▲ Up ◀ Prev ▶ Next

The "Social Engineering" of Internet Fraud

Jonathan J. RUSCH <rusch1@erols.com>
United States Department of Justice
USA

Abstract

Many online media have recently been focusing on the topic of Internet fraud. Business leaders, computer security experts, and lawyers, however, do not fully understand the kinds of frauds that can be conducted through or with the aid of the Internet, or the ramifications of such frauds for the future of e-commerce. This paper has three principal goals. First, it will identify the principal types of Internet frauds that law enforcement and regulatory authorities are observing. Second, it will explain the major psychological influence techniques that criminals use in conducting such frauds (including the similarities between those techniques and "social engineering" techniques of hackers). Third, it will propose some responses to the problem involving both government and the private sector.

The paper will begin by presenting a typology of the major forms of Internet fraud, referring not only to the type of crime each form involves but also to the nature of the deception -- whether deception of computer systems (e.g., packet sniffing and data harvesting) or of individuals (e.g., securities and other investment schemes) -- and the manner in which the criminal can obtain the victim's funds. It will then explore the principal psychological features of Internet fraud, particularly the commonalities between various types of fraud, through both the academic literature of social psychology and real-world examples. It will explore the attitudes and beliefs of criminal and victim about each other and about the medium of the Internet, to clarify the broader context in which fraud can occur. It will also discuss the principal social psychological influences that the criminal brings to bear on the victim (i.e., authority, commitment and consistency, liking and similarity, reciprocity, scarcity, and social proof), and why those influences operate so powerfully to persuade the victim to part with something of value. It will also note the typical types of hardware and software that are meant to provide online consumers with "security," while noting those aspects of online behavior that limit the effectiveness of those measures. Finally, it will propose new methods for addressing the psychology of online fraud in prevention and education methods as well as government enforcement measures, as part of a comprehensive approach to increasing consumer confidence in e-commerce. This paper is likely to make two significant contributions to INET'99. First, it will expose business leaders, security professionals, policy makers, and lawyers to an aspect of e-commerce and to relevant bodies of knowledge and experience with which they are certain to be unfamiliar. Second, it can help industry professionals to understand the limitations of hardware and software in providing a truly secure environment for e-commerce, and to begin to think with greater clarity and precision about what else can be done to develop truly comprehensive means of fostering that environment.

Contents

- I. Introduction
- II. Psychological influences in Internet fraud
  - A. Principles of social psychology
    - 1. Alternative routes to persuasion
    - 2. Attitudes and beliefs

        - 3. Persuasion and influence techniques
    - B. Application to Internet-fraud schemes
        - 1. E-mail and Web site scams
        - 2. Online auctions
        - 3. Securities and other investment schemes
- III. "Reverse-engineering" Internet fraud
- References
- Disclaimer

I. Introduction

Internet fraud is a form of white-collar crime whose growth may be as rapid and diverse as the growth of the Internet itself. (For our purposes, the term "Internet fraud" may be broadly defined as any fraud committed through or with the aid of computer programming or Internet-related communications such as Web sites, e-mail, and chat rooms.) According to the consumer organization Internet Fraud Watch, the number of consumer complaints it receives about Internet fraud schemes has risen dramatically in the past two years, from 1,152 in 1997 to more than 7,500 in 1998. [1] The U.S. Securities and Exchange Commission, which regulates securities markets within the United States, reports that it receives as many as 300 complaints per day from investors about alleged Internet fraud. [2] Moreover, the types of Internet fraud schemes that law enforcement authorities are identifying extend well beyond securities-based transactions to many other situations, such as spurious investment and business opportunities, online auctions, sales of computer- and Internet-related products and services, and credit card issuing. [1]

It is also apparent that the growth of Internet fraud to date is outpacing our understanding of the problem. We do not yet have reliable data concerning the full extent of the problem, either within the United States or the world at large. [2] We also have no systematic studies of the dynamics of fraud on the Internet -- that is, studies that would identify and explore the techniques that criminals use in persuading people to send checks, credit card numbers, or other valuable data for whatever the criminal purports to offer over the Internet. Such studies could help the law enforcement and computer security communities in addressing the problem of Internet fraud. They could also inform industry, consumer organizations, and government in devising prevention and education programs on Internet fraud, so that consumers can recognize and respond appropriately to potentially fraudulent overtures on the Net.

No single academic discipline or methodology is likely to yield all the answers we would seek from this kind of study. From my own experience in prosecuting major frauds such as telemarketing fraud, however, I believe that one phenomenon in Internet culture offers a promising line of inquiry. That phenomenon is "social engineering." "Social engineering" can be defined generally as the process by which a hacker deceives others into disclosing valuable data that will benefit the hacker in some way. [3, 4] Although hackers originally used "social engineering" to obtain codes or e-mail passwords for access to long-distance telephone lines or computers [5, 6, 7], more recent reports indicate that "social engineering" attacks can now be, and are being, used to acquire credit card numbers and other financial data:

- Last fall, for example, some CompuServe subscribers, who had just set up trial accounts with CompuServe after providing credit card or bank account information, were contacted a few days later by e-mail. The e-mail, which purported to be from a CompuServe account manager, stated that there were unspecified "problems with your account" and asked the subscriber to resubmit his log-on password and bank or credit card data. What was noteworthy about this attempt was the fact that it was directed only at new subscribers, who would be less likely to know that they should not respond to the e-mail. [8]
- Another situation involved Yahoo e-mail users who reportedly received e-mails from a person who falsely identified himself as a Yahoo employee. The "employee" told each recipient that

he had won a 56K modem from Yahoo, but that he would have to supply his name, address, telephone number, and credit card number to pay for shipping. A number of recipients did so before Yahoo learned of the false e-mail and contacted everyone who had responded to it. [9]

- More recently, law enforcement has received reports that people have received e-mails offering them the opportunity to participate in the Net equivalent of a chain letter, chain e-mail. After promising the recipient overwhelmingly large financial returns if the recipient sends only a small amount of money to another person on a list within the e-mail, the sender tells the recipient to place his or her name, address, and bank account information at the bottom of the list and to send it to a designated location.

Hackers and computer security professionals alike recognize that "social engineering," in effect, involves the same techniques as criminals carrying out a traditional fraud. [5, 10] Some of them have also acknowledged that the success of "social engineering" stems from the application of psychological techniques for interacting with and manipulating the victim to obtain the desired information. [11, 12, 13] This strongly suggests that we should look to social psychology -- "the scientific study of how people think about, influence, and relate to one another" [14] -- as one discipline that is peculiarly well-equipped to help us explore the "social engineering" of Internet fraud.

A paper as brief as this cannot hope to conduct that exploration in full, although it stems from a larger research effort in which I am now engaged. At most, it can offer only an "armchair tour," with social psychology as a guide, of the principal areas warranting that exploration. It will examine some of the more prevalent forms of Internet fraud in the light of social psychology, and note which psychological factors appear to be most influential in facilitating those forms of fraud. It will conclude by suggesting possible means of "reverse-engineering" Internet fraud -- that is, seeing what measures could be developed, based on the insights we gain through social psychology, that might hamper or reduce the incidence of certain Internet frauds.

II. Psychological influences in Internet fraud

A. Principles of social psychology

Three aspects of social psychology, especially the psychology of persuasion, are most useful for our purposes: alternative routes to persuasion, attitudes and beliefs that affect social interaction, and techniques for persuasion and influence.

1. Alternative routes to persuasion

In any situation where one person seeks to persuade another to do something, social psychology has identified two alternative routes that the persuader can employ. A *central route to persuasion* marshals systemic and logical arguments to stimulate a favorable response, prompting the listener or reader to think deeply and reach agreement. A *peripheral route to persuasion*, in contrast, relies on peripheral cues and mental shortcuts to bypass logical argument and counterargument and seek to trigger acceptance without thinking deeply about the matter. [14, 15] As every scheme to defraud necessarily involves the offering of goods or services in ways that misrepresent their objective qualities and features, the principals in the scheme can never afford to use a direct route to persuasion, and therefore invariably fall back on methods using peripheral routes to persuasion.

One way in which a criminal can make prospective victims more susceptible to peripheral routes to persuasion is by making some statement at the outset of their interaction that triggers strong emotions, such as excitement or fear. In other types of fraud that involve strong personal interaction, such as telemarketing fraud, criminals construct their schemes to ensure that at or near the beginning of their interaction with a prospective victim, they will make some statements or actions, such as the promise of a substantial prize worth hundreds or thousands of dollars, that will cause the prospective victim to become immediately excited. [16] These surges of strong emotion, like other forms of distraction, serve to interfere with the victim's ability to call on his or her capacity for logical thinking, such as his capacity for counterargument. [17] This aids the criminal in making false representations that exploit a peripheral route to persuasion.

2. Attitudes and beliefs

Another dimension of the social psychology of fraud involves the differences between the victim's attitudes and beliefs about the person soliciting his money over the Internet and the criminal's attitudes and beliefs about his intended or actual victims. In a typical commercial transaction where there is no question about the quality of the goods or services for sale, buyer and seller may begin with different levels of conviction about the appropriate price for that good or service, but each has a general expectation that both he and the other party will end up with something of genuine value that meets their realistic expectations.

In contrast, in a fraudulent transaction only the victim is likely to believe that both he and the offeror of the good or service share that same expectation. It may be that before people can become victims of a fraud, they must first succumb to the temptation -- called the false consensus effect -- that others share their feelings and ideas. [16] In fact, those who commit fraud often adopt or devise ways of referring to their victims in denigrating or demeaning terms. In this decade, for example, law enforcement authorities have found that participants in fraudulent telemarketing businesses typically refer to a victim as a "mooch" -- a variant of "moocher," a person who demands something for nothing. Use of such terms undoubtedly eases the task of presenting their victims with representations that are false or deceptive, and ultimately choosing not to deliver what they promised or some item vastly lower in value than the victims had expected. Participants in fraudulent schemes may also devise characterizations of their own actions that minimize the harm they cause to their victims or that foster a more positive self-image of their actions. At a court hearing relating to the indictment of several telemarketers for their scheme to defraud consumers, particularly older people, one telemarketer stated in his defense, "We targeted to people who were homebound. It was kind of like entertainment for the homebound." [18]

Finally, social psychology experiments have shown that for some people who tend not to scrutinize persuasive messages closely, their postmessage attitudes were less dependent on scrutinizing the message when they perceived the source to be more honest. Thus, some fraud victims may tend to rely primarily on their belief or impression that the person with whom they dealt was honest, and to give little thought to the message's substance. [20]

3. Persuasion and influence techniques

A substantial body of literature in social psychology demonstrates that there are at least six factors relying on peripheral routes to persuasion that are highly likely to persuade or influence others [19]:

- *Authority*. People are highly likely, in the right situation, to be highly responsive to assertions of authority, even when the person who purports to be in a position of authority is not physically present. A study of three Midwestern hospitals showed how responsive people can be to such assertions. In the study, 22 separate nurses' stations were contacted by a researcher who identified himself (falsely) as a hospital physician, and told the answering nurse to give 20 milligrams of a specified prescription drug to a particular patient on the ward. Four factors should have indicated that the nurses might have questioned the order: (1) It came from a "doctor" with whom the nurse had never before met or spoken; (2) the "doctor" was transmitting a prescription by telephone, in violation of hospital policy; (3) the drug in question was not authorized for use on the wards; and (4) the dosage that the "doctor" had specified was clearly dangerous, twice the maximum daily dosage. Yet in 95 percent of the cases, the nurse proceeded to obtain the necessary dosage from the ward medicine cabinet and was on her way to administer it to the patient before observers intercepted her and told her of the experiment. [19]

- *Scarcity*. People are also highly responsive to indications that a particular item they may want is in short supply or available for only a limited period. Indeed, research by Dr. Jack Brehm of Stanford University indicates that people come to desire that item even more when they perceive that their freedom to obtain it is or may be limited in some way. [19] The belief that others may be competing for the short supply of the desired item may enhance the person's desire even more. [19]
- *Liking and similarity*. It is a truly human tendency to like people who are like us. Our identification of a person as having characteristics identical or similar to our own -- places of birth, or tastes in sports, music, art, or other personal interests, to name a few -- provides a strong incentive for us to adopt a mental shortcut, in dealing with that person, to regard him or her more favorably merely because of that similarity. [19]
- *Reciprocation*. A well-recognized rule of social interaction requires that if someone gives us (or promises to give us) something, we feel a strong inclination to reciprocate by providing something in return. Even if the favor that someone offers was not requested by the other person, the person offered the favor may feel a strong obligation to respect the rule of reciprocation by agreeing to the favor that the original offeror asks in return -- even if that favor is significantly costlier than the original favor. [19]
- *Commitment and consistency*. Society also places great store by consistency in a person's behavior. If we promise to do something, and fail to carry out that promise, we are virtually certain to be considered untrustworthy or undesirable. We therefore are more likely to take considerable pains to act in ways that are consistent with actions that we have taken before, even if, in the fullness of time, we later look back and recognize that some consistencies are indeed foolish. [15]

  One way in which social custom and practice makes us susceptible to appeals to consistency is the use of writing. A leading social psychologist, Professor Robert B. Cialdini, has observed that unless there is strong evidence to the contrary, "People have a natural tendency to think that a statement reflects the true attitude of the person who made it." [19] Moreover, once the person who receives such a statement responds by preparing a written statement of his own -- whether a letter, an affidavit, or an e-mail -- it tends to make the writer believe in what he has written as well, adding to the impression that both parties have displayed their true attitudes and beliefs.

- *Social proof*. In many social situations, one of the mental shortcuts on which we rely, in determining what course of action is most appropriate, is to look to see what other people in the vicinity are doing or saying. This phenomenon, known as *social proof*, can prompt us to take actions that may be against our self-interest without taking the time to consider them more deeply. Cults from the Jonestown Temple to Heaven's Gate, for example, provide cogent evidence of how strong the effects of that phenomenon can be in the right circumstances. [19]

B. Application to Internet-fraud schemes

From the foregoing discussion, it is clear that so long as Internet-raud schemes continue to rely on text-based communications over the Net, commitment and consistency will be highly influential in any Internet fraud directed at consumers or investors. Although a more extensive study of victim behavior in Internet fraud schemes ought to be conducted in the future, it stands to reason that if people tend to place more confidence in representations solely because the representations are in writing, Internet fraud victims are likely placing more confidence in Web site text or e-mail messages than an objective observer would think appropriate.

Internet fraud schemes also employ two or more of the psychological influence techniques described above, although the choice and combination of these techniques vary substantially from one scheme to another.

1. E-mail and Web site scams

Fraudulent schemes committed exclusively through e-mail -- what we will call "e-mail scams" for convenience -- seem to be drawing on several psychological influences. In its simplest form, such as the CompuServe example I described earlier [8], an e-mail scam can rely exclusively on a false assertion of authority, particularly if the scam can target a group of people who are more vulnerable or susceptible to that assertion. Compared with longtime users of the Internet, who better understand the Internet's pleasures and pitfalls, consumers who have just obtained Internet access for the first time are much more likely to defer to that assertion, and to assume without question that there are logical reasons for the assertion to be made at that time.

A possible variant on e-mail scams that could similarly rely solely on false assertions of authority would involve the use of "frame-spoofing." "Frame-spoofing" is a type of exploit to which Web browsers may be vulnerable. In "frame-spoofing," one Web site could insert its own frame into another Web site without any indication that the frame belongs to the first Web site. Consumers who visited the second Web site, and saw a frame directing them to submit their credit card data on an online form in that frame, would likely assume that the second Web site was responsible for the direction and comply with that demand. [21]

The Yahoo "modem scam" I mentioned earlier [9] uses a relatively more interesting combination of psychological influences. It combines false assertions of authority, the reference to the sender being a Yahoo employee, with an invocation of reciprocation (i.e., the promise of a valuable item, a high-quality modem, in exchange for what appears to be a small financial transaction to cover shipping costs). This combination is typical of the "prize" and "promotion" telemarketing fraud schemes that victimized consumers throughout the United States for much of the 1990s. [17]

2. Online auctions

While many online auctions offer a wide range of legitimate goods and services, Internet Fraud Watch receives more complaints about online auctions than any other category of Internet fraud. [1] Three of the psychological influences mentioned above are dominant in these frauds: scarcity, through the victim's identification of a particular good that he is prepared to buy immediately at a price he or she considers acceptable; reciprocity, through the criminal's promise to deliver the ordered goods once the victim has sent payment; and similarity, through the victim's willingness to do business with someone who apparently shares his or her interests in the collectible or computer merchandise being sold.

3. Securities and other investment schemes

Many of the Internet securities schemes that regulatory and law enforcement authorities have identified rely on a different combination of psychological influences. One of the more widely publicized Internet securities schemes is the so-called "pump and dump" scheme, in which insiders at a shell company or small, thinly traded company use various means of exciting online investors' interest in their company so that investors are manipulated into "pumping" up the stock's price enough for the insiders to "dump" their stock at a substantial profit before the price falls. [21]

"Pump and dump" schemes often combine false or misleading assertions of authority with the use of social proof. In a typical "pump and dump" scheme, stock promoters collaborate with company insiders to pay writers for one or more online investment newsletters to make favorable statements about the company. If the writers, called "touts," do not disclose their compensation from the company -- a violation of SEC regulations -- prospective investors are likely to assume that the touts are offering their unbiased and independent expert opinion, and to consider that opinion authoritative and reliable.

Online investors who frequent bulletin boards where other online investors share information and recommendations about companies can also be subjected to a subtle form of manipulation by promoters and company insiders. Because someone can easily forge e-mail headers, securities regulators have seen situations in which the same person has posted multiple messages that appear to come from different people in different parts of the country. This can encourage the unwary online investor to believe that there is a genuine consensus among other online investors about the stock being promoted. [21]

In one securities scheme that the SEC pursued, the promoters sent more than six million unsolicited e-mails, built bogus Web sites, and distributed an online newsletter to promote two small, thinly traded companies that had agreed to pay them in cash and securities. [21] In another scheme, which resulted in both SEC civil enforcement and criminal prosecutions by the Department of Justice, a company chairman not only bribed an online newsletter to tout his stock, but drove up the price of the stock through a false press release that claimed nonexistent multi-million dollar sales, an acquisition that had yet to occur, and revenue projections with no basis in fact. [21]

III. "Reverse-engineering" Internet fraud

Now that we have examined some of the psychological factors that appear most influential in the "social engineering" of Internet-fraud schemes, we should take a few moments to consider some of the broader implications of that examination. All elements of society that have a stake in the future of the Internet -- consumers and consumer organizations, business, and government -- need to consider what measures should be employed to deal with Internet fraud, and how those measures relate to one another. Enforcement actions by government, such as criminal prosecutions and civil actions directed at fraudulent schemes, are necessary to bring criminals to book and to deter similar conduct by others. Enforcement actions, however, inform the public about fraud only sporadically. We need to identify other mechanisms and media that aid consumers in recognizing and handling potentially fraudulent solicitations that they receive over the Net.

In that regard, we also need to take into account some unavoidable features of modern life and human behavior. As one social psychology study put it,

Will (1982) [22] estimated that the average American is exposed to more than 1,500 persuasive messages daily from national advertisers alone. People have neither the resources to think exhaustively about every persuasive appeal to which they are exposed nor the luxury (or apparently the inclination) of being able to ignore them all. [23]

That view has even more force in the context of the Internet, where in 1998 spam constituted more than 96 percent of the 7.3 billion "commercial" e-mail messages sent in the United States and people on average received twice as many e-mails as they sent each day [24].

How, then, should we think about preventing and educating people about Internet fraud? One component of a fraud prevention effort should certainly be the use of hardware and software that can help consumers to reduce the sheer number of potentially fraudulent messages they receive. While I recognize that blocking and filtering software, for example, may raise significant legal and public policy issues in certain contents, I think everyone here would agree that if we must be served spam on a daily basis in massive quantities [24], we are at least entitled to exercise some control over how much of it we must consume.

Biometrics and public-key cryptography, too, have significant value in fraud prevention, if only to provide some assurance that unauthorized persons are not using our computers or monitoring our online transactions to gain access to our personal financial data. At the same time, we must remember that many of the Internet fraud schemes we have been discussing rely not on hacking or cracking techniques to gain unauthorized access by force to our financial data, but on psychological manipulation through direct or indirect interaction between criminals and victims. We must ensure, in other words, that online consumers and investors recognize that security and encryption techniques may allow them to transact business, in the utmost security, with utterly untrustworthy people.

How should we do that? A number of government and private-sector organizations have already been producing public education materials and messages for online consumers and investors. As we continue to develop these messages, we should take into account the findings of social psychology that could help us to determine whether the messages we devise for consumers are likely to be effective in informing or influencing the consumer's decisionmaking processes about Net-based transactions that may be fraudulent.

For example, one social psychology study found that people are more willing to change their attitudes when they think a message contains new information than when they think a message repeats previously encountered information. [25] A subsequent study found that while mere repetition of the same message does not produce more immediate attitude change than a single presentation of the message, repetition of highly similar messages does have a positive effect on immediate attitude change. [26] This suggests that any printed or online materials or public-service advertisements about Internet fraud schemes should not simply repeat the same basic message in exactly the same words. Instead, they should try to provide consumers with new information in different advertisements or materials or at least present the same arguments in new contexts and with slightly altered phrasing. [26]

We also need to consider, in preparing messages and information sources for public education on Internet fraud, whether we are taking full advantage of our knowledge of social psychology to ensure that those messages and information are as persuasive as we can make them. In the past, government agencies and consumer groups have often printed masses of consumer information brochures that presented information amounting to "Do this/Don't do that" -- much as our parents told us to eat our spinach or to do other things that seemed unappealing but that we were required to take on faith.

In contrast, when the American Association of Retired Persons (AARP) decided, several years ago, to conduct an extensive public education campaign for seniors about telemarketing fraud, they used an approach called "social marketing." Social marketing involves the application of knowledge about consumer psychology and marketing techniques to prepare public education efforts that are most likely to reach consumers with messages that they will take to heart. By conducting focus groups and surveys, the AARP determined that many of the people who were or might become victims did not even understand that telemarketing fraud was a crime and that people in telemarketing schemes were consciously choosing to deceive the people who sent them money. As a result, the AARP's campaign took as its principal theme "Telemarketing Fraud Is A Crime" and devised a comprehensive campaign that incorporated public events, videotapes, reports, flyers, and other materials that reinforced and expanded on that basic message. Perhaps we should review AARP's experience with its anti-telemarketing fraud campaign to see how its approach could be applied to develop effective messages about various forms of Internet fraud.

We should also continue to think creatively about combinations of hardware and software that could help to remind consumers of the risks associated with financial transactions they undertake on the Net, even when they use secure communications. In securities transactions, for example, we know that individuals who are active in online investing typically move quickly -- often too quickly -- in consulting chat rooms or other sources of information they prefer in making investment decisions, and in placing trades that can put large amounts of their funds at risk. One technology that might help to remind online investors of the relative degree of risk is "force-feedback" technology. If force-feedback allows a computer user to feel greater resistance in moving a cursor toward a particular area displayed on a monitor, it could someday allow an investor to feel greater physical resistance the more funds he was proposing to commit to a particular securities transaction. The degree of resistance could be varied to suit a particular investor's income and assets, so that a future Warren Buffett could feel the same degree of force-feedback resistance, relative to the percentage of his available funds he was committing, as a typical middle-class online investor.

This technology could be combined with "pop-up" messages programmed to appear whenever an online investor or consumer is about to send a substantial payment that exceeds a certain threshold that he has previously set. If we already program word processing programs to pop up a window that asks "Are you sure?" when we are about to delete a single word processing file, we could adapt that code to ask "Are you sure you've considered all of the available information about this company?" and to include a short checklist of readily available sources of information useful to investors, before we put at risk thousands of dollars in hard-earned savings, especially in thinly traded, speculative, or wholly spurious business ventures.

These approaches would not deprive an online investor of the right to make his own decisions about particular investments. They would, however, provide the investor timely reminders that a few muscular contractions, in clicking the mouse to complete the planned transaction, could have potentially substantial consequences. They might even encourage him to pause and consider whether he has in fact reviewed enough information to be making an investment decision based on logic and analysis rather than excitement and social proof. At any rate, they suggest that we should carefully consider a very different kind of "social engineering," conducted for the benefit of consumers, as part of a comprehensive and internally consistent approach to fostering meaningful consumer protection on the Internet.

References

[1] National Consumers League, Press Release, "NCL Releases Top Ten Internet Scams," Feb. 10, 1998, http://www.natlconsumersleague.org/top10net.htm

[2] Tom Lowry, "To catch a cyber thief," USA Today, Feb. 17, 1999, http://usatoday.com/life/cyber/tech/cte414.htm

[3] Jargon File 3.0.0 -- social engineering, http://www.it.com.au/jargon/social_engineering.html

[4] Del Armstrong and John Simonson, "An Intro to Computer Security," School of Engineering and Applied Sciences, University of Rochester, http://www.seas.rochester.edu:8080/CNG/docs/Security/node9.html

[5] Computer Incident Advisory Capability, U.S. Dept of Energy, CIAC Note 94-03a, July 6, 1994, http://www.ciac.org/ciac/notes/Notes03a.shtml#Engineering

[6] Jorma Kajava and Mikko T. Siponen, "Social Engineering - IT Security Threat of Informatics," http://www.ifi.uio.no/iris20/proceedings/9.htm

[7] Carnegie-Mellon Software Engineering Institute, CERT Coordination Center, "Social Engineering," CERT Advisory CA-90.04, revised Sept. 18, 1997, http://www.cert.org/advisories/CA-91.04.social.engineering.html

[8] "Spam scam nets newbies," New Scientist, October 31, 1998, http://www.newscientist.com/ns/981031/nspam.html

[9] Janet Kornblum, "Yahoo recovers from scam, hack," CNET News, Dec. 12, 1997, http://www.news.com/News/Item/Textonly/0,25,17318,00.html

[10] "Bernz's Social Engineering Tips," http://www.genocide2600.com/~tattooman/social-engineering/tips.html

[11] Al Berg, "Cracking a Social Engineer," LAN Times, Nov. 6, 1995, http://www.genocide2600.com/~tattooman/social-engineering.soc_eng2.html

[12] Harl, "People Hacking: The Psychology of Social Engineering," Talk at Access All Areas III Conference, May 7, 1997, http://www.genocide2600.com/~tattooman/social-engineering/aaatalk.html

[13] "Bernz's Social Engineering Intro and stuff," http://www.genocide2600.com/~tattooman/social-engineering/socintro.html

[14] David G. Myers, *Exploring Social Psychology* 3 (1994)

[15] John T. Cacioppo, Richard E. Petty, Chuan Feng Kao, and Regina Rodriguez, "Central and Peripheral Routes to Persuasion: An Individual Difference Perspective," 51 *Journal of Personality and Social Psychology* 1032 (1986)

[16] Transcript of Hearing, *United States v. St. Marie*, No. SACR96-135(A)-3 GLT at 25 (C.D. Cal., Feb. 19, 1997)

[17] Prepared Statement of Jonathan J. Rusch, U.S. Department of Justice, Before the United States Sentencing Commission, February 10, 1998, http://www.usdoj.gov/criminal/fraud/telemarketing

[18] Robert A. Osterhouse and Timothy C. Brock, "Distraction Increases Yielding to Propaganda by Inhibiting Counterarguing," 15 *Journal of Personality and Social Psychology* 344 (1970)

[19] Robert B. Cialdini, *Influence* (revised edition 1993).

[20] Joseph R. Priester and Richard E. Petty, "Source Attributions and Persuasion: Perceived Honesty as a Determinant of Message Scrutiny," 21 *Personality and Social Psychology Bulletin* 637 (1995)

[21] Securities and Exchange Commission, "Internet Fraud: How to Avoid Internet Investment Scams," Oct. 1998, http://www.sec.gov/consumer/cyberfr.htm

[22] George F. Will, "But First, A Message From . . .," *Newsweek*, May 10, 1982, at 98

[23] John T. Cacioppo, Richard E. Petty, and Katherine J. Morris, "Effects of Need for Cognition on Message Evaluation, Recall, and Persuasion," 45 *Journal of Personality and Social Psychology* 805 (1983)

[24] "Emarketer Tallies the Number of e-Mail Messages Sent in 1998," eMarketer, Feb. 1, 1999, http://www.emarketer.com/estats/020199_email.html

[25] D. W. Sears and J. L. Freedman, "Effects of Expected Familiarity with Arguments Upon Opinion Change and Selective Exposure," 2 *Journal of Personality and Social Psychology* 420 (1965)

[26] J. Lee McCullough and Thomas M. Ostrom, "Repetition of Highly Similar Messages and Attitude Change," 59 *Journal of Applied Psychology* 395 (1974)

Disclaimer

The views expressed herein are solely those of the author, and do not necessarily represent those of the Department of Justice or any component or officer thereof.

▲ Up ◀ Prev ▶ Next