CORPORATE TECHNOLOGIES GROUP

THE UNIFIED SERVICES PROVIDER

IN THIS ISSUE:

What's New At CTG?

In this article, we highlight how CTG's team-building—from cheering on the RubberDucks to tackling an escape room—mirrors the way we show up for our clients, collaborating and helping your team succeed just like we do our own.

Why Email Security Cannot Wait - How to Stop Spoofing Before It Happens

This article explains how Corporate Technologies Group helps businesses protect against email spoofing and phishing by configuring SPF, DKIM, and DMARC. CTG can determine the settings that work best for your business.

How Businesses Should Shape Their Tech Stack In 2026

This article gives you key steps to strengthen your technology, improve security, and set your business up for a stable, productive year.

This quarterly publication is provided courtesy of Brett Harney, President of Corporate Technologies Group, Inc.

OUR MISSION:

Our mission is to provide encompassing IT solutions for our clients through a consultative and solution-driven approach.

HAPPY HOLIDAYS FROM CORPORATE TECHNOLOGIES GROUP!

PARTNERING FOR YOUR SUCCESS IN 2026...AND BEYOND

As we head into the new year, we want to take a moment to say thank you.

At CTG, we believe the best technology support comes from real relationships — not transactional tickets — and this year reminded us just how important that mindset is. Beyond the day-to-day work, we were available to strengthen our own team by creating shared experiences.

From cheering on the RubberDucks together to putting our problem-solving skills to the test in an escape room, those moments were not about fun. They reinforced something that is central to who we are: when one of us wins, we all win.

That same philosophy extends to you.

We want you to think of Corporate Technologies Group as an extension of your own staff.

When you call us with a technology question — whether it is about cabling, phone systems, security, or simply asking for guidance — we show up as part of your team. It is not always about sales. Our goal is to build strong, long-term relationships and help your business technology thrive.

As you begin planning for what is next, know how much we appreciate the trust you place in us. We look forward to continuing to support you and your team in 2026...and beyond.

WHY EMAIL SECURITY CANNOT WAIT - HOW TO STOP SPOOFING BEFORE IT HAPPENS

Email is the lifeblood of modern business, but it's also one of the easiest ways for cybercriminals to attack your company. One of the most common tricks? Spoofing.

Spoofing is when someone sends an email that looks like it comes from a trusted source — a vendor, partner, or even a colleague — but it is fake.

Even a subtle change in an email address or domain can fool experienced employees, opening the door to phishing attempts or costly wire-transfer fraud. Sometimes it's the full domain, sometimes it's just the display name, and other times it's a clever lookalike address — but the goal is always the same: to trick someone into taking an action they shouldn't.

And no — email spoofing and domain spoofing aren't the same, but they often play together.

DID YOU KNOW ...

In simulated tests, the median time for a user to click a phishing link was just 21 seconds, and another 28 seconds to enter data. - 2024 Verizon DBIR

What's The Difference?

Email Spoofing

- *What it is:* The sender address in the "From" field of an email is forged to look like it came from someone you trust.
- *How it works:* The attacker can use any email address — even a completely fake one — to make it appear legitimate.
- *Goal:* Trick recipients into clicking links, downloading attachments, sharing credentials, or sending money.

Domain Spoofing

- *What it is:* A specific type of email spoofing where the attacker makes it appear that the email came from your actual domain (e.g., @yourcompany.com).
- *How it works: The attacker forges the domain or uses a lookalike domain to make the email seem authentic.*
- *Goal:* Bypass email filters and exploit trust in your brand, often leading to credential theft, financial fraud, or phishing attacks.

In short, all domain spoofing is a type of email spoofing, but not all email spoofing involves your domain. While email spoofing can use any fake address to trick recipients, domain spoofing specifically targets your brand's domain to make the message appear more credible and trustworthy. Spoofing isn't just a theoretical risk. These tactics are being used every day, with real financial and operational consequences for organizations of all sizes.

In 2022, a small manufacturing business thought they were responding to a routine email from their CEO asking for a wire transfer. Everything looked right. The tone felt familiar. The address was just close enough. By the time the team realized the message was spoofed, $2.46 million had already been sent. (secretservice.gov)

Financial institutions aren't immune either. Credit unions have been targeted with emails that appeared to come from internal teams or trusted member communications. Even with multi-factor authentication in place, some members were still tricked into entering their credentials on fake login pages. (fbi.gov)

(continued on page 3...)

How DMARC, DKIM, And SPF Help Protect You

Luckily, there are tools that make spoofing much harder. DMARC, DKIM, and SPF each work in diverse ways, and together they provide a layered defense:

SPF (Sender Policy Framework): SPF allows the domain owner to specify which mail servers are authorized to send emails for that domain. If an email comes from an unauthorized server, SPF can flag it as suspicious. SPF alone helps, but it does not verify the content of the email itself.
DKIM (DomainKeys Identified Mail): DKIM uses a digital signature to verify that the email has not been altered in transit and really comes from the domain it claims to be from. This adds another layer of validation, but like SPF, it is not perfect on its own.
DMARC (Domain-based Message Authentication, Reporting & Conformance): DMARC ties SPF and DKIM together. It tells receiving servers how to handle emails that fail SPF or DKIM checks and provides reporting so domain owners can monitor attempted spoofing. DMARC is the strongest defense because it allows you to enforce policies and see exactly how your domain is being used — or abused.

Why use them together?

Alone, SPF and DKIM help, but attackers can still bypass one or the other. When combined with DMARC, you get both verification and enforcement. SPF checks the sender, DKIM verifies the content, and DMARC ensures the system is working properly — creating a multi-layered defense that drastically reduces your risk of being spoofed.
What to do next

- Verify that your domain has SPF, DKIM, and DMARC configured correctly.
- Use DMARC reporting to monitor unauthorized attempts.
- Educate your team to recognize suspicious emails and confirm requests for sensitive actions via a trusted channel.

At CTG, we can check your email configuration and make sure these protections are active and working together. It is a small step that makes a significant difference — helping keep your business safe from phishing and spoofing attacks. Give us a call at **330-655-8144** or email **info@ctgusa.net** for more information.

The Unified Services Provider. One Partner. Every Solution. All Under One Roof.

Managing business technology often means juggling too many vendors—and too many bills. At Corporate Technologies Group, we make it easier by bringing everything under one roof. One team, one point of contact, and sometimes even one bill, all focused on protecting your data, controlling costs, and keeping your systems running the way they should.
With access to over 200 technology providers, we help businesses switch solutions without downtime, surprises, or budget pain.

From cybersecurity and communications to networks and managed services, we deliver best-of-class solutions built around your needs. If your current technology isn't cutting it—or a contract is coming up—CTG is the call that helps your technology move forward.

FREE OFFER!

FREE Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

The first five clients that email info@ctgusa.net and respond in the subject line with "**YES, WE WANT THE SECURITY AUDIT FOR FREE**" will receive this service at no cost or obligation. Our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all the businesses we've done this for discover that they are completely exposed to various threats in a number of areas.

CLICK HERE TO SIGN UP FOR YOUR FREE SECURITY AUDIT: https://ctgusa.net/aspirin-msp/

(Answer at the end of newsletter)

TECH TRIVIA

Which detail is most commonly spoofed to make a phishing email look legitimate?

A. The email subject line
B. The sender's display name
C. The email body text
D. The email attachment file name

HOW BUSINESSES SHOULD SHAPE THEIR TECH STACK IN 2026

If there is one lesson from this year, it is that resilience matters more than ever. Stability doesn't come from reacting faster — it comes from being prepared before something goes wrong.

Between rising cyber threats, tighter compliance requirements, and growing pressure to "do more with less," many organizations found themselves realizing just how interconnected their technology really is. One weak spot can create ripple effects across operations, finances, and trust.

As you start thinking about 2026, here are the top moves to consider positioning your business for stability, security, and growth:

- Begin with a full assessment of your managed services provider (MSP) — make sure you are receiving everything you pay for, that you are using the tools, and that nothing important has slipped through the cracks.
- Review all compliance requirements relevant to your industry (data privacy laws, financial regulations, and internal security standards).
- Update software, patch systems, and retire legacy tools that are no longer supported.
- Delete old/unnecessary emails and files, but more importantly — ensure you have a full backup and a documented disaster recovery plan in place for downtime, ransomware, or other cyber incidents.
- Perform a penetration test or security audit to surface vulnerabilities before they become problems.
- Review your technology service contracts: see if there are potential cost savings, redundancies, or opportunities to optimize spending while improving performance or security.

These steps may not grab headlines, but they're the foundation of resilient, well-run organizations. When the unexpected happens, it's the preparation that makes all the difference.

If you're not sure where to start — or want a second set of eyes on what you already have in place — that's exactly where CTG comes in. Reach out to our team at **330-655-8144** or email **info@ctgusa.net** to schedule a conversation.

We're here to answer questions, review your environment, and help ensure your technology is truly supporting your business as you head into 2026.

Let's make sure you're ready — together.

TECH TRIVIA ANSWER

Which detail is most commonly spoofed to make a phishing email look legitimate?

B

Attackers often spoof the sender's display name because it's the first thing people see, making the email look like it comes from someone they trust.

CORPORATE TECHNOLOGIES GROUP
THE UNIFIED SERVICES PROVIDER