

# Sweden DMARC & MTA-STS Adoption Report 2025



POWERDMARC

# Sweden DMARC & MTA-STS Adoption Report 2025



- ▶ Sweden is one of the most well-connected countries not only in Europe but also in the rest of the world. More than 98% of the Swedish population has internet access. While this is a good thing with numerous benefits for the population, the very high number of connected devices may serve as an ample ground for cybercrimes. Since 2019, ransomware attacks have increased by 144% and grown into Triple Extortion.
- ▶ This makes Sweden one of the most vulnerable countries in terms of the multitude of attacks and the cost of cybercrime. In December 2020, the Swedish government made an announcement about the formation of a National Cyber Security Center. The center is currently in the process of compiling targeted cooperation structures with various sectors, including energy, transportation, and telecommunication.
- ▶ This report will explore the cybersecurity landscape in Sweden, with an emphasis on analyzing the adoption levels of DMARC, SPF, MTA-STS, and DNSSEC email authentication protocols. After the analysis, we will then proceed to identify existing security gaps and offer suggestions on how to best improve the cybersecurity landscape in the country.

## Assessing the Threat Landscape

PowerDMARC's Sweden DMARC and MTA-STS Adoption Report 2025 will focus on the following important issues:

- ▶ What are the current adoption rates of SPF and DMARC in Sweden?
- ▶ How does MTA-STS adoption differ from one sector to another?
- ▶ To what extent do domains in the different sectors in Sweden enable DNSSEC?
- ▶ What measures can Sweden take to improve digital security in the country?
- ▶ What are the variations in exposure and vulnerability toward cyberattacks among different sectors?

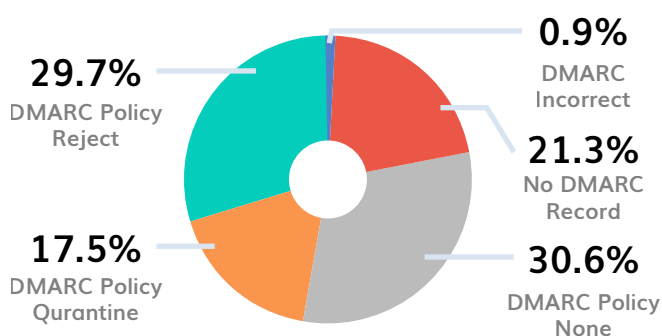
# Sectors Analyzed

Total domains analyzed: 700

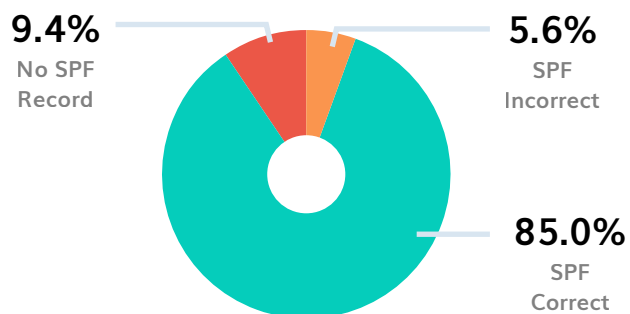
- ▶ Banking
- ▶ Education
- ▶ Government
- ▶ Healthcare
- ▶ Media
- ▶ Telecommunications
- ▶ Transport

## What Do the Numbers Say?

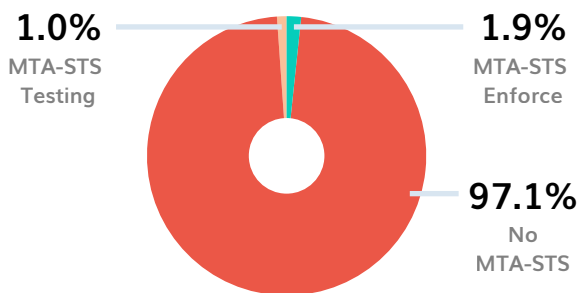
### DMARC Distribution in Sweden



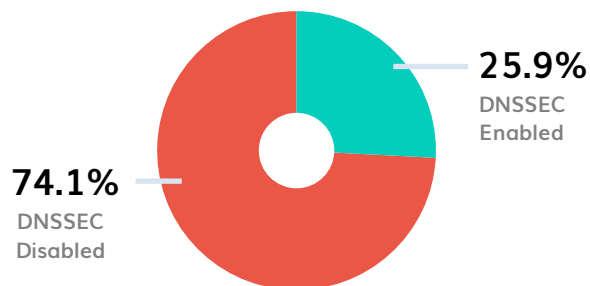
### SPF Distribution in Sweden



### MTA-STS Distribution in Sweden



### DNSSEC Distribution in Sweden



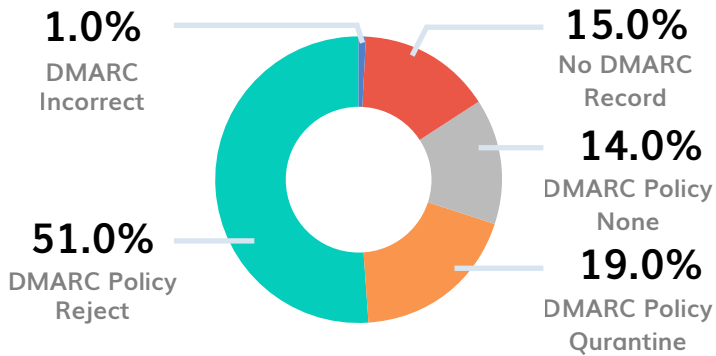
# Key findings:

- ▶ 85% of domains have correctly implemented SPF records.
- ▶ 77.86% of domains have correctly implemented DMARC.
- ▶ 29.86% have implemented a "Reject" policy, which offers the strongest protection.
- ▶ Only 2.86% of domains have valid MTA-STS records.
- ▶ 97.14% of domains have not implemented MTA-STS.
- ▶ 74.14% of domains have not implemented DNSSEC.

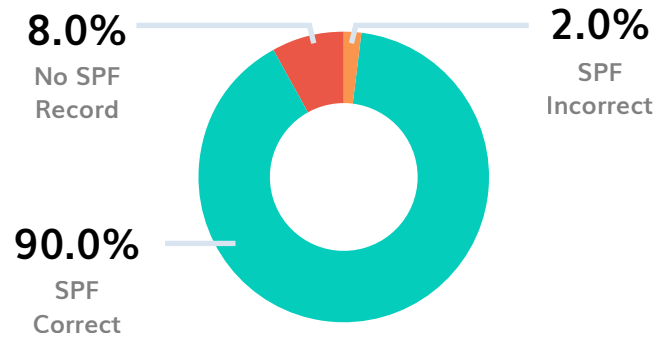
## Sector-wise Analysis of Domains in Thailand

### Banking

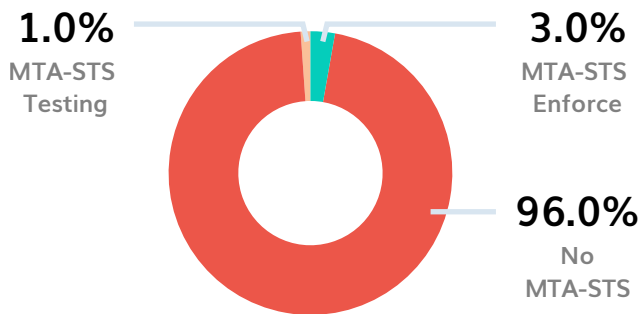
#### DMARC Adoption



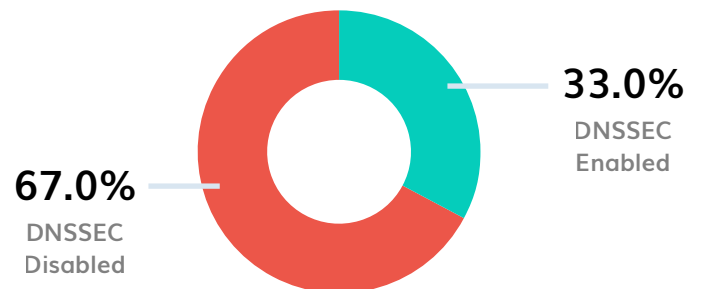
#### SPF Adoption



#### MTA-STS Adoption



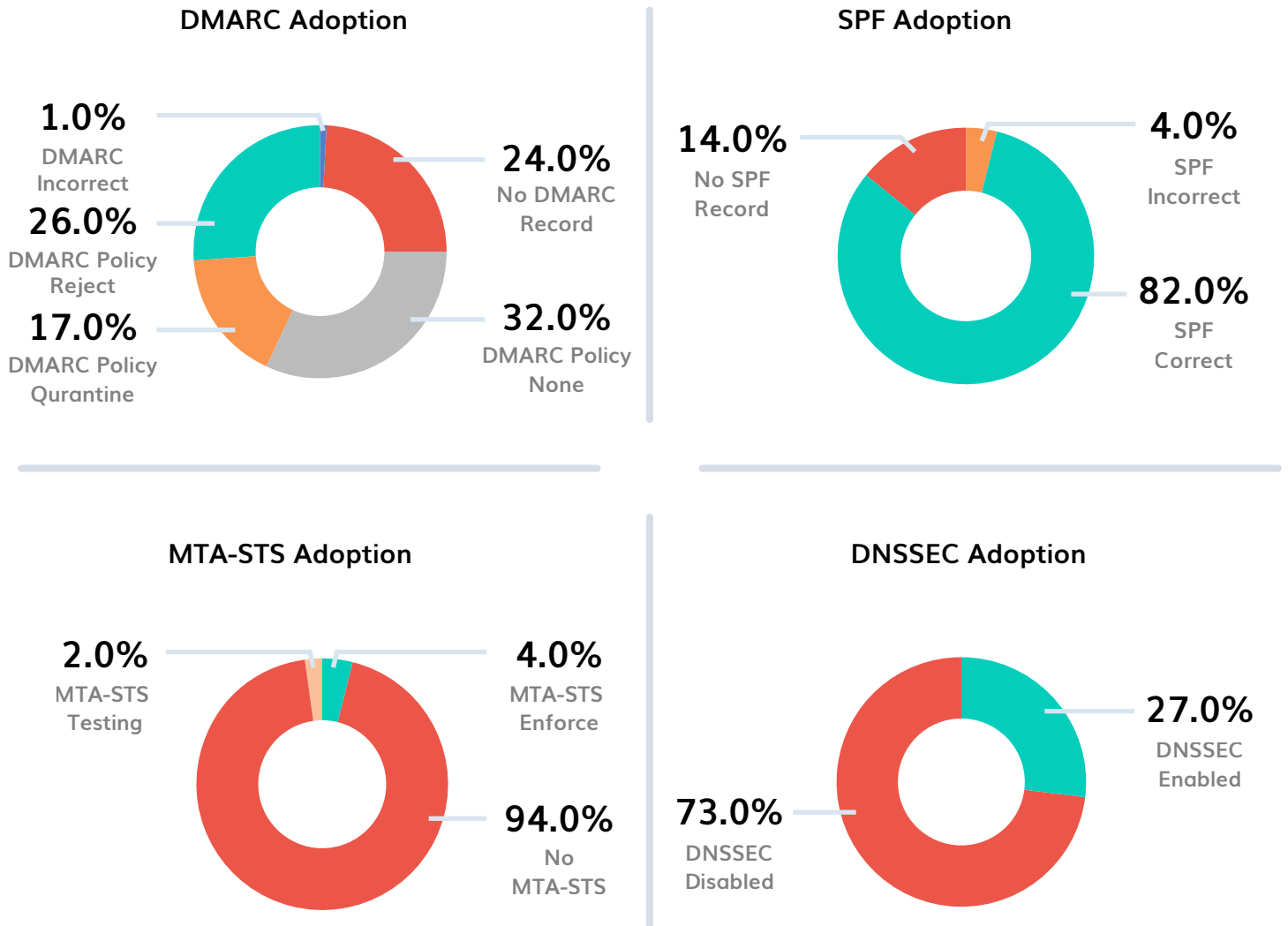
#### DNSSEC Adoption



# Key findings:

- ▶ Demonstrates the highest DMARC adoption rate at 84%.
- ▶ Has the highest rate of DMARC "Reject" policy implementation at 51%.
- ▶ Shows strong SPF adoption with 90% correct implementation.

## Education

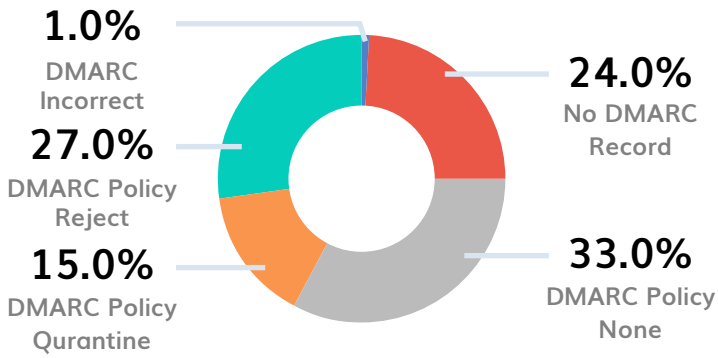


# Key findings:

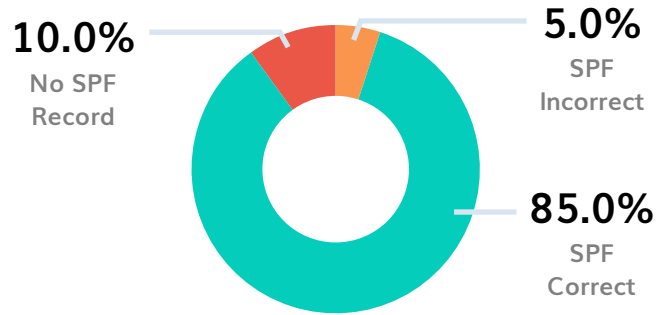
- ▶ Has a DMARC adoption rate of 75%.
- ▶ 32% of domains use a DMARC "None" policy, indicating a cautious approach.
- ▶ SPF adoption is solid at 82% correct implementation.

# Government

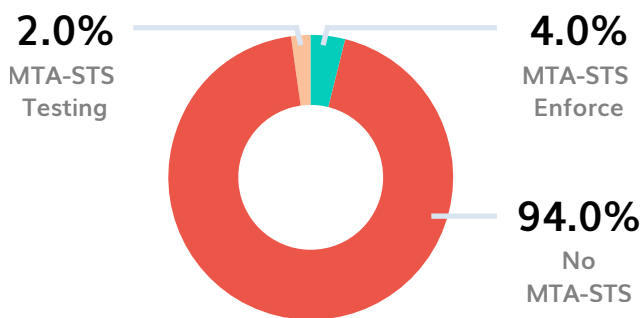
### DMARC Adoption



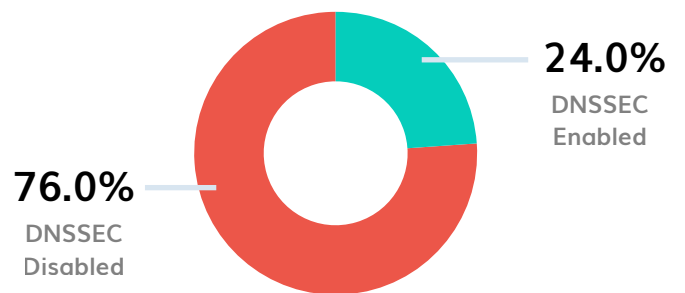
### SPF Adoption



### MTA-STS Adoption



### DNSSEC Adoption

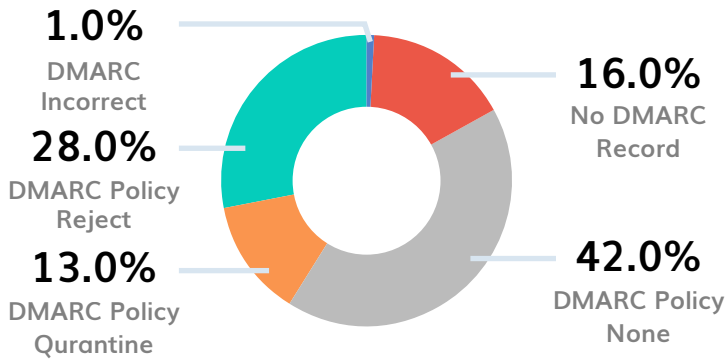


## Key findings:

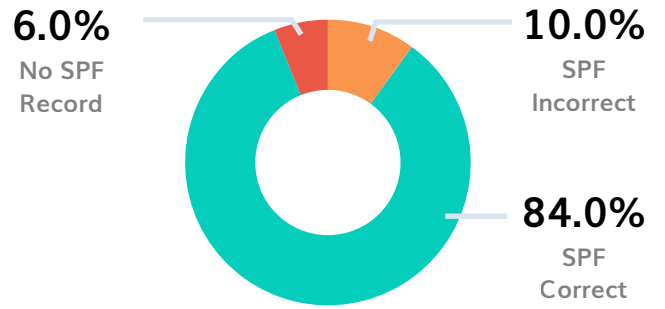
- ▶ Matches the education sector with a 75% DMARC adoption rate.
- ▶ Has a balanced DMARC policy distribution with 33% "None," 15% "Quarantine", and 27% "Reject."
- ▶ Shows strong SPF adoption at 85% correct implementation.

# Healthcare

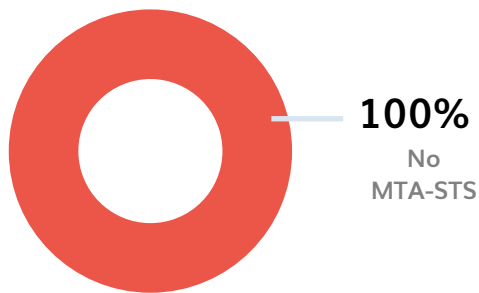
### DMARC Adoption



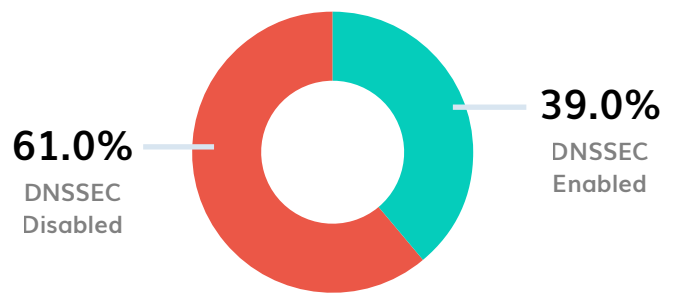
### SPF Adoption



### MTA-STS Adoption



### DNSSEC Adoption

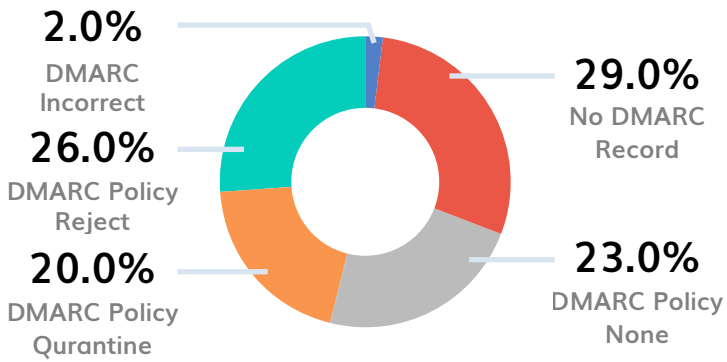


## Key findings:

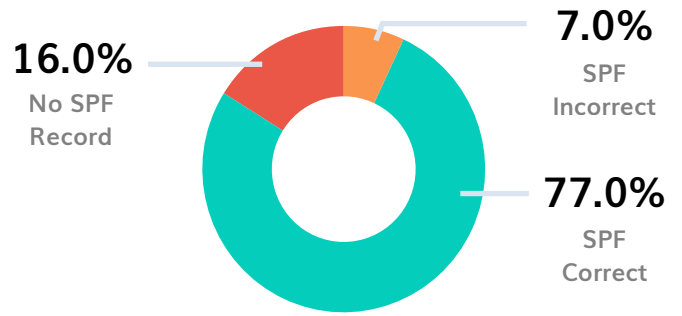
- ▶ Has a high DMARC adoption rate of 83%.
- ▶ Shows the highest use of DMARC "None" policy at 42%, suggesting a conservative approach.
- ▶ Demonstrates good SPF adoption at 84% correct implementation.

## Media

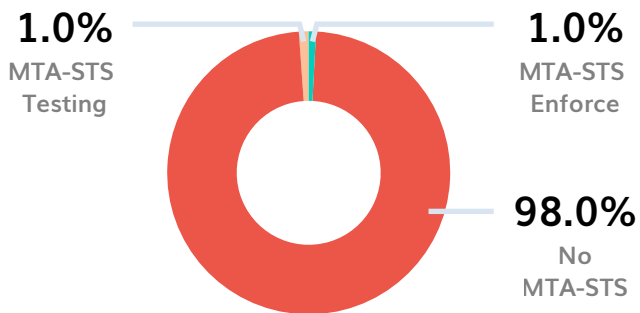
### DMARC Adoption



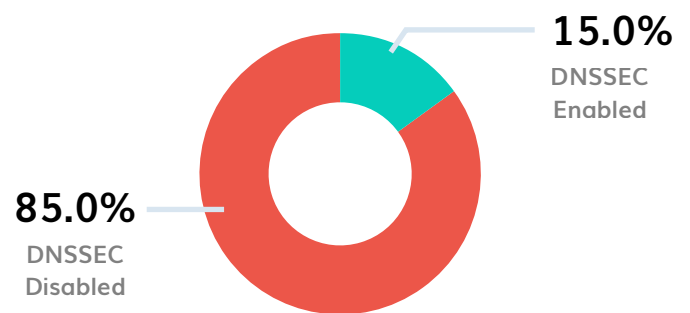
### SPF Adoption



### MTA-STS Adoption



### DNSSEC Adoption



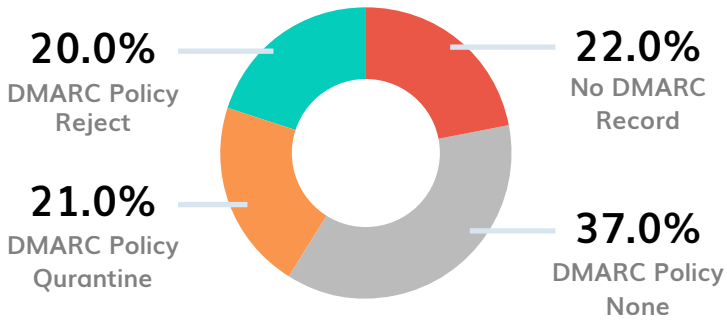
## Key findings:

- ▶ Has the lowest DMARC adoption rate at 69%.
- ▶ Shows the lowest correct SPF implementation at 77%.
- ▶ Has the highest rate of no SPF record at 16%.

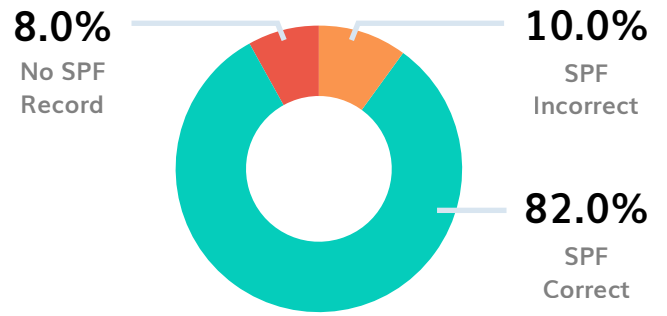


# Telecommunications

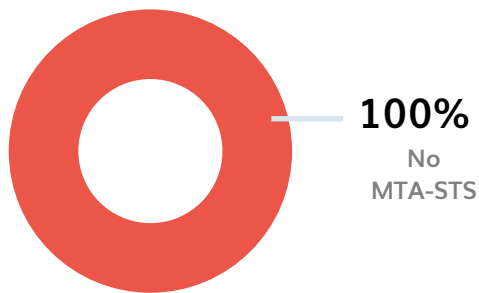
### DMARC Adoption



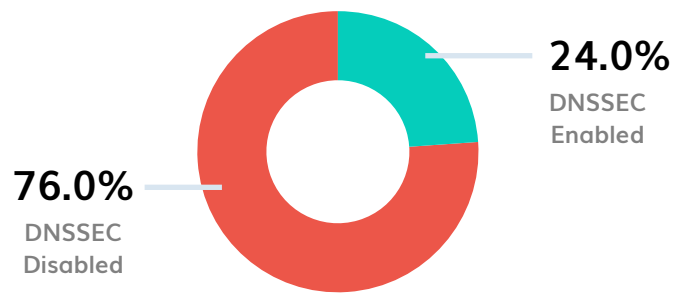
### SPF Adoption



### MTA-STS Adoption



### DNSSEC Adoption

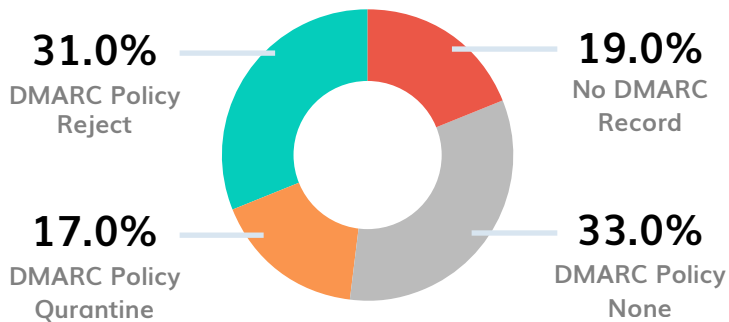


## Key findings:

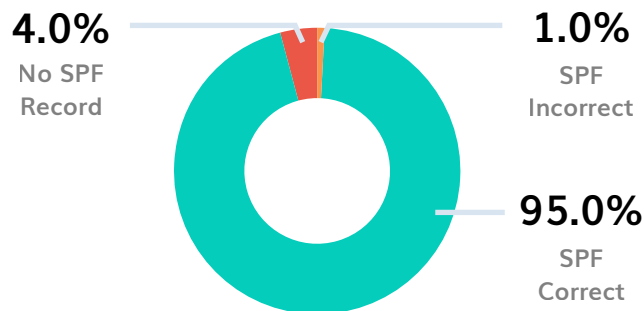
- ▶ Has a DMARC adoption rate of 78%.
- ▶ Shows a balanced DMARC policy distribution with a slight preference for "None" policy at 37%.
- ▶ Demonstrates good SPF adoption at 82% correct implementation.

# Transport

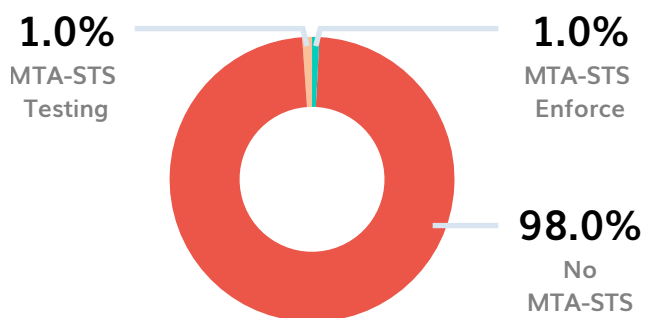
### DMARC Adoption



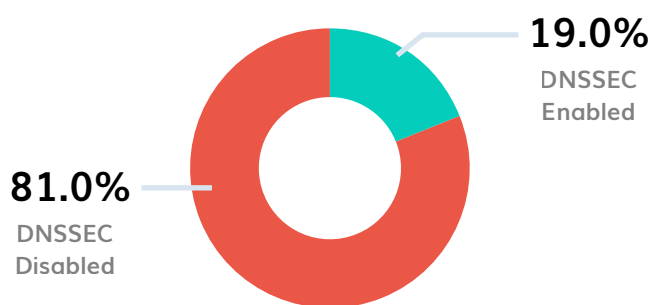
### SPF Adoption



### MTA-STS Adoption



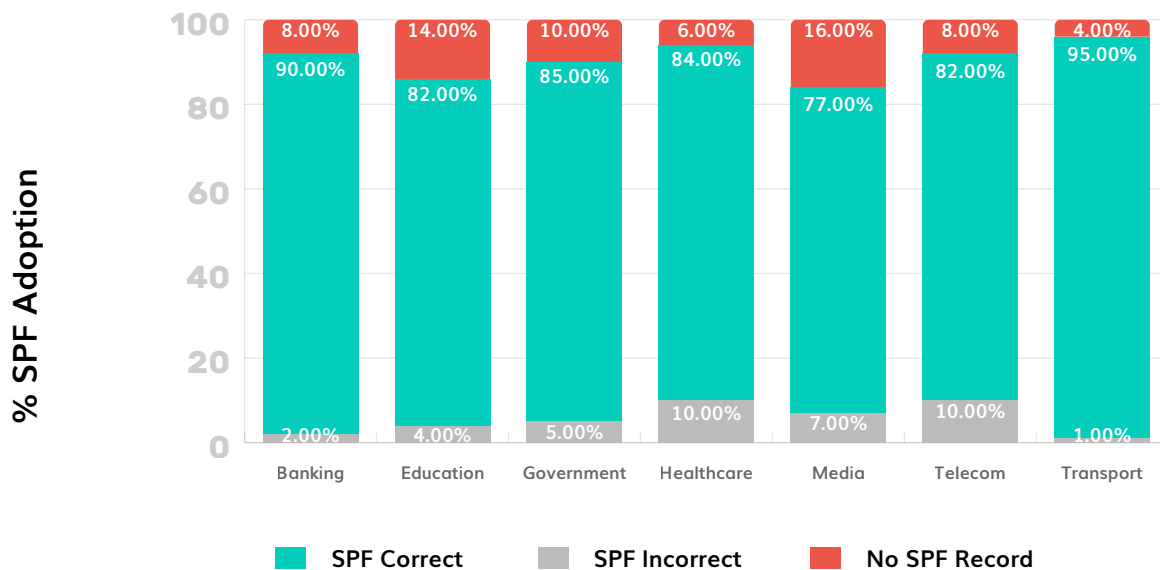
### DNSSEC Adoption



## Key findings:

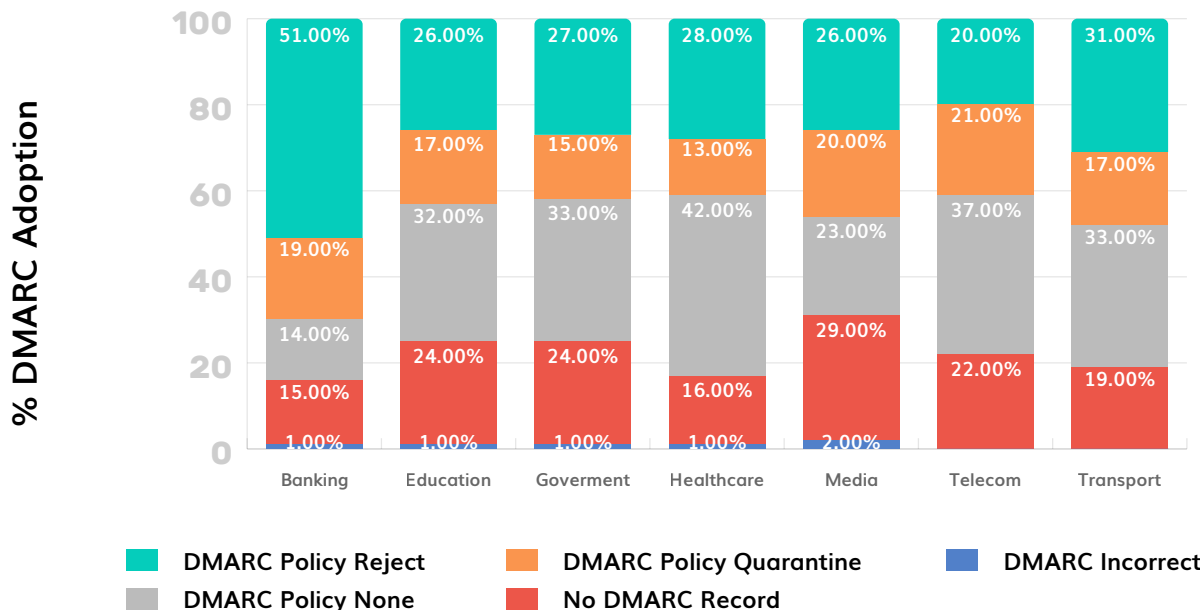
- ▶ Shows the highest correct SPF implementation at 95%.
- ▶ Has a high DMARC adoption rate of 81%.
- ▶ Demonstrates a balanced DMARC policy distribution with a slight preference for "None" policy at 33%.

# Comparative Analysis of SPF Adoption among Different Sectors in Sweden



The adoption rate for SPF was the lowest in the Swedish Media sector at 77%. The highest rate of SPF adoption was noted in the Swedish Transport sector at 95%, followed by the Banking sector at 90%.

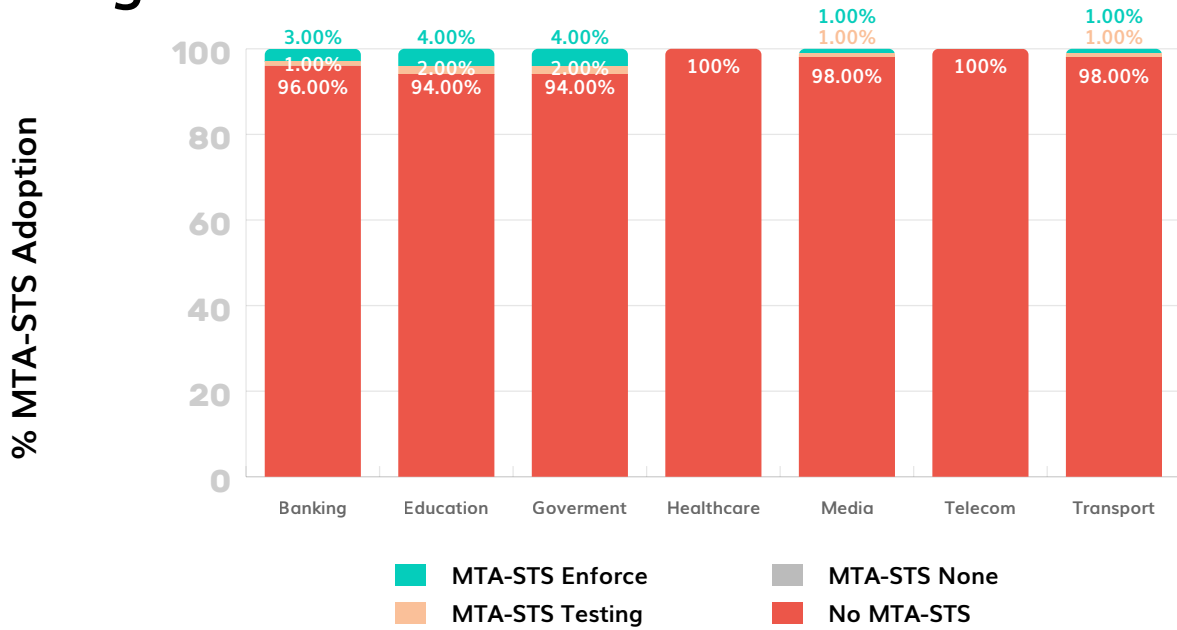
# Comparative Analysis of DMARC Adoption among Different Sectors in Sweden



DMARC adoption was highest in the Swedish Banking sector at 84%, while the Media sector was behind with the lowest adoption rate of 69%.

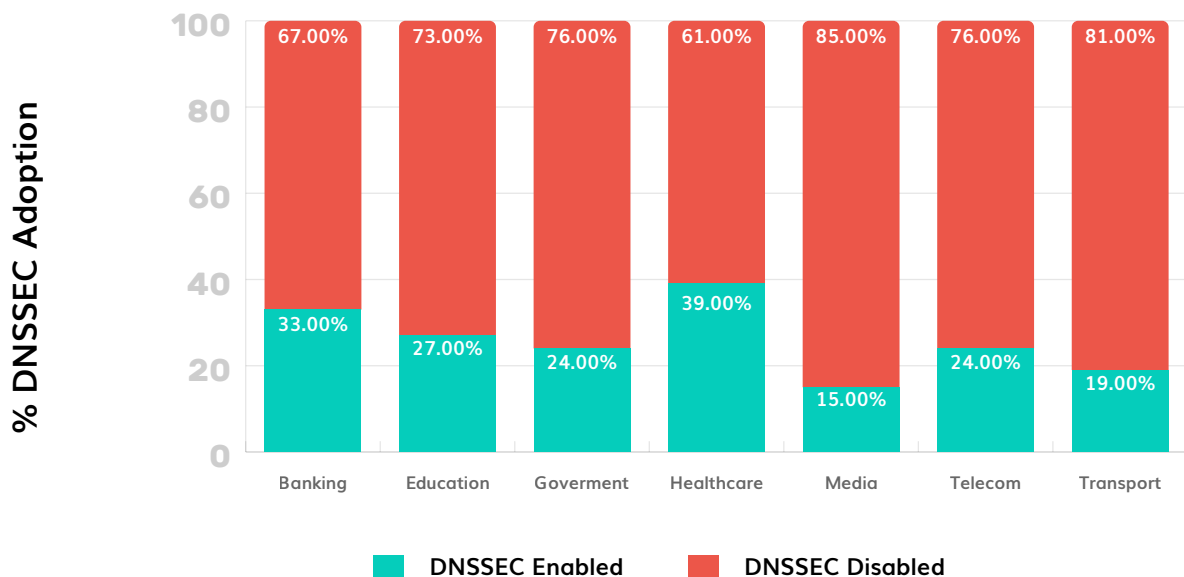
The Swedish Banking sector leads the charge in implementing the strictest DMARC policy ("reject") at 51%, Swedish higher than other sectors. The Telecommunications sector had the lowest "Reject" policy implementation at 20%

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



MTA-STS adoption was generally low across all sectors. The Education and Government sectors showed the highest adoption at 6%, while the Healthcare and Telecommunications sectors had no MTA-STS implementation at all.

# Comparative Analysis of DNSSEC Adoption among Different Sectors in Sweden



MTA-STS adoption was generally low across all sectors. The Education and Government sectors showed the highest adoption at 6%, while the Healthcare and Telecommunications sectors showed no MTA-STS implementation on analysis.

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

- ▶ Over 85.00% of Swedish domains have correctly implemented SPF records.
- ▶ 77.86% of domains have correct DMARC records. However, as many as 21.29% of Swedish domains still lack DMARC implementation.
- ▶ Among domains with DMARC, the policy distribution is fairly balanced:
  - 30.57% have a policy set to "none." This provides only minimal protection.
  - 29.86% have a "reject" policy. This provides maximum protection against email-based attacks
  - 17.43% use a "quarantine" policy. This ensures intermediate protection.
- ▶ MTA-STS adoption is very low. As many as 97.14% of Swedish domains lack this important layer of email security.
- ▶ DNSSEC implementation is limited. Only 25.86% of domains have it enabled, while 74.14% have it disabled.

## Critical Errors Organizations in Sweden Are Making

### ▶ SPF & DMARC Implementation Errors

While SPF and DMARC adoption rates among Swedish domains were quite high, common errors included:

- SPF records exceeding the 10 DNS lookup limit
- SPF records exceeding void limits
- Syntax errors
- Configuration errors

### ▶ Adoption of Permissive DMARC Policies

More than 70% of Swedish domains use no-action DMARC policies like "none". This leaves them vulnerable to cyber attacks.

### ▶ Lack of Support for Advanced Protocols

MTA-STS and BIMI adoption rates are very low across all sectors. The education and government sectors have the highest adoption rate, still only at 6%. The healthcare and telecommunications sectors have 0% MTA-STS adoption.

### ▶ Limited Support for DNSSEC

DNSSEC adoption rates were also analyzed to be considerably low among Swedish sectors. This left the domains vulnerable to DNS spoofing attacks.

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

- 1 A common mistake among domain owners in Sweden is keeping their DMARC policy at "none," which offers minimal protection against spoofing and BEC. For stronger security, they must enforce DMARC with a stricter policy like p=reject or p=quarantine to prevent domain impersonation effectively.
- 2 SPF and DMARC records were not implemented for many entities across different sectors in Sweden. Not only does the lack of these records expose domains to spoofing and phishing attacks, but it can also result in major compliance problems and email deliverability issues for Gmail and Yahoo senders. DMARC compliance is also mandatory for businesses handling/processing card payments under PCI DSS 4.0.
- 3 There was a significant lack of MTA-STS and TLS-RPT records for many of the analyzed domains. To ensure the effective prevention of man-the-middle attacks, it's important to address this major security gap.
- 4 Other recommendations include:
  - a) Staying within the 10 DNS lookup limit for SPF
  - b) Ensuring SPF and DMARC records do not contain errors
  - c) Avoiding the implementation of multiple SPF/DMARC records per domain
  - d) Implementing advanced layers of security like BIMI and MTA-STS



# How Can PowerDMARC Help?



PowerDMARC offers comprehensive, full-stack email authentication SaaS services that combine DMARC, SPF, DKIM, BIMI, MTA-STS, and TLS-RPT solutions. Our global team of cybersecurity experts helps MSPs, MSSPs, organizations, and governmental entities prevent email threats before it's too late!

If you are looking for professional guidance for configuring email authentication protocols without the hassle or technical complexity and improving email deliverability for you or your clients - try PowerDMARC today!

Contact the PowerDMARC team at [support@powerdmarc.com](mailto:support@powerdmarc.com) to book a 1:1 platform demo and explore our services. We can protect your next email from yet another hacker!