ISSUE 033
April 2026
Independence, Missouri

FCS TECH TALK

Your Trusted Technology Partner Since 1989

INSIDE THIS ISSUE:

THE RISK OF NAME SPOOFING IN EMAILS: HOW TRUST IS BEING USED AGAINST YOUR BUSINESS

The Illusion of Trust

For many small businesses, email remains one of the most trusted forms of communication. Messages appear to come from familiar names—employees, vendors, or leadership—and are often handled quickly without hesitation. This level of trust has been built over years of consistent communication and reliable interactions.

On the surface, this approach feels efficient. Employees recognize a name, assume legitimacy, and respond accordingly. Daily operations depend on this trust, allowing businesses to move quickly without needing to verify every message.

However, attackers have learned to exploit this exact behavior. Instead of attempting to break through technical defenses, they are manipulating perception—specifically, the names that users recognize and trust. This tactic, known as name spoofing, has become an increasingly effective method for gaining access to sensitive information and initiating fraudulent activity.

Much like weak passwords, name spoofing attacks often succeed quietly. There is rarely an immediate indication that anything is wrong. The email appears legitimate, the request seems reasonable, and the interaction proceeds as normal. By the time suspicion arises, the damage may already be done.

The Reality of Name Spoofing Attacks

Name spoofing occurs when an attacker sends an email that displays a familiar or trusted name, even though the underlying email address is different. At a glance, the message appears to come from someone within the organization or a known contact, making it far more convincing than traditional phishing attempts.

These attacks are particularly effective because most users focus on the display name rather than the actual email address. In a busy work environment, employees often rely on quick recognition instead of detailed verification.

Attackers use this to their advantage by impersonating:

- Company executives requesting urgent action
- Employees asking for internal information
- Vendors requesting payment updates
- IT staff providing “important” instructions

Because the message appears to come from a legitimate source, it bypasses the skepticism that would normally accompany an unknown sender.
This approach also allows attackers to evade many traditional security tools.

While advanced email filtering can detect suspicious domains or malicious links, name spoofing relies on social engineering rather than technical exploitation. The email itself may not contain obvious red flags, making it more difficult to identify and block.

The Business Impact Beyond IT

The consequences of a successful name spoofing attack can extend far beyond a simple email mistake. These incidents often lead directly to financial loss, data exposure, and operational disruption.

One of the most common outcomes is fraudulent payment requests. An attacker impersonates a vendor or executive and asks for a payment to be redirected or processed urgently. Because the request appears legitimate, employees may act quickly without verifying the details.
In other cases, attackers use name spoofing to gain access to sensitive information. An email that appears to come from management may request employee data, login credentials, or financial records. Once obtained, this information can be used for further attacks or sold to other malicious actors.

There is also a reputational risk. If clients or partners receive spoofed emails appearing to come from your business, it can damage trust and credibility. Even if the attack originates externally, the perception is that your organization’s communication has been compromised.

Unlike more visible cyberattacks, name spoofing incidents often go unnoticed until after the impact has occurred. Funds may already be transferred, or sensitive data may already be shared before the issue is identified.

How Name Spoofing Risks Develop Over Time

Name spoofing attacks are not typically the result of a single vulnerability. Instead, they exploit a combination of habits and gaps that develop over time.

Employees become accustomed to responding quickly to emails without verifying sender details. Internal processes prioritize efficiency, sometimes at the expense of validation. Email systems may lack proper configuration to detect or prevent impersonation attempts.
Over time, these factors create an environment where name spoofing can succeed with minimal resistance.

What Protection Against Name Spoofing Should Look Like

Addressing name spoofing requires a combination of technical controls and user awareness. Relying on a single solution is not enough, as these attacks are designed to bypass traditional defenses.

Email authentication protocols such as SPF, DKIM, and DMARC help verify that messages are coming from authorized sources. These configurations reduce the likelihood of attackers successfully impersonating your domain.

User awareness is equally important. Employees should be trained to:

- Verify the full email address, not just the display name
- Be cautious of urgent or unusual requests
- Confirm financial or sensitive requests through a secondary method

Monitoring and alerting provide additional visibility. Identifying unusual email patterns or impersonation attempts allows businesses to respond quickly and reduce potential impact.

These practices are not about slowing down operations—they are about introducing structure that protects the business while maintaining efficiency.

Not Sure Where to Begin?

We can help you implement the right protections to reduce the risk of email-based attacks, including name spoofing.

From securing your email environment to training employees on how to recognize and respond to suspicious messages, we provide a layered approach that fits your business.

TL;DR

“Name spoofing allows attackers to send emails that appear to come from trusted names like employees, vendors, or executives—tricking users into taking action without verifying the sender. These attacks often lead to financial loss, data exposure, and reputational damage because they rely on trust, not technical exploits. Small businesses are especially vulnerable due to fast-paced communication and limited verification processes. The best defense is a layered approach: email authentication (SPF, DKIM, DMARC), employee awareness, and clear policies for verifying sensitive requests.”

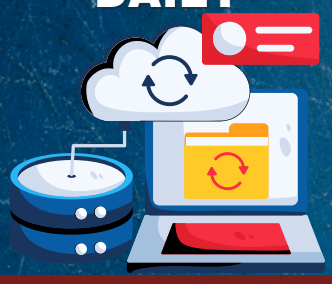
ISSUE 033
April 2026
Independence, Missouri

THIS MONTH'S PRODUCT SPOTLIGHT

CLICK TO VIEW A SHORT VIDEO!

MANAGED BACKUP SERVICES

BACKUPS DONE DAILY



RESTORE LOST/ CORRUPT FILES

GEO-REDUNDANT

FULLY ENCRYPTED

UNDERSTANDING VPN USE IN A SMAL BUSINESS ENVIRONMENT

Virtual private networks (VPNs) have become a standard tool for businesses that need to support remote work, protect sensitive data, and maintain secure connections outside the office. Employees now access company systems from home, while traveling, and across various networks. VPNs help create a secure pathway between the user and the business environment.

On the surface, using a VPN seems straightforward. Employees connect, their traffic is encrypted, and their activity is protected from outside visibility. This simplicity makes VPNs an attractive solution for small businesses looking to improve security without adding complexity.

However, improper use or misunderstanding of VPNs can introduce new risks rather than eliminate them.

In a properly managed environment, VPNs are part of a broader security strategy. Without clear guidance, users may assume that simply being connected to a VPN makes all activity safe. This can lead to risky behavior, reduced vigilance, and gaps in protection.

This is where understanding the do's and don'ts of VPN usage becomes critical.

The Do's and Don'ts of VPN Usage

Using a VPN correctly requires both technical configuration and user awareness.

Do:
- Use a business-grade VPN solution managed by your IT provider
- Connect to the VPN when accessing company systems remotely
- Keep devices updated and secured before connecting
- Use strong authentication, including multifactor authentication

Don't:
- Assume a VPN replaces antivirus or endpoint protection
- Connect to unknown or untrusted VPN services
- Disable the VPN when working with sensitive data
- Share VPN access credentials between users

When used properly, a VPN significantly reduces exposure to threats on public or unsecured networks. It encrypts data in transit and helps ensure that communication between users and business systems remains private.

However, a VPN does not make a device immune to threats. Malware, phishing attacks, and compromised credentials can still impact systems regardless of whether a VPN is in use.

Building Secure and Consistent VPN Practices

VPN usage should be consistent, monitored, and supported by clear policies. Simply providing access is not enough—businesses must ensure that employees understand when and how to use it.

As remote and hybrid work environments continue to grow, VPNs remain a valuable tool for maintaining secure access.

THE HIDDEN JOURNEY OF AN EMAIL

Sending an email feels almost instant. You type a message, click send, and within seconds it appears in someone else's inbox. On the surface, it seems like a simple, direct exchange between two people.

In reality, that message takes a much more complex journey. When an email is sent, it doesn't travel directly from your computer to the recipient.

Instead, it is broken into packets and routed through multiple servers across the internet. Each server helps determine the fastest and most efficient path, similar to how GPS systems route traffic.

During this process, the email may pass through several locations before reaching its destination, often in a matter of seconds.

Along the way, security checks such as spam filtering and authentication protocols help verify that the message is legitimate.

This behind-the-scenes process happens so quickly that most users never notice it.

Understanding how email travels highlights why security measures are so important—and how much technology is working silently to keep communication reliable.

Not as simple as we all thought...

THE SHIFT TO MODERN BUSINESS COMMUNICATION

The New Business Standard

Voice over Internet Protocol (VoIP) has quickly become a core part of how small businesses communicate. Traditional phone systems are being replaced by flexible, internet-based solutions that allow employees to stay connected from virtually anywhere. Whether working in the office, from home, or on the go, VoIP systems provide a consistent and reliable way to communicate.

For small businesses, this shift creates new opportunities. Communication is no longer tied to a physical desk phone or a single location. Calls can be made and received through mobile apps, desktop computers, or traditional handsets, all within the same system. This level of accessibility allows teams to remain responsive and connected regardless of where work takes place.

At first glance, the transition to VoIP may seem like a simple upgrade in technology. In reality, it represents a fundamental change in how businesses operate and interact with both customers and internal teams.
However, as adoption continues to grow, many businesses are beginning to realize that VoIP offers far more than just a new way to make phone calls.

When Flexibility Becomes a Competitive Advantage

Like many modern technologies, VoIP introduces a level of flexibility that traditional systems cannot match. It removes the limitations of location-based communication and allows businesses to operate more dynamically.

Employees can answer business calls from their mobile devices, transfer calls between locations seamlessly, and remain accessible without being tied to a desk. This flexibility supports hybrid work environments and ensures that communication continues without interruption.

Over time, this flexibility becomes a competitive advantage. Businesses that can respond quickly to customer inquiries, maintain consistent availability, and adapt to changing work environments are better positioned to succeed.

Instead of being constrained by physical infrastructure, organizations gain the ability to scale communication as needed. Adding new users, locations, or features can often be done quickly without significant hardware investments.

Soon businesses begin to recognize how improved communication directly impacts productivity and customer experience.

The Impact on Productivity and Efficiency

VoIP systems do more than enable communication—they enhance it. Features such as call routing, voicemail-to-email, auto attendants, and call analytics help streamline daily operations.

Employees spend less time managing missed calls, tracking down messages, or navigating complex phone systems. Instead, communication becomes more organized and easier to manage.

For example, voicemail messages can be delivered directly to an employee's email, allowing for faster response times. Call routing ensures that customers are directed to the right person without unnecessary delays. These small improvements add up to significant gains in efficiency.

Additionally, centralized management allows businesses to maintain consistency across all users. Settings, permissions, and features can be controlled from a single platform, reducing confusion and improving overall usability.

The result is a communication system that supports the way modern businesses operate, rather than slowing them down.

Maximizing the Benefits of VoIP

While VoIP offers significant advantages, its effectiveness depends on proper implementation and management. Businesses should ensure that their network infrastructure can support voice traffic and that security measures are in place to protect communication.

Clear policies and user training also play an important role. Employees should understand how to use the system effectively and take advantage of the features available to them.

When deployed correctly, VoIP becomes more than just a phone system. It becomes a central part of how a business communicates, collaborates, and operates. By aligning communication tools with modern work environments, businesses can improve efficiency, enhance customer experience, and support long-term growth.

Final Thoughts

The way businesses communicate is changing, and VoIP is at the center of that transformation. It offers flexibility, scalability, and functionality that traditional phone systems simply cannot match.

By embracing VoIP technology and using it effectively, organizations can position themselves for greater efficiency, stronger customer relationships, and continued success in an increasingly connected world.

ISSUE 033
April 2026
Independence, Missouri

SPRING CLEANING YOUR BUSINESS TECHNOLOGY: PRACTICAL IT TIPS FOR SMALL BUSINESSES

For many small businesses, spring cleaning is a time to organize workspaces, clear out clutter, and reset for the months ahead. It's an opportunity to improve efficiency and create a more productive environment. However, while physical spaces often get attention, the same level of care is not always applied to the technology that keeps the business running.

Over time, systems, devices, and accounts can accumulate digital clutter. Outdated files, unused software, inactive accounts, and inconsistent settings quietly build up in the background. These issues may not seem urgent, but they can impact performance, create confusion, and introduce unnecessary security risks. Just like your office, your IT environment benefits from regular maintenance and organization.

The good news is that IT spring cleaning does not require major changes. A few focused steps can help improve efficiency, strengthen security, and create a more reliable technology environment.

Start by Cleaning Up Files and Storage

One of the simplest places to begin is with file organization. Over time, shared drives, desktops, and cloud storage platforms can become filled with duplicate files, outdated documents, and unnecessary data. This clutter makes it harder for employees to find what they need and can slow down systems.

Take time to review storage locations and remove files that are no longer relevant. Organize folders in a way that makes sense for your team and ensure that important documents are easy to locate.

Review User Accounts and Permissions

As your business grows, user accounts and access permissions can become difficult to manage.

Employees may change roles, leave the company, or gain access to systems they no longer need. Without regular review, this can create unnecessary risk.

Spring is a great time to audit user accounts across all systems. Remove accounts that are no longer in use and ensure that each employee only has access to what is necessary for their role.

This process helps reduce the potential for unauthorized access and keeps your environment more secure.

Strengthen Security Settings

Security settings can drift over time, especially as systems are updated or new tools are added.

Take time to review your security configurations. Ensure that multifactor authentication is enabled wherever possible and that password policies are consistent across systems.

Check for any unnecessary open access points or outdated configurations that could create vulnerabilities. Small adjustments in security settings can significantly reduce risk and improve overall protection.

Evaluate Your Devices

Not all devices age the same way. Some may still perform well, while others begin to slow down or struggle with newer applications. Review your current hardware and identify any devices that may need to be upgraded or replaced. Older systems can impact productivity and may not support the latest security features.

Planning upgrades ahead of time helps avoid unexpected failures and ensures that your team has the tools they need to work efficiently.

Reinforce Good Employee Habits

Technology is only one part of your IT environment. Employee behavior plays a major role in maintaining security and efficiency.

Use this time to remind your team of best practices. Encourage strong password usage, caution with email attachments, and awareness of phishing attempts. Even simple reminders can make a meaningful difference.

When employees understand their role in maintaining security, they become an important part of your defense strategy.

Create a Plan Moving Forward

Spring cleaning is not just about addressing current issues. It is also about setting a foundation for the future.

Having a consistent approach helps prevent issues from building up again over time.

Not Sure Where to Start?

Don't worry. This is where we can help! As your IT Partner we can help guide you through any of these spring cleaning steps, taking the stress off of your plate and reducing administrative headaches.

We are happy to help do an entire IT environment assessment to show what things are being done well and what needs to have some attention.

Once we have a good overview of what your current environment needs we will be happy to begin implementing changes and improving your overall IT structure.

Final Thoughts

Spring is the perfect time to refresh not just your workspace, but your technology as well.

By taking a proactive approach to IT maintenance, small businesses can improve performance, reduce risk, and create a more efficient working environment.

These steps do not need to be complicated. Small, consistent improvements can have a lasting impact.

With a cleaner, more organized IT environment, your business is better positioned to operate smoothly and grow with confidence.

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 April's question of the month:

How does Name Spoofing occur?