The Tech chronicle

Fall Is Here!

Fall is here and we are loving the break from the summer heat. Aside from going the cider mill and touring our beautiful state to see the fall colors- we've found some fun events for everyone!

Movie in the Cemetery, annual Movie in the Cemetery is a fundraiser held at the historic Redford Cemetery. Come out for a creepy night of Halloween fun! Oct 8, 2022, 7:30 PM -11:30 PM. Location: Redford Cemetery, 15940 Telegraph Rd, Redford Charter Township, MI.

28th Annual Appleumpkin Festival, October 8th and 9th, 2022, Festival Hours: Sat. 9-6 and Sun. 10-5 Tecumseh, MI. Fun for the entire family! Midway rides & carnival games, inflatables (fee), Bungee Jump (fee). Make-it-take-it crafts, corn box and kid's putt putt golf, helicopter rides - (fee) and monster truck rides (fee).

Scarecrow Fest, Frankenmuth, October 15, 16, 2022 and October 22 and 23, 2022. The first weekend of Scarecrow Fest is Dogs Weekend on Saturday, October 15 and Sunday, October 16, with the Rock N Roll K9s Performance Team putting on shows. Scarecrow Fest will also be held the weekend of October 22 and 23, 2022, with the theme of Kids Weekend! Family-friendly festival at Frankenmuth River Place Shops!

Terror on Tillson Street - Tillson Street is located in Romeo, Michigan. If you are near Romeo Michigan, you need to drive down Tillson street after dark...if you dare. This street is famous for their outrageous Halloween decorations during the month of October. Decorating starts mid October and all the finishing touches will be done by October 31, 2022! This group of homeowners come together each year to put together a spooktacular display!

October 2022

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

Did you Know?

Wayne County is the oldest county in Michigan. The county was founded in 1796 and organized in 1815. Wayne County is included in the Detroit -Warren-Dearborn, MI Metropolitan Statistical Area. It is one of several U.S. counties named after Revolutionary War-era general Anthony Wayne.

What Makes A Strong Password?

And Why Do I Need One?

Think about some of your private accounts right now. Chances are that you have an e-mail, social media accounts, bank account and more that are all password-protected. Do you share passwords across different accounts, and are your passwords strong enough to keep cybercriminals away from your private information? If not, it might be time to evaluate.

Passwords offer the first line of defense when someone tries to access your sensitive information. Without passwords, anyone could gain access to your social media account, which could provide them with personal information that could harm you. Even worse, bank accounts would be easily accessible to cybercriminals who are hoping to rob you of your funds.

While many personal accounts are password-protected, your business accounts also need to be properly secured. But this doesn't just exclusively apply to you – it needs to be understood on a company-wide level. Every employee needs to use passwords to keep sensitive business information secure. Think about the damage a cybercriminal could do to your business if they gained access. They would permanently damage your company's reputation while also putting your employees' and customers' private information at risk.

However, it's not enough to simply put a password in place. The passwords you choose need to be complex. But what makes a password complex? A complex

Continued on pg.2

Continued from pg.1

password will utilize a mix of uppercase and lowercase letters, numbers, punctuation and special characters. Additionally, your password should not be related to any personal information, nor should you use dictionary words. Your password should be incredibly difficult for someone to guess, even if they know you well, but you also need to ensure that your password is something you can remember.

In addition to that, even with a complex password, it's likely still not enough protection. Each of your accounts and devices should have a unique password that hasn't been used anywhere else. If you use the same password across all accounts and devices, you're opening yourself up to a pretty extreme cyber-attack if one of your accounts is compromised. All a cybercriminal needs to do is hack your Facebook page, and they will have the password for your bank accounts and e-mail.

You might think that it'd be impossible to remember so many different complex passwords,

> **"Each of your accounts and devices should have a unique password that hasn't been used anywhere else."**

but software is available that can help. The best way to keep track of your passwords is to use a password manager. With a password manager, you only have to remember one master password, and the software keeps track of the rest. It will even help you create complex passwords for your different accounts to ensure that your information is as protected as possible.

If you oversee a team of employees, then it's vital that they understand why creating strong passwords is so important. Your team should have trainings on cyber security practices, including information on creating passwords. If just one employee fails to create a complex and unique password, it could open you up to a cyber -attack.

Creating strong passwords does not have to be difficult. If you're struggling to remember or create strong passwords, use a password manager. Strong passwords will help keep your sensitive information protected.

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/

3 Things Your Workforce Can Do to Help Your Company's Security Health

The biggest cyber security threat that businesses have to tackle is much closer than you'd think. Verizon's 2022 Data Breach Investigations report – found human error to be a key driver in 82% of breaches, which is why it is crucial for businesses to address cyber security awareness in the workplace and ensure that employees are equipped with the right guidance and resources to help minimize the risk to the organization.

When it comes to cyber security, engaging your workforce can be difficult, so focusing on simple but effective best practices is key. Here are 3 behaviors to encourage among your colleagues to best tackle rising cyber threats.

Be an Email Skeptic- According to Cisco's 2021 Cyber Threat Trends Report, phishing is responsible for 90% of attacks. Social engineering tactics are designed to fool humans, so if we consider that human error is the number one cause of cyber incidents, it makes sense that methods like phishing are among the most popular for hackers. It's therefore vital that business employees are wary of emails coming into their inbox and always err on the side of caution.

Advice for your employees- If you receive an email asking you to click on a link, always check the spelling of the URL and the sender's email to see if it's genuine. It can also be wise to consider the language style of the email. If it has a tone of urgency or contains a lot of grammatical errors, you should be very hesitant about opening any links and attachments. If you suspect a phishing email, report it to the security team.

Use MFA- Using Multi-Factor Authentication (MFA) adds an additional layer of security, making it harder for an attacker to gain access. There have been cases where simply using MFA would have prevented an entire data breach. Companies should aim to standardise MFA across company platforms and accounts.

Advice for your employees- MFA may seem like an inconvenience, but that extra step in the login process can make the difference in protecting your identity. You may have noticed that many public providers, such as Gmail, have implemented MFA on their service for most of their subscribers. You should use MFA wherever you can. It is also important to note that your MFA codes should never be shared with anyone, as attackers may also use social engineering techniques to trick you into sharing an MFA code to impersonate you.

Generate Strong Passphrases- The old days of unmemorable passwords has been usurped with passphrases. If your organization has not yet adopted a passphrase approach, there are still some standard practices that can protect the old-style passwords. Password complexity rules need not be the only protective mechanism. Your systems can be protected by adhering to strict password history, reuse, and reset requirements. Your company should have a password policy outlining password guidance and expectations. The policy should be read and acknowledged by employees and should be part of the new employee onboarding process.

Advice for your employees- Just as air-bags and seat belts can add to your automobile safety, you still must practice defensive driving techniques. Similarly, Multi-Factor Authentication is important to protect your identity, however, it is only one piece of a defensive security posture. While the expectation to create long passphrases, can be a source of irritation, it's hugely important for minimizing cyber risk.

Holding Your Team Accountable

Leaders often fail to hold their team accountable. During research for our book, *Powerscore*, we found that only 8% of leaders are good at holding people accountable. One of the main reasons that leaders fail in this area is that when it's done wrong, it makes things more difficult for everyone.

Here's an example: I was giving a keynote speech at a *Fortune* conference a few years back and asked the audience, "How many of you have goals for your teams that are written down?" Only 10% raised their hands. Failure to write down goals opens up the door to confusion. It becomes nearly impossible to hold someone accountable for delivering a result when you have failed to articulate what you're looking for.

In order to hold your team accountable, you need to be specific with goals and use numbers that others provide to measure performance. When I was still a young CEO with ghSMART, I struggled to hold a consultant accountable. She was brilliant and had great technical skills but failed to call clients proactively and didn't follow up with them. Many clients did not ask for her to come back as their trusted advisor.

I called her into my office and told her that she needed to work on her client relationships. She disagreed and stated that her clients loved her work. I said, "Well, one client told me that although he values your work, he feels you treat him like 'processed cheese' and that you rush to finish projects with him and then you move on to your next client project." She said that her work spoke for itself, and the meeting abruptly ended.

This was a huge failure on my part as I failed to set specific, mutually agreed upon goals and used vague wording. I talked about this with a mentor, and he said, "Make sure you have clear goals, in writing, so your consultants know what 'great' looks like. Then have somebody other than you collect data on their performance. Then you can sit down as a coach to review their results vs. their goals."

It was great advice that I immediately put into practice. When you properly hold people accountable, high performers will know they are performing, and they will keep doing what they are doing. And lower performers will know they are not

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.

Leave An Impression On Your Employees And Customers With The Proper Gratitude

How many times do you thank people every day? When a customer buys a product or service from you, you probably say, "Thanks for shopping with us. Please come again!" When a team member completes a task or helps out in any way, you probably also thank them. But are your thanks to customers and coworkers being received as well as you hope? In a time when competitors are right down the street and employees are looking for a company culture that suits their needs, gratitude becomes ever more critical.

It's essential that you work on your thanking skills so your gratitude is well received. You can do three things when thanking someone to make sure your appreciation leaves an impression: always use their name so that they feel personally acknowledged, include what you are specifically thanking someone for and thank people as soon as possible. When your thanks are personalized, specific, and prompt, they mean much more to the person receiving them.

Make Your Meetings More Productive

You're probably in meetings every day if you're a business owner. They can quickly become time-consuming if there is not a solid plan beforehand. If you are always leading meetings, here are a few things you can do to ensure they are as productive as possible.

- Invite only the necessary individuals and teams to the meeting. There's no point in having every employee attend every meeting.
- Create an agenda to keep your meeting from coming off the rails. Send the agenda to the relevant people before the meeting and make it conversational with a step-by-step plan.
- Set a start and end time to keep your day on track. This will tell your employees that you believe their time is valuable.
- Set the time for the meeting when everyone will be alert and ready to discuss the topic at hand. Also, utilize a note keeper so your team can reflect later on what was discussed in case they miss something.
- Set deadlines and create an action plan for your team during the meeting. This sets up accountability so you can ensure everyone will pay attention and play their part.

"Hello, tech support?"