DMARC Adoption in Qatar: 2024 Report

POWERDMARC

POWERDMARC

Case study

DMARC Adoption in Qatar: 2024 Report

- DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email authentication protocol designed to improve your email's security. DMARC has played a pivotal role in minimizing email threats like phishing and spoofing for years! So much so, that leading email service providers like Google and Yahoo are now enforcing it.

  DMARC is more than just your everyday email authentication protocol like SPF and DKIM. While the latter are important prerequisites in authenticating the sender, DMARC paves the way for a feedback mechanism. With DMARC, you can configure reports on email deliverability and authentication to be sent back to you. Moreover, you can also instruct the receiving servers on how to treat emails failing authentication checks.

Assessing the Threat Landscape

- With a surge in email-based threats in modern times, Qatar is no exception. Irrespective of the country or place, global technological advancements with the introduction of AI have increased the risk of cybercrime. This has had a worldwide impact, not sparing Qatar from the line of fire.
- According to this article by Economy Middle East, in the first quarter of 2023, Qatar recorded an 88% rise in phishing scams. This is in comparison to the value recorded in the first quarter of 2022. While the second quarter saw a 64% increase!
- Kaspersky's Spam and Phishing Report listed phishing due to social engineering scams as one of the top four email scams in Qatar.
- Qatar hasn't been sitting idle in the face of rising cyber threats either! The country has implemented various measures to enhance its cybersecurity. In 2021, the National Cybersecurity Agency was established in Qatar, to aid in the detection and prevention of cyber threats.
- However, it is still important for individuals and organizations to take proactive measures to protect themselves. Increasing adoption rates of authentication protocols like DMARC can be a great starting point!

In our Qatar DMARC Adoption Report for 2024, we will address the following major concerns:

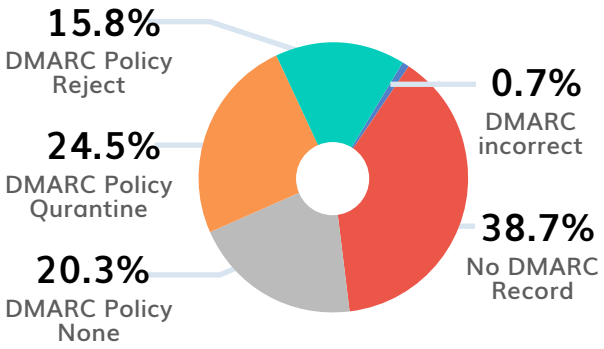
- What is the current situation of DMARC adoption and enforcement in organizations in Qatar?
- How can we improve domain security and email authentication infrastructure in Qatar to prevent impersonation attacks?
- Which industry sectors in Qatar are the most vulnerable to email phishing?
- How does PowerDMARC help organizations mitigate email-based threats?

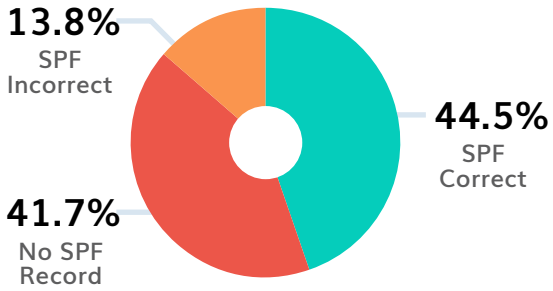
To gain better insight into the current scenario we analyzed 961 domains belonging to top businesses and organizations in Qatar, from the following sectors:

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

What Do the Numbers Say?

An in-depth SPF and DMARC adoption analysis was conducted while examining all 458 Qatar domains, which led to the following revelations:



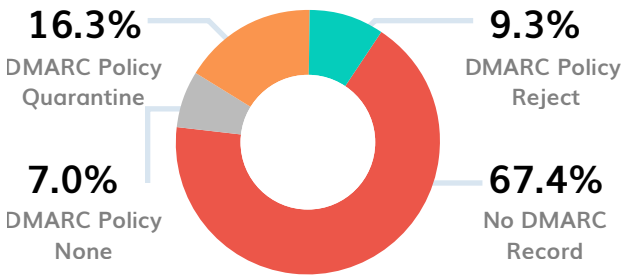


- Graphical Analysis: Among all 458 domains examined that belong to various organizations in Qatar, 294 domains (44.5%) possessed correct SPF records, while 191 domains (41.7%) unfortunately had no SPF records at all. 161 domains (35.15%) had correct DMARC records, while 5 of the domains (1.1%) had DMARC records that contained errors. A vast majority of domains (292 domains making up 63.75%) had no DMARC record found. 54 domains had their DMARC policy set at none (33.5%), enabling monitoring only, while 65 domains (40.4%) had their DMARC policy level set at quarantine, and 42 domains (26.1%) had their DMARC policy set at maximum enforcement (i.e. p=reject).

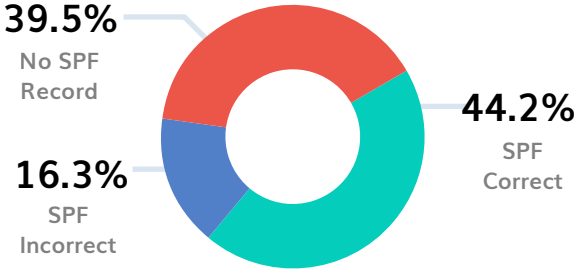
Sector-wise Analysis of Qatar Domains

Healthcare Sector

Qatar DMARC Adoption in the Healthcare Sector



Qatar SPF Adoption in the Healthcare Sector

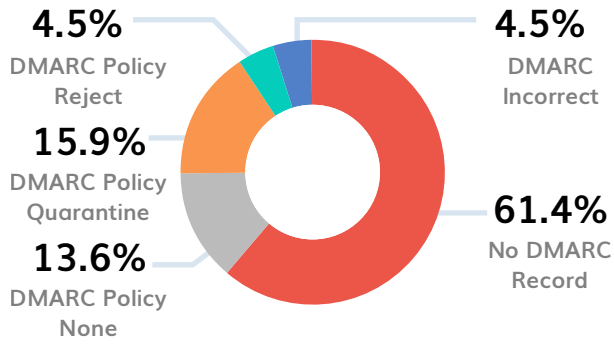


Key Findings:

- 39.5% of domains had no SPF record
- 7% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 67.4% of the domains

Energy Sector

Qatar DMARC Adoption in the Energy Sector



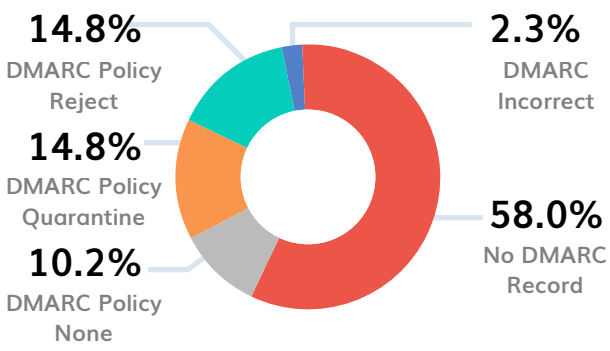
Qatar SPF Adoption in the Energy Sector

Key Findings:

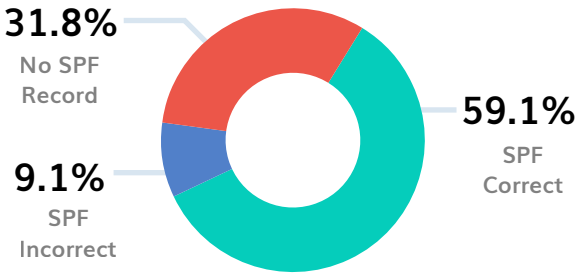
- 38.6% of domains had no SPF record
- 13.6% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 61.4% of the domains

Government Sector

Qatar DMARC Adoption in the Government Sector



Qatar SPF Adoption in the Government Sector

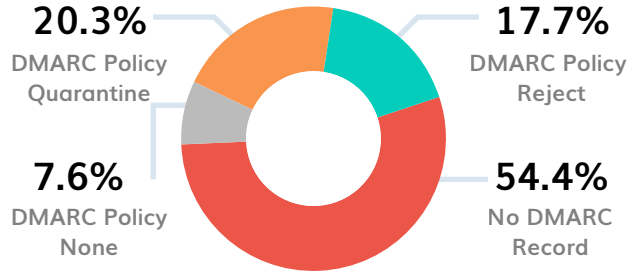


Key Findings:

- 31.8% of domains had no SPF record
- 10.2% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 58% of the domains

Banking Sector

Qatar DMARC Adoption in the Banking Sector



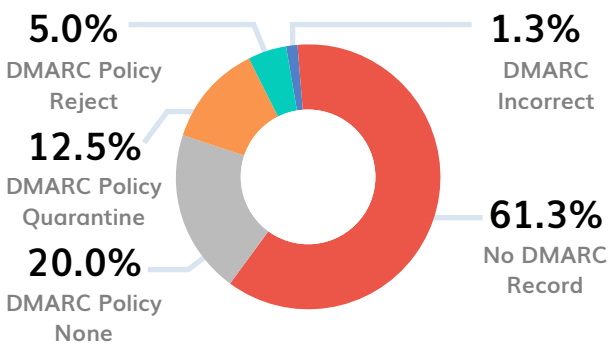
Qatar SPF Adoption in the Banking Sector

Key Findings:

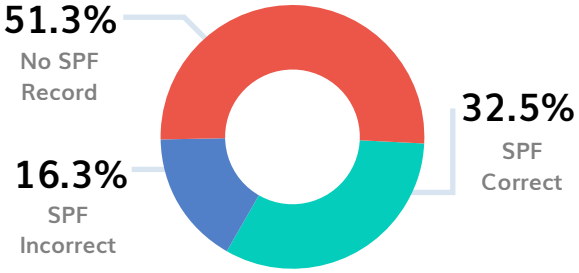
- 38% of domains had no SPF record
- 7.6% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 54.4% of the domains

Education Sector

Qatar DMARC Adoption in the Education Sector



Qatar SPF Adoption in the Education Sector

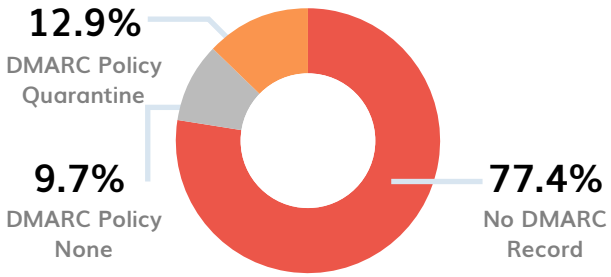


Key Findings:

- 51.3% of domains had no SPF record
- 20% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 61.3% of the domains

Telecom Sector

Qatar DMARC Adoption in the Telecom Sector



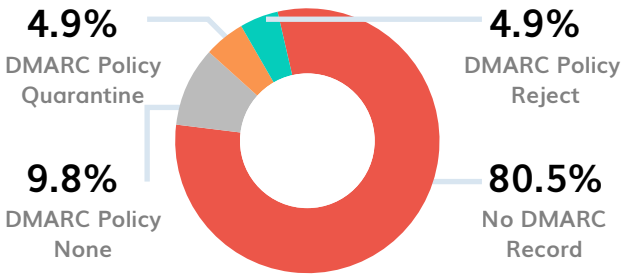
Qatar SPF Adoption in the Telecom Sector

Key Findings:

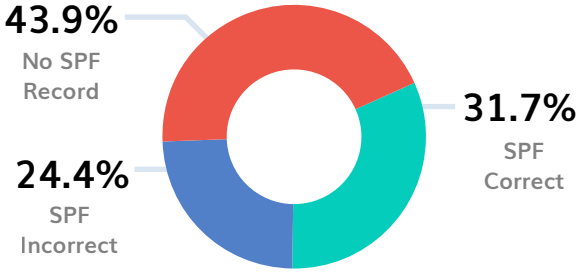
- 54.8% of domains had no SPF record
- 9.7% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 77.4% of the domains

Media and Entertainment Sector

Qatar DMARC Adoption in the Media and Entertainment Sector



Qatar SPF Adoption in the Media and Entertainment Sector

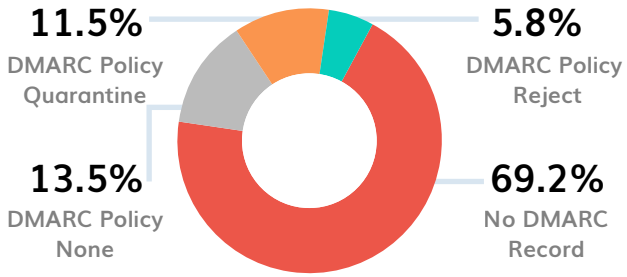


Key Findings:

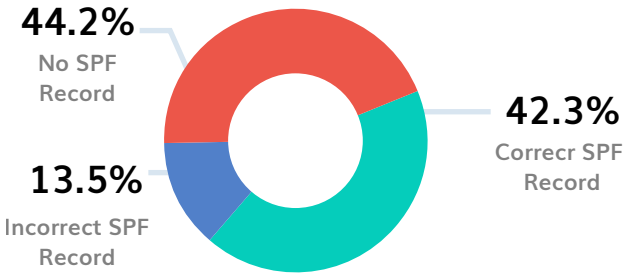
- 43.9% of domains had no SPF record
- 9.8% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 80.5% of the domains

Trasport Sector

Qatar DMARC Adoption in the Transport Sector



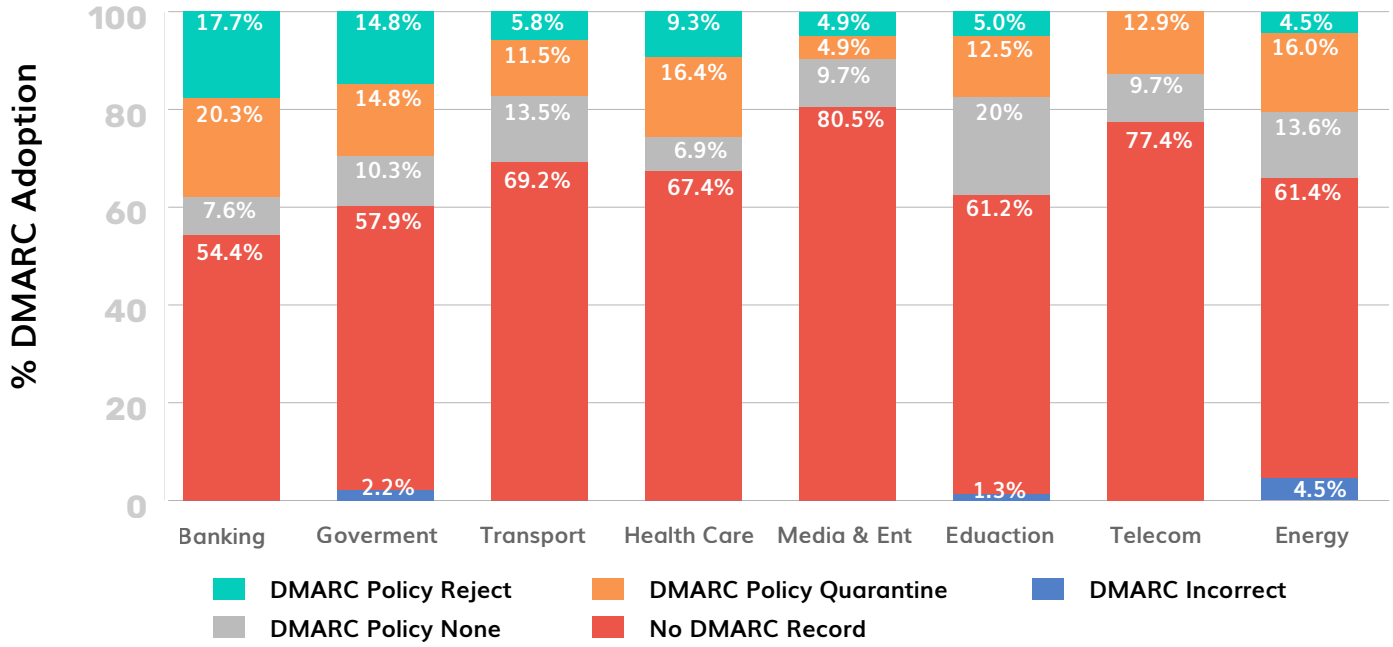
Qatar SPF Adoption in the Transport Sector



Key Findings:

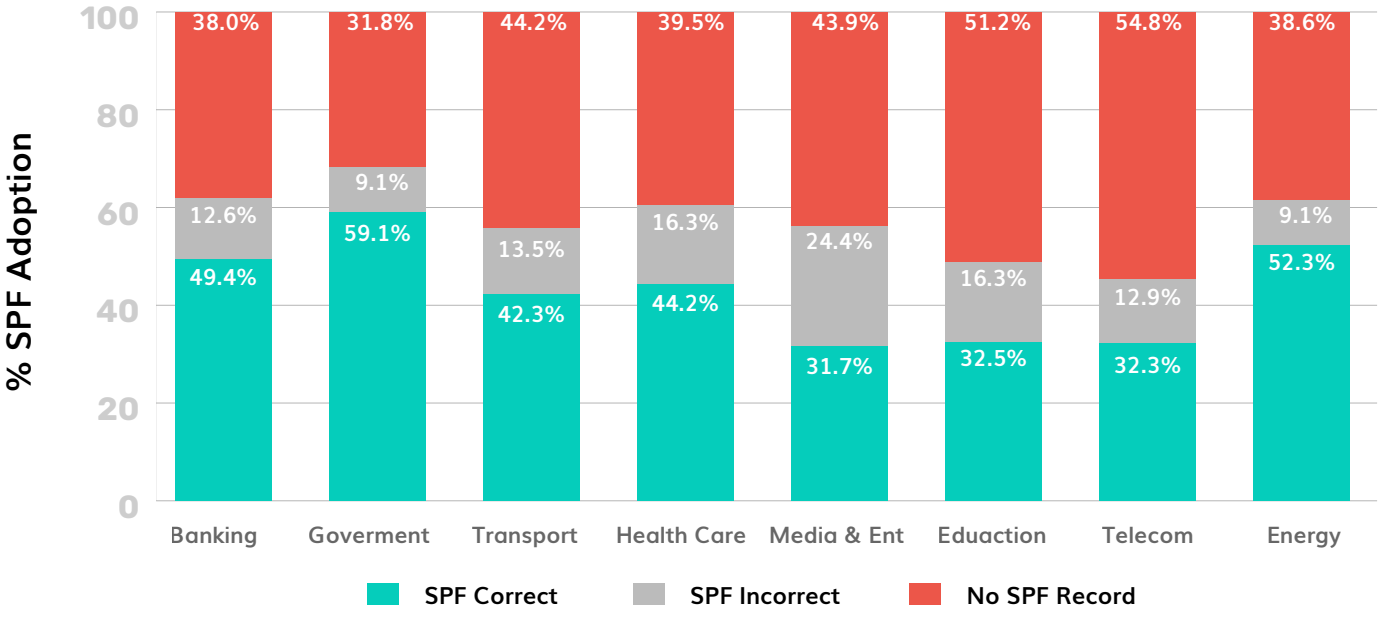
- 44.2% of domains had no SPF record
- 13.5% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 69.2% of the domains

Comparative Analysis of SPF Adoption among Different Sectors in Qata



- The SPF adoption rate was found to be **low** in Qatar's **Education** and **Telecom sectors.** The **highest** rate of SPF adoption was noted in the Qatar **Government, Banking,** and **Energy sectors.**

Comparative Analysis of DMARC Adoption among Different Sectors in Qatar



- Qatar **Media and Entertainment, Telecom,** and **Transport sectors** noted **low** rates of DMARC adoption. The **highest** rate of DMARC adoption was noted among **Banks** in Qatar. A large percentage of organizations in all sectors had no DMARC policy implemented.

Critical Errors Organizations in Qatar are Making

On analyzing 458 domains belonging to various sectors and industries in Qatar, we found that there were some critical errors that organizations in Qatar are making. These errors, if overlooked, could potentially leave them vulnerable to cyberattacks.

Incorrect SPF and DMARC Records

If your SPF or DMARC record syntax is incorrect, it negates the purpose of implementing these protocols. Having incorrect SPF or DMARC records may cause email delivery issues, or lead to messages being flagged as spam. This not only negatively impacts your email marketing campaigns, but can also harm your sender reputation.

Moreover, incorrect configurations will leave your domain vulnerable to phishing and spoofing attacks.

It is important to make sure you use a reliable tool like our SPF and DMARC record generator to create your records. This will ensure your records don't contain any syntax errors. You must also ensure your records are updated. For example, if you update your email vendors, you must add them as authorized sending sources in your SPF record.

SPF and DMARC Record Not Found

Many Qatar domains don't have SPF and DMARC records, which are important for safeguarding your domain from unauthorized use, spoofing, phishing, and ransomware. By adding SPF and DMARC records, you can boost your domain's security and defend against harmful activities. It's like putting locks on your doors and windows – it won't stop all the bad guys, but it'll definitely make them think twice before trying anything!

DMARC Policy Set at "None"

DMARC "none" is an important policy during the initial stages of your email authentication journey. However a few months in, if you are still stuck at "none" you're doing it wrong! DMARC none is a no-action policy that allows you to monitor your email channels and mail handling activities. However, it does not protect against cyber attacks. Enforcing your DMARC policy with "quarantine" or "reject," can minimize domain name impersonation.

Several organizations in Qatar had their DMARC policy configured at "none", limiting their domain protection capabilities. By using a DMARC analyzer to smoothly move towards enforcement, they can reduce the risk of domain abuse!

Missing MTA-STS and TLS-RPT

The email security feature called MTA-STS guarantees that SMTP emails are sent over encrypted channels using TLS, which stops attackers from intercepting them, like in DNS spoofing. By using MTA-STS, owners of domains can boost their email system's security. Yet, many Qatar domains don't have MTA-STS set up, leaving them open to potential attacks.

SMTP TLS Reports come in handy if you have MTA-STS implemented. In case your email is undelivered due to TLS encryption failures, these reports help you gain visibility.

Exceeding SPF Lookup Limit

Adhering to RFC standards, SPF sets a cap of 10 DNS lookup limits. If this threshold is exceeded, SPF may break. This may lead to authentication failures and inaccurate results during authentication. A large percentage of Qatar domains had invalid SPF records. It is possible that this is due to the very common DNS lookup limit issue.

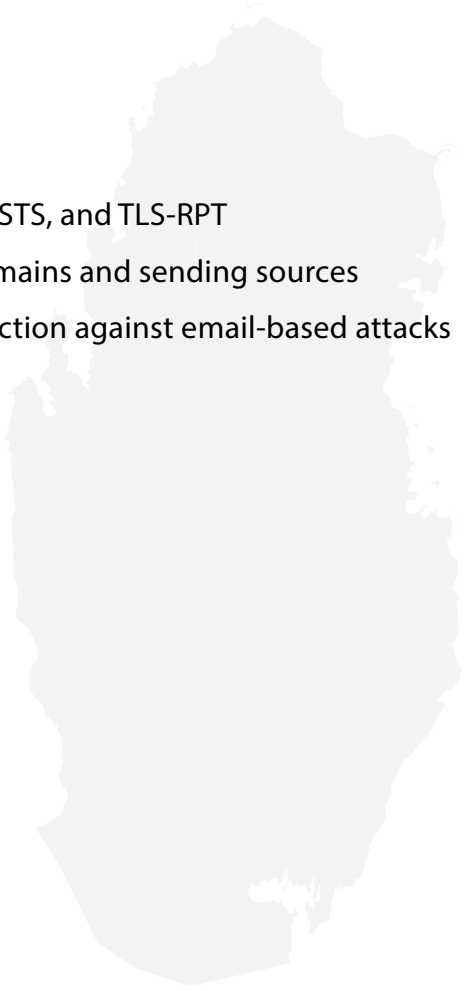
Too many DMARC/SPF records for the same domain

You cannot have more than one SPF or DMARC record for your domain. Configuring multiple SPF records for a single domain will make your SPF invalid. PowerDMARC comes across several customers making this error every day, which we have then corrected. Hence multiple record configurations for the same domain can be another mistake Qatar organizations may be making.

How Can Organizations in Qatar Improve Email Security?

- The following steps can be taken by Qatar 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



PowerDMARC Helps You in this Process

It's essential to set up DMARC, DKIM, and SPF on all gateways within a company to ensure email security. Consistently following these email sender best practices across all your domains and channels helps identify and block unauthorized or harmful email sources effectively.

PowerDMARC provides a full suite of email security services and hosted solutions that can assist you with your goals:

- **Configuration, Setup & Management**

  We help you configure, setup, and manage your SPF, DKIM, and DMARC records, to ensure that they are valid and error-free through hosted services.

- **Hosted Email Authentication**

  PowerDMARC offers a full suite of hosted email authentication services. This includes hosted DMARC, hosted DKIM, hosted SPF, hosted MTA-STS and TLS-RPT, and hosted BIMI. Our cloud-native platform helps you configure, update, and optimize your implementations without accessing your DNS multiple times!

- **Smart and Simple Reporting**

  Daily Aggregate (RUA) and Forensic (RUF) reports help you keep track of all emails that are passing and failing DMARC from your domains. Our DMARC reports are human-readable, and organized into tables, and charts. Colorful representation and visual elements make monitoring effortless and effective.

- **White-Glove Support**

  We help you shift to DMARC enforcement (p=reject/quarantine) safely, and in record time. Our team of domain security experts go above and beyond to help you consistently improve your compliance.

- **SPF Record Optimization**

  We allow you to always stay under the 10 DNS lookup and SPF length limit with SPF Macros. We keep you updated on any changes made by your ESPs in real-time, so you can implement them promptly.

- **Reputation Monitoring**

  We help organizations monitor their domains and IPs in 200+ DNS blocklists. This helps you get whitelisted faster to prevent your emails from getting rejected or flagged.

- **Real-time Alerts**

  With us you can configure a range of alerts depending on your preferences. We allow you to set up email, slack, discord, and webhook alerts, to receive notifications for any triggers you set for your domains or assets.

- **Google and Yahoo Compliance**

  Google and Yahoo have made SPF or DKIM mandatory for all email senders. Bulk senders must go one step further and implement DMARC as well to stay compliant. We help organizations and governments meet Google and Yahoo compliance at lightning speed!

- **PCI-DSS Compliance**

  DMARC implementation has been made mandatory by the PCI Data Security Standards Council. Every organization processing credit and debit card payments will need to implement the protocol by March 2025. We help you meet DMARC PCI-DSS requirements smoothly for your business to stay compliant with the latest standards.

- **Managed Security Services**

  MSP/MSSP-ready platform with a dedicated service desk to support your company's DMARC implementation efforts. Our DMARC MSP Partner Program helps you 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 Qatar. Get in touch with us at support@powerdmarc.com to find out how we can help protect your domain and business today!