# Thailand DMARC & MTA-STS Adoption Report 2024

POWERDMARC

# Thailand DMARC & MTA-STS Adoption Report 2024

- In the second half of 2023 and early 2024, Thai organizations faced an average of 1,892 cyber attacks per week, which is much higher than the global average of 1,040 attacks.

According to the report by the Nation, the Government/Military, Manufacturing, and Finance/Banking sectors have been especially targeted, suffering a combined total of 5,789 attacks in this period. Chanvith Iddhivadhana, Country Manager for Check Point Software in Thailand, noted: "Organizations in Thailand are facing an uphill battle. Cybersecurity attacks are getting more sophisticated and the volume of attacks has just been on the rise year after year."

It is important to note that 2023 has been alarming not only for Thailand but the world as a whole, as the number of ransomware attacks increased by 33% from the previous year). As Iddhivadhana stated, "To defend against the upcoming onslaught of attacks, organizations will require a consolidated, collaborative, and comprehensive platform approach to cybersecurity," and this is true both for Thailand and the rest of the world.

These alarming numbers are the reason why we have analyzed the threat landscape in Thailand to identify security gaps and pathways to fix the existing issues. Our report covers overall DMARC, SPF, MTA-STS, and DNSSEC adoption statistics along with an in-depth sector-wise analysis.

# Assessing the Threat Landscape

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

- To what extent are SPF and DMARC correctly adopted in Thailand?
- How widespread is MTA-STS adoption across different sectors?
- Is DNSSEC enabled by different domains in the country?
- What steps can be taken to reach safer and more secure networks in Thailand?
- Are some sectors more vulnerable to cyberattacks than others?

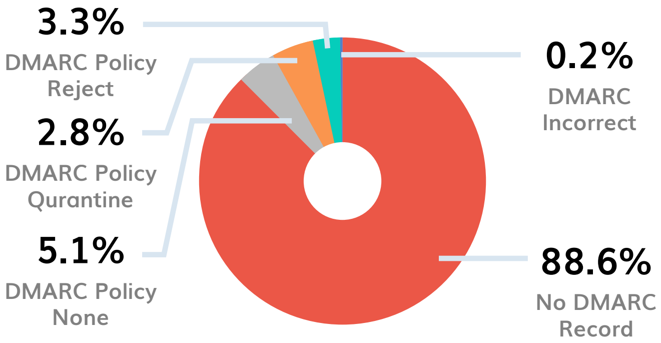
# Sectors Analyzed

**Total domains analyzed: 1350**

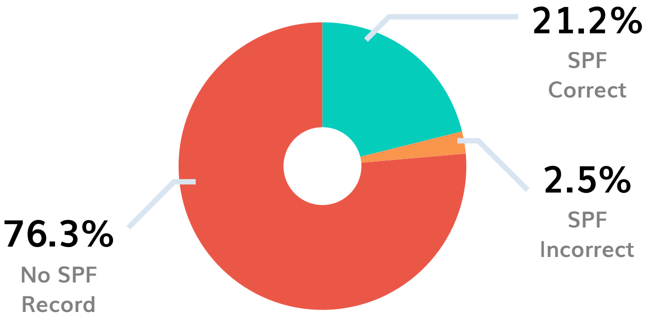
- Healthcare
- Media
- Banking
- Telecommunications
- Government
- Transport
- Miscellaneous-Business
- Education

# What Do the Numbers Say?

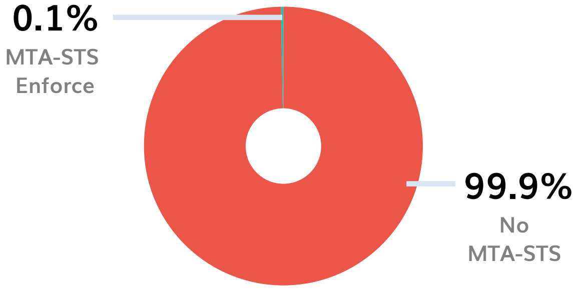
## DMARC Distribution in Thailand



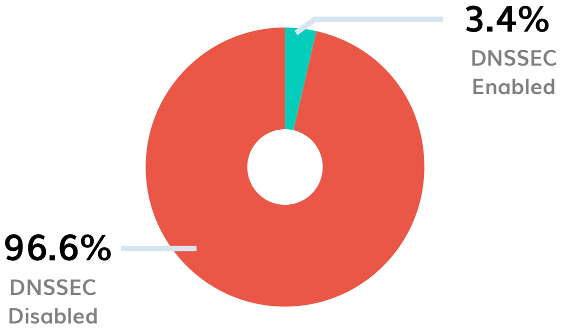
## SPF Distribution in Thailand



## MTA-STS Distribution in Thailand



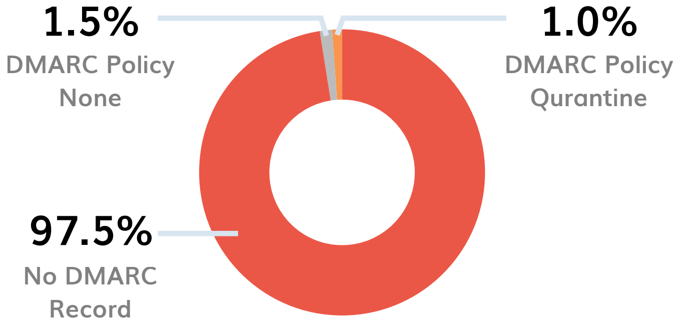
## DNSSEC Distribution in Thailand



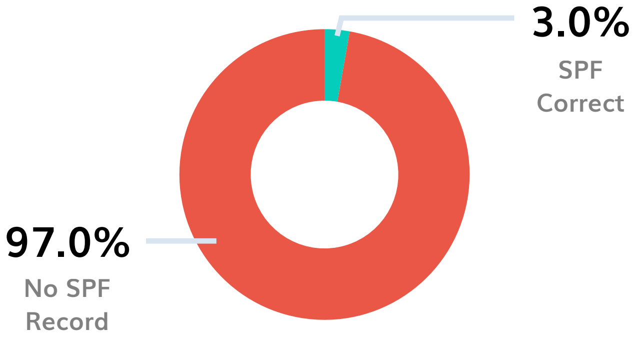
# Sector-wise Analysis of Domains in Thailand

## Healthcare Sector

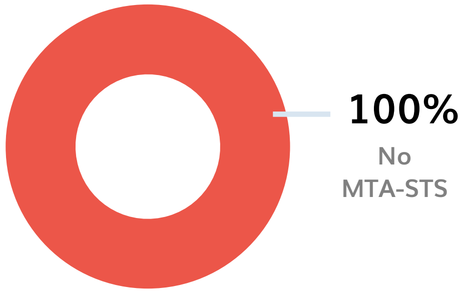
### DMARC Adoption



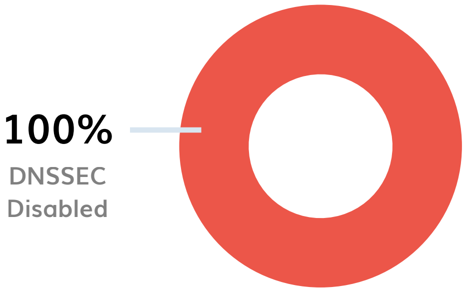
### SPF Adoption



### MTA-STS Adoption

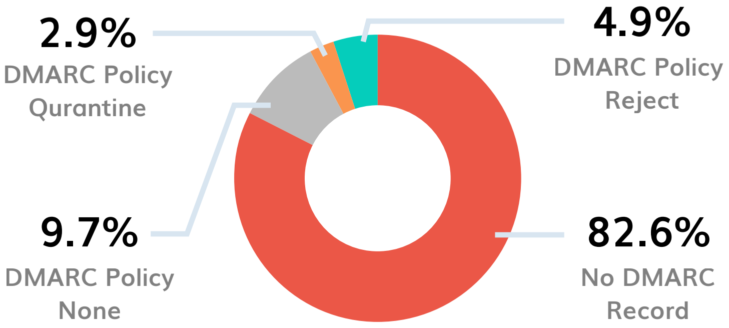


### DNSSEC Adoption

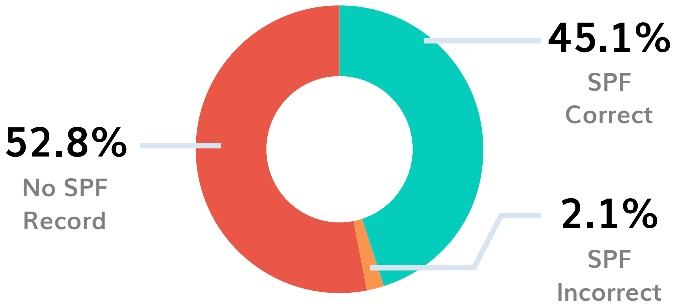


# Media Sector

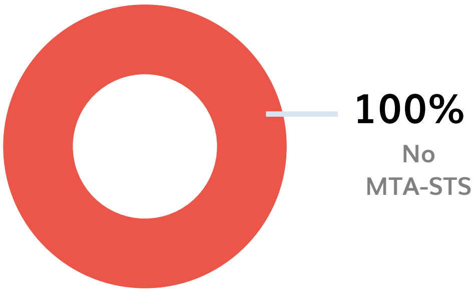
### DMARC Adoption



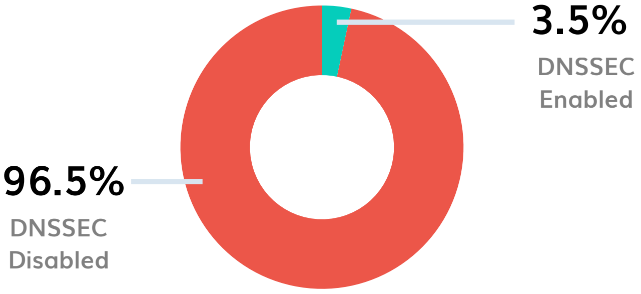
### SPF Adoption



### MTA-STS Adoption

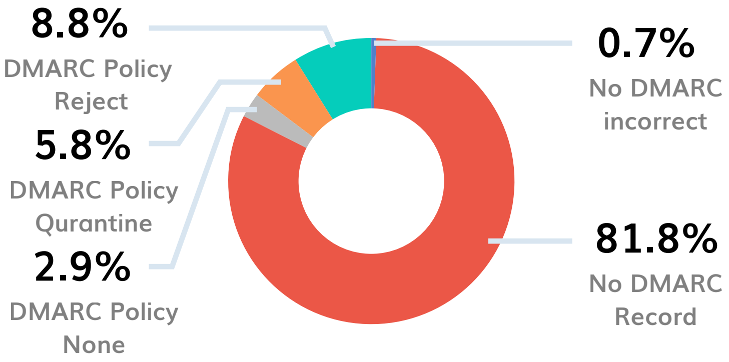


### DNSSEC Adoption

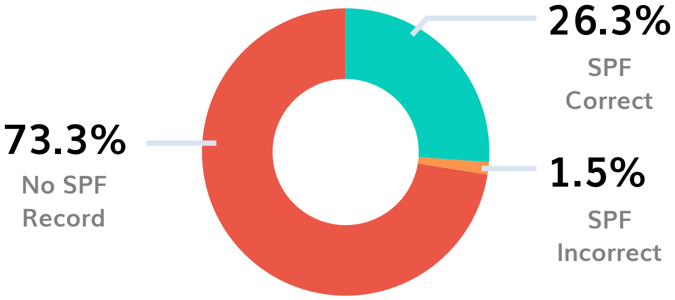


# Banking Sector

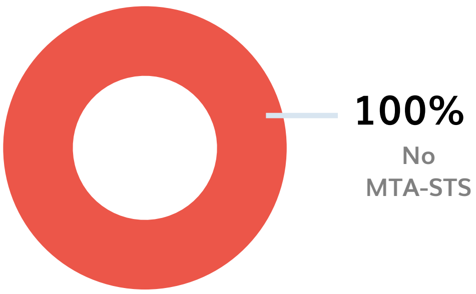
### DMARC Adoption



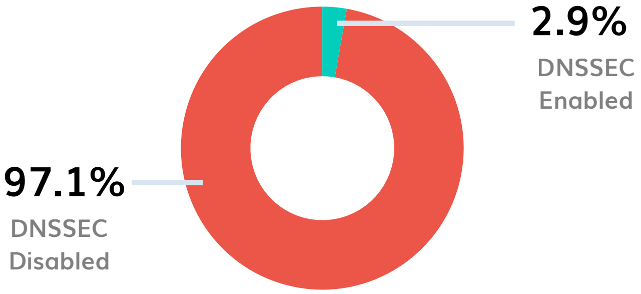
### SPF Adoption



### MTA-STS Adoption

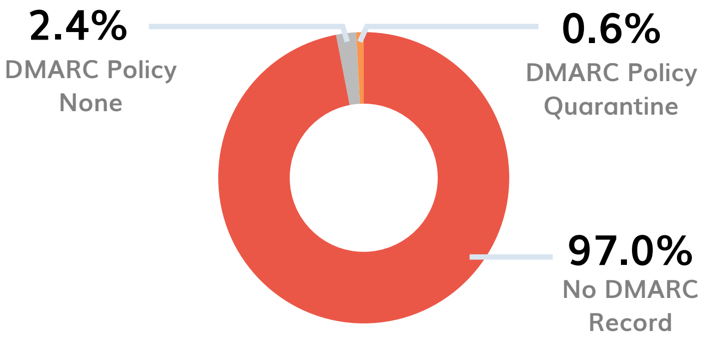


### DNSSEC Adoption

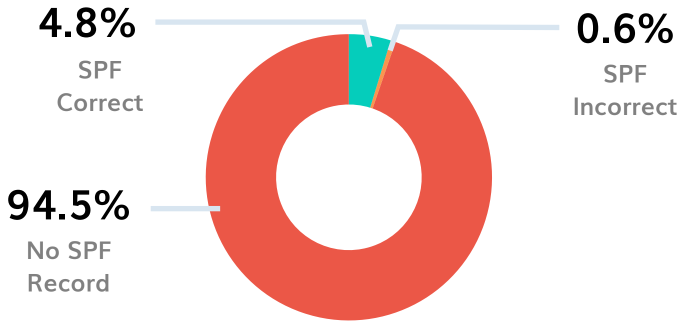


## Telecommunications

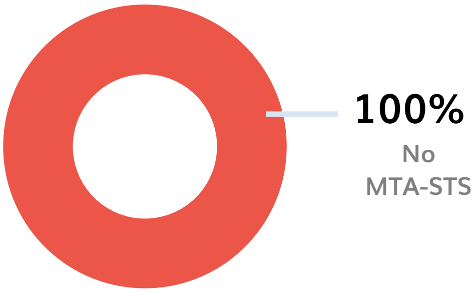
### DMARC Adoption



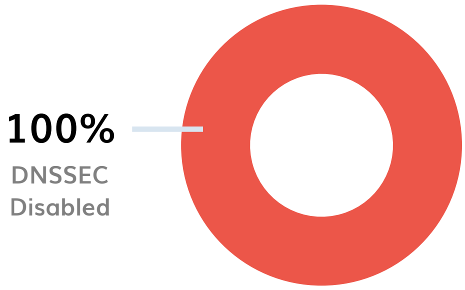
### SPF Adoption



### MTA-STS Adoption

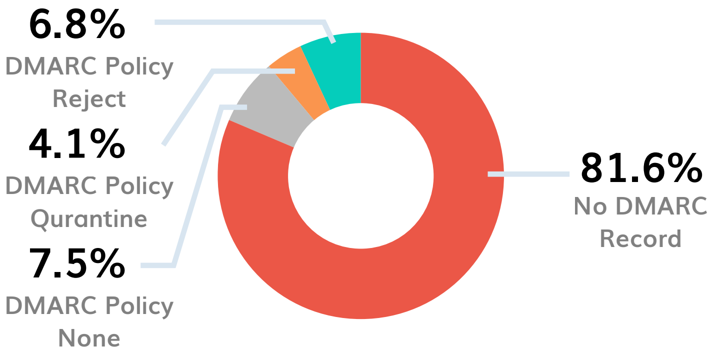


### DNSSEC Adoption

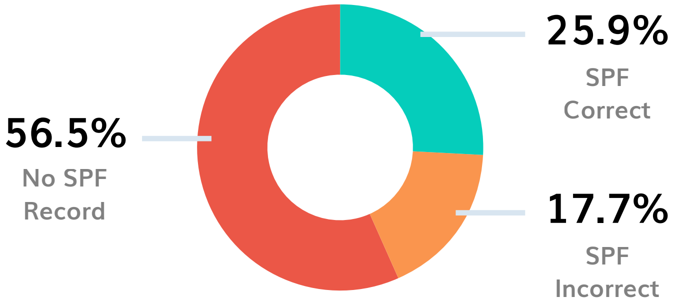


## Government Sector

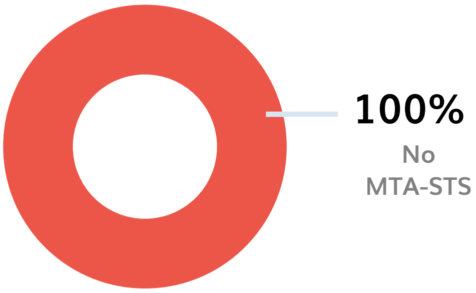
### DMARC Adoption



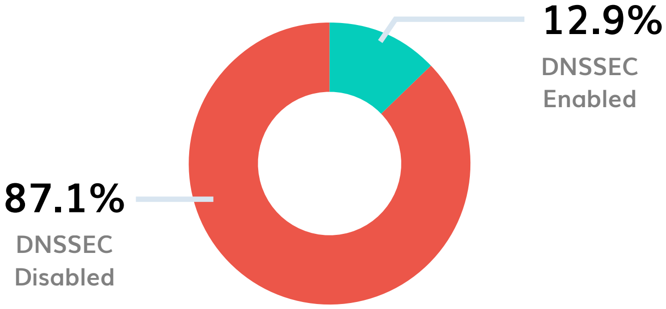
### SPF Adoption



### MTA-STS Adoption

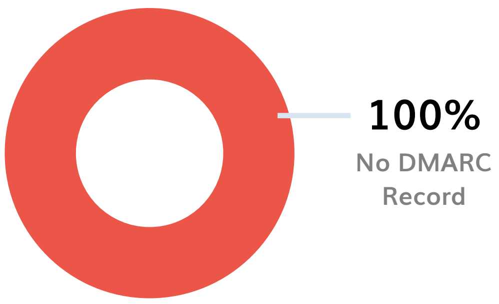


### DNSSEC Adoption

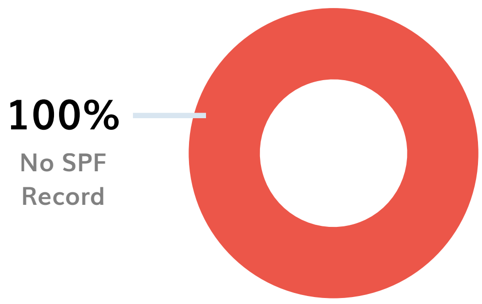


## Transport

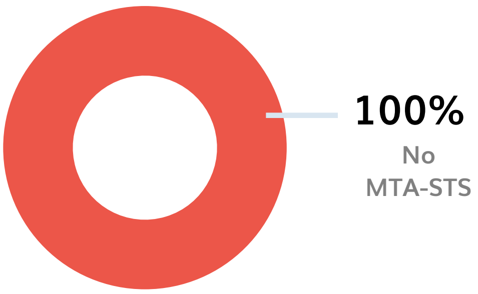
### DMARC Adoption



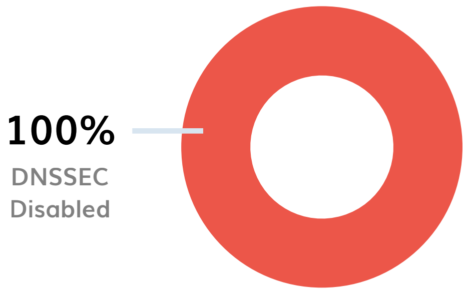
### SPF Adoption



### MTA-STS Adoption

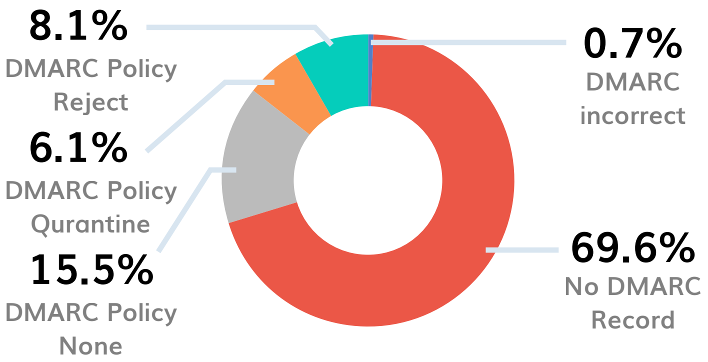


### DNSSEC Adoption

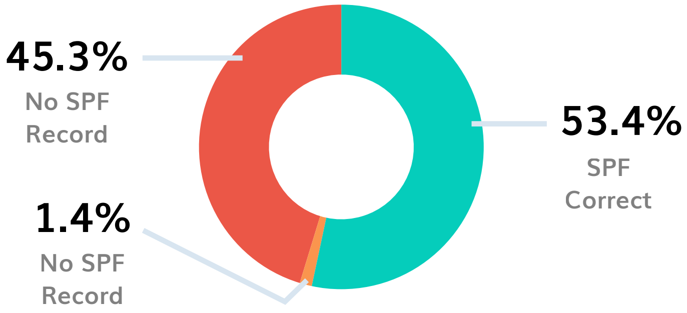


## Miscellaneous-Business

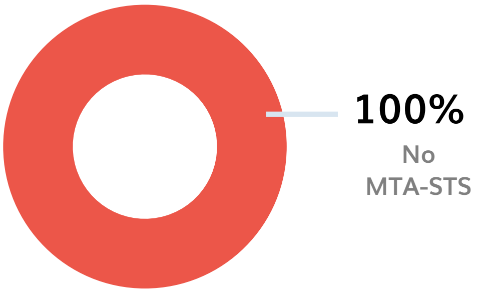
### DMARC Adoption



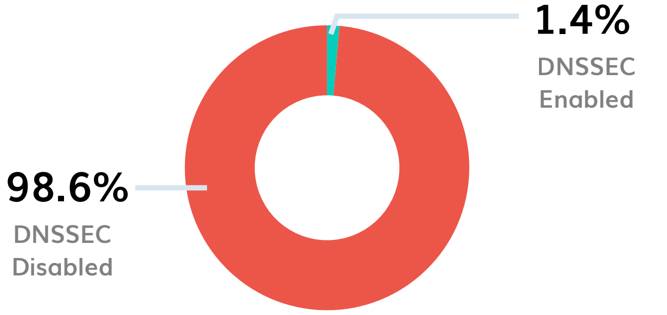
### SPF Adoption



### MTA-STS Adoption

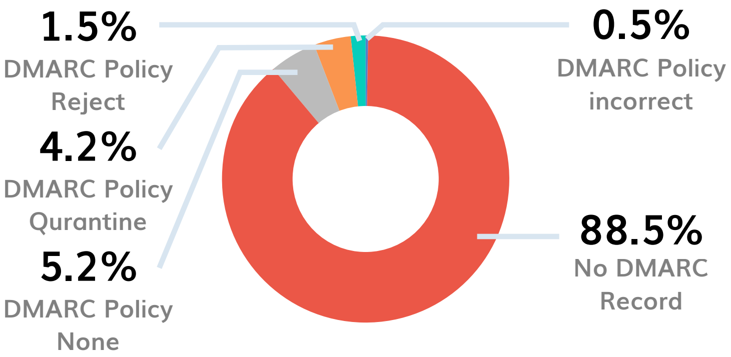


### DNSSEC Adoption

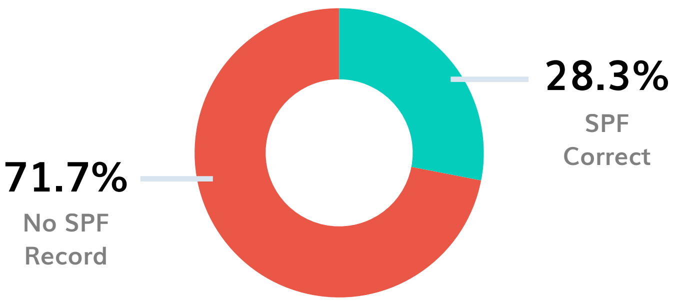


# Education

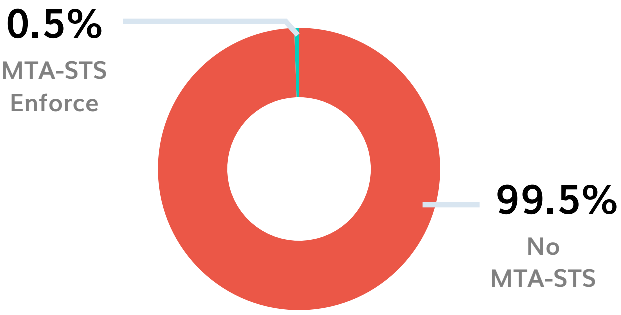
## DMARC Adoption



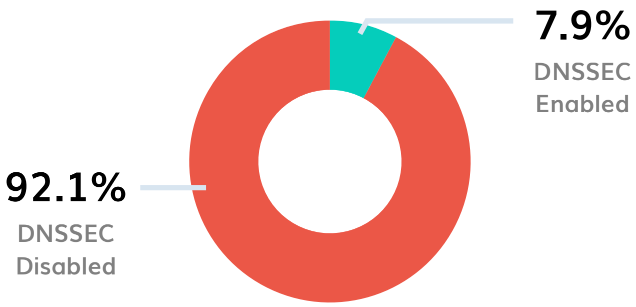
## SPF Adoption



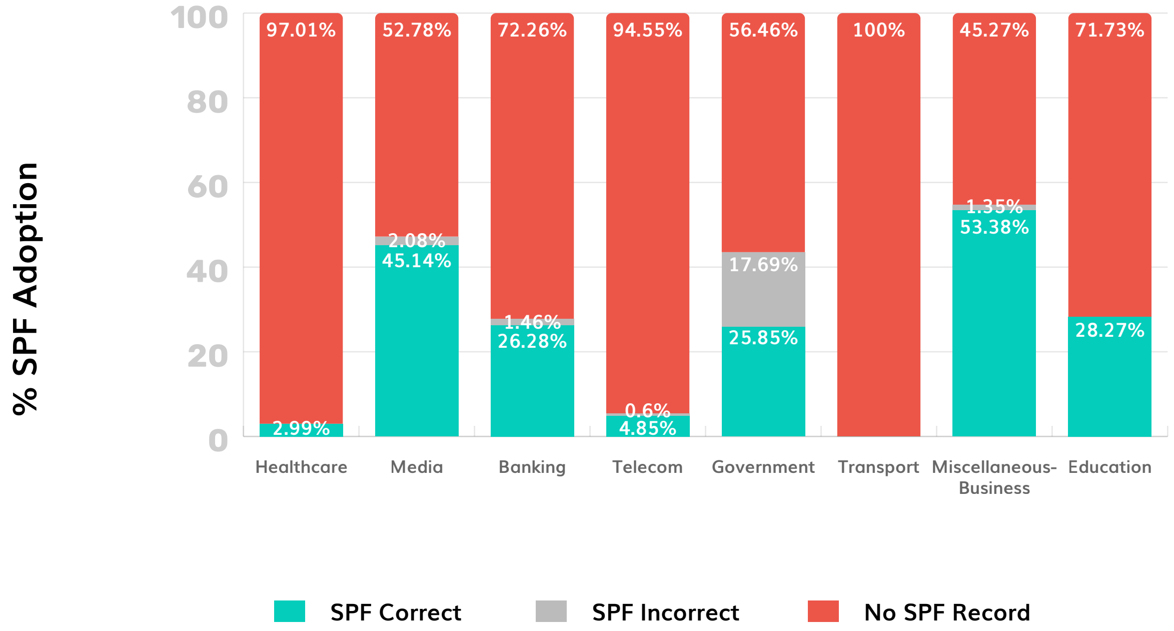
## MTA-STS Adoption



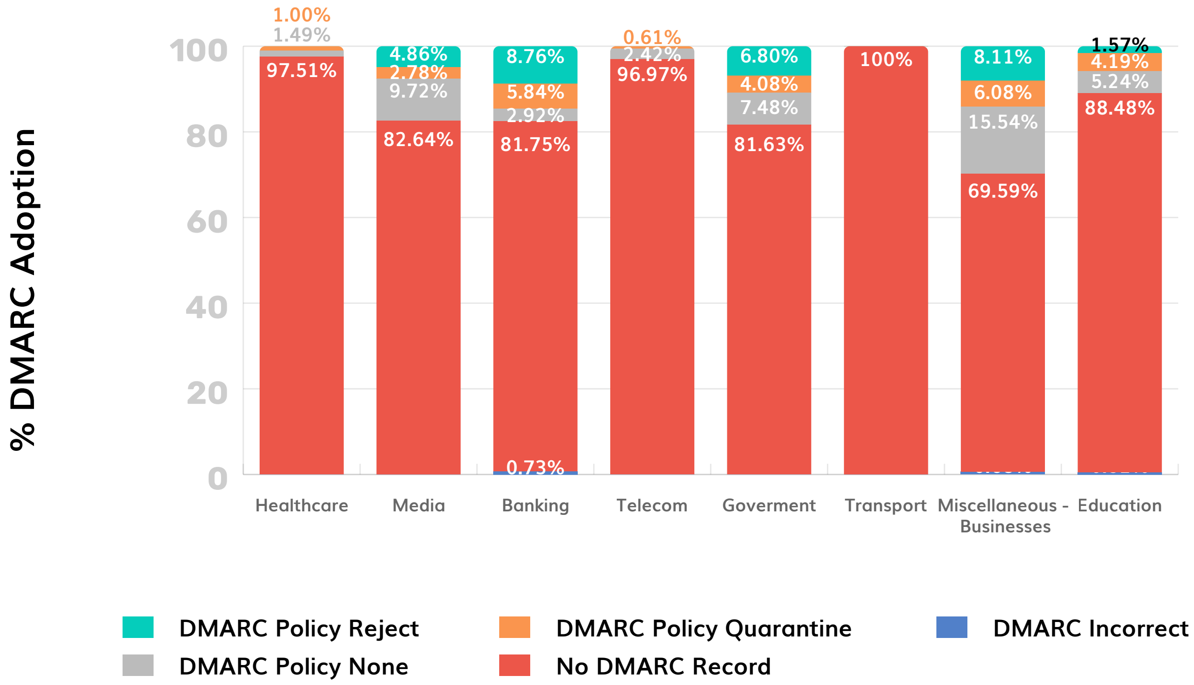
## DNSSEC Adoption



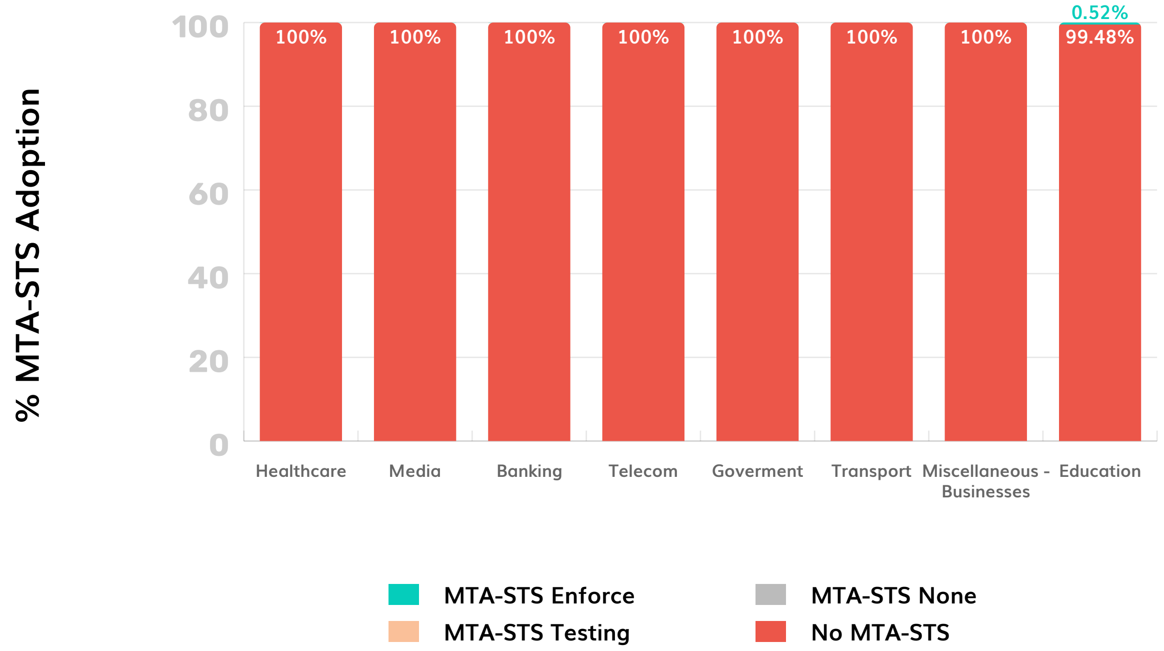
# Comparative Analysis of SPF Adoption among Different Sectors in Thailand



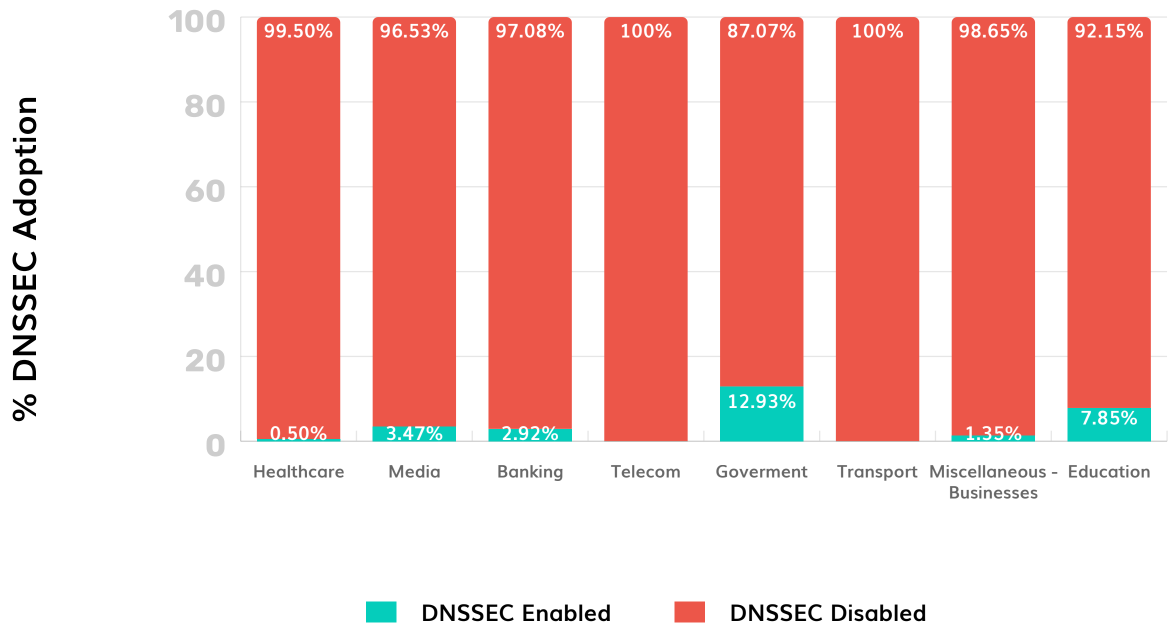
# Comparative Analysis of DMARC Adoption among Different Sectors in Thailand



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



# Comparative Analysis of DNSSEC Adoption among Different Sectors in Thailand



# DMARC & MTA-STS Adoption Rates: Key Statistics for Thailand

- 76.30% of Thai domains have no SPF record.
- As many as 88.59% of Thai domains have no DMARC record.
- Only 3.26% of the analyzed domains have a DMARC policy set to "reject."
- The majority of domains that have DMARC implemented have a policy set to "none," (5.11%), which provides no protection against the attacks.
- Only 0.07% of domains have valid MTA-STS implementation.
- Only 3.41% of domains have DNSSEC enabled, leaving 96.59% of domains vulnerable.

# Critical Errors Organizations in Thailand Are Making

1. There is a widespread lack of SPF records across various sectors in Thailand. The transport sector has the worst adoption rate with 100% of domains lacking SPF records, while the miscellaneous-business sector performs best with only 45.27% lacking SPF records.

2. DMARC implementation is also very low across all sectors. The business sector again has the highest correct DMARC adoption (29.73%), while the transport sector again has the worst adoption (0%).

3. The adoption of strict DMARC policies (i.e., "reject") is very low across all sectors. The banking sector has the highest adoption rate at 8.76%. Some important sectors, including healthcare, telecommunications, and transport, have no domains implementing the "reject" policy. This means that some crucial domains are very vulnerable to phishing attacks.

4. MTA-STS adoption is non-existent in almost all sectors. The only exception is the education sector. 0.52% of domains in education have valid MTA-STS implementation, which is still extremely low.

5. DNSSEC adoption is generally low across all sectors. The government sector has the highest adoption rate at 12.93%. The telecommunications and transport sectors have zero DNSSEC implementation.

6. The healthcare sector has the lowest email authentication (SPF, DMARC, MTA-STS) and DNSSEC adoption rates.

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

1 All organizations, especially those in sectors with low adoption rates such as healthcare, telecommunications, and transport, should make it a priority to implement SPF records for their domains.

2 Along with SPF, domain owners should focus on correctly implementing DMARC policies. After initial implementation, they should gradually move towards stricter policies, aiming for “quarantine” and ultimately “reject” policies.

3 To lower the risk of DNS spoofing attacks, organizations (especially those in transport and telecommunications) should prioritize enabling DNSSEC for their domains.

4 Given the near-zero adoption rate across all sectors, organizations should put significant effort into implementing MTA-STS.

5 Organizations should implement DKIM to add digital signatures to outgoing emails, thereby potentially preventing unauthorized alterations.

# How Can PowerDMARC Help?

If you are looking for full-stack email authentication SaaS services, then PowerDMARC is the best choice.

PowerDMARC combines DMARC, SPF, DKIM, BIMI, MTA-STS, and TLS-RPT solutions into a single centralized platform to help MSPs, MSSPs, governments, and non-profits in their fight against cyberattacks. You can significantly reduce the likelihood and success of phishing attacks, spoofing, domain abuse, or other forms of unauthorized use by implementing email authentication with the help of PowerDMARC.

PowerDMARC has come to prove that email authentication and email deliverability enhancement don’t have to be expensive and out of reach for businesses with tight budgets. Get in touch with the PowerDMARC team at support@powerdmarc.com to get the relevant pricing information and guidelines on how to best secure your presence online!