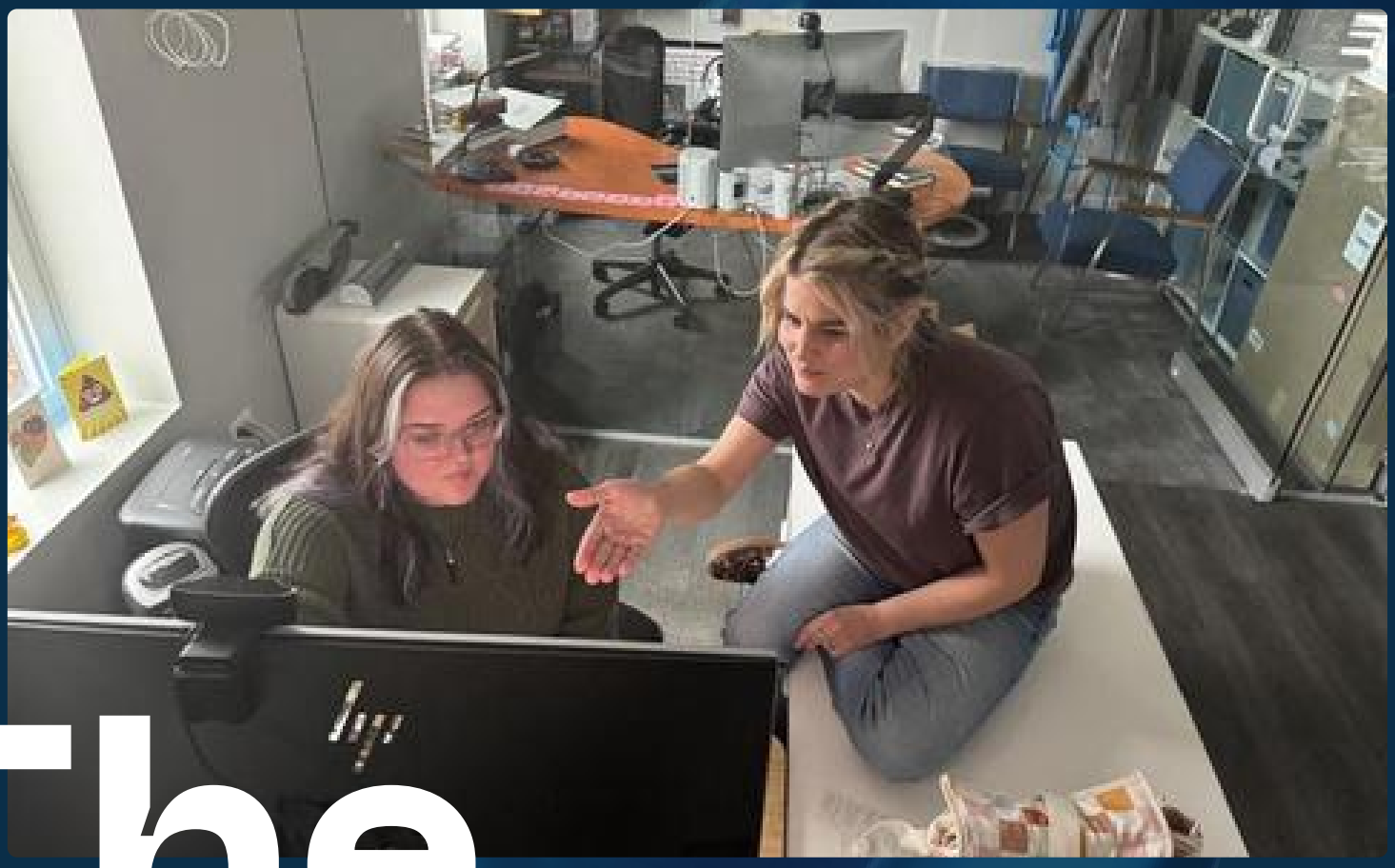
LeadingIT

May 2025



The NetWork

- 7 ALARMING SIGNS YOUR BUSINESS IS A TARGET FOR CYBERCRIME
- KEYBOARD SHORTCUTS THAT'LL MAKE YOU LOOK LIKE AN OFFICE WIZARD
- WHAT TO DO WHEN YOUR WI-FI ACTS UP: A SIMPLE TROUBLESHOOTING GUIDE FOR NON-TECHIES
- WHAT AN IT AUDIT REALLY TELLS YOU (AND WHY YOU SHOULDN'T SKIP IT)

7 Alarming Signs Your Business Is a Target for Cybercrime

Cybercrime is not a matter of "if" but "when" for many businesses. While large corporations dominate headlines, small and medium-sized enterprises (SMEs) are also attractive targets, with valuable data but fewer resources to defend themselves.

Here are seven alarming indicators that your business might be in the crosshairs of cybercriminals:

1**. Increased Phishing Attempts Targeting Employees:**
A spike in sophisticated phishing attacks is a major red flag. Cybercriminals use personal data to steal credentials, install malware, or trick employees into transferring funds. Pretexting attacks—where attackers invent convincing scenarios to steal sensitive information—have doubled in recent years.

When attacks spike, it's time to raise your defenses. Tighten up your email filters, remind employees to think twice before clicking, and run targeted awareness training.

2. Unusual Network Activity and Performance Issues: Keep a close eye on your network's behavior. Unexplained spikes in internet traffic, slow system performance, frequent crashes, or unauthorized access attempts to files or databases can indicate a breach or ongoing malicious activity. Cybercriminals often explore systems before launching attacks, leaving clues like these.

Regularly monitor network logs and consider investing in intrusion detection tools. Containing a breach in under 30 days can save over $1 million in damages.

3. Compromised Employee Accounts or Unauthorized Logins:
If employees report suspicious activity on their accounts, such as sent emails they didn't write or changes to their settings, it's a serious warning sign. Similarly, repeated failed login attempts from unknown locations or successful logins from unfamiliar devices should trigger an immediate investigation.

Stolen credentials give cybercriminals a direct route into your systems. Enforce multi-factor authentication (MFA) wherever possible, and stay vigilant for signs of unauthorized access

4. Data Breaches or Leaks in Related Industries or Competitors:

Cybercriminals often target specific industries or businesses with similar profiles. If your competitors or businesses in your sector have recently experienced data breaches, it significantly increases your risk. Attackers reuse tactics and exploit familiar vulnerabilities.

Stay informed about industry-specific threats and update your defenses accordingly. What happens to your peers today could happen to you tomorrow.

CONTINUE READING

5. Weak or Outdated Security Infrastructure:

Neglecting security updates, using outdated software, or lacking essential security tools like firewalls, antivirus software, and intrusion prevention systems makes your business an easy target. Hackers actively scan for known vulnerabilities, especially in unpatched systems.

In 2019, 60% of data breaches stemmed from vulnerabilities that had patches available but were never implemented. Stay on top of updates, run regular security audits, and ensure you have firewalls, antivirus software, and intrusion prevention tools in place.

6. Social Engineering Attempts Beyond Phishing:

Cybercriminals are becoming increasingly creative with their social engineering tactics. Be wary of fake IT support calls, suspicious probing, or physical attempts to breach your office.

Ongoing employee training and clear protocols for handling suspicious situations are key to staying one step ahead.

7. Publicly Available Sensitive Information:

If sensitive business information, such as customer lists, financial details, or internal documents, is inadvertently exposed online through misconfigured cloud storage, unsecured websites, or employee negligence, it paints a target on your back. Cybercriminals are always on the lookout for these easy opportunities.

Regularly audit your online footprint and enforce strict data-handling policies to avoid unintentionally putting your business at risk.

Conclusion: Stay Ahead of the Threat

Ignoring these warning signs can lead to severe consequences: financial losses, reputational harm, legal trouble, and major business disruption. However, being proactive makes a big difference.

With regular monitoring, employee training, strong security measures, and a clear incident response plan, you can build a robust defense against the growing threat of cybercrime. Recognizing the red flags is the first step toward keeping your business secure.

Keyboard Shortcuts That'll Make You Look Like an Office Wizard

Here's a roundup of essential keyboard shortcuts to help you save time, streamline your tasks, and navigate your computer like a pro. Not only will they help you work more efficiently, but they'll also make you look like an office wizard who knows all the tricks!

✂ Copy, Cut, and Paste

Ctrl + C / Command + C **Copy**
Ctrl + X / Command + X **Cut**
Ctrl + V / Command + V **Paste**

Select All

Ctrl + A / Command + A **Select All**

Switching Between Open Applications

Alt + Tab / Command + Tab

Minimize, Maximize, and Close Windows

Windows Key + Down Arrow: **Minimize**
Windows Key + Up Arrow: **Maximize**
Alt + F4 / Command + Q **Close the current window**

⬅ Undo and Redo

Ctrl + Z / Command + Z **Undo**
Ctrl + Y / Command + Shift + Z **Redo**

B Formatting Shortcuts

Ctrl + B / Command + B: **Bold**
Ctrl + I / Command + I: **Italic**
Ctrl + U / Command + U: **Underline**

Open File Explorer/Finder

Windows Key + E: **Open File Explorer**
Command + Space: **Open Spotlight search (and then type Finder)**

Take a Screenshot

Windows Key + Shift + S: **Capture a screenshot (and select the area to capture)**

Command + Shift + 4: **Capture a selected area of the screen**

Browser Shortcuts

Ctrl + T / Command + T: **Open a new tab**
Ctrl + W /Command + W: **Close the current tab**
Ctrl + Shift + T / Command + Shift + T: **Reopen the last closed tab**
Ctrl + L / Command + L: **Jump to the address bar**

Conclusion: Become a Productivity Wizard
Keyboard shortcuts are essential tools for boosting productivity and efficiency. Mastering these shortcuts will make you an office wizard and save you valuable time in your daily tasks.

What to Do When Your Wi-Fi Acts Up: A Simple Troubleshooting Guide for Non-Techies

Let's be honest — nothing tanks a productive day faster than Wi-Fi issues. You're on a Zoom call. You're uploading a file. You're in the middle of something important... and then your internet freezes. Again.

If this sounds familiar, don't worry — you're not alone. Wi-Fi troubles are one of the most common reasons businesses call for IT support, and the good news is that most of the time, the fix is easier than you think.

Whether you work in the office, remotely, or in a hybrid setup, here's a simple step-by-step guide to help you troubleshoot slow or spotty internet without needing an IT degree.

Step 1: Reboot Your Router (Yes, Really)

The oldest trick in the book is still one of the most effective. Restarting your router can fix common glitches by clearing out bugs and refreshing your connection.

How to do it:

- Unplug the router and modem (if they're separate)
- Wait 30 seconds
- Plug them back in and wait a couple minutes

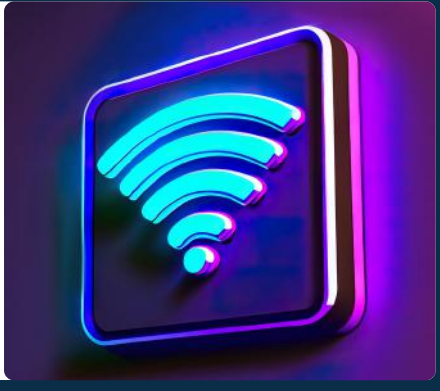
It's quick, easy, and works more often than not.

Step 2: Check Your Signal Strength

Is your Wi-Fi bad in some rooms but not others? That's a signal issue, not a service problem.
Try this:

- Move closer to your router and see if the connection improves
- Use tools like NetSpot or WiFi Analyzer to find dead zones
- Don't hide your router in a cabinet or behind equipment — it needs open space to broadcast effectively

Small business IT support providers like LeadingIT can help assess your office layout and recommend Wi-Fi extenders or mesh networks for seamless coverage.



Step 3: Test Other Devices

Before blaming your internet, check if other devices are struggling too.
If only one computer is having issues:

- Restart the device
- Disconnect and reconnect to Wi-Fi
- Run a quick speed test at Speedtest.net

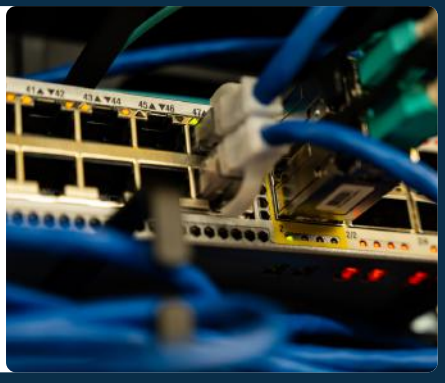
If multiple devices are slow or dropping off, it's time to look at your router, cabling, or your provider — or reach out to your network support services team for help.

Step 4: Disconnect Devices You're Not Using

Your network only has so much bandwidth. Printers, smart TVs, phones, and tablets all use it up — even when they're idle.
If your work computers are slowing down:

- Disconnect unused devices
- Pause large downloads or streaming services
- Use your router's settings (or ask your IT help desk) to prioritize business devices

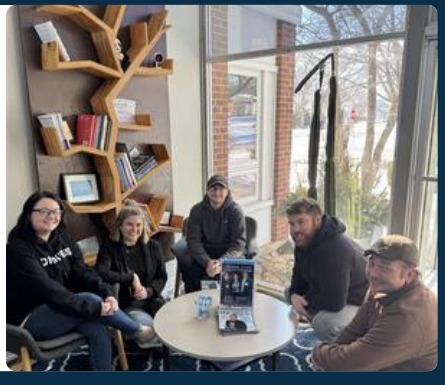
This one change can significantly reduce lag during work hours.



Step 5: Still Having Problems? Call in the Pros

If you're constantly fighting with your connection, the issue might be bigger than a router reset. Outdated hardware, interference, or even ISP issues could be at play. That's where LeadingIT's IT support comes in. We work with businesses across Chicagoland to solve performance issues, secure networks, and build reliable setups that just work — day after day.

Whether you need a better router, updated firmware, or ongoing network monitoring, our team is ready to help you stay connected and protected.



Conclusion: You shouldn't need a computer science degree to fix your Wi-Fi.
But you should have access to an IT team that's got your back when things don't work right.

Let LeadingIT take the stress out of staying connected. With proactive IT support, fast response times, and clear solutions, we'll make sure your tech helps you work smarter — not harder.

What an IT Audit Really Tells You (And Why You Shouldn't Skip It)

As a managed services provider (MSP), we often see businesses focused on the day-to-day operations of their technology. While keeping the lights on is crucial, neglecting a comprehensive understanding of your IT infrastructure's health and security can be a costly oversight. This is where an IT audit comes in as a vital diagnostic tool that unveils the true state of your digital ecosystem and provides a roadmap for a more secure, efficient, and resilient future.

Understanding the Core of an IT Audit

So, what exactly does an IT audit tell you? Think of it as a thorough physical for your technology environment. It goes beyond surface-level checks to delve into the intricate workings of your hardware, software, network, security protocols, and IT-related processes. The insights gleaned can reveal both strengths to build upon and critical weaknesses that demand immediate attention.

Clarity on Your IT Infrastructure

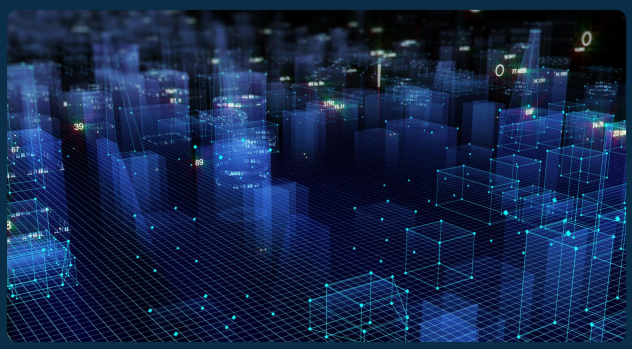
A key benefit of an IT audit is gaining a clear view of your current technology landscape. This includes an inventory of hardware and software assets, their age, licensing status, and overall performance. Are you running outdated servers or paying for unused software? An estimated $34 billion is wasted annually on unused software licenses. An audit helps you make informed decisions about upgrades and resource allocation while potentially saving you money.

Analyze Network Architecture and Performance

Beyond inventory, an audit assesses your network's architecture and performance. It identifies bottlenecks, single points of failure, and opportunities for optimization—all crucial for keeping your operations smooth, scalable, and resilient. A well-functioning network is the backbone of productivity and collaboration.

A Critical Look at Security Posture

Security is arguably the most vital part of any IT audit. It reviews your security policies, tools, and protocols—from firewalls to antivirus solutions and intrusion detection systems. An audit pinpoints vulnerabilities, evaluates your risk of cyberattacks, and offers clear guidance on strengthening your defenses. This is essential for protecting sensitive data, ensuring compliance, and preserving your reputation.



Evaluating IT Processes and Compliance

An audit also examines your IT processes and policies. Are your data backups reliable and tested? Are your onboarding and offboarding procedures secure? Strong processes reduce risks of data loss, breaches, and disruptions. Additionally, for industries bound by regulations like HIPAA, GDPR, or PCI DSS, an audit helps ensure you stay compliant, avoiding fines and legal trouble.

The Cost of Skipping: Why Proactive Audits Matter

So, why do some businesses skip IT audits? Often, it's due to concerns about cost or the assumption that if everything seems fine, there's no need to look closer. But this mindset is risky.

The costs of a data breach, prolonged downtime, or compliance failure can far exceed the investment in a proactive audit. For example, the average cost of a data breach in 2025 was $4.88 million, a price that could be avoided with regular IT audits.

Skipping your IT audit is like driving a car without checking the oil—you might get by for a while, but a costly breakdown is inevitable.

Conclusion: Invest in Your Digital Future with an IT Audit

An IT audit provides a clear understanding of your digital environment, uncovering opportunities to boost security, performance, and resilience. As your trusted MSP, we strongly recommend regular audits to empower better decisions and minimize risks. Don't wait for problems to appear—take charge of your IT landscape today and build a more resilient and scalable future.

$1000 REFERRAL PROGRAM

Do you know an organization that needs unlimited IT and cybersecurity support with an unbeatable guarantee?

You'll earn **$50** for every referral. If they sign up, you'll receive **$1000!**

815-788-6041 **GOLEADINGIT.COM/REFER**

SCAN TO LEARN MORE

DRIVEN – CHASES EXCELLENCE – HUMBLY CONFIDENT – ACCOUNTABLE – STAYS POSITIVE

LeadingIT Core Values Victor of the Month

Vanessa Canete, Level 2 Technician

iis this month's Values Victor for chasing excellence!

From start to finish, Vanessa brings a relentless drive to every task, always going above and beyond to support her team and deliver exceptional service to our clients. Her attention to detail, commitment to growth, and passion for doing things right makes her a standout example.

Vanessa, thank you for raising the bar and inspiring all of us to be better!

LeadingIT

We Help Chicagoland Organizations Eliminate Concerns Over IT and Cybersecurity Where the Unsolvable is Solved with Unlimited Support, and an Unbeatable Guarantee.

WE ARE CELEBRATING!

BIRTHDAYS

LAURA PIEKOS - MAY 21ST