Phishing Email Analysis Report

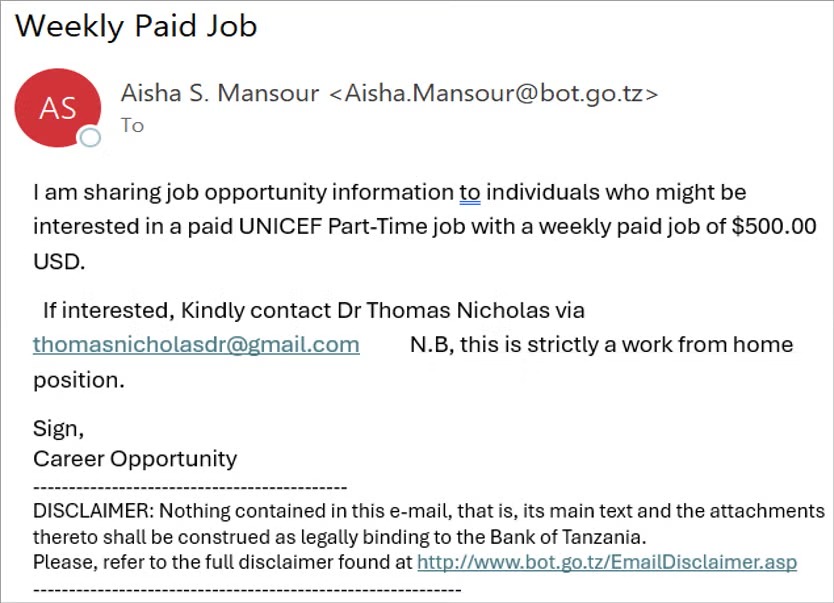
# Subject of the Email:

"Weekly Paid Job"

A vague subject line designed to attract attention and trigger curiosity or excitement.

# Sender's Email Address:

Aisha S. Mansour [Aisha.Mansour@bot.go.tz](mailto:Aisha.Mansour@bot.go.tz)



## Analysis:

- The domain @bot.go.tz belongs to the Bank of Tanzania, which is completely unrelated to UNICEF or recruitment for part-time jobs.  
- The mismatch between the sender’s organization (Bank of Tanzania) and the claimed job provider (UNICEF) is highly suspicious.  
- Official UNICEF communication would come from a UNICEF domain (e.g., @unicef.org), not from a government bank.

# Suspicious Content in the Email:

"...UNICEF Part-Time job with a weekly paid job of $500.00 USD."

## Analysis:

- Offering $500/week for part-time work without any job description or qualification details is a common red flag in phishing scams.  
- Scammers often use high-paying offers to entice users quickly.  
- Urging recipients to respond quickly is a psychological trick to prevent users from thinking critically or verifying legitimacy.  
- The use of a personal Gmail address instead of an official UNICEF or corporate domain is a huge red flag.

# Suspicious Email Mentioned:

thomasnicholasdr@gmail.com

## Analysis:

- Generic and personal email address — official recruiters from UNICEF or any major organization will never use personal Gmail accounts.  
- Scammers use throwaway Gmail/Yahoo accounts to collect personal information, conduct fraud, or scam money under the guise of processing fees, equipment costs, etc.

# Grammatical and Stylistic Errors:

- Random capitalizations: "Kindly contact Dr Thomas Nicholas", "Part-Time job", "UNICEF".  
- The awkward phrasing like "weekly paid job of $500.00 USD" is unnatural.  
- The sign-off is vague: "Sign, Career Opportunity" — not a real person or role.

# Disclaimer Abuse:

- Although the disclaimer references the Bank of Tanzania, the actual content is about a fake UNICEF job.  
- This adds a false sense of legitimacy to trick users into trusting the message.

# Summary of Red Flags:

|  |  |
| --- | --- |
| Red Flag | Description |
| Mismatched sender domain | Email from Bank of Tanzania promoting a UNICEF job |
| Unrealistic salary | $500/week for unknown part-time work |
| Gmail reply address | Not professional or traceable |
| Vague job details | No job description, responsibilities, or requirements |
| Urgency | Pushing users to contact quickly |
| Poor language | Grammar and formatting issues |
| Abuse of official disclaimers | Using legitimate disclaimers to gain trust |

# What to Do If You Receive Such Emails:

- Do not respond or click on any links.  
- Do not provide personal details or financial info.  
- Report the email as phishing in your mail client.  
- Verify job opportunities only via official websites (e.g., careers.unicef.org).

* Drafted by Aksah A