

Spam

Spam

Spam, also known as "bulk e-mail" or "junk e-mail," is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail. A common synonym for spam is unsolicited bulk e-mail (UBE). Definitions of spam usually include the aspects that email is unsolicited and sent in bulk."UCE" refers specifically to "unsolicited commercial e-mail."

E-mail spam slowly but exponentially grew for several decades to several billion messages a day. Spam has frustrated, confused, and annoyed e-mail users. Laws against spam have been sporadically implemented, with some being opt-out and others requiring opt in e-mail. The total volume of spam (over 100 billion emails per day as of April 2008) has leveled off slightly in recent years, and is no longer growing exponentially. The amount received by most e-mail users has decreased, mostly because of better filtering. About 80% of all spam is sent by fewer than 200 spammers. Botnets, networks of virus-infected computers, send about 80% of spam. The cost of spam is borne mostly by the recipient, so it is a form of postage due advertising.

E-mail addresses are collected from chat rooms, websites, newsgroups, and viruses which harvest users' address books, and are sold to other spammers. Much of spam is sent to invalid e-mail addresses. ISPs have attempted to recover the cost of spam through lawsuits against spammers, although they have been mostly unsuccessful in collecting damages despite winning in court.

A KMail folder of spam messages.

From the beginning of the Internet, sending of junk e-mail has been prohibited, enforced by the Terms of Service/Acceptable Use Policy (ToS/AUP) of internet service providers (ISPs) and peer pressure. Even with a thousand users junk e-mail for advertising is not tenable, and with a million users it is not only impractical but also expensive, costing businesses in the order of \$100 billion in 2007. As the scale of the spam problem has grown, ISPs and the public have turned to government for relief from spam, which has failed to materialize.

Types of spam

Spam has several definitions, varying by the source.

1. Unsolicited bulk e-mail (UBE)—unsolicited e-mail, sent in large quantities.
2. Unsolicited commercial e-mail (UCE)—this more restrictive definition is used by regulators whose mandate is to regulate commerce, such as the U.S. Federal Trade Commission.
3. Any email message that is fraudulent.
4. Any email message where the sender's identity is forged, or messages sent through unprotected SMTP servers, unauthorized proxies, or botnets (see Theft of service below).

Spamvertised sites

Many spam e-mails contain URLs to a website or websites. According to a COM touch report in June 2004, "only five countries are hosting 99.68% of the global spammer websites", of which the foremost is China, hosting 73.58% of all web sites referred to within spam.

Most common products advertised

According to information compiled by Spam-Filter-Review.com, E-mail spam for 2006 can be broken down as follows.

E-Mail Spam by Category

Products 25%

Spam

Financial	20%
Adult	19%
Scams	9%
Health	7%
Internet	7%
Leisure	6%
Spiritual	4%
Other	3%

419 scams

Advance fee fraud spam such as the Nigerian "419" scam may be sent by a single individual from a cyber cafe in a developing country. Organized "spam gangs" operating from Russia or Eastern Europe share many features in common with other forms of organized crime, including turf battles and revenge killings. As much as 80% of spam received by Internet users in North America and Europe can be traced to fewer than 200 spammers.

Phishing

Spam is also a medium for fraudsters to scam users to enter personal information on fake Web sites using e-mail forged to look like it is from a bank or other organization such as PayPal. This is known as phishing.

Mainsleaze

Spam sent by well-known companies is sometimes called mainsleaze. A widely-known instance of spamming by a large corporation was Kraft Foods' marketing of its Gevalia coffee brand. Another more recent offender was the company iDate, which used e-mail harvesting directed at subscribers to the Quechup website to spam their friends and contacts.

Mainsleaze is all but non-existent, as few well-known companies wish to be associated with spam.

Legality

Sending spam violates the Acceptable Use Policy (AUP) of almost all Internet Service Providers. Providers vary in their willingness or ability to enforce their AUP. Some actively enforce their terms and terminate spammers' accounts without warning. Some ISPs lack adequate personnel or technical skills for enforcement, while others may be reluctant to enforce restrictive terms against profitable customers.

As the recipient directly bears the cost of delivery, storage, and processing, one could regard spam as the electronic equivalent of "postage-due" junk mail. Due to the low cost of sending unsolicited e-mail and the potential profit entailed, some believe that only strict legal enforcement can stop junk e-mail. The Coalition Against Unsolicited Commercial Email (CAUCE) argues "Today, much of the spam volume is sent by career criminals and malicious hackers who won't stop until they're all rounded up and put in jail."

In the United States, most states enacted anti-spam laws, which have since been pre-empted by the CAN-SPAM Act of 2003.

Spam is legally permissible according to the CAN-SPAM Act of 2003 provided it follows certain criteria: a truthful subject line; no false information in the technical headers or sender address; "conspicuous" display of the postal address of the sender; and other minor requirements. If the spam fails to comply with any of these requirements, then it is illegal. Aggravated or accelerated penalties apply if the spammer harvested the email addresses using methods described earlier.

Spam

A review of the effectiveness of CAN-SPAM in 2005 showed that the amount of sexually explicit spam had significantly decreased since 2003 and the total volume had begun to level off. Senator Conrad Burns, a principle sponsor, noted that "Enforcement is key regarding the CAN-SPAM legislation." In 2004 less than 1% of spam complied with the CAN-SPAM Act of 2003.

Several countries have passed laws that specifically target spam, notably Australia and all the countries of the European Union.

Article 13 of the European Union Directive on Privacy and Electronic Communications (2002/58/EC) provides that the EU member states shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

In Australia, the relevant legislation is the Spam Act 2003 which covers some types of e-mail and phone spam, which took effect on 11 April 2004. The Spam Act provides that "Unsolicited commercial electronic messages must not be sent," which is an opt-in requirement. This contrasts with the U.S. CAN-SPAM act, which is opt-out (i.e., companies are free to send spam until the recipient directs the sender not to). Penalties are up to 10,000 penalty units (AUS \$110 per penalty unit), approximately USD 900,000, or 2,000 penalty units for a person other than a body corporate.

Legislative efforts to curb spam have been ineffective or counterproductive. For example, the CAN-SPAM Act of 2003 requires that each message include a means to "opt out" (i.e., decline future e-mail from the same source). It is widely believed that responding to opt-out requests is unwise, as this merely confirms to the spammer that they have reached an active e-mail account. To the extent this is true; the CAN-SPAM Act's opt-out provisions are counterproductive in two ways: first, recipients who are aware of the potential risks of opting out will decline to do so; second, attempts to opt-out will provide spammers with useful information on their targets. A 2002 study by the Center for Democracy and Technology found that about 16% of web sites tested with opt-out requests continued to spam.

Accessing privately owned computer resources without the owner's permission counts as illegal under computer crime statutes in most nations. Deliberate spreading of computer viruses is also illegal in the United States and elsewhere. Thus, some common behaviors of spammers are criminal regardless of the legality of spamming per se. Even before the advent of laws specifically banning or regulating spamming, spammers were successfully prosecuted under computer fraud and abuse laws for wrongfully using others' computers.

The use of botnets can be perceived as theft. The spammer consumes a zombie owner's bandwidth and resources without any cost. In addition, spam is perceived as theft of services. The receiving SMTP servers consume significant amounts of system resources dealing with this unwanted traffic. As a result, service providers have to spend large amounts of money to make their systems capable of handling these amounts of email. Such costs are inevitably passed on to the service providers' customers.

Other laws, not only those related to spam, have been used to prosecute alleged spammers. For example, Alan Ralsky was indicted on stock fraud charges in January 2008, and Robert Soloway plead guilty to charges of mail fraud, fraud in connection with electronic mail, and failing to file a tax return in March 2008.

Deception and fraud

Spammers may engage in deliberate fraud to send out their messages. Spammers often use false names, addresses, phone numbers, and other contact information to set up "disposable" accounts at various Internet service providers. They also often use falsified or stolen credit card numbers to pay for these accounts. This allows them to move quickly from one account to the next as the host ISPs discover and shut down each one.

Spam

Senders may go to great lengths to conceal the origin of their messages. Large companies may hire another firm to send their messages so that complaints or blocking of email falls on a third party. Others engage in spoofing of e-mail addresses (much easier than IP address spoofing). The e-mail protocol (SMTP) has no authentication by default, so the spammer can pretend to originate a message apparently from any e-mail address. To prevent this, some ISPs and domains require the use of SMTP-AUTH, allowing positive identification of the specific account from which an e-mail originates.

Senders cannot completely spoof e-mail delivery chains (the 'Received' header), since the receiving mailserver records the actual connection from the last mailserver's IP address. To counter this, some spammers forge additional delivery headers to make it appear as if the e-mail had previously traversed many legitimate servers.

Spoofing can have serious consequences for legitimate e-mail users. Not only can their e-mail inboxes get clogged up with "undeliverable" e-mails in addition to volumes of spam, they can mistakenly be identified as a spammer. Not only may they receive irate e-mail from spam victims, but (if spam victims report the e-mail address owner to the ISP, for example) a naive ISP may terminate their service for spamming.

Theft of service

Spammers frequently seek out and make use of vulnerable third-party systems such as open mail relays and open proxy servers. SMTP forwards mail from one server to another—mail servers that ISPs run commonly require some form of authentication to ensure that the user is a customer of that ISP. Open relays, however, do not properly check who is using the mail server and pass all mail to the destination address, making it harder to track down spammers.

Increasingly, spammers use networks of malware-infected PCs (zombies) to send their spam. Zombie networks are also known as Botnets (such as zombifying malware is known as a bot, short for robot). In June 2006, an estimated 80% of e-mail spam was sent by zombie PCs, an increase of 30% from the prior year. An estimated 55 billion e-mail spam was sent each day in June 2006, an increase of 25 billion per day from June 2005.

Statistics and estimates

The growth of e-mail spam

Spam is growing, with no signs of abating. The amount of spam users see in their mailboxes is just the tip of the iceberg, since spammers' lists often contain a large percentage of invalid addresses and many spam filters simply delete or reject "obvious spam".

In absolute numbers

- 1978 - An e-mail spam advertising a DEC product presentation is sent by Gary Thuerk to 600 addresses, though software limitations meant only slightly more than half of the intended recipients actually received it.
- 2005 - (June) 30 billion per day
- 2006 - (June) 55 billion per day
- 2007 - (February) 90 billion per day
- 2007 - (June) 100 billion per day

As a percentage of the total volume of e-mail

MAAWG estimates that 85% of incoming mail is "abusive email", as of the second half of 2007. The sample size for the MAAWG's study was over 100 million mailboxes.

Spamhaus estimates that 90% of incoming email traffic is spam in North America, Europe or Australasia.

Spam

Highest amount of spam received

According to Steve Ballmer, Microsoft founder Bill Gates receives four million e-mails per year, most of them spam. (This was originally incorrectly reported as "per day".)

At the same time Jef Poskanzer, owner of the domain name acme.com, was receiving over one million spam emails per day.

Cost of spam

A 2004 survey estimated that lost productivity costs Internet users in the United States \$21.58 billion annually, while another reported the cost at \$17 billion, up from \$11 billion in 2003. The world-wide productivity cost of spam is estimated to be \$50 billion. On a world-wide basis, the IT cost of dealing with spam was estimated to rise from \$20.5 billion in 2003, to \$198 billion by 2007. An estimate of the percentage cost borne by the sender of marketing junk mail (snail mail) is 88%, the percent cost borne by the sender of junk e-mail is 0.01%, with the recipient paying the rest.

Origin of spam

Origin or source of spam refers to the geographical location of the computer from which the spam is sent; it is not the country where the spammer resides, nor the country that hosts the spamvertised site. Due to the international nature of spam, the spammer, the hijacked spam-sending computer, the spamvertised server, and the user target of the spam are all often located in different countries.

In terms of volume of spam: According to Sophos, the major sources of spam in the fourth quarter of 2007 (October to December) were: * The United States (the origin of 21.3% of spam messages, down from 28.4% in Q3)

- Russia (8.3%, up from 4.4%)
- China (4.2%, down from 4.9%)
- Brazil (4%, up 3.7%)

When grouped by continents, spam comes mostly from:

- Asia (32.1%, up from 31.1%)
- Europe (27.1%, up from 24.8%)
- North America (26.5%, down from 32.3%)
- South America (12.5%, up from 9.1%)

In terms of number of IP addresses: The Spamhaus Project (which measures spam sources in terms of number of IP addresses used for spamming, rather than volume of spam sent) ranks the top three as the United States, China, and Russia, followed by Japan, Canada, and South Korea.

In terms of networks: As of 5 June 2007, the three networks hosting the most spammers are Verizon, AT&T, and VSNL International. Verizon inherited many of these spam sources from its acquisition of MCI, specifically through the UUNet subsidiary of MCI, which Verizon subsequently renamed Verizon Business.

Spam in culture

The often rambling and incomprehensible nature of spam has led to an underground culture, with video tribute on the Web site You Tube, cartoons based on spam titles (Spamusement!) as well as spam blogs such as My Pet Spam, Delightful Spam and The Spam Hunter Diaries.

Anti-spam techniques

Spam

The US Department of Energy Computer Incident Advisory Committee (CIAC) has provided specific countermeasures against electronic mail spamming.

Some popular methods for filtering and refusing spam include e-mail filtering based on the content of the e-mail, DNS-based blackhole lists (DNSBL), greylisting, spamtraps, Enforcing technical requirements of e-mail (SMTP), checksumming systems to detect bulk email, and by putting some sort of cost on the sender via a Proof-of-work system or a micropayment. Each method has strengths and weaknesses and each is controversial due to its weaknesses.

How bulk emailers operate

Gathering of addresses

In order to send spam, spammers need to obtain the e-mail addresses of the intended recipients. To this end, both spammers themselves and list merchants gather huge lists of potential e-mail addresses. Since spam is, by definition, unsolicited, this address harvesting is done without the consent (and sometimes against the expressed will) of the address owners. As a consequence, spammers' address lists are inaccurate. A single spam run may target tens of millions of possible addresses -- many of which are invalid, malformed, or undeliverable.

Sometimes, if the sent spam is "bounced" or sent back to the sender by various programs that eliminate spam, or if the recipient clicks on an unsubscribe link, that may cause that email address to be marked as "valid", which is interpreted by the spammer as "send me more".

Delivering spam messages

Internet users and system administrators have deployed a vast array of techniques to block, filter, or otherwise banish spam from users' mailboxes. Almost all Internet service providers forbid the use of their services to send spam or to operate spam-support services. Both commercial firms and volunteers run subscriber services dedicated to blocking or filtering spam.

Using Webmail services

A common practice of spammers is to create accounts on free webmail services, such as Hotmail, to send spam or to receive e-mailed responses from potential customers. Because of the amount of mail sent by spammers, they require several e-mail accounts, and use web bots to automate the creation of these accounts.

In an effort to cut down on this abuse, many of these services have adopted a system called the captcha: users attempting to create a new account are presented with a graphic of a word, which uses a strange font, on a difficult to read background. Humans are able to read these graphics, and are required to enter the word to complete the application for a new account, while computers are unable to get accurate readings of the words using standard OCR techniques. Blind users of captchas typically get an audio sample.

Spammers have, however, found a means of circumventing this measure. Reportedly, they have set up sites offering free pornography: to get access to the site, a user displays a graphic from one of these webmail sites, and must enter the word. Once the bot has successfully created the account, the user gains access to the pornographic material. Furthermore, standard image processing techniques work well against many captchas.

Using other people's computers

Early on, spammers discovered that if they sent large quantities of spam directly from their ISP accounts, recipients would complain and ISPs would shut their accounts down. Thus, one of the basic techniques of sending spam has become to

Spam

send it from someone else's computer and network connection. By doing this, spammers protect themselves in several ways: they hide their tracks, get others' systems to do most of the work of delivering messages, and direct the efforts of investigators towards the other systems rather than the spammers themselves. The increasing broadband usage gave rise to a great number of computers that are online as long as they are turned on, and whose owners do not always take steps to protect them from malware. A botnet consisting of several hundred compromised machines can effortlessly churn out millions of messages per day. This also complicates the tracing of spammers.

Open relays

In the 1990s, the most common way spammers did this was to use open mail relays. An open relay is an MTA, or mail server, which is configured to pass along messages sent to it from any location, to any recipient. In the original SMTP mail architecture, this was the default behavior: a user could send mail to practically any mail server, which would pass it along towards the intended recipient's mail server.

The standard was written in an era before spamming when there were few hosts on the internet, and those on the internet abided by a certain level of conduct. While this cooperative, open approach was useful in ensuring that mail was delivered, it was vulnerable to abuse by spammers. Spammers could forward batches of spam through open relays, leaving the job of delivering the messages up to the relays.

In response, mail system administrators concerned about spam began to demand that other mail operators configure MTAs to cease being open relays. The first DNSBLs, such as MAPS RBL and the now-defunct ORBS, aimed chiefly at allowing mail sites to refuse mail from known open relays. By 2003 less than 1% of corporate mail servers were available as open relays, down from 91% in 1997.

Open proxies

Within a few years, open relays became rare and spammers resorted to other tactics, most prominently the use of open proxies. A proxy is a network service for making indirect connections to other network services. The client connects to the proxy and instructs it to connect to a server. The server perceives an incoming connection from the proxy, not the original client. Proxies have many purposes, including Web-page caching, protection of privacy, filtering of Web content, and selectively bypassing firewalls.

An open proxy is one which will create connections for any client to any server, without authentication. Like open relays, open proxies were once relatively common, as many administrators did not see a need to restrict access to them.

A spammer can direct an open proxy to connect to a mail server, and send spam through it. The mail server logs a connection from the proxy -- not the spammer's own computer. This provides an even greater degree of concealment for the spammer than an open relay, since most relays log the client address in the headers of messages they pass. Open proxies have also been used to conceal the sources of attacks against other services besides mail, such as Web sites or IRC servers.

Besides relays and proxies, spammers have used other insecure services to send spam. One example is FormMail.pl, a CGI script to allow Web-site users to send e-mail feedback from an HTML form. Several versions of this program, and others like it, allowed the user to redirect e-mail to arbitrary addresses. Spam sent through open FormMail scripts is frequently marked by the program's characteristic opening line: "Below is the result of your feedback form."

As spam from proxies and other "spammable" resources grew, DNSBL operators started listing their IP addresses, as well as open relays.

Today, spammers use infected client computers to deliver spam. Many still rely on Web-hosting services of spam-friendly ISPs to make money.

Spam

Today, spammers use infected client computers to deliver spam. Many still rely on Web-hosting services of spam-friendly ISPs to make money.

Spammer viruses

In 2003, spam investigators saw a radical change in the way spammers sent spam. Rather than searching the global network for exploitable services such as open relays and proxies, spammers began creating "services" of their own. By commissioning computer viruses designed to deploy proxies and other spam-sending tools, spammers could harness hundreds of thousands of end-user computers. The widespread change from Windows 9x to Windows XP for many home computers, which started in early 2002 and was well under way by 2003, greatly accelerated the use of home computers to act as remotely-controlled spam proxies. The original version of Windows XP as well as XP-SP1 had several major vulnerabilities that allowed the machines to be compromised over a network connection without requiring actions on the part of the user or owner. While Windows 2000 had similar vulnerabilities, that operating system was never widely used on home computers.

Most of the major Windows e-mail viruses of 2003, including the Sobig and Mmail virus families, functioned as spammer viruses: viruses designed expressly to make infected computers available as spamming tools.

Besides sending spam, spammer viruses serve spammers in other ways. Beginning in July 2003, spammers started using some of these same viruses to perpetrate distributed denial-of-service (DDoS) attacks upon DNSBLs and other anti-spam resources. Although this was by no means the first time that illegal attacks have been used against anti-spam sites, it was perhaps the first wave of effective attacks.

In August of that year, engineering company Osirusoft ceased providing DNSBL mirrors of the SPEWS and other blocklists, after several days of unceasing attack from virus-infected hosts. The very next month, DNSBL operator Monkeys.com succumbed to the attacks as well. Other DNSBL operators, such as Spamhaus, have deployed global mirroring and other anti-DDoS methods to resist these attacks.

Zombie networks are particularly active in North America where about half of the Internet users are on a broadband connection and many leave their computers on all the time. In January, 2008, 8% of all e-mail spam was sent by the Storm botnet, created by the Storm Worm, first released in January, 2007. It is estimated that as many as 1 million or more computers have been infected and their owners are unwilling and unknowing participants.

Obfuscating message content

This article or section is missing citations or needs footnotes.

Using inline citations helps guard against copyright violations and factual inaccuracies. (November 2007)

Many spam-filtering techniques work by searching for patterns in the headers or bodies of messages. For instance, a user may decide that all e-mail they receive with the word "Viagra" in the subject line is spam, and instruct their mail program to automatically delete all such messages. To defeat such filters, the spammer may intentionally misspell commonly-filtered words or insert other characters, as in the following examples:

- V1agra
- Via'gra
- Vi@graa
- vi*gra

The principle of this method is to leave the word readable to humans (who can easily recognize the intended word for such misspellings), but not likely to be recognized by a literal computer program. This is only somewhat effective, because modern filter patterns have been designed to recognize blacklisted terms in the various iterations of misspelling. Other filters target the actual obfuscation methods; such as the non-standard use of punctuation or numerals into unusual places, for example: within in a word.

Spam

(Note: Using most common variations, it is possible to spell "Viagra" in over $1.3 * 10^{21}$ ways.)

HTML-based e-mail gives the spammer more tools to obfuscate text. Inserting HTML comments between letters can foil some filters, as can including text made invisible by setting the font color to white on a white background, or shrinking the font size to the smallest fine print.

Another common ploy involves presenting the text as an image, which is either sent along or loaded from a remote server. This can be foiled by not permitting an e-mail-program to load images.

As Bayesian filtering has become popular as a spam-filtering technique, spammers have started using methods to weaken it. To a rough approximation, Bayesian filters rely on word probabilities. If a message contains many words which are only used in spam, and few which are never used in spam, it is likely to be spam. To weaken Bayesian filters, some spammers, alongside the sales pitch, now include lines of irrelevant, random words, in a technique known as Bayesian poisoning. A variant on this tactic may be borrowed from the Usenet abuser known as "Hipcrime" -- to include passages from books taken from Project Gutenberg, or nonsense sentences generated with "dissociated press" algorithms. Randomly generated phrases can create spoetry (spam poetry) or spam art.

After these nonsense subject lines were recognized as spam, the next trend in spam subjects started: Biblical passages. A program much like Mark V Shaney is fed Bible passages and chops them up into segments. The reasoning is that this text, often very different from the writing style of today such as the King James Version, will confuse both humans and spam filters.

Another method used to masquerade spam as legitimate messages is the use of auto generated sender names in the From: field, ranging from realistic ones such as "Jackie F. Bird" to (either by mistake or intentionally) bizarre attention-grabbing names such as "Sloppiest U. Epiglottis" or "Attentively E. Behavioral". Return addresses are also routinely auto-generated, often using unsuspecting domain owners' legitimate domain names, leading some users to blame the innocent domain owners. Blocking lists use ip addresses rather than sender domain names, as these are more accurate. A mail purporting to be from example.com can be seen to be faked by looking for the originating ip address in the mails header, and Sender Policy Framework for example helps by stating that example.com will only send email from xx.xx.xx.xx ip.

Spam can also be hidden inside a fake "Undelivered mail notification" which looks like the failure notices sent by a mail transfer agent (a "MAILER-DAEMON") when it encounters an error.

Spam-support services

A number of other online activities and business practices are considered by anti-spam activists to be connected to spamming. These are sometimes termed spam-support services: business services, other than the actual sending of spam itself, which permit the spammer to continue operating. Spam-support services can include processing orders for goods advertised in spam, hosting Web sites or DNS records referenced in spam messages, or a number of specific services as follows:

Some Internet hosting firms advertise bulk-friendly or bulletproof hosting. This means that, unlike most ISPs, they will not terminate a customer for spamming. These hosting firms operate as clients of larger ISPs, and many have eventually been taken offline by these larger ISPs as a result of complaints regarding spam activity. Thus, while a firm may advertise bulletproof hosting, it is ultimately unable to deliver without the connivance of its upstream ISP. However, some spammers have managed to get what is called a pink contract (see below) — a contract with the ISP that allows them to spam without being disconnected.

A few companies produce spamware, or software designed for spammers. Spamware varies widely, but may include the ability to import thousands of addresses, to generate random addresses, to insert fraudulent headers into messages, to

Spam

use dozens or hundreds of mail servers simultaneously, and to make use of open relays. The sale of spamware is illegal in eight U.S. states.

So-called millions CDs are commonly advertised in spam. These are CD-ROMs purportedly containing lists of e-mail addresses, for use in sending spam to these addresses. Such lists are also sold directly online, frequently with the false claim that the owners of the listed addresses have requested (or "opted in") to be included. Such lists often contain invalid addresses. In recent years, these have fallen almost entirely out of use due to the low quality e-mail addresses available on them, and because some e-mail lists exceed 20GB in size. The amount you can fit on a CD is no longer substantial.

A number of DNSBLs, including the MAPS RBL, Spamhaus SBL, SORBS and SPEWS, target the providers of spam-support services as well as spammers. DNSBLs blacklist IPs or ranges of IPs to persuade ISPs to terminate services with known customers who are spammers or resell to spammers.

Related vocabulary

Unsolicited bulk e-mail (UBE)

A synonym for e-mail spam.

Unsolicited commercial e-mail (UCE)

Spam promoting a commercial service or product. This is the most common type of spam, but it excludes spam which are hoaxes (e.g. virus warnings), political advocacy, religious messages and chain letters sent by a person to many other people. The term UCE may be most common in the USA. Pink contract.

A pink contract is a service contract offered by an ISP which offers bulk e-mail service to spamming clients, in violation of that ISP's publicly posted acceptable use policy.

Spamvertising

Spamvertising is advertising through the medium of spam.

Opt-in, confirmed opt-in, double opt-in, opt-out

Opt-in, confirmed opt-in, double opt-in, opt-out refers to whether the people on a mailing list are given the option to be put in, or taken out, of the list.

Final, Ultimate Solution for the Spam Problem (FUSSP)

An ironic reference to naïve developers who believe they have invented the perfect spam filter, which will stop all spam from reaching users' inboxes while accidentally deleting no legitimate email.

2004

In May, 2004, Howard Carmack of Buffalo, New York was sentenced to 3 1/2 to 7 years for sending 800 million messages, using stolen identities. In May 2003 he also lost a \$16 million civil lawsuit to Earthlink.

On September 27, 2004, Nicholas Tombros plead guilty to charges and became the first spammer to be convicted under the CAN-SPAM Act of 2003. He was sentenced in July of 2007 to three years probation, six months house arrest, and fined \$10,000.

On November 4, 2004, Jeremy Jaynes, rated the 8th most prolific spammer in the world according to Spamhaus, was convicted of three felony charges of using servers in Virginia to send thousands of fraudulent e-mails. The court

Spam

recommended a sentence of nine years' imprisonment, which was imposed in April 2005 although the start of the sentence was deferred pending appeals. Jaynes claimed to have an income of \$750,000 a month from his spamming activities. On February 29, 2008 the Supreme Court of Virginia affirmed his conviction.

On November 8, 2004, Nick Marinellis of Sydney, Australia, was sentenced to 4 1/3 to 5 1/4 years for sending Nigerian 419 e-mails.

On December 31, 2004, British authorities arrested Christopher Pierson in Lincolnshire, UK and charged him with malicious communication and causing a public nuisance. On January 3, 2005, he pleaded guilty to sending hoax e-mails to relatives of people missing following the Asian tsunami disaster.

2005

On July 25, 2005, Russian spammer Vardan Kushnir, who is believed to have spammed every single Russian internet user, was found dead in his Moscow apartment, having suffered numerous blunt-force blows to the head. It is believed that Kushnir's murder was unrelated to his spamming activities.

On November 1, 2005, David Levi, 29, of Lytham, England was sentenced to four years for conspiracy to defraud by sending e-mails pretending to be from eBay, his brother Guy Levi, 22, was sentenced to 21 months after pleading guilty to conspiracy to defraud, and four others were each sentenced to six months for money laundering.

On November 16, 2005, Peter Francis-Macrae of Cambridgeshire, described as Britain's most prolific spammer, was sentenced to six years in prison.

2006

In January, 2006, James McCalla was ordered to pay \$11.2 Billion to an ISP in Iowa and barred from using the Internet for 3 years for sending 280 million e-mail messages.

On June 28, 2006, IronPort released a study which found 80% of spam emails originating from zombie computers. The report also found 55 billion daily spam emails in June 2006, a large increase from 35 billion daily spam emails in June 2005. The study used SenderData which represents 25% of global email traffic and data from over 100,000 ISP's, universities, and corporations.

On August 8, 2006, AOL announced the intention of digging up the garden of the parents of spammer Davis Wolfgang Hawke in search of buried gold and platinum. AOL had been awarded a US\$ 12.8 million judgment in May of 2005 against Hawke, who had gone into hiding. The permission for the search was granted by a judge after AOL proved that the spammer had bought large amounts of gold and platinum. In July, 2007 AOL decided not to proceed.

On October 12, 2006, Brian Michael McMullen, 22, of East Pittsburgh, Pennsylvania was sentenced to three years supervised release, five months home detention and ordered to pay restitution in the amount of \$11,848.55 for violating the CAN-SPAM Act of 2003.

On October 27, 2006, the Federal Court of Australia fined Clarity1 A\$4.5 million (US\$3.4 million; euro2.7 million) and its director Wayne Mansfield A\$1 million (US\$760,000; euro600,000) for sending unsolicited e-mails in the first conviction under Australia's Spam Act of 2003.

In November, 2006 Christopher William Smith (aka Chris "Rizler" Smith) was convicted on 9 counts for offenses related to Smith's spamming.

2007

Spam

On January 16, 2007, an Azusa, California man was convicted by a jury in United States District Court in Los Angeles in United States v. Goodin, U.S. District Court, Central District of California, 06-110, under the CAN-SPAM Act of 2003 (the first conviction under that Act). He was sentenced to and began serving a 70 month sentence on June 11, 2007.

On May 30, 2007, notorious spammer Robert Soloway was arrested after having being indicted by a federal grand jury on 35 charges including mail fraud, wire fraud, e-mail fraud, identity theft, and money laundering. If convicted, he could face decades behind bars. Bail was initially denied although he was released to a half way house in September. His trial is scheduled for March 24, 2008.

On June 25, 2007 two men were each convicted on eight counts including conspiracy, fraud, money laundering, and transportation of obscene materials in U.S. District Court in Phoenix, Arizona. The prosecution is the first of its kind under the CAN-SPAM Act of 2003, according to a release from the Department of Justice. One count for each under the act was for falsifying headers, the other was for using domain names registered with false information. The two had been sending millions of hard-core pornography spam e-mails. The two men were sentenced to five years in prison and ordered to forfeit US\$ 1.3 million.

Image spam

Image spam is an obfuscating method in which the text of the message is stored as a GIF or JPEG image and displayed in the email. This prevents text based spam filters from detecting and blocking spam messages. Image spam is currently used largely to advertise "pump and dump" stocks.

Often, image spam contains nonsensical, computer-generated text which simply annoys the reader. However, new technology in some programs tries to read the images by attempting to find text in these images. They are not very accurate, and sometimes filter out innocent images of products like a box that has words on it.

A newer technique, however, is to use an animated GIF image that does not contain clear text in its initial frame, or to contort the shapes of letters in the image (as in CAPTCHA) to avoid detection by OCR tools.

Blank spam

Blank spam is spam lacking a payload advertisement. Often the message body is missing altogether, as well as the subject line. Still, it fits the definition of spam because of its nature as bulk and unsolicited email.

Blank spam may be originated in different ways, either intentional or unintentionally:

- Blank spam can have been sent in a directory harvest attack, a form of dictionary attack for gathering valid addresses from an email service provider. Since the goal in such an attack is to use the bounces to separate invalid addresses from the valid ones, the spammer may dispense with most elements of the header and the entire message body, and still accomplish his or her goals.
- Blank spam may also occur when a spammer forgets or otherwise fails to add the payload when he or she sets up the spam run.
- Often blank spam headers appear truncated, suggesting that computer glitches may have contributed to this problem—from poorly-written spam software to shoddy relay servers, or any problems that may truncate header lines from the message body.
- Some spam may appear to be blank when in fact it is not. An example of this is the VBS.Davinia.B email worm which propagates through messages that have no subject line and appears blank, when in fact it uses HTML code to download other files.