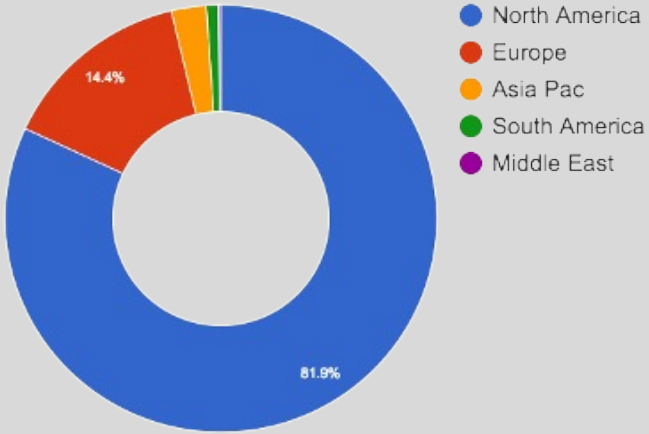
Modern Standards to Improve E-mail Security

Severin Walker (M3AAWG)
Lucimara Desiderá (CERT.br/NIC.br, LAC-AAWG)
Mariska Calabrese (Outreach.IO, M3AAWG)

What is M³AAWG?

Founded in 2004, Messaging, Malware and Mobile Anti-Abuse Working Group (**M³AAWG**) is the largest global industry bringing together all the stakeholders within the online community in a confidential, technology-neutral, and non-political open forum to develop cooperative approaches for fighting online abuse and exploitation.

Who is M³AAWG?
Constituencies and Demographics



"The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) is where the industry comes together to work against botnets, malware, spam, viruses, DoS attacks and other online exploitation"

260 member orgs "worldwide"
300-400 conference participants

Technology-neutral, non-political working body focusing on operational issues of Internet abuse

What Does M³AAWG Do?

Distill Industry Knowledge into BCPs

The “M” cubed:

Messaging: abuse on any messaging platform, from e-mail to SMS texting
Malware: abuse is often just a symptom and vector for viruses and malicious code
Mobile: addressing messaging and malware issues emerging on mobile as an increasingly ubiquitous platform

Develop and Publish:

- Best practice papers
- Position statements
- Training and educational videos

Regional AAWG Development

Peer Working Group in LAC

AAWG Principles and Objectives

- Promulgate anti-abuse norms and principles
- Further develop regional anti-abuse expertise
- Anti-abuse research
- BCPs within and across regions
- Represent regional anti-abuse expertise
- Exchange expertise among operators within the regions globally, among peer regions

The Need for SMTP Security

Why Further Secure Email?

- 91% of cyberattacks start with email
- 5-20% of emails are suspicious
- 50 to 80% increase in attacks each quarter
- 2,370% increase in losses due to BEC [1]

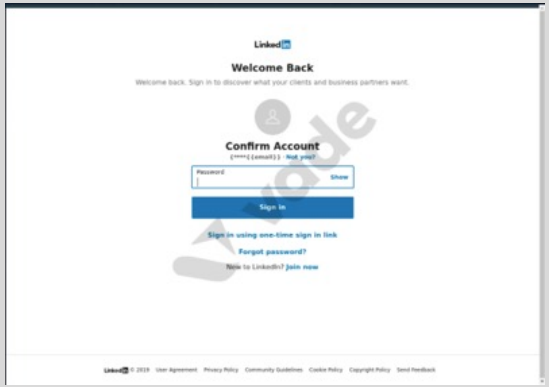
Sources:
VALIMAIL, PhishMe, Proofpoint's Human Factor Report, FBI

Business Email Compromise Techniques

- Reply-To Spoofing
  - From: sender@trusted.com
  - To: recipient@trusted.com
  - Reply To: hacker@badguy.com
- Lookalike Domains
  - From: sender@tru5ted.com
  - To: recipient@trusted.com
- Business Partner Spoofing
  - From: ”Bob Employee hacker@badguy.com”
  - To: “Alice Manager recipient@trusted.com” [1]

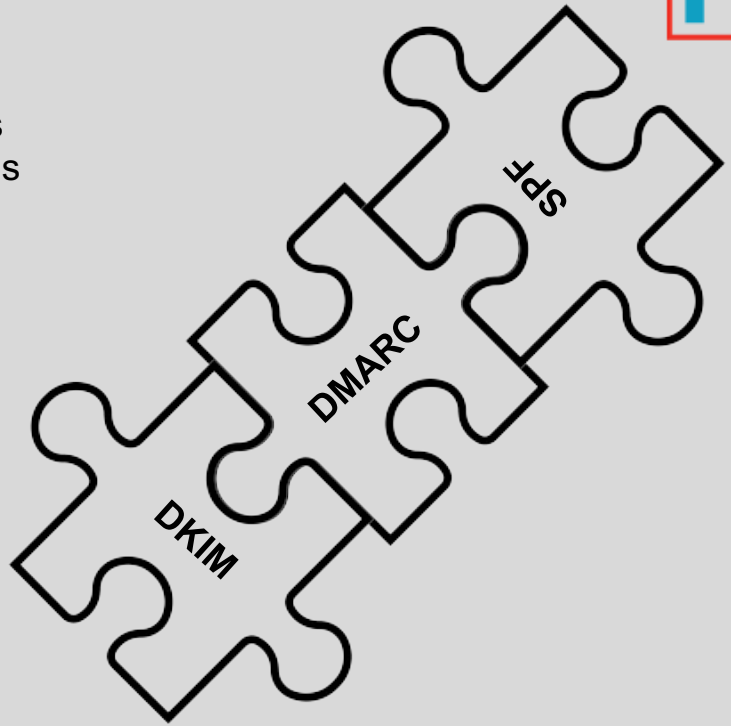
Exact-Domain Phishing

- Increasing Faster than any other attack vector
- Accounts for about one-third to two-thirds of all email attacks
- Content filters and training can’t always stop Well-Designed phishing attacks [1]



Domain Authentication

By combining SPF, DKIM, and DMARC implementations your domains are better protected against spoofed emails attempting to steal credentials or lure customers to malware and ransomware.



SPF

What is SPF?

- Sender Policy Framework is a whitelist of IPs kept in DNS [1]
- The specification allows for reflecting what IPs email is sent from and a suggested treatment of domain traffic from other IPs is observed

```
;; ANSWER SECTION:
comcast.net.
"v=spf1 ip4:69.252.207.0/25 ip4:96.114.154.128/25
ip4:96.103.146.48/28 ip4:96.102.19.32/28
ip4:96.102.200.0/28 include:_spfv6.comcast.net
include:_spf.mdp.comcast.net ?all"
```

```
;; ANSWER SECTION:
cert.br.
"v=spf1 mx a:listas.cert.br ip6:2001:12ff:0:7000::2
ip6:2001:12ff:0:7000::3 -all"
```

What is SPF?

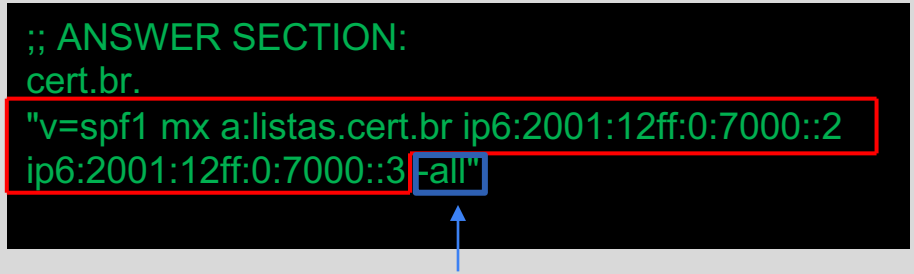
Match these IPv4 ranges or the SPF record for these two domains

```
;; ANSWER SECTION:
comcast.net.
"v=spf1 ip4:69.252.207.0/25 ip4:96.114.154.128/25
ip4:96.103.146.48/28 ip4:96.102.19.32/28
ip4:96.102.200.0/28 include:_spfv6.comcast.net
include:_spf.mdp.comcast.net ?all"
```

For informational purposes only, do not reject if the source IP doesn't match.

What is SPF?

Match this domain's MX, that A record, and these IPv6 ranges



You have the domain owner's permission to reject mail that does not match these items.

DKIM

DomainKeys Identified Mail

DKIM attaches cryptographic fingerprints/signatures to email using the private key of the sender and a DNS-published public key used by receivers. [2]

Verifies the Domain Source: Signatures are attached based on elements of the envelope headers

Verifies the Message Content's Integrity: A separate hash using the keypair can be used to sign for the content of the message itself.

DKIM In Use

```
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
s=eaxkvsyelrnxjh4cicqyjjmtjpetuwjx; d=amazon.com; t=1650837613; h=Date:From:Reply-
To:To:Message-ID:Subject:MIME-Version:Content-Type;
bh=TnoYsqpzIERIbuUyPGZM/HxyVZx+kAw4MuZoAwEyD1c=;
b=R/OxHbavPDPwioxACECJFlKiaJPbjHytKma0MBArpHm+kY24QYHkf7UPA4c+wLfZ
BRRRvdy8756XH/KK3dMDsgAXBqbZ5dYaZRgAZFhKeKqLWJIADGayv9841UJ4W5kB8zQ
GSxOH6BZb8jKe55dh61pM5v91RCOjeq/PPvy0c5c=
```

Tags and hashes inserted by the sender (Amazon) are:

- **v** (required), version
- **a** (required), signing algorithm
- **d** (required), Signing Domain Identifier (SDID)
- **s** (required), selector
- **c** (optional), canonicalization algorithm(s) for header and body
- **q** (optional), default query method
- **t** (recommended), signature timestamp
- **h** (required), header fields - list of those that have been signed
- **bh** (required), body hash
- **b** (required), signature of headers and body

DKIM In Use

```
% dig -t txt eaxkvsyelrnxjh4cicqyjjmtjpetuwjx._domainkey.amazon.com

…

eaxkvsyelrnxjh4cicqyjjmtjpetuwjx.dkim.amazonses.com. 3600 IN TXT
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCisozfWlrxtmMXPIaoQTDkgr76w
2mtWXYcVJGV7HnCrteA8Io/UBGrHc7HgEFXZYEwNM0Uz4ZwZy8GdqyzY9Oqtk1r8xw9RH
F6HhFE9KFKi7Q7UvXkyycwcjZM3RIqP7D6fv9NKn5yj5UsXH++SzG9RTgawJPHjS4SyHUx
DI7uQQIDAQAB"
```

Reciever looks up the public key for decrypting the hashes by retrieving the DNS TXT record for $*selector*._domainkey.$*domain* from the previous slide.

A verification header is inserted into the message before delivery.

```
dkim=pass header.i=@amazon.com
header.s=eaxkvsyelrnxjh4cicqyjjmtjpetuwjx header.b="R/OxHbav";
```

DMARC

DMARC: Domain-based Message Authentication, Reporting & Conformance

Combines SPF and DKIM check with an additional layer of policy and reporting instructions from the verified domain owner to the email receivers. [1]

Authentication: A combination of SPF and DKIM info provided by the sender, verifiable by the receiver.

Reporting: Designated method for providing the sender with valuable information how where their domain is being observed, whether passing or failing authentication checks.

Conformance: Gives instruction to the receiving on behalf of the verified domain owner on how messages should be treated based on the authentication process.

DMARC In Use

```
% host -t txt _dmarc.amazon.com

_dmarc.amazon.com descriptive text

"v=DMARC1;" "p=quarantine;" "pct=100;" "rua=mailto:report@dmarc.amazon.com;"
"ruf=mailto:report@dmarc.amazon.com"
```

```
% host -t txt _dmarc.santanderbank.com

_dmarc.santanderbank.com descriptive text

"v=DMARC1; p=reject; rua=mailto:santander@rua.dmp.cisco.com;
ruf=mailto:santander@ruf.dmp.cisco.com"
```

Tags and hashes in the DMARC records include:

- **v**, version
- **p,** Policy for what to do if authentication fails
- **pct,** How much “bad” traffic from this domain should be treated this way
- **rua,** Where to send daily reports of traffic seen with this domain with authentication results
- **ruf,** Where to send forensic (1:1) reports of the traffic seen

Benefit: DMARC Reporting

By publishing an address to send aggregate DMARC reports to, domain owners can gain free intelligence on how they're organization is being phished or how internal systems may be misconfigured.

DMARC rows of an aggregate record shown in tabular form

Source IP	Count	Disposition	SPF	DKIM	Header from	SPF domain (result)	DKIM domain (result)	
192.0.2.1	12	none	✓ Pass	✓ Pass	example.org	example.org (✓ Pass)	example.org (✓ Pass)	
192.0.2.1	1	none	✓ Pass	✗ Fail	example.org	example.org (✓ Pass)	example.org (✗ Fail)	
192.0.2.28	42	none	✗ Fail	✓ Pass	example.org	example.org (✗ Fail)	example.org (✓ Pass)	forwarder.example (✓ Pass)
192.0.2.82	21	none	✗ Fail	✗ Fail	example.org	discusslist.example (✓ Pass)	example.org (✗ Fail)	discusslist.example (✓ Pass)
...								

Example aggregate report formatted with XSL. Source: Wikipedia

Other Methodologies and Considerations

DNSSEC

DNS Cache poisoning, allowing for Man-in-the-Middle attacks, can impact SMTP anti-abuse policies.

DNSSEC was designed to protect the Internet from certain attacks, such as DNS cache poisoning. It is a set of extensions to DNS, which provide:

a) origin authentication of DNS data
b) data integrity
c) authenticated denial of existence [3]

Secure Email Transport

Domain and source authentication helps to verify that the email originated from the domain it purports to be from, but it does not protect against the plain-text nature of the SMTP protocol.

STARTTLS and DANE support can ensure that each section of an email's journey from the sender to the recipient mailbox is encrypted using modern strong TLS versions (rather than broken SSL or TLS <1.1).

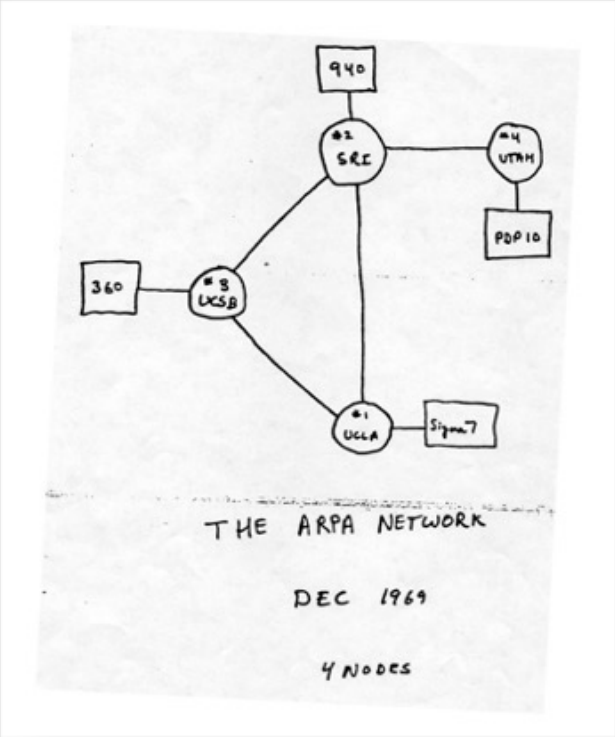
IPv6

While not developed as a security or authentication mechanism, IPv6 support can be an email administrator's opportunity to create stricter, modern policies. This will apply new protections against some of the largest global senders.

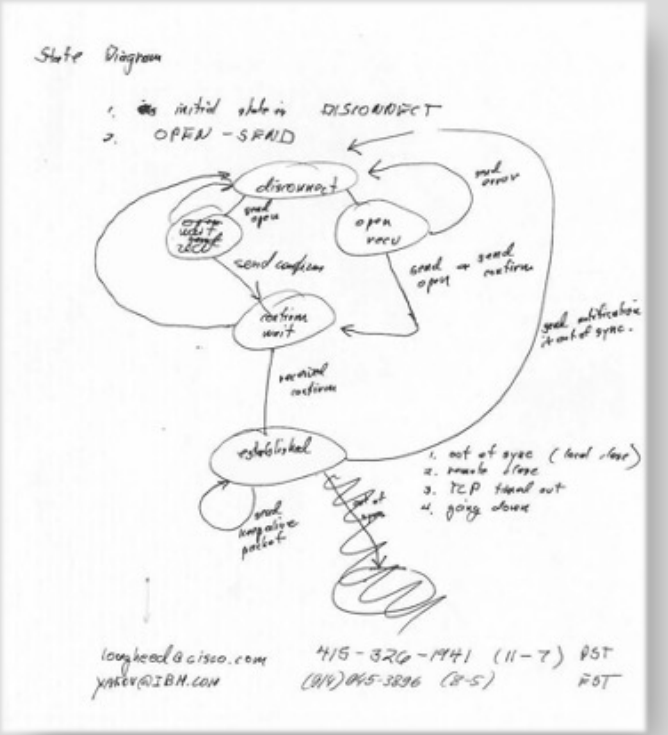
This can be done with the existing v4 policies as a fallback for some.

- "No Auth, No Entry" requirement
- PTR record requirement
- Encryption requirement

Historically, Security Was Not Part of the Project



https://twitter.com/darpa/status/1013047020326739969



https://computerhistory.org/blog/the-two-napkin-protocol/

Modern Internet Standards

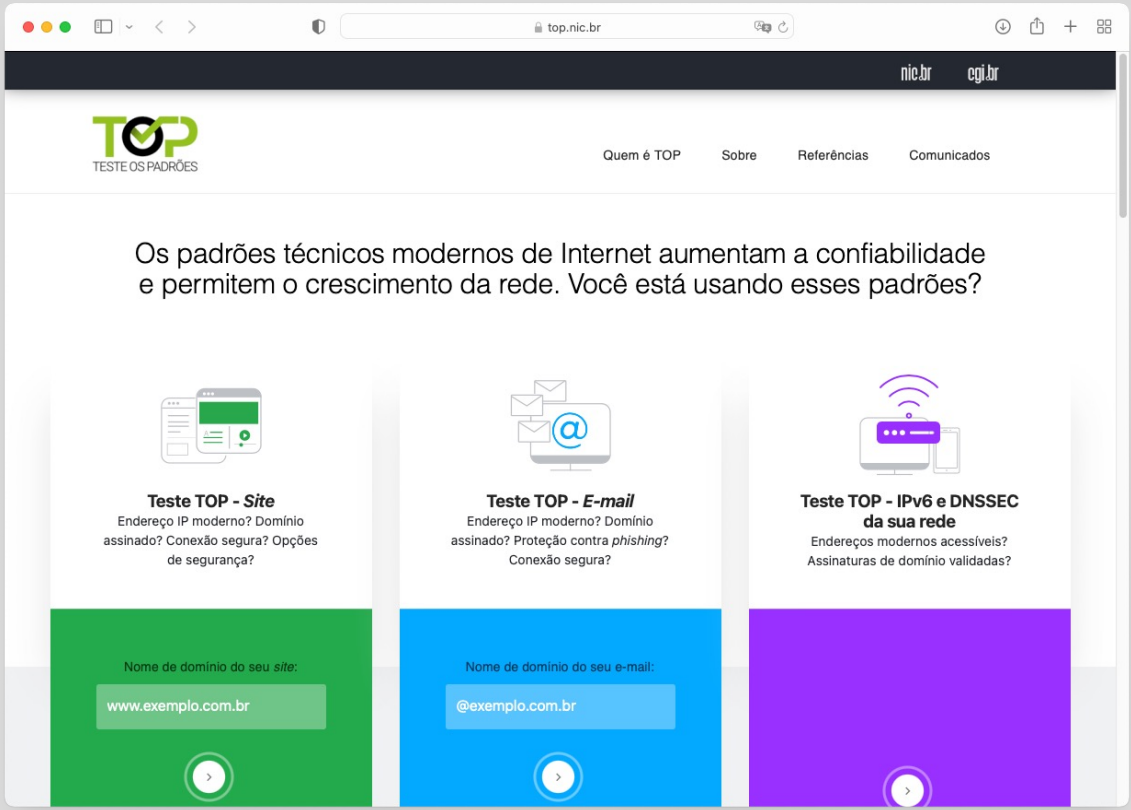
Provide for More Reliability and Further Growth of the Internet.

	Standards	Benefits of Adoption
Strong Encryption	Mandatory HTTPS + HSTS Current versions of TLS Forward Secrecy	• Transaction and data protection • Reduces the chances of encryption cracking • Prevents Crypto Cracking of (old) Captured Traffic
DNS Security	DNSSEC	• Protection against Cache poisoning • Enables the use of other technologies such as DANE
Email Security	STARTTLS • ideally w/ DANE DMARC, DKIM e SPF	• Protection against sniffing (“espionage”) • Increases the reputation of the legitimate message (helps prevent phishing of your brand)

IP Protocol	IPv6 is current
	IPv4 is legacy – and it's over
	• new networks will only get IPv6
	• mobile networks already have native IPv6 (BR)
		• Less complexity
		  • do not rely on CGN or translation v6 → v4
		  • reduces attack surface
		• Facilitates investigation and incident handling process

https://top.nic.br/

Tests for website, email and connectivity



Tests

- correct implementation of the standards
- based on:
  - RFC specifications
  - operational standards recommended by international entities

Report

- breakdown of all results
  - detailed references to the standards
  - pointers on how to fix possible problems

Based on the Internet.nl [4]

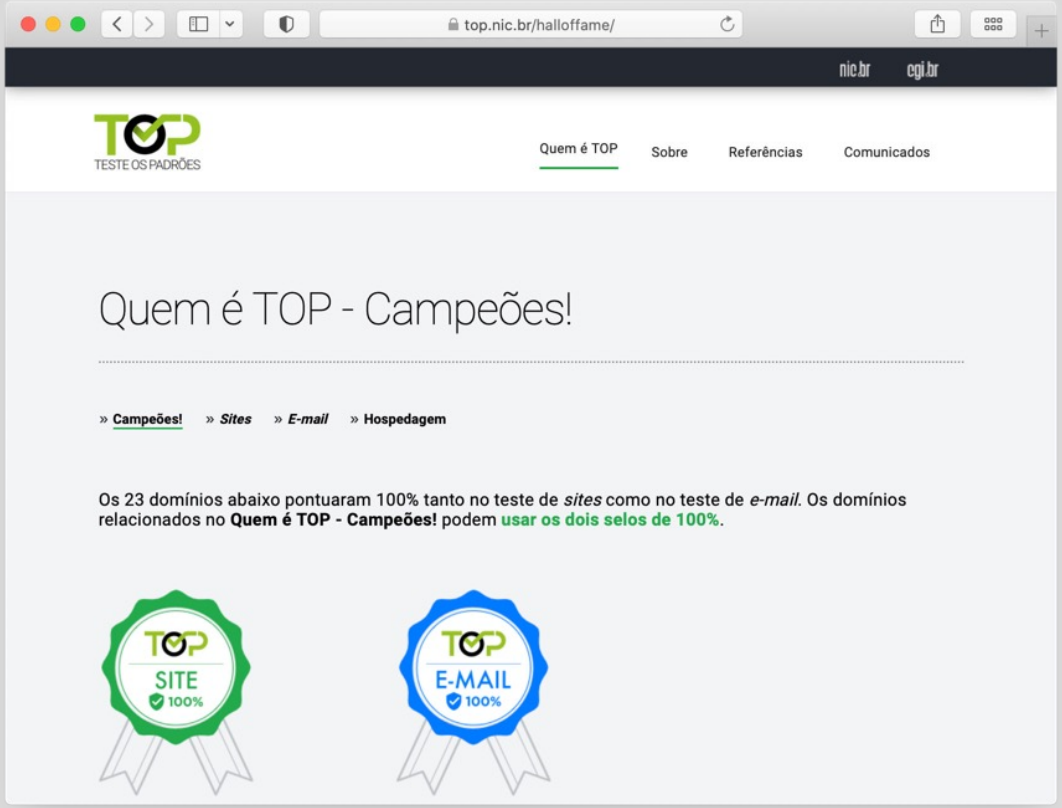
In partnership with the NLnet Labs

Apoiadores

conexis brasil.digital | REDETELESUL | abranet | abrint | AbraHosting | TelComp

https://top.nic.br/

TOP Hall of Fame (Campeões)



Hall of Fame

- **Champions!**
  - domains that score 100% in both website test and the email test
- **TOP – Site**
  - domains that score 100% in the website test
- **TOP – E-mail**
  - domains that score score 100% in the email test
- **TOP – Hospedagem**
  - hoster's own domain 2x 100% in both website test and the email test
  - customer domains 2x 100% in both website test and the email test
  - Trade register
  - Only per request

Questions?

M3AAWG Resources

M3AAWG Email Authentication Recommended Best Practices

M3AAWG Best Practices for Managing SPF Records

M3AAWG Sending Domains Best Common Practices

M3AAWG Initial Recommendations for Addressing a Potential MitM Threat

TLS for Mail: M3AAWG Initial Recommendations

References

1. Seth Blank (Valimail). EMAIL FUNDAMENTALS: AUTHENTICATION
   Presented to M3AAWG February 18, 2019 San Francisco, CA, USA

2. Alwin de Bruin and Tim Draegen. Demystify, Understand, & Use DMARC Hands On!
   Presented to M3AAWG October 8, 2018 Brooklyn, New York, USA

3. DNS SECURITY. Homepage (https://www.dnssec.net/)

4. Internet.nl

References

Standard	References
Mandatory HTTPS + HSTS Current versions of TLS Forward Secrecy	https://www.ssllabs.com/ssltest/ https://ssl-config.mozilla.org https://observatory.mozilla.org
DNSSEC	https://registro.br/tecnologia/dnssec/dnssec-para-provedores/ https://ftp.registro.br/pub/doc/tutorial-dnssec.pdf https://dnsviz.net
STARTTLS • ideally w/ DANE DMARC, DKIM e SPF	https://starttls-everywhere.org https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-secure-the-connections-of-mail-servers https://mecsa.jrc.ec.europa.eu/en/technical#starttls https://havedane.net https://dmarc.org https://dmarc.globalcyberalliance.org
IPv6	https://ipv6.br https://test-ipv6.com