Data Breach Today
Prevention. Response. Notification.
https://www.databreachtoday.com/

Cybercrime , Fraud Management & Cybercrime , Social Engineering

# FBI Warns: Beware of Spoofed Job Application Portals

Fraudsters Targeting Personal Information, Including Payment Card Details

Akshaya Asokan (asokan_akshaya) • January 23, 2020

The FBI's Internet Crime Complaint Center has issued an alert warning that fraudsters are using spoofed job application portals and websites to steal personal information, including payment card details, from would-be applicants.

**See Also:** Unlocking IAM - Balancing Frictionless Registration & Data Integrity

Scams that target job applicants in the U.S. have been steadily rising since early 2019, with victims reporting losses averaging nearly $3,000 each, according to the FBI alert issued Tuesday. And while these scams are not new, the FBI notes that cybercriminals are now relying on advanced social engineering techniques.

"Cybercriminals now pose as legitimate employers by spoofing company websites and posting fake job openings on popular online job boards," according to the FBI alert. "They conduct false interviews with unsuspecting applicant victims, then request [personally identifiable information] and/or money from these individuals."

The FBI notice cautions that fraudsters can use stolen data to wage account take-over attacks as well as open bank accounts or fabricate victims' identities.

## Website Spoofing

In the scams targeting job applicants, fraudsters are now targeting victims by spoofing popular job websites or well-known job portals, according to the alert. The bureau, however, did not name sites being targeted for spoofing.

Once the victim applies for a position through one of these spoofed domains, the fraudsters then contact the individual through email and confirm their "interviews," according to the alert.

In several cases, the scammers conducted interviews through teleconference apps that use email addresses instead of phone numbers, according to the FBI.

"After being interviewed by cybercriminals, victims are offered jobs, usually in a work-at-home capacity," according to the FBI. "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."

In many instances, the FBI notes, the fraudsters asked their victims to make payment upfront for what the scammers claim is the cost of background checks, screenings, job training and start-up equipment or supplies, according to the alert. Victims were told they would be reimbursed when they receive their first pay checks.

But once the attackers received the money, the criminals shut down all communication with the victims.

## Similar Attacks

A 2019 study by security firm Thales found that worldwide, website spoofing doubled in the second half of 2018, resulting in $1.3 billion in losses.

And in November, security analysts found that a new hacking group was using an array of sophisticated spoofing and social engineering techniques to imitate government agencies, including the U.S. Postal Service, in an effort to plant malware in victims' devices and networks through various phishing campaigns, according to security firm Proofpoint (see: *Phishing Campaigns Spoof Government Agencies: Report*)

---

### About the Author

Akshaya Asokan
*Senior Correspondent*

Asokan is senior correspondent for Information Security Media Group's global news desk. She has previously worked with IDG and other publications where she reported on developments in technology, minority-rights and education.