



# SENDING EMAILS BEST PRACTICES

Last year the amount of spam email sent globally increased by 100%, from 30 billion to 60 billion messages sent **per day**. With ever increasing amounts of spam being sent every day we spend more time sorting through our inboxes to find legitimate emails than ever before.

The result of this has been a growth in Email Defence and spam filtering; this however causes a problem itself. It is easy to create an email that appears to be spam to an Email defence Service.

Below are a few things you can consider to help your email reach its intended recipient.

If you are sending a message to someone you don't know then consider sending the email as plain text, rather than as HTML – A HTML email is simply an email that you can format with different fonts and images, plain text is exactly as it says, plain text. Spammers often use HTML computer code to hide "beacons." These are small graphics that when opened up triggers a "message opened" acknowledgement back to the sender.

Don't send attachments if the recipient does not know you. This is because many spammers and virus writers use attachments to spread pornography and malicious computer code, spam filters and anti-virus software sometimes view attachments with suspicion. In your message subject line, be as specific as possible. This point is especially relevant because spammers have become smart enough to write messages with perfectly plausible subjects, such as "Conference call tomorrow at 10 a.m." Do not send a generically titled message, but give as many straightforward details as you can in the subject line. In other words, instead of typing "Conference call tomorrow at 10 a.m." in your message subject line, trying something such as "Conference call with audit committee tomorrow at 10 a.m." Given the specifics of that subject line, spam filters would recognize the message is not generic, and would probably let it through to the recipient's inbox.

Even if your message is legit, stay away from message subject words that spam filters look for. A few suspect terms to avoid include: "for only" and "hello," subject lines that start with dollar signs, and words like "free" or "guaranteed" spelled with all capital letters.

## **Newsletters**

Ensuring that your solicited newsletter is successfully delivered to your recipients can also be tricky. Not getting it marked as spam depends on the way you format your emails and how you write your subject line.

A few rules to take into account.

1. Never send unsolicited emails. Ensure that people on your subscriber list are willing to receive your newsletter before sending.
2. Provide an opt-out option in your newsletter to allow recipients to unsubscribe if they wish to.
3. When collecting names and email addresses from your website, ask the new subscribers to add your email address to their address book. This will prevent spam filters from blocking your newsletter. (more important for the online web based email services such as Hotmail, Gmail and Yahoo).
4. Whenever a subscriber wants to be removed from your subscriber list, delete his email address from your subscriber list as soon as you can, you could be recognized as spam if not.
5. HTML emails are becoming more popular and most spam is HTML formatted. Thus, differentiating between opt-in newsletters and spam messages is difficult. Therefore, if you are sending your newsletter in HTML format, send a plain text alternative newsletter as well.
6. Investigate about newsletter advertisers before placing their advertisements in your newsletter. Your newsletter will be filtered in case their website URL has been previously used to send spam.
7. Your language used in your newsletter should be appropriate. Do not include topics such as making money or pornography which make your email look like spam. Do not use extra punctuation or odd spelling in your message.
8. Use images scarcely as messages that are entirely images are considered spam.
9. Include a link to files via a website URL instead of making use of attachments.
10. An effective way of ensuring that your newsletter is delivered and not marked as spam is to use an email marketing firm to distribute your newsletter.

List of things guaranteed to get you on a spam blocked list.

- Body of message contains one or more lines of "YELLING" (i.e., all-caps)
- Message includes Microsoft executable program
- Message body has at least 70 percent blank lines
- Message 'From:' field appears to not contain a real name
- Message 'From:' field ends in numbers
- Message header contains numbers mixed in with letters
- Message subject includes the term "offer"
- Message 'To:' field contains spaces
- Message 'Reply to:' field is empty
- Subject has exclamation mark and question mark
- Subject is ALL-CAPS
- Message subject starts with an advertising tag
- Message 'From:' field contains the term "friend"
- Subject contains "As Seen"
- Subject starts with dollar amount
- Subject contains "Double Your"
- Subject contains "For Only"
- Subject contains "FREE"
- Subject contains "Free Instant"
- Message contains excessive images without much text

- Message body claims not to be spam
- Message header indicates message was sent directly from dynamic IP address

The **COSMIC Email Protection Service** is a comprehensive and effective spam, phishing, virus, worm and email threat blocking service. Provided by a local East Devon Company always just a phone call away. Get your inbox back for pennies a day.

Visit [www.cosmic.org.uk](http://www.cosmic.org.uk) or call 01404 813226 for more information and an explanation of spam, phishing and viruses.