

AI Tools Are Everywhere

Are Your Employees Using Them Safely?

ChatGPT. Grammarly. Notion AI. Tools like these are becoming everyday staples in the workplace. From generating content and summarizing meetings to answering questions and writing code, AI tools promise a productivity boost—and employees are jumping in headfirst.

But there's a problem: Many are using these tools without any clear guidance. And that creates serious risks, especially for small businesses.

The Hidden Risk: Accidental Data Leaks

Unlike traditional software, AI tools often rely on cloud-based large language models (LLMs), which means whatever you type in can be stored and analyzed to improve the tool. That includes sensitive company data, customer information, internal documents, or proprietary code—sometimes unknowingly.

For example, an employee trying to save time might paste a draft client contract into ChatGPT for grammar help. It seems harmless. But if that contract includes private terms, pricing, or client names, it may violate confidentiality agreements—or worse, end up in training data used to generate responses for other users.

Why Small Businesses Are Especially at Risk

Large companies are already putting AI policies in place, blocking certain tools entirely or restricting how they're used. But small businesses often don't have internal policies or IT departments to review these tools—or the risks.

Employees at small companies tend to wear multiple hats and find creative ways to get work done faster. Without clear guidance, they may use AI tools for tasks involving sensitive data, unaware that they're crossing a line.

And unlike larger organizations, small businesses may not have the legal or financial safety net to absorb the fallout of a

Continued on pg. 2



July 2025

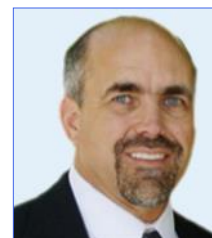
DOES TALKING TO IT SUPPORT LOOK SOMETHING LIKE THIS?



We can fix that.

Call To Find Out How
Book a FREE Discovery Call

505-792-2375



This monthly publication provided courtesy of David Luft, CEO of LDD Consulting, Inc.

Our Mission:

We promise to provide knowledgeable, courteous and prompt service. We care as much about your business as you do. If you are not completely satisfied, be sure to let us know. If we cannot resolve the issue, we will refund your money.

... continued from cover

data leak, reputational hit, or regulatory fine.

Real-World Consequences

In 2023, a global electronics company banned ChatGPT after employees reportedly pasted source code into the tool. In other cases, leaked prompts were found to contain proprietary strategy documents. For small businesses, the implications are just as serious.

Imagine an employee pastes confidential HR records into an AI

“Without clear guidance, employees may use AI tools for tasks involving sensitive data, unaware that they're crossing a line.”

tool to rewrite job descriptions. Or uses an AI-powered chatbot to troubleshoot an issue and includes internal system details. That data could be stored or accessed by third parties. If your client finds out, your business's credibility—and contract—could be at risk.

What Small Businesses Can Do

The good news? You don't have to block AI completely. But you do need a smart, simple framework for using it safely.

Here's where to start:

1. Set Clear Guidelines:

Create an AI usage policy that outlines what kinds of data can and cannot be shared with external AI tools. Make it clear that confidential or identifying information should never be input.

2. Educate Your Team:

Not everyone understands how AI tools work behind the scenes. Provide examples of risky behavior (e.g., pasting client emails, uploading financial reports) and explain why it matters.

3. Use Enterprise-Grade AI Tools Where Possible:

Some AI tools now offer business versions with stricter privacy settings and data handling agreements. These can provide a safer alternative to free consumer-grade versions.

4. Monitor for Unapproved Tool Use:

Talk to your IT provider about whether employee devices or networks are connecting to unauthorized AI platforms. Awareness is the first step in mitigation.

5. Revisit Your Security and Privacy Training:

Fold AI-specific examples into your regular cybersecurity training. Highlight how AI-related risks fit into your broader data protection strategy.

Final Thoughts

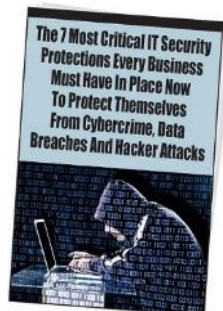
AI tools are here to stay—and used wisely, they can be a major advantage. But without guardrails, they open the door to data leaks, legal trouble, and lost trust.

Don't wait for a close call to act. Start the conversation now. A simple, clear policy could make all the difference between a productivity win and a privacy breach.

FREE REPORT:

7 Essential IT Security Protections to Safeguard Your Business from Cybercrime

Over **450,000 new malware threats** are detected every day, making businesses—and their bank accounts—prime targets. Worse yet, a data breach exposing client or patient information can lead to severe consequences: damaged reputations, hefty fines, civil lawsuits, and expensive litigation. By reading this report, you'll gain valuable insights to help safeguard your business and maintain the trust of your clients.



Call us at **505-792-2375** to Get Your **FREE** Copy Today

TECH TIP

LOCK YOUR
DEVICE WHEN YOU
STEP AWAY

Use Windows: Win + L

Use Mac: Ctrl + Cmd + Q

Lock it. Every time.





July often gets labeled the “slow season.” People are on vacation. Inboxes quiet down. Projects stall. It’s tempting to ease up and wait for things to pick back up in the fall.

But what if this season isn’t a lull—it’s an opening?

At LDD, we’ve learned that some of the most productive, strategic work happens when things feel a little quieter. Without the usual rush of back-to-back meetings or urgent requests, there’s finally space to think clearly, reset priorities, and strengthen the systems that carry your business forward.

In fact, summer can be the perfect time to:

- ⇒ Revisit annual goals and course-correct where needed
- ⇒ Tackle long-postponed tasks that keep falling off the list
- ⇒ Tighten up internal processes, documentation, or security gaps

Have deeper conversations about what’s working—and what’s not. It’s also a great time to reach out to clients, check in with your team, and prepare your technology for the demands of the fall season. While others are waiting for momentum to return, you can be quietly building it.

The businesses that stay strong over time don’t just react to the busy seasons—they use the quiet ones strategically. They invest in prevention, process, and planning. They don’t just wait for things to happen—they make things happen.

We’ve seen this mindset shift work firsthand. When clients use the summer months to strengthen their IT infrastructure or revisit their digital tools, they often enter Q4 more prepared, more efficient, and less reactive. A little work now can save a lot of stress later.

It’s easy to let July drift by. To push off decisions. To think, “We’ll get to it in September.” But when you reframe summer as a time to reset and realign, it becomes something else entirely: an advantage.

So if things feel slower than usual this month, that’s not necessarily a problem. It might be your best opportunity to regroup, refocus, and quietly move ahead—so when the busy season hits, you’re not scrambling. You’re ready.

Because summer isn’t just a season. It’s a mindset.

And momentum doesn’t come from waiting. It comes from using the time you have.

Client Spotlight

Personal Service is a Win for Us!

David and his team really took the time to understand our unique needs. We never felt pressured to buy anything that didn’t make sense for us. Instead, we were offered smart, tailored options that worked for our practice and budget. Their support is quick, reliable, and personal—no long holds or delays. Our staff appreciates how easy it is to get help when we need it, especially during our busiest times. That kind of responsiveness and attention to detail is hard to find. We truly value the relationship we’ve built with LDD.



Jolyn Williams
Manager
Home Dialysis of
Santa Fe

Quick Little Bytes



Google Search Just Got Smarter — Try This Trick

Google’s mobile app now includes an AI-powered “Ask” button. Tap it after a search result to get a quick summary of a long article—no need to scroll through pages of content. It pulls out key takeaways, saving time when you’re researching or troubleshooting on the go. Look for it on mobile under certain search results.

Keep Tabs on Your Data Breaches with This Free Tool

Not sure if your info has been exposed in a breach? Visit haveibeenpwned.com and enter your email address. It’s a fast, free way to find out if your accounts have been compromised—so you can change your passwords before someone else does. You can also sign up for alerts, so you’re notified if your email shows up in future breaches.



Making Technology Work for You
2420 Midtown PL NE, Suite K
Albuquerque, NM 87107

PRST STD
US POSTAGE
PAID
ABQ, NM
PERMIT 1187

Return Service
Requested

Inside This Issue

Are Your Employees Using AI Safely? | 1

Why Summer Might Be Your Secret Advantage | 3

«Name»
«Company Name»
«Street Address 1», «Street Address 2»
«City», «State» «Postal Code»

PROTECT YOUR TECH THIS STORM SEASON



Late summer and early fall often bring storms, power outages, and unexpected interruptions—and if you're not prepared, those can take a toll on your business tech.

Protect Your Equipment

Sudden power loss can damage servers, desktops, and networking gear. Make sure critical devices are plugged into surge protectors or, better yet, an uninterruptible power supply (UPS).

That gives you time to safely power down systems and avoid data corruption or hardware damage.

Check Your Backups

Power disruptions are a good reminder to double-check your backup setup. Are your backups running automatically? Are they stored in the cloud or offsite? When was the last time you tested a restore? Backups are only useful if they work—don't wait for an emergency to find out.

Remote Access Matters

If a storm keeps your team home for a day or two, can they still access the systems they need? Ensure secure remote access is in place and tested. A

little planning now can prevent major productivity losses later.

Watch for Power Fluctuations

It's not just outages that cause problems—brownouts and surges can silently damage electronics over time. Investing in quality power management for your office can save money (and headaches) in the long run.

Storm season can be unpredictable, but your IT setup doesn't have to be. With a few proactive steps, you can keep your systems protected—and your business up and running no matter what the weather brings.