October, 2022

TechSage Tech Talk

Insider Tips to Make Your Business Run Faster, Easier and More Profitable

INSIDE THIS ISSUE:

Keep Your Information Secure Page 1

Celebrate Cyber Security Month Page 2

Shiny New Gadget of the Month Page 3

3 Ways to Keep Up With Digital Changes & Connect With Your Customers Page 3

The Secret To Job Happiness Might Be Who Your Work With Page 3

The Biggest Vulnerabilities That Hackers Are Currently Exploiting Page 3

Want To Know the Secret About Cyber Insurance AND Lower Your Risk? Page 4

5 Mistakes Companies Are Making In The Digital Workplace Page 4

Save Recurring Email Text in Outlook's Quick Parts Page 4

We love technology and We love helping people.

Give me a call to find out whether we can help you better secure your data and get more out of technology.

-John Hill
Founder CEO

Keep Your Information Secure

We use passwords for just about everything. Most of us have to enter a password to get into our computers, then enter more passwords to access our e-mail, social media profiles, databases and other accounts. Even our cell phones and tablets can and should be password-protected. In fact, if you aren't securing all of your devices and accounts with passwords, you should definitely start. It could help prevent your business and personal information from becoming compromised.

Why Passwords?

We use passwords to ensure that those who don't have access to our accounts can't get access. Most of our devices hold large amounts of personal information. Think about the potential harm someone could do if they gained access to your personal cell phone. They would immediately be able to see all of your contacts, pictures and applications. They might even be able to log in to your e-mail, where they could obtain your banking information. If this type of access falls into the wrong hands, it could be detrimental to your life. Passwords offer the first line of defense to prevent others from obtaining sensitive information.

This becomes even more important if you own a business. Each of your employees should be utilizing strong passwords to access company information. If your business is not using passwords – or is using simple passwords – you could be opening yourself up to hackers and cybercriminals. If a cybercriminal gains access to your company's private information through a weak password, they will gain access to customer information, which could damage your reputation and open you up to lawsuits. That being said, everyone within your business needs to utilize complex and unique passwords.

Making A Strong Password

Not all passwords are created equal. When it comes to making a strong password, you must think about it. If you use a password that you can't remember, then it's essentially useless. And if you use a password that's too easy to remember, your password probably won't be strong enough to keep cybercriminals out. Your pass-

Continued on pg.2

Continued from pg.1

word should be long, have a mix of lowercase and uppercase letters, utilize numbers and special characters, have no ties to personal information and should not be a word from the dictionary.

In the grand scheme of things, it's not enough to just create complex passwords. They also need to be unique. In addition to this, you should use a different password for each and every one of your accounts to help maximize their effectiveness. Think about it this way: let's say you use the same password across your business e-mail accounts, social media accounts and bank accounts. If someone decrypts the password for your Facebook page, they now have the password for more valuable accounts. If you can't tell that your social media account was compromised, the cybercriminal could try to use that same password to gain access to more important accounts. It's a dangerous game that can be avoided by using unique and complex passwords for every account you use.

Remembering All Of These Passwords

You may be worried about remembering all of your passwords if you have to create a unique one for each of your accounts. Your first thought may be to write them down, but that might not be the most secure option. If someone gets their hands on your little black book of passwords, they'll immediately gain access to all of your accounts with a handy directory showing them exactly where to go. Instead, you should utilize a password manager to help keep track of all of this sensitive information.

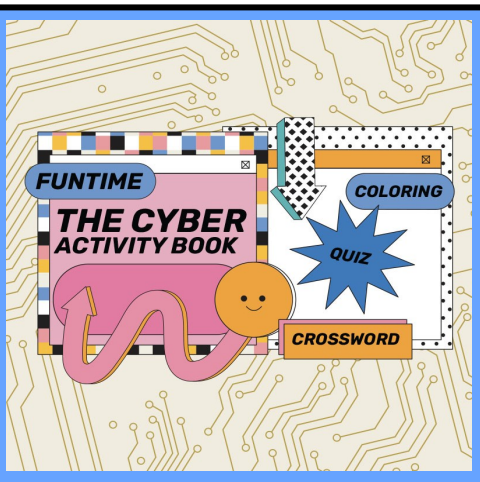
> **"You should use a different password for each and every one of your accounts to help maximize their effectiveness."**

With a password manager, you only have to worry about remembering the master password for your password manager. All of your other passwords will be securely hidden. Password managers also give you the option to create random passwords for your accounts to bolster their security. That way you can have the most complex password possible without worrying about forgetting it. Additionally, password managers can also help remember the answers to security questions and more so that you never get accidentally locked out of one of your accounts. They're easy to use, convenient and secure.

Passwords are an important part of your cyber security plan. Make sure you and your employees are using complex and unique passwords. It can also help you to implement some training so your employees understand the importance of secure passwords. When used correctly, passwords will help deter any would-be cybercriminals from accessing your sensitive information.

Celebrate Cyber Security Month

Enter into our contest by downloading the Cyber Activity Book contest. Complete all pages and return the interactive activity book by October 31 2022 for the chance to not only receive the answers, but also be entered into a drawing to win $100 Amazon Gift Card.



Download and enter the contest to win a $100 Amazon Gift Card

www.techsagesolutions.com/cyber-activity-book/

Shiny New Gadget Of The Month:

It might be surprising to hear, but our toothbrushes are some of the dirtiest items in our households.

There's a good chance that there are more than a million kinds of bacteria living on your toothbrush right now. Unfortunately, rinsing your toothbrush after brushing is only so effective. That's why Bril was invented.

Bril is a portable toothbrush case that sterilizes your toothbrush after every use.

It contains an all-natural ultraviolet light that kills 99.9% of germs on contact. It's simple to use as all you have to do is place your toothbrush inside and close the lid. Bril does the rest.

It's the quickest, most effective and easiest way to ensure your toothbrush head stays clean.

3 Ways to Keep Up With Digital Changes & Connect With Your Customers

Trends constantly change in the world of business, and this has become even more apparent since we entered the digital age.

Digital change can help any business connect with their customers on a closer level when the right steps are taken. Below, you will find a few ways to stay ahead of digital change and connect with your customer base.

- Hire a point person to oversee all of your digital content and respond to customer concerns and questions.
- Use the same social media sites as your customer base so they can find you and connect. This will make future communication easier and help get the word out if you have promotions.
- Ensure that your entire team is aligned with your digital goals.

The Secret To Job Happiness Might Be Who You Work With

If I were to ask you where job happiness comes from, how would you respond? Conventional wisdom says that your happiness at work comes from one of these four sources:

- "Follow your passion" (what)
- "Play to your strengths" (what again)
- "Do something with purpose" (why)
- "Live your values" (how)

It's also true that 95% of career-success books follow one of these lines of advice, but what if they're wrong?

What if your job happiness comes not from ***what*** you do, ***why*** you do it or ***how*** you do it … but instead comes from the people around you? Your bosses, peers, and subordinates all can play a huge role in your job happiness. Let me give you a few examples that support this idea.

I know a talented MBA who works for a public-private partnership with a mission that would make any do-gooder proud. He is planning to quit that job because he feels the firm's leadership disregards the human element of their work, bickers internally and lacks integrity. I'm reminded of a well-researched fact I learned during graduate school: employees don't quit jobs, they quit supervisors.

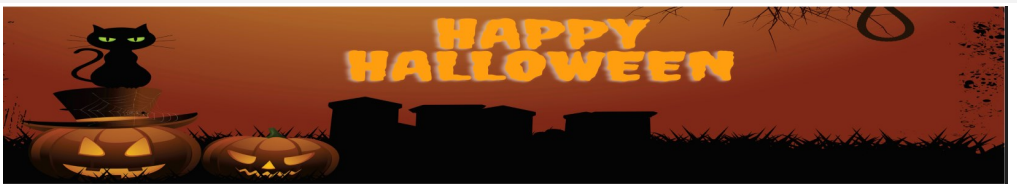
My firm once did a pro bono project for the US Navy where I observed a grueling exercise routine. I asked one of the instructors why anyone would sign up for that – and honestly, I think I expected a response about patriotism. Instead, he explained that they join to be part of a camaraderie. It was a community where they had each other's backs.

If the secret to job happiness is who you work with, then that means you should plan your career differently. Rather than meditate for too long on your passion and purpose, you could think about the kinds of people you really want to be around. Who do you want to be your customers? Who do you want to be your colleagues? What sorts of personalities?

Rather than sourcing job titles, you could be sourcing bosses and colleagues you want to work with. I recently told a young job-seeker, "Don't just go find any old job in your industry. The most important thing you can do right now is to find the right boss – to hire your boss. Hire the best boss in your industry – someone who will teach you, invest in you, tell you the truth, give you real feedback, put energy into helping you discover your ideal path and then help you achieve it."

Once you land your new dream job, be mindful of the time you are spending with the people you want to work with. Don't just track your goals and results, track the time you are spending working with the specific people in your company you want to work with.

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 best sellers. He stays active in his community and has advised many government officials.



THE BIGGEST VULNERABILITIES THAT HACKERS ARE CURRNETLY EXPLOITING

Software vulnerabilities are an unfortunate part of working with technology.

A developer puts out a software release with millions of lines of code. Then, hackers look for loopholes that allow them to breach a system through that code.

The developer issues a patch to fix the vulnerability. But it's not long before a new feature update causes more. It's like a game of "whack-a-mole" to keep your systems secure.

Without ongoing patch and update management, company networks are vulnerable. And these attacks are completely avoidable. 82% of U.S. cyberattacks in Q1 of 2022 were due to exploiting patchable vulnerabilities.

What new vulnerabilities are lurking in products from Microsoft, Google, Adobe, and others? We'll go through several. These were recently noted in a warning by the Cybersecurity and Infrastructure Security Agency (CISA).

Make Sure to Patch Any of These Vulnerabilities in Your Systems

Microsoft Vulnerabilities:

- CVE-2012-4969: An Internet Explorer vulnerability that allows the remote execution of code.
- CVE-2013-1331: This Microsoft Office flaw enables hackers to launch remote attacks.
- CVE-2012-0151: This Windows vulnerability allows user-assisted attackers to execute remote code.

Google Vulnerabilities:

- CVE-2016-1646 & CVE-2016-518: These Chrome & Chromium engine vulnerabilities both allow attackers to conduct denial of service attacks.

Adobe Vulnerabilities:

- CVE-2009-4324: This is a flaw in Acrobat Reader that allows hackers to execute remote code via a PDF file.
- CVE-2010-1297: A FlashPlayer vulnerability that allows remote execution and denial of service attacks. (Flash Player is no longer supported, so you should remove it).

Netgear Vulnerability:

- CVE-2017-6862: This router flaw allows a hacker to execute code remotely.

Cisco Vulnerability:

- CVE-2019-15271: This vulnerability impacts Cisco RV series routers, and gives a hacker "root" privileges.

Patch & Update Regularly!

These are a few of the security vulnerabilities listed on the CISA list. You can see all 36 that were added at https://www.cisa.gov

How do you keep your network safe from these and other vulnerabilities?

You should patch and update regularly. Work with a trusted IT professional (like us) to manage your device and software updates.

This ensures you don't have a breach waiting to happen lurking in your network.

Want To Know the Secret About Cyber Insurance AND Lower Your Risk?

Save the Date

Webinar Details:

LIVE: Thursday, November 17

Start Time: 10:00 AM - 11:00 AM CT

John Hill
CEO
Tech Sage Solutions

Rusty Goodwin
Executive Consultant
MidState Group

5 Mistakes Companies Are Making In The Digital Workplace

The pandemic has been a reality that companies around the world have shared. It required major changes in how they operate. No longer, did the status quo of having everyone work in the office make sense for everyone.

Many organizations had to quickly evolve to working through remote means.

Overcoming the challenges and reaping the benefits takes time and effort. It also often takes the help of a trained IT professional, so you avoid costly mistakes such as:

- Poor Cloud File Organization
- Leaving Remote Workers Out of the Conversation
- Not Addressing Unauthorized Cloud App Use
- Not Realizing Remote Doesn't Always Mean From Home
- Using Communication Tools That Frustrate Everyone

Save Recurring Email Text in Outlook's Quick Parts

Do you have certain emails you send to customers that have the same paragraphs of text in them?

For example, it might be directions to your building or how to contact support.

Stop retyping the same info every time.

Outlook has a feature called Quick Parts that saves and then inserts blocks of text into emails.

- Create a Quick Part by highlighting the text to save in an email.
- On the Insert Menu, click Quick Parts.
- Save Quick Part.

When ready to insert that text into another email, just use the same menu.

Then click to insert the Quick Part.