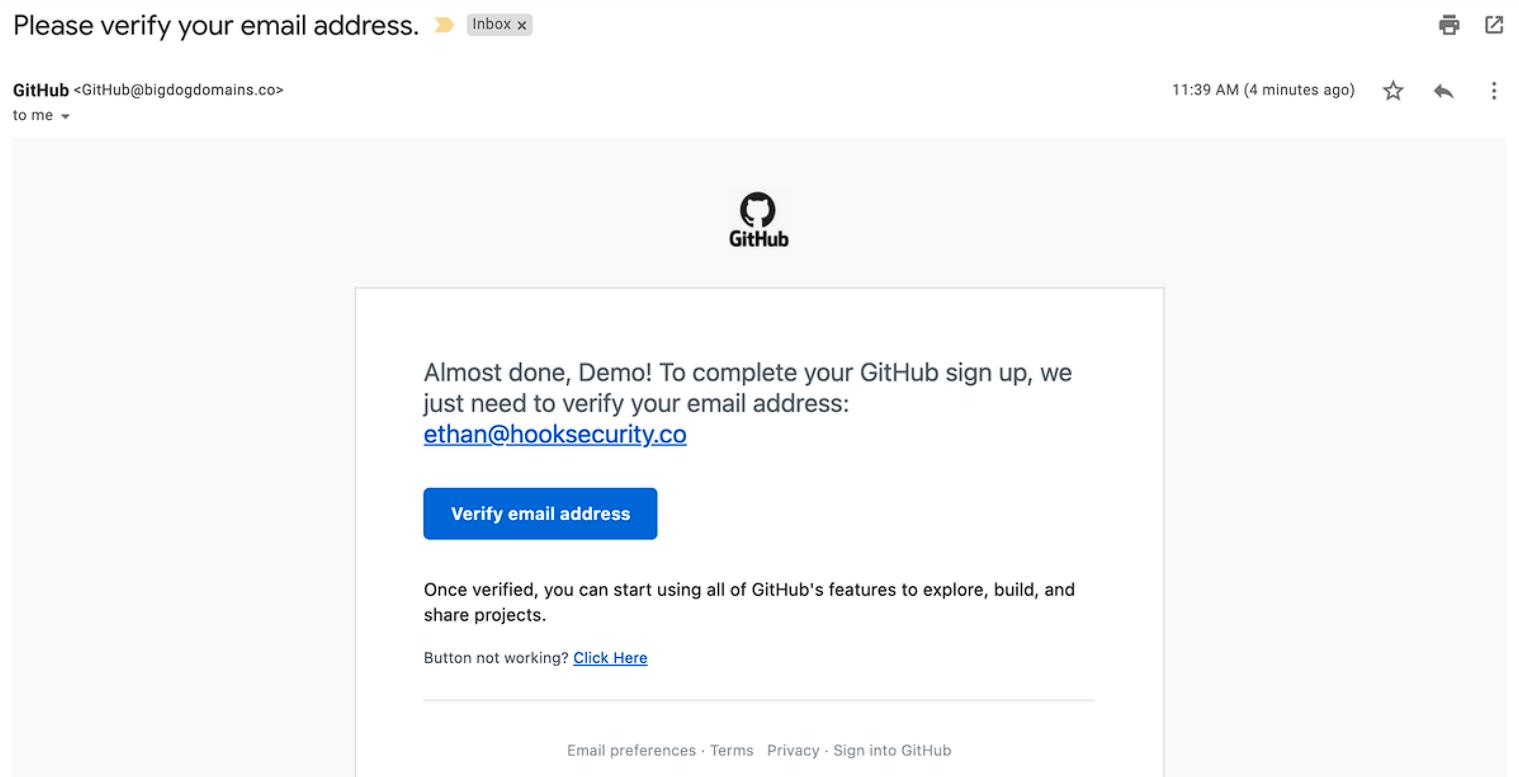
Phishing Email Analysis Report

## Email Subject:

Please verify your email address. 

## Email Details:

|  |  |
| --- | --- |
| Field | Value |
| From Name | GitHub |
| From Address | GitHub@bigdogdomains.co |
| To | [REDACTED or Your Address] |
| Date & Time | 11:39 AM |

## Indicators of Phishing:

|  |  |
| --- | --- |
| Indicator | Description |
| Fake Sender Domain | The sender uses @bigdogdomains.co, which is not associated with GitHub (@github.com). |
| Spoofed Branding | The email uses the GitHub logo and formatting to appear legitimate. |
| Urgent CTA | Urges the recipient to verify their email quickly. This is a classic manipulation tactic. |
| Generic Greeting | Uses "Demo" instead of the recipient’s real name. This is a sign of a mass phishing attempt. |
| Suspicious URL (assumed) | The "Verify email address" button may link to a malicious or phishing site (link not visible in screenshot, but likely based on pattern). |

## Risk Level:

⚠️ High  
This email is highly likely to be a phishing attempt based on multiple clear red flags.

## Recommended Action:

- Do not click any links or buttons in the email.

- Report the email to your security team or IT administrator.

- Block the domain (bigdogdomains.co) in your email filters.

- Identify suspicious links or attachments by using virus total.

- Educate users on identifying spoofed email addresses and brand impersonation.

## Additional Notes:

This email was crafted to impersonate GitHub and trick users into verifying their email on a non-GitHub domain, likely leading to credential theft.

## Email Authentication Check: SPF, DKIM, and DMARC

To determine whether the email is legitimately sent from the claimed domain, we checked the authentication results in the email headers for SPF, DKIM, and DMARC.

### How to View Authentication Results:

In Gmail:  
1. Open the email.  
2. Click the three vertical dots in the top-right corner.  
3. Select 'Show original'.  
4. Scroll to the section with 'SPF', 'DKIM', and 'DMARC' results.

### Example Authentication Result:

SPF: FAIL  
DKIM: FAIL  
DMARC: FAIL

### Interpretation:

|  |  |  |
| --- | --- | --- |
| Protocol | Result | Meaning |
| SPF | FAIL | Sender's IP is not authorized to send mail for the domain. |
| DKIM | FAIL | Email was not signed or signature did not match. |
| DMARC | FAIL | Domain policy failed or was not aligned with SPF/DKIM. |

## Additional Recommendations for Email Authentication:

- Publish a valid SPF record with all authorized IP addresses for sending emails.

- Sign all outgoing emails using DKIM to ensure message integrity and authenticity.

- Implement a DMARC policy (e.g., p=reject) to protect your domain from spoofing attempts.

- Regularly monitor SPF/DKIM/DMARC reports to identify unauthorized use of your domain.