# DMARC & MTA-STS Adoption in Switzerland: 2024 Report

POWERDMARC | ZENDATA CYBER SECURITY

POWERDMARC | ZENDATA CYBER SECURITY

Case study

# DMARC & MTA-STS Adoption in Switzerland: 2024 Report

- Email authentication has emerged as a frontier player in email security in 2024. Major email service and inbox providers like Google and Yahoo recently upgraded their mandatory sender requirements - making email authentication implementation compulsory for both non-promotional and promotional emails. But why this sudden revolution?

  Email fraud is on the rise. Phishing and spoofing attacks have become more rampant than before with an estimated 3.4 billion scam emails being sent by cybercriminals every day! To protect yourself and your customers from malicious emails, authentication is a must.

  DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email authentication protocol designed to give email domain owners the ability to protect their domain from unauthorized use, spoofing, and phishing attacks. You can set up your DMARC policy to reject unauthorized emails and even enable reporting to gain visibility on email channels, sending sources, and authentication results.

  The MTA-STS (Mail Transfer Agent Strict Transport Security) protocol is designed to improve the security of email communications by enforcing the use of Transport Layer Security (TLS) during email transmission. It helps protect email traffic from passive eavesdropping and active man-in-the-middle attacks.

## Assessing the Threat Landscape

- With the global surge in email-based threats, Switzerland is increasingly at risk. The rapid advancement of technology, particularly with the introduction of AI, has increased the potential for cybercrime worldwide. These technological innovations, while beneficial in many ways, have also created new vulnerabilities that cybercriminals are quick to exploit.

- Switzerland, much like other nations, is experiencing a significant uptick in cyber threats, making it important for organizations and governments to strengthen their cybersecurity posture. Organizations should now take a proactive approach to safeguarding sensitive information and maintaining the authenticity of email communications.
- According to an article published on Swissinfo.ch, in 2023, the federal office handled 187,000 reports through the antiphishing.ch website and took down 8,223 phishing websites in Switzerland.
- Furthermore, the Swiss National Cyber Security Centre's (NCSC) 2023 Anti-Phishing Report analyzed 10,000+ phishing websites impersonating brand names, out of which more than 60% were found to be Swiss brands. NCSC evidentiated how cybercrime almost doubled in Switzerland between 2022 and 2023, causing significant reason for alarm.

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

- What is the current situation of SPF and DMARC adoption and enforcement in organizations in Switzerland?
- What is the current status of MTA-STS adoption among organizations in Switzerland?
- Which industry sectors in Switzerland are the most vulnerable to email phishing and other cyberattacks?
- What is the rate of DNSSEC enablement among Swiss organizations?
- How can we improve the cybersecurity and email authentication infrastructure in Switzerland to prevent impersonation attacks?
- How can organizations mitigate email-based threats?

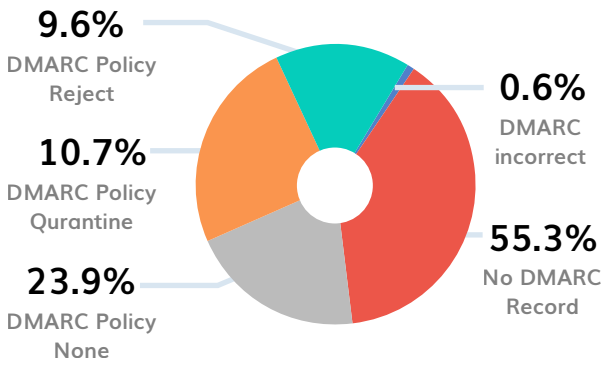
**To gain better insight into the current scenario we analyzed 1103 domains belonging to top businesses and organizations in Switzerland, from the following sectors:**

- Fitness
- Healthcare
- Media
- Government
- Telecommunication
- Job Board
- Transport
- Miscellaneous Businesses
- Banking
- Education

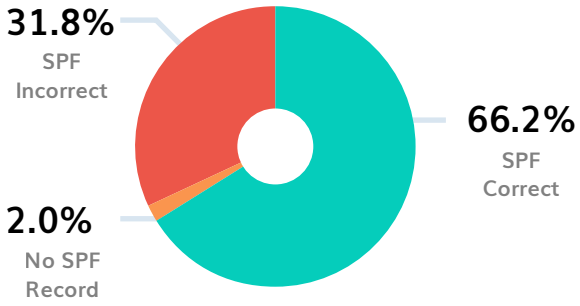
# What Do the Numbers Say?

An in-depth SPF and DMARC adoption analysis was conducted while examining all 458 Qatar domains, which led to the following revelations:

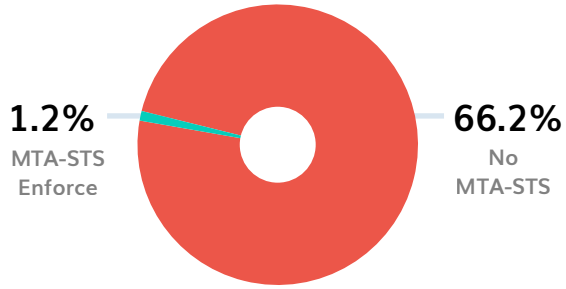
## DMARC Adoption Analysis of Swiss Domains



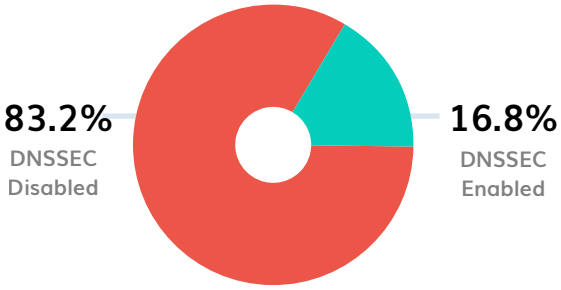

## SPF Adoption Analysis of Swiss Domains




## MTA-STS Adoption Analysis of Swiss Domains




## DNSSEC Adoption Analysis of Swiss Domains

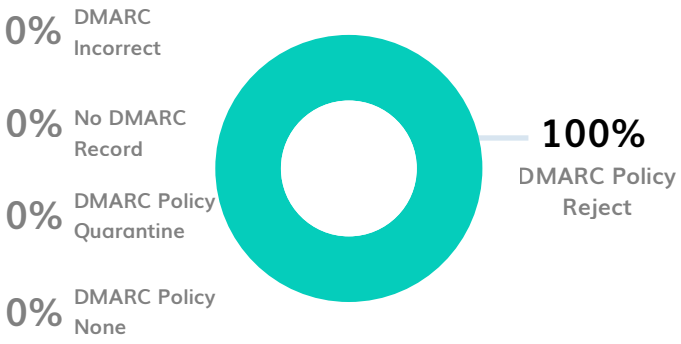



- **Graphical Analysis:** Among all 1103 domains examined that belong to various organizations in Switzerland, 730 domains (66.2%) possessed correct SPF records, while 351 domains (31.8%) unfortunately had no SPF records at all. 487 domains (44.2%) had correct DMARC records, while 6 of the domains (0.5%) had DMARC records that contained errors. A vast majority of domains (610 domains making up 55.3%) had no DMARC record found. 264 domains had their DMARC policy set at none (23.9%), enabling monitoring only, while 117 domains (10.7%) had their DMARC policy set at quarantine, and 106 domains (9.6%) had their DMARC policy set at maximum enforcement (i.e. p=reject).

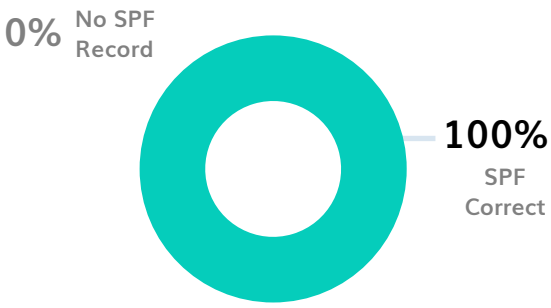
# Sector-wise Analysis of Domains in Switzerland

## Fitness Sector

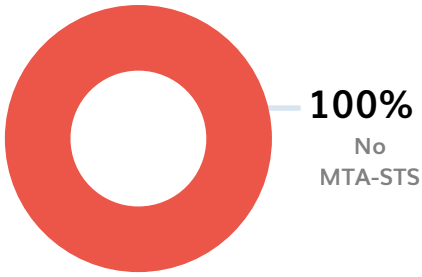
### DMARC Adoption Analysis in the Swiss Fitness Sector




### SPF Adoption Analysis in the Swiss Fitness Sector




### MTA-STS Adoption Analysis in the Swiss Fitness Sector



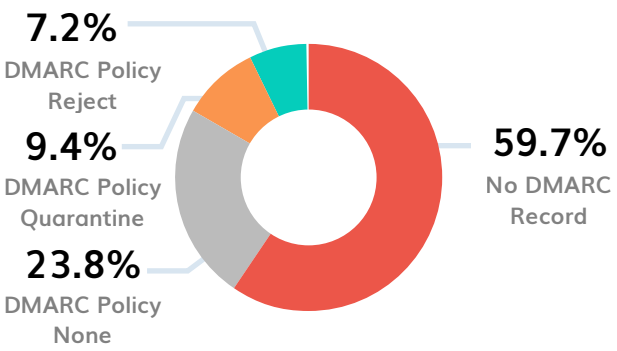

### DNSSEC Adoption Analysis in the Swiss Fitness Sector


**Key Findings:**

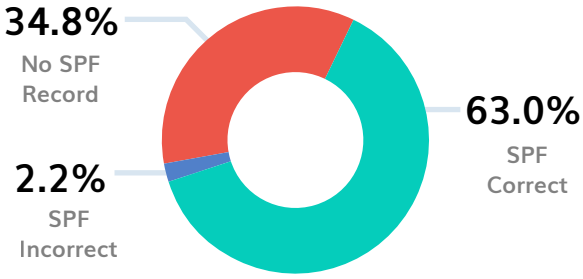
- All examined domains (100%) had correct SPF records
- All of the domains had their DMARC policy set at p=none offering no protection
- MTA-STS and DNSSEC were not implemented for any of the domains in the fitness sector

# Healthcare Sector

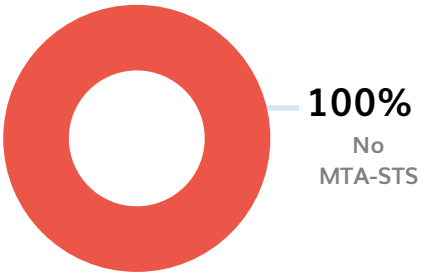
### DMARC Adoption Analysis in the Swiss Healthcare Sector




### SPF Adoption Analysis in the Swiss Healthcare Sector




### MTA-STS Adoption Analysis in the Swiss Healthcare Sector



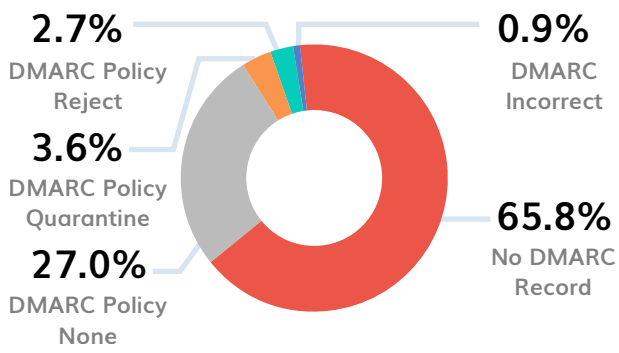

### DNSSEC Adoption Analysis in the Swiss Healthcare Sector


**Key Findings:**

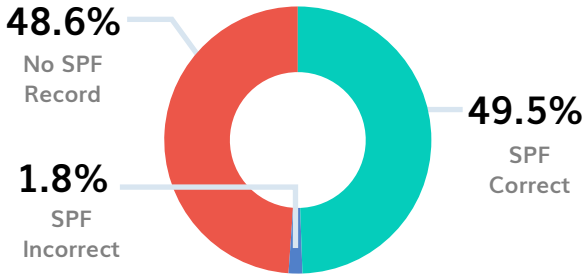
- 34.8% of domains had no SPF record
- 23.8% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 59.7% of the domains
- None of the domains in the Swiss Healthcare sector had MTA-STS implemented
- DNSSEC was disabled for 81.2% of the domains

# Media Sector

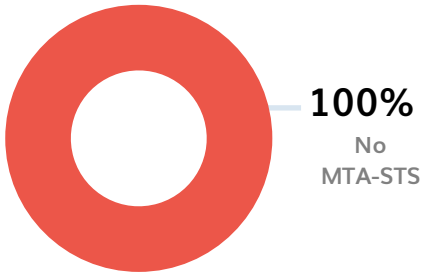
## DMARC Adoption Analysis in the Swiss Media Sector



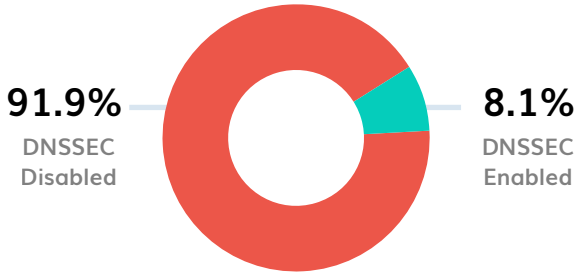

## SPF Adoption Analysis in the Swiss Media Sector




## MTA-STS Adoption Analysis in the Swiss Media Sector




## DNSSEC Adoption Analysis in the Swiss Media Sector

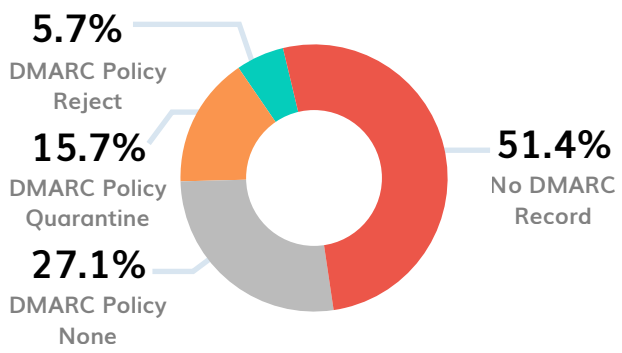



**Key Findings:**

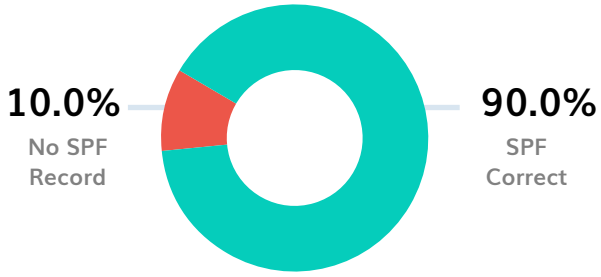
- 48.6% of domains had no SPF record
- 27.0% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 65.0% of the domains
- MTA-STS wasn't enabled for any of the examined domains
- DNSSEC was disabled for 91.9% of the domains

# Government Sector

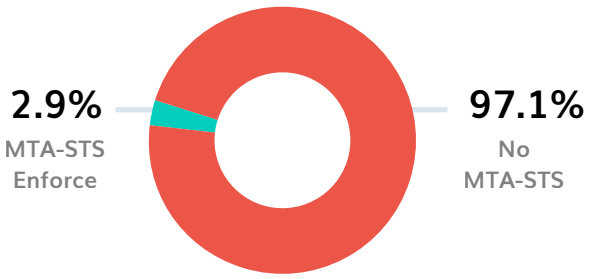
### DMARC Adoption Analysis in the Swiss Government Sector



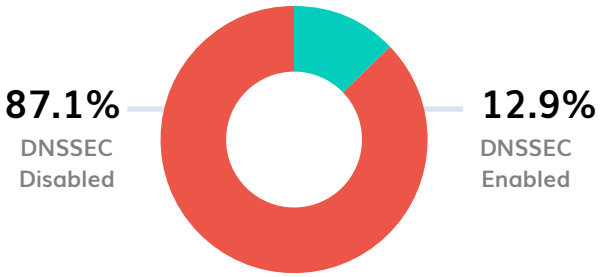

### SPF Adoption Analysis in the Swiss Government Sector




### MTA-STS Adoption Analysis in the Swiss Government Sector




### DNSSEC Adoption Analysis in the Swiss Government Sector

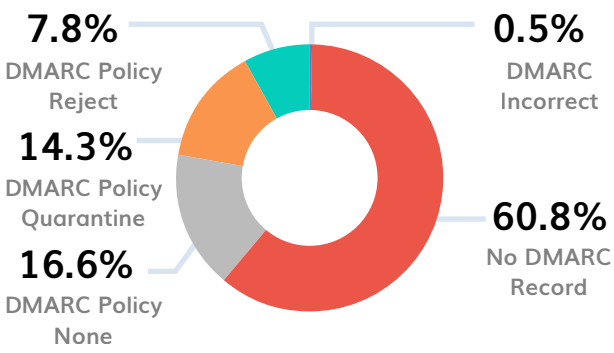



**Key Findings:**

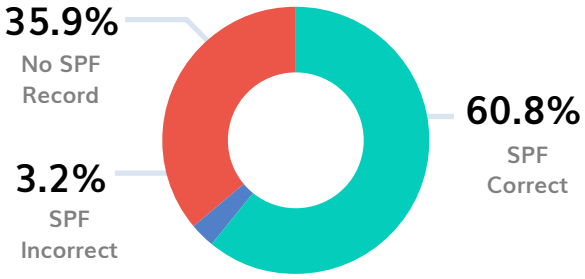
- 10% of domains had no SPF record
- 27.1% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 51.4% of the domains
- 97.1% of the domains didn't have MTA-STS implemented for them
- DNSSEC was also disabled for 87.1% of the domains in this sector

# Telecom Sector

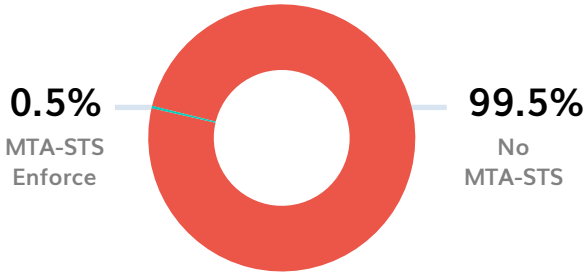
## DMARC Adoption Analysis in the Swiss Telecom Sector



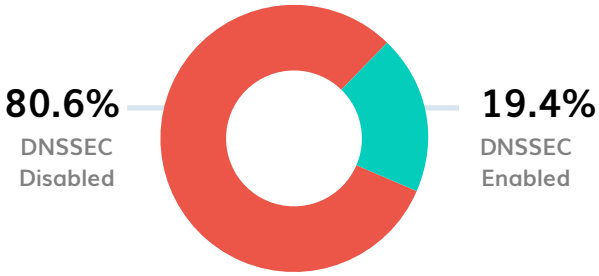

## SPF Adoption Analysis in the Swiss Telecom Sector




## MTA-STS Adoption Analysis in the Swiss Telecom Sector




## DNSSEC Adoption Analysis in the Swiss Telecom Sector

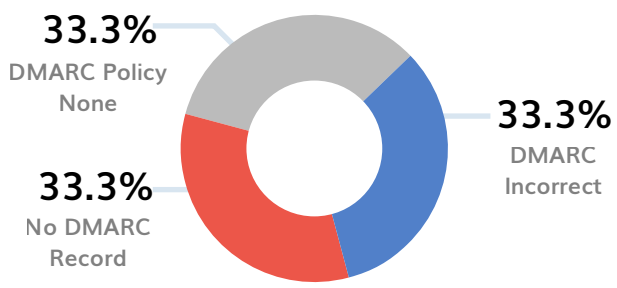



### Key Findings:

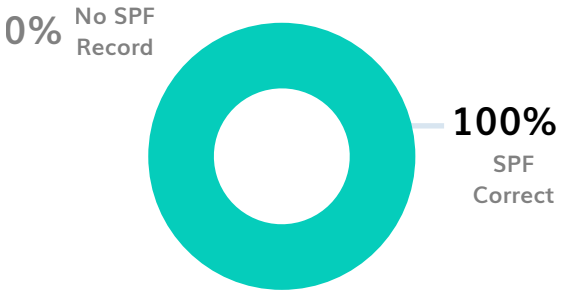
- 35.9% of domains had no SPF record
- 16.6% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 60.8% of the domains
- 99.5% of the domains did not have MTA-STS implementation
- 80.6% of the domains had DNSSEC disabled

# Job Boards

### DMARC Adoption Analysis in the Swiss Job Boards Sector




### SPF Adoption Analysis in the Swiss Job Boards Sector




### MTA-STS Adoption Analysis in the Swiss Job Boards Sector

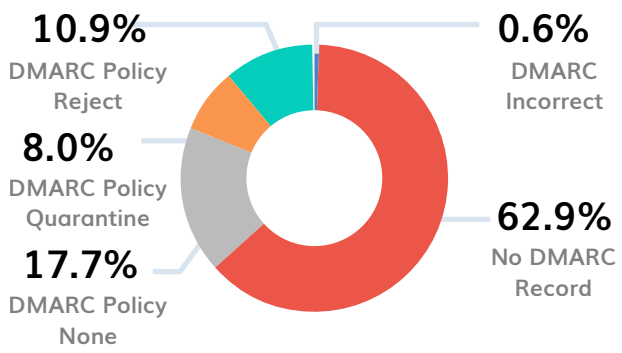

### DNSSEC Adoption Analysis in the Swiss Job Boards Sector


**Key Findings:**

- All domains examined in the Swiss Job Board sector had SPF enabled
- 33.3% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 33.3% of the domains
- MTA-STS was not enabled for any of the domains in this sector
- DNSSEC was disabled for 33.3% of the domains

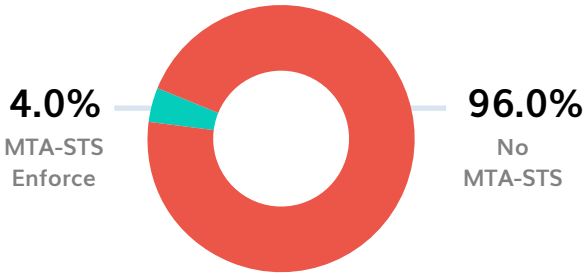
# Transport Sector

## DMARC Adoption Analysis in the Swiss Transport Sector




## SPF Adoption Analysis in the Swiss Transport Sector


## MTA-STS Adoption Analysis in the Swiss Transport Sector



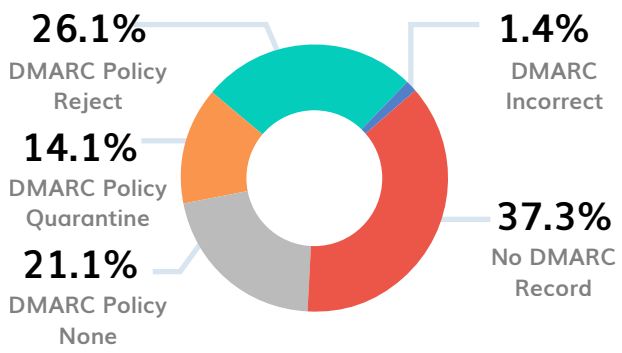

## DNSSEC Adoption Analysis in the Swiss Transport Sector


**Key Findings:**

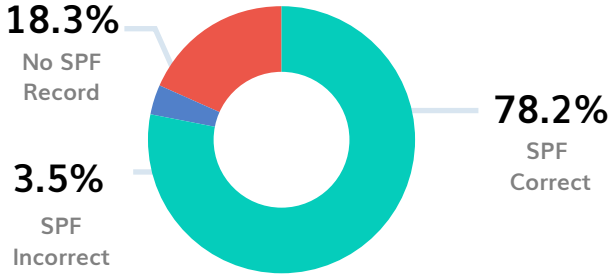
- 33.1% of domains had no SPF record
- 17.7% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 62.9% of the domains
- 96% of the domains did not have MTA-STS enabled
- DNSSEC was disabled for 78.9% of the domains

# Miscellaneous Businesses

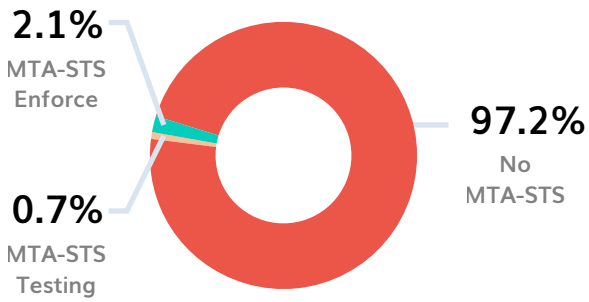
## DMARC Adoption Analysis in Swiss Miscellaneous Businesses Sector




## SPF Adoption Analysis in Swiss Miscellaneous Businesses Sector




## MTA-STS Adoption Analysis in Swiss Miscellaneous Businesses Sector



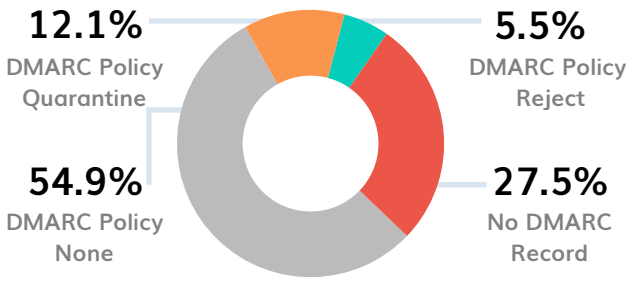

## DNSSEC Adoption Analysis in Swiss Miscellaneous Businesses Sector


**Key Findings:**

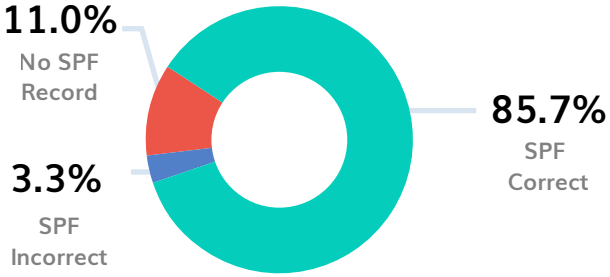
- 18.3% of domains had no SPF record
- 21.1% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 37.3% of the domains
- 97.2% of the domains did not have MTA-STS enabled with 0.7% still in Testing mode
- 90.1% of the domains had DNSSEC disabled

# Banking Sector

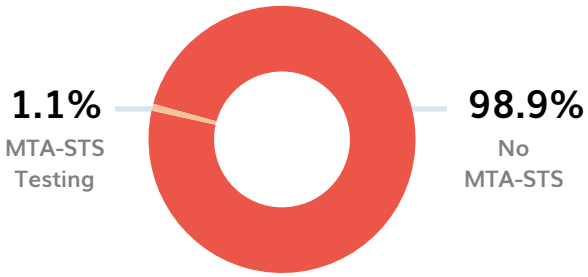
## DMARC Adoption Analysis in the Swiss Banking Sector



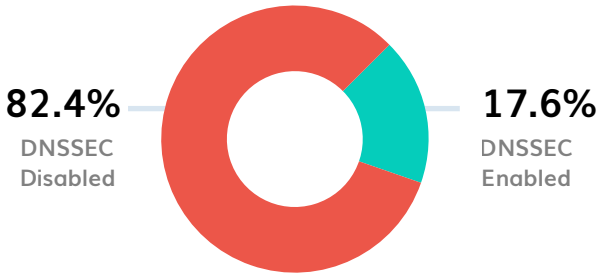

## SPF Adoption Analysis in the Swiss Banking Sector




## MTA-STS Adoption Analysis in the Swiss Banking Sector




## DNSSEC Adoption Analysis in the Swiss Banking Sector

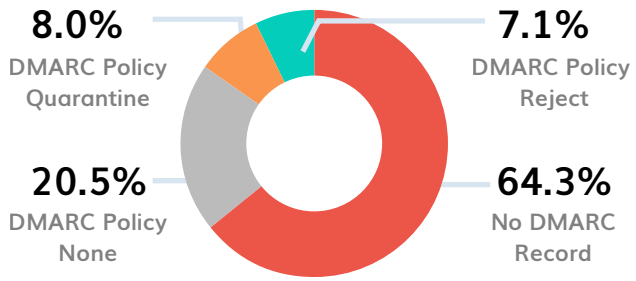



**Key Findings:**

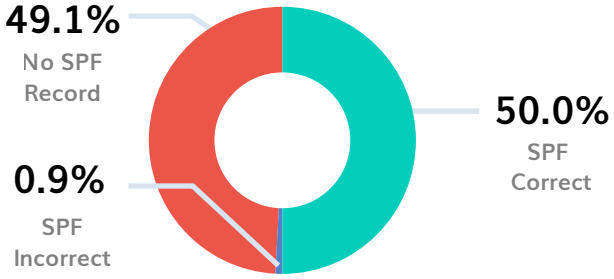
- 11% of domains had no SPF record
- 54.9% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 27.5% of the domains
- 98.9% of the domain did not have MTA-STS enabled
- DNSSEC was disabled for 82.4% of the domains in this sector

# Education Sector

### DMARC Adoption Analysis in the Swiss Education Sector




### SPF Adoption Analysis in the Swiss Education Sector



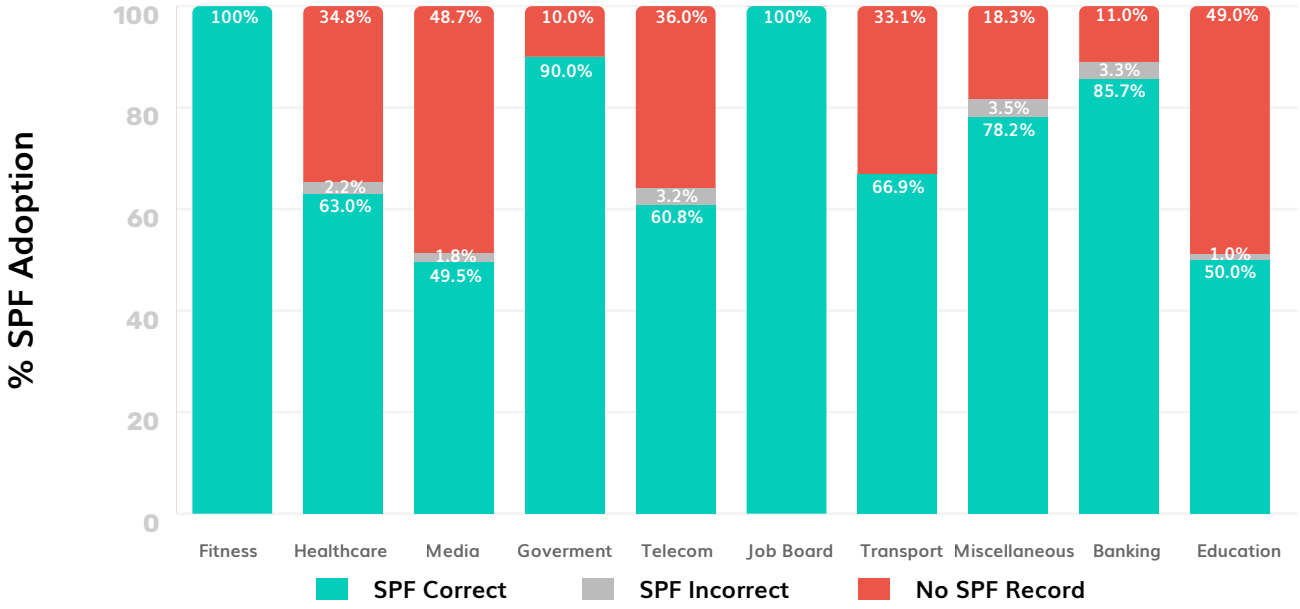

### MTA-STS Adoption Analysis in the Swiss Education Sector


### DNSSEC Adoption Analysis in the Swiss Education Sector


**Key Findings:**

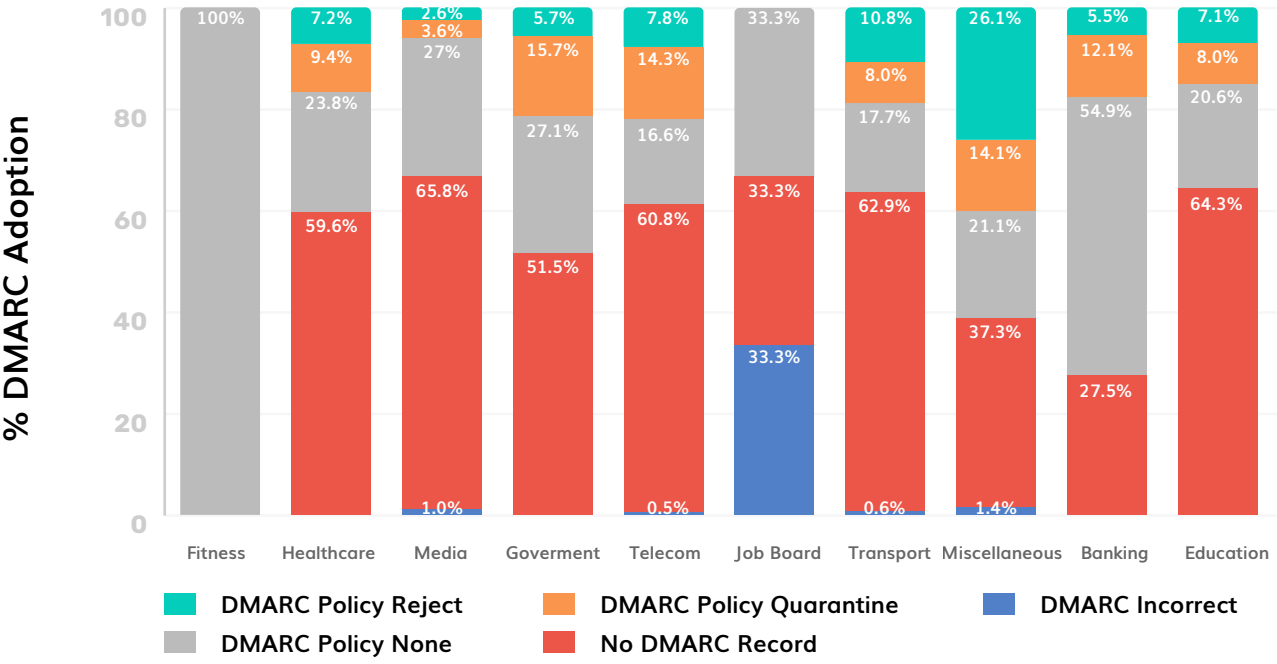
- 49.1% of domains had no SPF record
- 20.5% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 64.3% of the domains
- None of the domains examined had MTA-STS implemented
- DNSSEC was also disabled for 80.4% of the domains analyzed

# Comparative Analysis of SPF Adoption among Different Sectors in Switzerland



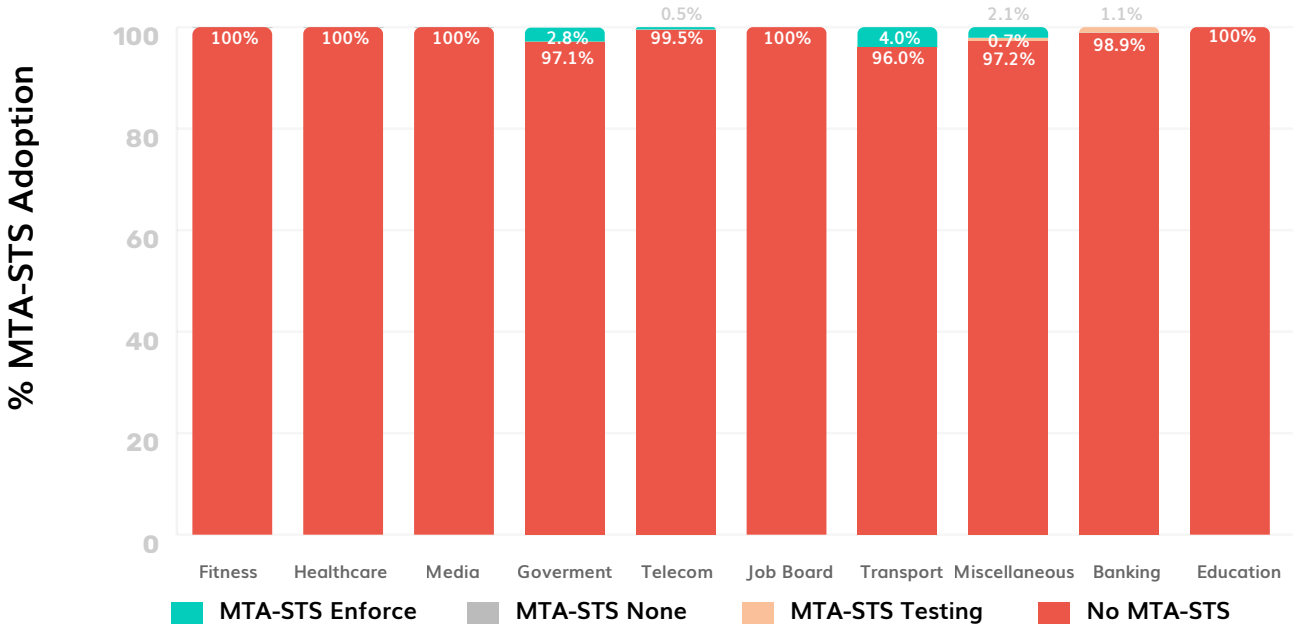

- The SPF adoption rate was found to be the lowest in Switzerland's Education and Media sectors. The highest rate of SPF adoption was noted in the Switzerland Government, Banking, Job Board, and Fitness sectors.

# Comparative Analysis of DMARC Adoption among Different Sectors in Switzerland



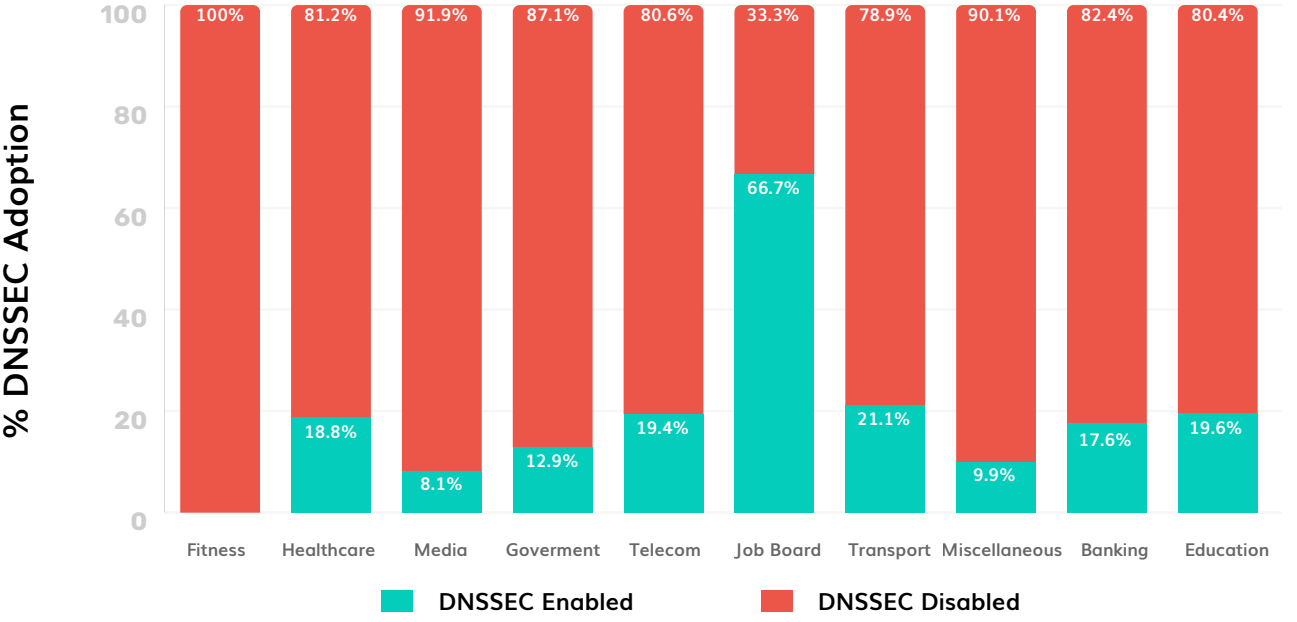

- Switzerland's Education, Media, and Transport sectors noted low rates of DMARC adoption. The highest rate of DMARC adoption was noted in the Swiss Fitness and Banking sectors. A large percentage of organizations in all sectors had "none" DMARC policy implemented.

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




- An average of 89.97%.of the domains in Switzerland among the 1103 domains analyzed, did not have MTA-STS implemented.

# Comparative Analysis of DMARC Adoption among Different Sectors in Switzerland




- An average of 80.69%.of the domains in Switzerland among the 1103 domains analyzed, had DNSSEC disabled for them.

# Critical Errors Organizations in Switzerland are Making

After reviewing 1103 domains across different sectors and industries in Switzerland, we identified significant errors that Swiss organizations and governments were making that were leaving them potentially vulnerable to exploits.

## Missing SPF and DMARC Records

Domains lacking SPF and DMARC records are at a higher risk of spam, spoofing, and phishing attacks, email deliverability issues, and poor domain reputation. This is because SPF and DMARC are email authentication protocols that work together to ensure that only authorized senders can send messages on behalf of your domain and unauthorized messages can be potentially rejected (if you are on DMARC p=reject).

Moreover, Google and Yahoo's updated sender requirements mandate all senders to implement SPF and bulk senders to enable DMARC. Domains failing to do so may get blocked when trying to send emails to Google and Yahoo inboxes

## Errors in Email Authentication Configuration

For SPF, common syntax errors include incorrect version tags, missing or extra spaces, incorrect mechanisms, unrecognized modifiers, exceeding character/lookup limits, and missing the `all` mechanism. For DMARC, syntax errors often involve incorrect version tags (e.g., `v=DMARC1;` is correct), missing or extra semicolons, incorrect policy tags, etc. Avoiding these errors ensures proper email authentication.

Similarly, syntax errors in your MTA-STA record or the MTA-STS policy file can also invalidate your configurations. Hence ensuring accuracy is imperative!

## Usage of Permissive or No-action DMARC Policies

A DMARC "none" policy is a no-action policy. This means that even if a message fails DMARC authentication - it still gets delivered to your recipient's inbox! Your domain at p=none is not protected against cyber attacks. To reinforce this, recently, Hacker Group Kimsuky launched a series of phishing attacks exploiting domains using permissive DMARC policies.

Starting with DMARC set to "none" helps in monitoring email traffic and activities, but staying at this level for too long is ineffective. By gradually yet safely upgrading your DMARC policy to "quarantine" or "reject," you can better protect against domain spoofing.

Many Swiss organizations currently have their DMARC policy set to "none," which weakens their domain security. Leveraging a DMARC analyzer can facilitate a smooth transition to stricter enforcement, significantly decreasing the risk of domain misuse.

### Missing MTA-STS and TLS-RPT Records

MTA-STS secures SMTP emails by enforcing transmission over encrypted TLS channels, preventing interception techniques such as man-in-the-middle attacks. Adopting MTA-STS significantly boosts your email's security. However, numerous domains in Switzerland have not implemented MTA-STS, making them susceptible to attacks. SMTP TLS Reports work alongside MTA-STS by offering insights into email delivery issues caused by TLS encryption failures.

### SPF Exceeding the Maximum Lookup Limit

RFC specifies SPF processing limits for domain owners, stating that SPF implementers must keep their DNS lookup count under 10. Several mechanisms and modifiers such as "include" "ptr" "redirect" etc adds to the lookup count. Your third party email vendors also add complexities. Hence exceeding the 10 DNS lookup limit is very common, breaking SPF and returning errors. A considerable portion of Swiss domains have invalid SPF records, likely due to the common issue of exceeding the DNS lookup limit.

### DNSSEC Disabled for Domains

DNSSEC is a collection of IETF extensions that help in digital signing information shared on your DNS. It enhances your DNS's security through authentication and facilitates protected information exchanges in DNS servers. DNSSEC can help prevent DNS-level cyber attacks like DNS spoofing.

The majority of Swiss domains belonging to all sectors had DNSSEC disabled leaving their DNS vulnerable to exfiltration and tampering.

### Multiple DMARC/SPF Records for the Same Domain

It's crucial to ensure that each domain has a single SPF and DMARC record. Having multiple records for the same domain will invalidate SPF. This is a common mistake among organizations in Switzerland, but it can be corrected. Therefore, it's important to avoid configuring multiple records for a single domain.

## How Can Organizations in Switzerland Improve Email Security?

To improve their email security posture, organizations and governments in Switzerland can take the following steps:

1. Ensure that they are staying under SPF character length and lookup limits
2. Implement accurate and error free SPF, DMARC and MTA-STS records
3. Publish only 1 SPF and DMARC record per domain
4. Enable DMARC RUA and RUF reports for monitoring domains and sending sources
5. Make a gradual and planned shift from p=none to p=reject DMARC policy for protection against email-based attacks
6. Enable MTA-STS and TLS-RPT to ensure TLS-encrypted SMTP communications
7. Enable DNSSEC to add a layer of authentication and security for your DNS
8. Enable BIMI to attach your brand logo to authenticated emails and increase customer trust

# How Can We Help You in this Process

Ensuring the security of your emails is paramount for organizations of all sizes. We understand the importance of safeguarding your communications from cyber threats. That's why we offer a comprehensive suite of email and domain security solutions tailored to meet your organization's needs.

- **Complete Email Authentication Suite**

  Our team provides expert guidance in configuring and managing key email authentication protocols like DMARC, DKIM, and SPF. We ensure that your records are error-free and optimized for the highest level of security.

- **Hosted Email Authentication Services**

  We offer a variety of hosted email authentication services, including hosted DMARC, DKIM, SPF, MTA-STS, TLS-RPT, and BIMI. Our cloud-native platform simplifies configuration and updates, eliminating the need for multiple DNS accesses.

- **Smart and Simple Reporting**

  Our smart and user-friendly reporting keeps you informed about your email authentication status. With daily aggregate and forensic DMARC reports, monitoring your email activity becomes effortless and effective. Reports can be further downloaded in PDF/CSV formats to share with your internal team.

- **Dedicated 24/7 Support**

  Our team of experts provides exceptional support to help you transition smoothly to DMARC enforcement and improve compliance. We go above and beyond to ensure you can make the most out of your protocols.

- **Optimized SPF Records**

  You can optimize your SPF records in a few easy steps by leveraging the power of SPF Macros on our platform. We help you stay within the DNS lookup and SPF length limits, ensuring your SPF protocol functions properly.

- **Reputation Monitoring**

  Keep an eye on your domain's reputation and address issues before they become problems with our reputation monitoring services. We track your domains and IPs across 200+ DNS blocklists to help prevent email rejections or flagging.

- **Real-time Alerts**

  Set up customized alerts to stay informed about any email security issues. Receive notifications via email, Slack, Discord, or webhook alerts, ensuring timely action to mitigate risks.

- **Compliance Assistance**

  Comply with the latest email sender requirements and compliance mandates including Google, Yahoo, and the upcoming PCI-DSS regulations. We help you meet these requirements fast and easily, by getting you started on our compliance program.

- **MSP Partnership Programs**

  Partner with PowerDMARC for managed security services tailored to your organization's needs. Our DMARC MSP/MSSP-ready platform and dedicated service desk ensure comprehensive support for your email security efforts. We also provide full-platform white labeling opportunities to our MSPs, dedicated training materials, and much more!

Let's join hands to increase the rate of DMARC adoption and strengthen the email security infrastructure in businesses across Switzerland. Get in touch with us at support@powerdmarc.com to find out how we can help protect your domain and business today!