GLOBAL CYBER ALLIANCE

DEFEND & DELIVER

DMARC

Email authentication for better email security

ONLY ONLINE BOOTCAMP

Shehzad Mirza

Director of Operations

smirza@globalcyberalliance.org

gca-dmarc@globalcyberalliance.org

Bootcamp Plan and Upcoming Webinars

Bootcamp Overview

Must attend live sessions for certificate (1 per week)

- **Week One: Getting Started**
  - **May 5th:** Webinar - BEC and DMARC in a Nutshell

- **Weeks Two and Three: Time to Implement!!**
  - **May 12:** What are SPF and DKIM?
  - DMARC in Detail and Online Technical Demos (**only need to attend one of the three**).
    - **Tuesday, May 18th** - demo of Window DNS
    - **Wednesday, May 19th** - demo Linux DNS
    - **Thursday, May 20th** - demo of Cloud DNS

- **Week Four: Ongoing Management**
  - **May 26th:** DMARC Reporting & Analysis: What Happens Next

- **Week Five: Wrap-up Session**
  - **June 2nd:** Bootcamp Review and Additional Protocols

Phishing

GLOBAL CYBER ALLIANCE

Phishing

PHISHING

- Could lead to
  - Ransomware or other malware
  - Fraud (false wire transfer requests)
  - Theft of PII
- Why is it successful?
  - Difficulty in determining if message came from legitimate source
  - From\Sender address is spoofed

Business Email Compromise (BEC) in $$$

City - $1.04 million
City - $1.73 million
City - $800K
Religious Institution - $1.75 million

(source: bleepingcomputer.com)

FBI 2020 Internet Crime Report

GLOBAL CYBER ALLIANCE

Crime Type	Loss
BEC/EAC	$1,866,642,107
Confidence Fraud/Romance	$600,249,821
Investment	$336,469,000
Non-Payment/Non-Delivery	$265,011,249
Identity Theft	$219,484,699
Spoofing	$216,513,728
Real Estate/Rental	$213,196,082
Personal Data Breach	$194,473,055
Tech Support	$146,477,709
Credit Card Fraud	$129,820,792
Corporate Data Breach	$128,916,648
Government Impersonation	$109,938,030
Other	$101,523,082
Advanced Fee	$83,215,405
Extortion	$70,935,939
Employment	$62,314,015
Lottery/Sweepstakes/Inheritance	$61,111,319
Phishing/Vishing/Smishing/Pharming	$54,241,075

Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	241,342
Non-Payment/Non-Delivery	108,869
Extortion	76,741
Personal Data Breach	45,330
Identity Theft	43,330
Spoofing	28,218
Misrepresentation	24,276
Confidence Fraud/Romance	23,751
Harassment/Threats of Violence	20,604
BEC/EAC	19,369
Credit Card Fraud	17,614
Employment	16,879
Tech Support	15,421
Real Estate/Rental	13,638
Advanced Fee	13,020
Government Impersonation	12,827
Overpayment	10,988

Agari Cyber Intelligence Division (ACID) – Threat Intel Brief: The Geography of BEC

Global locations of BEC threat actors.

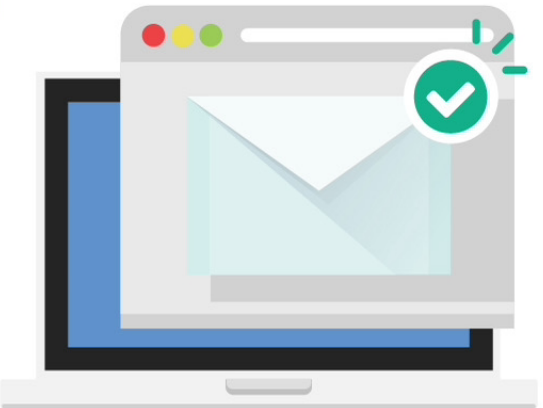
https://agari.com/insights/whitepapers/threat-intelligence-brief-geography-bec/

Types of Spoofing

- Display Name Spoofing - *“**Company** <person@yahoo.com>”*
- Lookalike Domain Spoofing - *“Company <person@c**0rn**pany.com>”*
- Domain Spoofing - *“Company <person**@company.com**>”*

SOLUTION:

DMARC



A PROVEN WAY TO MITIGATE RISK

Domain-based Message Authentication, Reporting and Conformance (DMARC)
It's like an identity check for your organization's domain name.

What is DMARC?

A DMARC policy allows a sender to indicate that their messages are protected, and tells a receiver what to do if one of the authentication methods passes or fails – such as send the message or junk/reject the message.

DMARC prevents spammers or phishers from using valid organization names for email fraud

DMARC increases customer **confidence and trust**

It protects the integrity of **your brand**

Additional Benefits of DMARC

- Inbox Protection on the Consumer side:
  - **DMARC Verification, not policy**
  - 80 percent of the current total number of worldwide email accounts (source: Valimail).
- Deliverability
- Visibility: Provides insight into attempts to spam, phish, or even spear-phish using your organization's brand/name

Two Parts to DMARC

- DMARC Policy
  - sending organization
  - use existing DNS infrastructure
- DMARC Verification
  - receiving organization
  - enable on email security system
  - checks all incoming messages for DMARC policy


DMARC
Myth
ONE
“
It’s used on email domain only
ANY domain can be impersonated and used in phishing attacks, so we need to do more than just securing only the domains used to send mail. Every domain owned by your organization should be secured with its own DMARC policy.
#GOTheDMARCWay

Authentication

DMARC implementation requires Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) in order to work

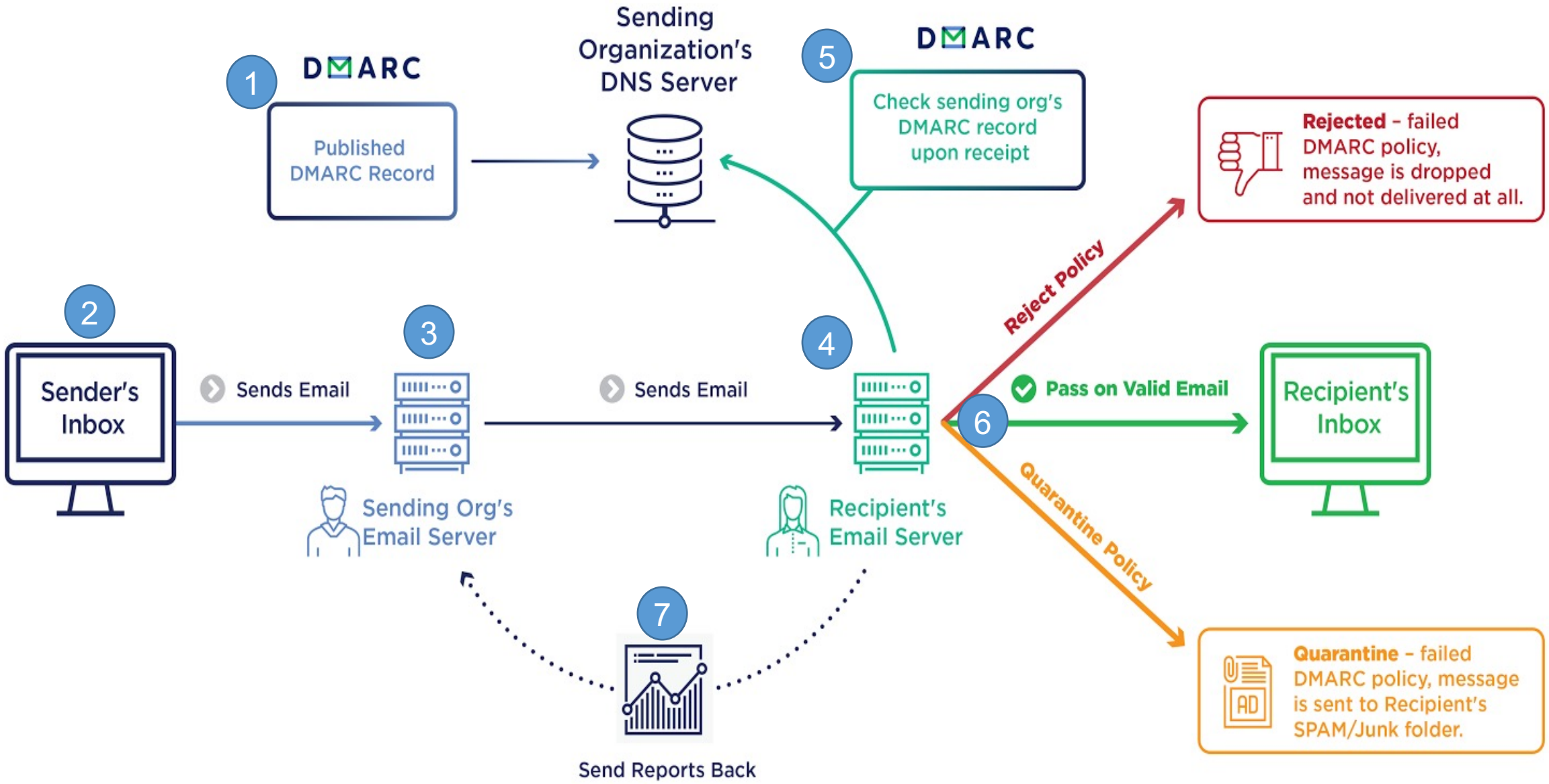
- SPF is used to define which mail servers are authorized to send mail
- DKIM is used to add a digital signature for an additional layer to authenticate the sender

DMARC Policy

What happens to the messages?

- Depends on the policy setting:
  - **None** - reports possible suspicious mail messages, but all mail is sent to inbox
  - **Quarantine** - fail SPF/DKIM and alignment, message is sent to spam/junk folder
  - **Reject** - fail SPF/DKIM and alignment, message is dropped and not delivered at all
- Best practice is to start at ‘None’ and gradually move to ‘Reject’

Overview


1
DMARC
Published DMARC Record
Sending Organization's DNS Server
5
DMARC
Check sending org's DMARC record upon receipt
Rejected – failed DMARC policy, message is dropped and not delivered at all.
2
Sender's Inbox
Sends Email
3
Sending Org's Email Server
Sends Email
4
Recipient's Email Server
Reject Policy
Pass on Valid Email
6
Recipient's Inbox
Quarantine Policy
Quarantine – failed DMARC policy, message is sent to Recipient's SPAM/Junk folder.
7
Send Reports Back

DMARC DNS TXT Record

- Basic:

  Host: _dmarc. <domainname>

  Value: v=DMARC1; p=none; rua=mailto:*<email address>*; ruf=mailto:*<email address>;*

- Complex:

  Host: _dmarc. <domainname>

  Value: v=DMARC1; p=none; rua=mailto:*<email address>*; ruf=mailto:*<email address>*; fo=1; adkim=r; aspf=r; pct=100; rf=afrf; ri=86400; sp=reject;

DMARC Reports

- DMARC generates two types of reports:
  - Aggregate
  - Forensic (or Failure)
- Reports will provide insight as to which messages were marked as suspicious
- Allows for IT staff to correct any issues with valid messages being dropped by the policy

Sample Aggregate Report

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
 <report_metadata>
  <org_name>google.com</org_name>
  <email>noreply-dmarc-support@google.com</email>
  <extra_contact_info>https://support.google.com/a/answer/2466580</extra_contact_info>
  <report_id>6156901232184779430</report_id>
  <date_range>
   <begin>1466121600</begin>
   <end>1466207999</
  </date_range>
 </report_meta
 <policy_publi
  <domain>gl                    omain>
  <adkim>r</a
  <aspf>r</aspf>
  <p>quarantine</
  <sp>quarantine</s
  <pct>100</pct>
 </policy_published>
 <record>
  <row>
   <source_ip>2607:f8b0:400
   <count>2</count>
   <policy_evaluated>
    <disposition>none<
    <dkim>pass</dki
    <spf>pass</spf
   </policy_evalua
  </row>
  <identifiers>
   <header_f                .org</hea
  </identifiers>
  <auth_results>
   <dkim>
    <domain>globalcyber      nce.org</domain>
    <result>pass</result>
   </dkim>
   <spf>
    <domain>globalcyberalliance.org</domain>
    <result>pass</result>
   </spf>
  </auth_results>
 </record>
```

Sample Forensic/Failure Report

```
Feedback-Type: auth-failure
User-Agent: szn-mime/2.0.41
Version: 1
Original-Rcpt-To: xxxx@seznam.cz
Source-Ip: 198.2.183.22
Authentication-Results: email.seznam.cz 1;
        spf_align=fail;
        dkim_align=fail
Delivery-Result: delivered\r\n\r\nReceived: from mail22.suw13.rsgsv.net (mail22.suw13.rsgsv.net [198.2.183.22
        by email-smtpd9.ng.seznam.cz (Seznam SMTPD 1.3.106) with ESMTP;
        Fri, 12 Jul 2019 10:01:20 +0200 (CEST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=fbl.mcsv.net; s=k1;
        t=1562918478; bh=z+cM1nqHlHrjpgwrd2iSbq3xmFeT/VO5Zoa5XOw5TY8=;
        h=Subject:From:Reply-To:To:Date:Message-ID:Feedback-ID:List-ID:
         List-Unsubscribe:Content-Type:MIME-Version;
        b=QhxQk+uH4sVDFSYWdTJrdFzJc3wTQ9TBBlq2FDnri+hfqMAMHaAfGVHytqUcnWL3x
         H6X0zZZkwp6KJc2vsm/cH1Xls10xaPWHG3ioK0aM5kv7BJfBX2PRAfzPR4eaBvakZi
         o2acfXIPaCZ+GeBNxaz5JKDTuteM/xavDjcbObXs=
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=mailchimpapp.net;
        s=k1; t=1562918478; i=rortega=3D3Dasmusa.org@mailchimpapp.net;
        bh=z+cM1nqHlHrjpgwrd2iSbq3xmFeT/VO5Zoa5XOw5TY8=;
        h=Subject:From:Reply-To:To:Date:Message-ID:List-ID:List-Unsubscribe:
         Content-Type:MIME-Version;
        b=iJriMQtloII7ciJrNISIOixgf2oWoCfaq/xO2XnLq9OzxEAXR8U0bgWa0lJU8wq3+
         0OlgUsrU/Vd43B+umAAnKaRLoT3JjoExWh5B84cGnr+9MkcJWf+RB4QilG8GWtEgVl
         O4W1o6pcuVupqSqOiCnrcuVI2L9hEwlXfnIqSMMQ=
Received: from localhost (localhost [127.0.0.1])
        by mail22.suw13.rsgsv.net (Mailchimp) with ESMTP id 45lQNZ5cXVzt6G
        for <xxxx@seznam.cz>; Fri, 12 Jul 2019 08:01:18 +0000 (GMT)
x-mcpf-jobid: mc.us7_22465175.1121249.5d283e46c424e.full_000002
Subject: =?utf-8?Q?New=20from=20microTalk=20for=2007=2F11=2F2019?=
From: =?utf-8?Q?American=20Society=20for=20Microbiology?= <rortega@asmusa.org>
Reply-To: =?utf-8?Q?American=20Society=20for=20Microbiology?= <rortega@asmusa.org>
To: <xxxx@seznam.cz>
Date: Fri, 12 Jul 2019 08:01:17 +0000
Message-ID: <1772a0600a0b532d47343e0f9.0636065ea3.20190712080112.ac71646aa0.3ffee3b2@mail22.suw13.rsgsv.net>
X-Mailer: MailChimp Mailer - **CIDac71646aa00636065ea3**
X-Campaign: mailchimp1772a0600a0b532d47343e0f9.ac71646aa0
X-campaignid: mailchimp1772a0600a0b532d47343e0f9.ac71646aa0
```

Concerns with Implementation

GLOBAL CYBER ALLIANCE

DMARC Myth TWO

It's a Silver Bullet

DMARC is not the cure for every cyber risk. It protects only one type of spoofing and should never be used alone. You need a layered defense with securing email, and DMARC is an important layer. I
DANE

DMARC Myth THREE

It's not good for privacy

With DMARC, you can view who is sending emails on your domain's behalf, thus protecting privacy by preventing hackers from using your domain to send suspicious messages within your organization and to your customers. DMARC reporting sets it above other secure email practices.

#GOTheDMARCWay

DMARC Myth FOUR

It's easy

Starting the implementation of DMARC may be relatively simple, but the real work –and most important part– comes with analyzing reports and adjusting your policy level fo

GLOBAL CYBER ALLIANCE

DMARC Myth FIVE

It's going to negatively impact my email

DMARC actually improves the delivery rate of the email you send to customers and others.

#GOTheDMARCWay

GLOBAL CYBER ALLIANCE

DMARC
M

It's only for large entities

Every organization with a public-facing domain

DMARC
Myth
SEVEN

Antispam filters are enough

While antispam software and email security gateways can protect against inbound phishing attempts, DMARC protects emails originating from your domain from being spoofed and used for phishing attacks.

#GOTheDMARCWay

Concerns with Implementation

- Not enough resources
  - Implementation can be time consuming, especially if there are multiple sub-domains
  - Resources needed more for analysis of reports than implementation

- Mailing list and Mail forwarders
  - Breaks DMARC (as well as SPF and DKIM)
  - Solution – Authenticated Received Chain (ARC) – arc-spec.org

Items to Plan for

- Understanding SPF, DKIM, and DMARC
- Access to DNS
- Understand the three policy levels of DMARC
- Does email server support DKIM?
- List of public domains used by organization
  - If you have subdomains - Consider creating a DMARC policy for sub-domains
- Potential Unknowns:
  - Is your organization using 3rd party vendors?
    - Do they support SPF and/or DKIM?
  - Mail systems that IT staff is unaware of
- DMARC report analysis
  - email address to send reports

Additional Resources

- **DMARC.org** (http://www.dmarc.org) - Great source for DMARC information
- **GCA DMARC -** https://dmarc.globalcyberalliance.org
- **Community Forum –** https://community.globalcyberalliance.org
- **GCA YouTube Channel**
  - **Webinars**
  - **Videos for GCA DMARC Setup Guide**
  - **DMARC Bootcamp**

GLOBAL CYBER ALLIANCE

Q&A

Thank You!

Next Session:
May 12th – What are SPF and DKIM?

Shehzad Mirza

gca-dmarc@globalcyberalliance.org