



Be better connected.

Configuring Email Security

MOREnet Staff

Marsha Goldberg (Help Desk) marsha@more.net

Jodi Gilpin (CORE) jodi@more.net

Dana Hunt (Network Consulting) dhunt@more.net

David Kessler (Network Consulting) kesslerd@more.net





OBJECTIVES

- Understanding email security
- DKIM, SPF, DMARC
- Configuring email settings
- Troubleshooting
- Discussion

HOSTED EMAIL

Most popular hosted email:

- Google
- Microsoft 365

DNS Hosting Providers:

- MOREnet
- GoDaddy
- Network Solutions

Examples of 3rd party services that send email:

- Infinite Campus or any other SIS program
- Mailgun
- School Messenger
- Zoho

Why does email need secure configurations?

- Primary communication method for personal, financial, business use
- Provides an additional layer of security
- Prevent spam, phishing, spoofing
- Required by cyber risk insurance companies
- Required by vendors (financial, etc.)

Google & Yahoo new email requirements

- In 2024 you may see an uptick in email that are not reaching your inboxes, the reason could be because of the new requirements that Google and Yahoo have implemented. Reference [article](#)
 - Understand what domains you use for email sending today (and whether they're already authenticated)
 - Authenticate your mail with custom DKIM
 - Authenticate your mail with custom SPF
 - Set up DMARC
 - Register your domain for [Google Postmaster Tools](#) and keep your spam complaint rates under 0.3%



SPF, DKIM, DMARC ROLES & SETUP

SPF

Sender Policy Framework - Validates that the sending server is authorized to send emails on behalf of the domain.

How it works:

- Recipient email server receives email
- Server checks return path of the email
- Server retrieves SPF record from sending server and performs SPF check
- Server performs cross check of approved IP addresses and the return path. If matches, email is accepted-If not, email sent back to original server.

SPF Weakness

Validation is not based on the 'from' address or domain. If 'from' address is fake, it is possible to pass authentication. Use of DMARC addresses this flaw.

- Example SPF record:
- `v=spf1 ip4:192.168.1.1 include:_spf.example.com ~all`
 - `v=spf1`: Indicates the version of SPF being used.
 - `ip4:192.168.1.1`: Authorizes the specified IPv4 address to send emails for your domain.
 - `include:_spf.example.com`: Includes additional SPF records from the specified domain.
 - `~all`: Suggests a soft fail if the email comes from a server not listed in the SPF record.

Check Validation of SPF record

- <https://dmarcian.com/spf-survey/>

SPF Reminders

- Once you build your SPF record it needs to be published to DNS to take effect
 - The third party (often MOREnet in Missouri) who manages your DNS
 - Publish yourself if you manage your own
- Remember to Update SPF Record as Needed:
 - Regularly review and update the SPF record if there are changes to your email infrastructure.
- If you include names (as opposed to only IP addresses/netblocks) you can have no more than 10 lookups in your SPF record. Use an SPF record analyzer to check.
- Check out the [SPF record syntax website](#) for more details

DKIM

DomainKeys Identified Mail

Enables domain owners to automatically 'sign' emails from their domain. Uses cryptography to mathematically verify that the email came from the domain.

DKIM Setup

- Generate DKIM key pair.
- Configure email server to sign outgoing emails.
 - If using Google Workspace here is an [article](#) to help turn this on for your domain
- Add DKIM DNS record:
 - Selector._domainkey.example.com. TXT "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSib3DQEBAQUAA4GNADCBiQ..."
- Contact service providers that send email on your behalf (SIS, School Messenger, HVAC, etc)
- Add the DKIM record to DNS.
- **Tips:**
 - Rotate keys periodically.
 - Ensure proper key management.

DMARC

Domain-based Message Authentication Reporting and Conformance

Tells a receiving email server what to do given the results after checking SPF and DKIM. Depending on the setting, the email server can reject, quarantine or deliver emails.

Builds on SPF and DKIM, both of which should be in place first

DMARC DNS TXT Record Format

- Name of text record: `_dmarc.your_domain.org`
- Sample value: `"v=DMARC1; p=none; sp=quarantine; pct=100; rua=mailto:dmarc_reports@domain.org"`
 - `v=DMARC1`; DMARC version. Always DMARC1
 - `p=(policy)`; Requested action for messages from domain.org that fail DMARC check. Servers have discretion on exactly how to handle them.
 - `none`; Send a report. Take no further action.
 - `quarantine`; The receiving server may send the message to spam, hold it, or further process it in some way
 - `reject`; Reject the message outright
 - `sp=(policy)`; Requested action for subdomains of domain.org
 - `pct=(number)`; Percentage of messages to be affected by the policy. Allows for gradual testing. If omitted default is 100.
 - `rua=(mailto:address)`; Address to send aggregate reports. Recommend to use a special account for this purpose.

DMARC Policy Record Examples

- Report only - Does not affect mail flow
 - "v=DMARC1;p=none; rua=mailto:dmarc_reports@domain.org"
- Moderately aggressive - Quarantine all failing messages from the domain, reject those from subdomains
 - "v=DMARC1;p=quarantine; sp=reject; rua=mailto:dmarc_reports@domain.org"
- Aggressive - Reject all failing messages
 - "v=DMARC1;p=reject; rua=mailto:dmarc_reports@domain.org"

SPF, DKIM & DMARC records are stored in the Domain Name System (DNS)

Checking up

There are several ways to check if the authentication methods have passed.

- Header
- MXToolbox
- Dmarcian

```
arc=pass (i=1 spf=pass  
spfdomain=example.com dkim=pass  
dkdomain=example.com dmarc=pass  
fromdomain=example.com) ;
```




Setting up DMARC, DKIM and SPF

- Identify who hosts your DNS records and email
- What systems send email on your behalf (Student Information System, Parent Portal, Text Caster, Internal Server with Mail Relay)
- Find form or instructions for submitting changes to Records
- Submit your request
- You should receive acknowledgment about your request
- Your changes will propagate to the world (give it time)
- Verify changes and test email
- Monitor and review email sent from DMARC entry

Identify your DNS host

```
Command Prompt
Microsoft Windows [Version 10.0.22631.2861]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kesslerd>nslookup
Default Server: UnKnown
Address: 2001:4888:3c:ff00:325:d::

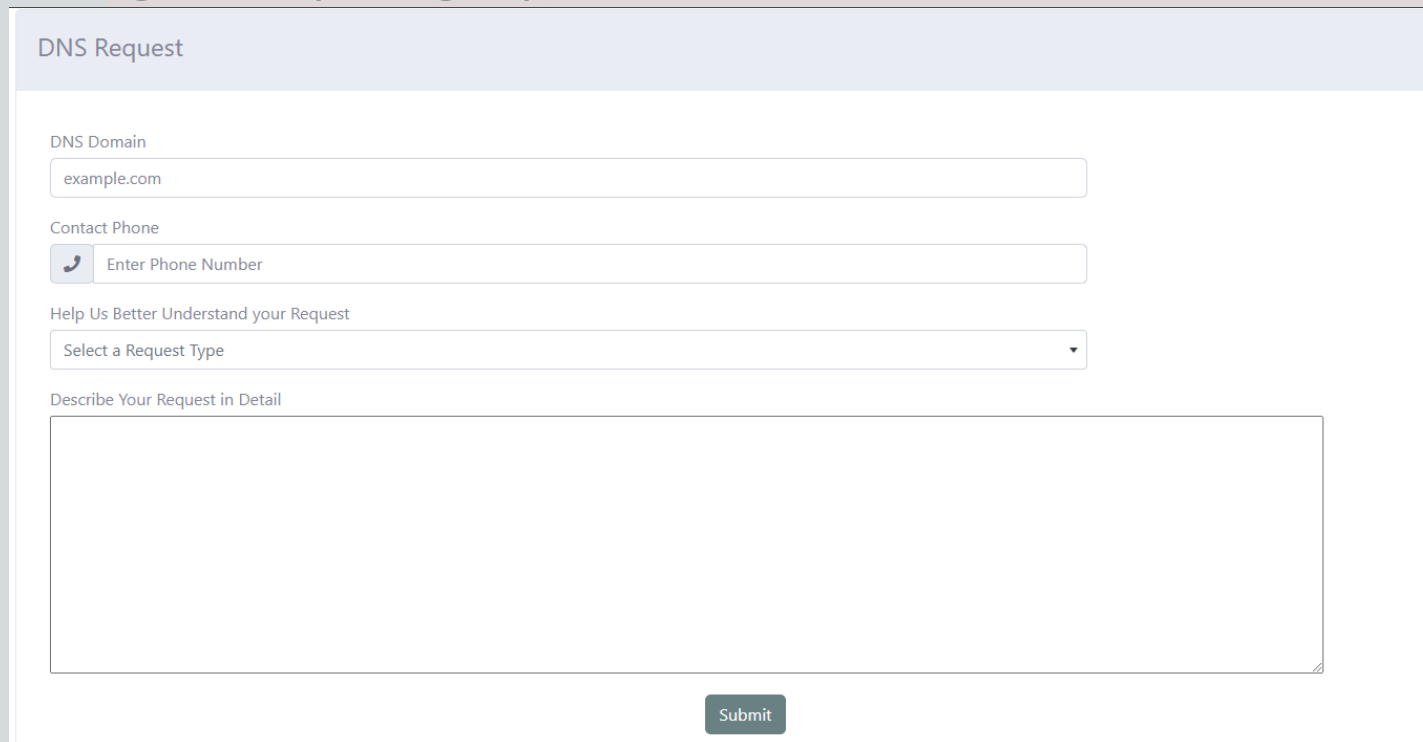
> set type=ns
> cpsk12.org
Server: UnKnown
Address: 2001:4888:3c:ff00:325:d::

Non-authoritative answer:
cpsk12.org nameserver = ns62.domaincontrol.com
cpsk12.org nameserver = ns61.domaincontrol.com
> exit

C:\Users\kesslerd>
```

Example DNS change form

- Log into your MyMOREnet and click on DNS, then click DNS Request, see screenshot below
- Or email register@more.net or help@more.net (copy and paste info please don't just send a screen shot as the records could get very lengthy)



DNS Request

DNS Domain

Contact Phone

Help Us Better Understand your Request

Describe Your Request in Detail



TROUBLESHOOTING



DISCUSSION

MOREnet 
Be better connected.

