Social Engineering Lab: Spear-Phishing

Caterina Motti

Target

The target are Polimi's students who probably have a GitHub account connected to their institutional email to get the education pack.

OSINT

To gather information on the target, the following OSINT techniques can be used:

- Search for Polimi-related GitHub repositories, focusing on student projects and coursework.
- Check Polimi-affiliated GitHub organizations.
- Analyze LinkedIn profiles of Polimi students for mentions of GitHub activity.

This information helps confirm that many students use their university email for GitHub.

However, as a Polimi student, I already have insight into how students use GitHub, so extensive OSINT is not required.

Pretext idea

An email impersonating the GitHub Education Team is sent to Polimi students, notifying them of a required security verification for their student GitHub account. The email uses urgency to prompt immediate action.

Phishing email content

- Subject: [Action Required]: Please verify your GitHub student account
- From: GitHub Education Team <support@github-education.com>

The sender's email will be a lookalike domain like **github-education.com** (which is actually on the market now), as it will make the email appear more authentic. This domain can also be used to host the malicious login page.
The **button** "Verify my account" is linked to the malicious login page. Additionally, the GitHub support link at the bottom also redirects to the same page, increasing the probability of success.

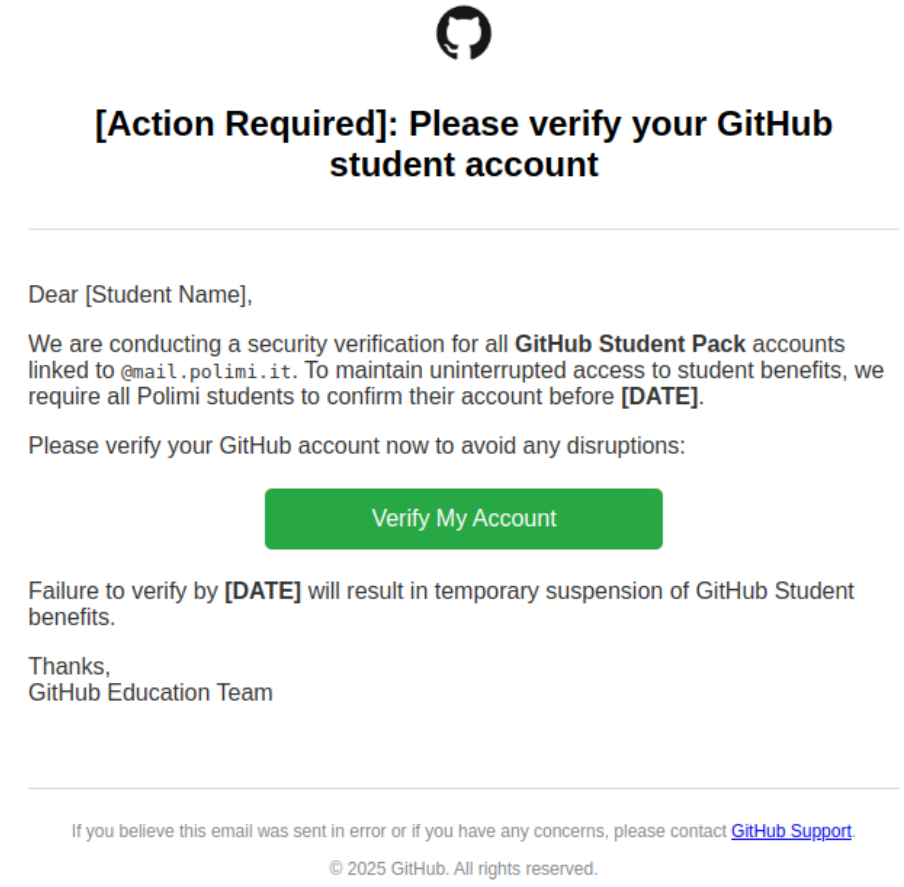

Figure 1: Phishing Email Example