Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

February 01, 2022

Alert Number

I-020122-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: **www.fbi.gov/contact-us/field-offices**

Scammers Exploit Security Weaknesses on Job Recruitment Websites to Impersonate Legitimate Businesses, Threatening Company Reputation and Defrauding Job Seekers

The FBI warns that malicious actors or 'scammers' continue to exploit security weaknesses on job recruitment websites to post fraudulent job postings in order to trick applicants into providing personal information or money. These scammers lend credibility to their scheme by using legitimate information to imitate businesses, threatening reputational harm for the business and financial loss for the job seeker.

Since early 2019, the average reported loss from this scheme is nearly $3,000 per victim, and many victims have also reported that the scheme negatively affected their credit scores.

TACTICS OF THE SCAMMERS:

Scammers spoof legitimate companies to post fraudulent job postings on commonly used employment-oriented networking sites. The lack of strong security verification standards on one recruitment website allowed anyone to post a job on the site, including on official company pages. Those postings would appear alongside legitimate jobs posted by the business, making it difficult for applicants and the spoofed company to discern which job posting was real and which one was fraudulent. Scammers also replicate legitimate job postings, alter the contact information, and post the now-fraudulent job announcement on additional networking sites.

Fraudulent job listings include links and contact information that direct applicants to spoofed websites, email addresses, and phone numbers controlled by the scammers where the applicant's personal information can be stolen and then sold or used in additional scams. The logos, images, email addresses, and spoofed websites closely resemble the information of the legitimate company. In some cases, the scammers use the identities of actual company employees to increase the perceived authenticity

of the job posts. They may continue to use those identities in their interactions with the job seekers during the fraudulent interview and hiring process.

BUSINESS RISK:

Companies should consider taking steps to protect their brand and reputation from scammers who use their name, images, and likeness to commit fraud through fake job postings. Job seekers who are unaware they have been scammed may write negative reviews of the victim company; thus, adversely impacting the company's ratings on career websites and social media platforms. Additionally, if a company is often associated with fake job postings, candidates may seek jobs with competitor companies rather than risk being scammed. Company time and resources may be expended to address inquiries from job seekers who applied for and/or accepted fraudulent jobs. The reputational damage to companies could make it difficult to hire qualified personnel, and can erode customer and investor trust in the business, negatively impacting sales and profitability.

REPRESENTATIVE EXAMPLES:

The FBI identified instances of malicious actors impersonating companies and posting fraudulent jobs on networking sites.

- In August 2021, a company noticed a new, unusual job posting on their company profile on a commonly used networking site that was not posted by the company. The information on the fraudulent posting was possibly intended to steal Personally Identifiable Information (PII) or other sensitive information, and included a spoofed website domain. While the company was working to remove the fraudulent job posting, they received emails from job seekers who had applied, including some who were offered the position by the scammers.

- In April 2021, a human resources (HR) manager was contacted by a job seeker who applied for a position listed on a commonly used networking site. The job seeker had applied for the job and was quickly contacted, interviewed, and offered the position by the scammers. However, the job seeker became suspicious that the job was illegitimate and reached out to the company directly. The HR manager confirmed the job was not posted by the company and was fraudulent. The scammers used a spoofed email address and assumed the identities of legitimate company employees.

- In September 2020, a company posted a legitimate job on the website of a commonly used employment-oriented service. Job seekers notified the company they had been scammed by a

separate posting masquerading as the company's legitimate job posting. The scammers used the identifying information of the HR manager, Owner, and President on illegitimate job postings which were then posted to other networking sites.

RECOMMENDATIONS FOR EMPLOYERS:

- Proactively search for fraudulent job postings under your business name on common networking sites and locations where your business posts employment opportunities. If fraudulent profiles or jobs are found, report them to the website administrator to have them removed. Additionally, report all observed cyber criminal activity to the FBI Internet Crime Complaint Center (IC3) at IC3.gov.
- Understand the security features of online recruitment platforms used to prevent unauthorized job postings using your company account. Enable options to block unauthorized posts and require secured verification.
- Maintain strict controls for users on networking sites your organization uses by adding individual users and setting strict access levels. Practice the principle of least privilege. Do not share your account's email and password among users.
- Monitor for fraudulent activity on networking sites and all accounts your organization maintains with those sites. Watch for unauthorized account changes, changes to your employer profile, messages coming from your account that you did not send, and jobs that you did not post. If available, enable automatic notifications of changes and enable multi-factor authentication for all changes to account settings.
- List job postings on your official business website with instructions on how to apply, including the legitimate contact information for your company.
- If your company has been used in fake job postings, make applicants aware of it by adding a warning to your job listing or careers web page. Include a list of red flags to help applicants identify fraudulent ads, such as misspellings, grammatical errors, or incorrect contact information. Additionally, include ways to determine jobs that are legitimately posted by you; for example, "We will not hire through text message/social media/email alone," "We require in-person completion of an I-9 document," or "We will not send you a check to cash on our behalf." Refer applicants to additional resources like those found on the Internet Crime Complaint Center (IC3) website. *(www.ic3.gov)*
- Educate your employees about fraudulent application scams and create a plan to help employees identify and report suspicious job postings. Ensure employees involved in the hiring process know that victims of recruitment scams may contact them and that a sensitive response to their situation may help mitigate potential damage to your company's reputation.

RECOMMENDATIONS FOR JOB SEEKERS:

- 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.
- Verify job postings found on networking and third-party websites on the hiring company's own website or through legitimate HR representatives at the hiring company.
- 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://".

For additional information on how individuals can protect themselves from hiring scams, see Cyber Criminals Use Fake Job Listings to Target Applicants' Personally Identifiable Information (Alert Number I-012120-PSA)

The COVID-19 pandemic has drastically changed interview and hiring processes making it imperative that businesses and job applicants verify the legitimacy of postings and employment opportunities. The FBI urges the American public to use caution when applying for and accepting positions through an entirely remote process that has limited or no in person meetings, contact, and onboarding.

VICTIM REPORTING AND ADDITIONAL INFORMATION:

The FBI encourages the public to report information concerning suspicious or criminal activity to their local FBI field office (http://www.fbi.gov/contact-us/field-offices) or the FBI's Internet Crime Complaint Center (www.ic3.gov).