March 2026

TechTidbit.com

brought to you by Tech Experts

Did One Of These Fool You Last Year?

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

You're not imagining it. Scam emails are getting harder to spot.

Phishing attacks are becoming more convincing, more targeted, and more frequent.

Let's rewind a moment…

Phishing is when criminals pretend to be a company you trust and try to trick you into clicking a link, opening an attachment, or logging in to a fake website.

Their goal is usually to steal passwords, money, or access to your systems.

The reason it works so well is simple: It relies on familiarity and distraction.

Last year, the company most often impersonated by scammers was Microsoft.

That's not because Microsoft has done anything wrong, but because so many businesses rely on its email, files, and cloud services.

One stolen Microsoft login can open the door to email accounts, documents, and even financial data.

Close behind were Facebook and Roblox, with other familiar names like Amazon, Google, and PayPal also commonly abused.

Security researchers noticed a big spike in phishing toward the end of last year. That makes sense.

People are busy, inboxes are full, and there's a lot going on with shopping, renewals, year-end tasks, and business and personal income tax preparation.

Scammers know this and time their attacks carefully.

What makes things more worrying is how realistic these messages have become. Criminals now use AI to create fake login pages and "security alerts" that look almost identical to the real thing.

Some attacks don't just steal your password but also grab the extra security codes you use to log in, allowing attackers straight through the front door.

So how do you stay safe?

The most important habit is to slow down. Any email or text that claims there's an urgent problem with an account should immediately raise suspicion.

Instead of clicking, open your browser and go directly to the company's website yourself to check. If something feels off, it probably is.

Extra protection also matters. Using multi-factor authentication, which is a second check like a code sent to your phone, can stop criminals even if they get your password.

Keeping devices protected with up-to-date security software and making sure your team knows what phishing looks like can make a huge difference.

Phishing isn't going away.

But with the right awareness and a few sensible safeguards, it doesn't have to catch you out.

What makes things more worrying is how realistic these messages have become. Criminals now use AI to create fake login pages and "security alerts" that look almost identical to the real thing.

Implementing Zero Trust For Small Business

"For years, Zero Trust seemed too complex or expensive for smaller teams. But the landscape has changed.

Today, it is a practical, scalable defense, essential for any organization."

Think about your office building. You probably have a locked front door, security staff, and maybe even biometric checks.

But once someone is inside, can they wander into the supply closet, the file room, or the CFO's office?

In a traditional network, digital access works the same way: a single login often grants broad access to everything. The Zero Trust security model challenges this approach, treating trust itself as a vulnerability.

For years, Zero Trust seemed too complex or expensive for smaller teams. But the landscape has changed.

Today, it is a practical, scalable defense, essential for any organization.

It's about verifying every access attempt, no matter where it comes from. It's less about building taller walls and more about placing checkpoints at every door.

And it's not just about outsiders. It also limits damage from everyday mistakes - like clicking a bad link - or from a compromised vendor account. With Zero Trust, access is granted based on identity, device health, and context, and only to the specific resources needed. That "least privilege" approach shrinks the blast radius when something goes wrong, making incidents easier to contain and faster to recover from.

Transform your security posture

Adopting Zero Trust isn't just a technical change, it's a cultural one. It shifts the mindset from broad trust to continuous monitoring and validation.

Your teams may initially find the extra steps frustrating, but explaining clearly why these measures protect both their work and the company will help them embrace the approach.

The goal is to foster a culture of ongoing governance that keeps Zero Trust effective and sustainable.

Your actionable path forward

Start with an audit to map where your critical data flows and who has access to it. While doing so, enforce MFA across the board, segment your network beginning with the highest - value assets, and take full advantage of the security features included in your cloud subscriptions.

Achieving Zero Trust is a continuous journey, not a one-time project. Make it part of your overall strategy so it can grow with your business and provide a flexible defense in a world where traditional network perimeters are disappearing.

Contact us to schedule a Zero Trust readiness assessment for your business.

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).

Beyond Chatbots: Preparing Your Company For "Agentic AI" In 2026

AI chatbots can answer questions. But now picture an AI that goes further, updating your CRM, booking appointments, and sending emails automatically. This isn't some far-off future. It's where things are headed in 2026 and beyond, as AI shifts from reactive to proactive, autonomous agents.

This next wave of AI is called "Agentic AI." It describes AI that can set a goal, figure out the steps, use the right tools, and get the job done on its own. For a small business, that could mean an AI that takes an invoice from inbox to paid, or one that runs your whole social media presence. The upside is massive efficiency, but it also means you need to be prepared. When AI gets more powerful, having the right controls matter.

What makes an AI agent "agentic?"

A research article on the evolution and architecture of AI agents explains the big shift like this: AI is moving from tools that wait for instructions to systems that work toward goals on their own. Instead of just helping with tasks, AI starts doing the work, making it possible to hand off whole processes and collaborate with it like a teammate.

The 2026 opportunity for your business

For small businesses, this is about real leverage. Agentic AI can work around the clock, clear out repetitive bottlenecks, and cut down errors in routine processes. That means things like personalizing customer experiences at scale or even adjusting supply chains in real time become possible.

And this isn't about replacing your team. It's about leveling them up. AI takes the busywork so your people can focus on strategy, creativity, tough problems, and relationships, the things humans do best. Your role shifts too, from doing everything yourself to guiding and supervising your AI.

What you need before you launch agentic AI

Before you hand over your processes to an AI agent, you need to make sure those processes are rock solid. The reasoning is simple: AI will amplify whatever it touches, order or chaos, with equal efficiency. That's why preparation is key. Start with this checklist:

Clean and Organize Your Data: AI agents make decisions based on the data you give them. Garbage in means not just garbage out; it can lead to major errors. Audit your critical sources.

Document Workflows Clearly: If a human can't follow a process step by step, an AI won't be able to either. Map out each workflow in detail before you automate.

Building your governance framework

Just like with human team members, delegating to an AI agent requires oversight. That means setting up clear guardrails by asking a few key questions:

- What decisions can the AI agent make on its own?
- When does it need human approval or guidance?
- What are its spending limits if it handles finances?
- Which data sources is it allowed to access?

Answering these questions lets you build a framework that becomes your company's rulebook for its "digital employees."

Security is another critical piece. Every AI agent needs strict access controls, following the principle of least privilege. Regular audits of agent activity are now a non- negotiable part of good IT hygiene.

Embracing the role of strategic supervisor

Agentic AI is a true force multiplier, but it depends on clean data and well-defined processes. It rewards careful preparation and punishes the hasty. By focusing on data integrity and process clarity now, you position your business not just to adapt, but to lead. Contact us today for a technology consultation on AI integration. We can help you audit workflows and create a roadmap for reliable, effective adoption.

"Before you hand over your processes to an AI agent, you need to make sure those processes are rock solid. The reasoning is simple: AI will amplify whatever it touches, order or chaos, with equal efficiency."

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

Passwords Protect People, Not Just Data

Machines start up. Systems exchange signals. Processes run quietly in the background, hour after hour, day after day. For many businesses, that technology isn't just supporting the operation - it is the operation.

Behind it sits something called Operational Technology (OT).

Unlike office IT systems such as email, file storage, and accounting software, OT controls the physical world. It's the hardware and software that tells equipment what to do, when to do it, and how to do it safely.

Production lines, control panels, monitoring systems, sensors, and the networks that connect them all fall into this category. If IT is where information gets created and shared, OT is where information becomes motion, pressure, temperature, speed, and output.

The challenge is that OT security often hasn't matured at the same pace as modern cyber threats. Many OT environments were built years ago, designed for reliability and safety rather than hostile internet-era conditions.

They were expected to run for a long time, change slowly, and stay stable. That mindset makes sense in an industrial setting - but it can leave gaps when today's reality includes remote access, vendor connectivity, cloud reporting, and increasing links between the plant floor and the business network.

One of the biggest weak spots is still surprisingly simple: passwords.

In OT environments, it's common to find shared logins, default credentials that were never changed, passwords written down near the equipment, or accounts that haven't been updated in years.

Sometimes it happens because "everyone has always used the same operator login."

The problem is that the old assumption - "OT is isolated" - is often no longer true.

As OT and IT become more connected, a compromise that starts in the office can reach operational systems. A criminal who gains access to a user's email account or laptop can look for saved passwords, reused credentials, remote access tools, mapped shares, or documentation that reveals how OT systems are managed.

If passwords are reused between environments, that attacker may not need a clever exploit. They can simply log in.

That matters because OT attacks don't just affect data. They can halt production, disrupt critical services, damage equipment, create safety risks for staff, or force a shutdown while you verify what changed.

Even when nothing catastrophic happens, uncertainty is expensive: if you can't trust system readings or configurations, the safest choice is often to stop and inspect.

The good news is that improving password security is one of the highest-impact steps most organizations can take without rebuilding their entire OT environment.

A few practical moves make a major difference:

Use longer passwords or passphrases. Length dramatically increases the effort required to guess or crack a password.

Make passwords unique. Unique credentials reduce lateral movement.

Add multi-factor authentication (MFA) wherever possible. MFA can stop intruders even if a password is stolen.

Of course, OT environments need care. You can't treat a production controller like a disposable laptop. Changes should be planned, tested, documented, and scheduled to avoid downtime.

OT systems are designed to be dependable and almost invisible when they're working properly. That "quiet reliability" can make security easy to overlook. Yet the systems that control physical processes deserve the same discipline and attention as office IT - often more, because the consequences are bigger.