



LAYOFFS FUEL UPTICK IN EMPLOYMENT SCAMS

ZEROFOX INTELLIGENCE

F-2023-01-18a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Impersonations, Fraud, Domain Violations

January 18, 2023



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EST) on January 17, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Layoffs Fuel Uptick in Employment Scams

Key Findings

- A recent uptick in layoffs across industries has seen increased efforts by threat actors to target job seekers with employment scams.
- The tech industry has been particularly hard-hit with layoffs since 2022.
- Threat actors utilize employment-related scams in order to obtain sensitive personal and financial information on their victims.
- Fake job postings in 2022 cost victims nearly double what they did in 2020.
- Even though organizations are not responsible for the creation of fraudulent job postings, their brands can be negatively impacted by these scams.

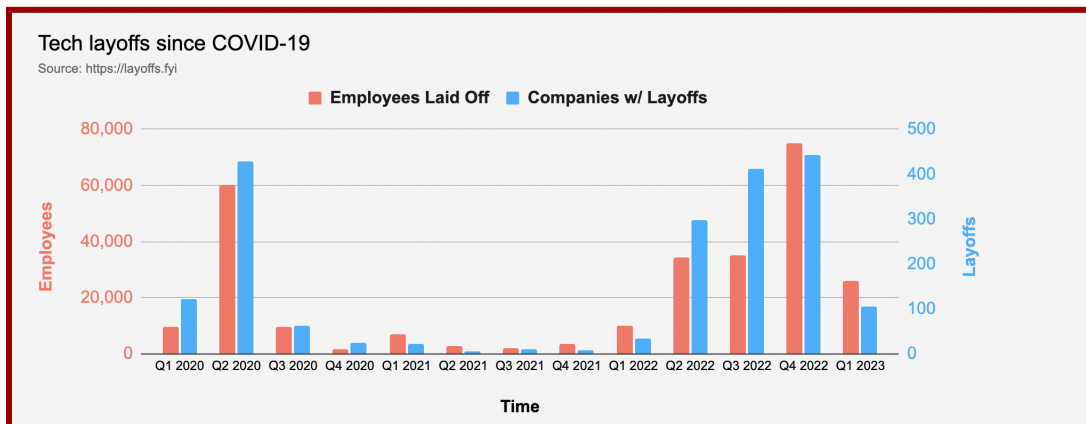
Analyst Commentary

Employment scams have plagued the job market for years, causing headaches for applicants and organizations alike. These scams are perpetrated by fraudsters attempting to take advantage of job seekers by pretending to be employees or representatives of well-established organizations in order to obtain personal or financial information from the victim. The bad actors utilize various methods, including impersonating legitimate organizations, gathering personal information via fraudulent employment applications, or asking for banking information as part of job offers. The onset of the COVID-19 pandemic ushered in an unprecedented rise in employment scams, as threat actors leveraged the remote work environment to exploit job seekers. Most recently, layoffs across multiple industries throughout 2022 have coincided with increased efforts by threat actors to target job seekers; ZeroFox Intelligence identified a 30 percent increase in impersonation accounts of organizations from Q3 to Q4 in 2022.

Pay-to-play recruitment scams are easy to conduct and are often used to exploit individuals making a career change. Scammers often target prestigious, high-paying industries such as tech, oil and gas, and financial services and pretend to be recruiters.



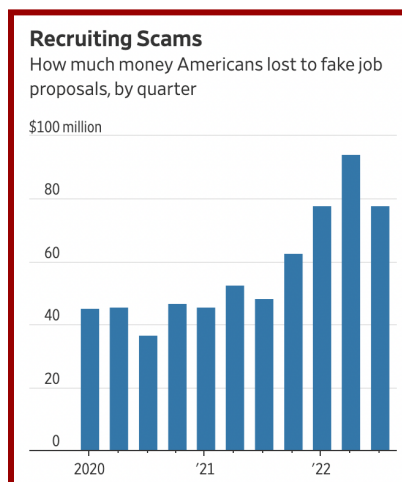
The tech industry has been particularly hard-hit by layoffs throughout 2022 and into 2023, making its laid-off workers prime targets for employment scams.¹



Source: [Layoffs.fyi](https://layoffs.fyi)

Fake recruiters will continuously monitor employment sites for new targets. Scammers also tend to target new college graduates and other eager job seekers that may be looking to make a career change. Some social media scams even invoke emotional and financial drivers, such as student loan debt forgiveness, to convince a would-be employee to take the fraudulent offer.

In addition to these employment scams causing reputational damage to the impersonated organizations and disappointing the victim job seekers, the Federal Trade Commission reports that they have also been costing these victims significantly more overall in lost funds.



Source: Federal Trade Commission

¹ <https://www.wsj.com/articles/laid-off-workers-are-flooded-with-fake-job-offers-11673387875>



In the second quarter of 2022, these fake employment scams cost job seekers almost double in losses compared with the same timeframe in 2020. Despite significant efforts by employment websites to identify and remove fraudulent job postings,² the chart above indicates that threat actors remain very successful in targeting job seekers. The current economic and employment environment enables threat actors to take advantage of job seekers who may be desperately looking for work—and therefore may not be as diligent about spotting red flags that indicate a job posting is fraudulent.

ZeroFox Intelligence has identified the following common red flags that may indicate a job scam:

- Interviews are not conducted in-person or through a secure video call.
- Interviews are conducted via teleconference applications that use email addresses instead of phone numbers.
- Potential employers contact victims through non-company email domains and teleconference applications.
- Potential employers require employees to purchase start-up equipment from the company.
- Potential employers require employees to pay upfront for background investigations or screenings.
- Potential employers request credit card information.
- Potential employers send an employment contract to physically sign asking for personally identifiable information (PII).
- Job postings appear on job boards but not on the organizations' websites.
- Recruiters or managers do not have profiles on the job board, or the profiles do not seem to fit their roles.

Recommendations

- Clearly indicate on organizations' websites and through official communication channels where job seekers can find authentic job postings. This will give something definitive to point to should an organization's brand be impersonated in fake job recruitment scams, as well as provide job seekers with clear messaging and guidance on how to seek employment at the organization safely.
- Engage relevant agencies such as the Internet Crime Complaint Center, Better Business Bureau, Federal Bureau of Investigation, and the Federal Trade Commission should job scams be identified that are leveraging an organization.
- Protect job seekers, recruiters, and organizational reputation by engaging ZeroFox for ongoing monitoring of social and digital platforms for impersonation accounts promoting fake job postings. In addition, ongoing

² [hXXps://finance.yahoo\[.\]com/news/job-offer-just-received-heres-133003087.html](https://finance.yahoo.com/news/job-offer-just-received-heres-133003087.html)



monitoring of domains is important to identify fraudulent websites that have been stood up to leverage a brand in order to attract job seekers.

- Utilize ZeroFox's disruption services in order to remediate any fraudulent content or websites.



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.