

EMPLOYMENT SCAM INFORMATION GUIDE

Protect Yourself from Fake Job Offers and Hiring Fraud

CONTENTS

- 1. What Are Employment Scams?
- 2. Common Types of Employment Scams
- 3. Red Flags to Watch For
- 4. How Scammers Target Job Seekers
- 5. Case Studies & Real Examples
- 6. Steps to Protect Yourself
- 7. What to Do If You've Been Scammed
- 8. Resources & Support Contacts

1. WHAT ARE EMPLOYMENT SCAMS?

Employment scams are fraudulent schemes where criminals pose as employers or recruiters to steal money, personal information, or labor from job seekers. These scams exploit people's desire for employment, flexible work arrangements, or better compensation.

Key Statistics:

- Employment scams ranked among the top 10 scams reported to the FTC in 2024
- The average victim loses \$1,000-\$3,000 in direct monetary losses
- 16% of job seekers have encountered a job scam at some point
- Remote work opportunities are used as bait in over a third of these scams
- Identity theft is a common outcome, even when no money is directly stolen

2. COMMON TYPES OF EMPLOYMENT SCAMS

Advance Fee Scams

Scammers promise employment but require upfront payment for "training," "certification," "background checks," "software," or "equipment." After payment, the job opportunity vanishes.

Fake Job Listings

Scammers post counterfeit job listings on legitimate job boards to collect personal information or to direct applicants to fake websites where they can steal credentials.

Reshipping Scams

Victims are hired to receive packages at home and forward them to another address. The packages often contain items purchased with stolen credit cards, making the victim an unwitting accomplice to fraud.

Money Laundering/Payment Processing Scams

"Employees" are asked to receive funds into their personal accounts and transfer them elsewhere after keeping a percentage as payment. These funds are typically proceeds from other scams.

Identity Theft Scams

Fake employers collect personal information, Social Security numbers, and copies of identification documents through fabricated application processes for identity theft purposes.

Work-From-Home Scams

Scammers advertise lucrative, easy work-from-home opportunities that either don't exist or are illegal operations. Common examples include envelope stuffing, craft assembly, or data entry schemes.

Impersonation Scams

Criminals impersonate legitimate companies or create companies with names similar to well-known businesses to add credibility to their fraudulent job offers.

3. RED FLAGS TO WATCH FOR

Job Listing Red Flags

- Positions offering unusually high pay for minimal qualifications
- Jobs that don't require an interview or have minimal screening
- Listings with poor grammar and spelling errors
- · Vague job descriptions with few specific requirements
- · Positions that promise "guaranteed" employment
- Job listings not found on the company's official careers page

Communication Red Flags

- Job offers extended without a formal interview process
- Interviews conducted only via text or messaging apps
- Pressure to accept a position immediately
- Communication from personal email addresses rather than company domains (e.g., gmail.com instead of companyname.com)
- Recruiters unwilling to provide clear details about the company or position

Financial Red Flags

- Requests for payment for any reason (training, equipment, software, etc.)
- · Requirements to purchase specific equipment or software from designated vendors
- Requests for bank account information during early application stages
- Offers to send checks before work begins
- Unusual payment methods (wire transfers, cryptocurrency, gift cards)
- Job descriptions primarily focused on receiving/transferring money

Information Request Red Flags

- Requests for sensitive personal information before a job offer
- Asking for Social Security numbers or copies of identification for "background checks" before a formal offer
- Requests to complete credit checks as part of initial application
- Pressure to provide financial account information quickly

4. HOW SCAMMERS TARGET JOB SEEKERS

Targeting Methods

- Creating fake profiles on professional networking sites
- · Monitoring public resumes on job boards for potential targets
- Setting up legitimate-looking but fraudulent job sites
- Posting jobs on legitimate employment websites
- Creating fake company websites that mimic real corporations
- Sending unsolicited job offers via email or messaging

Vulnerable Populations

- Recent graduates with limited job-hunting experience
- People seeking remote or flexible work opportunities
- Unemployed individuals with urgent financial needs
- Those seeking second jobs or supplemental income
- Career changers lacking industry knowledge
- Workers in industries experiencing high unemployment
- Non-native English speakers who may miss subtle red flags

Psychological Tactics

- Creating artificial urgency ("position must be filled immediately")
- Offering salaries significantly above market rates
- · Promising unrealistic benefits or work conditions
- Exploiting economic anxiety and financial pressure
- · Using flattery and claims of being "particularly impressed" with randomly selected candidates
- Building false rapport through extended messaging or communications

5. CASE STUDIES & REAL EXAMPLES

Case Study: Remote Assistant Scam

Taylor was excited to find a remote executive assistant position paying \$35/hour with minimal experience required. After a brief text interview, she was "hired" and sent a check for \$3,500 to purchase home office equipment from a "company vendor." The check initially cleared, and Taylor wired \$3,000 to the supposed vendor. The check was later identified as fraudulent, leaving Taylor responsible for the full amount plus bank fees.

Case Study: Tech Support Impersonation

James applied for an IT support role with what appeared to be a major tech company. The "hiring manager" conducted a job interview over Google Hangouts and offered James the position immediately. Before starting, James was asked to purchase specific software using gift cards for "compatibility with company systems." After sending \$800 in gift cards, all communication ceased.

Case Study: Data Entry Identity Theft

Maria applied for a data entry position through a job listing site. The application required her full name, address, SSN, and a photo of her driver's license for a "background check." After providing this information, Maria never heard back. Two months later, she discovered multiple credit accounts had been opened in her name.

Case Study: Reshipping Scheme

Robert was hired as a "shipping coordinator" working from home. His job involved receiving packages and forwarding them internationally, keeping \$50 per package processed. After three weeks, federal investigators contacted Robert—he had been reshipping items purchased with stolen credit cards. Though he wasn't charged with a crime, he received no payment for his work and spent significant time dealing with the investigation.

6. STEPS TO PROTECT YOURSELF

Research Before Applying

• Verify the company exists with a legitimate web presence

- Search the company name plus "scam" or "fraud" to see warnings
- Check the company's official website for the job listing
- Look up company reviews on sites like Glassdoor or Better Business Bureau
- Verify the recruiter's identity on professional networking sites
- Check that email addresses use the company's official domain

During the Application Process

- · Be wary of jobs that don't require interviews or offer immediate hiring
- Watch for employers using free email services rather than company domains
- Be skeptical of vague job descriptions or those promising high pay for little work
- Never pay money to secure a job opportunity
- Be cautious about jobs requiring you to purchase specific equipment
- Ask detailed questions about job responsibilities, reporting structure, and company policies

Protecting Your Information

- Never provide Social Security numbers until you've verified the job is legitimate
- Don't share banking information during early application stages
- Use caution when uploading copies of identification documents
- Consider using a separate email address for job searching
- Limit personal information on publicly available resumes
- · Be careful about completing application forms on unfamiliar websites

Interview Safety

- Be suspicious if the entire hiring process occurs via text or messaging apps
- For remote interviews, verify you're using the company's official platform
- Take time to think about offers rather than accepting immediately
- Get all job details, including compensation and duties, in writing
- Trust your instincts if something feels wrong or too good to be true

7. WHAT TO DO IF YOU'VE BEEN SCAMMED

Immediate Actions

- Cut off all communication with the scammer
- Document everything (emails, texts, job listings, website screenshots)
- Contact your bank immediately if you've shared financial information or sent money
- Change passwords for any accounts where you used credentials during the application
- Alert the legitimate company if a scammer was impersonating them

Financial Recovery Steps

- Report fraudulent checks or unauthorized transfers to your financial institution
- · Dispute any fraudulent charges on credit cards or bank accounts

- Request a credit freeze if you suspect identity theft
- Monitor your credit report for unauthorized activity
- · Contact credit reporting agencies to place fraud alerts

Reporting the Scam

- Report to the Federal Trade Commission at ReportFraud.ftc.gov
- File a report with the FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov
- Report to your state's attorney general office
- File a police report, especially if identity theft occurred
- Report fake job listings to the job board where you found them
- Report to the Better Business Bureau's Scam Tracker

Identity Protection

- If you shared your Social Security number, visit IdentityTheft.gov
- Consider investing in an identity protection service
- Review your credit reports regularly (AnnualCreditReport.com)
- Watch for signs of tax fraud (rejection of tax returns, notices about unreported income)
- Be alert for future scam attempts, as victims are often targeted multiple times

8. RESOURCES & SUPPORT CONTACTS

Government Resources

- Federal Trade Commission: ReportFraud.ftc.gov or 1-877-FTC-HELP
- FBI Internet Crime Complaint Center: www.ic3.gov
- Identity Theft Resource Center: www.idtheftcenter.org or 1-888-400-5530
- U.S. Department of Labor (for employment scams): www.dol.gov/agencies/whd/contact
- Consumer Financial Protection Bureau: www.consumerfinance.gov or 1-855-411-2372

Job Search Safety

- Better Business Bureau: www.bbb.org/scamtracker
- National Consumers League Fraud Center: fraud.org
- Career OneStop (government-sponsored job resources): www.careeronestop.org
- · Your state's workforce development or unemployment agency

Legitimate Job Search Sites with Scam Protection

- LinkedIn: www.linkedin.com/help/linkedin/topics/6973/6974/146376
- Indeed: www.indeed.com/support/contact
- Glassdoor: help.glassdoor.com/s/topic/0TO1M000000UTtbWAG/support
- USA Jobs (government positions): www.usajobs.gov/Help/working-in-government/fraud

Financial Assistance

- Consumer Credit Counseling Services: www.nfcc.org or 1-800-388-2227
- Financial Empowerment Centers (available in many cities)
- Local community action agencies
- Legal Aid services for low-income individuals: www.lsc.gov/what-legal-aid/find-legal-aid

REMEMBER:

- · Legitimate employers never require payment to be hired
- · Take your time making employment decisions
- Research thoroughly before providing personal information
- If a job seems too good to be true, it probably is
- © 2025 This guide may be freely distributed to help protect potential victims of employment scams.

