

Philippines DMARC & MTA-STS Adoption Report 2024



POWER DMARC

Philippines DMARC & MTA-STS Adoption Report 2024



The Philippines recently found itself to be the central focus of cyber attacks. The country experienced the highest number of cyber attacks in Southeast Asia in 2023, with an alarming 75% of businesses in the Philippines falling victim. This number is higher than the Asia-Pacific regional average of 59%.

In fact, 29% of organizations across different sectors have reported a substantial increase in the number of security-related attacks, making it a matter of urgent importance.

This is why the Philippine government decided to implement the National Cyber Security Plan (NCSP) 2023-2028 to protect both state and non-state sectors from the increasing number and intensity of cyberattacks.

Based on the analysis of 1650 domains, this PowerDMARC report discusses key challenges in the Philippines' cybersecurity landscape and provides useful recommendations on how to best overcome these challenges.

Assessing the Threat Landscape

Our Philippines DMARC and Email Authentication Adoption Report (2024) will address the following questions:

- ▶ What's the current situation around SPF and DMARC adoption in the Philippines?
- ▶ To what extent does the country face DNSSEC adoption challenges?
- ▶ What makes the Philippines so vulnerable to cyberattacks?
- ▶ What measures should be implemented to ensure enhanced email security in the Philippines?
- ▶ Is MTA-STS commonly adopted?
- ▶ Are some sectors more vulnerable to cyber attacks than others in the Philippines?

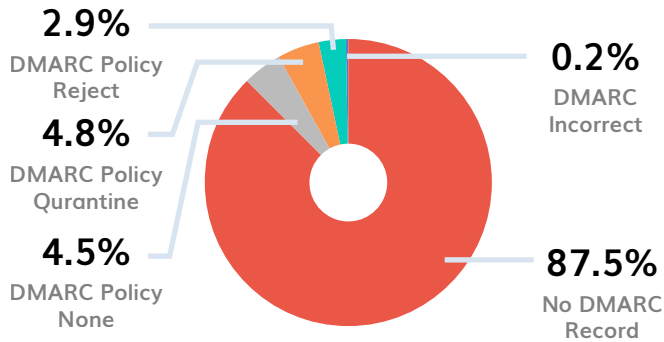
Sectors Analyzed

Total domains analyzed: 1650

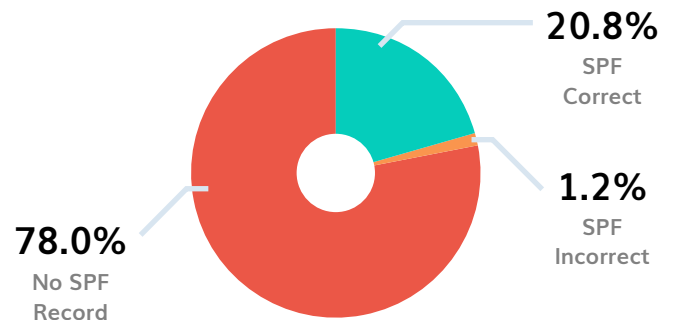
- ▶ Healthcare
- ▶ Media
- ▶ Banking
- ▶ Telecommunications
- ▶ Government
- ▶ Transport
- ▶ Education
- ▶ Miscellaneous-Business

What Do the Numbers Say?

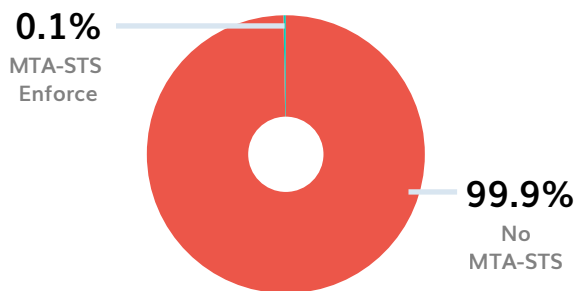
DMARC Distribution in Philippines



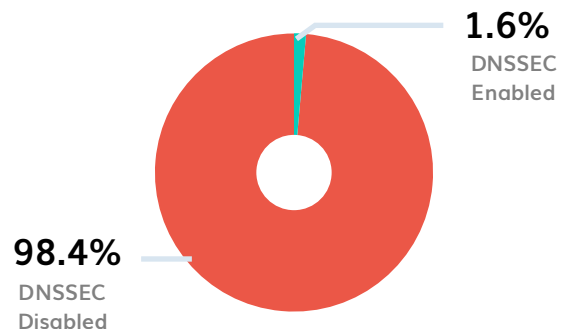
SPF Distribution in Philippines



MTA-STS Distribution in Philippines



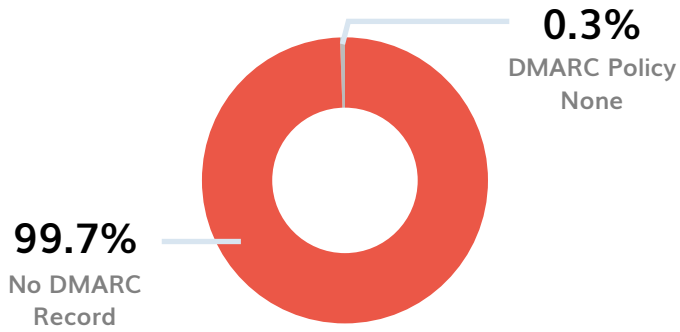
DNSSEC Distribution in Philippines



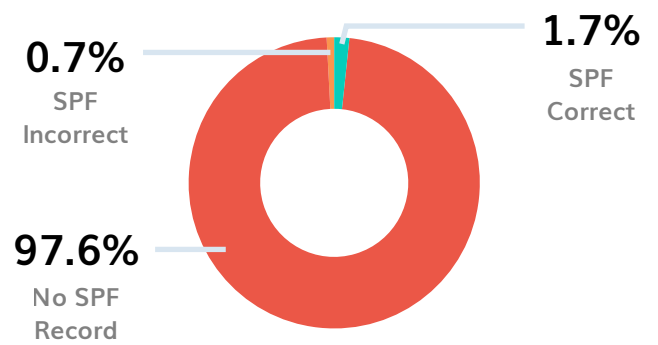
Sector-wise Analysis of Domains in Philippines

Healthcare Sector

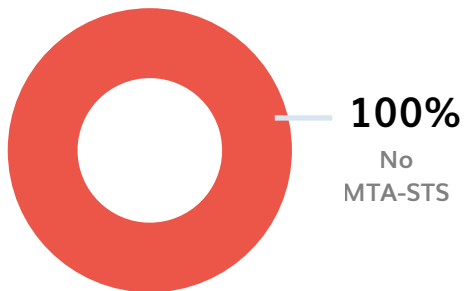
DMARC Adoption



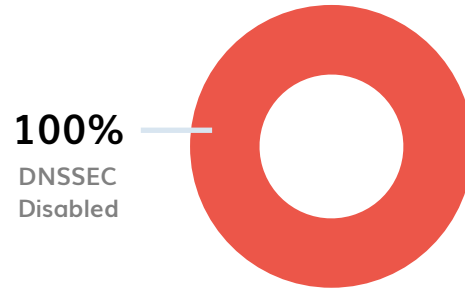
SPF Adoption



MTA-STS Adoption

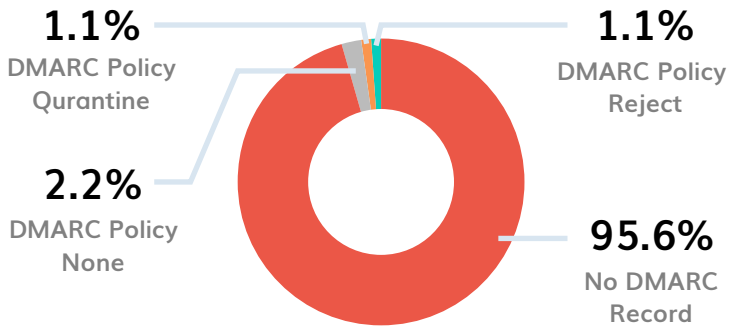


DNSSEC Adoption

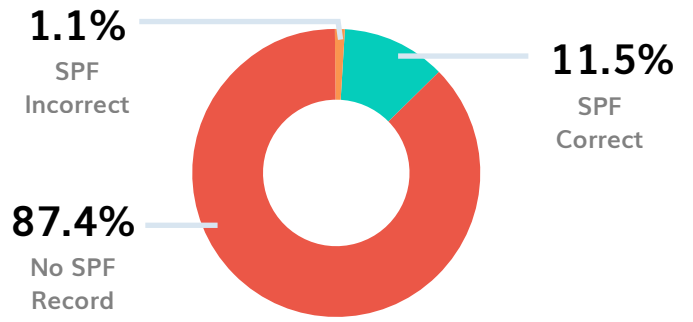


Media Sector

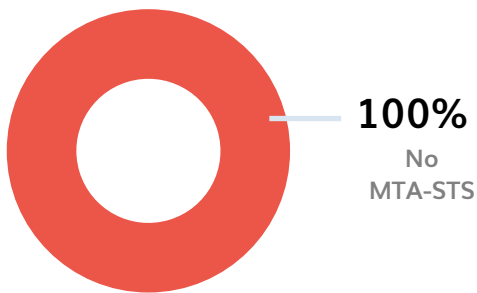
DMARC Adoption



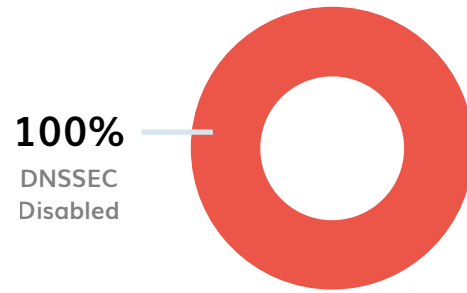
SPF Adoption



MTA-STS Adoption

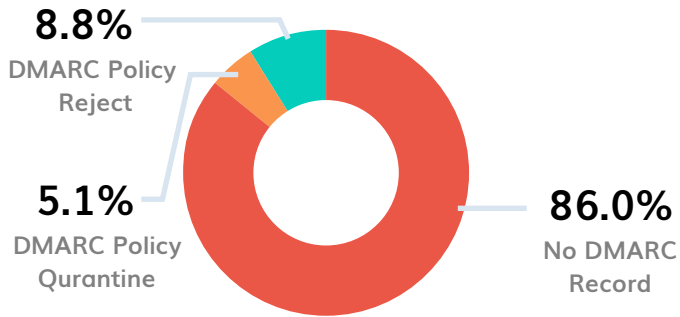


DNSSEC Adoption

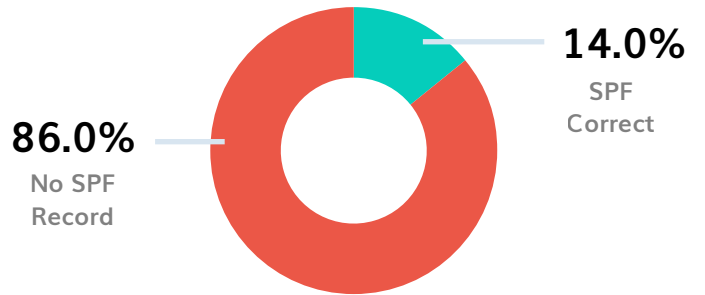


Banking Sector

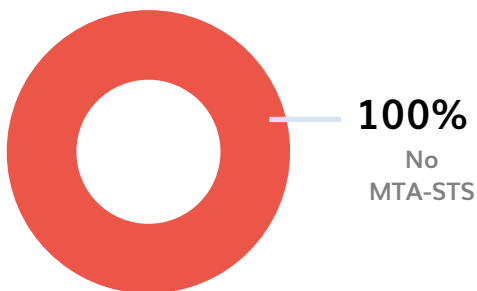
DMARC Adoption



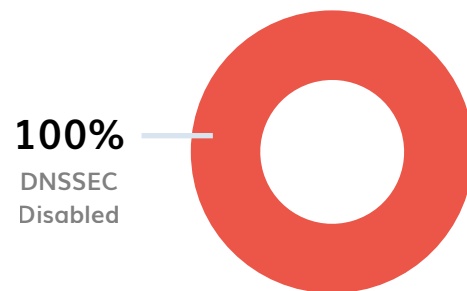
SPF Adoption



MTA-STS Adoption

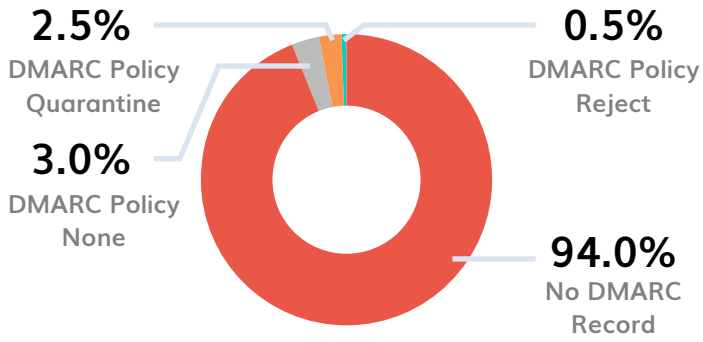


DNSSEC Adoption

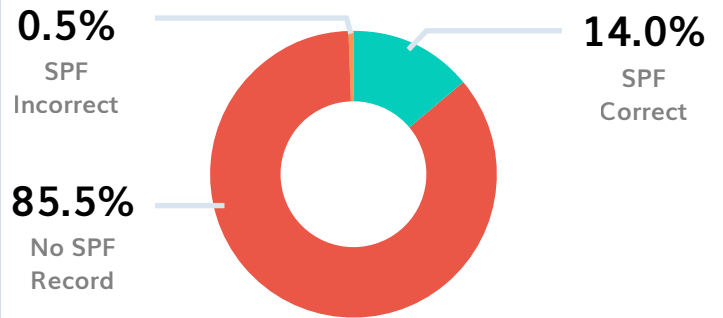


Telecommunications

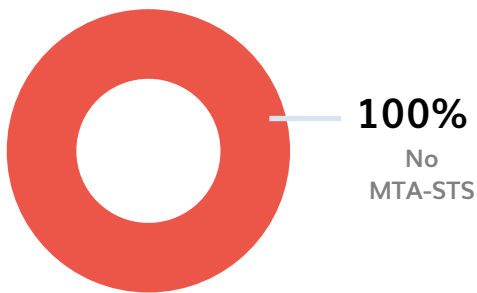
DMARC Adoption



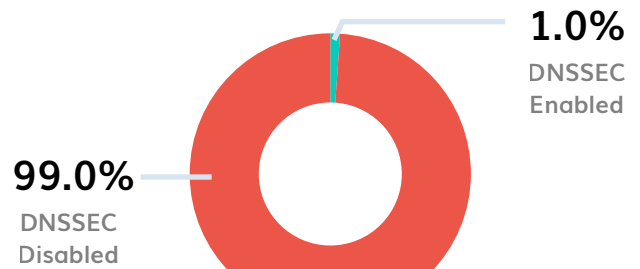
SPF Adoption



MTA-STS Adoption

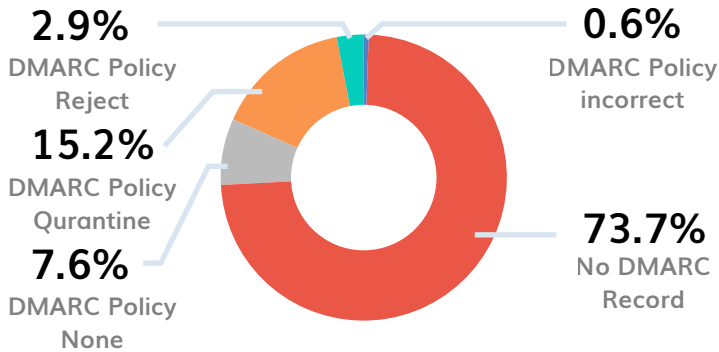


DNSSEC Adoption

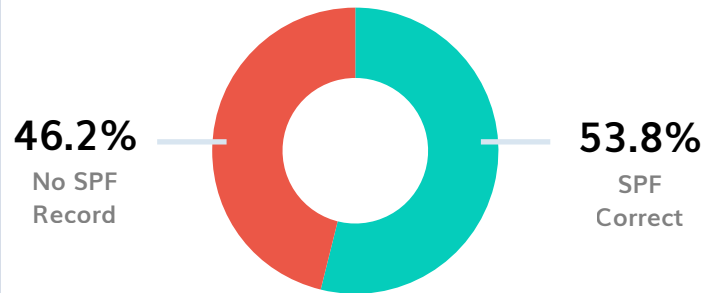


Government Sector

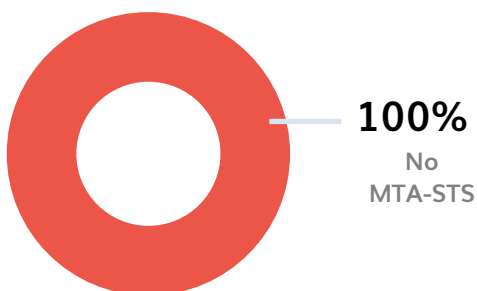
DMARC Adoption



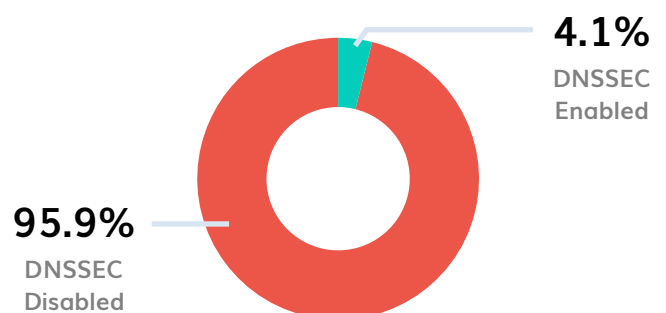
SPF Adoption



MTA-STS Adoption

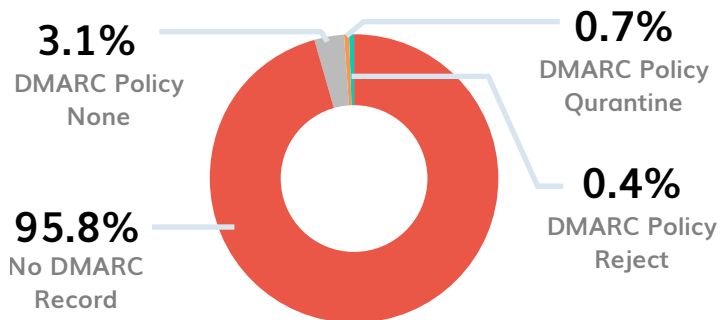


DNSSEC Adoption

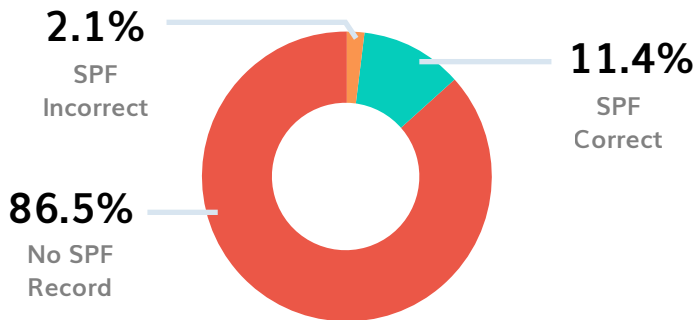


Transport

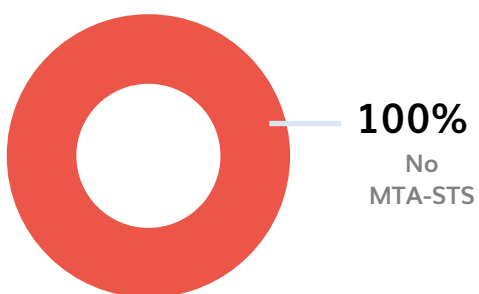
DMARC Adoption



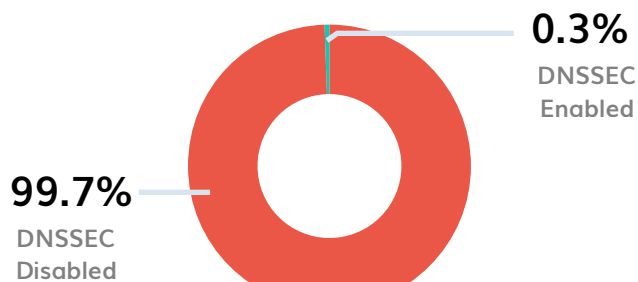
SPF Adoption



MTA-STS Adoption

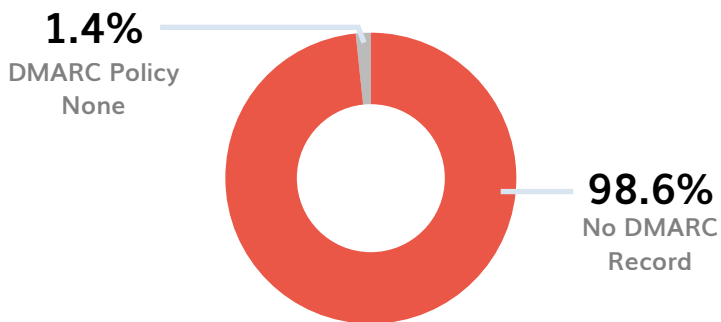


DNSSEC Adoption

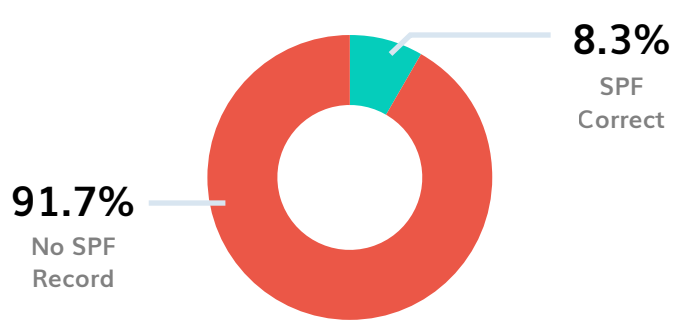


Education

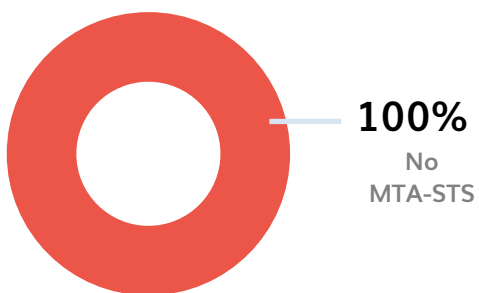
DMARC Adoption



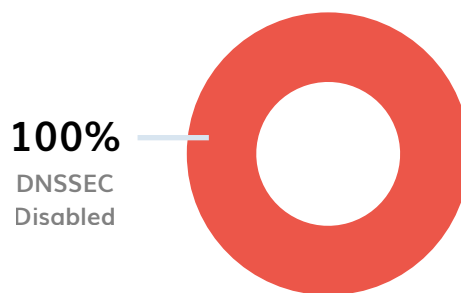
SPF Adoption



MTA-STS Adoption

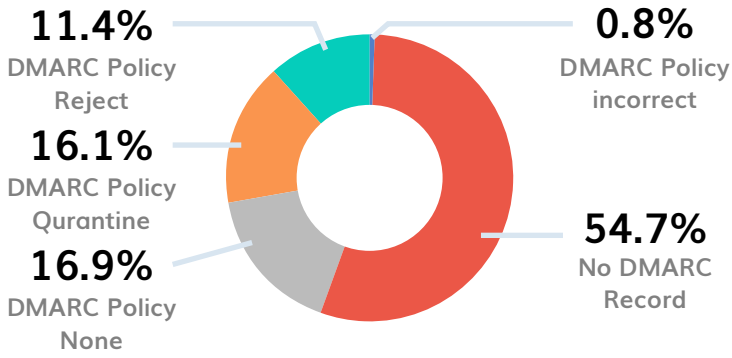


DNSSEC Adoption

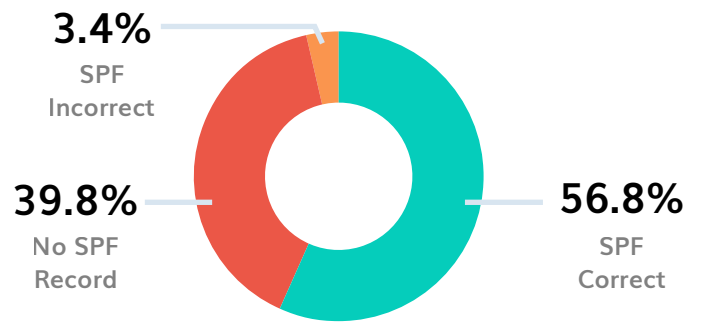


Miscellaneous-Business

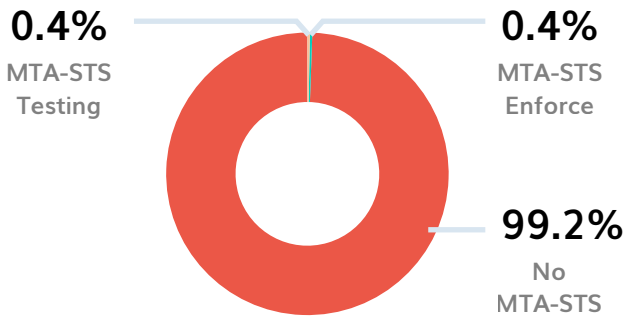
DMARC Adoption



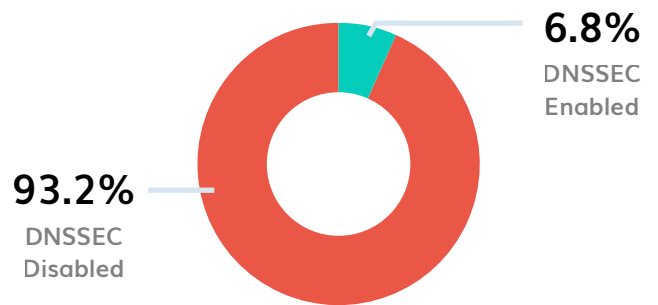
SPF Adoption



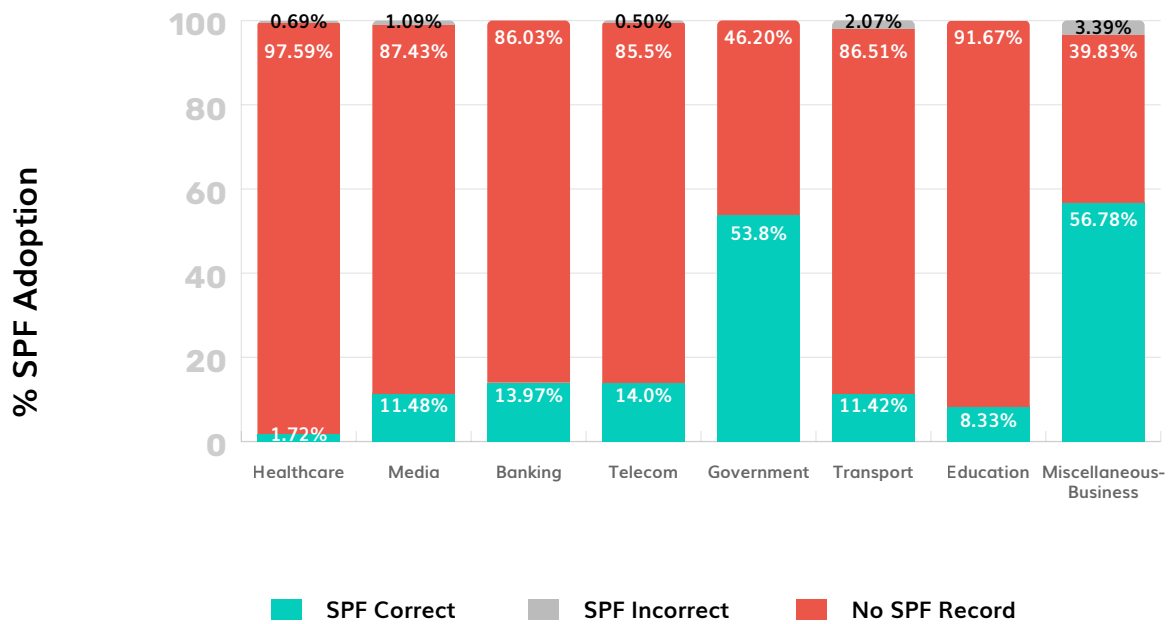
MTA-STS Adoption



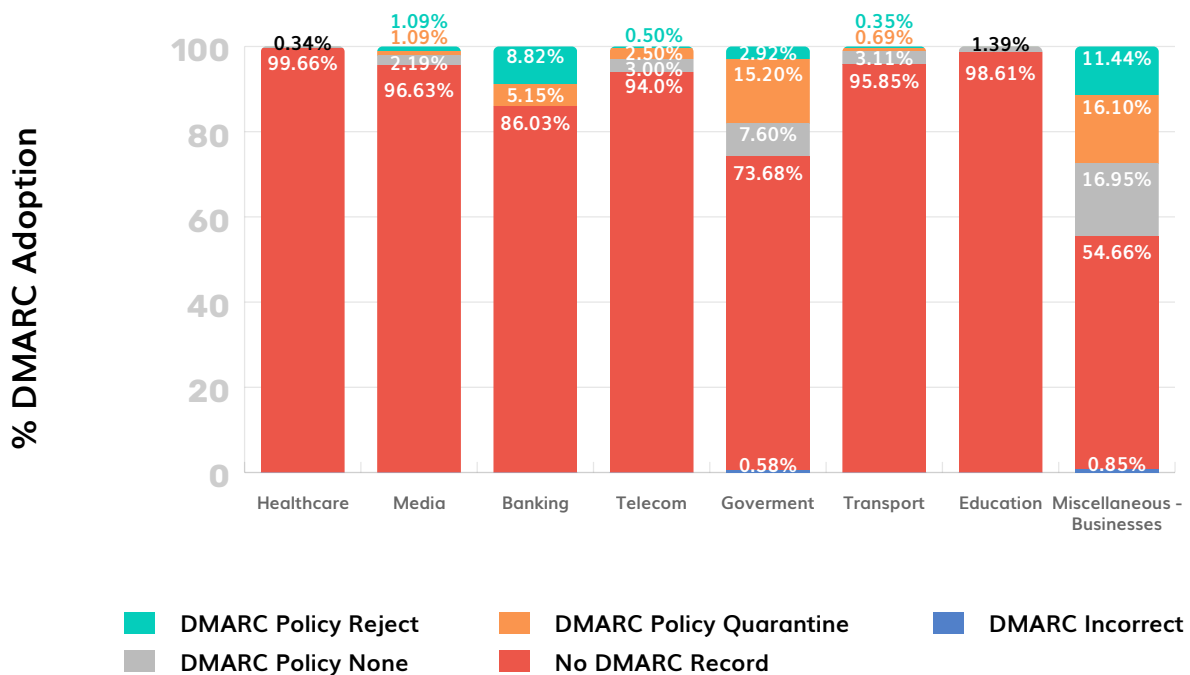
DNSSEC Adoption



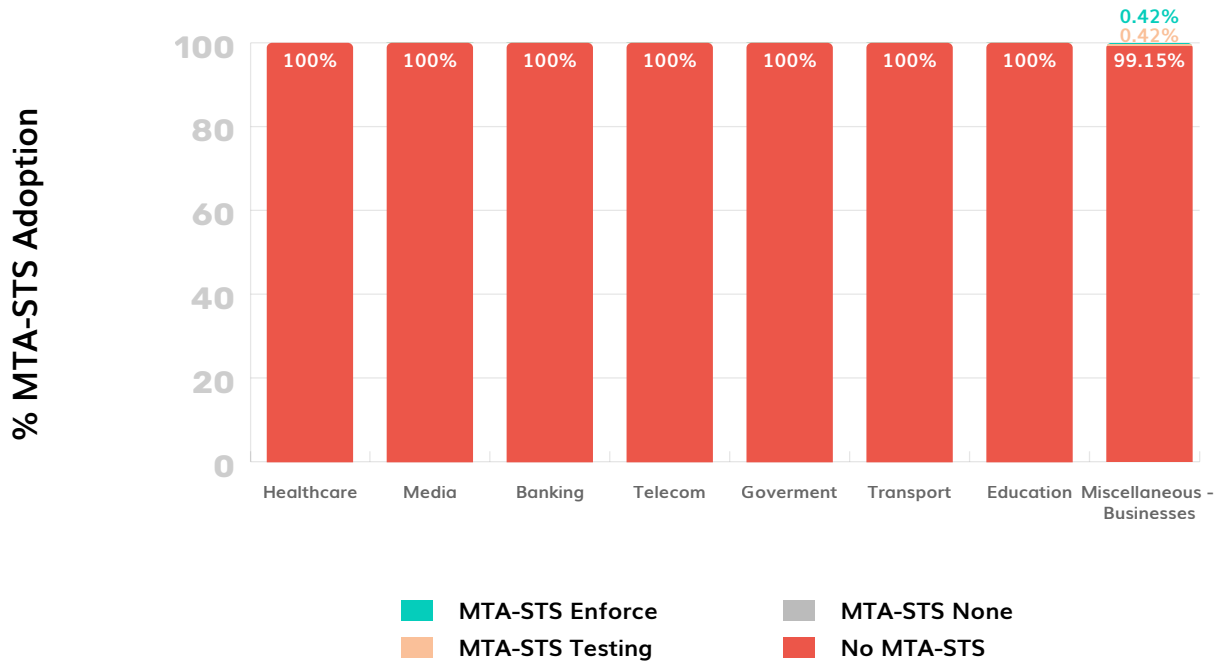
Comparative Analysis of SPF Adoption among Different Sectors in the Philippines



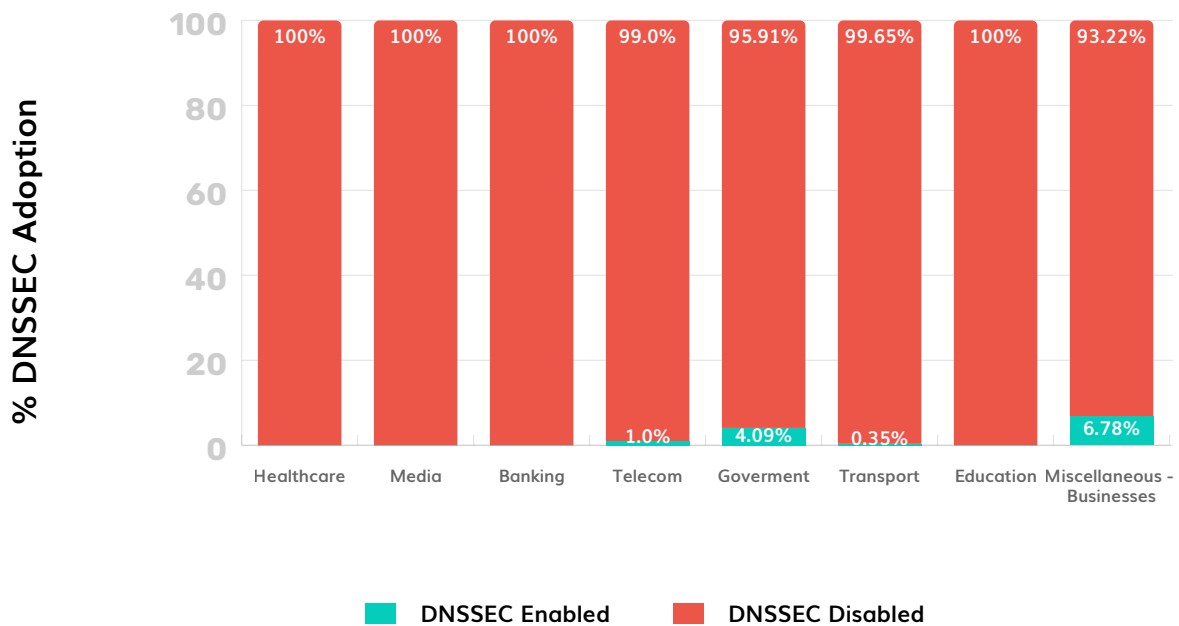
Comparative Analysis of DMARC Adoption among Different Sectors in Philippines



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



Comparative Analysis of DNSSEC Adoption among Different Sectors in Philippines



DMARC & MTA-STS Adoption Rates: Key Statistics for the Philippines

- ▶ 78% of analyzed domains in the Philippines do not have an SPF record.
- ▶ Less than 10% of the analyzed Philippine domains have DMARC correctly configured.
- ▶ A whopping 87.52% of the analyzed Philippine domains do not have a DMARC record.
- ▶ Of the domains with DMARC implemented, only 2.91% have the most strict and secure DMARC policy (i.e., "reject") in place.
- ▶ 98.42% of domains in the Philippines have DNSSEC completely disabled. This makes the country very vulnerable to DNS spoofing attacks.
- ▶ Nearly all (99.88%) domains in the Philippines have not implemented MTA-STS.
- ▶ None of the domains with MTA-STS implemented have enforced policies.

Critical Errors Organizations in the Philippines Are Making

- 1 A large number of domains in the healthcare sector do not have an SPF record.
- 2 The healthcare sector has the worst performance also in DMARC implementation, with an adoption rate of less than 1%.
- 3 The correct DMARC adoption rates for the majority of sectors in the Philippines are below 6%.
- 4 For the majority of domains, the strictest DMARC policy (i.e. DMARC Reject) has either a very low or zero adoption rate.
- 5 Almost no sectors in the Philippines have MTA-STS adoption.
- 6 Similar to MTA-STS, DNSSEC adoption is also extremely low regardless of the sector.
- 7 Critical sectors like healthcare (97.59%), banking (86.03%), and telecommunications (85.50%) have extremely high percentages of domains without SPF records.
- 8 The education sector has very low adoption of email security measures, with 91.67% of domains lacking SPF records and only 1.39% having correct DMARC implementation.
- 9 DMARC adoption is also critically low In the Philippine government sector.

How Can Organizations in the Philippines Improve Email Security & Deliverability?

- 1 Given the concerning low number of SPF records, both governmental and non-governmental entities should start paying particular attention to SPF adoption.
- 2 Not only should significant effort be put into implementing DMARC policies, but organizations should also strive to put in place the strict type (i.e. DMARC Reject) of policies.
- 3 It is also important to pay attention to DNSSEC enablement to secure data exchanges in the DNS.
- 4 It can be argued that MTA-STS adoption is non-existent. For secure transmission of emails, the proper adoption of MTA-STS is of utmost significance.
- 5 Out of all sectors, the healthcare sector remains the most vulnerable. Given the importance of sensitive medical data that is often sent over emails, both the government as well as private healthcare institutions should pay more attention to correct SPF, DMARC, MTA-STS, and DNSSEC implementation.
- 6 As many cybersecurity incidents take place as a result of human error, it is important to organize training sessions for organizational employees, as well as the general population.



How Can PowerDMARC Help?



PowerDMARC provides an extensive range of email and domain security SaaS services for varying business needs and requirements. Our team of experts knows the intricacies of email authentication and can help organizations easily implement DMARC, SPF, and MTA-STS, with little to no technical knowledge needed!

Whether you are based in the Philippines, or anywhere else in the world, having access to all the major email authentication protocols from a single, all-encompassing platform will allow you to in time enhance your domain protection and email deliverability. This will help you save a significant amount of time and financial resources in your fight against hackers and minimize the possibility of human error.

Feel free to contact us at support@powerdmarc.com with any questions that you might have and we will help you find the best answers and solutions to your security challenges.