

How to Spot a Phishing Email

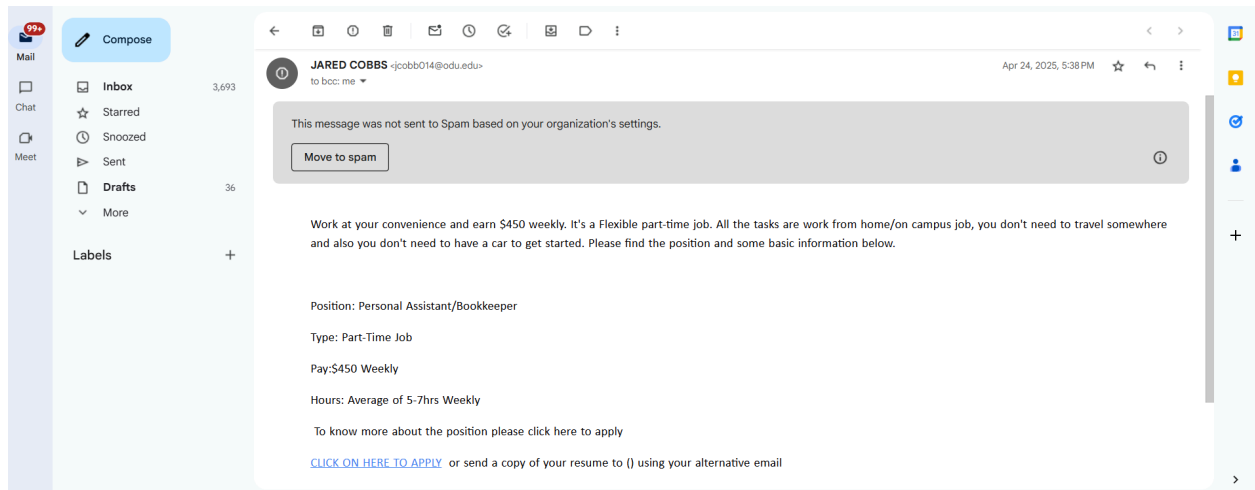
Introduction

Phishing emails are deceptive emails meant to trick users to share personal information or click on malicious links. This report analyzes a phishing email that was detected by my organization, sent from "JARED COBBS jcobb014@odu.edu (mailto:jcobb014@odu.edu)" on April 24, 2025, for a part-time job. Analyzing its warning signs, this report explains how to identify phishing attempts and protect oneself against them.

Analysis of the Phishing Email

The title "ALL STAFF AND STUDENTS PART-TIME/FULL-TIME PERSONAL ASSISTANT JOB OPPORTUNITY OPENING!!!" in the email contains certain suspicious features:

- **Suspicious Sender Address:** The sender, "jcobb014@odu.edu," is an apparent valid university address. But attackers often employ or hijack genuine emails to appear authentic. The sender's name, "JARED COBBS," does not assure genuineness because names can be forged.
- **Generic Greeting:** It starts with "Good day," which is a generic greeting and does not name the recipient. Legitimate job offers tend to use personalized greetings, while phishing messages use generic greetings in a bid to target many people at once.
- **Urgent and Enticing Offer:** The "promise of \$450 a week" for a "flexible part-time job" with limited hours (5–7 hours per week) is not possible and is meant to lure recipients. Such offers exploit economic incentives to prompt immediate action without scrutiny.
- **Suspicious Link:** The email has a "CLICK ON HERE TO APPLY" link, which would be malicious. Phishing emails most likely use links to send individuals to spoofed sites that steal credentials or install malware. The lack of descriptive language in the link and the fact that there is no URL presented are suspicious.
- **Request for Personal Information:** Asking for a resume transmitted to an unknown email address (provided as "()") is not typical. Legitimate job prospects provide proper contact details and hardly ask for sensitive files through unsolicited mail.



Prevention Tips

To avoid falling into the trap of phishing emails like these:

- **Verify the Sender:** Call the sender through official channels (e.g., a known university representative) to verify the authenticity of the email.
- **Avoid Clicking Links:** Mouse-over the links (but not click) to inspect the URL. If it looks unfamiliar or suspicious, don't click.
- **Be Skeptical of Offers:** Question unsolicited job offers, especially those promising high pay for little work.
- **Report Suspicious Emails:** Use your email's "Move to Spam" or reporting feature to alert your organization.

Conclusion

This phish uses a spoofed university email address, generic language, and an enticing job ad to trick users into clicking a possibly malicious link or sharing personal information. Recognizing these warning signs guards against phishing attacks, a common cyber threat. Users can safeguard their information by being vigilant and following prevention strategies, giving birth to a safe digital environment.