INTERNET FRAUD SCAMS

Commercial Bank

COMMON ON-LINE SCAMS & RED FLAGS

- Job
- Auction
- Lottery
- Investment

ONLINE JOB SCAMS

The most frequent types of on-line job scams include:

- Work at home jobs
- Mystery shopper jobs
- Payment transfer jobs
- Unsolicited job offers

WORK AT HOME JOB SCAMS

While there are some legitimate work at home jobs, beware of the following:

- Bogus work at home scams typically emanate from outside of the United States
- Fake job web sites often look very impressive and provide an air of legitimacy
- Job applications are professional looking

MYSTERY SHOPPER SCAMS

- Fraudulent mystery shopping promoters use newspaper ads and emails to create the impression that they're a gateway to lucrative mystery shopper jobs with reputable companies.

- These solicitations usually promote a web site where consumers can "register" to become mystery shoppers- after they pay a fee for information about a certification program, a directory of mystery shopping companies, or a guarantee of a mystery shopping job.

PAYMENT TRANSFER JOB SCAMS

- Payment transfer scams begin with a fraudster pretending to be an employer.
- The fraudster uses a job ad to lure in an unsuspecting job seeker, or information from a resume they have found.
- The con artists can be quite convincing, and may even steal company names and corporate logos to convince victims that they are legitimate.
- After the fraudster has won the job seeker's trust, they trick the job seeker into giving up bank account numbers.
- The reasons given for this can be clever. One common reason the con artists give out is to say they only deliver paychecks by "direct deposit".

PAYMENT TRANSFER JOB SCAMS

- The job seeker is asked to forward or wire money from a personal bank account, a PayPal account, or from a Western Union office to another account or person.
- The other account or person is often overseas.
- The job seeker is instructed to keep a small percentage of the money as their payment.
- Sometimes the payment for making the money transfer is as low as $15.00, sometimes it is as high as several hundred or several thousand dollars.

UNSOLICITED JOB SCAMS

- Unsolicited job scams involve phishing e-mails where the fraudster is hoping for a response from a potential victim job seeker.

- A job scam artist will attempt to gain their victim's confidence with well-rehearsed pitches and phone resources to extract personal information, even over the phone. It's important to remember that this information typically is not required before an in-person interview.

WORK AT HOME SCAM
RED FLAGS

- The company is trying to prove something by adding words like legitimate or guaranteed to their business name.
- The email address is from a free email account such as Hotmail, AOL, yahoo, or g-mail.
- You are unable to validate that it is a real business.
- They don't have any other contact information besides an email address.
- They hire you without an interview or reviewing your resume.
- The job description says "No Experience Necessary".

WORK AT HOME SCAM
RED FLAGS

- It's a pyramid scheme of any type where you recruit others to work under you.
- The job title is vague or includes the words rebate processor, data entry, stuff envelopes, home assembly, process claims, or anything of that nature.
- The job simply sounds to good to be true.

MYSTERY SHOPPER SCAM
RED FLAGS

The FTC says consumers should be skeptical of mystery shopping promoters who:

- Advertise for mystery shoppers in a newspaper's 'help wanted' section or by email. While it may appear as if these companies are hiring mystery shoppers, it's much more likely that they're pitching unnecessary-and possibly bogus-mystery shopping "services".
- Sell "certification". Companies that use mystery shoppers generally do not require certification.
- Guarantee a job as a mystery shopper. It is usually sporadic work.

MYSTERY SHOPPER SCAM
RED FLAGS

- Charge a fee for access to mystery shopping opportunities.
- Sell directories of companies that provide mystery shoppers.

PAYMENT TRANSFER & UNSOLICITED JOB

RED FLAGS

- The company emailed you out of the blue and you didn't apply for the job or contact them in any way.
- Request for bank account numbers and Social Security Number.
- Request to "scan the ID" of a job seeker for example, a drivers' license.
- Scam artists will say they need to scan job seekers' IDs to "verify identity".

LOTTERY & INVESTMENT SCAMS

What? You've been informed that you won a lottery for a contest that you hadn't entered?

You mean that a disposed Dictator has Millions of dollars in a US Bank account and will pay you a percentage of that if you will only help him out?

LOTTERY & INVESTMENT SCAMS

Don’t hope that it’s legit. If it’s too good to be true - it’s FRAUD.

LOTTERY & INVESTMENT SCAMS
RED FLAGS

Here are key points for avoiding scam lotteries:

- You cannot win a legitimate lottery if you have not entered it.
- In almost all cases you must purchase a ticket to enter a legitimate lottery.
- **You never have to pay to collect winnings from a legitimate lottery. You pay taxes AFTER you receive the winnings. There are no other fees.**
- If you hold a winning lottery ticket, you notify the lottery (they do not notify you; not by email, not by phone, not by mail).
- It is illegal under U.S. federal law to play ANY foreign lottery from the United States.

AUCTION SCAMS

Computers, sports memorabilia, rate coins, designer fashions, and even cars.

These are just a few of the items offered for sale every day on legitimate online auction sites.

They're also just a small sample of the items used to lure unsuspecting victims into online auction fraud schemes.

AUCTION SCAMS

Most of the one million-plus transactions that take place each day on these websites are legitimate; just a fraction actually result in some type of fraud.

There are a variety of auction frauds, but here are some of the more common ones to watch out for:

1. Overpayment fraud
2. Wire transfer schemes
3. Second chance schemes

AUCTION SCAMS

- **Overpayment fraud** – targets the seller. A seller advertises a high-value item, like a car or a computer, on the Internet. A scammer contacts the seller to purchase the item, then sends the seller a counterfeit check or money order for an amount greater than the price of the item. The purchaser asks the seller to deposit the payment, deduct the actual sale price, and then return the difference to the purchaser.

AUCTION SCAMS

- **Wire transfer schemes-** start with fraudulent and misleading ads for the sale of high-value items being posted on well-known online auction sites. When buyers take the bait, they are directed to wire money to the crooks using a money transfer company. Once the money changes hands, the buyer never hears from them again.

AUCTION SCAMS

- **Second-chance schemes**- involve scammers who offer losing bidders of legitimate auctions the opportunity to buy the item(s) they wanted at reduced prices. They usually require that victims send payment through money transfer companies, but then don't follow through on delivery.

AUCTION SCAM
RED FLAGS

- Ask the seller for a phone number and verify it.
- Beware of buyers who insist on wire transfers as the only form of payment they'll accept.
- For big-ticket items, use a legitimate online escrow service that will hold the payment until you receive what you've ordered.
- If you receive an overpayment as a seller, don't cash it but instead ask for the exact purchase price.
- Don't ever give out your social security number or your diver's license number; a legitimate seller wouldn't ask.
- Be skeptical if the price sounds to low.

QUESTIONS?

If you have any questions, please contact our Security Officer at **989-875-5517**