DMARC Adoption in Saudi Arabia: 2023 Report

POWERDMARC

POWERDMARC

Case study

DMARC Adoption in Saudi Arabia: 2023 Report

Assessing the Threat Landscape

- In 2022, Saudi Arabia saw a huge surge in digital fraud and phishing attacks. According to an analysis released by Kaspersky, in Q2 of 2022 phishing, scams, and social engineering hit the roof in Saudi Arabia with a whopping 168% increase in attacks. The analysis conducted by the organization shed light on 5,808,946 phishing attacks that were detected by their security systems in Saudi Arabia in quarter 2 alone.
- Security analysts have further estimated the cost of a data breach resulting from a single attack incident is expected to exponentially rise in Saudi Arabia in the year 2023. Based on recent studies, it is known that phishing continues to be a widespread and growing problem globally, including in the Middle East region, and that it is constantly evolving to evade detection and increase its effectiveness. It is important for individuals and organizations to stay informed and take proactive measures to protect themselves against phishing attacks

The above-mentioned statistics on the lack of email security in Saudi Arabia raise some serious concerns:

- What is the current situation of DMARC adoption and enforcement in organizations in Saudi Arabia?
- How can we improve the cybersecurity and email authentication infrastructure in Saudi Arabia to mitigate impersonation attacks?

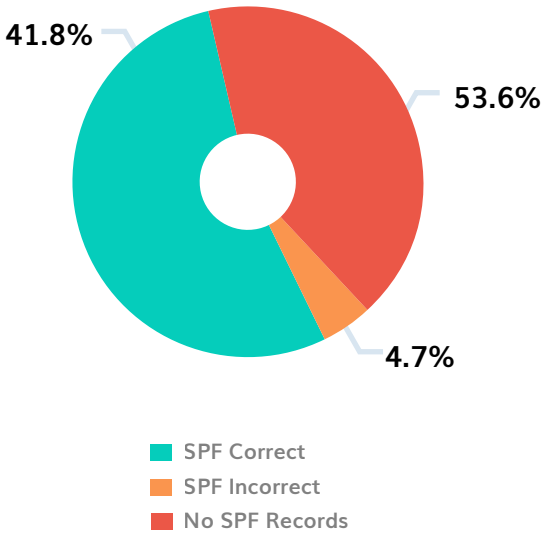
To gain better insight into the current scenario we analyzed 1049 domains belonging to top businesses and organizations in Saudi Arabia, from the following sectors:

- Banking
- Government
- Healthcare
- Energy
- Telecommunications
- Education
- Transport
- Media and Entertainment

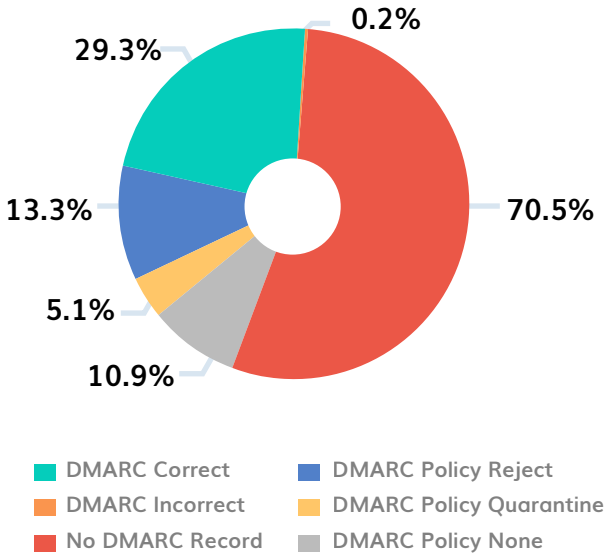
What Do the Numbers Say?

An in-depth SPF and DMARC adoption analysis was conducted while examining all 1049 Saudi Arabian domains, which led to the following revelations:

Saudi Arabia SPF Adoption



Saudi Arabia DMARC Adoption



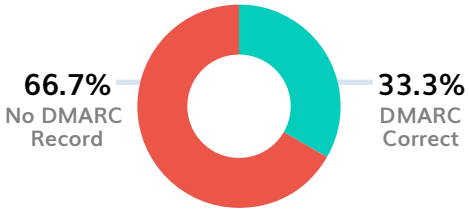
- Graphical Analysis: Among all 1049 domains examined that belong to various organizations in Saudi Arabia, 438 domains (41.8%) possessed correct SPF records, 49 domains (4.7%) had incorrect SPF records, while a ruling majority of 562 domains (53.6%) unfortunately had no SPF records at all. 307 domains (29.3%) had correct DMARC records, while 2 of the domains (0.2%) had DMARC records that contained errors. A vast majority of domains (740 domains making up 70.5%) had no DMARC records at all. 114 domains had their DMARC policy set at none (10.9%), enabling monitoring only, while 54 domains (5.1%) had their DMARC policy level set at quarantine, and 139 domains (13.3%) had their DMARC policy set at maximum enforcement (i.e. p=reject).

Sector-wise Analysis of Canadian Domains

Telecom Sector

SPF Adoption Analysis: Telecom Sector

DMARC Adoption Analysis: Telecom Sector



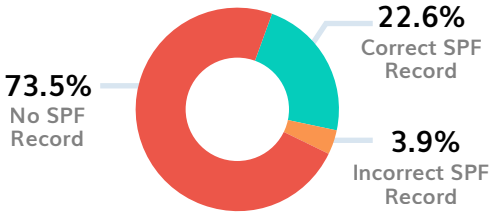
DMARC Enforcement Rates: Telecom Sector

Key Findings:

- 33.3% of domains in the Saudi Arabian Telecom sector had no SPF record
- 38.5% of domains with DMARC implemented had a DMARC policy set at p=none
- No DMARC record was found for 60.7% of the domains

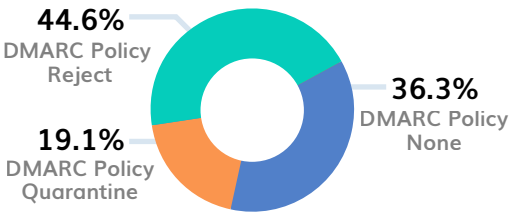
Healthcare Sector

SPF Adoption Analysis: Healthcare Sector



DMARC Adoption Analysis: Healthcare Sector

DMARC Enforcement Rates: Healthcare Sector

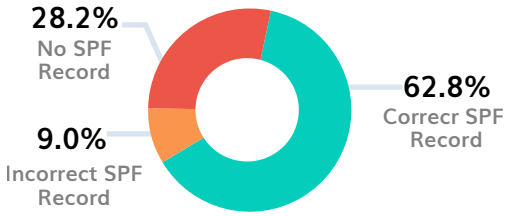


Key Findings:

- 73.5% of the domains had no SPF record published in their DNS
- 84.3% of the domains had no DMARC record published in their DNS
- 36.3% of the domains with DMARC implemented were on a "none" policy

Transport Sector

SPF Adoption Analysis: Transport Sector



DMARC Adoption Analysis: Transport Sector

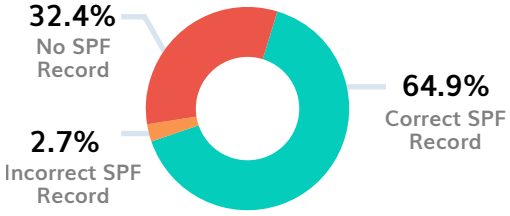
DMARC Enforcement Rates: Transport Sector

Key Findings:

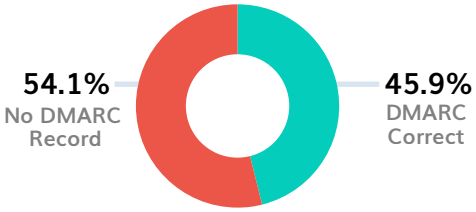
- 28.2% of the domains had no SPF record published in their DNS
- 52.6% of the domains had no DMARC record published in their DNS
- 43.2% of the domains with DMARC implemented were on a “none” policy

Energy Sector

SPF Adoption Analysis: Energy Sector



DMARC Adoption Analysis: Energy Sector



DMARC Enforcement Rates: Energy Sector

Key Findings:

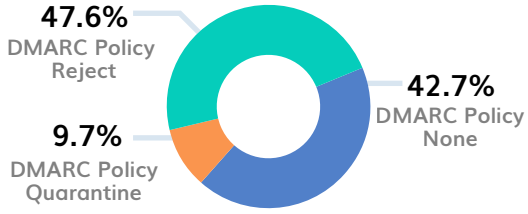
- 32.4% of the domains had no SPF record published in their DNS
- 54.1% of the domains had no DMARC record published in their DNS
- 35.3% of the domains with DMARC implemented were on a “none” policy

Media & Entertainment Sector

SPF Adoption Analysis: Media & Entertainment Sector

DMARC Adoption Analysis: Media & Entertainment Sector

DMARC Enforcement Rates: Media & Entertainment Sector



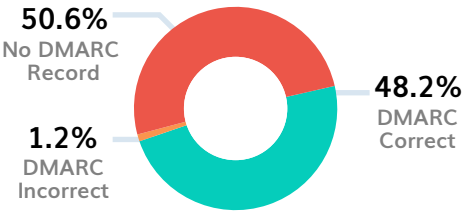
Key Findings:

- 58.1% of the domains had no SPF record published in their DNS
- 77.4% of the domains had no DMARC record published in their DNS
- 42.7% of the domains with DMARC implemented were on a “none” policy

Education Sector

SPF Adoption Analysis: Education Sector

DMARC Adoption Analysis: Education Sector



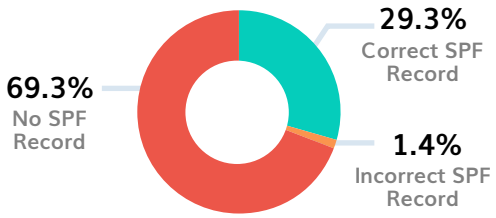
DMARC Enforcement Rates: Education Sector

Key Findings:

- 23.5% of the domains had no SPF record published in their DNS
- 50.6% of the domains had no DMARC record published in their DNS
- 48.8% of the domains with DMARC implemented were on a “none” policy

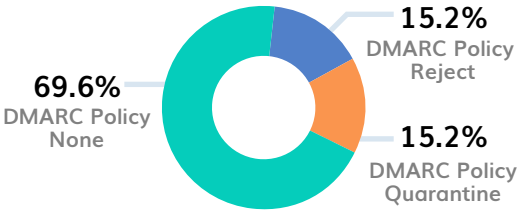
Banking Sector

SPF Adoption Analysis: Banking Sector



DMARC Adoption Analysis: Banking Sector

DMARC Enforcement Rates: Banking Sector

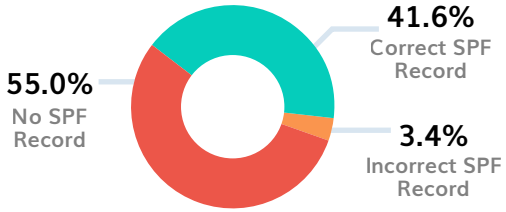


Key Findings:

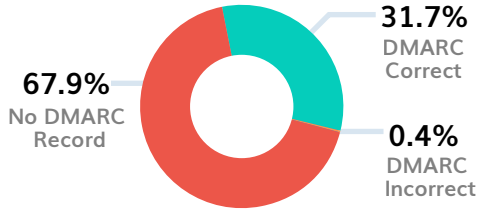
- 69.3% of the domains had no SPF record published in their DNS
- 77.6% of the domains had no DMARC record published in their DNS
- 15.2% of the domains with DMARC implemented were on a “none” policy

Government Sector

SPF Adoption Analysis: Government Sector



DMARC Adoption Analysis: Government Sector

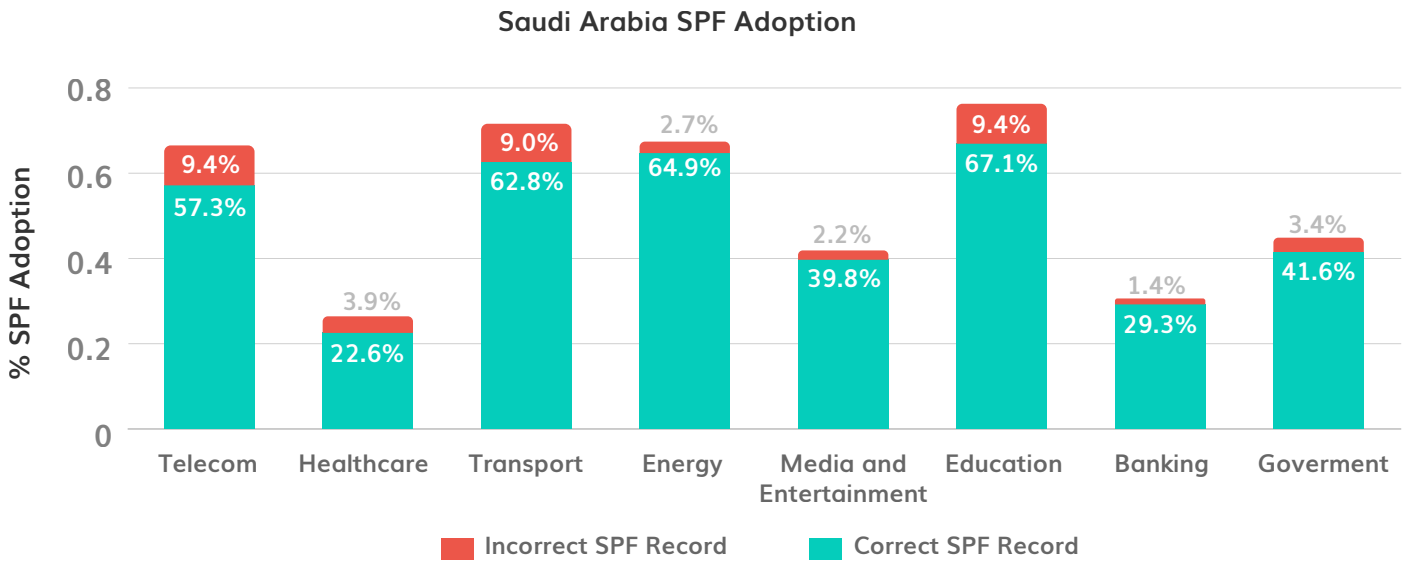


DMARC Enforcement Rates: Government Sector

Key Findings:

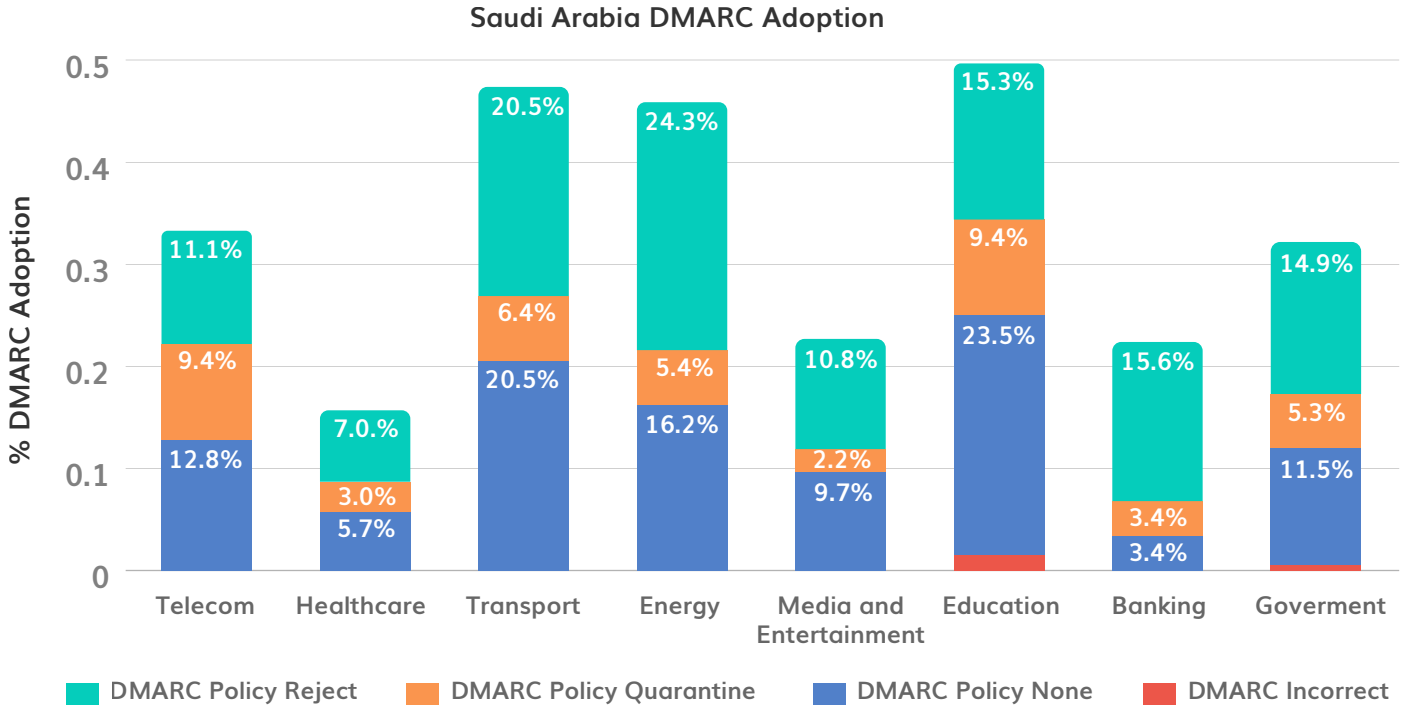
- 55% of the domains had no SPF record published in their DNS
- 67.9% of the domains had no DMARC record published in their DNS
- 36.3% of the domains with DMARC implemented were on a “none” policy

Comparative Analysis of SPF Adoption among Different Sectors in Saudi Arabia



The SPF adoption rate was found to be the lowest in the Saudi Arabian healthcare sector, closely followed by the banking and media & entertainment sectors. The highest rate of SPF adoption was noted in the Saudi Arabian education sector.

Comparative Analysis of DMARC Adoption among Different Sectors in Saudi Arabia



The Saudi Arabian healthcare sector also noted the lowest rate of DMARC adoption, closely followed by the banking and media & entertainment sectors. The highest rate of DMARC adoption was noted among educational institutions in Saudi. A large percentage of organizations in all sectors had their DMARC policies at monitoring only.

Critical Errors Organizations in Saudi Arabia are Making

On analyzing 1049 Saudi Arabian domains from various sectors and industries, it is evident that organizations in Saudi Arabia are making some critical errors that can jeopardize their online reputation and the safety of their clients:

Incorrect SPF records

Incorrect SPF records can result in emails being marked as spam or rejected by recipient mail servers, causing delivery problems. If a large number of emails are marked as spam or rejected, the sender's domain may be considered untrustworthy, resulting in a negative impact on their email reputation. Incorrect SPF records can prevent proper authentication of emails, making them vulnerable to phishing attacks and other forms of email fraud. If emails from a sender with an incorrect SPF record are marked as spam, recipients may become confused about the sender's identity, damaging the sender's credibility.

It's important to have a well-configured and up-to-date SPF record to ensure that emails sent from your domain are properly authenticated and delivered to their intended recipients.

Low SPF and DMARC adoption rates

A high percentage of domains altogether lacked the presence of SPF and DMARC records. SPF and DMARC are industry standards when it comes to protecting your domain against unauthorized use, minimizing spoofing, phishing, BEC and also serving as the first line of defense against ransomware attacks.

DMARC policy lacking enforcement

DMARC helps protect against phishing and spoofing attacks, where attackers use a fake or misleading email address to trick recipients into revealing sensitive information when on an enforced policy like p=quarantine/reject. Without DMARC enforcement, these types of attacks are more likely to succeed.

DMARC at none is a beginner-friendly policy that allows domain owners to monitor their compliances without worrying about email deliverability issues. However, it offers no protection against attacks.

Lack of MTA-STS implementation

MTA-STS is an email authentication protocol that enforces TLS-encryption for SMTP emails in transit. This helps prevent man-in-the-middle attacks like DNS spoofing, and helps domain owners strengthen the security of their email systems. The lack of MTA-STS is an existing vulnerability in most Saudi Arabian domains.

Too many DNS lookups for SPF

As specified by RFC, SPF has a 10 DNS lookup limit, exceeding which can break SPF resulting in false negatives during authentication. Saudi Arabian domains showed a considerable percentage of invalid SPF records due to too many DNS lookups.

Multiple SPF records for the same domain

More than one SPF record for a single domain also leads to invalid SPF. The domain analysis revealed the presence of multiple SPF records for the same domain in some cases. For it to be considered valid, a single SPF record per domain is the way to go.

Steps to be Taken for Improving Email Security in Saudi Arabia

- The following steps can be taken by Saudi Arabian organizations to improve their overall email security posture:

1. Staying under the 10 DNS lookup limit for SPF
2. Having error-free SPF and DMARC records
3. Having a single SPF/DMARC record per domain
4. Implementing additional layers of security like BIMI, MTA-STS, and TLS-RPT
5. Enabling DMARC RUA and RUF reports for monitoring domains and sending sources
6. Shifting from p=none to p=reject DMARC policy for protection against email-based attacks

How can PowerDMARC Help You in this Process?

To achieve a secure email ecosystem, DMARC/DKIM/SPF must be enabled in all gateways within the company. Everything within the company must use a single set of security standards to detect and prevent accidental and malicious email sending sources. PowerDMARC provides a full suite of email security services and hosted solutions that enable you to protect your brand reputation and customers against a wide range of email-borne threats.

- **Configuration:** We help you configure your SPF, DKIM, and DMARC records, to ensure that they are valid and error-free through hosted services.
- **Setup:** As soon as you sign up for our DMARC trial we help you set up your DMARC dashboard, and you gain visibility within 72 hours.
- **Monitoring:** We monitor security incidents in email traffic 24X7 and control legitimate sending sources with alerts, reporting, and responsive actions.
- **Reporting:** Daily Aggregate (RUA) and Forensic (RUF) reports help you keep track of all emails that are passing and failing DMARC from your domains.
- **Enforcement:** We provide full DMARC enforcement (p=reject/quarantine) in record time.
- **PowerSPF:** We allow you to always stay under the 10 DNS lookup limit and updated on any changes made by your ESPs in real-time.
- **Latest Authentication Protocols:** We use the latest email authentication techniques such as MTA-STS, TLS-RPT, and BIMI, along with the standard protocols, to effectively mitigate all impending challenges in email security and authentication.
- **Managed Security Services:** MSP/MSSP-ready platform with a dedicated service desk to support your company's DMARC implementation efforts and to monitor the email authentication health of your domain and the safety of your users.

Let's join hands to increase the rate of DMARC adoption and strengthen the email security infrastructure in businesses across Saudi Arabia. Get in touch with us at support@powerdmarc.com to find out how we can help protect your domain and business today!