Key Concepts

# Key organizations in spam management

# Service Providers

## Domain Registries and Registrars

A domain registry tracks all of the names registered in an Internet domain such as .COM or .JP. A registrar takes orders from customers and forwards them to the appropriate registries. Most registrars have acceptable use policies and can suspend registrations used for in violation of policy.

## E-mail Service Providers (ESP)

ESPs provide outbound bulk mail service to third parties. In some cases they maintain the mailing lists, in others the client provides the list at the time they do the mailing. ESPs have to deal with outbound spam from their customers, which involves vetting the clients and their mailing lists, the mail they send, and dealing with complaints from recipients.

Many ESPs also provide click metrics, by putting links to the ESP’s own web servers into the mail that let them track which mail got how many clicks. This provides another means to analyze and manage the response to customer mail.

## Hosting & Cloud Providers

Hosting providers provide servers for web, mail, and other Internet services. Their clients can usually send outgoing mail, either directly or through a mail server at the provider. Web servers provide landing pages for links in mail, which can be disabled if linked from spam.

## Internet Service Providers (ISP)

ISPs deal with both incoming and outgoing spam. Most provide e-mail service for their users, so they are responsible for filtering and managing incoming spam in their mail service. For outgoing spam, they have to manage both mail sent through their service, and mail and other abuse coming from malicious users and compromised customer hosts. The outgoing spam can be anything their network can carry, from mail to instant messages to VoIP.

## IP Address Space Registries

Five Regional Internet Registries (RIRs) (ARIN, RIPE, LACNIC, APNIC, and AfriNIC) manage IP address space, both directly and via local subregistries. Spammers often seek blocks of IP space for snowshoe spamming (sending small amounts of spam over large numbers of IPs), by making fraudulent requests to the RIRs, thus allowing for outright fraudulent ‘hijacking’ of space not currently in active use.

## Mail Box Providers (MBP)

Many providers offer mail directly to individuals and organizations. The largest include Microsoft Hotmail, Yahoo! Mail, and Google Gmail, but there are many smaller ones operating both under their own names and as “white label” providers who run mail under their own names. The inbound and outbound issues are similar to those for ISP mail systems.

## Telephone (mobile) companies

SMS and VoIP spam is delivered through the telephone network, so telephone companies often have some or all of the data and facilities needed to investigate and remediate incidents. An increasing number of companies in the mobile space are setting up spam reporting facilities so that end-users can complain about abusive activity.

# Inter-Governmental agencies

## European Union (EU)

Founded 1993, Brussels, Belgium <http://europa.eu>

The EU is an economic and political partnership among European countries. The European Union issues legal directives that are implemented in the individual member countries. The EU operates the European Union Agency for Network and Information Security (ENISA) which is active in the investigation of spam and network abuse <http://www.enisa.europa.eu>

## G-8 24-7 High Tech Crime Network, Organization of American States (OAS)

Founded 2002, Washington DC <http://www.oas.org/juridico/english/cyber_g8.htm>

The G-8 Hi-tech Crime Network provides points of contact in each participating country to facilitate the assistance with urgent investigations involving electronic evidence.

**International Criminal Police Organization (Interpol)**

Founded 1953, Lyon France <http://interpol.int>

Formerly the International Criminal Police Commission (ICPC). INTERPOL is an intergovernmental organization facilitating international (intra-agency) police cooperation. Its work focuses primarily on public safety, organized crime, piracy, illicit drug production and trafficking, human trafficking, money laundering, child sexual abuse material, and computer crime. The INTERPOL Global Complex for Innovation (IGCI) located in Singapore, SG will open in late 2014. It is intended to be a cutting-edge research and development facility for the identification of crimes and criminals, innovative training, operational support and partnerships, including a strong focus on cyber-crime. INTERPOL plays a strong role in training of enforcement officials, and assisting investigations of spam, hacking and other cyber-abuse.

## London Action Plan (LAP)

Founded 2005, London, England <http://www.londonactionplan.org>

The LAP is an informal 40-member organization of civil anti-spam agencies, founded by the U.S. Federal Trade Commission, Industry Canada, and The United Kingdom’s Office of Fair Trading with some related NGOs as observers. The LAP do case coordination, information exchange (including the development of Mutual Legal Assistance Treaties (MLATs)) and capacity building among their members.

## National Cyber-Forensics & Training Alliance (NCFTA)

## Founded 2002, Pennsylvania, USA <http://ncfta.net>. Companies, Government, and Academia work together to neutralize cyber crime. The NCFTA helps to train criminal investigators in cybercrime research and techniques. Their initiatives focus on Financial Services, Botnets, Intellectual Property crime (with a focus on retail goods), and illicit pharmacological sales

## Organisation for Economic Co-operation and Development (OECD)

Founded 1948, Paris France http:/[http://oecd.org](http://www.oecd.org)

The OECD has published white papers for their 130 + member countries describing issues with, and responses to, spam. The OECD published a Spam Toolkit in 2006 <http://www.oecd.org/internet/consumer/36494147.pdf>

Canada submitted an update entitled ‘Best Practices to Address Online and Mobile Threats’ to the toolkit in 2012 <http://www.cauce.org/2012/10/best-practices-report.html>

#

#

# Law Enforcement Agencies

Governments take a variety of approaches to spam and the incumbent cybercrime related to spam (compromised systems, phishing, hacking and illegal goods sold).

What follows is a list of North American government agencies that involve themselves in various aspects of spam remediation by legal means. As can be seen from the list, there are a wide variety of legal approaches and remedies that can be taken to prosecute spammers and the products they promote.

* The Canadian Competition Bureau <http://www.competitionbureau.gc.ca> The bureau applies consumer rights laws, such as deceptive advertising found in spam, focusing on fraud prevention. The bureau has both civil and criminal authority.
* Industry Canada runs the Spam Reporting Centre and coordinates the application of Canada’s Anti-Spam Legislation (CASL) <http://fightspam.gc.ca>
* The Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/index_e.asp> The OPC applies the Canadian privacy law, PIPEDA, for example, the OPC investigates the scraping of email addresses from websites used in spam.
* U.S. Department of Justice (DOJ) <http://www.justice.gov> The DOJ prosecutes federal criminal spam cases, including counterfeit goods (copyright infringement cases).
* U.S. Federal Bureau of Investigation (FBI) <http://www.fbi.gov> The FBI has prosecuted many criminal spam cases, and taken down American-based spam support infrastructure such as McColo. The FBI also cooperates with criminal law enforcement at the International level to affect arrests and take-downs (for example, the Mariposa botnet in The Netherlands).
* U.S. Federal Trade Ccommission (FTC) <http://www.ftc.gov> A civil enforcement agency that has underttaken numerous initiatives against spammers. They have also coordinated several Spam Summits. The FTC is charged with the primary enforcement of the CAN SPAM act of 2003.
* U.S. Food & Drug Administration (FDA) <http://www.fda.gov> The FDA undertakes investigations into illegal pharmaceutical sales and illicit sales of (contaminated, false labelling) nutritional substances being sold via spam.
* U.S. Internal Revenue Service (IRS) <http://www.irs.gov> The IRS investigates tax-related issues (undeclared income, money laundering and offshore money havens) with both civil and criminal laws.
* United States Postal Service (USPS) <https://www.usps.com> The USPS investigates money laundering (work at home, secret shopper schemes) as well as intercepting illicit drugs shipments
* U.S. Secret Service <http://www.secretservice.gov> The USSS investigates and prosecutes incursion into financial institutions (banks, credit card companies, and so on).
* U.S. Securities and Exchange Commission (SEC) <http://www.sec.gov> The SEC has undertaken numerous investigations and prosecutions of stock spam schemes.

#

#

# NGOs

## Anti-phishing Working Group (APWG)

Founded 2004, California USA <http://apwg.org>

The APWG is an association of major financial services companies, ISPs, researchers and related infrastructure providers. They publish best practices documents and educate their members about anti-phishing trends and techniques. They also publish quarterly statistics on phishing trends.

## CAUCE (Coalition Against Unsolicited Commercial E-mail)

Founded 1997, New York, USA [http://cauce.org](http://www.cauce.org)

CAUCE is an all-volunteer Internet end-user advocacy organization. CAUCE has moved beyond its original mission of advocating for anti-spam laws, to a broader stance of defending the interests all users in the areas of privacy and abuse in all its forms on the Internet.

## Global Standard for Mobility Association (GSMA)

Founded 1982, Paris, France <http://gsma.com>

Formerly the Groupe Speciale Mobile. The GSMA set standards for telephone mobility, and operates in the public policy arena.

## Internet Corporation for Assigned Names and Numbers (ICANN)

Founded 1998, California USA [http://icann.org](http://www.icann.org)

ICANN coordinates top level domain names (.com, .net, .org, and so forth) and also runs the Internet Assigned Names Authority, IANA, which does important clerical work for the IETF and the Regional Internet Registries (RIRs).

## Internet Engineering Task Force (IETF)

Founded 1995, Virgina USA [http://ietf.org](http://www.ietf.org)

The IETF develops and maintains technical standards for the Internet, including those for e-mail, XMPP (instant messaging), and http (web page transport.) Recent standards have added improved security and anti-spam features.

## The Internet Society (ISOC)

Founded 1992, Geneva Switzerland [http://isoc.org](http://www.isoc.org)

ISOC organizes and funds capacity development programs and publishes documents. It also provides the organizational umbrella for the IETF.

## International Telecommunication Union (ITU)

Founded 1865, Geneva Switzerland <http://itu.int>

The ITU maintains most telephone standards, including those for cellular phones and SMS. They have published some documents and done some training for spam mitigation.

## Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)

Founded 2003, California USA [http://m3aawg.org](http://www.m3aawg.org)

M3AAWG (formerly MAAWG) is an association of major ISPs, ESPs, and related infrastructure providers. They publish best practices documents and educate their members about anti-abuse trends and techniques.

## Microsoft Digital Crimes Unit (DCU)

Founded 1996, Washington state USA <http://www.microsoft.com/government/ww/safety-defense/initiatives/pages/digital-crimes-unit.aspx>

A coalition of industry, criminal law enforcement organizations, academia, and NGOs focusing on child sexual exploitation crimes, piracy and IP crimes, and malicious software crimes, particularly botnet-driven Internet attacks.

## Signal Spam

Founded 2005, Paris France <https://www.signal-spam.fr>

Signal Spam is a not-for-profit public/private partnership of French Authorities & Law Enforcement Agencies, Internet Services Providers and email industry partners.

#

#

# Spamming Techniques

The earliest e-mail spam was sent directly from the spammer’s own mail system. That rapidly became a problem for spammers, since the system managers were alerted to the spamming activity by the load on their mail server, and complaints from the recipients. Since then they have both spread out their own sending patterns to make the origin of the spam harder to detect, and hijacked innocent third parties’ computers to send spam.

*Botnets* are collections of compromised computers, known as *bots* or *zombies.* They are remotely coordinated over the Internet by *bot herders*. A single botnet can consist of hundreds of thousands or some cases as many as tens of millions of computers. Criminals use them to send spam, by downloading the spam and recipient addresses to the botted computers and commanding them to mail it.

Early on, each bot sent a large amount of spam, making it easy to detect. As botnets got bigger and spammers got more sophisticated they spread out the spam, so botnets now send only a trickle of spam from each bot to avoid detection.

Spammers also use *compromised servers*, legitimate servers typically hosting innocuous software that have security holes that allow installation of malicious software that sends spam. Content management packages and blogging packages are the most common compromise targets. The compromised servers often send legitmate mail from their normal applications, the spam is harder to filter since it comes from the same host as the legitimate mail.

A somewhat similar technique is *snowshoe* spamming, in which the spammer gains control over large ranges of IP addresses, and then sends spam from his own computers, spreading the spam sources over many different IP addresses, again to avoid detection by message counting filters. (The name comes from the way snowshoes spread out the wearer’s weight to avoid sinking into the snow.) Snowshow spammers often use thousands or tens of thousands of IP addresses at once.

*Greymail* is, as its name suggests, intermediate between legitimate mail and outright spam, mail that the recipient could technically have been said to have opted into, but clearly does not want. Greymail often comes from *co-registration*, asking for people to sign up for something of minor value, with a hard to see disclaimer that their contact info may be shared with “partners”. In fact that means that it’s sold to vast numbers of undesirable mailers. One system manager tracked an address for a person known as “Nadine” who accidentally mistyped her address in a co-registration form in 2003 and instead entered an otherwise unused address on his system. In the subsequent decade, that address received over 300,000 pieces of spam,

Spam in other media has also adapted as the technology and rules have changed. Junk phone calls were originally made by live callers in boiler rooms, but now are more likely to be made by software on PCs via VoIP. Junk text messages have been sent from specialized devices that act as a multiple mobile phones with multiple SIM cards, but now are as likely to come through e-mail or VoIP gateways.

# Mitigation techniques

E-mail providers have developed a variety of techniques to stop incoming or outgoing techniques.

## DNS Blacklists or Blocklists

DNS blacklists (sometimes called blocklists) publish lists of IP addresses from which they recommend that receivers refuse mail. The reasons include that the IP addresses have been observed to send spam, or particular kinds of spam such as from botnets, or the provider that manages the addresses have a no-mail policy for those addresses. The lists are published in the Domain Name System which allows the lists to be checked quickly at the time mail delivery is attempted. The technical structure of DNSBLs is documented in RFC 5782, and best practices for maintaining them are described in RFC 6471.

## DNS Whitelists

DNS whitelists are the approximate converse of DNS blacklists, IP addresses that send good mail, or perhaps that send enough good mail that they shouldn’t be blacklisted even if they send some spam.

## Bulk counters

Since spam is, by definition, sent in bulk, one way to detect it is to look for large number of similar messages. Bulk counters compute “signatures” for each message and count the number of times each signature appears. Bulk counting can’t distinguish between spam and legitimate bulk mail, so some external means is required to distinguish the two. The Distributed Checksum Clearinghouse is a network of computers that share signature counts using open source software, <http://www.dcc-servers.net/dcc>.

## Adaptive filters

Much spam can only be identified by looking at individual messages to see if they contain text and other material characteristic of spam. Since spam varies both from message to message and over time, successful filters look at a wide variety of characteristics and combine them to compute a score for the message. They also adapt the criteria dynamically, e.g., increasing the score for a phrase that has appeared in a lot of spam, or decreasing the score for a phrase that has appeared in mail incorrectly characterized as spam. SpamAssassin is a widely used open source spam filter that combines many techniques including adaptive filters.

## Disposable and other special-use addresses

Since mail systems can handle an effectively unlimited number of addresses, some of them allow each user to have multiple addresses, so the user can give a unique hard to guess address to each correspondent, often of the form user-abcdef@mailsystem.com where abcdef is unique to each correspondent. The addresses can subsequently be turned off if the correspondent starts sending spam or leaks the address to spammers. Zoemail was a patented commercial implementation of this scheme.

## Mail authentication

Large amounts of spam are sent with forged return addresses. Mail authentication allows senders to show that their mail is actually from its nominal sender. Authentication can be useful to combat phishing, and for some kinds of whitelisting of specific senders.

Commonly used authentication schemes include SPF (RFC 4408) and DKIM (RFC 6376.) DMARC is an emerging authentication scheme that builds on SPF and DKIM (http://dmarc.org).

## Feedback loops

Many mail systems offer their users “spam” or “junk” buttons they can use to report unwanted mail. *Feedback loops* (FBLs) allow mail senders to register their sending IP addresses so they can receive copies of reports of messages they sent. The senders are expected to deal appropriately with the reports to minimize the overall number of complaints.

## Network monitoring

ISPs and other network operators monitor the traffic passing through their networks to check for unusual traffic that may indicate abuse. For example, if a host that is not supposed to be running an instant messaging server starts sending or receiving large amounts of IM traffic, something is probably wrong.

## Outbound mail management

Many ISPs and hosting companies place controls on the mail their users send. A common technique called “port 25 blocking” requires their users to send outgoing mail through a known mail server where it can be monitored and managed. Some hosting companies do semi-transparent mail filtering, in which mail sent directly from customer computers is transparently redirected through filtering systems run by the hosting provider that manage volume and monitor for indications of spam.

## Other techniques

The Anti-Spam Research Group of the Internet Research Task Force developed a fairly comprehensive list of anti-spam techniques. It is stored in wiki form at http://wiki.asrg.sp.am/.

# References

* *The Story of Nadine*, about coregistration abuse, <<http://www.honet.com/nadine/default.htm>>.
* *DNS Blacklists and Whitelists*. RFC 5782, J. Levine. February 2010, <http://www.rfc-editor.org/info/rfc5782>
* *Overview of Best Email DNS-Based List (DNSBL) Operational Practices*. RFC 6471. C. Lewis, M. Sergeant. January 2012. <<http://www.rfc-editor.org/info/rfc6471>>.
* *ASRG anti-spam technique taxonomy,* <<http://wiki.asrg.sp.am/>>
* *Apache SpamAssassin* project, open source spam filter, <<http://spamassassin.apache.org/>>
* *Zoemail locks out spam*, PC Magazine, April 20, 2004, <[http://www.pcmag.com/article2/0,2817,1554989,00.asp](http://www.pcmag.com/article2/0%2C2817%2C1554989%2C00.asp)>
* *Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1*. RFC 4408, M. Wong, W. Schlitt. April 2006, <<http://www.rfc-editor.org/info/rfc4408>>.
* *DomainKeys Identified Mail (DKIM) Signatures*. RFC 6376, D. Crocker, Ed., T. Hansen, Ed., M. Kucherawy, Ed.. September 2011, <<http://www.rfc-editor.org/info/rfc6376>>.