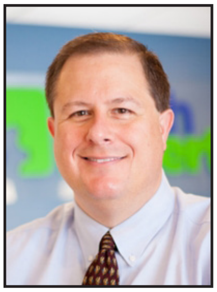
October 2025

TechTidbit.com

brought to you by Tech Experts

Scary Cyber Scams Your Business Should Watch Out For



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

Cyber scams don't need to be sophisticated to cause serious damage to a business.

In fact, many of today's most effective scams rely on busy people making quick decisions and not having time to double-check what they're doing.

Staying informed is one of the best ways to stay protected. So here are five scams we're seeing right now:

Robocall scams

With artificial intelligence, scammers can clone someone's voice using only a short audio clip. You get a call that sounds exactly like a supplier or even a colleague, asking you to urgently confirm bank details. It feels genuine, but it isn't.

Some scams even use this information to carry out a "SIM swap", tricking a phone provider into moving your number to a criminal's SIM card so they can intercept security codes.

Crypto investment scams

A convincing email or social media post might offer an incredible return on a business investment. Some of these projects, known as "rug pulls", are designed to collect funds and then disappear, leaving investors with nothing.

Romance scams (sometimes called pig-butchering scams)

These might sound unrelated to business, but they're not. Scammers build trust over weeks or months, often through social media or messaging apps, and then persuade someone to share sensitive information or even send money.

In some cases, they use AI-generated images or videos to make the scam more believable and later threaten to leak personal material unless they're paid.

Malvertising

Criminals hide malicious links inside paid ads on legitimate sites. An employee looking for a new supplier or tool could click an ad and unknowingly install malware onto a company laptop.

Formjacking

This is where criminals inject code into an online checkout form to steal payment or login details. If staff buy supplies or services from websites that aren't secure, those details can be intercepted.

The common thread is simple: these scams exploit human attention and trust.

Regular reminders and training help staff stay alert, question unexpected requests, and think twice before clicking. A little extra caution can stop a scam before it starts.

We can help you make sure your team is vigilant about these scams and more. Get in touch - email info@mytechexperts.com, or call (734) 457-5000

With artificial intelligence, scammers can clone someone's voice using only a short audio clip. You get a call that sounds exactly like a supplier or even a colleague, asking you to urgently confirm bank details.

The Hidden Cybersecurity Risk In Your Business

"Cybersecurity depends on routine discipline - applying updates, checking access controls, and staying vigilant for unusual activity. When teams are overwhelmed, those routines break down."

It happens far too often. A small business believes its cybersecurity is under control…

…until a routine check uncovers something unexpected, like an old piece of malware quietly running in the background. Or a phishing attack that slipped through weeks ago.

The surprising part? These incidents don't usually involve cutting-edge hackers or advanced tools. They succeed because simple, everyday safeguards have been missed.

And one of the biggest reasons those basics get missed?

Employee burnout.

When staff are tired, stressed, or stretched too thin, important cybersecurity habits start to slide. It's not about carelessness - it's about capacity.

In businesses without a dedicated IT team, employees are already wearing multiple hats.

A manager might put off installing an important software update because they're scrambling to get quotes out before a client deadline.

An accounts assistant might click a suspicious link late at night while rushing to balance the books.

A senior staff member might skip double-checking security settings on a new laptop because they're too busy keeping operations afloat.

These small slips may seem harmless in the moment, but they create cracks in the armor. Cybersecurity depends on routine discipline - applying updates, checking access controls, and staying vigilant for unusual activity. When teams are overwhelmed, those routines break down.

Attackers know this. They don't need to be geniuses to take advantage of exhaustion and stress. Many of today's most common scams - fake login pages, phishing emails that look like vendor invoices, or texts pretending to be from a bank - rely on one thing: distraction. Just a single moment of inattention can give them the foothold they need.

And the consequences can be devastating. We've seen businesses in southeast Michigan deal with payroll delays, compliance headaches, and even the loss of major clients after a seemingly minor mistake opened the door to a cyber incident.

The real cost isn't just money - it's the erosion of trust with employees, partners, and customers.

Technology alone can't prevent that. You can have the best firewall or antivirus in the world, but if an exhausted employee clicks the wrong link, those defenses may not be enough.

That's why the most effective protection starts with people. Supported employees make fewer mistakes. Realistic workloads, clear priorities, and regular training all help staff stay alert and confident.

Creating a workplace culture where it's encouraged to pause, question, and double-check can make all the difference.

Think of it this way: when your team feels like they're sprinting a marathon every day, cybersecurity becomes a chore - just another box to check. But when they have the bandwidth to slow down and follow best practices, those simple defenses work exactly as they should. And more often than not, that's enough to stop an attack before it begins.

If you're worried that burnout might be putting your business at risk, you're not alone. Many small businesses in our community face the same challenge. The good news? You don't have to manage it by yourself.

With the right IT partner, you can take some of that burden off your team's shoulders. We handle the updates, monitoring, and security checks in the background, so your employees can focus on their jobs - without sacrificing safety.

If you'd like help staying ahead of cybersecurity threats, we're here. Let's talk.

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).

Advanced Strategies To Lock Down Your Business Logins

Good login security works in layers. The more hoops an attacker has to jump through, the less likely they are to make it all the way to your sensitive data.

For small and mid-sized businesses, this layered approach can be the difference between a near miss and a costly breach.

The first and most obvious layer is password hygiene. Unfortunately, many businesses still allow short, predictable logins or let staff reuse the same credentials across multiple systems.

That gives attackers a head start. A stronger approach is to require unique, complex passwords for every account. Even better, swap out traditional passwords for passphrases - short sentences that are easier for humans to remember but much harder for machines to crack.

Since most people can't keep dozens of long, random strings in their heads, a password manager is a smart addition. It lets employees generate and store strong credentials securely, so no one has to rely on sticky notes or memory alone.

But passwords aren't enough. Multi-factor authentication (MFA) has become one of the most effective defenses against compromised logins. It works by adding an extra verification step, like a code sent to a phone or an approval in an authenticator app.

Even if a hacker does steal a password, MFA forces them to clear another hurdle before gaining access. The key is to apply it consistently. Leaving one "less important" account unprotected is like locking your front door but leaving the garage wide open.

Another important safeguard is access control, often called the principle of least privilege. The fewer people who have administrative rights, the fewer chances there are for those credentials to be stolen or misused.

Keep high-level privileges limited to the smallest possible group, and avoid using those accounts for everyday work.

Instead, maintain separate admin logins and store them securely. The same rule applies to third-party vendors: give outside users only the access they need, and nothing more.

Device and network security also play a role. Even the strongest login policies won't mean much if an employee signs in from a compromised laptop or an unsecured public Wi-Fi connection.

That's why company laptops should be encrypted and protected with strong passwords, while mobile devices should have security apps in place - especially for staff who travel or work remotely.

Firewalls should remain active both in the office and for home-based workers, and automatic updates for browsers, operating systems, and applications should always be turned on. Those updates frequently include security patches that close holes attackers are quick to exploit.

Email deserves special mention because it remains one of the most common gateways for login theft. One convincing message is all it takes for an employee to hand over credentials to an attacker.

Advanced phishing and malware filtering can block many of these messages before they ever land in an inbox. On the technical side, setting up SPF, DKIM, and DMARC records makes your company's domain harder to spoof, reducing the chances of a successful impersonation attack.

Just as important, regular user training helps employees learn how to verify unexpected requests and spot suspicious links before they click.

Finally, even the best defenses can be bypassed. That's why preparation matters just as much as prevention. An incident response plan ensures your team knows what to do the moment something looks wrong, minimizing panic and downtime.

Routine vulnerability scanning and credential monitoring can catch issues before they escalate. And reliable, tested backups guarantee that even if attackers gain access, your business can recover quickly without paying a ransom or suffering permanent data loss.

None of these steps need to happen overnight. The best way to approach login security is to start with the weakest link - maybe it's an old, shared admin password or the lack of MFA on your most sensitive systems - and fix that first.

Then move on to the next gap. Over time, those small improvements add up to a solid, layered defense that protects your team, your data, and your reputation.

In the end, good login security isn't just about keeping hackers out. It's about giving your employees confidence that when they log in, they're working in a safe, secure environment. With the right layers in place, your logins become a security asset - not a weak spot.

> *"None of these steps need to happen overnight. The best way to approach login security is to start with the weakest link - maybe it's an old, shared admin password or the lack of MFA on your most sensitive systems - and fix that first."*

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

The Long-Term Costs Of Slow Computers

We've all been there. You press the power button on your computer, grab a cup of coffee, and by the time it finally boots up, you could've answered three emails and called a client back. At first, you tell yourself it's just a small annoyance. But over time, that sluggish computer quietly chips away at your productivity - and your team's morale.

The truth is, old or underperforming devices cost businesses far more than the price of replacing them. Let's break down the hidden ways slow computers impact your company.

Lost productivity adds up

When every task takes longer than it should, productivity suffers. If an employee wastes just 15 minutes a day waiting for programs to load or systems to respond, that's more than an hour a week. Multiply that across a 20-person team and you're losing over 1,000 hours of productive time every year. That's not just inconvenience - it's real money left on the table.

Employee frustration and morale

Nothing drains motivation faster than feeling like your tools are working against you. Slow logins, constant freezes, and endless restarts leave employees frustrated before they even begin their day. That frustration doesn't stay in front of the screen - it spills into customer service interactions, team collaboration, and overall job satisfaction. When employees feel held back by technology, their energy and focus shift away from the work that really matters.

Increased support costs

A sluggish computer isn't just a time waster - it's a resource drain. Older devices often need more IT support for troubleshooting crashes, replacing outdated components, or recovering from errors. While patching things together may seem cheaper than replacing equipment, those repair bills and lost hours add up quickly. In many cases, businesses spend more keeping an old machine alive than they would on a modern replacement.

Security risks of outdated hardware

It's not just speed you need to worry about. Older computers may no longer receive security updates from the manufacturer, leaving them vulnerable to cyber threats. Hackers look for weak entry points, and an outdated device without current protections can serve as an open door into your entire network.

Repair or replace?

So how do you know when it's time to retire a slow device versus investing in a repair? A good rule of thumb is the "50 percent rule." If fixing the computer costs more than half the price of a new one - or if it's more than five years old - replacement is usually the smarter choice. Repairs may buy you a little more time, but they rarely restore the performance and security of modern systems.

Think of it like maintaining a car. At some point, the cost of repeated repairs outweighs the benefits, and a new, reliable vehicle is the better investment. The same goes for your business technology.

The smart move forward

Upgrading computers doesn't just remove frustration - it gives your employees tools that support their best work. Faster machines mean quicker logins, smoother multitasking, fewer errors, and improved security. That translates into happier employees, more satisfied clients, and fewer hidden costs dragging on your bottom line.

If your team spends more time waiting on their computers than getting work done, it's time to take a hard look at your equipment. A well-planned upgrade cycle saves money, improves morale, and helps your business run at the speed it needs to compete.