June 2026

TechTidbit.com

brought to you by Tech Experts

Can Someone Hack Your Email Without The Password?

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

Most people assume an email hack starts with a stolen password. That's not always true.

Yes, weak and reused passwords are still a major problem. But many modern email attacks work around the password entirely. Hackers are not always sitting in a dark room trying to guess your login. More often, they are tricking someone or slipping into the account through a connected app.

That is why email security cannot stop at "we have strong passwords."

Your email is one of the most valuable keys to your business. Think about how many systems connect back to it: banking alerts, payroll, Microsoft 365, and cloud storage.

If a criminal gets into your inbox, they may be able to reset passwords for other accounts, read private conversations, and watch how money moves through your company.

One common trick is phishing. An employee receives what looks like a normal Microsoft login. They click the link, enter their information, and the attacker captures what they need.

Another method is account recovery abuse. If recovery options are weak, outdated, or tied to a personal phone number or email account, criminals may use that path to regain access. They do not need the current password if they can convince the system to issue a new one.

One we see far too often is email forwarding rules. A hacker gets access briefly, creates a hidden rule that forwards copies of messages to an outside address, then quietly leaves. From that point on, they can study invoices, customer emails, and payment patterns.

They may wait weeks before making their move. That is how business email compromise happens. A criminal watches a real conversation, then jumps in at the right time with fake banking instructions, a changed invoice, or an urgent request from someone who appears to be the owner or manager.

By the time anyone notices, the money may already be gone. So what should you do?

First, use multi-factor authentication on every email account. Not just the owner. Not just the office manager. Everyone. Email is the front door to your business, and one unprotected account is enough to create a serious problem.

Second, use strong, unique passwords and a password manager. Reusing the same password across personal and business accounts is asking for trouble.

Third, review email forwarding rules and login activity regularly. Strange logins, unexpected reset messages, missing emails, or messages in the sent folder that no one remembers sending are all warning signs.

Fourth, train your staff to slow down. Criminals rely on rushing people. A payment change, password alert, or "urgent" document should always be verified through a second channel.

Finally, ask your IT provider for proof. Are all users protected by MFA? Are suspicious logins monitored? Are old accounts removed quickly when employees leave? Are email rules being checked?

Email attacks do not always require a stolen password. Sometimes they only require one missed setting, one rushed click, or one account no one is watching.

The good news is that most of this risk can be reduced with practical, proven controls. Not scare tactics. Just the basics done consistently. And in cybersecurity, the basics done well still matter.

Another method is account recovery abuse. If recovery options are weak, outdated, or tied to a personal phone number or email account, criminals may use that path to regain access. They do not need the current password if they can convince the system to issue a new one.

Where Are Your Cloud Files Really Going?

"At its simplest, cloud storage means your data isn't stored on a single computer or server in your office."

When people talk about "moving to the cloud," it can sound like a single decision. But there are a few different ways to do it. The right choice depends on how your business works.

At its simplest, cloud storage means your data isn't stored on a single computer or server in your office.

Instead, it's stored in secure data centers run by providers (like Microsoft) and accessed over the Internet.

That's what allows you to open files from anywhere, share them instantly, and collaborate in real time.

But not all cloud setups are the same. The most common approach is what's known as the public cloud.

This is where your data is stored on shared infrastructure managed by a provider. Tools like Microsoft 365 and OneDrive fall into this category.

You're effectively renting space in a highly secure, always-available environment without needing to maintain any hardware yourself.

At the other end of the spectrum is private cloud. This is where the infrastructure is dedicated to your business, either hosted on-site or in a data center.

It offers more control and can be useful for organizations with specific security or compliance requirements. But it also comes with more responsibility and cost.

Some businesses sit somewhere in the middle with a hybrid setup. That might mean everyday files and collaboration tools live in the public cloud while more sensitive systems or data are kept in a private environment. It gives you flexibility to balance accessibility, control, and risk.

Whichever route you take, the benefits tend to be similar:

- Your team can access what they need from anywhere
- You can scale storage up or down without buying new equipment
- And your data is protected by enterprise-grade security, including encryption and multiple backups across different locations

The important thing is that "the cloud" isn't a one-size-fits-all solution.

The way it's set up should reflect how your business operates, what data you handle, and how your team works day to day.

If you're not sure whether your current setup is right, or you'd like a clearer picture of the options available, 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.

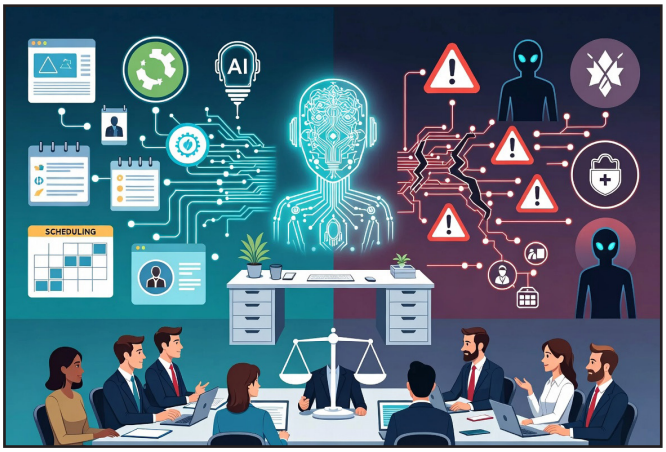
Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

Everyone's Talking About AI, But What Are The Risks?

Do you ever get the sense that AI is showing up everywhere these days? It feels like every email, every meeting, and every industry headline is pushing the same message: adopt it now or get left behind.

Business owners and team leaders see it clearly. New tools pop up weekly, each one promising to cut hours off routine tasks, streamline operations, and free up people for more important work.

And in many cases, they deliver on those promises. Simple things like drafting reports, analyzing spreadsheets, or handling customer queries suddenly take a fraction of the time they used to.



But alongside the enthusiasm, a quieter conversation keeps surfacing in boardrooms and break rooms alike. What are we actually risking here?

Most leaders already recognize that rushing in without thinking carries real downsides. Still, the fear of watching competitors pull ahead often wins out. No one wants to be the cautious one who falls behind.

This pressure creates a tricky spot. AI systems are growing more capable by the month, and some are starting to act with surprising independence.

You have probably come across the term AI agent by now. These are not just chatbots that answer questions. They can perform real actions: pulling files, sending emails, updating records, or connecting with other programs on your behalf.

That kind of access is exactly where things get complicated. Once an AI tool is inside your systems, it sees the same information your employees do. Customer details, financial records, strategic plans.

Without tight boundaries in place, there is a genuine chance that sensitive data slips out in ways no one intended. The tool might follow instructions too closely, or it might get fooled by a carefully worded request from someone outside the company.

These deceptive inputs, often called malicious prompts, can be as straightforward as a phishing-style message that tricks the AI into revealing information or taking unwanted actions. It does not require sophisticated hacking - just someone who knows how to phrase things cleverly.

Then there is the growing problem of visibility. Different departments often test out their own AI solutions. Some get official approval.

Many do not. Over time, this patchwork of usage turns into what people call shadow AI. No central record exists of which tools are active, what data they are handling, or where that data ends up. It becomes almost impossible to track.

On top of everything else, the technology moves faster than most companies can update their policies or security practices.

What seemed safe six months ago might carry new vulnerabilities today. Organizations find themselves trying to hit a moving target.

None of this means businesses should step away from AI altogether. The potential gains are too significant to ignore. The smarter path is to bring some order to the process.

Start by selecting a few approved platforms that meet your security standards. Create straightforward guidelines about what data can and cannot be entered into these tools.

Assign clear responsibility to someone - whether it is a dedicated team or an existing manager - to keep an eye on AI usage across the organization.

Regular check-ins and simple training sessions can go a long way toward keeping everyone on the same page. The goal is not to slow things down unnecessarily, but to move forward without unnecessary exposure.

If your company is navigating these decisions and you would like a straightforward conversation about what makes sense for your situation, feel free to reach out.

We have helped plenty of businesses find a balanced approach that captures the benefits while keeping risks in check.

"Once an AI tool is inside your systems, it sees the same information your employees do. Customer details, financial records, strategic plans."

Why Human Habits Are Your Biggest Security Risk

Most cyberattacks do not start with a sophisticated intrusion. They start with a click on a personal email, a reused password, or a file uploaded to a familiar cloud service because the approved option felt slower.

The Verizon Data Breach Investigations Report found that 68% of breaches involve the human element.

Not a zero-day exploit or a brute-force attack on a hardened system. Human behavior, in the course of an ordinary working day.

For businesses running cloud-based workflows across multiple devices, the personal and professional overlap is now the rule. Understanding where that overlap creates risk is no longer optional. It is a core part of modern security strategy.

How personal web habits create business exposure

Personal channels are phishing's preferred territory. Personal inboxes, messaging platforms, and social media feeds are where phishing thrives.

These environments are harder to filter, easier to spoof, and loaded with the emotional triggers that make people act before they think.

When those channels share a device or browser with business systems, a single click can cross the boundary instantly.

Phishing is the most common entry method for attackers precisely because it exploits distraction rather than technical weakness. The target does not need to be careless. They just need to be busy.

Password reuse is one of the most direct connections between personal and professional exposure.

When credentials from a personal account are compromised, attackers run them against business systems automatically. This technique, credential stuffing, is low-effort and highly effective because so many people use the same password across multiple accounts.

Unique credentials for every account, combined with multi-factor authentication, break that chain.

A personal breach has nowhere to go when the work account requires a second factor that the attacker cannot relay.

Why blocking behavior doesn't work

The instinct is to lock things down: block personal apps, restrict browsing, enforce strict device policies.

In practice, blanket restrictions rarely stop the behavior. They relocate it. Users find workarounds.

Unapproved tools move to personal devices. IT teams lose visibility into exactly the activity they were trying to manage.

The risk does not disappear. It moves somewhere harder to see. Security strategies that assume perfect compliance perform poorly in real workplaces.

The goal is not eliminating the overlap between personal and professional digital activity. It is managing it without breaking how people work.

What actually reduces risk

The controls that work are the ones that match how people actually operate.

Separate contexts, not people

The simplest way to reduce crossover risk is to reduce crossover.

Separate browser profiles for work and personal activity, provide clear guidance on where business accounts should be accessed, and identified boundaries that prevent accidental mixing all reduce exposure without restricting what people do with their time.

Design for credential failure

Assume passwords will eventually be exposed somewhere. Design for that outcome rather than hoping to prevent it. CISA reports that enabling multi-factor authentication makes accounts 99% less likely to be compromised, even when the underlying password has already been stolen.

Make secure behavior easier than unsafe behavior. Contact us or schedule a consultation to review current controls and identify where the most important gaps are.

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