Internet Crime Schemes

Current and ongoing Internet trends and schemes identified by the **Internet Crime Complaint Center** (IC3) along with its description:

Auction Fraud

Auction fraud involves fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.

Consumers are strongly cautioned against entering into Internet transactions with subjects exhibiting the following behavior:

- The seller posts the auction as if he resides in the United States, then responds to victims with a congratulatory email stating he is outside the United States for business reasons, family emergency, etc. Similarly, beware of sellers who post the auction under one name, and ask for the funds to be transferred to another individual.
- The subject requests funds to be wired directly to him/her via Western Union, MoneyGram, or bank-to-bank wire transfer. By using these services, the money is virtually unrecoverable with no recourse for the victim.
- Sellers acting as authorized dealers or factory representatives in countries where there would be no such dealers should be avoided.
- Buyers who ask for the purchase to be shipped using a certain method to avoid customs or taxes inside another country should be avoided.
- Be suspect of any credit card purchases where the address of the card holder does not match the shipping address. Always receive the card holder's authorization before shipping any products.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

In addition, visit eBay and PayPal for additional security alerts and fraud prevention tips.

Auction Fraud — Romania

Auction fraud is the most prevalent of Internet crimes associated with Romania. The subjects have saturated the Internet auctions and offer almost every in-demand product. The subjects have also become more flexible, allowing victims to send half the funds now, and the other half when the item arrives.

The auctions are often posted as if the seller is a United States citizen, then the subject advises the victim to send the money to a business partner, associate, sick relative, a

family member, etc., usually in a European country. The money is usually transferred via MoneyGram or Western Union wire transfer. The Internet Crime Complaint Center has verified in order to receive funds via Western Union, the receiver must provide the complete information of the sender and the receiver's full name and address. The funds can be picked up anywhere in the world using this information. There is no need to provide the money transfer control number (MTCN) or the answer to any secret question, as many subjects have purported to the victims. Money sent via wire transfer leaves little recourse for the victim.

The most recent trend is a large increase in bank-to-bank wire transfers. Most significantly, these wire transfers go through large United States banks and are then routed to Bucharest, Romania or Riga, Latvia.

Similarly, the sellers also occasionally direct the victims to pay using phony escrow services. Sometimes actual escrow websites are compromised and other sites resembling them are created by the subjects. Once the funds are wire transferred to the escrow website, the seller discontinues contact. See also, Escrow Fraud.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

In addition, visit eBay and PayPal for additional security alerts and fraud prevention tips.

Counterfeit Cashier's Check

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.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

Credit Card Fraud

The Internet Crime Complaint Center has received multiple reports alleging foreign subjects are using fraudulent credit cards. The unauthorized use of a credit/debit card, or card number, to fraudulently obtain money or property is considered credit card fraud. Credit/debit card numbers can be stolen from unsecured websites, or can be obtained in an identity theft scheme.

Visit any of the three credit bureaus, Equifax, Experian, or TransUnion, for more information or to place a fraud alert on your credit report.

Visit the Federal Trade Commission for additional information on security and fraud prevention tips.

]

Debt Elimination

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.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

Parcel Courier Email Scheme

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.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

Employment/Business Opportunities

Employment/business opportunity schemes have surfaced wherein bogus foreign-based companies are recruiting citizens in the United States on several employment-search websites for work-at-home employment opportunities. These positions often involve reselling or reshipping merchandise to destinations outside the United States.

Prospective employees are required to provide personal information, as well as copies of their identification, such as a driver's license, birth certificate, or social security card. Those employees that are "hired" by these companies are then told that their salary will be paid by check from a United States company reported to be a creditor of the employer. This is done under the pretense that the employer does not have any banking set up in the United States.

The amount of the check is significantly more than the employee is owed for salary and expenses, and the employee is instructed to deposit the check into their own account, and then wire the overpayment back to the employer's bank, usually located in Eastern Europe. The checks are later found to be fraudulent, often after the wire transfer has taken place.

In a similar scam, some web-based international companies are advertising for affiliate opportunities, offering individuals the chance to sell high-end electronic items, such as plasma television sets and home theater systems, at significantly reduced prices.

The affiliates are instructed to offer the merchandise on well-known Internet auction sites. The affiliates will accept the payments, and pay the company, typically by means of wire transfer. The company is then supposed to drop-ship the merchandise directly to the buyer, thus eliminating the need for the affiliate to stock or warehouse merchandise. The merchandise never ships, which often prompts the buyers to take legal action against the affiliates, who in essence are victims themselves.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

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.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

In addition, visit Escrow.com for security alerts and fraud prevention tips.

Identity Theft

Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business, sometimes as a response to an email solicitation to update billing or membership information, or as an application to a fraudulent Internet job posting. See also, Phishing/Spoofing.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

In addition, visit the Federal Trade Commission for additional information on security and fraud prevention tips.

Internet Extortion

Internet extortion involves hacking into and controlling various industry databases, promising to release control back to the company if funds are received, or the subjects are

given web administrator jobs. Similarly, the subject will threaten to compromise information about consumers in the industry database unless funds are received.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

Investment Fraud

Investment fraud is an offer using false or fraudulent claims to solicit investments or loans, or providing for the purchase, use, or trade of forged or counterfeit securities.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

Lotteries

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.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

Nigerian Letter or "419"

Named for the violation of Section 419 of the Nigerian Criminal Code, the 419 scam combines the threat of impersonation fraud with a variation of an advance fee scheme in which a letter, email, or fax is received by the potential victim. The communication from individuals representing themselves as Nigerian or foreign government officials offers the recipient the "opportunity" to share in a percentage of millions of dollars, soliciting for help in placing large sums of money in overseas bank accounts. Payment of taxes, bribes to government officials, and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are out of the country. The

recipient is encouraged to send information to the author, such as blank letterhead stationary, bank name and account numbers, and other identifying information using a facsimile number provided in the letter. The scheme relies on convincing a willing victim to send money to the author of the letter in several installments of increasing amounts for a variety of reasons.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

Visit the Economic and Financial Crimes Commission to learn more about combating financial and economic crimes in Nigeria.

Phishing/Spoofing

Phishing and spoofing are somewhat synonymous in that they refer to forged or faked electronic documents. Spoofing generally refers to the dissemination of email which is forged to appear as though it was sent by someone other than the actual source. Phishing, often utilized in conjunction with a spoofed email, is the act of sending an email falsely claiming to be an established legitimate business in an attempt to dupe the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information after directing the user to visit a specified website. The website, however, is not genuine and was set up only as an attempt to steal the user's information.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

Visit the Anti-Phishing Working Group, for more information on phishing and email spoofing.

Ponzi/Pyramid

Ponzi or pyramid schemes are investment scams in which investors are promised abnormally high profits on their investments. No investment is actually made. Early investors are paid returns with the investment money received from the later investors. The system usually collapses. The later investors do not receive dividends and lose their initial investment.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

Reshipping

The "reshipping" scheme requires individuals in the United States, who sometimes are coconspirators and other times are unwitting accomplices, to receive packages at their residence and subsequently repackage the merchandise for shipment, usually abroad.

"Reshippers" are being recruited in various ways but the most prevalent are through employment offers and conversing, and later befriending, unsuspecting victims through Internet Relay Chat Rooms.

Unknown subjects post help-wanted advertisements at popular Internet job search sites and respondents quickly reply to the online advertisement. As part of the application process, the prospective employee is required to complete an employment application, wherein he/she divulges sensitive personal information, such as their date of birth and social security number which, unbeknownst to the victim employee, will be used to obtain credit in his/her name.

The applicant is informed he/she has been hired and will be responsible for forwarding, or "reshipping", merchandise purchased in the United States to the company's overseas home office. The packages quickly begin to arrive and, as instructed, the employee dutifully forwards the packages to their overseas destination. Unbeknownst to the "reshipper," the recently received merchandise was purchased with fraudulent credit cards.

The second means of recruitment involves the victim conversing with the unknown individual in various Internet Relay Chat Rooms. After establishing this new online "friendship" or "love" relationship, the unknown subject explains for various legal reasons his/her country will not allow direct business shipments into his/her country from the United States. He/she then asks for permission to send recently purchased items to the victim's United States address for subsequent shipment abroad for which the unknown subject explains he/she will cover all shipping expenses.

After the United States citizen agrees, the packages start to arrive at great speed. This fraudulent scheme lasts several weeks until the "reshipper" is contacted. The victimized merchants explain to the "reshipper" the recent shipments were purchased with fraudulent credit cards. Shortly thereafter, the strings of attachment are untangled and the boyfriend/girlfriend realizes their Cyber relationship was nothing more than an Internet scam to help facilitate the transfer of goods purchased online by fraudulent means.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

Visit the Economic and Financial Crimes Commission to learn more about combating financial and economic crimes in Nigeria.

Spam

With improved technology and world-wide Internet access, spam, or unsolicited bulk email, is now a widely used medium for committing traditional white collar crimes including financial institution fraud, credit card fraud, and identity theft, among others. It is usually considered unsolicited because the recipients have not opted to receive the email. Generally, this bulk email refers to multiple identical messages sent simultaneously. Those sending this spam are violating the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, *Title 18, U.S. Code, Section 1037*.

Spam can also act as the vehicle for accessing computers and servers without authorization and transmitting viruses and botnets. The subjects masterminding this Spam often provide hosting services and sell open proxy information, credit card information, and email lists illegally.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.

Third Party Receiver of Funds

A general trend has been noted by the Internet Crime Complaint Center regarding work-at-home schemes on websites. In several instances, the subjects, usually foreign, post work-at-home job offers on popular Internet employment sites, soliciting for assistance from United States citizens. The subjects allegedly are posting Internet auctions, but cannot receive the proceeds from these auctions directly because his/her location outside the United States makes receiving these funds difficult. The seller asks the United States citizen to act as a third party receiver of funds from victims who have purchased products from the subject via the Internet. The United States citizen, receiving the funds from the victims, then wires the money to the subject.

If you believe you may have fallen victim to this type of scam and wish to report it, please file a complaint with us.