

# Cyber Scam Artists: A New Kind of .con

Robert Fried

# Cyber Scam Artists: A New Kind of .con

**By Robert B. Fried, BS, MS**

## Abstract

Scam Artists have been around for centuries. Time progressed and technological innovations emerged and so have a new breed of con artist; the online fraudster. Utilizing various aspects and tools of the Internet, the online fraudster has become more successful then ever in defrauding a large target audience. So successful, that the issue has been the subject of much concern in recent years. Although, much is being done on multiple levels of government and within the public and private sectors, online fraud is still continuing to thrive. As long as the fraudster is motivated by greed and able to deceive others, fraud will always be in existence.

This paper will closely examine the emergence of the fraudster into cyberspace. It will discuss what tactics and methods the online fraudster utilizes in his/her attempts to successfully deceive others. Furthermore, it will provide a profile of those individuals who are victimized by such fraudsters. Moreover, it will analyze the steps being taken to help deal with the issue of online fraud. Lastly, several conclusions will be drawn regarding Internet fraud.

## The Venture Into Cyberspace

Imagine a medium in which information or ideas can be disseminated to a large audience of individuals in a relatively short period of time. If you haven't been living under a rock in recent years, you would know that such a thought is in fact reality. The Internet, once used mainly by academic institutions and governmental agencies, has now found its way into the commercial and private sectors of countries around the globe.

The number of 'netizens' increases greatly with the passing of each day. As the population of people on the Internet continually grows, so do the potential threats and vulnerabilities associated with it. The Internet can provide a wealth of information. However, it can also be viewed as a breeding ground for fraud.

What is Internet Fraud? The Federal Bureau of Investigation defines Internet fraud as "any fraudulent scheme in which one or more components of the Internet, such as Web sites, chat rooms and e-mail, play a significant role in offering nonexistent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transferring victim's funds, access devices or other items of value to the control of the scheme's perpetrator" [1].

Just think, the Internet has made things so much easier for the fraudster. No longer is there a need to rent office space, hire employees and spend countless hours on a

telephone pitching to targeted audiences. Time and funding have been reduced significantly. As a result, the Internet looks extremely attractive. Furthermore, with the usefulness, popularity and global reach of the Internet continuously growing, it doesn't take much to try and understand why fraudsters are venturing off into cyberspace.

# Fraudsters: Who Are They? / What is Their Motive?

So, who are these online fraudsters? According to Dr. Fred Cohen, a recognized leader in the area of computer viruses and information protection and security, fraudsters are characterized as individuals "who defraud others". Fraudsters have been around for centuries. Cohen asserts "throughout the centuries, people have perpetrated frauds of all sorts in order to gain through taking advantage of others" [2].

Virtual scam-artists are similar to the traditional scam artists encountered in the real world. Their fundamental motive is greed. However, there is one distinct difference; they utilize a completely different medium/environment in their mission to ultimately accomplish their goal of successfully deceiving others.

The typical traditional fraudster starts his/her venture off in a similar manner to that of a business entrepreneur. In regards to financing his/her operation, a relatively small amount of money is required. It is believed that funds in the range of one hundred to one thousand dollars are needed to allow the operation to get up and running. As little as one individual to as many as twenty can staff a typical operation. Some operations can be small and generally done on one's spare time, while others may involve full time work and as much as office space. No matter how sophisticated the operation may be, each fraudster must rely on his/her ability and motivation to find the weaknesses of their target audiences and exploit them out of greed [3].

During the months of May 2000 through November 2000 the Internet Fraud Complaint Center (IFCC) conducted an extensive study. The IFCC is a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI) to help address the issue of fraud committed through the Internet. In this survey, the IFCC was able to compile data, which allowed a general profile of a typical online fraudster to be made [4]. According to the survey, the data suggests that individuals who are involved in fraudulent activities via the Internet are generally, individuals and not businesses. Furthermore, these individuals are predominantly males residing in largely populated states. The data also suggests that these individuals have diversified international backgrounds with representation in the United States, Eastern Europe and Canada [4].

In a recent article relating to the emergence of Internet fraud stemming from the recent terrorist attacks on the World Trade Center and the Pentagon (fake donation funds, etc.), an official at Britain's National Criminal Intelligence Service (NCIS) stated "fraudsters typically exploit human misery, so they invariably create human misery. They are without scruples because this is how they make money. It is very grubby money" [5].

There is a saying: "another day, another dollar". If there is a dollar to be made, the fraudster will do what it takes to make it.

# Fraud Exists in Various Corners of Cyberspace

The Internet has allowed for people thousands of miles away to communicate with one another in real time. The most dominant forms of communication over the Internet are web sites. Other aspects of the Internet including electronic mail, newsgroups, usenet, "chat" rooms, Internet relay chats, list serves and bulletin boards also serve as major mediums of communication.

A fraudster can create and maintain web sites with the ultimate goal of trying to defraud others. Depending on the skill of the fraudster or those working for him/her, a web site can be made to look very attractive and legitimate. If the web site appeals to the web surfer's eye, he/she may be inclined to see read/click on. Many times, the information on the web site can be so appealing that the web user forgets to think about the legitimacy of the site. In a sense, the information on the web site, along with its look, help to "pull the web surfer in".

Electronic mail is of great use to online fraudsters. In literally a few minutes, an online fraudster can create a personalized email and send it to thousands of individuals in his/her target audience. Using e-mail to accomplish such a task is known as "spamming" [6]. The fraudster knows that many people will simply delete the e-mail once it arrives. However, it is also likely that many will be made curious by the 'subject heading' of the e-mail message, and therefore click the message to read on. Of the people who do open the message, a small percentage just may fall into the fraudster's trap.

Bulletin boards have also proven useful to online fraudsters. Bulletin boards are typically the location where many individuals exchange information with one another. Many online fraudsters utilize message boards to offer "unbelievable" opportunities or "get rich quick" schemes to subscribers/browsers of such boards. Fraudsters, who target securities investors for example, utilize the message boards to pass on bogus "inside" information on certain stocks or corporations. Many fraudsters prefer this medium because it adds the benefit of them being able to easily hide their true identities with the use of aliases. Using multiple aliases, a fraudster can make it seem as though many people share the same opinions or have the same "inside" information that the fraudster does [6].

# Types of Online Scams Used by Fraudsters: Auctions

According to a study released in May 2001 by the Internet Fraud Complaint Center (IFCC), Internet auction fraud makes up a majority (64%) of all online fraud [7]. Internet auction houses have become extremely popular in recent years. An online auction is very similar to a real life auction. The only differences in an online auction are that the auction has a global reach and that there is no need to have an auction house with limited seating.

On the Internet, it is quite possible to have multiple bidders and millions of potential bidders for a specific item. It's a great concept; however, there are multiple reasons, why Internet auction fraud is the number one type of online fraud to be reported.

According to the IFCC's May 2001 study "Internet auction fraud involves "non-delivery, misrepresentation, triangulation fee stacking, black market goods, multiple bidding and shill bidding" [7]. In regards to "non-delivery", this type of fraud involves having an auction on an item that in reality does not exist. 'Misrepresentation' results when the seller deceives the potential buyers. Essentially the seller lists false values and conditions for the items up for bid. 'Triangulation' involves the buying of an item (by the perpetrator) using fake identities and payment information to a bidder at an online auction web site. The winning bidder and online merchant are later questioned as to how they came across the stolen merchandise. In regards to 'Fee stacking', this type of fraud involves the tacking on of extra fees by the seller after the auction closes. 'Black-market goods' are another type of Internet auction fraud. 'Black market goods' are generally goods that are shipped to the winning bidder without a box, instructions or manufacturer's warranty. 'Multiple bidding' occurs when the buyer places multiple bids for the same item using different aliases. Once the other potential bidders have lost interest and the auction is coming to a close, the high bids are withdrawn and the item is won at a lower bid. In regards to 'shill bidding' the seller, using different aliases/or with the help of associates, bids on the item, which results in driving the price of the item [7].

It is estimated that in the year 2000, auction customers lost $4 million. For the calendar 2000 calendar year 30,000 complaints were received. The IFCC has estimated that over 1.3 million transactions take place daily on online auction sites. Obviously many victims fail to report that they have been victimized by online auction fraud. This failure may be attributed to lack of knowledge as to the actual gender, address, or location of the perpetrator [7].

# Types of Online Scams Used by Fraudsters: Investment Fraud

Online investment fraud is a type of Internet fraud, which is becoming all too common. Many brokerage houses/firms are providing clientele with great incentives to manage their accounts online. Furthermore, a countless number of websites have popped up within recent years that offer financial advice. Although a majority of these websites offer reliable news and advice on specific stocks and corporations, the web user should be weary.

In a recent study conducted by ABCNews.com, it was found that seven million Americans used the Internet to trade investments. This figure suggests that approximately twenty five percent of all investment trades made by individual investors take place online [8]. That number is astounding. It is no wonder why many fraudsters prey on those individuals who manager their investment portfolios via the Internet.

There are several different tactics that the fraudster can employ when attempting to commit investment fraud. Typically fraudsters generate and distribute online newsletters. Such newsletters, which are commonly found on web sites, bulletin boards or via e-mail, often carry no subscription fee and offer the online investor 'valuable' information about specific stocks/corporations. Many of these online newsletters are in fact legitimate. It is known that many corporations legally pay individuals to create and distribute newsletters promoting their companies. They newsletters are legitimate as long as the company files that such a newsletter has been made, who created it, how much they were paid, and to whom it was distributed.

At any given time there may be hundreds of thousands of newsletters of the sort floating around cyberspace. However, it is often difficult for the average web surfer/individual online investor to determine the legitimacy of the information provided in the newsletters. If the fraudster spends a little time and effort in developing the newsletter and making it appealing to the human eye, he may just be successful in deceiving some of those in his targeted audience. Based on the information they obtain from such newsletters, many individual investors may chose to either buy or sell a particular stock featured in the newsletter. It doesn't take a genius to realize that a fraudster can profit considerably from either investing or selling the stocks he/she features in his/her newsletters [9].

Many fraudsters are also turning to message boards to disseminate financial information. Many websites feature message boards, company information and real time quotes on companies trading on the NYSE or NASDQ stock market exchanges. The most popular website of this sort is Yahoo! Financial. To gain access to such information it only takes the few keystrokes necessary to enter in the URL of the web site into the web browser. Information is then at your fingertips. One can easily view all the information about a particular corporation or its stock history. The web surfer can view anything from the latest real time quotes, company news, and press releases to even the most recent trades made by top executives in that specific corporation. If one wants to be able to post any information on the message board of a particular stock a simple registration process needs to be completed. No information needs to be verified to obtain the user ID and password necessary to gain full access to the boards. A few simple questions and a fraudster can be just moments away from posting a message to his/her targeted audience. If the fraudster wants to make even more of a statement about a particular stock or corporation he/she intends to focus on, it only takes a few more minutes of his/her time to generate more accounts/aliases.

Fraudsters interested in committing investment fraud via the Internet are finding their way into live 'chat' rooms. It is here where fraudsters can engage in real-time conversations with individuals who are interested in investing. Through the use of such 'chat' rooms, fraudsters can easily disseminate information to those individuals in the chat room he/she intends to deceive. 'Chat' rooms can be a great tool for the online fraudster. Not only can he/she engage in real-time conversation with his/her target audience, he/she can also hide his/her identity through the use of aliases as well.

There are several categories of Internet Investment fraud. One of the common is known as the “pump and dump” scam. In such a scam, the fraudster creates in his/her intended target’s mind the need to either buy or sell a stock immediately. Usually the fraudster creates newsletters or posts on message boards claiming knowledge of inside information on a particular stock. In reality, this is just a neat little game the fraudsters play to reel their victims in. The fraudsters who typically own shares of stock in this company want others who are gullible to buy the stock. In a sense, by promoting a stock, the fraudster is engaged in the “pumping” aspect of the scheme. Once the stock price has increased, the fraudster will then decide to sell or “dump” the stock. As a result, the gullible investors lose money, while the clever fraudster may profit enormously from the scheme. The fraudster may also employee this type of scheme if he/she wants to merely affect a corporation’s stock price out of spite [9]. “Fraudsters frequently use this ploy with small, thinly-traded companies because it’s easy to manipulate a stock when there’s little or no information available about the company” [9].

Some of the less common schemes employed by fraudsters targeting online investors are those that fall into the following categories: the pyramid, “risk free” fraud and off shore frauds. The pyramid is a commonly used tactic and will be discussed later in great detail in the next section. Risk free fraud involves investment opportunities associated with selling too good to be true investments. Usually, such deals are offered via the Internet and it doesn’t take much money or effort for the individual investor (the fraudster’s gullible target) to become involved. It is not uncommon for the investment and so called “unbelievable opportunity” to be non-existent. With regards to offshore fraud, this type of fraud, involves investments in overseas countries or markets. With the use of the Internet previous barriers, which prevented many from becoming involved in such investments, have been eliminated. However, these investments are particularly risky because they are ventures into areas outside the United States and they become difficult to investigate if the investor suspects fraud [9].

# Types of Online Scams Used by Fraudsters: Others

Online fraudsters have many ways of using the Internet to put their plan to deceive others into action. We have seen how the various aspects of the Internet are used. Now, we will examine just how these online "tools" help the fraudster accomplish his/her goals.

According to the Federal Trade Commission (FTC) and the National Fraud Information Center (NFIC), ‘pyramid schemes’ are gaining tremendous popularity amongst fraudsters [10]. Essentially, a pyramid scheme is "a fraudulent system of making money which requires an endless stream of recruiters for success. Recruits (a) give money to the recruiters and (b) enlist fresh recruits to give them money" [11]. One may think that such a system is legal. However, the opposite is true. In fact, "the result of such a scheme is inevitable: at best a few people walk away with a lot of money, while most recruits lose whatever money they put into the scheme. The only way anybody can make money through a pyramid scheme is if people are defrauded into giving money upon a promise of getting something in return when it is impossible for them to get anything at

all in return. That is to say, in plain English, schemes such as these 'always' constitute fraud" [11].

Online fraud can encompass a wide range of categories. According to Internet Fraud Watch statistics compiled for the year 2000, the top 10 forms of Internet Fraud are: online auctions (78%), general merchandise sales (10%), Internet Access Services (3%), Work-At-Home (3%), Advance Fee Loans (2%), Computer Equipment/Software (1%), Nigerian Money Orders (1%), Information Adult Services (1%), Credit Card Offers (0.5%) and Travel/Vacations (0.5%) [12].

# A Profile of the Victims

The results of a 'Six Month Data Trends Report', conducted in the year 2000, by the IFCC, allowed for a profile of a typical online fraud complainant. The results of the report concluded that the typical complainant was generally an individual who is male and between the ages of 30 and 50. It was found that a majority of the complainants reside in the United States, Canada and the United Kingdom. The results of the report show that a majority of the complainants from the United States reside in California, Washington, Florida and New York [4].

Although, the IFCC's report helps to profile victims of online fraud, the report is only somewhat accurate. The report focuses primarily on individual complaints and not those of businesses. Furthermore, the data that was collected only allows for analysis on victims who have actually filed complaints with the IFCC. Unfortunately, many victims do not contact law enforcement or file complaints with the proper authorities. Internet Fraud often goes unreported because victims are either embarrassed or simply unaware of how to properly file a complaint [4].

# Steps Being Taken

Internet fraud has become a very serious issue. Due to public concern the United States government has begun to take action on dealing with the matter. Much in the way of research and investigations is being done on the issue. Governmental agencies are even beginning to address the subject.

The IFCC is one example of how the US government is trying to do its part. The IFCC, as stated previously, is a partnership that exists between both the FBI and NW3C. Its mission is "to develop a national strategic plan to address fraud over the Internet and to provide support to law enforcement and regulatory agencies at all levels of government for fraud that occurs over the Internet" [1].

There has also been a joined effort by the FBI, NW3C, the United States Postal Service (USPS) and the Securities and Exchange Commission (SEC) to combat Internet fraud. In May 2001, 'Operation Cyber Loss' was initiated. During one of its operations, the FBI was able to capture and arrest 90 suspected online fraudsters. Although the

operation reflects a small number of online crimes committed, it is an effort by governmental agencies to show that the matter is not being overlooked [13].

Recently, the Federal Trade Commission had announced that they have compiled a database that it believes is helpful in combating Internet fraud. The database is cleverly named 'ConsumerSentinal'. "While it gives no information about live investigations, 'ConsumerSentinal' does take in information from those who have been victimized by alleged Internet abusers. All anyone needs to do to report a potential abuser is to click the site's complaint button. The also site offers consumers easy to find online information on the top cyberscams" [14]. The database is available to each law enforcement agency in the country. Such a tool is extremely valuable. However, how will the complainant actually know whether his/her claim has been addressed? [14].

With the rise in online investment fraud, the SEC has taken some measures to deal with the matter. The SEC has been actively taking complaints from investors who feel they have been victimized by online fraudsters. The have been doing their part by attempting to take quick action to investigate the matter and find out who is responsible for committing securities fraud. Furthermore, the SEC has been working closely with all federal, state and criminal authorities [9]. To help online investors become more educated about online investment fraud, the SEC and others in the financial industry offer the following advice: "never invest based solely on bulletin board postings or an online newsletter, look for key phrases, take your time on proposed opportunities, research the company you are dealing with or are interested investing in, consult a trusted third party, don't submit financial information online, be wary of international opportunities, if you have a complaint you should act promptly" [8].

Along with the many US governmental agencies, the United States Congress is also actively playing its part. Recently, it has held hearings on the future of Internet commerce. These hearings address Internet commerce safety issues. Furthermore, members of the House telecommunications subcommittee have held hearings to address how the nation is going to go about boosting consumer confidence levels while shopping for goods online. Many individuals believe that the e-commerce and such will grow steadily into the future. Members of Congress are trying to do what they can at this point to help the technology sector grow. Like anything, obstacles will be met along the way, and matters such as Internet fraud are just one of the many that need to be dealt with [13].

# Summary, Conclusions, and Further Work

The virtual cyber scammer is really no different then the traditional scam artist of the real world. However, the online scam artist has many advantages over the traditional scam artist. The online scam artist can target a tremendously large audience without ever having to come into physical contact with those he/she plans to deceive. Furthermore, the online scam artist doesn't need much time, effort or money to reach his/her intended audience. It may take only fifteen minutes or so for the online fraudster to compose and send a customized email message to thousands of people. It would take months if not

more, for the traditional scam artist to accomplish such a task. This is just one reason why many fraudsters are making their way into cyberspace.

Not only is it easy for cyber scammers to deceive others online. It is also easy for them to cover their tracks. With the use of aliases and such they can hide their identity and location. Furthermore, because the perpetrator and victim may be a far distance from one another, multiple jurisdictions may be involved; this makes the situation more difficult to deal with. Moreover, with a majority of victims neglecting to file complaints, making it less likely for the fraudster to get caught; why would anyone want to pick another profession?

Recently, many US governmental agencies have begun to catch on to the many forms of cyber scamming occurring via the Internet. They have begun to take active steps in helping catch those individuals who have or have attempted to defraud others online. In fact, many governmental agencies have even begun to form partnerships with one another. These partnerships have even in resulted in the creation of centralized locations that help take victim's complaints.

Although there seems like a lot of progress has been made in attempting to combat Internet fraud, more has to be done. Internet fraud exists now, and it will continue to thrive well into the future. There will always be those who because of greed, want to defraud others. It is a known fact that fraudsters have been around since the beginning of mankind. There will always be those who will, through human nature, fall victim to fraudsters. Therefore, the issue can never be resolved it can only be addressed. The best way to address the issue is by informing and educating others on the issue. Through education comes knowledge. From knowledge comes understanding. If one understands then one is more likely to think before they ultimately click!

# References


**[1]. About the Internet Fraud Complaint Center**

http://www.fbi.gov/hq/cid/fc/ifcc/about/about_ifcc.htm

**[2]. Threat Profiles: Fraudsters**

**All.net Security Database: Threat 7**

**[3]. Profile: Fraudsters**

**University of New Haven CJ 625 Course CD: Slide 32**

**[4]. IFCC: Six Month Data Trends Report (May-November 2000)**

**[5]. Matusic, Karen. "Beware of Internet Appeals". Reuters Limited: September 19, 2001**

http://www.cbsnews.com/now/story/0,1597,311791-412,00.shtml

**[6]. Cyberguards: Internet Fraud: Need Assistance?**

http://www.cyberguards.com/fraud.html

**[7]. IFCC: Internet Auction Fraud: May 2001**

http://www.ifccfbi.gov/strategy/AuctionFraudReport.pdf

**[8]. Raphael, Rebecca. "Online Investment Scams". ABCNews.com: July 7, 2000**.

http://abcnews.go.com/onair/2020/2020_000707_onlineinvesting_feature.html

**[9]. Internet Fraud: How to Avoid Internet Investment Scams**

http://www.sec.gov/investor/pubs/cyberfraud.htm

**[10]. Cahlin, Michael. "Avoiding Online Scams". Smart Computing: March 1997**

http://www.smartcomputing.com/editorial/article.asp?article=articles%2F1997%2Fmar97%2F97n0333%2F97n0333%2Easp

**[11]. Carroll, Robert Todd. "The Skeptics Dictionary" "Pyramid Schemes, Chain Letters and Ponzi Schemes".**

http://skepdic.com/pyramid.html

**[12]. Internet Fraud Watch: 2000 Internet Fraud Statistics**

http://www.fraud.org

**[13]. Carlson, Caron. "Cyber Cops Nab 90 Fraudulent Suspects." e-Week: May 24, 2001**

http://www.zdnet.com/eweek/stories/general/0,11011,2764859,00.html

**[14]. Radcliff, Deborah. "FTC Tracks Spammers and Fraudsters." Computerword: Feburary 14, 2001**

http://www.computerworld.com/cwi/story/0,1199,NAV65-663_STO57716,00.html

**Cyber Criminals Most Wanted: The First One-Stop Cybercrime Prevention Website**

http://www.ccmostwanted.com/

# About the Author

Robert Fried holds a B.S. and an M.S. in Forensic Science with a concentration in Advanced Investigation. He also holds Certificates in Law Enforcement Science, Forensic Computer Investigation, and Information Protection and Security from the University of New Haven and SEARCH. Fried has extensive knowledge of forensic science, however, most recently he has worked extensively in the developing field of "digital forensics" and has published in this area by organizations such as the SANS Institute. He is also a member of the NorthEast chapter of the High Technology Crime Investigation Association (HTCIA).