



Glossary

Updated April 2011

Ad Blocker - A software utility which can be either a browser add-on or integrated within a browser which prevents advertisements from being displayed or third party content from being served. Examples include *Adblock Plus* and *Noscript*. Leading browsers offer limited controls to block third party content including Microsoft Internet Explorer 9 and Mozilla Firefox.

Address Specification (also known as: email address spec or addr-spec) - Addresses occur in several message header fields to indicate senders and recipients of messages. An address may either be an individual mailbox, or a group of mailboxes. [RFC 5322]

Ad Exchange - Ad exchanges facilitate auction-based, real-time buying and serving of ads. Ad exchanges operate by serving as intermediaries between *ad networks*, *publishers*, and *advertisers*. Ad exchanges provide a sales channel to publishers and ad networks, as well as aggregated inventory to advertisers. Ad exchanges' business models and practices may include features that are similar to those offered by ad networks.

Ad Impression (or impressions) - Total number of times an ad (or malvertisement) is served on one or more sites. A single malvertising creative may be served to multiple users as a result of a single incident with upwards to 100,000 or more impressions, depending on the site(s) the malvertising is served on and the frequency of rotation of the ad on the site(s) and the life of the campaign.

Ad Network - An ad network is a company that works with a group of Web sites and sells advertising space on their behalf. Ad networks provide an outsourced sales capability for publishers and a means to aggregate inventory and audiences from numerous sources in a single buying opportunity for media buyers. Ad networks may provide specific technologies to enhance value to both publishers and advertisers, including unique targeting capabilities, creative generation, and optimization. Ad networks' business models and practices may include features that are similar to those offered by ad exchanges.

Ad Servers - An ad server is a web server which stores and delivers advertisements used in online marketing and delivers them to website visitors. Ad servers are constantly updated so that the website or webpage on which the ads are displayed contains new advertisements - e.g., banners (static images/animations), text, Flash animated GIFs and / or applets among other content types. In addition, the ad server also performs various other tasks like counting the number of impressions/clicks for an ad campaign and report generation, which helps in determining the ROI for an advertiser on a particular website. Ad servers come in two flavors: local ad servers and third-party or remote ad servers. Local ad servers are typically run by a single publisher and serve ads to that publisher's domains, allowing fine-grained creative, formatting, and content control by that publisher. Remote ad servers can serve ads across domains owned by multiple publishers. They deliver the ads from one central source so that advertisers and publishers can track the distribution of their online advertisements and have one location for controlling the rotation and distribution of their advertisements.

Ad Space - The location on a page of a site in which an *advertisement* can be placed. Each space on a web site is uniquely identified. Multiple ad spaces can exist on a single page and can change over time.



Adware - A type of Advertising Display Software that delivers advertising content potentially in a manner or context that may be unexpected and unwanted by users. Many adware applications also perform tracking functions, and therefore may also be categorized as Tracking Technologies. Some consumers may want to remove Adware if they object to such tracking, do not wish to see the advertising caused by the program, or are frustrated by its effects on system performance. On the other hand, some users may wish to keep particular adware programs if their presence subsidizes the cost of a desired product or service or if they provide advertising that is useful or desired, such as ads that are competitive or complementary to what the user is looking at or searching for.

Adblock Plus - One of the most popular ad blockers available. <http://adblockplus.org>

Advertisement (also called “Creative” or “Advertising Banner”, and often abbreviated as “Ad”) - A single unique image, text link, message, applet, or interactive program (as in the case of Flash or Shockware) targeted to an advertiser’s customer or prospect. Advertisements are used to fill *Ad Space*. The same ad may run on multiple sites and may be delivered through one or more *ad networks* or *ad exchanges*.

Advertiser - The party who pays for the ad and has a product or service they wish to raise awareness to and persuade a viewer to take action. In fraudulent advertising and malvertising, a legitimate company’s brand or product may unknowingly be used in an attempt by a cybercriminal to appear legitimate and to get users to take action in which malware may be downloaded.

Advertising Banner (also called Ad Banner or Banner) - A static graphical image (GIF or JPEG files) or interactive content (Flash files) used to display an advertising unit on a web site.

ADSP - Author Domain Signing Practices. A policy framework for DKIM enabling the sender of a message to publish DKIM signing practices and optionally request handling of messages without a valid DKIM signature. Early versions of ADSP were known as ASP (Author Signing Practices) or the original SSP (Sender Signing Practices). Specified as RFC 5617.

Agency - An organization that, on behalf of clients, plans marketing and advertising campaigns, drafts and produces advertisements and places advertisements in the media. In online advertising, agencies often use third party technology (ad servers), placing advertisements with publishers, ad networks and other industry participants.

APWG - Anti Phishing Working Group - www.antiphishing.org

ASRG - Anti Spam Research Group. A working group chartered by the IETF to examine approaches to reduce or eliminate spam. – www.asrg.sp.am

At Risk User (or PC) - User’s PC (consumer or business user), which may be unpatched and / or has a vulnerability (potentially including a zero-day vulnerability), which may be exploited to execute arbitrary instructions or code of an attacker’s choice. As operating systems and browsers have become hardened, increasingly such vulnerabilities have targeted web sites, third party applications and browser ad-ons.

BATV - Bounce Address Tag Validation. A cryptographic signature-based approach to encode the bounce address otherwise known as the RFC5321 Mail From to enable the recipient to determine if a bounce message is legitimate. <http://brandenburg.com/CSV/draft-levine-mass-batv-00.html>

BITS - The technologically-focused division of the US Financial Services Roundtable. www.bitsinfo.org



BL / BlockList / BlackList - A list of IP addresses or domains that have been reported and listed as sources of unwanted email or spam, usually accessible via DNS. There are public and private blacklists. Public blacklists are published and made available to the public - many times as a free service, sometimes for a fee. There are hundreds of well-known public blacklists. There may be thousands in existence. The number grows each day, as many blacklisting systems allow ISP's and System Administrators to start their own list based upon another.

Botnet - A type of Remote Control Software, specifically a collection of zombie machines running malware under a common command. A botnet's originator can control the group remotely. The botnet is usually a collection of zombie machines running programs under a common command and control infrastructure on public or private networks. Botnets have been used for sending spam remotely, installing more spyware without consent and other illicit purposes.

Campaign Life - The duration that an ad (legitimate or malicious) is served. As with phishing and other exploits, campaigns are often timed for weekends to increase the amount of time they can be distributed before they are detected, removed or blocked. Typically measured in days and hours.

CLEAR - Compatible Low-overhead Email Authentication and Responsibility. A (PRE-IETF) working group drafting the standard and implementation of CSV.

Click Fraud - A fraudulent business activity (and at times a criminal act) that occurs in pay-per-click online advertising. Click fraud occurs when a person, automated script, or computer program imitates a legitimate user clicking on an ad for the purpose of generating a charge per click without having actual interest in the target of the ad's link.

Content Headers - From:, To:, Friendly From, subject line and other headers included in the body of an email message. Usually displayed by the Mail Client. These are not normally available to the MTA (Mail Transport Agent or server) unless the entire contents of the email message are transmitted.

CSV - Client SMTP Validation. A proposed standard for lightweight authentication of the connecting mail server. Uses the HELO/EHLO handshake. <http://mipassoc.org/csv/draft-ietf-marid-csv-intro-01-06dc.html>

Dangerous Download - A scenario in which a user clicks on a link and is sent (and receives) a malware binary. Other scenarios include when the user clicks on the window in the mistaken belief that, for instance, an error report from the PC itself is being acknowledged, or that an innocuous advertisement popup is being dismissed or accepting a video or music download. (See Spyware).

DK - Domain Keys. A crypto based signing approach to authenticating email proposed by Yahoo that has since been made obsolete by DKIM. <http://antispam.yahoo.com/domainkeys>

DKIM - DomainKeys Identified Mail is a successor to two other authentication protocols – Domain Keys (DK) by Yahoo! and Internet Identified Mail (IIM) by Cisco.

Domain - A domain (or domain name) consists of one or more dot-separated components. [...] [RFC 5321].

DNS - Domain Name System. A distributed, hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. DNS is how computer networks query Internet domain names and translate them into IP addresses. The domain name is the textual reference for an IP address or range of IP addresses.



Drive by Download - A term used to describe threats which do not require any user intervention whatsoever to infect or compromise a user. Drive-by downloads can occur by simply visiting a website, viewing an e-mail message or by clicking on a deceptive popup window.

EHLO - Extended HELO (See HELO) - A command used during the initiation of a mail exchange session that identifies the connecting server and also indicates additional command set capabilities beyond the ones available under HELO.

Envelope Headers - These are the SMTP headers used by SMTP. They are not normally available to the user mail client unless they are written into the email body during the mail exchange process.

ESPC – Email Sender & Provider Coalition - <http://www.espcalition.org/>

EV SSL (Extended Validation Secure Socket Layer) - An [X.509 public key certificate](#) issued according to a specific set of identity verification criteria. These criteria require extensive verification of the requesting entity's identity by the certificate authority (CA) before a certificate is issued.

Fake Anti-Virus (also called Rogue Anti-Virus) - A type of malvertisement in which a user is shown a dialog box that appears similar to that of a legitimate anti-virus program and informs the user that his or her machine is infected even though it really may not be. Fake anti-virus dialogs are socially engineered to encourage the user to take action. Examples include clicking on a link or entering a credit card number to purchase software to “clean” the machine and remedy the problem, (even though it in reality infects the user’s machine).

From headers - The originator header fields indicate the mailbox(es) of the source of the message. The "From:" field specifies the author(s) of the message, that is, the mailbox(es) of the person(s) or system(s) responsible for the writing of the message. The "Sender:" field specifies the mailbox of the agent responsible for the actual transmission of the message. For example, if a secretary were to send a message for another person, the mailbox of the secretary would appear in the "Sender:" field and the mailbox of the actual author would appear in the "From:" field. If the originator of the message can be indicated by a single mailbox and the author and transmitter are identical, the "Sender:" field SHOULD NOT be used. Otherwise, both fields SHOULD appear.

The originator fields also provide the information required when replying to a message. When the "Reply-To:" field is present, it indicates the mailbox(es) to which the author of the message suggests that replies be sent. In the absence of the "Reply-To:" field, replies SHOULD by default be sent to the mailbox(es) specified in the "From:" field unless otherwise specified by the person composing the reply.

In all cases, the "From:" field SHOULD NOT contain any mailbox that does not belong to the author(s) of the message. [RFC 5322].

Friendly From (also known as: Display Name, Pretty Name) - The optional “display-name” phrase of characters as defined in the Address Specification of RFC 5322, i.e. [display-name] <local-part “@” domain>, e.g. [John Smith] <jsmith@example.com>.

FP – False Positive - email mis-identified as spam.



Header Fields (also known as: Headers) - The Internet standard for email specifies a heading format. The header is the part of the message that contains much of the routing information for the message. This includes the sender, recipient, subject and other information. It requires a specific format to allow programmatic parsing of the header data during delivery. Headers contain not only the "Subject:" line but a complete path that the email took along various machines on the Internet to reach its destination. Spam senders tend to forge various portions of the headers. Header fields are lines composed of a field name, followed by a colon (":"), followed by a field body, and terminated by CRLF [...]. [RFC 5322].

HELO - A command used in SMTP during the initiation of a mail exchange session. It nominally identifies the connecting mail server. Also see EHLO.

Host - [...] a host is a computer system attached to the Internet [...] and supporting the SMTP protocol. Hosts are known by names (see "domain"); identifying them by numerical address is discouraged. [RFC 5321].

IETF - Internet Engineering Task Force. The body responsible for developing internet standards and addressing technical issues. Generally meets formally twice a year. www.ietf.org

IFRAME (or "Invisible Frame") - An HTML tag that can be used to "source in" content from another URL within a web page. While IFRAMES have many legitimate uses on the web, they are often used by malvertisers to inject malicious content into a web page or ad.

IIM - Identified Internet Mail - A crypto based signing approach to authenticating email proposed by Cisco. <http://www.ietf.org/internet-drafts/draft-fenton-identified-mail-01.txt>

Incident - Unique occurrence of a malicious ad being submitted into the ad supply chain and served to users. Also referred to as a "malvertisement".

Insertion order - A purchase order between a seller of interactive advertising and a buyer (usually an advertiser or its agency). Typically, an online and automated process, allowing advertisers to place an order based on desired audience reach and frequency and with the ability to upload creative.

IP Address - A unique number assigned to a device connected to the Internet. An IP address can be dynamic, meaning it changes each time a connection is made (and thus when an email message is sent) or it can be static, meaning it does not change upon reconnection.

JavaScript - A web scripting language that can be used to embed dynamic content into a web page. JavaScript is run by a JavaScript interpreter integrated into a web browser and has access to the full HTML DOM (document object model), user interaction events such as mouse overs, clicks, etc, and third-party plug-ins. There are many legitimate uses of JavaScript, but it is often used by malvertisers to write malicious scripts. Note that JavaScript is distinct from the Java programming language and is a separate programming language of its own, which derives its name from the fact that its syntax is similar to Java. As such, the JavaScript security model is distinct from the security model implemented by the Java Virtual Machine (JVM) and the Java Applet Security model. JavaScript's security model is not as "sandboxed" as that of Java, and as a result can often be abused more easily by malvertisers.

MAAWG - Messaging Anti-Abuse Working Group. ISP centric member based trade organization. www.maawg.org

Malvertisement -- A malicious advertisement that exhibits behavior including, but not limited to, conducting a drive-by-download, delivering deceptive downloads such as fake anti-virus pop-ups and/or redirecting the user to sites that the user has not elected to visit.



Malvertising – The cybercriminal practice of injecting malvertisements into legitimate online advertising networks.

Malware - Refers to a broad range of malicious software delivered via exploits that attempt to execute on an "at-risk" PC or mobile device. May include a range of malicious software including key loggers, trojans, spyware, virus and the like. See Spyware.

MARID - MTA Authorization Records in DNS working group. Tasked with developing authentication standards within IETF, this working group was dissolved in September 2004 when consensus could not be reached on various issues. This was primarily due to the IPR assertions made by Microsoft and the inability to resolve licensing issues with Open Source advocates. <http://www.imc.org/ietf-mxcomp/mail-archive/msg05054.html>

MTA (also known as: mail server) - Mail Transfer Agent. A mail server which accepts, relays, receives or transmits mail. These SMTP servers and clients provide a mail transport service and therefore act as "Mail Transfer Agents" (MTAs) [...]. [RFC 5321]

MUA (also known as: email client) -Mail User Agent. A client application that allows users to send and retrieve email from their computers. Common MUAs include Microsoft Outlook, Thunderbird, Entourage, and Eudora. MUA's are the component within the SMTP system that is responsible for creating email messages for transfer to an MTA.

Mailbox and Address - As used in [RFC 5321 – SMTP], an "address" is a character string that identifies a user to whom mail will be sent or a location into which mail will be deposited. The term "mailbox" refers to that depository. The two terms are typically used interchangeably unless the distinction between the location in which mail is placed (the mailbox) and a reference to it (the address) is important. An address normally consists of user and domain specifications. The standard mailbox naming convention is defined to be "local-part@domain" [...]. [RFC 5321]

No-Script - A Firefox extension which offers protection for Firefox, Seamonkey and other Mozilla-based browsers. This free add-on allows JavaScript, Java and Flash and other plugins to be executed only by trusted web sites of your choice (e.g. your online bank). Use of No-Script is not recommended for all but the most sophisticated user and then only for limited purposes. <http://noscript.net>

Obfuscated Script - Web scripts crafted to prevent easy inspection of its malicious content or to counter pop-up blocker and analytics software. Execution of malicious web scripts often link to malicious servers to download additional malware or dynamically malicious content into a web page. They can cause the web browser to crash when an exploit is used to target buffer overflow vulnerability and fails. These obfuscated scripts are often hosted on hijacked websites and increasingly compromise search and display advertising. Typically, they are crafted to exploit end-of-life browser and application vulnerabilities, to download and install further malware, compromising user's personal information and financial data. Use of obfuscated script should be discouraged and disallowed.

OTA - Online Trust Alliance (OTA). Non-profit member organization focused on enhancing online trust and the vitality of online services through the advancement of best practices, collaboration, public policy and promotion of technical solutions. <https://otalliance.org>



Phishing - A form of identity theft in which a scammer forges email message to trick recipients into giving out sensitive personal information, such as credit-card, bank account, Social Security numbers or other data. The term was coined by the fraudsters who imitate legitimate companies in emails to entice people to erroneously share passwords or data. Recent victims include Charlotte's Bank of America, Best Buy and eBay, where people were directed to Web pages that looked nearly identical to the companies' sites.

PRA - Purported Responsible Address. Term defined and referenced by the SenderID protocol, this is the email address in the email body (RFC5322) headers that is responsible for the origination of the email according to an algorithm (patent pending) from Microsoft. This generally resolves to the RFC5322 "From" header but can also resolve to the Sender:, Resent-Sender or Resent-From.

PTR Record - Pointer Record. PTR is a Domain Name System record type (RFC1035), the common use of which is for publishing information used for Reverse DNS Lookups

PGP - Pretty Good Privacy. Software used to encrypt and protect email as it moves from one computer to another and can be used to verify a sender's identity

Re-direct - A redirect is a response that a web server issued to a web browser that instructs the web browser to obtain the requested content from another URL than the one originally specified by the client. Redirects are often used when one ad server syndicates (or sub-syndicates) ad space to another ad server. For instance, a Web publisher's ad management server might re-redirect to a third-party hired by an advertiser to distribute its ads to target customers; and then another re-redirect to a "rich media" provider might also occur if streaming video were involved before the ad is finally delivered to the consumer. Redirects are also used by the cybercriminal to change the content after the ad is being served.

Reverse DNS Lookup (also known as: Reverse DNS Resolution) - This is the determination of a domain name for a given IP address using the Domain Name System. The process of reverse DNS resolution uses the pointer DNS record type (see: *PTR record*). Reverse DNS lookup is a popular method for validating legitimate SMTP connections to an SMTP server, often identifying spammers who use unauthorized domain names from compromised IP addresses. If a spam filter or MTA can't match the IP address to the domain name, it can further scrutinize or reject the message.

RFC - Request For Comments. This is a format (and process) for internet standards from IETF. See OTA summary of relevant standards & their normative references.

https://otalliance.org/resources/authentication/auth_standards.pdf

RFC5321 -The internet standard for SMTP. This dictates how mail servers exchange mail.

RFC5322 - The internet standard for how the content of mail including some headers is formatted.

RFC 4406 - Sender ID: Authenticating E-Mail.

RFC 4407 - Purported Responsible Address in E-Mail Messages, see SenderID.

RFC 4408 - The internet standard document and reference for the Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1.

RFC 5617 - Author Domain Signing Practices (ADSP), see ADSP.

RMX - An earlier IP-based authentication standard on which SPF is based.



Rootkit - A program that fraudulently gains or maintains administrator level access that may also execute in a manner that prevents detection. Once a program has gained access, it can be used to monitor traffic and keystrokes; create a backdoor into the system; alter log files; attack other machines on the network; and alter existing system tools to circumvent detection. Rootkit commands replace original system command to run malicious commands chosen by the attacker and to hide the presence of the Rootkit on the system by modifying the results returned by suppressing all evidence of the presence of the Rootkit. Rootkits are an extreme form of System Modification Software.

SenderID (SIDF, Sender ID Framework) - The informal name for an anti-spam program that combines two existing protocols: Sender Policy Framework and CallerID. SenderID authenticates email senders and blocks email forgeries and faked addresses. Negotiated by Microsoft and Meng Weng Wong summer of 2004. Now a standard – RFC4407.

<http://www.microsoft.com/mscorp/twc/privacy/spam/senderid/overview.mspx>

SES - Signed Envelope Sender Protocol. This approach uses a cryptographic token to sign the return path. Many see it as complimentary to SPF. <http://ses.codeshare.ca/>

Signers - Elements in the mail system that sign messages on behalf of a domain are referred to as signers. These may be MUAs (Mail User Agents) MSAs (Mail Submission Agents), MTAs (Mail Transfer Agents), or other agents such as mailing list exploders. In general, any signer will be involved in the injection of a message into the message system in some way. The key issue is that a message must be signed before it leaves the administrative domain of the signer. [RFC 4871]

Smishing - SMS Phishing.

SMTP - Simple Mail Transport Protocol. This is the standard that dictates how internet-based mail servers exchange mail.

SPF - Sender Policy Framework. A standard for authenticating the Mail From: field in communications between MTAs. Some proposed versions include HELO checks. SPF is also incorporated into SenderID which is a merged proposal that includes Caller ID (Microsoft).

SPIM - Spam over Instant Message (IM). Typically used to send links for phishing or to get users to download malware.

SPIT - Spam over IP Telephony.

Spyware - Computer software that is installed to surreptitiously intercept the user's interaction with a computer, collect data without the user's informed consent and or take partial control of the user's machine. Spyware programs can collect various types of information, such as Internet surfing habits, but can also interfere with user control of the computer in other ways, such as installing additional software, and redirecting web browser activity. The software usually does not contain generally accepted standards of notice describing what the purpose and/or behavior of the software is nor does it usually contain visible or functioning choice mechanisms for complete uninstall. The programs are typically characterized by behaviors that can be considered deceptive if not harmful to the user and/or his computer.

SRS Sender Rewrite Scheme - Protects the return path (Mail From) by having each relaying MTA (Server) rewrite the headers in a specific way to provide accountability. <http://www.libsrs2.org/>

SSID (Service Set Identifier) – A name that identifies a particular 802.11 wireless LAN network.



Third-party ad server - Third party companies that specialize in managing, maintaining, serving, tracking, and analyzing the results of online ad campaigns. They deliver targeted advertising that can be tailored to consumers' declared or predicted characteristics or preferences.

Verifiers - Elements in the mail system that verify signatures are referred to as verifiers. These may be MTAs, Mail Delivery Agents (MDAs), or MUAs. In most cases it is expected that verifiers will be close to an end user (reader) of the message or some consuming agent such as a mailing list exploder. [RFC 4871].

addr-spec = local-part "@" domain

Web Site / Publisher - The web site visited and having ads served from it. A publisher also refers to an individual or organization that prepares, issues, and disseminates content for public distribution or sale via their web site.

© 2011 Online Trust Alliance. All rights reserved.

Material in this publication is for educational and informational purposes only. Neither the publisher, the Online Trust Alliance (OTA) nor the authors assume any liability for any errors or omissions nor how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. The views expressed in this publication do not necessarily reflect the views of OTA member companies or affiliated organizations.

OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. For updates visit No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database, web site or retrieval without the written consent of OTA.

For suggestions and clarifications to this glossary, email staff@otalliance.org