THE NATIONAL CYBERSECURITY SOCIETY

DMARC

Did you know?

√ Email filters are not foolproof

√ Email spoofing can damage your company's reputation

√ Hackers can gain access and send nefarious emails using your email account

√ Junk folders don't capture all your spam

√ 70% of cyber incidents involve phishing or scamming a victim

DMARC is a Domain-based Message Authentication, Reporting and Conformance. The process is built on Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) standards to authenticate email senders by adding linkage to the sender field of the email, which enables the destination email systems to trust email delivered from the sender's domain. The objective of DMARC is to prevent fraudulent activity and detect email spoofing sent from the domains under the organization's control.

FACT 1: RISK OF NOT USING DMARC

1. It is difficult to determine and separate a legitimate message from a fraudulent one. Email filters are not foolproof. This means that harmful email may be delivered to the user's inbox instead of sending it to junk or spam folder.
2. Emails that look legitimate increase the likelihood that a spammer and/or phisher can steal your passwords and personal information such as bank accounts, credit cards etc.
3. Email spoofing can damage the company's reputation and exploit the consumer's trust.

FACT 2: HOW DOES DMARC WORK

1. Authentication of email messages received is checked to ensure it is a legitimate message.
2. Generating a summary by Domain Name server of all messages received (patterns of email traffic)
3. Informing the legitimate domain name owners of the attempted misuse of their domain to send spoofing/phishing emails.

FACT 3: HOW TO IMPLEMENT DMARC

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

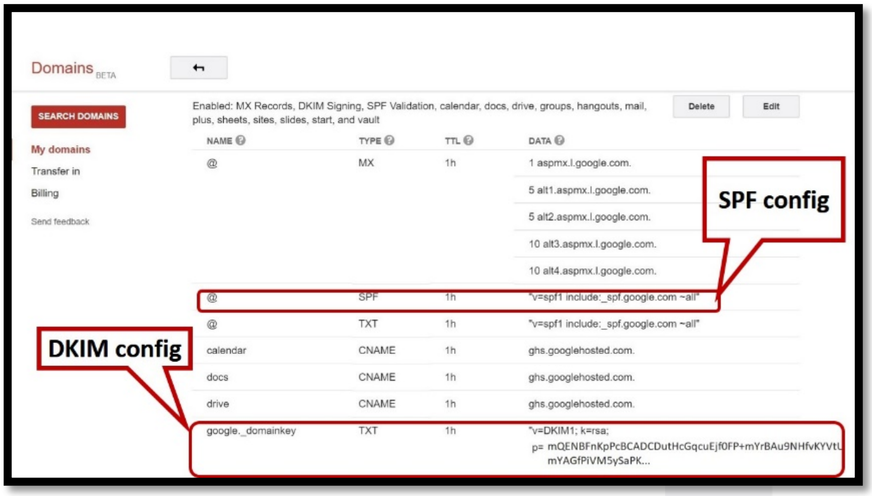
JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

DMARC continued…

1. Configure SPF and DKIM for the DNS (domain name server) for the registrar for your particular domain.

   An example using Google Domains listed below. However, the configuration for other domain registrars such as Bluehost or GoDaddy will be similar.

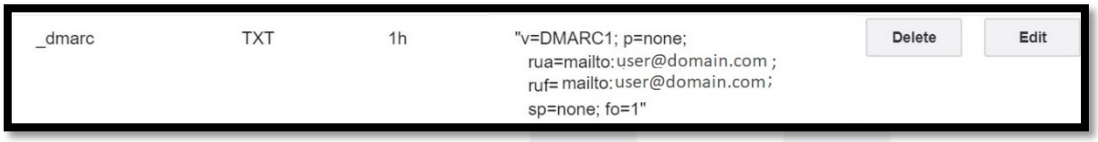


Enabled: MX Records, DKIM Signing, SPF Validation, calendar, docs, drive, groups, hangouts, mail, plus, sheets, sites, slides, start, and vault

NAME	TYPE	TTL	DATA
@	MX	1h	1 aspmx.l.google.com. 5 alt1.aspmx.l.google.com. 5 alt2.aspmx.l.google.com. 10 alt3.aspmx.l.google.com. 10 alt4.aspmx.l.google.com.
@	SPF	1h	"v=spf1 include:_spf.google.com ~all"
@	TXT	1h	"v=spf1 include:_spf.google.com ~all"
calendar	CNAME	1h	ghs.googlehosted.com.
docs	CNAME	1h	ghs.googlehosted.com.
drive	CNAME	1h	ghs.googlehosted.com.

google._domainkey	TXT	1h	"v=DKIM1; k=rsa;
			p= mQENBFnKpPcBCADCDutHcGqcuEjf0FP+mYrBAu9NHfvKYVtU
			mYAGfPiVM5ySaPK...

2. Set up a DMARC Record for each DNS
   - Configure and verify identifier alignment/domain alignment (https://dmarc.org/2016/03/best-practices-for-email-senders/)
   - Can be added as a "TXT"resource record in Google Domains (see image below)
   - Specify an email address to receive reports aggregated by domain ("rua" in the example below) and forensic/individual reports ("ruf" in the example below.



_dmarc	TXT	1h	"v=DMARC1; p=none;
			rua=mailto:user@domain.com ;
			ruf= mailto:user@domain.com;
			sp=none; fo=1"

   - Be sure to use one (or two for the two different levels of reports) email addresses that will be monitored for threats regularly

FACT 4: WHO CAN USE DMARC?

Anyone - DMARC specification doesn't require licensing and is free to everyone to implement it.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

DMARC continued...

ADDITIONAL RESOURCES:

- DMARC Guidelines and Tips
  - https://dmarc.org/2016/03/best-practices-for-email-senders
  - https://en.wikipedia.org/wiki/DMARC
  - https://otalliance.org/resources/ota-spf-dmarc-resources-tools
- DMARC Deployment Tools
  - https://dmarc.org/resources/deployment-tools/
- DMARC Setup Guide
  - https://dmarc.globalcyberalliance.org/
- NIST (National Institute of Standards and Technology) Guidelines
  - https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1945.pdf
- United States Computer Emergency Readiness Team (US-CERT)
  - https://www.us-cert.gov/ncas/bulletins.xml

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.