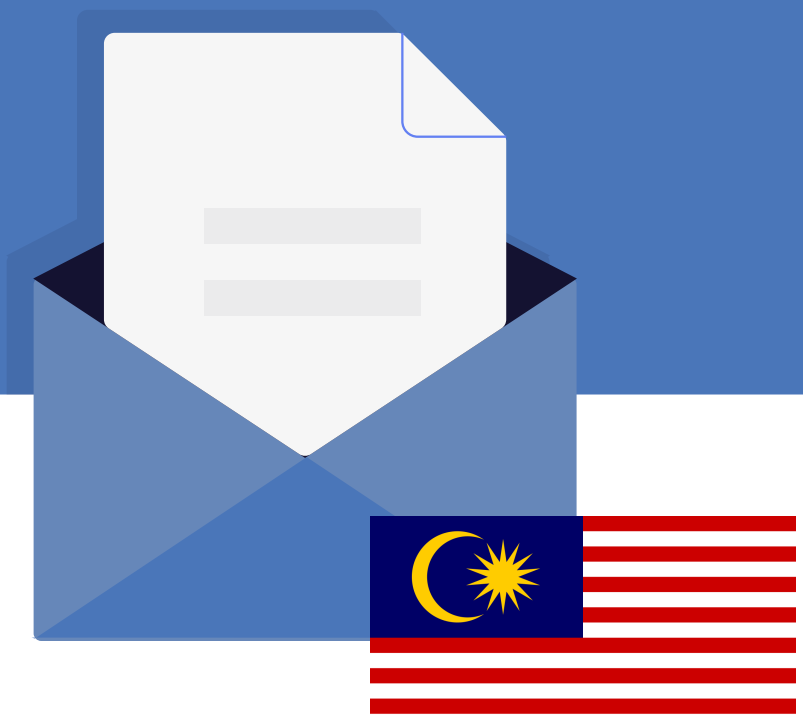
DMARC & MTA-STS Adoption in Malaysia: 2024 Report



POWERDMARC

POWERDMARC

Case study

DMARC & MTA-STS Adoption in Malaysia: 2024 Report

- 2024 can be considered the year of email security revolution! Earlier this year, Google and Yahoo successfully rolled out their updated email authentication sender requirements making authentication mandatory for all senders. But the question remains, what pushed them to take such a drastic (yet necessary) step?

  With the introduction of AI, email-based attacks including phishing, spoofing, ransomware, and BEC are now more common than ever before. According to this article by Harvard Business Review, research conducted in 2024 showed that 60% of participants fell victim to artificial intelligence (AI)-automated phishing emails. The article further explains how AI has reduced the cost associated with launching such cyber attacks by 95% while increasing their success rates.

  DMARC (Domain-based Message Authentication, Reporting and Conformance)
  DMARC is an email authentication security protocol that empowers domain owners to safeguard their domains from misuse, such as unauthorized usage, spoofing, and phishing attempts. By configuring your DMARC policy, you can reject emails that are not authorized and enable reporting to monitor email channels, identify sending sources, and review authentication outcomes.

  MTA-STS (Mail Transfer Agent Strict Transport Security)
  MTA-STS is an email authentication protocol offering protection on the receiving end this time. It is designed to enhance the security of email communications by mandating the use of Transport Layer Security (TLS) during email transmission. This protocol helps protect email traffic from being intercepted through passive eavesdropping and prevents active man-in-the-middle attacks.

Assessing the Threat Landscape

- According to Verizon's 2024 Data Breach Investigation Report, it takes users less than 60 seconds to fall victim to an email phishing scam. This means that the damage is done before you have time to even think or act! This is why relying on users to do the right thing is never an option. Organizations must work together to improve their own email defenses.

- Kaspersky's anti-phishing technologies identified close to 500,000 attempts to access phishing links on business devices in Southeast Asia in 2023. This was mostly associated with financial institutions and payment systems. The Payment Card Industry Data Security Standard (PCI-DSS) has therefore introduced their version 4 compliance mandates, making DMARC mandatory from 2025.

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

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

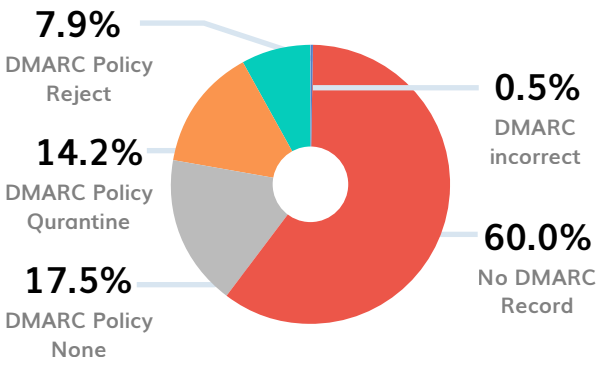
To gain better insight into the current scenario we analyzed 974 domains belonging to top businesses and organizations in Malaysia, from the following sectors:

- Healthcare
- Media
- Government
- Telecommunication
- Job Board
- Transport
- Miscellaneous Businesses
- Banking
- Education

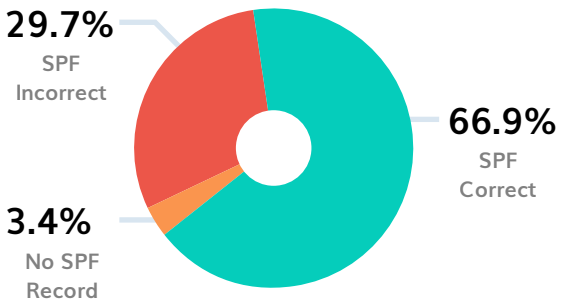
What Do the Numbers Say?

An in-depth SPF, DMARC, MTA-STS, and DNSSEC adoption analysis was conducted while examining all 974 Malaysian domains, which led to the following revelations:

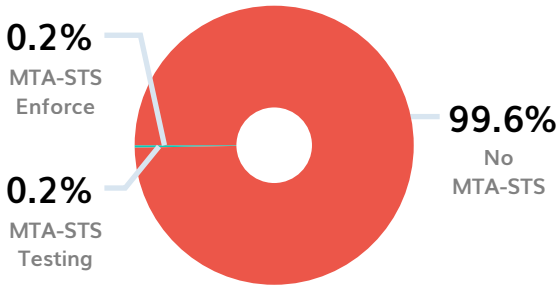
DMARC Adoption Analysis in Malaysia



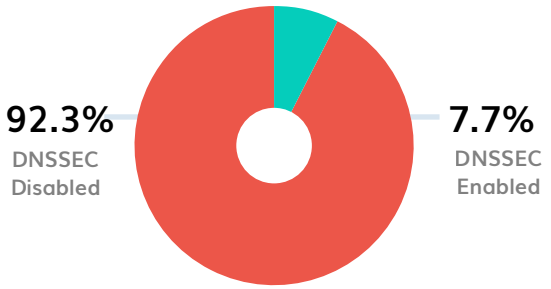
SPF Adoption Analysis in Malaysia



MTA-STS Adoption Analysis in Malaysia



DNSSEC Adoption Analysis in Malaysia

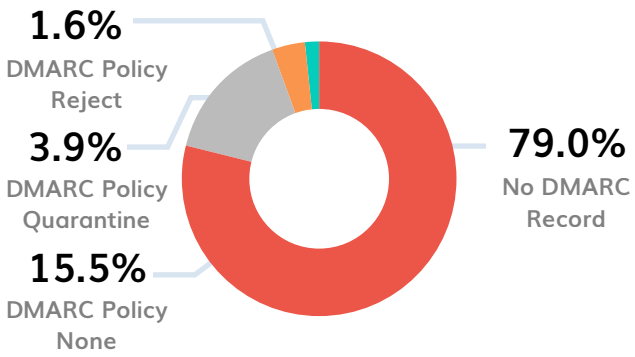


- **Graphical Analysis:** Among all 974 domains examined that belong to various organizations in Malaysia, 652 domains (66.9%) possessed correct SPF records, while 289 domains (29.7%) unfortunately had no SPF records at all. 385 domains (39.5%) had correct DMARC records, while 5 of the domains (0.5%) had DMARC records that contained errors. A vast majority of domains (584 domains making up 60%) had no DMARC record found. 170 domains had their DMARC policy set at none (17.5%), enabling monitoring only, while 138 domains (14.2%) had their DMARC policy set at quarantine, and 77 domains (7.9%) had their DMARC policy set at maximum enforcement (i.e. p=reject).

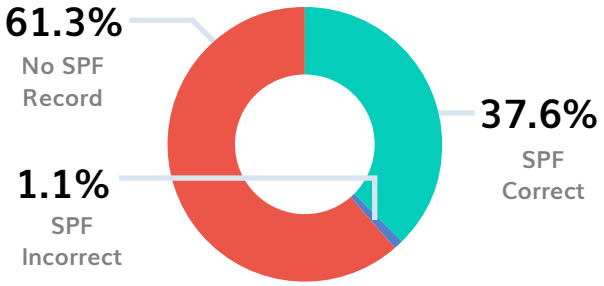
Sector-wise Analysis of Domains in Malaysia

Healthcare Sector

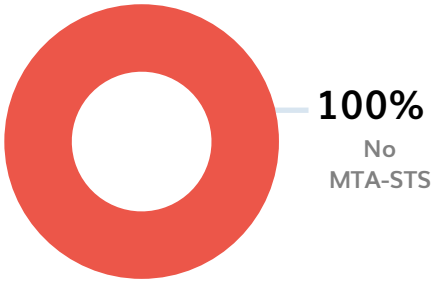
DMARC Adoption Analysis in the Malaysian Healthcare Sector



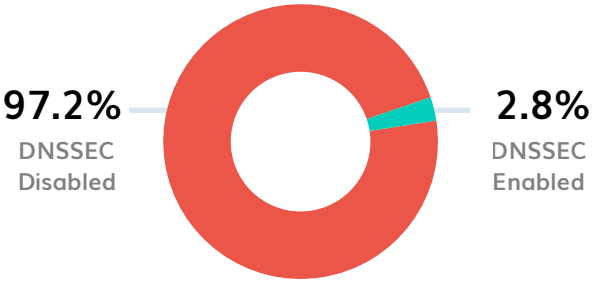
SPF Adoption Analysis in the Malaysian Healthcare Sector



MTA-STS Adoption Analysis in the Malaysian Healthcare Sector



DNSSEC Adoption Analysis in the Malaysian Healthcare Sector

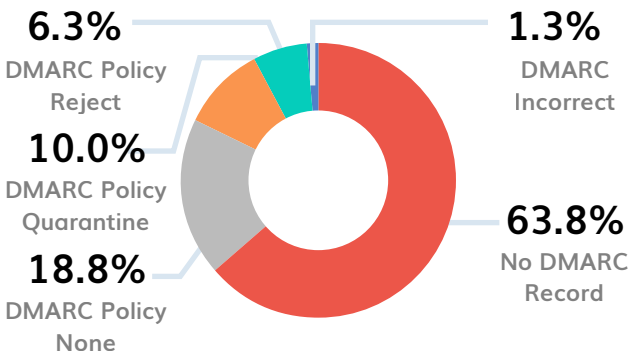


Key Findings:

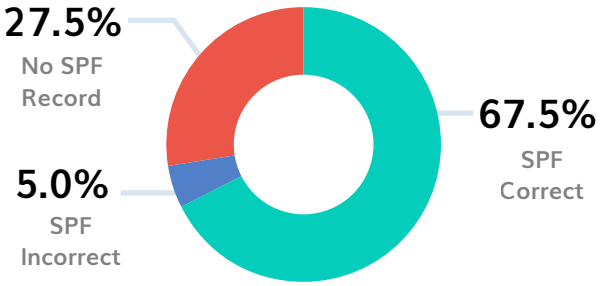
- 61.3% of domains had no SPF record
- 15.5% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 79% of the domains
- None of the domains in the Malaysian Healthcare sector had MTA-STS implemented
- DNSSEC was disabled for 97.2% of the domains

Media Sector

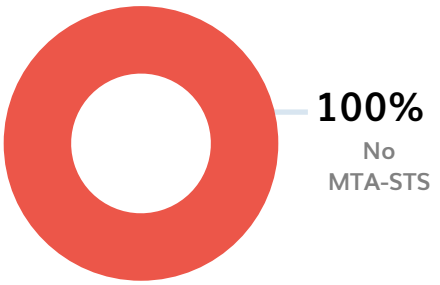
DMARC Adoption Analysis in the Malaysian Media Sector



SPF Adoption Analysis in the Malaysian Media Sector



MTA-STS Adoption Analysis in the Malaysian Media Sector



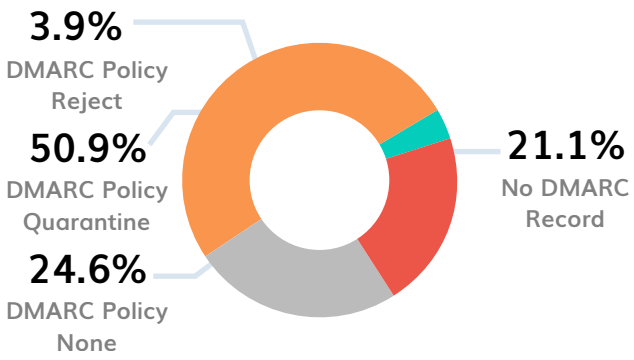
DNSSEC Adoption Analysis in the Malaysian Media Sector

Key Findings:

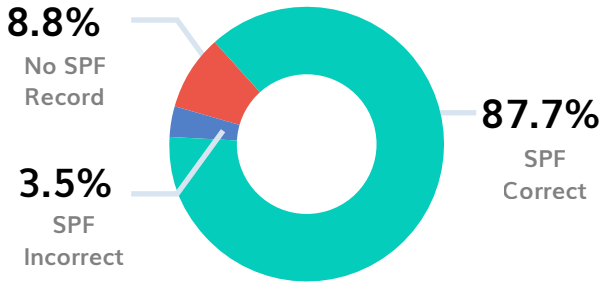
- 27.5% of domains had no SPF record
- 18.8% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 63.8% of the domains
- MTA-STS wasn't enabled for any of the examined domains
- DNSSEC was disabled for 95% of the domains

Government Sector

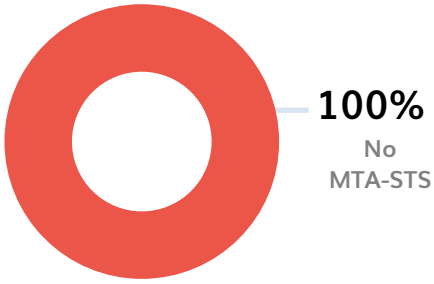
DMARC Adoption Analysis in the Malaysian Government Sector



SPF Adoption Analysis in the Malaysian Government Sector



MTA-STS Adoption Analysis in the Malaysian Government Sector



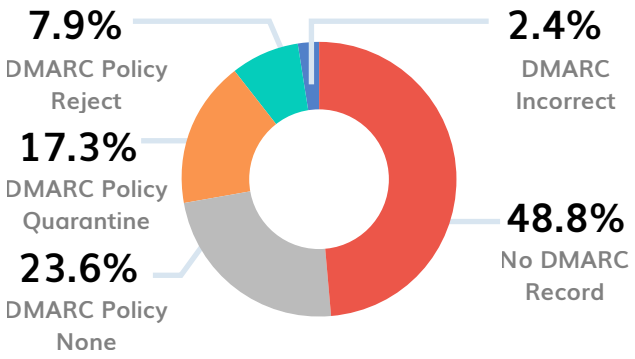
DNSSEC Adoption Analysis in the Malaysian Government Sector

Key Findings:

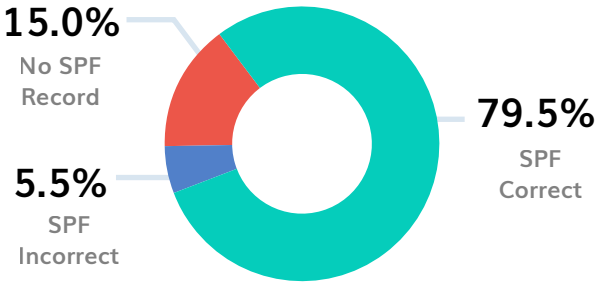
- 8.8% of domains had no SPF record
- 24.6% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 21.1% of the domains
- None of the domains had MTA-STS implemented
- DNSSEC was also disabled for 57.9% of the domains in this sector

Telecom Sector

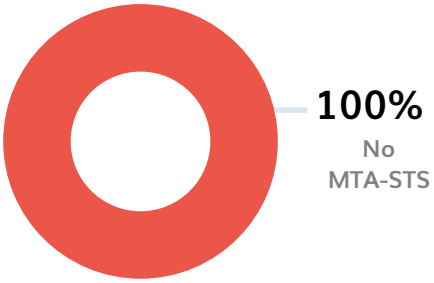
DMARC Adoption Analysis in the Malaysian Telecom Sector



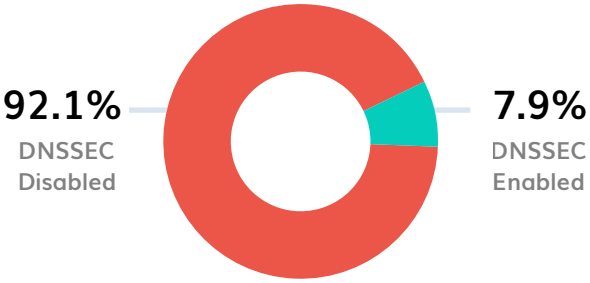
SPF Adoption Analysis in the Malaysian Telecom Sector



MTA-STS Adoption Analysis in the Malaysian Telecom Sector



DNSSEC Adoption Analysis in the Malaysian Telecom Sector

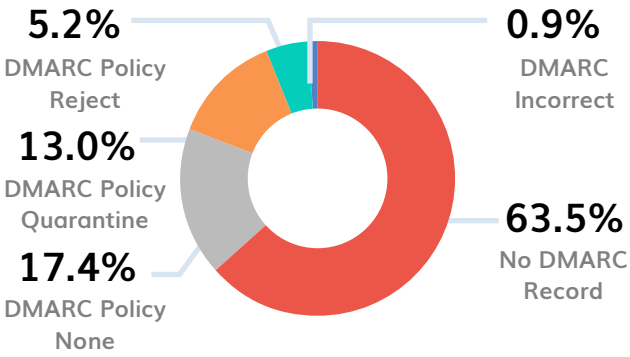


Key Findings:

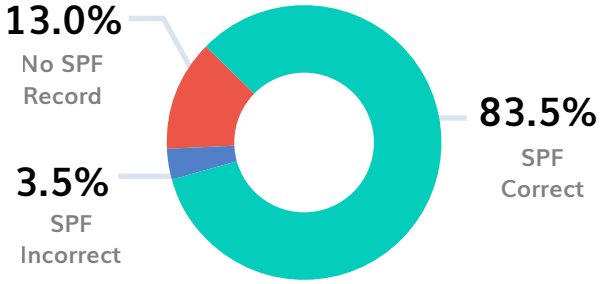
- 15% of domains had no SPF record
- 23.6% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 48.8% of the domains
- None of the domains had MTA-STS implemented
- 92.1% of the domains had DNSSEC disabled

Job Boards

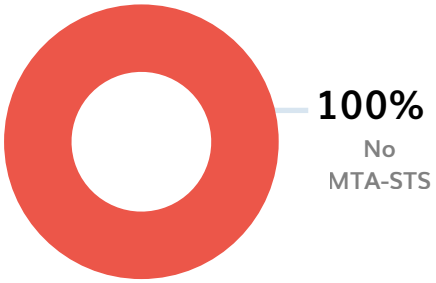
DMARC Adoption Analysis in the Malaysian Job Boards Sector



SPF Adoption Analysis in the Malaysian Job Boards Sector



MTA-STS Adoption Analysis in the Malaysian Job Boards Sector



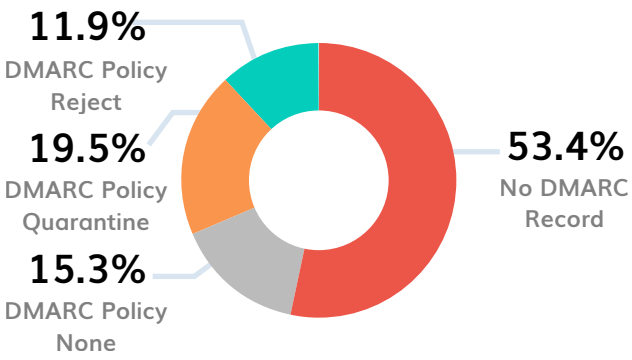
DNSSEC Adoption Analysis in the Malaysian Job Boards Sector

Key Findings:

- 13% of the domains analyzed have no SPF record
- 17.4% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 63.5% of the domains
- MTA-STS was not enabled for any of the domains in this sector
- DNSSEC was disabled for 94.8% of the domains

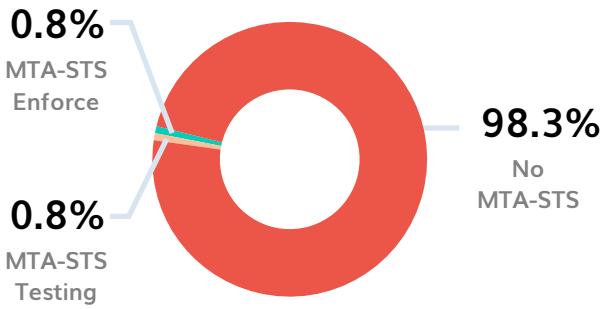
Transport Sector

DMARC Adoption Analysis in the Malaysian Transport Sector



SPF Adoption Analysis in the Malaysian Transport Sector

MTA-STS Adoption Analysis in the Malaysian Transport Sector



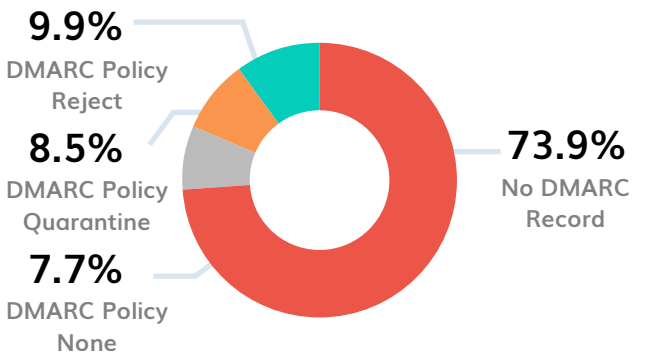
DNSSEC Adoption Analysis in the Malaysian Transport Sector

Key Findings:

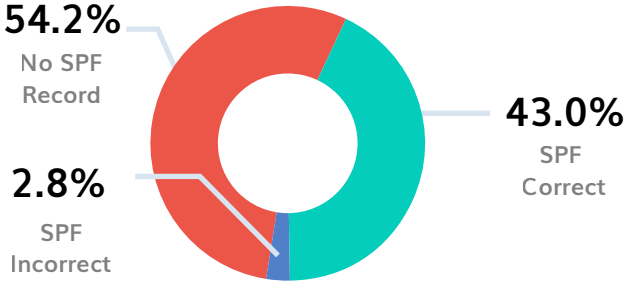
- 18.6% of domains had no SPF record
- 15.3% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 53.4% of the domains
- 98.3% of the domains did not have MTA-STS enabled
- DNSSEC was disabled for 95.8% of the domains

Miscellaneous Businesses

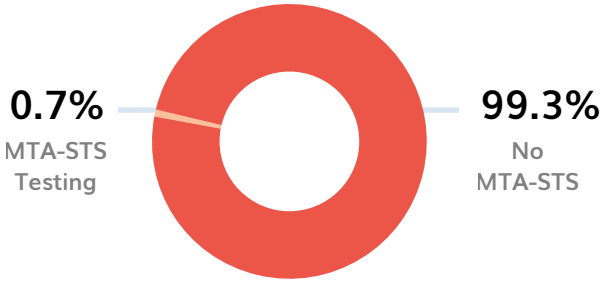
DMARC Adoption Analysis in Malaysian Miscellaneous Businesses Sector



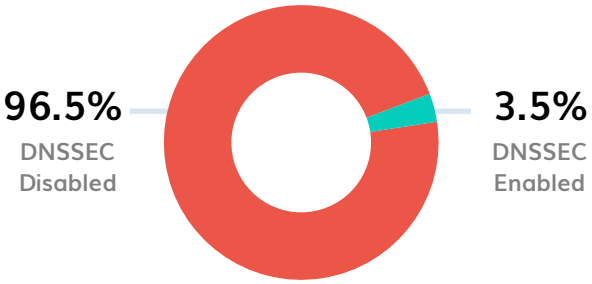
SPF Adoption Analysis in Malaysian Miscellaneous Businesses Sector



MTA-STS Adoption Analysis in Malaysian Miscellaneous Businesses Sector



DNSSEC Adoption Analysis in Malaysian Miscellaneous Businesses Sector

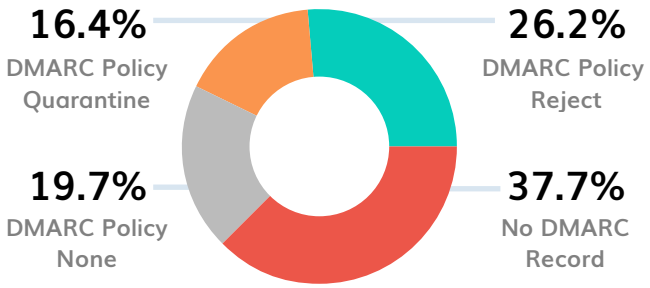


Key Findings:

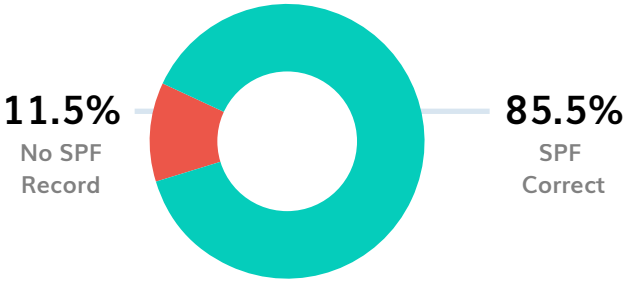
- 54.2% of domains had no SPF record
- 7.7% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 73.9% of the domains
- 99.3% of the domains had MTA-STS disabled
- 96.5% of the domains had DNSSEC disabled

Banking Sector

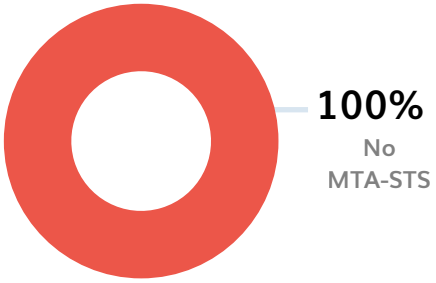
DMARC Adoption Analysis in the Malaysian Banking Sector



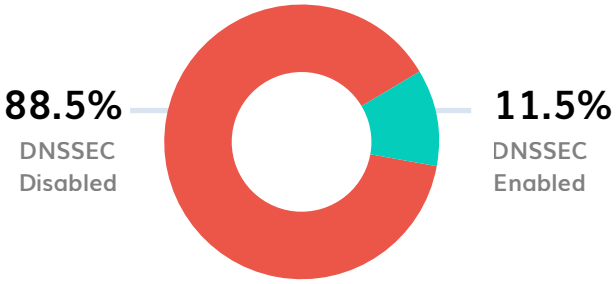
SPF Adoption Analysis in the Malaysian Banking Sector



MTA-STS Adoption Analysis in the Malaysian Banking Sector



DNSSEC Adoption Analysis in the Malaysian Banking Sector

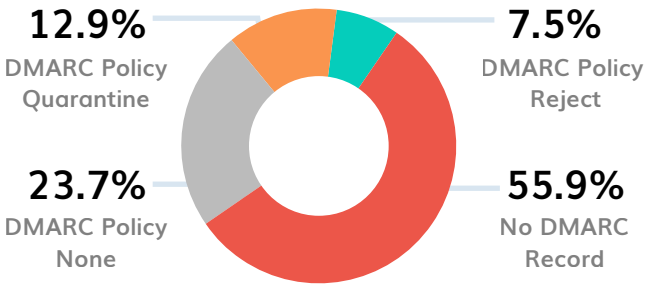


Key Findings:

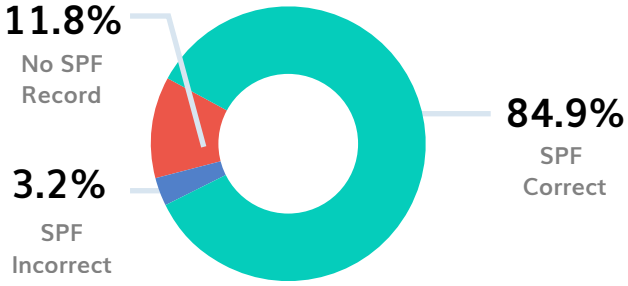
- 11.5% of domains had no SPF record
- 19.7% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 37.7% of the domains
- None of the domains had MTA-STS enabled
- DNSSEC was disabled for 88.5% of the domains in this sector

Education Sector

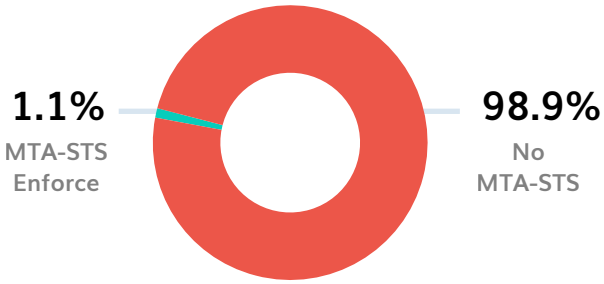
DMARC Adoption Analysis in the Malaysian Education Sector



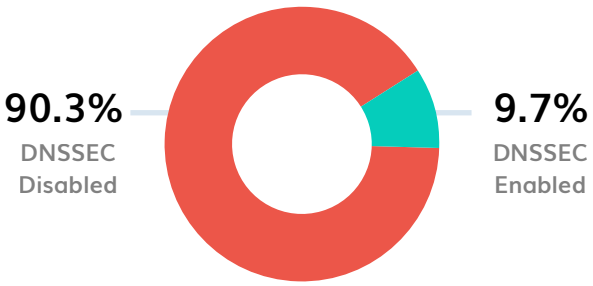
SPF Adoption Analysis in the Malaysian Education Sector



MTA-STS Adoption Analysis in the Malaysian Education Sector



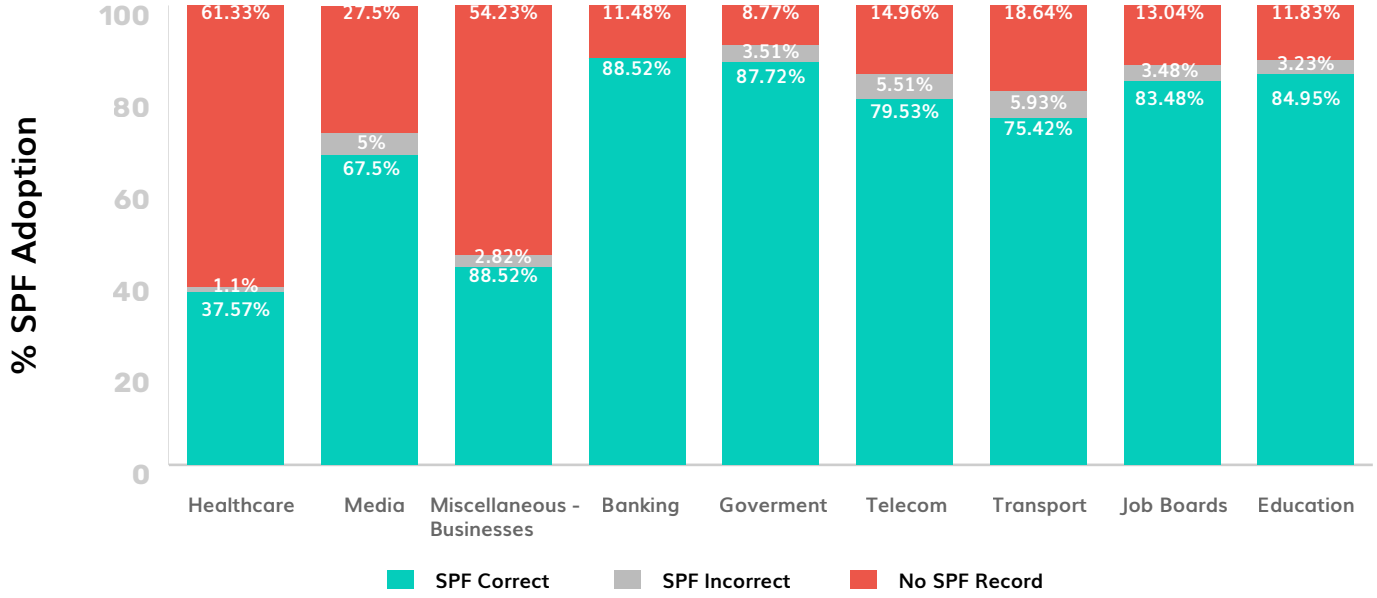
DNSSEC Adoption Analysis in the Malaysian Education Sector



Key Findings:

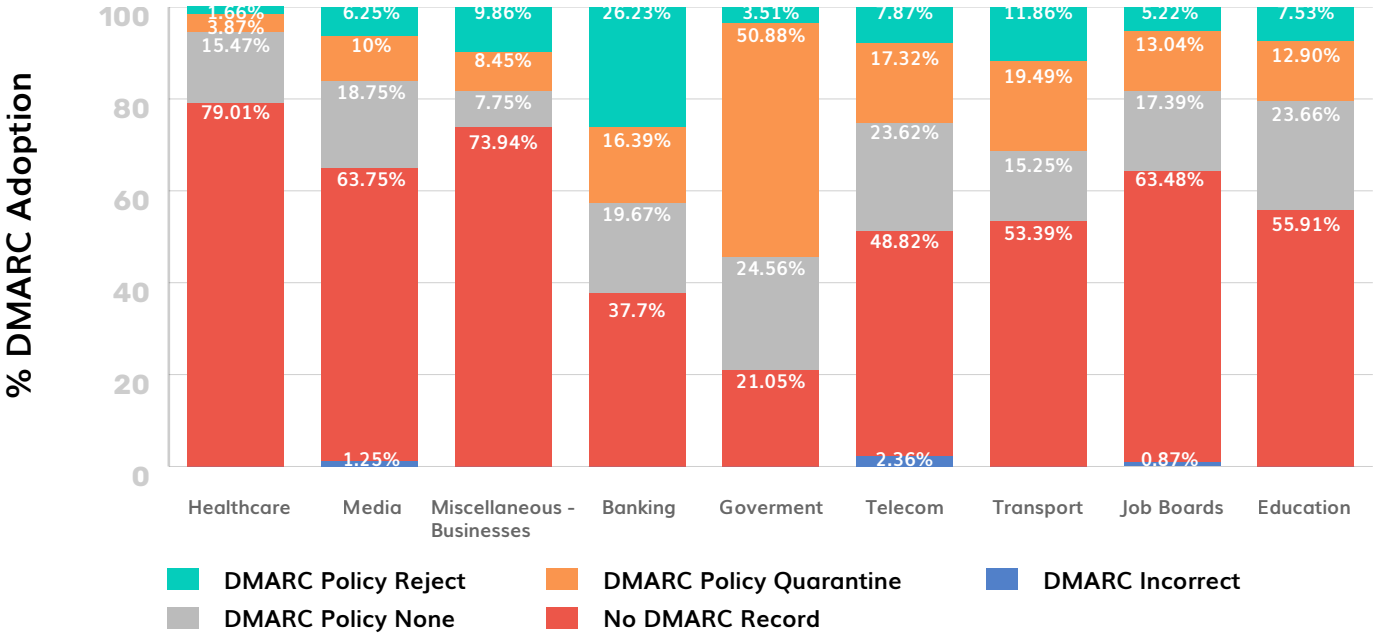
- 11.8% of domains had no SPF record
- 23.7% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 55.9% of the domains
- 98.9% of the domains examined had MTA-STS implemented
- DNSSEC was also disabled for 90.3% of the domains analyzed

Comparative Analysis of SPF Adoption among Different Sectors in Malaysia



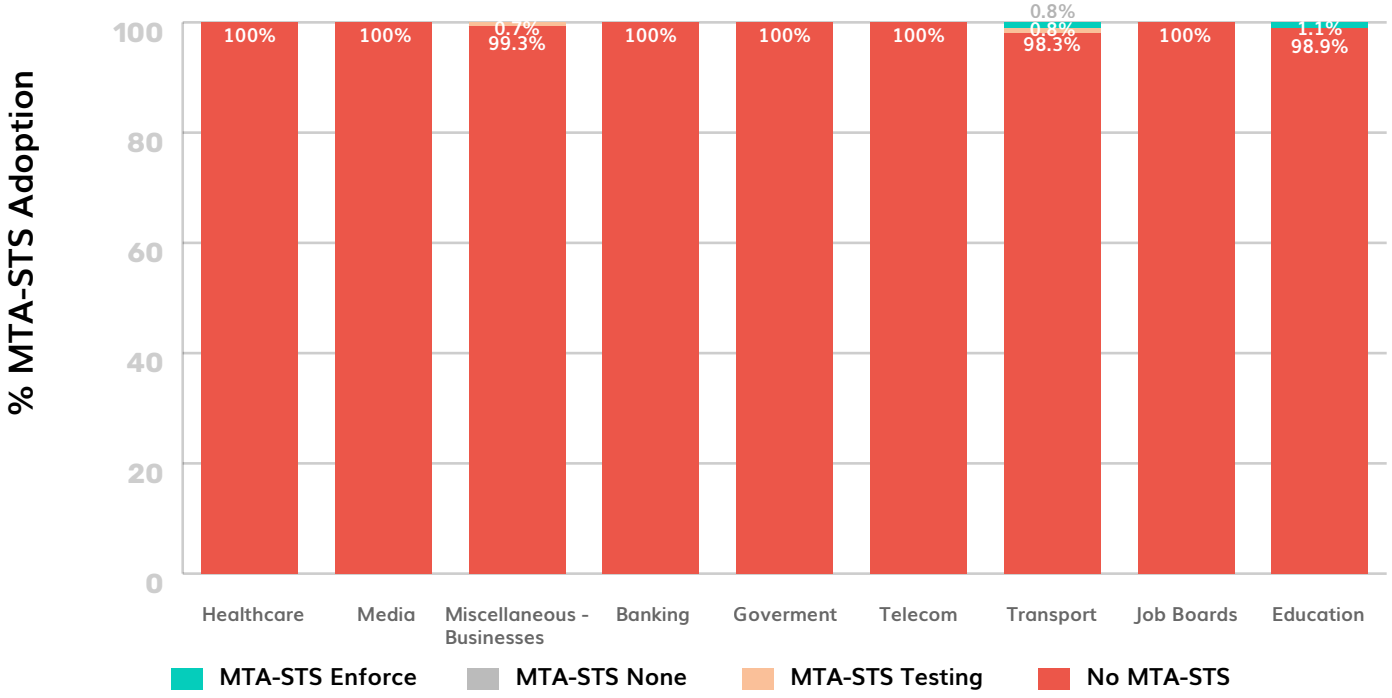
- The SPF adoption rate was found to be the lowest in the Malaysian Healthcare sector. The highest rate of SPF adoption was noted in the Malaysian Government, Banking, Job Board, and Education sectors.

Comparative Analysis of DMARC Adoption among Different Sectors in Malaysia



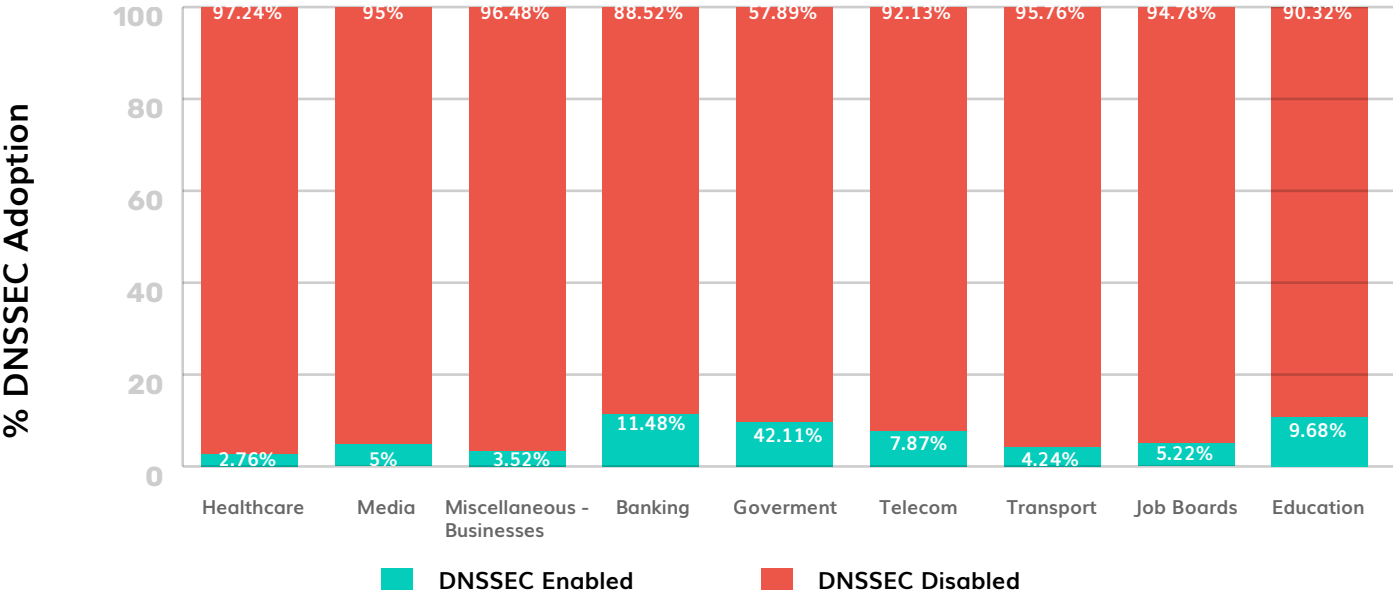
- Malaysia's Healthcare, Miscellaneous Businesses, Media, and Job Boards sectors noted low rates of DMARC adoption. The highest rate of DMARC adoption was noted in the Malaysian Government and Banking sectors. A large percentage of organizations in all sectors had "none" DMARC policy implemented.

Comparative Analysis of MTA-STS Adoption among Different Sectors in Malaysia



- 99.6%.of the domains in Malaysia among the 974 domains analyzed, did not have MTA-STS implemented.

Comparative Analysis of DNSSEC Adoption among Different Sectors in Malaysia



- 92.3% of the domains in Malaysia among the 974 domains analyzed, had DNSSEC disabled for them.

Critical Errors Organizations in Malaysia are Making

Through an analysis of 974 domains spanning various sectors and industries in Malaysia, we uncovered numerous critical mistakes made by Malaysian organizations and government entities, exposing them to potential security breaches.

Absence of SPF and DMARC Records

Many Malaysian organizations failed to implement SPF and DMARC records, which are essential for email authentication. Without these protocols, their domains are more susceptible to spam, phishing, and spoofing attacks.

Additionally, Google and Yahoo have updated their sender requirements, requiring all senders to implement SPF and bulk senders to enable DMARC. Domains that fail to comply with these standards risk being blocked from sending emails to Google and Yahoo inboxes.

Improper Configuration of Email Authentication

There are frequent errors in the setup and configuration of email authentication mechanisms. These mistakes can undermine the effectiveness of SPF, DMARC, and MTA-STS leaving the organization vulnerable to email-based threats.

Use of No-action DMARC Policies

Several organizations adopted DMARC policies that are too permissive (p=none) or do not take any action on unauthorized emails. This approach fails to protect the domain adequately, as it does not prevent potentially harmful emails from being delivered.

Lack of MTA-STS and TLS-RPT Records

Missing MTA-STS and TLS-RPT records is another common issue. These protocols enhance email security by enforcing TLS encryption and providing reports on email delivery issues, respectively. Without them, email communications can be less secure.

Disabled DNSSEC for Domains

Many domains do not have DNSSEC (Domain Name System Security Extensions) enabled. DNSSEC adds a layer of security to the DNS lookup process, protecting against certain types of attacks. Without it, domains are more vulnerable to DNS spoofing and cache poisoning.

SPF Records Exceeding Maximum Lookup Limit

SPF records are often configured to include too many DNS lookups, surpassing the maximum limit of 10. This can cause SPF checks to fail, reducing the effectiveness of email authentication and potentially leading to legitimate emails being rejected.

Multiple DMARC/SPF Records for a Single Domain

Some organizations mistakenly create multiple DMARC or SPF records for the same domain, leading to conflicts and misconfigurations. This can cause email authentication to malfunction, increasing the risk of unnecessary authentication failures.

How Can Organizations in Malaysia Improve Email Security?

- To enhance their domain security and authentication posture, organizations and governments in Malaysia can consider the following measures:

1. Stay within the SPF character length and lookup limits.
2. Implement accurate SPF, DMARC, and MTA-STS records without errors.
3. Publish a single SPF and DMARC record per domain.
4. Activate DMARC RUA and RUF reports to monitor domains and sending sources.
5. Gradually transition from a p=none to a p=reject DMARC policy for better protection against email-based attacks.
6. Enable MTA-STS and TLS-RPT to ensure SMTP communications are TLS-encrypted.
7. Activate DNSSEC for an added layer of authentication and security for your DNS.
8. Enable BIMI to attach your brand logo to authenticated emails, thereby increasing customer trust.

How Can We Help You in this Process

Ensuring the security of your emails is paramount for organizations of all sizes. We understand the importance of safeguarding your communications from cyber threats. That's why we offer a comprehensive suite of email and domain security solutions tailored to meet your organization's needs.

Complete Email Authentication Suite

Our team offers expert guidance on setting up and managing key email authentication protocols like DMARC, DKIM, and SPF. We ensure your records are error-free and optimized for maximum security.

Hosted Email Authentication Services

We offer various hosted email authentication services, including Hosted DMARC, Hosted DKIM, SPF Macros, Hosted MTA-STS, Hosted TLS-RPT, and Hosted BIMI. Our cloud-based SaaS platform simplifies configuration and updates, eliminating the need for multiple DNS accesses.

Smart and Simple Reporting

Our smart, user-friendly reporting keeps you updated on your email authentication status. With daily aggregate and forensic DMARC reports, monitoring your email activity is easy and effective. You can download reports in PDF or CSV formats to share with your team.

Dedicated 24/7 Support

Our team of experts provides top-notch support to help you transition smoothly to DMARC enforcement and improve compliance. We ensure you get the most out of your protocols.

Optimized SPF Records

Optimize your SPF records easily using SPF Macros on our platform. We help you stay within DNS lookup and SPF length limits, ensuring your SPF protocol works effectively.

Reputation Monitoring

Monitor your domain's reputation and address issues early with our reputation monitoring services. We track your domains and IPs across 200+ DNS blocklists to help prevent email rejections and flagging.

Real-time Alerts

Set up customized alerts to stay informed about email security issues. Receive notifications via email, Slack, Discord, or Webhooks to take timely action and mitigate risks.

Compliance Assistance

Meet the latest email sender requirements and compliance mandates, including those from Google, Yahoo, and upcoming PCI-DSS regulations. Our compliance program helps you get started quickly and easily.

MSP Partnership Programs

Partner with PowerDMARC for managed security services tailored to your organization's needs. Our DMARC MSP/MSSP-ready platform and dedicated service desk offer comprehensive support for your email security. We also provide 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 Malaysia and Southeast Asia. Get in touch with us at support@powerdmarc.com to find out how we can help protect your domain and business today!