1991 – 2021
30 YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

February 2023

Kim Nielsen, CISSP, CCSA
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

Metaverse: What is It and What Will Cybersecurity There Look Like?

If you hang around techies, you've probably heard the word metaverse" buzzing around in the past year or so.

By reputation alone, the metaverse seems to be some kind of new reality that's entirely online and self-supported by the internal players.

Wait, is this a video game or a social media marvel?

Let's dive into what the metaverse is, and what the next level of cybersecurity will look like in that digital landscape.

What is the Metaverse?
That's a good question, and one many people have asked since the term really took off worldwide when Mark Zuckerberg announced that Facebook would focus future updates on the metaverse, which plans to include 2D and 3D features that will work on your typical WiFi devices like your phone, to virtual reality equipment specially designed for immersion. You can *really* shop, *really* work, and *really* interact with others. It's like one of those massive online roll playing games you used to play as a kid, but actual companies are on there – and so is your Facebook account.

Some companies are betting on the new future, and already planning games and experiences unique to the metaverse. For example, Roblox – which is already an online gaming platform – is developing video games specifically for Virtual Reality. Other brands have opted to use the metaverse more so as a marketplace for NFTs.

How does this differ from, say, Minescape or World of Warcraft?

Continued on pg.2

Continued from pg.1

Largely, because the real world will agree to participate in it. If you can buy Raybans and get a job as a Starbucks barista in the metaverse, talking to the real managers of those companies, then it's a little different than playing swords and dragons – even if that line seems to get thinner with every technological marvel.

Security Goes Meta

Whenever popular technology changes or advances, there are new privacy concerns to address and hackers to keep out. Meta, evidently some kind of "next level internet," is sure to have its fair share of vulnerabilities. All new inventions do! How can users address these risks as they make the move to Meta?

Security in virtual reality requires a different way of thinking. For example, did you know that pranksters are already using the fact that avatars are constantly followed by "cameras?" That footage gives hackers massive amounts of data to work with if they can access the feed. Adding more protections to your camera's security settings is critical, and should be on the top of your list when first making an avatar. Meanwhile, vulnerable virtual reality devices that you might use to log in could be the entry point for malware and hackers, too. Your equipment needs to be locked down tight, and sophisticated enough to have strong defenses built in.

You should also beware that digital privacy rights are nowhere near as comprehensive as the ones we hold in the real-world. Think about all of the times and places that it's illegal to record another person. The metaverse would have to disclose that it's watching you, but signing that would give them way more liberty to track your whereabouts than many people feel comfortable with in real life. Be careful what you share in the metaverse!

We will also have to be more wary of phishing scams when it's already tough to figure out whether the avatar you're chatting with is a person, AI or a bot working for the bad guys. They could fake the likeness and a very similar handle to your close friend and convince you to send money or information, similar to how many spear-phishing campaigns operate via email.

All of these concerns will amplify if and when the metaverse gains popularity, and individuals and businesses alike scramble to join without double-checking they're going about it as safely as possible. Thus, there is a chance of encountering **zero-day vulnerabilities** as the metaverse grows; those are exploitable areas in the current software, which may be discovered first by either hackers or the engineers. Make recommended updates ASAP so that you don't fall victim to a zero-day attack.

Is Metaverse Safe?

In some ways, we will have to rely on the Metaverse itself to include inherent safety features, and also for the law to catch up to the real world when it comes to privacy concerns. We're still hammering out data privacy laws for the regular old Internet! Meanwhile, we can still take steps to preserve our data's anonymity when creating profiles and interacting in the metaverse.

What threats and security solutions will emerge as the metaverse grows more popular and society evolves? Only time will tell!

Free Executive Guide: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This guide will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
https://www.cti-mi.com/protectdata223
or call our office at (248) 362-3800

Security Corner

SPAM? Don't Just Click 'Delete'

Sometimes, spam is clearly recognizable as fake. Others look like viable sales pitches…and sometimes they're disguised as phishing messages to make you think that you're interacting with something or someone that you're not. Hopefully you recognize false messages for what they are and don't engage, but what do you do next?

Don't Click Delete

Don't just send them to the Trash. You should *report* instances of spam and phishing. Email and text apps should have built-in functionalities to block and report the sender. You can also forward texts to 7726 (SPAM).

If you get a phone call (that's actually called *vishing*, or voice phishing) then you should report it to the Federal Trade commission.

This helps the authorities track down these threat actors and prosecute them. The FTC is better equipped to track and find scam artists, and that keeps ALL of us safer.

Conclusion

If you only *delete* the messages, then the spammer will be able to keep targeting other people, and possibly even come back with a more personalized scam for you. Instead, keep the authorities hot on their trail by reporting these messages.

Next time you see spam in your inbox, you'll be prepared to take care of it – the right way.

For more information about SPAM and other cyber threats, call us at 248-362-3800 or visit: https://bit.ly/3XW9FJf

Helpful Tips For Keeping Your Shared Cloud Storage Organized

Cloud file storage revolutionized the way we handle documents. No more having to email files back and forth. No more wondering which person in the office has the most recent copy of a document.

But just like the storage on your computer's hard drive, cloud storage can also get messy. Files get saved in the wrong place and duplicate folders get created.

When employees are sharing the same cloud space it can be challenging to keep things organized. Storage can be difficult to keep efficient.

Disorganized cloud storage systems lead to problems. This includes having a hard time finding files. As well as spending a lot of extra time finding needed documents.

Has your office been suffering from messy cloud storage? Does it seem to get harder and harder to find what you need? Here are several ways to tidy up cloud storage spaces and save time:

Use a Universal Folder Naming Structure
When people are free to use different naming structures for folders, it makes it harder for everyone.

They often can't find what they need. It also leads to the creation of duplicate folders for the same thing.

Map out the hierarchy of folders and how to name each thing. For example, you might have "departments" as an outer folder and nest "projects" inside.

With everyone using the same naming system, it will be easier for everyone to find things. You also reduce the risk of having duplicate folders.

Keep File Structure to 2-3 Folders Deep
When you have too many folders nested, it can take forever to find a file. You feel like you must click down one rabbit hole after another. When people need to click into several folders, it discourages them from saving a file in the right place.

To avoid this issue, keep your file structure only two to three folders deep. This makes files easier to find and keeps your cloud storage more usable.

Don't Create Folders for Fewer Than 10 Files
The more folders people have to click into to find a document, the more time it takes. Folders can quickly add up as employees create them, not knowing where a file should go.

Implement a rule for your cloud storage that restricts folder creation to 10 files or more.

This avoids having tons of folders with less than a handful of files in them. Have someone that can act as a storage administrator as well. This can then be the person someone asks if they're not sure where to store a file.

Promote the Slogan "Take Time to Save It Right"
We're all guilty from time to time of saving to something general, like the desktop on a PC. We tell ourselves that we'll go back at some point and move the file where it should be.

This issue multiplies when you have many people sharing the same cloud storage space. Files that aren't where they belong add up fast. This makes it harder for everyone to find things.

Promote the slogan "take time to save it right" among the staff. This means that they should take the extra few seconds to navigate where the file should be to save it.

This keeps things from getting unmanageable. If you use a file structure that's only 2-3 folders deep, then this should be easier for everyone to abide by.

Have You Had Data Exposed In A Data Breach?

There's a reason that browsers like Edge have added breached password notifications. Data breaches are an unfortunate part of life. And can have costly consequences for you. Hackers can steal identities and compromise bank accounts, just to name a few.

Cybercriminals breach about 4,800 websites every month with form jacking code. It has become all too common to hear of a large hotel chain or social media company exposing customer data.

- Microsoft Customer Data Breach
- 5 Million Records Exposed in a Student Loan Breach
- U-Haul Data Breach of 2.2 Million Individuals' Data
- Neopets Breach May Have Compromised 69 Million Accounts
- One Employee Computer Causes a Marriott Breach

5 Tech Checks To Make Before You Travel

Our technology inevitably comes with us when we travel.

When you go on a trip, not having your technology there when you need it can ruin your day. Travel smarter and more securely by doing several checks before you go.

Use our handy tech travel checklist. It can save you from suffering from lost devices, missing chargers, or a data breach. Be sure to check:

- Your Cords & Adapters
- Your Power
- Your Mobile Plan
- Your Backup
- Your Device Security

3 Ways to Take Control of Your Schedule

Every day is busy for those who lead or own a business, but you must stay organized and stick to your schedule to ensure everything gets completed. This is a difficult task for many business leaders, though. Little distractions can cause us to procrastinate and get behind on our work, making for long workdays. If you find yourself struggling to stay on schedule, give some of the following tips a try.

- Set deadlines for every important task.
- Turn off app notifications on your phone so your attention stays on your work.
- Delegate tasks to others if you feel overwhelmed.