How to Protect Yourself from Email Spoofing

by James Miller - Wednesday, September 25, 2019

https://www.searchbug.com/info/email-spoofing-protection/

Email spoofing is a cornerstone of spam, malware, and worm attacks. These attacks on personal email addresses are bad enough. But, an email cyber attack can be devastating if it breaches a business email database.

So, understanding email spoofing and knowing how to stop spoofed emails are critical for protecting your customer information and business reputation. Fortunately, it's easy to take preventative measures.

Let's start with the basics.

What is email spoofing?

Email spoofing is sending emails with a forged sender address. Spam and phishing emails often use email spoofing to trick email recipients into thinking that the email is from a legitimate source, like a friend or business.

Emails get tagged with two pieces of information when they're sent:

MAIL FROM: this is the email address that the email came from. There are two components to the MAIL FROM data: the email address that is visible to the end user, and the email address that only the email servers see.

The email address that's visible to the end user is the one that's most commonly forged, since the spoofer wants the receiving email server to accept the email.

RCPT TO: this is the email address that the email is being sent to. This is not always visible to the end user.

Your email client uses these two data points to generate the **From** and **Reply-to** fields you see when you get emails. Spoofers forge the **From** name and email address to trick you into opening the email.

Legitimate email spoofing

There are situations where spoofing is used legitimately. Some email systems are set up with an email forwarder. The receiving email server will only accept emails from the email forwarder. Incoming mails are spoofed to look like they've been sent from the email forwarder so the receiving email server will properly inbox emails.

However, the vast majority of email spoofing is illegitimate. So, anti-spoofing measures have essentially zero negative impact on your email correspondence.

The other good news is that spam folders and authentication protocols catch most spoofed emails. However, you may need to have your email administrator set up authentication protocols, if you have an email service provider that sends emails on your behalf.

Email authentication protocols are good passive protection. But, there's also a way to actively protect yourself, especially if you send marketing emails.

How to stop spoofed emails with email verification

This might seem confusing at first, because spoofed emails are ones that you *receive*. But, here's how email verification protects you from email attacks.

A business's email database is a gold mine for spammers and scammers. So, many cyber criminals will sign up for your marketing email list. Then, when you send them an email, they can reply to that email with a scam email. Marketers also use this tactic to get email addresses for cold email.

Their email is more likely to be delivered, because it's a reply email. And, it's more likely to be opened, because it looks like the email is from a marketing lead. Usually, the scammer will forge the sender information so it's harder for you to find the email and remove it from your database.

This sort of email attack can compromise your entire customer email database, since malicious software usually mines contact lists for emails. So, email verification is incredibly valuable for protecting your customers and business reputation.

However, standard email verification won't completely protect you. Many email verification services only tell you whether or not the email is valid. A valid email address is simply an address which exists and can receive emails.

This type of email validation doesn't warn you if an email inbox is toxic or dangerous to send emails to. So, you need a more complete email verification service that also detects:

- Spam traps.
- Dangerous inboxes.
- Disposable emails.
- Bot created email addresses.

With this information, you can identify and remove malicious email addresses. Checking emails one-by-one is too time consuming for checking whole customer email databases. The best way to implement email verification is through batch processing or data integration.

Here's how both methods work.

Bulk email verification

Batch email verification is best if you manually manage and upload your lists to your email service

provider. As long as your lists are formatted as .csv, .txt, or Excel files, batch processing is a fast and simple bulk email verification method.

All you need to do is upload your email list to your email verification service, like Searchbug.

You'll typically receive your results in a matter of minutes. The results are delivered in a .csv file with the valid and safe emails from your list. That's it. All you have to do is plug those emails into your email software and send away.

Integrated email verification

Data integration is a more efficient and streamlined way to verify emails. However, it requires a tad bit of tech savvy to implement.

Data integration works by connecting your email handling system to your data reseller's system with an email verification API. The API integrates with a unique URL. So, you don't always need to know how to code. However, you do need to know where to add the URL and how to instruct your software to check the email addresses. So, it's often best to let your tech team handle the integration.

Usually, the API is integrated into your email collection form or your CRM system. That way, the emails are verified in real-time as people enter information in the email address form field. Or, emails get checked before your email system sends messages.

In either case, integrated email validation creates an automated, internal email checker. It's passive protection for your email databases.

What to do now

If you're not using email validation, you could potentially expose your customers to email attacks and risk your company's reputation. That's a hefty risk that we certainly don't recommend.

If you need to verify emails and protect yourself with dependable data, check out Searchbug's batch email verification or email verification API.

Searchbug.com