



Contact Information:
Bill Reimann
breimann@securence.com
952-253-3219
www.securrence.com

Glossary of Terms Related to Spam

Address Harvester: A program that searches web pages and filters newsgroup postings looking for valid email addresses to be used for spam purposes. (See also harvesting.)

Bayesian Filtering: A statistical approach to determining whether an email is spam, based on probability inference techniques pioneered by English mathematician Thomas Bayes.

DNS Black List (dnsBL): Same as RBL (see below).

Blacklist: A feature of anti-spam software that allows users to designate IP addresses, domain names, and individual email addresses from which no mail will be accepted. This is sometimes called a "Static Black List" because the user defines the list.

Complex Dictionary Checking: A feature of anti-spam software that screens text for rude words and isn't fooled by various spam tricks, such as the replacement of letters with look-alike numerals or characters (such as "1nterestr@te").

CSS Spam: Exploits Cascading Style Sheets (CSS), which are used to control the display of web pages, in order to conceal messages in spam. Spammers can also use CSS to recycle old HTML-based tricks that fool spam filters who don't understand CSS.

Denial of Service (DoS) Attack: Where a hacker sends attachments or other unusual or excessive traffic in an attempt to bring down email systems.

Dictionary Attack: A program that bombards a mail server with millions of alphabetically generated email addresses in the hope that some addresses will be guessed correctly. This technique is also used to crack passwords.

Directory Harvest Attack (DHA): When a spammer bombards a domain with thousands of generated email addresses in an attempt to collect valid email addresses from an organization. (See also harvesting.) In order for this to be a harvest, there must be a way to trick the system into telling the spammer which email addresses are valid and which are not. This exploits flaws in the mail systems to tell the spammer this information.

False Negative: When anti-spam software fails to identify a spam message as spam.

False Positive: When anti-spam software wrongly identifies a legitimate message as spam.

Greylist: Senders who are not blacklisted (excluded) or whitelisted (accepted) can be placed on a greylist. Some anti-spam software can send greylisted addresses an automated response, challenging the sender to confirm their legitimacy. ...or items that are greylisted might be dealt with more cautiously.

Ham: All email that a recipient does not consider to be spam. (See also spam.)

Harvesting: The process of scanning the internet to identify email addresses in order to create lists for spamming.

Honeypot: A computer system on the internet set up to attract and trap spammers and hackers. Sometimes this is a mailserver set up to appear to be an open relay. We use honeypots in the form of email addresses that don't belong to real people, and then spammers are encouraged to spam these boxes.

Joe Job: Circa 1996, a Joe Job is spam run forged to appear as though it came from an innocent party, who is then generally flooded by the bounces; or, the act of performing such a run. Modern Joe Jobs involve forged email headers and other nasty tricks to make it really convincing. And with the advent of dnsBLs like SPEWS (The Spam Prevention Early Warning System) and peoples' personal lists, a successful Joe Job can really hurt the victim.

Listwashing: The process of removing email addresses from a mailing list at the request of the recipient.

Mail Drop: An email address set up to receive email resulting from spam sent from a different ISP. The spammer will cancel the account from which the spam originated in an attempt to avoid detection.

Munging: A technique to protect email addresses from harvesting by changing them and rendering them invalid. Recipients of an email from a 'munged' address are told how to decode it, so that they can then reply to a valid address. (See also obfuscation.)

Morph: A method that a spammer uses to avoid detection by anti spam software that involves modifying an email header.

Mousetrapping: A technique that page-jackers use that trick the user into visiting an illegitimate site, and after doing so, when trying to leave, they encounter only additional, unwanted pages.

NDR Spam: Uses a faked standard email non-delivery report (NDR) that a recipient will think is genuine, tricking them into opening an attachment that is spam. Spammers can send such an NDR directly or make a legitimate server send it for them, adding to its credibility.

Network Check (also known as reverse DNS check): When an anti-spam engine uses a Domain Name System to check an email's IP address to ensure that it originated from a valid domain name or web address.

Newsgroup: An electronic forum where readers post articles and follow-up messages on specified topics. Newsgroups are often targeted by spammers seeking to harvest email addresses.

Obfuscation: When spammers attempt to hide data to prevent its detection. This also occurs when email recipients use HTML or JavaScript to obscure mailto links and email addresses so that addresses remain readable and clickable, but cannot be harvested. (See also Munging.)

Open relay: An SMTP email server that allows the third-party relay of email messages. The relay feature is a part of all SMTP-based servers and it has legitimate uses, but spammers have learned how to locate unprotected servers and hijack them to send spam.

Opt-in: The process of agreeing to receive email from a business source. Double opt-in refers to a double-check procedure in which a decision to be included on a mailing list is confirmed.

Opt-out: The process of declining to receive email from a business source or unsubscribing if the recipient is already on a mailing list.

Page-jacking: This involves stealing the contents of a website by copying some of its pages, placing them on a site that appears to be legitimate, and having the contents indexed by major search engines, so that unsuspecting users can be tricked into linking to the illegitimate site. (See also Mousetrapping.)

Phishing: Pronounced “fishing,” this involves creating a replica of a legitimate web page to hook users and trick them into submitting personal or financial information or passwords.

Phreaking: This involves illegally breaking into the telephone network to make free long-distance phone calls or to tap phone lines. This term is also used to include the act of breaching the security of any network.

Ratware: Software that spammers use to automate spam campaigns, coordinate spam services, and generate, send and track spam messages.

Real-time Black List (RBL): A publicized list of IP addresses known to be sources of spam, which can be used to create a network blacklist to filter out mail originating from these addresses. (See dnsBL.)

Spam: All unsolicited commercial email (UCE) and unsolicited bulk email (UBE) that a recipient does not want to receive. (See also CSS spam, NDR spam and ham.)

Spambot: A program that spammers use to harvest email addresses from the internet.

Spam Trap: An option in an online form that is pre-selected by default, so that unwary users opt-in to receive spam. It can also be used to refer to a software filter that blocks email addresses known to send spam.

Spoofing: When spammers forge an email address to hide the origin of a spam message. Email scammers and virus writers also use this trick. Scammers spoof address lines to fool people into thinking an email has arrived from a legitimate source, such as an online bank. Similarly, virus writers have passed off viruses as security patches by spoofing their origin as being, for example, from Microsoft technical support.

Tarpitting: The use of traffic monitoring to identify remote IP addresses sending a suspiciously large volume of email. Access to the mail system from suspected spam addresses can then be slowed or temporarily suspended.

Teergrube (or tarpit): An intentionally slow server that aims to trap spammers using harvesting programs.

Web Bug: A Web Bug is small graphic that is inserted in an email or web page that alerts a spammer when a message is read or previewed.

Whitelist: A list of external email addresses, IP addresses, and domains trusted by the entire organization or individual users. All mail from these addresses is delivered, bypassing the spam filters.

Note: Just like blacklists, there are four terms that map to analogous black list terms:

- **RWL** – Real-time white list. These are lists of IP addresses that have somehow been verified to be from a known good host. Often to be on a RWL, companies will pay to be listed and there may be a penalty if they do send spam.
- **DNSWL** – same as RWL
- **Whitelist** – a user-defined list of email addresses, hosts, domains, subjects, etc.
- **Static Whitelist** – same as Whitelist

Zombie

An insecure web server or computer that is hijacked and used in an DoS Attack or to send spam.