

The Tech chronicle

Fun in March

March is an exciting month- not only does it usher in spring but there are some great things happening in Michigan. Check out these fun and unique events.

Butterflies Are Blooming, Frederik Meijer Gardens and Sculpture Park, 1000 East Beltline NE, Grand Rapids, MI-Dates March 1- April 30, 2023. How long are butterflies at Frederik Meijer Gardens? About a month! Be wowed by 7000 tropical Butterflies of 50 different species!

Scooby-Doo!™ Mansion Mayhem - at The Henry Ford. February 12, 2023-April 9, 2023, Time: 9:30 a.m.-5 p.m. in The Gallery by General Motors.

Milford Maple Syrup Events, February 26, 2023 and March 4, 5, 11, 12, 18, 19, 25 and 26, 2023 from 11:00 to 3:30pm. at Kensington Metropark located at 4570 Huron River Parkway, Milford, MI

St. Patrick Parade Corktown Races, Michigan Central Station, Detroit, MI. March 12, 2023. The Corktown Races have become one of the largest 5 km races in Michigan.

Spring Tea and Tour - at the Ford House, March 19, 2023 and March 23, 2023 at 12 p.m. 1100 Lake Shore Road, Grosse Pointe Shores, MI 48236. Enjoy an elegant tea service with small bites and sweets in the Ford House's beautiful Lake Shore Room overlooking Ford Cove and Lake St. Clair. After the tea, take a stroll at your own pace through the historic home and spend time enjoying the grounds.

March 2023



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

Did you Know?

Michigan ranks first in state boat registrations.



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 information, leaving your employees

Continued on pg.2

Continued from pg.1

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.

Attacks Involving Passwords

How do your employees 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.

Your team should be using long, complex passwords for their accounts, and each password for every account should be different. Encourage your employees to use password managers that 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.

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

Do You Safeguard Your Company's Data And Your Customers' Private Information BETTER THAN Equifax, Yahoo and Target Did?



If the answer is "NO" – and let's be honest, the answer *is* no – you are leaving yourself and your company open to massive liability, *millions* in fines and lost business, lawsuits, theft and so much more.

Why? Because you are a hacker's #1 target. They know you have access to financials, employee records, company data and all that juicy customer information – social security numbers, credit card numbers, birth dates, home addresses, e-mails, etc.

Don't kid yourself. Cybercriminals and hackers will stop at NOTHING to steal your credentials.

Why Not Take 4 Seconds Now To Protect Yourself, Protect Your Company And Protect Your Customers?

Our 100% FREE and 100% confidential, exclusive CEO Dark Web Scan is your first line of defense. To receive your report in just 24 hours, visit the link below and provide us with your name and company e-mail address. Hopefully it will be ALL CLEAR and you can breathe easy. If your company, your profits and your customers are AT RISK, we'll simply dig a little deeper to make sure you're protected.

Don't let this happen to you, your employees and your customers. *Reserve your exclusive CEO Dark Web Scan now!*

Get your free Dark Web Scan TODAY

<https://www.denbeconsulting.com/dark-web-scan/>

Get More Free Tips, Tools and Services At Our Website: www.denbeconsulting.com
(810) 207-3188

Your Business NEEDS Cyber Insurance

Establishing effective and efficient cyber security policies is one of the most important aspects of protecting your business. We often discuss why cyber security is so important and the different cyber security practices your business can implement. We also mention how advanced cyberthreats and cyber-attacks have become as hackers improve their tactics and technology. For this reason, you may wonder if there's anything that will cover your business if it falls victim to a cyber-attack even though you have strong cyber security practices in place. Thankfully, cyber insurance is available to business owners who have proven they take cyber security seriously. Cyber insurance (sometimes referred to as cyber liability insurance) is the coverage an organization can acquire to protect against losses incurred by a data breach or other malicious security incidents. Cyber insurance policies differ from provider to provider, but most will include the following coverages:

Customer And Employee Outreach -If your business is the victim of a cyber-attack and precious information is stolen, who are some of the first people you need to contact? Your customers and employees, of course. They need to be aware that a cyber-attack occurred, and their information may have been compromised. **Recovering Stolen Data** -It can be costly to hire a data recovery professional to recover stolen customer or business information, but it is necessary after suffering a cyber-attack. Most cyber insurance policies will pay for a professional's help.

Software Hardware Repair/Replacement -Cybercriminals can wreak havoc on your software and hardware. If they damage or corrupt your computers, network or programs, your cyber insurance policy will help cover the cost of repair or replacement. Some insurance policies will also cover any financial loss due to business interruption caused by a cyber-attack and ransomware demands.

Cyber insurance will not cover your system upgrades, estimated future financial losses due to a breach or decreased valuation of your business caused by a cyber-attack. It's vital you know exactly what is covered by your policy before beginning coverage. Starting a new cyber insurance policy is easier said than done. Since cyber insurance has grown in popularity, most providers have become more selective about who they cover, meaning you have to meet some criteria to qualify for a policy. The most essential thing any cyber insurance provider will look at will be the strength of your current network security and cyber security practices. Ensure you utilize multifactor authentication throughout your entire business and hold training sessions annually with your team. Purchase a firewall and do whatever else you can to improve your security. If you don't, the rates for your policy will be astronomical, if you can even get one at all. Suppose your business is within an industry that requires a certain level of cyber security compliance. In that case, you should be meeting your requirements or else you won't qualify for a cyber insurance policy. This shouldn't be an issue for your business since you must be compliant regardless of your interest in cyber insurance. Just make sure you look into your compliance requirements before applying for a cyber insurance policy to ensure you don't get denied coverage. If you work with third-party vendors, you must do your due diligence and ensure they meet their cyber security requirements. Doing thorough research on the parties you interact with will help you get more affordable cyber insurance rates. Additionally, it would be best if you had an incident response plan in place. The insurance provider needs to know you're prepared to help your customers and your business if disaster strikes. Cyber insurance can help further protect your business if you become the victim of a cyber-attack. In today's society, where every business and their customers' information is a target for cybercriminals, make sure you're as secure as possible. Build a strong cyber security plan and apply for cyber insurance to get maximum protection.

Don't Come Back To Work

Don't come back to work. Instead, move forward in leading your company and managing your career by embracing remote work. Even though ghSMART has been remote-only for over 26 years, I never fully realized how enthusiastic I am about remote work until I heard that many 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 Stanford University 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 and 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



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.

Working Remotely? **Improve Your Work-Life** **Balance In 3 Steps**

As many businesses continue to utilize remote workers, some employees are struggling to find a proper work-life balance. They constantly find themselves drawn back to their work after completing all tasks for the day, which takes away from their ability to enjoy hobbies or spend time with their families. Maintaining a proper work-life balance is beneficial to all aspects of our lives, including productivity and overall happiness. If you're struggling to maintain your work-life balance, here are three ways to include more personal time in your daily routine.

Set Boundaries: Don't allow yourself to be pulled back into work. Turn off your work phone and e-mail when your shift has ended for the day.

Create A Workspace: Do not work in the same areas you use for relaxation. This will make it more difficult to relax when you've finished working.

Dress Professionally: It might be tempting to wear sweatpants while working from home, but try to wear the same clothes you would wear if you had to go into an office. When the workday comes to a close, you can dress in more comfortable clothing, allowing you to easily unwind.

Is Your Workplace
Becoming Toxic? Watch Out
For These Warning Signs!

Over the past year, the idea of toxic workplaces has garnered quite a lot of attention. No employee wants to work in a toxic workplace and no business owner wants to run one, but how do you know if your business is gradually becoming more toxic? Here are a few warning signs to watch out for.

Mass Turnover: Are employees quitting in droves? Do you know why? You should be holding exit interviews with the employees who are leaving to determine why they want to work elsewhere. Allow them to speak openly, and you'll gain valuable insight.

Low Employee Morale: If your employees are not enthusiastic about their work or tend to work on individual tasks more often, you may have a morale problem. Hold a meeting with your team and allow them to speak freely to understand where the morale issue stems from.

Gossiping Employees: Are your employees talking negatively about each other or the business? If so, you must catch and correct it as soon as possible. Figure out why gossip has increased at your company and develop solutions to solve



"According to IT, the security leak is coming from your workstation."