ISSUE 034
May 2026
Independence, Missouri

FCS TECH TALK

Your Trusted Technology Partner Since 1989

INSIDE THIS ISSUE:

THE GROWING ROLE OF AI IN SMALL BUSINESS

The Illusion of Trust

Artificial intelligence has quickly become one of the most talked-about technologies in business. From automated customer support to content creation and data analysis, AI tools are now accessible to companies of every size—not just large corporations with dedicated IT departments.

For many small businesses, this creates both opportunity and uncertainty. Owners and employees see the potential benefits of AI, but they also question where it fits into their operations and how it should actually be used.

On the surface, AI appears to offer an easy solution to common business challenges. It can save time, improve efficiency, automate repetitive tasks, and help employees work more productively. In many cases, these benefits are real.

However, like any technology, AI is most effective when used properly. Without clear guidelines and realistic expectations, businesses can unintentionally create security risks, spread inaccurate information, or rely too heavily on tools that still require human oversight.

Much like cloud computing or remote work technologies when they first became popular, AI is not something businesses should ignore—but it is something they should approach strategically.

The Reality of AI in the Workplace

AI is already being used in many small businesses, even if owners do not realize it.

Employees may use AI tools to draft emails, summarize meetings, create marketing content, analyze spreadsheets, or assist with customer communication.

These tools can dramatically reduce the amount of time spent on repetitive administrative work. Tasks that once took hours may now take minutes, allowing employees to focus on higher-value responsibilities.

For example, AI can assist with:

- Drafting professional emails and documents
- Summarizing long reports or meetings
- Creating marketing ideas and social media content
- Organizing data and identifying trends
- Improving customer response times
- Automating repetitive workflows

Used correctly, AI becomes less about replacing employees and more about improving efficiency and supporting day-to-day operations.

However, problems begin when businesses treat AI as fully autonomous or assume that everything it generates is accurate. AI systems are designed to predict and generate responses—not guarantee correctness.

This means employees still need to review information carefully, verify important details, and apply human judgment before relying on AI-generated content.

The Risks of Improper AI Usage

While AI offers significant advantages, improper use can create serious concerns for small businesses.

One of the biggest risks involves sensitive information. Employees may unknowingly enter confidential company data, customer records, passwords, financial details, or internal documents into public AI platforms without understanding where that information goes or how it may be stored.

This creates potential security and compliance issues, especially for businesses handling sensitive client information.

There is also the risk of inaccurate or misleading output. AI-generated responses can sound highly professional and convincing even when the information is incomplete or incorrect. If employees rely on this information without verification, mistakes can quickly spread into customer communication, financial reporting, or operational decisions.

Another concern is overreliance. Businesses that attempt to replace too much human involvement with AI often discover that automation alone cannot manage relationships, critical thinking, or decision-making effectively.

AI can assist employees, but it should not replace accountability or oversight.

The Business Impact Beyond Productivity

When implemented properly, AI can create meaningful improvements throughout a business. Employees spend less time on repetitive tasks, response times improve, and operations become more streamlined.

For small businesses with limited staff, this can be especially valuable. AI tools may help employees accomplish more without immediately increasing headcount.

At the same time, businesses that fail to establish proper AI policies may expose themselves to unnecessary risk. Without structure, employees may use unauthorized AI tools, upload sensitive information, or unintentionally create inconsistent communication standards. Over time, this can lead to security concerns, compliance problems, and operational confusion.

There is also a reputational component to consider. Customers still expect professionalism, accuracy, and human interaction. Businesses that rely too heavily on automated responses can appear impersonal or disconnected if AI is not used carefully.

The goal should not be to remove people from the process. Instead, businesses should focus on using AI to support employees while maintaining quality, consistency, and security.

How AI Usage Develops Over Time

In many organizations, AI adoption happens gradually rather than through a formal rollout. Employees experiment with tools independently, discover ways to save time, and begin incorporating AI into daily tasks.

Over time, this informal usage can expand rapidly across departments without any centralized guidance or oversight.

This creates a situation where businesses may not fully understand:
Which AI tools employees are using
What company data is being shared
How information is being generated
Whether security standards are being followed

Much like shadow IT, unmanaged AI usage can introduce hidden risks that grow over time if left unaddressed.

Not Sure Where to Begin?

We can help your business implement AI tools safely and effectively while reducing unnecessary risk.

TL;DR

"Artificial intelligence can help small businesses improve productivity, automate repetitive tasks, and support employees in areas like communication, organization, and customer service. However, AI should be used carefully and strategically—not relied on without oversight. Improper use of AI can create security risks, expose sensitive company information, and lead to inaccurate or misleading content. Businesses should establish clear guidelines around what employees can use AI for, what information should never be entered into AI tools, and how AI-generated content should be reviewed. When combined with proper security practices and human oversight, AI can become a valuable tool that helps small businesses work smarter while maintaining professionalism, accuracy, and control."

ISSUE 034
May 2026
Independence, Missouri

THIS MONTH'S PRODUCT SPOTLIGHT

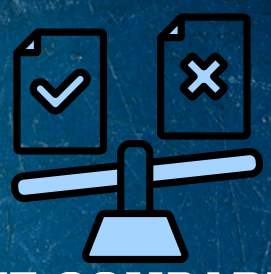
CLICK TO VIEW A SHORT VIDEO!

FREE INTERNET SERVICE CHECK

STOP OVERPAYING

GET FASTER SPEEDS

GET THE BEST VALUE



WE COMPARE FOR YOU

THE PRODUCTIVITY BENEFITS OF USING A DOCKING STATION

For many employees, the workday starts by connecting power cables, monitors, keyboards, and other accessories to a laptop before work can begin. While this process may seem minor, these small interruptions can add up over time and quietly reduce productivity.

This is where docking stations can make a significant difference.

A docking station allows a laptop to connect to monitors, internet, power, and accessories through a single cable. Instead of plugging in multiple devices individually, employees can quickly connect to their full workstation setup within seconds.

As laptops continue to replace traditional desktop computers in many businesses, docking stations have become an important tool for improving efficiency and creating a more organized work environment.

The Reality of Modern Work Environments

Today's employees often split time between home, the office, conference rooms, and remote locations. Laptops provide flexibility and portability, but they are not always ideal as a permanent workstation on their own. Smaller screens, limited ports, and constant cable management can create frustration throughout the day.

Employees frequently work with multiple applications at once, attend virtual meetings, and manage cloud-based systems simultaneously.

Docking stations help bridge the gap between mobility and functionality. Employees keep the flexibility of a laptop while gaining the advantages of a desktop-style workstation when seated at their desk.

The Benefits Beyond Convenience

Docking stations can also simplify IT management by creating more consistent workstation setups across the organization.

Employees become familiar with a standard setup, and troubleshooting becomes easier when hardware is configured similarly throughout the office.

This becomes especially valuable in hybrid work environments where employees frequently move between desks or locations.

What a Proper Docking Setup Should Include

Businesses should choose docking stations that are reliable, compatible with their hardware, and capable of supporting future growth.

A proper setup should provide stable connectivity, adequate charging power, and support for additional monitors and accessories when needed.

When implemented correctly, docking stations improve organization, reduce frustration, and help employees work more efficiently throughout the day.

Not Sure Which Docking Solution Is Right for Your Business?

We can help evaluate your current workstation setup and recommend docking solutions that improve productivity.

PUBLIC WIFI: CONVENIENCE VS RISKS

Public Wi-Fi networks have become a normal part of business travel and remote work. Employees connect in coffee shops, airports, hotels, and waiting rooms every day without thinking twice about it. On the surface, these networks provide a convenient way to stay productive outside the office.

However, public Wi-Fi can also introduce serious security risks.

Unlike a secured business network, public wireless connections are designed for convenience rather than protection.

Cybercriminals can sometimes monitor traffic, create fake hotspots, or attempt to intercept sensitive information from connected devices.

This becomes especially dangerous when employees access business email accounts, customer records, financial systems, or cloud storage while connected to unsecured networks.

Businesses should assume employees will occasionally work remotely and take steps to secure those connections properly. VPN solutions, multifactor authentication, endpoint protection, and employee awareness training all help reduce the risks associated with public Wi-Fi usage.

Remote work should remain productive, but it should also remain secure.

WHY SMALL BUSINESSES SHOULD REGULARLY REVIEW USER ACCOUNT ACCESS

For many small businesses, user accounts are created as needed and rarely thought about again. Employees receive access to email, business applications, shared folders, and internal systems so they can perform their daily responsibilities efficiently.

At first glance, this process seems harmless. Once access is granted and employees are able to work without interruption, there may appear to be little reason to revisit those permissions later.

However, over time, user access can become one of the most overlooked security risks within a business.

As employees change roles, departments evolve, software platforms expand, and staff turnover occurs, businesses often accumulate outdated accounts, unnecessary permissions, and inactive users that continue to maintain access to sensitive systems.

Much like leaving unused keys floating around an office, unmanaged account access creates opportunities for security issues, accidental mistakes, and unauthorized activity.
While these risks often develop quietly in the background, they can have a major impact if left unaddressed.

The Reality of Access Management

Every employee typically requires access to multiple systems in order to perform their job effectively. Email platforms, cloud storage, accounting software, CRM systems, communication tools, and remote access platforms are all commonly used throughout the workday.

As businesses grow, managing these accounts becomes increasingly complex.
Employees may receive temporary access to systems during special projects, retain permissions from previous positions, or continue accessing applications they no longer actively use. In some situations, accounts belonging to former employees may remain active longer than expected.

Over time, these small oversights can create unnecessary exposure throughout the organization.

Many businesses assume that cyberattacks only occur through sophisticated hacking techniques. In reality, compromised credentials remain one of the most common ways attackers gain access to business systems. If an unused or poorly managed account becomes compromised, attackers may be able to access sensitive data, send fraudulent emails, or move throughout connected systems without immediate detection.

The Business Impact Beyond Security

The risks associated with poor account management extend beyond cybersecurity alone.

Inactive accounts and excessive permissions can also create operational challenges. Employees may accidentally access information they no longer need, outdated accounts may continue consuming software licenses, and businesses may struggle to maintain visibility into who has access to what systems.

In hybrid and remote work environments, these challenges become even more significant. Employees frequently access systems from multiple locations and devices, increasing the importance of maintaining secure and well-managed account access.

What Proper Access Management Should Look Like

Managing user access effectively requires consistency, visibility, and clear processes.

- Businesses should regularly review:
- Active employee accounts
- Former employee accounts
- Administrative privileges
- Remote access permissions
- Shared accounts and credentials
- Access to sensitive files and systems

Employees should only have access to the systems and information necessary for their specific responsibilities. This approach, often referred to as "least privilege access," helps reduce unnecessary exposure throughout the business.

Multifactor authentication should also be enabled whenever possible to help protect accounts from compromised passwords and unauthorized logins.

Clear onboarding and offboarding procedures are equally important. When employees join, change roles, or leave the company, access permissions should be reviewed and adjusted accordingly.

Not Sure Who Has Access to Your Business Systems?

We can help review user accounts, identify unnecessary access, and implement secure account management practices that improve visibility and reduce risk.

From Microsoft 365 account reviews to access control policies and multifactor authentication deployment, we help small businesses maintain secure and organized technology environments that support long-term growth.

ISSUE 034
May 2026
Independence, Missouri

WHY SMALL BUSINESSES SHOULD TAKE SOFTWARE UPDATES SERIOUSLY

For many small businesses, software updates are often viewed as an inconvenience. Notifications appear during busy workdays, devices request restarts at inconvenient times, and employees may postpone updates simply to avoid interruptions.

At first glance, delaying an update may not seem like a major issue. If systems are still functioning properly, many businesses assume there is little urgency to install the latest patches or upgrades immediately.

However, software updates play a much larger role than most people realize. Behind the scenes, updates help fix security vulnerabilities, improve performance, address software bugs, and maintain compatibility with modern applications and services. Without regular updates, devices and systems gradually become more vulnerable, less reliable, and harder to support.

Much like routine maintenance on a vehicle, software updates help prevent larger problems from developing over time. While skipping a single update may not cause immediate issues, repeatedly delaying updates can quietly introduce significant risks throughout a business environment.

The Reality of Modern Cyber Threats

Cybercriminals actively search for outdated systems that contain known vulnerabilities. In many cases, attackers do not need to create entirely new attack methods. Instead, they take advantage of weaknesses that software vendors have already identified and released fixes for.

Once a vulnerability becomes publicly known, businesses that fail to install updates may become easy targets.

This is especially dangerous for small businesses because outdated devices often remain connected to email systems, cloud platforms, financial software, and sensitive customer information. A single unpatched system can sometimes create an entry point that impacts an entire network.

Operating systems, web browsers, firewalls, business applications, and even printers regularly receive security updates designed to close vulnerabilities and improve protection. Without these updates, businesses may unknowingly leave systems exposed long after security flaws have already been discovered.

The Business Impact Beyond Security

Software updates do more than improve cybersecurity. They also help maintain overall performance and reliability.
Outdated software can lead to slow systems, application crashes, compatibility problems, and unstable performance. Employees may experience issues opening files, connecting to cloud services, joining meetings, or accessing business applications efficiently.

Over time, these small frustrations can reduce productivity and create unnecessary downtime.

Compatibility is another growing concern. Modern software platforms frequently evolve, and older systems may eventually lose support for newer tools and integrations. Businesses that fall too far behind on updates may discover that critical applications no longer function properly or become increasingly difficult to maintain.

How Update Problems Develop Over Time

Most update-related issues develop gradually rather than all at once.
An employee postpones a restart because they are busy. A workstation misses several update cycles. Older software versions remain in use because “everything still works.” Temporary delays slowly become long-term neglect.

Over time, systems throughout the organization begin operating at different patch levels with inconsistent security protections.
This creates an environment where vulnerabilities become harder to track and manage.

Many businesses also struggle with updates because they lack centralized visibility into which devices are current and which systems may be falling behind.
Without proper oversight, outdated systems can remain unnoticed for months or even years.

What Proper Update Management Should Look Like

Effective update management requires consistency, planning, and visibility. Businesses should ensure that operating systems, business applications, antivirus platforms, firewalls, and firmware are all reviewed and updated regularly.
Automatic updates can help simplify this process, but they should still be monitored to ensure updates are installing properly and not creating unexpected issues.

Businesses should also:

- Replace unsupported software and operating systems
- Schedule maintenance windows for updates and restarts
- Review devices regularly for missing patches
- Test critical updates when necessary
- Maintain backups before major upgrades

Employee awareness is equally important. Users should understand why updates matter and avoid repeatedly postponing security patches simply for convenience. When properly managed, updates become part of a proactive IT strategy rather than a reactive response to problems.

The goal is not just to install updates—it is to maintain a stable, secure, and reliable technology environment that supports the business long-term.

Planning for Long-Term Technology Health

As technology continues evolving, maintaining updated systems becomes increasingly important for both security and operational efficiency.

Businesses that stay current with updates are often better positioned to adopt new technologies, maintain compatibility with modern applications, and reduce unexpected downtime.

In contrast, businesses that consistently delay updates may eventually face larger problems that require costly emergency upgrades, system replacements, or recovery efforts.

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 May's question of the month:

What is a risk of using AI when working?