September, 2022

TechSage Tech Talk

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 get more out of technology.

-John Hill
Founder CEO

It's Time For A Refresh!

The 4 Cyber Security Trainings You Must Do With ALL Employees

Students are returning to the classroom now that back-to-school season is officially underway. During the first few weeks, teachers will be reteaching their students the topics they learned in the previous school year to help them regain knowledge they may have forgotten during summer break. But students aren't the only ones in need of a refresher every year. Your employees also need to be refreshed on company policies, values and, most importantly, cyber security practices.

Did you know that human error accounts for 95% of all successful cyberattacks? When a cybercriminal is planning an attack, they look for weak points within a company's cyber security plan. The easiest spot for hackers to exploit is a company's employees.

New cyberthreats are created on a consistent basis, and it's important that your employees know what to do when they encounter a potential threat. If your employees are not routinely participating in cyber security trainings, your business could be at risk, regardless of size.

Every single one of your employees should be familiar with your cyber security practices. When they're hired on, they should go through an initial training that lays out all of your practices, and they should also participate in refresher trainings throughout the year to ensure that the entire team is on the same page with cyber security. At the very least, you should host at least one security training annually. If you've never put together a cyber security training, you may be wondering what topics you need to cover with your team. Below, you will find four of the most important topics to cover.

Responsibility For Company Data

This is your opportunity to explain to your employees why cyber security is so important. They need to understand why cybercriminals are interested in your company's data and what they could potentially do with it. Everyone on your team has a legal and regulatory obligation to protect the privacy of your company's information. When discussing this topic with your team, it's imperative that they know the ramifications of falling victim to a cyber security threat.

Continued on pg.2

Continued from pg.1

Internet Usage

Does your company have restrictions on what websites your employees can use while at work? If not, that's something you should look into. Every device that's used by your employees should have safe browsing software downloaded onto it to prevent them from stumbling upon dangerous sites that could put your company's data at risk. Your employees should know what sites are acceptable to use and that they should not be accessing their personal accounts while connected to your company's network. They should never click on links that are sent from an anonymous source or are found on an unapproved website.

E-mail

If your employees utilize e-mail while at work, it's important that they know which e-mails are safe to open. Employees should not respond to e-mails that are from people they aren't familiar with, as that could be a cybercriminal attempting to gain access to your company's data. Employees should only accept and open e-mails that they are expecting or that come from a familiar e-mail address.

Protecting Their Computers

If your employees have their own personal computers, they should be doing everything in their power to keep them protected. Whenever they walk away from their computer, they should make sure it's locked; they should also never leave their computer in an unsecure location. Also, ensure that your employees are backing up their data routinely and have downloaded necessary antivirus software.

It's of the utmost importance that your team has been fully trained in your cyber security practices. If they haven't, they could open your business up to all sorts of cyber-attacks that will damage your company's reputation from a customer perspective. Your business will also no longer be compliant, and insurance companies may not cover your claims if your team is not participating in regular training.

Ensuring that your team is aware of your cyber security practices and actively taking steps to strengthen your cyber security is the best way to stay compliant and prevent cyber-attacks. If your team is not regularly going through cyber security training, you need to start. It will offer more protection to your business, which will make your customers more comfortable doing business with your company.

> **"Human Error Accounts for 95% of all successful cyber-attacks."**

Cyber Insurance 101 for Small Businesses

Cyber insurance is a type of insurance that protects businesses against financial losses caused by a cyberattack or data breach. While it cannot prevent cyber incidents, it can assist businesses in recovering from the monetary turmoil following a breach.

Download the Infographic below:
www.techsagesolutions.com/what-is-cyber-insurance/

SHINY NEW GADGET OF THE MONTH

Logitech Litra Glow

Zoom calls have become a part of our daily routine regardless of whether you work remotely, in the office or a combination of the two. If you'll be on camera every day, don't you want to look your best? That's exactly how you'll look with the Logitech Litra Glow light. The Litra Glow uses innovative geometry and is frameless to provide more light to the areas within your camera's view. It uses soft and diffused light that's easy on your eyes in case you have to be on the call for an extended period of time. Whether you're on Zoom calls, shooting marketing videos or doing anything else webcam -related, the Litra Glow provides you with perfect light for any situation.

Improve Your Confidence In Your Business By Identifying Your Value

To see success in your business, you need to identify your worth, which will help improve your confidence. Not everyone knows how to identify their value, so we've gathered three tips to help you out.

Understand Your Value – You need to figure out who you want to be in your business and industry. After you fully understand this, it's important to create a solid mission statement that supports your values.

Receive And Give Love – Keep your complimentary reviews from customers to use as a reference point to provide additional support. Also, be sure to find ways to appreciate those who have helped you and your business.

Create A Game Plan – After considering what your offerings are likely worth, whom you're looking to serve and what they'd be willing to pay, you can name your final price.

3 Questions No Leader Should Ever Ask

Over the years, I have advised many board members and CEOs of large companies on their most important leadership issues. In life, people like to think that there aren't inherently right and wrong questions to ask, but I think that's a misconception – especially in the world of business. "Right" questions are the ones that matter. They cut to the heart of the issue and produce an answer that a leader can act on. The "right" questions help leaders get results.

On the other hand, you have "wrong" questions. The mere act of asking these questions can lead you down the wrong path and prevent you from achieving your full potential in your career. Over the years, I've heard the "wrong" questions asked a multitude of times, and they can usually be grouped into three distinct categories.

Ethical Questions

The wisest, most successful leaders I have worked alongside all seem to lead according to this rule regarding ethical questions: "If you have to ask, then don't." In other words, if there is something that makes you feel that it is in the gray area or that taking an action might even be misinterpreted as unethical, then just don't do it. I've never seen a leader regret having held back from taking an action when they had an ethical question. "How unethical would it be if…" is a question no leader should ever ask.

Questions Regarding Underperformance

There is a cycle of "facing reality" that my clients sometimes go through. They have a bold vision: a goal to achieve something great. And when they realize that they don't have the team to make it happen, they start to fantasize and think, "I wonder if Fred or Amy will rise to the occasion and suddenly display strengths or show a burst of energy we have not seen to achieve these results." Subordinates typically follow a very predictable pattern of performance. Great leaders know who they can count on to do what. So you rarely see great leaders asking themselves, "I wonder if my subordinate will suddenly perform well in a role that does not appear to fit their talents and interests."

Questions About Trusting Your Boss

There is a saying that people don't quit companies, they quit bad bosses. So if you find yourself wondering whether you can trust your boss or not, you likely can't. Go find a boss you can trust, one who will hold your interests in high regard. Rarely do you see great leaders staying in roles where they ask themselves, "I wonder if I can trust my boss."

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.

"Nourish the mind like you would your body. The mind cannot survive on junk food." - Jim Rohn

YOU NEED TO WATCH OUT FOR REPLY-CHAIN PHISHING ATTACKS

Phishing. It seems you can't read an article on cybersecurity without it coming up.

That's because phishing is still the number one delivery vehicle for cyberattacks.

80% of surveyed security professionals say that phishing campaigns have significantly increased post-pandemic.

Phishing not only continues to work, but it's also increasing in volume due to the move to remote teams.

Many employees are now working from home. They don't have the same network protections they had when working at the office.

One of the newest tactics is particularly hard to detect. It is the reply-chain phishing attack.

What is a Reply-Chain Phishing Attack?

You don't expect a phishing email tucked inside an ongoing email conversation between colleagues. Most people are expecting phishing to come in as a new message, not a message included in an existing reply chain.

The reply-chain phishing attack is particularly insidious because it does exactly that. It inserts a convincing phishing email in the ongoing thread of an email reply chain.

How does a hacker gain access to the reply chain conversation? By hacking the email account of one of those people copied on the email chain.

The hacker can email from an email address that the other recipients recognize and trust. The attacker also gains the benefit of reading down through the chain of replies. This enables them to craft a response that looks like it fits.

They may see that everyone has been weighing in on a new product idea for a product called Superbug. So, they send a reply that says, "I've drafted up some thoughts on the new Superbug product, here's a link to see them."

The reply won't seem like a phishing email at all. It will be convincing because:

- It comes from an email address of a colleague. This address has already been participating in the email conversation.
- It may sound natural and reference items in the discussion.
- It may use personalization. The email can call others by the names the hacker has seen in the reply chain.

Business Email Compromise is Increasing

Business email compromise (BEC) is so common that it now has its own acronym. Weak and unsecured passwords lead to email breaches. So do data breaches that reveal databases full of user logins.

Tips for Addressing Reply- Chain Phishing

Here are some ways that you can lessen the risk of reply-chain phishing in your organization:

- Use a Business Password Manager
- Put Multi-Factor Controls on Email Accounts
- Teach Employees to be Aware

Microsoft Productivity Score Overview

Productivity can be challenging to track, no matter where employees are working. How do you know they're using their tools as effectively as possible? How can you enable them to adopt best practices?

You can't grade productivity simply by "clock in/clock out" times. In today's hybrid and mobile offices, the value and work product an employee brings is a better gauge. But you also must look at what may be getting in the way of great employees doing great work.

If your company uses Microsoft 365 then you have a tool you can use to find nuggets of productivity gold. This tool is Microsoft Productivity Score.

What Does Microsoft Productivity Score Do?

Microsoft Productivity Score looks at some core areas of your employees' workflow and gives you helpful insights that you can share with your staff. These insights help to boost their performance. It also includes hardware-related information.

You can use this to see if your company tools are holding people back.

How Productivity Score Helps Your Company

- Automatic Metrics Tracking
- Insights to Understand the Data
- Recommended Actions to Take

MS Productivity Score looks at the following areas.

- People Experiences
- Communication
- Content collaboration
- Mobility
- Meetings
- Teamwork
- Technology Experiences
- Endpoint analytics (You need Intune for these)
- Network connectivity
- Microsoft 365 apps health
- Special Reports

Reduce Risk When You Lose a Mobile Device

Few things invoke instant panic like a missing smartphone or laptop. These devices hold a good part of our lives. This includes files, personal financials, apps, passwords, pictures, videos, and so much more.

The things you do in the minutes after missing a device are critical. This is the case whether it's a personal or business device. The faster you act, the less chance there is for exposure of sensitive data.

Steps to Take Immediately After Missing Your Device

- Activate a "Lock My Device" Feature
- Report the Device Missing to Your Company
- Log Out & Revoke Access to SaaS Tools
- Log Out & Revoke Access to Cloud Storage
- Active a "Wipe My Device" Feature

Technology Tools You Should Uninstall

While older technology may still run fine on your systems that doesn't mean that it's okay to use. One of the biggest dangers of using outdated technology is that it can lead to a data breach.

Outdated software and hardware no longer receive vital security updates. No security patches means a device is a sitting duck for a cybersecurity breach.

Get Rid of This Tech Now If You're Still Using It

- Internet Explorer
- Adobe Flash
- Windows 7 and Earlier
- macOS 10.14 Mojave and Earlier
- Oracle 18c Database
- Microsoft SQL Server 2014 (losing support in 2024)