Cyber Criminals Use Fake Job Listings to Target Applicants' Personally Identifiable Information

What are Fake Job or Hiring Scams?

Fake Job or Hiring Scams occur when criminal actors deceive victims into believing they have a job or a potential job. Criminals leverage their position as “employers” to persuade victims to provide them with personally identifiable information (PII) or to send them money.

Threat

Fake Job Scams have existed for a long time but technology has made this scam easier and more lucrative. Cyber criminals now pose as legitimate employers by spoofing company websites and posting fake job openings on popular online job boards. They conduct false interviews with unsuspecting applicant victims, then request PII and/or money from these individuals. The PII can be used for any number of nefarious purposes, including taking over the victims’ accounts, opening new financial accounts, or using the victims’ identity for another deception scam (such as obtaining fake driver’s licenses or passports).

Methods

Criminals first spoof a legitimate company’s website by creating a domain name similar in appearance to a legitimate company. Then they post fake job openings on popular job boards that direct applicants to the spoofed sites. Applicants can apply on the spoofed company websites or directly on the job boards. Applicants are contacted by email to conduct an interview using a teleconference application. According to victims, cyber criminals impersonate personnel from different departments, including recruiters, talent acquisition, human resources, and department managers.

After being interviewed by cyber criminals, victims are offered jobs, usually in a work-at-home capacity. In order to appear legitimate, the criminals send victims an employment contract to physically sign, and also request a copy of the victims’ driver’s licenses, Social Security numbers, direct deposit information, and credit card information. Criminals may also tell victims they need to pay upfront for background checks or screenings, job training, start-up equipment, or supplies. In many cases, victims are told they

will be reimbursed in their first paycheck. Once they get money, criminals stop communicating with their victims.

Trends

Since early 2019, victims have reported numerous examples of this scam to the FBI. The average reported loss was nearly $3,000 per victim, in addition to damage to the victims' credit scores. While hiring scams have been around for many years, cyber criminals' emerging use of spoofed websites to harvest PII and steal money shows an increased level of complexity. Criminals often lend credibility to their scheme by advertising alongside legitimate employers and job placement firms, enabling them to target victims of all skill and income levels.

Indicators

Cyber criminals executing this scam request the same information as legitimate employers, making it difficult to identify a hiring scam until it is too late. Some indications of this scam may include:

- 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 request credit card information.
- Job postings appear on job boards, but not on the companies' websites.
- Recruiters or managers do not have profiles on the job board, or the profiles do not seem to fit their roles.

Tips to Protect Yourself

- Conduct a web search of the hiring company using the company name only. Results that return multiple websites for the same company (abccompany.com and abccompanyllc.com) may indicate fraudulent job listings.
- Legitimate companies will ask for PII and bank account information for payroll purposes AFTER hiring employees. This information is safer to give in-person. If in-person contact is not possible, a video call with the potential employer can confirm identity, especially if the company has a directory against which to compare employee photos.
- Never send money to someone you meet online, especially by wire transfer.

- Never provide credit card information to an employer.
- Never provide bank account information to employers without verifying their identity.
- Never share your Social Security number or other PII that can be used to access your accounts with someone who does not need to know this information.
- Before entering PII online, make sure the website is secure by looking at the address bar. The address should begin with “https://”, not “http://”.
    - However: criminals can also use https:// to give victims a false sense of security. A decision to proceed should not be based solely upon the use of “https://”.

What to Do If You Are a Victim

If you are a victim of a hiring scam, the FBI recommends taking the following actions:

- Report the activity to the Internet Crime Complaint Center at www.ic3.gov or your local FBI field office, which can be found online at www.fbi.gov/contact-us/field-offices.
- Report the activity to the website in which the job posting was listed.
- Report the activity to the company the cyber criminals impersonated.
- Contact your financial institution immediately upon discovering any fraudulent or suspicious activity and direct them to stop or reverse the transactions.
- Ask your financial institution to contact the corresponding financial institution where the fraudulent or suspicious transfer was sent.