Phishing Email Analysis Report

1. Objective

To evaluate the provided GitHub notification email against common phishing indicators and determine its legitimacy.

2. Sample Email Overview

Subject: Notification of Third-Party OAuth Application Authorization

From: The GitHub Team (sent via a GitHub domain) **Date:** (Timestamp not provided)

Content Transcription:

Hey John!

A third-party OAuth application (AWS CodeBuild) with read:org and repo scopes was recently authorized to access your account. Visit https://github.com/settings/connections/applications/41387c6857fcb0509a45 for more information.

To see this and other security events for your account, visit https://github.com/settings/security-log

If you run into problems, please contact support by visiting https://github.com/contact

Thanks, The GitHub Team

3. Detailed Analysis

Aspect	Findings
Sender's Email Address	Expected to originate from `notifications@github.com` or a similar GitHub domain. No mismatch or spoofed domain is visible in the content.
Email Headers	Full headers not provided. A legitimate GitHub email typically passes SPF, DKIM, and DMARC checks—this should be verified via a header analyzer if in doubt.
Links & Destinations	All URLs use the `github.com` domain and point to official GitHub settings pages. Hover behavior reflects genuine GitHub SSL-protected links (https://).
Attachments	None.
Language & Tone	Informative and friendly. No urgent demands, threats, or scare tactics are used.
URL Mismatch	None detected. Link text and actual destinations both reference legitimate GitHub URLs.

Aspect	Findings
Spelling & Grammar	No errors. The copy uses correct punctuation, spelling, and consistent capitalization.
Visual Design & Branding	Matches GitHub’s standard styling: informal greeting, correct use of “The GitHub Team,” and consistent formatting.

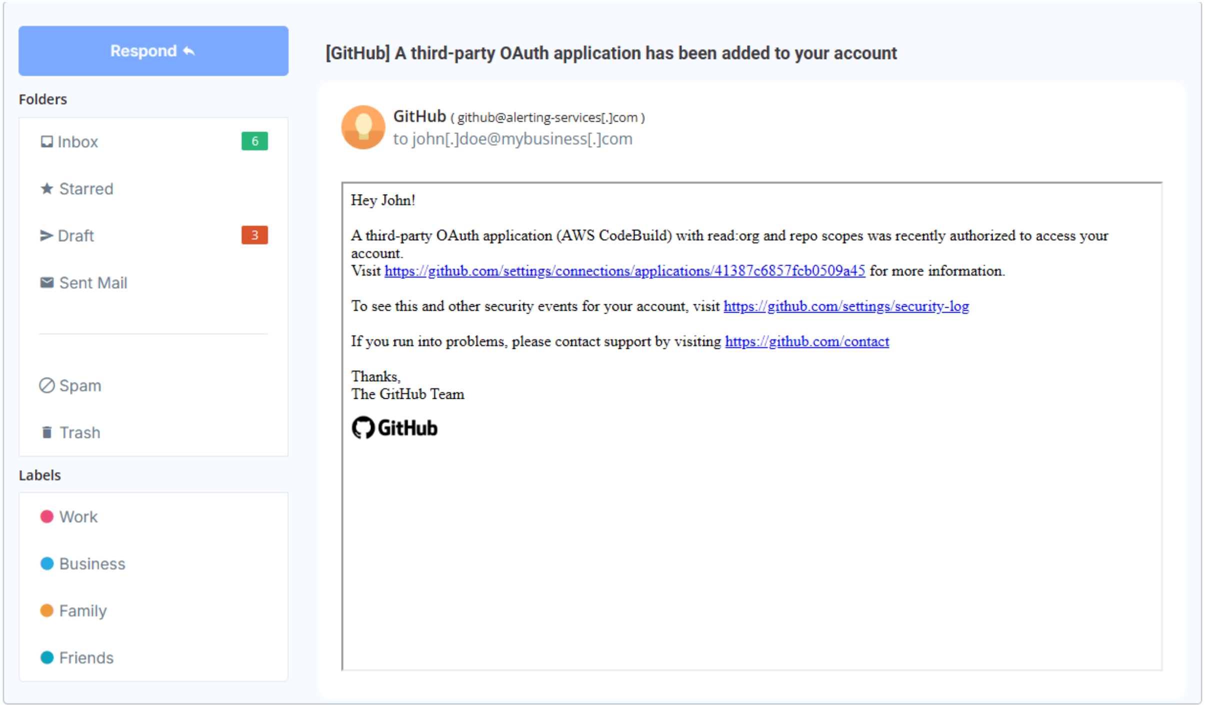
4. Phishing Traits Summary

No phishing characteristics were identified in this email:

- Domain authenticity appears intact (github.com)
- Links and hover URLs match legitimate destinations
- No attachments or embedded forms
- Neutral, non-urgent language
- Proper spelling and grammar

5. Recommendations

- Always verify the sender’s email address and check SPF/DKIM results in the header.
- Hover over every link before clicking to confirm it leads to the expected domain.
- If in doubt, navigate directly to GitHub in your browser instead of using embedded links.
- Regularly review your GitHub security log (https://github.com/settings/security-log) for unexpected authorizations.
- Enable two-factor authentication on your GitHub account for extra security.



[GitHub] A third-party OAuth application has been added to your account

GitHub (github@alerting-services[.]com)
to john[.]doe@mybusiness[.]com

Hey John!

A third-party OAuth application (AWS CodeBuild) with read:org and repo scopes was recently authorized to access your account.
Visit https://github.com/settings/connections/applications/41387c6857fcb0509a45 for more information.

To see this and other security events for your account, visit https://github.com/settings/security-log

If you run into problems, please contact support by visiting https://github.com/contact

Thanks,
The GitHub Team

GitHub