How can you tell if a job posting is legitimate? Indicators that an employer email may be fraudulent include:

- There are typos or spelling mistakes in the email
- The message is sent from a personal rather than an employer email account (example: @hotmail.com rather than @thecompany'sname.com)
- The employer asks you to send them confidential information or money
- You receive an unsolicited interview or job offer

Tips to avoid online scams:

- Always safeguard your personal information
- Never provide your social security number, bank account information, or other sensitive information via email
- Never respond to requests for check deposits, package pickups, or money transfers
- The only time an employer should ask for your bank account information is after you have accepted an offer and are filling out payroll forms
- A legitimate employer will always ask you to fill out tax forms
- Unfortunately, scammers can be very savvy at avoiding detection and finding ways to email or call potential victims. Be cautious when using job boards and social media.

What should you do if you were scammed? Review next steps:

- Find out what to do if you paid someone you think is a scammer, gave them some personal information, or if they have access to your phone or computer at the Federal Trade Commission: What to do if you were scammed.
- Report the activity to the Internet Crime Complaint Center at https://www.ic3.gov/
- Report the activity to the website on which the posting was listed
- Report the activity to the company the cyber criminals impersonated
- Contact your financial institution immediately upon discovering any fraudulent or suspicious activity and direct them to stop or reverse the transactions
- Ask your financial institution to contact the corresponding financial institution where the fraudulent or suspicious transfer was sent

Review the following information for additional tips to keep your information safe while job searching: FTC Advice for Avoiding Job Scams