ARE EMAILS TO YOUR MEMBERS SAFE?

A STARTING GUIDE TO IMPLEMENTING DMARC

TOM HAFEMANN
CTO – WCCU
TSHAFEMANN@WCCU.COOP

CORY JAEGER
DIRECTOR OF IT – WCCU
CAJAEGER@WCCU.COOP

WHY IS THIS HAPPENING?

- “Email is involved in more than 90% of all network attacks and without DMARC, it can be hard to tell if an email is real or fake. DMARC allows domain owners to protect their domain(s) from unauthorized use by fighting phishing, spoofing, CEO fraud, and Business Email Compromise”
- NCUA, in PCI DSS 4.0, Requires Anti-Phishing protection and specifically calls out **SPF**, **DKIM** and **DMARC -** https://dmarcian.com/pci-requires-dmarc/
- The standards of DMARC, DKIM, and SPF, all work together to help insure that nobody can send email using your domain name without your explicit permission.
- Without a DMARC reject policy, anyone can send emails **using your domain name**.
- Spoofed sender = return address spoof

WHAT'S HAPPENING?

- DMARC means Domain-based Message Authentication, Reporting, and Conformance
  - First published in 2012
- DKIM means DomainKeys Identified Mail
- SPF means Sender Policy Framework

SPF AND DKIM – PERQUISITES FOR DMARC

- DKIM (DomainKeys Identified Mail) is a protocol that allows an organization to take responsibility for transmitting a message by signing it in a way that mailbox providers can verify. DKIM record verification is made possible through cryptographic authentication.

- An SPF record identifies the mail servers and IPs that are allowed to send email on behalf of your domain. Receiving servers check your SPF record to verify that incoming messages that appear to be from your organization are sent from servers allowed by you. Domains can have one SPF record*. SPF records can only cause no more than 10 DNS lookups***

  Verify DNS lookup limits with a tool like https://DMARCian.com/SPF-survey/ or https://mxtoolbox.com/SPF.aspx

WHO SHOULD BE DOING THIS?

- Every Credit Union!
- Every domain owner need to configure their SPF, DKIM, and DMARC records properly themselves — both in order to prevent spam from their domain, and to make sure that legitimate emails from their domain are not marked as spam.
- More Specifically, any Credit Union that has 3rd parties send out email on your domain
- Even more specifically, any Credit Union that has any third party that sends out emails concerning debit and credit cards. Like PSCU, Shazam, FIS, Fiserv, etc
- Google and Yahoo implemented DMARC, DKIM, SPF alignment restrictions in February 2024
- There is a very high likelihood that you will be spoofed and it will cost the credit union significant money, along with significant reputation hit.

WHEN DOES THIS NEED TO BE ACCOMPLISHED?

- According to the NCUA, PCI DSS 4.0, which includes DMARC alignment, will take effect by March 31st 2025
- If you don't accomplish this, not only will you be out of compliance, but you increasingly run a significant risk of email attacks and spoofing.
- There are major scheduling backlogs with some 3rd party providers that may cause significant delays in implementation. – DON’T WAIT TO START

WHERE IS THIS DONE?

- This is all done in DNS and the mail servers that send email for your domain.
- You must work with your 3rd and 4th party vendors

OTHER THOUGHTS?

- If you have ever thought of changing your domain name, this would be the time to do it!

PCI DSS DOESN'T APPLY TO US – WHY DO DMARC?

- Protect your members
  - Emails from your domain(s) really are from you
- Protect your CU
  - **Reputational Risk**
    If your members receive a fraudulent email from fraud@YourCUDomain.org, warning them of a possible fraudulent charge, will they click a link to find out more?

    Will you be on the hook for their financial losses even though you never sent that email?

    Will they accept your explanation of why "it isn't our fault"? (Remember Home Depot and Target breaches?)
- Ask LA Federal CU:
  https://www.agari.com/resources/case-studies/los-angeles-based-large-credit-union

DMARC DNS RECORDS

DMARC uses a DNS TXT record named _dmarc on your domain or sub-domain

- _dmarc.yourcu.org
  Ex: v=DMARC1; p=none; rua=mailto:dmarc-reporting@yourcu.org;

- _dmarc.statements.yourcu.org
  Ex: v=DMARC1; p=reject; rua=mailto:dmarc-reporting@yourcu.org;

DMARC POLICIES

- Three Policies are Available:
  - p=none – Deliver normally
  - p=quarantine – Varies by email host (May go to spam folder, be moved to admin quarantine, be flagged as suspicious, or may even be delivered normally.)
  - p=reject – Do not deliver the email at all

DMARC AGGREGATION REPORT

The rua= tag lets you request reports about DMARC success/failure

- It specifies the email address reports are sent to
- Applies to all three policy types
- Tip: Don't send them to yourself. Use a DMARC aggregation service.
  - Getting useful information from reports is difficult
  - Aggregation services can provide summaries over time and allow you to dig into detail

DMARC FORENSICS REPORT

The ruf= tag lets you request detailed forensics reports

- Tip: Don’t bother
- Could expose sensitive information
- Virtually no email hosts send forensics reports
  - I’ve received six in the past five years

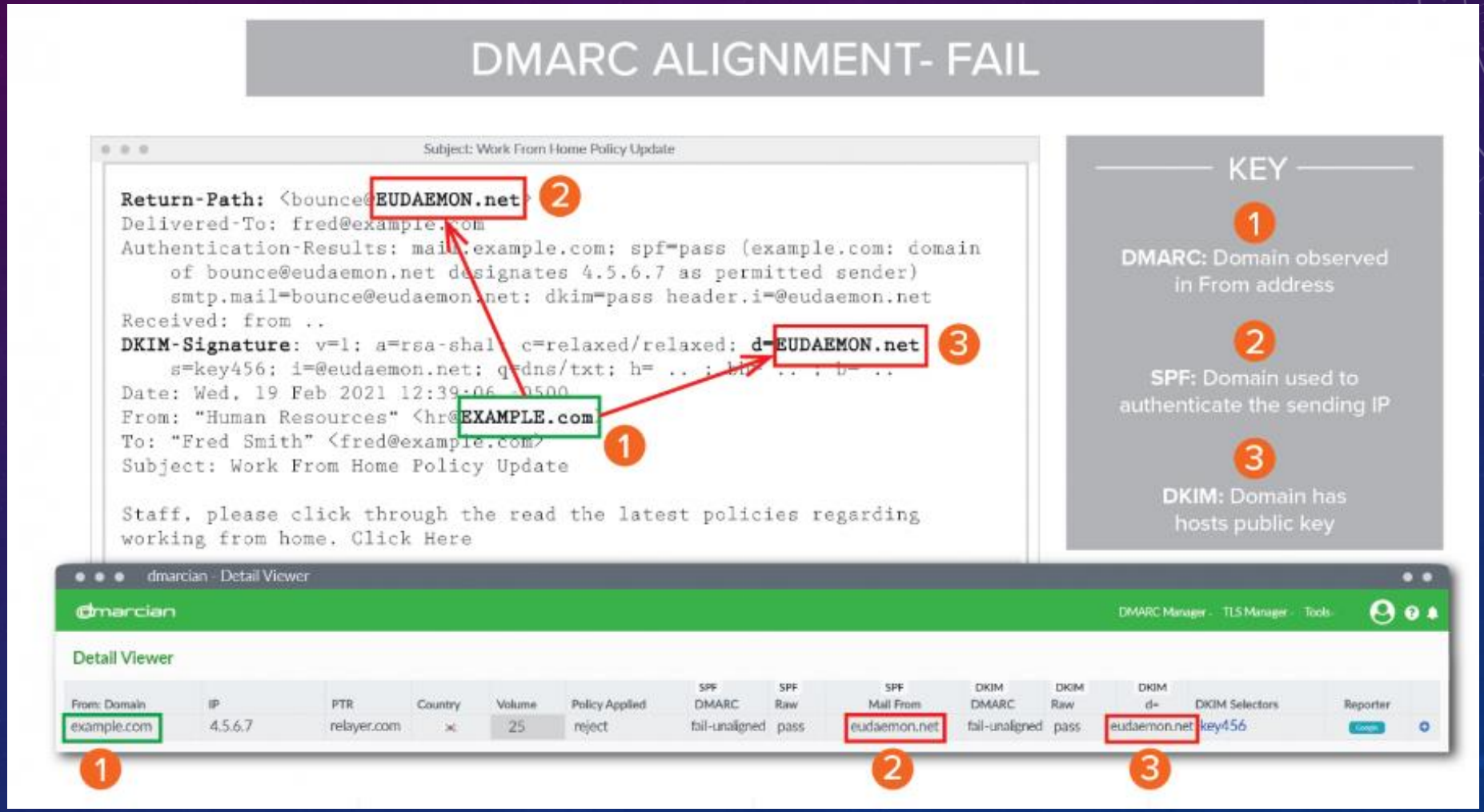
HOW DOES IT WORK

The RECEIVING mail server:

- Checks for DMARC record in DNS
- It checks for SPF record and validates sending IP
- It looks up DKIM key (if present) and verifies digital signature
- It checks for DMARC email header alignment (more on this soon)
- If everything checks out, email is delivered
- IF DMARC fails, the server refers to the policy
- IF DMARC includes a reporting email address, XML reports are sent (eventually)

DMARC IN PRACTICE

DMARC ALIGNMENT (THE HARD PART)



Source: https://dmarcian.com/alignment/

CHALLENGES – 3RD PARTY SUPPORT

- THIS WILL LIKELY COST TIME AND MONEY!
  Many vendors are not doing this for free (even though they should be).
- Some vendors understand and support DMARC better than others.
- Best practice is to delegate a sub-domain to each vendor or type of email. Ex:
  - @statements.yourcu.org – Member statement email vendor
  - @offers.yourcu.org – Member marketing/informational bulk email vendor
  - Each sub-domain can have its own SPF and DMARC record

IMPLEMENTING DMARC “SAFELY”

- Create an account with a DMARC aggregator
  - Include the rua= tag that your aggregator assigns in all your DMARC records
- Start with a p=none policy on your top-level domain
- Assign a sub-domain to each of your 3rd parties who send email on your behalf
  - Set a p=none policy on the sub domain
  - Verify that emails are passing DMARC checks
  - Set a p=quarantine policy for a short time
  - Set a p=reject policy
- After all of your emails are passing DMARC checks, move to “quarantine” then “reject” (You may have to take some risks!)

SPF (-ALL VS ~ALL VS +ALL)

-ALL – FAIL (Hard Fail)

- Tells mail server that there are NO other SPF-authorized senders

~ALL – SOFT FAIL

- Tells mail servers, that there MAY BE other senders, but mark the email
- A crutch to avoid accidentally blocking legitimate email
- DMARC will treat it the same as FAIL when validating SPF!

+ALL – PASS

- DON’T DO THIS – Allows ALL email servers to send on your behalf.

DMARC AGGREGATOR RESOURCES

Most of these have free trials or offer free (but limited) services.

Reviews: https://postmarkapp.com/blog/best-dmarc-tools

- DMARCIAN - https://DMARCian.com/
- DMARC Analyzer - https://DMARCanalyzer.com/
- DMARCLY - https://www.dmarcly.com
- Valimail for MS365 - https://www.microsoft.com/en-us/security/blog/2019/06/03/secure-cloud-free-DMARC-monitoring-office-365/ (https://tinyurl.com/56bw4ckb)
- PowerDMARC - https://powerdmarc.com/
- EasyDMARC - https://easydmarc.com/

OTHER RESOURCES

- DMARCIAN Email Tools - https://dmarcian.com/domain-checker/
- MX Toolbox - https://mxtoolbox.com/dmarc.aspx
- DMARC generator - https://mxtoolbox.com/DMARCRecordGenerator.aspx
  - SPF generator - https://mxtoolbox.com/SPFRecordGenerator.aspx
- DMARC compliant mailers – https://dmarc.io/sources/
- CUSO Magazine – Technologies Your CU Should be Implementing
  - https://cusomag.com/2023/08/21/email-security-technologies-your-credit-union-should-be-implementing/
- Check/Enable DKIM for MS365 – https://security.microsoft.com/authentication?viewid=DKIM
- PCI DSS 4.0 - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf and https://dmarcian.com/pci-requires-dmarc/
- What is BIMI - https://postmarkapp.com/blog/what-the-heck-is-bimi

MORE RESOURCES

- MAILHARDENER.COM
  - SPF/DKIM/DMARC Guide and info - https://www.mailhardener.com/kb/email-hardening-guide
  - Free Tools - https://www.mailhardener.com/tools/
  - Other Services (free for personal use) - https://www.mailhardener.com/
- RFCs
  - DMARC RFC: https://www.rfc-editor.org/rfc/pdfrfc/rfc7489.txt.pdf
  - DKIM RFC: https://www.rfc-editor.org/rfc/pdfrfc/rfc5672.txt.pdf
  - SPF RFC: https://www.rfc-editor.org/rfc/pdfrfc/rfc7208.txt.pdf

- Learn more at https://www.dmarc-academy.com/

- This presentation: https://dmarc.wccu.coop/ppt/