

# **Phishing Email Analysis Report**

**Analysis Of A Suspicious Email  
Conducted In An Isolated  
Virtual Environment**

**By:  
Junaid AbdulRahman A  
Cybersecurity Analyst**

**Date:29 November 2025**

## **1. Executive Summary**

A thorough analysis of a suspicious email conducted in an isolated virtual environment with multiple analysis techniques revealed a sophisticated phishing attempt targeting sensitive information. The email disguised as a transaction alert, to deceive user into clicking a malicious link embedded in “cancel transaction” button. Investigation, including the header inspection, sender IP address and the URL reputation analysis confirmed the suspicious email as a phishing email designed to exfiltrate sensitive information.

## 2. Email Metadata Analysis

## 2.1 Sender Information

- **Sender IP Address:** 23.251.234.51
  - **Sending Server:** SJ1PR19MB6332.namprd19.prod.outlook.com  
(2603:10b6:a03:455::6)
  - **Return-Path:** 0106018a71901afd-bbc67141-d1e8-42bc-89a7-4877f9564d7d-000000@apnorptheast-1.amazonaws.com

- **IP Reputation Check (AbuseIPDB):** The sender IP address was identified in the AbuseIPDB database, with multiple reports including a recent report just 8 hours ago, indicating the ongoing malicious activity.

The screenshot shows a dark-themed web interface for AbuseIPDB. At the top left is the logo "AbuseIPDB". At the top right is a menu icon. Below the header, a message states "23.251.234.51 was found in our database!". A note below it says "This IP was reported 16 times. Confidence of Abuse is 25%:" followed by a question mark icon. A large orange button displays the confidence level "25%". Below this, a table lists the following information:

ISP	Amazon Web Services, Inc.
Usage Type	Data Center/Web Hosting/Transit
ASN	<a href="#">AS16509</a>
Hostname(s)	e234-51.smtp-out.ap-northeast-1.amazonaws.com
Domain Name	amazon.com
Country	United States of America
City	Seattle, Washington

Below the table, a note says "IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly." Two green buttons are present: "REPORT 23.251.234.51" and "WHOIS 23.251.234.51".

At the bottom, a section titled "IP Abuse Reports for 23.251.234.51:" provides summary statistics: "This IP address has been reported a total of 16 times from 10 distinct sources. 23.251.234.51 was first reported on October 26th 2023, and the most recent report was 8 hours ago."

## 2.2 Email Authentication Results

- **SPF (Sender Policy Framework): PASS**
  - The SPF record validated successfully, suggesting that the sending server is authorized to send mail on behalf of the domain. However, SPF alone is not a reliable indicator of legitimacy.
- **DKIM (DomainKeys Identified Mail):** The DKIM signature is validly structured and shows the email was signed by Amazon SES using RSA-SHA256. However this does not also validate its legitimacy.
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance): NONE**
  - The domain lacks a DMARC policy, increasing the likelihood of unauthorized use and spoofing.
- **Return-Path:** Different from “FROM” address, indicating spoofing attempt.

# 3. Content Analysis

## 3.1 Text Body

- Urgency tactics(You sent 0.79 ETH over the Ethereum Network)
- Poor grammar and spelling errors.

## 3.2 Embedded URL Analysis

- Extracted URL Found in link: <https://firesonic.ca>
- Performed scans on the extracted URL using the following tools:
  - **URLScan.io**

The screenshot shows the URLScan.io interface for the domain `firesonic.ca`. Key details include:

- Submitted URL: <https://firesonic.ca/>
- Effective URL: <https://firesonic.ca/404.html>
- Submission: On November 29 via manual (November 29th 2025, 10:58:27 am UTC) from NG (United States) – Scanned from CA (Canada)
- TLS certificate: Issued by Sectigo Public Server Authentication ... on August 11th 2025. Valid for a year.
- Scans: firesonic.ca scanned 9 times on urlscan.io
- Verdict: No classification
- Live information: Google Safe Browsing: No classification for firesonic.ca, Current DNS A record: 198.57.247.141 (AS46606 - UNIFIEDLAYER-AS-1, US), Domain created: April 10th 2023, 17:55:59 (UTC), Domain registrar: DOMAINscand.ca Inc.
- Domain & IP information: IP/ASNs, IP Detail, Domains, Domain Tree, Links, Certs, Frames
- Screenshot: Shows a 404 error message: "Sorry, this page doesn't exist. Please check the URL or go back a page. 404 Error: Page Not Found."
- Page Title: 404 Error
- Page URL History: 1. <https://firesonic.ca/> [HTTP 302] <https://firesonic.ca/404.html> [Page URL]

- **VirusTotal**

The screenshot shows the VirusTotal interface for the domain `firesonic.ca`. Key details include:

- Community Score: 2 / 98
- Security vendors flagged as malicious: 2/98
- URL submitted: <https://firesonic.ca/>
- Last Analysis Date: 2 months ago

- **Symantec SiteReview**

The screenshot shows the Symantec SiteReview interface for the domain `firesonic.ca`. Key details include:

- URL submitted: <https://firesonic.ca:443/>
- This URL is categorized as a security risk
- Phishing
- Last Time Rated/Reviewed: > 7 days

### 3.3 Threat Intelligence on Domain

- **Domain:** firesonic.ca

A WHOIS lookup revealed  
Registrar DOMAINScanada.ca Inc.  
Registered On:2023-04-10

The domain appears to be registered 2 years back and lacks a solid reputation, which is consistent with common phishing infrastructure.

## 4. Threat Intelligence Analysis

### 4.1 IP Address Reputation

- **IP Address:** 23.251.234.51
- The IP address has been reported multiple times on AbuseIPDB for malicious activity. Indicating active abuse, with reports linked to spam, and suspicious traffic. This IP should be treated as hostile and blocked in security systems.

### 4.2 Indicators of Compromise (IoCs)

- Email Header Anomalies: Missing DMARC, mismatched Return-Path and sending server.
- Malicious URL: The URL embedded in the email links to a suspicious domain.
- Malicious IP: 23.251.234.51

## 5. Threat Assessment

- **Type of Attack:** Credential harvesting via phishing email.
- **Risk Level:** High (active malicious links and IP address, multiple abuse reports).
- **Potential Impact:** financial fraud, identity theft.

## 6. Recommended Actions

- Block sender address and associated IPs at firewall and email gateway.
- Add malicious URL to URL filtering blacklist.
- Quarantine and delete suspicious emails from user inboxes.
- Educate users on identifying phishing attempts (urgent language, mismatched URLs).
- Report domains/IPs to relevant CERT authorities.

## 7. Conclusion

These analysis **confirm that the email is part of an active phishing campaign** designed to deceive user into divulging sensitive information and potentially execute malicious code. Multiple indicators including spoofed sender domains, mismatched return paths, missing DMARC checks, and malicious URLs multiple reported IP address confirms, that the email did not originate from a legitimate source. With the presence of urgency in the subject line and body text, combined with embedded links redirecting to fraudulent URL, aligns with common phishing tactics aimed at credential harvesting and financial fraud.