Analysis of DMARC Implementation in Republic of Croatia

Dražen Pranić
Atlantic Grupa d.d., Zagreb, Croatia
drazen.pranic@atlanticgrupa.com

***Abstract* - Many security reports and analyses continuously emphasize email service as the cause or starting point of numerous security incidents. The insecurity of email service results in a steady increase in financial fraud caused by compromising user accounts. The use of more advanced authentication protocols such as DMARC, significantly reduces the risk of these threats. The DMARC protocol and its role in improving email service authentication will be explained in detail. Numerous advantages of the DMARC protocol and implementation challenges will be highlighted. The extent to which DMARC is applied in Republic of Croatia will be shown by an analysis of DMARC implementation at most important companies per total income and relevant entities of public sector. Analysis will show how much are companies and public sector focused on security of email service and will give an insight into the DMARC complexity.**

Key words: email security, phishing, DMARC, authentication

I. Introduction

The insecurity of email services is a fact that is regularly pointed out by various security reports and analyses. Analyses of numerous security incidents indicate that one of the most common initial vectors of attacks is phishing email. Thus, according to one of the most respected security reports, the Verizon Data Breach Report, phishing email attacks are responsible for over 36% of the analysed incidents. Unfortunately, this devastating statistic has been unchanged for years. [1]

One of the world's largest insurance companies, AIG, said in its annual report: "The business email compromise of electronic mail service accounts (BEC) has overtaken ransomware as the main reason for claims." The report further explains that business compromise email service accounts caused by phishing attacks. [2]

The extent of this problem, i.e., its financial scale, is explained in more detail in the Report prepared by the US FBI on an annual basis. Namely, in the period from July 2016 to July 2019, the total reported damage is 26,2 billion $. The damage was caused by a total of 166,349 reported incidents. [3]

Analytics firm Gartner predicts that by 2023, e-mail service compromise attacks will double every year to more than $ 5 billion $ per year and will be a source of huge financial losses for many companies. Gartner also points out weaknesses in the authentication of e-mail services as one of the more important reasons why these simple attacks are still relevant. They recommend the implementation of advanced email authentication as one of the controls that significantly reduces the risk of such attacks. We will explain this in more detail in the following chapters of this paper. [4]

II. The Importance of Email Authentication

Attacks aimed at compromising business email account are generally very simple. The most common form of such attacks is when an attacker changes, falsifies the "from" field of the e-mail message to deceive the recipient of the message.

A particularly effective method of attack is "CEO Fraud" in which attackers pretend to be the organization's management and persuade employees to enable payment to fake account or to transfer money from a business account without authorization. According to the Ministry of the Interior of the Republic of Croatia, this is one of the seven most used financial online frauds. [5]

Email authentication aims to reduce the risk of such and similar scams that exploit the insecurity of email services. The basic task of email authentication is to make the process of sending and receiving emails as secure as possible and significantly aggravate identity impersonation of the email sender.

Each sender’s email is analysed in detail by the incoming recipient email server. Criteria for analysing the message itself is based on the authentication method defined by the sender of the message. Based on this information, the recipient's email server defines whether to deliver, quarantine, or reject the received message.

This process is applied regardless of which type of authentication is used. When receiving the message, the recipient's server analyses certain data in the message and DNS records of the sender's domain. Based on the analysis of the authentication methods used, the message recipient's server decides on the authenticity of the sent message.

In the following chapters of this paper, we will explain the most important authentication methods:

- Sender Policy Framework (SPF),
- DomainKeys Identified Mail (DKIM),
- Domain Message Authentication Reporting and Conformance (DMARC).

III. Sender Policy Framework

The Sender Policy Framework (SPF) is a method of email authentication whose purpose is detection of forgery of the sender's address during e-mail delivery. SPF allows authorized publishing hosts to send emails on behalf of a given domain. Publishing hosts IP addresses are defined in SPF DNS TXT record. SPF uses the Return-Path value to check the source email server.

Recipient email server is responsible for email validation. The decision is made by the check_host function described in RFC 7208 [6] that takes three arguments on input (IP address of the sender, the domain, the MAIL FROM or HELO identity) and returns one of the seven possible results: None, Neutral, Pass, Fail, SoftFail, TempError and PermError. Most important results are Pass and Fail. “Pass result means that the client is authorized to inject mail with the given identity while a Fail result is an explicit statement that the client is not authorized to use the domain in the given identity”. [6] SPF email record check is performed as shown in Figure 1:

1. Receiving email server check a SPF record from the DNS server of the sending email server and analyses the list of IP addresses that are authorized to send emails.
2. If the sender's IP address satisfies the SPF check, then the receiving email server will continue to process the email.
3. If the SPF check is not successful, then the email will be rejected according to the receiving email server settings.

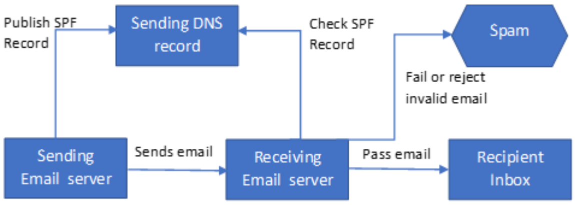


Figure 1. SPF record check

The biggest drawback of the SPF authentication method is that the From Field, which is only visible to the recipient of the email, is not checked. An attacker can specify his domain in the MAIL FROM or Return-Path value satisfy the SPF check and change the sender field and thus deceive the recipient of the email. Therefore, Sender Policy Framework can’t help in email spoofing attacks. Unfortunately, many companies just rely on that basic level of email authentication.

IV. DomainKeys Identified Email

DomainKeys Identified Mail (DKIM) permits a person, role, or organization that owns the signing domain to claim some responsibility for a message by associating the domain with the message. Assertion of responsibility is validated through a cryptographic signature and by querying the Signer’s domain directly to retrieve the appropriate public key.[7]

The email server adds the digital signature of the message to the message itself using its private key. The sender's public key is available using the appropriate DKIM record in the sender's DNS domain. The DKIM DNS records are stored in the following format: selector._domainkey.domain. The domainkey is a fixed string, and the selector is a randomly chosen string by the domain owner. [8]

The recipient email server verifies the digital signature of the sender's public key message. It will detect the DKIM signature and look up the sending email server public DKIM key in DNS record. If the key is found, it can be used to decrypt the DKIM signature. This is then compared to the values retrieved from the received mail. If they match, the DKIM is valid. DKIM email record check is shown in Figure 2

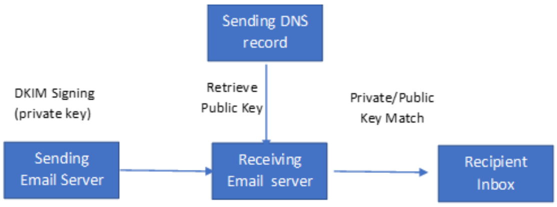


Figure 2. DKIM record check

Applying DKIM authentication prevents an attacker from intercepting an email message, changing it, and sending the changed email message to the recipient.

However, as with the SPF authentication method, DKIM does not check the From Field, which is only visible to the email recipient. An attacker can send a signed message from his DKIM domain and change the From Field of the message and thus deceive the recipient of the email.

V. Domain Message Authentication Reporting and Conformance

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a mechanism by which email operators leverage existing authentication and policy advertisement technologies to enable both message-stream feedback and enforcement of policies against unauthenticated email. [9]

It is based on the Sender Policy Framework and DomainKeys Identified Email protocols explained in the previous chapters. It solves the most important problem of email authentication, which is the unauthorized change of the From Field.

DMARC is based on the results of SPF and /or DKIM, and at least one of the above authentication methods is required for implementation. It is recommended to use both authentication methods to support the DMARC mechanism, due to the additional level of verification. In the case of using only one authentication method, the use of DKIM is recommended, since it provides a higher level of security and eliminates above mentioned security problems present with the SPF mechanism.

DMARC policies are published by Domain Owners and applied by Mail Receivers. A Domain Owner advertises DMARC participation of one or more of its domains by adding a DMARC DNS TXT record. [9]

DMARC records define how you handle messages that comply or not comply with this authentication method. There are three DMARC records / policies:

1. p = none

   Email traffic is only monitored. No additional activities are taken.
2. p = quarantine

   Unauthorized emails are quarantined or spammed by receiving email server.
3. p = reject

   Unauthorized messages are rejected by receiving email server.

When checking the compliance of an email message with the DMARC protocol, it is first checked whether the SPF and / or DKIM requirements are met. If they are then compliance with DMARC requirements is checked. Depending on the results of DMARC compliance and defined DMARC policies, emails are delivered to the recipient.

Consider an example DMARC TXT RR for the domain "sender.dmarcdomain.com" that reads "v=DMARC1;p=reject;pct=100;rua=mailto:postmaster@dmarcdomain.com". In this example, the sender requests that the receiver outright reject all non-aligned messages and send a report, in a specified aggregate format, about DMARC policy applied to a specified address. [10]

DMARC compliance addresses the biggest shortcoming of SPF and DKIM email authentication methods. Namely, DMARC connects the results of SPF and DKIM methods with the content of the e-mail message, i.e., with the content of the sender's field. The domain found in the email sender field is the part of the message that connects the entire DMARC processing.

Today, anyone can buy a domain and set up the appropriate SPF and DKIM records. Therefore, the result of the SPF and DKIM record analysis must be associated with the domain located in the email sender field. This concept is known as identifier alignment. [11] Identifier matching allows existing email authentication methods to become relevant to the content of the message itself. Matching all identifiers is the biggest challenge when implementing the DMARC protocol.

An important part of identifier matching relates to external service providers who communicate with other participants on behalf of the sender.

VI. DMARC REPORTING

DMARC protocol makes a major contribution in the field of reporting. Namely, without the DMARC protocol, it is not possible to answer the simple question: "Which email senders send messages on behalf of my organization"? Without the DMARC protocol, the answer to this question is not possible.

The DMARC protocol enables aggregate and detailed failure/forensic reports. Aggregate reports are sent automatically at a defined interval to the addresses specified in the "rua" parameter, by all email servers on the recipient's side that are set to the appropriate way.

The DMARC aggregate feedback report is designed to provide Domain Owners with precise insight into:

- authentication results,
- corrective action that needs to be taken by Domain Owners, and
- the effect of Domain Owner DMARC policy on email streams processed by Mail Receivers. [12]

Forensic reports defined in the "ruf" parameter, in addition to the above information, contain additional information such as the subject of the message, the header of the message and the URL of the links contained in the body of the message. Forensic reports are typically sent immediately upon receipt of a message that does not meet the DMARC authentication method.

Managing DMARC reports can be a challenge for many organizations. Namely, organizations with many users of email service can expect a huge number of received DMARC reports that need to be analysed. An additional challenge is that DMARC uses XML as a report format. This indicates the need to use ready-made software solutions or platforms for the analysis of DMARC reports.

As the DMARC protocol has grown in popularity, there are more and more such platforms on the market that offer several functionalities, the most important of which are:

- archiving DMARC reports,
- enrichment of DMARC status,
- check the status of SPF / DKIM / DMARC records,
- setting different notifications,
- integration with various security solutions.

VII. CHALLENGES WITH DMARC IMPLEMENTATION

Implementing the DMARC protocol is a complex and long process. This is especially true for large organizations. Such organizations often work with external service providers who need to send emails on behalf of the organization. Example of such service providers are marketing platforms like MailChimp or human capital management platforms like SAP SucessFactors. Prior to the full implementation of the DMARC protocol, the DMARC compatibility of the organization's email infrastructure and the external service providers used by the organization must be ensured. If DMARC is implemented hastily, there is a risk of rejecting many legitimate emails.

Best practice for the implementation of the DMARC protocol emphasizes the importance and need for a phased approach. In the first phase, it is necessary to set up the so-called DMARC auditing.

That is, it is necessary to set the appropriate DMARC record for example: *v = DMARC1; p = none; rua = mailto: dmarc@example.com*. With this record, the DMARC policy is placed in the supervisory or auditing mode, which means that electronic messages will not be rejected in the event of a failed DMARC check. The “*rua”* parameter defines the email address to which the bulk DMARC reports will be sent.

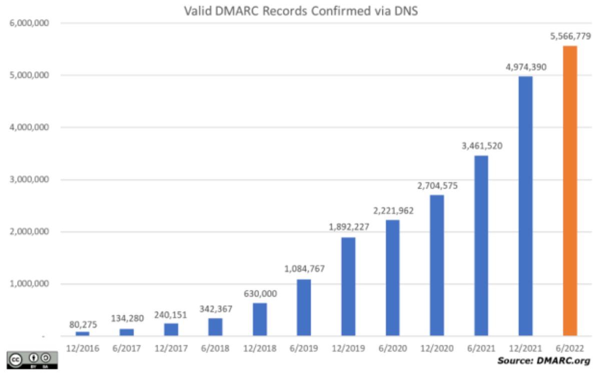
Once DMARC is implemented in the auditing mode, the most demanding part of the implementation begins: the analysis of all external email servers that send messages on behalf of the organization. Once the DMARC policy has been put into auditing mode, at least few months must pass to collect enough bulk DMARC reports to identify all internal and external e-mail senders.

Not all email servers (belonging to the organization itself or external service providers) are at the same level of DMARC compliance. Some are at the very beginning and have, for example, only implemented SPF record and others can be almost compliant with the DMARC protocol. Depending on the number of senders and their level of compliance with the DMARC protocol, it depends on how long it takes for the full implementation of the DMARC protocol. This implies setting the DMARC record / policy *p = reject.* In our example, the DMARC record would look like this: *v = DMARC1; p = reject; rua = mailto: dmarc@example.com.*

Often these activities can be quite complex. Many organizations do not have enough knowledge, human resources for this implementation. As a result, many organizations see the risk of rejecting emails much higher than the risk of receiving unauthorized, spoofed email messages. Therefore, it is not surprising that in addition to the DMARC platform externalization service, the market also offers a service of full implementation of the DMARC protocol. Providers of such a service guarantee the application of p = reject for the agreed domain.

Perhaps it is the growing number of DMARC service providers that is improving the rather poor statistics on the use of the DMARC protocol. Namely, according to the security company Agari, only 34% of the world's largest companies (Fortune 500) have achieved full compliance with the DMARC protocol. In an extremely detailed analysis, Agari included almost 500 million Internet domains. Nearly 13 million domains have valid DMARC DNS record but nearly 4.8 million domains have p=reject DMARC DNS record. [13]

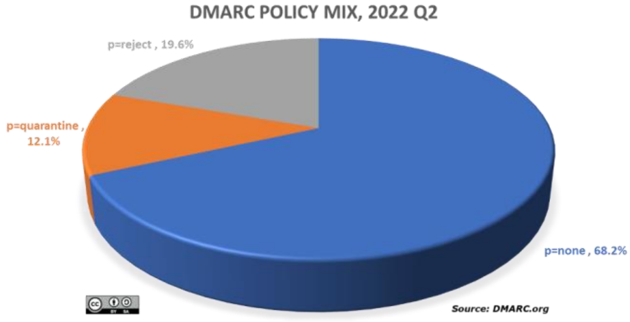
At the same time implementation of DMARC protocol is growing. Following graph is taken from Dmarc.org and shows the total of valid DMARC policies as published every six months from the end of 2016 through 2022. (The figures below are derived from analysis of data generously provided by Domain Tools). [14]



Source: DMARC.org

Figure 3. Valid DMARC records confirmed via DNS

These statistics can provide false sense of compliance since majority of DMARC policy records is p=none. This is shown on Figure 4.



Source: DMARC.org

Figure 4. Dmarc policy mix

DMARC research analysis which is done on top one million domains in the three lists Alexa, Majestics, and Tranco between December 2018 and May 2020 show similar results. According to most recent scan, DMARC is only used by up to 11.5% of all examined domain. It is worth mentioning that DMARC policy p=none is implemented on 67.9% domains. [15]

While a "p=none" DMARC policy is not inherently a problem, it can leave a domain vulnerable to abuse by email spoofers and phishing attacks. It does not provide any direct benefit to the domain owner beyond receiving reports on DMARC activity. In scenario where p=none is not changed for a long period of time this means that DMARC is not implemented at all.

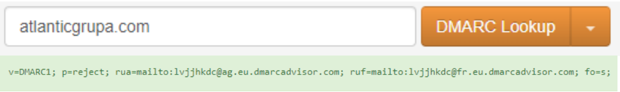
VIII. Analysis of DMARC implementation in Republic of Croatia

In this chapter will be given detail analysis of DMARC implementation in largest Croatian companies and compare it with world statistic. This will show where Croatia is compared to other countries. Is DMARC recognized as very important part of email security?

According to 2022 annual report of Republic of Croatia CERT email incidents related to phishing and phishing URL are responsible for 43% of total security incidents. This result is same compared to last year report and correlates with world statistics. It is obvious that email security is very important issue in Republic of Croatia as well. [16]

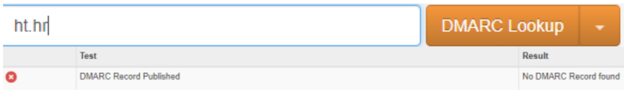
Analysis of DMARC implementation is given for most important Croatian companies based on total value created and relevant entities of public sector. List of top 200 most important companies is taken from business magazine Lider. Their methodology is ranking companies according to added value which is sum of gross wages and gross profit.[17] Some small companies in top 200 without registered internet domain are replaced with companies out of top 200. Added are additional companies from finance sector due to the importance on whole society. In total analysis included DMARC records for three hundred and thirteen internet domains.

DMARC records were analysed with MxToolbox Web page https://mxtoolbox.com/. On figure 5. and figure 6. are given examples of DMARC protocol implementation.



```
v=DMARC1; p=reject; rua=mailto:lvjjhkdc@ag.eu.dmarcadvisor.com; ruf=mailto:lvjjhkdc@fr.eu.dmarcadvisor.com; fo=s;
```

Figure 5. Example of implemented DMARC protocol



	Test	Result
✗	DMARC Record Published	No DMARC Record found

Figure 6. Example of not implemented DMARC protocol

DMARC implementation analysis of all entities in scope of this research on table 1. shows that 32% of them have some DMARC record and 68% don’t have DMARC record.

DMARC policy	Count	Percentage
Not in use	213	68%
Policy none	50	16%
Policy quarantine	28	9%
Policy reject	22	7%

Table 1. DMARC analysis on all entities

DMARC implementation analysis of private sector on 234 domains in table 2. shows that 38% of analysed companies have some DMARC record and 62% don’t have DMARC record.

DMARC policy	Count	Percentage
Not in use	145	62%
Policy none	48	20%
Policy quarantine	24	10%
Policy reject	20	8%

Table 2. DMARC analysis on private sector

DMARC implementation analysis on top 100 private companies in table 3. shows that 39% of analysed companies have some DMARC record and 61% don’t have DMARC record.

DMARC policy	Count	Percentage
Not in use	61	61%
Policy none	21	21%
Policy quarantine	8	8%
Policy reject	10	10%

Table 3. DMARC analysis on top 100 private companies

DMARC implementation analysis on 79 most relevant public institutions (e.g., government bodies, parliament, public agencies, justice system etc.) shows that 14% of analysed entities have some DMARC record and 86% don’t have DMARC record.

DMARC policy	Count	Percentage
Not in use	68	86%
Policy none	3	4%
Policy quarantine	5	6%
Policy reject	3	4%

Table 4. DMARC analysis on public sector

These analyses show that private sector in Croatia is far more advanced in email domain spoofing protection area than public sector. In private sector in total 18% of companies have at least some levels of protection (p=quarantine) or full protection (p=reject). Private sector also has potential for improvement because 20% of companies have DMARC policy p=none. This indicates some level of DMARC awareness.

Public sector is almost two times worse than private sector with only 10% of DMARC p=reject or p=quarantine. This indicates low level of awareness and lack of resources. Public sector is providing important digital services for whole Croatian citizenship. Poor DMARC practise is significantly increasing identity impersonation attacks based on email spoofing. Therefore, it is not surprising that the statistics of email attacks from the annual report of the Croatian CERT is worrying.

If we compare DMARC implementation in Croatia’s top 100 private companies with world’s largest companies situation is not so bright. [18] DMARC analysis done by email security company Agari in table 5. showed significantly largest DMARC adoption in US and UK companies than in Croatia. Australian and German companies are also at more advanced level.

DMARC policy	F 500	FTSE 100	ASX 100	HDAX 100
Not in use	19%	18%	16%	41%
Policy none	37%	35%	44%	28%
Policy quarantine	9%	9%	17%	10%
Policy reject	34%	38%	23%	21%

Table 5. DMARC Breakout: World’s Largest Companies

One of the reasons why US and UK private companies have significantly better DMARC results is the fact that there are binding legal directives for their public sector. [19] [20] Directives like this also have tremendous impact on private sector through raising DMARC awareness and giving strong push to its implementation. Definitively strong regulative is always an efficient way to overcome neglecting important security controls.

Analysis of DMARC implementation in banking and pharmaceutical sector in Republic of Croatia is partially proving this thesis. Those sectors are at more advanced level compared to rest of private sector but still lacking comparing to world’s largest companies.

DMARC policy	Count	Percentage
Not in use	8	40%
Policy none	6	30%
Policy quarantine	3	15%
Policy reject	3	15%

Table 6. DMARC analysis in banking sector

DMARC policy	Count	Percentage
Not in use	5	56%
Policy none	1	11%
Policy quarantine	1	11%
Policy reject	2	22%

Table 7. DMARC analysis in pharmaceutical sector

At the same time insurance sector in Republic of Croatia is completely neglecting DMARC importance. That statistic is even worse than public sector which is disappointing.

DMARC policy	Count	Percentage
Not in use	11	73%
Policy none	3	20%
Policy quarantine	1	7%
Policy reject	0	0%

Table 8. DMARC analysis in insurance sector

Better DMARC statistics in banking and pharmaceutical sector is highly related with sensitive type of business and strict regulation. Risk of email impersonation is quite high in those sectors and minimizing that risk with implementing DMARC is only reasonable option.

IX. Conclusion

The insecurity of email services is unfortunately always a hot topic due to significant financial loses. Attackers use anything that will grab the attention of the email recipients and make such messages as authentic as possible. It is the method of falsifying the From field that helps them a lot. Full implementation of the DMARC protocol significantly reduces the risk of such simple attack methods.

It is clear from the paper that this is not an easy task. However, the benefits of DMARC implementation far outweigh the risks that this implementation brings.

Analysis of DMARC implementation in largest Croatian companies and relevant entities of public sector has shown that this is neglected since only 7% have full DMARC compatibility and 9% have DMARC in quarantine mode. Situation in public sector is even worse. In private sector banking and pharmaceutical sector are leading in this area but still with significant space for improvement.

Probably the best way to push DMARC implementation in private and public sector in Republic of Croatia is binding legal DMARC directive. That kind of directives provided DMARC implementation momentum in USA and UK.

References

[1] 2021 Data Breach Investigations Report, https://enterprise.verizon.com/resources/reports/dbir/, May 2021.

[2] Cyber Claims: GDPR and business email compromise drive greater frequencies, https://www.aig.ae/content/dam/aig/emea/uae/documents/aig-cyber-claims-report-2020.pdf,

[3] Business Email Compromise The $26 Billion Scam, https://www.ic3.gov/Media/Y2019/PSA190910, 10.9.2019.

[4] Protecting Against Business Email Compromise Phishing, https://www.gartner.com/doc/reprints?id=1-1Z0GPFC0&ct=200512&st=sg, 19.3.2020.

[5] Internet fraud, https://policija.gov.hr/prevencija/racunalna-sigurnost/internet-prijevare/456

[6] Scott Kitterman. 2014. Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1. RFC 7208. https://doi.org/10.17487/RFC7208

[7] Murray Kucherawy, Dave Crocker, and Tony Hansen. 2011. DomainKeys Identified Mail (DKIM) Signatures. RFC 6376. https://doi.org/10.17487/RFC6376

[8] Dennis Tatang, Florian Zettl and Thorsten Holz, The Evolution of DNS-based Email Authentication: Measuring Adoption and Finding Flaws; RAID '21: 24th International Symposium on Research in Attacks, Intrusions and Defenses, San Sebastian, Spain, October 2021, https://dl.acm.org/doi/fullHtml/10.1145/3471621.3471842

[9] Murray Kucherawy and Elizabeth Zwicky. 2015. Domain-based Message Authentication, Reporting, and Conformance (DMARC). RFC 7489. https://doi.org/10.17487/RFC7489

[10] Anatomy of a DMARC resource record in the DNS, https://dmarc.org/overview/

[11] Murray Kucherawy and Elizabeth Zwicky. 2015. Domain-based Message Authentication, Reporting, and Conformance (DMARC). RFC 7489. https://doi.org/10.17487/RFC7489

[12] Murray Kucherawy and Elizabeth Zwicky. 2015. Domain-based Message Authentication, Reporting, and Conformance (DMARC). RFC 7489. https://doi.org/10.17487/RFC7489

[13] 2022 Email Fraud & Identity Deception Trends, https://static.fortra.com/agari/pdfs/guide/ag-acid-2022-email-fraud-identity-deception-trends.pdf.

[14] DMARC policies increase 28% Through June 2021, https://dmarc.org/2021/10/dmarc-policies-increase-28-through-june-2021/, October 2021.

[15] Dennis Tatang, Florian Zettl and Thorsten Holz, The Evolution of DNS-based Email Authentication: Measuring Adoption and Finding Flaws; RAID '21: 24th International Symposium on Research in Attacks, Intrusions and Defenses, San Sebastian, Spain, October 2021, https://dl.acm.org/doi/fullHtml/10.1145/3471621.3471842

[16] Annual report of the national CERT for 2022., https://www.cert.hr/wp-content/uploads/2023/02/CERT-G.I.-2022..pdf, 8.2.2023.

[17] Liderovih 500 najboljih: Pogledajte kojih je deset najuspješnijih kompanija u Hrvatskoj, https://lidermedia.hr/biznis-i-politika/liderovih-500-najboljih-pogledajte-kojih-je-deset-najuspjesnijih-kompanija-u-hrvatskoj-145091, 21.9.2022.

[18] 2022 Email Fraud & Identity Deception Trends, https://static.fortra.com/agari/pdfs/guide/ag-acid-2022-email-fraud-identity-deception-trends.pdf.

[19] Binding Operational Directive 18-01: Enhance Email and Web Security, https://www.cisa.gov/binding-operational-directive-18-01

[20] Updating our security guidelines for digital services, https://technology.blog.gov.uk/2016/06/28/updating-our-security-guidelines-for-digital-services/