

DMARC: Domain-based Message Authentication, Reporting & Conformance

What is DMARC?

DMARC, which stands for “Domain-based Message Authentication, Reporting & Conformance”, is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author (“From:”) domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.

DMARC is a way to make it easier for email senders and receivers to determine whether or not a given message is legitimately from the sender, and what to do if it isn't. This makes it easier to identify spam and phishing messages, and keep them out of peoples' inboxes.

DMARC is a standard that allows email senders and receivers to cooperate in sharing information about the email they send to each other. This information helps senders improve the mail authentication infrastructure so that all their mail can be authenticated. It also gives the legitimate owner of an Internet domain a way to request that illegitimate messages – spoofed spam, phishing – be put directly in the spam folder or rejected outright.

Why is DMARC important?

With the rise of the social internet and the ubiquity of e-commerce, spammers and phishers have a tremendous financial incentive to compromise user accounts, enabling theft of passwords, bank accounts, credit cards, and more. Email is easy to spoof and criminals have found spoofing to be a proven way to exploit user trust of well-known brands. Simply inserting the logo of a well known brand into an email gives it instant legitimacy with many users.

Users can't tell a real message from a fake one, and large mailbox providers have to make very difficult (and frequently incorrect) choices about which messages to deliver and which ones might harm users. Senders remain largely unaware of problems with their authentication practices because there's no scalable way for them to indicate they want feedback and where it should be sent. Those attempting new SPF and DKIM deployment proceed very slowly and cautiously because the lack of feedback also means they have no good way to monitor progress and debug problems.

DMARC addresses these issues, helping email senders and receivers work together to better secure emails, protecting users and brands from painfully costly abuse.

What type of illegitimate email does DMARC address?

DMARC is designed to protect against direct domain spoofing. When an email is sent by an unauthorized sender (whether it is sent by a malicious actor, or even an unauthorized or non-participating department of the company that owns/operates the domain), DMARC can be used to detect the unauthorized activity and (if so configured) request that those messages be blocked or discarded when they are received.

How does DMARC work, briefly, and in non-technical terms?

A DMARC policy allows a sender to indicate that their messages are protected by SPF and/or DKIM, and tells a receiver what to do if neither of those authentication methods passes – such as junk or reject the message. DMARC removes guesswork from the receiver's handling of these failed messages, limiting or eliminating the user's exposure to potentially fraudulent & harmful messages. DMARC also provides a way for the email receiver to report back to the sender about messages that pass and/or fail DMARC evaluation.

How does email forwarding affect DMARC?

If you are forwarding your A-State email (@astate.edu, @smail.astate.edu or @asusystem.edu) to another A-State email address, DMARC will not impact the deliverability of your email.

There are two ways that an email can be forwarded; one of them is manual, which has **no effect on email authentication** since the forwarded email is contained in a new email.

The second way, when the emails are **automatically forwarded** is when things become slightly complex and challenging. In our environment, automatically forwarded email to an external address will fail. This is due to the URL rewriting of links since we are changing the body of the email it will no longer pass DKIM causing DMARC to fail. The same is true if you are forwarding from an external address to an A-State email address.

The best way to ensure forwarded email is delivered, is to not use automatic forwarding and instead forward the message manually.

How are mailing lists impacted by DMARC?

Most modern implementations of mailing lists (Mailman, ListServ, etc.) provide support for DMARC. However, it may not be enabled by default. If you are a member of a mailing list and you have stopped receiving messages from the list, please contact the list admin and ask about making the list DMARC compliant.

I am no longer receiving email from a particular sender. What should I do?

Please contact the ITS Help Desk and submit a ticket. Include as much information about the sender as possible (email address, approximate date the email was sent, subject, etc.) so we can track the message in our system to see why it was not delivered.

ITS will provide you with details about why the message was not delivered.+

For further assistance, contact the ITS Help Desk at 870-972-3933 or stop by IT Support Services (itsupportservices@astate.edu). It is located on the bottom floor of the Dean B. Ellis Library, Room 149.

Revision #3

Created 2024-05-07 14:23:29 UTC by Joe Burleson

Updated 2025-07-03 15:24:32 UTC by Brandon Lyons