Glossary - Email Concepts

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

Acceptable Use Policy (AUP)
A policy statement, made by an ISP, in which the company sets out its "rules" for use of the account.

Agent
Outside program, executed via a GWGuardian process. Agents can be executed in various instances, such as when a user receives email, or when a message is sent to a mail list.

Alias
Virtual entry that is redirected to another destination. In GWGuardian, there are two types of aliases: Domain aliases are domain names that are redirected to another domain. Global aliases are email addresses that are redirected to another email address.

Allow List
Allows end users to designate email addresses and domain names from which all mail will be accepted, even if individual messages earn high spam ratings.

APIG
All Party Internet Group - A discussion forum for Parliamentarians and media industry

Auto Responder
A program or a script that automatically sends a response when someone sends a message to its address. The most common uses of auto responders are for subscribe and unsubscribe confirmations, welcome emails and customer-support questions.

B

Ban on Spam
Nickname given to the spam legislation passed by the European Union called "Directive on Privacy and Electronic Communications".

Bayesian Filtering
The use of a statistical theory to calculate the probability of a message being spam, based both on its content and on past results, to separate genuine emails from spam. Bayesian filtering is based upon the work of Thomas Bayes.

Blacklists
Anti-spam feature that allows users to designate a source or IP address from which no email will be accepted.

Bloc/Block List
Lists of spammers created either by internet service providers (ISPs) or by grassroots anti-spam groups.

Blocked Attachment
Any file type attached to an email message that is identified as a potential threat.

Bot
A program or script that automatically browses the World Wide Web in search of specific information (such as email addresses).

Browser Compatibility
The term browser compatibility refers to the fact that web-browsing applications from different companies sometimes display the same web pages with different formatting. This is to say that they interpret the code behind a web page (code which consists of HTML tags) differently. Sometimes these differences are minimal, but unfortunately these interpretational differences can sometimes also mean that you simply cannot view some parts of a website that have used particular HTML code tags because your web browser does not know how to display those parts (which use specific HTML tags).

C

CAN-SPAM
Nickname given to the spam legislation passed by the United States of America.

Catch Rate
The percentage of spam email caught by an anti-spam solution. It measures the efficiency of the solution at identifying and stopping spam.

CAUCE
The Coalition Against Unsolicited Commercial Email. A volunteer organization that is attempting to create / amend spam laws worldwide.

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

Checksum Database
Early spam blocking method that consisted in assigning a unique identifier to each spam message found and then building a database of these identifiers so that incoming email can 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 throwaway accounts and advertise the click-through page.

Content filtering
Scans plain text for key phrases and the percent of HTML, images and other indications that the message is spam.

Cracker
A malicious or criminal programmer who creates email-borne malware such as viruses.

Crawler
A program or script that automatically browses the World Wide Web in search of specific information (such as email addresses).

D

Denial of Service (DOS)
A burst of repeated request intentionally sent to overwhelm a server's CPU power, resulting in total incapacity to treat regular requests.

Dictionary Attack
Common harvesting tactic that consists in automatically requesting likely email addresses to a specific server by combining letters and numbers in an attempt to find, or validate, active email addresses.

Directive
Parameter that can be used to pass context-specific information to an agent or when specifying a message. For instance, in the auto reply message, %DATE is a directive that is substituted for the current date in the actual message.

DNSBL / DNS Black list
DNS Blackhole List - An online database of email spam sites that may be used for email spam filtering, either on a personal basis or on an entire domain. Problem sites are added to DNSBLs almost instantly when spam becomes a problem, and are removed again once the problem is dealt with. DNSBLs typically come in two flavors: Exploit-Targetting blacklists (ie: list of open relays, open proxies, etc ...) and Spammer-Targetting blacklists (The spamhaus SBL and Spamcop are typical spammer-targetting lists). Interchangeable with RBL.

E

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

ESMTP
Extended version of SMTP. Supports protocols for authentication, encryption, message size restrictions and more.

Exploits Block List (XBL)
(from Spamhaus.org) A real-time DNS-based database of IP addresses of illegal 3rd party exploits, 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
The result of an anti-spam engine blocking a legitimate message by error, on assumption that it is spam.

Filter
An email feature that manipulates email messages based on the analysis of their structure and/or contents.

Fingerprinting
Technology that identifies similar, yet not identical, messages as part of the same, already-identified spam broadcast.

Fingerprinting (file)
Technology that scans email attachments in search of forbidden file formats, thus avoiding that a forbidden file (such as *.exe) is concealed using a modified file extension.

Flood
Large quantities of material sent at once to an Internet / email server.

G

H

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

Heuristics
Anti-spam technology based on mathematical models and rules which determine the likelihood of an email message to be spam or legitimate.

Hijacking / Pagejacking

The act of taking control of a third-party system to relay spam or other forms of email malware.

Honeypot
Bogus email address set up to be harvested and spammed in order to gather up-to-date examples of spam.

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

I

Internet Death Penalty
Extreme situation where all traffic from a heavily spamming domain is blocked at the packet level, essentially shutting that domain off from the rest of the internet.

Internet Service Provider (ISP)
A company that provides various Internet connection subscriptions

J

Joejob / Joe
Taking revenge on an anti-spammer by using the anti-spammer's email address as the return address of a spam mailing. The Joe Job victim is then inundated with angry responses and server delivery messages.

K

Keyword Filtering
A technology that filters spam based upon keywords in the header or body of the message.

L

Landing Page
A web page that is linked to an email for the purpose of providing additional information directly related to products or services promoted in the email.

LDAP
Lightweight Directory Access Protocol - A client/server protocol for accessing information in network directories such as Novell Directory Services (NDS), Microsoft Active Directory, or directories that follow the X.500 standard. It is the standard protocol for the exchange of directory entries between different servers.

LDIF
LDAP Data Interchange Format. The format used by an LDAP server when returning information for LDAP requests.

List Address
A single address that has multiple members who will all receive messages sent to the list address.

Listwashing
The process of removing email addresses from an address list rather than deleting the list entirely.

M

Machine-learning
Ability of certain anti-spam technologies, such as Bayesian filtering, to self- create and update their own heuristics checklist.

Mail Bomb / Bombing
Act of sending massive email bursts to a server up until the time a server or account crashes because of treatment overload.

Mailing list
A special collection of email addresses. When an email is sent to a mail list, it is distributed to all recipients on the list.

Mainsleaze
A mainstream company that actually spams or uses third parties to spam on its behalf.

Malware
Malicious software or scripts intentionally created to harm networks and systems. Includes viruses, worms and trojans.

Munge
To modify an email address in such a way that address harvesters won't get a usable address, but humans are still able to interpret it (john.smithatcompany.com) .

N

Nigerian 419 Scam
The scam involves the recipient receiving a fake email from a supposed official in Nigeria or some other country who, in return for an "advanced fee" or "Transfer Tax", will share in their wealth with the sender. Recipients are asked to give their bank account information so they can wire the money, which leads to the bank account being emptied.

Nuke

Refers to an ISP canceling a user's account.

O

ODBC
Open Database Connectivity. ODBC is an application programming interface (API) used to access third-party databases.

Open Proxy
A proxy that will allow other machines to use it to make connections to services on its behalf, whether they would normally have permission to access the service or not.

Open Relay
An email server processing mail where sender and receiver are not local users. Such servers are often open to attack, and are sometimes hijacked and used to send large amounts of spam.

Opt-in
Email advertising lists in which recipients are signed up without their knowledge or permission, but may request to be removed from.

Opt-out
Email advertising lists in which recipients are signed up without their knowledge or permission, but may request to be removed from.

P

Phishing
A high-tech scam that uses spam to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive information.

POP3
Post Office Protocol version 3 - The most common protocol for authentication and transmission of email messages over the Internet.

Pre-existing Business relationship
The recipient of the email has purchased, requested information, responded to a questionnaire or a survey, or had offline contact with you.

Pump and dump
A spammers' twist on the stock scam. A spammer sends out thousands of emails touting a stock. If enough people buy the stock, the price goes up, and then the spammer dumps the stock at a profit.

Q

Quarantine
Storage of suspected spam or malware-carrying email. Quarantines usually notify users of the presence of email and allow them, at various levels, to read / release the messages without risking harm to their computer.

Quarantine Report
A quarantine report is an administrator-sent email message that allows end user to see how many email messages containing viruses, spam, blocked attachments or other filtered mail have been withheld from the end user’s Inbox. The quarantine report contains a URL link in the body of the email message to allow end users to manage their own quarantined email in the web-based M+Quarantine application.

R

RBLs™(DUL/MAPS)
RBL or Real-Time Blacklist is the trademark term used by DUL/MAPS. The Generic term for DNS-based blacklists in current use is DNSBL.

Revenge / Malicious Spam
Spam that contains a third person's identification in the header or message body and that is deliberately sent to harm this person's reputation.

Reverse DNS
A method that consists in verifying the DNS (address) of a sender before accepting the message for delivery by using the PTR record of the ip addresses from which the message is sent.

Robot
A program or script that automatically browses the World Wide Web in search of specific information (such as email addresses).

ROKSO
Register of Known Spam Operators - (from Spamhaus.org) A list of known spammers or spam gangs.

S

SBL
Spam Block List.

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

SMTP
Simple Mail Transfer Protocol, the basic "language" that e-mail servers use to communicate across the internet.

Spam
Unsolicited, unwanted, bulk, commercial email.

Spambot
A robot that specializes in gathering email addresses for a spammer to use. It basically follows links and saves any email addresses it finds as it goes along.

Spamware
Any kind of material used for spamming.

Spim
Spam in the instant messaging world.

Spoofing
The practice of forging a return email address.

Spyware
Software that transmits information back to a third party without notifying the user.

T

Trojan (Horse)
A malicious, security-breaking program that is disguised as something benign, such as a game.

U

UCE(M)
Unsolicited commercial email, the acronym for spam.

V

Vertical Spam
A large number of spam messages sent to few recipients.

Virus
Any piece of code that has built-in, automatic replication and propagation methods. Viruses usually deliver a payload, or piece of malicious code that carries out some destructive operation on the host machine.

W

Whack-A-Mole
An action where a spammer, whose IP address has been blocked because of spamming, jumps to another IP address or subnet to evade blocking.

Whitelist
Anti-spam feature that lets users designate a source or IP address from which all email will be accepted without any scanning.

Worm
Email-carried 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.

X

Y

Z

Zombie / Zombie Drone
A computer which has been hacked into and is being used by the hackers to launch an attack or spam at other computers.

Back to top