VOLUME 5, ISSUE 2 FEBRUARY 2022

MTC TECH TALK

For Humans Not Geeks!

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

POP QUIZ: You Just Discovered One Of Your Employees Had Their Laptop Stolen... Quick, What Do You Do?

What's In This Issue?

Meeting Tree Computer
☎ (845) 237-2117

Over the last couple of months, I've come across some alarming statistics that you should know. There are more than 12,000 laptops found in US airports each week and 62,000 lost electronic devices recovered from New York's metropolitan buses, taxis, trains and stations each year! The bottom line is that no matter how careful you are with your laptop, mistakes occur and the loss (or theft) of a laptop is likely to happen to you or your employees at some point.

Even in the hands of a relatively unsophisticated hacker, all of your laptop information can be siphoned off an unsecured laptop, allowing an open back door into your network. This is akin to giving a thief the key to your office and the code to deactivate the alarm. Imagine the embarrassment of having to contact all of your customers to let them know that THEIR confidential information may be compromised because one of YOUR unsecured laptops is the hands of a criminal!

Asking employees to be more careful about where they keep their laptop IS a good step in the right direction, but accidents happen, and thieves are always on the prowl. That's why it's so important to take measures to lock down and secure any mobile devices that you and your staff use to access our company's network. Here are just a few:

Encrypt All Information – Drive encryption software, such as BitLocker (which is included in some versions of Microsoft Windows), can secure all the data on your hard drive. Also, check your computer to see if it has a Trusted Platform Module (TPM) chip which is generally more secure than those without a TPM. Ask your IT support partner (or us) if BitLocker can be enabled on your computer or laptop.

If you're an Apple user, use FileVault to encrypt the startup disc on your Mac. FileVault 2 is available in OS X Lion or later. Just google "how to deploy FileVault" for detailed instructions.

Multi-Level Access Security – Lock your device with a PIN or a password, but don't rely only on passwords only to keep your laptop safe. Hackers can usually break most passwords in a few hours. We recommend adding a second way for people to prove that they are who they say they are BEFORE they are able to log in.

Use biometrics and Multifactor Authentication whenever possible. Face- and fingerprint-based authentication are included in Windows Hello, which is an important part of Windows 10. It's part of the increased security that prompted the US Defense Department to start moving to Windows 10 as rapidly as possible.

Enable Tracking Feature – Next, always enable your laptop's tracking feature. If it's stolen, you can use this feature to locate and lock it. In Windows 10, this feature is called Find My Device; in macOS, it's just called Find My.

Remote Wipe – Although full disc encryption, strong password use and remote locking are critical features to implement, in situations where data is incredibly valuable and is anticipated to retain its value for decades, it is best to install a remote wiping tool as well.

Remote wiping makes it possible to delete data from a laptop or computer without having to be in front of the device. It needs to be set up beforehand, but if remote wiping capabilities are enabled, you can erase the data remotely and prevent the attacker from stealing the information and using it to launch further cyber attacks.

Log / Back-Up Information – It's critical to log and back-up all information on business laptops to ensure smooth operations in the event of loss or destruction. We can automate the backups so they are done ON SCHEDULE and in a way that won't interfere with the use of the laptop.

The Right Response – What happens when an employee loses a laptop? Do you have a next step action plan in place? Either way, we suggest calling us immediately to report the loss (Note: clients on our Premium Managed Services Plan will get after-hours support for situations like this). The sooner we know, the sooner we can take preventative actions to lock that laptop out of the network. A blame culture where people are afraid to report losses is the worst thing you can do for the security of your business.

Take the time NOW to help your team secure their laptops and limit the damage to your business in the event of loss or theft. While it's impossible to stop all thefts from occurring, having a comprehensive cybersecurity strategy in place can help to limit any resulting damages.

We specialize in securing business data like yours, making sure it is available whenever you need it, so give us a call at 845-237-2117 to discuss best practices.

Your Tech Tip of the Month

Seven Deadly Technology Sins

Meeting Tree
COMPUTER
Meeting Tree Computer Corp.
A referral from a friend, client or colleague is the highest compliment we can receive.
www.MeetingTreeComputer.com Phone: (845) 237-2117
Seven Deadly Technology Sins

We all do it. We make mistakes doing things we shouldn't do, but what if those things you're doing —or not doing— could cost you your company and everything you've worked so hard to achieve?

We've put together a list of the top 7 Deadly Technology Sins to help guide you toward a more productive and cybersecure future

https://www.meetingtreecomputer.com/tech-tip-72-seven-deadly-technology-sins/

Help Your Team Get More Done: Turn Work Into A Game

Even the most exciting workplace is packed with dull tasks that have to be done for smooth operations. But human brains don't embrace boring tasks with passion. The answer is to make the tasks fun. Have you heard of gamification? It's a way of making something more motivating by turning it into a game.

For example, you could offer a reward for new staff completing a series of onboarding tasks. How about a personalized mug with their usual drink order printed on the side?

When you need to train staff, don't just make them sit through training videos. Add in interaction. Maybe they could complete an interactive quiz along the way?

The ultimate gamification is awarding points and using leader boards. This helps your team feel their work is being recognized and can also strengthen their feelings of belonging. Just be careful not to constantly reward only the same top achievers. Have spot prizes to publicly reward any member of your team for positive behaviour.

"Friend In Need" Scams

Have you heard about 'friend in need' scams on WhatsApp? If not, you need to be aware of them and tell your team, too.

You get a message that looks like it's from someone you know, asking for your help. It will either request money, personal information, or your six digit WhatsApp PIN.

Doesn't feel right? Trust your gut. It's possible your friend has been hacked. Call them using their cell number (not via WhatsApp) and let them know.

You can protect your own WhatsApp account by enabling two-step verification, so your account is PIN protected. Tap settings, then account. Tap two-step verification. Press enable, then enter a PIN and confirm it. You can also enter an email address which we recommend as a backup security measure in case you forget your PIN.

Is Cyber Security Training Really Necessary?

This is a question we often hear. And the answer is always a big **YES!**

Every business, every industry, and every person are targets.

You can have the best product or the best equipment to secure your business, but your humans are the asset that will keep your business running successfully. When it comes to cybersecurity, their level of awareness is a skillset that is more important than the locks on the building doors. If you can teach someone to spot a bad link in an email and not click it... then you don't need to worry about mitigating the effects of a cyber-attack.

Cybercriminals know that the easiest point of entry into a business is via human error, and their tactics grow daily to gain access to your business.

Regular training doesn't just help your staff help you. It can also build a culture of security awareness within the business. Staff find it hard to act against a culture. They'll think "if no-one else bothers to check links before clicking them, why should I?" That way of thinking also works the other way.

Regular training will help you identify areas where your security isn't as robust as it could be and make appropriate changes. Our complimentary **baseline employee cybersecurity assessment** will quickly assess where your teammates are in their level of awareness of the variety of ways that criminals will try to fool them.

If you don't already invest in cyber security training, please do think about it this year. The benefits are massive.

Can I print straight from my Android device?

Yes, if your printer has Bluetooth or Wi-Fi. On your phone switch on Default Print Service in the settings. Open the file you want to print. Tap the menu (the three dots), print, and select your printer.

How do I see how much space apps are taking up?

In Windows 10 and 11 go to Settings -> System -> Storage.

Tap on Cleanup recommendations to see what software you're not using and could remove.

Does turning it off and on again really work?

Often, yes.

Restarting any device allows it to refresh every process, which can often solve small annoying problems.

The Security Problem Of John's "Other" Laptop

The security problem of John's "other" laptop
How to keep your business's data ultra-safe during the Work From Home revolution
Meeting Tree COMPUTER

How to keep your business's data ultra-safe during the Work From Home revolution.

Working From Home and hybrid working are here to stay. And that means as businesses, we need to get a grip on security in our staff's homes as much as we do in the office.

We've written a new guide to look at all the issues: https://www.meetingtreecomputer.com/files/2022/01/WFH-Security-Guide-Meeting-Tree-Computer.pdf

Submit Your Question Here:

mduci@meetingtreecomputer.com

This is how you can get in touch with us:

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

Follow Us