How to Protect Your Sender Reputation with Email Authentication and Verification

by Amber Iven - Monday, April 26, 2021

https://www.searchbug.com/info/email-authentication/

Email authentication verifies that an email is legitimate. It proves that it comes from who claims to send it. This is very important, especially for SaaS apps, as email scams and phishing abound.

Have you ever gotten an email from, say, “Paypal” (not “PayPal”) saying that your account has been suspended and you need to click the button to login and check your information? Email imposters impersonate companies from banks to social media platforms and other trusted companies in an attempt to get access to customer login information and sensitive data.

This fraud is an issue for you as a business owner or app developer. First of all, if an imposter sends a series of emails to your users that compromises their information, those users lose faith in you and your business. Even though they shouldn’t have trusted the fake email, it’s your reputation on the line.

Second, you want to make sure your users receive your legitimate emails. So how can you make sure they get the right ones and avoid the fakes? Email authentication and verification can help ensure your users get the good emails and not the bad ones.

What is Email Authentication?

Email authentication prevents fraudulent uses of email by verifying that it is not forged. Like in the example above, email authentication helps prevent scammers from sending emails under the guise of a trusted company.

However, you’ve probably received fake emails from senders posing as PayPal, Amazon, Apple, etc. So as you can see, fraudsters are getting very good at passing authentication protocols. But there are ways you can protect yourself and your business.

If you take a look in your spam folder right now, you’ll see a number of emails you probably don’t recognize that did not pass authentication. The email authentication process goes as follows:

First, when your business sends an email, you establish rules that allow emails from your domain name to be authenticated. Then the email sender publishes these rules. Think of it like a digital ID. These rules are identifiers that can only be matched by the legitimate sender.

When the receiving mail server gets the email, it authenticates the message by checking the rules published by the domain owner against the message it received. If it doesn’t pass authentication, the email gets flagged or rejected. If it does match, the email is delivered.

This is great news when it comes to preventing fraudsters from impersonating your business and sending your users fake emails. However, it still doesn't guarantee that your emails will make it into your users' inboxes even though your emails are authentic.

There are a number of factors that contribute to the deliverability of your emails. But basically, you want as many of your emails to get opened as possible. That means you must avoid sending messages to accounts that will never receive them. We'll tell you how.

What is Email Verification?

You want to be sure your emails make it into your users' inboxes. So you have to be sure your customer email addresses are valid and that your emails don't land in their spam folders.

Email verification is the process of validating email addresses. The verification process identifies addresses that are fake or invalid, addresses that are catch-all, and addresses that are spam traps (more on this in a second).

These email addresses enter your database most commonly through webforms. Legitimate users will enter incorrect email addresses to avoid being flooded by unwanted emails. About 60% of consumers provide incorrect information on purpose. Specifically regarding email addresses, about one-third of consumers give a fake address.

That is a large portion of your data to consider, and that's just the portion that's intentionally entered incorrectly. That doesn't even account for typos that enter your database. Fortunately, there are a few things you can do:

How to Verify Email Addresses

First, to prevent unintentional mistakes like typos and missing domains, you can set up validation error messages. This alerts users to mistakes in formatting so that they can be corrected before the data is submitted.

Second, you can set up an email validation API that catches and discards fake, invalid, catch-all, and spam trap email addresses before they ever enter your database. The data is verified in real time at the point of entry. This way you know that only good data is available for you to use.

Third is batch email verification. You can (and should) use this tool if you already have a list of customer email addresses that haven't yet been verified. Once the invalid email addresses are identified, you can weed them out of your list and improve your overall deliverability.

If you have a clean list already, or you're using the email validation API to verify data at the point of entry, you should still conduct a regular "cleaning" using batch email verification. Emails that are good when you collect them change over time. This is called data decay and about 30% of customer data decays each year. Data decay results from data that changes or becomes outdated.

So once you have all of your customer data verified, you should still check it regularly---at least twice a year---to catch those email addresses that change or become abandoned. That way you don't waste time and money sending emails to customers that will never see them. And consequently, you improve your sending reputation by increasing your open rates and decreasing bounces and unopened messages.

How Bad Email Data Enters Your Database

Earlier we mentioned three categories of email addresses: fake or invalid, catch-all, and spam traps. This is what we mean by those terms:

Fake and Invalid Email Addresses

Again, fake email addresses are entered intentionally by users to avoid receiving your messages. Invalid addresses could be those same fake addresses that don't lead to an actual inbox, or they could be addresses that are accidentally entered incorrectly and therefore won't receive your messages.

Catch-all Email Accounts

Catch-all email addresses are used commonly by corporate email servers. This means that whether the email address is valid or not, the message will be sent to the "catch-all" account for review. For example, if you have firstname.lastname@domain.com, but the user's name is misspelled, that message might be sent to a catch-all account (based on the domain name) to verify whether the message is legitimate or spam.

So, if your email verification results in a "catch-all" status, you know there might be a mistake with the address because it didn't hit your customer's account.

Spamtraps

A spamtrap is an account that is not used by a real person but is monitored to catch spam senders. It is, like the name suggests, a trap.

Do you have an old email account, maybe one you set up as a teen, that you never officially deactivated? You probably just abandoned it for a new address. These old, outdated email accounts can be repurposed as spamtraps.

Because of your inactivity on the account, it's unlikely that anyone sending mail to that account got the address legitimately. So a sender to that account likely got the address illegally or unethically. In this way, the old email account repurposed as a spamtrap can identify and block these senders as spam.

Someone might actually submit this old information to you knowing that they don't use the account and won't have to worry about your future messages. But if it's been repurposed as a spamtrap after all this time, there's a chance you could be flagged if you send mail to it.

Spambot Submissions

Finally, you want to catch email addresses submitted by spambots, too. Spambots can submit forms to get access to user data and spam their accounts.

Sometimes the information on bot submissions is clearly unintelligible and fake. But are you or someone from your team manually looking at this information on a daily basis? The best way to weed these out, especially since they can be submitted as actual addresses just not by the people who own them (you risk TCPA violation here…) is to verify them either at the point of entry or via cleaning process.

You protect yourself as well as your customers by keeping these bot submissions out of your system. For more information, check out our article on How to Prevent Bots from Submitting Forms here.

How Bad Email Data Affects Your Sending Reputation

Your sending reputation is based on a number of factors. You can check out our in-depth article here on how to get your messages into your customers' inboxes. But for our purposes here, we're going to simplify it.

Consider all of those different types of email addresses that can enter your database that will never actually receive your messages. Not only do you want to save yourself time and money by not emailing invalid accounts, you also want to make sure your emails make it to the legitimate addresses.

Your sending reputation is based on how successful your messages are and vice versa. If a large percent of your emails bounce (a "return to sender" situation), are left unopened, or are marked as junk or spam, your sending reputation suffers. A poor sending reputation means that the chances of future emails going straight to the junk or spam folder increases.

So the more successfully your messages reach legitimate inboxes, are opened, read, even forwarded, the better your sending reputation becomes. And the better your sending reputation, the better your chances of landing your messages in your customers' inboxes.

Getting rid of those "bad" email addresses listed above by using email verification tools keeps you from sending undeliverable messages and protects you and your customers.

How to Implement Email Authentication

We covered how to verify your email list to improve your email deliverability and consequently your sending reputation. But how do you properly configure email authentication? We're going to get technical for a minute….

There are three different standards that enable email authentication: SPF, DKIM, and DMARC.

The **Sender Policy Framework (SPF)** allows you, the sender, to determine which IP addresses are allowed to send email from your particular domain.

DomainKeys Identified Mail (DKIM) provides an encryption key and digital signature that only you

can match. Without it, fraudsters will fail to pass this level of authentication if the message is faked or altered.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) uses SPF and DKIM to authenticate an email message. DMARC allows email senders to determine how to handle email messages that do not pass SPF or DKIM authentication tests.

They can be sent to the junk or spam folder or undelivered altogether. This protects your reputation by preventing unauthenticated senders from emailing from your domain. It also helps to identify patterns and more consistently keep spam and phishing attempts out of users' inboxes.

An ideal email authentication system uses SPF, DKIM, and DMARC together. You can work with your development team or domain administrator to make sure they get set up properly.

How Email Authentication and Verification Affect Your Sender Reputation

Configuring email authentication helps to make sure that no one can forge your domain. That means that your users avoid receiving spam emails and phishing attempts from fraudsters using your brand as a front. However, it also helps make sure your legitimate emails get to your users' inboxes.

By configuring email authentication, you increase the likelihood that receiving mail servers will recognize your IP address and domain and trust the authenticity. Therefore, the receiving mail server will deliver your emails more consistently.

But keep in mind the other factors that secure your sending reputation as well. You can use an email verification tool to weed out those bad email addresses that increase your bounce rate. The higher percent of your emails that are delivered successfully the better your sending reputation.

At that point it's just an endless cycle: your emails get delivered, your reputation improves; your reputation improves, more emails get delivered. Check out Searchbug's email verification tools and clean your email list today!

Searchbug.com