ISSUE 032
March 2026
Independence, Missouri

FCS TECH TALK

Your Trusted Technology Partner Since 1989

INSIDE THIS ISSUE:

THE RISK OF WEAK IDENTITY SECURITY: WHY PASSWORDS ALONE ARE NO LONGER ENOUGH

The Illusion of Security

For many small businesses, passwords have long been considered a sufficient method of protecting systems and data. A strong password policy, periodic updates, and basic user discipline have traditionally been viewed as adequate safeguards. On the surface, this approach feels reasonable. Employees are trusted, systems appear secure, and daily operations continue without disruption.

However, the modern threat landscape has evolved significantly. Attackers are no longer relying solely on technical vulnerabilities. Instead, they are targeting identity—specifically the credentials that grant access to business systems. This shift has made passwords alone an increasingly unreliable form of protection.

Much like shared passwords, weak identity security often fails quietly. There is rarely an immediate indication that credentials have been compromised. Unauthorized access can occur without triggering alarms, allowing attackers to operate undetected for extended periods.

The Reality of Credential-Based Attacks

Today's cyberattacks frequently begin with valid login credentials. Phishing emails, credential harvesting websites, and data breaches all contribute to a growing pool of exposed usernames and passwords. Attackers use these credentials in automated attempts across multiple platforms, often gaining access without needing to exploit software vulnerabilities.

This approach is effective because it bypasses traditional security measures. Firewalls, antivirus software, and endpoint protections are designed to stop malicious activity—not legitimate logins. When an attacker signs in using valid credentials, they can appear indistinguishable from an authorized user.

This is especially dangerous in cloud-based environments, where access to email, file storage, financial systems, and collaboration tools is centralized under a single identity. A compromised account can quickly become a gateway to multiple critical systems.

The Business Impact Beyond IT

The consequences of weak identity security extend far beyond technical concerns. A compromised email account can be used to manipulate vendor communications, redirect payments, or send fraudulent messages to clients. Access to internal systems can lead to data exposure, operational disruption, and reputational damage.

In many cases, the financial impact of these incidents is significant. Unlike ransomware attacks, which are highly visible, identity-based attacks often go unnoticed until after damage has occurred. By the time the issue is identified, funds may already be transferred, or sensitive information may already be exposed.

Additionally, businesses may face compliance challenges if they are unable to demonstrate proper access controls and accountability. As regulatory expectations continue to increase, identity security is becoming a critical component of operational risk management.

How Identity Risks Develop Over Time

Weak identity security is rarely the result of a single decision. Instead, it develops gradually. Employees reuse passwords across multiple systems. Multifactor authentication is delayed or inconsistently applied. Legacy accounts remain active after employees leave the organization.

Over time, these small gaps accumulate. Each one increases the potential attack surface, creating opportunities for unauthorized access. Without regular review and proactive management, identity risks can grow unnoticed.

What Modern Identity Security Should Look Like

Modern identity security focuses on layered protection rather than reliance on a single factor.

Multifactor authentication adds a critical second layer, requiring users to verify their identity through an additional method such as a mobile app or authentication code.

Role-based access controls ensure that employees only have access to the systems and data necessary for their roles. Regular account reviews help identify inactive or unnecessary access, reducing exposure.

Monitoring and alerting provide visibility into login activity, allowing businesses to detect unusual behavior and respond quickly. These practices are not about limiting productivity—they are about creating structure and reducing uncertainty

Resilience Through Strong Identity Controls

The transition from password-based security to identity-based protection represents a broader shift in how businesses approach cybersecurity. Rather than assuming credentials will remain secure, organizations prepare for the possibility that they may be compromised.

This mindset allows for faster detection, more effective response, and reduced impact when incidents occur. Strengthening identity security is not just a technical improvement—it is a foundational step toward long-term business resilience.

Final Thoughts

Security decisions made today shape the stability of a business in the future. While passwords will always play a role, they are no longer sufficient on their own.

By implementing stronger identity controls, businesses can reduce risk, improve visibility, and build a more secure operational environment.

Not Sure Where to Begin?

We can help you with every step of implementing a modern idenity security plan. Proactively filling security gaps and educating employees on the importance of a multi layered security plan. Small businesses that spend the time to prevent security breaches now, save themselves time and resources preventing a breach in the future. Let us help today!

TL;DR

"Passwords alone are no longer enough to protect your business. Most modern cyberattacks use stolen credentials, allowing attackers to log in as legitimate users and bypass traditional security tools. These attacks often go unnoticed and can lead to financial loss, data breaches, and operational disruption. Weak identity security builds over time through habits like password reuse, lack of multifactor authentication, and unmanaged accounts. To reduce risk, businesses need layered protection—such as MFA, access controls, and login monitoring".

ISSUE 032
March 2026
Independence, Missouri

THIS MONTH'S PRODUCT SPOTLIGHT

CLICK TO VIEW A SHORT VIDEO!

MANAGED PHONE SERVICES

- Use your Office Phone Anywhere
- Internet Connection is all you Need
- Designed to Grow with you
- Seemless Connection
- Mobile/Desktop App Compatible
- Affordable Cost

MANAGING DEVICES IN A HYBRID WORK ENVIRONMENT

The Shift Beyond the Traditional Office

The modern workplace is no longer confined to a single office. Employees now work from home, on the road, and across multiple locations. This flexibility has become a standard part of business operations, allowing organizations to improve productivity, attract talent, and adapt to changing work expectations.

However, this shift also introduces new challenges for managing and securing business devices.

In a traditional office environment, most systems operate within a controlled network. Security tools, updates, and monitoring are centralized, and devices rarely leave the building. Hybrid work removes that structure. Devices now connect from home networks, public Wi-Fi, and remote locations, often outside the visibility of internal IT systems.

This change requires a different approach to device management—one that focuses on consistent control regardless of location.

Every Device as a Potential Entry Point

Each device that connects to company systems represents a potential entry point for attackers.

Laptops, desktops, and mobile devices all serve as access points to email, file storage, financial systems, and other critical resources.

Without proper oversight, several risks begin to emerge:

- Outdated operating systems and applications
- Missing security patches
- Unapproved or risky software installations
- Weak or inconsistent security settings

Individually, these issues may seem minor. Over time, however, they create gaps that attackers can exploit. A single unpatched device or misconfigured system can provide the access needed to compromise an entire environment.

The challenge is not just the number of devices, but the lack of consistency in how they are managed.

Building Long-Term Resilience

Device management is not a one-time project. It is an ongoing process that evolves alongside the business and the threat landscape.

As organizations grow, add employees, and adopt new technologies, the number and variety of devices will continue to increase. Without a structured approach, managing this environment becomes increasingly difficult.

By implementing consistent device management practices early, businesses create a scalable foundation for future growth. They gain visibility, improve security, and reduce the likelihood of unexpected issues.

WHY MULTIFACTOR AUTHENTICATION IS NO LONGER OPTIONAL

Multifactor authentication (MFA) has transitioned from a recommended security feature to a fundamental requirement. As credential-based attacks continue to increase, relying solely on passwords is no longer sufficient.

MFA introduces an additional layer of verification, making it significantly more difficult for attackers to gain access—even if credentials are compromised. This simple step can prevent the majority of unauthorized login attempts.

The challenge for many small businesses is not understanding the value of MFA. Not understanding the value can cause the implementation of MFA to not be consistent or standaraized across all employee accounts.

Ensuring consistent adoption across all users and systems is critical. Partial implementation can leave gaps that attackers can exploit.

When deployed correctly, MFA provides a strong balance between security and usability. It protects critical systems without creating unnecessary complexity for employees.

We are here to help. Let us help implement MFA to all employees the correct way while ensuring that there is clear understanding of the importance of each user having MFA on al accounts.

ARE YOU USING AI TOO MUCH?

The Rise of Everyday AI

Artificial intelligence has quickly become part of daily business operations. From drafting emails and summarizing documents to generating reports and assisting with customer communication, AI tools are now widely accessible and easy to use.

For small businesses, this presents a clear advantage. Tasks that once required significant time and effort can now be completed in seconds. Productivity increases, workloads decrease, and employees are able to move faster than ever before. At first glance, this seems like an obvious win.

However, as AI adoption accelerates, a new question is beginning to emerge: is it possible to rely on AI too much?

When Convenience Becomes Dependence

Like many technological advancements, AI introduces convenience. It reduces friction in daily tasks and helps employees work more efficiently. Over time, however, that convenience can shift into dependence.

When employees begin relying on AI for writing communications, making decisions, interpreting data, and solving problems, they may gradually reduce their own critical thinking and analysis. This shift does not happen all at once. It develops slowly and often without notice. AI becomes the default starting point rather than a supporting tool. Instead of asking how to approach a task, the mindset changes to asking what AI suggests should be done. While this may seem efficient, it introduces risk.

The Risk of Over-Reliance

AI tools are powerful, but they are not perfect. They generate responses based on patterns rather than true understanding. Because of this, they can provide incomplete or outdated information, misinterpret context, or produce answers that sound confident but are ultimately incorrect.

When users rely on AI without verification, these errors can pass unnoticed into business decisions, client communications, or internal processes. In professional environments, even small inaccuracies can have significant consequences. A misinterpreted contract clause, an incorrect financial assumption, or an unclear client message can create confusion, delays, or reputational damage.

The risk is not that AI makes mistakes. The risk is that those mistakes are accepted without question.

The Loss of Institutional Knowledge

Another concern with overusing AI is the gradual erosion of internal knowledge. When employees consistently rely on AI to draft documents, solve technical issues, or answer routine questions, they may retain less information over time. Skills that were once developed through experience begin to fade, replaced by dependency on external tools.

This can create challenges for organizations in the long term. If employees are unable to operate effectively without AI assistance, the business becomes more vulnerable to disruptions, errors, and inefficiencies. Knowledge is not just about completing tasks—it is about understanding how and why those tasks are performed.

AI as a Tool, not a Replacement

The goal is not to avoid AI. When used correctly, it provides significant value by reducing repetitive work, improving efficiency, supporting decision-making, and enhancing productivity. The key is to position AI as a tool rather than a replacement for thinking.

For example, AI can draft an email, but the user should review the tone and accuracy before sending it. AI can summarize data, but the user should validate the conclusions. AI can suggest ideas, but the user must still apply judgment and context. This approach ensures that AI enhances human capability rather than replacing it.

Maintaining Accountability

One of the most important considerations in using AI is accountability. When an employee sends a message, makes a decision, or completes a task, they remain responsible for the outcome regardless of whether AI was used in the process.

This means taking the time to verify AI-generated content before sharing it, understanding the information being presented, and maintaining ownership over decisions. AI can assist in the process, but it does not replace responsibility. Maintaining this mindset helps prevent errors and ensures that business standards are upheld.

Balancing Efficiency with Judgment

The most effective use of AI comes from balance. Too little use may result in missed opportunities for efficiency, while too much use can lead to over-reliance and reduced critical thinking.

Businesses that strike the right balance automate repetitive tasks, support employees with AI tools, and maintain human oversight in decision-making. This combination allows organizations to benefit from AI without sacrificing quality, accuracy, or accountability.

ISSUE 032
March 2026
Independence, Missouri

MAINTAINING A HEALTHY LIFESTYLE WHILE WORKING AT A COMPUTER ALL DAY

The Modern Work Reality

For many employees in small businesses, the workday is spent almost entirely in front of a computer. Emails, meetings, reports, customer communication, and day-to-day operations all take place through a screen. While this allows for efficiency and flexibility, it also introduces challenges that are easy to overlook.

Sitting for long periods, focusing on a screen, and maintaining a repetitive routine can gradually impact both physical and mental health. Unlike more physically active roles, these effects are often subtle at first. There is no immediate disruption, but over time, small habits can lead to fatigue, discomfort, and reduced overall well-being.

The good news is that maintaining a healthy lifestyle in a computer-based role does not require major changes. Small, consistent adjustments throughout the day can make a meaningful difference.

The Impact of Prolonged Sitting

One of the most common challenges of desk-based work is prolonged sitting. Remaining in the same position for extended periods can contribute to back pain, poor posture, and decreased circulation. Over time, this can lead to more significant health concerns if not addressed.

The key is not to eliminate sitting entirely, but to reduce how long it happens without interruption. Standing up periodically, stretching, or taking short walks can help reset posture and improve circulation. Even brief movement throughout the day can reduce strain on the body and improve overall comfort.

Many employees find that setting simple reminders or building movement into their routine helps maintain consistency without disrupting productivity.

Creating an Ergonomic Workspace

A well-designed workspace plays an important role in maintaining physical health. Small adjustments to desk setup can significantly reduce strain on the neck, shoulders, and back.

Positioning the monitor at eye level helps prevent forward head posture, while keeping the keyboard and mouse at a comfortable height reduces strain on the wrists. A supportive chair that encourages proper posture can also make a noticeable difference over the course of a full workday.

These changes are not about creating a perfect environment, but about reducing unnecessary stress on the body. Over time, proper ergonomics contribute to greater comfort and fewer distractions caused by physical discomfort.

Managing Screen Time and Eye Strain

Extended screen time can lead to eye fatigue, dryness, and difficulty focusing. This is especially common when switching between multiple applications or working on detailed tasks for long periods.

One simple approach to reducing eye strain is to take regular breaks from the screen. Looking away periodically, even for a short time, allows the eyes to reset. Adjusting screen brightness and ensuring proper lighting in the workspace can also help reduce strain.

Being mindful of screen time does not mean reducing productivity. It means creating small moments of rest that allow for sustained focus throughout the day.

Staying Mentally Engaged Without Burnout

Working at a computer all day can be mentally demanding, even if the work is not physically exhausting. Constant communication, task switching, and information processing can lead to cognitive fatigue.

Taking short mental breaks throughout the day helps maintain focus and reduce burnout. Stepping away from the desk, even briefly, provides an opportunity to reset and return with a clearer perspective.

It is also important to create boundaries between work and personal time, especially in hybrid or remote environments. Without clear separation, the workday can extend beyond its intended limits, making it more difficult to recharge.

The Role of Hydration and Nutrition

Hydration and nutrition are often overlooked in desk-based roles. It is easy to become focused on tasks and forget to drink water or take proper breaks for meals.

Staying hydrated supports concentration and energy levels, while balanced meals help maintain consistent performance throughout the day. Small habits, such as keeping water nearby or scheduling regular breaks, can help reinforce these behaviors.

Avoiding excessive reliance on caffeine and quick snacks can also contribute to more stable energy levels over time.

Incorporating Movement into the Workday

Movement does not need to be limited to structured exercise outside of work hours. Incorporating small amounts of activity throughout the day can have a meaningful impact.

Simple actions such as standing during calls, walking while thinking through a problem, or taking a few minutes to stretch can break up long periods of inactivity. These moments add up over time and help create a more balanced routine.

The goal is not to disrupt productivity, but to integrate movement in a way that supports both health and efficiency.

Building Sustainable Habits

Maintaining a healthy lifestyle while working at a computer is not about making drastic changes all at once. It is about building habits that are sustainable over time.

Small adjustments, when practiced consistently, become part of the daily routine. Over time, these habits improve comfort, reduce fatigue, and support overall well-being.

Final Thoughts

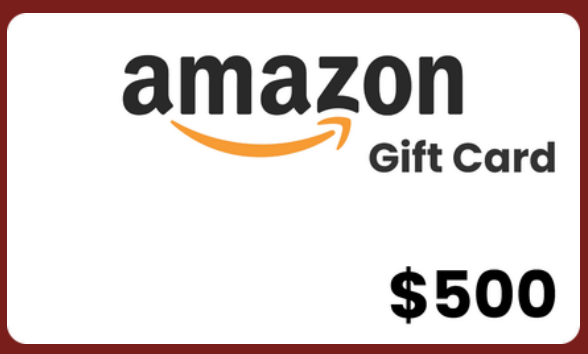
Working at a computer all day does not have to come at the expense of health. By making intentional choices throughout the day, individuals can maintain both productivity and well-being.

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 March's question of the month:

What should Modern Identity Security look like?