Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

For Release: November 13, 2002

Federal, State, and Local Law Enforcers Tackle Deceptive Spam and Internet Scams

"Spam Harvest" Results Reap Help for Consumers Trying To Avoid Spam

The Federal Trade Commission and 12 federal, state, and local law enforcement and consumer protection agencies today announced a four-part initiative launched to fight deceptive spam and Internet scams. The centerpiece of the initiative is a group of more than 30 law enforcement actions, including three FTC complaints and four settlements with spammers caught in an FTC sting. In addition, 10 of the law enforcers signed letters to approximately 100 spammers warning them that their spam appeared to be illegal and that law enforcers could take action against them if they continued their fraudulent scams. Ten agencies participated in the FTC's "Spam Harvest," an initiative designed to test which actions consumers take online that put them most at risk for receiving spam. The operation also developed consumer education material, including a publication, "E-mail Address Harvesting: How Spammers Reap What You Sow," that uses the lessons learned from the Spam Harvest to provide tips to consumers who want to minimize their risk of receiving spam.

"We're committed to pursuing law enforcement actions against deceptive or fraudulent spammers," said J. Howard Beales, III, Director of the FTC's Bureau of Consumer Protection. "But we also want to inform consumers about how they might reduce the amount of unwanted spam in their in-box. The lessons we learned from the spam harvest research project suggest some approaches for consumers who want to keep their e-mail address out of the hands of spammers."

THE FTC CASES:

The FTC charged that one defendant used deceptive spam, including unauthorized use of logos of well-known financial institutions including Radian Bank, Prudential, and Fannie Mae, to induce victims to disclose sensitive financial information such as income, mortgage balances, and home values. The spammers purported to offer consumers competitive financing and refinancing loans. The defendants also allegedly forged e-mail headers - a technique known as "spoofing," - so that any undeliverable messages went to e-mail addresses unaffiliated with the defendants. One unaffiliated third party was swamped with more than 30,000 bounce-back and angry "do not spam me" e-mails intended for the defendants. The FTC also alleged that the defendants deceptively claimed that consumers who received their solicitations could opt out of future offers. The FTC charged the defendants with unfair and deceptive practices, violations of the FTC Act, and with "pretexting,"- posing as an entity it was not in order to get sensitive financial information - a violation of the Gramm-Leach-Bliley Act. This matter was filed under seal. The seal was not lifted by press time.

Related Documents:

"Email Address Harvesting: How Spammers Reap What You Sow"

"Spam Email: Harvesting Your Email Address"

Case Chart

FTC v. GM Funding, Inc., Robert Damian Kutzner, Global Mortgage Funding, Inc., and Damian Robert Kutzner (Central District of California, Southern Division)

Complaint for Permanent Injunction and Other Equitable Relief [PDF 22KB]

EX Parte Temporary Restraining Order with Asset Freeze and Other Equitable Relief [PDF 1MB]

Stiputated Order of Preliminary Injunction as to Defendants GM Funding, Inc., Robert D. Kutzner, Global Mortgage Funding, Inc., and Damian R. Kutzner [PDF 972KB]

The FTC alleged that NetSource One and James R. Haddaway, operating as WorldRemove, used spam and the Internet to sell a service they claimed would reduce or eliminate spam from consumers' e-mail. The claims were false. In fact, using an undercover account to test the claims, the FTC found it received more spam after signing up for the service. The agency charged the defendants with violations of the FTC Act.

Brian Silverman, doing business as BES Systems, Electro Depot, Dallas Tech Surplus, and New York Tech Surplus offered laptop computers for sale via Internet auction houses, including eBay. The FTC alleges that Silverman accepted only cash, checks, or money orders for payment from winning bidders. In many instances he failed to provide the computers or provide refunds to his victims, the agency alleged. The FTC charged him with violating the FTC Act and the Mail or Telephone Order Merchandise Rule.

Four individuals who used spam to promote chain e-mail schemes have settled FTC charges that their schemes were illegal. In February 2002, the FTC sent warning letters to more than 2,000 spammers whose chain-letter spam also contained deceptive claims that the FTC's Director of Marketing Practices could vouch for the illegal pyramid's legality. The agency used its spam database, which contains more than 20 million unsolicited commercial e-mails, to identify individuals who had received warnings and who continued to send the messages. Undercover investigators sent money to Jessica Drees, Heidi Freitas, Rosaline Leahy, and Nancy Merrill, who accepted the payments. Settlements will bar their participation in illegal chain letter schemes in the future.

Ten NetForce partners signed letters that were sent to100 spammers who send similar chain letter or pyramid scheme e-mails that warned the spammers that their activities are illegal and may prompt law enforcement actions.

The Spam Harvest

In an effort to determine what online activities place consumers at risk for receiving spam, Northeast Netforce investigators "seeded" 175 different locations on the Internet with 250 new, undercover e-mail addresses and monitored the addresses for six weeks. The sites included chat rooms, newsgroups, Web pages, free personal Web-page services, message boards and e-mail service directories. One hundred percent of the e-mail addresses posted in chat rooms received spam; the first received spam only eight minutes after the address was posted. Eighty-six percent of the e-mail addresses posted at newsgroups and Web pages received spam; as did 50 percent of addresses at free personal Web page services; 27 percent from message board postings; and nine percent of e-mail service directories.

Spam Harvest partners also found that the type of spam received was not related to the sites where the e-mail addresses were posted. For example, e-mail addresses posted to children's newsgroups received a large amount of adult content and work-at-home spam.

Help For Consumers

Results of the harvest indicated that spammers use different methods, as well as different sources, to seize consumers' e-mail addresses. Consumers who receiving large amounts of objectionable spam may want to change their e-mail address and follow some safer surfing tips suggested in the FTC's publication, "E-mail Address Harvesting: How Spammers Reap What You Sow," available online at http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm.

- Consider "masking" your e-mail address.

"johndoe@myisp.com" could be masked as "johndoe@spamaway.myisp.com."

- Use a separate screen name for online chatting.
- Set up disposable e-mail addresses for discrete projects.
- Use two e-mail accounts - one for public posting, one for personal messages.
- Use a unique e-mail address, containing both letters and numbers.

In addition to the FTC, members of the Northeast Netforce include: The Connecticut Attorney General, the Maine Attorney General, the Massachusetts Attorney General, the New Hampshire Department of Justice, the New Jersey Division of Consumer Affairs, the New York City Department of Consumer Affairs, the New York State Attorney General, the New York State Consumer Protection Board, the Rhode Island Attorney General, the United States Attorney for the District of Massachusetts, the United States Postal Inspection Service, and the Vermont Attorney General.

The Commission votes to file the complaints and accept the consent settlements were 5-0.

NOTE: The Commission files a complaint when it has "reason to believe" that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. The complaint is not a finding or ruling that the defendant has actually violated the law. The case will be decided by the court.

Copies of the complaints and consents are available from the FTC's Web site at http://www.ftc.gov and also from the FTC's Consumer Response Center, Room 130, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. Copies of the FTC publication, "E-Mail Address Harvesting: How Spammers Reap What You Sow," can be found at http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm. Additional information about spam can be found at http://www.ftc.gov/spam. The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on any of 150 consumer topics, call toll-free, 1-877-FTC-HELP (1-877-382-4357), or use the complaint form at http://www.ftc.gov. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

MEDIA CONTACT:

Claudia Bourne Farrell,

Office of Public Affairs

202-326-2181

STAFF CONTACT:

Barbara Anthony or Cindy P. Kapadia,

FTC's Northeast Region

212-607-2829

or

Eric Wenger or James Kohm,

Bureau of Consumer Protection

202-326-2310 or 202-326-2640

(FTC File No. 022-3234 Jessica Farrah Drees)
(FTC File No. 022-3235 Heidi H. Freitas)
(FTC File No. 022-3236 Rosaline Leahy)
(FTC File No. 022-3237 Nancy H. Merrill)
(FTC File No. 022-3077 NetSource One and James R. Haddaway)
(FTC File No. 022-3302 Brian Silverman, d/b/a BES Systems)

Federal, State, and Local Law Enforcers Tackle Deceptive Spam and Internet Scams

(http://www.ftc.gov/opa/2002/11/netforce.htm)