

Pause before you respond.

A quick handout for students and job seekers. Real employers do not need you to rush, pay money, or share sensitive information before you can independently verify the opportunity.

Urgent warning: Do not send money, buy equipment with a check, purchase gift cards, or provide bank details, passwords, or a Social Security number to "secure" a job.

Common warning signs

They send a check for equipment.

A fake-check scheme asks you to deposit money and send some back or buy equipment from a chosen seller.

They ask you to pay first.

Legitimate employers do not ask candidates to pay fees, buy gift cards, or send cryptocurrency to start a job.

The interview stays on an app.

Be cautious when a recruiter avoids a normal call or video meeting and pushes Telegram, WhatsApp, text, or chat only.

The offer feels rushed or unrealistically easy.

Pressure, unusually high pay, or an offer without a real interview should make you stop and verify.

The email or website does not match the company.

Look for personal email accounts, misspelled domains, and links that do not lead to the company's official careers page.

They request sensitive information too early.

Do not share banking details, passwords, government ID numbers, or your Social Security number before you verify the employer.

What to do next

1 Stop and do not send anything.

Do not click new links, deposit a check, pay a fee, or provide sensitive information.

2 Verify independently.

Find the employer's official website yourself. Use the number or contact form there to confirm the role and recruiter.

3 Save evidence and report it.

Keep messages, email addresses, payment requests, and links. Report suspected fraud to the platform and the FTC at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud).



Check a suspicious job offer

Free browser-based job-scam safety tools, checklists, domain checks, and guides.
offersentry.com