How Spam Filters work

In order to increase the quality of the sendings, brands often choose to work with an email service provider (ESP) instead of sending the emails on their own. The ESP then asks the brand to set up SPF, DKIM and other standards. But why is this needed? Let's have a brief overview on how a typical multi-stage spam filter works today.

IP Filter

The very first information a potential receiver of an email gets is the IP address of the sending server who tries to connect. If the IP address is known to be a source of spam, it's most likely that the receiver will return an error code that it won't accept the email or even worse, simply reject the connection.

As a sender of emails it's highly important to monitor the IP reputation of the sending email servers. Brands who rely on the services of an ESP, of course pass the responsibility for that to the ESP.

Receiver of emails often use reputation data from third parties in addition to their own to get better results. This can be blacklists which contain IP addresses with a bad reputation or whitelists like the Certified Senders Alliance whitelist, which contains IP addresses from certified senders fulfilling high quality standards and therefore with a good reputation.

Authentication

Even if a brand is working with an ESP they need to set up some records in their domain for technologies like SPF, DKIM and DMARC to work. Why is that important? These three technologies enable the receiver to authenticate the sender. Simply put, the receiver can tell if an incoming email is legit and really from the brand indicated by the senders address. Receivers can identify malicious emails with forged sender addresses and filter them out.

Implementing these technologies doesn't necessarily lead directly to higher delivery rates for brands sending emails, but it's essential to be distinguishable from all the spammers out there and it's needed to build up trust.

Content Analysis

Until now the receiver did only work with information from the connection or from the email header. Next step is analyzing the content of the email. This can include certain word filters, text to image ratio, patterns of typical bad or good email, reputation of web addresses linked in the email, reputation of attachments, of course traditional virus scanning, and more.

User Engagement and User Filters

Many receivers also check how the end user reacted on similar emails in the past. If a user didn't like emails about a certain topic in the last years it's most likely he won't like it now. Or if the majority of the end users flag the emails of a specific campaign as spam, it's likely that these mails will end up in the spam folder for the other users as well. Last but not least, users can set up individual filter rules. Keeping user engagement in mind, it's obvious that technical solutions aren't enough. The content has to be interesting and relevant as well.

Conclusion

Spam filters are getting more and more sophisticated and complex. The best way to successfully reach the inbox is to not try to outsmart these filters, but to follow best practices and send the best email you possibly can. ESPs can take care of a big part of this, but brands need to cooperate with them to set up advanced technologies like DMARC. The CSA certification ensures that a sender cis compliant with these best practices and ensures optimal delivery.

More helpful documents like the “eco Directive for Permissible Email Marketing” can be downloaded for free on https://certified-senders.eu/documents/

Authors: Technical Team of the Certified Senders Alliance