May 2026

TechTidbit.com

brought to you by Tech Experts

Your Next Best Employee Probably Won't Be Human

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

What would happen if your competitor could suddenly get twice as much work done… without hiring anyone new?

No extra desks, recruitment fees, or bigger payroll. Just more output.

That's the shift we're moving into.

You've probably heard people talk about AI and wondered what that means for a normal business like yours.

An AI worker isn't a robot. It's software that can think through tasks in a surprisingly human way.

It can read documents, write emails, summarize meetings, analyze numbers, draft proposals, create job descriptions, and even help write computer code.

If you're using Microsoft 365, you're already seeing early versions of this built into tools like Word, Outlook and Teams.

Right now, many SMBs are dabbling. Someone asks AI to tidy up an email. Someone else uses it to help write a report.

But the real advantage comes when a business is properly set up to use AI across the organization.

And this is where some companies are going to struggle.

AI tools work best when your data is organized and accessible. If your files are scattered across personal laptops, old servers, and mystery cloud apps no one remembers signing up for, AI can't safely "see" the information it needs.

If your security is weak, giving AI deeper access could create risk.

Being ready for AI doesn't mean being technical. It means having tidy systems, clear permissions (who can access what), strong security, and leadership that's willing to adapt processes.

Because this isn't a small improvement.

The people building these tools are predicting dramatic leaps forward very quickly. Tasks that currently take hours could shrink to minutes.

Research that once required days might happen in seconds.

When that becomes normal, businesses that can plug in AI workers smoothly will accelerate. Those that can't will feel slower, more expensive, and less responsive.

And this isn't about replacing your team. It's about giving them superpowers.

And in the next few years, the businesses that win won't necessarily be the biggest or the oldest. They'll be the ones that were ready.

If you'd like to discuss how AI could benefit your business, get in touch.

AI tools work best when your data is organized and accessible. If your files are scattered across personal laptops, old servers, and mystery cloud apps no one remembers signing up for, AI can't safely "see" the information it needs.

Beware The Next Generation Of Phishing Attacks

"AI is being used to write malicious code, malware is increasingly assembled as it runs, and AI-assisted scams are becoming more common."

If phishing scams are supposed to trick people, why do so many of them still feel clumsy?

For years, the answer was simple: Most scams were mass-produced.

The same email, the same fake website, sent to thousands of people and hoping a few would fall for it.

That approach is still around, but it's starting to evolve.

When generative AI first appeared, there was a lot of talk about "dynamic websites."

Instead of one fixed site for everyone, pages would be generated on the spot, shaped by who you are, where you are, and what device you're using.

That future never really arrived for everyday businesses. It was complex and rarely worth the effort.

Cybercriminals, however, don't need perfect systems.

They need something convincing. Security researchers have shown how this idea could be used for phishing. While it's still largely experimental, it gives a clear picture of the next generation of scams.

A victim clicks a link and lands on a webpage that looks harmless. There's no obvious malicious code sitting on the page.

Once it loads, the page asks a legitimate AI service to help generate content.

That content is then assembled and run directly in the person's browser.

The result is a phishing page that's created especially for that visitor.

The wording, layout, and code can all be different every time. There's no single fake website for security systems to spot and block - because the scam doesn't fully exist until someone opens it.

Before you panic, this method isn't widespread yet. But the building blocks are in use.

AI is being used to write malicious code, malware is increasingly assembled as it runs, and AI-assisted scams are becoming more common.

For you, this changes the rules slightly.

Phishing is no longer just about spotting bad spelling or sloppy design.

Future scams may look even more polished, personalized, and completely legitimate. Some will appear to come from legitimate senders.

That's why modern protection focuses less on "don't ever click the wrong thing" and more on limiting the damage if someone does.

Tools like multi-factor authentication, secure browsers, and email filtering still work, even when a fake page looks convincing.

Remember this: phishing isn't going away.

To stay protected now, you must assume the next scam will look professional and make sure your defenses don't rely on people spotting obvious mistakes.

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).

Tech Overload Or Tech Opportunity?

Has your team had to adapt to new systems recently?

Perhaps you've rolled out new software, introduced automation, or started experimenting with AI tools inside Microsoft 365.

A few years ago, that level of change might have left people feeling overwhelmed.

Today, something different is happening.

Research shows that most employees have experienced organizational change in the past year, and the most common reason is new technology.

You might expect that constant updates and new tools would drain energy. In reality, many workers report feeling more engaged, not less.

Artificial intelligence is playing a big role in this shift.

Around half of employees now use AI tools regularly at work. They say it helps them complete tasks faster, improve the quality of what they produce, and generally feel more productive.

When technology removes repetitive or frustrating parts of a job, it creates breathing space.

That said, there is a clear warning for business owners.

When companies don't provide approved, secure AI tools quickly enough, employees don't stop using them. They find their own.

This is known as shadow AI, where staff use unapproved tools without IT oversight.

It usually comes from good intentions. People want to work efficiently. But it can expose sensitive company data and create security risks.

The demand for smarter tools is coming from inside your business, not from software vendors pushing features.

There's another factor that matters just as much as the technology itself: employees want to feel listened to during periods of change.

When leadership checks in, explains decisions clearly, and responds to feedback, engagement rises sharply.

When change feels imposed without conversation, enthusiasm drops.

The businesses thriving right now are guiding innovation carefully.

They are introducing new tools with structure, strengthening security, and having regular conversations about what support people need.

Technology isn't settling down any time soon.

Handled properly, though, it can energize your workforce rather than exhaust it.

And if you need help working out the right tech for your business, we can help. Give us a call at (734) 457-5000, or email info@mytechexperts.com.

"You might expect that constant updates and new tools would drain energy. In reality, many workers report feeling more engaged, not less."

The "Session Cookie" Hijack: Why MFA Can't Always Save You

MFA is a strong front-door lock. But it's not the only thing that decides whether someone can get in.

After you sign in, your browser keeps you logged in using a session token (often stored as a cookie). It's the digital version of a wristband at an event: once you've been checked, the wristband proves you belong there.

If an attacker steals that wristband, they may not need to beat your MFA prompt at all.

That's the core of session cookie hijacking. The attacker isn't "cracking" MFA. They're skipping it by replaying your already authenticated session.

This isn't a reason to stop using MFA. It's a reason to stop treating MFA as the finish line.

Why MFA isn't a "game over" control

MFA is still one of the best upgrades most businesses can make, but it doesn't end an attack on its own.

The reason is that attackers don't always try to beat the login step. They try to go around it.

Cloudflare notes that "attackers are finding new ways to circumvent MFA" and that modern incidents are rarely one isolated technique. They're "part of a chain of attacks."

In other words, MFA can block a lot of credential theft, but it doesn't automatically protect what happens after a user successfully signs in. That's where session cookie hijacking comes in.

What a session cookie is and why attackers want it

When you sign into a web app, the site needs a way to remember that you've already proved who you are.

That's what a session is: a temporary "logged-in" state that saves you from entering your password and MFA code on every click.

Kaspersky explains that session hijacking is "sometimes called cookie hijacking" because cookies are commonly used to store the session identifier that keeps you authenticated.

Proofpoint describes session tokens as digital "keys" that let a user stay authenticated. It warns that stealing valid tokens lets attackers impersonate legitimate users and potentially bypass authentication measures "like MFA." That's why session cookie hijacking is so highly leveraged.

If an attacker can steal the cookie or token that represents your active session, they're not trying to defeat the login process. They're attempting to reuse what you already completed and access the same apps and data as if they were sitting at your keyboard.

How session cookie hijacking actually happens

AiTM phishing – Adversary-in-the-middle (AiTM) phishing is the "proxy login" trap. You think you're signing into a normal service, but you're actually signing into a lookalike page that sits between you and the real site.

The attacker relays the login in real time, so everything appears to work, including MFA.

Browser-in-the-Middle session stealing. It's similar in spirit, but it's even more "hands- on" from the attacker's side. Instead of stealing a password and running away, the attacker effectively places themselves in control of the browsing session.

Cookie theft from the endpoint. Not every session hijack starts with a fancy proxy. Sometimes, the attacker simply steals session data from the device itself, allowing attackers to impersonate legitimate users.

MFA is a baseline, not a finish line

MFA is still essential. It blocks a huge amount of credential theft and makes basic account takeover harder.

But session cookie hijacking is a reminder that attackers don't always try to defeat the login step. Sometimes, they reuse what happens after it.

The practical response is layered and realistic. When those controls work together, MFA stops being a checkbox and becomes a strong baseline backed by protections around the session itself.

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