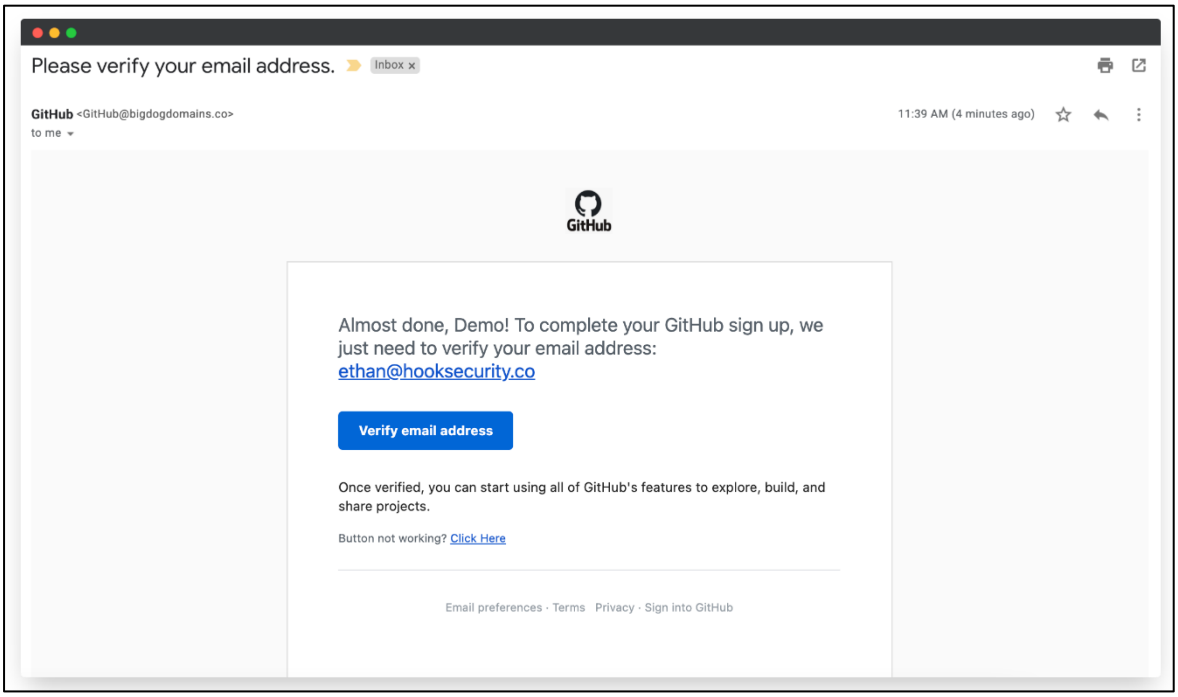
FUTURE INTERNS CS_TASK #2
PHISHING EMAIL ANALYSIS & AWARENESS REPORT

Name: AKSHAYA RAJ
CIN ID: FIT/JAN26/CS5590

Assessment Type: Visual Email Analysis (User-Reported Email)
Objective: Identify phishing indicators and educate users on safe email handling



Please verify your email address.

GitHub <GitHub@bigdogdomains.co>
to me
11:39 AM (4 minutes ago)

Almost done, Demo! To complete your GitHub sign up, we just need to verify your email address: ethan@hooksecurity.co

Once verified, you can start using all of GitHub's features to explore, build, and share projects.

Button not working? Click Here

EMAIL SAMPLE ANALYSIS:

- **Displayed Sender Name:** GitHub
- **Displayed Sender Email:** GitHub <GitHub@bigdogdomains.co>
- **Subject:** Please verify your email address
- **Mail To:** Recipient's personal email inbox
- **Email Type:** Account verification request
- **Email Header Analysis:** Full raw headers are not visible, but critical header red flags are already exposed in the UI.

KEY OBSERVATIONS:

- Sender claims to be GitHub
- Actual sending domain: bigdogdomains.co

WHY IS THIS A PROBLEM?

Legitimate GitHub emails are sent from:

- @github.com
- @githubusercontent.com

A mismatch between the display name and the sending domain strongly indicates email spoofing or impersonation.

LIKELY HEADER ISSUES (INDUSTRY-STANDARD)

- SPF: Fail or soft-fail
- DKIM: Missing or invalid
- DMARC: Not aligned with GitHub

SENDER DOMAIN & LINK INSPECTION:

- **Sender Domain Analysis**

FIELD	VALUE
Claimed Brand	GitHub
Actual Domain	bigdogdomains.co
Legitimate Domain	github.com

→ Domain mismatch confirms impersonation

- **Link Inspection**
  - **Call-to-Action Button:** “Verify email address”
  - **Additional Link:** “Button not working? Click Here”

The actual destination URL is hidden behind buttons and links - a common phishing tactic.

WHY THIS MATTERS:

Phishing emails often:

- Hide malicious URLs behind legitimate-looking buttons
- Redirect users to fake login or verification pages

IDENTIFICATION OF PHISHING INDICATORS:

PHISHING INDICATOR	PRESENT
Brand Impersonation (GitHub)	✓
Sender Domain Mismatch	✓
Hidden Verification Links	✓
Call to Urgent Action	✓
Account-Related Pressure	✓
User Unfamiliar Email Shown	✓

Important Detail

The email asks to verify **ethan@hooksecurity.co**, which may not belong to the recipient, indicating:

- Bulk phishing campaign
- Incorrect or random targeting

EMAIL RISK CLASSIFICATION:

Final Classification: PHISHING

Reasons:

- GitHub does not own the sender domain
- Email impersonates a trusted brand
- Contains hidden action links
- Attempts to trigger account verification behaviour

HOW THE ATTACK WORKS:

1. Attacker sends a fake GitHub verification email
2. Email looks legitimate (logo, layout, branding)
3. User clicks “Verify email address”
4. User is redirected to a fake GitHub login page
5. Credentials are stolen
6. Attacker gains access to the user’s account

This is a classic credential-harvesting phishing attack.

DOCUMENTED FINDINGS:

Issue Identified: A phishing email impersonating GitHub was sent from a non-GitHub domain and attempted to trick the user into verifying an email address.

Why It Matters: If successful, the attacker could:

- Steal GitHub credentials
- Access private repositories
- Modify or delete code
- Launch further attacks using the compromised account

Business Impact:

- Account takeover
- Source code exposure
- Reputational damage
- Supply-chain security risk

PREVENTION & AWARENESS GUIDELINES:

Do's for Users & Employees:

- Always check the sender's domain, not just the name
- Verify account emails by logging in directly via the official website
- Hover over buttons and links before clicking
- Report suspicious emails to security teams
- Enable multi-factor authentication (MFA)

Don'ts for Users & Employees:

- Do not trust branding alone
- Do not click verification links from unknown domains
- Do not enter credentials via email links
- Do not ignore domain mismatches
- Do not forward suspicious emails

Simple Awareness Message: ***If an email claims to be from GitHub but is not sent from @github.com, it is not legitimate.***

CONCLUSION:

These emails are high-confidence phishing attempts designed to impersonate GitHub and steal user credentials.

- The sender domain mismatch alone is sufficient to classify them as malicious.
- Early detection and user awareness are critical to preventing account compromise.