CONTACT:
Research Section
5000 NASA Boulevard, Suite 2400
Fairmont, WV 26554
Ph: 877-628-7674
Fax: 304-366-9095
Web: www.nw3c.org

Internet Fraud (2014)

Internet Fraud occurs either wholly or in part via the Internet. With the democratization of technology, more consumers are able to access markets with ease. [1] [1] This democratization has both positive and negative repercussions for consumers. The positive, for example, is one may now peruse the catalogues of previously inaccessible stores or easily access goods from local artisans and trades people. The negative includes more and new ways for consumers to find themselves vulnerable to criminals.

How It Occurs

Internet Fraud often involves overlapping activities by criminal elements that may include contacting potential victims, posing as a representative of a company, claiming a fraudulent computer issue or by stating a false need to "verify" account information. A common avenue is using email, instant messaging, texting or malware to obtain name, DOB, SSN, mailing address or other personally identifiable information needed to steal the victim's identity. In any instance, the criminal then uses that information in a variety of ways, some of which include using that data to purchase prepaid debit cards, phone cards, and gift cards or pay as you go cell phones. The criminals may also use the information to apply for credit in the victim's name, apply for a bank loan, mortgage, car loan etc, or they may sell the information to another criminal outfit.

Online auctions constitute another access point for criminals to acquire identity information and strip consumers of money or merchandise. A few common forms of Internet Fraud occur on these websites and may involve a consumer not receiving or receiving an incorrect product or a vendor not receiving a payment after sending a sold item. There is a wide variety of internet fraud types that include those designed to take money, goods, or identity information from individuals. One way to understand Internet fraud is to look at it as equivalent to crimes that occur offline; in fact, almost all crimes committed offline are committed online. The difference is that the Internet allows criminals a higher level of anonymity, access to a substantial number of potential victims, and involves schemes that are easy for criminals to implement, change, or discard.

Criminals online are remarkably adept at creating official looking documents and websites to lure potential victims. Prior to the Internet, these types of crimes were most often committed

[1] The democratization of technology refers to the open evolution of technical knowledge and hardware that result in greater accessibility. This democratization also allows users to affect their online worlds; allowing for innovative changes in both the development and revisions of tools and how individuals interact with each other online.

face to face, via phone, or post. The Internet makes it possible for a criminal to create a document or website that can reach millions of potential victims simultaneously, thereby expanding the potential profit gained by their fraudulent schemes. An added advantage to using the Internet, as a means to commit fraud, is that the victim rarely encounters the perpetrator, the reach of the scammer crosses jurisdictional lines and the perpetrator can take simple steps to hide their tracks.

For practical purposes, it is most helpful to address Internet fraud by the specific type of fraud committed. The Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) collaborated to establish the Internet Fraud Complaint Center in 2000, known today as the Internet Crime Complaint Center (IC3). The center's mission is:

> To serve as a vehicle to receive, develop and refer criminal complaints regarding the rapidly expanding area of cybercrime. The Internet Crime Complaint Center (IC3) gives the victims of cybercrime a convenient and easy-to-use reporting mechanism that alerts authorities to suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, local, tribal and international levels, IC3 provides a central referral mechanism for complaints involving Internet-related crimes.[2]

IC3 operates as a repository for online fraud complaints, tracks, and aids in defining online fraud types. When defining and explaining the intricacies of online fraud it is important to note that fraud type categories are not mutually exclusive. Each fraud type may share similar means to arrive at different goals. For example, Identity Theft is a fraud category of its own; however, Identity Theft often leads to other categories of fraud like Credit Card Fraud. Fraud Types frequently reported the IC3 include:

Auction Fraud

The Internet Crime Complaint Center defines Auction Fraud as "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."[3]

Online shoppers visit auction websites to buy and sell various items in an online format that resembles a real-life auction. Prospective buyers can bid on almost any item imaginable such as virtual currency, antique merchandise, or innumerable types of services. Upon winning the auction, the purchaser sends payment with the expectation of receiving. The fraud occurs when an item purchased fails to arrive or upon arrival the item delivered is not what the buyer bid on or not in the same condition as advertised.

The reverse is also possible where the purchaser negotiates a purchase with a seller and pays for the item using a stolen credit card, forged check or altered money order. Lag time for processing these financial instruments through the seller's bank often enable the con artist to obtain the merchandise long before the bank discovers that the check or money order is fraudulent.

Perhaps the most popular and well-known auction site on the Internet is eBay. Others include WebStore, eBid, and Overstock.[4] In recognition of the potential the Internet poses for abuse, many of the well-established auction sites are rating the reputation of their participants to better assure users of the safety of the site. Some are even beginning to implement measures whereby

they hold a purchaser's funds in escrow until delivery of the merchandise and the purchaser verifies their satisfaction. The purchaser may then authorize the release of the funds to the seller. Use of a credit card for such purchases may offer some measure of safety depending on the reimbursement policies of the issuing company but the system is still vulnerable to fraud.

There are several variations of Auction Fraud:

- *Triangulation* is one of the more complex Auction Fraud schemes and may involve three victims at one time. A thief finds a high-value item for sale on a site such as Amazon.com and posts it for sale on a different online auction site at a lower price. The winning bidder pays the scammer for the item. Meanwhile, the thief will purchase the item on Amazon.com with the credit card information provided by the purchaser from the other site. When the credit card owner becomes aware of the charge, which exceeds the original bid, the bank cancels the transaction, contacts Amazon.com and reverses the purchase. Amazon.com will then contact the online auction bidder and force them to surrender the item to them for non-payment even though the bidder thought they bought the item legitimately. This is an example of triangulation involving three victims, the credit card owner (victim #1)Amazon.com, (victim #2) and the online auction bidder who thought they bought the item but ends up having to surrender it to Amazon.com and can't get back the money paid for the item.[5] (victim #3)

- *Hidden charges*, which includes handling, packaging, postage and shipping of the product by the seller, are often a component or additional aspect of a fraud. Instead of having a flat rate on the shipping and handling, like most companies, these charges are hidden and not seen by the buyer when agreeing to purchase the item.[6] As a result, the buyer ends up paying more than anticipated.

- *Bid shielding* occurs when two or more people trying to get the lowest cost on an item work together to affect the final bid price. One person places a low bid for an item while the other bidder(s) place an absurdly high bid for the same item in the hope of scaring other bidders away. In the final moments of bidding, the higher bidder(s) will withdraw their offer leaving the lower bid as the best offer. In this case, the victim of the fraud is the seller of the item. Worse yet this type of fraud is extremely difficult to prove and recourse to the seller is extremely limited. Whether buying or selling, it is always best to check the policies of the auction site before doing business with them to avoid falling victim to this type of fraud.

Online Salvage Vehicle Auctions

One of the most common types of Auction Fraud is Online Salvage Vehicle Auctions (OSVA). An OSVA involves "salvage vehicles purchased or sold through Internet-based Online Auctions through online commerce companies…. Some of the related crimes to Online Salvage Vehicle Auction Fraud are Cloned Vehicles, Counterfeit Vehicles and Salvage Switches."[7] 3.5 million Vehicles are sold at auction in the U.S. each year and many of those auctions take place online. Because these auction websites often have minimal moderation and offer a high level of anonymity, it is a welcoming environment for criminals. Because this environment is global, it leads to both national and international crimes that include terrorism funding and money laundering.

To aid local and state law enforcement officers in combating criminals taking advantage of OSVAs, NW3C created a specialized training, The Online Salvage Vehicle Auction Fraud (OSVAF) that provides law enforcement with knowledge about vehicle theft and best practices in the investigation of vehicle-related crimes. Special topic areas include "the identification of motor vehicles; cloned vehicles; vehicle title fraud; salvage and rebuilt vehicle investigations; fraudulent vehicle purchases; export of stolen vehicles; vehicle parts, and The National Motor Vehicle Title Information System (NMVTIS) requirements."[8]

Tips on how to decrease risk: Auction Fraud

The Federal Bureau of Investigation outlines the following tips to help consumers avoid becoming a victim of auction fraud. Keep in mind that these tips, either individually or as a whole, will not make one immune to victimization. An individual is a victim because a criminal committed a crime, not because they bought something online from someone who is committing a crime. With that being said, the following tips may create awareness of the more common schemes.

- Thoroughly read the consumer guides, rules, or codes of conduct for the auction website you plan to use. Fully understand both the buyer's and seller's responsibilities before taking part in an auction.
- Read the websites fraud policy and decide if you find that policy satisfactory for your needs.
- Find out if the auction company has taken measures to insure monies or items lost to fraud.
- Find out as much as you can about the seller. It is reasonable to ask questions about the product and selling history. Try to get the seller on the phone instead of communicating solely through email. It is often helpful to Google the seller, the item for sale, the business, etc. Check out the business with the Better Business Bureau. You may even check the Secretary of State website of the state where the business is located to make sure it is in the state's business/corporation registry.
- Read the feedback the website offers about the seller.
- Some ways of paying for or accepting an item are also part of a fraud. It is important to understand and be comfortable with the methods the seller makes available to the buyer.
- When in doubt, use a credit card to purchase items. In many cases, a credit card holder may successfully dispute fraudulent purchases made from a stolen credit card number.
- Remember, when problems occur during international money transactions or item delivery it may be difficult for the company and local law enforcement to track and rectify the problem.
- Make sure to talk to the seller about the condition of the item, when you should receive it, and if they offer a warranty on the item.
- Go over the exact cost of the item and any normally relatable costs such as shipping and handling before the seller ships the item.
- Do not give out personal information including your SSN, driver's license number or other government-provided number associated with your identity.[9]

Non-delivery of Merchandise or Services

Another common form of Internet Fraud is Non-delivery of Merchandise or Services. An example of non-delivery of merchandise is a buyer not receiving an item paid for or receiving an item of far less value than expected. The same non-delivery fraud may occur with offers of services for sale that include those in which providers requestor require payments in advance, such as travel fees or moving costs. When it comes time to utilize the service, a buyer finds their purchase is fraudulent and the service in question may or may not exist, or may not be usable as advertised. A common version of this fraud is the Real-Estate Rental Scam in which potential renters search online for a rental property, and arrange with the presumed owner or rental agency, only to find the rental either does not exist or does exist but is not a rental property.[10] On the other hand, sometimes suppliers do generate services, such as web site design, but are never paid by the recipient. Both consumers and merchants may be victims of non-delivery in online frauds.

Tips on how to decrease risk: Non-delivery of Merchandise or Services

- Research the company or individual you are buying from to make sure they are legitimate and trustworthy.
- Be wary of P.O. Box Numbers. Request the street address and phone number of the individual or business and speak with them directly over the phone or check if the phone number given is legitimate.
- If a seller cannot or will not provide you with a street address or phone number(s), then it may be safer to find another vendor.
- Test to see if the email address provided by the seller is active, and pay close attention to the type of email service they are using. Criminals who employ these fraud techniques often use free Internet services (Gmail, yahoo, hotmail, etc). Pay attention to the services the seller uses, especially where there are credit card transactions.
- Find out as much as you can about the seller. It is reasonable to ask questions about the product and selling history. Try to get the seller on the phone instead of communicating solely through email. It is often helpful to Google the seller, the item being sold, the business, etc. Check out the business with the Better Business Bureau. You may even check the Secretary of State website of the state where the business is located to make sure it is in the state's business/corporation registry.
- Maintain a critical eye with unsolicited offers for money or business opportunities. The old adage is just as true in cyberspace as it is everywhere else; if it sounds too good to be true, then it most likely is too good to be true.
- Remember, when problems occur during international money transactions or item delivery it may be difficult for the company and local law enforcement to track and rectify the problem.
- Make sure to talk to the seller about the condition of the item, when you should receive it, and if they offer a warranty on the item.
- When in doubt, use a credit card to purchase items. In many cases, a credit card holder may successfully dispute fraudulent purchases made from a stolen credit card number.
- If you use a credit or debit card, make sure the website/webpage on which you are entering your information is secure.[11]

Business Opportunity Schemes

The key word in Business Opportunity Schemes is *opportunity*. The prospect of quick and easy money or just an *opportunity* to earn a little extra cash is the lure that draws many victims to these frauds. Work-from-home schemes continue to attract victims into ventures that cost them money rather than making it for them. Some criminals use these "work-from-home" frauds to move stolen money or merchandise purchased with stolen credit cards. As part of the work-from-home duties, the victim may find that their "job" is to repackage and reship merchandise. When the use of the stolen credit card is discovered, and the merchant provides the authorities with the address where the merchandise was delivered, the work-at-home entrepreneur finds that they were receiving and concealing stolen property. At this juncture in the scheme, the individual who sent/received items or money may be charged as a part of a criminal conspiracy for forwarding the merchandise to the person who actually committed the credit card fraud.

Another serious risk posed by this type of fraud is that the con artist may convince the victim that to be eligible for hire they must provide sensitive personal information for a credit check, background check or simply to have their paychecks direct deposited to their bank account. The unwary victim then finds that their prospective employer has compromised their identity.[12]

Tips on how to decrease risk: Business Opportunity Schemes

- Maintain a critical eye with unsolicited offers for money or business opportunities. The old adage is just as true in cyberspace as it is everywhere else; if it sounds too good to be true, then it most likely is too good to be true.
- Research the company or individual you are buying from to make sure they are legitimate and trustworthy.
- Be wary of P.O. Box Numbers. Request the street address and phone number of the individual or business and speak with them directly over the phone or check if the phone number given is legitimate.
- Test to see if the email address provided by the seller is active, and pay close attention to the type of email service they are using. Criminals who employ these fraud techniques often use free Internet services (Gmail, yahoo, hotmail, etc). Pay attention to the services the seller uses, especially where there are credit card transactions.
- If a seller cannot or will not provide you with a street address or phone number(s), then it may be safer to find another vendor.
- Make sure the individual or company you are buying from is the one that holds the correct copyright(s). [13]

Identity Theft

Identity theft happens when someone steals your personal information and uses it without your permission.[14] Identity theft is typically a precursor to an occurrence of identity fraud, that is, the use of someone else's identity to obtain goods or services of which the perpetrator does not have legitimate access. Identity theft and identity fraud are the terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in a way that involves fraud or deception, typically for economic gain.[15] This very serious crime may affect finances, credit score and history as well as negatively influence a victim's reputation. Resolving an identity theft can take time, money, and patience.[16] Once compromised, a victim

may spend years cleaning up their credit history as well as monitoring their credit report for additional occurrences.

Tips on how to decrease risk: Identity Theft

- Make sure to adequately shred all ATM receipts, bank and credit card statements, and credit/debit cards.
- Do not give your credit/debit card information over the phone if you did not make the phone call.
- Educate yourself about the companies (your credit card company or bank) to call if you find your wallet is lost or stolen.
- Make sure to check your credit card and bank statements regularly. Report any fraudulent transactions to credit card company, your bank, file a report with your local police office, and report the incident to the Internet Crime Complaint Center (IC3) at https://www.ic3.gov.
- Consider using a credit monitoring service at will advise you of unauthorized activity on your card(s).
- If you know that your identity was stolen, request a credit bureau indicate that on your credit report.[17]

Credit Card Fraud

Credit Card Fraud committed online is a multi-faceted crime. Initially, criminals use stolen or forged credit card numbers to purchase items from web sites. Upon receipt of payment, the merchant ships the merchandise to the criminal. When an individual discovers their credit card number was stolen and used to make purchases, they may make a "charge-back" to the merchant. If the merchant shipped the merchandise, they are without the merchandise and without payment. The legitimate owner of the credit card must dispute the purchases with the credit card issuer and resolve any resultant credit issues on their credit report. Most credit card companies are good about making the original owner of the credit card whole with little difficulty as long as the owner discovers and reports the incident in a timely manner.

Credit card fraud involves multiple victims: the web merchant, the card-holder, the card issuer and ultimately everyone who does business with the credit card company as losses are often passed on to their customers via higher interest rates. All who are directly affected must spend time and/or money resolving the fraudulent issue.

To get a true appreciation of the potential damage, we must also consider the original crime committed was obtaining or stealing the credit card number. It may have involved pick pocketing, burglary, or hacking into someone's computer. It may have also involved an insider such as a retail clerk copying or "skimming" the information from a card rendered for legitimate payment, or any of a number of other methods by which someone's credit card information may end up in the hands of someone not authorized to have and use it.

Tips on how to decrease risk: Credit Card Fraud

- Do not provide your credit card number on unsecure websites.

- Do not assume all websites are secure, even if the website purports to be secure. Read the fine print on the website's main page to find which security software is in use.
- Buy items from websites or retailers you know to be legitimate.
- Be wary of P.O. Box Numbers. Request the street address and phone number of the individual or business and speak with them directly over the phone or check if the phone number given is legitimate.
- Find out as much as you can about the seller. It is reasonable to ask questions about the product and selling history. Try to get the seller on the phone instead of communicating solely through email. It is often helpful to Google the seller, the item for sale, the business, etc. Check out the business with the Better Business Bureau. You may even check the Secretary of State website of the state where the business is located to make sure it is in the state's business/corporation registry.
- Test to see if the email address provided by the seller is active, and pay close attention to the type of email service they are using. Criminals who employ these fraud techniques often use free Internet services (Gmail, yahoo, hotmail, etc). Pay attention to the services the seller uses, especially where there are credit card transactions.
- If a seller cannot or will not provide you with a street address or phone number(s), then it may be safer to find another vendor.
- Remember, when problems occur during international money transactions or item delivery it may be difficult for the company and local law enforcement to track and rectify the problem.[18]

SPAM/SpIM

SPAM is unsolicited emails sent indiscriminately to multiple parties that include commercial messages. SpIM is unwanted text messages to cell phones or other mobile devices. Both can be intrusive and time consuming.[19] When someone sends a million people an email to try to sell them a worthless product, this is an example of SPAM.[20] SpIM is much like SPAM, and can be a vehicle for viruses and other malware.[21]

Tips on how to decrease risk: SPAM

There is not much an individual can do to avoid receiving SPAM in their email inbox. In effect, SPAM happens, but there are steps you can take to avoid activating the potentially dangerous aspects of SPAM.

- Some commercial email providers will provide their customers with SPAM protection. Check your email settings and make sure that function is turned on. One may also install security software that will block SPAM.
- Do not take seriously unsolicited emails that prompt you to enter identifying information (including your credit or debit card number) or your passwords for any of your online accounts.
- Pay attention when clicking on links provided in emails, especially if they include an unsolicited offer. These links tend to be phishing sites that collect information that may lead to identity theft.

- Ignore emails from unknown individuals that offer you a large sum of money for providing them with a small favor; these messages are scams.
- Do not open emails with attachments from unknown individuals; such attachments are often used to transfer malware or viruses.
- Speak with the Information Technology specialists at your work place and ask them to advise you about how to handle or discard any SPAM you receive in your office email account.
- If you receive a SPAM email, you can report it to the Internet Crime Complaint Center at https://www.ic3.gov.[22] .

Romance Scams

Probably the best way to define a Romance Scam is as a situation in which the fraudster disingenuously pursues a romantic relationship with a target for the purpose of exploiting the resultant emotional connection. By searching dating web sites, blogs, or social media, the scammer will attempt to identify likely victims. They analyze information that may indicate susceptibility (such as being recently divorced or widowed) and availability for a romantic connection. Personal information of the potential victim and information relating to income will be of particular interest; for example, if the potential victim mentions that they are retired or disabled there is the likelihood of a steady source of income from an insurance company or social security. A recently widowed individual might indicate a target that has recently inherited money from a deceased spouse or is receiving the spouse's pension benefits.

The fraudster builds trust through conversations online with the victim, creating a false online persona, which often includes a photo obtained elsewhere on the Internet to further conceal their identity and lure the victim. Building these relationships may take months or even years. Eventually, when the emotional bond is sufficiently established, a series of issues will arise that will require the victim to assist their love interest financially. Initial requests are typically small but as the victim indicates a level of trust and willingness to invest financially in the relationship, the fraudster gradually increases the requests. There are reported cases where the victims have turned over in excess of $500,000.00. In at least one instance in Australia, a 67- year - old widowed grandmother was involved in a Romance Scam spanning more than four years that ultimately cost her close to $90,000.000. Unfortunately, when she finally arranged to meet her online love interest at a villa she rented in Johannesburg, she was never heard from again. Her body was found in the villa and her belongings were eventually tracked to the person authorities identified as the long distance love of her life.[23]

According to the IC3 Internet Crime Report in 2013, there were 6412 reported incidents of Romance Scams that accounted for losses of $81,796,169.00. [24] It is important to keep in mind that since only a fraction of such incidents are reported, there is really no accurate way of determining what portion of all such scams this number represents.

Tips on how to decrease risk: Romance Scams

The best way to avoid falling victim is to learn the common signs of a Romance Scam. The following behaviors may indicate that your online significant other is defrauding you; they may:

- Only communicate with you via your email accounts or instant messaging.
- Tell you they love you very early on in the relationship.
- If the picture they send of themselves looks like they could be a celebrity.
- Says that they are a citizen of the U.S., but they are traveling or living with relatives/friends in another country.
- The person is unable to follow through with any plans to meet you in person, especially if they cannot do so because of a very serious event at home.
- If they ask you to send them money.[25]

Overpayment Fraud

There are many variations of overpayment frauds. These frauds often incorporate the use of fake checks or money orders that the scammer altered in some manner to reflect a higher value than the original purchase amount. Typically, the scammers will offer an explanation as to why the payment must be made in this manner, then request that the recipient deposit the funds into their personal account and return the difference. The scammer depends on a certain lag time for processing before the bank discovers the financial instrument in question is not valid. According to the bank, the responsible party in this scenario is the recipient of the check. The victim finds that not only have they lost the item they supposedly sold but they also have lost the money they forwarded as well as the total amount of the check or money order.[26]

Tips on how to decrease risk: Overpayment Fraud

- Find out as much as you can about the seller. It is reasonable to ask questions about the product and selling history. Try to get the seller on the phone instead of communicating solely through email. It is often helpful to Google the seller, the item for sale, the business, etc. Check out the business with the Better Business Bureau. You may even check the Secretary of State website of the state where the business is located to make sure it is in the state's business/corporation registry.
- Know that it may take a few weeks for a financial institution to discover that a check, even a cashier's check, is counterfeit. If the check is fraudulent, the seller (individual/business) is responsible for the stolen monies.
- A good rule of thumb is to verify each check with the issuing bank, and research any phone number yourself; never rely on the information the buyer provides to you.[27]

Costs and Statistics

According to the *IC3 2013 Internet Crime Report*, 119,457 of the 262,813 reported complaints included some sort of loss involving Internet fraud. This came to a total loss of $781,841,611.00 with an average dollar loss for those reporting of $6,245.00.[28]

JP Morgan's *2014 CyberSource Online Fraud Report* estimates that $3.5 billion was lost to Internet Fraud in 2013. According to its 14th annual survey, "merchants reported losing an average 0.9% of total online revenue to fraud." The report further stated that international orders

are more risky than domestic orders. Merchants reported the annual fraud rate of foreign orders at twice the rate of U.S. orders.[29]

For perspective, the Federal Trade Commission announced in its 2013 annual report that U.S. consumers attributed a reported loss of $1.6 billion to fraud with Identity Theft as the number one fraud type reported.[30]

The Response/Current Efforts

IC3, previously the Internet Fraud Complaint Center, is a partnership between the National White Collar Crime Center (funded by the BJA) and the Federal Bureau of Investigation. IC3's mission is to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime.[31]

In 2014, NW3C and Symantec launched a collaborative website, *Victims of Internet Crimes Empowered* (VOICE) at www.victimvoice.org serves as a comprehensive reference point for victims of Internet crime. VOICE offers victims information regarding how they may seek help; educate themselves, their families and communities about Internet crime; and steps they may take to protect themselves from Internet crime. [32]

Fraud.org, a project of the National Consumers League, also allows users to file a complaint online. FTC Commissioner Maureen K. Ohlhausen states, "Fraud.org is an important partner in the FTC's fight to protect consumers from being victimized by fraud." This site teaches users about frauds such as telemarketing fraud, Internet fraud, identity theft, and business fraud.[33] Fraud.org's mission is to give consumers the information they need to avoid becoming victims of telemarketing and Internet fraud. More than 100,000 unique visitors come to Fraud.org every month. Through their anti-fraud advocacy, consumer education efforts, and direct consumer counseling, Fraud.org has helped millions of consumers protect themselves against malicious scams.[34]

"For More Information"/Links

Federal Consumer Information Center – http://www.pueblo.gsa.gov/scamsdesc.htm

Federal Trade Commission - http://www.ftc.gov

Internet Crime complaint Center – http://www.ic3.gov

National Crime Prevention Council - http://www.ncpc.org/

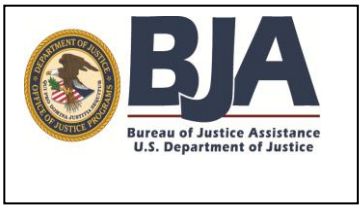
National Consumer League – http://www.fraud.org

Symantec - http://securityresponse.symantec.com/avcenter/hoax.html

United States Department of Justice – http://www.usdoj.gov/criminal/fraud/

United States Department of Justice Office of the Attorney General - http://www.justice.gov/ag/

Voice - https://www.victimvoice.org/



Maintenance and revisions: NW3C Research Section

This project was supported by Grant No. 2012-MU-BX-4004 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

[1] Friedman, Thomas L. *The Lexus and the Olive Tree*. New York: Farrar, Straus, Giroux, 1999. Print.
[2] IC3 Mission Statement, located at http://www.ic3.gov/about/default.aspx retrieved June 13, 2014
[3] Internet Crime Complaint Center. Internet Crime Schemes: Auction Fraud, retrieved June 12, 2014 from http://www.ic3.gov/crimeschemes.aspx
[4] Online Auction Sites Review 2013. (2013). 2013 Online Auction Sites Comparisons. Retrieved on March 13, 2013 from http://online-auction-sites.toptenreviews.com/.
[5] DoIT Division of Information Technology. (August 30, 2012). Triangulation, the latest eBay auction fraud. Retrieved on March 13, 2013 from http://www.doit.wisc.edu/news/story.aspx?filename=1770.
[6] NCPC. Online Auction Fraud. Retrieved on March 18, 2013 from http://www.ncpc.org/cms-upload/ncpc/File/aucfraud.pdf.
[7] NW3C. "Vehicle Theft: Online Salvage and VIN Cloning." National White Collar Crime Center Specialty Training. 2013. Lecture.

[8] NW3C. "Vehicle Theft: Online Salvage and VIN Cloning." National White Collar Crime Center Specialty Training. 2013. Lecture.
[9] Internet Fraud." *FBI*. FBI, 17 Mar. 2010. Web. 1 Oct. 2014. http://www.fbi.gov/scams-safety/fraud/internet_fraud.
[10] IC3. (2013). 2013 Internet Crime Report. Retrieved on September 3, 2014 from http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf
[11]"Internet Fraud." *FBI*. FBI, 17 Mar. 2010. Web. 2 Oct. 2014. http://www.fbi.gov/scams-safety/fraud/internet_fraud.
[12] IC3. (2013). 2013 Internet Crime Report. Retrieved on September 3, 2014 from http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf
[13]"Internet Fraud." *FBI*. FBI, 17 Mar. 2010. Web. 2 Oct. 2014. http://www.fbi.gov/scams-safety/fraud/internet_fraud.
[14] Federal Trade Commission, definition of Identity Theft: retrieved June 12, 2014from http://www.consumer.ftc.gov/features/feature-0014-identity-theft
[15] U.S. Justice Department, definitions of identity theft and identity fraud, retrieved June 10,2014 from http://www.justice.gov/criminal/fraud/websites/idtheft.html
[16] Federal Trade Commission. Identity Theft. Retrieved on June 12, 2014 from http://www.consumer.ftc.gov/features/feature-0014-identity-theft
[17]"Common Fraud Schemes" *FBI*. FBI, 17 Mar. 2010. Mon. 6 Oct. 2014. http://www.fbi.gov/scams-safety/fraud/fraud#id.
[18] [18] Internet Fraud." *FBI*. FBI, 17 Mar. 2010. Mon. 6 Oct. 2014. http://www.fbi.gov/scams-safety/fraud/internet_fraud/internet_fraud#ccf.
[19] Federal Communications Commission. (May 18, 2011). Spam: Unwanted Text Messages and Email. Retrieved on March 20, 2013 from http://www.fcc.gov/guides/spam-unwanted-text-messages-and-email.
[20] Definition of Spam retrieved June 12, 2014 from http://www.yourdictionary.com/spam
[21] Definition of spIM. Retrieved June 10,2014 from http://www.yourdictionary.com/spim-or-spim
[22] "Spam Free." *SpamFree Free Email Spam Resources and Info RSS*. Web. 6 Oct. 2014. http://www.spamfree.org/dangerous-email/.
[23] Police Probe African Death of Scam Victim, March 4, 2013, 9news Australia, retrieved June 13, 2014 from http://news.ninemsn.com.au/national/2013/03/04/13/02/police-probe-african-death-of-scam-victim?mch=mobilenh&mchpost=pos2
[24] Annual report of the Internet Crime complaint Center 2013, located at http://www.nw3c.org/docs/IC3-Annual-Reports/2013-ic3-internet-crime-report.pdf?sfvrsn=4
[25] Foxworth, Darrell. "Looking for Love? Beware of Online Dating Scams." *FBI*. FBI, 14 Feb. 2013. Web. 6 Oct. 2014. http://www.fbi.gov/sandiego/press-releases/2013/looking-for-love-beware-of-online-dating-scams.
[26] Federal Trade Commission. (Dec. 2012). Fake Checks. Retrieved on April 8, 2013 from http://www.consumer.ftc.gov/articles/0159-fake-checks
[27] "BBB Business Tips to Avoid Overpayment Scams." *BBB Business Tips to Avoid Overpayment Scams*. 14 July 2014. Web. 7 Oct. 2014. http://www.bbb.org/east-texas/news-events/news-releases/2014/07/bbb-business-tips-to-avoid-overpayment-scams/.
[28] Annual report of the Internet Crime complaint Center 2013, located at http://www.nw3c.org/docs/IC3-Annual-Reports/2013-ic3-internet-crime-report.pdf?sfvrsn=4
[29] JP Morgan CyberSource 14th Annual Online Fraud Report retrieved June 12, 2014 from http://forms.cybersource.com/content/fraudreportus2013-ty
[30] Federal Trade Commission. (Feb. 2014) FTC Announces Top National Consumer Complaints for 2013. Retrieved on September 5, 2014 from http://www.ftc.gov/news-events/press-releases/2014/02/ftc-announces-top-national-consumer-complaints-2013
[31] IC3 Mission Statement, located at http://www.ic3.gov/about/default.aspx retrieved June 13, 2014
[32] Victims of Internet Crimes Empowered. (Apr. 2014). If you have been a victim of cybercrime, you have a voice. Retrieved September 3, 2014 from https://www.victimvoice.org/.
[33] Fraud.org. Home page. Retrieved on June 13, 2014 from http://www.fraud.org/.
[34] Fraud.org. About Fraud.org. Retrieved on April 29, 2013 from http://www.fraud.org/about-fraudorg