Terms and other related definitions.

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.

Blackhole list
A publicised list, usually commercial, 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.

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.

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 lookalike " numerals or characters (such as "1nterest r@te").

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 organisation.

Domain Name System blackhole list (DNSBL)
Commerical lists of networks that either allow spammers to use their systems to " send spam, or have not taken action to prevent spammers from abusing their " systems.

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.

Hacker
Someone who intentionally breaches computer security, usually to cause " disruption or gain confidential information such as financial details.

Ham
All email that a recipient does not consider to be 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. Usually this is a mailserver set up to appear to be an open relay.

Listwashing
The process of removing email addresses from a mailing list at the request of " the recipients.

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.

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

Mousetrapping
A technique that page-jackers use, so that users " tricked into visiting an illegitimate site encounter only additional, unwanted " pages when they click the Back button to try to escape.

Network check (also known as reverse DNS check)
When an anti-spam engine uses a Domain Name System database 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. Often targetted by spammers seeking to harvest email addresses.

Obfuscation

Spammers' attempts to hide data to prevent its detection. Also, 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.

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.

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.

Real-time blackhole list (RBL)
This differs from a blackhole list in that it " actively boycotts TCP/IP addresses known to send spam or host spammers. Enabling " such a list results in all mail from those addresses being refused, including " valid email. This can, however, result in innocent users complaining to their " ISPs and those ISPs enacting stronger anti-spam measures in order to get the RBL " ban lifted.

Social engineering
Conning email recipients into opening messages, revealing passwords or providing " other confidential information by appealing to their curiosity, gullibility or " computing naivety.

Spam
All unsolicited commercial email (UCE) and unsolicited bulk email (UBE) that a " recipient does not want to receive.

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

Spam trap
An option on 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.

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 small graphic 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 organisation or individual users. All mail from these addresses is " delivered, bypassing the spam filters.

Zombie

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