Best Practices For Sending Email

Stricter and more sophisticated spam filters flag more email as spam than ever before. To ensure that the person-to-person emails that you send through the Perfect Patients mail system reach their destination, use the following best practices. Most reputable email providers also provide their own recommendations, and we encourage you to search out and read those as well.

Message format

Make your message layout as simple as possible. Avoid complex formatting, elaborate layouts, and multiple images. This is especially important if you use HTML content programs like Microsoft Publisher, which create complex HTML and styles, to create your content.

If you send HTML email, ensure that it is properly constructed. Items like missing or empty tags, poor formatting, and nonstandard conventions are spam indicators.

If you need rich media content, link to a media-rich page on your website.

Use a mail client that provides features such as providing HTML and text versions of the message content, correctly constructed and formatted email headers, and adherence to specifications for sending email.

Links

Do not use links that contain IP addresses. All reputable sites on the Internet use domain names to identify themselves. Using IP addresses is a trigger for spam filters.

If you link to other companies' sites in your message content, ensure that they are reputable sites. Providing links to disreputable sites in your message content will cause your email to be marked as spam.

Spammers use abbreviated URLs to mask the destination of the link, which causes spam filters to flag messages with shortened URLs as spam.

Word Choice

Avoid the following spam triggers:

- Excessive or unusual punctuation (especially exclamation points (!) and question marks(?))
- Capitalization of all letters (LIKE THIS)
- Words such as *urgent*, *free*, and *guaranteed*
- Spaces between every letter in a word, such as H e l l o

Use personalized greetings and salutations. For example, use “Hey Bob” instead of “Hey” or “To Whom It May Concern.” Generic greetings make your content more likely to appear as unsolicited mail to spam filters.

Do not include a disclaimer that your email is not spam, and do not claim compliance with some legal criteria. Legitimate email does not need to advertise compliance.

Use conversational language. Message content that follows a consistent limited verbiage or template will appear to be computer-generated content and will be flagged as spam. Spellings like “str@nge” or “g00gle” in your emails will classify the emails as spam.

Do not overtly reference topics that usually indicate spam. For example, highly recognized brands, medications, sexual innuendo, drugs, and financial schemes are easily recognizable as topics contained in spam. An email that mentions topics considered spam will cause your email to be marked as spam, even if the intent of the message is legitimate.

Attachments

Attachments are a common way of distributing viruses, making filters increasingly strict about attachments. Blocking zip file attachments is a prolific example of this.

Avoid attaching files to your messages. Use sharing platforms such as DropBox, Box.com, etc.

If you need to send attachments, use attachment names that are simple and specific, and spell them correctly. Oddly named or spelled attachments are a common way of transporting viruses.

Maximum file size for attachments is 50MB