



UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND

Media contact: 571-305-4041

FOR IMMEDIATE RELEASE



Job Seekers Beware: Employment Scams on the Rise

QUANTICO, VA (Oct. 5, 2020) – At any given time, there may be as many scams posted online as there are actual job openings. The U.S. Army Criminal Investigation Command’s Major Cybercrime Unit is warning the Army community about employment scams being on the rise.

An employment scam is any attempt to defraud job seekers through the use of deception with the intention of personal or financial gain. According to the 2019 Internet Crime Report released by the Internet Crime Complaint Center, this method is proven to be effective in attempting to collect personal and financial information or steal money from job seekers.

“Employment scams have always been a problem, but we have seen an increase this year due to the pandemic,” said Edward Labarge, the director of CID’s Major Cybercrime Unit. “Scammers are taking advantage of the fact that millions of Americans have lost their jobs creating a target rich environment for these types of scams to thrive.”

CID special agents say these scams have potential to target a Soldier’s family members, or even a Soldier close to the end of enlistment or due to retire and seeking new employment. Scammers will target job seekers with the intent of financial gain, theft of job seekers personal information, and identity theft.

“All forms of employment scams are on the rise due to the pandemic,” said Labarge. “Be wary of any unsolicited job offer received via email. If it sounds too good to be true, it probably is.”
MCU also encourages the Army community to be weary of well-known employment online sites and recommends double-checking by verifying the posting with the actual business listing the job.

“Indeed, LinkedIn, and other major job boards are ideal places for finding jobs,” said Labarge. “However, these sites are also used by scammers so do your due diligence. If at all possible, cross reference any job openings on these sites to postings on the actual company’s website.”

Types of employment scams.

Below are examples of employment scams you may encounter. This is not an all-inclusive list.

Data Entry

Data entry employment scams often promise a lot of money for a job not requiring much skill. These scams often involve an upfront payment by the job seeker for processing or training. These jobs rarely pay as well as advertised and employee loses money initially paid.

Home-based Medical Billing

This scam involves the victim investing money into the business materials to start a medical billing business. However, the business material company rarely has any association with anyone in the medical community. Victims of this scam, like others, lose all of the money invested.

Money Transfers

Popular among scammers, the job involves moving money quickly between bank accounts, through money wire transfer services, or via gift and debit cards to another person. To the employee (victim), the job may appear legitimate, but the originating source of the funds is often unknown. In some instances, victims are sent fake checks, instructed to deposit to their account, and immediately transfer the money. Only to find out, the check was fake and now the employee (victim) is responsible for repayment to the financial institution.

Online Reshipping

Reshipping is a very serious job scam, because those who fall for it unintentionally become criminals. Reshipping jobs are work-at-home jobs involving repacking and forwarding ill-gotten goods. Victims of reshipping scams rarely receive any money, even for shipping charges paid out of their own pocket.

Stuffing Envelopes

Stuffing envelopes is a job scam that typically involves signing up and paying a fee to stuff envelopes from home. Once enrolled, you receive instructions how to get others to buy into the same job offer you did. Those who fall victim to this type of scam rarely see any substantial income.

Unsolicited Job Offers

Scammers, often pretending to be a recruiter from a reputable company, identify possible victims through social media and professional networking sites. Contact, initiated via email, text, or direct message, proposes an opportunity to interview or an immediate job offer. Once the unsuspecting victim accepts the interview or job offer, the scammer focuses on obtaining the victim's banking or Personally Identifiable Information.

Employment Scam Warning Signs

- You are offered guaranteed employment as long as you pay for up-front costs like credit checks or application fees.
- Misspellings and bad grammar in the job description.
- Recruitment via text message or a direct messaging application.
- Promises to make lots of money doing minimal work from home.
- Requests to pay or transfer money on behalf of someone else.
- The company insists on an online interview over a messaging service.
- Requests your personal information during, or before, a job interview.
- If it sounds too good to be true, it probably is.

Employment Scam Victim Reporting

- If you provided personal or bank information, contact your bank and any relevant financial institutions as soon as possible.
- Notify local law enforcement.
- Report it to commercial, state, and federal agencies:
 - The Better Business Bureau
 - The Federal Trade Commission
 - Internet Crime Complaint Center
 - State Consumer Protection Offices

Army personnel or their families who are victims of an Internet-based crime should report the crime to their local CID office. Individuals can also report crime tips to CID anonymously via a specialized application at <https://www.cid.army.mil/report-a-crime.html>.

For more information about computer security, other computer-related scams, and to review previous cybercrime alert notices and cyber-crime prevention flyers visit the Army CID MCU website at <https://www.cid.army.mil/mcu-advisories.html>. To report a crime to Army CID, visit www.cid.army.mil