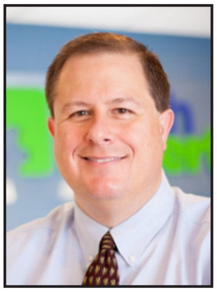
June 2025

TechTidbit.com

brought to you by Tech Experts

AI Is Already in Your Business - Did You Notice?



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

Whether you realize it or not, artificial intelligence is already part of how your business runs.

That email feature that predicts what you're about to type? The chatbot that handles customer questions after hours?
The software that flags invoices or suggests what to reorder?

That's all AI.

It's slipped into our everyday tools - quietly, efficiently, and without much fanfare. Which is exactly why you need to stop and take a closer look.

AI can save time, cut costs, and even help you grow. But it also comes with risks if you're not keeping an eye on how it's being used.

Let's be clear: this isn't about becoming a tech company. It's about protecting your business.

Here's what's at stake:

If you're using AI - powered tools to make decisions - hiring, pricing, marketing - you need to know how those decisions are made. AI isn't magic. It's built by humans, and sometimes it gets things wrong. It can carry bias. It can make bad calls. And if it does, you're still the one responsible.

That means someone in your business needs to be accountable. Not to micromanage every tool, but to check the work. AI should support your team, not replace their judgment.

Another big concern: data.

AI tools often need data to learn and work well. But how that data is handled matters - a lot. Are you sharing sensitive client info with third - party tools? Do your employees know what's safe to upload and what's not? A careless mistake could cost you a client... or worse, lead to a breach.

So, what can you do without hiring a full - time tech guru?

Start with a simple policy.

Write down what tools you're using that involve AI - whether it's something as small as a Gmail add - on or a full - blown business platform. Be clear about what's okay to use, what needs approval, and how data should be treated.

Then train your team.

They don't need to become programmers - but they do need to know the basics. What AI is. What it can do. What it can't. And when to raise a red flag.

You don't need to be scared of AI. But you do need to be smart about how it is being used.

Used right, it can give you a real advantage over your competitors. Used carelessly, it can create a mess that's hard to clean up.

We help businesses like yours use AI responsibly - without getting lost in the weeds. If you want help setting up clear guidelines or choosing tools that make sense for your team, we're ready when you are.

Let's make AI work for you - not against you. Give us a call at (734) 457 - 5000.

AI isn't magic. It's built by humans, and sometimes it gets things wrong. It can carry bias. It can make bad calls. And if it does, you're still the one responsible.

Ransomware: Why Paying Up Could Destroy Your Business

Picture this: You sit down at your desk, fire up your computer, and something's off. Nothing works.

Your files are encrypted. Your systems are frozen. And staring you in the face is a message demanding thousands of dollars in cryptocurrency to get your data back.

It's not a movie plot. It's ransomware. And it's hitting small businesses like yours more often than ever.

The gut reaction? Pay the ransom and make it go away.

But that's exactly what the criminals are counting on.

Here's the truth they don't tell you: Paying the ransom rarely ends the nightmare.

Even if you pay, there's no guarantee you'll get your data back. In many cases, the criminals either don't unlock everything - or they do, but your data is corrupted or incomplete.

Worse, some businesses pay the ransom only to be hit again a few months later by the same attackers.

Why? Because paying once paints a target on your back.

> *"Worse, some businesses pay the ransom only to be hit again a few months later by the same attackers. Why? Because paying once paints a target on your back."*

And it's not just your files at risk anymore. Modern ransomware doesn't just lock your data - it steals it.

Attackers threaten to leak sensitive information unless you cough up more cash. Financial records. Client files. Employee info. It all becomes leverage. And if you don't pay? They publish it online.

Backups? They thought of that, too. Many ransomware variants are designed to find and destroy backup systems before you even realize what's happening. So even if you think you're protected, you might not be.

Here's another kicker: The real cost of a ransomware attack goes way beyond the ransom. Studies show that the total damage - including downtime, recovery, lost productivity, and reputation damage - can be ten times the actual demand.

That's right. A $10,000 ransom could turn into a six - figure problem.

Now let's talk about the long game.

Every ransom paid helps fund the next wave of attacks. The tools get better. The tactics get trickier. And the pool of targets gets bigger. Paying up doesn't just hurt your business - it fuels the engine that drives this entire criminal enterprise.

So what's the smart play? Don't focus on ransom. Focus on recovery.

That means:

- Having backups that can't be touched by attackers.
- Testing those backups regularly - don't just set it and forget it.
- Training your team to spot the red flags and respond fast.
- Creating a disaster recovery plan that actually works when you need it.

You might not be able to stop every threat from getting in. But you can make sure a ransomware attack doesn't take your business down with it.

If you're not sure where to start, we can help. We build cybersecurity and recovery plans specifically for small businesses - without the jargon, the scare tactics, or the six - figure price tag.

Let's make sure you never have to choose between paying criminals or going out of business. Reach out. We've got your back. 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).

What Is A Password Spraying Attack?

Password spraying is a complex type of cyberattack that uses weak passwords to get into multiple user accounts without permission. Using the same password or a list of passwords that are often used on multiple accounts is what this method is all about. The goal is to get around common security measures like account lockouts.

Attacks that use a lot of passwords are very successful because they target the weakest link in cybersecurity: people and how they manage their passwords.

> *"Attacks that use a lot of passwords are very successful because they target the weakest link in cybersecurity: people and how they manage their passwords."*

What is password spraying and how does it work?

A brute-force attack called "password spraying" tries to get into multiple accounts with the same password. Attackers can avoid account shutdown policies with this method.

Attackers often get lists of usernames from public directories or data leaks that have already happened. They then use the same passwords to try to log in to all of these accounts. Usually, the process is automated so that it can quickly try all possible pairs of username and password.

Password spraying has become popular among hackers, even those working for the government, in recent years. Because it is so easy to do and works so well to get around security measures, it is a major threat to both personal and business data security.

As cybersecurity improves, it will become more important to understand and stop password spraying.

How does password spraying differ from other cyberattacks?

Password spraying is distinct from other brute-force attacks in its approach and execution. While traditional brute-force attacks focus on trying multiple passwords against a single account, password spraying uses a single password across multiple accounts.

Understanding brute-force attacks

Brute-force attacks involve systematically trying all possible combinations of passwords to gain access to an account. These attacks are often resource- intensive and can be easily detected due to the high volume of login attempts on a single account.

Comparing credential stuffing

Credential stuffing involves using lists of stolen username and password combinations to attempt logins.

How can organizations detect and prevent password spraying?

Detecting password spraying attacks requires a proactive approach to monitoring and analysis. Organizations must implement robust security measures to identify suspicious activities early on.

Implementing Strong Password Policies. Organizations should adopt guidelines that ensure passwords are complex, lengthy, and regularly updated.

Deploying Multi-Factor Authentication. Multi-factor authentication (MFA) significantly reduces the risk of unauthorized access by requiring additional verification steps beyond just a password.

Conducting Regular Security Audits. Regular audits of authentication logs and security posture assessments can help identify vulnerabilities that could facilitate password spraying attacks.

Enhancing Login Detection. Organizations should set up detection systems for login attempts to multiple accounts from a single host over a short period. Implementing stronger lockout policies that balance security with usability is also crucial.

Incident Response Planning. This plan should include procedures for alerting users, changing passwords, and conducting thorough security audits.

Taking action against password spraying

To enhance your organization's cybersecurity and protect against password spraying attacks, contact us today to learn how we can assist you in securing your systems against evolving cyber threats.

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

Windows 10 Is Retiring - Here's What Your Business Needs to Know

October 14 is a date you don't want to ignore. That's the day Microsoft officially stops supporting Windows 10.

What does that mean? No more security updates. No more bug fixes. No more help when something breaks. Your computers won't suddenly stop working - but they will become much more vulnerable to cyberattacks.

Outdated systems are hacker bait.

Cybercriminals love businesses that don't upgrade on time. Once Microsoft pulls the plug on Windows 10 updates, any newly discovered holes in the system stay wide open. Malware, ransomware, data theft - it all becomes easier. If your business handles sensitive data or customer info, staying on Windows 10 could even land you in legal trouble.

You could pay for Microsoft's Extended Security Updates (ESU) - but it'll cost you. $61 per device the first year, doubling each year to $427 per device by year three. That's a pricey way to avoid a real solution.

So what's the right move?

If your computers are compatible, upgrading to Windows 11 is free. It's more secure, faster, and better for multitasking. But not every Windows 10 machine can make the jump.

Start with a compatibility check. Download Microsoft's free PC Health Check tool and run it on each device. If the message says the PC doesn't meet requirements, don't panic. Sometimes a small setting (like enabling TPM 2.0 or Secure Boot) is all that's needed. In other cases, especially with older machines, replacement may be the only path forward.

Why upgrading now matters:

Waiting until the deadline creates a storm of problems - rushed decisions, unavailable hardware, staff confusion, downtime. Planning ahead means you can upgrade on your terms, not in a crisis.

Plus, Windows 11 brings serious benefits:

Stronger security: Built-in protections like TPM 2.0 and Secure Boot block modern threats before they start.

Better multitasking: New tools like Snap Layouts make it easier to juggle emails, spreadsheets, and documents.

Built-in Microsoft Teams: Collaboration is easier with Teams integrated directly into the taskbar.

Performance boost: Windows 11 uses system resources more efficiently, meaning faster boot-ups and smoother workflows.

Here's your quick upgrade checklist:

- Run the PC Health Check on all business machines.
- Back up your data - files, emails, settings - before doing anything.
- Test your critical software and hardware for Windows 11 compatibility.
- Schedule the upgrade during a low-impact time.
- Train your team on what's new to minimize disruption.
- Have IT support lined up to help with any snags along the way.

Need help? That's what we're here for.

We'll take care of the entire process - device checks, upgrade planning, installations, and post-upgrade support - so your team stays focused and your business stays secure.

Don't wait until the deadline. Let's get ahead of it, together.