DMARC EMAIL CHANGES AT NSF

Frequently Asked Questions (FAQs) for the External Community

Overview

Domain-based Message Authentication, Reporting & Conformance (DMARC) is an email authentication and reporting protocol intended to improve email security by providing stronger controls to prevent the illegitimate use of organization emails. DMARC enables email providers to verify that email was sent from a trusted source rather than from bad actors such as spammers, hackers or phishers. Since DMARC is designed to increase email security, certain practices such as auto-forwarding or using services authorized to send messages on behalf of organizations can cause emails to fail DMARC protocol checks. Emails that fail the DMARC protocol checks may experience distribution issues including being marked as spam, quarantined, or even rejected by the receiving email system. The Department of Homeland Security's (DHS') Binding Operational Directive (BOD) 18-01 mandated all federal agencies implement DMARC.

What exactly is DMARC?

DMARC is a set of requirements issued by DHS to all federal agencies. It was required to be implemented by October 16, 2018. DMARC is comprised of protocols inserted into organization's IT systems to prohibit the illegitimate use of organization email. These protocols authenticate emails to ensure they are coming from a valid source. Certain email practices such as using services that are authorized to send messages on behalf of an organization (e.g., Constant Contact, GovDelivery, Amazon SES) or auto-forwarding emails to secondary (non-organization) email accounts can impact message delivery, since bad actors such as hackers may use similar practices.

Why is it important that I know about DMARC?

Since NSF's implementation of DMARC, the Foundation has observed that a few external organizations use email routing practices (such as auto-forwarding to personal accounts) that cause messages to be blocked from distribution because they are flagged as potentially fraudulent by the required DMARC protocols. This means that you may not be receiving important NSF communications. It is important for you to know that if your email is auto-forwarded to another account, such as a personal email account, you may not receive emails from NSF in that forwarded account.

How do I know if I am impacted by DMARC?

If you have been receiving NSF emails, nothing needs to be done.

If the email account at your organization or institution is configured to automatically forward emails to a third-party email service provider, such as Google or Yahoo, it is possible that NSF emails are not being delivered to your third-party email address. Please verify that you are receiving NSF emails in your primary organization/institution mailbox. Messages that are manually forwarded are not impacted.

If you have not received NSF sent emails, please contact your Sponsored Research Office (SRO) so they are aware others at your organization may be impacted. You might also contact the email administrator in your IT Department to tell them about your issue and ask them to confirm email configurations are compatible with DMARC.

Who can I contact at NSF if I have more questions?

Please contact NSF's IT Help Central at ITHelpCentral@nsf.gov. Agency staff have been receiving information about DMARC requirements and are being encouraged to report suspected DMARC-related email issues to NSF's IT Help Central Services for further analysis.

Published by Office of Information and Resource Management, April 2019