VOLUME 4, ISSUE 6 JUNE 2021

MTC TECH TALK

For Humans Not Geeks!

Your resource for the latest technology updates and opportunities for your success.

What's In This Issue?

Meeting Tree Computer
☎ (845) 237-2117

While employees are instrumental when it comes to protecting your business from cyberthreats, they can also become targets for hackers and cybercriminals, without even knowing it.

Here are four ways your employees might be endangering your business and themselves — and what you can do about it.

1. They're Not Practicing Safe And Secure Web Browsing. One of the most basic rules of the Internet is to not click on anything that looks suspicious. These days, however, it can be harder to tell what's safe and what isn't.

A good rule of thumb is to avoid websites that do not have "https" in front of their web address. The "s" tells you it's secure – https stands for Hypertext Transfer Protocol Secure. If all you see is "http" – no "s" – then you should not trust putting your data on that website, as you don't know where your data might end up. Another way to practice safe web browsing is to avoid clicking on ads or by using an ad blocker, such as uBlock Origin (a popular ad blocker for Google Chrome and Mozilla Firefox). Hackers can use ad networks to install malware on a user's computer and network.

2. They're Not Using Strong Passwords. This is one of the worst IT security habits out there. It's too easy for employees to use simple passwords or to reuse the same password over and over again or to use one password for everything. Or, worse yet, all of the above.

Cybercriminals love it when people get lazy with their passwords. If you use the same password over and over, and that password is stolen in a data breach (unbeknownst to you), it becomes super easy for cybercriminals to access

virtually any app or account tied to that password. No hacking needed!

To avoid this, your employees must use strong passwords, change passwords every 60 to 90 days, and not reuse old passwords. It might sound tedious, especially if they rely on multiple passwords, but when it comes to the IT security of your business, it's worth it. One more thing: the "tedious" argument really doesn't hold much water either, thanks to password managers like 1Password and LastPass that make it easy to create new passwords and manage them across all apps and accounts.

> **"Education is a powerful tool and, when used right, it can protect your business and your employees."**

3. They're Not Using Secure Connections. This is especially relevant for remote workers, but it's something every employee should be aware of. You can find WiFi virtually everywhere, and it makes connecting to the Internet very easy. A little too easy. When you can connect to an unverified network at the click of a button, it should raise eyebrows.

And unless your employee is using company-issued hardware, you have no idea what their endpoint security situation is. It's one risk after another, and it's all unnecessary. The best policy is to prohibit employees from connecting to unsecured networks (like public WiFi) with company property. Instead, they should stick to secure networks that then connect via VPN. This is on top of the endpoint security that should be installed on every device that connects to your company's network: malware protection, antivirus, anti-spyware, anti-ransomware, firewalls, you name it! You want to put up as many gates between your business interests and the outside digital world as you can.

4. They're Not Aware Of Current Threats. How educated is your team on today's cybersecurity threats? If you don't know, or you know the answer isn't a good one, it's time for a change. One of the biggest threats to your business is a workforce that doesn't know what a phishing e-mail looks like or doesn't know who to call when something goes wrong on the IT side of things.

If an employee opens an e-mail they shouldn't or clicks a "bad" link, it can compromise your entire business. You could end up the victim of data breach, or a hacker might decide to hold your data hostage until you pay up. This happens every day to businesses around the world – and hackers are relentless. They will use your own employees against you, if given the chance.

Your best move is to get your team trained up and educated about current threats facing your business. Working with a managed service provider or partnering with an IT services firm is an excellent way to accomplish this and to avoid everything we've talked about in this article. Education is a powerful tool and, when used right, it can protect your business and your employees.

Your Tech Tip of the Month — Restart Your Computer!

"Have you tried restarting your system yet?" We've all heard this phrase when dealing with technical support, but have you ever wondered why? View the link below to find out! In the meantime, here are 7 instances when a reboot can really help:

- If your computer feels hot
- If the fans inside your device are making excessive noise
- After completing a software or firmware update
- After you've installed new hardware
- You're experiencing application crashes
- Things are freezing or taking extra long to respond
- A file or application won't open

If you're still experiencing issues with your system after a couple reboots, give the experts at Meeting Tree Computer a call toay at: 845-237-2117. Read more here: http://bit.ly/MTC-TT-Restart-Computer

Did you know... Alexa doubles up as a PA?

Alexa is great for many things. She always reminds us when it's time to take dinner out of the oven. She gives an accurate weather forecast. And she definitely has a good grasp of our music tastes.

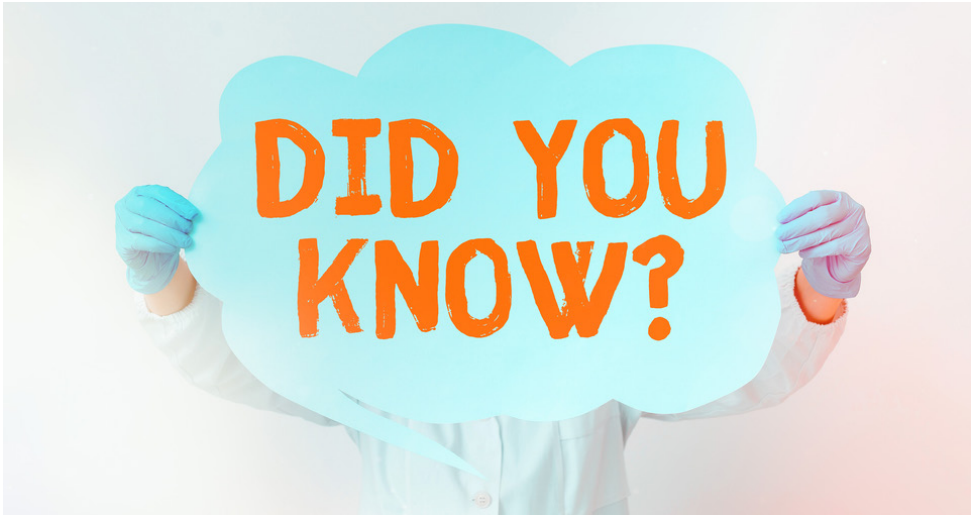
But did you know Alexa can be even more useful than that? She can help with your work life and make you more productive.

Give Alexa access to your contacts and calendar. She makes it faster to call colleagues, schedule meetings, and find someone's details. She can also give you reminders for appointments and meetings, which is perfect when your head is down and you're losing track of time. You can also use a great service called Zapier to connect your Alexa to hundreds of other apps - some of which you may use for work already.

Whether you're working from home or the office, make Alexa work harder to make your life easier.

As an added word of caution: Since the technology behind the Amazon Echo and Google Home is powered by AI, it stores command history to help make the device "smarter". That way, it can better respond to future commands.

Take these basic precautions to enhance safety and protect your privacy when using Alexa devices: Choose a strong password, use a pin for voice purchases, delete your Alexa recording daily, turn off the microphone and camera when you're not using the device, and chose a wake word that is seldom used in conversation.



We'd Love To Hear Your Thoughts

Imagine traveling back in time to the year 2000 and putting your current smartphone into the hands of your younger self. Your young mind would be blown!

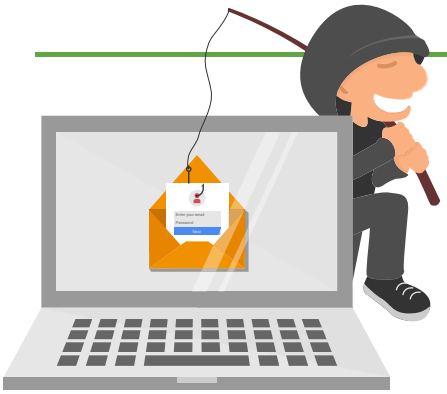
Technology has been both lauded and condemned as it has developed over the past 21 years. We often complain about the addictive qualities of our phones, but how would we keep business going without them?

There's also something to be said about the way social media and video calling has kept people connected during the pandemic.

Mobile phones have revolutionized the way we live our lives. Who would have guessed 20 years ago that we wouldn't be buying physical music albums (or even MP3s)... and instead we'd just rent music, or listen to it for free?

What about Audible, the Kindle and other ways of consuming books? Has the digitalization of books taken something away from reading, or do you think this is a more convenient lifestyle?

What are your favorite and worst pieces of the technology that we take for granted today? We'd love to hear your thoughts.



Every Minute, 4 More Businesses Become Victims Of Malware

And with one billion pieces of malware out there, it's highly likely that your business will be affected at some point.

It's scary stuff.

Worse still, some kinds of malware are very difficult to recover from. It's rarely as simple as deleting an infected file. The most destructive malware can be the hardest to tackle.

You need to protect your business with more than just antivirus software.

Keeping your data safe and secure requires a combination of the following:

- Specialist software
- Staff training
- And other safety measures, which will differ from business to business, depending on many factors

While it's not realistic to protect yourselves from 100% of malware attacks (without completely crippling your staff's ability to freely do their work), you can take the right measures to minimize the risks and be instantly aware when you are under attack.

Is your business prepared for this?

For a limited time, we're offering a FREE security review. Visit www.meetingtreecomputer.com/contact to book a no obligation 15-minute video call.

My Wi-Fi is working but my computer keeps disconnecting

It's possible that your PC's network card isn't receiving full power. Go to advanced settings in power options. Click 'Wireless adapter settings', and 'Expand power saving mode'. Set this to maximum power, and you should see some improvement.

My keyboard is making weird noises and won't type words correctly

You may have accidentally enabled toggle keys and filter keys. To disable them, go to your control panel and select 'Ease of access'. Click on 'Change how your keyboard works', then uncheck the boxes next to Toggle keys and Filter keys.

My monitor is blank - I promise it's plugged in!

Great start! Next, try replacing your power cable with one that is definitely working and see what happens. If it's still blank, try connecting your monitor to another PC. Still not working? It's probably a problem with the monitor. If it works on another PC, it's likely a problem with computer's graphics card.

Submit Your Question Here:

mduci@meetingtreecomputer.com

4 Signs You're Under Attack From Ransomware

Ransomware is a subset of malware and an attack is one of the most terrifying things that can happen to your business.

It is a computer attack where a hacker locks you out of your systems and data. And you must pay a ransom, typically in Bitcoin, to get access again.

What most people don't realize is that hackers often access your system weeks before they launch the attack so, there are signs to look out for – ways to spot if your system has already been breached, and an attack is imminent.

Download Our Brand-New Guide And Know How To Keep Your Business Safe:
http://bit.ly/MTC-4signs-ransomware-PDF

This is how you can get in touch with us:

call: 845-237-2117 | email: info@meetingtreecomputer.com
website: www.meetingtreecomputer.com

Follow Us