September 2025

TechTidbit.com

brought to you by Tech Experts

Five Simple Ways To Keep Your Business Data Clean

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

Data is everywhere, and if you are not utilizing it to your advantage, you are missing out.

It is found in emails, customer profiles, inventory systems, or basically throughout your entire workflow. But relying on outdated or inaccurate information can lead to confusion, slow down your team, and ultimately cost you a lot of money.

With the right IT partner and these simple steps, you can keep everything clean and running smoothly.

Decide what info actually matters

Identify the key data that keeps your business running smoothly, like customer contacts, order details, or payment terms.

Then, create simple guidelines your team can easily follow. When everyone uses the same format, it keeps things organized without making it complicated.

Show your team the right way to do it

Most data errors occur when people aren't sure what's expected of them.

Rather than overwhelming your team with lengthy manuals, provide a simple, clear guide. How should names be formatted? What's the correct way to enter addresses?

A brief, straightforward session without jargon can make a big difference in maintaining consistency.

Use smart tools to prevent errors

Some mistakes can be caught the moment they happen. You just need the right tools. Use form validations so emails, dates, and numbers follow the right format. Then make certain fields required, like phone numbers or email addresses. If your CRM allows it, set up automatic checks for common errors.

Tidy things up often

Don't wait too long to clean up your data. A quick monthly review helps you spot duplicates, fix mistakes, and update old info before it creates bigger issues.

Keep your documentation updated

Things change fast with new systems, tools, and team members.

That's why it helps to keep a simple note on where your data comes from, who handles it, and how it should be used.

Don't wait too long to clean up your data. A quick monthly review helps you spot duplicates, fix mistakes, and update old info before it creates bigger issues.

Is Your Smart Office a Security Risk? What Small Businesses Need to Know About IoT

"Begin with all of your network's smart devices, such as cameras, speakers, printers, and thermostats. If you are not aware of a device, you cannot keep it safe."

Your office thermostat, conference room speaker, and smart badge reader are convenient, but they're also doors into your network. With more devices than ever in play, keeping track can be tough, and it only takes one weak link to put your entire system at risk.

That's why smart IT solutions matter now more than ever. A trusted IT partner can help you connect smart devices safely, keep data secure, and manage your whole setup without stress.

Here's some practical steps for small teams getting ready to work with connected tech.

Know what you've got

Begin with all of your network's smart devices, such as cameras, speakers, printers, and thermostats. If you are not aware of a device, you cannot keep it safe.

- Walk through the office and note each IoT device
- Record model names and who uses them

With a clear inventory, you'll have the visibility you need to stay in control during updates or when responding to issues.

Change default passwords immediately

Most smart devices come with weak, shared passwords. If you're still using the default password, you're inviting trouble.

- Change every password to something strong and unique
- Store passwords securely where your team can consistently access them

It takes just a minute, and it helps you avoid one of the most common rookie mistakes: weak passwords.

Segment your work

Let your smart printer talk, but don't let it talk to everything. Use network segmentation to give each IoT device space while keeping your main systems secure.

- Create separate Wi-Fi or VLAN sections for IoT gear
- Block IoT devices from accessing sensitive servers
- Use guest networks where possible

Segmented networks reduce risk and make monitoring easy.

Keep firmware and software updated

Security flaws are found all the time, and updates fix them. If your devices are out of date, you're wide open to cyberattacks.

- Check for updates monthly
- Automate updates when possible
- Replace devices that are no longer supported

Even older units can be secure if they keep receiving patches.

Monitor traffic and logs

Once your devices are in place, watch how they talk. Unexpected activity could signal trouble.

- Use basic network tools to track how often and where devices connect
- Set alerts for strange activity, like a badge reader suddenly reaching the Internet
- Review logs regularly for odd patterns

You don't need an army of security experts, just something as simple as frequent check-ins and awareness of odd behavior.

Set up a response plan

Incidents happen; devices can fail or malfunction. Without a plan, every problem turns into a major headache.

Your response plan should include who to contact when devices act weird and how you'll isolate a problematic devices.

A strong response plan lets you respond quickly and keep calm when things go wrong.

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).

Get to Know Your AI: Generative Vs. Agentic

If it feels like every week there's a new tech buzzword flying around, you're not imagining it. Between generative AI, agentic AI, large language models, and more, it's easy to feel like you need a decoder ring just to keep up.

Here's the good news: You don't need to understand every acronym. What really matters for small and mid-sized businesses in southeast Michigan comes down to two types of AI that are reshaping how work gets done:

- Generative AI
- Agentic AI

And no, they're not the same thing.

Generative AI: The "create-on-command" helper

You've probably already crossed paths with generative AI. Think ChatGPT writing emails, or tools that create images or summarize long reports. It's a great "assistant" when you need content quickly or want to save time on routine tasks.

But here's the catch: Generative AI waits for you. You have to ask, and then it delivers. It's helpful - but it won't tap you on the shoulder when it spots a problem.

Agentic AI: The "take-action" partner

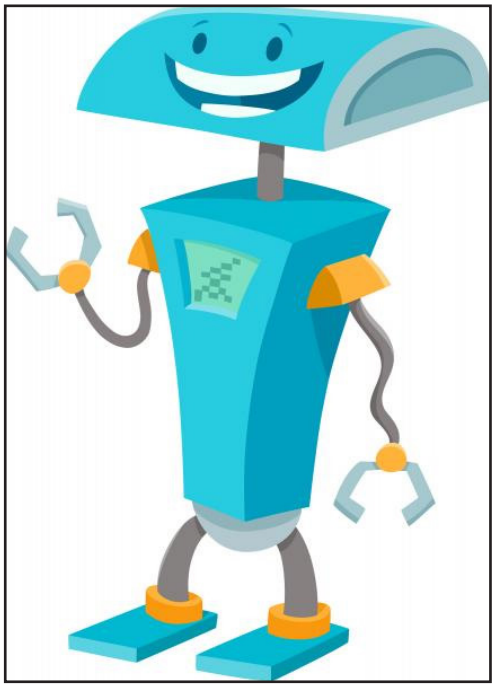
Agentic AI works differently. Instead of just reacting, it acts. You give it a goal, and it can figure out the steps to get there.

For example, imagine AI that helps reduce customer churn. It could analyze client data, test strategies, and even launch follow-up emails - without you needing to babysit it every step of the way.

Of course, with that autonomy comes responsibility. Agentic AI relies on accurate data and clear rules to make sure it's making the right choices. Without that structure, it can veer off track.

Why should you care?

Here's the thing: Both types of AI have real potential for businesses like yours.



Generative AI saves time. Drafting emails, creating documents, even building first drafts of policies - all faster.

Agentic AI saves brain space. It can take on repeatable tasks and keep things moving forward in the background.

But - and this is important - neither is a silver bullet. AI should be a tool, not a replacement for good strategy, human judgment, or proper IT oversight.

What this means for someone like you

If you've ever felt like technology is running your day instead of supporting it, AI can help lighten the load. But only if it's introduced thoughtfully with clear guardrails.

Picture this: Instead of scrambling when your CRM crashes or worrying whether backups are really working, you have smart systems in place that not only respond quickly but also prevent problems before they happen. That's the promise of blending traditional IT with the right AI support.

So, is it for you?

Maybe. The truth is, AI isn't a magic wand - it's more like a powerful new tool in the toolbox.

Whether it's worth using depends on your business goals, your data, and how much oversight you have.

That's where a trusted IT partner comes in. Someone local who knows the compliance pressures you're under and who can help you test the waters without risking your reputation.

Because at the end of the day, you don't need another buzzword. You need peace of mind that your technology is supporting your business - not adding to the chaos.

Curious how AI could actually boost productivity in your office? Let's talk. We'll cut through the jargon and help you decide what makes sense - no hype, no guesswork.

"But - and this is important - neither is a silver bullet. AI should be a tool, not a replacement for good strategy, human judgment, or proper IT oversight."

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

When That "Trusting Email" Might Be the Most Dangerous

You know how you'd trust an email that looks just like one from your bank - or maybe even from your own team?

That resemblance can lull us into thinking everything's okay... until a fraudulent link or message slips through. For small businesses, those moments can be costly.

Why it matters more than ever

Phishing isn't just "someone asking for passwords." It's evolved. Messages now tug at urgency, making it harder than ever to spot what's real. And once an email passes your "looks fine" test, that's often when trouble starts.

The new tricks

Today's phishing attacks are slicker than ever:

Polished, professional emails: Gone are the obvious typos and bad formatting. Many attacks now look identical to the real thing, sometimes even mimicking ongoing conversations.

Urgency tactics: Phrases like "act now" or "update immediately" push people into clicking before thinking.

AI-generated voice scams: Fraudsters can now clone voices, leaving phone messages or even "live" calls that sound eerily like someone you know.

These aren't just theoretical risks. Businesses across industries, from law firms to healthcare practices to financial offices, are seeing these attacks land in inboxes every day.

Five smart defenses

Here's how to build a stronger, people-first defense against phishing:

Refresh your team's training: Short, scenario-based sessions go a long way. Ask, "What would you do if?" and keep it conversational. The goal isn't to scare anyone, but to equip them.

Run a phishing drill: Sending a harmless test email can be a powerful teaching tool. When someone clicks, you have a chance to follow up with gentle coaching - not criticism.

Add technical checkpoints: Strong spam filters, authentication tools like DMARC, and multi-factor authentication all help reduce risk. Passwords alone aren't enough anymore - they're simply too easy to guess.

Create a clear response plan: If someone suspects a phishing attempt, they should know exactly who to tell. A quick, confident response is often the difference between "close call" and "serious breach."

Pause before you click: Encourage employees to take a breath when something feels off. Verifying a request with a quick phone call - or by starting a new email thread - takes seconds but can prevent a crisis.

Why this hits close to home

For small- and mid-sized businesses, phishing isn't just an inconvenience - it can lead to compliance headaches, financial losses, and damaged reputations. Local firms already face tight budgets, lean teams, and constant pressure to stay productive. A single wrong click can throw all of that into chaos.

That's why prevention matters so much. These aren't just IT issues - they're business continuity issues. Protecting against phishing keeps the doors open, the clients confident, and your team focused on their work instead of scrambling to clean up a mess.

The bigger picture

Cybercriminals thrive on the hope that small businesses will underestimate them. They count on teams being busy, distracted, or unsure of what to look for. By putting a few safeguards in place - both technical and human - you turn that vulnerability into strength.

At the end of the day, this isn't about technology for technology's sake. It's about giving yourself and your team the peace of mind that comes with knowing you're prepared. Because once your business culture shifts from "reacting after the fact" to "noticing before it happens," you've already won half the battle.