# 

# Email Threat Investigation Report

**Analyst:** Sceptre

**Date:** 21 October 2025

**Time zone:** London (UTC+01:00)

**Environment:** Microsoft 365 Defender (Email & Collaboration)

## Investigation Summary – What Happened?

A phishing email was delivered to bob@socialgore.onmicrosoft.com’s junk folder instead of being quarantined.  
The email originated from billing@marketplacebusiness.co.uk and contained a suspicious link to neon-lab.test.  
Authentication checks for SPF, DKIM, and DMARC all failed.  
The purpose of this investigation was to analyse how the email was handled, whether other users were targeted, and confirm whether any links were clicked.

## Stakeholder Impact – Who was involved?

Primary recipient: bob@socialgore.onmicrosoft.com  
Additional user: jenny@socialgore.onmicrosoft.com  
  
The incident was contained within a controlled testing environment. No real users or production mailboxes were impacted.

## Findings – What did I find?

1. The email was delivered to Junk, not Quarantine.  
2. The sender billing@marketplacebusiness.co.uk had no valid SPF, DKIM, or DMARC configuration.  
3. The Reply-To domain differed from the From domain, a strong indicator of spoofing.  
4. Message headers included a custom X-Lab: marketplace-campaign-2025.  
5. User click telemetry from UrlClickEvents confirmed one click to http://neon-lab.test/sim-order-review.  
6. Multiple recipients (Bob and Jenny) received similar messages, confirmed via KQL searches.

## Immediate Actions – When did this occur and is it still happening?

Initial delivery: 21 October 2025 at 14:22 (UTC+01:00)  
Click event recorded: 21 October 2025 at 14:33 (UTC+01:00)  
The campaign consisted of four emails, all received within the same hour.  
No further emails were observed after initial testing.  
Issue resolved by raising the DFIR-Sceptre-AntiPhish policy to Priority 1 so it evaluates before Microsoft defaults.

## Affected Systems and Data – Where in the environment did this happen?

System: Microsoft 365 Defender (Email & Collaboration)  
Mailbox: Bob’s mailbox (Junk folder)  
Domains involved:  
- marketplacebusiness.co.uk (spoofed sender)  
- neon-lab.io (reply-to domain)  
- neon-lab.test (URL destination)

## Indicators of Compromise (IoCs)

Sender Address: billing@marketplacebusiness.co.uk - Spoofed sender used for phishing  
Reply-To: reply@neon-lab.io - Redirects to fake business domain  
URL: http://neon-lab.test/sim-order-review - Phishing link used for simulation  
IP Address: 114.29.236.247 - Source IP (Hong Kong)  
X-Header: X-Lab: marketplace-campaign-2025 - Custom header inserted by spoofing tool  
Message-ID: <20251021132159.229693EC4@emkei.cz> - Originates from emkei.cz spoofing service

## Root Cause – Why did this happen?

The phishing email originated from a spoofed sender pretending to be Marketplace Business, aiming to trick recipients into clicking a fake order-related link.  
The attacker exploited the absence of email authentication controls (SPF, DKIM, and DMARC) on the spoofed domain, allowing the message to appear legitimate.  
The message successfully reached the recipient’s junk folder, demonstrating how unauthenticated messages can still bypass certain detection layers if they don’t meet quarantine thresholds.

## Nature of the Attack – How did this happen?

The phishing message was crafted to resemble a legitimate order update from Marketplace Business, a brand name chosen to appear trustworthy and familiar.  
The attacker embedded a link to http://neon-lab.test/sim-order-review, a fake order review page intended to lure users into clicking.  
Because the .test domain isn’t part of the public DNS and lacks reputation data, the link didn’t trigger reputation-based filtering or known-malicious indicators, allowing the message to pass initial checks.

## Recommendations – What steps should be taken to reduce risk or stop the activity?

1. Maintain DFIR-Sceptre-AntiPhish policy at Priority 1.  
2. Enable quarantine for all messages failing SPF, DKIM, or DMARC authentication.  
3. Conduct ongoing user awareness training on recognising mismatched sender and reply domains.

Investigation completed by Sceptre – London (UTC+01:00).