

|  |  |  |
| --- | --- | --- |
|  | Github |  |

Phishing Email Example

Phishing Email Analysis Report

1. EMAIL Overview :

o From: GitHub GitHub@bigdogdomains.co   
o Subject: Please verify your email address.

o Time: 11:39 AM (4 minutes ago)   
o Recipient: To me (the user receiving the email)   
o Email Type: Account verification (purported GitHub sign up confirmation)

2.Senders Email Address Check:

o The email is supposedly from GitHub, but the sender email is GitHub@bigdogdomains.co.

o The legitimate domain for GitHub emails is usually github.com.

o The domain bigdogdomains.co is suspicious because it does not relate to GitHub or any known GitHub domain. This is a strong spoofing indicator

3.Email Header Anlysis:

o Email headers would show mismatches in the 'From' domain and sending IP

4. Link and attachment inspection:

 

|  |  |  |  |
| --- | --- | --- | --- |
|  | o | The email contains a call-to-action button "Verify email address" and a |  |

hyperlink: ethan@hooksecurity.co (email displayed), and a "Click Here" link for button not working.

o Hovering over these links (if you had the actual email) could reveal suspicious URLs that are not GitHub’s official domain.

o The domain in the sender email bigdogdomains.co might host a phishing site. o No attachments are visible, but phishing could occur solely by deceptive links.

5.Email body content analysis:

The email is trying to confirm email verification for GitHub account sign-up. This is a common phishing lure as hackers want to capture new account details.

●The greeting "Almost done, Demo!" is generic but references "Demo," suggesting it could be semi-personalized or just a placeholder.

●No urgent or threatening language used here, which is less typical but still a phishing approach via deception.

●The use of the email ethan@hooksecurity.co is suspicious as it doesn't match the sender domain and could be a bait address.

●The link text and actual URL domain likely mismatch (requires hover check).

●The domain bigdogdomains.co is inconsistent with GitHub, showing high likelihood of spoofing.

 