



WHITE PAPER

Glossary of Spam Terms

THE JARGON OF THE SPAM INDUSTRY

Table of Contents

A	
Acceptable Use Policy (AUP)	5
Alias	5
Autoresponder	5
B	
Ban on Spam	5
Bayesian Filtering	5
C	
CAN-SPAM	5
Catch Rate	5
CAUSE	5
Challenge Response Authentication	6
Checksum Database	6
Click-through	6
Content Filtering	6
Crawler	6
D	
Denial of Service (DoS)	6
Dictionary Attack	6
DNSBL	6
E	
EC Directive	7
E-mail Bomb	7
Exploits Block List (XBL) (from Spamhaus.org)	7
F	
False Negative	7
False Positive	7
Filter Scripting	7
Fingerprinting	7
Flood	7
H	
Hacker	8
Header	8
Heuristic Filtering	8
Honeypot	8
Horizontal Spam	8

I	
Internet Death Penalty	8
Internet Service Provider (ISP)	8
J	
Joe Job	8
K	
Keyword Filtering	9
Landing Page	9
LDAP	9
Listwashing	9
M	
Machine-learning	9
Mailing List	9
Mainsleaze	9
Malware	9
Mung	9
N	
Nigerian 419 Scam	10
Nuke	10
O	
Open Proxy	10
Open Relay	10
Opt-in	10
Opt-out	10
P	
Pagejacking	10
Phishing	10
POP3	11
Pump and Dump	11
Q	
Quarantine	11
R	
RBLs	11
Reverse DNS	11
ROKSO	11
S	
SBL	11
Scam	11
Segmentation	11
SMTP	12
Spam	12
Spambot	12
Spamhaus	12
Spamming	12

Spamware	12
SPEWS.....	12
Spider.....	12
Spim.....	12
Spoof.....	12
Spyware.....	12
T	
Training Set.....	13
Trojan Horse	13
Trusted Senders List.....	13
U	
UCE.....	13
W	
Whack-A-Mole	13
Worm.....	13
V	
Vertical Spam.....	13
Z	
Zombie.....	13

A

Acceptable Use Policy (AUP)

A policy statement, made by an ISP, whereby the company outlines its rules and guidelines for use of the account. It also specifies unacceptable uses for the account.

Alias

An alternative name for a mailbox. For example, john.doe@abc.com could create the alias johnny@abc.com.

Autoresponder

A program or a script that automatically sends a response when it receives an e-mail message. The most common uses of autoresponders are for subscribe and unsubscribe confirmations, welcome messages and customer-support questions.

B

Ban on Spam

Nickname given to the anti-spam legislation passed by the European Commission called Privacy and Electronic Communications Directive. More information can be found at http://ec.europa.eu/information_society/policy/ecom/todays_framework/privacy_protection/spam/index_en.htm

Bayesian Filtering

Based on Thomas Bayes' theorem, Bayesian filtering calculates the probability of a message being spam, based both on its content and on past results, to distinguish legitimate e-mails from spam. The theorem states that "the probability that an e-mail is spam, given that it has certain words in it, is equal to the probability of finding those certain words in spam e-mail, times the probability that any e-mail is spam, divided by the probability of finding those words in any e-mail"¹.

C

CAN-SPAM

Acronym for Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003. Anti-spam legislation passed by the United States of America.

Catch Rate

The catch-rate measures the efficiency of a Spam solution. The calculation used is: (# of Spam messages caught / total # of Spam messages) x 100.

CAUCE

The Coalition Against Unsolicited Commercial E-Mail. A non-profit organization that attempts to reduce spam by creating and/or amending spam legislation worldwide.

1. See Wikipedia article Bayesian spam filtering, http://en.wikipedia.org/wiki/Bayesian_spam_filtering/

Challenge Response Authentication

An authentication technique whereby an unrecognized sender is prompted (the challenge) to provide some private information (the response) in order for his/her e-mail to be delivered to the recipient.

Checksum Database

Early spam blocking method that assigned a unique identifier to each spam message found and then built a database of these identifiers so that incoming e-mail could be compared with the contents of the database.

Click-through

A web page that exists merely to redirect users to another site. Spammers typically create click-through pages on throw-away accounts and advertise the click-through page. The Click-through Rate (CTR) is used to calculate the how often the web page is visited.

Content Filtering

Spam scanning plain text for key phrases and the percentage of HTML, images and other indications that the message is spam.

Crawler

See Bot

D

Denial of Service (DoS)

An attempt to make a computer resource unavailable to its intended users. Considered an Internet crime.

Dictionary Attack

A system of combining letters and numbers in an attempt to find active e-mail addresses. Any addresses to which messages are delivered, as opposed to being bounced back, are legitimate.

DNSBL

DNS Black List or DNS Blackhole List. An online list of e-mail spam sites that may be used for e-mail spam filtering, either on a personal basis or on an entire domain. Sites are added to DNSBLs when spam becomes a problem and are removed once the problem is resolved. Typically, there are two types of DNSBLs: Exploit-Targeting blacklists (i.e.: list of open relays, open proxies, etc.) and Spammer-Targeting blacklists (Spamhaus SBL and Spamcop are typical spammer-targeting lists).

E

EC Directive

Nickname given to the spam legislation passed by the United Kingdom, called The Privacy and Electronic Communications Regulation 2003.community.

E-mail Bomb

Act of sending copious amounts of e-mail in an attempt to overflow a mailbox or crash the mail server. It can also be used to describe an e-mail message with an attached ZIP file that contains a ZIP, which contains another ZIP file and so on. An e-mail bomb can block scanning engines and cause a DoS, for example.

Exploits Block List (XBL) (from Spamhaus.org)

A real-time DNS-based database of illegal 3rd party exploits IP addresses, including open proxies, spam messages with built-in worms/viruses and other types of Trojan-horse exploits utilized by spammers.

F

False Negative

The result of an anti-spam engine failing to identify a spam message and letting it through to a user's inbox.

False Positive

Legitimate mail is incorrectly recognized by a spam solution and not delivered to a mail inbox. Filter An e-mail security solution feature that scans e-mail messages based on the analysis of their structure and/or contents.

Filter Scripting

An anti-spam filtering method that uses a programming language (such as Vircom's Sieve) to write generic and/or specific filters to block spam.

Fingerprinting

[E-mail] Technology that identifies similar, but not identical, messages as part of the same, already identified spam broadcast. [File] Smart file type detection. A technology that scans e-mail attachments in search of forbidden file formats (e.g. *.exe) in order to prevent them from concealed with modified file extensions.

Flood

Large quantities of email sent to an Internet / e-mail server in a short amount of time.

H

Hacker

A malicious or criminal programmer who infiltrates computer systems or creates e-mail-borne malware such as viruses.

Header

The top portion of an e-mail that contains the sender's name, date the message was sent, recipients' names, title, routing details, message priority, and other structural information.

Heuristic Filtering

A spam filtering technique, based on mathematical models and rules, which determines the likelihood of an e-mail message to be spam or legitimate.

Honeypot

A program disguised as a legitimate resource (open proxy or mail relay) to gather information about spammers and their activities.

Horizontal Spam

Spam messages sent to the greatest number of recipients regardless of their relevance to the recipient.

I

Internet Death Penalty

Extreme situation whereby all traffic from a domain that hosts spammers is blocked at the packet level, essentially shutting the domain off from the rest of the Internet.

Internet Service Provider (ISP)

A company that provides access to the Internet to consumers.

J

Joe Job

A spam attack that uses a spoofed or forged sender address, often as an act of revenge. Joe-job attacks result in non-delivery reports, out-of-office notices, challenge-responses, auto-responders, etc. which are generated with the forged sender address. The barrage of spam can often sully the sender's reputation and incur the wrath of the unfortunate recipients.

K

Keyword Filtering

Filtering spam based upon keywords in the header or body of the message.

L

Landing Page

A web page that upon which a person lands after clicking on a link or advertisement, often part of a spam message.

LDAP

Lightweight Directory Access Protocol. Standard protocol for the exchange of directory entries between servers.

Listwashing

The process of removing individual e-mail addresses from an address list, which usually contain addresses of people who have not chosen to subscribe to the list.

M

Machine-learning

A sub-field artificial intelligence. Machine learning automatically extracts information from data and, in the context of spam filtering, creates and updates heuristic checklists.

Mailing List

A type of Internet forum. A set of e-mail addresses used for widespread distribution of information or information sharing. Individuals must subscribe to the mailing list to participate.

Mainsleaze

A term used to describe a credible or legitimate company that spams or uses third parties to spam on its behalf.

Malware

A combination of malicious and software. It is software or scripts designed to harm computers, networks and systems. Examples are viruses, worms, trojans and spyware.

Mung

To obscure or modify an e-mail address so that automated e-mail address harvesters cannot obtain valid e-mail addresses. The address is munged from a computer's perspective but not a human's.

N

Nigerian 419 Scam

An advance fee fraud. Solicits and attempts to persuade people to advance money to the sender while promising a huge gain. The sender is usually in dire straits and the message is often a plea for help. Recipients are asked to provide personal information such as their bank account numbers.

Nuke

Refers to an ISP canceling a user's account. Also a DoS.

O

Open Proxy

A proxy that allows computers to use it to make connections to services on their behalf, whether they would normally have permission to access the service or not.

Open Relay

An SMTP (mail) server configured in such a way that it allows anyone on the Internet to relay (i.e. send) mail through it. Often open to attack and hijacked to send large amounts of spam.

Opt-in

The option to receive bulk e-mail (like subscribe). This is typically a newsletter or advertising from companies. Failure to obtain permission to send the bulk messages is important because, without it, the message is considered spam.

Opt-out

The option to discontinue receiving bulk e-mail (like unsubscribe). There is a possible risk that the opt-out feature may actually be confirming the e-mail address instead of opting out of the bulk e-mail.

P

Pagejacking

A form of spamming a search engine's index (spamdexing) whereby spammers make a copy of a website and use it to redirect surfers to malicious websites.

Phishing

A scam that uses spam to deceive people into disclosing their credit card numbers, bank account information, passwords and other sensitive information. Phishers often masquerade as trustworthy or wellknown businesses.

POP3

Post Office Protocol version 3. A standard mail protocol for authenticating and retrieving mail over the Internet. Unlike IMAP (where mail resides on the server), POP3 moves messages from the server to the users' computers

Pump and Dump

A spammers' twist on the stock scam. Involves the touting of a company's stock through false, and often, misleading statements to the marketplace. After pumping the stocks' value, spammers make huge profits by selling (dumping) their shares at inflated prices

Q

Quarantine

Mail that has been blocked because of suspicious content, viruses or forbidden attachments, usually sent to a quarantine folder.

R

RBLs

See DNSBL.

Reverse DNS

A process to determine the hostname associated with a given IP address. This feature ensures that users are from legitimate domains.

ROKSO

Register of Known Spam Operations. A database, maintained by Spamhaus.org, of professional spam operations that have been terminated by a minimum of 3 Internet Service Providers for spam offenses².

S

SBL

Spamhaus Block List. A real-time database of IP addresses of spam-sources, including known spammers, spam gangs, spam operations and spam support services.³

Scam

A fraudulent or deceptive act.

Segmentation

Dividing an e-mail list based upon interest categories, purchasing behavior, demographics and more for the purpose of targeting specific e-mail campaigns to an audience most likely to respond to the messaging or offer.

²www.spamhaus.org

³www.spamhaus.org

SMTP

Simple Mail Transport Protocol. The protocol used to deliver mail to its destination.

Spam

Unsolicited, bulk e-mail. Also known as junk mail.

Spambot

A bot designed to collect e-mail addresses from the Internet to be used to build mailing lists for sending spam.

Spamhaus

An Internet Service Provider or other organization that provides service to spammers.

Spamming

The act of sending spam.

Spamware

Any program used by spammers to facilitate their spamming activities. Examples include generating email address lists and make use of open relays.

SPEWS

Spam Prevention Early Warning System. A list of known spam sources and spam-friendly hosts. For more information, go to <http://www.spews.org/>.

Spider

See Bot.

Spim

A type of spam which targets instant messaging.

Spoof

In the context of network security, a spoofing attack is a situation in which a person or program successfully masquerades as another by falsifying data. With phishing, a legitimate Web page (such as a bank's) is reproduced in look and feel by the phisher. The intent is to trick users into thinking that they are connected to a trusted site. The phisher then harvests personal information.

Spyware

Software that is secretly, and without consent, installed on a computer to intercept personal information or to take control of the computer.

T

Training Set

See Machine-Learning.

Trojan Horse

Malicious software that is disguised as being something benign, such as a game.

Trusted Senders List

Also known as whitelist. Anti-spam feature that lets users designate a source or IP address from which all e-mail will be accepted without any scanning.

U

UCE

Unsolicited commercial e-mail. Also known as spam.

W

Whack-A-Mole

Terminating a spammer's throw-away account.

Worm

E-mail borne computer program that replicates itself and that often, but not always, contains some functionality that will interfere with the normal use of a computer or a program.

V

Vertical Spam

A large number of spam messages sent to few recipients.

Z

Zombie

A computer compromised and is being used for malicious purposes. Zombies are often used to send spam.