Cybercrime Prevention Flyer



Report a crime to U.S. Army
Criminal Investigation Command

Major Cybercrime Unit

27130 Telegraph Road Quantico, Virginia 22134

Email

MCU Web Page



DISTRIBUTION:This document is authorized for the widest release without restriction.

CPF 00014-20-CID361-9H

29 September 2020

Employment Scams

You could be an Army spouse, teen, or recent college graduate seeking employment. You might be a Soldier about to ETS or retire and looking for your next professional adventure. Perhaps you are just looking to earn some extra money with a part-time job. Whatever the situation, do not fall victim to employment scams.

If you are a job seeker, scammers will target you with the intent on stealing your money, your personal information, and your identity. But with some awareness, you can identify employment scam warning signs, reducing your likelihood of becoming a victim.

What is an employment scam?

An employment scam is an attempt to defraud job seekers through the use of deception with the intention of personal or financial gain.

Types of employment scams.

Below are scams you may encounter. It is not meant to be an allinclusive list.

Data Entry

Data entry employment scams often promise a lot of money for a job that does not require 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 you will lose any money you initially paid.

Home-based Medical Billing

This scam involves the victim investing money into the business materials to start their own 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 victim is responsible for repayment to the financial institution.



Cybercrime Prevention Flyer

Online Reshipping

Re-shipping is a very serious job scam, because those who fall for it unintentionally become criminals. Re-shipping jobs are work-at-home jobs that involve repacking and forwarding ill-gotten goods. Victims of re-shipping 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



Cybercrime Prevention Flyer

US Postal Inspection Service

Resources

AARP Scam Tracking Map

Better Business Bureau Scam Tracker

Facebook Cybercrime Prevention Flyer

LinkedIn Cybercrime Prevention Flyer

To receive future MCU Cybercrime Prevention Flyers, send an email to: Subscribe CPF

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flyer, along with the views and opinions of authors, products or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations.