Avoiding Scams

Deal locally, face-to-face —follow this one rule and avoid 99% of scam attempts.

- **Do not extend payment to anyone you have not met in person.**
- **Beware offers involving shipping -** deal with locals you can meet in person.
- **Never wire funds (e.g. Western Union)** - anyone who asks you to is a scammer.
- **Transactions are between users only**, no third party provides a "guarantee".
- **Never give out financial info** (bank account, social security, account, etc).
- **Do not rent or purchase sight-unseen**—that amazing "deal" may not exist.
- **"(company name)voicemails"** - Any message asking you to access or check "**(company name)** voicemails" or "**(company name)** voice messages" is fraudulent - **no such service exists.**

Recognizing scams

Most scams attempts involve one or more of the following:

- **Email or text from someone that is not local to your area.**
- **Western Union, Money Gram, cashier check, money order, shipping, escrow service, or a "guarantee."**
- **Inability or refusal to meet face-to-face to complete the transaction.**
- **The scammer will often send an official looking (but fake) email that appears to come from (company name) or another third party, offering a guarantee, certifying a seller, or pretending to handle payments.**

Examples of Scams

1. Someone **claims your** transaction is guaranteed, that a buyer/seller is officially certified, OR **that a third party of any kind will handle or provide protection** for a payment:
    - These claims are fraudulent, as transactions are between users

2. Distant person offers a genuine-looking (but fake) cashier's check:

- You receive an email or text (examples below) offering to buy your item, pay for your services in advance, or rent your apartment, sight unseen and without meeting you in person.
- A cashier's check is offered for your sale item as a deposit for an apartment or for your services.
- Value of cashier's check often far exceeds your item—scammer offers to "trust" you, and asks you to wire the balance via money transfer service.
- Banks will cash fake checks AND THEN HOLD YOU RESPONSIBLE WHEN THE CHECK FAILS TO CLEAR, sometimes including criminal prosecution.
- Scams often pretend to involve a 3rd party (shipping agent, business associate, etc.).

3. Someone requests wire service payment via Western Union or MoneyGram:

- Deal often seems too good to be true, price is too low, or rent is below market, etc.
- Scam "bait" items include apartments, laptops, TVs, cell phones, tickets, other high value items.
- Scammer may (falsely) claim a confirmation code from you is needed before he can withdraw your money.
- Rental may be local, but owner is "travelling" or "relocating" and needs you to wire money abroad.
- Scammer may pretend to be unable to speak by phone (scammers prefer to operate by text/email).

4. Distant person offers to send you a cashier's check or money order and then have you wire money:

- This is ALWAYS a scam in our experience—the cashier's check is FAKE.
- Sometimes accompanies an offer of merchandise, sometimes not.
- Scammer often asks for your name, address, etc. for printing on the fake check.
- Deal often seems too good to be true.

5. Distant seller suggests use of an online escrow service:

- Most online escrow sites are FRAUDULENT and operated by scammers.
- For more info, do a google search on "fake escrow" or "escrow fraud."

6. Distant seller asks for a partial payment upfront, after which they will ship goods:

- He says he trusts you with the partial payment.
- He may say he has already shipped the goods.
- Deal often **sounds too good to be true**.

7. Foreign company offers you a job receiving payments from customers, then wiring funds:

- Foreign company may claim it is unable to receive payments from its customers directly.
- You are typically offered a percentage of payments received.
- This kind of "position" may be posted as a job, or offered to you via email.

How to avoid phishing attempts and protect your account information

- Never click on email links that ask you for any personal or account information.
- Make sure to login to your account **only by navigating manually to (company name. Com)**

- If you are unsure about the status of your account or your posts, the safest way to check is to go directly to craigslist.org and login.
- If you do not see any problems within your account, you can safely ignore any messages to the contrary.
- Never provide a phone authentication code to anyone else.
- craigslist will only ask for you to enter it on our site as part of the posting process.
- **Use common sense**. If an email seems suspicious, fishy, or too good to be true. . . it probably is!

Think you've been phished?

If you see strange activity or unfamiliar posts on your account page, please change your password immediately and manually delete the ads.

If you use the same password for your email account (or any other services), you may want to change those passwords as well.

Ask a question. Don't be afraid of opening a dialog with the seller. A good seller will encourage communication in order to get your business.

Look at the item. What condition is it in? What condition do you expect it to be in?

Read the description of the item thoroughly. Has this item been in use for the last decade...in storage for a while, or only driven by his grandma on Sunday.

Look at the type of image being displayed. Is it a photo of the actual object, or is it a stock photo of the item. (e.g. a stock image of a Canon camera lens, or the actual picture of the lens you are trying to buy).

To avoid this scam: (company name. Com) jobs are always posted on **(company name .com)**/jobs, and there is never any upfront fee to apply or interview for one.

To avoid this scam: (company name) covers phishing fraud on its website - here's what the company says. "**(company name)** will never send you an unsolicited e-mail that asks you to provide sensitive personal information like your social security number, tax ID, bank account number, credit card information, ID questions like your mother's maiden name or your password. If you receive a suspicious e-mail please report it immediately."

The "Fake Product" (company name) Scam

This **(company name)** scam afflicts site buyers who believe they're purchasing a genuine, brand name product only to find that the product is a rip-off and nowhere near worth the money paid for it. Counterfeit sellers are a fact of life on **(company name)** and, even though the company does solid work in vetting and kicking fake sellers off the site, too many bogus sellers slip through the cracks and into the **(company name)** platform.

To avoid this scam: Simply ignore the caller or emailer, and never use **(company name)**