# EMAIL @ AUTHENTICATION

VerticalResponse
www.verticalresponse.com

Tweet

follow us on:

# EMAIL AUTHENTICATION

## How VerticalResponse Sets You Up for Inbox Success

## What is Email Authentication?

Email authentication – in very simple terms, is identifying the sender of an email. When people talk about authenticating email, they are referring to a handful of different methods email senders can implement that allow the receiver of an email and the Internet Service Provider (ISP) to validate the identity of the sender. If the identity of the sender cannot be authenticated, then ISPs can block the message or put it through additional filtering. So without authentication, a message's chance of being filtered or blocked is greatly increased.

*VerticalResponse employs all necessary authentication processes that need to be in place.*

## What Are The Different Methods Used To Authenticate Email & Why Are They Important?

1. **Sender ID** and **SPF** record checks both verify the identity of the sender by ensuring the From Address is properly associated with the sending IP Address that the mail is coming from. An IP Address is essentially the "address" of your computer in the digital world.

2. **Domain Keys** were designed to verify that the sending domain really belongs to who the email says it does.

3. **DKIM** is often referred to as the next generation for Domain Keys, digitally signing the email verifying sending domain and message integrity.

It is important to have these mechanisms in place as high volume emailers. These mechanisms allow us to build a sending reputation by enabling the receiving email networks to recognize that VerticalResponse is sending the email (and as a result it can be trusted not to be spam).

We have built a strong sending reputation over time and are able to get great inbox delivery rates. Without these mechanisms we would not be a trusted sender and could easily be blocked, or see mail delivered to the bulk folder.

# Why is Authentication Important?

One particularly frustrating type of spam is called **spoofing**. This is when a sender of an email pretends to be or "spoofs" the identity of someone else in order to have a better chance at having the message delivered and read. This is against the **law** and ISPs spend a lot of time fighting this type of spam. By authenticating the email sent from our system, receiving email networks are able to recognize that VerticalResponse is sending the email, and that it can be trusted.

While authenticating email is important for the reasons above, there are no technical standards for authenticating – which is why there are several methods. Some of these authentication mechanisms need to be in place to ensure specific ISPs are able to recognize VerticalResponse as the sender. For example, Sender ID needs to be in place to ensure that Hotmail specifically can recognize us. And we must have DKIM in place to have a feedback loop with Yahoo.

In fact – in order to get the best possible inbox delivery rates with the ISPs that offer them – we need to be running a tight ship and have all these in place from SPF to Sender ID to DKIM.

# Does Authentication Guarantee Inbox Placement?

It's important to clarify that having these authentication mechanisms in place will not completely solve delivery problems. Validating a domain has nothing to do with the content or value of the message; it only validates the identity of the responsible sender.

Authentication will not balance out weak practices used in content creation, permission standards, bounce handling, complaints or filter triggers.

So by ensuring that you are following good mailing practices, combined with these authentication methods, your mail will be set up for inbox success!