November 2026

TechTidbit.com

brought to you by Tech Experts

Why Your Best Employee Might Be Your Biggest Business Risk



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

Every small business has one. The person who knows where everything is, how everything works, and who to call when something breaks.

Maybe it's the office manager who has run payroll for 12 years or the bookkeeper who is the only one who really understands your accounting system. Maybe it's you.

That person is usually your most valuable employee. They're also one of your biggest risks.

The problem nobody notices

I see this all the time with clients. Things run smoothly, so nobody thinks twice about it. Then that person takes a two-week vacation, has a family emergency, or hands in their notice, and suddenly, the business can't do things it has done every week for years.

Invoices don't go out and vendors don't get paid. Or nobody knows the login for the supplier portal.

None of this happens because that employee did anything wrong. They're so good at their job that everyone else stopped needing to learn it. Over time, the knowledge ends up in one person's head instead of somewhere the business can reach it.

Why it's easy to put off

Fixing this never feels urgent. Your key person is busy, and asking them to write down everything they do feels like a distraction.

Some people also worry that documenting their job makes them easier to replace. Talk about that openly. The point is to keep the business running when they're out sick and to let them take a real vacation without checking email from the beach.

Start with what would hurt most

You don't need a giant procedures manual. Ask one question: If this person were gone for two weeks starting tomorrow, what would break first?

Payroll, billing, ordering, and anything with a hard deadline usually tops the list. Work through it one item at a time and have your key person write down the steps the way they actually do them. Include the odd exceptions, like the customer who gets billed differently or the vendor who only takes checks.

Cross-train a backup

Written steps won't cover everything. Pick a second person for each critical task and have them do it with the expert watching, at least once or twice. That's usually when you find the steps nobody thought to write down.

Don't forget passwords and accounts. One of the most common problems we run into is that the only person who can log in to a critical system is the person who's gone. Register business accounts to a company email address, not a personal one, and keep logins in a password manager the business controls.

Check yourself, too

In a lot of small businesses, the person holding all the knowledge is the owner. If that's you, the same advice applies. Your business shouldn't stall because you're unreachable for a week.

Your best people are worth protecting. Making sure the business doesn't depend entirely on any one of them is a big part of that.

Some people also worry that documenting their job makes them easier to replace. Talk about that openly. The point is to keep the business running when they're out sick and to let them take a real vacation without checking email from the beach.

Tech Experts®
Information Technology Professionals

Empowering clients to do more with technology.
We support, manage, and optimize business IT.

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

Why Shared Logins Are a Security Risk for Your Business

"When someone leaves, their email account usually gets shut off. Nobody thinks about the shared password they've known for three years."

It happens in almost every office. One login for the accounting software, one for the shipping account, one for the company Facebook page. The password lives on a sticky note or in a shared spreadsheet, or it gets texted to whoever needs it next.

It feels efficient. Everyone can get in, nobody waits on IT, and there's only one password to remember. But shared logins create problems most businesses don't notice until something goes wrong.

You can't tell who did what

When five people use the same account, every action looks like it came from one person. If an invoice gets deleted, a setting gets changed, or a large order goes through by mistake, there's no way to know who did it.

That matters for honest mistakes. It matters even more if something dishonest happens.Without individual accounts, there's no record to follow.

Former employees may still have access

This is the problem we see most often. When someone leaves, their email account usually gets shut off. Nobody thinks about the shared password they've known for three years.

Changing it means tracking down everyone who uses it and updating every device where it's saved. So the password stays the same, and a former employee can still log in to your vendor portal, your bank, or your customer records.

Shared passwords are rarely strong

A password that a whole team needs to remember tends to be simple, and it often stays the same for years. It gets reused on other sites. Because it's written down and passed around, it ends up in more places than anyone realizes.

If a criminal gets that password through a phishing email (a fake message designed to trick someone into handing over login details) or a breach at another website, they get the same access as your entire team.

Extra login protection gets harder

Multifactor authentication adds a second step to logging in, usually a code sent to your phone. It's one of the best ways to stop someone from using a stolen password.

Shared accounts make it awkward. The code goes to one person's phone, so everyone else has to ask them for it. Many businesses end up turning it off on shared accounts, which removes protection from the accounts that need it most.

What to do instead

Start with a list of every shared login in your business: software, websites, vendor portals, banking, and social media.

For each one, check whether the service allows individual user accounts. Many do, often at no extra cost. Give each person their own login with only the access their job requires.

Where a shared account can't be avoided, keep the password in a business password manager instead of a spreadsheet or sticky note. You decide who can see each password, and you can remove someone's access in seconds when they leave.

And change shared passwords whenever someone with access leaves the company. Add it to your offboarding checklist so it doesn't get missed.

Shared logins save a few minutes, but they cost you the ability to know who can get into your business. A little cleanup now closes a gap most companies don't realize they have.

If you'd like help reviewing your shared accounts or setting up a password manager, give us a call at (734) 457-5000, or reach out at info@mytechexperts.com.



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).

How To Protect Your Business Social Media Accounts From Hackers



Who can log in to your company's Facebook page right now? What about Instagram, LinkedIn, or your Google business listing?

For a lot of businesses, the honest answer is "I'm not sure." Social media accounts pass through many hands over the years. The person who set up the page may have left in 2019 or the marketing agency you stopped working with may still have permission to post or run ads.

None of this seems urgent until someone else takes over the account. Then your page starts posting scams to your customers, your ad account runs up charges, and you're stuck trying to prove to the platform that the business is really yours.

Start with a list

You can't protect accounts you don't know about. Make a list of every company page, profile, channel, and advertising account. Include old ones you no longer use since abandoned accounts are easy targets and still carry your name.

For each account, write down:
• Who owns it
• Who has administrator access
• Which email address and phone number are used for recovery

That last item is easy to miss. Scheduling tools, review sites, and old marketing platforms often keep permission to publish long after anyone remembers connecting them.

Make sure the recovery email and phone number belong to the business, not to an individual. A business address you control is far easier to manage than a former employee's personal inbox.

Give everyone their own access

Most platforms let you add people to a business page using their own login. Use that feature instead of sharing one password around the office.

Give each person the lowest role that lets them do their job. Someone who writes posts doesn't need the ability to remove other administrators or change payment details. Keep full administrator access to a small group of trusted people, and make sure at least two of them work for your company.

Require multifactor authentication for everyone with access. It adds a second step to logging in, usually a code sent to a phone or an app, so a stolen password alone isn't enough to get in.

When an employee leaves or you stop working with an agency, remove their access that same day.

Protect the recovery email

This step gets overlooked more than any other. If someone breaks into the email account tied to your social media, they can often reset the password and take control without ever knowing your social media login.

Turn on multifactor authentication for that email account too, and give it a strong password that isn't used anywhere else.

Whoever controls that inbox can control every account connected to it.

Review access regularly

Access has a way of piling up again. Set a reminder to review your list every few months. Check who has access, remove anyone who no longer needs it, and disconnect apps nobody uses.

Have a plan before something goes wrong

If an account is hacked, the first few hours matter. Your team shouldn't be hunting for instructions while scammers post from your page.

Keep each platform's official account recovery instructions somewhere your team can find them quickly, along with your advertising account details and billing contacts.

Decide ahead of time who will contact the platform, who will warn customers, and who will call your bank if unexpected ad charges appear.

Social media is often the first place customers look for your business.

A little organization now makes it much harder for someone else to take it over.

"Give each person the lowest role that lets them do their job. Someone who writes posts doesn't need the ability to remove other administrators or change payment details."

What to Ask A Vendor After They Report a Data Breach

The email usually arrives without warning. Your payroll provider, accounting platform, or customer database company says it has had a "security incident" and they're looking into it.

The notice is often short on details. That's because many vendors send it before they've finished their own investigation. But you still have to decide what your business should do next, and you can't do that without better information.

These are the questions we'd ask, and why each one matters.

Is this notice real?

Start here. Criminals pay attention to breach announcements, and they often follow up with fake password-reset emails or "support" messages that look like they came from the vendor.

Don't click links in the notice. Go to the vendor's website or customer portal by typing in an address you already know, and check for the announcement there. If you need to call, use a phone number from your contract or an old invoice, not one from the email.

Was our business affected, and what information was involved?

A general announcement doesn't tell you whether your data was part of it. Ask directly. Then find out exactly what was exposed: employee Social Security numbers, bank account details, customer contact lists, invoices, or login information.

The answer shapes everything that follows. A leaked email list calls for a different response than leaked payroll records.

When did it start, and when did it stop?

Ask for three dates: when the unauthorized access began, when the vendor discovered it, and when they shut it down.

The gap between the first two can be weeks or months. Any unusual activity in your own accounts during that window deserves a closer look.

What could the intruder actually do?

Being able to view information is one thing. Being able to copy, change, or delete it is something else. Ask which of these the attacker could do. Changed bank details on a vendor record, for example, can lead to payments going to the wrong place.

Do any connections to our other systems need to be reset?

Most business software connects to other tools you use, like email, accounting, payment processing, file storage, or backups. Those connections run on digital keys that let one system talk to another. Some businesses also use single sign-on where one login opens several applications.

Ask whether any of these keys, connections, or sign-on links need to be reset or turned off. If an attacker got hold of them, they may be able to reach your other systems even after the vendor fixes its own problem.

How do you know nothing was taken?

Vendors often say there is "no evidence" that data was copied or misused. That can be true and still not mean much.

Ask what records support that statement, and whether those records cover the whole period of the breach. If the vendor only kept 30 days of activity logs and the intruder was inside for 90, "no evidence" really means "we can't tell."

What do you need us to do?

Get the vendor's instructions in writing. You may need to install an update, reset certain passwords, review recent transactions, disconnect an integration, or warn your employees about scam emails that use the breach as cover.

Written instructions help your team follow the steps correctly. They also give you a record if questions come up later.

Keep a paper trail

Save the original notice, every update that follows, the questions you asked, the answers you received, and notes on what your business did in response, with dates.

This record matters more than most people expect. Your insurance company may ask for it. So might customers, employees, or regulators.

Know when to get help

Depending on what information was involved and where your business operates, you may have legal obligations of your own, such as notifying customers or employees. Your IT provider, cyber insurance carrier, and attorney can help you figure out what applies.

You didn't cause the vendor's breach, but your business still has to respond to it. The sooner you get clear answers to these questions, the sooner you'll know what your business needs to do.

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

Copyright © 2026 Tech Experts® All Rights Reserved.

Tech Experts® and the Tech Experts logo are registered trademarks of Tech Support Inc.