August 2026

TechTidbit.com

brought to you by Tech Experts

The Threats Hiding In The Tools You Use Every Day

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

How do you imagine a cyberattack? A sophisticated hacker breaking through layers of security? Using advanced tools that no regular business could possibly defend against?

The reality is usually way less glamorous.

Many breaches start with something small. A forgotten account that was never removed. A laptop that missed an update. A security setting that was switched off and never switched back on.

These are the kinds of gaps attackers actively search for because they're far easier to exploit than forcing their way through a heavily protected system.

In other words, the danger often comes from the things nobody realized were a problem.

One of the biggest changes in cybersecurity right now is the growing focus on identities.

Instead of attacking systems directly, criminals increasingly target usernames and passwords.

Once they gain access to a legitimate account, they can move through a business much more easily because, from the outside, it looks like a normal user logging in.

That can happen surprisingly quickly. In some cases, ransomware attacks have escalated within hours of the initial breach.

The challenge is that modern businesses are complicated. Staff work remotely. Devices move between home and office.

New software gets introduced. Small gaps appear naturally, unless someone is constantly monitoring them.

Even security tools themselves can become blind spots.

You may have protection installed, but if it is misconfigured, outdated, or partially disabled, it creates a false sense of security.

Attackers also rely heavily on something known as "living off the land" techniques.

This means using legitimate tools already built into Windows and Microsoft 365 to carry out malicious activity.

Because those tools are commonly used by IT teams every day, suspicious behavior can blend into normal activity more easily.

Artificial intelligence is likely to accelerate this problem.

AI tools can help criminals identify weaknesses faster, automate attacks, and adapt techniques more quickly than before.

But many of the most effective protections are the basics done well.

Strong passwords, multi-factor authentication, regular updates, controlled access permissions, and ongoing staff awareness training remain some of the strongest defenses available.

If you'd like help spotting and closing small security gaps before somebody else finds them, get in touch.

Many breaches start with something small. A forgotten account that was never removed. A laptop that missed an update. A security setting that was switched off and never switched back on.

It's Happening, Whether You Like It Or Not

"Employees may paste confidential documents into public chatbots, connect AI assistants to email accounts, or allow AI tools to access files and calendars without fully understanding what happens to that data afterwards."

AI tools are becoming a normal part of the working day.

Someone uses one to tidy up a report. Someone else asks a chatbot to summarize meeting notes. A team member installs an AI browser extension because it helps them work faster.

Most of this happens with good intentions.

But some businesses have no visibility of it at all.

This is known as "shadow AI".

It describes employees using AI tools that haven't been approved, reviewed, or properly managed by the business.

In many ways, it's like shadow IT, where staff adopt their own software without involving the IT team.

The difference is that AI tools can interact with company information in deeper ways.

Employees may paste confidential documents into public chatbots, connect AI assistants to email accounts, or allow AI tools to access files and calendars without fully understanding what happens to that data afterwards.

The motivation is easy to understand. These tools save time, reduce admin, help people get through work more efficiently.

So, banning AI outright rarely works.

If employees feel the tools genuinely help them, they often continue using them secretly. At that point, the business loses even more visibility and control.

The better approach is usually to accept that AI is now part of modern work, then guide people towards safer, approved options.

Newer AI systems are becoming more capable very quickly. Tools are no longer limited to generating text or summaries.

They can search files, access systems, organize information, trigger workflows… and even carry out actions automatically.

Without proper oversight, that creates obvious security and compliance concerns.

For businesses using Microsoft 365, approved tools like Copilot offer a safer route because they sit inside existing permissions and security controls.

That doesn't remove risk completely, but it does give businesses much better visibility over how AI is being used.

Whatever tools you're using, the important thing is not to ignore the issue.

If you need better oversight on how your team is using AI tools, we can help. Get in touch.

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).

SIM Swapping: How Hackers Steal Your Phone Number

One morning, your phone drops to "No Service" and stops receiving calls and texts. You assume it's a network glitch and you get on with your day.

But across town, someone has just convinced your mobile carrier that they're you.

They've moved your number onto a SIM card sitting in their own phone.

Every call and text meant for you now goes to them, including the security codes that protect your email and your bank logins.

This is a SIM swap. The attacker never touches your password or breaks into a single system. They take over your phone number, then use it to reset everything attached to it.

They start by gathering a few details about you, often pulled from an old data breach or your social media.

Then they call your carrier, claim your phone was lost or damaged, and ask to activate your number on a new SIM. If the agent believes the story, your number is theirs in minutes.

From there, the SMS codes you rely on become their codes (SMS is the text message system most accounts use to send those one-time login codes). Password reset links and login verifications all land on their device instead of yours.

Researchers at Princeton University tested five major US carriers by posing as customers and trying to move numbers they didn't own. **They succeeded on 80% of their first attempts**, mostly because the carriers were leaning on security questions a motivated attacker could answer.

The losses reported to the FBI run into the tens of millions of dollars a year, and the true figure is almost certainly higher, because most victims report the end result, like a drained account, rather than the phone takeover that caused it.

Your personal mobile number is probably the recovery method for nearly everything you log into, from your Microsoft 365 account to your business bank.

If that one number falls into the wrong hands, a lot can fall with it. Don't panic though. This is very fixable, and the setup is quick and free:

Lock your number with your carrier

Every major provider now offers a free toggle that blocks anyone from moving your SIM or porting your number without your say-so.

Move your important logins off text-message codes

For your email, banking, and admin accounts, switch from SMS codes to an authenticator app or a passkey. Both keep working even if someone steals your number because the approval happens on your device, not through your phone signal.

Add a separate passcode to your carrier account.

Most carriers let you set a PIN or passcode that's required before any change is made to your account. It's one more wall between an attacker and your number.

Many carriers now send a text or email alert when someone requests a SIM change on your account. If that alert shows up and it wasn't you, call your carrier right away.

If you'd like a hand checking which of your accounts still rely on text-message codes, or help locking down your team's numbers, just reply and we'll walk you through it.

"Your personal mobile number is probably the recovery method for nearly everything you log into, from your Microsoft 365 account to your business bank."

The Employee Who Left Six Months Ago Still Has Access

When someone leaves your company, you probably collect their keys, take back the laptop, and shut off their email. Job done, right?

Not quite.

Over the years, most employees pick up access to more systems than anyone tracks. There's Microsoft 365, your accounting software, your CRM, cloud storage, payroll, vendor portals, remote access tools, and shared mailboxes.

Then there are the accounts nobody remembers: a Canva login someone set up for marketing, a Facebook page a former employee managed, a Dropbox folder shared with a manager years ago, an app someone connected to their Microsoft 365 account and forgot about.

The employee leaves, their email gets disabled, and everyone assumes their access went with it. It often doesn't.

What is access creep

Access creep happens when employees pick up new permissions as they change roles, but the old ones never get removed.

Someone starts in customer service, moves to sales, and eventually becomes a manager. Each job change adds new access. Rarely does anyone go back and take the old access away.

After five years, that employee may be able to reach far more of your business than their current job requires. When they leave, all of that access leaves the building with them, at least on paper. In reality, it usually stays right where it was.

Offboarding needs to be a process, not a checklist item

Turning off someone's email is a start, but it only closes one door. What about the cloud app they logged into with a separate password? The vendor site where their account is still active? The shared password they know? The company social media account they had the keys to?

Offboarding works best when it starts before the employee's last day.

Someone should know which systems they can reach, which devices they hold, which passwords or codes they know, and whether they have access to any shared accounts.

From there, equipment gets returned, individual accounts get disabled, shared passwords get changed, remote access gets pulled, and email forwarding or delegation gets reviewed.

Don't forget the accounts your IT provider doesn't manage directly. Your bookkeeper may have logins for banking or payroll.

A salesperson might hold customer portal credentials. Whoever runs your marketing may control social media accounts, your website, ad platforms, or your email marketing tool. Those accounts need the same attention.

The account nobody is watching is the one that gets hacked

Most former employees have no interest in logging back into your systems. That's not the real risk. The real risk is that their old account is still sitting there, active and unused. If that account gets compromised months or years later, an attacker may find it still opens the door to your business. Nobody notices, because nobody remembers the account exists. That makes forgotten accounts an easy target.

Don't wait until someone leaves

Access should match the job. When someone's role changes, their access should change with it.

A periodic review of who can reach what often turns up old accounts, admin permissions nobody needs anymore, forgotten vendor logins, and software nobody uses. You might be surprised by what's still active.

Ask yourself this: if you made a list today of everyone who can access your company's systems and data, could you say for certain that everyone on that list still belongs there?

If your honest answer is "I think so," it's worth a closer look.

Give us a call for a no-charge, no-obligation review of your user accounts and access, and we'll help you build a process that covers employees joining, changing roles, and leaving for good.

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