New Zealand DMARC & MTA-STS Adoption Report 2025

POWERDMARC

POWERDMARC

Case study

New Zealand DMARC & MTA-STS Adoption Report 2025

- New Zealand's public sector is under growing pressure from phishing and spoofing attacks targeting government domains. To respond, the government launched the Secure Government Email (SGE) Framework, which requires all agencies to adopt open standards, including DMARC (set to "reject"), SPF, DKIM, MTA-STS, and TLS-RPT, by October 2025. The framework replaces the legacy SEEMail system and introduces regular reporting, issue remediation, and secure email transmission standards. This report reviews adoption progress and outlines steps to reduce cyber risk, enforce email integrity, and protect public sector communications.

Assessing the Threat Landscape

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

- How successful has New Zealand been in deploying SPF and DMARC across domains?
- What is the current level of MTA-STS adoption in New Zealand organizations?
- Which sectors in New Zealand are most exposed to email-based cyber threats?
- What common missteps are New Zealand organizations making in email authentication?
- What specific actions should domain owners in New Zealand take to improve their email security posture?

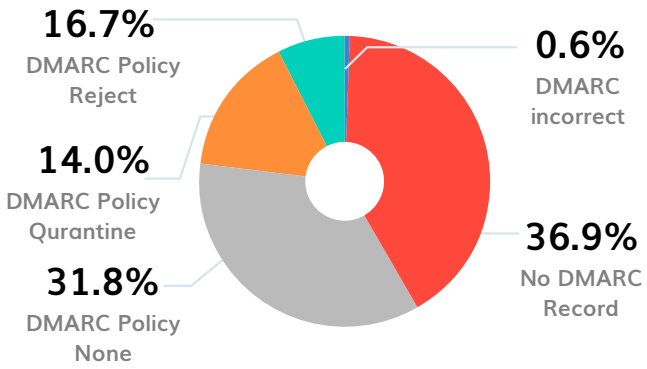
Sectors Analyzed

Total domains analyzed: 976

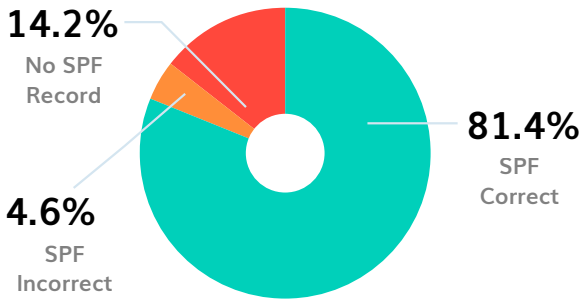
- Finance
- Healthcare
- Media
- Government
- Other
- Telecommunications
- Transport
- Education

What Do the Numbers Say?

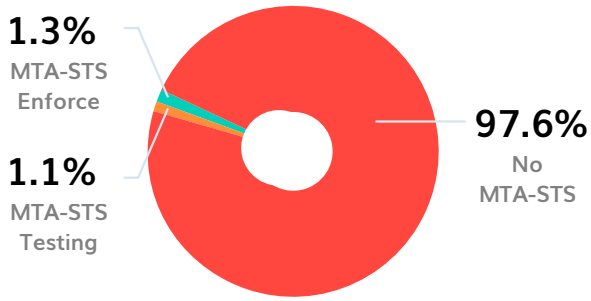
New Zealnd DMARC Adoption Analysis



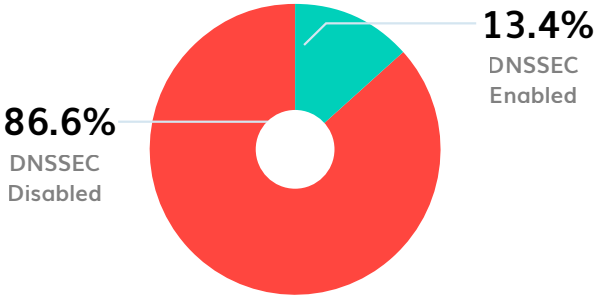
New Zealnd SPF Adoption Analysis



New Zealnd MTA-STS Adoption Analysis

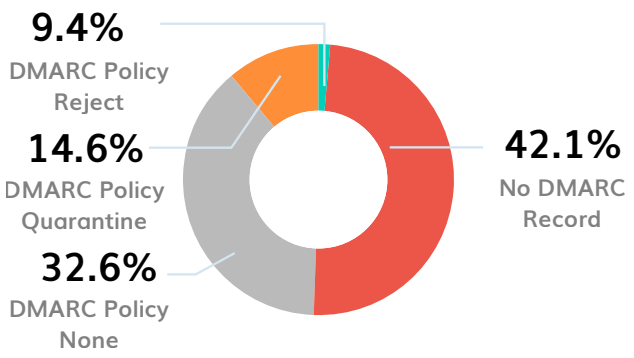


New Zealnd DNSSEC Adoption Analysis

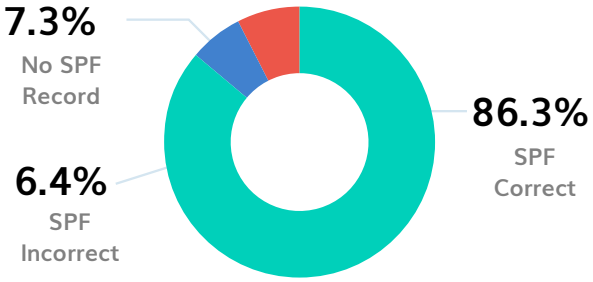


Finance

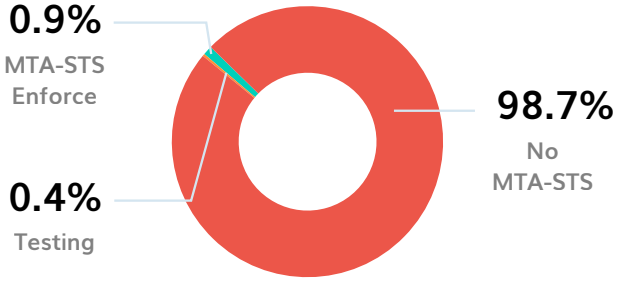
DMARC Adoption Analysis (Finance)



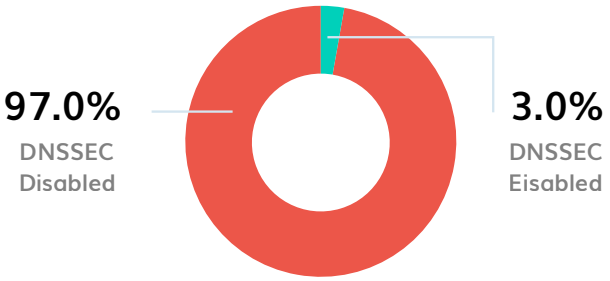
SPF Adoption Analysis (Finance)



MTA-STS Adoption Analysis (Finance)



DNSSEC Adoption Analysis (Finance)

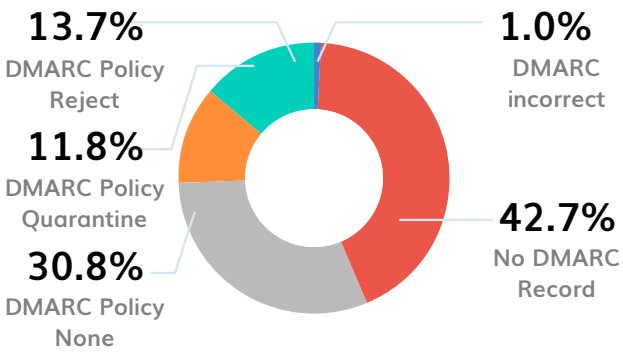


Key Findings:

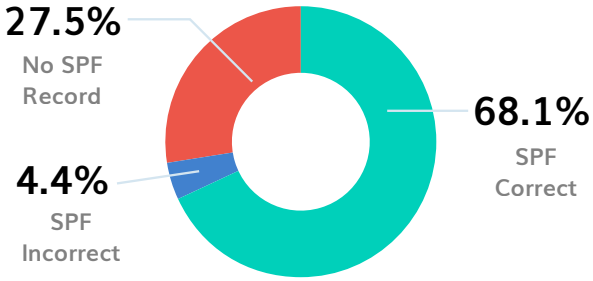
- 86.3% of domains have correct SPF records.
- 42.1% of domains do not have a DMARC record.
- 97.0% of domains have DNSSEC disabled.
- Only 0.9% of domains have implemented MTA-STS enforcement, while 98.7% have no MTA-STS.

Healthcare

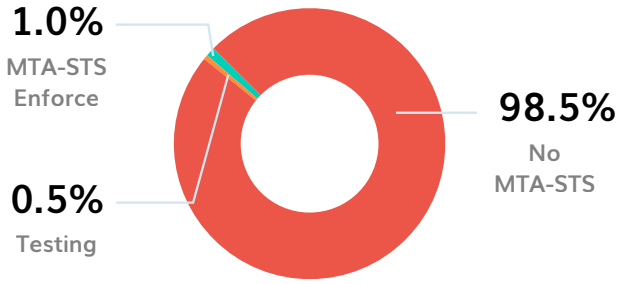
DMARC Adoption Analysis (Healthcare)



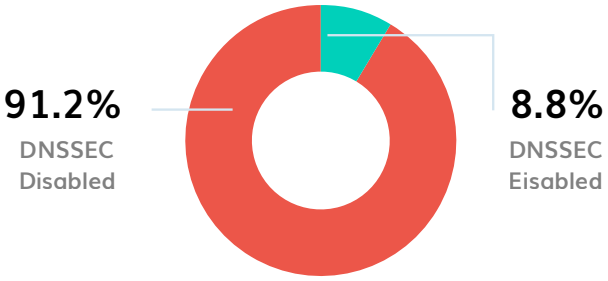
SPF Adoption Analysis (Healthcare)



MTA-STS Adoption Analysis (Healthcare)



DNSSEC Adoption Analysis (Healthcare)

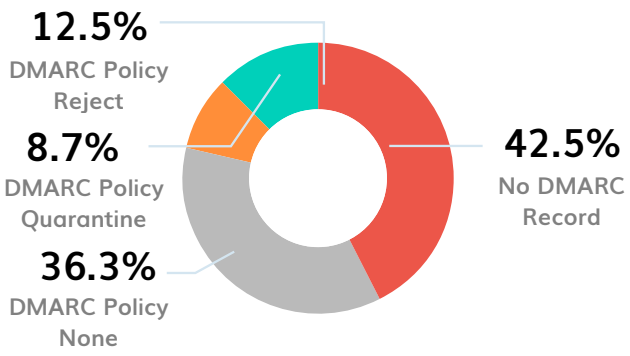


Key Findings:

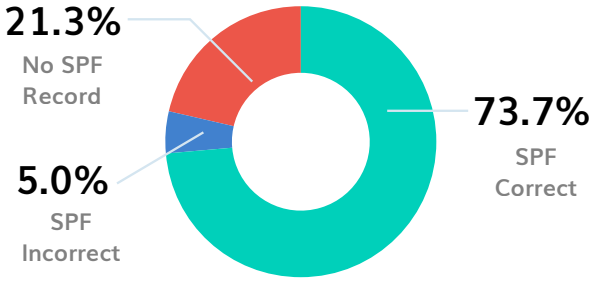
- 68.1% of healthcare domains have correct SPF records.
- Only 1.0% of domains have implemented MTA-STS enforcement, while 98.5% lack MTA-STS entirely.
- 42.7% of domains do not have a DMARC record.
- 91.2% of healthcare domains have DNSSEC disabled.

Media

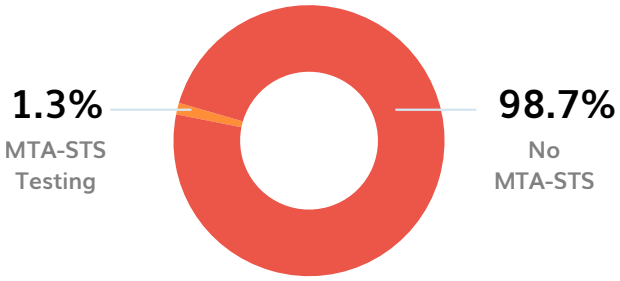
DMARC Adoption Analysis (Media)



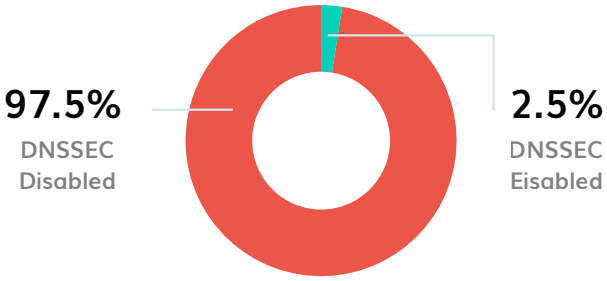
SPF Adoption Analysis (Media)



MTA-STS Adoption Analysis (Media)



DNSSEC Adoption Analysis Media

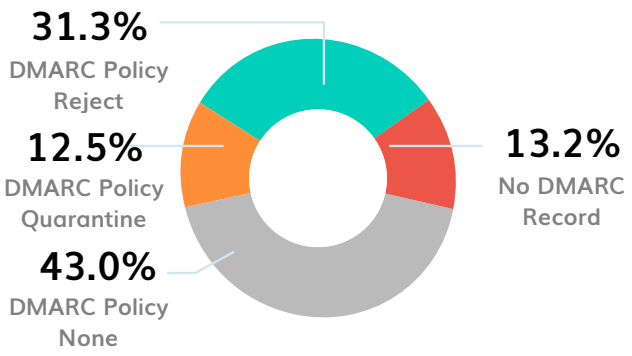


Key Findings:

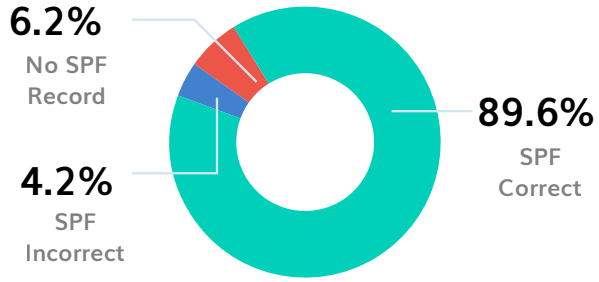
- 73.7% of domains have correct SPF records.
- 0% MTA-STS adoption observed in this sector; only 1.3% are in testing, while 98.7% have no MTA-STS.
- 42.5% of domains have no DMARC record.
- 97.5% of domains have DNSSEC disabled.

Government

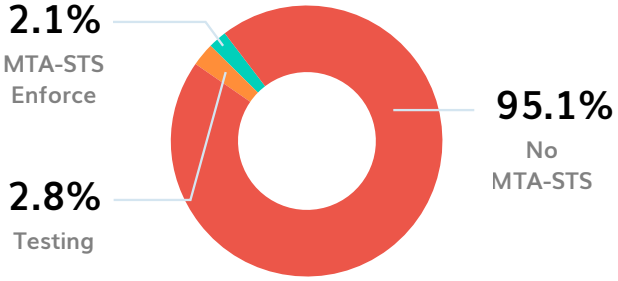
DMARC Adoption Analysis (Government)



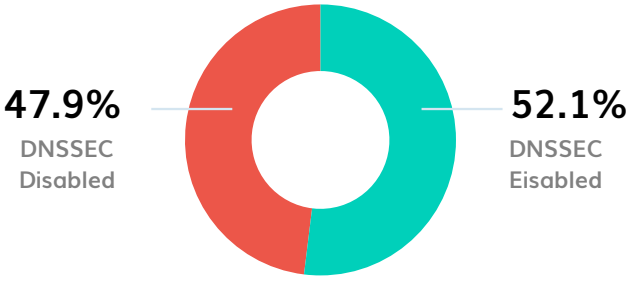
SPF Adoption Analysis (Government)



MTA-STS Adoption Analysis (Government)



DNSSEC Adoption Analysis (Government)

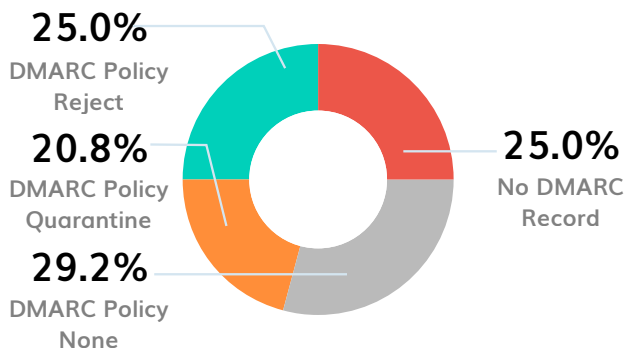


Key Findings:

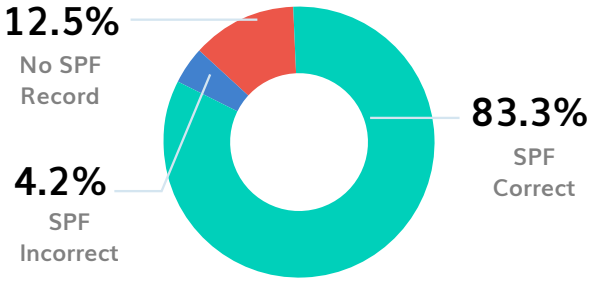
- 89.6% of government domains have implemented SPF records correctly.
- 13.2% of government domains do not have a DMARC record.
- MTA-STS adoption is extremely limited, with 95.1% of domains lacking MTA-STS records and only 2.8% in testing; no full deployment observed.
- DNSSEC adoption is moderate, with 52.1% of government domains enabled.

Other

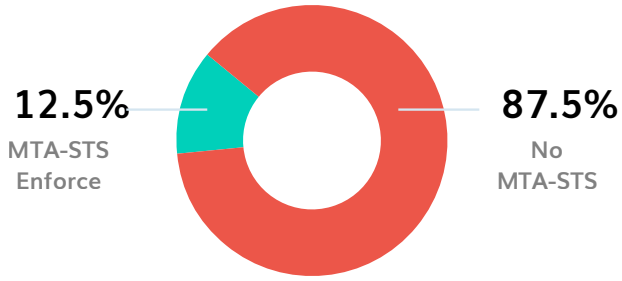
DMARC Adoption Analysis (Other)



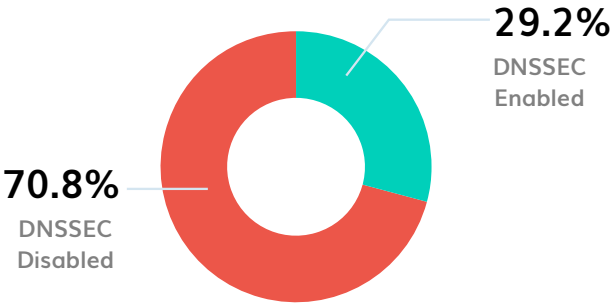
SPF Adoption Analysis (Other)



MTA-STS Adoption Analysis (Other)



DNSSEC Adoption Analysis (Other)

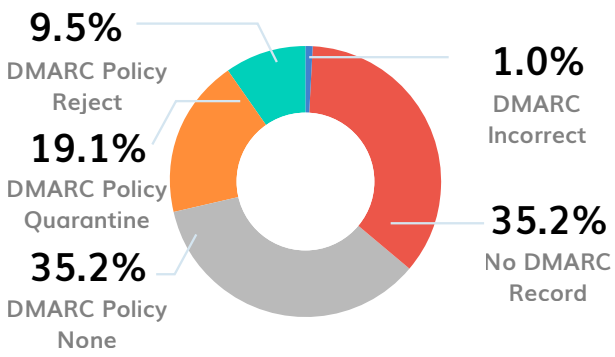


Key Findings:

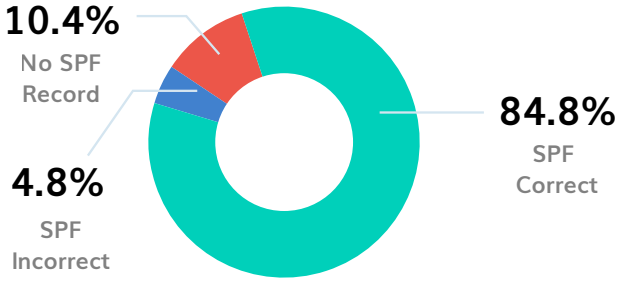
- 83.3% of domains have correctly implemented SPF records.
- 25.0% of domains have no DMARC record.
- MTA-STS adoption is very limited, with only 12.5% of domains enforcing MTA-STS; 87.5% have not implemented it.
- DNSSEC adoption remains low, with 70.8% of domains having DNSSEC disabled, and only 29.2% enabled.

Telecommunications

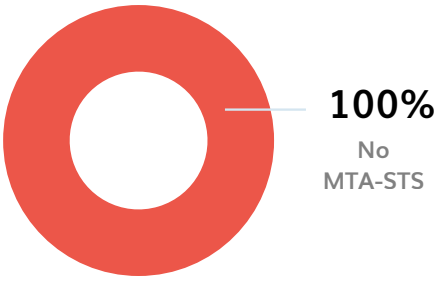
DMARC Adoption Analysis (Telecommunications)



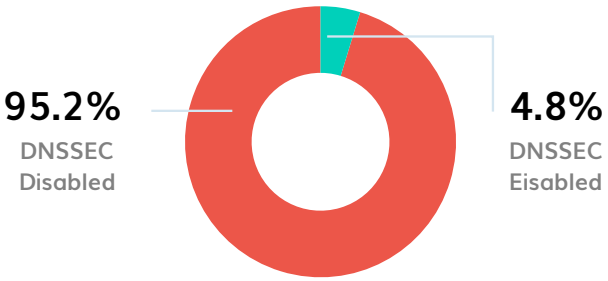
SPF Adoption Analysis (Telecommunications)



MTA-STS Adoption Analysis (Telecommunications)



DNSSEC Adoption Analysis (Telecommunications)

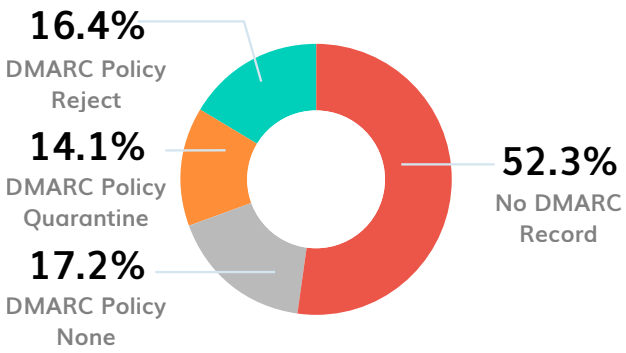


Key Findings:

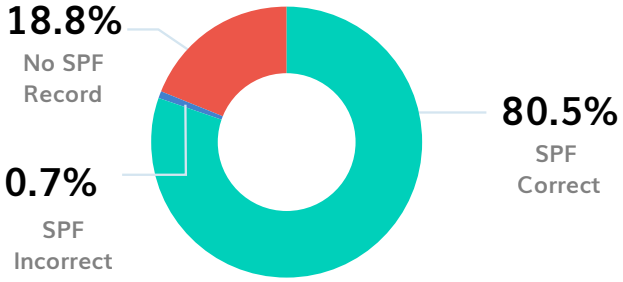
- 84.8% of domains have correct SPF records.
- 35.2% of domains have no DMARC record.
- MTA-STS adoption is nonexistent in this sector—no domains have implemented MTA-STS.
- 95.2% of domains have DNSSEC disabled.

Transport

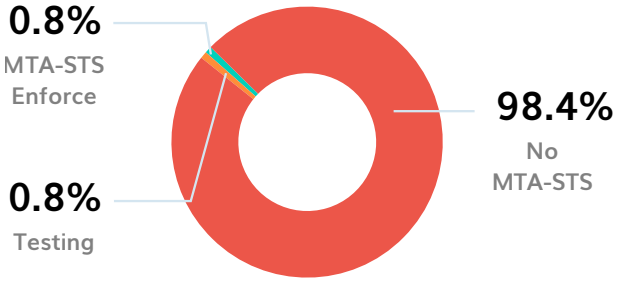
DMARC Adoption Analysis (Transport)



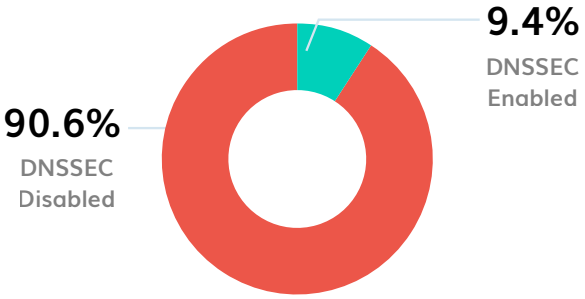
SPF Adoption Analysis (Transport)



MTA-STS Adoption Analysis (Transport)



DNSSEC Adoption Analysis (Transport)

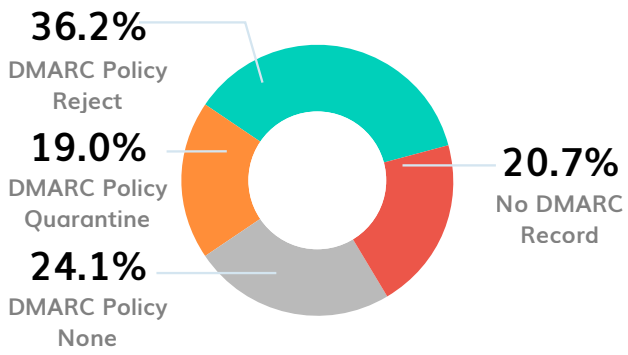


Key Findings:

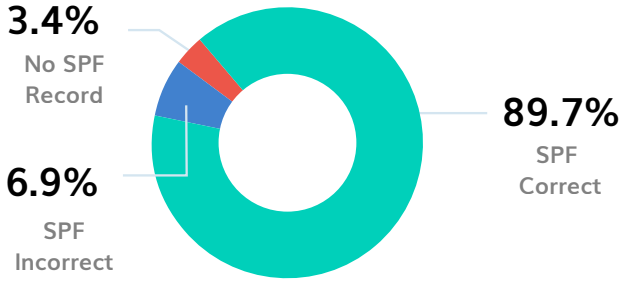
- 80.5% of transport sector domains have correct SPF records.
- 52.3% of domains lack a DMARC record.
- MTA-STS adoption is extremely low, with only 0.8% of domains enforcing MTA-STS and 98.4% having no MTA-STS record.
- DNSSEC is not widely adopted; just 9.4% of domains have DNSSEC enabled, while 90.6% are disabled.

Education

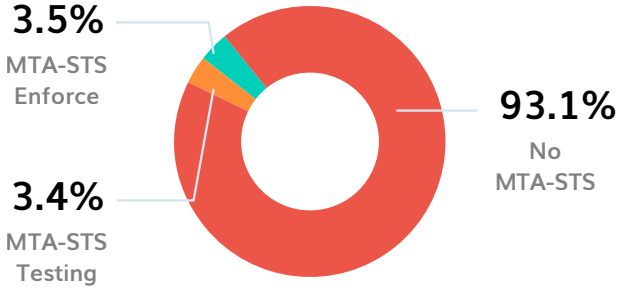
DMARC Adoption Analysis (Education)



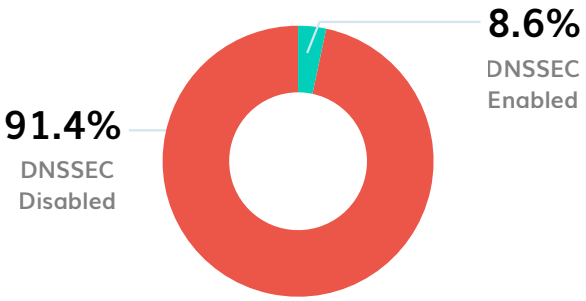
SPF Adoption Analysis (Education)



MTA-STS Adoption Analysis (Education)



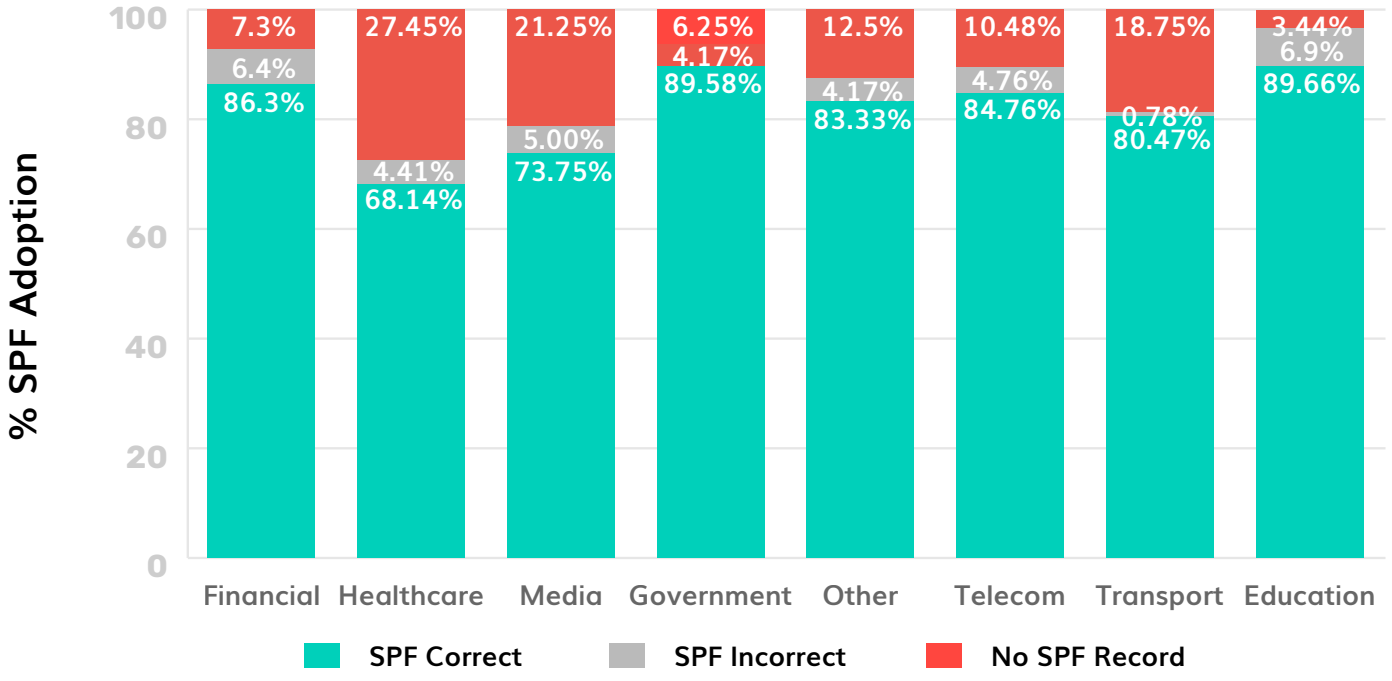
DNSSEC Adoption Analysis (Education)



Key Findings:

- 89.7% of education domains have correctly implemented SPF records.
- 20.7% of domains lack a DMARC record, while an additional 24.1% use a DMARC “None” policy (monitoring only).
- MTA-STS adoption is extremely limited: only 3.5% of domains enforce MTA-STS, with 93.1% having no MTA-STS record.
- DNSSEC adoption is low in the sector, with only 8.6% of education domains enabled.

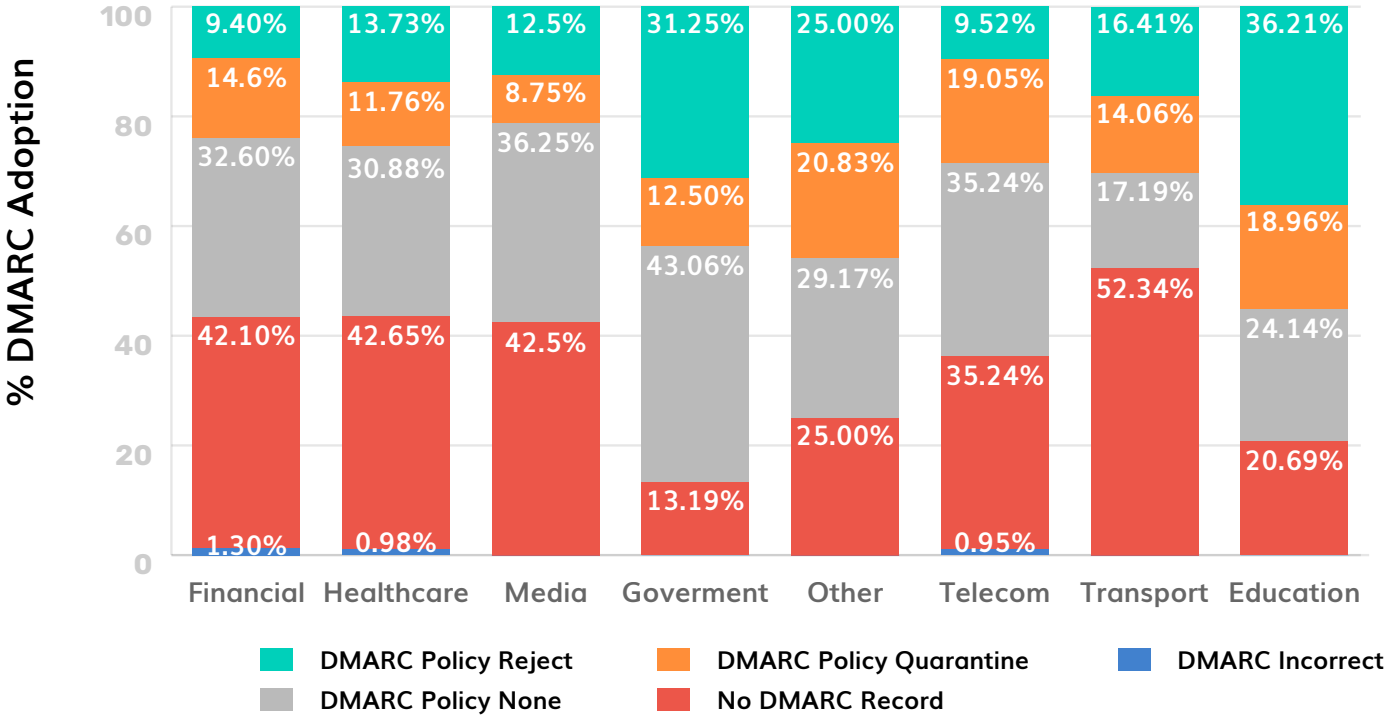
Comparative Analysis of SPF Adoption among Different Sectors in New Zealand



Key Findings:

The Education sector leads in correct SPF implementation, with 89.66% of domains properly configured. The Government sector follows closely at 89.58%. In contrast, the Healthcare sector lags behind, with only 68.14% of domains implementing SPF correctly — the lowest among all sectors analyzed.

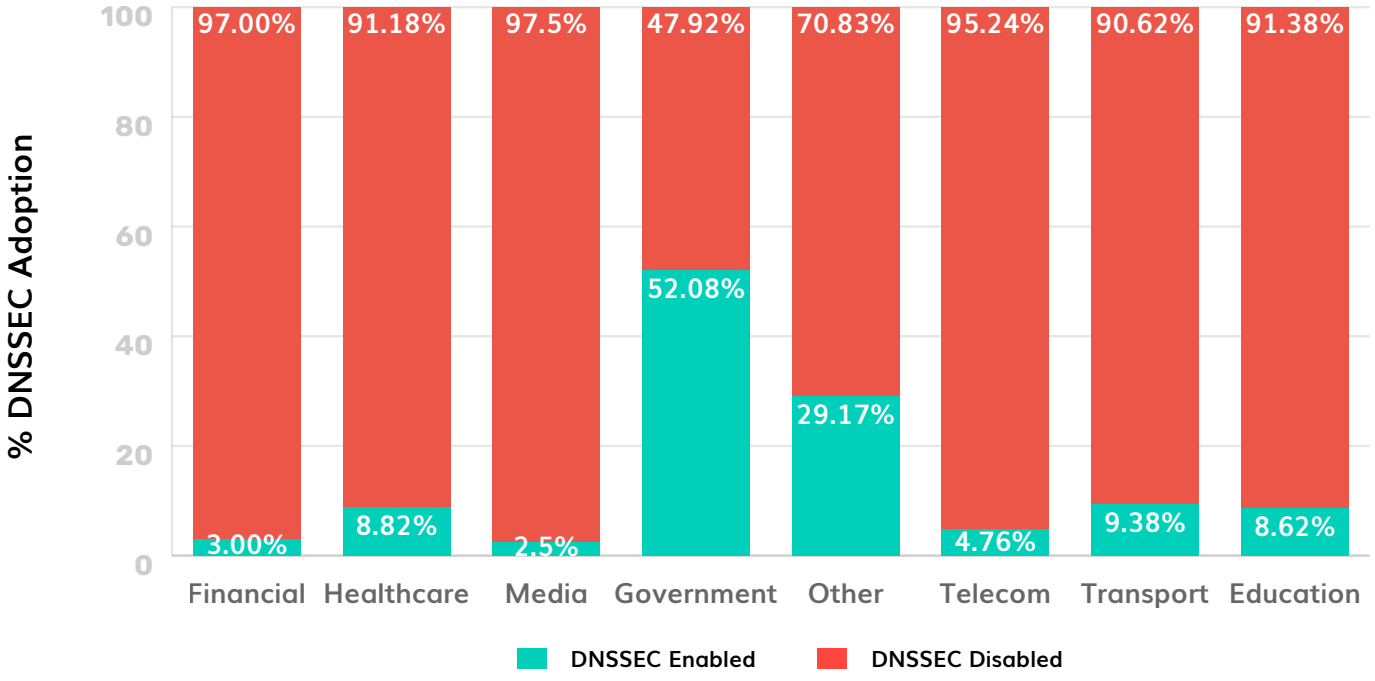
Comparative Analysis of DMARC Adoption among Different Sectors in New Zealand



Key Findings:

In New Zealand, the Government sector has the highest DMARC adoption, with just 13.19% of domains lacking records. The Transport sector trails behind, with 52.3% of domains missing DMARC. The Education sector leads in strict “Reject” policy adoption at 36.2%, followed closely by the Government. Telecommunications and Finance show the lowest use of “Reject” policies.

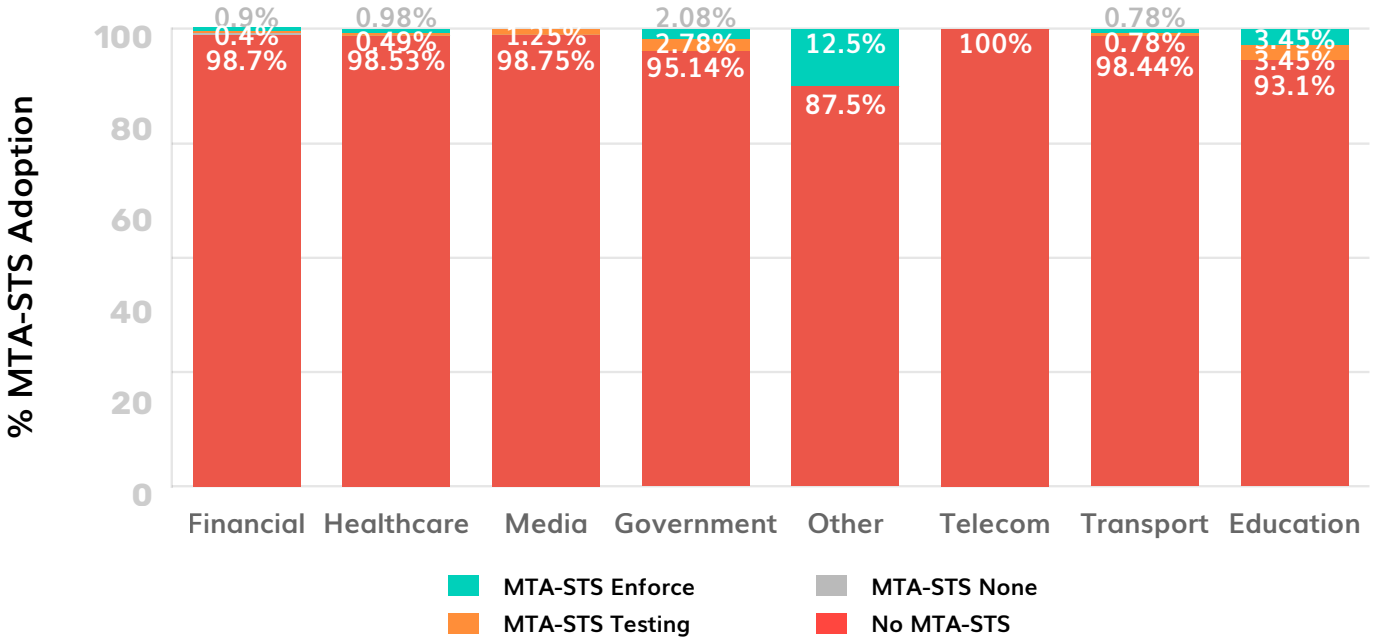
Comparative Analysis of MTA-STS Adoption among Different Sectors in New Zealand



Key Findings:

MTA-STS adoption in New Zealand remains minimal across all sectors, with over 90% of domains lacking implementation. The “Other” category shows the highest adoption, yet only 12.5% have enforced it. The Telecommunications sector reports zero MTA-STS usage—neither in testing nor enforcement.

Comparative Analysis of DNSSEC Adoption among Different Sectors in New Zealand



Key Findings:

DNSSEC adoption in New Zealand is low across the board. The Government sector leads with 52.08% of domains enabled, while the Media sector lags behind at just 2.5%. Most sectors — including Finance, Healthcare, Transport, Education, and Telecommunications — have DNSSEC disabled on over 90% of domains.

DMARC & MTA-STS Adoption Rates: Key Statistics for New Zealand

- **Total Domains Analyzed: 976**
- **62.5% have a correct DMARC record; 36.9% have no DMARC record.**
- **31.8% set to "none," 14.0% "quarantine" (Q), and 16.7% "reject."**
- **Only 2.36% have a valid MTA-STS record; 97.64% have none.**
- **81.2% have a correct SPF record; 14.2% have no SPF record.**
- **86.6% have DNNSSEC disabled.**

Critical Errors Organizations in New Zealand Are Making

1 Widespread Absence of DMARC Records

Several New Zealand domains still lack a DMARC record, leaving them vulnerable to email spoofing. Without DMARC, organizations lack visibility into unauthorized email activity, and government domains fail to meet SGE compliance requirements.

Examples:

"A DMARC record does not exist for this domain or its base domain."

2 Missing or Invalid SPF Records

Many domains in New Zealand either lack an SPF record or have one that is syntactically incorrect. Without a valid SPF configuration, mail servers cannot authenticate the sender, making it easier for attackers to deliver spoofed or fraudulent emails. To prevent legitimate emails from being rejected or marked as spam, organizations must publish a valid, error-free SPF record that includes all authorized senders.

Examples:

"Does not have a SPF TXT record" error.
"ip4: ~all is not a valid ipv4 value"
"ip-1 is not a valid ipv4 value"

3 Misconfigured and Multiple SPF Records

Even when SPF records exist, misconfigurations are common, such as multiple SPF records per domain or exceeding the 10 DNS lookup limit, both of which violate RFC 7208. Organizations should consolidate SPF data into a single TXT record and optimize it by removing unnecessary "include" mechanisms.

Examples:

"has multiple SPF TXT records"
"Parsing the SPF record requires 11/10 maximum DNS lookups."
"Parsing the SPF record requires 12/10 maximum DNS lookups."

4 Weak or Incorrect DMARC Policies

Many domains with DMARC records remain at a p=none (monitor-only) policy, which offers no protection against spoofing. Some also publish multiple DMARC records: an invalid setup that can cause unpredictable mail server behavior. After the initial monitoring phase, organizations should shift to a p=quarantine or p=reject DMARC policy and ensure only one valid DMARC record is in place per domain.

Examples:

v=DMARC1; p=none; aspf=s; adkim=s; pct=100; fo=1;...
"Multiple DMARC policy records are not permitted."

5 Unrelated or Extraneous TXT Records

Some domains have unnecessary TXT records on critical subdomains like _dmarc and _mta-sts, which can disrupt email authentication. Regular DNS audits are essential to ensure only the required protocol records are published on these subdomains.

Examples:

"Unrelated TXT records were discovered. These should be removed, as some receivers may not expect to find unrelated TXT records at ..."

6 Lack of MTA-STS Implementation

Mail Transfer Agent Strict Transport Security (MTA-STS) enforces encrypted email delivery, guarding against man-in-the-middle and downgrade attacks, and is required for SGE compliance. However, most domains in New Zealand have yet to implement it. Organizations should adopt and enforce MTA-STS to ensure secure, encrypted email transmission.

Examples:

"An MTA-STS DNS record does not exist for this domain."

7 DNSSEC Not Widely Enabled

The data reveals that DNSSEC is disabled for most New Zealand domains. All organizations are strongly encouraged to enable DNSSEC to enhance DNS integrity and security.

Examples:

"A DNSSEC DNS record does not exist for this domain."

How PowerDMARC Helps You Stay Secure and Error-Free

- PowerDMARC is a comprehensive email authentication platform trusted by MSPs, MSSPs, enterprises, and governments worldwide to protect domains against spoofing, phishing, and impersonation attacks.

Here's how we empower you to secure your email from day one:

1. Simplified DMARC Deployment: Use our free DMARC Analyzer to generate your DMARC record.
2. Insightful, Visual Reporting: Forget deciphering complex XML files with the help of our intuitive, human-readable dashboards.
3. Hassle-Free SPF Management: Create flawless SPF records with our free generator and instantly validate them with our SPF checker tool.
4. Proactive Domain Health Analysis: Use our Domain Health Analyzer to instantly scan your DNS for hidden misconfigurations.
5. Effortless MTA-STS & TLS-RPT: Implement and manage MTA-STS and TLS-RPT without the complexity.
6. One-Click DNSSEC Verification: Quickly use our DNSSEC Checker to confirm that your domain is protected against DNS-level attacks.

Need Help or a Quick Demo?

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