Phishing Email Analysis Report

Sample Source: Screenshot of a GitHub-like phishing email

Phishing Indicators Identified:

1. Spoofed sender domain: GitHub@bigdogdomains.co (not a legitimate GitHub domain)
2. Urgent call to action: "Verify your email address" with a suspicious link
3. Brand impersonation: GitHub logo and name used to deceive users
4. No personalization: Uses "Demo!" instead of actual user name
5. Link redirection: Button likely points to a phishing domain (not shown but commonly obfuscated)
6. Unusual sender domain: bigdogdomains.co, not affiliated with GitHub

Simulated Email Header Analysis:

Return-Path: <GitHub@bigdogdomains.co>

Received: from unknown (HELO mx.mailserver123.com) [193.105.55.11]

by mail.example.com with ESMTP; Tue, 28 May 2025 11:39:01 +0000

Received-SPF: Fail (bigdogdomains.co: domain does not designate this IP as a valid sender)

Authentication-Results: spf=fail; dkim=none; dmarc=fail

From: "GitHub" <GitHub@bigdogdomains.co>

To: ethan@hooksecurity.co

Subject: Please verify your email address

Conclusion:

This email demonstrates multiple phishing traits, including spoofed identity, unauthorized domain use, and social engineering tactics. It is designed to mislead the recipient into clicking a link under the impression it's from GitHub.