DMARC and Domain Alignment in Email Marketing

It's Not About Trust, It's About Control

It's not always the case that everything runs smoothly on the Internet. Spam, phishing, Man-in-the-Middle attacks, spoofing; the list of sophisticated methods villains of the Internet utilize, is long. In almost all cases a medium is involved which we all use on daily basis: Email. For obvious reasons, cyber-criminals do not use their own identities. Rather, they like to make use of well-known companies and brands; often payment services, banks, online shops, or delivery companies. Basically, every brand can be affected.

The sheer number of traps and pitfalls raises suspicion. So much suspicion that many Internet Service Providers (ISP) do a thorough inspection of each email, before delivering it to the recipient. Smaller ISPs even do not accept incoming email on the first delivery attempt, trusting that a reputable sender will make another attempt (Greylisting). Other ISPs demand that the sender is authenticated or certified by means of a whitelist (like the one of the Certified Senders Alliance, CSA) in order for email to be delivered.

This is an issue for brands. Their goal is for the emails to actually reach the addressees' inbox. Trust is the most important door opener for ISPs. If an email sender is regarded as trustworthy, the chances are high that the email will be delivered to the inbox. This trust, labeled "Computational Trust" by Tobias Herkula, Manager Anti Spam Research Team of Cyren, must first be earned. This is where domain alignment comes into play. Domain alignment means that the domains used in SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) must, at least partially, match the From address of the email. For further information regarding Protect Brand Indetity in email see here.
SPF and DKIM are well-known methods of email authentication. The recipient will see the From address as the sender's address. To give an example: A traditional letter on paper will usually display the sender's address on the envelope and on the letter itself. Both will match with the name in the signature. This is common sense. No one would trust a letter that has different addresses on the envelope and in the text.
Unfortunately, it's not that easy for email. Many marketeers use external Email Service Providers (ESP). Here the From address of the email's header and the physical address, the address of the sending host, do not match.

Additionally, domain alignment is a mandatory precondition for implementing DMARC (Domain-based Message Authentication, Reporting and Conformance), another authentication method supported by many big ISPs like AOL, Microsoft, or Google. DMARC is based on SPF and DKIM and helps in identifying the email's sender. Moreover, the brand can define how to handle emails which only appear to be sent by them.

All in all, a good reputation and trustworthiness is tremendously important for marketeers in email marketing because they have a direct impact on the deliverability of emails. By implementing DMARC and the related domain alignment, brands can ensure that their identity cannot be misused which would have a big impact on their reputation. Consequently, marketeers in the field of email marketing should discuss DMARC with their email service providers. More information about DMARC and domain alignment can also be found in the Certified Senders Alliance library at https://certified-senders.org/library/.

Author: Sebastian Kluth, Technical Lead CSA