Saudi Arabia (KSA) DMARC & MTA-STS Adoption Report 2025

POWERDMARC

POWERDMARC

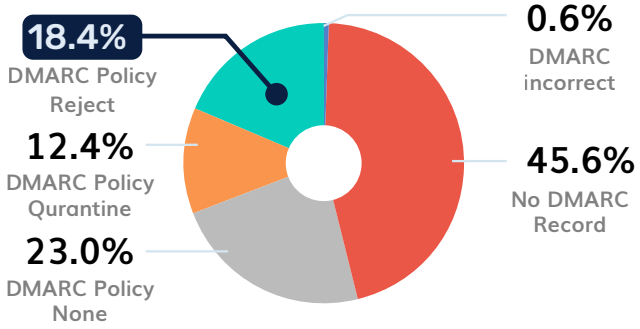
Case study

Saudi Arabia (KSA) DMARC & MTA-STS Adoption Report 2025

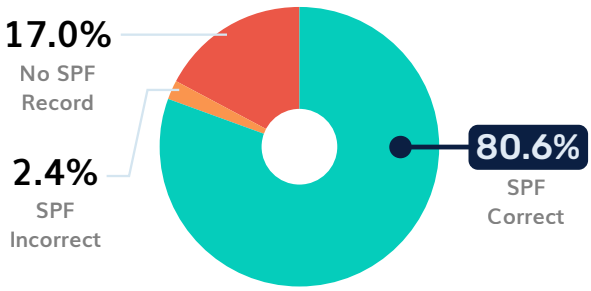
- Riyadh is accelerating **Vision 2030** through giga-projects like NEOM and a surging fintech ecosystem. However, this digital leap has expanded the attack surface. In response, the **National Cybersecurity Authority (NCA)** has enforced the **ECC-2:2024 (Essential Cybersecurity Controls)**.

- While 73% of Saudi organizations now prioritize digital and technology-related risks, significantly higher than the 51% global average, a critical technical gap remains. This PowerDMARC analysis of **1,234 domains** across 18 sectors reveals strong starts in basic authentication (SPF) but falls behind in enforcement (DMARC p=reject) and encryption (MTA-STS).

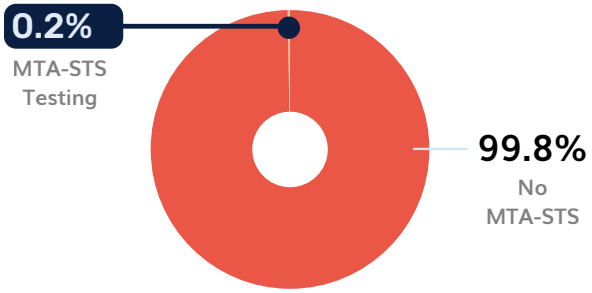
KSA DMARC Adoption Analysis



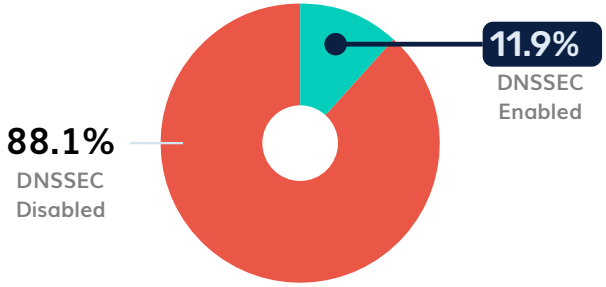
KSA SPF Adoption Analysis



KSA MTA-STS Adoption Analysis



KSA DNSSEC Adoption Analysis



KSA Email Security Metrics

The Kingdom faces a significant "Enforcement Gap."

Metric	Adoption Rate	Status	Risk Level
SPF Adoption	80.6%	Good	Low (though 1 in 6 still fail)
DMARC Coverage	54.4%	Moderate	CRITICAL (45.6% have NO DMARC)
DMARC Enforcement (p=reject)	18.4%	Failing	ULTRA-HIGH (81.6% are passive)
MTA-STS Adoption	0.2%	Extremely low	MAXIMUM (99.8% exposed to MITM)
DNSSEC Adoption	11.9%	Poor	High

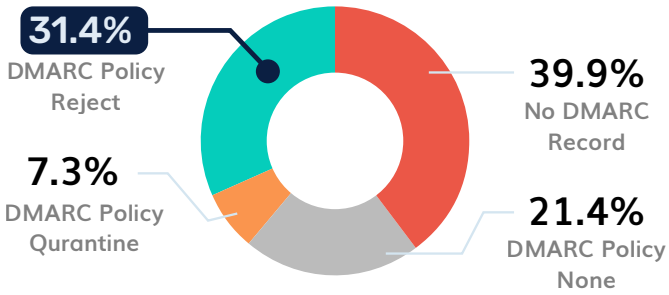
Translation: Attackers can spoof 4 out of 5 Saudi domains with ease. Recent **ZATCA-themed tax scams** have already defrauded citizens of millions by exploiting these exact technical gaps.

Sector-by-Sector Breakdown

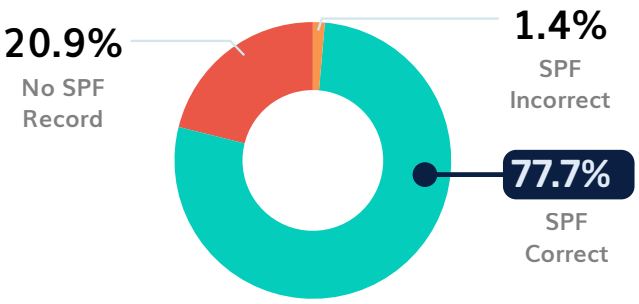
1 Government

The government sector leads the nation in **DMARC enforcement**, driven by the **National Cybersecurity Authority's (NCA) ECC-2:2024** mandates. However, the stakes remain the highest here.

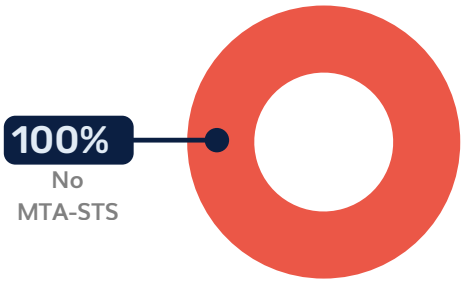
DMARC Adoption Analysis (Government)



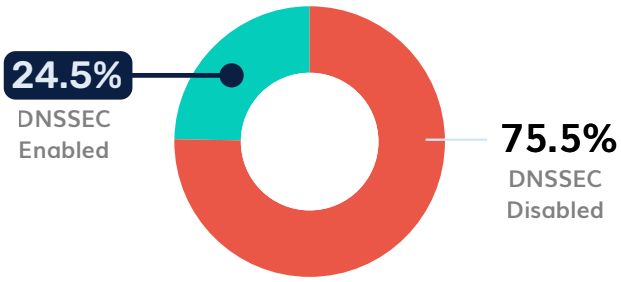
SPF Adoption Analysis (Government)



MTA-STS Adoption Analysis (Government)



DNSSEC Adoption Analysis (Government)



Metric	Percentage
SPF	77.7%
DMARC (Reject)	31.4%
No DMARC	39.9%
MTA-STS	0.0%
DNSSEC	24.6%

The Threat:

In 2025, dark web threat actors leaked login credentials for various systems, including the **Noor System** and platforms under the **Ministry of Human Resources**.

Vision 2030 Impact:

Impersonation of platforms like **Absher** or **Nafath** doesn't just steal data; it erodes the "Digital First" trust foundational to Saudi Arabia's modernization.

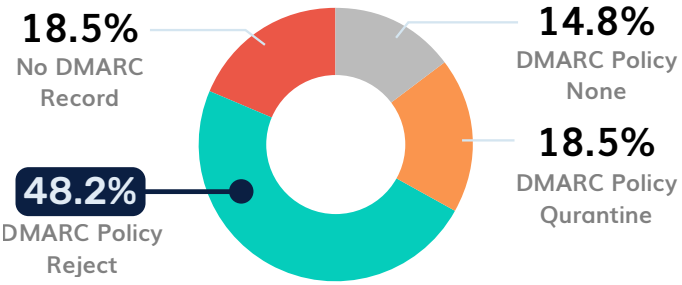
The PowerDMARC Solution

PowerDMARC automates the path to p=reject to meet NCA ECC-2:2024 mandates, ensuring .gov.sa domains are fortified against state-sponsored impersonation.

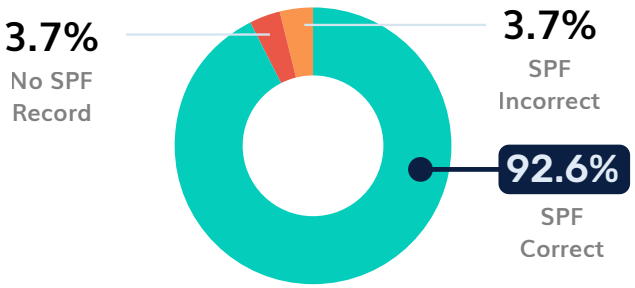
2 Banking

Under the strict oversight of **SAMA (Saudi Central Bank)** and its **Cyber Security Framework**, the banking sector is the most fortified, yet remains the "Crown Jewel" for attackers.

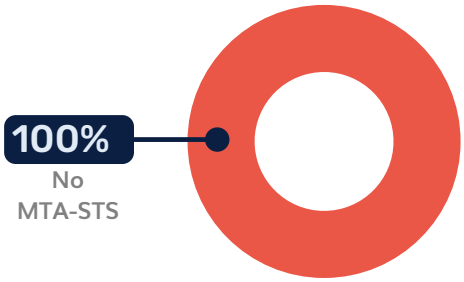
DMARC Adoption Analysis (Banking)



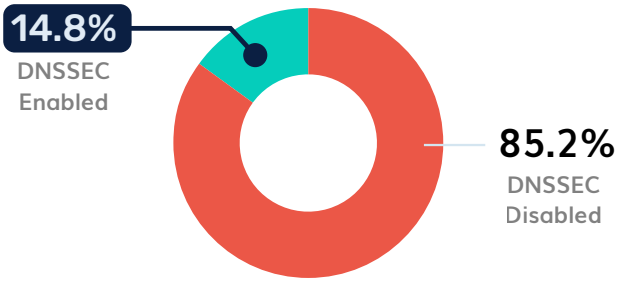
SPF Adoption Analysis (Banking)



MTA-STS Adoption Analysis (Banking)



DNSSEC Adoption Analysis (Banking)



Security Protocol	Adoption Rate
SPF	92.6%
DMARC (Reject)	48.2%
No DMARC	18.5%
MTA-STS	0.0%
DNSSEC	14.8%

The Threat:

Recent leaks advertised over **690,000 high-value account records** from Saudi banks on Chinese cybercrime forums.

The "Final Mile" Risk:

While nearly 50% have hit p=reject, the remaining domains are exploited for **Business Email Compromise (BEC)**.

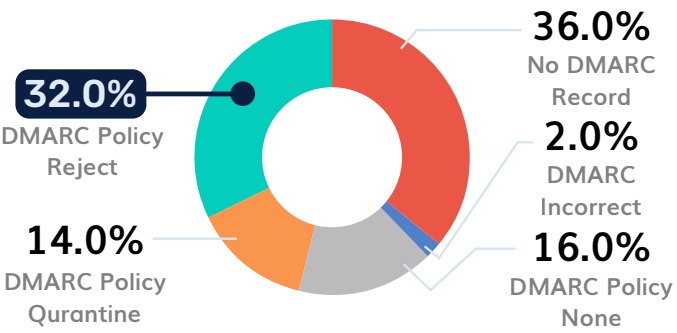
The PowerDMARC Solution

Our platform aligns with SAMA's Cybersecurity Framework by enforcing strict DMARC policies and providing encrypted forensic reports to stop financial fraud and BEC.

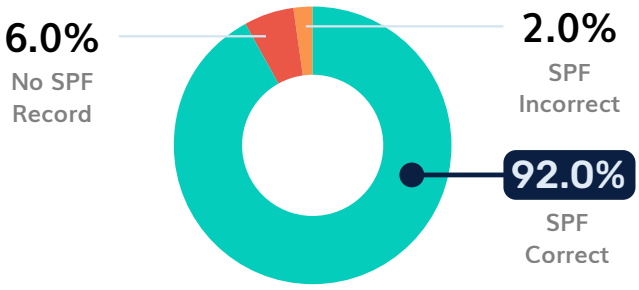
3 Energy

The backbone of the Saudi economy. Following the 2025 campaigns targeting **Aramco** supply chains, the vulnerability of this sector is a matter of national security.

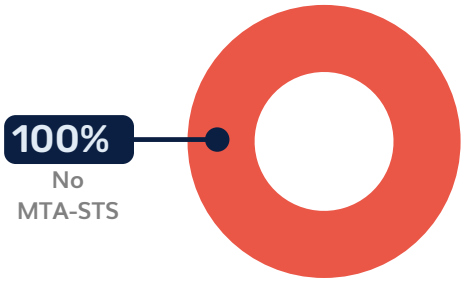
DMARC Adoption Analysis (Energy)



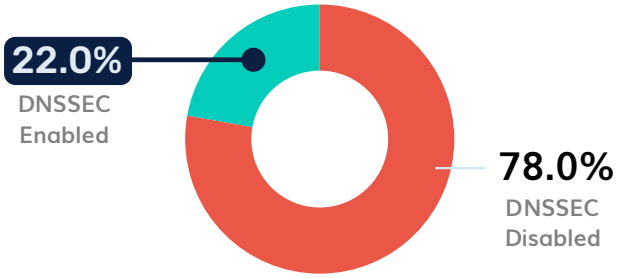
SPF Adoption Analysis (Energy)



MTA-STS Adoption Analysis (Energy)



DNSSEC Adoption Analysis (Energy)



Security Protocol	Adoption Rate
SPF	92.0%
DMARC (Reject)	32.0%
No DMARC	36.0%
MTA-STS	0.0%
DNSSEC	22.0%

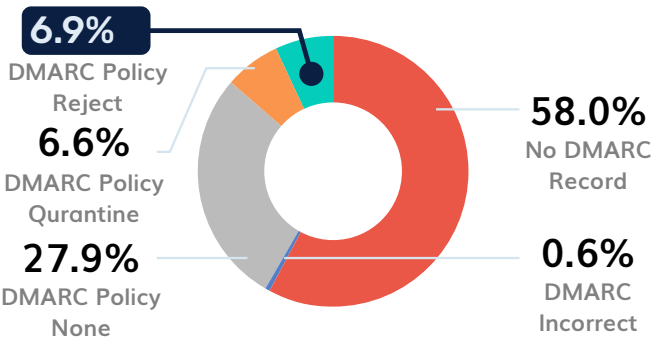
OT Risk:
Attackers use spoofed supplier emails to deliver ransomware that bridges the gap between IT and OT systems, threatening oil production.

The PowerDMARC Solution
PowerDMARC secures global energy supply chains by identifying and blocking spoofed vendor emails that target critical OT (Operational Technology) infrastructure.

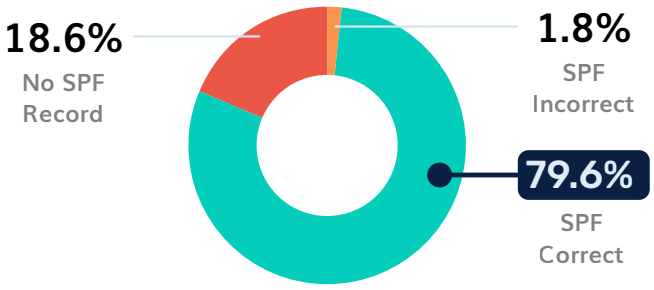
4 Technology

The very sector building the Kingdom's future is the most technically exposed.

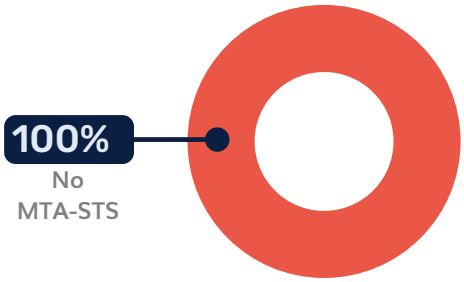
DMARC Adoption Analysis (Technology)



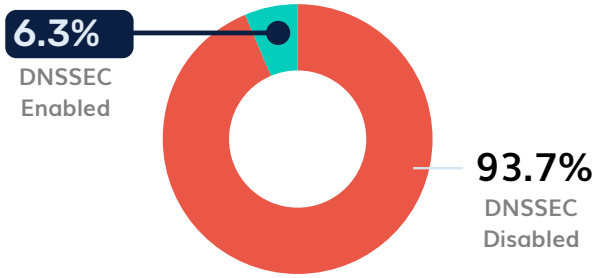
SPF Adoption Analysis (Technology)



MTA-STS Adoption Analysis (Technology)



DNSSEC Adoption Analysis (Technology)



Security Protocol	Adoption Rate
SPF	79.6%
DMARC (Reject)	6.9%
No DMARC	58.0%
MTA-STS	0.0%
DNSSEC	6.3%

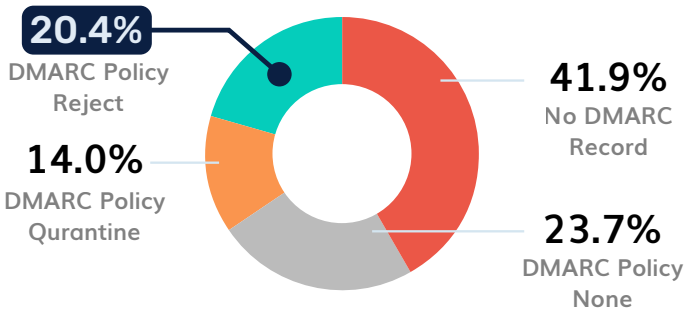
IP Theft:
58% of domains offer zero protection. This is exploited to phish tech founders by spoofing major VC firms like **STV**.

The PowerDMARC Solution
We solve the problem by instantly identifying unauthorized senders across massive tech ecosystems, protecting intellectual property and venture funding communications.

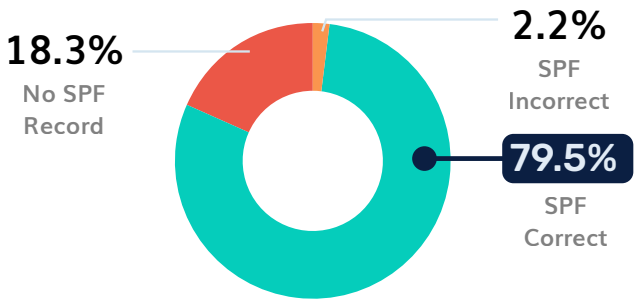
5 Healthcare

A primary target for ransomware and the theft of **Protected Health Information (PHI)**.

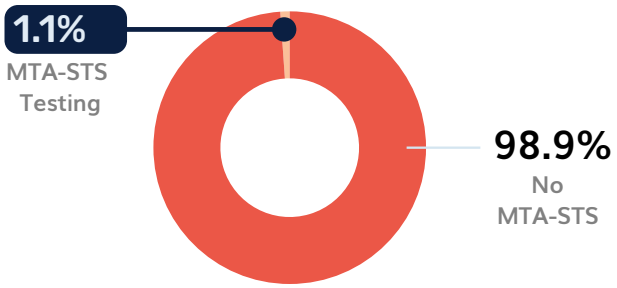
DMARC Adoption Analysis (Healthcare)



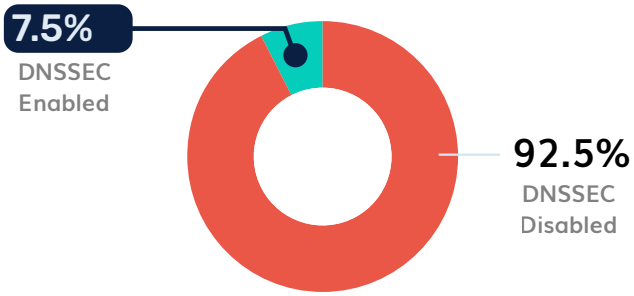
SPF Adoption Analysis (Healthcare)



MTA-STS Adoption Analysis (Healthcare)



DNSSEC Adoption Analysis (Healthcare)



Security Protocol	Adoption Rate
SPF	79.5%
DMARC (Reject)	20.4%
No DMARC	41.9%
MTA-STS	1.1%
DNSSEC	7.5%

Patient Privacy:
Spoofed clinic bills are being used to harvest biometric data, which cannot be reset like a password if stolen.

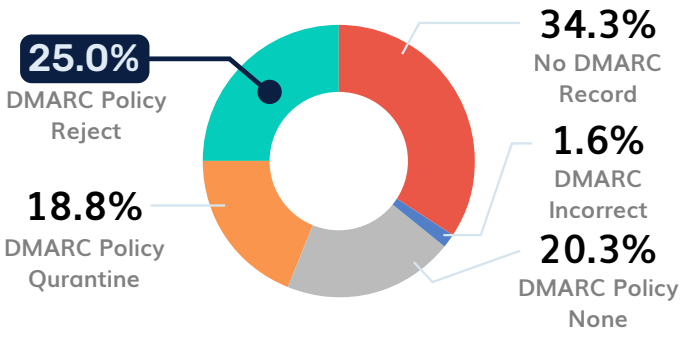
The PowerDMARC Solution

PowerDMARC safeguards patient data by enforcing email authentication and hosted MTA-STS, ensuring medical communications and records remain encrypted and untampered.

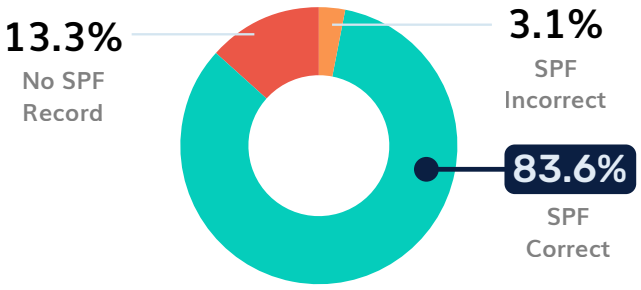
6 CMA Regulated Entities

Capital Market Authority entities act as the gatekeepers of wealth. Their lack of enforcement is a systemic risk to the **Tadawul**.

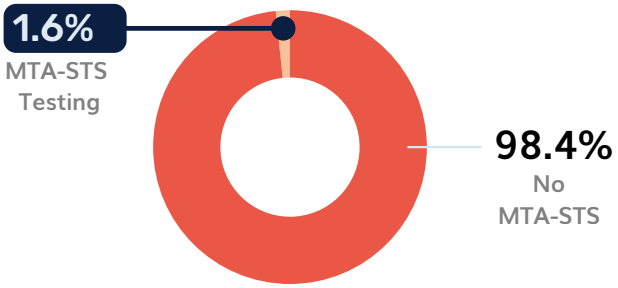
DMARC Adoption Analysis (CMA)



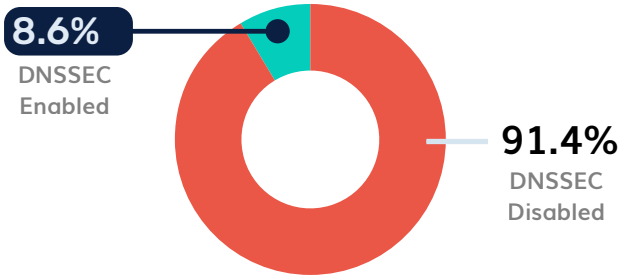
SPF Adoption Analysis (CMA)



MTA-STS Adoption Analysis (CMA)



DNSSEC Adoption Analysis (CMA)



Security Protocol	Adoption Rate
SPF	83.6%
DMARC (Reject)	25.0%
No DMARC	34.3%
MTA-STS	1.6%
DNSSEC	8.6%

Market Manipulation:

Spoofed market alerts can trigger panic selling or "pump and dump" schemes on the **Tadawul**.

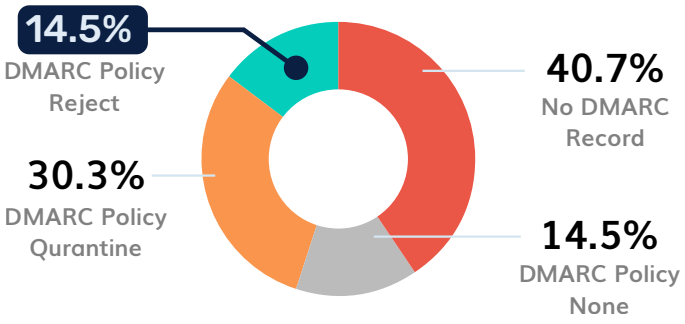
The PowerDMARC Solution

We provide real-time threat intelligence to stop market-manipulating spoofing attempts, ensuring that Tadawul alerts and investor communications remain authentic.

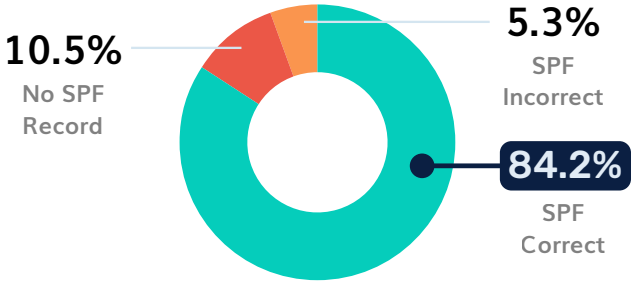
7 Telecoms

The critical gateway for **SIM-swap attacks** and Multi-Factor Authentication (MFA) bypass.

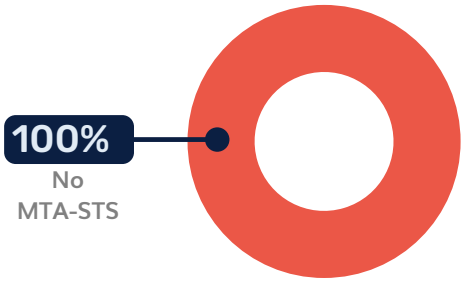
DMARC Adoption Analysis (Telecoms)



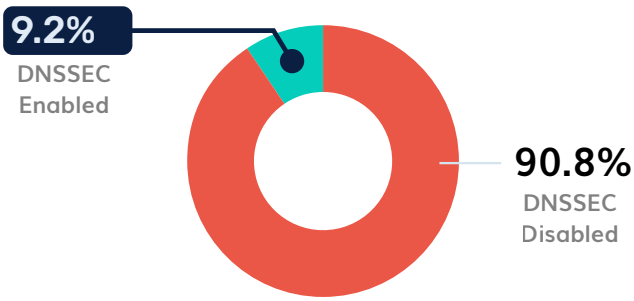
SPF Adoption Analysis (Telecoms)



MTA-STS Adoption Analysis (Telecoms)



DNSSEC Adoption Analysis (Telecoms)



Security Protocol	Adoption Rate
SPF	84.2%
DMARC (Reject)	14.5%
No DMARC	40.7%
MTA-STS	0.0%
DNSSEC	9.2%

The Scam:

Fake **STC** or **Mobily** bills enable attackers to harvest credentials used to social engineer customer service agents.

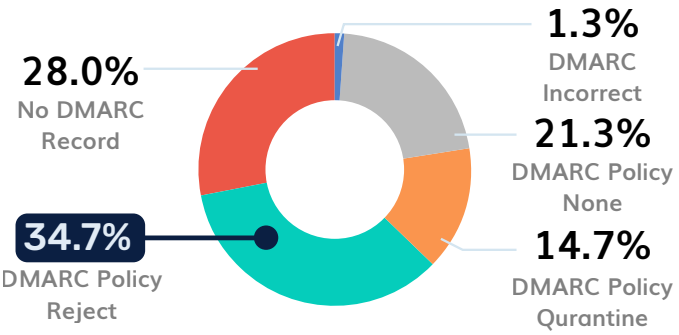
The PowerDMARC Solution

PowerDMARC prevents SIM-swap and account takeover triggers by blocking fraudulent billing alerts and social engineering attempts sent from spoofed telecom domains.

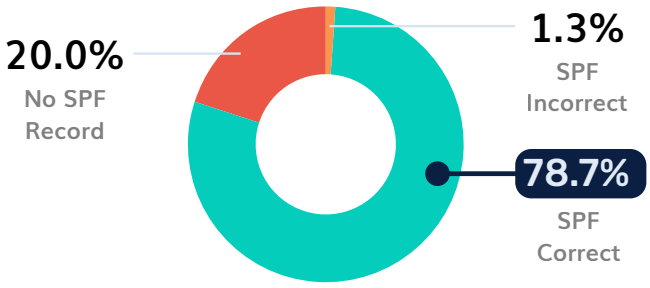
8 Education

A resilient sector compared to others, yet a prime target for high-value research theft.

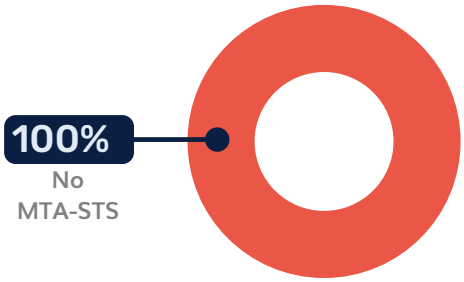
DMARC Adoption Analysis (Education)



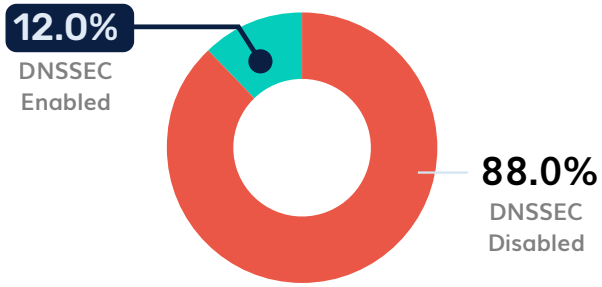
SPF Adoption Analysis (Education)



MTA-STS Adoption Analysis (Education)



DNSSEC Adoption Analysis (Education)



Security Protocol	Adoption Rate
SPF	78.7%
DMARC (Reject)	34.7%
No DMARC	28.0%
MTA-STS	0.0%
DNSSEC	12.0%

Researcher Phishing:

Fake **KAUST** or **KSU** IT alerts are used to steal logins and high-value academic data.

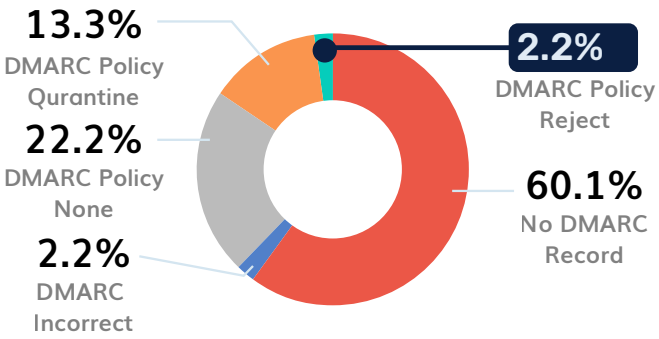
The PowerDMARC Solution

Our platform stops academic credential harvesting by ensuring only authorized IT systems can send emails on behalf of universities and research institutions.

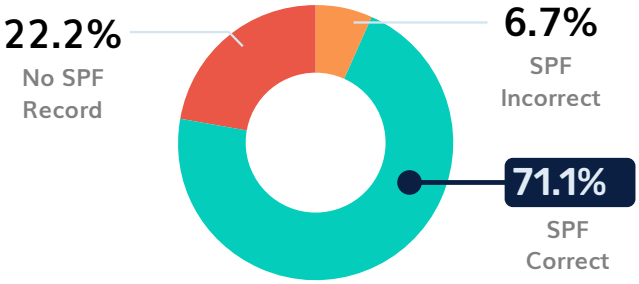
9 Media

The front line of the information war.

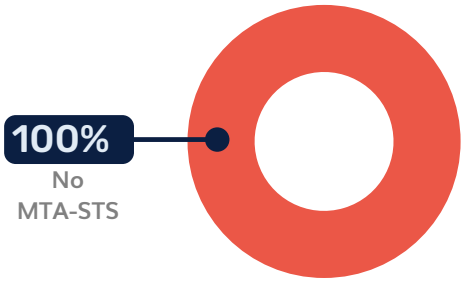
DMARC Adoption Analysis (Media)



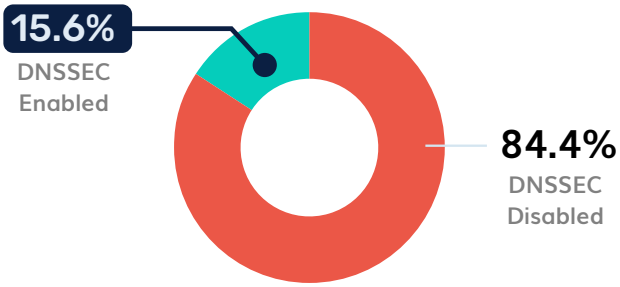
SPF Adoption Analysis (Media)



MTA-STS Adoption Analysis (Media)



DNSSEC Adoption Analysis (Media)



Security Protocol	Adoption Rate
SPF	71.1%
DMARC (Reject)	2.2%
No DMARC	60.1%
MTA-STS	0.0%
DNSSEC	15.6%

Disinfo Vectors:

Attackers can send emails as **Al Arabiya** or **Saudi Gazette** to spread panic or fake news.

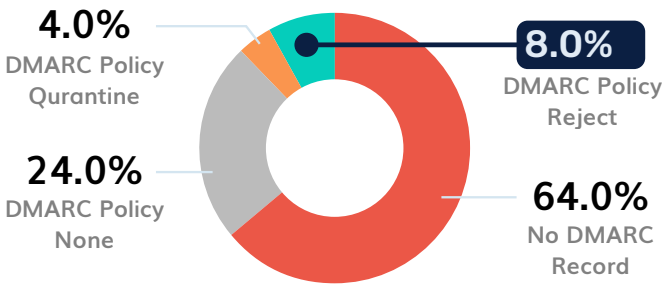
The PowerDMARC Solution

PowerDMARC protects national discourse by preventing attackers from hijacking the reputation of news organizations to spread disinformation or fake news.

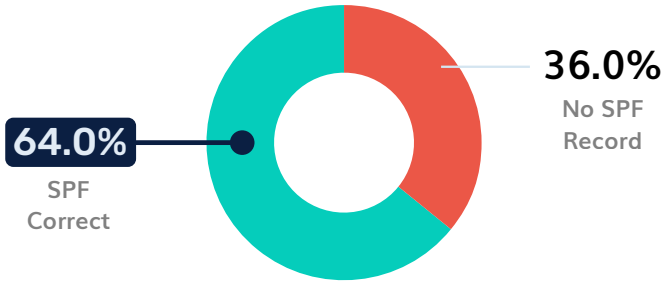
10 Retail & E-commerce

Exploiting the Kingdom's high consumer spending power.

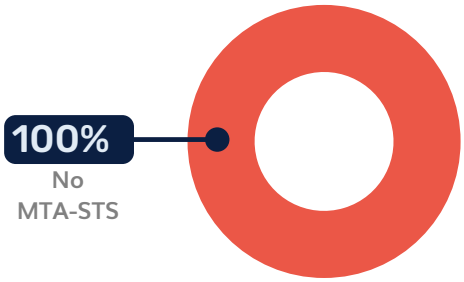
DMARC Adoption Analysis (Retail)



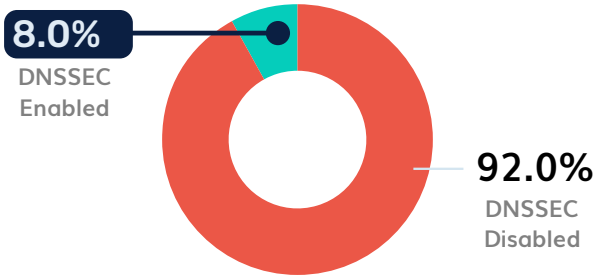
SPF Adoption Analysis (Retail)



MTA-STS Adoption Analysis (Retail)



DNSSEC Adoption Analysis (Retail)



Security Protocol	Adoption Rate
SPF	64.0%
DMARC (Reject)	8.0%
No DMARC	64.0%
MTA-STS	0.0%
DNSSEC	8.0%

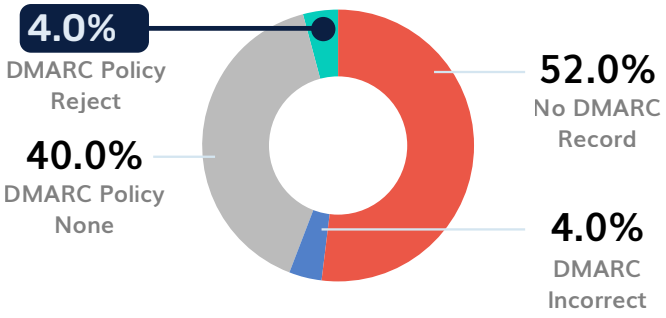
Holiday Scams:
Fake Jarir or **Panda** discounts harvest credit cards during Ramadan surges.

The PowerDMARC Solution
We protect retail brands during high-traffic seasons like Ramadan by blocking fake discount offers and phishing campaigns that harvest customer payment data.

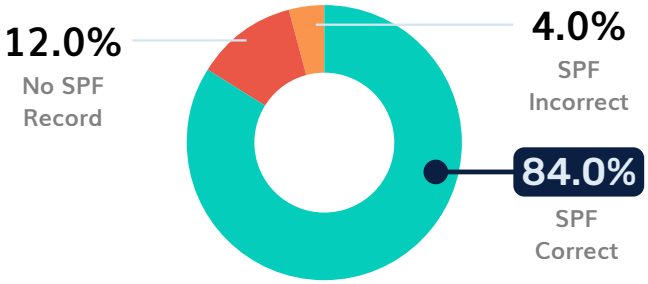
11 Construction

Giga-scams for the Giga-projects.

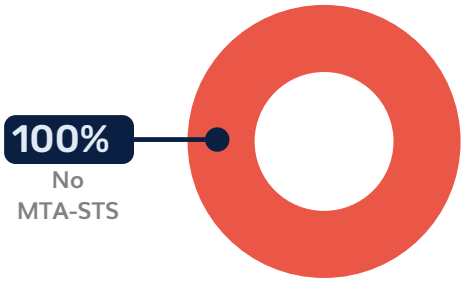
DMARC Adoption Analysis (Construction)



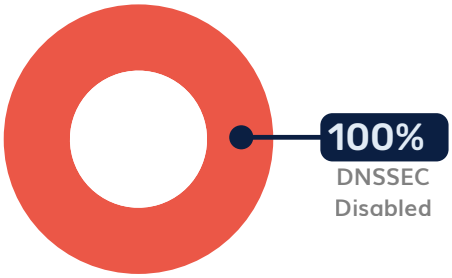
SPF Adoption Analysis (Construction)



MTA-STS Adoption Analysis (Construction)



DNSSEC Adoption Analysis (Construction)



Security Protocol	Adoption Rate
SPF	84.0%
DMARC (Reject)	4.0%
No DMARC	52.0%
MTA-STS	0.0%
DNSSEC	0.0%

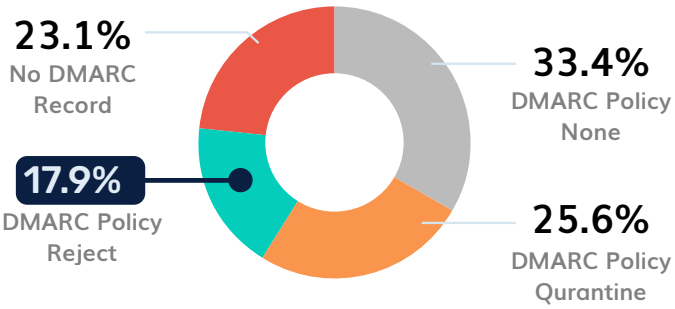
Giga-Scams:
Bogus invoices targeting **NEOM** and **Red Sea Global** projects drain billions in capital.

The PowerDMARC Solution
PowerDMARC secures Giga-project supply chains against multi-million dollar invoice fraud by enforcing strict domain protection for contractors and developers.

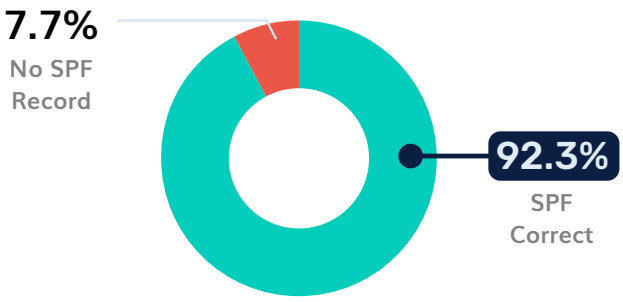
12 Insurance

Personal identity and claims fraud.

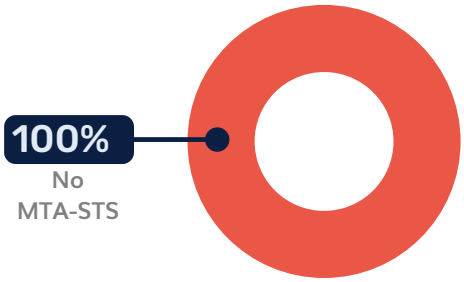
DMARC Adoption Analysis (Insurance)



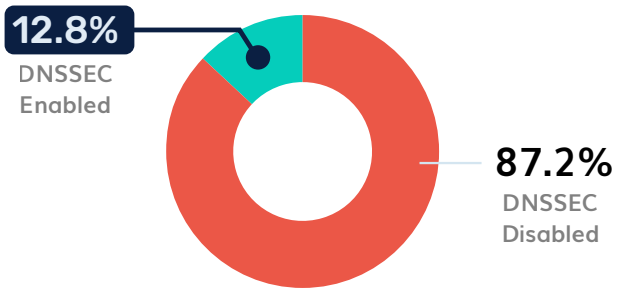
SPF Adoption Analysis (Insurance)



MTA-STS Adoption Analysis (Insurance)



DNSSEC Adoption Analysis (Insurance)



Security Protocol	Adoption Rate
SPF	92.3%
DMARC (Reject)	18.0%
No DMARC	23.1%
MTA-STS	0.0%
DNSSEC	12.8%

Claims Fraud:

Spoofed **Bupa** or **Tawuniya** emails are used to deny payouts or steal sensitive data.

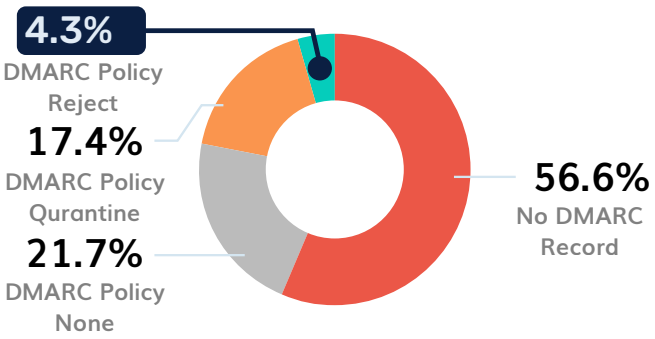
The PowerDMARC Solution

Our solution ensures that claims and policy communications are authenticated, stopping attackers from stealing sensitive medical identity data through spoofed insurance emails.

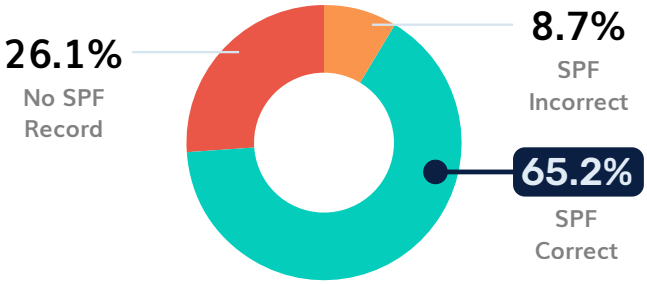
13 Finance

A massive surface area outside of SAMA-regulated banks.

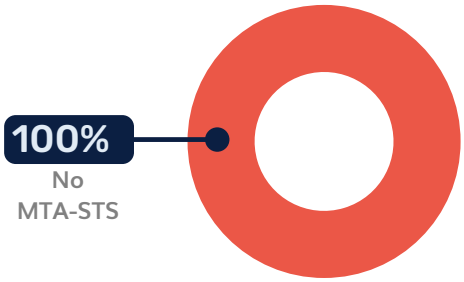
DMARC Adoption Analysis (Finance)



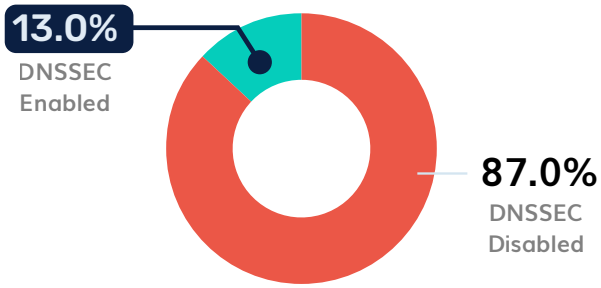
SPF Adoption Analysis (Finance)



MTA-STS Adoption Analysis (Finance)



DNSSEC Adoption Analysis (Finance)



Security Protocol	Adoption Rate
SPF	65.2%
DMARC (Reject)	4.4%
No DMARC	56.6%
MTA-STS	0.0%
DNSSEC	13.0%

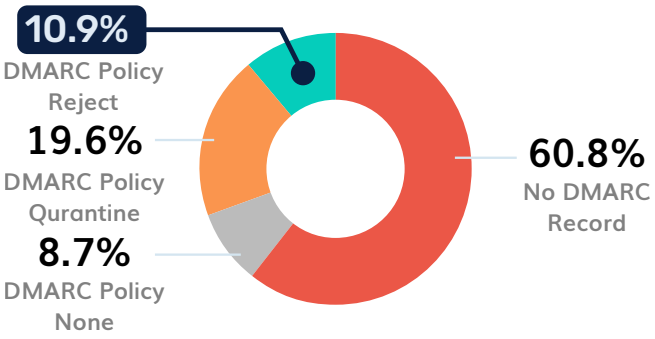
SME Risk:
Invoice fraud via spoofed finance domains often cripples small-to-medium enterprises.

The PowerDMARC Solution
We bridge the security gap for SMEs and finance firms by providing an easy-to-manage platform that stops invoice fraud and Business Email Compromise (BEC).

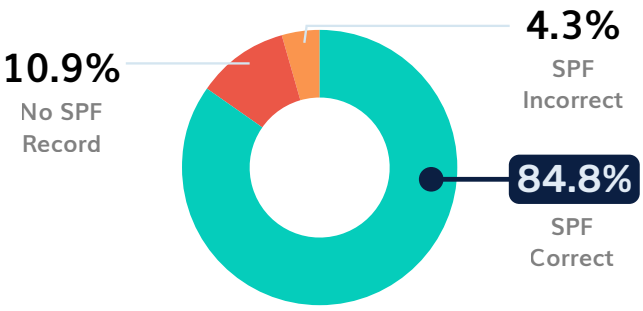
14 Transport & Logistics

The logistics hub ambition faces a "digital checkpoint" problem.

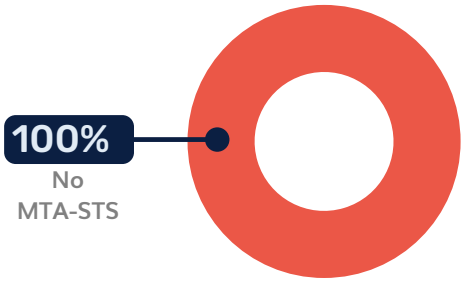
DMARC Adoption Analysis (Transport)



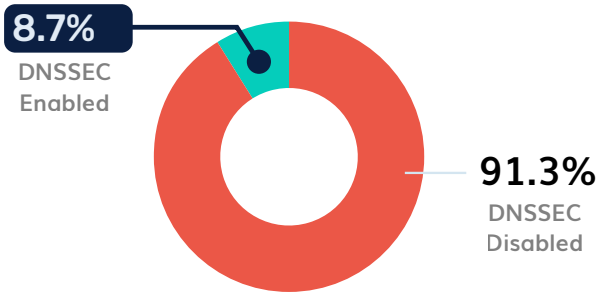
SPF Adoption Analysis (Transport)



MTA-STS Adoption Analysis (Transport)



DNSSEC Adoption Analysis (Transport)



Security Protocol	Adoption Rate
SPF	84.8%
DMARC (Reject)	10.9%
No DMARC	60.8%
MTA-STS	0.0%
DNSSEC	8.7%

Cargo Redirection:

Spoofed **SAPTCO** or shipping line emails are used to redirect cargo and scam fares.

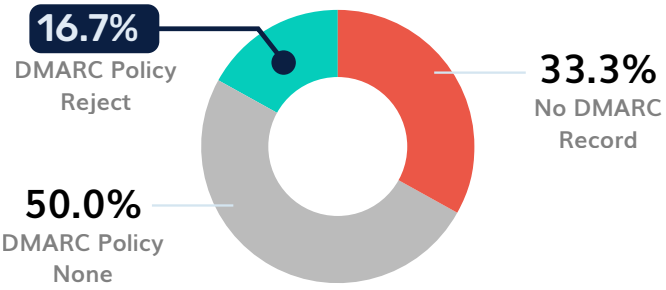
The PowerDMARC Solution

PowerDMARC secures the "Digital Silk Road" by preventing cargo theft and logistics redirection through the authentication of shipping manifests and transport alerts.

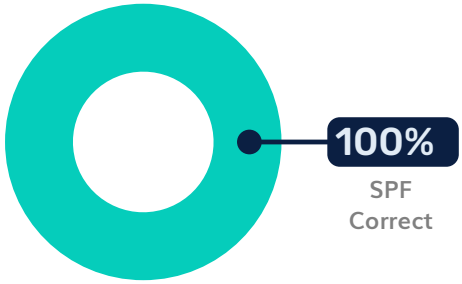
15 Real Estate

High-value, low-frequency transactions are a playground for wire fraud.

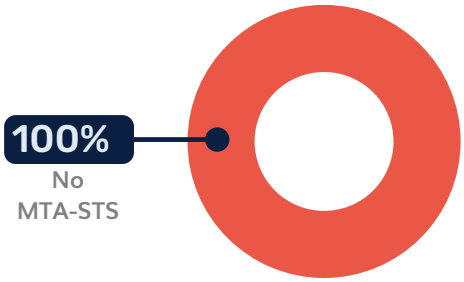
DMARC Adoption Analysis (Real Estate)



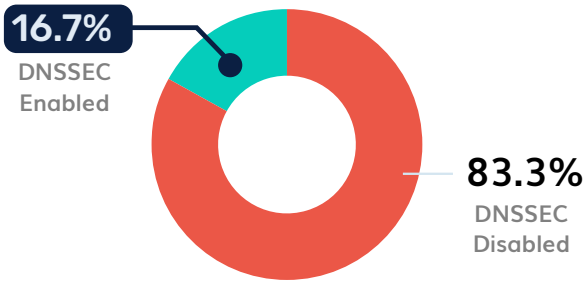
SPF Adoption Analysis (Real Estate)



MTA-STS Adoption Analysis (Real Estate)



DNSSEC Adoption Analysis (Real Estate)



Security Protocol	Adoption Rate
SPF	100.0%
DMARC (Reject)	16.7%
No DMARC	33.3%
MTA-STS	0.0%
DNSSEC	16.7%

Escrow Fraud:

Fake **Emaar** or **ROSHN** offers phish credentials to initiate SAR 50M+ invoice frauds.

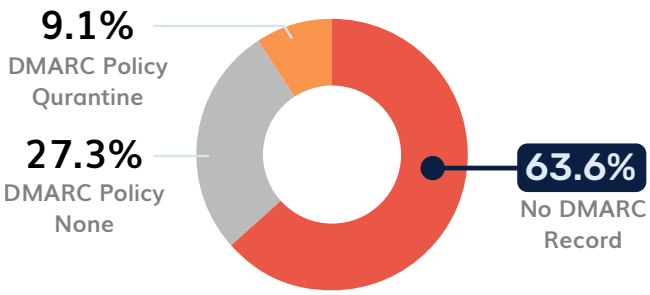
The PowerDMARC Solution

We protect high-value property transactions by ensuring that only genuine, authenticated emails can be sent from prestigious real estate development domains.

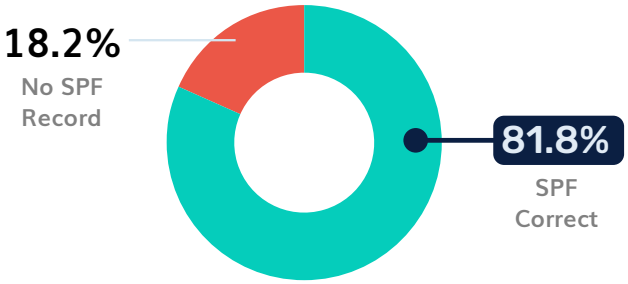
16 Travel & Tourism

Affecting millions of travelers.

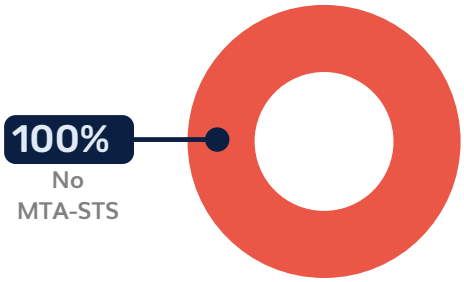
DMARC Adoption Analysis (Travel & Tourism)



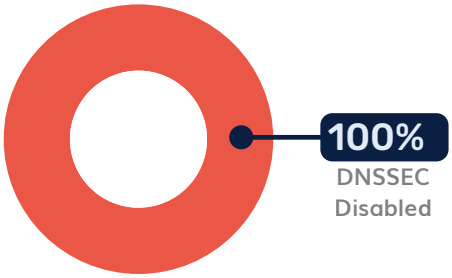
SPF Adoption Analysis (Travel & Tourism)



MTA-STS Adoption Analysis (Travel & Tourism)



DNSSEC Adoption Analysis (Travel & Tourism)



Security Protocol	Adoption Rate
SPF	81.8%
DMARC (Reject)	0.0%
No DMARC	63.6%
MTA-STS	0.0%
DNSSEC	0.0%

Hajj/Umrah Fraud:

0% enforcement means attackers can spoof **Saudia** airlines or Hajj ministries at will. Pilgrims are targeted with fake “visa refund” or “booking update” phishes.

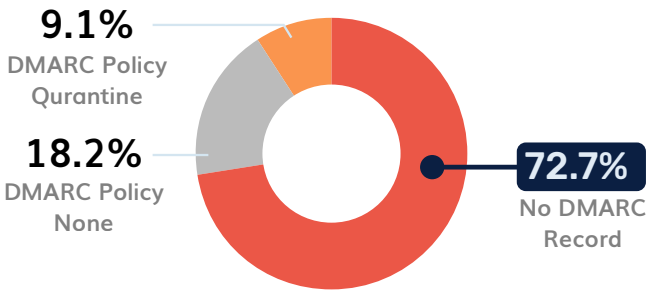
The PowerDMARC Solution

PowerDMARC protects pilgrims and tourists by blocking fraudulent booking and visa scams that impersonate airlines and tourism ministries.

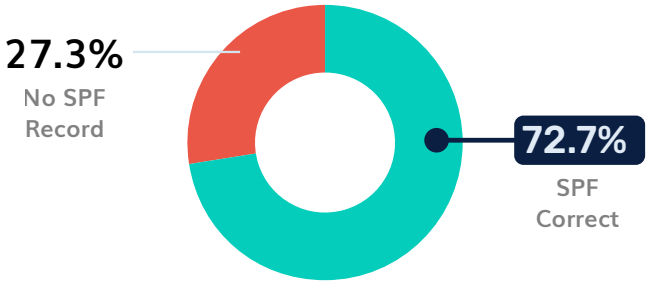
17 Food & Beverage

Supply chain disruptions that threaten food security.

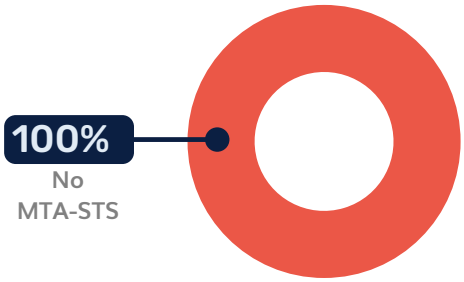
DMARC Adoption Analysis (Food)



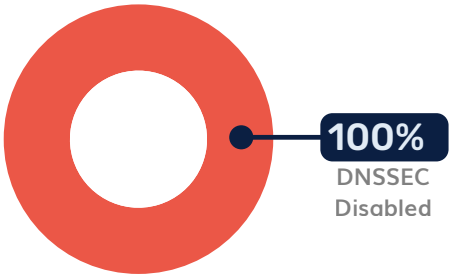
SPF Adoption Analysis (Food)



MTA-STS Adoption Analysis (Food)



DNSSEC Adoption Analysis (Food)



Security Protocol	Adoption Rate
SPF	72.7%
DMARC (Reject)	0.0%
No DMARC	72.7%
MTA-STS	0.0%
DNSSEC	0.0%

Supply Problems:

Fake **Almarai** or **Nadec** orders can disrupt chains or lead to massive logistics waste.

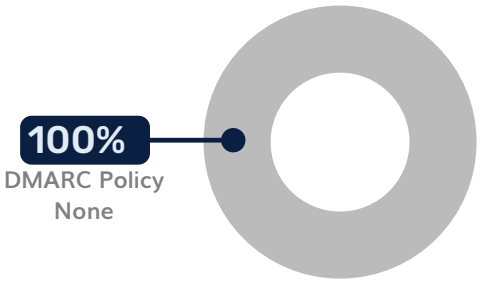
The PowerDMARC Solution

Our platform prevents supply chain problems by authenticating purchase orders and logistics communications, ensuring the integrity of the national food supply.

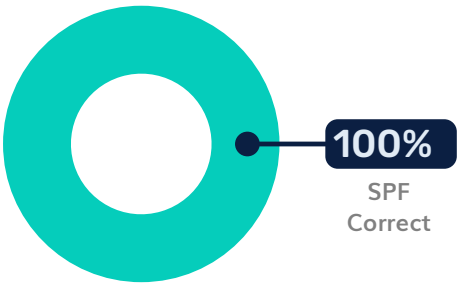
18 Fintech

The sector built on digital trust is under threat.

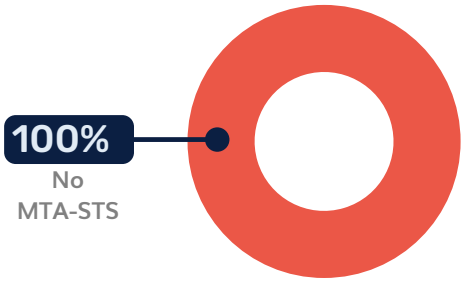
DMARC Adoption Analysis (Fintech)



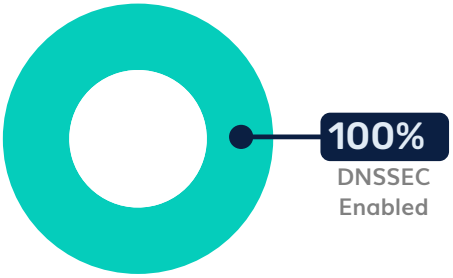
SPF Adoption Analysis (Fintech)



MTA-STS Adoption Analysis (Fintech)



DNSSEC Adoption Analysis (Fintech)



Security Protocol	Adoption Rate
SPF	100.0%
DMARC (Reject)	0.0%
No DMARC	0.0%
MTA-STS	0.0%
DNSSEC	0.0%

Wallet Draining:

Spoofed **STC Pay** alerts can lead to direct financial loss for millions of app users.

The PowerDMARC Solution

We enable rapid, secure scaling for fintechs by moving domains from passive p=none to active p=reject without disrupting critical transactional email flow.

Under the Hood: Four Structural Weaknesses in KSA

Beyond sector-specific data, four systemic vulnerabilities compromise the Kingdom's digital defenses. As Saudi Arabia pushes toward **Vision 2030**, the gap between basic compliance and active enforcement has become a primary target for sophisticated threat actors.

1. The "Comfort Trap" of p=none

While KSA shows a high intent to secure domains, **23.0%** of domains are stuck in the "Comfort Trap" of p=none. This monitoring-only mode provides visibility but stops zero attacks.

Metric	Detail	Status
Active Monitoring (p=none)	23.0% of DMARC-enabled domains	**Vulnerable**
Primary Risk	False sense of security while spoofing continues.	**High**

"Keeping DMARC to p=none for too long is like hiring a security guard to watch your door being kicked in but forbidding them from intervening. You see the crime, but you don't stop it. As more state governments mandate anti-spoofing measures, we must move from watching to blocking."

Maitham Al Lawati, CEO, PowerDMARC

2. SPF Complexity and the Giga-Project Scale

Saudi Arabia has a strong SPF foundation at **80.6%**, but the **19.4%** failure rate often stems from the technical "10-lookup limit." This is particularly prevalent in massive entities like **NEOM** or **Aramco** that use dozens of third-party SaaS vendors.

Metric	Detail	Status
SPF Adoption	80.6%	**Strong Start**
SPF Failure Rate	19.4% (PermError due to lookup limits)	**Critical Gap**

"In the world's race to digitize, organizations are layering CRMs, marketing tools, and HR platforms onto their domains. Each one adds a DNS lookup. Once you hit that 10-lookup ceiling, your SPF record breaks, and legitimate business emails start disappearing into spam folders. 'SPF Optimization' is no longer optional for enterprises; it's a deliverability lifeline."

Yunes Tarada, Service Delivery Manager, PowerDMARC

3. MTA-STS: The Encryption Blind Spot

With a dismal **0.2%** adoption rate, the Kingdom faces a near-total exposure to **Man-in-the-Middle (MiTM)** attacks. Without MTA-STS, attackers can force "Downgrade Attacks," stripping away encryption to read sensitive government or financial data in plain text.

Metric	Detail	Status
MTA-STS Validity	0.2%	**Abysmal**
Exposure Level	99.8% of domains risk plain-text interception.	**Maximum Risk**

"Standard email encryption is polite; it asks to be used. MTA-STS is a mandate; it requires it. With 99.8% of Saudi domains lacking this, it is easy for a sophisticated attacker to intercept and read sensitive corporate communications in transit. Enabling MTA-STS can significantly improve the KSA's email defense."

Ayan Bhuiya, Operations & Delivery Shift Lead, PowerDMARC

4. DNSSEC: The Foundation of Identity

DNSSEC adoption sits at **11.9%**. Without it, the "phonebook of the internet" is unprotected. This allows for DNS hijacking, where an attacker can redirect a company's entire email flow to a rogue server.

Metric	Detail	Status
DNSSEC Adoption	11.9%	**Weak**
Primary Risk	DNS Hijacking and redirection of email traffic.	**High**

"DNSSEC helps ensure that DNS responses haven't been tampered with. For organizations in Saudi Arabia that manage sensitive citizen data, it adds an important layer of trust and integrity to online services."

Ahona Rudra, Marketing Manager, PowerDMARC

Global Benchmarking: Saudi Arabia in Context

To understand the "Saudi Gap," we compare the Kingdom's 2025 data against global leaders and emerging markets. While Saudi Arabia leads in some foundational areas, its **Enforcement Rate (p=reject)** is the critical differentiator.

The Global Leaderboard: 2025 Data

Source: PowerDMARC 2025 Regional Adoption Reports

Country	SPF Correct	DMARC Adoption	DMARC Enforcement (p=rejct)	MTA-STS
 Sweden	85.0%	77.9%	**29.9%**	2.9%
 Norway	85.2%	83.1%	**29.0%**	2.8%
 Belgium	90.1%	79.1%	**24.7%**	<1.0%
 Peru	86.1%	66.0%	**17.9%**	0.6%
 Nigeria	70.3%	45.9%	**14.2%**	0.0%
 Saudi Arabia	80.6%	54.4%	**18.4%**	**0.2%**
 Japan	95.0%	74.6%	**9.2%**	0.5%

Critical Insights: Where the Kingdom of Saudi Arabia Stands

1 The Enforcement Leader in the Region:

Saudi Arabia's **18.4%** enforcement rate is actually higher than Japan's (9.2%), showing that Saudi regulators (NCA/SAMA) are effectively pushing for actual protection, not just "check-the-box" compliance.

2 The Encryption Crisis:

Despite superior DMARC enforcement compared to Japan, KSA trails significantly in **MTA-STS (0.2%)**. This suggests that while Saudi domains are getting better at stopping spoofing, they are still highly vulnerable to interception.

3 The Nordic Scenario:

To reach global parity, KSA must nearly double its current enforcement rate to match nations that leverage automated platforms to manage the transition to p=reject.

The PowerDMARC Verdict

- Saudi Arabia has real regulatory teeth and a growing enforcement rate. However, as KSA builds the world's most advanced smart cities, its email transit remains largely unencrypted and open to interception.

- The move from **80.6% SPF** to a kingdom-wide **p=reject** and **MTA-STS** adoption is the final hurdle in securing the digital gates of Vision 2030.

The Path to Compliance & Security

The data shows that Saudi Arabia's **18.4%** reject rate trails global leaders like Belgium (**24.7%**). To secure Vision 2030, the NCA and private entities must move beyond "passive monitoring" (p=none).

Immediate Action Plan:

1. **Move to p=reject:** This will ensure a much higher level of protection for KSA domains.
2. **Solve SPF Limits:** Use "SPF Flattening" to bypass the 10-lookup limit common in complex Saudi multi-vendor setups.
3. **Host MTA-STS:** Close the 99.8% encryption gap to prevent Man-in-the-Middle intercepts.

PowerDMARC provides a localized, NCA-aligned platform to automate these transitions without service disruption.

PowerDMARC Perspective: Securing the Digital Heart of Vision 2030

Saudi Arabia has truly excelled in building a modern and robust digital infrastructure. As the Kingdom advances toward its Vision 2030 objectives, continued attention to implementation consistency remains important from a national cybersecurity perspective. While the NCA ECC-2 mandates have significantly increased awareness and adoption, data indicate that further progress is needed to achieve full operational maturity.

Looking ahead to 2026, a key focus area is the gradual shift from monitoring-centric approaches to more proactive security measures. Strengthening email security through wider adoption of stricter DMARC policies, such as p=reject, and addressing gaps in MTA-STS deployment can help organizations move beyond baseline compliance. These steps support improved resilience, help protect domain integrity, and contribute to maintaining trust in Saudi Arabia's digital ecosystem amid evolving spoofing and interception threats.

Turn Visibility into Defense Today

The Kingdom's high foundational adoption rates prove that Saudi organizations are ready for a secure digital future; they now require the technical leadership to finalize the journey - and PowerDMARC is here to help!

Secure your piece of the Kingdom's digital future by moving from passive observation to **active protection** today.

Need Help or a Quick Demo?

Contact us at PowerDMARC to fortify Saudi domains, one Reject at a time.