

## Why Email Best Practices?

When addressing the topic of email in any type of communication, one must consider the concept of spam. This brings up some key questions we must answer, ones that do not have simple answers:

- Is our email a legitimate email or is it spam?
- What are the consequences of sending it out if it's considered spam?
- When can I send email advertising to a list of email addresses?
- When can't I?

The answers are available, though only we can answer them, and to answer successfully, we must be as objective as possible. The following information aims to inform what current standards are in order to come to an objective decision about our email marketing strategy.

### Email communication spectrum: legitimate vs. spam

Consider the entire spectrum of email communication. At one end, you have email that nearly everybody considers spam. Qualifications:

- You didn't ask for the email
- You don't know the sender
- The subject line is misleading and isn't relevant to the content
- You have no interest in the content
- There is no way to get the sender to stop sending you email

The other end of the spectrum is an email that nearly everybody considers a legitimate email based on recognized best practices.

***Example:** you visit an online pet food store. You use a web-based online form to submit your email address and tick a box that says "send me a weekly email with special offers on cat food". The store sends a confirmation email, which you respond to. From then on, you receive an email once a week with special offers on cat food.*

However, even at these two ends of the spectrum, some will believe that any kind of email is legitimate, and conversely, some will believe that any kind of marketing email is spam.

We want to be as close as we can to good end of the spectrum. However, there is no clear line that defines a legitimate email from spam. This determination is different for each individual email recipient. What is clear is that the further we move away from the best practices of email, the **greater chance/percentage of recipients will think that our email is spam**. What we can focus on is managing the probability of being perceived as spam by choosing to follow best practices.

***Example:** See the cat food special offer email. Suppose the pet food store includes a special offer for dog food in the email. Most people wouldn't be bothered, but a small percentage would begin to see that email as spam.*

*Suppose that you are a regular customer and buyer of cat food. You never specifically requested special offers by email, but the store sends them to you anyway. Some people wouldn't be bothered, but a larger percentage would see the email as spam.*

*Suppose the specials offers sent by email were for cat, dog, fish, hamster, bird, and monkey food? Probably a higher percentage would see the email as spam.*

*What if you've never shopped at the pet food store, and don't have a pet? Nearly everyone would agree that this email is spam.*

### **Risk Assessment: What makes a legitimate email?**

Best practice emails are based **on permission**, meaning that the recipient of that email has explicitly asked for those emails, or explicitly consented to receive them. Qualifications are:

- The recipients requested the email
- The email arrives in a timely or regular manner
- The email is relevant to the needs of the recipient
- The email allows the recipient to quickly grasp who sent it and what it's about
- The recipient can stop getting the emails easily and any time

To simplify, it means the recipient took deliberate action with express purpose of getting those emails.

***Example:** ticking a box marked "add me to your email list".*

***Example:** during an online ordering process, **ticking a box** if you **don't** want to get emails*

***Example:** during an online ordering process, **not ticking the box** if you **don't** want to get emails*

In the last example, the recipient has given you permission to send them emails, but not **explicit** permission. Some people will be surprised to find that they are on an email list. Those who find this undesirable will consider the email spam, and we will have moved towards the bad end of the email spectrum.

### **Matching Expectations**

Another aspect of email best-practices is fulfilling recipient expectations. Any email recipient has expectations of what information and content they are going to get. The further away from meeting these expectations, the more likely the recipient will consider the email as spam. It's important for people to know exactly what they are going to get before giving us their email address. They should know what will be in the emails they receive, and how often the emails are sent. Sometimes a sample email can be helpful to completely meet expectations.

This is important because **permission is always temporary**. Renewal and upkeep on recipient's permission must be cultivated through our email practices, by staying on the legitimate end of the email spectrum and matching recipient expectations. Interests and needs of our recipients can and will change over time, and we must account for this. Recipients can perceive spam not just emails that they never want, but also emails that they don't need, hence the importance of matching the right email content to the right recipient through consideration of audience targeting. The more assumptions we make, the greater chance we head towards the spam end of the email marketing spectrum.

### **So What? Why is sending spam bad?**

Simple compliance with [anti-spam law](#) doesn't mean protection from any negative effects of sending spam. Consider the following:

- Recipients do not decide whether you are spamming based on anti-spam law criteria. Each recipient has their own idea of what is spam and what isn't. They don't care what the law says.

- Most of the negative consequences of sending spam have nothing to do with legal punishment, and the ability to prove compliance won't save you from negative consequences.
- The only thing anti-spam compliance protects from is prosecution by authorities.

### **What are the real consequences of sending email that's considered spam?**

Every time an individual decides we're sending them spam, that person's relationship with our institution is damaged. Our image, brand, and reputation weaken in the eyes of that recipient. It's folly to underestimate how much people dislike businesses or organizations that send unwanted and unsolicited emails.

Ultimately, it doesn't matter if the sender thinks they deserve the spam moniker or not. It doesn't matter that some recipients think the sender's emails are more valuable than other recipients. The more you move down the spam end of the spectrum, the higher the percentage of people will regard email messages as spam, and the greater the risk of negative consequences and damage to our brand.

The real risk with these consequences is that they often are undetected. Most people who think you're sending spam don't complain to the sender. Instead, they complain to others who have the power to stop email delivery, or simply mark the sender as spam so they never see the emails, even if they still are successfully received in their inbox.

### **Conclusion**

Being considered a spammer risks an institution's reputation and customer relationships. To prevent this, we must continuously assess whether our email plan meets these criteria of legitimate email and avoids the consequences of being considered spam.

Excerpts, quotes, and information taken from:

<http://www.email-marketing-reports.com/basics/permission/>

### **Emma permission standards:**

*"To ensure compliance with federal legislation and our terms of use, make sure "everyone" in the list you're importing:*

- *Is a customer, member or subscriber of your business or organization;*
- *Has signed up or otherwise asked to receive your emails:*
- *Has purchased a good or service from you in the past 18 months*

**NOTE:** *You may NOT email any address that has been purchased, rented, appended, harvested or in any way obtained from a third party or without the email address owner's awareness and permission. In addition, you may NOT email any address that was initially obtained more than 18 months ago and has not received any correspondence from you since that time."*

In all likelihood, the Emma permission standards exist to stay compliant with the [CAN-SPAM Act of 2003](#), a description of which is available on the FTC's Bureau of Consumer Protection website (Emma is following item 7):

<http://business.ftc.gov/documents/bus61-can-Spam-act-compliance-guide-business>