The importance of authenticating your email

Breadcrumb

Insight navigation

Nov 2023

The importance of authenticating your email

In early 2024, changes will be implemented that will impact email delivery if you do not have adequate email authentication in place.

Categories Technology Consulting

Nov 2023

-
-
-
-

Vincent Sharp

Lead Solutions Architect: Modern Workplace

Email

vincent.sharp@waterstons.com

Email has been around even longer than the internet, and is based on regular mail with the same inherent problems: by default, anyone with your address can send you a letter and say they are someone else.

Authenticating your outbound email is a way of demonstrating to recipients that your messages are sent from a valid source, and that they are not forged or spoofed by malicious actors. By authenticating your outbound email, you can:

- Improve the deliverability and reputation of your email, and reduce the chances of your emails being rejected or marked as spam by email providers

- Protect recipients from malicious messages pretending to use your domains, and protect your brand.

Why now?

Methods to authenticate your email have been around for many years, and while adoption has been increasing in response to , it is far from universal.

From February 2024, Google and Yahoo are introducingstricter requirements for email to be delivered to its accounts, including the need to have some form of email authentication in place.

Although this may result in some email delivery problems for organisationsthat haven’t kept up, this is a positive step to encouraging wider adoption of email authentication.

You are more likely to encounter email delivery problems if you:

- Have no email authentication setup
- Are a large organisation, or send a lot of messages
- Send bulk/high volume emails
- Make use of an on-premise message hygiene/email security solution, and do not have the correct records in place

How do I authenticate email?

There are different methods of authenticating your outbound email, the most common being SPF, DKIM, and DMARC. These methods use DNS records to verify that you are the legitimate sender of your email domain, and that your messages have not been tampered with in transit.

- SPF (Sender Policy Framework) lists the services that are allowed to send as your email domain
- DKIM (DomainKeys Identified Mail) – this method uses keys similar to a digital certificate (think HTTPS websites) to prove that a message hasn’t been modified in transit and is therefore legitimate. This requires configuration of your email system or message hygiene solution, and not all support this
- DMARC (Domain Message Authentication, Reporting & Conformance) – this mouthful builds on top of SPF & DKIM to further cement authentication, as well as provides feedback on the messages sent from your domain, and whether they align to your policies. This is particularly useful if you don’t know what services you have that use your email domain. A tool is generally required to present this information in an actionable way.
- ARC (Authenticated Receive Chain) – provides a ‘chain of custody’ for forwarded emails, retaining the authentication state of previous versions of the message.

Each method on its own is not foolproof, and the sophistication of malicious actors is ever-increasing in response to defences, but taken together they make it much more difficult for malicious actors to pretend to be you.

Be aware there is also a reliance on the receiving system to be properly configured; you can setup authentication perfectly, but if the receiving system doesn’t check or use this information properly then messages can be mistreated. This is most commonly down to misconfigured or lack of message hygiene policies.

How do I check if I’m covered?

One of the easiest ways to assess your email authentication and security is the National Cyber Security Centre’s‘check your email security’ tool.

This performs both email authentication checks for your outbound email, and privacy checks for your inbound mail.

What if I need help?

Some of the common things we can do to help include:

- Getting started with or remediating your email authentication
- Selecting or implementing a DMARC reporting tool
- Have too many services in your SPF record

If you’d like to speak to us about these or any element of email security, please get in touch at info@waterstons.com