

SFGate.com

U.S. Internet fraud at all-time high 'Nigerian' scam and other crimes cost \$198.4 million

Eric Rosenberg, Hearst Newspapers
Saturday, March 31, 2007

(03-31) 04:00 PDT Washington -- Americans lost a record amount to Internet fraud schemes last year, and the notorious "Nigerian 419" scam is blamed for the largest individual losses.

A government report on 2006 Internet crimes also records the sudden emergence of extortionists who use e-mail to deliver ominous threats that grave consequences await unless money is sent.

The new federal statistics show that Americans reported losing an all-time high of \$198.4 million to Internet fraud in 2006, up 8 percent from 2005 levels of \$183 million and 191 percent from 2004 levels of \$68 million.

Law enforcement officials believe that actual losses are higher -- many victims don't report the crimes because they are embarrassed or afraid to do so.

Of the Internet criminals who could be traced to their location, 61 percent resided inside the United States, followed by criminals based in the United Kingdom at 16 percent. Nigeria-based criminals were next at 6 percent.

According to the new statistics, victims of the 419-type scams had an average loss of \$5,100 last year, an increase of \$100 per incident compared with 2005 levels and an increase of \$2,100 per incident compared with 2004.

Federal officials call the scheme the Nigerian 419 scam because it originated in that West African country, where Section 419 of the Nigerian criminal code deals with fraud. In Nigeria, the 4-year-old Economic and Financial Crimes Commission says it has successfully cracked down on the large majority of home-grown scammers and has recovered more than \$750 million for victims all over the world. The agency works closely with the FBI, said commission head Nuhu Ribadu, and most scam e-mails now originate elsewhere in Africa or in Eastern Europe. But he acknowledges that the name has stuck even as the scammers have moved elsewhere.

There are numerous variations of the 419 theme, but the general outlines are familiar to almost everyone with an e-mail account. In an unsolicited e-mail, a purported African official says he needs the recipient's help in transferring millions of dollars from the bank account of a deceased African leader, company official or senior government bureaucrat. The e-mail recipient will receive a sizable percentage by helping him do so.

That aid would be in the form of cash that the thief says is needed to cover "transaction costs" up

front to consummate the deal.

Once a victim pays, the African official invariably requires additional funds when the transaction encounters fictitious snags.

The U.S. Secret Service pegs annual U.S. losses to the 419 scam -- both through the Internet and regular mail solicitations of victims -- in the range of "hundreds of millions of dollars."

"It is amazing the kind of people who fall for this," said Johannes Ullrich, an Internet fraud expert with the Sans Institute in Bethesda, Md., a computer and Internet security training organization. "It's not just the bored retiree, but it's also professional people you would think who would know better. The greed factor turns off their brains."

Shawn Mosch, of Bloomington, Minn., who runs a Web site -- ScamVictimsUnited.com -- dedicated to warning consumers about such schemes, says the 419 scam has raked in huge sums. She said one person who contacted her organization claimed to have lost between \$200,000 and \$300,000.

The extortion e-mail scam -- also known as the hit-man scheme -- involves a threatening note warning the victim that he will be killed unless he pays thousands of dollars. The FBI calls it a "recent high activity scam" that began appearing in e-mail inboxes last December. Some solicitations demand payment of \$20,000 or more.

Like many 419 scams, the hit-man solicitations often are peppered with broken English and misspellings. One such solicitation forwarded to the FBI in December said ominously: "I have followed you closely for one week and three days now. ... Do not contact the police or F.B.I. or try to send a copy of this to them, because if you do I will know, and might be pushed to do what I have being (sic) paid to do."

The FBI has received about 159 complaints since the scam emerged, said John Hambrick, the top FBI official at the Internet Crime Complaint Center. The FBI has received no reports of money loss or murder threats that were carried out, he said in an interview.

The hit-man con "is almost the reverse of the 419 scam," said Hambrick. "This is a threat of the loss of life and the other is an enticement to enrich you. I think folks are more willing to believe that someone is going to make them wealthy."

The Internet Crime Complaint Center, which has been tracking Internet fraud trends for six years, is a joint enterprise of the FBI and the National White Collar Crime Center, an agency that trains law enforcement officers to combat economic and cyber crimes.

Of the 86,279 fraud complaints in 2006 that the Internet center referred to law enforcement

agencies for investigation, Internet auction fraud accounted for the highest volume, with 45 percent of complaints.

Complaints about Internet auction fraud usually involve instances of a victim who buys goods or services through an online auction but never receives the merchandise from the seller after making payment, or the victim is selling goods through an auction, ships the goods to a buyer and doesn't receive payment.

In terms of volume, complaints about nondelivery of items purchased on the Internet was in the second place, followed by Internet-related check and credit card fraud.

Chronicle Foreign Editor Gail Bensinger contributed to this report.

<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/03/31/MNGSCOVGGI1.DTL>

This article appeared on page **A - 1** of the San Francisco Chronicle