



The Center for Career and Professional Advising

Beware of Job/Employment Scams

Employment scams are on the rise. According to the [Identity Theft Resource Center](#), job scam reports surged 118% in 2023 from 2022. As job seekers report scams annually, the Haverford student community hasn't been spared from this trend.

Common Types of Scams

- [Fraudulent Job Postings](#)—Scammers are now acting as employers by posting jobs online and in other, seemingly real, mediums to obtain your contact information and money.
- [Check/Gift Card/Money Order Scams](#)—Requests for checks and gift cards/money orders to be received/purchased are not job responsibilities of reputable employment opportunities; these practices are scams.
- [Email Scams](#) (also known as Phishing): Acting as employers, scammers use email or text messages to steal your passwords, account numbers, or Social Security numbers.

Warning Signs

- Incorrect or awkward phrasing and grammar, misspellings or typos.
- Position requires upfront fees such as purchasing gift cards or sending/receiving money via any method.
- Requests to correspond using an alternate email address, WhatsApp, or text messages.
- Job postings or offer emails are from @gmail.com accounts and not the company domain. Legitimate URL domains typically end in .com, .edu, .org, or a country's government domain (such as .gov for the US)
- You may be asked for personal information, such as your social security number, or to complete a background check before being interviewed for the position.
- An email references finding you on Handshake but does not come through the Handshake platform or the employer email account.
- Request to send a photocopy of your ID (e.g., driver's license) to "verify your identity."
- You are hired without ever interviewing or meeting your potential employer.
- Pressure and language asking you to act quickly or face consequences, such as losing your job offer.
- Interviews are conducted solely via text message or Zoom chat.
- Restricting communication with the employer (i.e., only they will reach out to you/instructing you not to initiate communication)
- While there are many legitimate and great opportunities to work remotely, unfortunately, many scammers utilize "remote" and "work from home" to grab student's attention.

Tips to Avoid Employment Offer Scams

- Adjust your LinkedIn profile so your email address is only visible to you. Increasingly, scammers may target individuals by pretending to be an actual person from the organization you may recognize. Once you accept the connection request, they collect personal contact information and target your email directly.

- For all social media accounts, only connect with folks that you actually know or with whom you have a mutual and trusted relationship.
- Configure your LinkedIn profile to NOT automatically share a personal email address with connections in your network.
- Be aware of the scams that Haverford's IITS has identified by reviewing campus-wide emails.

What to Do About Suspicious Postings

It is essential to take action if you encounter suspicious postings in Handshake or receive a phishing email containing a job offer for a position you have not applied for.

Follow these steps to take action:

1. Report your experience to the CCPA at hc-ccpa@haverford.edu or 610-896-1181.
2. End all communication with the employer, and if personal information was disclosed, monitor or block your accounts.
3. If you have sent money to a fraudulent employer, immediately contact your bank or credit card company to close your account and dispute the charges.
4. If you receive a phishing email at your Haverford email address or from a fraudulent/suspicious Haverford College email address, contact [Haverford's Instructional & Information Technology Services \(IITS\)](#) at ITServiceDesk@haverford.edu. You can also contact IITS to verify if an email is legitimate. Report a phishing attempt using the IITS' reporting website: [Report a Phishing Attempt Form](#).