EMPLOYMENT SCAMS
A Guide for Employers

Employment scams are increasingly sophisticated, targeting job seekers with fake job offers, impersonating legitimate companies and exploiting personal and financial information. While job seekers need to remain vigilant, employers can play a key role in preventing and combating job scams.

Scammers may misuse your brand by creating fake job postings, setting up look-alike websites using similar domain names or creating fake employee profiles and sending phishing emails.

Warning Signs Scammers Might be Impersonating Your Company

Increased Inquiries
An unexpected surge in calls or emails to Human Resources (HR) from potential applicants about job postings that do not match any current openings.

Applicant Confusion
HR receiving calls or emails from people asking to verify job offers or interview schedules or claiming to have been interviewed or hired for a role that does not exist.

Increase in Resumes
A sudden increase in resumes for roles that were not advertised by your company.

Fake Company Websites
Websites using similar domain names as your company, slight misspellings of your company name and the addition of words like “careers” or “hiring” to your company name.

To safeguard your brand and prospective employees, consider the following:

Monitor Fake Job Postings

Search for Fraudulent Listings
Create alerts to notify you whenever your company is mentioned online, especially on job boards or social media, by using tools such as Google Alerts.

Website and Job Board Authentication
Direct job applicants to apply through official company websites or verified job boards. Clearly state on your company's website where legitimate listings can be found.

Raise Awareness

Educate Job Seekers
Inform job seekers about common signs of scams, such as unrealistic job offers, requests for personal information, demands for payments for applications, etc. Inform them of your company's legitimate recruitment process.

Awareness Campaigns
On your official website, place clear warnings about potential scams and details of your actual recruitment process. Ensure internal teams, especially HR and IT, are aware of these types of scams and know how to spot red flags.

Training for Employees
Provide training for HR and recruitment teams to recognize the signs of job scams and deal with affected candidates.

Issue Public Alerts
When a scam is identified, issue public alerts on your company's website and social media channels and provide guidance on how job seekers can avoid them.

Strengthen Recruitment Practices

Use Secure Communication Channels
Ensure all official email communication with candidates happens via company emails (e.g. -"@company.com") rather than public domains such as Gmail or Yahoo.

Application Portals
Provide an official, secure platform for job applications, and warn candidates about applying through third-party websites not affiliated with the company.

Vetting of Recruiters
If you use third-party recruiters, ensure they are legitimate by conducting background checks and regularly auditing their work.

Use Reputable Job Platforms
Only post job openings on verified and reputable platforms. Avoid lesser-known websites unless they have strict vetting procedures.

Consistent Job Postings
Use standardized templates with clearly defined roles, qualifications and responsibilities. Scammers may try to manipulate postings if your process is inconsistent.

Provide Strong Branding on Job Listings
Ensure your company's official online presence is easily recognizable (e.g. - well-maintained LinkedIn profiles and verified job posts).

Dedicated Contact for Scam Reports
Have a point of contact for candidates to verify the legitimacy of job offers or report suspicious behavior. This process should be clearly communicated on your company's website.

What to Do if You Suspect a Scam

Issue a Public Statement or Warning
Depending on the severity of the situation, you might want to issue a public notice on your website or social media channels to warn potential applicants that the job posting is fake and to clarify that you are not affiliated with it.

Report the Scam

- **Federal Trade Commission (FTC):** reportfraud.ftc.gov

- **Job Board Platforms:** Notify the job board (e.g. - Indeed, LinkedIn) about suspicious postings or recruiters.

- **Local Law Enforcement:** Contact the police if personal or financial information has been compromised.