

What's New



Keep your family safe with Security Center. They are a full service home and commercial security company servicing Central Florida for over 35 years. Security Center installs and services some of the most advanced fire, burglar, and video surveillance alarm systems in the area. Contact them at **386-427-8007** www.securitycenterflorida.com



Keep your family safe with Security Center

Our in-house 24-hour monitoring ensures responsiveness.

CALL 386.427.8007 NOW

Upgrade your security system to a fail safe cellular monitoring.

March 2023



This monthly publication is provided courtesy of Chris Kane president and founder of HALIFAXtec.

Providing the best solutions to make sure your technology is safe and running smoothly. We're your one-stop-shop for IT Service and Support. We make technology work for you, instead of you working on your technology!



Improve Your Cyber Security Awareness

Learn About Today's Most Common Types Of Cyber-Attacks

If you've turned on the news sometime during the past few years, you've probably heard of more than one instance where a business closed due to a cyber-attack. You may think your business is small enough and hackers won't target you, but this couldn't be further from the truth. Every business is at risk of experiencing a cyber-attack and should be well-prepared to defend against these threats. With the right type of attack, a cybercriminal can gain valuable information about your business, customers and employees, which can be used to damage your reputation and hurt you financially.

If you're a business owner or leader and you want to ensure your business is well-protected, check out the most common cyber-attacks that are affecting companies today. From there you can implement cyber security plans and tactics to ensure your business is protected from cybercriminals.

Phishing Scams: Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure. Phishing scams can wreak havoc on your business and personal life. You may have seen an e-mail from someone claiming to be Amazon or your credit card company asking for specific sensitive information. Often, the e-mail address does not line up with who the person is claiming to be.

When a phishing scam targets your business, they'll likely request valuable information from your employees such as passwords or customer data. If your employees fall for the scam, they could give a cybercriminal unprecedented access to your network and systems. This may also allow the cybercriminal to steal private employee and customer

Continued on pg.2

Continued from pg.1

information, leaving your employees vulnerable to identity theft. Phishing scams can be averted by using common sense and providing cyber security training to your employees. Most companies will not request private information over e-mail. That being said, if an employee receives a suspicious e-mail, they should do their due diligence to ensure the e-mail is genuine before responding in any way.

Malware: Malware is software installed on a computer without the user's consent that performs malicious actions, such as stealing passwords or money. There are many types of malware, including spyware, viruses, ransomware and adware. You can accidentally download malware onto your computer by clicking on sketchy links within e-mails or websites. You might not even notice you have malware on your computer right now. If your computer is operating more slowly than usual, web browsers are taking you to random sites or you have frequent pop-ups, you should scan your computer for malware.

Prevention is key in stopping malware from affecting your business. Hiring and utilizing a managed services provider is the best way to protect your business, as they will continually monitor your network for exploitable holes. With malware, it's always better to play it safe than sorry. If a cybercriminal is able to use ransomware on your network, your business could be stuck at a standstill until you pay the ransom. Even if you can pay the ransom, your reputation will still take a hit, and your business could be greatly affected. Be careful where you click on your phone, too, since malware attacks on cellphones have become more common over the past few years.

access your network or computer systems? They most likely use a password to log in to their computer, access their e-mail and much more. What would happen if someone with bad intentions gained access to one of your employee's passwords? Depending on the individual's access, they could obtain sensitive information about your business, customers and employees.

"Every business is at risk of experiencing a cyber-attack and should be well-prepared to defend against these threats."

Your team should be using complex, random phrase passwords for their accounts, and each password for every account should be different. Providing a password manager for employees to use will allow them to create the most complex passwords possible and keep track of them more easily. You can also incorporate multifactor authentication to ensure nobody can steal a password and gain access immediately. You should make your employees aware of this during your annual cyber security training.

If your business falls victim to a cyber-attack, it could have lasting consequences for everyone involved. Now that you know the most common types of cyber-attacks, you can start implementing plans to ensure you and your business stay protected.

Free Report Download:

The Business Owner's Guide To IT Support Services And Fees

You'll learn:



- The three most common ways IT companies charge for their services and the pros and cons of each approach
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate

Claim your FREE copy today at www.halifaxtec.com/thank-you-itbuyersguide



Chat GPT is a language model developed by OpenAI that can generate human-like language in various contexts using deep learning techniques. It has been pre-trained on massive datasets such as the Common Crawl and Wikipedia, enabling it to understand language structure and syntax. Chat GPT is useful for applications like language translation, text summarization, and chatbot development, and has the ability to continually learn and improve over time. It represents a major breakthrough in natural language processing and has the potential to transform communication with computers. This technology will continue to improve over time, so stay tuned!

The Funny Pages



Don't Come Back To Work

Don't come back to work, instead, move forward in leading your company and your career by embracing remote work. ghSMART has been remote-only for 26 years, I never fully realized how enthusiastic I am about remote work until I heard that companies are forcing workers to come back into offices.

Before the COVID-19 pandemic, "work where you want" was a rare concept – but during the pandemic, basically every company that could function with people working remotely shifted to that mode out of necessity. I thought that mode would stick, and we'd see the landscape of cities shift from "places people go to work every day" to "places people go to work sometimes, eat, shop, learn and play." But it seems I was wrong.

There isn't a great argument against the idea of remote work, but there is one *for* it. Remote work improves financial and operating performance and productivity for companies while also improving job and life satisfaction for employees. A 2015 study published in the *Quarterly Journal of Economics* showed a 13% performance increase from remote working, and employee attrition rates fell by 50%.

Even with all of the research information available that shows remote work is beneficial, there are still some myths floating around. For example, many say you can't build a great company culture when your business operates remotely. This is entirely false. I think an excellent culture begins with doing what's best for people. Making people commute to



offices daily does not seem to be in anybody's best interests.

Another common myth states that people don't work as hard remotely as they do in an office. I believe that if you have a transparent culture where performance is measured, you can pay people according to the value they are creating. They will be incentivized to work productively and not lollygag – even if they are working remotely. But I guess many companies have not yet figured out how to pay employees based on a scorecard of measurable results and instead pay based on hours worked. They should be worried about lollygagging anyway, both in the office and for people who work remotely.

If you run or own a company, please continue to experiment with allowing your people to work remotely when possible. I believe this is the future of work, both because of the demonstrable benefits to companies in operating and financial performance and the benefits to workers due to having more control over their time.



Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times bestsellers. He stays active in his community and has advised many

2 Selling Strategies Your Business Should Avoid

In the world of business, there are good and bad selling strategies. Strong selling strategies bring your customers back for more and encourage them to refer their friends and family. In contrast, poor strategies will send your customers running for the hills. They'll never look back at your business and will tell everyone about their negative experiences. If you or your selling team are utilizing any of the following strategies when selling to customers, you should put a stop to it immediately, or your sales will begin to decline.

Not Addressing The Customer's Main Problem: When customers approach you for a specific product or service, they most likely have a reason for coming. Listen to your customers' concerns rather than overexplaining your product or service. If you provide a solution to their problem, you'll likely earn a sale.

Arguing With Customers: Has a customer ever said something unreasonable or completely wrong about your product? You might have been quickly

defensive, but starting an argument with a customer will never lead to a sale, even if you're right. Listen to them and figure out where they're coming from before responding.

BECOME A BETTER BUSINESS LEADER BY DITCHING THESE HABITS

You want to be the best leader possible if you own or operate a business, but you may have developed habits over the years that are preventing you from being your best. As you grow in your role, you must overcome habits and certain ways of thinking that might impede your progress. If you're utilizing any of the following habits, it's time to change the way you're approaching things.

Black-And-White Thinking: There is plenty of grey in the world of business. You can't look at things as being one way or another. There are many different ways to approach each problem.

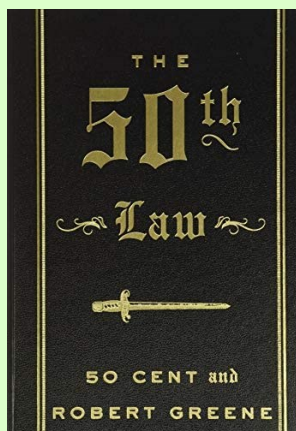
Your Opinion Matters More: You must listen to your team if you hope to be a great leader. You won't be right with every decision. Hear suggestions from your team and make an informed choice in order to determine the best path for your business.



The 50th Law By 50 Cent and Robert Greene

Fear is one of the greatest obstacles any entrepreneur or business leader will face. They fear they'll make a mistake that will cost their business thousands of dollars, or they might worry their product or service isn't good enough. These fears can become so intense they could even cause a business to fail.

Many entrepreneurs have tried to overcome their fear, and now *The 50th Law* by Robert Greene and 50 Cent is here to help. *The 50th Law* explores the concept of fearlessness and takes a deep dive into courageous entrepreneurs who held nothing back in order to achieve their goals. 50 Cent shares the business and personal plans that helped him escape poverty and the chronic fear he felt in his early years. This philosophical read is definitely worth checking out because it will encourage readers to put fear in the rearview mirror.



Want To Improve Your Business? *Track These 2 Key Performance Indicators*

Many businesses determine their level of success by looking at specific key performance indicators. Some popular KPIs include tracking revenue, customer satisfaction, lead generation and client retention rate. But not everyone knows there are several other KPIs worth checking out for their businesses. Below are two KPIs your business should track if you aren't already.

Contact To Customer Conversion Rate: How many times does your team have to reach out to a potential customer before making a sale? The fewer touches your team has before a sale, the better their approach may be.

Churn: How many customers do you lose each month? By tracking this KPI, you'll recognize when customers are dropping off so you can make the necessary adjustments to keep them.