Federal Trade Commission Anti-Spam Efforts

Spam Technology Workshop

National Institute of Standards and Technology

February 17, 2004

About this Presentation

The views expressed in this presentation are those of the speaker and not necessarily those of the FTC or its staff

The FTC, the Internet, and Spam

- Independent civil law enforcement agency
- Active in online matters since 1994
- Interested in spam since 1998
- Active campaign of research, education, and enforcement
- "CAN-Spam" Act gives us additional responsibilities

FTC Research and Education

- **"Remove Me" Surf:** Do spammers honor requests to be removed from mailing lists?
- **"Spam Harvest":** Where do spammers get people's email addresses?
- **"False Claims in Spam" Study**
- **FTC Spam Forum**
- **Operation Secure Your Server:** Worldwide effort to close spammers' access to anonymity
- **Public and business education brochures**

FTC's "Remove Me" Surf

- FTC tested 215 spam messages with "remove me" claims– "Click here [or reply] to be removed from mailing list"
- 63% of these links and reply options did not function
- Contrary to a common belief, trying to opt out did *not* result in a greater volume of spam received
- Spammers making false "remove me" claims received a warning from the FTC & law enforcement partners that such claims may violate the FTC Act.

FTC's "Spam Harvest" Project

- Spammers scan the Internet for email addresses: capturing addresses this way is known as "harvesting."
- The FTC placed email addresses throughout the Internet to see which places were harvested most often.
- 1 address received spam 8 minutes after it was posted in a chat room. ALL addresses placed in chat rooms got spam.
- 86% of addresses posted on websites and newsgroups received spam, even though some addresses were placed only in source code and weren't visible on the sites.

FTC Study: False Claims in Spam

- The FTC's study found that 66% of a spam sample contained signs of falsity in the from line, subject line, or text.
- Falsity in the from line revealed spammers' desire to mask their identity.
- Falsity in the subject line showed that spammers use deception to get recipients to open and read their messages.
- Falsity in the text was designed to trick consumers into falling for worthless offers.

FTC Spam Forum

- 87 panelists in 3 days of discussions in April and May, 2003: spam advocates and opponents, marketers, technologists, law enforcement, and international regulators
- Emphasis on mechanics and costs of spam, and potential solutions to spam
- Unique effort to gather all stakeholders in one room.

Operation Secure Your Server

- International law enforcement efforts to notify owners of open relays and open proxies of spam-related consequences.
- Spammers use these servers to send spam anonymously and avoid anti-spam filters.
- To date, 26 international law enforcement agencies have contacted over 25,000 open relay/proxy owners in 21 languages.

FTC Enforcement Against Spammers

- To date, the FTC has filed over 55 spam-related cases.
- We have sued spammers for deceptive *content* and deceptive and unfair spamming *techniques*

Spam Database

- uce@ftc.gov
- Established 1998
- Almost 87 million received as of 2/10/04
- Messages indexed using RetrievalWare
- Headers parsed with scripts
- Available for full text searching in HQ Internet Lab and FTC regional offices

FTC Enforcement Against Spammers

- Our spam-related cases have targeted:
  - **Chain E-Mail**
  - **Email "spoofing"–** forging the sender's identity
  - **"Phishing"–** spam used to engage in identity theft
  - Failure to honor a **"remove me"** claim
  - **Subject lines and from lines** that deceive recipients into opening a message they would have deleted
  - **False claims** in spam offering anti-spam services and spam-related business opportunities.

Law Enforcement Partnerships

- Net Force: our regional law enforcement and education campaigns in 2002-03 that included cases targeting spam
- Spam Task Force: New partnership between FTC, other federal agencies, and states to share expertise and information in investigations targeting spammers

CAN-SPAM Act of 2003

("***C***ontrolling the ***A***ssault of ***N***on-***S***olicited ***P***ornography ***a***nd ***M***arketing ***Act***")

- Commercial as primary purpose
- Effective date of January 1, 2004
- Creates civil and criminal violations
- May be enforced by federal and state law enforcement and ISPs
- Directs the FTC to establish rules, conduct studies, write reports

CAN-Spam Act: New Civil Violations

- False or misleading header information
- Deceptive subject lines
- Failure to provide an opt-out method and honor opt-out requests
- Failure to include:
  - Identification that the message is an advertisement
  - Sender's valid physical postal address
- For "sexually oriented" messages:
  - Failure to include warning label (to be created by FTC)
  - Failure to require additional steps to view material after opening message

CAN-Spam Act: New Civil Violations

- Aggravated violations for spam *plus*:
  - Harvesting
  - Dictionary attack
  - Using someone else's computer without their authorization
  - Automated creation of multiple email accounts
- FTC may specify other aggravated violations to cover practices contributing to the spam problem

CAN-Spam Act: New Rules, Studies & Reports

- Additional rules interpreting certain CAN-Spam provisions
- Studies
  - Do-Not-Email Registry: Authorized, but not required
  - Special labeling of sexually explicit spam
  - Labeling of all spam
  - Bounty system to promote enforcement
- Report to Congress due in 2 years

CAN-Spam Act: Civil Enforcement
Federal

- FTC Enforcement:
  - Similar to FTC Act enforcement: Cease & desist orders and injunctive relief without proving knowledge
  - Plus, civil penalties up to $11,000 per violation: must show actual knowledge or knowledge fairly implied
- Other federal regulators can enforce the Act against entities outside FTC jurisdiction
- FCC will oversee regulation of wireless spam

CAN-Spam Act: Civil Enforcement
State and Private

- State Enforcement:
  - Injunctive relief
  - Damages: Actual loss or up to $250 per violation ($2 million cap, but not for false or misleading headers)
  - May receive treble damages for willful, knowing or aggravated violations
  - State spam laws are preempted unless they prohibit falsity or deception or are not spam-specific
- ISP Enforcement:
  - Injunctive relief
  - Damages: Actual loss or up to $25 per violation ($1 million cap)
    - For false or misleading headers, up to $100 per violation and no cap
  - May receive treble damages for willful, knowing or aggravated violations
  - No private claim for spam recipient

CAN-Spam Act: New Criminal Violations

- New criminal violations for spam-related unauthorized access and spoofing, and false header and email account information
- Criminal penalties include imprisonment and forfeiture of assets

Tech Solutions?

- Consumers and Systems
  - Protection
- Law Enforcement
  - Identification

www.ftc.gov/spam

- Don M. Blumenthal, Esq.
- Internet Lab Coordinator
- Federal Trade Commission
- 600 Pennsylvania Ave., N.W., Room H292
- Washington, DC 20580
- 202-326-2255
- dblument@graywolf.ftc.gov