

# Kuwait DMARC & MTA-STS Adoption Report 2024



POWER DMARC

# Kuwait DMARC & MTA-STS Adoption Report 2024



- ▶ Between 2022 and 2023, more than 20,000 Kuwait citizens were impacted by cybercrime, incurring over \$160 million in costs. The Electronic and Cyber Crime Department at the Ministry of Interior in Kuwait has faced several challenges in addressing the need for data privacy and cybersecurity awareness in the country, especially since the rise of artificial intelligence (AI).

Officials from the Kuwait Cyber Crime Department reported that cyber attackers targeted private firms and government institutions in Kuwait, to steal sensitive information. This highlighted the need to enhance cybersecurity in the country by implementing modern solutions and strategies.

## Why Is DMARC & MTA-STS Adoption Important?

DMARC and MTA-STS are both email authentication protocols designed to enhance the security of domain names. DMARC allows domain owners to authenticate messages sent from their domain, preventing phishing emails impersonating legitimate domains from reaching recipients. MTA-STS on the other hand prevents unencrypted messages from being delivered to your mailbox, ensuring a secure connection during email transfer.

DMARC and MTA-STS play a pivotal role in email and domain security, preventing a variety of cyber attacks including phishing, spoofing, ransomware, business email compromise, man-in-the-middle, and DNS spoofing.

# Assessing the Threat Landscape

- ▶ Do you know how easy it is to get phished? Verizon's 2024 DBIR report says - it takes less than 60 seconds! This means that if an email impersonating an organization's domains reaches their clients - there is a 90% chance that the receiver will get scammed! This is why organizations need to take active measures to stop such emails from reaching their customers in the first place.
- ▶ With more than 3.4 billion phishing emails sent every day, implementing email authentication has been made mandatory by even tech giants like Google and Yahoo.

## In our Kuwait DMARC and Email Authentication Adoption Report for 2024, we will address the following major concerns:

- ▶ What is the current situation of SPF and DMARC adoption and enforcement in organizations in Kuwait?
- ▶ How can we improve the cybersecurity and email authentication infrastructure in Kuwait to prevent impersonation attacks?
- ▶ What is the current status of MTA-STS adoption among organizations in Kuwait?
- ▶ Which industry sectors in Kuwait are the most vulnerable to email phishing and other cyberattacks?
- ▶ What is the rate of DNSSEC enablement among Kuwait organizations?
- ▶ How can organizations mitigate email-based threats?

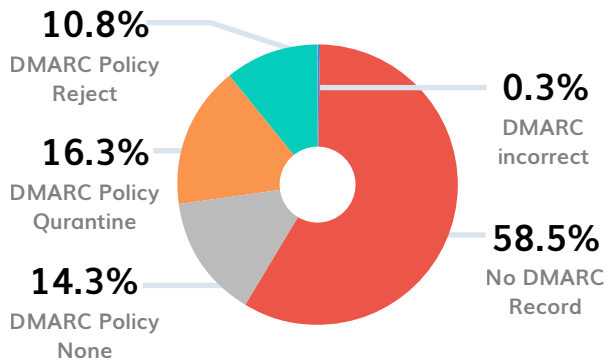
## To gain better insight into the current scenario we analyzed 400 domains belonging to top businesses and organizations in Kuwait, from the following sectors:

- ▶ Healthcare
- ▶ Media
- ▶ Government
- ▶ Telecommunication
- ▶ Transport
- ▶ Financial
- ▶ Education
- ▶ Energy
- ▶ Miscellaneous Businesses

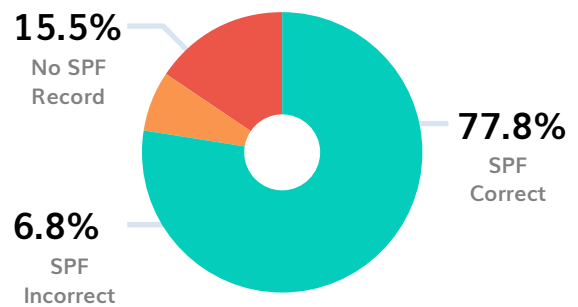
# What Do the Numbers Say?

An in-depth SPF, DMARC, MTA-STS, and DNSSEC adoption analysis was conducted while examining all 400 Kuwait domains, which led to the following revelations:

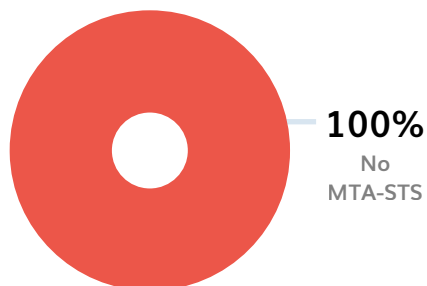
## Kuwait DMARC Adoption Analysis



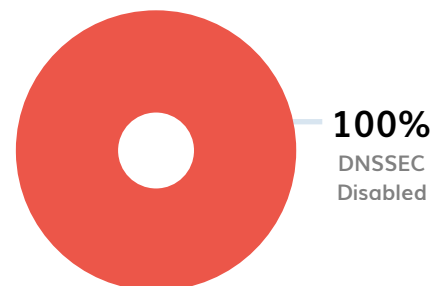
## Kuwait SPF Adoption Analysis



## Kuwait MTA-STS Adoption Analysis



## Kuwait DNSSEC Adoption Analysis

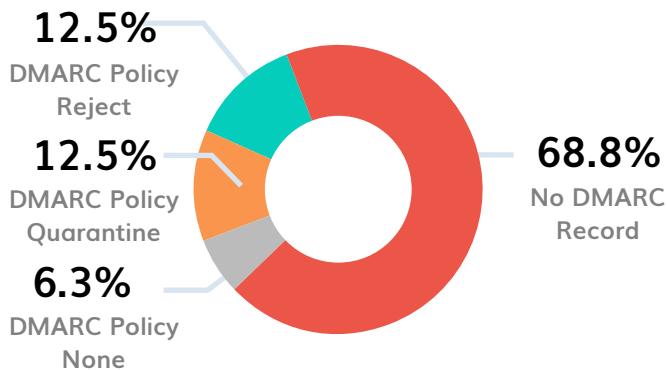


- **Graphical Analysis:** Among all 400 domains examined that belong to various organizations in Kuwait, 311 domains (77.75%) possessed correct SPF records, while 62 domains (15.5%) unfortunately had no SPF records at all. 165 domains (41.25%) had correct DMARC records. A vast majority of domains (234 domains making up 58.5%) had no DMARC record found. Out of the domains with DMARC implemented, 57 had their DMARC policy set at none (14.25%), enabling monitoring only, while 65 domains (16.25%) had their DMARC policy set at quarantine, and 43 domains (10.75%) had their DMARC policy set at maximum enforcement (i.e. p=reject). Additionally, none of the Kuwait domains that were examined had MTA-STS or DNSSEC enabled.

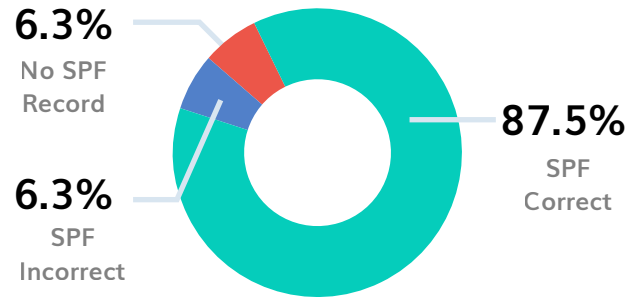
# Sector-wise Analysis of Domains in Kuwait

## Healthcare Sector

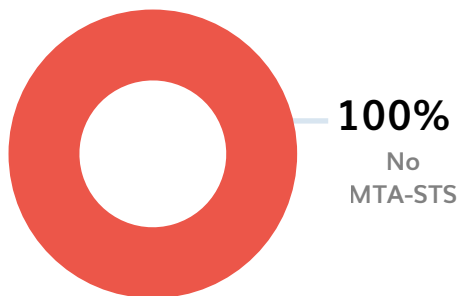
DMARC Adoption Analysis in the Kuwait Healthcare Sector



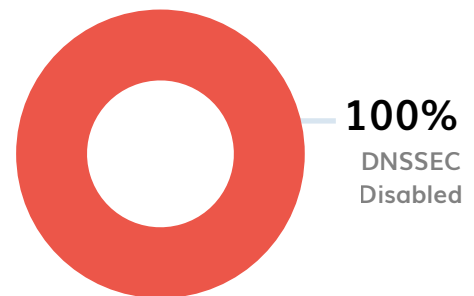
SPF Adoption Analysis in the Kuwait Healthcare Sector



MTA-STS Adoption Analysis in the Kuwait Healthcare Sector



DNSSEC Adoption Analysis in the Kuwait Healthcare Sector

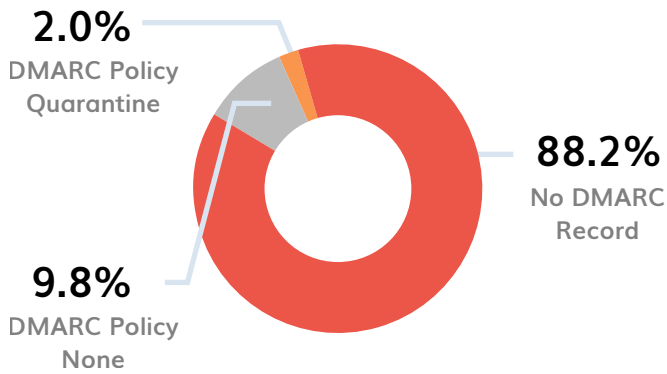


### Key Findings:

- ▶ 6.3% of domains had no SPF record
- ▶ 6.3% of the domains had their DMARC policy set at p=none
- ▶ No DMARC record was found for 68.8% of the domains
- ▶ None of the domains in the Kuwait Healthcare sector had MTA-STS implemented
- ▶ DNSSEC was disabled for all the domains

# Media & Entertainment Sector

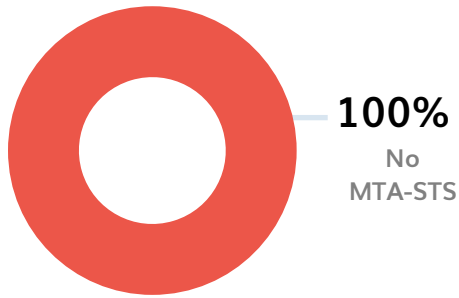
### DMARC Adoption Analysis in the Kuwait Media & Entertainment Sector



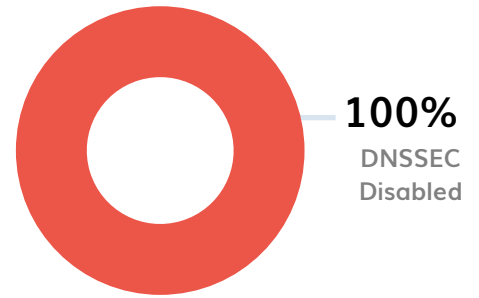
### SPF Adoption Analysis in the Kuwait Media & Entertainment Sector



### MTA-STS Adoption Analysis in the Kuwait Media Sector



### DNSSEC Adoption Analysis in the Kuwait Media Sector

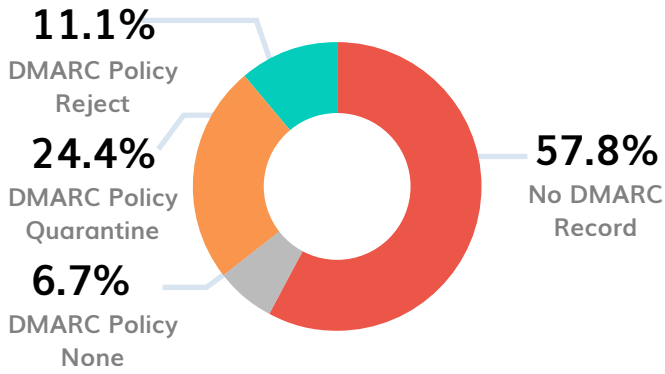


#### Key Findings:

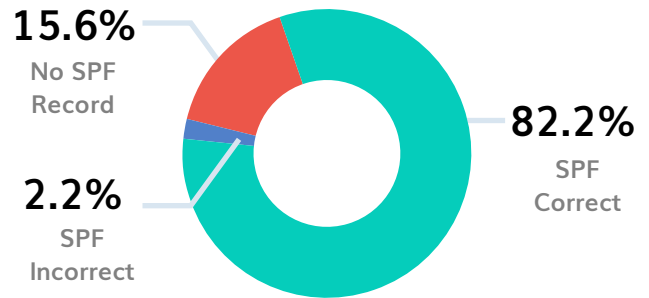
- ▶ 31.4% of domains had no SPF record
- ▶ 9.8% of the domains had their DMARC policy set at p=none
- ▶ No DMARC record was found for 88.2% of the domains
- ▶ MTA-STS wasn't enabled for any of the examined domains
- ▶ DNSSEC was disabled for all of the domains

## Government Sector

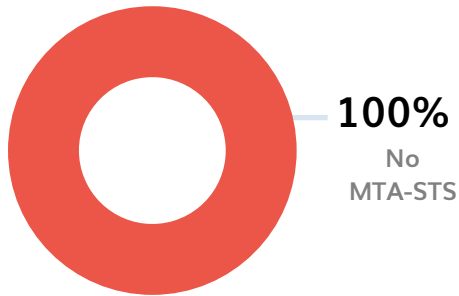
### DMARC Adoption Analysis in the Kuwait Government Sector



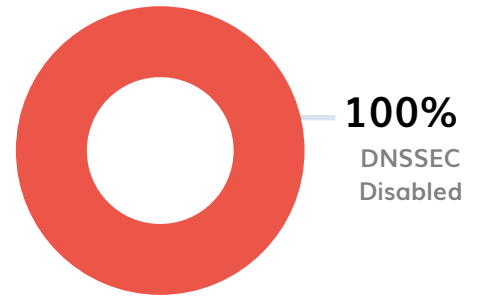
### SPF Adoption Analysis in the Kuwait Government Sector



### MTA-STS Adoption Analysis in the Kuwait Government Sector



### DNSSEC Adoption Analysis in the Kuwait Government Sector

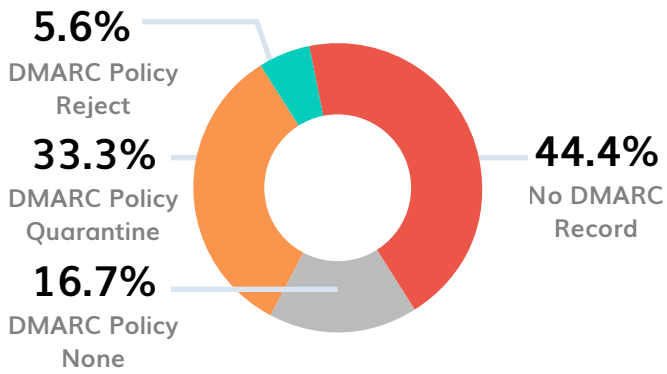


### Key Findings:

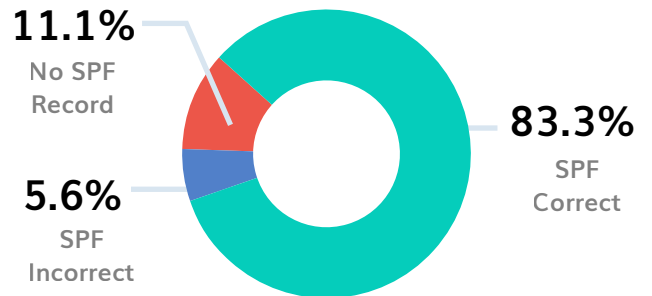
- ▶ 15.6% of domains had no SPF record
- ▶ 6.7% of the domains had their DMARC policy set at p=none
- ▶ No DMARC record was found for 57.8% of the domains
- ▶ None of the domains had MTA-STS implemented
- ▶ DNSSEC was also disabled for all of the domains in this sector

# Telecom Sector

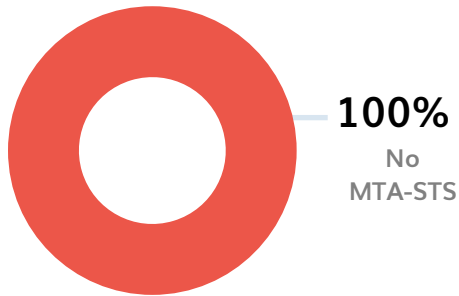
### DMARC Adoption Analysis in the Kuwait Telecom Sector



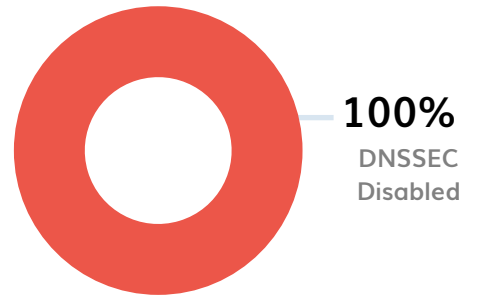
### SPF Adoption Analysis in the Kuwait Telecom Sector



### MTA-STS Adoption Analysis in the Kuwait Telecom Sector



### DNSSEC Adoption Analysis in the Kuwait Telecom Sector



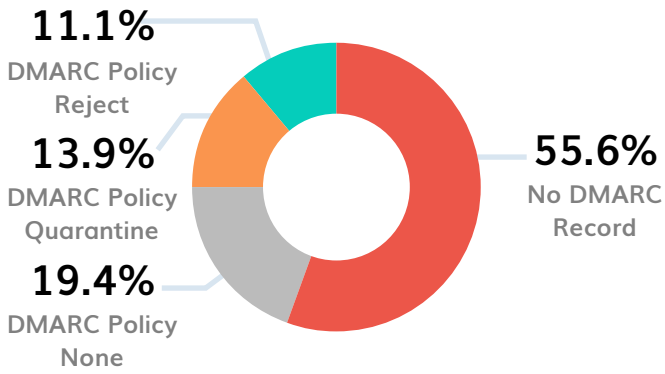
### Key Findings:

- ▶ 11.1% of domains had no SPF record
- ▶ 16.7% of the domains had their DMARC policy set at p=none
- ▶ No DMARC record was found for 44.4% of the domains
- ▶ None of the domains had MTA-STS implemented
- ▶ All of the domains had DNSSEC disabled

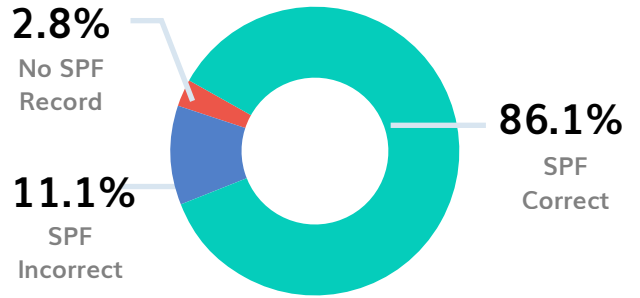


# Transport Sector

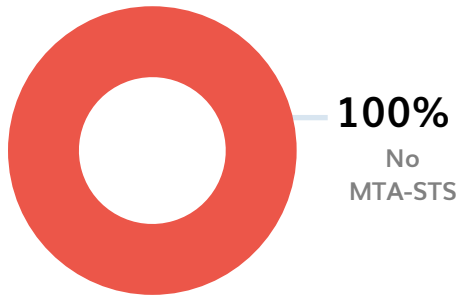
### DMARC Adoption Analysis in the Kuwait Transport Sector



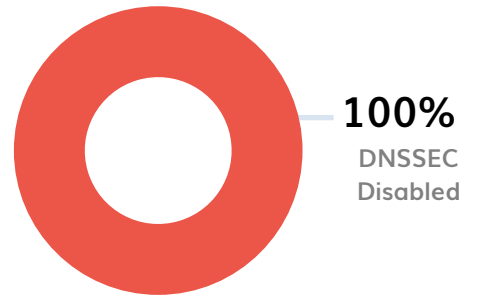
### SPF Adoption Analysis in the Kuwait Transport Sector



### MTA-STS Adoption Analysis in the Kuwait Transport Sector



### DNSSEC Adoption Analysis in the Kuwait Transport Sector

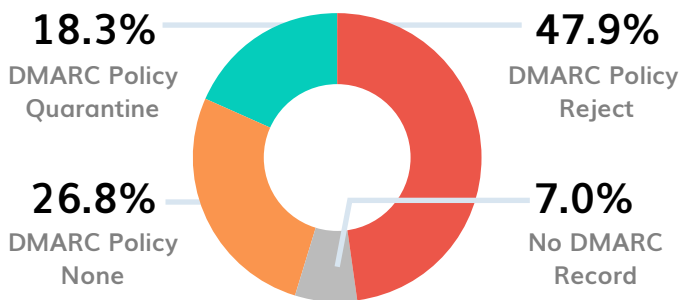


## Key Findings:

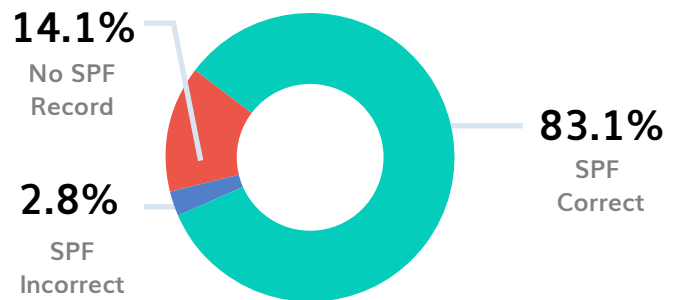
- ▶ 2.8% of domains had no SPF record
- ▶ 19.4% of the domains had their DMARC policy set at p=none
- ▶ No DMARC record was found for 55.6% of the domains
- ▶ None of the domains had MTA-STS enabled
- ▶ DNSSEC was disabled for all of the domains

## Financial Sector

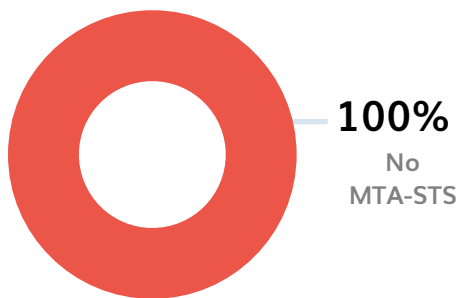
### DMARC Adoption Analysis in the Kuwait Financial Sector



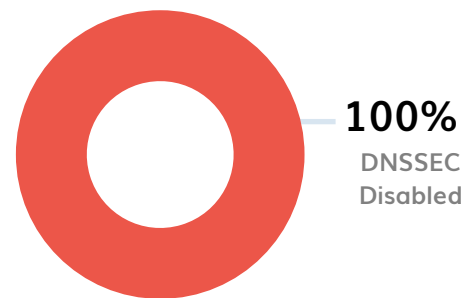
### SPF Adoption Analysis in the Kuwait Financial Sector



### MTA-STS Adoption Analysis in the Kuwait Financial Sector



### DNSSEC Adoption Analysis in the Kuwait Financial Sector

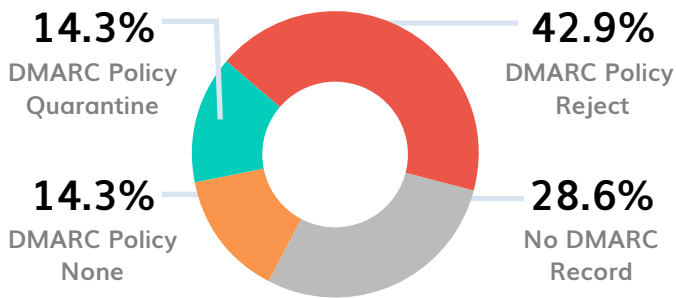


#### Key Findings:

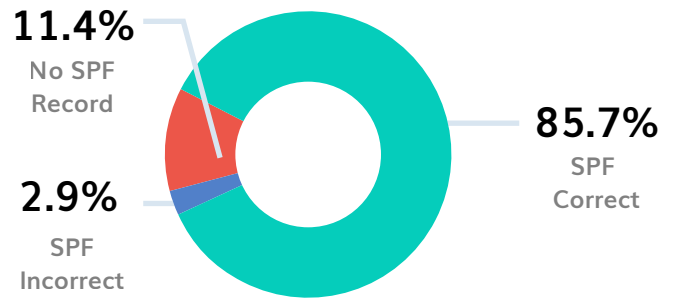
- ▶ 14.1% of domains had no SPF record
- ▶ 7% of the domains had their DMARC policy set at p=none
- ▶ No DMARC record was found for 47.9% of the domains
- ▶ None of the domains had MTA-STS enabled
- ▶ DNSSEC was disabled for all of the domains in this sector

## Education Sector

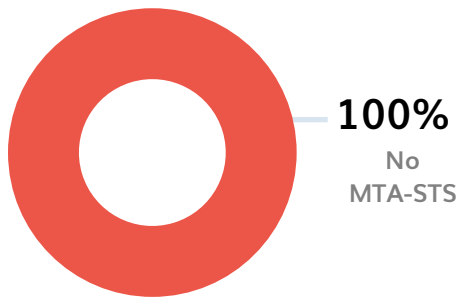
### DMARC Adoption Analysis in the Kuwait Education Sector



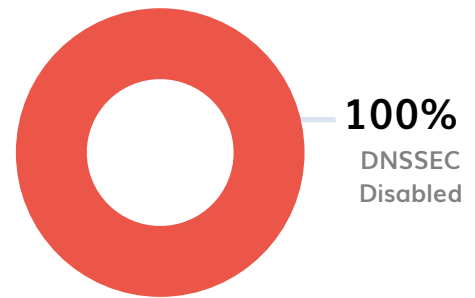
### SPF Adoption Analysis in the Kuwait Education Sector



### MTA-STS Adoption Analysis in the Kuwait Education Sector



### DNSSEC Adoption Analysis in the Kuwait Education Sector

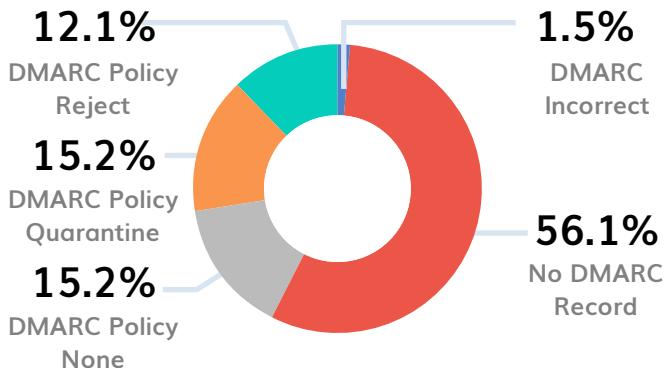


### Key Findings:

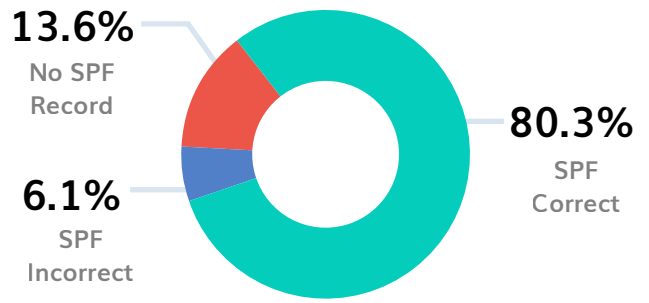
- ▶ 11.4% of domains had no SPF record
- ▶ 28.6% of the domains had their DMARC policy set at p=none
- ▶ No DMARC record was found for 42.9% of the domains
- ▶ None of the domains examined had MTA-STS implemented
- ▶ DNSSEC was also disabled for all of the domains analyzed

# Energy Sector

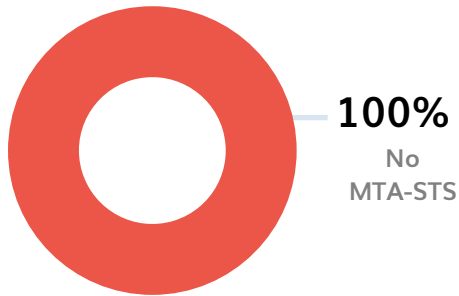
### DMARC Adoption Analysis in the Kuwait Energy Sector



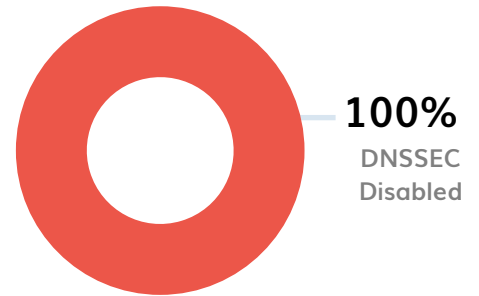
### SPF Adoption Analysis in the Kuwait Energy Sector



### MTA-STS Adoption Analysis in the Kuwait Energy Sector



### DNSSEC Adoption Analysis in the Kuwait Energy Sector

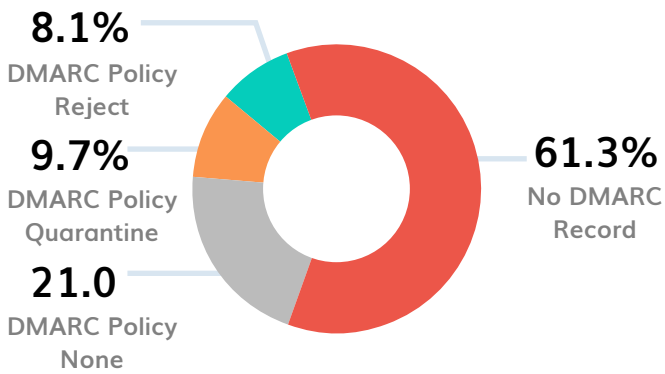


### Key Findings:

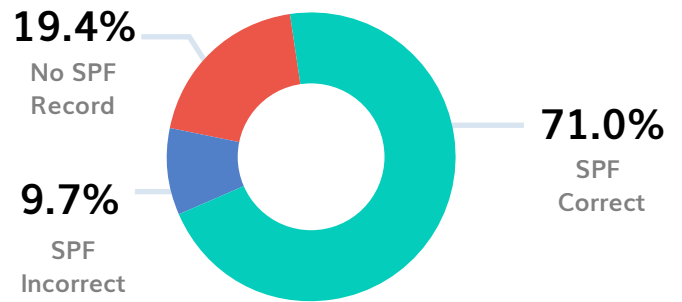
- ▶ 13.6% of domains had no SPF record
- ▶ 15.2% of the domains had their DMARC policy set at p=none
- ▶ No DMARC record was found for 56.1% of the domains
- ▶ None of the domains examined had MTA-STS implemented
- ▶ DNSSEC was also disabled for all of the domains analyzed

## Miscellaneous Businesses

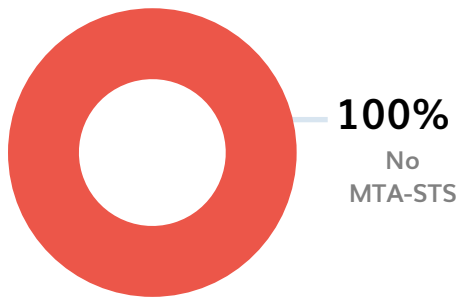
DMARC Adoption Analysis Among Kuwait Miscellaneous Businesses



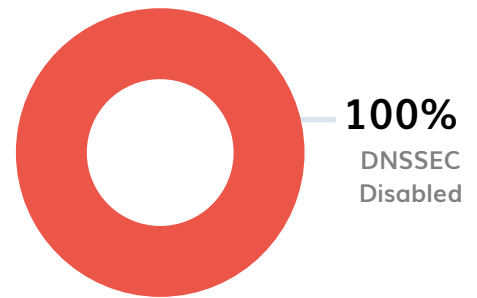
SPF Adoption Analysis Among Kuwait Miscellaneous Businesses



MTA-STS Adoption Analysis Among Kuwait Miscellaneous Businesses



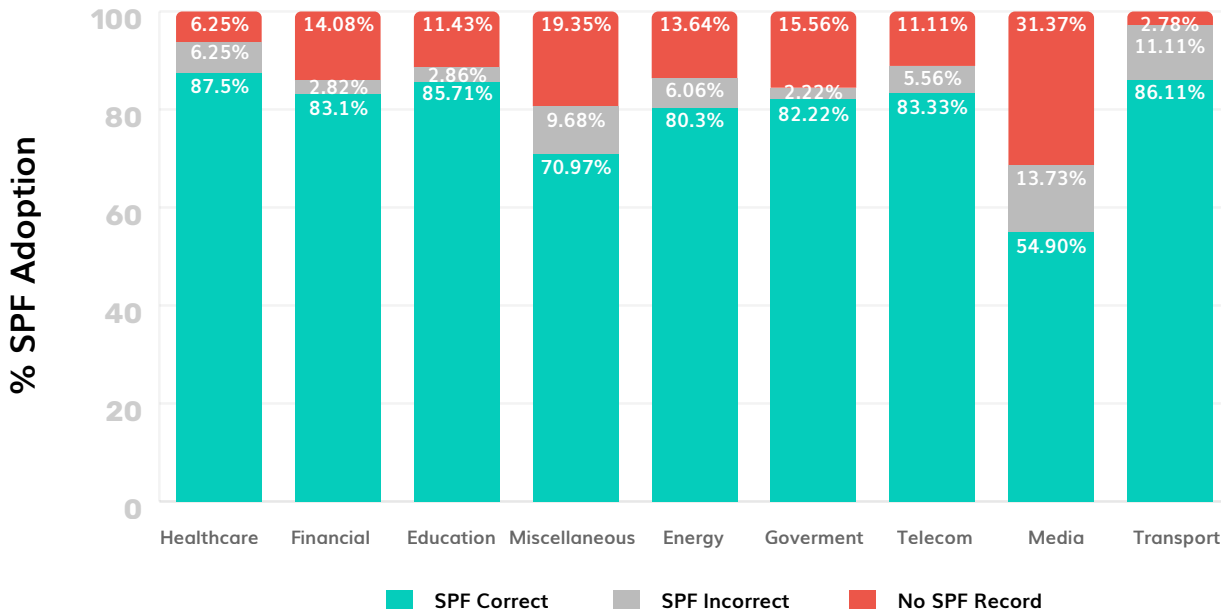
DNSSEC Adoption Analysis Among Kuwait Miscellaneous Businesses



### Key Findings:

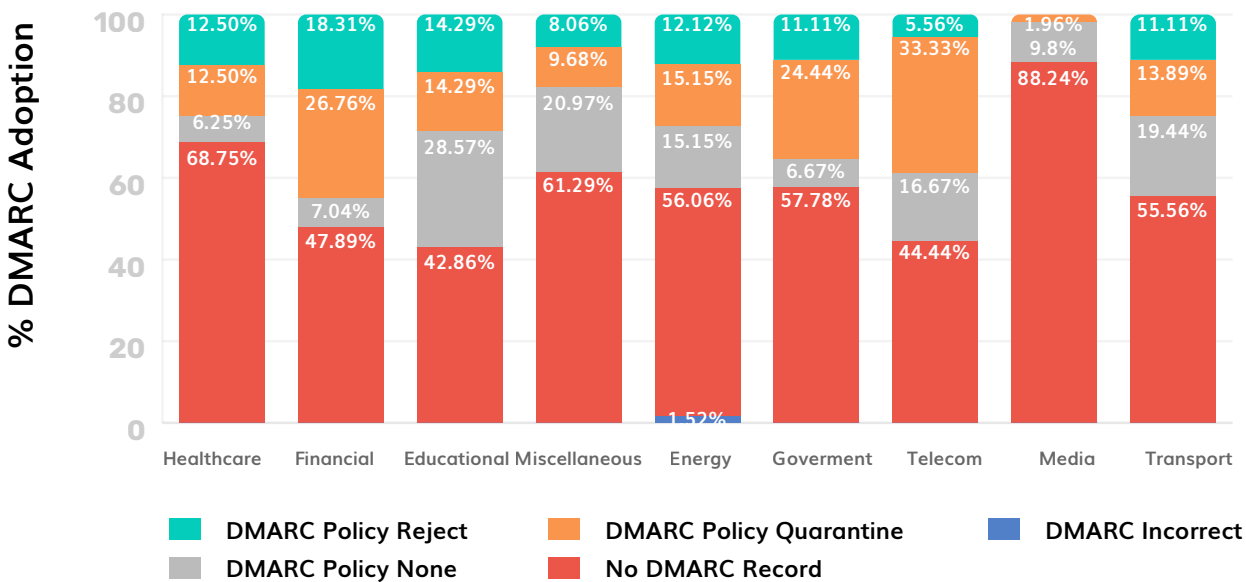
- ▶ 19.4% of domains had no SPF record
- ▶ 21% of the domains had their DMARC policy set at p=none
- ▶ No DMARC record was found for 61.3% of the domains
- ▶ All of the domains had MTA-STS disabled
- ▶ All of the domains had DNSSEC disabled

# Comparative Analysis of SPF Adoption among Different Sectors in Kuwait



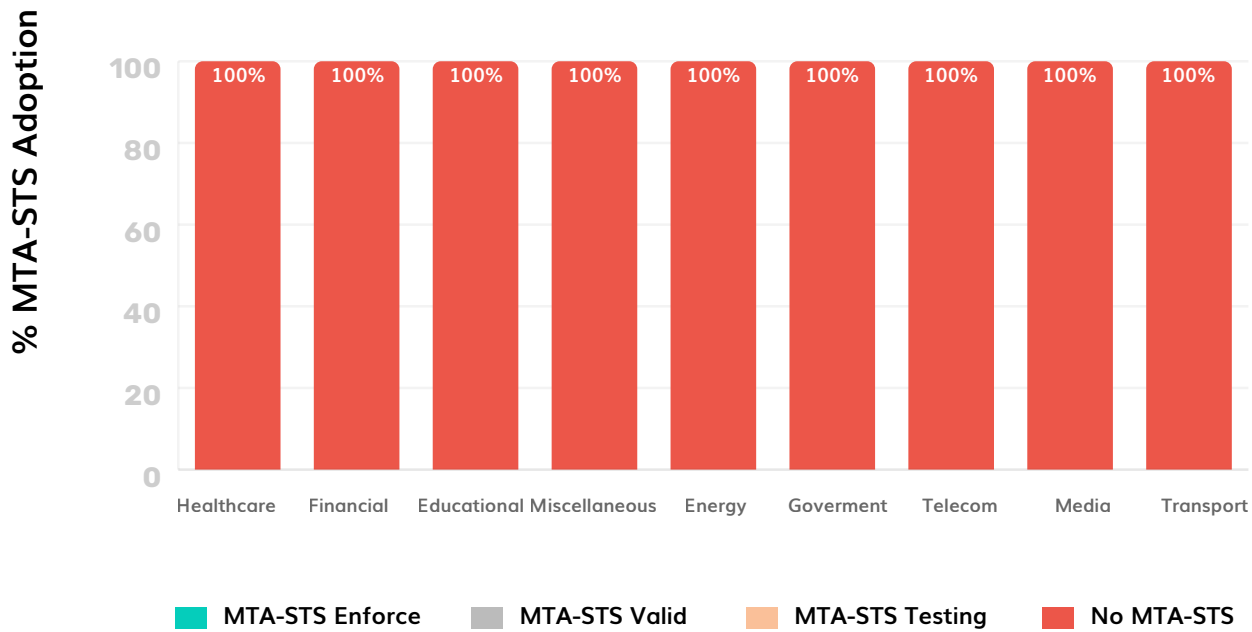
- ▶ The adoption rate for SPF was the lowest in the Kuwait Media sector. The highest rate of SPF adoption was noted in the Kuwait Healthcare, Transport, and Education sectors.

# Comparative Analysis of DMARC Adoption among Different Sectors in Kuwait



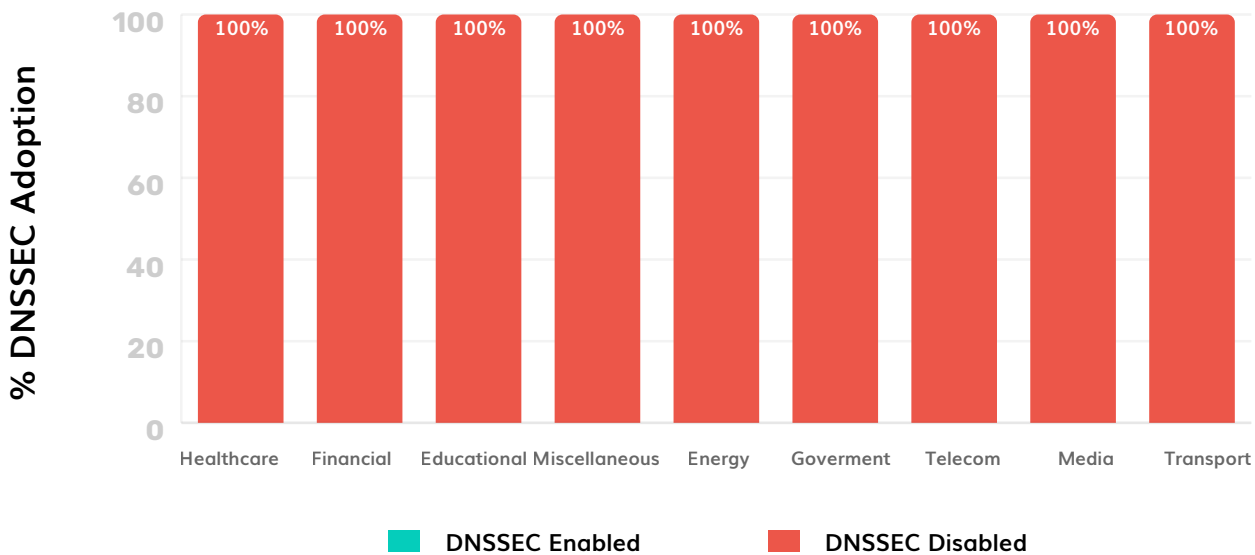
- ▶ Kuwait's Media and Healthcare sectors noted low rates of DMARC adoption. The highest rate of DMARC adoption was noted in the Kuwait Financial, Telecom, and Educational sectors. A large percentage of organizations in all industries had "none" DMARC policy implemented.

# Comparative Analysis of MTA-STS Adoption among Different Sectors in Kuwait



▶ The 400 domains analyzed in Kuwait, did not have MTA-STS implemented.

# Comparative Analysis of DNSSEC Adoption among Different Sectors in Kuwait



▶ The 400 domains analyzed in Kuwait had DNSSEC disabled for them.

# Critical Errors Organizations in Kuwait are Making

From the analysis, we uncovered several critical errors organizations in Kuwait were making when it came to implementing email authentication protocols and protecting their domain names. Let's discuss them:

## ▶ No SPF or DMARC Record Configured

SPF and DMARC records were not implemented for several organizations in Kuwait. These protocols play a crucial role in preventing email-based threats. The lack of implementation leaves the domains vulnerable to spoofing and phishing attacks. This can also lead to deliverability issues for Gmail and Yahoo senders.

## ▶ Email Authentication Configuration Errors

If email authentication protocols are configured incorrectly, they can cause more harm than good! The presence of syntax errors, redundant spaces, or using the wrong resource type can lead to issues with your email's authentication.

## ▶ Usage of DMARC None Policies

DMARC policy is the most important part of your DMARC record, defining the action to be taken by received mail servers against unauthenticated messages. Using the "none" policy is good for beginners, however, sticking to a permissive policy like none for a long time is not ideal. This leaves domains vulnerable to phishing and spoofing attacks.

## ▶ No MTA-STS or TLS-RPT Records

MTA-STS and TLS-RPT records were not set up for any of the analyzed domains. These protocols enforce TLS encryption and prevent man-the-middle attacks, thereby enhancing email security.

## ▶ DNSSEC Disabled

DNSSEC was disabled for all of the analyzed domains. DNSSEC authenticates DNS query responses, preventing DNS spoofing and cache poisoning. Without it, Kuwait domains remain vulnerable to DNS hijacking attacks.

## ▶ Too Many SPF DNS Lookups

A maximum of 10 DNS lookups is permitted without breaking SPF. Exceeding this limit causes SPF permanent errors and may even lead to deliverability issues. Several Kuwait domains had SPF records exceeding limits which reduced the effectiveness of the authentication process.

## ▶ Multiple DMARC/SPF Records

It is best practice to set up single SPF and DMARC records per domain. Multiple records can lead to validation errors, confusion, and misinterpretation on the receiver's end. Several Kuwait domains had multiple records implemented per domain, leading to ineffective authentication.



# How Can Organizations in Kuwait Improve Email Security & Deliverability?

► Given below are a few key recommendations for improving email security and deliverability among organizations and government entities in Kuwait:

- 1 Stay under RFC-specified SPF DNS, void, and length limits.
- 2 Use automated DNS record generator tools to create error-free SPF, DMARC, and MTA-STS records.
- 3 Publish only 1 SPF and DMARC record per domain.
- 4 Comply with Google and Yahoo's email sender requirements.
- 5 Gradually transition from a p=none to a p=reject DMARC policy while monitoring your reports.
- 6 Enable MTA-STS and TLS-RPT for advanced protection against MITM attacks.
- 7 Activate DNSSEC to secure DNS query responses.
- 8 Enable BIMI to send branded emails for visual verification and authentication



# How Can PowerDMARC Help?

PowerDMARC is a one-stop solution chosen by businesses of all sizes to increase their email authentication adoption and deliverability easily! Our comprehensive platform offers the following features and benefits:



## ▶ Complete Email Authentication Suite

Set up a DMARC, SPF, DKIM, MTA-STS, TLS-RPT and BIMI easily with an automated setup, onboarding training and dedicated assistance.

## ▶ Hosted Email Authentication Services

Manage and monitor your email authentication with Hosted DMARC, Hosted DKIM, SPF Macros, Hosted MTA-STS, Hosted TLS-RPT, and Hosted BIMI.

## ▶ Smart and Simple Reporting

Read DMARC data easily with simplified and human readable DMARC reports, that can be downloaded in PDF or CSV formats to share with your team.

## ▶ Dedicated 24/7 Support

Get 24/7 dedicated support in smoothly making your transition from no-action to enforced DMARC policies.

## ▶ Optimized SPF Records

One-click SPF record optimization with unlimited lookups using Macros.

## ▶ Reputation Monitoring

Monitor your domain and IP reputation across 200+ DNS blocklists.

### ▶ Real-time Alerts

Set up custom real-time attack alerts to quickly detect and prevent spoofing attacks.

### ▶ Compliance Assistance

Meet email sender requirements and compliance mandates, including those from Google, Yahoo, and upcoming PCI-DSS regulations.

### ▶ MSP Partnership Programs

Partner with PowerDMARC to secure your clients' domain names while making exceptional profits! Our DMARC MSP/MSSP-ready platform offers full-platform white labeling, dedicated video training sessions, rebranded marketing materials, and more for our MSPs.



Let's join hands to increase the rate of DMARC & MTA-STS adoption and strengthen the email security infrastructure in businesses across Kuwait and the Middle East. Contact us at [support@powerdmarc.com](mailto:support@powerdmarc.com) to find out how we can help protect your domain and business today!