

Job Scams in 2023

Published 11/22/2023 by [Giuseppe Aloisi](#)

What are job scams?

Job scams are fraudulent activities or schemes designed to deceive individuals seeking employment by offering fake job opportunities. These scams are usually orchestrated by individuals or organizations with the intention of stealing money, personal information, or both from job seekers. Job scams can take various forms, but they often share common characteristics. Here are some common types of job scams:

Most people apply for positions through job boards such as Indeed, Glassdoor, or LinkedIn. Sometimes, these job boards harbour different kinds of scams that target people looking for employment. This blog post will identify the most common job scams, tips to avoid them and how to keep yourself safe.

Let's take a moment to review some of the top job scams seen by ITS in 2023.

Advance fee scams

Advance Fee Scams are scams that ask you to send a payment or gift card to “secure” the position. After this money/gift card is received, the scammer will cut ties, or try and get more money out of you. Before you know it, you may have been scammed for hundreds of dollars.

Work-from-home scams

During the pandemic, work-from-home jobs became extremely popular as the world grappled with the stagnation of the world economy. As a result of this, scams revolving around work-from-home became much more popular. Scammers will advertise these jobs, emphasizing easy work with extremely high pay. Similar to advance fee scams, scammers will ask you to submit a fee to get the position, and when you start the position, the job will usually end up recruiting someone else to the scam.

Scammers may ask you for personal info for identity theft purposes, perform illegal work for them (e.g. re-shipping things), or ask you to send money in exchange for a cheque they send you but will eventually get bounced. Check the reputation of the company and the recruiter to validate information before sending your information.

Pyramid schemes

Pyramid Schemes are one of the most common scams to occur. As the name suggests, it works in a pyramid format. Starting with one person, they will try and recruit a set of people, who will have to buy their way into the company. Once this set of people begins to work, they may have to sell various types of products in order to advance in the company and make money. The employees also gain a cash bonus when they recruit more employees. This would lead to a cycle where people are being recruited and then recruiting more employees. The cycle would in theory continue forever until there is no one left to recruit.

Takeaways

This is just the tip of the iceberg when it comes to scams. Scams are often unique and the next one is often more calculated than the last. During your job search, if there is something that seems suspicious or too good to be true, it probably is. Always ask questions and report suspicious emails using the 'Report Phishing' button in your Outlook app.

Should you unfortunately fall victim to a scam, it's important to not be embarrassed or ashamed. Falling victim to these scams is not your fault. Here are some steps you may follow if you have fallen victim or suspect a scam.

1. Stay calm. Panic may lead to mistakes or threat actors taking advantage of your situation
2. Contact your local authorities' non-emergency line
3. Report and contact the Canadian Centre for Cybersecurity:
<https://cyber.gc.ca/en/incident-management>
4. For Seneca security-related concerns contact servicedesk@senecacollege.ca
5. Never pay any ransom to threat actors because there is no guarantee they will honour any transaction
6. Have backups of your data in the Cloud, external drive, or another machine
7. Share online secure practices with family members and friends