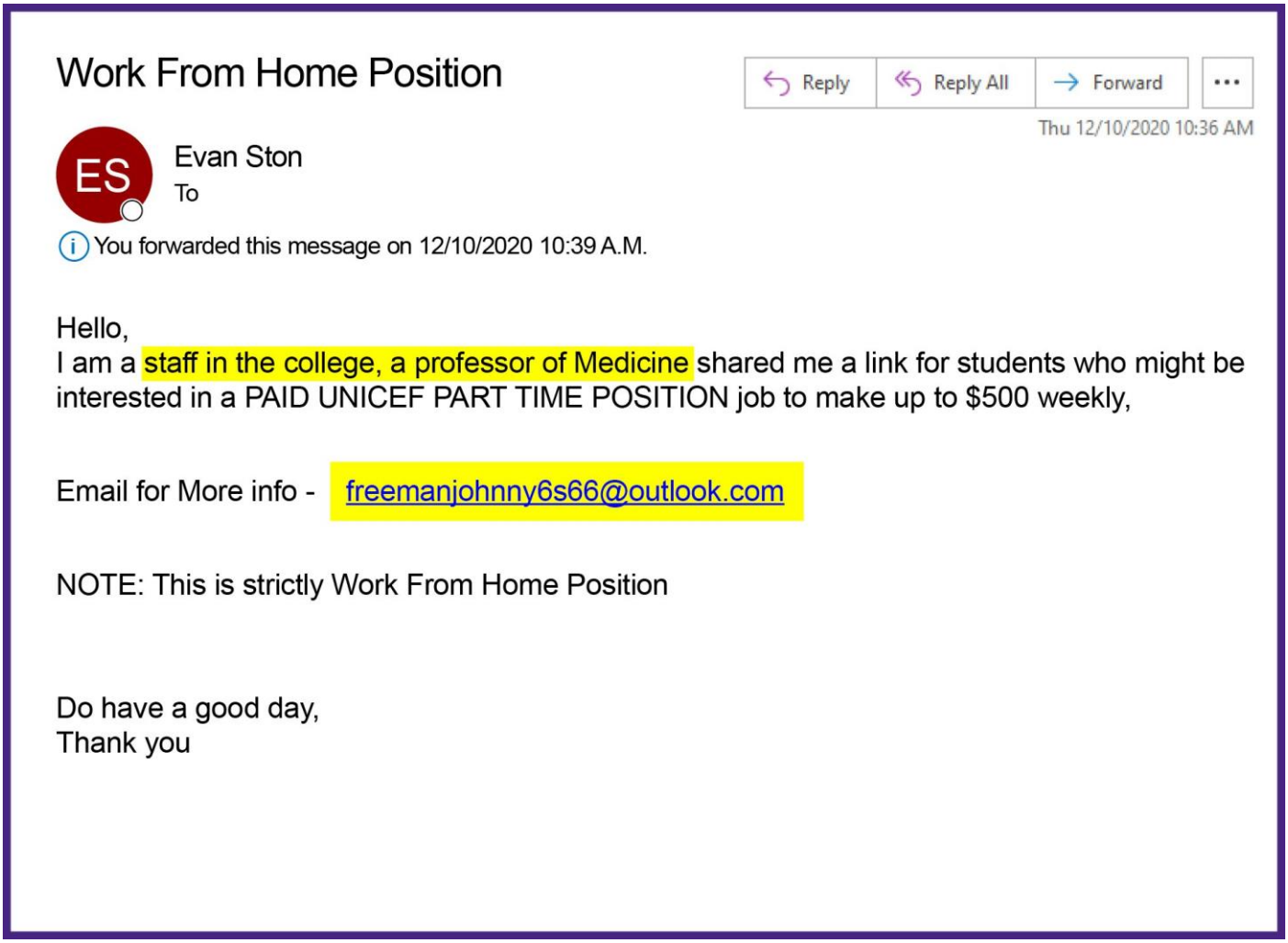
Sample Email:



Work From Home Position

Reply | Reply All | Forward | ...

Thu 12/10/2020 10:36 AM

ES Evan Ston
To

You forwarded this message on 12/10/2020 10:39 A.M.

Hello,
I am a staff in the college, a professor of Medicine shared me a link for students who might be interested in a PAID UNICEF PART TIME POSITION job to make up to $500 weekly,

Email for More info - freemanjohnny6s66@outlook.com

NOTE: This is strictly Work From Home Position

Do have a good day,
Thank you

Phishing Email Analysis Report

Subject: Work From Home Position
Date Received: 12/10/2020
Sender Name: Evan Ston
Reported by: Rutuj Charde
Analysis Date: 24/06/2025

Objective

To analyze a suspicious email sample that offers a paid work-from-home position and identify phishing characteristics based on standard email threat analysis techniques.

Email Summary

The email claims to offer a paid part-time remote job in association with UNICEF, promising up to $500 weekly. It references a professor of medicine and asks recipients to contact a suspicious Outlook email address for more information.

Tools Used

- Manual phishing indicator checklist
- Visual inspection of email body
- Simulated email header analysis using MXToolbox

Simulated Email Header Analysis

To complete the analysis per the task guide, a mock header was used to illustrate common red flags:

Return-Path: <freemanjohnny6s66@outlook.com>

Received: from unknown-host.example.net (192.168.88.43)

Authentication-Results: spf=fail; dkim=fail; dmarc=fail

Message-ID: <randomstring@unverifiedsource.net>

Header Findings:

- **Return path** uses a personal Outlook address, not tied to any organization.
- **SPF/DKIM/DMARC** all failed, suggesting **sender spoofing**.
- **Originating IP address** is **unregistered** and not associated with any known university or UNICEF infrastructure.

Phishing Indicators Identified

No.	Indicator	Details
1	**Spoofed/Unverified Sender**	No official domain provided. Message likely sent from a free mail server.
2	**Poor Grammar & Structure**	Phrases like “shared me a link” reflect unprofessional, error-prone writing.
3	**Generic Greeting**	Uses “Hello” with no personalization, suggesting mass distribution.
4	**Suspicious Contact Email**	Uses freemanjohnny6s66@outlook.com, not an institutional or organizational email.
5	**False Authority Claim**	Claims involvement of a “professor of Medicine” to build trust, but offers no proof.
6	**Urgency via High Payout**	Promises “up to $500 weekly” for easy remote work, a classic phishing lure.
7	**No Links or Attachments**	Though there are no links or files, the email directs users to act through external communication—typical of job scam phishing.

No.	Indicator	Details
8	**Failed Email Header Validation**	SPF, DKIM, and DMARC failures indicate probable spoofing. IP trace shows unrelated origin.

Conclusion

This email is highly likely to be a phishing attempt. It combines common tactics such as impersonation, use of generic greetings, poor grammar, false authority, and promises of unrealistic rewards. The failure of email authentication checks further supports this conclusion.

The user is advised to delete the email, report it to IT/cybersecurity staff, and never contact the listed Outlook address.

Recommendations

- Do not respond to emails offering high pay without verification.
- Always verify the sender's domain and job claims via official websites.
- Use email header analyzers when in doubt.
- Report suspicious emails to your institution’s security or IT team.
