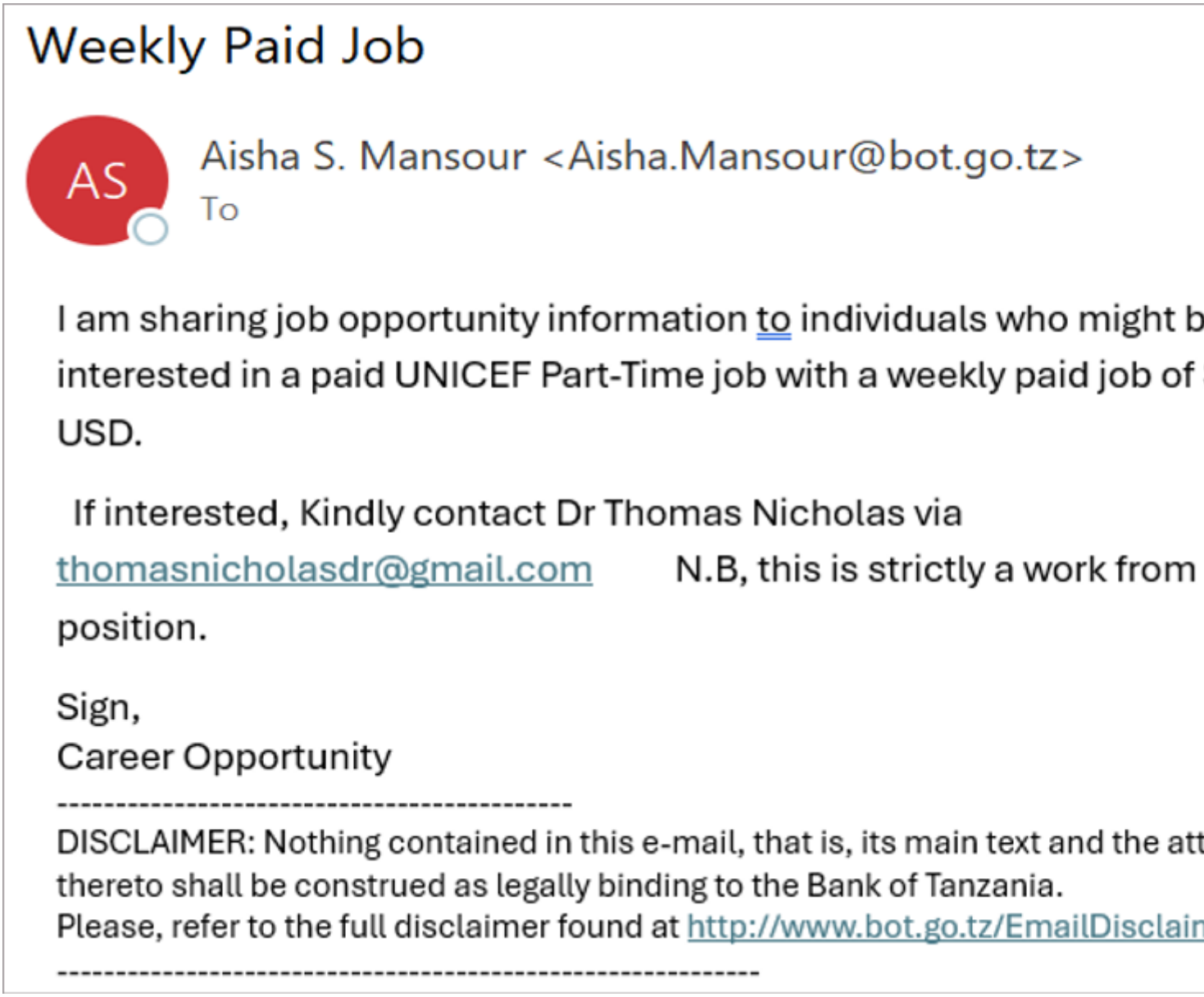
Published on *University of Colorado* (https://www.cu.edu)

Avoid Being a Phishing Scam Victim [1]



Phishing scams involve fraudulent online messages that impersonate trusted sources, aiming to trick you into exposing sensitive information or installing malware. Cybercriminals often use fake links and deceptive directives in messages that appear to come from university officials or other trusted individuals. However, by staying vigilant and recognizing the signs of phishing, you can better protect your personal and university data.

Phishing attempts can be subtle and deceptive. Before clicking any links or downloading attachments, assess the email's legitimacy using these quick checks:

- **Mismatch in email address:** does the sender's e-mail address align with the supposed

organization?
- **Generic greetings:** is the greeting vague or non-specific, such as “Dear associate?”
- **Too good to be true:** does the message offer something that seems excessively beneficial or unrealistic?
- **Urgent or threatening language:** is there a sense of urgency or a threat that pressures you to take immediate action?
- **Link verification:** if the email contains links, do their URLs match what you expect or seem legitimate?
- **Request for personal information:** does the email ask for sensitive information such as passwords or financial data?
- **Strange requests:** does the email contain unusual or abrupt business requests?
- **Trust your instincts:** does something feel off? If so, it probably is.

Important to know

CU or any reputable organization will never ask for your passwords in an email or phone call.

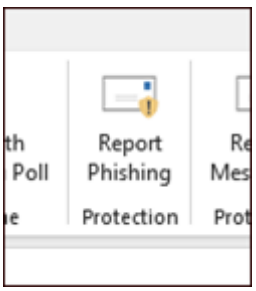
Even if an email appears credible, avoid clicking any links, opening attachments, or calling any numbers provided. Instead, verify its authenticity by visiting the organization’s official website for contact information or by reaching out directly using a known email address or phone number.

While the tips will help you to avoid falling victim to phishing scams, you can take these additional steps to reduce your risk of becoming a target in the first place:

- **Be mindful of social media:** limit the personal information you share as even minor details can be used for identity theft or fraud.
- **Create strong passwords:** use unique and robust passwords for each of your accounts.
- **Enable multi-factor authentication (MFA):** add this extra layer of security whenever possible. Learn more about MFA. [2]
- **Keep software updated:** regularly update your software to incorporate the latest security enhancements.

Reporting phishing email

If you receive a suspicious email in your CU email account, use the Report Phishing icon in Outlook. Microsoft will screen the suspected phish and forward it to your campus IT or information security department for further review, if needed.



If you have fallen victim to a phishing scam, report the incident [3] to your campus IT service desk or information security immediately. Quick reporting allows the investigative team to assess the impact and respond accordingly.

Learn more about phishing

Visit your campus website for specific guidance.

- CU Anschutz [4]
- CU Boulder [5]
- CU Denver [4]
- UCCS [6]
- System Administration [7]

Updated 2/26/2025

Groups audience:
Office of Information Security

Source URL:https://www.cu.edu/security/avoid-being-phishing-scam-victim

Links
[1] https://www.cu.edu/security/avoid-being-phishing-scam-victim [2] https://www.cu.edu/security/multi-factor-authentication-added-protection-cybercrime [3] https://www.cu.edu/security/reporting-incident
[4] https://www.cuanschutz.edu/offices/information-security-and-it-compliance
[5] https://oit.colorado.edu/services/it-security [6] https://oit.uccs.edu/security [7] https://www.cu.edu/uis