ISSUE 021
April 2025
Independence, Missouri

FCS TECH TALK

Your Trusted
Technology Partner Since 1989

INSIDE THIS ISSUE:

THE END OF SUPPORT FOR WINDOWS 10: HOW TO PREPARE FOR THE TRANSITION

On **October 14, 2025**, Microsoft will officially end support for Windows 10, marking the close of an era for one of the most widely used and influential operating systems in history.

Launched in 2015, Windows 10 has powered millions of devices worldwide, from personal computers to enterprise systems. This milestone signifies more than just the end of a product life cycle; it represents a shift in focus towards newer technologies, particularly Windows 11. With this impending change, users and organizations must begin preparing for the future to ensure continued security, efficiency, and compliance.

What Does "End of Support" Mean?

When Microsoft ends support for an operating system, it stops releasing updates, patches, and security fixes for that product. After **October 14, 2025,** Windows 10 will no longer receive these critical updates, leaving any systems still running the OS increasingly vulnerable to security threats, performance issues, and compatibility problems.

Microsoft has a structured life cycle for its products, typically providing mainstream support for five years (including feature updates and security patches) followed by extended support for an additional five years (focusing on security updates).
As of 2024, Windows 10 has entered its extended support phase, meaning it only receives security updates and critical patches. When this period ends, the OS will be officially "retired," and users will need to migrate to newer platforms.

The Impact of Windows 10's End of Support

1. Security Risks

The most significant consequence of the end of support is the security risk posed to unsupported systems. After the end date, Microsoft will no longer release security updates to fix vulnerabilities that may be discovered. Hackers often target older, unsupported systems, knowing that any newly discovered vulnerabilities will remain unpatched. For both individual users and businesses, this could mean an increased risk of cyberattacks, including ransomware, data breaches, and system compromises.

2. Software and Hardware Compatibility Issues

As software and hardware manufacturers focus on supporting modern operating systems, Windows 10 will gradually lose compatibility with new applications, drivers, and hardware components. Developers typically optimize their products for supported systems, which means future applications might not function properly on Windows 10, leading to operational inefficiencies or forcing users to seek costly workarounds.

3. Compliance Challenges for Businesses

For businesses, continuing to use an unsupported operating system can have regulatory implications. Many industries are subject to strict compliance regulations regarding data protection and cybersecurity, such as GDPR in Europe or HIPAA in the United States. Running outdated and unsupported software can result in non-compliance, potentially leading to legal consequences, fines, and reputational damage.

4. Diminishing Performance and Reliability

Without regular updates and bug fixes, Windows 10's performance may degrade over time. The absence of optimizations, driver updates, and system patches could lead to crashes, freezes, and slower performance, particularly as newer software and hardware components are released without backward compatibility.

Why Microsoft is Ending Support for Windows 10

The end of support for Windows 10 aligns with Microsoft's broader strategy of focusing on newer technologies and operating systems, particularly Windows 11.
When Windows 10 was first launched, Microsoft had dubbed it "the last version of Windows" with plans to evolve it continuously through updates.
However, technological advancements, new hardware innovations, and shifting user needs eventually led Microsoft to develop Windows 11, released in 2021.

Windows 11 comes with a host of improvements over Windows 10, including enhanced security features, a more modern and streamlined user interface, improved gaming performance, and better integration with cloud services and mobile devices. As Microsoft focuses on evolving Windows 11 and future iterations, it is only natural that older versions like Windows 10 will be phased out.

How to Prepare for the End of Windows 10 Support

The end of Windows 10 support is less than 6 months away. Users and organizations should start preparing now to ensure a smooth transition to newer operating systems.

Here are the key steps to take:

1. Upgrade to Windows 11

For most users, upgrading to Windows 11 is the most straightforward solution. Windows 11 is a natural progression from Windows 10, with many similar features, but enhanced security and performance. Microsoft has made the upgrade process relatively simple, and most users of Windows 10 are eligible for a free upgrade, provided their hardware meets the necessary requirements.
Check System Requirements
Before upgrading, it's essential to check whether your hardware meets the minimum requirements for Windows 11, which include:

- A compatible 64-bit processor with at least 1 GHz speed
- 4 GB of RAM or more
- 64 GB of storage or more
- A TPM 2.0 chip (Trusted Platform Module)
- Secure Boot capability
- A DirectX 12 compatible graphics card

If your device doesn't meet these requirements, you may need to either upgrade your hardware or purchase a new device that supports Windows 11.

2. Consider Hardware Upgrades

If your current PC is incompatible with Windows 11, it may be time to consider a hardware upgrade.
While some devices may be able to run Windows 11 after a few component upgrades (such as adding a TPM 2.0 module or increasing RAM), others may require replacing entirely.
When choosing new hardware, consider future-proofing your investment by opting for components that not only meet today's standards but also anticipate future demands.

3. Backup Important Data

Before upgrading your system, it's crucial to back up all important data. Whether you are transitioning to Windows 11, switching to a different operating system, or purchasing a new device, data backups ensure that your files, documents, and applications are protected in case anything goes wrong during the transition. FCS can help with any of your backup needs to make sure that your data will be safe and secure during a transition.

4. Plan for a Transition Period

Organizations, in particular, should plan for a transition period during which they evaluate software compatibility, retrain staff, and test systems running on the new OS. This is especially important for businesses that rely on custom-built software or specialized applications that may need updates to work on Windows 11. Establish a timeline that includes testing, deployment, and contingency planning to ensure minimal disruptions during the transition. FCS can help assist with any of these needs.

Windows 11 represents a significant step forward with its modernized user experience, tighter integration with cloud-based services, and advanced security features, including improved protection against malware and ransomware attacks.

Additionally, Microsoft continues to push innovations like Windows 365, a cloud-based PC service that allows users to access a full Windows desktop environment from virtually any device, representing a potential future direction for personal and enterprise computing.

The end of support for Windows 10 is inevitable, but with the right preparation, it doesn't have to be disruptive. Whether you're a business leader planning a large-scale migration or an individual user upgrading your home computer, FCS can help you to ensure a smooth transition to a more modern, secure operating system.

TL;DR

Microsoft will officially end support for Windows 10 on October 14, 2025. After that date, no more updates or security patches will be released, leaving systems vulnerable to cyber threats, software incompatibility, and compliance issues.
To stay secure and compliant, users and businesses should begin planning their upgrade to Windows 11 now. Key steps include checking hardware compatibility, backing up data, considering new devices if needed, and preparing for a smooth transition.
Windows 11 offers enhanced security, better performance, and deeper cloud integration—making it a smart move for the future.
FCS is here to help you to plan and transition your business to Windows 11 so you are fully prepared for end of support for Windows 10.

ISSUE 021
April 2025
Independence, Missouri

THIS MONTH'S PRODUCT SPOTLIGHT

CLICK TO VIEW A SHORT VIDEO!

WEBSITE DEVELOPMENT SERVICES

CUSTOM WEBSITE BUILDING

FAST AND SECURE WEBSITE HOSTING

WEBSITE UPDATES AND REVAMPS

QUICK TECHNICAL WEBSITE SUPPORT

WHERE DO DELETED FILES GO?

It may seem like the file is gone for good when you delete it from your computer. However, the truth is more complicated than that. A deleted file doesn't really disappear from your hard drive; it stays there until new data fills up the space it occupied.

What Happens When You Delete a File?

It's not as easy as it seems to delete a file. When you send a file to the Trash or Recycle Bin, it is not erased from your hard drive right away. It is instead taken to a temporary storage place and stays there until you decide to empty the bin. The file's data stays on the hard drive even after the bin is empty; it is marked as free space that can be used by other files.

When you delete a file, you remove its record from the file system. The file system is like a directory that keeps track of all the files on your computer. The operating system will no longer know where the file is, but the data inside will still be there. This is why it's often possible to recover deleted files with special software, as long as the space hasn't been filled with something else.

Getting rid of files is a lot like taking the title off of a VHS tape (for those of you who remember VHS tapes 😁). People who are looking for the movie can still find it on the tape, but without the name, it's like the movie doesn't exist. Also, when you remove a file, you're removing its label from the file system. The data, on the other hand, stays on the hard drive until it's overwritten.

To manage data successfully and safely, you need to understand this process. For instance, deleting private information might not be enough if you want to be sure it's gone for good. If you want to delete the information on your hard drive safely, you may need to use extra tools.

Take Charge of Your Information

If you want to keep your digital life safe, you need to know where deleted files go and how to recover them. You can keep your information safe from unauthorized access by managing your data and backing it up regularly. If you need help safely deleting sensitive files or have questions about how to handle your data, please contact us.

MAXIMIZING THE POWER OF MICROSOFT 365

Power Platform tools, such as Power Automate and Power BI, help businesses automate repetitive tasks and gain insights from their data, driving productivity and informed decision-making.

Staying current with regular training and updates ensures your team continues to make the most of new features and improvements.

Partnering with Microsoft 365 experts can provide valuable guidance, whether you're just getting started or looking to refine your setup. And don't overlook the basics—effective email and time management through Outlook and Calendar are essential to keeping daily operations on track.

Lastly, the ability to use Microsoft 365 tools across multiple devices—from desktops to smartphones—means your team can remain productive and connected from virtually anywhere.

With the right approach, Microsoft 365 becomes more than just a set of tools—it becomes the backbone of a modern, agile business.

Microsoft 365 offers a dynamic suite of cloud-based tools designed to streamline operations and enhance collaboration for businesses of all sizes.

At the heart of Microsoft 365 is Microsoft Teams, a hub for communication that brings together chat, video meetings, file sharing, and collaboration in one place.

For file storage and easy access across devices, OneDrive offers secure cloud storage that supports seamless remote work.

Businesses looking to tailor their digital tools can turn to Power Apps, which allows the creation of custom applications to meet unique workflow needs.

To truly get the most out of Microsoft 365, it's important to go beyond the basics. Embracing the full potential of Teams can significantly enhance collaboration across departments.

SharePoint enables businesses to customize their digital workspace, fostering better content management and internal communication.

CYBER SECURITY SPRING CLEANING

Spring is the season of fresh starts—and while many think about cleaning out closets or reorganizing their desks, it's also a great time to tidy up something even more critical: your Cyber Security.

Cyber threats continue to evolve, and small to mid-sized businesses are increasingly in the crosshairs. A "set-it-and-forget-it" approach just won't cut it anymore. That's why we at FCS encourage our clients to think of spring as the ideal time to reassess, refresh, and reinforce their digital defenses.

Below, we've outlined five essential steps every business should take this season to tighten security—and how FCS can guide and support you at every turn.

1. Review and Remove Unused Accounts

The Risk: When employees leave or change roles, they often leave behind user accounts with lingering access to critical systems. These forgotten accounts become low-hanging fruit for attackers.

Spring Action: Conduct a thorough user access audit. Disable or delete inactive accounts and ensure active users only have the permissions they need.

How FCS Helps: FCS performs regular user access reviews for our clients. We use centralized tools to track account activity and flag unused or suspicious logins. If you're using Microsoft 365, we help you manage user roles and implement policies that limit unnecessary access across Teams, SharePoint, and OneDrive.

2. Update and Patch Software Regularly

The Risk: Unpatched software is a leading cause of data breaches. Cybercriminals actively exploit known vulnerabilities in outdated applications and operating systems.

Spring Action: Update all operating systems, productivity tools, antivirus software, and even firmware on hardware like firewalls, printers, and routers.

How FCS Helps: FCS offers fully managed patching and update services. We monitor all your systems to ensure everything is current—and we test patches before deployment to prevent downtime. Whether you're running Windows endpoints, cloud-based apps, or legacy software, we've got you covered.

3. Enforce Strong Passwords and Multi-Factor Authentication (MFA)

The Risk: Weak or reused passwords are still one of the top ways attackers gain access. Without MFA, a compromised password can open the door to your entire network.

Spring Action: Encourage your team to update passwords and implement MFA across all major services and apps.

How FCS Helps: We enforce password complexity policies through Active Directory and Microsoft 365. Plus, FCS configures and supports MFA deployment—including app-based or token-based authentication—for services like email, remote access, and cloud platforms. If you're not sure how to roll it out effectively, we'll walk you through every step.

4. Verify (and Test) Your Backups

The Risk: Backups that aren't tested regularly can fail when you need them most. And in the event of ransomware or accidental deletion, data recovery could be your lifeline.

Spring Action: Confirm your backup systems are working, current, and secure. And test your ability to restore files quickly.

How FCS Helps: We don't just back up your data—we build recovery plans around it. FCS offers fully managed backup solutions, both onsite and in the cloud, with regular testing to ensure restorability. Our clients benefit from versioning, encryption, offsite redundancy, and quick-response recovery if the worst happens.

5. Refresh Employee Security Training

The Risk: Employees are your first line of defense—and also one of the biggest vulnerabilities if not properly trained. Phishing, social engineering, and careless clicking are top causes of breaches.

Spring Action: Run a Cyber Security refresher course. Revisit best practices, share real-world threat examples, and consider launching a phishing simulation.

How FCS Helps: FCS offers ongoing Cyber Security training and simulated phishing campaigns to raise awareness and reduce risky behavior. Our content is tailored for SMBs—clear, non-technical, and designed to actually stick. You'll get reports on who clicked what, where improvements are needed, and how your team is progressing over time.

ISSUE 021
April 2025
Independence, Missouri

DON’T IGNORE YOUR PERSONAL GMAIL: WHY IT DESERVES SERIOUS SECURITY

When it comes to email security, work emails are usually top of the list to secure with—strong passwords, two-factor authentication, IT monitoring... the works.

But what about that old personal Gmail account you’ve had since college? The one tied to your social media, shopping, banking, and maybe even some work logins? That’s often left wide open—and that’s a problem.

Here’s why your personal Gmail account deserves just as much protection as your business inbox.

Your Gmail account is likely connected to:

- Amazon, Netflix, Uber, PayPal
- Facebook, Instagram, LinkedIn
- Banking, tax software, online shopping
- Cloud storage (Google Drive, Dropbox)
- Password recovery for dozens of accounts

If someone gains access to your Gmail, they can reset passwords, impersonate you, access sensitive data, and even commit identity theft—all without ever touching your work email.

Old Accounts = Weak Spots

Let’s be honest—if you created your Gmail in 2010, you probably haven’t reviewed its security settings in a while. That means:

- Outdated or reused passwords
- No two-factor authentication (2FA)
- Forgotten apps and services with access
- No alerts or monitoring for suspicious activity

Hackers love low-hanging fruit, and older, unprotected accounts are easy targets.

Work Security Doesn’t Extend to Personal Accounts

Even if your workplace uses enterprise-grade security, that protection doesn’t apply to your personal email. And if you use your Gmail for anything work-related (remote logins, document access, email forwarding), you could be creating an unexpected vulnerability for your company too.

The Real Risks of an Unsecured Gmail Account

- Identity Theft – One compromised account can unlock access to dozens of others.
- Phishing & Scams – Hackers can send phishing emails from your name to your contacts.
- Financial Fraud – Access to online shopping or bank-linked services can lead to unauthorized purchases.
- Data Leaks – Old emails may contain sensitive attachments, personal info, or login credentials.

How to Protect Your Gmail Account Today

Here’s how you can secure your personal Gmail account in less than 15 minutes:

- Turn on 2-Step Verification – Adds a second layer of protection.
- Use a Strong, Unique Password – Avoid reusing old passwords.
- Check Recent Activity – Look for any unfamiliar devices or locations.
- Review Third-Party App Access – Revoke anything you don’t recognize or use.
- Set Up Recovery Options – Make sure you can regain access if you ever get locked out.
- Update Your Backup Email & Phone Number – These should always be current.
- Enable Security Alerts – Google will notify you of any suspicious activity.

Clean Out Old Emails and Sensitive Info

Your inbox might be storing more than you realize—old tax documents, passwords, banking details, contracts, or ID scans. If your account is ever compromised, these can be goldmines for hackers.

Take a few minutes to:

- Search for sensitive keywords like "password," "SSN," "bank," "tax," etc.
- Delete or move sensitive documents to a secure, encrypted location.
- Empty your trash and spam folders regularly.

Bottom Line: If You Use It, Protect It

Your personal Gmail is probably the most overlooked vulnerability in your digital life. Don’t wait until it’s too late.

Whether you use it daily or only occasionally, taking a few simple steps now can protect your identity, your data, and your peace of mind.
If you're not sure where to start—or want help reviewing your personal email security—reach out. We're always here to help.

WE LOVE REFERRALS

The greatest gift anyone can give us is a referral to another business in need of IT services. Referrals help us keep costs down so we can pass the savings to our clients.

If your referral ends up becoming a client - we’ll gift them their first month of service at no charge AND we’ll gift you a $500 Amazon Gift Voucher.

Simply introduce me via email to stan@fcskc.com and I’ll take it from there. I personally promise we’ll look after your referral's business with a high level of care and attention (just like we do with all our clients).
-Stan

We Want Your Feedback

Here at Ferguson Computer Services, we value your feedback greatly and would appreciate if you took time from your busy schedule to leave us a review. These reviews let us know what we are doing well and what we might be able to improve on in the future.

Leave a Google Review

Leave a Facebook Review

TECHNOLOGY TRIVIA TIME

Technology Trivia Question of the Month! Send the correct answer to winner@fcskc.com to be entered to win a $50 gift card to Amazon.

Here is April's question of the month:

In what year did Windows 10 launch?