VOLUME 4, ISSUE 11 NOVEMBER 2021

MTC TECH TALK

For Humans Not Geeks!

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

6 Proven Business Strategies to Help Combat Security Risks

What's In This Issue?

We hear about it all the time; that some government entity or big business has been hacked. But while these incidents get the media spotlight whenever a breach occurs, smaller businesses are coming increasingly under fire from malware and spyware attacks. Although many of these go unnoticed by the media:

"More than half of all small businesses suffered a breach within the last year. It costs an average of $200,000 to remediate. And yet only 14% of SMBs are prepared to defend themselves from a cyberattack and mitigate risk." - CNBC

Luckily, you can beat those odds. There are some basic strategies to help keep would-be hackers away.

Cloud Security
Small businesses are increasingly jumping on the Cloud bandwagon, allowing their employees to work from anywhere at any time with easy access to the information they need to get the job done.

Cloud security is a responsibility that is shared between the cloud provider and the customer (you). Although you have every right to expect providers to protect your sensitive data, the burden is and cannot be carried by them alone. Cloud service providers must ensure that their infrastructure is secure and their users' data is protected. At the same time, customers must make sure they password-protect their apps, encrypt their data and install anti-virus for optimum cyber resiliency.

Network Security
Network security consists of the policies, processes, and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or theft. It is designed to protect all devices and data from external attacks. Types of network security include firewalls, VPNs, email security, anti-virus/malware software, network segmentation, access control, web, and WiFi security.

Creating strong WiFi, router, firewall passwords, and creating and enforcing company-wide

cybersecurity policies are low-cost security measures that immensely improve your network security. The policies should be written in plain language that everyone understands and should be available to all staff members. These policies should teach them the importance of strong passwords, email security, how to deal with sensitive data, set strict social media rules, and how to best store, protect and
use business devices in and away from the office.

Updates, Patches, And Upgrades
Patching software and hardware systems is one of the most critical security functions and an absolute requirement for all organizations. As annoying as you may find it, updating all tools and software promptly and verifying that the updates are indeed installed is essential when working towards cyber resilience. The easiest way to accomplish this is to arrange for your IT support partner to manage updates for you. Ask them to take care of this overnight or after hours and you won't have to waste time waiting for your computer to get the job done.

Data Backups
Every business needs a sound data backup implementation plan and strategy. Why? What would happen to your office or business if you lost access to your business information for a day? What about if a ransomware attack deleted all of your data?

Whenever possible, adhere to the 3-2-1 backup rule. The 3-2-1 rule is an easy-to-remember acronym for a common approach to keeping your data safe in almost any failure scenario. The rule is: keep at least three (3) copies of your data, store two (2) backup copies on different storage media, with one (1) of them located offsite.

Physical Computer Security
Physical security protects your data by preventing people from literally getting their hands on it. All the firewalls in the world won't save you from someone walking out with your server. In 2015, a thief forced their way into the server room of children's charity Plan UK. They stole five servers containing information on 90,000 supporters, including names, addresses, contact details, and bank account numbers.

Some easy things to do to prevent unauthorized access to sensitive data:

1. Keep the doors to your server room locked when no one is there.
2. Don't write passwords down on publicly posted pieces of paper.
3. Don't plug unknown flash/USB drives into your computer.
4. Install monitor privacy screens
5. Shred all sensitive documents before leaving the office.

Implement Employee Training
Most employees don't think much about how they might be compromising your company's cybersecurity. And that's bad. One click, on one bad link, in one bad email can cause a lot of damage. Providing them with ongoing, up-to-date know-how on security threats, phishing, and social engineering scams, risks, and best practices is crucial in the fight against cyber criminals

Unfortunately, no level of security offers 100% protection (wouldn't it be great if it did); mistakes get made, hackers work overtime to outsmart even the best of technicians. However, implementing some of these basic security measures will go a long way towards mitigating your cyber risk

Your Tech Tip of the Month

4 Ways to Speed Up Windows

Are you trying to work but your computer is not allowing it? Do you need to wait twenty minutes after you login before you can start working? Do you get that good old spinning wheel of death every time you click on something?

There are 4 steps to help speed up your system before needing to call the professionals:

1. Reboot your system
2. Check for any unwanted startup apps
3. Uninstall unnecessary programs
4. Check for updates

This month's tech tip shows you how:
https://www.meetingtreecomputer.com/tech-tip-69-4-ways-to-speed-up-windows/

If You've Ever Reused a Password to Sign Up to Something New, You Have a Problem...

It's something many people admit to doing: They reuse the same password across a few different services.

Not judging you if you've done it. It's easy to see why thousands of people do this every day. It feels like an easy way to get signed up to something. If you reuse a password, you won't have to go through the hassle of trying to remember it, and needing to reset the password in the future.

However. You only have to do this once, and you're at big risk of something called **credential stuffing.**

This is where hackers get hold of millions of real usernames and passwords. These typically come from the big leaks we hear about in the news. And then they try all those details to see if they can login to other digital services. They use bots to stuff the credentials into the login box, hence the name.

Because it's automated, they can sit back until their software manages to log into an account... and then they can do damage or steal money. Stats suggest that 0.1% of breached credentials will result in a successful login to another service.

The best way to protect yourself against this kind of attack is to never, ever reuse passwords.

Use a password manager to generate long random passwords, remember them for you and auto fill them. The less hassle for you, the less likely you are to reuse a password. Consider giving a password manager to each of your staff as well.

The Chip Shortage Hurts!

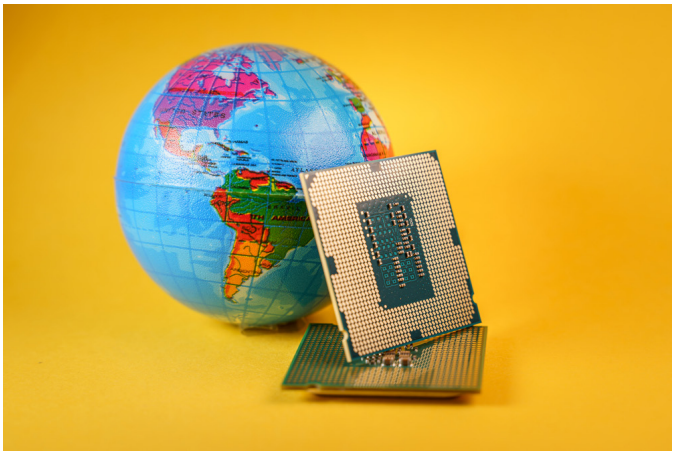
Did you know that sales of PCs are at an all-time high right now? And the types of computers people are buying is changing.

Partly that's been driven by businesses investing in better mobile technology for their teams, to make hybrid working even easier.

An increase in desktop sales is being driven by consumer demand for top end gaming PCs.

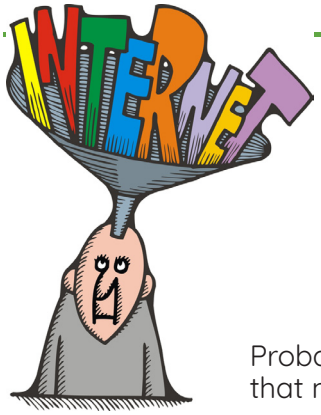
I've been reading a market intelligence report (I do this, so you don't have to), and it says:

- Ultra slim laptops now dominate the market with 44.3% of sales
- Traditional laptops are next at 26%
- Traditional desktops make up 18.1% of sales



One thing that's starting to bite is the worldwide chip shortage. Have you heard about this? There's so much demand for chips in all devices, not just computers. Yet supply is down. It's starting to affect many manufacturers, especially those making computers.

So, if you're thinking of upgrading your business's technology, you need to work ahead more than usual.



How Much Do You Think About Your Browser?

Probably not that much.

We know this, because 75% of Internet Explorer and Edge browsers are out of date.

These are normally updated when your operating system is updated. When you update Windows, Edge gets updated. When you update MacOS, Safari gets updated.

If you have an out-of-date browser, this either means that you're not updating your operating system, or you're using a browser that's not native to your operating system (such as Chrome or Firefox).

Either way, please take a moment to check that you don't have any updates waiting to be installed.

Running a browser that hasn't been updated puts you at increased risk of security issues. Updates are there to keep you and your data safe. It also means your browser runs faster, and gives you additional features that can help with productivity.

It's simple to check for updates. Just go to: **www.whatismybrowser.com.** It'll instantly tell you at the top if you need to apply any updates.

It takes seconds to check if you're running the latest version of your browser. Check it today and ask your team to do the same. Alternatively, speak to your IT partner (us) and they can reassure you if they're checking and updating on your behalf.

Oh no... I've sent an email to the wrong person... can I get it back?

Yes, don't panic!
In Outlook, open the message in **Sent Items**, select **Actions > Recall This Message**, then **Delete the unread copies of this message.**

Is there an easier way to add appointments to my Outlook calendar?

If you're scheduling a meeting or appointment via email, simply drag that email to your calendar and it will create an appointment for you.

I'm trying to send a photo via email, but it's telling me the file is too large.

This one is easy. Select the photo file you'd like to send. Right click it and select **Send To > Mail Recipient**. A pop-up window will open which allows you to select the picture size. Click **Attach**, and it will resize the image and attach it to your message.

The Tax Relief You Should Know About

Have you heard of Section 179?

It's part of the IRS tax code that's aimed at helping small businesses, just like yours. When you buy new IT equipment or software you can deduct the full purchase price from your gross income this year. But you must have purchased the IT equipment or software and put it into service by the end of the day on December 31. And this year there's extra urgency due to major supply chain issues (see pg. 3).

You really should invest now in anything you think you'll need in 2022.

Call me now at **845-237-2117** to tell me what you need!

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