



THOMAS R. SUOZZI  
County Executive

NASSAU COUNTY  
**SPiN**  
A Crime Prevention Partnership  
SECURITY / POLICE INFORMATION NETWORK



LAWRENCE W. MULVEY  
Commissioner

## Internet Crimes

**Online pharmacy fraud:** consumers respond to e-mails by buying drugs from Internet pharmacies that may not meet industry standards. The danger is that consumers may receive counterfeit, tainted and diluted drugs. Online pharmacy fraud incorporates numerous crimes and potentially dangerous health considerations. The scheme often starts with SPAM-level email circulation sent to potential customers offering a staggering variety of scheduled drugs without a prescription. Customers are sometimes required first to submit private information and fees for a membership. This may turn into the last contact they have with the company. Victims are now unable to recover their membership fee and faced with the fear of possible identity theft from a phishing scheme.

**Auction fraud:** an item is purchased but never delivered. Many of the cases involve straightforward scams where consumers allegedly "won" the bid for merchandise through an Internet auction Web site, sent in their money, but never received the merchandise. Internet auction sites give buyers a "virtual" flea market with new and used merchandise from around the world; they give sellers a global storefront from which to market their goods. But the online auction business can be risky business. The Federal Trade Commission (FTC) wants to help buyers and sellers stay safe on Internet auction websites. Among the thousands of consumer fraud complaints the FTC receives every year, those dealing with online auction fraud consistently rank near the top of the list. The complaints generally deal with late shipments, no shipments, or shipments of products that aren't the same quality as advertised; bogus online payment or escrow services; and fraudulent dealers who lure bidders from legitimate auction sites with seemingly better deals.

**Sweepstakes or lottery fraud:** participants pay to play or to receive their winnings. Potential victims are notified via e-mail that they have won a large prize in a foreign lottery. In most cases, the victim is asked to provide either an up-front fee, or bank account or social security numbers so that the lottery can transfer the money. The lottery scheme deals with persons randomly contacting email addresses advising them they have been selected as the winner of an International lottery. The Internet Crime Complaint Center has identified numerous lottery names being used in this scheme. The email message usually reads similar to the following: "This is to inform you of the release of money winnings to you. Your email was randomly selected as the winner and therefore you have been approved for a lump sum payout of \$500,000.00. To begin your lottery claim, please contact the processing company selected to process your winnings." An agency name follows this body of text with a point of contact, phone number, fax number, and an email address. An initial fee ranging from \$1,000 to \$5,000 is often requested to initiate the process and additional fee requests follow after the process has begun. These emails may also list a United States point of contact and address while also indicating the point of contact at a foreign address.

**Identity fraud:** Internet thieves steal money through identity theft -- by pretending to be the victim and using their name, Social Security number, account numbers or other information. The thieves may access the information by: Hacking into industry or individual computer databases.

**Phishing**, or sending e-mail or pop-up messages that deceives consumers into disclosing personal or financial information. The newest type of phishing scam is one that focuses on a single user or a department within an organization. The Phish appears to be legitimately addressed from someone within that company, in a position of trust, and request information such as login IDs and passwords. Spear phishing scams will often appear to be from a company's own human resources or technical support divisions and may ask employees to update their username and passwords. Once hackers get this data they can gain entry into secured networks. Another type of spear phishing attack will ask users to click on a link, which deploys spyware that can steal data.

**Spoofing**, or directing consumers to a "spoofed" or fake Web site that looks just like one they know, such as their banks, to type in personal information.

Downloading spyware from the Internet onto a computer to collect its owner's personal information.

E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations.

**Financial fraud:** the promise of a guaranteed loan if a fee is paid in advance, appeals from fraudulent charities, work-at-home jobs that require large upfront payments and requests for financial assistance that will pay off with more money later.

Financial institutions and credit card issuers are well aware of the magnitude of online fraud. Most offer a variety of services to help their customers avoid fraud and reduce financial loss. One of those services is usually some form of online fraud alert.

**Debt elimination** schemes generally involve websites advertising a legal way to dispose of mortgage loans and credit card debts. Most often, all that is required of the participant is to send \$1,500 to \$2,000 to the subject, along with all the particulars of the participant's loan information and a special power of attorney authorizing the subject to enter into transactions regarding the title of the participant's homes on their behalf. The subject then issues bonds and promissory notes to the lenders that purport to legally satisfy the debts of the participant. In exchange, the participant is then required to pay a certain percentage of the value of the satisfied debts to the subject. The potential risk of identity theft related crimes associated with the debt elimination scheme is extremely high because the participants provide all of their personal information to the subject.

**The Counterfeit Cashier's** check scheme targets individuals that use Internet classified advertisements to sell merchandise. Typically, an interested party located outside the United States contacts a seller. The seller is told that the buyer has an associate in the United States that owes him money. As such, he will have the associate send the seller a cashier's check for the amount owed to the buyer.

The amount of the cashier's check will be thousands of dollars more than the price of the merchandise and the seller is told the excess amount will be used to pay the shipping costs associated with getting the merchandise to his location. The seller is instructed to deposit the check, and as soon as it clears, to wire the excess funds back to the buyer or to another associate identified as a shipping agent. In most instances, the money is sent to locations in West Africa (Nigeria).

Because a cashier's check is used, a bank will typically release the funds immediately, or after a one or two day hold. Falsely believing the check has cleared, the seller wires the money as instructed.

In some cases, the buyer is able to convince the seller that some circumstance has arisen that necessitates the cancellation of the sale, and is successful in conning the victim into sending the remainder of the money. Shortly thereafter, the victim's bank notifies him that the check was fraudulent, and the bank is holding the victim responsible for the full amount of the check.

**Escrow Services Fraud** In an effort to persuade a wary Internet auction participant, the perpetrator will propose the use of a third-party escrow service to facilitate the exchange of money and merchandise. The victim is unaware the perpetrator has actually compromised a true escrow site and, in actuality, created one that closely resembles a legitimate escrow service. The victim sends payment to the phony escrow and receives nothing in return. Or, the victim sends merchandise to the subject and waits for his/her payment through the escrow site which is never received because it is not a legitimate service.

**The Parcel Courier** Email Scheme involves the supposed use of various National and International level parcel providers such as DHL, UPS, FedEx and the USPS. Often, the victim is directly emailed by the subject(s) following online bidding on auction sites. Most of the scams follow a general pattern which includes the following elements:

- The subject instructs the buyer to provide shipping information such as name and address.
- The subject informs the buyer that the item will be available at the selected parcel provider in the buyer's name and address, thereby, identifying the intended receiver.
- The selected parcel provider checks the item and purchase documents to guarantee everything is in order.
- The selected parcel provider sends the buyer delivery notification verifying their receipt of the item.
- The buyer is instructed by the subject to go to an electronic funds transfer medium, such as Western Union, and make a funds transfer in the subject's name and in the amount of the purchase price.
- After the funds transfer, the buyer is instructed by the subject to forward the selected parcel provider the funds transfer identification number, as well as their name and address associated with the transaction.
- The subject informs the buyer the parcel provider will verify payment information and complete the delivery process.

Upon completion of delivery and inspection of the item(s) by the receiver, the buyer provides the parcel provider funds transfer information, thus, allowing the seller to receive his funds.

**Sources:** [WWW.CRIME-RESEARCH.ORG](http://WWW.CRIME-RESEARCH.ORG)  
[WWW.IC3.GOV/COMPLAINT](http://WWW.IC3.GOV/COMPLAINT)

The NCPD does not necessarily endorse the views expressed on a particular website or guarantee the accuracy or completeness of information on them.

NCPD/SPIN