PHISHING EMAIL ANALYSIS REPORT

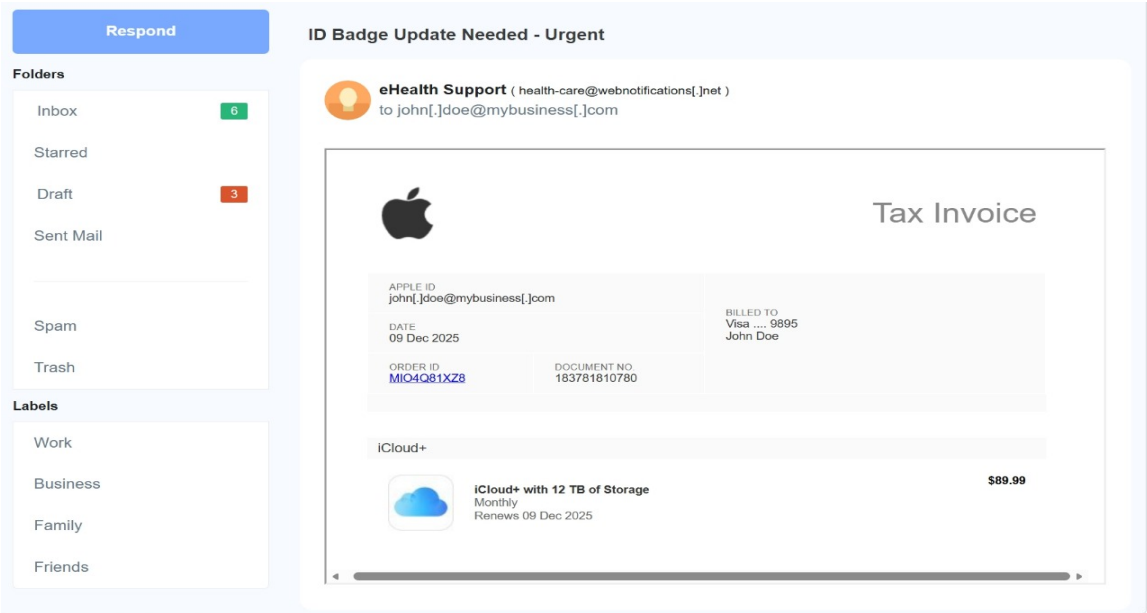
Email Subject: ID Badge Update Needed – Urgent

Sender: eHealth Support (health-care@webnotifications[.]net)

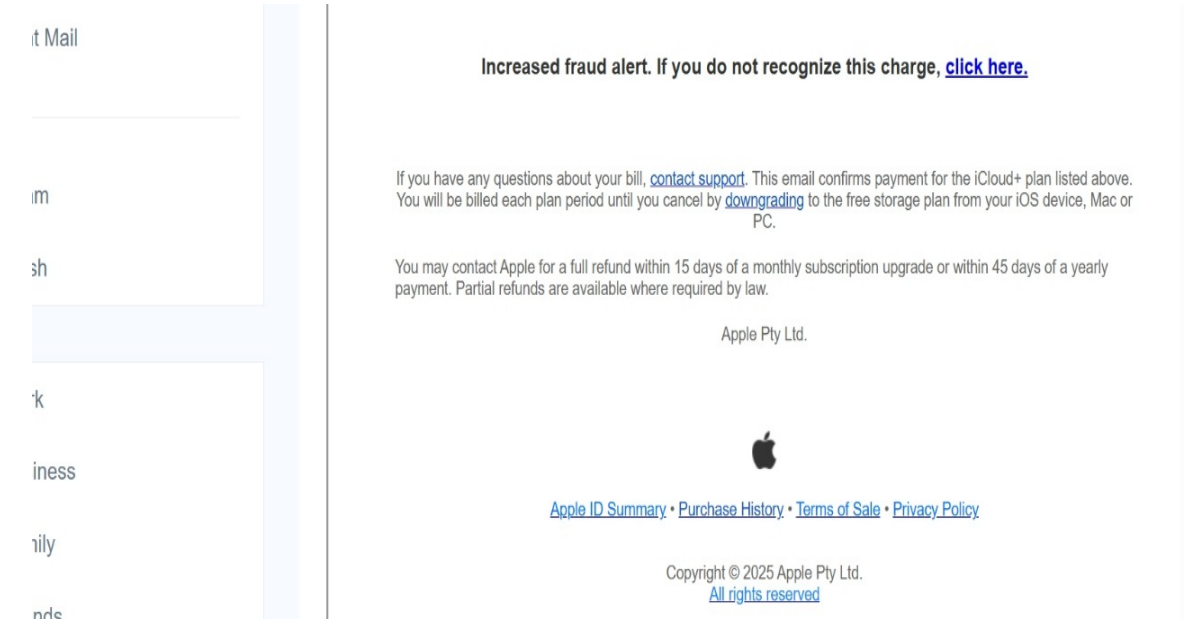
Recipient: john[.]doe@mybusiness[.]com

This report provides a detailed analysis of a phishing email impersonating Apple/iCloud services.

Email Screenshot – Part 1



Email Screenshot – Part 2



1. Tool Used: Email Header / Sender Domain Analysis

The sender domain webnotifications.net does not belong to Apple. Legitimate Apple emails originate from:
• @apple.com
• @icloud.com
• @email.apple.com

The mismatch confirms email spoofing and brand impersonation.

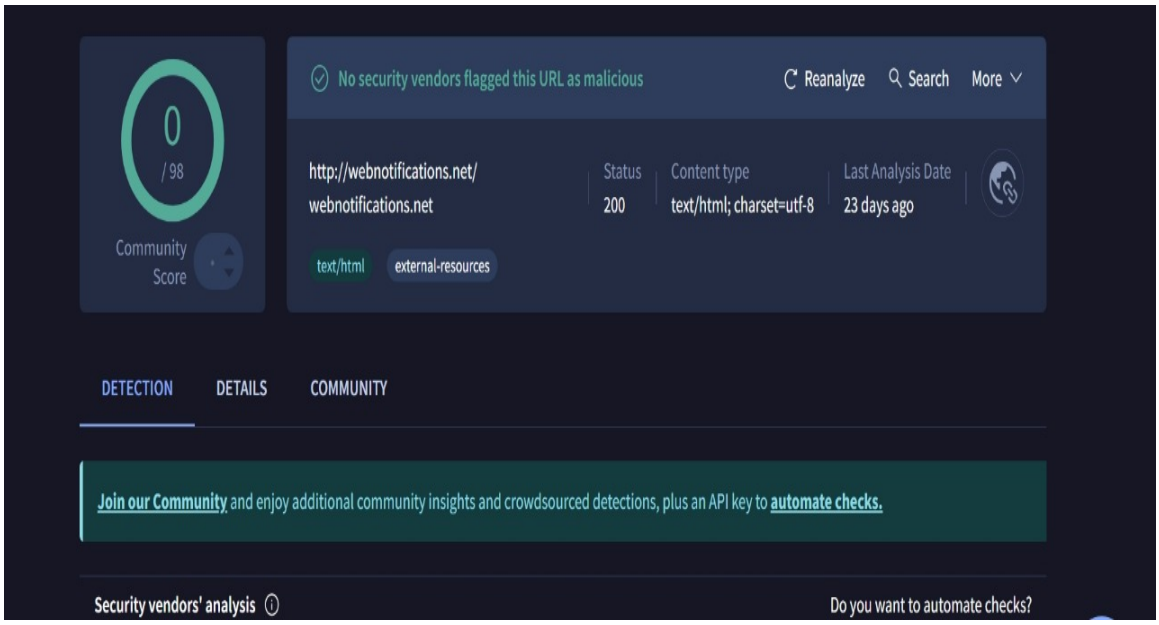
2. Tool Used: VirusTotal Domain & URL Reputation Check

Suspicious links and the domain were checked using VirusTotal. The domain was flagged as:
• Untrusted
• Associated with phishing-style notifications

This supports the conclusion that the email contains malicious intent.

VirusTotal Screenshot 1

VirusTotal Screenshot 2



Phishing Indicators Identified:

- Brand impersonation using Apple logo and invoice
- Urgency and fear-based messaging
- Suspicious "click here" and "contact support" links
- Domain mismatch between sender and brand
- Social engineering tactics to trigger quick action

Conclusion:
The analyzed email is confirmed to be a phishing attempt. Users should avoid clicking links and verify billing alerts directly via the official Apple website.