ISSUE 030
January 2026
Independence, Missouri

FCS TECH TALK

Your Trusted
Technology Partner Since 1989

INSIDE THIS ISSUE:

WHY "WE'VE NEVER BEEN HACKED" IS ONE OF THE MOST DANGEROUS ASSUMPTIONS IN IT

Many business owners feel confident about their technology because nothing bad has happened—at least not that they are aware of. "We've never been hacked" is a phrase we hear often, and on the surface, it sounds reassuring. Unfortunately, this assumption can create a false sense of security that leaves businesses more vulnerable than they realize.

The reality is that most cyber incidents do not look like dramatic system failures or obvious ransomware screens. Modern attacks are designed to be quiet, persistent, and difficult to detect. In many cases, organizations are compromised for weeks or months before anyone realizes something is wrong.

What "Being Hacked" Actually Looks Like Today

When people think of a cyberattack, they often imagine locked computers, flashing warnings, or complete system shutdowns. While those incidents do occur, they are not the most common form of compromise today. Many successful attacks involve stolen credentials, unauthorized email access, or subtle changes that blend into normal business activity.

An attacker may log into an email account using a stolen password and quietly monitor conversations. They may set up email forwarding rules, harvest contact lists, or wait for the right opportunity to impersonate an employee or vendor. From the outside, everything looks normal. Email still works. Files are still accessible. No alarms go off.

Because the signs are subtle, businesses often conclude nothing is wrong—until financial loss, data exposure, or reputational damage forces the issue.

Why Most Breaches Go Undetected at First

Small and mid-sized businesses rarely have continuous security monitoring in place. Without active oversight, there is nothing watching for suspicious logins, unusual email behavior, or abnormal access patterns.

Attackers understand this. They know that many organizations rely on default configurations and reactive alerts. As a result, modern attacks are designed to avoid triggering obvious warnings. A login from a new location, an inbox rule quietly redirecting messages, or a compromised account sending only a handful of emails per day may not raise immediate concern.

By the time a breach is discovered, attackers may have already achieved their goal—whether that is financial fraud, data theft, or gaining a foothold for future attacks.

The Cost of Assuming Everything Is Fine

The belief that "nothing has happened" often delays important security improvements. Businesses may postpone updates, advanced protections, or monitoring because there appears to be no urgency. Unfortunately, this creates an environment where attackers face little resistance.

When an incident finally becomes visible, the impact is often much greater than it would have been with earlier detection. Recovery costs increase, investigations take longer, and trust—both internal and external—can be damaged.

In many cases, the most expensive part of a breach is not the technical recovery, but the downtime, lost productivity, and disruption to normal operations.

Common Blind Spots in Small Business IT

Several factors contribute to why businesses believe they are safe when they may not be. Email systems are often trusted by default, even though they are the most common entry point for attackers.

User access tends to grow over time without regular review, creating unnecessary exposure. Security alerts, if they exist at all, may be ignored or misunderstood.

Another major blind spot is assuming that security tools alone are enough. Technology is critical, but without proper configuration, monitoring, and ongoing management, even good tools can leave gaps. Security is not a one-time setup—it is an ongoing process that must evolve as threats change.

Why Detection Matters More Than Ever

Preventing attacks is important, but detection is equally critical. No environment is immune to risk, and even well-protected systems can experience attempted compromises. The difference between a minor incident and a major disruption often comes down to how quickly the issue is identified and addressed.

Early detection can stop an attacker before damage occurs. It can prevent fraudulent emails from spreading, stop unauthorized access, and protect sensitive information. Without visibility, businesses are left reacting after the fact.

This is why proactive monitoring has become such a vital part of modern IT management.

The Risk of Relying on Confidence Instead of Evidence

Confidence in your technology should be based on evidence, not assumptions. Knowing that systems are being monitored, access is reviewed, and suspicious activity is investigated provides real assurance. Simply believing that nothing has happened does not.

Cybersecurity is not about fear—it is about awareness and preparedness. The goal is not to expect the worst, but to be ready if something does occur.

Shifting from Reactive to Proactive IT

Many organizations only address IT issues after something breaks. While this approach may seem cost-effective in the short term, it often leads to higher long-term risk and expense. Proactive IT focuses on prevention, visibility, and continuous improvement.

This mindset shift allows businesses to identify weaknesses before they are exploited, respond faster to issues, and make informed decisions about their technology.

Building Resilience Instead of False Security

True security is not defined by the absence of known incidents. It is defined by resilience—the ability to prevent, detect, and respond effectively. Businesses that invest in visibility, layered protection, and proactive management are better positioned to handle threats, even as they evolve.

The most dangerous assumption in IT is believing that silence means safety. Asking the right questions, reviewing security regularly, and maintaining active oversight are what truly protect a business in today's threat landscape.

Perhaps most importantly, resilience is ongoing. Threats evolve, technology changes, and businesses grow. Security must be reviewed regularly, adjusted as needed, and treated as a living part of the organization—not a one-time project. Regular reviews, testing, and improvement ensure that protections remain effective as the environment changes.

The goal of modern IT security is not to promise that nothing will ever happen. That promise cannot be realistically made. The goal is to ensure that when something does happen, it is detected early, handled professionally, and resolved with minimal impact.

Businesses that focus on resilience rather than assumptions are better positioned for long-term stability. They operate with confidence rooted in awareness, preparation, and control—not in the dangerous belief that "we've never been hacked, so we must be safe."

TL;DR

Many businesses assume they are secure because they haven't experienced an obvious cyber incident, but modern attacks are often silent and go undetected for long periods. Small businesses are frequent targets because attackers know security and monitoring are often limited. Real protection comes from proactive monitoring, layered security controls, and having a clear response plan in place—not from relying on the belief that "nothing has happened."

THIS MONTH'S PRODUCT SPOTLIGHT

CLICK TO VIEW A SHORT VIDEO!

SECURITY AWARENESS TRAINING

- Engaging Monthly Video Training
- Relevant Topics for Real World Threats
- Quick and Easy to Follow Material

WHY EMPLOYEE MISTAKES ARE NORMAL—AND HOW TO REDUCE THE RISK

When cybersecurity incidents happen, the first reaction is often to look for someone to blame. In reality, most security issues don't occur because employees are careless or irresponsible. They happen because modern cyberattacks are designed to exploit normal human behavior.

Attackers rely on urgency, trust, and familiarity. A convincing email that appears to come from a manager, vendor, or customer can prompt even the most cautious employee to click a link or respond quickly. These attacks are intentionally crafted to look legitimate and often arrive during busy moments when people are focused on getting work done.

It's important for businesses to understand that employee mistakes are not a failure of character—they are a predictable part of how humans interact with technology. Expecting perfection from employees is unrealistic, especially when attackers are constantly refining their techniques.

This is why training alone is not enough. Security awareness education plays a critical role in helping employees recognize suspicious activity, but even well-trained users can be fooled by advanced phishing emails or social engineering attempts. The goal of training is not to eliminate mistakes entirely, but to reduce their frequency and ensure employees know how to respond quickly when something feels off.

Technology must act as a safety net. Strong email filtering, multi-factor authentication, and endpoint protection help stop threats before employees ever see them. When a malicious message slips through, these layered controls can prevent a single click from turning into a major incident. This approach acknowledges human error while limiting its impact.

Creating a security-aware culture also makes a significant difference. Employees should feel comfortable reporting suspicious emails or unusual activity without fear of blame.

Quick reporting allows issues to be investigated and contained early, often before any damage occurs. When security is treated as a shared responsibility rather than a disciplinary issue, employees become part of the defense instead of a perceived risk.

Reducing cybersecurity risk is about designing systems that assume mistakes will happen and preparing for them accordingly. Businesses that combine employee awareness with strong technical protections are far more resilient than those relying on one approach alone.

By recognizing that mistakes are normal—and planning for them—small businesses can significantly reduce their exposure to cyber threats while empowering employees to work confidently and securely.

HOW TO AUTOMATE SIMPLE REPETITIVE TASKS

Small business owners often spend more time on repetitive tasks than they realize. Email follow-ups, scheduling reminders, or copying data between systems can eat hours out of your week. The good news is that many of these tasks can be automated—without hiring extra staff or buying complicated software.

Email

One of the easiest ways to start is with email rules. Most email clients, including Outlook and Gmail, allow you to automatically sort incoming messages, flag important contacts, or move messages into folders. For example, you can automatically send invoices to a "Finance" folder or flag emails from key clients for quick attention.

Calendar

Calendar automation is another simple win. Set recurring reminders for meetings, deadlines, or client follow-ups so you don't have to manually track them. Many calendar apps can also auto-suggest meeting times or send reminders to attendees, saving you coordination time.

Spreadsheets

For spreadsheet or data entry tasks, look for built-in macros or templates. Even a small macro that formats data or imports customer info automatically can save significant effort each week.

Recap

The key is to start small and focus on high-impact tasks. Identify the tasks you do most frequently and look for built-in automation tools you already have. By automating just a few daily or weekly tasks, you can free up time for strategy, growth, and client care—while reducing errors and stress.

WHAT 2025 TAUGHT US ABOUT CYBER SECURITY FOR SMALL BUSINESSES

Looking back on 2025, one thing became clear: cyber security was no longer a concern reserved for large enterprises. Throughout the year, cyber threats continued to grow in volume and sophistication, and small businesses felt the impact more than ever. The lessons from 2025 reinforced why cyber security must be treated as a core business responsibility.

Important Takeaways

One of the most important takeaways from the year was how dramatically cyber attacks evolved. Attackers increasingly relied on automation and AI-assisted tools to scale phishing campaigns, impersonation attempts, and credential theft. These attacks moved faster, appeared more convincing, and were harder to detect than in previous years. For many small businesses, even well-written or familiar-looking emails proved to be malicious.

Another lesson from 2025 was that being "too small to target" was a dangerous misconception. Attackers consistently focused on small and mid-sized businesses because they often lacked dedicated security staff, advanced monitoring, and formal response plans. Automated attacks did not discriminate by size, and a single successful breach was often enough to expose financial data, customer information, or internal systems.

Importance of Visibility and Detection

The year also underscored the importance of visibility and detection. Many organizations discovered incidents weeks or even months after the initial compromise. During that time, attackers were able to monitor email conversations, collect sensitive information, and attempt fraudulent transactions. These incidents made it clear that prevention alone was not enough—businesses needed the ability to detect unusual activity and respond quickly before damage escalated.

Legal and regulatory pressure increased throughout 2025 as well. More organizations faced lawsuits, regulatory scrutiny, and contractual disputes following breach disclosures. Many businesses learned that having "basic security" in place did not eliminate risk. Misconfigurations, weak controls, and insufficient protections often resulted in serious legal and financial consequences, making cyber security a business risk—not just an IT issue.

Employee Impact to Cyber Security

Employee behavior remained a critical factor in many of the year's incidents. Phishing and social engineering continued to be leading causes of breaches despite increased awareness. This reinforced an important reality: people will make mistakes. Security strategies that acknowledged human error—and were designed to limit its impact—proved far more effective than those relying on training alone.

There was a large surge in the efforts of Small Businesses implementing SAT (Security Awareness Training) which has been proven to drastically reduce the number of "human error" mistakes that can lead to a cyberattack.

Importance of Resilience

Perhaps the most valuable lesson of 2025 was the importance of resilience. No system proved immune to attack, but businesses that layered their security, monitored activity, maintained reliable backups, and prepared response plans were far better positioned to recover. These organizations experienced less downtime, lower costs, and significantly less disruption.

Having a good plan is only part of the equation. The other half is the ability to adapt and continue to improve. Businesses that took action to improve weaknesses and implement new strategies as new threats occur became even more prepared for a potential cyberattack.

Final Thoughts

As businesses moved into 2026, the takeaway from 2025 was not fear—it was preparation. Cyber security was no longer something that could be "set and forgotten." It required ongoing attention, regular review, and a proactive mindset.

Small businesses that carried these lessons forward entered 2026 more resilient, better protected, and better prepared for the evolving threat landscape.

WHAT SMALL BUSINESSES NEED TO KNOW ABOUT MICROSOFT LICENSING CHANGES

Microsoft’s licensing structure has always been complex, and 2026 brings several updates that small businesses need to understand. Between new pricing adjustments, added AI features, and bundled security tools, these changes can directly impact budgets, IT planning, and how businesses use Microsoft 365. Staying informed is critical to maximize value and avoid paying for features your company doesn’t need—or missing out on essential capabilities.

Business vs. Enterprise Plans

One of the first considerations for small businesses is understanding the difference between Microsoft’s Business and Enterprise plans. Business plans are designed for companies with fewer than 300 employees and include core productivity apps such as Word, Excel, and Teams. Enterprise plans, meanwhile, are tailored for larger organizations and include additional security, compliance, and analytics features.

In 2026, Microsoft is further distinguishing these tiers. Many of the newly integrated AI features—like Copilot in Word, Excel, and Teams—are initially being added to Enterprise plans, with Business plans receiving a delayed rollout. Small businesses need to carefully evaluate whether upgrading to an Enterprise plan is worth the additional cost or if they can achieve similar efficiency gains through add-on options.

AI and Security Add-Ons

Microsoft is bundling more AI-driven tools and advanced security features directly into Microsoft 365 subscriptions. While this adds significant value, it also increases pricing for commercial licenses. For example, AI-powered analytics, automated meeting summaries, and advanced threat protection now come as part of higher-tier plans or optional add-ons.

Small businesses must decide which capabilities are critical to daily operations. AI features can significantly improve productivity, but if your organization isn’t ready to adopt them, it may be more cost-effective to stick with core plans while monitoring rollout schedules for future adoption.

Price Increases and Cost Management

Price adjustments are a key part of Microsoft’s 2026 licensing updates. Some small businesses may notice a 10–15% increase in annual subscription fees depending on the plan and add-ons. These increases reflect the added AI and security capabilities, but they can strain tight IT budgets if not anticipated.

To manage costs, businesses should:

- Review existing Microsoft 365 licenses and identify unused features
- Consolidate users onto the most appropriate plan tier
- Evaluate third-party tools vs. built-in Microsoft functionality
- Plan for phased adoption of new features to spread expenses
-

Proactive license management can prevent overpaying while ensuring all users have access to the tools they need.

Legacy Licensing and Transition Planning

Another important consideration for small businesses is legacy Microsoft licenses. Many organizations are still using older perpetual licenses like Office 2019 or Office LTSC, which do not include the latest AI or security enhancements. As Microsoft phases out support for older platforms, businesses may face additional migration costs or compatibility challenges.

Planning early ensures a smooth transition to subscription-based Microsoft 365 plans without disrupting daily operations. IT teams should inventory existing licenses, identify expiration dates, and map business needs to current Microsoft offerings.

Security and Compliance Implications

Licensing changes also affect security and compliance. Enterprise plans and certain Business tiers now include enhanced threat detection, phishing protection, and conditional access features. Missing out on these tools can leave small businesses vulnerable to attacks and regulatory issues.

We can help to ensure licensing aligns with security policies, including multi-factor authentication, secure email filtering, and backup solutions. Proper license alignment can turn Microsoft 365 into both a productivity and a security platform, reducing reliance on multiple third-party tools.

Practical Steps for Small Businesses

To navigate Microsoft’s licensing changes effectively, small businesses should consider the following steps:

1. Audit Current Licenses – Understand who has what license, and which features are actually being used.
2. Evaluate Feature Needs – Identify AI, security, and collaboration features that will add real value.
3. Plan for Migration – If using older versions, schedule upgrades or transitions to subscription plans in advance.
4. Budget for Increases – Factor in price changes and optional add-ons when planning 2026 IT budgets.
5. Engage Your MSP – Work with IT professionals to align licenses with business goals, avoid overpaying, and implement best practices for security and productivity.

Conclusion

Microsoft’s licensing updates in 2026 reflect the company’s broader strategy of integrating AI, advanced security, and productivity tools into its subscription ecosystem. For small businesses, these changes are both an opportunity and a challenge.

By understanding plan tiers, evaluating feature needs, and planning migrations carefully, businesses can optimize Microsoft 365 investments while ensuring employees have the tools needed to work efficiently and securely.

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 January's question of the month: True or False?

All Cyberattacks are noticeable