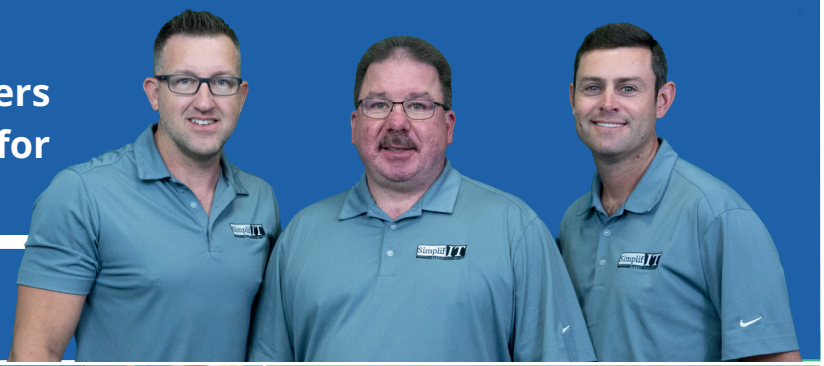
The SimplifIT Advantage

Proven strategies to help leaders make clear technology decisions for measureable business results.



Business leaders depend on technology. SimplifIT allows you to focus on growing your business with secure and compliant IT solutions that are proven to work & keep you safe.

- Craig Willard, COO
- Eric Elder, CTO
- Nick Landers, CMO

SimplifIT
MANAGED IT | CYBERSECURITY

A Message From Our Team

This month, we want to cover something we are seeing and hearing across the region with increasing frequency: scams that are getting smarter, more personal, and more damaging for business leaders.

It used to be easy to spot a fraud attempt. Today, it is not. Attackers are using AI to generate convincing images, impersonate trusted contacts, and craft messages that look and sound exactly like the real thing. We have seen it affect community members, business owners, and organizations that had no reason to expect it.

The good news is that awareness is still one of the most powerful defenses available, and that is exactly what this issue is designed to build.

We are also addressing a question we hear often from business leaders: what should good IT actually look and feel like? Not in a technical sense, but in a day-to-day, practical, business sense. If you have ever wondered whether you are getting what you should from your technology investment, this issue gives you a clear framework to find out.

This month covers the threat landscape, what proactive IT and cybersecurity really means for a small business, and a simple self-assessment you can use right now.

We hope it is useful. As always, we are here when you need us.

All the best!

The Team at SimplifIT

Inside This Issue

Cybercriminals Are Targeting Your Industry Right Now. Here's What to Know.

Cybercriminals aren't casting wide nets anymore. They're researching specific industries, specific roles, and specific moments. Here's what's happening and what you can do about it.

There's a shift happening in how small businesses get targeted, and most owners don't see it until they're already dealing with the fallout.

For years, the common image of a cyberattack was something obviously suspicious: a strange email with broken English, a phone call with an obvious script, or a ransomware screen that appeared out of nowhere. Those still exist. But the attacks causing the most damage right now look nothing like that.

Today's scams are researched. They're patient. They use real names, real relationships, and real context to manufacture urgency, and they target industries where a fast-moving workflow makes the difference between catching it and missing it entirely.

What's Changed and Why It Matters Now

The tools attackers use have gotten dramatically better. AI can now generate convincing emails, realistic images, and believable impersonations in minutes. A bad actor no longer needs technical sophistication. They just need access to publicly available information: a LinkedIn profile, a Facebook page, a company website, and enough patience to build a convincing story.

A situation in our community recently illustrated this well. A bad actor took over someone's social media account, used real photos from the profile to generate an AI image depicting a fake family emergency, and posted it as if it came directly from the account owner. Friends and family who had every reason to trust what they were seeing sent money within hours. The real account owner lost money, dealt with reputational damage, and spent weeks untangling the fallout.

The same playbook runs inside businesses every day: impersonation, urgency, and exploiting trusted relationships. The context changes. The outcome doesn't.

The Five Industries Getting Hit Hardest

According to the FBI's 2024 Internet Crime Complaint Center report and Verizon's 2024 Data Breach Investigations Report, these industries consistently rank at the top for cyber incidents.

Healthcare logged the highest number of reported incidents among all critical infrastructure sectors in 2024, with 444 incidents and 238 ransomware attacks. IBM puts the average cost of a healthcare breach at $9.77 million, the highest of any industry for 14 consecutive years. Sensitive records, fast-moving workflows, and regulatory pressure make it a perennial target.

Manufacturing reported more ransomware incidents than any other critical infrastructure sector, 258 in 2024 alone. When production stops, the pressure to pay and restore operations is immediate. Any business that depends on consistent workflow or vendor relationships faces a version of this same vulnerability.

Financial Services firms face an average breach cost of $6.08 million, and business email compromise accounted for $2.77 billion in reported losses to the FBI in 2024. This isn't limited to banks. Any business that sends payments, manages payroll, or handles client funds is operating in the same threat environment.

Professional, Scientific, and Technical Services including accounting firms, legal practices, and consultants, saw 2,599 incidents and 1,314 confirmed breaches in 2024 according to Verizon. These businesses hold sensitive client data, manage financial transactions, and communicate regularly with people who have strong reasons to trust them. That combination is exactly what attackers look for.

Retail faced 725 incidents and 369 confirmed breaches in 2024, with 99% driven by financial motivation. Credential theft, payment data, and social engineering attacks targeting employees are the primary vectors.

What This Means If You're Not in One of These Industries

The industries above make headlines because of their size and incident volume. But the tactics used against them are not industry-specific. Vendor impersonation, fraudulent payment instructions, credential theft, and urgency-based deception work just as well against a five-person service firm as they do against a large hospital system. If your business sends payments, manages client information, or relies on vendor relationships, you are operating in the same risk environment.

What to Do About It

None of this requires an expensive overhaul. It requires a few deliberate habits applied consistently.

Build a verification step into any financial request. Any instruction to update banking information or redirect a payment should require a phone call to a number you already have on file, not a reply to the message making the request. This single habit stops a significant percentage of invoice and wire fraud.

Separate personal and business accounts. If your business systems can be accessed through personal logins, a personal compromise becomes a business problem immediately.

Train your team on current tactics. Your team needs to know what fraud actually looks like right now, with real examples and a clear process for flagging something before acting on it.

The Bottom Line

Scams targeting small businesses aren't random. They're researched, timed, and increasingly realistic. The businesses that stay ahead aren't doing anything complicated. They're building simple, consistent habits that make them harder to compromise than the next target.

Need Help With Your AI Strategy?

Organizations need **an approved, secure path** to use AI safely so they get speed and efficiency without creating risk. You don’t have to ban it, but do need to secure it.

Would you like to strategize about AI for your organization? Join us for our regular AI Strategy Workshops held at our office. Contact us at 502.783.6630 or email Nick@WeSimplifIT.com for an invitation.

Cyber Stars: Kelley Hawkins and Kristi Buffenmeyer
Everyday Matters | Owner and Executive Director

Every once in a while, you get to partner with leaders whose values don't just shape what they build — they shape how they protect it. That's Kelley Hawkins and Kristi Buffenmeyer at Everyday Matters. Kelley is the Owner and founder. Kristi is the Executive Director. Together, they lead an organization serving individuals with disabilities across Kentucky — providing residential housing, day training, personal assistance, and vocational skill development. When the people in your care depend on you at that level, the stakes of getting technology wrong aren't abstract. They're personal.

Kelley brings executive-level clarity to technology and security decisions. She stays close, asks the right questions, and holds the organization accountable because she knows what's actually at risk. That ownership at the top sets the tone for everything else. Kristi carries that standard into day-to-day operations, ensuring the organization runs efficiently and securely in a way that reflects the mission — the kind of leader who makes the right policies stick because her team understands why they matter.

What stands out most is how far ahead both of them think. They embrace technology when it helps their team serve more people, more effectively — and they do it thoughtfully, with safety at the center. They model what great leadership looks like: committed to their people, serious about security, and willing to innovate to get there. We are honored to partner with them and the entire Everyday Matters team.

About Everyday Matters: Everyday Matters, LLC provides residential housing, day training, personal assistance, and vocational skill development for individuals with disabilities across Kentucky. Their mission: Providing Support. Empowering Lives. Building Futures.

Back to Basics: The Cybersecurity Fundamentals That Never Fail

Most businesses don't have a clear baseline for what their IT and cybersecurity strategy should deliver. Without one, it's hard to know whether what you have is working.

There's a question worth sitting with as a business leader: What should good IT actually look and feel like?

Not technically, but in a business sense. What should your day-to-day experience be? What should your invoices reflect? What should happen when something breaks, and what should be happening when nothing is?

If those questions don't have clear answers, you may not have a strong baseline to evaluate your current approach. And without a baseline, it's difficult to know whether your IT and cybersecurity investment is genuinely serving your business or quietly costing you more than it should in time, disruption, and unmanaged risk.

Here's a framework for thinking through each area.

IT Should Be Simple to Work With

The first thing a well-functioning IT strategy gets right isn't technical. It's operational.

A business should have a single, clear point of contact for everything IT-related. One number. One relationship. One place where accountability lives. If your team regularly gets directed to contact vendors independently, or navigates support without consistent follow-through, that's worth examining. A well-structured IT engagement simplifies your operations. It doesn't add to them.

Onboarding a new employee should be smooth and documented. Support requests should be accessible without requiring technical fluency on your end. A useful self-assessment: think about the last time your team needed IT help. How easy was that experience? Would you describe it as effortless, or as something you had to manage yourself?

Security Should Be Ongoing, Not a Checkbox

Cybersecurity isn't something that gets configured once and quietly runs in the background. An effective strategy continuously evolves as threats change and comes with clear visibility into what's being done and why.

Some useful questions when evaluating your current security posture: How are defenses updated as new threats emerge? What does your incident response process look like if something goes wrong tomorrow, not in principle, but step by step? Which security tools are included in your current setup, and which are add-ons?

If those answers aren't clear or documented, that's a productive starting point for further evaluation, whether internally or with whoever manages your security today.

Pricing Should Be Predictable

IT costs should be straightforward to plan around. A well-structured arrangement means a fixed monthly investment with documented processes for changes such as new users, licensing adjustments, and scope additions, rather than surprises that show up on invoices after the fact.

If your current IT costs feel unpredictable or difficult to audit, it's worth reviewing the structure of your agreement. Clarity in pricing is usually a reflection of clarity in the service itself.

Response Time Should Be Measurable, Not Just a Promise

Response time is one of the most commonly cited pain points in IT, and one of the easiest to evaluate with the right information. The relevant questions go beyond "how fast do you respond?" to include: Who responds, and when? How are different types of issues prioritized? What does after-hours support actually look like?

Strong IT support can answer these questions with documented processes and real data. If your current experience doesn't match what was promised, that gap is worth understanding and addressing.

Your IT Strategy Should Be Forward-Looking

One of the clearest signs of a well-functioning IT strategy is that it includes planning, not just maintenance. That means regular conversations about hardware lifecycles before they become emergencies, visibility into compliance requirements before they become liabilities, and guidance on emerging tools like AI before employees start using unapproved solutions on their own.

Ask yourself: when was the last time your IT strategy prompted a proactive recommendation rather than a reactive fix? If the answer is hard to come by, it may be worth revisiting whether your current approach is built to support that kind of forward-looking thinking.

The Standard Is Higher Than You Might Think

Many businesses settle into an IT experience that mostly works and mostly stays out of the way. The gap between "mostly fine" and genuinely well-served is where a lot of invisible cost accumulates: downtime, unmanaged risk, and a team that has learned to work around their technology rather than with it. This framework is a starting point for identifying where those gaps might exist.

Strategic Planning Session: Let's Plan Your 2026 IT Strategy Together

Here's what we know: the businesses that win this year won't be the ones reacting to problems. They'll be the ones planning ahead. That's why we offer Strategic IT Planning Sessions.

What We'll Cover:

Security gaps that need attention before they become incidents Hardware and software that's due for replacement or upgrade AI opportunities that could save your team time and money Compliance requirements (CMMC, cyber insurance, industry standards) Growth plans and how your IT needs to scale with you ROI Analysis—direct, measurable impact on your bottom line

Scan The QR Code To Schedule Your Session Today

Simplif IT
MANAGED IT | CYBERSECURITY

102 Enterprise Drive
Suite A
Frankfort, KY 40601

502.783.6630

WeSimplifIT.com

Proactive vs. Reactive: What the Difference Actually Looks Like

Everyone says they do proactive IT. Here's how to tell the difference in approaches in about 60 seconds.

Reactive Approach:

You find out something is wrong when something stops working. Your team loses hours waiting for systems to come back online. Hardware fails without warning because no one was tracking its age. A software license expires and takes down a workflow. The problems weren't unpredictable. They just weren't being watched.

Proactive Approach:

Problems get caught and resolved before you feel them. Systems are monitored, patched, and maintained on a schedule. You're never surprised by end-of-life hardware or an expired license. IT gets simpler over time because someone is managing the details before they become your problem.

Reactive Cybersecurity:

Security reviews happen after something goes wrong. The first sign of a vulnerability is the breach itself, and by then you're managing notification requirements, potential data loss, and the trust damage that comes with it. A response plan gets written in the middle of a crisis, when it's hardest to think clearly.

Proactive Cybersecurity:

Your defenses evolve as threats do. Suspicious behavior gets flagged before it becomes an incident. A documented response plan exists before you need it, and your team has practiced it.

Reactive AI Strategy:

Employees are already using AI tools you haven't approved, feeding in data you haven't reviewed, and making decisions based on output no one has validated.

Proactive AI Strategy:

Your team has an approved, secure path to use AI tools, with clear rules about what data stays off limits. AI is saving real time in real workflows. Leadership knows what's being used and why.

A proactive approach to IT, security and AI saves businesses budget and helps leaders accomplish more.

Could a Scammer Get Into Your Business? A Quick Self-Assessment

Scammers don't need to be sophisticated. They need one open door. This checklist helps you find yours before someone else does.

Use it as a starting point, not a final verdict. Every unchecked box is a conversation worth having.

Phishing and Email Security

□ Your team can recognize a convincing phishing email, not just an obvious one

□ Suspicious emails have a clear reporting process so nothing gets ignored

Most successful attacks start with email. The goal isn't to scare your team. It's to make "pause and verify" a reflex, not an afterthought.

Credential and Account Security

□ No one on your team reuses passwords across personal and business accounts

□ Multi-factor authentication is active on email, banking, payroll, and remote access

□ Business systems are not managed through personal logins

Credential reuse is one of the most common and most preventable vulnerabilities in small businesses. One compromised personal account can become a business problem within hours.

Financial and Vendor Security

□ Any request to update vendor banking details triggers a phone verification before processing

□ Wire transfers and payment approvals require a second confirmation step

Team Readiness

□ Your team has seen real, current examples of how scams actually look, not just an annual reminder

Training isn't a one-time event. Current tactics require current awareness, especially as AI makes impersonation more convincing than ever.

Do you know another business we can serve? Ask us about our referral program.