Texas Council Risk Management Fund

EMAIL SPOOFING: WHY IT STILL WORKS – AND HOW TO STOP IT

Email remains the most widely used communication tool in business — and unfortunately, one of the most abused. As organizations continue to strengthen their defenses, cybercriminals have evolved their techniques just as quickly. One of the simplest yet most effective threats is email spoofing, a tactic that fuels phishing, fraud, and business email compromise (BEC) attacks.

In 2025, spoofing remains a core component of global phishing campaigns, which continue to grow in both volume and sophistication. Cybersecurity reports warn that nearly half of all companies still do not have a DMARC (Domain-based Message Authentication, Reporting, and Conformance) policy configured, leaving them vulnerable to spoofed messages that appear to come from trusted internal or external senders.[1]

What Is Email Spoofing?

Email spoofing occurs when attackers forge the "From" address to make an email look legitimate. This allows them to impersonate:

- Executives
- Vendors
- Internal departments
- Well-known brands

Because email protocols were not originally built with strong authentication in mind, spoofing remains an easy gateway for attackers to deliver convincing phishing messages.

In modern phishing campaigns, spoofed emails are often enhanced through automation and artificial intelligence, making it harder for traditional security tools and employees to recognize.[2]

Even when domains are properly secured, threat actors can attempt spoofing by making small changes to the send from email address. For example, two spoofing attempts to our parent organization over the past few months have involved fraudulent email addresses (@sedgvick.com; or @Sedwick.com). Note the slight misspellings of "Sedgwick" in the email addresses. Consistent cyber security awareness training can help prevent this type of spoof.

Why Email Spoofing Is Still a Serious Threat

Recent threat intelligence data highlights how serious the spoofing problem remains:

[1] 2025 EMAIL THREATS REPORT - assets.barracuda.com

[2] Phishing Statistics 2025: AI, Behavior & $4.88M Breach Costs

- More than three-quarters of companies are not actively preventing spoofed emails, increasing the likelihood that employees will receive fraudulent messages.[3]
- Spoofing is a core tactic behind the surge in phishing attacks, which have reached millions of incidents per month from 2023 to 2025.[4]
- AI-enhanced phishing has caused a staggering 1,265% increase in malicious emails, many of which rely on spoofed domains or identities.[5]
- Business Email Compromise — heavily reliant on spoofing techniques — caused $2.7 billion in losses in the U.S. alone.[6]

The combination of spoofing, AI-driven content generation, and social engineering continues to make email the #1 attack vector for initial access across organizations of all sizes.[7]

How Email Spoofing Impacts Organizations

The costs of a successful spoofing attack extend far beyond the initial compromise:

- Financial Loss: BEC attacks frequently lead to fraudulent wire transfers or invoice payments.
- Data Breach Risk: Spoofed emails often serve as the first step in credential theft or malware installation.
- Reputational Damage: Attackers who impersonate your brand can erode customer trust.
- Operational Disruption: Even a single compromised account can trigger widespread incident response and downtime.

In 2025, organizations continue to experience more than 8,000 data breaches in the first half of the year alone, underscoring the scale of email-enabled threats.[8]

How to Protect Your Organization From Email Spoofing

The good news: spoofing is preventable with the right controls and practices. Security experts recommend the following:

1. **Implement SPF, DKIM, and DMARC**
   Major email providers — including Google, Yahoo, and Microsoft — now require these protocols for improved deliverability and to combat spoofing. SPF and DKIM authenticate messages, while DMARC adds policy enforcement and reporting.
2. **Enforce a Strong DMARC Policy (Reject or Quarantine)** [9]
   Many organizations publish DMARC but fail to enforce it. Spoofing attempts continue to thrive when DMARC is set to "none."

---

[3] 2025 EMAIL THREATS REPORT - assets.barracuda.com
[4] Email Phishing and DMARC Statistics- 2025 Security Trends
[5] Phishing Statistics 2025: AI, Behavior & $4.88M Breach Costs
[6] Phishing Statistics 2025: AI, Behavior & $4.88M Breach Costs
[7] Phishing Statistics 2025: AI, Behavior & $4.88M Breach Costs
[8] Email Phishing and DMARC Statistics- 2025 Security Trends
[9] Email Security Threats and Statistics 2025

3. **Use AI-Enhanced Email Security Tools**
   Attackers are already using AI; defenses must keep pace. AI-driven email filtering can detect polymorphic phishing content and unusual patterns.
4. **Invest in Employee Awareness Training**[10]
   The human element is involved in over 60% of breaches, making ongoing training critical. Behavioral phishing training has been shown to reduce incidents by up to 86%.
5. **Monitor for Impersonation Attempts**[11]
   Use domain monitoring tools to detect unauthorized sources attempting to send on behalf of your organization.

Final Thoughts

Email spoofing remains one of the most deceptively simple and dangerous cyber threats facing organizations today. As attackers increasingly leverage automation and AI, traditional defenses alone are no longer sufficient. The combination of strong email authentication, modern security tools, and well-trained employees provide the best defense against this persistent threat.

A small step — like implementing and enforcing DMARC — can dramatically reduce risk and safeguard both your brand and your people.

The TCRMF Cyber Risk Services Advisor has started to schedule Incident Response Plan Tabletop Testing visits for members. To be included on the schedule, contact Lee Cain, Cyber Risk Services Advisor, at 512-619-1437 or Lee.Cain@sedgwick.com.

[10] Phishing Threat Trends Report - knowbe4.com
[11] Phishing Trends Report (Updated for 2025) - Hoxhunt