# Burma
# DMARC & MTA-STS Adoption Report 2024

POWERDMARC

POWERDMARC

Case study

# Burma DMARC & MTA-STS Adoption Report 2024

- Given the fact that 90% of attacks on organizations start from malicious emails, companies should implement strong email security measures to prevent cyberattacks and data breaches. Among other regions, the situation around cyberattacks is concerning South East Asia too, with scam victims losing $385.6m in the first half of 2024, a 24.6% increase compared with the same period of the previous year. Some Southeast Asian countries even experienced more than 347 million cyber attack cases in the first half of 2023 alone, with the highest number of cases being due to ransomware incidents.

- UNODC estimates “financial losses between US $18 billion and $37 billion from scams targeting victims in East and Southeast Asia in 2023 alone, with a high proportion of these losses attributed to scams committed by organized crime groups in Southeast Asia.”

- The scope of sectors discussed here in relation to DMARC, SPF, MTA-STS, and DNSSEC implementation includes healthcare, business, banking, government, telecommunications, transport, and education.

## A Brief Overview of Email Authentication & Why It’s Important

### DMARC

DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email authentication protocol that, by expanding on SPF and DKIM, helps prevent email spoofing and phishing attacks.

### SPF

Sender Policy Framework (SPF) is designed to verify the validity and safety of emails by enabling domain owners to filter which mail servers are valid and authorized to send emails from their domain.

- **MTA-STS**

  Mail Transfer Agent Strict Transport Security (MTA-STS) makes TLS encryption mandatory for inbound emails, ensuring secure email transmission over an encrypted SMTP connection.

## Assessing the Threat Landscape

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

- What's the state of SPF and DMARC adoption?
- How prevalent is MTA-STS adoption?
- What's the DNSSEC enablement rate?
- How can Burma improve email security to stop impersonation attacks?
- Which sectors are most vulnerable to phishing?
- How can organizations combat email-based threats?

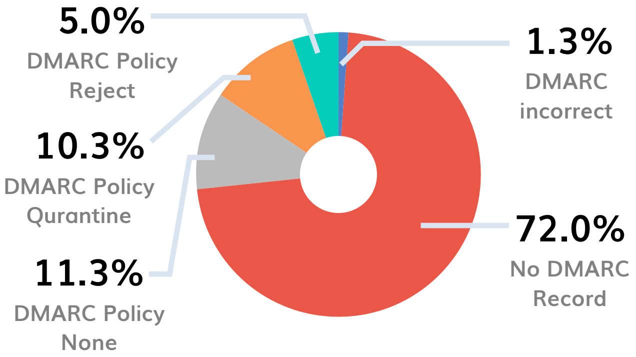
## Sectors Analyzed

Overall, over **300 domains** have been analyzed across **7 sectors.**

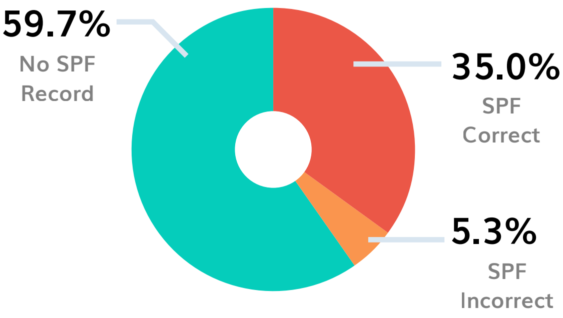
- Healthcare
- Banking
- Government
- Telecommunication
- Transport
- Education
- Miscellaneous - Businesses

# What Do the Numbers Say?

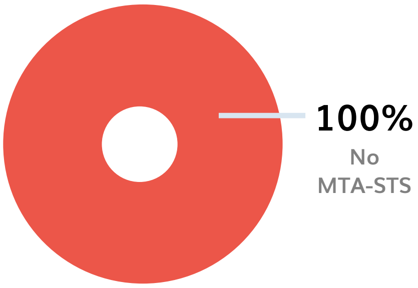
## DMARC Distribution in Burma



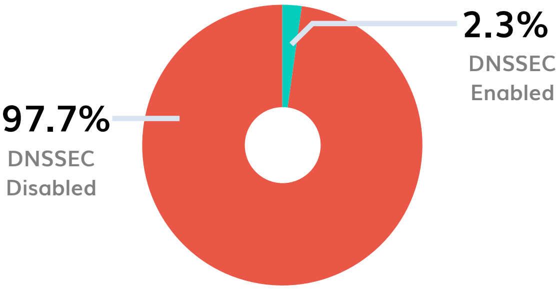
## SPF Distribution in Burma



## MTA-STS Distribution in Burma



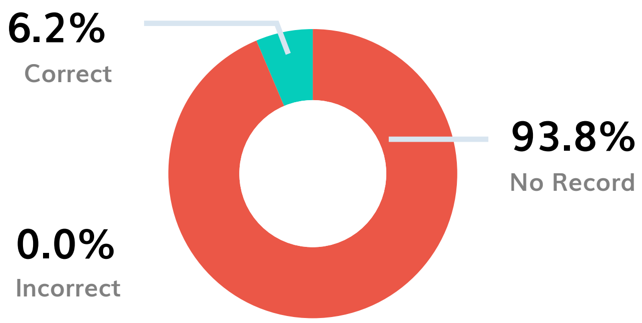
## DNSSEC Distribution in Burma



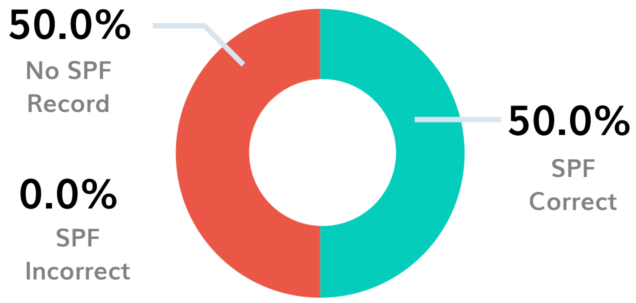
# Sector-wise Analysis of Domains in Burma

## Healthcare Sector

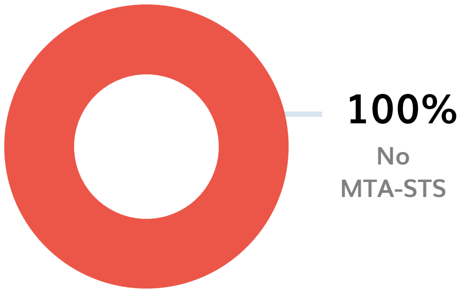
### DMARC Adoption



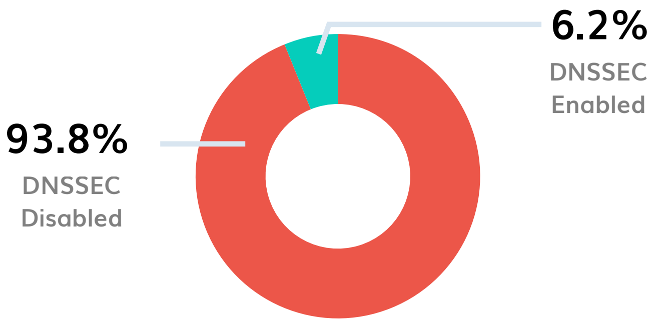
### SPF Adoption



### MTA-STS Adoption

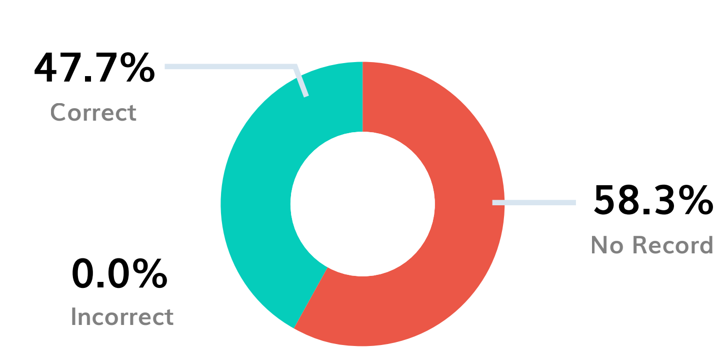


### DNSSEC Adoption

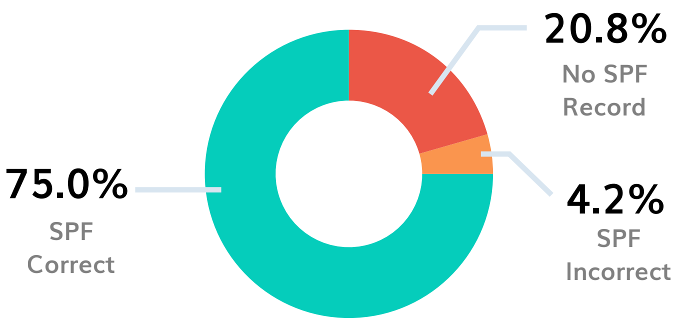


## Banking Sector

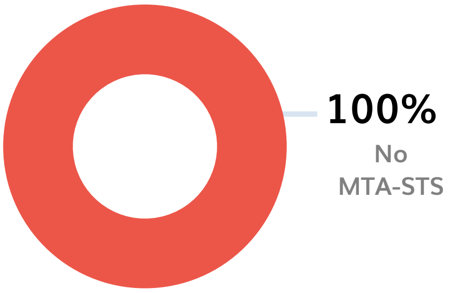
### DMARC Adoption



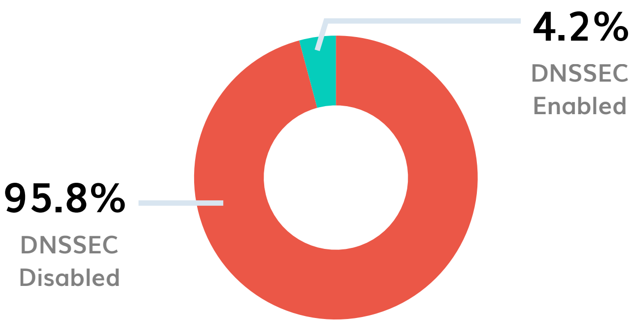
### SPF Adoption



### MTA-STS Adoption

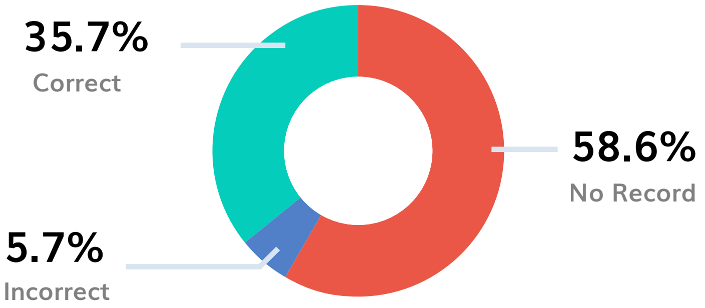


### DNSSEC Adoption

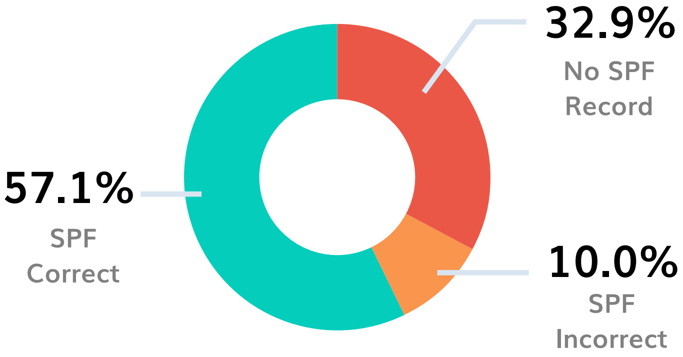


## Government Sector

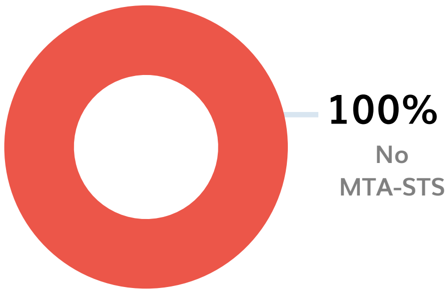
### DMARC Adoption



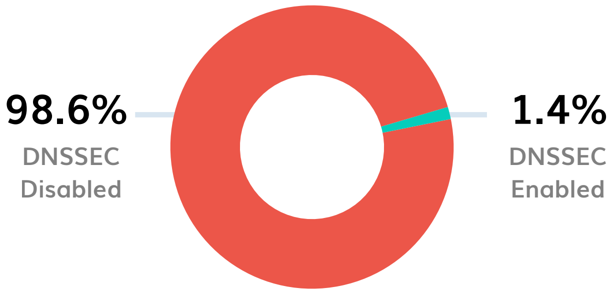
### SPF Adoption



### MTA-STS Adoption

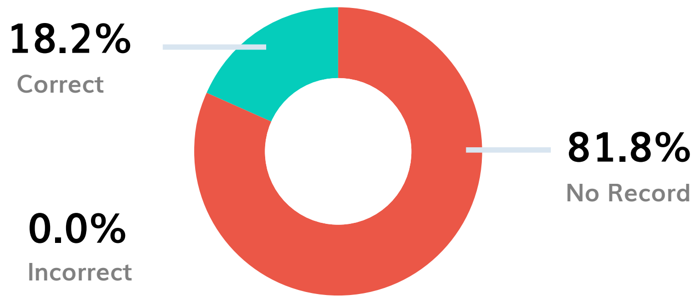


### DNSSEC Adoption

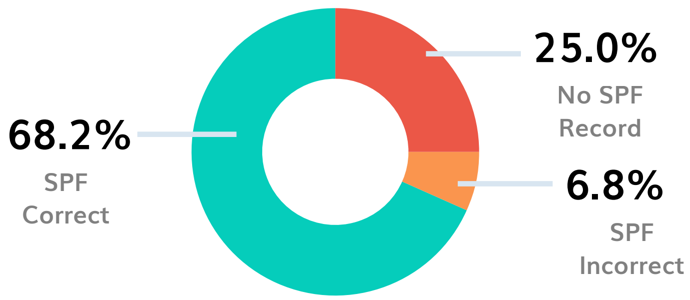


## Telecommunication Sector

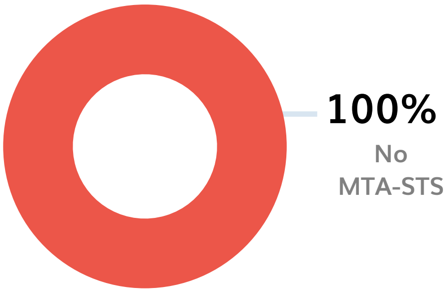
### DMARC Adoption



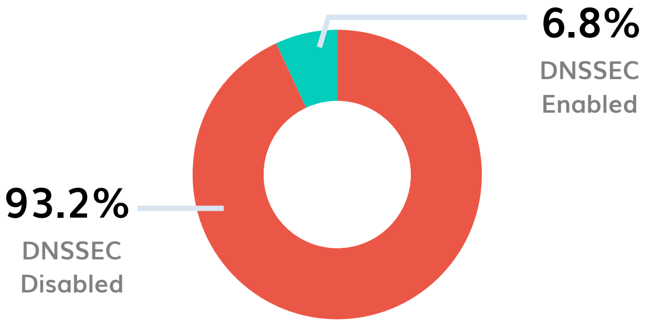
### SPF Adoption



### MTA-STS Adoption

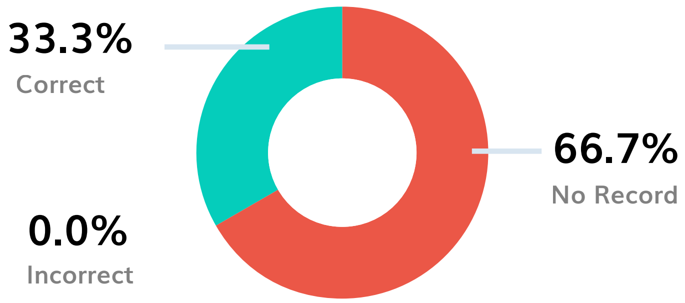


### DNSSEC Adoption

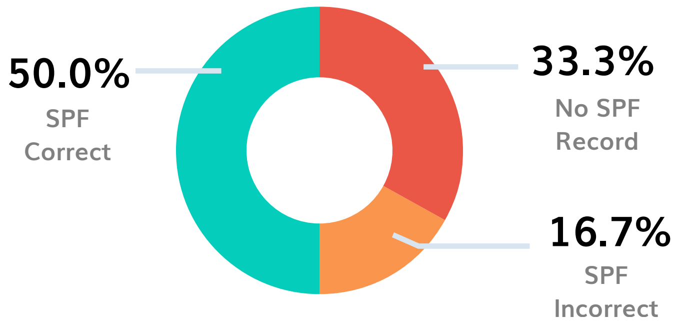


## Transport Sector

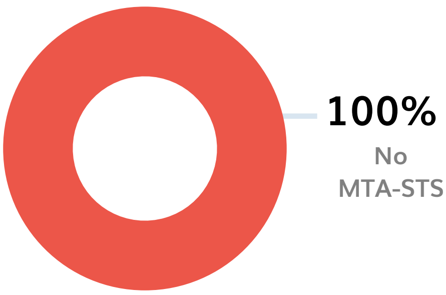
### DMARC Adoption



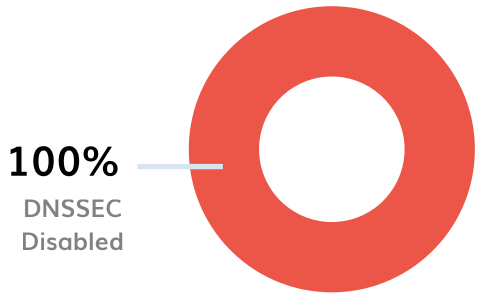
### SPF Adoption



### MTA-STS Adoption

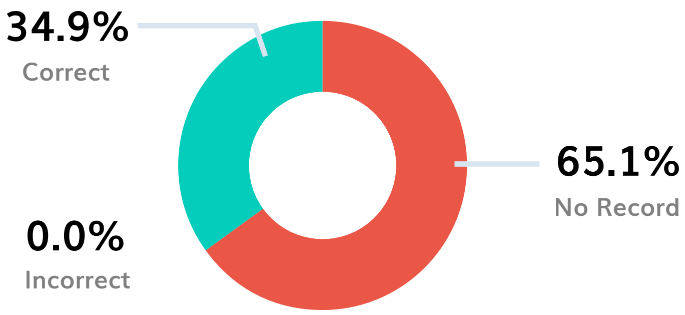


### DNSSEC Adoption

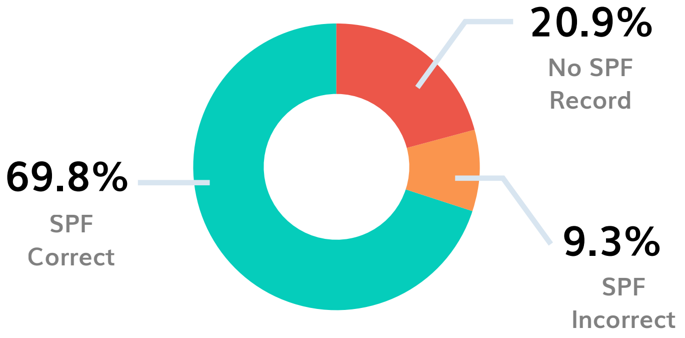


## Miscellaneous - Businesses

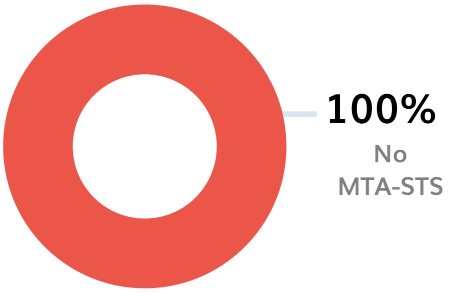
### DMARC Adoption



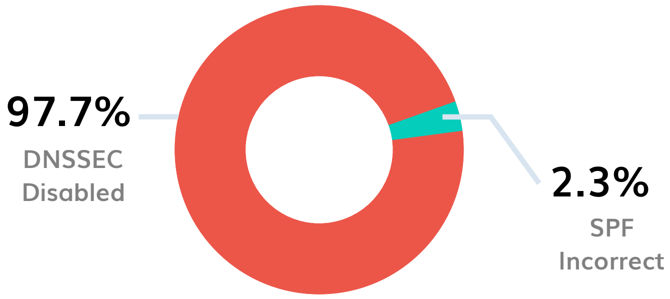
### SPF Adoption



### MTA-STS Adoption

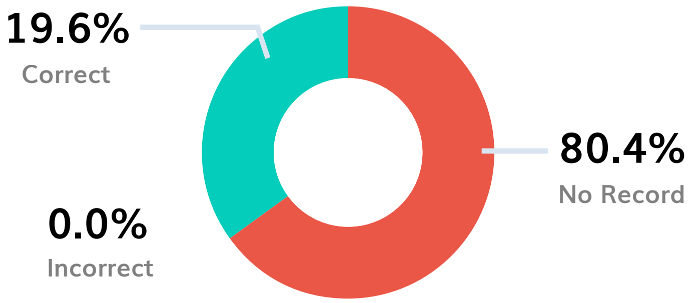


### DNSSEC Adoption

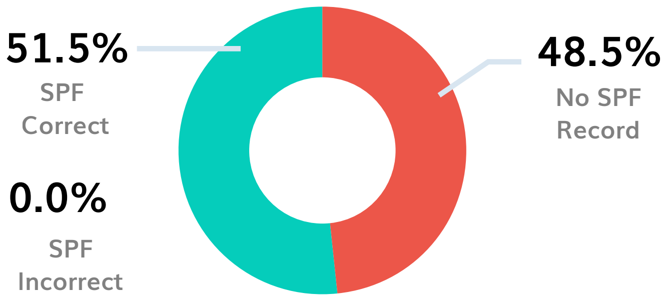


## Education Sector

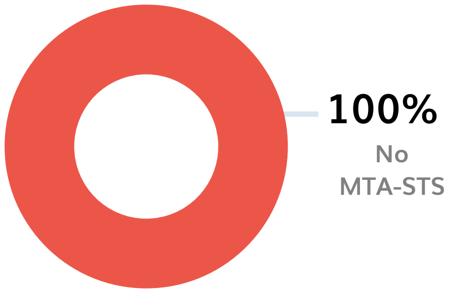
### DMARC Adoption



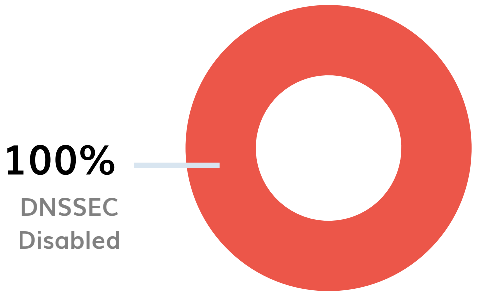
### SPF Adoption



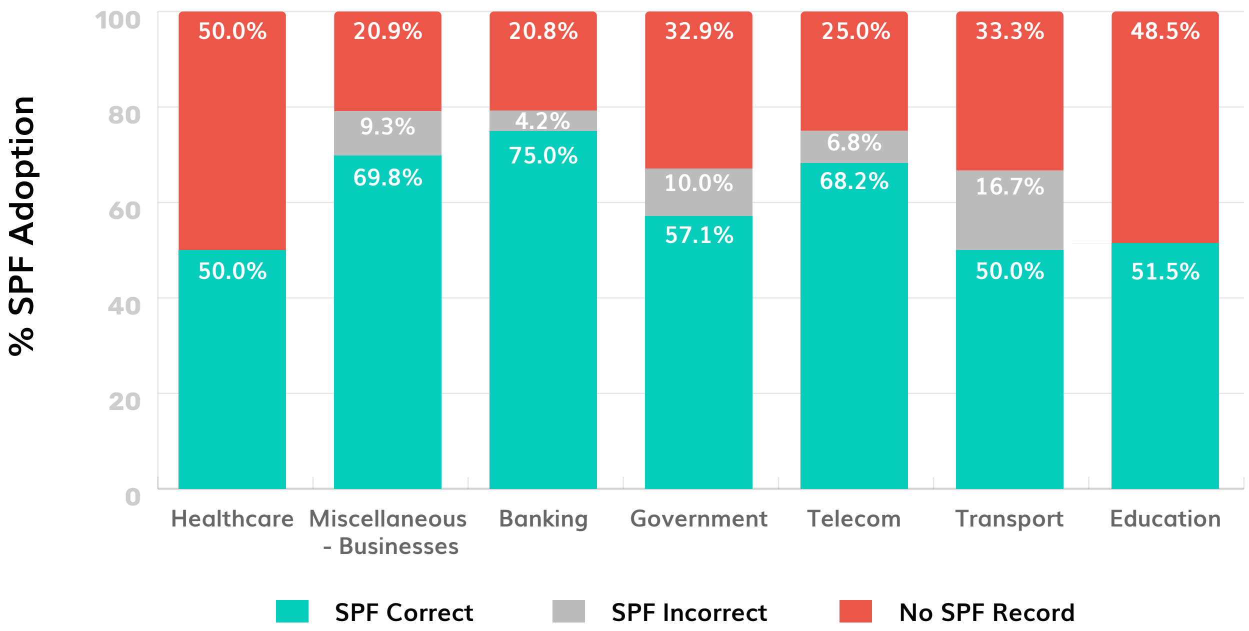
### MTA-STS Adoption



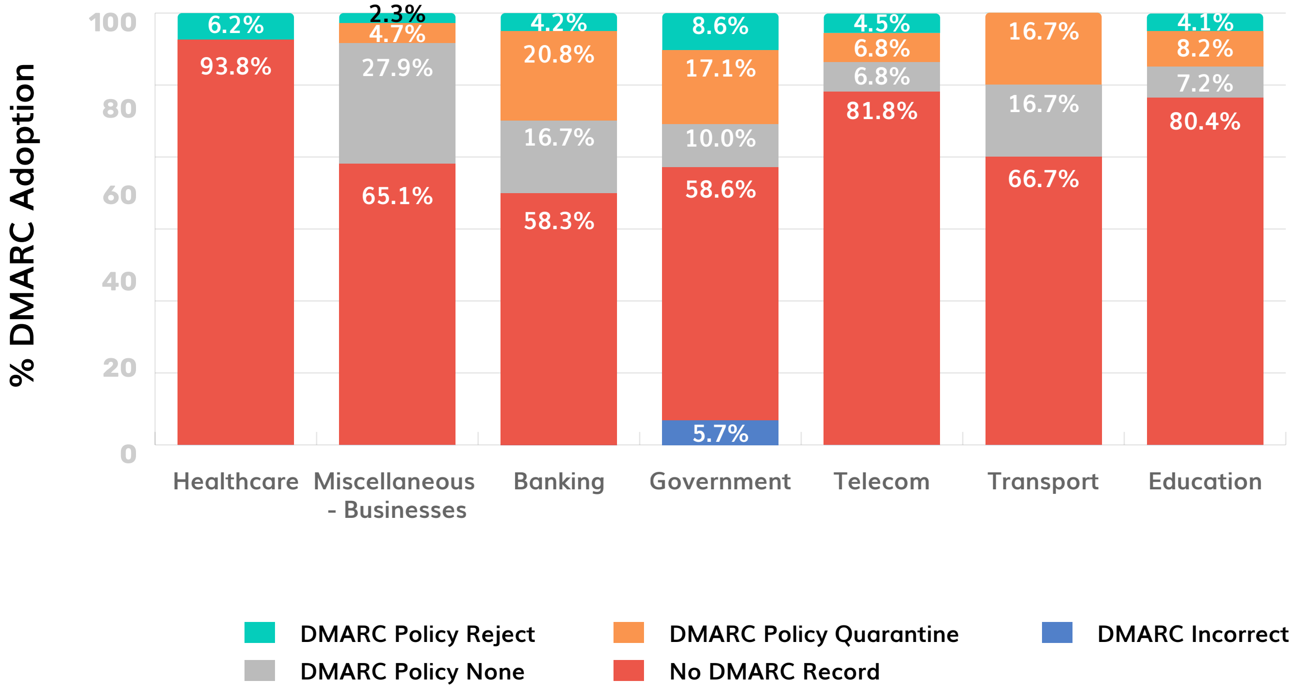
### DNSSEC Adoption



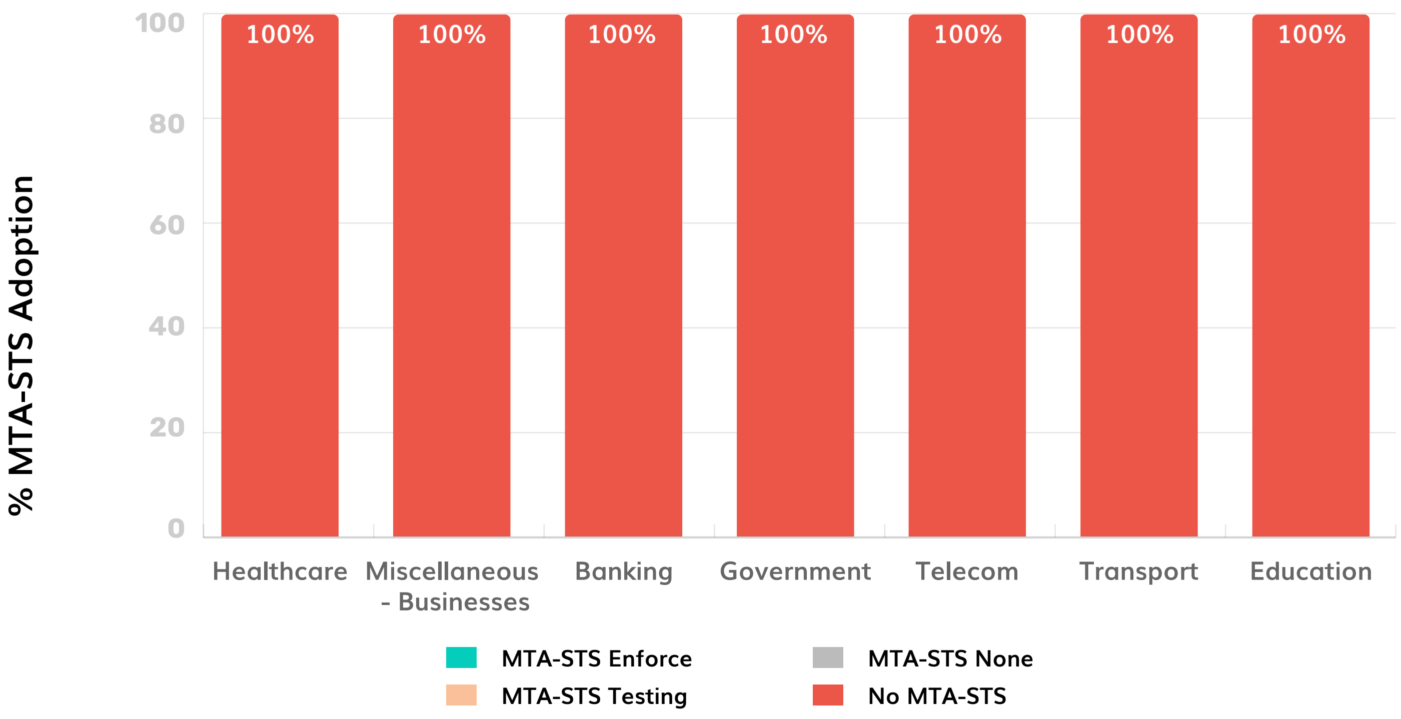
# Comparative Analysis of SPF Adoption among Different Sectors in Burma



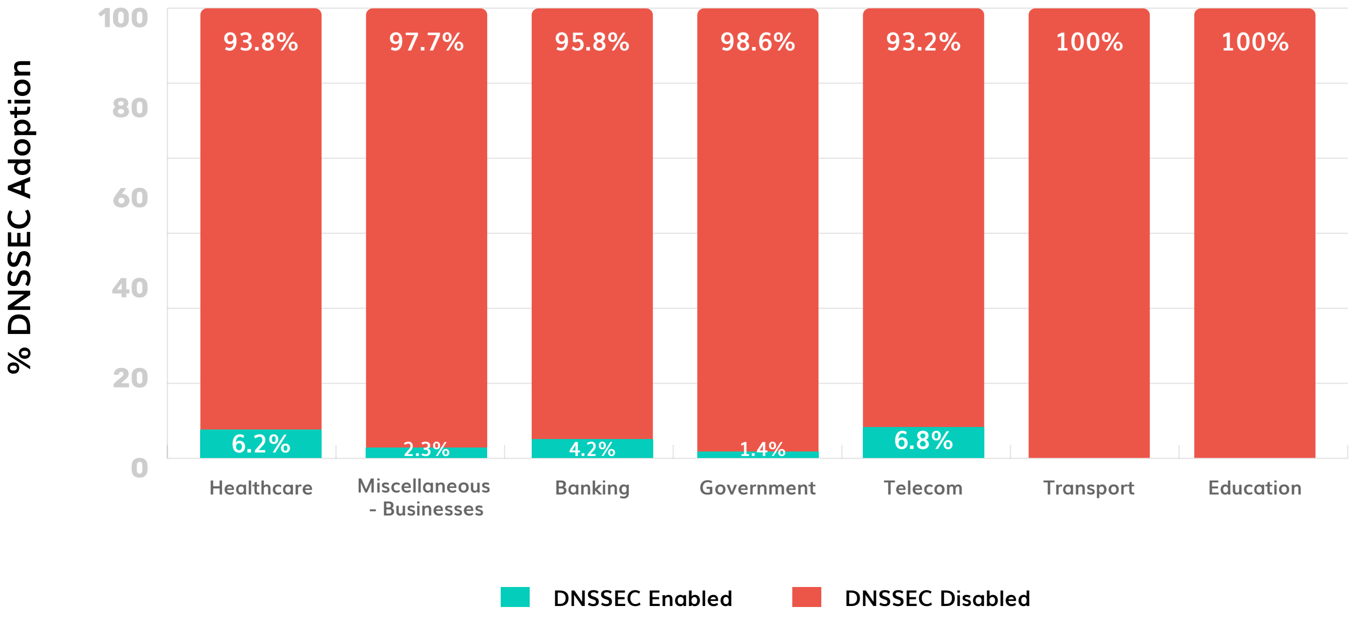
# Comparative Analysis of DMARC Adoption among Different Sectors in Burma



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



# Comparative Analysis of DNSSEC Adoption among Different Sectors in Burma



# DMARC & MTA-STS Adoption Rates: Key Statistics

- **More than 80%** of organizations in the Burma Healthcare sector **do not have DMARC implemented.**
- **More than 93%** of Burma Telecommunication entities **are not protected against spoofing attacks.**
- **More than 80%** of Burma Healthcare institutions **do not have SPF implemented.**
- The Government sector shows a significant lack of DMARC records, with **only 25 out of 70 domains being compliant.**
- Overall, **105 domains lack SPF records**, indicating a vulnerability to email spoofing.
- Only **80 out of 300 domains** have **DMARC correctly configured**, highlighting a critical area for improvement in email security.
- No business domains have MTA-STS enabled.

# Critical Errors Organizations in Burma Are Making

From the above analysis, we have identified numerous critical errors that organizations in Burma are making regarding the implementation of email authentication protocols. Here are some key highlights:

1. MTA-STS configuration is lacking significantly.

2. The DMARC implementation rates are very low in sectors as important as healthcare and education.

3. The SPF configuration rates are also low.

4. SPF and DMARC configurations include numerous errors.

5. There is widespread use of overly permissive DMARC policies (i.e. p=none).

6. DNSSEC is completely disabled for domains in certain sectors, leaving domains vulnerable to DNS-based attacks.

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

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

1 Ensure effective MTA-STS configuration.

2 Make sure you are within SPF lookup limits and try to avoid SPF void errors.

3 To avoid syntax errors, you can use automated tools for error-free SPF, DMARC, and MTA-STS record generation.

4 Pay attention to publishing one DMARC record as well as one SPF record per domain.

5 Make a gradual/phased transition from p=none to p=reject DMARC policy while monitoring reports.

6 Enable MTA-STS and TLS-RPT to protect yourself against MITM attacks.

7 Activate DNSSEC will help you secure DNS responses.

# How Can PowerDMARC Help?

We offer targeted email security and authentication services for wide-ranging internet protocols, such as DMARC, SPF, DKIM, MTA-STS, TLS-RPT, and BIMI. We also give our clients detailed DMARC reports that can be easily read and understood by humans.

Please feel free to get in touch with us at support@powerdmarc.com and learn about the numerous ways in which we can help protect your domain and business from malicious cyberattacks!