to a new office this month! We have been blessed with growth, and our current office is getting a little tight. We will be moving to a larger facility at 601 Three Mile NW in Grand Rapids at the end of this month. We are excited about the move and the new digs, but moving is always painful. However, there will be no disruption to the high level of service you have come to expect from Bridge IT Support. Thank you for allowing us to serve you!

October 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.

Employees Keeping Your Data Safe?

... Don't Count On It

In any business, big or small, employees can be your biggest IT threat, and they might not even realize it. Businesses already face countless cyberthreats, like data breaches, cyber-attacks, online viruses and malicious e-mails. But despite all these outside threats, the real problem can come from the inside.

One of the biggest threats to your business's security is simply a lack of awareness on the part of your employees. It comes down to this: your employees just aren't aware of current threats or how to safely navigate e-mails and the web. They might not be aware when they connect to an unsecured WiFi network or if they're using a firewall. They may be haphazard in all things IT.

There are a lot of variables.

Your best defense, in this case, is training. Get all of your employees on the same page. Look at your current training and find the gaps, or start putting together training if you don't have it. You want a training program that covers all your bases and gives your employees the knowledge and tools they need to keep themselves and your business secure. (Don't know where to begin? Work with professional IT specialists. They know what your employees NEED to know!)

Another major security threat is phishing e-mails. On any given day, you and your employees can

Continued on page 2

... continued from cover

be on the receiving end of dozens, if not hundreds, of fraudulent e-mails. Data from Symantec shows that 71% of targeted cyber-attacks stem from phishing e-mails. While awareness regarding phishing scams is better than ever, it's still far from perfect. And it doesn't help that phishing e-mails have gotten more advanced.

> **"71% of targeted cyber-attacks stem from phishing e-mails."**

Phishing e-mails are typically disguised as messages from a legitimate source, such as a colleague, a bank or an online retailer. They try to trick recipients into clicking a link or opening a file (which you should NEVER do if you are not 100% sure about the source). But there are easy ways to identify scam e-mails:

1. They're impersonal. They may be addressed to "customer," "to whom it may concern" or "my friend." But be careful – sometimes they are addressed properly and use your name.

2. They're full of spelling and grammar errors. Not every phishing e-mail will have these errors, but it's good to read e-mails word for word rather than just glancing over them. Unusual errors often mean a scam is lurking.

3. The "from" e-mail address is unfamiliar. This is one of the easiest ways to pinpoint a scam e-mail. Look at the sender, and if the address is filled with numbers, letters, misspelled words or is weirdly long, there's a good chance it's from a scammer.

The other major issue facing your business is your employees connecting to unsecured WiFi hot spots. It is such an easy mistake to make. Whether it's a remote employee or an employee working during lunch at a corner café, you never know when they might connect to unsecured WiFi (it doesn't help that it's everywhere these days). One Spiceworks study found that upward of 61% of employees connect to unsecured public WiFi while working remotely.

The problem is, you never know who is watching or if the public WiFi is really the network you intend to connect to. Hackers can easily set up a "fake" network to divert traffic to their hot spot to circulate malware and steal data.

Another WiFi threat might be right at home. If you have employees who work from home, you need to make sure their home WiFi connection is secure. Too often, homeowners leave their WiFi wide-open because it's home. They think no one's going to sneak onto their WiFi or they keep it unsecure because it's easier to connect a lot of devices.

While it might be easier to connect to, it can cause *huge* problems. For one, WiFi signals can reach hundreds of feet. It's easy to sit outside of an apartment or out on the street and find dozens of WiFi signals. If any of these signals are unsecure, a hacker can sit outside undisturbed and go to work accessing data and planting malware.

It all comes back to this: Work with your employees to establish IT best practices. Educate them on threats and how to protect themselves and your company. Help them develop a positive IT security mindset at the office, at home or anywhere they work, whether they're using company equipment or their own.

Don't know where to start? Don't worry – one phone call and we can help get you started. Don't wait. Let's secure your business today.

Security Byte: Email Security

One of the most common points that can bring malware into your system is email. People trying to hack into computer systems will very commonly send out infected attachments, or emails with links to websites that try to compromise your system. Good email protection can stop these threats before they even reach you.

Many IT companies recommend a robust spam filter to tackle this problem. We recommend this, plus more with Google's G Suite email. It gives you advanced spam filtering, malware and phishing protection, along with account protection.

They are one of the best in the entire industry at protecting their users and can be HIPAA-compliant with a signed BAA. This is why we strongly recommend anyone using any outdated email such as an insecure AOL or Yahoo email, or a GoDaddy email, to move to G Suite immediately.

Cartoon Of The Month

"You know, in the tech world being disruptive is seen as a positive."

... continued from page 4

1) Recognize your stress. You must come to terms with the fact that you need to manage your stress. If you don't, you won't be able to fuel your productivity.

2) Change your mindset. Most of us view stress as a negative. Instead, remind yourself you can manage your stress. It's not a brick wall but rather a door you can open to new possibilities.

3) Find new motivation. With a new outlook on stress, you can use it to take action and get things done. Tasks and deadlines will always be there, and when you feel stress, you can buckle down to get those tasks done, because once you are done, you will feel great.

Inc., 7/19/2019

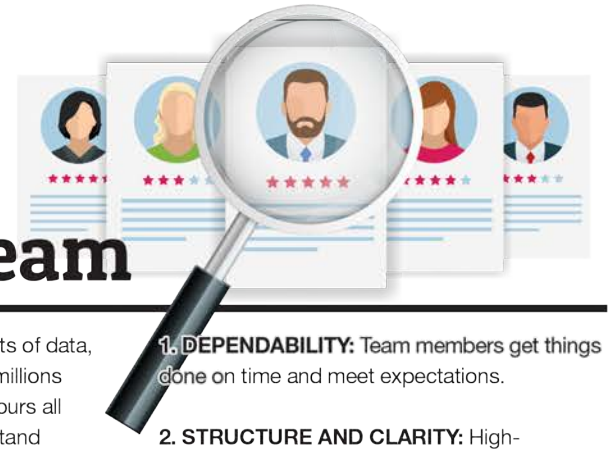
A Classic Marketing Horror Story

New Coke is one of the most cited marketing failures of all time. Before New Coke was introduced in 1985, Pepsi was capturing the taste buds of consumers. Coke's sales had slumped going into the '80s and Pepsi was becoming the soft drink of choice.

The Coca-Cola Company needed to act. They assumed people switched to Pepsi for the sweeter flavor and decided they needed a sweeter flavor of their own. On April 23, 1985, New Coke hit store shelves, and people, for the most part, liked it. But you don't mess with a classic or brand loyalty.

People still wanted "old" Coke and were up in arms when they thought it was going away. New Coke's marketing was confusing, and people had no idea what was happening with their favorite drink. Sales plummeted, and after just over two months on store shelves, New Coke was pulled and Coca-Cola Classic was introduced.

Creating The Perfect Team



Google has collected endless amounts of data, conducted countless studies, spent millions of dollars and logged thousands of hours all in the name of trying to better understand their employees. One initiative was to try and understand what makes a team effective. Specifically, **Google wanted to know why some teams excelled while others didn't.** The study was called Project Aristotle, and they gathered up some of Google's best talent to try and understand, codify and decipher how to create high-functioning teams.

The results of Project Aristotle may forever change how you go about assembling a team. Before the study, Julia Rozovsky, Google's people analytics manager, felt that the best teams came from compiling the best people. The "best of the best" would surely be the way to go. As she later stated, *"We were dead wrong."*

Google assembled organizational psychologists, sociologists, statisticians, engineers and researchers to attack this issue. For over two years, Project Aristotle studied 180 Google teams and analyzed over 250 different team attributes, looking for the magic dream-team formula, but they came up empty. Nothing was standing out to ensure you would be putting together an outstanding team.

They stumbled across some research by psychologists and sociologists that focused on what are known as "*group norms*": the traditions, behavioral standards and unwritten rules that govern how teams function when they work together. Following this new line of thought, they went in search of behaviors that magnified the effectiveness of a team and found five key characteristics of enhanced teams. Julia Rozovsky listed their findings as follows:

1. DEPENDABILITY: Team members get things done on time and meet expectations.

2. STRUCTURE AND CLARITY: High-performing teams have clear goals and have well-defined roles.

3. MEANING: The work has personal significance to each member.

4. IMPACT: The group believes their work is purposeful and positively impacts the greater good.

But #5 is the most important of all of them:

5. PSYCHOLOGICAL SAFETY: Imagine a setting where everyone is safe to take risks, voice their opinions and ask judgment-free questions; imagine a culture where everyone can let down their guard. That's psychological safety. Google found that teams with psychologically safe environments were more successful.

Psychological safety is dependent on team dynamics. There is no concern about authority or power. Everyone is focused on the clearly defined goal and *open* to whatever will help them obtain it. They are comfortable with the people on their team. The chemistry is proactive. They chat, they laugh, they have fun and they enjoy each other's company. There is no pecking order, no interest in titles, power or credit.

If you want an effective team, focus more on chemistry, diversity, balance and camaraderie. Then stir in talent, subjective and objective people, introverts and extroverts, fast and steady people, young and old and some brilliant nerds. A team full of quarterbacks will never win a Super Bowl.

Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys *and* 52 Essential Habits For Success, *he's shared the podium with esteemed figures from across the country, including former President George H.W. Bush, former Secretary of State Colin Powell, Anthony Robbins, Tom Peters and Steven Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.*

bridge
IT SUPPORT

6080 Fulton St. E, Suite C
Ada, MI 49301

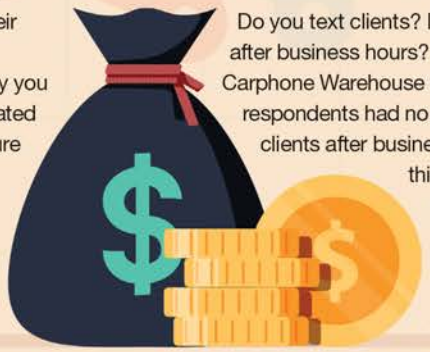
Inside This Issue

3 Ways To Make Your Business Grow

Invest In Advertising: Look at what's available and what makes sense for your niche. Need to go local? Newspapers combined with Facebook ads may make sense. Online advertising through Google and Facebook are a crucial way to reach customers, local, regional or global. It can take some experimenting to get it just right.

Invest In Training: As the world changes, so does business. Ensure your employees are at the top of their game when it comes to both industry standards and the way you do business. Keep them educated on best practices and make sure training is consistent across the board.

Invest In Your Team: Your employees make your business work. You want to make sure they're operating at their best. Offer a healthy work environment that promotes their well-being. It can be as simple as offering great perks like flexible hours, remote work, professional development, catered lunches – the list goes on. Happy employees are the best employees. *Smallbiz Technology, 2/12/2019*



ARE YOU MAKING THESE MISTAKES WHEN TEXTING IN YOUR BUSINESS?

Do you text clients? Do you text clients after business hours? A recent report by Carphone Warehouse found that 73% of respondents had no problem texting with clients after business hours. However, this can lead to serious issues, namely when it comes to drawing the line when communicating with clients (or employees). It breaks the professional barrier. After-hours texting says you're available 24/7. It can intrude on your personal life, and when you don't text back, it can harm that professional relationship. If you must text, treat it like an email: stick to working hours and keep it business-focused.

Don't open doors to unprofessional behavior. Texting is a very casual form of communication, and it's easy to forget you're chatting with a client or employee. You must be careful about what you say, especially if you're in a management position. Keep it professional and courteous. *Small Business Trends, 7/8/2019*

USE THESE TOP TIPS TO FUEL YOUR PRODUCTIVITY

Stress can be a burden on your productivity, but there are ways you can use it to your advantage and turn it into something positive. Here are three tips to do just that:

Continued on page 3