Norway DMARC & MTA-STS Adoption Report 2025

POWERDMARC

Norway DMARC & MTA-STS Adoption Report 2025

- In Norway, phishing and other forms of social engineering fraud are on the rise, with 18% of Norwegians reporting they or a family member has been affected by financial fraud or identity theft in the past year. This represents roughly 800,000 individuals, according to Insurance Edge.
- Email authentication plays a critical role in reducing email fraud by verifying identities and preventing unauthorized access.
- Explore the latest stats below in Norway's 2025 DMARC and MTA-STS Adoption Report by PowerDMARC.

Assessing the Threat Landscape

PowerDMARC's Norway DMARC and MTA-STS Adoption Report 2025 will address the following key questions:

- How successful has Norway been in implementing SPF and DMARC across public and private sector domains?
- What is the current rate of MTA-STS adoption among Norwegian organizations?
- Which industries in Norway face the highest risk from phishing, spoofing, and email-delivered threats?
- What are the most common configuration errors or gaps in email authentication practices across Norwegian domains?
- What specific measures should Norwegian domain owners take to strengthen email integrity and comply with the national security framework?

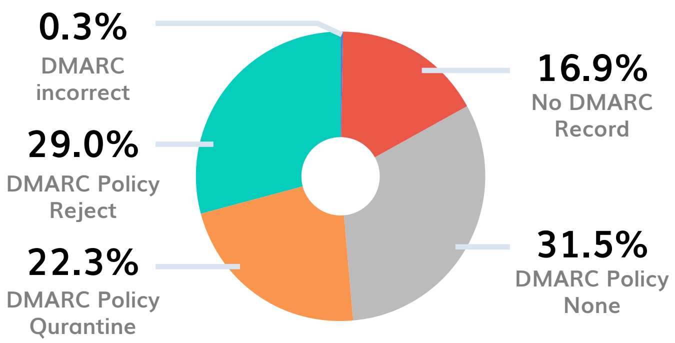
Sectors Analyzed

Total domains analyzed: 641

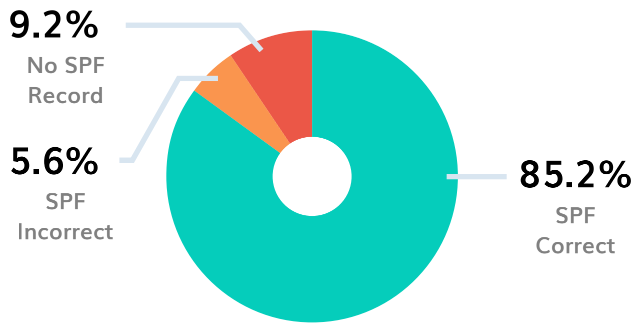
- Telecommunications
- Education
- Government
- Other
- Financial
- Healthcare
- Transport

What Do the Numbers Say?

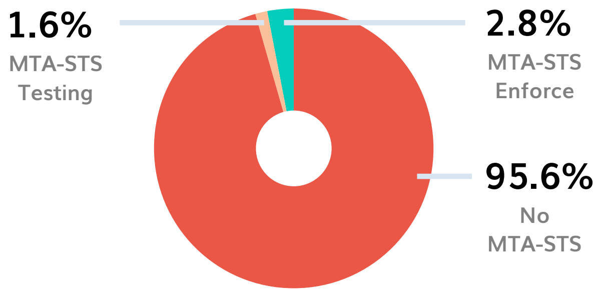
DMARC Distribution in Norway



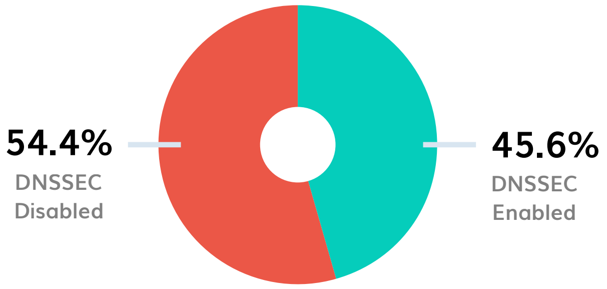
SPF Distribution in Norway



MTA-STS Distribution in Norway



DNSSEC Distribution in Norway



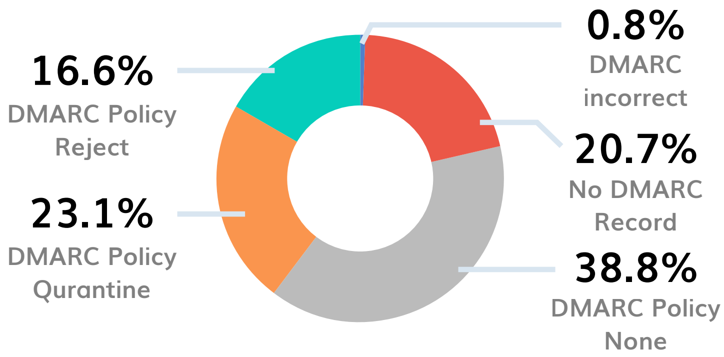
Key Findings:

- 85.2% of Norwegian domains have correct SPF records.
- 29.0% of domains have implemented a DMARC “Reject” policy.
- 16.9% of domains have no DMARC record.
- 95.6% have not deployed MTA-STS.
- 45.6% of domains have DNSSEC enabled.

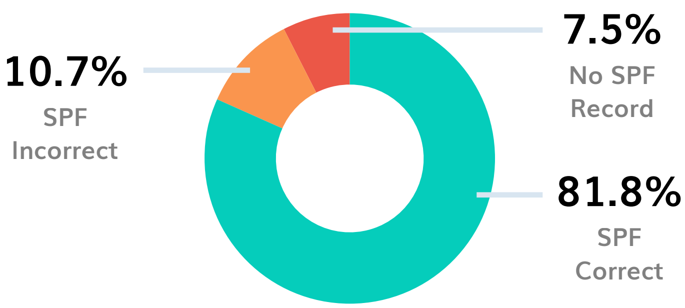
Sector-wise Analysis of Domains in Norway

Telecommunications

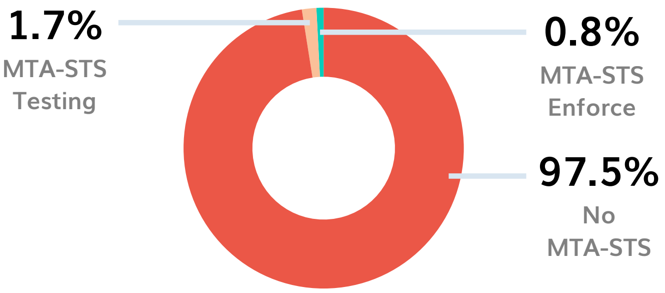
DMARC Adoption



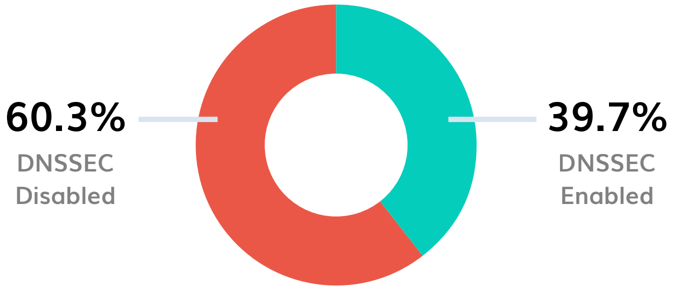
SPF Adoption



MTA-STS Adoption



DNSSEC Adoption

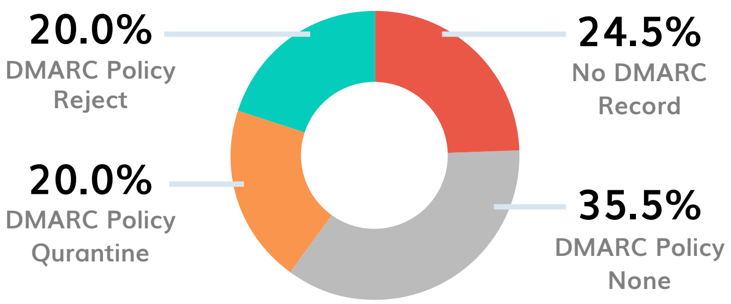


Key Findings:

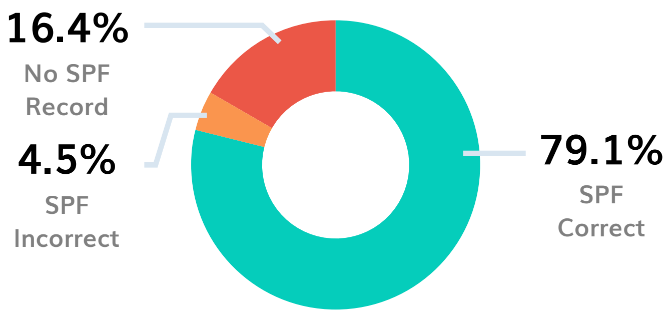
- 81.8% of telecommunications domains have correct SPF records.
- Only 16.6% of domains have implemented a DMARC "Reject" policy.
- 20.7% of domains have no DMARC record.
- 97.5% of domains have not deployed MTA-STS.
- 39.7% of domains have DNSSEC enabled.

Education

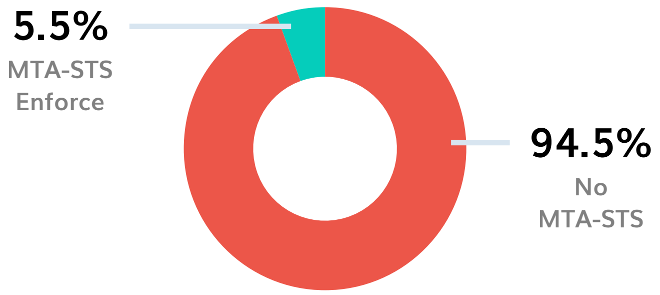
DMARC Adoption



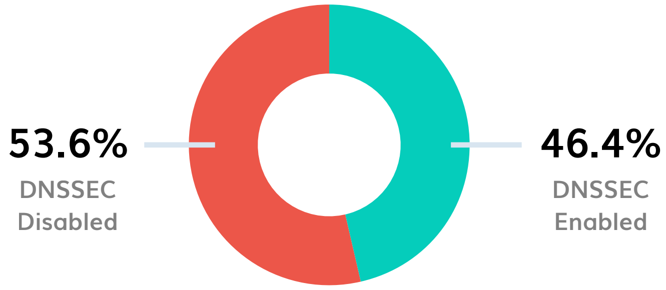
SPF Adoption



MTA-STS Adoption



DNSSEC Adoption

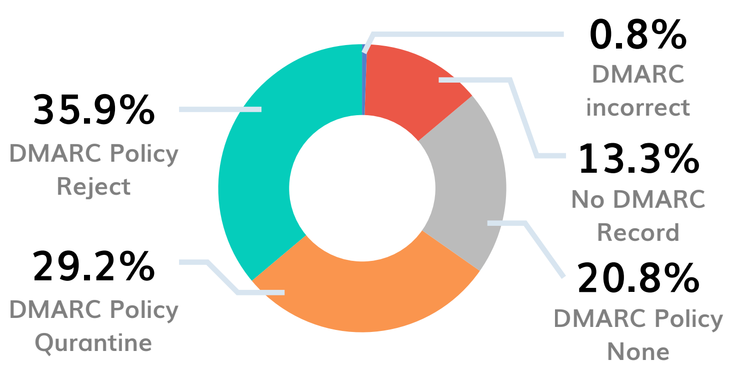


Key Findings:

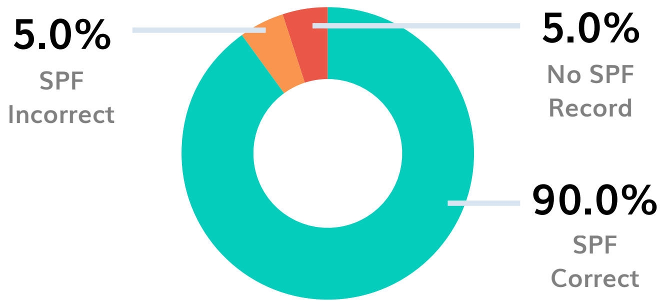
- 79.1% of education sector domains have correct SPF records.
- Only 20.0% of domains have implemented a DMARC “Reject” policy.
- 24.5% of domains have no DMARC record.
- Only 5.5% of domains have implemented MTA-STS at enforcement; the majority (94.5%) have not deployed MTA-STS.
- 46.4% of domains have DNSSEC enabled.

Government

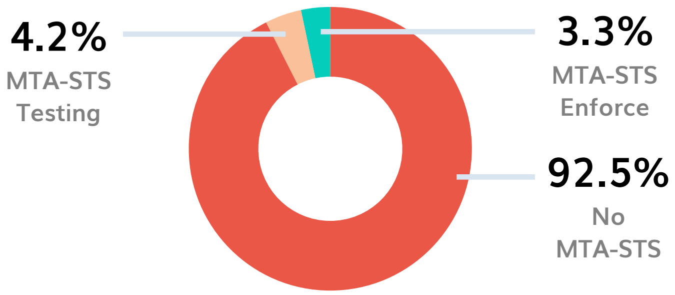
DMARC Adoption



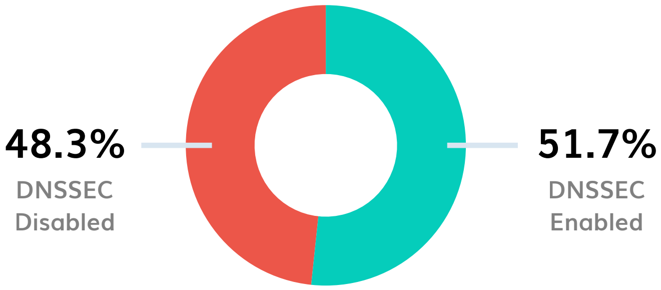
SPF Adoption



MTA-STS Adoption



DNSSEC Adoption

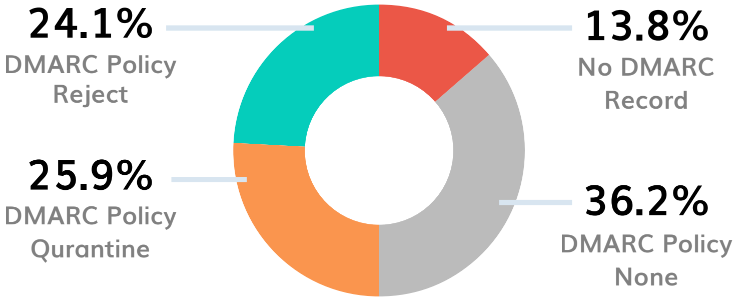


Key Findings:

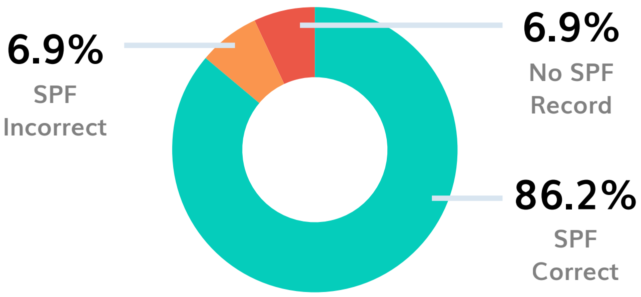
- 90.0% of government domains have correct SPF records.
- 35.9% of domains have implemented a DMARC “Reject” policy.
- 13.3% of domains have no DMARC record.
- Only 3.3% of domains have implemented MTA-STS at enforcement. The majority (92.5%) have not deployed MTA-STS.
- 51.7% of domains have DNSSEC enabled.

Other

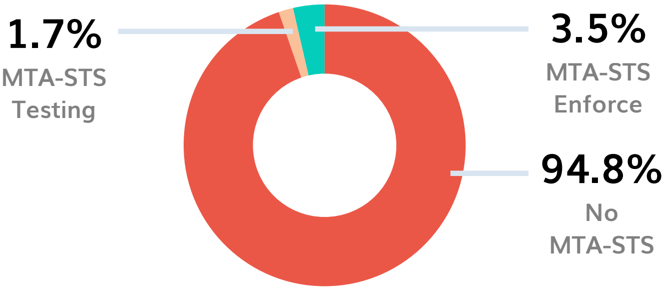
DMARC Adoption



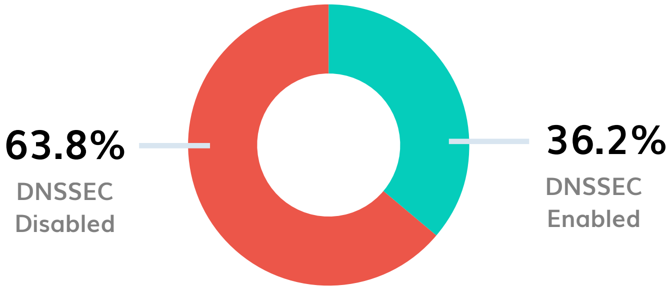
SPF Adoption



MTA-STS Adoption



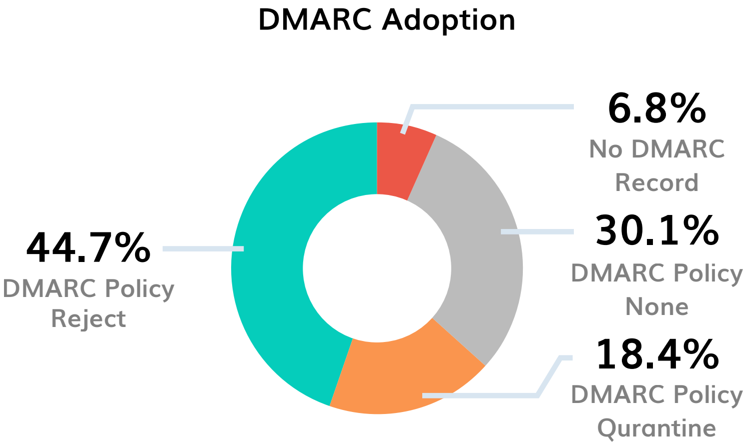
DNSSEC Adoption

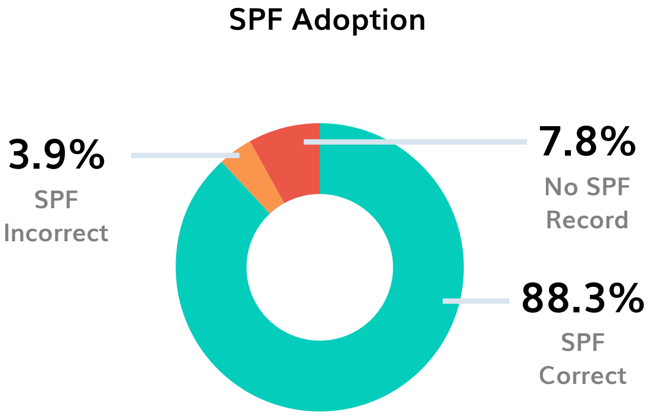


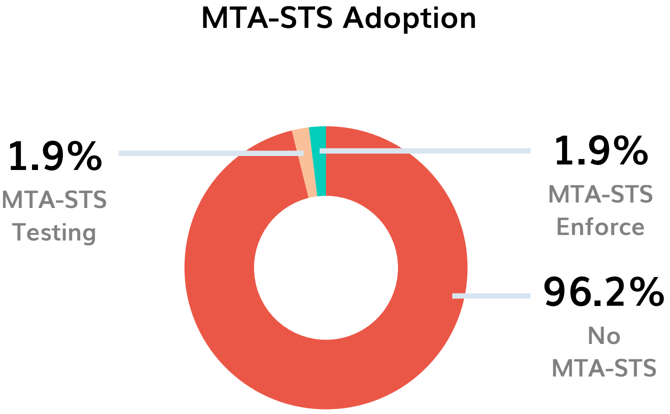
Key Findings:

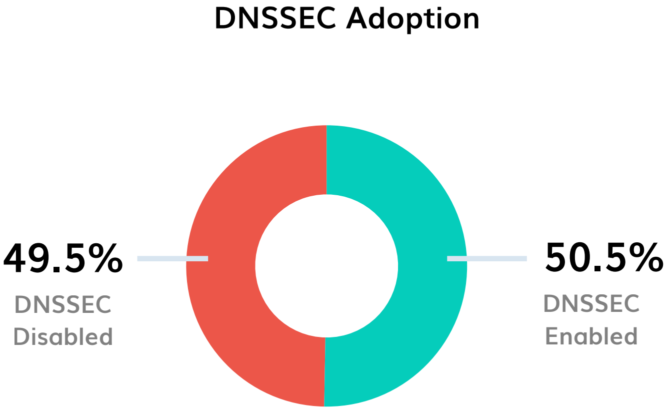
- 86.2% of domains in the 'Other' sector have correct SPF records.
- 24.1% of domains have implemented a DMARC "Reject" policy.
- 13.8% of domains have no DMARC record.
- Only 3.5% of domains have implemented MTA-STS at enforcement. The majority (94.8%) have not deployed MTA-STS.
- 36.2% of domains have DNSSEC enabled.

Financial







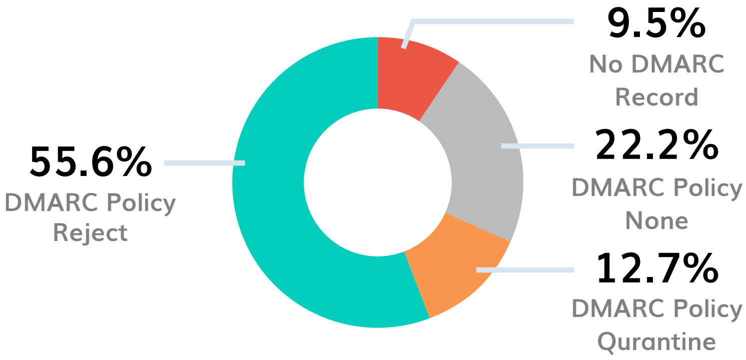


Key Findings:

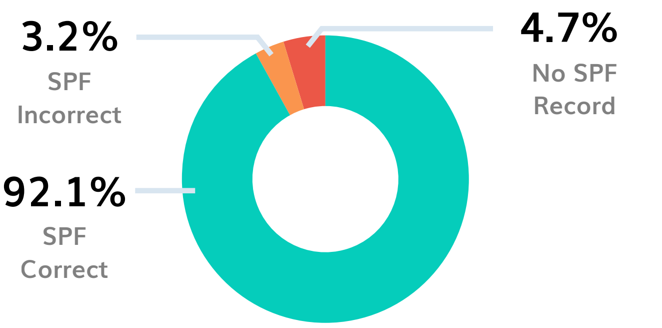
- 88.3% of finance sector domains have correct SPF records.
- 44.7% of domains have implemented a DMARC “Reject” policy.
- 6.8% of domains have no DMARC record.
- Only 1.9% of domains have implemented MTA-STS enforcement, with an additional 1.9% in testing mode. The vast majority (96.2%) have not deployed MTA-STS.
- 50.5% of domains have DNSSEC enabled.

Healthcare

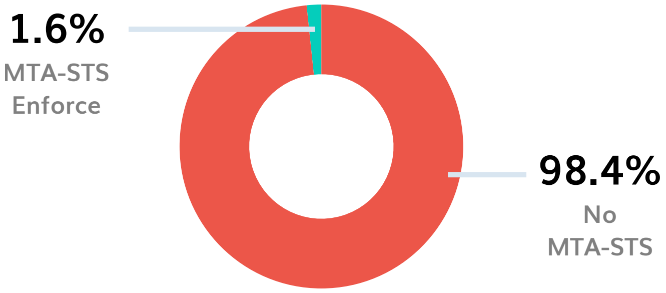
DMARC Adoption



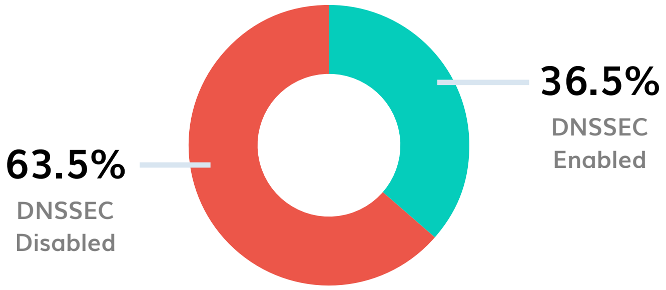
SPF Adoption



MTA-STS Adoption



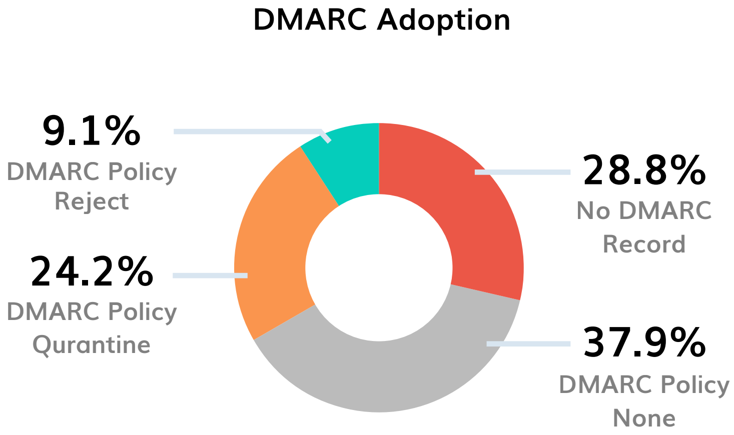
DNSSEC Adoption

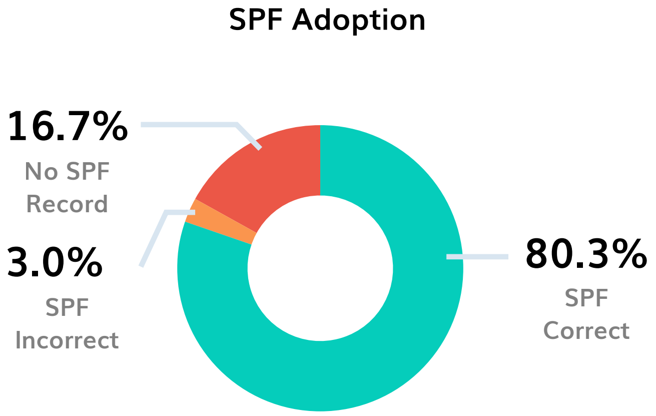


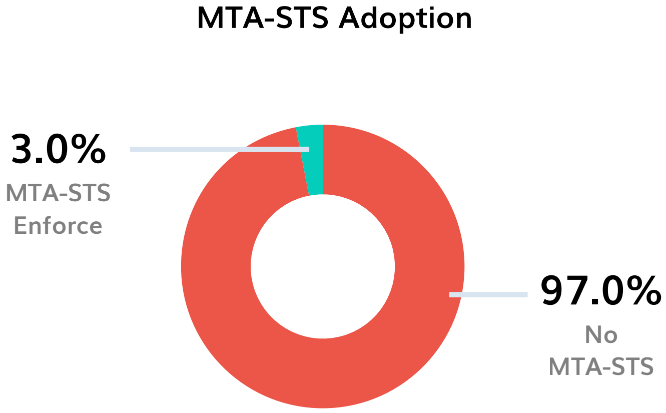
Key Findings:

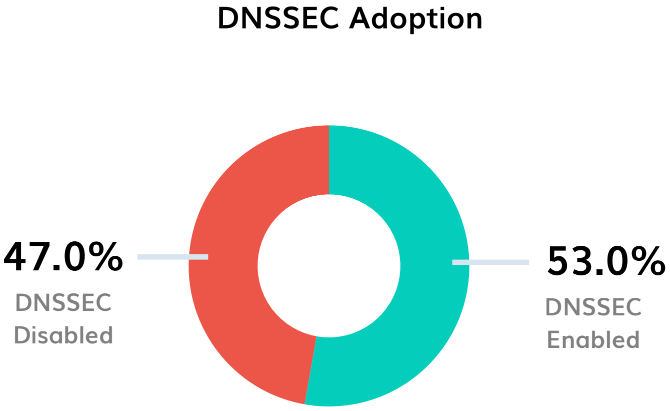
- 92.1% of healthcare sector domains have correct SPF records.
- 55.6% of domains have implemented a DMARC "Reject" policy, while 9.5% have no DMARC record.
- Adoption of MTA-STS is extremely low in this sector at only 1.6%
- 36.5% of domains have DNSSEC enabled.

Transport





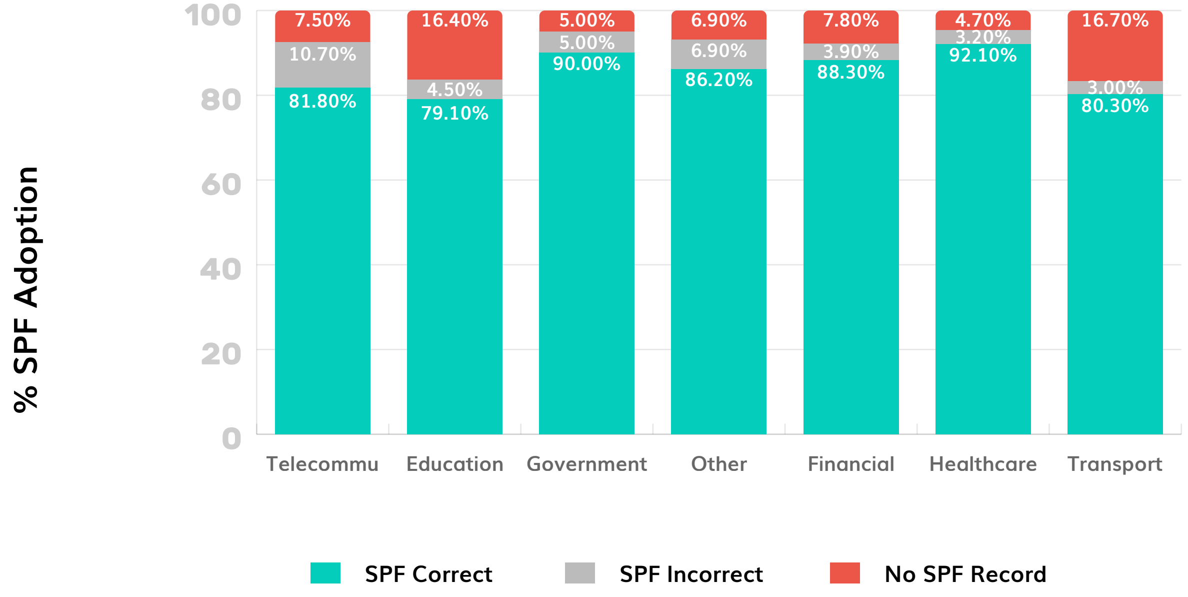




Key Findings:

- 80.3% of transport sector domains have correct SPF records.
- 9.1% of domains have implemented a DMARC "Reject" policy, while 28.8% have no DMARC record.
- 97.0% of domains have not deployed MTA-STS.
- 53.0% of domains have DNSSEC enabled.

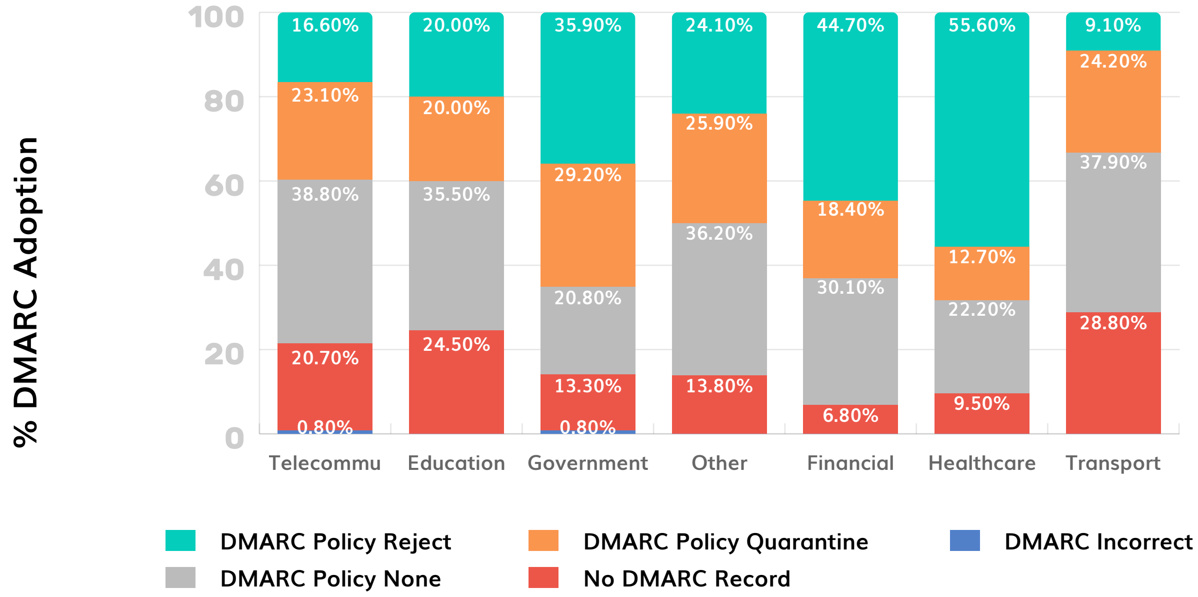
Comparative Analysis of SPF Adoption among Different Sectors in Norway



Key Findings:

*The Norwegian **Healthcare** sector has the highest rate of correct SPF implementation at **92.1%**, followed by the **Government** sector at **90.0%**. Conversely, the **Education** sector has the lowest rate of correct SPF adoption among the listed sectors, at **79.1%**.*

Comparative Analysis of DMARC Adoption among Different Sectors in Norway

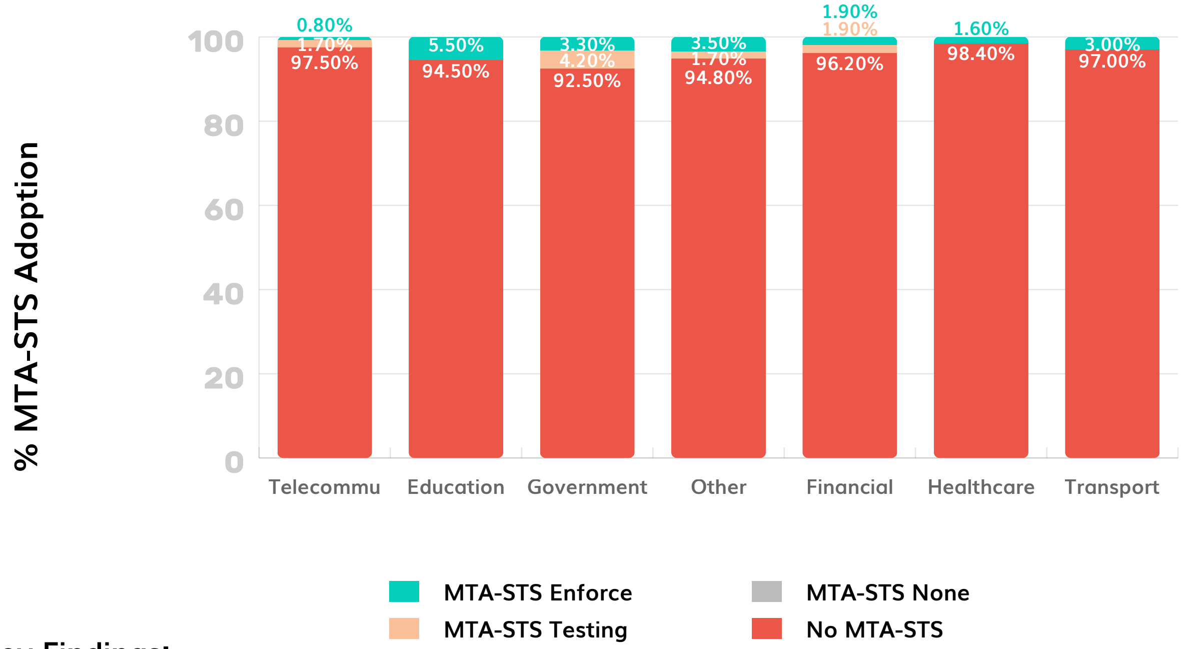


Key Findings:

*The Norwegian **Financial** sector shows the highest overall DMARC adoption; only **6.8%** of its domains lack a DMARC record. In contrast, the **Transport** sector has the lowest DMARC adoption, with **28.8%** of domains in this sector not implementing DMARC.*

*The **Healthcare** sector leads in adopting the strictest DMARC "Reject" policy, at **55.6%**. It is closely followed by the **Financial** sector (**44.7%**). By comparison, the **Transport** sector has the lowest rate of "Reject" policy adoption at **9.1%**.*

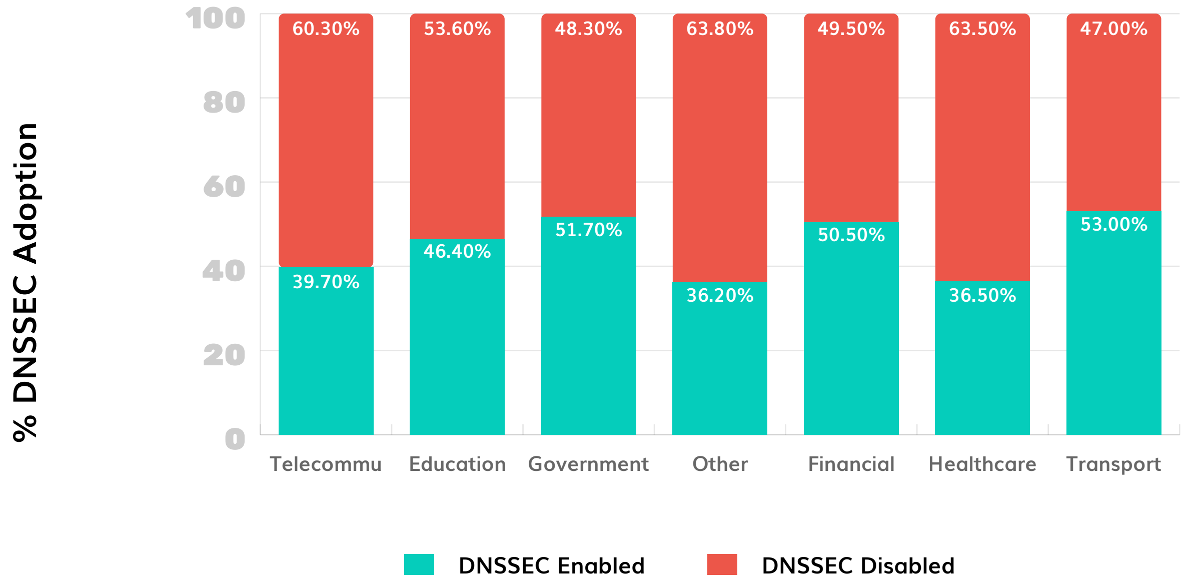
Comparative Analysis of MTA-STS Adoption among Different Sectors in Norway



Key Findings:

The highest level of enforcement is seen in the Norwegian ***Education*** *sector; however, even there, only* ***5.5%*** *of domains have enforced MTA-STS. The* ***Telecommunications*** *sector shows* ***0.8%*** *enforcement and* ***1.7%*** *in testing mode.*

Comparative Analysis of DNSSEC Adoption among Different Sectors in Norway



Key Findings:

The Norwegian ***Other*** *sector reports the lowest adoption rate, with* ***only 36.2%*** *of domains having DNSSEC enabled. In contrast, the* ***Transport*** *sector leads with the highest DNSSEC adoption at* ***53.0%****, followed closely by the* ***Government*** *sector at* ***51.7%****.*

Adoption rates in other major sectors range from ***36.5%*** *(Healthcare) to* ***50.5%*** *(Financial).*

DMARC & MTA-STS Adoption Rates: Key Statistics for Norway

- Total Domains Analyzed: 641
- 85.2% of domains have a correct SPF record, while 9.2% have no SPF record.
- 16.9% of domains have no DMARC record. Of those with a DMARC record, the policies are distributed as follows:
    - 29.0% are set to “reject”
    - 22.3% are set to “quarantine”
    - 31.5% are set to “none”
- MTA-STS adoption is alarmingly low. Only 2.8% of domains have an "enforce" policy, while 95.6% domains have not deployed MTA-STS.
- 45.6% of domains have DNSSEC enabled.

Critical Errors Organizations in Norway Are Making

SPF and DMARC adoption is relatively high across Norway. However, the implementation isn’t void of errors. More specifically:

1. DMARC Implementation Errors
    - Several domains are missing DMARC records entirely.
    - Several domains have a DMARC policy of p=none, which means that no action is taken against emails that fail authentication. This is a good starting point for monitoring, but it doesn’t protect against spoofing.
    - The presence of syntax errors and multiple DMARC records was also noticed among Norwegian domains, leading to invalid configurations.

    Recommendation: Use a DMARC generator tool to create your record, transition to a DMARC enforcement policy while monitoring email activity closely, and publish only 1 DMARC record per domain.

2. SPF Implementation Errors
    - Several domains have SPF records exceeding the 10 DNS lookup limit, resulting in permerror. Example: “Parsing the SPF record requires 11/10 maximum DNS lookups.”
    - Several domains are missing SPF records.
    - The presence of syntax errors and multiple SPF records was also noticed among Norwegian domains, leading to invalid configurations.

    Recommendation: Regularly audit your SPF records to stay under SPF hard limits or use automated SPF optimization solutions.

3 The Subdomain Loophole: Inconsistent DMARC Policies

A critical error was observed where a domain is protected with a strict p=reject policy, but its subdomains are explicitly left unprotected with sp=none (or no sp tag, which defaults to the main policy). This creates a significant loophole. Attackers cannot spoof the main domain, but they can still easily spoof its subdomains.
Example: v=DMARC1;p=reject;sp=none;...

Recommendation: Organizations must ensure their DMARC policy for subdomains (sp) matches the primary domain's enforcement policy (p=reject or p=quarantine) to close this attack vector.

4 Advanced Security Divide: Low MTA-STS Adoption

While the foundational security issues above are common, the data also shows a stark divide in the adoption of advanced security protocols.

- The majority of domains (95.6%) lack MTA-STS (for enforcing encrypted email transport). This was observed in nearly every sector. This leaves the domains vulnerable to adversary-in-the-middle attacks and DNS spoofing threats.

- A small handful of organizations, primarily in the Financial and Government sectors, have successfully deployed it. This proves that implementation is achievable and sets a standard for others.

Recommendation: All organizations should implement both MTA-STS and DMARC to protect against advanced threats like man-in-the-middle attacks for inbound email security, while also preventing spoofing and impersonation threats on outbound messages.

5 Low DNSSEC Adoption

DNSSEC adoption rates are alarmingly low across Norwegian sectors, with an overall adoption of only 45.6%, leaving the majority of domains highly vulnerable to DNS spoofing and hijacking attacks.

Recommendation: To prevent domain hijacking and build digital trust, Norwegian organizations must prioritize the widespread adoption of DNSSEC.

How Can PowerDMARC Help

- PowerDMARC delivers a unified, comprehensive suite for email authentication, chosen by thousands of organizations, enterprises, and government agencies to defend their domains against phishing, impersonation, and other email-based attacks.

  Our platform provides the tools to fortify domain security and improve deliverability:

1. **Streamlined DMARC Implementation:** Get started in minutes with our DMARC analyzer. Our platform offers clear guidance and live monitoring, empowering you to safely configure DMARC, enforce your policy (p=quarantine or p=reject), and block fraudulent emails.

2. **Clear, Visual Analytics:** Stop struggling with complicated XML reports. Our DMARC report analyzer translates raw DMARC data into intuitive, easy-to-read dashboards that give you an immediate, clear understanding of your email channels, traffic sources, and deliverability.

3. **Error-Free SPF Management:** Generate accurate SPF records and validate them instantly. Our Hosted SPF solution automatically optimizes your record, helping you overcome SPF limits and prevent errors.

4. **Domain Health Scans:** Instantly check your domain for hidden email authentication vulnerabilities. Our Domain Health Analyzer pinpoints misconfigurations and provides clear, step-by-step instructions to resolve them quickly.

5. **Simplified MTA-STS & TLS-RPT:** Easily implement and manage advanced protocols like MTA-STS and TLS-RPT with hosted services.

6. **Instant DNSSEC Validation:** Use our simple DNSSEC Checker to quickly verify if your domain has the protocol configured properly.

Need Help or a Quick Demo?

Email us at support@powerdmarc.com to book a 1:1 session with our experts today!