Real Businesses Send Spam, Too!

Unsolicited Commercial Email or Spam has grown at epidemic proportions. It is rapidly becoming the number one problem that Information Technology departments deal with on a day-to-day basis, surpassing computer viruses. The volume and percentage of unwanted email received in business and personal email inboxes is starting to overwhelm and drown out legitimate email. Although the vast majority of this bulk email is being perpetrated by individual spammers and a few large bulk mailers pushing pornography, gambling, get rich schemes, 'medicinal cures' and bootleg software, real businesses have been caught in the web also by committing several errors. The three ways a legitimate business falls into the Spam mode are: 1. Legal non-Compliance, 2. Violating Trust, and 3. Lack of Value. Legal non-Compliance Through the end of 2003 it was very difficult to comply with Spam laws as twenty six states had passed their own laws dealing either directly with the process of sending unsolicited commercial email or the format requirements of bulk email. With the passage of the Federal law - "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" or better known as the CAN-SPAM Act of 2003, it has become a lot easier to understand and apply the rules. Real businesses should have no problem complying with all aspects of the law and those that don't will find themselves in legal jeopardy for significant penalties. The process components of the law won't be an issue for real businesses, they don't fake the reply address, they don't hijack someone else's mail server nor do they contain falsified routing information. Where they are likely to fail are in three specific areas. 1) Neglecting to include a valid physical address in the body of the email. 2) Not having a functional Internet-based opt-out mechanism, which must be active for a minimum of 30 days after the email has been sent. 3) Failing to include clear and conspicuous identification that the message is an advertisement or solicitation. Most State laws approached this similar provision by requiring the use of the letters ADV: in the beginning of the subject line. The Federal doesn't specify how this is to be accomplished; thereby, leaving it open to a wide range of interpretation. There are several additional areas that are process related that may trip up the sender unintentionally. 1) The sender rents or purchasing a defective email list, for example one that has individuals that have already opted-out of email communications. 2) They use a 'tricky' subject line to entice recipients to open the message. Subject lines that stretch the truth could be identified as misleading the purpose of the email and therefore be a violation. 3) Agents or related 3rd parties that have business relationship with the firm send out Spam. This could put the company in jeopardy if it can be proven that they were aware of the related company's activities. Although the Federal law isn't perfect one significant advantage it does offer to real businesses is that there is now only one place they need to go to check the rules before a company embarks onto an email marketing program. Violating Trust Trust is one of the major stumbling blocks keeping the publics' enthusiasm for the Internet in check. And when it comes to providing their email address that is in the eye of the storm. The overwhelming concern people have about providing a company their email address is that it will be shared, loaned, rented, sold or carelessly unprotected. Sharing lists internally between product lines, departments, or divisions and externally with 'business partners' stretches the permission basis originally given by the subscriber. When opt-in lists developed at one website are resold to list brokers, real businesses that rent these lists automatically become spammers because recipients are typically applying this litmus test to commercial email they receive: "Email marketing is for product/service information I've specifically requested, Spam is sent without asking for it". Businesses embarking down the eMarketing path often have in-house databases that include email addresses of suspects, prospects, and clients. The conversion of these lists, developed on a relationship basis, to a formal subscriber list treads a fine line and should be considered very carefully before assuming that permission has been granted. Lack of Value Every time you send email to your list members, you will be judged, and in some cases, it may appear to have been done unfairly. In today's environment subscribers are now becoming annoyed at a variety of shortcomings, such as messages about products they seldom buy, messages that serve the sender more than the recipient, unsubscribe processes that don't work, 'hard sell' messages or even messages in formats that can't be properly displayed in the recipient's mail program. The plain simple truth is that even in a permission email environment, recipients are now applying their own tests for Spam whether they opted in or not. These are natural human reactions to the mailings they receive - it can be as straightforward as "Email marketing is email I like, Spam is email I don't like." How to Fix Real businesses need to insure that they aren't jeopardizing their brand name by meeting or exceeding the best practices for email marketing. Auditing the list, evaluating your content and insuring proper conformance with the documentation process in the permission mailing process are the key components to a successful campaign.

About the Author

The Natural History of Genes program website is now part of the Genetic. If you were looking for a particular page on the Natural.

Source: http://www.productsherbal.com