VOLUME 5, ISSUE 8 AUGUST 2022

MTC TECH TALK

For Humans Not Geeks!

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

Top 5 Online Safety Tips for Parents to Share with Your Kids

What's In This Issue?

Meeting Tree Computer
☎ (845) 237-2117

In today's climate, is there anything more prevalent than the Internet? We've grown so accustomed to using it that the Internet seems to help us meet any need or want. But 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, or maybe we were lucky and able to browse through our parents' encyclopedia. Doing research used to take time and effort 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 them protected. So, before your kids get a social media account or dive headfirst into the web, look at the following security measures.

Put Yourself in Control

Nearly every device connected to the Internet has the option to set up some level of parental control, offering your child a safe place to explore their curiosity online.

You can restrict what websites and apps your children visit and which websites you want to be blocked. You can also set time constraints and limits so your child can only use the device for a certain amount of time.

This step-by-step guide will help you to set up the proper controls and privacy settings on the networks, gadgets, apps, and sites your kids use to give them a safer online experience: https://www.internetmatters.org/parental-controls/

Address Potential Risks

Parental Controls and Privacy Settings are valuable tools to help minimize the risks your children may face, but they are not always 100% effective. Teach your children skills like critical thinking and resilience to know what to do if they encounter risk.

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 email address to anyone online.

While they won't fully understand the consequences of revealing personal information online, you should teach them to be cautious and thoughtful about what they post and share. Encourage your children to ask themselves before posting anything if:

1. The information (i.e., name, phone number, home address, email, name of school) or photo is something they would give a stranger. Or
2. If the images, videos, and comments they intend to post would be something that they'd be comfortable showing/sharing with you.

If the answer is no, don't post it.

Teach Them to Keep Their Location Private
Most apps, networks, and devices have geo-tagging features which make whereabouts public and can lead someone directly to you. For privacy reasons, it is best to turn this feature off.

You can block the function from your device, including browsers, phones, operating systems, and even applications. To disable 'location services' and enable the 'do not track', go to your device's privacy settings and simply turn it off.

Teach your kids that although some applications and social media platforms will ask to enable location services when you set them up, not all of them actually need it to work properly.

Advise Them To:
- Only use secure and legal sites (sites with the little padlock icon that start with HTTPS – 'S', which indicates they are safe websites) to download music and games.
- Check attachments and pop-ups for viruses before they click or download anything.
- Use Public Friendly WiFi when they're out and about to filter inappropriate content. Also, encourage them to use the parental control tools on their device just in case they do connect to an unfiltered WiFi - such as at a friend's house.
- How to block abusive comments and report content that worries them (see "Be #SocialNetworkSavvy").

Be #SocialNetworkSavvy
If your child uses social networks, be sure they know how to:
- Report inappropriate and/or offensive posts
- Block someone
- Keep information private
- Feel comfortable to ignore friend requests from people they don't know

It can be challenging to stay on top of what apps your child is using and who they are talking to online – find out more about the latest apps at the InternetMatters.Org Website.

If you suspect online enticement or sexual exploitation of a child, immediately report it by calling 911, contacting the FBI at https://tips.fbi.gov/, file a report with the NCMEC at 1-800-843-5678 or go online to https://report.cybertip.org./.

Just as with everything else in life, we can't eliminate every possible risk associated with technology, but by taking reasonable precautions, we can greatly reduce it. The best defense is critical thinking – understanding when things are too good to be true or knowing to pause for a few seconds to consider the consequences of clicking on something, installing an app, or entering a password or private information. It's not always easy, even for savvy adults, but it's something we all must learn to deal with in our digital age.

Your Tech Tip of the Month

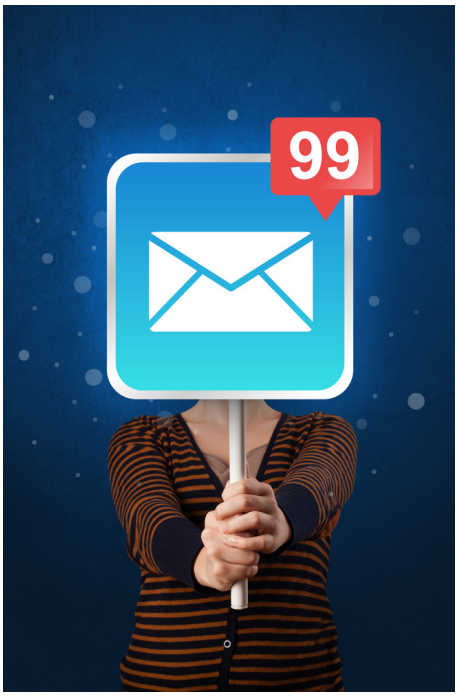
3 Ways to Recover Lost Files

Did the files you store on your desktop go missing? Unfortunately, you're not alone, the question, "where are my files in Windows 10" has been asked by an incredibly large number of people on Google.

Luckily, many times when files go missing from your computer, they're not really lost. In this tech tip article, we'll discuss why this can happen and what we can do to recover lost files.

https://www.meetingtreecomputer.com/tech-tip-24-3-ways-to-recover-lost-files/

Who Else Is Sick of Spam?



For business owners, spam is bad news.

Not only is it annoying, but it's also eating up hours of your team's time. In fact, it's estimated that people who get more than a hundred emails per day could be losing up to 80 hours of their time each year simply sorting out spam.

Other than the negative impact of spam on productivity, have you considered how else it might be harming your business?

Considering that a proportion of these emails will be phishing attempts (messages where the sender wants you to take an action that will secretly give them access to sensitive data), it's also a significant security risk to your data security.

Of course, there are things you can do to cut down the time spent dealing with spam emails and reduce your risk. The first important step is to make your people aware of the risks of spam, how to spot spam emails, and the best way is to deal with it (ignore and delete).

Your next option is to use the spam and junk email filters available from your email service, and/or bringing in dedicated anti-spam and anti-phishing tools. Not only will implementing these strategies save time, but they will also significantly lower the risk of malware or a data breach.

Did You Know... Paying Ransomware Makes You A Bigger Target?

Ransomware is evil. It's where cybercriminals infiltrate your network (or device) and steal or hold your data hostage by encrypting it. The data is still there, but you can't access it.

Then they demand you pay a hefty ransom fee for access to the encryption key and if you don't pay the demand (which can be tens or even hundreds of thousands of dollars), they will threaten to delete your data.

Official advice is not to pay any demands. However, a new survey has shown that a massive 97% of business leaders who've experienced a ransomware attack in the past would pay up quickly if they were attacked again.

The problem is, that even when you pay a ransomware demand, there's no guarantee that you'll get your data back. And something else that you should consider when faced with the decision is that payment does not guarantee that you won't ever meet with further extortion. By letting cyber criminals know that your business pays ransom fees, you're much more likely to face subsequent attacks in the future.

In fact, 80% of ransomware victims who paid up were then hit a second time by the same attackers.

The best defense against ransomware is being prepared. You need to educate your people on cyber security and best practices, have a working backup, a ransomware resilience plan, and all the right security measures in place BEFORE you get attacked.

Are You Blacklisting or Whitelisting?

You know what it means to be blacklisted, right? (we don't mean through personal experience, of course). Blacklisting is where you block something you don't trust. It's used to keep networks and devices safe from bad software and cyber criminals.

But there's another, safer way of doing that – it's called whitelisting.

Rather than trying to spot and block threats you assume that everyone and everything is a threat, unless they've been whitelisted (approved by you).

What is the right approach when it comes to keeping your business data safe? That debate has been ongoing, with many IT professionals holding different views.

The main differences...

- Blacklisting blocks access to suspicious or malicious entitiesWhitelisting allows access only to approved entities

- Blacklisting's default is to allow access
- Whitelisting's default is to block access

- Blacklisting is threat-centric
- Whitelisting is trust-centric

There are pros and cons to each approach. While blacklisting is a simple, low maintenance approach, it will never be comprehensive as new threats emerge daily. It's also easy to miss a threat, as cyber criminals continuously develop software to evade blacklist tools.

Whitelisting takes a stricter approach and therefore comes with a lower risk of access. But it's more complex to implement and needs more input. It's also more restrictive for people using the network and devices.

Confused?

You're not alone!
If you'd like to discuss which approach is best for your business, get in touch.

How can I avoid being phished?

The best thing is to treat every email with caution. If you're unsure, check the address it's been sent from, look for grammatical errors, and see if the layout looks like a normal email from that person or company. If you're unsure, don't click any links and ignore attachments.

What's an insider threat?

Insider threat refers to someone within your business who (accidentally) gives cyber criminals access to your devices or network. Usually, it's not malicious. But it's why regularly training your team in cyber security is a must.

How do I choose the right backup for my data?

Security and reliability should be your main considerations. Get in touch and we'll tell you what we recommend.

What Could Digital IT Transformation Do For Your Business?

What did Netflix and Lego do... and Kodak famously didn't?

We have all seen a LOT of change over the past couple of years. We've changed the way we work. The way we shop. And the way we interact with others.

How has your business changed? What change do you need to make in the years ahead? And how does your technology help to power that?

We've written a new guide about digital IT transformation for your business. Read case studies, and how digital IT transformation affects businesses of every size, in our new guide:
https://meetingtreecomputer.com/files/2022/05/Digital-Transformation-Guide-Letter-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