Internet Classified Scams

The Office of the
Minnesota Attorney General
helping people afford their lives and live with dignity, safety, and respect

While the Internet offers convenience, it can also enable scam operators to defraud buyers and sellers. Fraudsters can use the Internet to dupe individuals looking to buy or sell items such as cars, boats, rental housing, or other products and services.

Take, for example, the following scenarios:

"Trisha" posted an advertisement on an Internet classified website to sell a bike for $60. Trisha received an email from "Jerry Smith" offering to purchase the bike. Mr. Smith sent Trisha a check for $1,400, and instructed her to keep $100 and wire the funds to a shipper. Trisha did as she was instructed. Five days later, Trisha received a notice from her bank that the check was fraudulent.

"Jake" was looking for a home to rent and responded to an advertisement on an Internet classified website. The purported owner told Jake that she was a sergeant in the United States Air Force and had to report for active duty, so she needed someone to care for her property. She subsequently forwarded paperwork to Jake, which he completed by providing his address, phone number, income, and driver's license number. After receiving the paperwork, the scammer asked Jake to send a substantial amount of money to her sister in California. Luckily, Jake became suspicious and, after conducting a property search, he confirmed that the "owner" did not really own the property. Unfortunately, the fraudster obtained Jake's personal information, which places him at risk for identity theft.

Most Internet classified scams involve fraudsters trying to convince a victim to send money to someone who is not who they pretend to be. Fraudsters often request that you wire money or use an Internet payment service to fraudulently obtain your money. Many perpetrators of Internet scams operate in countries outside of the United States, complicating law enforcement actions and attempts to retrieve money. People who are asked to wire or otherwise submit payment to a party in another country who they do not know should exercise great caution, as this is a primary red flag for a potential Internet classified scam.

Consumers must also consider their personal safety in situations where they are asked to bring cash to a meeting with a potential "seller." There have been reports across the country of buyers being robbed or worse when they arrive at an arranged location to pick up a television, computer or other item listed in an online ad.

Overview of Internet Classified Scams

Internet classified scams are twists on Advance Fee Scams, a fraud that has been around for many years. The scam artist capitalizes on advancements in cheap technology to create an email address, produce a glitzy website, manufacture authentic-looking counterfeit checks, and replicate official-looking logos and trademarks to make the scammer appear legitimate. Communication between potential buyers and sellers is established through online classified sites, such as *craigslist.com* or *ebay.com*. While most communications occur via email or text message, some scammers negotiate through phone calls, using Caller ID spoofing to hide the scammer's actual telephone number. Whether on the buying or selling side of the transaction, the scammer uses various appeals to persuade the victim to send the scammer money either by using fake online pay systems or by wiring money to the scam artist. Once the payment is made, the scammer disappears along with the victim's money.

Consumer Tips to Avoid Internet Classified Scams

1. Consider your safety first. Whether buying or selling a product online, you will most likely not know the person with whom you are transacting. Take the following precautions to protect your safety: arrange to meet in a public place—many local police departments have set up safe zones at their stations to complete transactions; tell others where you are going, who you will be meeting and when you expect to return; ask a friend, family member or coworker to join you; bring a cell phone; if the situation seems suspicious or potentially dangerous, move to a safe location as quickly as possible.

2. Beware of Internet payment services that you are asked to access through a link or in the body of an email. Remember that links can be masked, and logos and trademarks can be faked online. If you intend to use what you believe is a well-known Internet payment service, visit that company's website yourself, rather than trust the information that another party is suggesting.

3. Don't be rushed. If someone really wants to do business with you, they will wait until you are ready to make a legitimate transaction. Furthermore, if an individual wishes to make changes to the terms of the transaction, such as where and how the payment is sent, do not let your eagerness to complete the transaction blind you to potential problems.

4. Be wary of wiring money to a party that you don't know. Many people mistakenly think that wire transfers, like personal checks, can be canceled at any time. This is not true. If you wire money via Western Union or MoneyGram, it's impossible to retrieve the money once it's picked up at the other end. Because it can be picked up anywhere in the world, the money is virtually untraceable. Once money is wired overseas, United States law enforcement agencies may have little ability to recover lost funds.

5. Cashier's checks are NOT the same as cash. Counterfeit checks can look very authentic. Just because the money appears to be available in your account doesn't mean that the check has cleared and is legitimate. Federal rules require banks to make deposits "available" to consumers quickly, often the following business day. A check takes a long time to clear. It may take a bank weeks to discover that the deposited check was fraudulent. The bank may still bounce the check if it's a forgery. Once a victim wires funds onward from such a check, he or she may be liable to the bank for the amount wired. Typically the bank will not cover the loss, and expects the victim to pay the difference. If you do receive a check, attempt to locate the source of the check and verify its legitimacy by contacting the issuing bank. Do not use the contact information that appears on the check. Do a little leg work and obtain the contact information independently through legitimate directories.

6. A deal that sounds too good to be true probably is. Always be wary of someone who wants to pay more than your asking price or who wants to sell you an item at an unbelievably low price.

7. Be wary of "third parties" or "agents." If a third party is actually owed any money, their client should be making the payment, not you. Do not wire money to a third party.

The Federal Bureau of Investigation, United States Secret Service, the United States Postal Inspection Service, and local law enforcement officials, such as county attorneys and police departments, have authority and jurisdiction over online crime. If you would like to report an incident of an online crime, you may contact some of these agencies as follows:

Federal Bureau of Investigation
Minneapolis Office
1501 Freeway Boulevard
Brooklyn Center, MN 55430
(763) 569-8000
www.ic3.gov (Internet Crime Complaint Center)

United States Secret Service
Minnesota Electronic Crimes Task Force
300 South Fourth Street
Minneapolis, MN 55415
(612) 348-1800
www.secretservice.gov

United States Postal Inspection Service
Criminal Investigation Service Center
433 West Harrison Street, Room 3255
Chicago, IL 60699-3255
(877) 876-2455
postalinspectors.uspis.gov