ISSUE 029
December 2025
Independence, Missouri

FCS TECH TALK

Your Trusted Technology Partner Since 1989

INSIDE THIS ISSUE:

WHY THE NEW YEAR IS THE IDEAL TIME FOR SMALL BUSINESSES TO IMPLEMENT CYBER SECURITY CHANGES

The beginning of a new year is often associated with fresh starts, renewed focus, and long-term planning.

For small business owners, it's a time to review what worked, what didn't, and what needs improvement. While goals like increasing revenue, improving customer experience, or expanding services are common, cyber security is frequently overlooked. Yet, in today's increasingly digital business environment, strengthening cyber security should be one of the most important priorities at the start of the year.

Cyber threats continue to grow in scale, sophistication, and impact. Small businesses are no longer operating under the radar. The new year offers the perfect opportunity to take a proactive approach to cyber security—before an incident forces reactive and costly decisions.

A Strategic Reset Point for Small Business

The new year naturally aligns with business planning cycles. Budgets are reviewed, processes are reassessed, and strategic goals are set. This makes it the ideal time to evaluate your existing cyber security measures and identify gaps. Many small businesses operate with systems that have evolved organically over time—new software added here, remote access enabled there—often without a comprehensive security plan.

Starting fresh allows business owners to step back and ask critical questions:

- Are our systems up to date and supported?
- Who has access to sensitive data, and is it appropriate?
- Are our backups reliable and regularly tested?
- Do we have clear policies for handling security incidents?

Addressing these questions early in the year helps cyber security become part of the overall business strategy rather than a rushed response to a breach later on.

Small Businesses Are Prime Targets

One of the most dangerous myths in cyber security is the belief that cybercriminals only target large corporations. In reality, small businesses are often seen as easy targets. Attackers know that smaller organizations typically have fewer resources, limited IT support, and less formal security controls. Automated attacks, such as phishing emails and ransomware campaigns, do not discriminate by business size.

In many cases, cybercriminals specifically seek out small businesses because a single successful attack can yield financial gain, customer data, or access to larger supply chains. Implementing stronger cyber security measures at the start of the year significantly reduces the likelihood of falling victim to these common attacks.

Establishing Strong Security Habits from Day One

Cyber security is not a one-time project—it is an ongoing practice. The new year is the perfect time to establish consistent habits that will carry through the months ahead. This includes:

- Enforcing strong password and multi-factor authentication policies
- Scheduling regular software and system updates
- Implementing routine data backups and testing recovery processes
- Providing ongoing cyber security awareness training for employees

When these practices are introduced early and communicated clearly, they become part of the company culture. Employees are more likely to take security seriously when it is positioned as a core business value rather than a temporary initiative.

Employee Awareness: A Critical First Line of Defense

Human error remains one of the leading causes of security incidents. Phishing emails, social engineering attacks, and compromised credentials often succeed because employees are unaware of the risks or unsure how to respond. The new year is an excellent time to refresh or introduce employee training programs. Cyber security training does not need to be overly technical. Simple education on recognizing suspicious emails, protecting passwords, reporting incidents, and safely handling data can dramatically reduce risk.

Making this training part of the new year onboarding or annual review process reinforces accountability and shared responsibility.

Protecting Customer Trust and Brand Reputation

Trust is one of the most valuable assets a small business has. Customers expect that their personal and financial information will be protected. A data breach—no matter the size—can severely damage that trust and lead to customer loss, negative publicity, and long-term reputational harm.

Starting the year by strengthening cyber security sends a clear message to customers, partners, and stakeholders that your business takes data protection seriously. This is especially important for businesses handling payment information, personal records, or confidential client data.

In many industries, demonstrating strong cyber security practices can also be a competitive advantage.

Cost Control Through Prevention

Cyber incidents are expensive. The costs can include system downtime, lost productivity, data recovery, legal fees, regulatory penalties, and reputational damage. For small businesses, even a short period of downtime can be financially devastating.

Implementing cyber security improvements at the beginning of the year allows businesses to plan costs in advance and spread investments strategically.

Preventative measures—such as security software, managed services, or professional assessments—are often far more affordable than recovering from a breach. A proactive approach helps control expenses and reduces financial uncertainty throughout the year.

Supporting Business Growth and Digital Transformation

Many small businesses plan to grow in the new year by adopting new technologies. Cloud platforms, remote work tools, e-commerce systems, and digital customer engagement tools offer tremendous benefits—but they also introduce new security risks if not properly managed.

By strengthening cyber security at the start of the year, businesses create a secure foundation that supports growth. This ensures that as new tools and systems are introduced, they are protected from the outset. Cyber security becomes an enabler of growth rather than a barrier or afterthought.

Meeting Compliance and Regulatory Expectations

Depending on the industry, small businesses may be subject to data protection laws and regulations. Even if formal compliance is not required, customers and partners increasingly expect responsible data handling. The new year provides a natural timeline to review compliance requirements, update policies, and document cyber security practices.

Having clear cyber security policies in place—such as data handling procedures, incident response plans, and access controls—helps reduce legal risk and demonstrates due diligence if an incident does occur.

Creating a Proactive and Prepared Environment

Instead of waiting for something to go wrong, businesses take ownership of their risk and prepare for potential threats. This resilience not only protects systems and data but also gives business owners peace of mind.

A proactive cyber security approach allows leaders to focus on innovation, customer service, and growth—confident that their digital assets are protected.

In an environment where cyber threats are constant and evolving, starting the year with stronger cyber security is not just a smart move—it is an essential investment in the long-term success and stability of your small business.

TL;DR

The new year provides an ideal opportunity for small businesses to review and strengthen their cyber security as part of annual planning, budgeting, and goal-setting. Despite common misconceptions, small businesses are frequent targets for cyber attacks, often because they lack formal security measures. Implementing cyber security improvements early in the year helps reduce risk, prevent costly disruptions, protect customer data and trust, and build strong security habits across the business. A proactive approach also creates a secure foundation that supports growth, new technology adoption, and long-term business resilience.

ISSUE 029
December 2025
Independence, Missouri

THIS MONTH'S PRODUCT SPOTLIGHT

CLICK TO VIEW A SHORT VIDEO!

ADVANCED EMAIL PROTECTION

WHAT 2025 TAUGHT US ABOUT AI FOR SMALL BUSINESSES

2025 was a pivotal year for artificial intelligence, and small businesses learned that AI is no longer a futuristic concept—it's a practical tool that can transform operations, customer engagement, and decision-making. From automating routine tasks to offering data-driven insights, AI has become an essential part of running a modern small business.

AI Streamlines Daily Operations

One of the clearest lessons of 2025 is that AI can save time and reduce errors by handling repetitive tasks. Small business owners who implemented AI discovered that chatbots could answer customer questions 24/7, AI-powered scheduling tools could manage appointments, and automated marketing systems could optimize campaigns without constant human oversight. By delegating these tasks to AI, teams were able to focus on higher-level strategy and growth initiatives.

Data-Driven Decisions Made Simple

Small businesses often feel overwhelmed by data, but AI in 2025 helped make sense of it. Even companies with modest datasets could benefit from predictive analytics to forecast demand, identify customer trends, and make inventory decisions more efficiently. AI tools helped translate raw numbers into actionable insights, allowing small businesses to respond faster to market changes and make smarter choices without needing a full analytics team.

Enhancing Customer Experience

AI proved to be a powerful tool for personalizing interactions with customers. Automated email campaigns, product recommendations, and follow-ups became smarter and more targeted. Customers received timely offers and relevant information, creating a sense of personal attention that was previously difficult for small businesses to scale. AI allowed small businesses to compete with larger competitors by delivering professional, tailored experiences at a fraction of the cost.

Security and Ethical Use Matter

With AI tools accessing sensitive customer and business data, 2025 highlighted the importance of cybersecurity and ethical use. Small businesses that integrated AI responsibly—implementing strong data protection measures and complying with privacy standards—reaped the benefits while avoiding risks. Ensuring that AI tools are secure and transparent is crucial for maintaining customer trust and protecting business reputation.

Start Small, Scale Smart

Another key takeaway from 2025 is the importance of gradual implementation. Small businesses that began with simple AI applications, such as automating a single workflow or using AI to analyze marketing campaigns, were better positioned to expand later. By testing, refining, and scaling incrementally, businesses could maximize benefits while minimizing disruption.

THE MOST USED KEYS ON A KEYBOARD IN 2025

In 2025, usage patterns reflect not only traditional typing habits but also the rise of digital communication, coding, and AI-assisted tools. While every key has its purpose, some keys dominate daily use more than others.

Top Alphanumeric Keys

The letters E, A, R, I, O, T, N, and S remain the most frequently typed letters in English, a pattern consistent for decades. On the numeric side, keys like 1, 0, and 5 see the most action, largely due to online forms, passwords, and spreadsheet work.

Modifier and Functional Keys

With increased reliance on shortcuts and productivity software, Shift, Ctrl (or Cmd on Mac), and Alt have become essential. Users employ these keys constantly for copy-paste commands, text formatting, and navigating software efficiently.

The Enter/Return key is another heavy hitter, reflecting both coding activity and the constant flow of messaging apps, email, and document editing.

Impact of AI and Automation

Interestingly, AI-powered writing assistants and automated text tools have slightly shifted key usage. While overall typing volume may decrease in some industries, shortcuts and functional keys are now used more frequently to activate tools, auto-fill, and implement AI-driven commands.

Conclusion

In 2025, the most used keyboard keys reflect a combination of traditional typing habits and modern digital workflows. Letters like E, A, R, I, O, functional keys like Enter, Shift, Ctrl, and navigation keys such as Backspace and Tab remain central to how people interact with technology every day.

As AI and new input methods continue to shape productivity, key usage patterns will likely evolve further in the coming years.

2025: A DEFINING YEAR FOR DATA BREACHES IN THE U.S. ESPECIALLY FOR SMALL BUSINESS

As 2025 wraps up, data breaches in the United States once again highlighted the pervasiveness and persistence of cyber threats. Breaches affected millions of Americans across industries, with digital attackers continuing to refine their tactics—from phishing to supply-chain compromises to ransomware. While much of the media spotlight often falls on large corporations and major institutions, small businesses were hit particularly hard this year, underscoring the reality that cyber risk does not discriminate by size.

Widespread Breach Activity Across Multiple Sectors

According to mid-year data, the U.S. experienced a significant rise in reported breaches in 2025 compared to 2024, with more than 1,700 publicly disclosed data compromise incidents in the first half of the year alone.

Healthcare continued to be a high-impact sector, with over 66 reported incidents affecting more than 7 million people in June alone—including a major breach that affected over 5.4 million individuals. Beyond healthcare, breaches spanned finance, technology, education, and government systems, with personal data such as names, email addresses, physical addresses, and in some cases highly sensitive details exposed or stolen.

Small Businesses: Out Front of the Target List

While large data breaches make headlines, the bulk of breach activity in 2025 impacted small businesses. Recent analysis found:

- 71% of data breaches occurred at businesses with fewer than 250 employees, with companies under 10 employees accounting for nearly a quarter of incidents.

This disproportionate impact on small organizations reflects systemic gaps in basic cyber defenses, limited IT resources, and a lack of dedicated security staff—making small firms comparatively easy targets. As a result:

- Small business breaches often exposed employee and customer contact information, business financial records, and internal operational data.
- The cost of breach recovery—lost revenue, legal fees, remediation, and reputational harm—frequently surpassed $50,000 per incident and in many cases far more.

Evolving Attack Techniques and Growth in AI-Driven Threats

2025 saw attackers increasingly use AI-assisted methods to enhance traditional breach vectors such as phishing, business email compromise (BEC), and social engineering. Reports indicate that AI-generated phishing campaigns have become more sophisticated and harder to detect, leading to higher breach success rates.
Patterns from breach investigations this year also revealed:

- Supply-chain attacks targeting vulnerabilities in third-party tools and service providers, enabling attackers to compromise many organizations at once.
- Credential theft and social engineering remaining dominant methods for initial access.

Legal and Regulatory Repercussions Grow

An emerging storyline in 2025 has been the surge in litigation following breach disclosures. Class action and regulatory actions increasingly aimed at both large organizations and smaller firms accused of failing to adequately protect customer data.
The threat of legal liability has become a catalyst for many small businesses to rethink their data protection strategies, but too often only after a breach occurs.

What This Means for Small Businesses Going Into 2026

The data from 2025 makes one thing clear: small businesses are prime targets in the modern cyber threat landscape. Factors driving this include:

- Limited cybersecurity budgets and staffing
- Use of outdated technology and insecure configurations
- Insufficient employee training on phishing and social engineering threats
- Lack of robust backup and recovery plans

Building a More Resilient 2026

Data breaches in 2025 reinforced a difficult truth: no business—large or small—is immune from cyber risk.

As we move into 2026, the lessons of 2025 should serve as a call to action—for business owners, leaders, and policymakers alike—to elevate cyber security from an afterthought to a core business priority.

ISSUE 029
December 2025
Independence, Missouri

WHAT'S NEXT FOR MICROSOFT IN 2026: AI, PRODUCTS, PRICING, AND PLATFORM SHIFTS

As 2026 approaches, Microsoft is preparing for a year of significant transformation across products, services, and its overall business strategy. Following major initiatives in 2025, the company is doubling down on artificial intelligence (AI), security, cloud adoption, and platform modernization. These changes will affect individual users, enterprises, and small businesses alike.

AI Integration Across Products

Artificial intelligence is at the center of Microsoft's roadmap for 2026. AI features are expected to become deeply embedded across all major platforms, including Microsoft 365, Azure, Windows, and developer tools. Unlike the AI capabilities of previous years, which primarily assisted with automation and productivity, the 2026 push emphasizes more autonomous, context-aware AI agents.

These AI agents will help users:

- Draft and edit content with advanced language models.
- Automate data management, analysis, and reporting.
- Identify potential cybersecurity threats and recommend responses.
- Optimize workflows across Microsoft Teams, Office apps, and cloud services.

This expansion signals Microsoft's intent to make AI a core productivity tool, not just an add-on feature. Businesses adopting these tools can expect efficiency gains, while also needing to evaluate the security and privacy implications of AI usage.

Microsoft 365: Pricing, Features, and Security Enhancements

2026 will bring notable changes to Microsoft 365. New AI-powered features will be integrated across business and enterprise plans, including:

- Enhanced document and spreadsheet automation.
- AI-driven insights for email and calendar management.
- Advanced cybersecurity protections, such as phishing detection, malicious link scanning, and behavioral anomaly alerts.

Alongside these feature expansions, Microsoft is raising prices for many commercial plans. The increases are intended to reflect the added AI and security capabilities. Businesses, particularly small and medium-sized companies, will need to evaluate whether the added tools justify the higher subscription costs.

These changes also reflect a trend toward bundling productivity and security, making Microsoft 365 not just a collaboration suite but a platform for safer, more efficient business operations.

Platform and Product Transitions

Several platforms and legacy services are slated for retirement or transformation in 2026:

- Windows 11 SE, Microsoft's education-focused OS, will reach end-of-support, prompting schools and educational institutions to transition to mainstream Windows 11 editions.
- Legacy authentication and integration tools, including some SharePoint Add-Ins and Azure ACS components, will be phased out, encouraging organizations to adopt modern cloud identity solutions like Microsoft Entra ID.
- Enterprise products such as Windows Server 2022 and Office LTSC 2021 for Mac will see shifts from mainstream support to extended support, requiring IT teams to plan migrations carefully.

These moves align with Microsoft's strategy of consolidating its ecosystem around cloud-optimized, secure, and AI-ready platforms.

Security Enhancements and Hardware Integration

Security remains a key focus for Microsoft in 2026. Notable improvements include:

- Hardware-accelerated encryption for BitLocker, improving both performance and resistance to low-level attacks.
- Integration of advanced threat protection directly into Microsoft 365 and Windows, allowing real-time detection of phishing, malware, and suspicious account activity.
- Enhanced identity protection through multi-factor authentication, conditional access policies, and AI-driven login risk assessments.

These updates reinforce Microsoft's positioning of security as a built-in feature rather than a separate product, reducing the burden on IT departments, particularly in smaller organizations.

AI and Cloud Services Growth
Azure continues to expand as Microsoft's primary cloud platform, with a strong focus on AI-driven services.

Businesses can expect:

- Improved developer tools for building AI applications.
- Increased adoption of AI-powered analytics and business intelligence.
- Expanded compliance and data protection features to meet regulatory demands in healthcare, finance, and government sectors.

These investments in AI and cloud integration position Microsoft to compete with other major tech firms while offering small businesses scalable tools for digital transformation.

Workplace Policies and Collaboration
Microsoft is also refining its workplace culture in 2026:

- Updated remote and hybrid work policies aim to balance flexibility with collaboration.
- Enhanced Microsoft Teams features will support project management, AI-assisted meeting summaries, and automated task tracking.
- Training and adoption programs for AI and security tools will become more widespread, helping employees use Microsoft products effectively and safely.

2026 is shaping up to be a pivotal year for Microsoft, with AI, security, and cloud services at the forefront of its strategy. Businesses, IT professionals, and end users will need to adapt to changes in pricing, product support, and new feature adoption to fully leverage Microsoft's evolving ecosystem.

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 December's question of the month:

Are Small Businesses more or less likely to be targeted by a cyber attack?