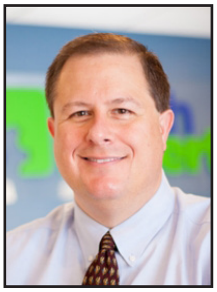
February 2023

TechTidbit.com

brought to you by Tech Experts

How Is The Metaverse Going To Change Business?



Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

The new buzzword around town is "metaverse." But what does that actually mean for businesses? Is it just something that social media companies need to be concerned about?

According to people like Apple's CEO Tim Cook, the metaverse is coming. He stated that "Life without AR will soon be unthinkable." Whether that's a short-term or long-off prediction, companies need to be ready.

First comes the understanding of what the metaverse is. Metaverse is a general term – hence why it's not capitalized like a proper name. The metaverse refers to a collective upgrade of the internet to a 3D virtual environment. This would be a world interconnected between various sites. These sites would reflect the immersive games that you see today.

Did Facebook/Meta invent the metaverse? No. The idea of connected 3D immersive worlds has been around for decades. Several online gaming companies have staked a territory in the metaverse. But their applications are less interconnected.

What's one of the best representations of the early metaverse? It's a short-lived software called Adobe Atmosphere. This 3D immersive experience included interconnected online worlds.

It also gave people the ability to chat with others. It was a bit before its time but shows how the concept of the metaverse has been around for a while.

The metaverse is getting attention now because technology has advanced. It has begun to catch up to the needs of such a world. This includes fast internet connections and immense processing power. It also includes a delivery method for 3D that works on most PCs.

Are we there yet? Not quite. But the metaverse is picking up steam. Recently, Microsoft announced a partnership with Meta. This partnership is to bring Microsoft 365 apps into the metaverse.

This means collaboration in an entirely new way. Microsoft notes that 50% of Gen Z and millennials expect to do some of their work in the metaverse in the next two years.

How could the metaverse impact your company?

With companies like Microsoft looking at the future of AR/VR, it could be a reality soon. You can expect the metaverse to touch your own company in some way in the next few years. Here's a preview of what it may impact.

Where to advertise

When the internet was first introduced, companies didn't immediately realize its potential.

Now, most companies wouldn't consider operating without a website. It's a necessity for driving leads and converting sales.

If the metaverse takes off as a new 3D iteration of the internet, it could be just as important.

This means exploring metaverse-type advertising in virtual worlds. Also, potentially creating your own VR site or showroom.

How to service customers

As the popularity of social media took off, companies realized customers used it to reach out.

Seventy-nine percent of consumers expect companies to respond to a social media message. And they expect that response within a day.

To address that need, many businesses have a social media presence. The metaverse may be the next step.

If people begin hanging out there, they will expect to interact with businesses in that space. Just like they do now with social networks.

This means companies need to be aware of how customers may be using the metaverse as it grows. Adding a question about metaverse use to a year-end customer survey could be a way to be proactive on this topic.

Employee training

One of the touted benefits of the metaverse is its ability to enable more immersive training. This could greatly increase training capabilities and thoroughness for everyone from doctors to forklift operators.

Mobile Malware Has Increased 500% - What Should You Do?

Cybersecurity researchers uncovered an alarming mobile statistic. During the first few months of 2022, mobile malware attacks surged by 500%.

For years, mobile phones have become more powerful. They now do many of the same functions as a computer.

Yet, people tend to secure their computers better than they do their smartphones.

This is a behavior that needs to change. Over 60% of digital fraud now occurs through mobile devices. That makes them highly risky if proper safeguards aren't followed.

Use Mobile Anti-malware

Yes, your mobile phone needs anti-virus/anti-malware too! Malware can and does infect smartphones and tablets. Ensure that you have a reliable mobile anti-malware app installed.

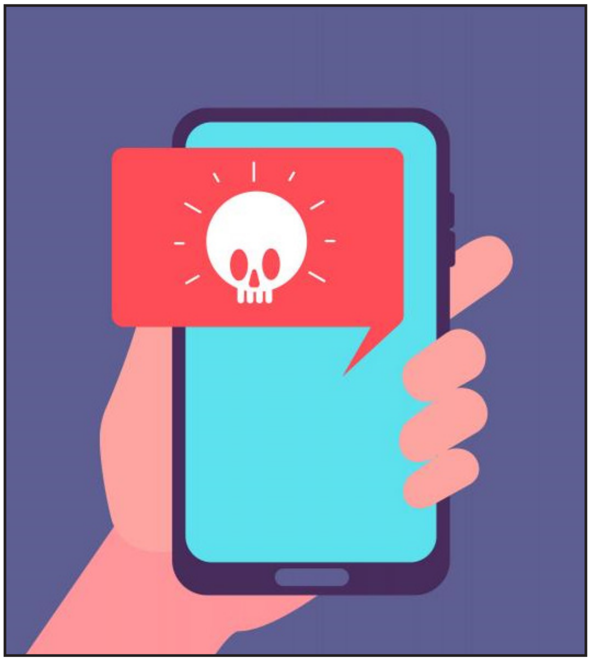
Don't download apps from unknown sources

Only download mobile apps from trusted sources. Do not download outside a main app store. Trusted app stores include places like:

- Apple App Store
- Google Play
- The Microsoft Store
- Amazon Appstore

Don't assume email is safe

Many people prefer checking email on their phone rather than PC because it's so handy. But they have a false sense of security about the safety of emails when viewed on a mobile device.



It's difficult to hover over a link without clicking when on a smartphone. If you see something questionable and want to check the link, open the email on your PC where you can do that.

Beware of SMS phishing (aka "smishing")

In March of 2022, text spam outpaced robocalls. Unwanted text messages rose by 30%, ten percent higher than robocalls. Many of those spam texts are smishing.

Be on the lookout for text messages that don't quite make sense. For example, getting a shipping notification when you haven't ordered anything.

Remove old apps you no longer use

Go through your device and remove old applications that you are no longer using. There is no reason to keep them around, potentially leaving your device at risk.

Keep your device updated

Speaking of updates, you also need to keep your device's operating system updated. Are you using the current version of Android or iOS?

Not installing updates can mean your phone has vulnerabilities. These vulnerabilities allow hackers to breach your data.

Use a VPN when on public Wi-Fi

Public Wi-Fi is dangerous. Most people understand that, but many connect to it out of necessity. Reduce your risk by using a VPN app.

Use mobile security solutions to prevent a data breach

Don't wait until your phone is infected with malware to secure it properly. It's only a matter of time before you are the next victim.

8 Tech Checks To Make Before You Travel

Our technology inevitably comes with us when we travel. Most of us won't even travel to the end of the block without our smartphones. 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.

Check your apps

Have you ever sat at an airport gate wondering why it looked so empty? You then found out that your gate had changed, and you had no idea. You go rushing to the other end of the concourse, hoping you're not too late.

How did everyone else know about the gate change? They most likely had the app for the airline and received a notification.

Before you leave for a trip, make sure to download any apps you may need. It's better to download them when you're at home on your own Wi-Fi. If you wait until you're at the airport, reception may be an issue.

Some of the apps you may want to grab or update before your trip are:

- Airline app
- Train app
- Hotel app
- Theme park app
- Camping ground app
- Weather app
- City tourism app

Check your cords & adapters

People leave behind countless chargers and adapters every day. They litter airports, restaurants, and train stations around the world.

Make sure to bring a backup charger for your laptop, tablet, or phone. Otherwise, you may find yourself paying a premium for a new charger in a gift shop. Your device could also go black if you lose its charger and can't quickly get a new one.

Check your power

A great way to ensure you have the power you need is to buy a small charging battery. You can find these in most major retailers or online. They are small "blocks" that hold a charge and can power up a cell phone in a pinch.

Having this extra backup also helps you avoid potential juice-jacking ports. These are fake or compromised public USB charging ports. Hackers use them to steal your data when you plug in.

Check your mobile plan

If you're traveling out of the country, you'll want to check your mobile plan. If you don't have the ability to call internationally, then you may not be able to text or call home.

Carriers can add an international capability to your plan, but ask about pricing. It can get expensive if you're on long calls or using mobile data.

An alternative is to set up a VoIP app you can use with your office, friends, or family while you're traveling. These enable both calls and SMS, but you do need an internet connection.

Check or add a VPN

Free Wi-Fi may be a welcome site when you're on the road, but it can also be dangerous. You don't know who else is using that Wi-Fi. A hacker hanging out on the connection can easily steal your data if you're not protected.

It's better to use either your mobile carrier connection or a virtual private network (VPN) app. VPN plans are inexpensive and will keep your data encrypted, even if you're on public Wi-Fi.

Check your backup

Unfortunately, mishaps occur when traveling. You may leave your phone behind on a boat, have your luggage lost, or get your device stolen while in a crowded area. Ten percent of all laptop thefts happen in airports.

Don't lose all your data with the device! Back up your devices to the cloud or local storage before you travel. This ensures that you won't lose the valuable information on your device. You also won't need to think twice about enacting a remote "wipe my device" command if necessary.

Check your device security

Make your devices as secure as possible before you hit the road. When we're traveling, our minds are occupied by other things. So, you may not think to check your antivirus or avoid suspicious phishing links.

Protect your devices before you go using:

- Antivirus/anti-malware
- DNS filtering
- Screen lock with passcode
- Sharing features turned off
- VPN application
- Find-My-Device feature turned on

Check your double checks

What do we mean by checking your double-checks? Use the buddy system as a backup. When the family is getting off a plane, each should check with the other that they have all their devices.

If you're traveling alone, have a friend or family member check up by text. Did you grab your charger? Is your VPN turned on? Those little reminders can go a long way toward avoiding digital travel nightmares.

Improve the security of your devices now

Don't leave your devices unprotected. This could mean a breach of your banking app or personal data. Contact us for device security solutions to reduce your risk.

Article used with permission from The Technology Press.

Create new service requests, check ticket status, and review invoices in our client portal: http://TechSupportRequest.com

Contact Information

Tech Experts
Support Team
(734) 240-0200
support@MyTechExperts.com

Main Office
(734) 457-5000
info@MyTechExperts.com

Sales Inquiries
(888) 457-5001
sales@MyTechExperts.com

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Tech Experts® and the Tech Experts logo are registered trademarks of Tech Support Inc.

Don't Waste Money On The Wrong Tech

Have you ever felt like you've wasted money on technology that you thought would change your world?

The right tech can be truly transformative. You can grow your business more quickly, help employees be more productive and your systems run more smoothly.

That allows you to focus on strategy and to stop sweating the small stuff.

But the wrong choices can be more trouble than they're worth. That leaves you to foot the bill for a solution that solves nothing or, worse, creates problems of its own.

Here's our best advice for making the right tech choices in your business.

Don't fixate on digital transformation for its own sake. Focus on what you want to achieve and choose the tech that helps you to get there.

Be open to the idea of process change if the tech can create efficiencies. But your tech should support you – not force you to work the way it wants you to.

Define your objectives and seek expert advice before making a big change. That software might look like the answer to everything, but is it well established?

Is it reliable? Is there good support, and are there regular updates? Could an alternative do the same thing for a smaller investment?

Focus on your data. Big corporations have a deep understanding of their data and work hard to define how success will be measured. Think about how you're able to access your data, how you can protect it, and what it can tell you about your choices.

Enter the cloud. Cloud solutions can help you keep your data better protected and are often more scalable so that they can grow with you.

Ask for help. You can't be an expert in everything, so if there's something you don't understand, or if you can't decide what's best for you, ask an expert.

If you're thinking about change and want to make the right tech decisions for your business, we're here to support you all the way. Just get in touch.

Are You Still Using That Same Old Password?

We talk a lot about strong passwords. It's kind of our job. But they're really important if you want to protect your online accounts and keep your data safe.

So why are we hearing that '123456' is still the most common password? Researchers found it used more than 100,000 times in a recent study.

'Admin' is another popular choice, found 17,000 times, followed by the highly creative 'root' and 'guest'. Often these are pre-set default passwords which you're supposed to change when you first login – but too many people don't bother.

Names – personal names, celebrities, even football teams – are also common, as are profanities. One swearword cropped up 300,000 times in the study (we'll let you guess which word it was).

But popular choices make for weak passwords. A brute force attack involves throwing thousands of passwords at a system.

So if you're using any of these examples, it wouldn't take long for an attacker to gain access to your account.

A good solution is to use a password manager. This will create long, strong, random passwords that are impossible to guess. It also stores them securely and auto fills them, saving you time.

An even safer solution is Passkeys. These could take over from passwords entirely – Apple and Microsoft are already rolling them out across their apps and accounts. Passkeys consist of two 'keys': One on your device and one within the application.

When they connect and recognize each other as the right fit, you gain access to your account… all without clicking a button.

The best part is that you never have to remember a password. It's all done within your device and the application, so it's unlikely that a cyber criminal will ever be able to get their hands on your log in credentials. And there are 123456 reasons why that's a good thing.

Need help to find the right password manager? Get in touch.