the NetWork

LeadingIT

Chicagoland CybersecurITy Support

April 2025

Windows 10 End of Support: A Looming Deadline for Your Business

Why Is Your Internet So Slow? The Hidden IT Issues You Didn't Know About

VPNs: The Right Way to Use Public Wi-Fi Without Getting Hacked

Sick of IT Headaches? Here's Why Your Tech Keeps Breaking (And How to Fix It)

LeadingIT Core Values Victor

GoLeadingIT.com 815-788-6041 @goleadingit

Windows 10 End of Support: A Looming Deadline for Your Business

The clock is ticking. Microsoft's official end-of-support date for Windows 10 is October 14, 2025. This means that after October 2025, your Windows 10 computers will no longer receive security updates from Microsoft, making them vulnerable to new cyber threats. You may also find that new software won't work, and if something goes wrong, you won't get official help from Microsoft.

That said, this isn't just a routine software update; it's a pivotal moment that requires prompt action. Understanding the consequences and starting to plan now to prevent disruptions and minimize security risks is essential.

What Happens After End of Support?

After October 14, 2025, Microsoft will no longer provide security updates, bug fixes, or technical support for Windows 10. This leaves systems vulnerable to:

- Increased Security Risks: Without patches, systems become prime targets for cyberattacks. The 2017 WannaCry ransomware attack, which impacted over 160,000 users—98% of whom were running outdated Windows 7—highlights the dangers of unsupported software.
- Software Incompatibility: New software and hardware may not be compatible with an unsupported operating system.
- Compliance Issues: Many industries have regulations requiring up-to-date operating systems.
- End of SoftwareVendor Support: Many software vendors will also end support of their software on Windows 10, leaving you without updates or fixes for critical applications.

The Crucial Question: Upgrade or Replace?

The most pressing concern for many businesses revolves around whether they can simply upgrade to Windows 11 or if they'll need to replace their hardware entirely. Unfortunately, the answer isn't straightforward and depends on the age and specifications of your existing systems.

Windows 11 has stricter hardware requirements than its predecessor. For instance, it requires a processor with at least 1 gigahertz (GHz) or faster with two or more cores on a compatible 64-bit processor or System on a Chip (SoC), 4 GB RAM, and 64 GB or larger storage device. For those with older hardware, a simple upgrade to Windows 11 will likely be impossible. This means that your business will need to replace its PCs.

Act Now to Avoid Delays and Increased Costs

As the end-of-support deadline nears, businesses must brace for a surge in demand for new PCs and the strain this will put on global manufacturing and logistics. Component shortages have already led to increased lead times, with some businesses reporting delays of up to 12 weeks for essential hardware.

The rush to replace outdated systems could drive up prices, adding to the financial burden. Securing hardware early will not only prevent delays but also shield your business from rising costs and disruptions.

continue reading on page 7...

Pictured on the cover: Kelly, Laura, Daniel, Alex, Seth

VPNs: The Right Way to Use Public Wi-Fi Without Getting Hacked

Public Wi-Fi is convenient, but it can also be a security nightmare. When you connect in places like coffee shops or airports, your personal information is vulnerable to hackers. They can steal your passwords, bank details, and messages surprisingly easily.

In fact, nearly one in five people have experienced security problems because of public Wi-Fi, and that number rises to almost one in four for daily users. Thankfully, a VPN can make public Wi-Fi safer.

Why Public Wi-Fi Is a Security Risk

Public Wi-Fi networks are typically unsecured, meaning anyone on the same network can potentially intercept your data. Hackers use various techniques, such as "man-in-the-middle" attacks, to eavesdrop on your internet activity. They can also set up fake Wi-Fi hotspots that look legitimate, tricking users into connecting and unknowingly sharing sensitive information.

How a VPN Protects You

A VPN encrypts your internet connection, making it nearly impossible for hackers to see your data. Here's how it helps:

- **Encryption:** A VPN scrambles your data into unreadable code, preventing cybercriminals from accessing your information.
- **Secure Connections:** Even if a hacker tries to intercept your data, they'll only see encrypted information rather than sensitive details like passwords or credit card numbers.
- **Anonymous Browsing:** A VPN hides your IP address, making it difficult for websites and attackers to track your online activity.
- **Safe Access to Websites:** Some websites block users from certain regions or networks, but a VPN allows you to access restricted content securely.

Best Practices for Using Public Wi-Fi Securely

While a VPN is your best defense, combining it with these best practices ensures maximum protection:

1. **Always Use a VPN –** Enable your VPN before connecting to public Wi-Fi to encrypt your internet traffic from the start.
2. **Turn Off Auto-Connect –** Disable the setting that automatically connects your device to available Wi-Fi networks to avoid accidentally joining a rogue hotspot.
3. **Use HTTPS Websites –** Always check for "https://" in the URL, as these sites encrypt data between your browser and the server.
4. **Avoid Accessing Sensitive Information –** AVOID logging into banking apps, email, or other personal accounts while on public Wi-Fi.
5. **Enable Two-Factor Authentication (2FA) –** Even if a hacker gets your login credentials, they won't be able to access your account without the second verification step. A 2019 Microsoft study reported that 2FA prevents 99.9% of all automated hacks.
6. **Keep Your Software Updated –** Regularly update your device's operating system and security software to patch vulnerabilities.

continue reading on page 7…

Why Is Your Internet So Slow? The Hidden IT Issues You Didn’t Know About

Few things are more frustrating than slow internet, especially when you are trying to run a business. Video calls freeze, cloud applications lag, and employees lose valuable time waiting for pages to load. While most people blame their internet service provider (ISP), the truth is that the issue often lies within your own IT infrastructure. Let’s explore the hidden causes of slow internet and how to fix them.

1. Outdated Networking Equipment

Your router and modem play a crucial role in delivering fast and stable internet. Many businesses continue using outdated equipment without realizing that older routers cannot handle the bandwidth demands of modern applications. A slow or unreliable router can bottleneck your entire network.

SOLUTION: Upgrade to a business-grade router that supports the latest Wi-Fi standards. Look for devices that offer Quality of Service (QoS) settings, which allow you to prioritize essential business applications over non-critical internet traffic. Choosing the right router can make all the difference.

2. Network Congestion from Too Many Devices

Every device connected to your network takes up bandwidth. If too many devices are using the internet simultaneously, speeds can drop significantly. This is especially problematic in businesses where employees are constantly using cloud applications, video conferencing, and file-sharing tools.

SOLUTION: Implement network segmentation by creating separate Wi-Fi networks for employees, guests, and critical business applications. Use bandwidth management tools to allocate network resources efficiently.

3. Poor Wi-Fi Signal Strength

Weak Wi-Fi signals lead to slow speeds and frequent disconnections. Physical obstacles such as walls, metal objects, and electronic interference can degrade Wi-Fi performance. Many businesses rely solely on a single router, which is often not enough to cover the entire office.

SOLUTION: Use Wi-Fi extenders or upgrade to a mesh Wi-Fi system that provides better coverage throughout your office. Consider using wired connections for critical workstations to ensure consistent speed and reliability.

4. Background Applications Hogging Bandwidth

Many background applications consume significant amounts of bandwidth without you realizing it. Cloud backups, software updates, and streaming services can slow down your connection for other essential tasks.

SOLUTION: Monitor network traffic using tools to identify bandwidth-heavy applications. Schedule backups and updates for non-peak hours to prevent disruptions during business operations.

5. ISP Throttling and Bandwidth Limits

Some ISPs impose data caps or throttle speeds during peak usage hours. If your business consistently uses large amounts of data, your ISP may be slowing your speeds to manage network congestion.

SOLUTION: Contact your ISP to understand your data limits and upgrade to a higher-tier business plan if necessary. Consider using a secondary ISP or a load balancing router to distribute internet traffic more effectively.

6. Malware and Unauthorized Network Usage

Cyber threats such as malware and unauthorized users on your network can consume bandwidth and slow down your internet speed. A compromised network not only affects performance but also poses significant security risks.

SOLUTION: Use enterprise-grade firewalls and regularly scan your network for unauthorized devices. Implement strong password policies and use multi-factor authentication (MFA) to prevent unauthorized access.

Final Thoughts

Slow internet is more than just an annoyance. It directly impacts productivity and business operations. By identifying these hidden IT issues and taking proactive steps to resolve them, you can improve network performance and ensure a smooth online experience for your team.

Sick of IT Headaches? Here’s Why Your Tech Keeps Breaking (And How to Fix It)

If you feel like your business is constantly dealing with slow computers, crashing software, or never-ending password resets, you’re not alone. IT headaches are one of the biggest productivity killers for small businesses. But why does your tech keep breaking? And more importantly, how can you fix it for good?

Let’s break it down.

1 *Outdated Hardware & Software*

Just like a car that hasn't had an oil change in years, old tech will eventually break down. Many businesses continue using outdated hardware and software because "it still works," but the reality is:

- Older systems are slower and prone to crashes.
- Unsupported software creates major security risks.
- Compatibility issues make it difficult to integrate new tools.

► **FIX IT:** Regularly update your hardware and software. If your computers are more than 3-5 years old, consider replacing them. Use automated patch management tools or work with an IT provider to ensure updates happen on schedule. Learn more about why software updates are critical.

2 *Lack of Preventative IT Maintenance*

Most small businesses take a "fix it when it's broken" approach to IT, but that’s like never servicing your car until the engine fails. Preventative maintenance is key to reducing IT headaches.

► **FIX IT:** A proactive IT strategy includes:

- Regular system monitoring for potential issues.
- Scheduled maintenance and health checks.
- Automatic backups to prevent data loss.

Managed IT services can handle all of this, keeping your business running smoothly. See how proactive IT maintenance can save your business money.

3 *Cybersecurity Issues & Malware*

Nothing grinds operations to a halt like a malware infection or cyberattack. Phishing scams, ransomware, and data breaches can lock you out of your systems and cost thousands in damages.

► **FIX IT:** Strengthen your cybersecurity by:

- Using multi-factor authentication (MFA).
- Providing employee cybersecurity awareness training.
- Deploying endpoint security solutions and firewalls.

Find out why small businesses are top targets for cybercriminals.

4 *Poor Network Infrastructure*

Is your Wi-Fi constantly dropping? Are your cloud applications slow? Weak network infrastructure is a common culprit behind IT frustrations.

► **FIX IT:** Optimize your network by:

- Upgrading to a business-grade router.
- Using a managed Wi-Fi solution to prevent congestion.
- Running regular network performance tests.

5 *Unreliable IT Support*

If you rely on a break-fix IT guy or an overwhelmed internal IT team, issues are bound to pile up. A reactive approach means problems get fixed after they cause downtime, leading to lost productivity and frustration.

► **FIX IT:** Partner with a Managed Service Provider (MSP) who offers 24/7 monitoring, fast support, and a proactive strategy to prevent IT issues before they happen.

Final Thoughts

Your technology should empower your business, not slow it down. By addressing these common IT headaches with proactive solutions, you can eliminate tech frustrations and focus on growing your business.

Want to stop IT headaches for good? Let's talk! LeadingIT specializes in unlimited IT management for businesses in Chicagoland. Contact us today to learn how we can keep your technology running smoothly.

Windows 10 End of Support: A Looming Deadline for Your Business

continued from page 2...

Conclusion: Being Proactive Is Key

Taking proactive steps now to address the Windows 10 end-of-support issue will save your business from costly disruptions, increased cybersecurity risks, and potential operational delays. Don't wait for the deadline to sneak up on you—contact LeadingIT today to schedule a consultation and develop a tailored migration strategy. Time is running out—act now to secure a smooth transition before it's too late.

VPNs: The Right Way to Use Public Wi-Fi Without Getting Hacked

continued from page 3...

Choosing the Right VPN

Not all VPNs are created equal, so choosing a reputable provider is crucial. Look for these features when selecting a VPN:

- Strong Encryption: AES-256 encryption is the gold standard for security.
- No-Logs Policy: Ensure the provider doesn't store records of your internet activity.
- Fast Speeds: Some VPNs slow down connections, so choose one known for speed and reliability.
- Multiple Server Locations: More server options allow better access to content and security.

Conclusion: Stay Secure, Stay Private

Public Wi-Fi is unavoidable, but that doesn't mean you have to put your data at risk. Using a VPN, along with smart security practices, allows you to browse safely and confidently. Don't take chances with your sensitive information—protect yourself with a VPN every time you connect to public Wi-Fi.

LeadingIT Core Values Victor of the Month

Congrats to Alex Del Fiacco, this month’s Values Victor for being Driven at LeadingIT!

Alex started as a bench technician and worked his way up to Level 1 Technician through sheer hard work and determination. His drive is a big part of why our team and our clients keep succeeding.

Every day, Alex proves that being driven means pushing through challenges and constantly aiming higher. Thanks, Alex, for your hard work and dedication!

LEADINGIT VALUES:

- We Are Driven
- We Chase Excellence
- We Are Humbly Confident
- We Are Accountable
- We Stay Positive

WE ARE CELEBRATING!

Birthdays

Alex Del Fiacco - April 4th

Anniversaries

Jeremiah Bird - 4/15/24

LeadingIT

$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!**

LEARN MORE

GOLEADINGIT.COM/REFER

815-788-6041

Continue reading on our blog at goleadingit.com/blog

LeadingIT

Serving the Chicagoland area with
offices in Woodstock, Downtown Chicago,
and now in Manteno, IL