

Email Marketing

Email Marketing

Email marketing is a form of direct marketing which uses electronic mail as a means of communicating commercial or fundraising messages to an audience. In its broadest sense, every email sent to a potential or current customer could be considered email marketing. However, the term is usually used to refer to:

1. Sending emails with the purpose of enhancing the relationship of a merchant with its current or old customers and to encourage customer loyalty and repeat business.
2. Sending emails with the purpose of acquiring new customers or convincing old customers to buy something immediately.
3. Adding advertisements in emails sent by other companies to their customers.
4. Emails that are being sent on the Internet (Email did and does exist outside the Internet, Network Email, FIDO etc.)

Researchers estimate that US firms alone spent \$400 million on email marketing in 2006.

Advantages

Email marketing (on the Internet) is popular with companies because:

1. The advantage of a mailing list is clearly the ability to distribute information to a wide range of specific, potential customers at a relatively low cost.
2. Compared to other media investments such as direct mail or printed newsletters, it is less expensive.
3. An exact Return on investment can be tracked ("track to basket") and has proven to be high when done properly. Email marketing is often reported as second only to search marketing as the most effective online marketing tactic.
4. It is instant, as opposed to a mailed advertisement; an email arrives in a few seconds or minutes.
5. It lets the advertiser "push" the message to its audience, as opposed to a website that waits for customers to come in.
6. It is easy to track. An advertiser can track users via web bugs, bounce messages, UN-subscribes, read-receipts, click-throughs, etc. These can be used to measure open rates, positive or negative responses, correlate sales with marketing.
7. Advertisers generate repeat business affordably and automatically
8. Advertisers can reach substantial numbers of email subscribers who have opted in (consented) to receive email communications on subjects of interest to them
9. Over half of Internet users check or send email on a typical day.
10. Specific types of interaction with messages can trigger other messages to be automatically delivered.
11. Specific types of interaction with messages can trigger other events such as updating the profile of the recipient to indicate a specific interest category.
12. Green - email marketing is paper-free

Disadvantages

Many companies use email marketing to communicate with existing customers, but many other companies send unsolicited bulk email, also known as spam.

Internet system administrators have always considered themselves responsible for dealing with "abuse of the net", but not "abuse on the net". That is, they will act quite vigorously against spam, but will leave issues like libel or trademark infringement to the courts. Most administrators passionately hate spam, which they define as any unsolicited email. Draconian measures — such as taking down a corporate website with or without warning — are an entirely normal

Email Marketing

response to spamming. Typically, the "Terms of Service" in Internet companies' contracts allow this, so the spammer has no recourse.

Illicit email marketing antedates legitimate email marketing, since on the early Internet (see Arpanet) it was not permitted to use the medium for commercial purposes. As a result, marketers attempting to establish themselves as legitimate businesses in email marketing have had an uphill battle, hampered also by criminal spam operations billing themselves as legitimate.

It is frequently difficult for observers to distinguish between legitimate and spam email marketing. First off, spammers attempt to represent themselves as legitimate operators, obfuscating the issue. Second, direct-marketing political groups such as the U.S. Direct Marketing Association (DMA) have pressured legislatures to legalize activities which many Internet operators consider to be spamming, such as the sending of "opt-out" unsolicited commercial email. Third, the sheer volume of spam email has led some users to mistake legitimate commercial email (for instance, a mailing list to which the user subscribed) for spam — especially when the two have a similar appearance, as when messages include HTML and flashy graphics.

Due to the volume of spam email on the Internet, spam filters are essential to most users. Some marketers report that legitimate commercial emails frequently get caught by filters, and hidden; however, it is somewhat less common for email users to complain that spam filters block legitimate mail.

Companies considering an email marketing program must make sure that their program does not violate spam laws such as the United States' CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act), the European Privacy & Electronic Communications Regulations 2003 or their Internet provider's acceptable use policy. Even if a company follows the law, if Internet mail administrators find that it is sending spam it is likely to be listed in blacklists such as SPEWS.

CAN-SPAM compliance

Because the CAN-SPAM Act of 2003 authorizes a USD 11,000 penalty per violation for spamming each individual recipient, many commercial email marketers within the United States utilize a service or special software that helps ensure compliance with the Act. A variety of older systems exist which do not ensure compliance with the Act. To comply with the Act's regulation of commercial email, services typically: require users to authenticate their return address and include a valid physical address, provide a one-click unsubscribe feature, and prohibit importing lists of purchased addresses which may not have given valid permission.

In addition to satisfying legal requirements, service providers stepped in to help customers to set up and manage their own email marketing campaigns. The services provide email templates, automatically handle subscriptions and removals, and generate statistics on how many messages were received and opened, and whether the recipients clicked on any links within the messages.

Opt-in email advertising

Opt-in email advertising or permission marketing is a method of advertising via electronic mail whereby the recipient of the advertisement has consented to receive it. It is one of several ways developed by marketers to eliminate the disadvantages of email marketing.

Email has become a very popular mode of communication across the world. It has also become extremely popular to advertise through. Some of the many advantages of advertising through email are the direct contact with the consumer and is "inexpensive, flexible, and simple to implement" (Fairhead, 2003). There are also disadvantages attached to email advertising such as, alienating the consumer because of overload to messages or the advertisement getting deleted without getting read.

Email Marketing

Permission email marketing may evolve into a technology that uses a handshake protocol between sender and receiver (Fairhead, 2003). This system is intended to eventually result in a high degree of satisfaction between consumers and marketers. If opt-in email advertising is used, the material that is emailed to consumers will be "anticipated." It is assumed that the consumer wants to receive it, which makes it unlike unsolicited advertisements sent to the consumer (often referred to as spam). Ideally, opt-in email advertisements will be more personal and relevant to the consumer than untargeted advertisements.

A common example of permission marketing is a newsletter sent to a firm's customers. Newsletters like this are a way to let customers know about upcoming events or promotions, or new products. In this type of advertising, a company that wants to send a newsletter to their customers may ask them at the point of purchase if they would like to receive this newsletter.

With a foundation of opted-in contact information stored in a database, marketers can automatically send out promotional materials. The marketers can also segment their promotions to specific market segments.

Terms

An auto responder is a computer program that automatically answers e-mail sent to it. They can be very simple or quite complex.

The first auto responders were created within mail transfer agents that found they could not deliver an e-mail to a given address. These create bounce messages such as "your e-mail could not be delivered because..." type responses. Today's auto responders need to be careful to not generate e-mail backscatter, which can result in the auto responses being considered E-mail spam.

Auto responders are often used as e-mail marketing tools, to immediately provide information to their prospective customers and then follow-up with them at preset time intervals.

Such follow-up auto responders can be divided into two categories:

1. Outsourced ASP model — these auto responders operate on the provider's infrastructure and are usually configurable via a web-based control panel. The customer pays a monthly usage fee. This is easiest to implement for the end-user.
2. Server-side — enables users to install the auto responder system on their own server. This requires technical skills.

Auto responders are also incorporated into electronic mailing list software, to confirm subscriptions, unsubscriptions, posts, and other list activities.

A bounce message, or Delivery Status Notification (DSN) message, aka Non-Delivery Report/Receipt (NDR), Non-Delivery Notification (NDN), or simply a bounce is an automated electronic mail message from a mail system informing the sender of another message about a delivery problem. The original message is said to have bounced.

Click-through rate or CTR is a way of measuring the success of an online advertising campaign. A CTR is obtained by dividing the number of users who clicked on an ad on a web page by the number of times the ad was delivered (impressions). For example, if your banner ad was delivered 100 times (impressions delivered) and one person clicked on it (clicks recorded), then the resulting CTR would be 1 percent.

Email Marketing

Banner ad click-through rates have fallen over time, often measuring significantly less than 1 percent. By selecting an appropriate advertising site with high affinity (e.g. a movie magazine for a movie advertisement), the same banner can achieve a substantially higher click-through rate. Personalized ads, unusual formats, and more obtrusive ads typically have higher click-through rates than standard banner ads.

CTR is most commonly defined as number of clicks divided by number of impressions and generally not in terms of number of persons who clicked. This is an important difference because if one person clicks 10 times on the same advertisement instead of once then the CTR would increase in the earlier definition but would stay the same in term of latter definition.

Opt in e-mail is a term used when someone is given the option to receive "bulk" e-mail, that is, e-mail that is sent to many people at the same time. Typically, this is some sort of mailing list, newsletter, or advertising. Obtaining permission before sending e-mail is critical because without it, the e-mail is Unsolicited Bulk Email, better known as spam.

There are several common forms of opt-in e-mail:

Unconfirmed opt-in

A new subscriber first gives his/her address to the list software (for instance, on a Web page), but no steps are taken to make sure that this address actually belongs to the person. This can cause e-mail from the mailing list to be considered spam because simple typos of the email address can cause the email to be sent to someone else. Malicious subscriptions are also possible, as are subscriptions that are due to spammers forging email addresses that are sent to the e-mail address used to subscribe to the mailing list.

Confirmed opt-in (COI)

A new subscriber asks to be subscribed to the mailing list, but unlike unconfirmed opt-in, a confirmation e-mail is sent to verify it was really them. Many believe the person must not be added to the mailing list unless an explicit step is taken, such as clicking a special web link or sending back a reply e-mail. This ensures that no person can subscribe someone else out of malice or error. Mail system administrators and non-spam mailing list operators refer to this as confirmed subscription or closed-loop opt-in.

Some marketers call closed loop opt-in "double opt-in."

The term double opt-in was coined by marketers in the late 90s to differentiate it from what they call single opt-in, where a new subscriber to an e-mail list gets a confirmation e-mail telling them they will begin to receive e-mails if they take no action. This is compared to double opt-in where the new subscriber must respond to the confirmation e-mail to be added to the list.

Some marketers contend that double opt-in is like asking for permission twice and that it constitutes unnecessary interference with someone who has already said they want to hear from the marketer.

The term double opt-in has also been co-opted by spammers, diluting its value.

Opt-out

Instead of giving people the option to be put in the list, they are automatically put in and have the option to be taken out.

E-mail Authentication

E-mail authentication is a technique for validating that a person claiming to possess a particular email addresses actually does so. This is normally done by sending an email containing a token to the address, and requiring that the party being

Email Marketing

authenticated supply that token before the authentication proceeds. The email containing the token is usually worded so as to explain the situation to the recipient and discourage them from supplying the nonce (often via visiting a URL) unless they in fact were attempting to authenticate.

For example, suppose that one party, Alice, operates a website on which visitors can make accounts to participate or gain access to content. Another party, Bob, comes to that website and makes an account. Bob supplies an email address at which he can be contacted, but Alice does not yet know that Bob is being truthful (consciously or not) about the address. Alice sends a token to Bob's email address for an authentication request, asking Bob to click on a particular URL if and only if the recipient of the mail was making an account on Alice's website. Bob receives the mail and clicks the URL, demonstrating to Alice that he controls the email address he claimed to have. If instead a hostile party, Chuck, were to visit Alice's website attempting to masquerade as Bob, he would be unable to register for an account because the confirmation would be sent to Bob's email address, which Chuck does not control.

This degree of email authentication is considered by many anti-spam advocates to be the minimum degree necessary for any opt-in email advertising or other ongoing email communication.

- **Have questions? Find out how to ask questions and get answers.**

The email open rate is a measure primarily used by marketers as an indication of how many people "view" or "open" the commercial electronic mail they send out. One of the earliest metrics applied in email marketing, its continued use is controversial due to conflicting views on its usefulness.

Open rates are typically measured using an HTML IMG tag embedded in outgoing emails, calling for a small, transparent tracking image. When the client or browser used to display the email requests that image, then an "open" is recorded for that email by the image's host server.

The open rate for an email sent to multiple recipients is then most often calculated as the total number of "opened" emails, expressed as a percentage of the total number of emails sent or -- more usually -- delivered. The number delivered is itself measured as the number of emails sent out minus the number of bounces generated by those emails.

This method leads to problems with interpretation, since the request for the tracking image gives no indication of whether the email's recipient actually viewed or read the email or its contents.

In addition, many webmail services and email clients block images by default, or the recipient may elect to receive text-only versions of an email. In both cases, no image call can ever be made, further reducing the accuracy of the open rate measure.

As a result, open rates are broadly rejected as an absolute measure of a commercial email's performance. However, many marketers use open rates as a relative measure, for example to compare the performances of emails sent to similar recipient groups, but at different times or with different subject headers.