The Tech chronicle

What To Do?

Michigan in February is many things, including icy, cold and gray, however, in the middle of winter, we also find natural beauty and unique seasonal fun.

All the fun things to do in Michigan can turn an otherwise simple chilly day into an exciting adventure filled with winter sports like ice skating, amazing winter art, or extraordinary and unique events. Go explore and have some winter fun with these great ideas!

Plymouth Ice Festival-February 3-5, 2023. Did you know the Plymouth Ice Festival is one of the largest free ice festivals in Michigan? Be sure to check out the lit ice gardens in the evenings. The Plymouth Ice Festival is one of our favorite Michigan events this weekend!

Hartland Township Winterfest – Heritage Park, February 11, 2023, beginning at 1:00 p.m. Celebrate the winter season! Bring your family to enjoy sledding, entertainment, food, and ice skating. The night will conclude with fireworks show at dusk. Activities will be held at and around Hartland's Heritage Park, located at 12439 Highland Road.

Autorama-Detroit, Huntington Place / Cobo. February 24 -26, 2023. Check out sweet rides, vendors and eats! We love this show and will be there again this year!
Hawk Island Park - Michigan Snow Tubing in Lansing with Magic Carpet!Located at 1601 E Cavanaugh Rd, Lansing, MI 48910. East of Grand Rapids. Hawk Island is one of Michigan's most popular snow tubing destinations. Make your reservations early. Rush down one of their several thrilling 16 ft wide sculpted snow lanes and drop 50-60 feet over a course of 500-600 feet! A magic carpet uphill conveyor lift will bring you back to the top of the hill to do it all again! Snow making machines are used. Enjoy their outdoor fires with hot chocolate, s'mores and other snacks. There is a vehicle entrance fee at Hawk Island.

February 2023

This monthly publication provided courtesy of Dennis Jock of DenBe Computer Consulting.

Did you Know?

Alpena is the home of the world's largest cement plant.

Give Your Business The Protection It Needs

With Cyber Insurance

Being at risk for cyber-attacks is a growing concern among small-business owners. Cybercriminals often target small businesses because they hold sensitive information and have weaker security infrastructures than larger businesses. For this reason and more, it should be no surprise that 88% of small-business owners feel vulnerable to a cyber-attack, according to a recent survey conducted by the U.S. Small Business Administration.

To protect your business and your customers, you must implement strong cyber security practices in your business. You need to run your employees through annual cyber security training so they know the newest cyberthreats and how to avoid putting the company at risk. You should also utilize a firewall, back up your data on all computers, secure your WiFi networks and ensure your entire team understands the importance of strong passwords.

To give your business an extra layer of protection, though, you can get cyber insurance coverage.

Cyber insurance, often called cyber liability insurance, covers the damage your business suffers if you're the victim of a cyber-attack or data breach. Here are a few areas where having cyber insurance can help.

Ransomware Attacks
Imagine that a cybercriminal gains access to sensitive information, such as your employees' Social Security numbers or your customers' credit card numbers. You know the release of this information could cause irreparable harm to your business, and you're willing to pay whatever it costs to prevent this from happening. This is the goal of ransomware attacks. Hackers threaten to publish sensitive information or lock you out of vital programs if you don't pay them. Cyber insurance will help you pay the ransom.

Continued on pg.2

Continued from pg.1

Customer Outreach

If sensitive customer information gets stolen from your business, you have a legal obligation to inform your customers. The average cost of notifying customers of a breach and other post-breach responses is $1.72 million, according to the Ponemon Institute Cost of Data Breach Study. That's a cost most small businesses cannot afford, but cyber insurance will help cover it.

Data Recovery

If your business becomes the victim of a data breach, you're going to want to get that information back. Your policy can protect you and your employees from identity theft, as your insurance provider may pay for identity recovery services. These are invaluable services, since data and identity recovery can take years to handle on your own.

Cyber insurance can also help cover the costs of customer and employee lawsuits after a data breach, lost income due to network outages and even regulatory fines. Most cyber insurance policies come with exclusions to which you need to pay attention. Your policy will probably not cover attacks that happened before your coverage started, future profits affected by a data breach or the loss of valuation after a cyber-attack.

> **"Cyber insurance providers like to provide coverage to businesses that are proactive with cyber security practices."**

But how do you get cyber insurance for your company? You have to meet certain qualifications to get a policy, due to the rise in cyber-attacks and cyber security awareness. Every cyber insurance provider will look at the strength of your network security before considering your business for coverage. If your network is weak and at a high risk of being targeted, they are not going to take a chance on you.

If your business is within an industry that requires cyber security compliance, make sure you're compliant. If you're not, cyber insurance providers won't even give your business a second thought before rejecting your application for coverage. This shouldn't be an issue, as most businesses stay compliant, but double-check your requirements to ensure all your bases are covered.

If you're considering cyber insurance but are worried about the cost, you can do a few things to make it more affordable. Cyber insurance providers like to provide coverage to businesses that are proactive with cyber security practices. Implementing an incident response plan will show providers your business has procedures in place to handle emergencies if they arise. Researching all third parties you work with and showing they have strong cyber security practices will also benefit you.

Cyber insurance can be an incredibly beneficial cyber security element to add to your business. As new cyber-attacks and threats continue to develop, it's essential to get all of the protection you possibly can.

Common Phishing Attacks

Phishing is among the biggest cyber threats facing organizations.

One of the most frustrating things about this is that most people know what phishing is and how it works, but many still get caught out. The growing sophistication of phishing scams has contributed to that. They might still have the same objective – to steal our personal data or infect our devices – but there are now countless ways to do that.

1. Email Phishing: Most phishing attacks are sent by email. The crook will register a fake domain that mimics a genuine organization and sends thousands of generic requests.

The fake domain often involves character substitution, like using 'r' and 'n' next to each other to create 'rn' instead of 'm'.

In other cases, the fraudsters create a unique domain that includes the legitimate organization's name in the URL. The example below is sent from 'olivia@amazonsupport.com'. The recipient might see the word 'Amazon' in the sender's address and assume that it was a genuine email.

There are many ways to spot a phishing email, but as a general rule, you should always check the email address of a message that asks you to click a link or download an attachment.

2. Spear Phishing: There are two other, more sophisticated, types of phishing involving email.

The first, spear phishing, describes malicious emails sent to a specific person. Criminals who do this will already have some or all of the following information about the victim:

Their name, place of employment, email address and specific information about their job role. The fraudster has the wherewithal to address the individual by name and (presumably) knows that their job role involves making bank transfers on behalf of the company. The informality of the email also suggests that the sender is a native English speaker, and creates the sense that this is a real message rather than a template.

3. Whaling: Whaling attacks are even more targeted, taking aim at senior executives. Although the end goal of whaling is the same as any other kind of phishing attack, the technique tends to be a lot subtler.

Tricks such as fake links and malicious URLs aren't helpful in this instance, as criminals are attempting to imitate senior staff.

Whaling emails also commonly use the pretext of a busy CEO who wants an employee to do them a favor. Emails such as this might not be as sophisticated as spear phishing emails, but they play on employees' willingness to follow instructions from their boss. Recipients might suspect that something is amiss but are too afraid to confront the sender to suggest that they are being unprofessional.

4. Smishing and Vishing: With both smishing and vishing, telephones replace emails as the method of communication.

Smishing involves criminals sending text messages (the content of which is much the same as with email phishing), and vishing involves a telephone conversation.

One of the most common smishing pretexts are messages supposedly from your bank alerting you to suspicious activity. These messages suggest that you have been the victim of fraud and tells you to follow a link to prevent further damage. However, the link directs the recipient to a website controlled by the fraudster and designed to capture your banking details.

It's one thing to help a client identify a problem, but it's another to help them solve it. You'll need to convince clients to accept your expertise to solve their problems. Many intelligent people struggle with closing deals, so I devised the following three strategies to help anyone become a better closer.

Summarize The *Underlying* Need

I once went into the office of a greatly admired billionaire CEO with a colleague. He had been asked to come strategize for 90 minutes on how to identify and solve the CEO's top leadership problems. The CEO talked about scary changes in his industry while laying out his heart about his team and their strategies. When he stopped talking, my colleague was presented with the perfect opportunity to summarize the client's underlying need. Instead, he directly asked the CEO what he thought the next steps should be. The CEO was unamused and said, "Well, I don't know. I was hoping you might tell me."

My colleague should have taken a moment before responding to analyze the emotion behind what was just told to him. Once the client realizes you understand their situation, they're more likely to listen to your plan of action.

Say What You Plan To Do

Smart people worry about putting themselves out there by offering a plan. They fear that another smart person is going to disagree with them. They worry about proposing a plan that doesn't work. That's why many advisors stay "safely vague" rather than offer a specific plan. But being vague doesn't help leaders solve their biggest problems. You must have the courage to propose a plan. The key is to be as specific as possible. Break down your ideas and lay them all out. If the client has concerns about any areas, you can address them, but they'll be happy to see the wheels are turning in your mind as you come up with solutions to their problems.

Ask If They Want Your Help

So many smart people get a gag reflex when it comes time to ask for the sale. They think selling is evil. They don't view themselves as salespeople. And besides, if a client realizes how great a consultant is, they will ask for the sale themselves, won't they? But business doesn't happen that way. The client wants to know you want to help. It's *their* insecurity that often holds the client back from closing themselves. That's why you have to do it. And don't view it as selling – view it as an offering of help. Don't you think it's nice to offer to help somebody accomplish something important to them?

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 government officials.*

Keep Your Customers Happy By Avoiding These 3 Selling Strategies

You've probably been on the receiving end of some poor sales strategies without even realizing it. For example, a salesperson said something that rubbed you the wrong way, sending you out through their doors and into the arms of a competitor. While it might have been a frustrating experience for you then, it's much worse if you or your sales team use these tactics in your business.

You want your customers to enjoy working with you, so you and your sales team must utilize strong sales strategies. Here are three selling tactics you want to avoid at all costs.

Not Addressing The Customer's Primary Problem: Customers rarely walk into a place of business on a whim anymore. They usually have a very specific problem they need help to solve. Fully listen to their concerns and provide a solution to their problem. Do not push your products or services down the customer's throat if they have nothing to do with their dilemma.

Overpromising And Underdelivering: Some salespeople think the key to boosting sales numbers is to promise their customers the world, even if what they're promising is impossible. If you fail to deliver on your promise, you're essentially lying to your customers, which destroys their trust in your business.

Arguing With Customers: You may know your product or service better than your customers, but that doesn't mean you should combat them if they have concerns or unrealistic expectations. Stay silent and ask questions about what they need. The second you start arguing with them, you've lost the sale.

"I think these, 'take your kid to work' days are just a ploy to get free tech support."

How To Make A Positive Experience For Unhappy Customers

When a customer is upset with your business or team, you may think there's no way to sway their opinion. This couldn't be further from the truth. You have the power to please and change the views of unhappy customers. By utilizing the following strategies, you'll know how to handle displeased customers and maybe even turn them into lifelong clients.

Listen To Them. Your customer's complaint likely has nothing to do with you personally, but how you respond to them can make or break their lifetime value. Be empathetic and listen to what they say.

Be A Creative Problem-Solver. After you hear the concerns or complaints from your clients, ask yourself if their problem is solvable. In most cases, it is, but it will require some brainstorming. Think outside of the box and deliver exceptional service, and you'll gain a customer for life.

Work Efficiently To Solve The Problem. When you get a complaint from a customer, don't sit on it. They want an immediate solution or response, so take a minute to think and come up with a solution that works for everyone.