September 2026

TechTidbit.com

brought to you by Tech Experts

The First Question I Ask Every New Client



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

When I sit down with a new client for the first time, I don't start by asking what software they use or what their network looks like.

I ask one simple question: When was the last time you actually tested your backup?

Not "do you have a backup." Almost everyone says yes to that. I mean **REALLY** tested, like we do at Tech Experts. Restore a file, open it, and make sure the contents are really there.

The answer tells me more about a business's real risk than almost anything else I could ask. Most of the time, people pause.

They know backups are running and they've seen the "green checkmark" or the automated email confirming success. What they haven't done is actually try to get their data back.

The action of making sure the backups are restorable matters more than people realize. A backup that runs every night but has never been tested is really just a hope, not a plan.

I've seen businesses discover their backups were incomplete, corrupted, or hadn't run properly in months, and they only found out when they needed the files most, or when disaster struck.

By then, it's too late to fix quietly. It becomes a crisis instead of a non-event.

The second question I ask

Once we've talked about backups, I ask something else: who can see what on your network?

This one usually gets a longer pause. Most business owners can tell me who has a login. Most can't tell me what each of those logins can actually access. In a busy office, permissions pile up over time. That employee who got access to the accounting share for a one-time project keeps it long after the project ends. Even worse (and we see this all the time) is when a former employee's account gets disabled but never fully removed.

By themselves, none of these seem like an urgent problem. Together, they add up to a business that doesn't really know who can touch its data. That's a hard position to defend from, whether the threat is a hacker or just an honest mistake.

Why I ask these two first

Neither question is technical. I'm not asking about firewalls or encryption or anything like that. I'm asking whether you actually know what would happen if something went wrong today. This helps me understand a client's risk tolerance, and how much importance they place on their IT systems.

Most businesses I meet have invested in tools. They have antivirus and a firewall, and some kind of backup system. What they often haven't done is confirm that any of it actually works the way they think it does.

Untested backups and unmanaged access are two of the most common ways I've seen businesses get hurt. These companies aren't careless, they just didn't know they should be checking these things.

That's really what these two questions are getting at. It's not about whether you have the right tools. It's about whether you actually know your own risk. Most business owners are surprised by how much clarity comes from just asking.

Most businesses I meet have invested in tools. They have antivirus and a firewall, and some kind of backup system. What they often haven't done is confirm that any of it actually works the way they think it does.

Tech Experts®
Information Technology Professionals

Empowering clients to do more with technology.
We support, manage, and optimize business IT.

Need Help? Email support@MyTechExperts.com, or call (734) 240-0200

Are Your AI Problems Business Problems In Disguise?

"If nobody takes ownership of how AI fits into the business, good ideas can stay trapped inside individual departments instead of becoming part of everyday work."

By now, you've probably experimented with AI in some form.

Maybe it's helping write documents, summarize meetings, analyze spreadsheets, or speed up customer service.



You see the potential very quickly…

But then the excitement fades.

A handful of people keep using it every day, a few others stop using it altogether, and before long, you're left wondering why the big AI transformation never fully arrived.

It's tempting to blame the technology, but the problem is often much more human.

Businesses struggle because they haven't changed the way work happens around AI tools.

Imagine introducing a new piece of machinery into a factory but keeping the same production process around it. You'd never see the full benefit.

AI works in the same way.

If employees are expected to experiment but still judged entirely on speed, consistency, and avoiding mistakes, most will stick with the methods they already know.

If nobody takes ownership of how AI fits into the business, good ideas can stay trapped inside individual departments instead of becoming part of everyday work.

The same challenge appears when there isn't a clear approach to how AI should be used across the business.

Employees want to know what they're allowed to use, what information can be shared, and where the boundaries are.

Without clear guidance, many people become cautious. Others simply make up their own rules.

Getting the best results from AI usually means changing the way work gets done, not only adding new software.

Give people permission to experiment, create clear ownership, and build AI into existing processes rather than leaving it as an optional extra.

AI is moving into workplaces quickly.

Giving people the skills, confidence, and guidance to use it well may turn out to be as important as the technology itself.

If you'd like help putting the right foundations in place, give us a call at (734) 457-5000, or email us at info@mytechexperts.com.



We Love Referrals!

The greatest gift anyone can give us is a referral to your friends and business colleagues. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll give them their free first month of service (for being a friend of yours) AND we'll give you a $250 Amazon Gift Card.

Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

Why Hackers Don't Need Ransomware Anymore

Is your business ready for an attack that doesn't lock your files but steals them instead?

Cybercriminals are changing their approach, and it's worth understanding what that shift means for you.

For years, ransomware was the story. Hackers broke in, encrypted your files, and demanded payment to get them back.

That threat hasn't gone away, but a quieter and in some ways more dangerous tactic is catching on: stealing your data first and threatening to publish it if you don't pay.

That data might be financial records, customer information, contracts, intellectual property, or internal documents you'd never want made public.

Between privacy regulations and the damage to your reputation, having sensitive information exposed can hurt just as much as losing access to your systems, sometimes more.

This shift matters because it changes the calculation for business owners. With traditional ransomware, restoring from a good backup often took the leverage away from the attacker. Data theft works differently.

Once your information is copied, having a backup doesn't undo the exposure. The only real protection is keeping attackers from getting their hands on the data in the first place.

Attackers are looking for the easiest way in

One of the biggest openings hackers exploit is outdated software.

Any device or application that hasn't been updated is a potential doorway, and that includes file sharing platforms, remote access tools, internet-facing devices, and other systems your business depends on every day.

A single unpatched vulnerability has been enough, in some cases, for attackers to compromise dozens of organizations before anyone noticed something was wrong.

Hackers actively scan the internet for these gaps, so a system that's been overlooked for even a few weeks can become an easy target.

That's why keeping your systems patched and current remains one of the most effective things a business can do to protect itself.

It's not flashy, and it doesn't make headlines, but it closes off the doors attackers rely on most.

Modern attacks are harder to catch

Hackers are also getting better at hiding in plain sight. Rather than using obviously malicious software that antivirus tools are built to catch, many now rely on legitimate tools already built into Windows and other operating systems.

Because these tools are normally used for everyday administration, it becomes much harder for security software to tell the difference between an IT technician doing routine work and an attacker moving through your network.

Virtual servers have become a favorite target for this reason. These are the systems that host multiple applications and services at once, which means a single compromised server can give an attacker access to far more than they'd get from a single computer.

Once an attacker gets into one, they can move through your systems quickly and cause widespread damage before anyone realizes there's a problem.

The best defense is still the basics

Attacks keep evolving, but the fundamentals of good cybersecurity haven't changed much at all. The businesses that hold up best under these newer, sneakier attacks tend to do a few things consistently well:

- Keep operating systems and applications fully patched
- Monitor for unusual activity across every device on the network
- Maintain visibility into who is accessing systems and what they're doing

Have a tested incident response plan in place before trouble hits

None of this is new advice. But businesses that stick to these basics put themselves in a much stronger position, both to avoid an attack and to recover quickly if one happens anyway.

Cyber threats aren't going to stop getting more sophisticated. The encouraging part is that your defenses don't have to fall behind. A little consistency with the fundamentals goes a long way.

If you'd like help understanding where your business stands or strengthening your defenses, give us a call at (734) 457-5000.

"That threat hasn't gone away, but a quieter and in some ways more dangerous tactic is catching on: stealing your data first and threatening to publish it if you don't pay."

Could This Be The Future Of Cybersecurity?

Most cybersecurity tools work reactively.

Something suspicious happens, the system spots it, and then tries to stop the damage before it spreads.

That's incredibly important.

But Microsoft is working on something that pushes much further: using AI to find weaknesses before attackers discover them.

The new system is called MDASH, and the idea behind it is genuinely interesting.

Microsoft has built a platform that uses more than 100 specialized AI agents working together to search for hidden security flaws inside Windows.

These agents are designed to inspect different parts of the system, test for weaknesses, and flag potential vulnerabilities automatically.

Simply put, Microsoft is using AI to hunt for security holes at a scale humans simply couldn't manage alone.

And it appears to be working.

During testing, the system reportedly uncovered multiple previously unknown vulnerabilities inside important parts of Microsoft Windows.

This included flaws that attackers could potentially have exploited remotely over the internet.

Some of those vulnerabilities were considered critical.

These are the kinds of weaknesses that, in the wrong hands, could allow attackers to take control of systems or run malicious code.

What makes this more impressive is the accuracy.

One of the biggest problems with AI-driven security tools has always been false alarms.

Systems that flag hundreds of "possible issues" which turn out to be nothing. That creates noise, wastes time, and makes security teams less effective.

Microsoft claims MDASH has been unusually good at avoiding that problem while still finding genuine risks.

Now, before anyone assumes AI is about to solve cybersecurity completely, it's important to keep this in perspective.

This technology is mainly being used internally by Microsoft engineers now.

It's still early days, and even if these systems become more widely available, they won't suddenly replace the fundamentals that keep businesses safe.

Because most cyberattacks still succeed through ordinary gaps:

- Weak passwords
- Unpatched systems
- People clicking the wrong link
- Poor access controls
- Missing backups

Those remain the biggest risks for most businesses today.

AI-driven security tools may eventually become a powerful extra layer of protection, especially for large organizations managing huge and complex systems.

The idea of intelligent agents constantly scanning for hidden weaknesses before criminals find them is a very promising direction for the future.

But the basics are more important right now.

A fully patched system with strong passwords, multi-factor authentication, good backups, and sensible user awareness training will protect most businesses far better than chasing the latest AI security trend without solid foundations underneath it.

The future of cybersecurity probably will involve more AI working behind the scenes, both defending systems and, unfortunately, helping attackers too.

But while the technology evolves, the core principles of staying safe haven't changed.

Good security still comes down to reducing risk, limiting opportunities for attackers, and making sure the simple things are consistently done well.

If you want to make sure your business security is up to scratch, we'd be happy to help. Get in touch. You can call (734) 457-5000 or email info@mytechexperts.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

TECH EXPERTS

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

Copyright © 2026 Tech Experts® All Rights Reserved.

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