Report | April 2026

Email Spoofing Threats Targeting the GCC Region

CTM360®

INDUSTRY	COUNTRY	REGION	DATE
Banking	GCC	GCC	Apr, 2026

Summary

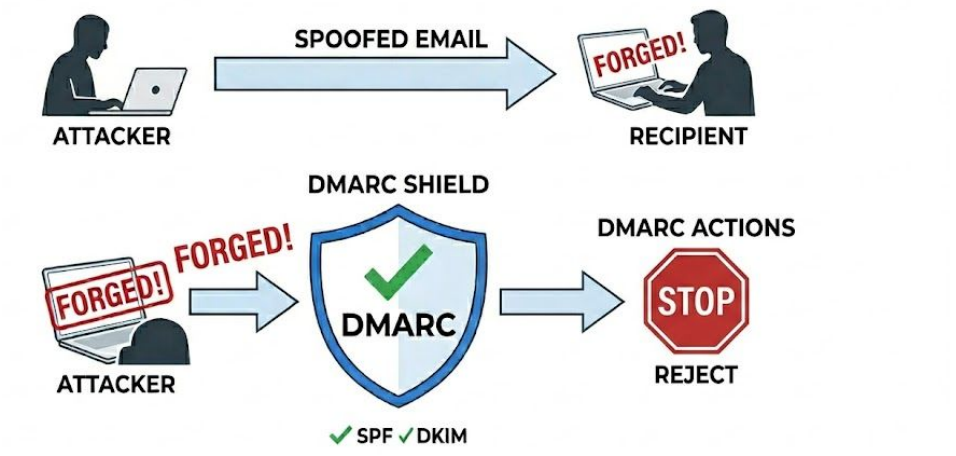
As part of **CTM360's** DMARC management services, our specialized email security platform, **DMARC360**, has identified a sophisticated, large-scale email spoofing campaign targeting prominent entities within the GCC banking sector.

Detailed analysis of DMARC aggregate reports reveals that threat actors are leveraging a deceptive infrastructure to impersonate legitimate financial organizations, aiming to distribute high-volume fraudulent communications to unsuspecting recipients. To date, this campaign has distributed more than **250K** unauthorized emails, highlighting a coordinated effort to exploit brand trust and bypass traditional security perimeters.

Understanding The Threat: What is email Spoofing and the Protective Role of DMARC?

To establish a baseline for defense, it is critical to understand the mechanics of the attack and the primary protocol used to neutralize it.

- **Email Spoofing Definition:** A technique where attackers forge the "From" address of an email to impersonate a trusted organization.
- **The Goal:** Attackers use spoofing to trick recipients into making unauthorized financial payments or revealing sensitive data.
- **DMARC's Role:** A protocol that builds on SPF and DKIM to verify that the sender is authorized to use the domain.
- **The Power of Enforcement:** Implementing a DMARC "Reject" policy (p=reject) allows mail servers to block fraudulent emails before they reach the recipient's inbox.



Technical Infrastructure & Observations

The following table details the origin and approach of the fraudulent traffic, as identified through DMARC forensic and aggregate reporting.

Attacker's Source IPs	**45[.]86[.]xxx[.]xxx**	**2a10[:]1fc0[:]a[:]0[:]216[:]xxxx[:]xxxx[:]xxxx**
Deceptive PTR (Reverse DNS)	mail[.]sharjahxxxx[.]xxx **Lookalike domain**	-
Geo Location	Estonia	United Kingdom
Network Owner	BlueVPS OÜ	Clouvider Limited
Approach	Mimicking a legitimate subdomain as IP PTR	IP did not have a PTR (reverse DNS) record
Detection	Activity was immediately flagged because the emails sent from this source IP were failing SPF, DKIM, and DMARC checks. An attacker distributed spoofed emails to large numbers of recipients, including invalid addresses, which caused the spoofed domain to receive numerous non-delivery reports (NDRs) even though it never sent the original emails, a phenomenon known as **backscatter.**	

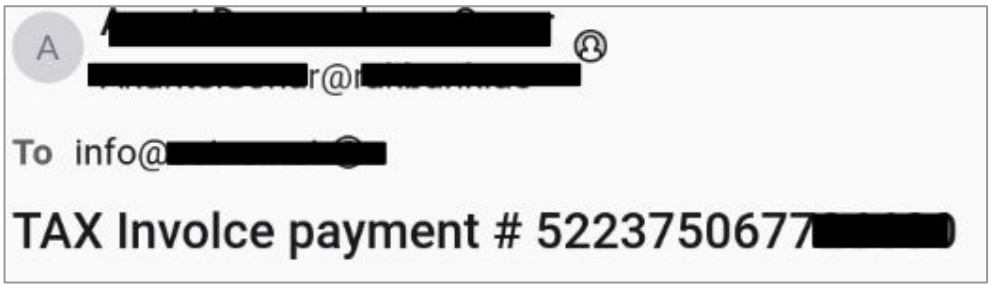
However, since these IPs were neither authorized by the domain's SPF record nor able to pass DKIM authentication, the resulting DMARC failure caused the activity to be promptly flagged in DMARC reports.

Campaign Scale and Volume

According to the observed DMARC reports, this campaign has generated more than **250K** unauthorized emails as seen through the DMARC reports of several DMARC360 members in the GCC.

Email Spoofing Incident Example

Based on the forensic report data, the attacker is sending fraudulent emails that impersonate different well-known GCC banks, using deceptive subject lines such as 'TAX Invoice payment' to pressure recipients into making unauthorized financial payments.



Effectiveness of DMARC Policy

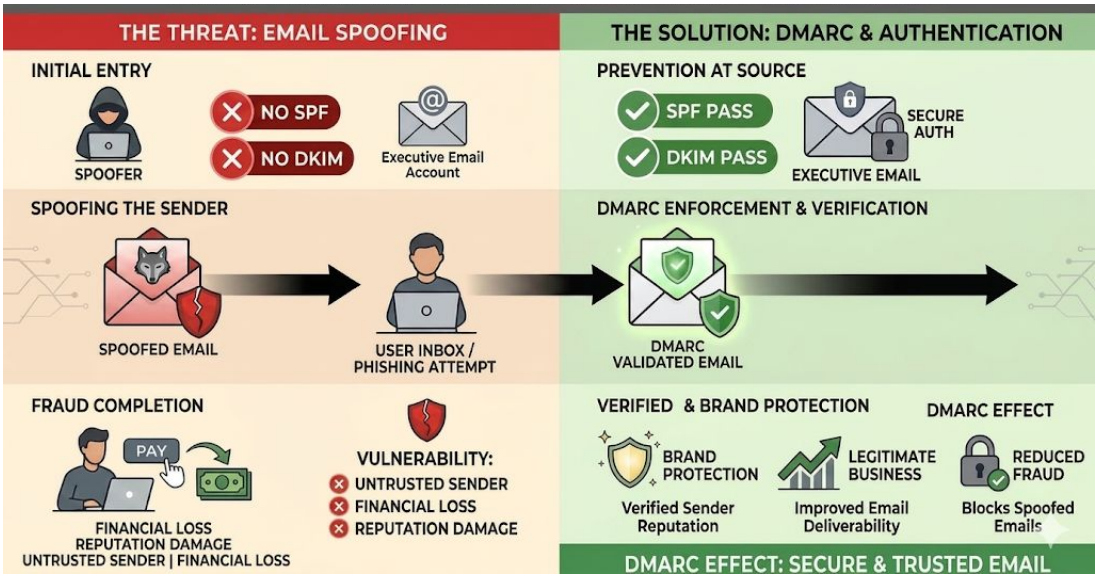
The analysis shows that the majority of spoofed emails were successfully rejected due to the domain's DMARC "reject" policy.

With DMARC set to p=reject, receiving mail systems were able to identify failures in SPF and DKIM authentication and block these messages accordingly. This confirms that a properly configured and enforced DMARC policy is highly effective in mitigating large-scale spoofing attempts.

In some instances, these emails may still appear as "rejected" in recipient email gateway logs, which is expected and indicates that the policy is operating as intended.

Shift of Responsibility to Recipients

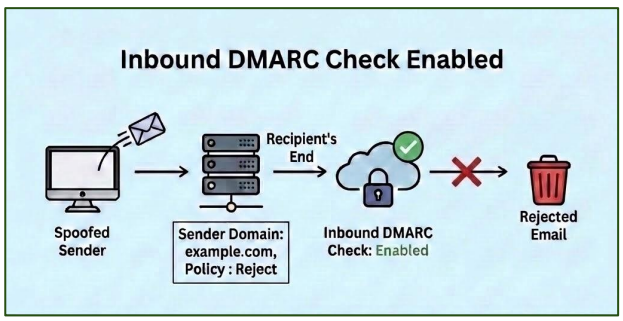
NOTE: The sender enforced a "reject" DMARC policy, therefore, any failure to block spoofed emails lies with recipients not checking or honoring DMARC policy, which is beyond the sender's control.

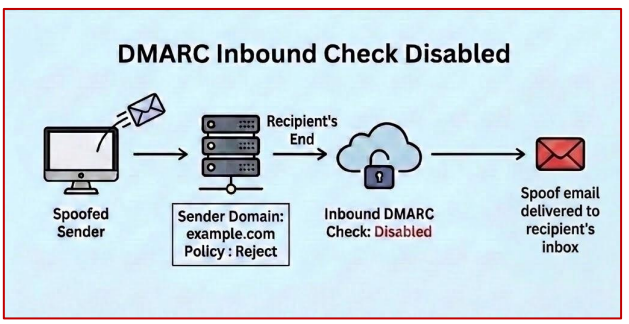


Strategic Recommendations

To safeguard your domains against such spoofing campaigns and protect your brand reputation, we recommend implementing the following:

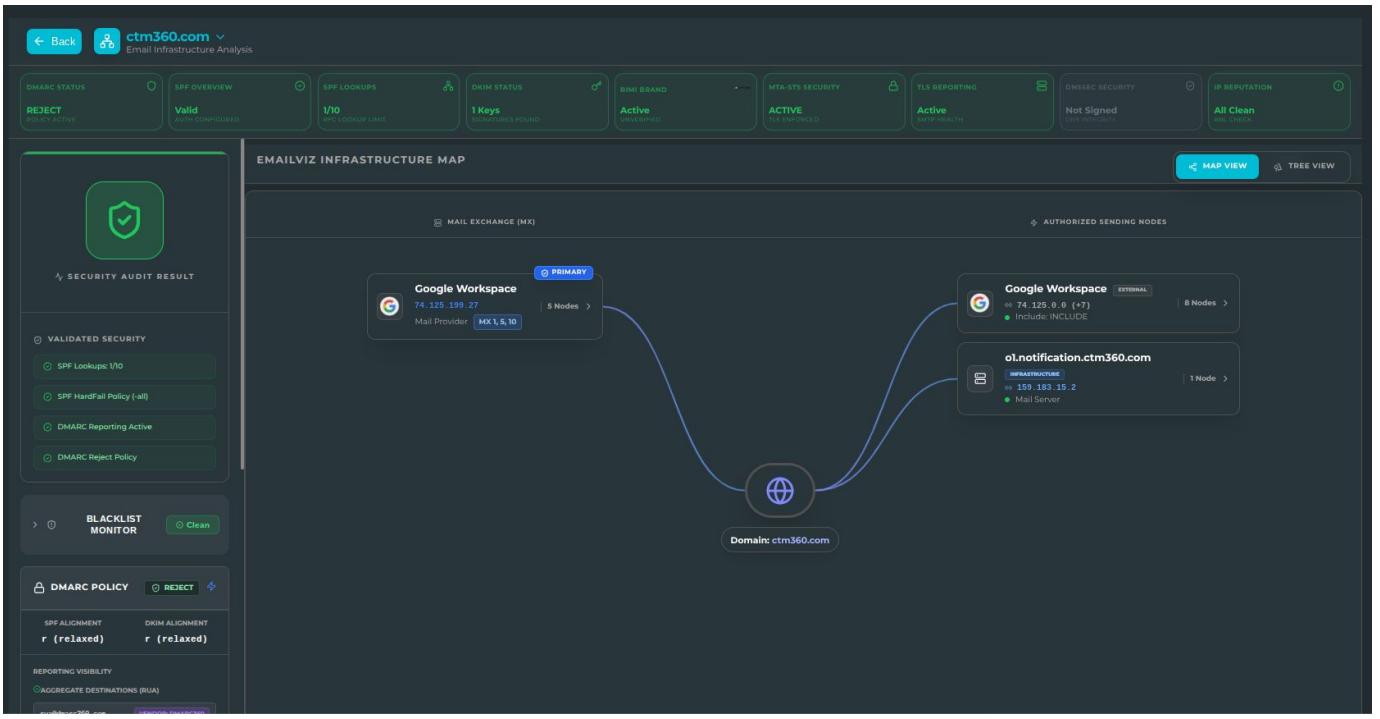
- **Establish Strong Foundations:** Configure SPF, DKIM, and DMARC with strict policies to prevent attackers from mimicking your domain.
- **Activate Comprehensive Reporting:** Include both RUA (Aggregate) and RUF (Forensic) tags in your DMARC record. This allows your DMARC provider to analyze spoofing samples, identify malicious URLs, and take immediate action against threats.
- **Transition to Full Enforcement:** Progress to a p=reject policy to automatically block unauthorized mail. Before reaching this stage, verify that all authorized senders are correctly aligned to ensure zero disruption to business communications.
- **Leverage Advanced Analytics:** Utilize a specialized monitoring DMARC tool to gain visibility into your email ecosystem. This simplifies the detection of spoofing campaigns, uncovers security gaps, and streamlines the resolution of configuration issues.
- **Enable Backscatter Protection in your email gateway:** Activate backscatter protection in the email gateway to filter out illegitimate Non-Delivery Reports (NDRs). This ensures that only bounce messages from emails actually sent by the organization are accepted, eliminating the operational noise caused by spoofing attacks.
- **Implement BIMI (Brand Indicators for Message Identification):** Deploy BIMI to display your organization's official logo next to authenticated emails in the recipient's inbox. This provides an immediate visual cue that the email is trusted and verified.
- **Ensure DMARC Checks Are Enabled for Inbound Emails: Liability shifts to** recipients for enabling DMARC check on their **inbound emails** as they may still receive spoofed emails from domains where DMARC is configured.





Note: Major cloud providers like Google and Microsoft **enable inbound DMARC check** by default. However, if you are utilizing an **on-premises email gateway**, you must manually ensure that inbound DMARC verification is **enabled** to maintain email security.

- **Utilize CTM360 EmailViz:** EmailViz module in our HackerView platform, performs external health checks on your domains. It provides a comprehensive analysis of your email infrastructure to ensure all authentication protocols are correctly configured and optimized.



Conclusion

This campaign's persistence proves that email spoofing remains a high-impact threat vector. However, organizations utilizing a strictly enforced DMARC policy successfully neutralized the threat. By implementing these safeguards, your organization can transform passive monitoring into a proactive defense shield.

CTM360 enables you to navigate this transition with confidence. Our **DMARC360** platform helps you implement the DMARC framework safely, ensuring you reach full enforcement without impacting the deliverability of your legitimate emails. By providing granular visibility and expert management, **CTM360** secures your ecosystem to effectively protect your domains against spoofing, safeguarding both your brand reputation and business continuity.

ABOUT US

CTM360 provides a consolidated platform that includes external attack surface management, digital risk protection (brand protection & anti-phishing, data leakage protection, and unlimited managed takedowns), security ratings, third party risk management, email intelligence (dmarc) and cyber threat intelligence.

CONTACT US:

+973 77 360 360

info@ctm360.com

www.ctm360.com

21st Floor, East Tower Bahrain Financial Harbour, Kingdom of Bahrain