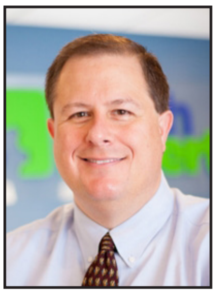
July 2026

TechTidbit.com

brought to you by Tech Experts

The Inbox Hiding Place You Don't Think To Check



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

If a hacker got into your email account, you would probably do the obvious thing and change your password right away. That is a good instinct. But it does not always solve the problem.

There is a small feature buried in your inbox settings that attackers use to stay hidden long after you have locked them out. It is called an inbox rule, and most business owners have no idea it exists.

What is an inbox rule?

An inbox rule is a setting that automatically moves emails into folders, flags certain messages, or forwards them to another address. You may already use rules to keep your inbox organized, sorting invoices into one folder and newsletters into another.

That same feature is exactly what makes it so useful to a criminal.

How attackers use inbox rules against you

When someone breaks into an email account, one of the first things they often do is create a hidden rule of their own. These rules can quietly forward copies of your emails to an outside address, move important messages out of your main inbox, or mark them as read so you never notice them arrive.

This happens fast. In many cases, attackers set up these rules within seconds of gaining access, before you even know anything is wrong.

That speed gives them a real advantage. With a hidden rule in place, an attacker can read your conversations, pull out sensitive information, and hide the security alerts that would normally tip you off. If they are after your finance team or leadership, they can also sit back and watch for the right moment to reroute a payment.

Here is the part that catches most people off guard: changing your password does not remove these rules. If you reset your password but skip this step, the attacker may still be reading everything that comes into your inbox.

How to check for hidden inbox rules

The good news is that this is easy to check once you know where to look. Every inbox rule has a name, and one that looks strange, generic, or unfamiliar is worth a closer look. Take a few minutes to review your rules periodically, and always check them right after any suspected security issue.

You do not need advanced technical skills to do this. Most email platforms list all active rules in one settings screen - anything you did not create yourself should raise a flag.

The takeaway

Modern cyberattacks do not always rely on complicated hacking techniques. Sometimes they simply use a feature that is already sitting inside your inbox, working exactly as it was designed to, just for the wrong person's benefit. A quick habit of checking your inbox rules can close a gap that a password reset alone will not. If you would like a hand making sure your business email is locked down the right way, give us a call.

When someone breaks into an email account, one of the first things they often do is create a hidden rule of their own. These rules can quietly forward copies of your emails to an outside address, move important messages out of your main inbox, or mark them as read so you never notice them arrive.

Need Help? Email support@MyTechExperts.com, or call (734) 240-0200

Those Little Jobs Add Up… Delegate Them To AI

"Copilot in Teams can summarize discussions in a more practical way, pulling out decisions, highlighting what still needs doing, and helping people get straight to the important points."

When people think about AI at work, they often imagine things like writing reports, analyzing data, or answering emails.

That's useful, of course. But it's not where most of your time goes.

In a typical working day, it's the smaller jobs that really slow things down. Following up after meetings, tidying documents, fixing spreadsheets, chasing information.

They're not difficult, but combined, they eat into hours you'd rather spend elsewhere.

This is where tools like Microsoft Copilot are becoming genuinely helpful.

Take meetings as an example. The real time cost usually comes afterwards. Notes need checking, actions need confirming, and anyone who missed the call needs catching up.

Copilot in Teams can summarize discussions in a more practical way, pulling out decisions, highlighting what still needs doing, and helping people get straight to the important points.

It's a similar story with writing.

Most people aren't staring at a blank page. They're trying to improve something that already exists. A draft might be too long, unclear, or not quite right for the audience.

Copilot can reshape that content, tighten it up, and adjust the tone without you having to rewrite everything from scratch.

Spreadsheets are another common frustration.

You know what you want the outcome to be but remembering how to get there isn't always straightforward.

Instead of searching for formulas or watching tutorials, you can describe what you need in plain language and let Copilot handle much of the process.

Microsoft has also started bringing everything together more effectively.

Shared pages and notebooks mean ideas, notes, and files don't end up scattered across different tools.

It becomes easier to keep projects moving without constantly switching between apps.

And for those repetitive tasks that crop up every day, simple workflows can now be created just by describing the process.

Routine updates, reminders, and approvals can run in the background without needing manual input each time.

As a reassurance, this isn't to replace people. It's to remove the small points of friction that build up during the day.

When those start to disappear, work feels smoother, and your team can focus more on the things that move the business forward.

If that sounds like something you'd like to learn more about, 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).

The 4-Step Legacy IT Debt Audit Your Business Needs

Legacy systems and outdated technology create hidden costs that drain your budget and slow your business down.

If you're running software that hasn't been updated in years, relying on hardware past its prime, or patching together workarounds to keep things running, you're carrying technical debt.

According to TechTarget, "A technical debt audit involves systematically identifying, assessing, and prioritizing areas of technical debt within an organization's IT landscape. This process helps organizations understand the scope and impact of their debt, enabling them to create a strategic plan for remediation."

Here's how to conduct a practical audit of your legacy IT systems.

Inventory your current IT assets

Start by creating a complete list of every system, application, and piece of hardware your business uses. Include the age of each asset, its current version, the vendor's support status, and who depends on it daily.

This isn't just about servers and computers - document your software licenses, cloud subscriptions, and any custom applications built years ago that still run critical processes.

Assess business impact and risk

For each item in your inventory, evaluate how it affects your operations. Ask: What happens if this system fails tomorrow? Does it handle sensitive customer data? Is it connected to other critical systems?

CIO.com emphasizes that "assessing the impact of technical debt on business operations" and "prioritizing remediation efforts based on risk and value" are essential steps in managing technical debt effectively.

Systems that pose security risks or could halt business operations should rise to the top of your priority list.

Calculate the true cost of keeping it

Legacy systems cost more than their maintenance contracts. Factor in the staff time spent on workarounds, the productivity lost to slow performance, the security vulnerabilities that put you at risk, and the opportunities you're missing because your systems can't support new capabilities.

Compare these ongoing costs against the investment required to modernize or replace the system.

Create a prioritized remediation roadmap

Based on your risk assessment and cost analysis, build a realistic plan for addressing your technical debt. Some systems may need immediate replacement while others can be phased out gradually.

Budget for both quick wins that deliver immediate value and longer-term projects that address foundational issues.

Set clear timelines, assign ownership, and establish metrics to track your progress.

If you'd like help conducting a thorough legacy IT audit or developing a modernization strategy that fits your budget and timeline, contact us to discuss your specific situation. You can give us a call at (734) 457-5000, or email us at info@mytechexperts.com.

> *"If you're running software that hasn't been updated in years, relying on hardware past its prime, or patching together workarounds to keep things running, you're carrying technical debt."*

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 Hidden Cost Of "Just This One Time"

Most technology problems do not begin with a major failure. They start with a small shortcut.

An employee needs to send a large file, so they upload it to a personal cloud storage account. Someone forgets their laptop charger and borrows a family computer to finish a proposal. A manager shares a password with a coworker because it is quicker than creating a new login.

Each decision seems harmless on its own. After all, everyone is just trying to get their job done.

The trouble is that these "just this once" moments have a habit of becoming everyday habits.

Over time, businesses end up with important files scattered across personal accounts, passwords shared between multiple employees, and sensitive information stored in places that were never meant for business use. Nobody intended to create a security risk. It simply happened one shortcut at a time.

This is one of the biggest challenges we see when working with small businesses.

Most owners invest in firewalls, antivirus software, and secure backups. Those are all important. But even the best technology cannot protect information that has quietly drifted outside of your managed systems.

Imagine an employee leaves your company. If company files are stored in their personal cloud account, do you still have access?

If customer contacts are saved on a personal phone, can you retrieve them? If passwords were shared through text messages or sticky notes, how many accounts need to be changed?

These situations create unnecessary stress during what is already a busy time.

The same problem appears when businesses begin to grow.

What works for five employees often breaks down at fifteen or twenty. New staff members need access to files. Teams need to collaborate. Managers need confidence that information is protected without slowing everyone down.

That is why consistency matters. Instead of asking employees to figure out the best way to share files or store documents, give them one approved method and encourage everyone to use it. Instead of sharing passwords, use a password manager that allows secure access without exposing the actual password. Instead of allowing business information to spread across personal devices and accounts, keep it inside systems that your business owns and controls.

The goal is not to make work more complicated. It is to remove uncertainty.

Employees generally want to do the right thing. If the secure option is also the easiest option, people will naturally follow it.

This is also a good reminder to review your business processes every so often. Ask yourself a few simple questions. Where are our important files stored? Who has access to them? Are we relying on personal accounts for business work? Would someone else be able to find what they need if a key employee was away for a week?

You might be surprised by the answers.

Small improvements made today can prevent much larger problems later. Better organization, clearer processes, and a few sensible security practices can save hours of frustration while reducing your risk at the same time.

Technology should make running your business easier, not leave you wondering where your information is or who can access it.

If you are not sure whether your business has developed a few "just this once" habits over the years, we would be happy to help you take a closer look. Sometimes the biggest improvements come from fixing the small things before they become expensive problems.