June, 2022

TechSage Tech Talk

TechSage Solutions

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

INSIDE THIS ISSUE:

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 met more out of technology.

-John Hill
Founder CEO

How To Prepare For Gen Z In The Workforce

Be Proactive And Update Your Cyber Security Practices

Technology has evolved leaps and bounds over the last 20 years. In fact, in the next few years, the first generation to grow up with smartphones and social media, will join the workforce. It might seem like Generation Z will be the most cyber-secure generation, considering they've always had the Internet and other advanced technologies at the tips of their fingers, but reports are starting to show that this is not the case. Many business owners fear that Generation Z's desire to share content online will lead them to accidentally reveal sensitive information that can cause financial, legal and branding damage to their business.

Online scammers have surely taken note of the power that social media influencers have over their fans and followers. Steve Durbin, CEO of the Information Security Forum, believes that organized criminal groups will begin posing as influencers in an effort to manipulate tech-dependent individuals into giving up sensitive information related to their employer. He's not the only business leader who's concerned either.

According to a study from the UK's advisory, conciliation and arbitration service, 70% of surveyed managers were concerned about Gen Z entering the workforce. Instant gratification, resistance to authority and poor face-to-face communication were listed as the main concerns. Additionally, *Entrepreneur* magazine has stated that many Gen Zers struggle to differentiate between friends they've made online and those in the real world. The National Cybersecurity Alliance's Annual Cybersecurity Attitudes And Behaviors Report

Continued on pg.2

Continued from pg.1

stated that millennials and Gen Zers are more likely to experience a cyberthreat. That report also stated that Gen Zers and millennials have had their identities stolen more often than baby boomers. There's good reason for business leaders to be concerned about the next generation entering the workforce.

If you're a business leader who's worried about cyber security and bringing the digital generation into your workplace, don't fret quite yet. There are plenty of things you can do to prepare your business and ensure it stays cyber-secure. You must be proactive if you want your company to keep up-to-date with the best cyber security practices.

One of the first things you'll want to do is implement or update a cybersecurity training program. You need to have every member of your team buy into a cyber-secure culture, and the best way to get them on the same page is with a training program. That way there will be no questions, and cyber security practices won't change from employee to employee. When new employees start, you will already have a cyber-secure culture established, so it will be much easier to train them on your processes.

> **"When new employees start, you will already have a cyber-secure culture established, so it will be much easier to train them on your processes."**

Additionally, you want to ensure that all of your software is receiving its necessary updates. Failing to update software can leave your company vulnerable to cyber-attacks since those updates usually fill any holes that hackers can exploit. When a new software update is released, try not to wait. If your employees use smartphones for work, make sure they have the proper security software installed – and that it stays updated.

Another great option to take care of all of your cyber security and IT needs is to hire a managed services provider. With an MSP, your business will have its data backed up, the reliability and quality of your computer systems will be improved and you'll save time that you can reallocate elsewhere in the business. There's no better or more affordable way to improve your company's cyber security than by hiring an MSP to take care of all of your technological needs.

While the new generation will certainly come with their own set of challenges and obstacles, you don't have to worry about their cyber security practices if you're proactive. Use password managers, hire an MSP and start a training program as soon as possible to jump-start the creation of your cyber-secure culture. We've introduced new generations to the workforce many times before, and Gen Z shouldn't be more challenging than any of the others. There will just be slightly different challenges.

WHY ANNUAL TECHNOLOGY AUDITS ARE ESSENTIAL

Before making key budgeting decisions, it is critical to understand your company's most pressing concerns, particularly those affecting security, compliance and backup solutions.

Regular IT audits can help you with this.

Find out more by downloading the infographic at www.techsagesolutions.com/audits-are-essential/

GOOGLE SEARCH TIPS

One way you can save time on your personal and work-related searches is to learn some “secret” Google search tips.

These help you narrow down your search results and improve productivity by helping you find the information you need faster.

- Search a Specific Website Using “site:” Type in the search bar site:(site url) (keyword)
- Find Flight Information Without Leaving Google. Just type in the flight number and the name of the airlines, for example, type in the search bar American AA 1977
- Look for Document Types Using “filetype:” Type in the search bar filetype: (type) (keyword)
- Get Rid of Results You Don’t Want Using “(keyword)” Type in the search bar (keyword) -(keyword)
- Locate Similar Sites Using “related:” Type in the search bar related:https://website.com

THINGS YOU SHOULD NEVER DO ON A WORK COMPUTER

Save Your Personal Passwords in the Browser

If your company’s network is compromised the malicious actors can leverage your passwords to access your accounts. Side not, you should NEVER store passwords in the browser.

Store Personal Data

This bad habit and leaves your wide open to:

- Loss of your files
- Your personal files being computer-accessible

Visit Sketchy Websites

You should never visit any website on your work computer that you wouldn’t be comfortable visiting with your boss looking over your shoulder.

Allow Friends or Family to Use It

Allowing anyone else to use your work computer could constitute a compliance breach of data protection regulations that your company needs to adhere to.

Confidence

Confidence is an incredibly important trait in the world of business. You may think that all of the great CEOs and entrepreneurs of the last few decades never lose their confidence, but you’d be surprised. New CEOs usually have impostor syndrome and struggle with the idea that they’re good enough for their role. Self-made billionaires often worry that their fortune will take an embarrassing hit. Even private equity investors look at the looming recession and grow concerned.

We often find that leaders are less confident when they obsess about things that are out of their control, rather than taking action in areas where they have some control. *The Wall Street Journal* recently reported that externally, most CEOs are most worried about a recession, global trade and politics. Internally, they’re much more concerned about retaining top talent, dealing with disruptive technologies and developing the next generation of leaders. While it’s good to be aware of the external issues, it’s such more important to master the internal problems within your control.

In order to fully boost your own confidence, you must have a high level of confidence in your team. If you are already confident in your team, keep doing what you’re doing to hire and develop top talent.

If you aren’t confident in them, then you should work on hiring the right people. If you’ve found yourself in this position and you’re simply not confident enough in your team, there are a few things you can do to boost your confidence.

Your first option is to invest your own time into hiring, training and developing your team yourself. You’ll need to set ample time aside so you can truly master the necessary skills to see the best results. Additionally, you can hire a company like ghSMART to do it for you. There are options for an immediate fix that will help adjust your confidence while also building your team’s skills.

Confidence is not necessarily an inherent trait we get from our genes. We can build and grow our confidence skills by taking care of the things we can control. There will always be outside pressures that are out of our control, and there’s simply nothing we can do about it. Instead, focus on hiring and maintaining top talent, developing your company’s digital capabilities and training the next generation of leaders. You’ll see positive results before you know it.

Dr. Geoff Smart is the chairman and 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.*

BOOSTING VOIP SECURITY

Given the variety of threats imposed by attackers on VoIP systems, it's necessary to optimize your VoIP security ASAP.

Here are 6 valuable tips to get you started.

Tip #1. Set Up a Firewall

If spam or a threat comes your way, the firewall will identify and gain control over it, shielding your system shielded from the attack. A good setup will allow the data packets you send to travel unhindered.

Tip #2. Use Strong Passwords

Use randomly generated passwords consisting of at least 12 characters including numbers, upper- and lower-case letters and symbols. Most VoIP phones come with pre-set passwords, often available publicly, change these immediately.

Tip #3. Restrict Calling

Many VoIP attacks happen due to toll fraud. So, if your business runs locally, there's no need to have the international call option enabled. You should also block 1-900 numbers to avoid toll fraud.

Tip #4. Encourage Your Team to Report Suspicious Behavior

You should hold periodical Cybersecurity Training to keep your environment safe at all times. Train your employees how to spot unusual network activity and report suspicious behavior.

Tip #5. Deactivate Web Interface Use

Unless it's absolutely necessary for you to use the web interface, be sure to secure it very strictly. It's enough for a single phone user falling prey to leave the whole system exposed to an external party. All your data can be stolen in text format as a result.

Tip #6. Use a VPN for Remote Workers

Virtual Private Networks (VPNs) are great software that encrypts traffic regardless of your employee's location. You can set up such a network for your remote staff to prevent data leaks and breaches. A well configured VPN won't degrade the call quality.

Got Questions about Cyber Insurance?

Join Justin Reinmuth, CEO and founder of McCormich & Reinmuth Insurance and John Hill, CEO and founder on TechSage Solutions discussing Cyber Insurance and why it is a necessity. This is a FREE Executive Webinar.

John Hill
CEO TechSage
Solutions

Webinar Details:

LIVE: Tuesday, June 14
Start Time: 1:00 pm – 2:00 pm

Justin Reinmuth
CEO McCormick &
Reinmuth Insurance

To register, go the below link:
www.techsagesolutions.com/webinar/

Happy 30th Anniversary UNINTECH
Congratulations Clifford and Elisa