TECHNOLOGY TIMES
NOVEMBER 2026
Insider Tips to Make Your Business Run Faster, Easier and More Profitably



The Hidden Side of AI:
Is Your Business Prepared?

Recently, at Seymour's monthly Chamber of Commerce meeting, there was a great deal of discussion about AI and the growing number of scams emerging. Representatives from Tennessee State Bank shared what they've been seeing, particularly among seniors, and it's a little scary just how sophisticated some of these schemes have become. We're seeing many of the same tactics being used in the business world.

AI is changing the way businesses work. It's also changing the way cybercriminals operate.

The same technology helping businesses improve productivity and security is making scams more convincing, phishing emails harder to detect and sensitive data easier to expose when it's used carelessly.

While businesses are using AI to boost security and productivity, cybercriminals are using the same technology to make attacks more convincing.

AI impersonation: Sounding right isn't enough anymore

Video and audio used to help distinguish someone real from someone trying to scam you. Now, AI lets cybercriminals create realistic voice messages, phone calls and videos that make their requests seem legitimate.

Even if you can spot telltale signs of AI-generated content today, those clues are disappearing quickly. Many of the warning signs people once relied on are already outdated. Instead of depending on employees to detect a fake, establish verification procedures for sensitive requests such as money transfers or account changes.

AI may be able to imitate a person's voice or appearance, but it can't bypass strong security procedures and multi-factor authentication.

AI-generated phishing: Harder to spot than ever

Phishing messages once contained spelling mistakes, grammatical errors and awkward wording that made them easier to recognize. Typos, generic greetings and urgent language became familiar warning signs.

Today, many phishing emails are well written, personalized and difficult to distinguish from legitimate communication. AI has made these scams more polished and convincing than ever before.

Rather than focusing only on how a message looks, pay attention to what it's asking you to do. Don't trust a message simply because it gets the details right.

Shadow AI: Think before you share sensitive data

When employees use AI tools that haven't been approved by the business, they may unintentionally expose sensitive company information to platforms that haven't been properly vetted.

An AI tool can't read every file in your organization on its own, but it won't stop someone from pasting confidential financial reports, customer information or internal business plans into a prompt and asking for help.

Before employees use any AI tool for work, your business should understand how it handles data, where that information is stored and whether it meets your security and compliance requirements.

A good IT partner doesn't tell you to avoid AI. They help you use it confidently by putting the right safeguards, policies and security controls in place, so your business can embrace new technology without creating unnecessary risk.

CD TECHNOLOGY

Pumpkin Pie
(FromFreshPumpkin)





Ingredients

1 sugar pumpkin
9 inch single crust pie
2 eggs
1 cup packed light brown sugar
1 tablespoon all-purpose flour
1/2 teaspoon salt
2 1/2 teaspoons pumpkin pie spice
12 oz can evaporated milk

Directions

- Cut pumpkin in half and remove seeds. Place cut side down on a lined cookie sheet. Bake at 325˚F for 30 to 40 minutes, or until the flesh is tender.
- Scoop out and puree.
- Increase oven temperature to 450˚F
- Slightly beat eggs. Add brown sugar, flour, salt, 2 cups of the pumpkin puree, pumpkin pie spice, and evaporated milk. Stir well after each addition.
- Pour into the unbaked pastry shell. Protect the crust to prevent over browning.
- Bake 10 minutes at 450˚F, then reduce to 350˚F. Bake an additional 40 to 50 minutes, or until a toothpick inserted near the center comes out clean and crust is golden.
- Cool pie - refrigirate - best served cold

This is our favorite pumpkin pie recipe. In fact Thomas didn't like and wouldn't eat pumpkin pie befor this one. It makes a pie that is so super light and fluffy– not thick and pasty like pies made with can pumpkin. I think it is the perfect sweetness but if you want a sweeter pie, you can add a little more brown sugar or some regular sugar to taste.



CD Technology Connects with Tennessee's Trucking Industry

Thomas and Rebekah Hill recently represented CD Technology at the 2026 Tennessee Trucking Association Annual Convention, where they were honored to participate as an exhibitor.

The convention provided a great opportunity to connect with trucking and transportation professionals from across Tennessee, strengthen existing relationships, and make plenty of new connections. They enjoyed sharing how CD Technology helps businesses reduce downtime, increase productivity, and ensure compliance through reliable IT support and cybersecurity.

Congratulations to the Tennessee Trucking Association's new leadership team and to all of this year's award recipients. Your leadership and dedication continue to move Tennessee's trucking industry forward.

A special congratulations also goes to the Tennessee Trucking Foundation on the tremendous support generated through the convention auction. It was exciting to see the trucking community come together to raise funds for the Foundation and its important work.

Thank you to the Tennessee Trucking Association for a fantastic convention. CD Technology was proud to be part of it, and we look forward to continuing the connections we made!



Your Cybersecurity Needs an Immune System, Not a Medicine Cabinet



Most medicine cabinets tell a story. There's cold medicine left over from last winter, vitamins bought in bulk, half-used bottles of cough syrup and a prescription that should probably have been thrown out months ago.

Cybersecurity can end up looking much the same. A new threat prompts one purchase, an insurance requirement leads to another and a vendor recommendation adds something else. Over time, the more useful question becomes whether your business has the right protections in place and if they're doing what they need to do.

Cyber myth: More tools mean better cybersecurity

It's an easy assumption to make. If one security product adds protection, then adding more should make your business even safer. But that's where the myth starts to break down.

Multiple layers of protection can be valuable, but only when each one serves a clear purpose. Adding another product may address a specific concern, but it can also create unnecessary overlap or additional complexity if no one considers how everything fits together.

What matters is whether the right safeguards are in place, properly managed and working together to address the risks your business faces.

Healthy cybersecurity works like a system

Your immune system isn't a shelf of individual remedies. It's a coordinated system designed to recognize problems and respond to them.

Your company's cybersecurity should work the same way, but for many businesses, the pieces don't always come together that neatly.

Tools get purchased to solve specific problems. Employees receive policies and training. New safeguards are added as risks change or requirements evolve. Each decision may make sense on its own, but over time, those individual pieces can become disconnected from the bigger picture.

That's where coordination matters. The right safeguards should complement each other rather than simply coexist.

Security tools are part of that system, but they're most effective when they work as part of a broader approach that still fits the business's needs.

Give your security a check-up

You don't need to understand the technical details of every cybersecurity product your company uses. But you should be able to get clear answers to a few basic questions.

1. What are we currently using, and why?

Someone on your team or a trusted outside partner should be able to explain what your major security protections do and why they're there. If nobody can give you a clear answer, that's worth looking into.

2. Where do our protections overlap, and where are the gaps?

Overlap isn't automatically a problem. Sometimes layered protection is intentional. What matters is knowing whether your security approach was designed that way or simply grew over time without much coordination.

3. Who is making sure everything is working?

A tool can generate alerts around the clock, but that doesn't help much if nobody is reviewing them or knows what should happen next. The important thing is knowing that someone is responsible for the outcome and paying attention.

4. When did we last reevaluate what we need?

Businesses change. People join and leave, new applications get adopted and teams start working in different ways. Cybersecurity that made sense when it was first implemented may no longer fit the business as it exists today.

Cybersecurity Myth Busters:

6 Things Small Businesses Still Get Wrong



Cybersecurity advice is everywhere, but not all of it is accurate. It's worth taking a step back every so often to separate what you know from what you only think you know.

Some have circulated for so long that it's taken on a life of its own, repeated until it sounds like fact even when it's outdated or wrong.

When bad advice goes unchallenged, it creates blind spots. And blind spots are exactly what cybercriminals look for.

The good news is these gaps are simple to close once you know where they are. Here are six myths we hear regularly from small business owners, along with the truth behind each one.

Myth 1: We're too small for cybercriminals to care about

There is no such thing as a business too small for an opportunistic cybercriminal. It doesn't matter if you're a one-person operation, a small business with a dozen employees or a large corporation. If you have exposed accounts or vulnerable systems, bad actors will take advantage of it. A small business offers valuable data, access to bank accounts or entry points to customers and vendors.

Fact: Hackers choose targets based on opportunity, not size.

Myth 2: Employees will recognize a phishing email

Some myths have circulated for so long that they've taken on lives of their own, repeated until they sound like fact even when they're outdated or wrong.

Thanks to AI, it's become harder to catch a scam email from the text alone. Instead, your team needs to think about sender behavior. For example, ask yourself if the supposed sender would:

- Make an unusual request
- Change payment instructions
- Request sensitive information
- Send a new or unusual login link

If anything seems off, double-check before clicking or responding.

Fact: A convincing email can still be a scam.

Myth 3: MFA fully protects our accounts

Multi-factor authentication (MFA) is important, but it's not invulnerable. Hackers use MFA fatigue to their advantage, counting on employees approving requests out of habit. For example, "prompt bombing" floods your phone with requests in hopes you'll approve access just to get them to stop.

continued on page 5 ...

SHINY NEW GADGET OF THE MONTH

A Webcam That Keeps You in the Frame

OBSBOT Tiny 3 is built for people who move when they present. Its motorized camera tracks the speaker and keeps them in frame during calls, presentations and training sessions. So you can move around the room or step up to a whiteboard without stopping to readjust the camera. It supports 4K video, voice and gesture controls, and dedicated desk and whiteboard modes for more flexible hybrid meetings.



What's in your IT budget?



Not Every Power Strip Is A Surge Protector

Check the label to make sure the device specifically offers surge protection and look for a UL 1449 listing.

A few other tips can help keep your home or office safer:

• **Replace old surge protectors**. Their protective components wear down over time, especially after significant surges.

• **Never "daisy chain" power strips** by plugging one into another.

• **Don't overload them.** High-wattage appliances and space heaters should generally be plugged directly into an appropriate wall outlet.



• **Inspect regularly.** Replace any unit with scorch marks, damaged cords, loose plugs or signs of overheating.

• **Consider whole-building protection.** A whole-home or commercial surge protective device can provide another layer of defense against larger electrical surges.

Remember: a power strip gives you more outlets. A surge protector helps protect what's plugged into them.



CARTOON OF THE MONTH



"Do you still have regular coffee?"

... continued from page 4

Keep in mind, MFA is a tool, not a shield. Hackers are finding ways to get around weaker authentication methods, which is why MFA needs support from the controls around it.

Fact: MFA should be part of a broader security strategy.

Myth 4: Our backups have us covered

Ask yourself: If your business was hit with a ransomware attack tomorrow, could you restore your data? How long would it take?

A backup is great when you know it's going to work. However, an untested backup isn't something you can rely on during an incident. Knowing how long your business will be down can save you time and money.

Fact: Having backups is not the same as being able to recover.

Myth 5: Cybersecurity is only IT's responsibility

Your IT department does a lot to keep your business safe, but they can't control every click employees make. Cybersecurity decisions happen across every department. It takes only one bad click to open your systems to threats.

Employee security awareness training matters. When everyone knows what to look for and when to ask for help, they become part of your cybersecurity defenses.

Fact: Training employees to make good decisions strengthens your cybersecurity.

Myth 6: We know what to do if something happens

It's Tuesday morning. Several employees suddenly can't access their files. Many teams discover in that moment that nobody has answered the basic questions:

- Should employees shut down their computers?
- Who calls IT?
- What do you do if communication systems are down?
- When does the insurance company get involved?
- Who communicates with customers?

Don't rely on memory in the moment. Have an incident response plan.

Fact: Your recovery plan shouldn't debut during an incident.

Cybersecurity awareness starts with the facts

Strong cybersecurity starts with the facts. Many security gaps come from assumptions that go unchallenged.

If any of these myths sound familiar, it may be time to reassess your cybersecurity strategy. The businesses that stay ahead work with a trusted IT partner to identify gaps, strengthen their defenses and stay ahead of evolving threats.

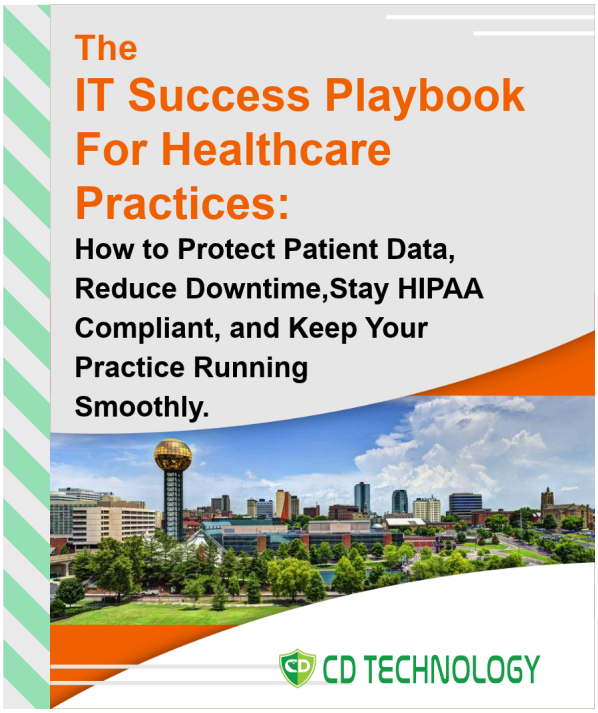
FREE REPORT

What Every Small Business Owner Should Know Before Hiring an IT Provider

Two IT providers can look similar on paper and deliver very different levels of support. Our free IT Buyer's Guide shows you what good IT support should include, where extra costs and gaps can hide and the questions to ask before you sign or renew.

You don't need to be an IT expert.
You just need to know what to look for.

Download your FREE copy today at: www.CDTechnology.com/ITBuyersGuide/ or call our office at (865) 909-7606.





Know What Needs To Come First

If your roof is leaking and your kitchen is showing its age, both may need work. But only one of them is going to ruin your week. Your IT budget can put you in the same position. There may be plenty worth spending money on, but deciding what comes first isn't always obvious.

The real work of IT budgeting is deciding what deserves attention now, what you should prepare for next and what can reasonably wait.

Some expenses address problems that could disrupt the business or become more costly over time. Others prepare you for changes you already know are coming. And some can stay on the list for another quarter without creating a bigger problem.

The roof and the kitchen may both need attention. The difference is knowing which one can wait.

You shouldn't have to treat every IT expense like an emergency.
We can help you review what's on your list, understand the business impact and prioritize your spending, including telling you what can wait.