"I Brought You A Good News": An Analysis of Nigerian 419 Letters

Marilyn A. Dyrud, Oregon Institute of Technology

Abstract

Nigerian 419 letters (so called because 419 is the fraud section of the Nigerian penal code) offer fertile ground for classroom activities related to persuasion. Originally sent as paper mail, 419s now appear by the thousands via fax and email. An examination of over 100 emails received by the author reveals several persuasive techniques that make the scam successful. The paper also includes pedagogical suggestions.

Introduction

Congratulate me: I am potentially worth \$1.62 billion! This is good news indeed. Not only am I, a lowly writing teacher at a small technical institute, about to become wealthy beyond my wildest dreams, I have received letters from such luminaries as Yassar Arafat's widow, who wants my personal assistance in consolidating her late husband's estate.

All of us, from time to time, have received these pesky emails or, in the olden days, actual paper letters. All promise fabulous riches *if*—and this is a big if—the recipient will simply forward a bank account number and allow the sender to park substantial funds in that account. While this scam seems to be utterly transparent, many have taken the bait. According to the United States Secret Service, 419 letters account for an annual loss in this country of hundreds of millions of dollars (US Secret Service, 2002). The international loss, since the mid-1980s, is estimated at more than \$5 billion ("Nigerian Scam Buster," n.d.).

For those of us who teach business correspondence, 419 letters offer fertile ground for classroom activities related to persuasion. This paper explores this international phenomenon, focusing on the scam, variations on the theme, persuasion tactics, and classroom exercises.

The Basic Scam

Nigeria is the richest country in Africa, courtesy of a mid-20th century oil boom. It is also, however, one of the most corrupt countries on the planet, second only to Bangladesh (419 Eater, 2005). Indeed, notes Femi Oyesanya, corruption permeates Nigerian culture: "Financial fraud is Nigeria's fifth-largest source of business income" (Oyesanya, 2004). One of the more lucrative ventures has been the advance fraud fee initiative, more commonly referred to as the "419 scam," because it violates Section 419 of Nigeria's Criminal Code:

Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years. If the thing is of the value of one thousand naira

[\$7.41US, at current exchange rates] or upwards, he is liable to imprisonment for seven years (South African Police Services, 2004).

The scam began in the 1980s, following Nigeria's oil bust (Delio, 2002) and first involved investment opportunities, typically sent to businesses on stolen letterhead with counterfeit postage. The volume was substantial: in a 1998 crackdown, United States postal officials seized and destroyed 2.3 million letters at JFK Airport in three months (McDermott, 1998), and in the United Kingdom, about 1.5 million were intercepted during the same time period (APCO, n.d.).

With the advent of electronic communications technology, specifically email and fax, the numbers have skyrocketed: some 250,000 scammers, worldwide, send out thousands of messages daily (419 Eater, 2005), using venues such as Internet cafés and free email accounts through conventional providers such as *Yahoo!* and *Hotmail*. Recipients' addresses are gleaned through bulletin boards and public Internet discussion spaces, association and organization lists, illegally purchased email lists, and email address harvesting programs. Scammers have multiple email accounts, and they may change addresses on a daily basis (McGuire, 2000-3).

While the 419 scam is certainly criminal activity, the scammers tend to be white collar professionals, according to the head of Nigeria's Interpol bureau, Hafez Ringim, including "attorneys, chartered accountants, chemical engineers" (Kaplan, 2001). Some, as noted in a 1995 *Economist* article, are viewed as "folk heroes," most notably Fred Ajudua, who sees himself as "a black man's Robin Hood, getting repayment from white men for slavery and colonialism" ("Great Nigerian Scam,"1995).

Once a person's address is in the 419 email system, letters are frequent. Table 1 indicates the breakdown of 419 emails I received during a 10-month period, excluding duplicates. Most notable is the escalation of numbers in the last few months, averaging one for every two working days.

Table 1
Types of emails received

Month	Estate	Investment	Lottery*	Totals
September 2004	3	3	1	7
October	1	6	3	10
November	2	2	3	7
December	3	2	1	6
January 2005	5	2	1	8
February	6	10	4	20
March	2	9	1	12
April	7	6	1	14
May	9	2	1	12
June	8	5	2	15
Totals	46	47	18	111

* Lottery letters are not technically 419s, but they are included in the tabulation as another type of scam increasing in frequency.

The initial contact is an email from an important-sounding person, such as a lawyer, banking or government official, former politician, Catholic priest, business executive--even deposed royalty! The email offers the recipient the opportunity to reap rich rewards by assisting the sender in one of several ways: estate disposition, real estate purchase, or seductive business deals, such as buying crude oil at below-market prices (US Secret Service, 2002). Following is an example of a typical email, with the spelling, punctuation, and spacing as in the original:

Good day to you.

I know you dont mind my contacting you by this means since we have not met before this time. My name is Mrs. Neri Keita-widow from Angola. My late husband served in the past Angolan government before his death.

Recently my husband's will was read and to our joy and relief, he has kept the sum of \$8million USD in trust for the upkeep of the family.

This money he deposited(cash) with a security deposit/finance company in Europe with a firm instruction that I should seek for assistance to invest it abroad in any good business.

Hence I need your help to invest this money in any good business like real estate there in your country.

This will be a joint venture arrangement that will demand trust and sincerity which you will benefit immensely from this project, as I will rely on you for it's success. Please do indicate your willingness to assist me through my email—neri001@post.cz so that I can give you the details.

Bye while expecting your quick response (October 13, 2004).

The tone is invariably polite and delightfully Victorian, as in the following examples:

- "I have the privilege to request your assistance. . ." (October 16, 2004).
- "... I was divinely inspired to contact you" (March 26, 2005).
- "I am contacting you in anticipation of a cordial business relationship" (February 11, 2005).
- "I humbly wish to seek your assistance in a matter that is very important and needs utmost trust and confidence" (March 16, 2005).

If the recipient responds favorably, either via email or telephone, the scam progresses to the next level, typically a request for money to cover various "processing fees." Heidi Evans, a reporter for the *Daily News*, recounts her brief experiment answering an estate disposition plea, which would entitle her to collect a portion of \$10.5 million left by an unknown relative. After answering the initial query, she then telephoned, as directed, a female attorney in Lagos, Nigeria, who asked her for \$970 for a "stamp duty free." The newspaper paid, and Ms. Evans was then instructed to pay another fee of \$1,550 for "document processing," which her paper declined to pay, thus ending the experiment (Evans, 2005).

For those who keep paying, assuming that "this will be the last request," fees escalate into the tens of thousands of dollars. Eventually, the victim will be asked to meet face-to-face with the principals in Lagos or a European locale where s/he may be greeted with a trunkful of "disguised" money, often stained black with a mixture of Vaseline and iodine. The scammers dip a sample \$100 note in an alkaline solution to remove the iodine and voila! Real money! Of course, this is all a ruse, as the trunk contains only black paper, cut to simulate bank notes ("Nigerian Scams," 2000). Furthermore, the victim may be asked to pay thousands of dollars for the chemicals necessary to return the notes to their natural state (APCO, n.d.).

Visiting Nigeria can be dangerous. Scammers will arrange a "special entry" for victims that precludes the need for a valid visa, a violation of Nigerian law ("Nigerian Frauds," 2005), and victims may find themselves kidnapped and held for ransom or even murdered. Citing United States State Department statistics, Michelle Delio, of *Wired News*, notes that "25 murders or disappearances of Americans abroad have been directly linked to 419 fraud. Other people have been held against their will, beaten and blackmailed" (Delio, 2002). Other tales are equally disconcerting: in 2001, 15 foreign business people visiting Nigeria for 419 scams were threatened with physical harm (Kaplan, 2001), and three Americans were held hostage for \$30,000 ransom ("Nigerian Victims," 2002). In 1999, Danut Tetrescu, a Romanian businessman who had flown from Bucharest to Soweto to collect his millions, was kidnapped and held for \$500,000 ransom ("Nigerian Scams," 2002).

The situation is so threatening that a number of US agencies have issued warnings on the Web, including the FBI, Secret Service, Department of the Treasury, Internet Fraud Complaint Center, and the Better Business Bureau. Internationally, law enforcement agencies in the United Kingdom, New Zealand, Australia, and Canada have also posted warnings.

Yet, despite Internet cautions, people continue to swallow the bait. Apparently, the persuasive nature of the email, combined with the possibility of instant wealth, is sufficiently seductive. And, of course, the documentation the victim receives seems official and real. Once victims enter into the relationship and pay appropriate fees, they receive a wealth of courier-delivered documents, including

- Fund Management Agreement
- Fund Remittance Voucher
- International Remittance Department, Approval Order
- Final Notification of Transfer, Fund Release Order
- Power of Attorney Form
- Authority Verdict of the Panel of Judges
- Affidavit of Fund Ownership

- Approval/Transfer of Payment Warrant
- Transfer Confirmation Slip
- Confirmation of Banking Particulars
- Certificate of Registration Official Receipt
- Analysis of Fund Transfer of Fund
- Schedule Fund Release Order Form ("Nigerian Scams," 2002)

While these all sound impressive and appropriately bureaucratic to the novice investor, some can be dangerous if they fall into the wrong hands; *e.g.*, the power of attorney form, which empowers the scammer to use all of the victim's personal assets.

According to McGuire (2000-3), the usual return on an email campaign is about 1-2%, with 1% more common: "That means that for every 1,000 letters sent out, at least 10 will get replies. Of those ten, at least one will continue the relationship to the phase that requires money and gifts be sent." Normally sensible people succumb to the allure of instant wealth, as the following cases indicate:

- The Teis from St. Louis paid over \$54,000, which included their children's college fund; took out a second mortgage on their house; and spent many hours making arrangements for the visit of Nigerians to St. Louis, including hotel reservations and buying expensive suits for their guests--all for the promise of \$5 million. Mr. Tei is a licensed tax preparer (Brooks, 1994).
- Eric, a family man from Singapore, lost \$190,751 in payments to a Nigerian scammer who offered a percentage in a non-existent \$25 million estate disposition ("Nigerian Scam Buster," n.d.).
- The United Kingdom's National Criminal Intelligence Service indicated that about 150 Britons last year lost a total of £8.4 million, an average of £56,675 per victim. One, who traveled to Africa to collect his share, ended up beaten and tortured ("Nigerian Scam Buster," n.d.).
- Canadians have lost about \$30 million to the scam (RCMP, 2003).
- An American businessman who met with Nigerians at a London hotel ended up committing suicide when he discovered he had lost more than \$50,000 (APCO, n.d.).
- Two Asian women have lost £25 million, and a Norwegian woman lost £120,000 and her home (APCO, n.d.).

To give an example of the scope of the problem in this country, the Financial Crimes Division, an arm of the Secret Service, has established "Operation 4-1-9"; it currently receives about 300-500 letters and 100 phone calls per day from potential victims (Gamma, 2005). Victims lose an average of \$3,864 ("Be Careful," 2003).

Variations on a Theme

Like all good campaigns, the Nigerian 419 scam has legs, a number of variations on the common theme; these include religion, charitable donations, and exploiting current events.

While use of religion to extort money is certainly not an innovative strategy, imagine my surprise when I received an email, with the subject line "God Bless as You Assist," from the Catholic bishop of Nigeria! Bishop Greg Williams, who, by the way, is non-existent on the Internet and is not listed in the diocesan database for an important international Catholic bishops' conference held in Nigeria in 2003, needs assistance with fulfilling a promise to a "prominent politician" to deal with an overseas account: "You should understand my position that I can not handle this to avoid scandal and blackmail" (September 29, 2004).

A more common ploy is to appeal to the recipient's sense of religious obligation, as in this January 12, 2005, email from Mrs. Aisha Alade Barmaiyi, "a new Christian convert." She is looking for "an honest Christ [sic] or muslim who will receive this fund [of \$18 million] and utilise it for things that will glorify the name of God."

Many of the writers who use a religious theme want their very substantial funds to be used for charitable work, a second variation on the basic scam. Mrs. Rose Welsh, in London for medical treatment, wants her late husband's £10 million "to do mighty works for the Almighty... to provide succor to poor and destitute persons, orphanages, and widows and for propagating peace in the universe" (January 31, 2005). Similarly, Mrs. Recheal Wely, a Kuwaiti whose husband left her a legacy of \$12.6 million, wants his money donated to "churches, orphanages, Research centers and widows propagating the word of God and to ensure that the house of God is maintained" (February 10, 2005).

Despite the humanitarian impulses displayed in these types of emails, they are simply the second verse of the same old song: emotional ploys to appeal to sympathetic people in an attempt to extort money.

A third variation uses current events. The most recent involves scammers who impersonate officials of the Homeland Security Department and then contact the families of slain US soldiers in an attempt to recover money from their now-deceased loved one's friends. In another twist, the bogus "agent" is attempting to track down money purportedly stolen from the Iraqi Central Bank by one of Saddam's sons (MSNBC, February 2005). Assistant Secretary Michael Garcia, of the United States Immigration and Customs Agency, has stated, "This really is one of the worst e-mail scams we've ever seen, targeting the families of American soldiers killed in Iraq. This is really despicable" (MSNBC, June 2005).

Prior events exploited by the scammers include the December 2004 tsunami in Southeast Asia, the 2001 World Trade Center attacks, the 2000 crash of the Concorde, and a whole host of airplane, car, and train crashes, in addition to local African bombings, murders, and other assorted mayhem. Most refer to websites that the recipient can check. A follow-up on the websites, though, reveals that many of the links are either inactive or offer articles that are overviews of the incidents, not passenger lists. Further investigation into Christian Eich, mentioned as a victim of the Concorde disaster in several emails, indicates that he was indeed among those killed; this leads to the unsettling conclusion that scammers may troll victim lists for names of real people to exploit in their emails.

Persuasion Techniques

Scammers use a number of strategies to reel in their intended victims, including appeals to pity, trust, and avarice. Notes FBI cybercrime agent Dale Miskall, "Nigerians are just great at social engineering . . . and Americans are quite gullible" (MSNBC, June 2005).

Ad miseriocordium, the logical fallacy involving appeals to pity, is one of the most commonly used tactics. To judge by the emails, wealthy Nigerians are dying off at a terrific rate due to all sorts of malicious cancers: breast, pancreas, and esophageal chief among them. They are also suffering from debilitating strokes and hearts attacks yet apparently have enough energy left to send emails all over the world. Their dying wish is for a person with a "good heart" to help them deal with their substantial fortunes. An April 1, 2005, appeal from Larry Moore, a United Arab Emirates merchant dying of prostate and esophageal cancers, is typical: "I am writing this from my laptop computer in my hospital bed where I wait for my time to come. I pray that God uses you to support and assist me with good heart."

Some are ludicrously transparent, such as John Kredoski's November 13, 2004, email. He lives in Reno, has suffered a heart attack, and has chosen to write to me because I am "a fellow American." "Do not," he cautions, "associate this letter as numerous letters we receive from Africa. If you need my passport to prove my identity, I will send it to you." For a native-born American, his syntax and vocabulary are curiously similar to his Nigerian counterparts.

Other pathos-based appeals come from children of deposed politicians and wives of military men murdered in coups, all of whom are either in hiding or have fled their country to avoid a similar fate. Coincidentally, they all have millions of dollars tied up in either hidden domestic accounts or secret foreign accounts.

Another major appeal is trust. Virtually all of the emails, especially those referring to childless couples who have died intestate, use the word "trust," as the following examples show:

- "I am trusting you with my money" (November 13, 2005).
- "... I therefore need a honest, trustworthy and reliable assistance of a foreigner..." (April 4, 2005).
- "... trusting in you and believing that you will never let me down now or in the future" (April 25, 2005).
- "... I will need the help of a trustworthy foreign partner to enable us to put claims to this funds. .. (May 6, 2005).

Trust, however, involves a reciprocal agreement, and by their very nature, scammers repeatedly violate trust. A touching summer story on NBC's *Dateline* featured Pam Krause of Almond, Wisconsin. Ms. Krause, out of compassion, thought she was helping a West African mother in desperate straits, only to discover she had fallen prey to yet another scam: she lost \$18,000 (MSNBC, June 2005).

A third major technique is an undisguised appeal to greed. Potential victims are typically offered 5-30% of the fund, in the case of estate dispositions. Investment emails offers a much larger percentage, 20-40%, of a much larger pot, up to \$120 million.

Senders claim to be representatives for one of several legitimate-sounding Nigerian or South African companies, such as

- Nigerian National Petroleum Corporation (the most common)
- Central Bank of Nigeria
- Anglogold Corporation
- Apex Paying Bank
- Liquefied Natural Gas
- Petrol Ivoire

All the recipient has to do is stand in as "beneficiary" or "overseas agent" and allow the use of a bank account as a parking space for millions of dollars: minimal work for maximum reward. Dr. George Kenneth, of the Nigerian National Petroleum Corporation, cautions "utmost secrecy": "I want you to understand that having put in over 25 years of service to my country, my colleagues and I are careful not to have our name and image tarnished" (March 20, 2005).

Classroom Exercises

Nigerian scam letters present a number of possibilities for classroom exploration, limited only by the individual instructor's imagination and the amount of time available.

In-Class Exercises

Small group discussions are effective for having the class analyze a number of issues in a limited time. Divide the class into groups of three or four and give each group a different, but representative, letter. Depending on the goals for the exercise, groups could analyze their letters for any one of the following:

- Persuasive strategies: How does the writer appeal to the audience? What specific techniques are used? How effective are they?
- Audience: Who is the letter appealing to? What are audience traits? Are the typical salutations of "Dear Sir" or "Dear Sir/Madam" effective?
- Language usage: Is the polite 19th-century language charming? Annoying? How effective is the extreme deference? How do ESL attributes affect the message?
- Subject lines: How effective are all cap subject lines such as "URGENT," "REPLY ASAP," or
 the less conventional "Beloved in Christ," "Fulfill my last wish, please," "You are the only one,"
 or "Cry for help"?

• Format: Given that printed format is dependent on the printer used, many 419 emails are written in single-spaced 10-point Arial, with wide margins and haphazard paragraphing. Some are in all upper case. How effective is the formatting? How can the writers make the document more visually appealing? Or do they care?

Research Exercises

For instructors who have the luxury of a little more time or who wish to delve more deeply into the factual content of 419s, having students research some of the names mentioned is an enlightening exercise. For example, on November 10, 2004, I received an email from "Peterside Kanyon Doe," purportedly the only son of a slain ruler of Liberia, Samuel Kanyon Doe, who was "brutally murdered by a mentally disturbed soldier named Price Yormie Johnson." Since the 1990 murder of his father, Peterside has been hiding in the Liberian countryside. Before his death, Samuel had secreted a cache of money in Europe, which has only now come to Peterside's attention. He seeks my help in obtaining the money and establishing a "new identity" in America so he can start a new life. For my assistance, he will give me a share of the money. In a postscript, he notes that I can "read about this event in any book on Liberia history past and present." Overall, the email is a plaintive, rather poignant plea for help.

Following up on Peterside's suggestion, I checked an online encyclopedia for information about his father. Samuel Kanyon Doe was indeed killed by a deranged soldier in 1990. But the story is not nearly so sympathetic as his son suggests: at the tender age of 28, Doe was the leader of a 1980 political coup which resulted in the murder of the then-president of Liberia, William R. Tolbert. Doe rose to power after rigging an election and changing his birthdate (the Nigerian constitution requires presidents to be at least 32 years old); he then ruled despotically for the next decade. Notes the source, "The greed for power, the corruption, nepotism and the abuse of human rights which Doe had reproached Tolbert [for] had become a trademark of his [own] regime" ("President," 2005).

Another possibility is to have students examine some of the websites mentioned, which are offered as proof for the information in the email. In an October 20, 2004, email, Gideon Arp Moi asks for the assistance of someone who would be willing to travel to Europe to receive two trunks of money which his father, former Kenyan president Daniel Moi, has left with a security company. The email insists that this money resulted from the sale of gold and diamonds and offers links to two stories on the BBC website.

A check of the stories, however, reveals that Daniel Moi was the subject of some rather intense investigations in one of Kenya's "biggest financial scandals"; the gold and diamonds he allegedly sold did not exist (BBC, 2004). Moreover, he was also implicated in investigations regarding the disappearance of nearly \$14 billion from Kenya's Euro Bank, which subsequently collapsed (BBC, 2003).

Conclusions

Using 419 letters in the business communication classroom offers rich pedagogical possibilities for a study of persuasion through small group discussions and student research. As this paper has shown, scammers are accomplished persuaders who garner substantial, albeit unethical, rewards for their

efforts. Having students analyze these letters helps to develop their critical faculties for evaluation of Web information and provides an entertaining class activity.

"In Nigeria," Finance Minister Ngozi Okonjo-Iweara has said, "we are always amazed that anyone could be stupid enough to respond to such an offer" (419 Eater, 2005). In America, however, the potential of instant wealth is embedded in our cultural mythology: there's always the chance of winning the lottery or of a windfall inheritance from that eccentric uncle, who has stashed thousands of dollars in coffee cans neatly stacked in his basement. It is not stupidity that Nigerian scammers prey upon: it is hope.

References

419 Eater. (2005). The ethics of scambaiting. Retrieved March 29, 2005, from http://www.419eater.com/html/ethics.htm

APCO. (n.d.). Fraud prevention: West African 419 letters. Retrieved June 27, 2005, from http://www.uk-fraud.info/types/letters.html

BBC. (2003, June 27). "Stop harassing me," says Moi. Retrieved June 25, 2005, from http://news.bbc.co.uk/2/hi/africa/3025878.stm

BBC. (2004, January 23). Ex-Kenya leader "switched \$76m." Retrieved June 25, 2005, from http://news.bbc.co.uk/2/hi/africa/3338023.stm

Be careful when bidding online: Internet fraud. (2003, June 6). Medical Economics, 80 (11), 10.

Brooks, G. (1994, June 24). Outmaneuvered: How a recurring scam cost an accountant and his wife \$54,000. Wall Street Journal, A1.

Delio, M. (2002, July 17). Meet the Nigerian e-mail grifters. *Wired News*. Retrieved February 2, 2005, from http://www.wired.com/news/print/0,1294,53818,00.html

Evans, H. (2005, June 5). Don't let her web of lies rip you off. *Daily News*. Retrieved June 27, 2005, from http://www.nydailynews.com/news/crime_file/story/315987p-270397c.html

Gamma Investigative Research, Inc. (2005). *Public awareness advisory regarding "4-1-9" or "advance fee fraud" schemes.* Retrieved June 27, 2005, from http://www.privateye.com/usss.htm

Great Nigerian scam. (1995, January 7). The Economist, 36.

Kaplan, D. E. (2001, May 27). A land where con is king. U.S. News & World Report, 130 (18), 28-9.

McDermott, J. (1998, November 11). US Postal Service is cracking down on Nigerian scams. Wall Street Journal, 1.

McGuire, A. M. (2000-3). Nigerian scam letters: Sent out by the thousands. Retrieved February 2, 2005, from http://www.fraud.com/ScamSpeak/Nigerian/419 Hidden Facts/emails sent out by the thousands.htm

MSNBC. (2005, February 18). *E-mail scam targets slain soldiers' families*. Retrieved March 10, 2005, from http://www.msnbc.msn.com/id/6995633/

MSNBC. (2005, June 10). "Nigerian scams" keep evolving. Retrieved June 28, 2005, from http://www.msnbc.msn.com/id/8171053/

Nigerian frauds 419: "Scam central," frequently asked questions. (2005). Retrieved April 23, 2005, from http://www.freemaninstitute.com/419faq.htm

- The Nigerian scam buster. (n.d.). Retrieved April 12, 2005, from http://www.nigerianscambuster.com/
- Nigerian scams: Schemes, scams, frauds. (2002). Retrieved February 2, 2005, from http://www.crimes-of-persuasion.com/Crimes/Business/nigerian.htm
- Nigerian victims: Schemes, scams, frauds. (2002). Retrieved June 27, 2005, from http://www.crimes-of-persuasion.com/Nigerian/nigerian_victims.htm
- Oyesanya, F. (2004, March 28). *Nigerian Internet 419 on the loose*. Retrieved May 25, 2005, from http://www.nigeriavillagesquare1.com/Articles/oyesanya.html
- President Samuel K. Doe. (2005). Retrieved June 27, 2005, from http://www.liberiapastandpresent.org/SamuelKDoe.htm
- RCMP. (2003, October 8). Nigerian letter scam. Retrieved February 2, 2005, from http://www.rcmp-grc.gc.ca/qc/faq/nigeria e.htm
- South African Police Services. (2004, November 4). *About 419 scams*. Retrieved March 27, 2005, from http://www.419legal.org/pages.php?p=10
- US Secret Service. (2002). *Public awareness advisory regarding "4-1-9" and "advance fee fraud" schemes.* Retrieved February 2, 2005 from http://secretservice.gov/alert419.shmtl