August, 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

Internet Safety Tips For Parents

In today's climate, is there anything more prevalent than the Internet? In fact, we've grown so accustomed to using it that the Internet now seems to help us meet any need or want. Unfortunately, we don't often think about the effect that has on our kids, who have never known a world without this level of technology.

For the most part, the Internet is an incredible boon to our children. They can look up anything they're curious about and will be met with more information than previously fathomed. Many of us remember visiting the library to research topics, and even then, resources were limited compared to what can easily be found online today. While the Internet offers many benefits for kids, there are risks. That's why it's important to keep your children protected. Before your kids get a social media account or dive headfirst into the web, take the following security measures.

Parental Restrictions

Nearly every device that can connect to the Internet has some level of parental control. With computers and laptops, you can restrict what websites and apps your children visit. You can also specify which websites you want totally blocked. This is an option on many tablets and smartphones as well. With those, you can actually set time constraints and limits that make it so your child can only use the device for a certain amount of time, and you can even completely restrict usage at night.

Potential Risks

When your children first start using the Internet, you must ensure they understand any potential risks. We all know people aren't always who they say they are on the Internet.

Continued on pg.2

Continued from pg.1

Similarly, not all information found online is true. When your kids visit websites or use apps, remind them not to share any personal information about themselves. They should never give out their address, school information, phone number or even their e-mail address to anyone online. Even if the person requesting this information claims to be someone they know, they might not be. If your child is using social media, inform them not to accept friend requests from people they don't know. It's important that kids understand all of the risks to ensure they stay safe in the digital and physical world.

Get Familiar

If your children are using the Internet, you should become familiar with the websites and applications they use. Make sure all websites have the little padlock icon by them, which indicates they are safe websites. Look through the apps and websites your children frequent to ensure they're safe for them to use and do not contain any inappropriate content.

> **"Your children's first interactions with the Internet will most likely stem from you, so do your best to set a great example for them."**

Lead By Example

Your children's first interactions with the Internet will most likely stem from you, so do your best to set a great example for them. This is your opportunity to model positive online habits for your children. Your social media posts should also be appropriate and not break any of the online rules you set for your own child. In their eyes, it won't be fair if you or someone else in the family can do things they cannot.

Our children are some of the most important people in our lives, so it makes sense that we would do everything in our power to keep them protected. Just make sure your protective efforts extend from the physical world into the digital world as well.

21 Security Best Practices for Working Remotely in 2022

The global pandemic has forced companies worldwide to rapidly shift and adapt to a primarily remote workforce and decentralized network environments. Unfortunately, employees who are worried about a potentially deadly virus, or who feel underprepared and overwhelmed by the various challenges of working from home, have quickly become the number one target for cybercriminals.

Working remotely is rapidly becoming a new standard operating procedure, which is why we've put together a list of 21 best practices to help you maintain a strong security strategy in 2022, regardless of where or how you get your work done.

Receive your 21 Security Best Practice checklist at
www.techsagesolutions.com/checklist-remote-workforce22/

SHINY NEW GADGET OF THE MONTH

Oura Ring Generation 3

For the past few years, fitness trackers have become all the rage. Between Fitbits and the Apple Watch, nearly everyone has or is familiar with fitness trackers. One of the most common complaints about many fitness trackers is comfort. Oura decided to take the wristband out of the equation with the Oura Ring. The Oura Ring is a fitness tracker that you wear on your finger. It tracks sleep, activity and readiness measurements.

This device is even more accurate than other fitness trackers since the finger is a better spot to record heart-rate data.

Through temperature sensors, a library of informational resources and much more, the Oura Ring is the perfect fitness tracker for just about anyone who is looking to improve or maintain their physical health.

Practicing Self-Care in A Leadership Position

It can be difficult to take your eyes off your business, even for a moment, to focus on yourself and your needs – but it's a necessity. You can't be a successful leader if you aren't properly maintaining your mental and physical health. Thankfully, there are steps you can take if it feels like your work is damaging your personal health.

First, you should acknowledge that you can't do everything on your own. You must work on delegating some of your responsibilities so you can take care of yourself. It's also essential that you create the time and space to care for yourself. Additionally, don't forget to prioritize yourself. Worry about your needs before trying to fix everyone else's problems; this will make things much easier in the long run.

3 Ways to Run Meetings Like A CEO

In my opinion, most meetings are a complete waste of time. Although the relayed information might be important, it isn't always delivered in an effective way, since most managers do not know how to run meetings. Successfully leading huddles or meetings is an important part of building great relationships and leading talented teams. If you want to start getting more from your employees and your meetings, try utilizing the following three methods to run your meetings like a CEO.

Always Request An Agenda

Early in my career, an acquaintance invited me to a business lunch. I can remember wondering, "What does he want to talk to me about?" After a little bit of small talk, he unveiled his agenda. He wanted to sell me a new insurance policy. It ended up being a huge waste of time for both of us. After that meeting, I made sure to only accept invitations that had an agenda – this comes with three distinct benefits. The first is the fact that you can see what will be discussed in the meeting, and you can decline the invite if it doesn't pertain to you or your work. The second is that you can actually prepare for the meeting. The final benefit is that it makes you appear competent. Since you can come prepared, it will look like you have everything under control.

Ask Questions And Avoid Talking Too Much

One of the biggest mistakes managers make when leading a meeting is trying to dominate the conversation. You may be thinking, "Aren't CEOs supposed to tell their attendees what to do in meetings?" The answer is no; the great CEOs don't. In fact, the best CEOs will spend their time asking questions that are strategic, reflective and related to accountability. This helps them brainstorm new ideas with their team, ensure everyone is on the same page and put the responsibility on others so they can follow up in the future.

Discuss, Debate And Decide

The beginning of your meetings should focus on your strategy and what needs to be discussed. After a topic is introduced, CEOs will say things like "Let's debate what we should do about this. Who has some ideas?" That brainstorming will help develop the best solution, and the CEO will then make a decision about what to do or who should handle each responsibility. Your meetings need to be focused on production. If you give people the freedom to speak openly, you will accomplish much more.

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.*

How Using the Slam Method Can Improve Phishing Detection

Why has phishing remained such a large threat for so long? Because it continues to work. Scammers evolve their methods as technology progresses, employing AI-based tactics to make targeted phishing more efficient.

If phishing didn't continue returning benefits, then scammers would move on to another type of attack. But that hasn't been the case. People continue to get tricked.

In May of 2021, phishing attacks increased by 281%. Then in June, they spiked another 284% higher.

Studies show that as soon as 6 months after a person has been trained on phishing identification, their detection skills can begin waning as they forget things.

Give employees a "hook" they can use for memory retention by introducing the SLAM method of phishing identification.

What is the SLAM Method for Phishing Identification?

One of the mnemonic devices known to help people remember information they are taught is the use of an acronym. SLAM is an acronym for four key areas of an email message that should be checked before trusting it. These are:

S = Sender
L = Links
A = Attachments
M= Message text

By giving people the term "SLAM" to remember, it's quicker for them to do a check on any suspicious or unexpected email without missing something important.

All they need to do is run down the cues in the acronym.

S = Check the Sender

It's important to check the sender of an email thoroughly. Often scammers will either spoof an email address or use a look- alike address that people easily mistake for the real thing.

L = Hover Over Links Without Clicking

Hyperlinks are popular to use in emails because they can often get past antivirus/anti-malware filters. You should always hover over links without clicking on them to reveal the true URL. This often can immediately call out a fake email scam due to them pointing to a strangely named or misspelled website.

A = Never Open Unexpected or Strange File Attachments

Never open strange or unexpected file attachments, and make sure all attachments are scanned by an antivirus/anti-malware application before opening.

M = Read the Message Carefully

If you rush through a phishing email, you can easily miss some telltale signs that it's a fake, such as spelling or grammatical errors.

Get Help Combatting Phishing Attacks

Both awareness training and security software can improve your defenses against phishing attacks. Contact us today to discuss your email security needs.

5 WAYS MICROSOFT 365 CAN ENABLE THE HYBRID OFFICE

"Hybrid office" has become more than a buzzword. It is now the reality for many companies. 63% of high-growth companies utilize a "productivity anywhere" hybrid work approach. Here are some of the ways you can use Microsoft 365 to optimize a productive hybrid office:

- **Microsoft Teams & Expanded Features**
  - Webinar Registrations
  - Full VoIP phone system
- **New Meeting Options for RSVP in Outlook**
  - RSVP in person or virtually
- **Better Framing for More Engaging Meetings**
  - The ability to adjust the room view to see faces clearer
- **Using PowerPoint to Present**
  - An upcoming technology called Cameo will integrate seamlessly with Teams and allow you to appear alongside your presentation
- **Speaker Coach**
  - •Personalized feedback on how to improve your presentations

POPULAR SMISHING SCAMS TO WATCH OUT FOR

Smishing is a form of phishing that uses text messages (as opposed to emails) to trick unknowing recipients into clicking a malicious link or otherwise "mining" personal information through their replies.

They became a particularly popular method of attack during the COVID-19 pandemic and preyed on peoples fear and easy spread of misinformation.

Some popular methods include:

- Text Messages Being Sent to You That Spoof Your Own Number
- Problem With a Delivery
- Fake Appointment Scheduling
- Offer of a Free Gift
- Security issue with your account (often impersonates Netflix or Amazon)