ISSUE 035
June 2026
Independence, Missouri

# FCS TECH TALK

## Your Trusted Technology Partner Since 1989

## INSIDE THIS ISSUE:






## THE EMPLOYEE HAS LEFT... BUT DID THEIR ACCESS?

**The Employee Has Left... But Did Their Access?**

When an employee leaves a business, there is usually a checklist of tasks to complete. Company equipment is returned, payroll is updated, and managers begin looking for a replacement.

Unfortunately, one of the most important tasks is often overlooked: removing access to company systems.

For many small businesses, user accounts remain active long after an employee has departed. Sometimes this happens because the business plans to reuse the account. Other times it simply gets forgotten during a busy transition.

While it may seem harmless, inactive accounts can become one of the easiest ways for attackers to gain unauthorized access to a business.

Just like locking the doors after someone leaves your office, disabling access to your technology should be a standard part of every offboarding process.

**Why Former Employee Accounts Matter**

Today's employees often have access to much more than just their work email.

Depending on their role, they may have accounts for Microsoft 365, Google Workspace, accounting software, CRM platforms, cloud storage, password managers, remote access tools, vendor portals, and countless other business applications.

If even one of those accounts remains active after an employee leaves, it creates an unnecessary security risk. Former employees typically have no intention of causing problems, but unused accounts are attractive targets for cybercriminals. If login credentials have ever been exposed in a data breach or reused across multiple websites, attackers may eventually discover them.

Without proper monitoring, an inactive account can remain unnoticed for months while still providing access to valuable business information.

**The Challenges Small Businesses Face**

Most small businesses may not feel they are large enough to have to worry about the effects of leaving employee access open even after they have left.

Instead, account management often becomes overlooked. During a busy employee transition, it is easy for one or two accounts to be left active due to no real process being in place.

The problem becomes even larger as businesses adopt more cloud-based software. A single employee may have access to ten or more different systems, each requiring separate administrative action to disable.

Without a documented offboarding process, businesses can quickly lose track of who still has access and what permissions remain active.

Over time, these forgotten accounts begin to accumulate, creating unnecessary security exposure throughout the organization.

**More Than Just Email**

Many business owners assume that disabling an employee's email account is enough.

In reality, email is only one piece of the puzzle.

Employees often have access to shared files, customer databases, financial records, internal documentation, collaboration platforms, remote desktop software, and cloud applications. Even access to a seemingly minor system can provide attackers with valuable information about your business.

Former accounts may also remain connected to mobile devices, web browsers, or third-party applications that continue syncing data long after employment has ended.

Proper offboarding means reviewing every system the employee accessed—not just their email account.

**Building a Better Offboarding Process**

The good news is that reducing this risk does not require expensive technology.
It starts with having a consistent process every time an employee leaves the organization.

Businesses should maintain an inventory of critical systems, disable accounts promptly, remove unnecessary permissions, recover company-owned devices, and confirm that shared passwords have been changed whenever appropriate.

Regular account reviews are equally important. Even businesses with excellent offboarding procedures should periodically review active user accounts to ensure that only current employees retain access.

These routine audits often uncover forgotten accounts that have remained active for months or even years.
A few minutes of review today can prevent a much larger security incident tomorrow.

**Technology Should Support Security**

Modern identity management tools can make account management significantly easier.

Features like single sign-on, multi-factor authentication, centralized user management, and automated account provisioning help businesses maintain better visibility into who has access to company resources.

When employee accounts are managed centrally, disabling one user can automatically remove access across multiple business applications at the same time.

This not only improves security but also simplifies the entire offboarding process for growing organizations.

As businesses continue adopting more cloud services, centralized identity management becomes increasingly valuable for maintaining both security and operational efficiency.

**Not Sure If Former Employees Still Have Access?**

Many businesses are surprised by how many inactive accounts remain in their environment after several years of employee turnover.

We can help review your Microsoft 365, Google Workspace, and other business systems to identify unused accounts, remove unnecessary access, and ensure your offboarding process helps protect your business from unnecessary risk.

Any employee offboarding we can handle 100% of the account removal for you to ensure all accounts are properly removed and access is terminated.

Properly offboarding old user accounts is just a small step that can have large postive impacts.

TL;DR

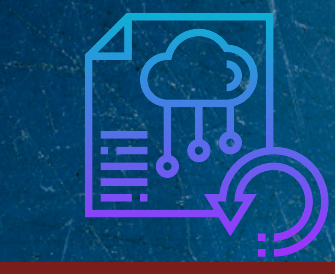
*"When an employee leaves your business, don't let their accounts stay behind. Forgotten user accounts can provide an easy entry point for cybercriminals and create unnecessary security risks. A consistent offboarding process—including disabling accounts, removing permissions, reviewing connected devices, and updating shared passwords—helps protect sensitive business data. Regular account audits and centralized identity management can further strengthen security while making employee transitions much easier to manage."*

ISSUE 035
June 2026
Independence, Missouri

## THIS MONTH'S PRODUCT SPOTLIGHT

CLICK TO VIEW A SHORT VIDEO!

# MICROSOFT 365 BACKUP



RESTORE LOST DATA

INFINITE DATA RETENTION

STORE ALL M365 DATA

AUTOMATIC DAILY BACKUPS

## WHY EVERY BUSINESS SHOULD HAVE A PASSWORD MANAGER

Passwords remain one of the first lines of defense against cyber threats, yet many businesses still rely on employees to remember dozens of unique logins. As a result, passwords are often reused, written on sticky notes, or saved in unsecured documents, creating unnecessary security risks.

A business password manager helps eliminate these problems by securely storing login credentials in an encrypted vault. Employees only need to remember one master password while the password manager generates and stores strong, unique passwords for every account.

At Ferguson Computer Services, we recommend and deploy Keeper Password Manager because it combines enterprise-grade security with an easy-to-use interface.

Keeper allows businesses to securely store passwords, generate strong credentials, enable multi-factor authentication, and safely share login information with authorized employees without exposing passwords through email or chat.

Password managers also simplify employee onboarding and offboarding. Administrators can quickly grant access to new team members or revoke access when someone leaves the organization, helping ensure that former employees no longer have access to sensitive business systems. Beyond improving security, a password manager also boosts productivity.

Employees spend less time resetting forgotten passwords or searching for login information and more time focusing on their work. As cyber threats continue to target stolen credentials, implementing a password manager is one of the simplest and most effective ways to strengthen your organization's overall security.

Interested in Getting Started with Keeper?

We can help your business implement Keeper Password Manager, migrate existing passwords, and train your team on best practices so your organization stays secure without sacrificing productivity.

## WHY EVERY BUSINESS SHOULD TEST THEIR BACKUPS

Most businesses understand the importance of backing up their data, but far fewer take the time to verify those backups actually work. Unfortunately, many organizations only discover a backup problem after data has already been lost.

Whether it's caused by hardware failure, ransomware, accidental deletion, or a natural disaster, recovering critical information depends on having a backup that can be successfully restored.

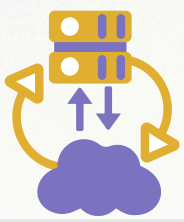
**Backups Are Only as Good as Their Recovery**

Regular backup testing confirms that important files, servers, and business applications can be restored quickly when needed. It also helps identify failed backup jobs, corrupted files, or configuration issues before they become a major problem.

A successful backup strategy includes both routine monitoring and periodic recovery testing to ensure everything is functioning as expected.

The best backup is the one you never have to use—but if the unexpected happens, knowing your data can be restored provides confidence, minimizes downtime, and helps keep your business running.

We can schedule quarterly restoration backup testing so you know that your data is easily recoverable and secure.



## YOUR WEB BROWSER COULD BE YOUR BIGGEST SECURITY RISK

For most employees, the web browser is the application they use more than any other throughout the workday. Whether checking email, accessing cloud applications, researching information, or collaborating with coworkers, nearly every business task begins inside a browser.

Because browsers have become such an essential part of modern work, they are also one of the primary targets for cybercriminals. Many business owners assume their antivirus software alone is enough to keep employees safe online.

While antivirus plays an important role, it cannot stop every web-based threat. Malicious websites, fake login pages, harmful browser extensions, and compromised downloads can still place sensitive business information at risk.

The good news is that improving browser security often requires only a few simple changes that significantly reduce exposure.

**The Reality of Browser-Based Threats**

Today's cyberattacks rarely rely on obvious viruses alone. Instead, attackers frequently target employees through the websites they visit and the browsers they use every day.

A single click on a fraudulent login page can expose Microsoft 365 credentials. An unapproved browser extension may quietly collect browsing activity or capture sensitive information. Even legitimate websites can become compromised and unknowingly distribute malicious code.

Employees often have dozens of browser tabs open simultaneously while accessing email, financial software, customer records, and cloud storage. Because browsers connect so many business systems together, compromising a browser session can provide attackers with access to valuable company data.

Without proper security controls, the browser can become one of the easiest entry points into an organization's environment.
The Business Impact Beyond Security
Browser security affects much more than cybersecurity.

Unauthorized extensions, excessive cached data, and outdated browser versions can reduce performance, create compatibility issues, and increase support requests. Employees may experience slower browsing, application errors, or inconsistent behavior across different devices.

Businesses also face compliance concerns when employees install unapproved browser add-ons or store sensitive information in unsecured browser tools. Passwords, payment information, and customer data should never rely solely on browser storage when more secure alternatives are available.

By standardizing browser settings and limiting unnecessary extensions, organizations create a more consistent, secure, and reliable experience for employees.

**What Better Browser Security Looks Like**

Protecting your business starts with treating the web browser as a critical business application rather than just a way to access the internet.

Businesses should regularly review:

- Approved web browsers
- Browser update status
- Installed extensions and add-ons
- Saved passwords and autofill settings
- Safe Browsing and security features
- Employee web browsing practices

Keeping browsers updated ensures the latest security patches are installed, while limiting extensions reduces unnecessary risk. Businesses should also encourage employees to use a dedicated password manager instead of storing credentials directly within the browser.

Combining secure browser settings with multifactor authentication, endpoint protection, and employee security awareness training creates multiple layers of protection against today's web-based threats.

**Not Sure If Your Browsers Are Properly Secured?**

Your browser is often the gateway to your email, cloud applications, financial systems, and business data. Making sure it is properly configured is an important part of protecting your organization.

We can help review your browser security settings, remove unnecessary extensions, implement password management solutions, and ensure your employees are browsing safely. Small improvements today can significantly reduce security risks while creating a faster, more consistent experience across your entire business.

ISSUE 035
June 2026
Independence, Missouri

# THE HIDDEN RISKS OF SHADOW IT

For many small businesses, employees are constantly looking for ways to work more efficiently. When they discover a new file-sharing platform, note-taking application, AI tool, messaging app, or project management system, it may seem like an easy way to improve productivity.

In many cases, these tools are adopted with good intentions. Employees simply want to complete tasks faster, collaborate more effectively, or solve a problem without waiting for formal approval.

However, when software is introduced without the knowledge or oversight of the business, it creates what is commonly known as "Shadow IT."

Shadow IT refers to any technology, application, or cloud service that employees use without being approved or managed by the organization. While these tools may appear harmless, they often introduce security risks, compliance concerns, and operational challenges that quietly grow over time.

As businesses continue adopting cloud-based services and remote work becomes more common, managing Shadow IT has become an important part of maintaining a secure and organized technology environment.

**The Reality of Unmanaged Technology**

Today's employees have access to thousands of business applications with only a few clicks. any cloud services offer free versions, quick sign-up processes, and easy integration with existing business accounts.

An employee may begin using a personal file-sharing platform, install an unapproved browser extension, create an online form, or subscribe to a new collaboration tool without realizing the potential risks.

Over time, multiple employees may adopt different solutions to accomplish similar tasks. Files become scattered across several platforms, customer information may be stored outside approved systems, and IT administrators lose visibility into where important business data resides.

These situations rarely happen intentionally. Instead, they develop gradually as employees focus on solving immediate business challenges rather than considering long-term security or management.

Without centralized oversight, organizations often have little understanding of how many applications are actually being used throughout the business.

**The Business Impact Beyond Security**

Shadow IT creates challenges that extend far beyond cybersecurity.

When employees use multiple applications for the same purpose, collaboration becomes inconsistent. Important documents may exist in several locations, version control becomes more difficult, and teams may struggle to determine which information is current.

Businesses may also unknowingly pay for duplicate software subscriptions while existing business platforms already provide similar functionality. From an IT perspective, supporting dozens of unapproved applications increases complexity, consumes valuable time, and makes troubleshooting more difficult.

Standardizing technology not only improves security but also creates a more efficient and productive workplace.

**What Proper Technology Management Should Look Like**

Managing Shadow IT begins with understanding what technology employees are already using.

Businesses should regularly review:

- Approved business applications
- Cloud storage platforms
- AI and productivity tools
- Browser extensions
- File-sharing services
- Communication platforms
- Software subscriptions

Organizations should also establish clear policies explaining how employees can request new software when business needs arise.

Rather than discouraging innovation, businesses should encourage employees to bring forward new technology ideas so they an be evaluated for security, compatibility, licensing, and long-term support before implementation.

Regular software reviews help identify duplicate applications, reduce unnecessary spending, and ensure business information remains stored within approved systems.

When employees and IT work together, organizations can adopt new technology safely while maintaining visibility and control.

**Planning for Long-Term Technology Success**

Technology will continue evolving rapidly, and employees will always discover new tools that promise to improve productivity. The goal should not be to prevent innovation but to ensure every new application supports the business without introducing unnecessary security risks or operational challenges.

Businesses that establish clear software approval processes, maintain visibility into their technology environment, and review applications regularly are better positioned to support future growth while protecting sensitive information.

Shadow IT often begins with a single employee solving a small problem. Over time, those individual decisions can create a complex technology environment that is difficult to secure, manage, and support.

Taking a proactive approach today helps ensure your technology remains organized, secure, and aligned with your business objectives.

**Not Sure What Applications Your Employees Are Using?**

Many businesses are surprised to learn just how many cloud services, browser extensions, AI tools, and software subscriptions are being used throughout their organization without formal approval.

We can help evaluate your technology environment, identify unmanaged applications, review potential security risks, and develop practical software policies that support both productivity and security.

# 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 June's question of the month:

What is one risk of leaving a former employee with an active account?