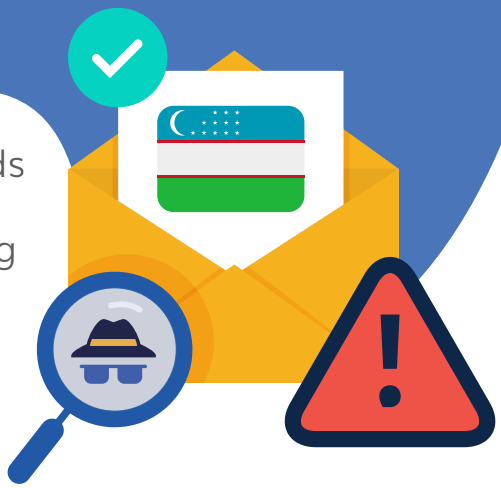
Uzbekistan DMARC Adoption Report 2023

POWERDMARC

POWERDMARC

Case study

The Importance of DMARC Adoption in Uzbekistan



- Enhancing DMARC adoption within Uzbekistan holds the key to fortifying the nation's digital fortress, symbolizing a proactive stride towards safeguarding both today's assets and tomorrow's prosperity. In the wake of escalating cyber attacks, Uzbekistani organizations must improve their defenses against email-borne attacks, shielding their clientele from digital malice.
- With Email authentication such as DMARC, organizations in Uzbekistan can display their devotion to practicing strong email authentication and security that fortifies their brand image, and adequately protects their email and information. This is especially important for financial, governmental, healthcare, and educational establishments that exchange sensitive information via email.

Is Uzbekistan Adequately Protected Against Email Fraud?

- Uzbekistan has seen a steady increase in targeted phishing attacks, spoofing, and malware infections since 2020. Presidential Resolution No. PP-167, issued on May 31, 2023, has sanctioned a fresh set of cybersecurity regulations for companies. Titled "On additional measures to enhance the cybersecurity system of critical information infrastructure facilities in the Republic of Uzbekistan," the resolution outlines the new requirements, encouraging organizations to take a proactive approach to cybersecurity and incident response.
- The regulations are likely to affect all businesses with important information systems in the field of agriculture, banking and finance, chemicals, defense and national security, energy, IT, mining, public health, telecoms, etc.
- The State Unitary Enterprise "Cybersecurity Center" reported a staggering 1.3 million cyberattacks targeting "uz" segment websites in 2021 alone, underscoring the utmost relevance of cybersecurity and financial fraud concerns in Uzbekistan.
- The above-mentioned statistics highlight the lack of email security in Uzbekistan, and the immediate need to be proactive.

In this report, we focussed on answering the following questions:

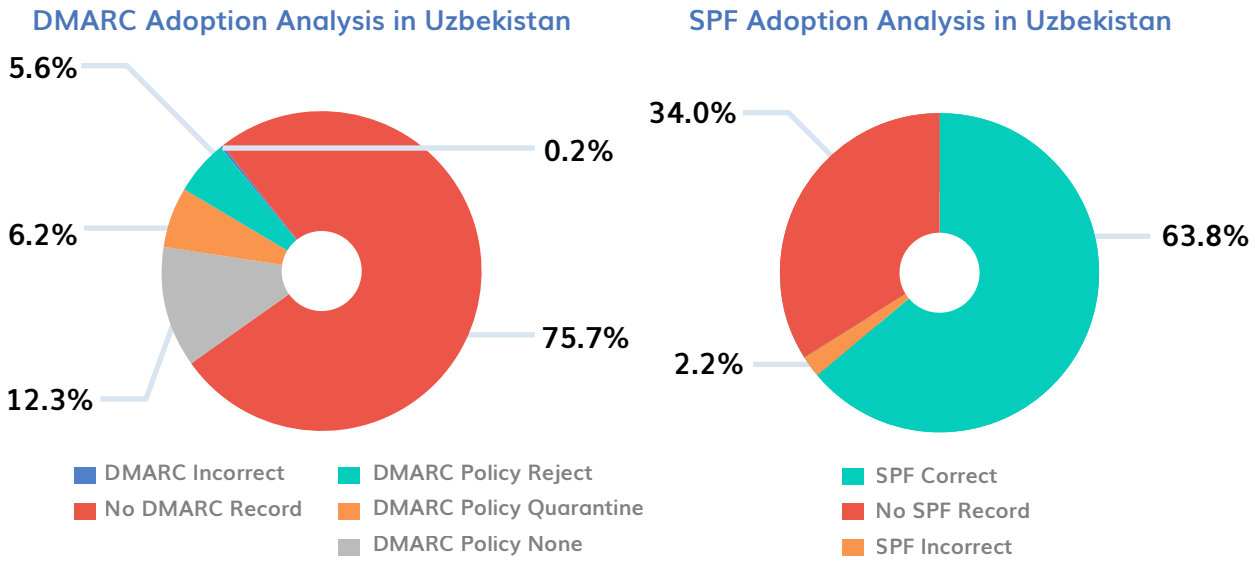
- What is the current situation of DMARC adoption and enforcement in organizations in Uzbekistan?
- How can we improve the cybersecurity and email authentication infrastructure in Uzbekistan to mitigate impersonation attacks?

To gain better insight into the current scenario we analyzed 826 domains belonging to top businesses and organizations in Uzbekistan, from the following sectors:

- Healthcare
- Energy
- Government
- Banking
- Educational
- Telecommunication
- Media and entertainment
- Transport

What Do the Numbers Say?

An in-depth SPF and DMARC adoption analysis was conducted while examining all 826 Uzbekistani domains, which led to the following revelations:

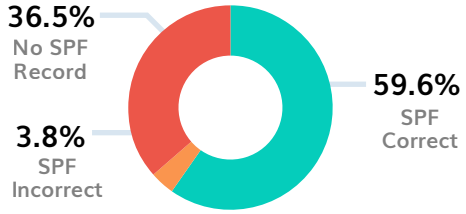


- Graphical Analysis: Among all 826 domains examined that belong to various organizations in Uzbekistan, 527 domains (63.8%) possessed correct SPF records, while 281 domains (34.02%) unfortunately had no SPF records at all, and 18 domains (2.2%) had incorrect records. 199 domains (24.09%) had correct DMARC records, while 2 of the domains (0.2%) had DMARC records that contained errors. A vast majority of domains (625 domains making up 75.66%) had no DMARC records at all. 102 domains had their DMARC policy set at none (12.3%), enabling monitoring only, while 51 domains (6.2%) had their DMARC policy level set at quarantine, and 46 domains (5.8%) had their DMARC policy set at maximum enforcement (i.e. p=reject).

Sector-wise Analysis of Uzbekistani Domains

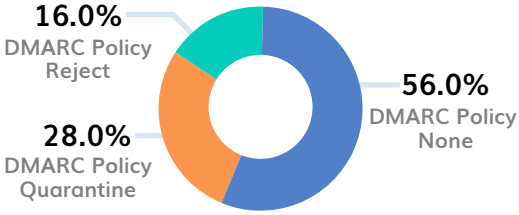
Healthcare Sector

SPF Adoption Analysis: Healthcare Sector



DMARC Adoption Analysis: Healthcare Sector

DMARC Enforcement Rates: Healthcare Sector



Key Findings:

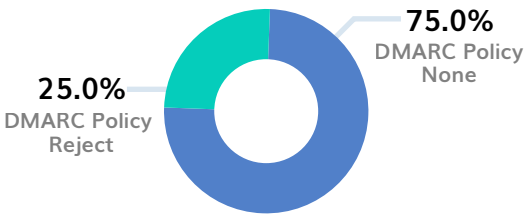
- 36.5% of domains in the Uzbekistan Telecom sector had no SPF record
- 56% of DMARC-implemented domains were at p=none offering no protection
- No DMARC record was found for 76% of the domains

Energy Sector

SPF Adoption Analysis: Energy Sector

DMARC Adoption Analysis: Energy Sector

DMARC Enforcement Rates: Energy Sector

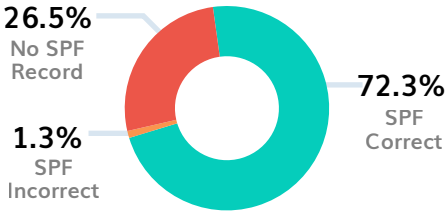


Key Findings:

- 33.3% of the domains had no SPF record published in their DNS
- 66.7% of the domains had no DMARC record published in their DNS
- 75% of the domains with DMARC implemented were on a “none” policy

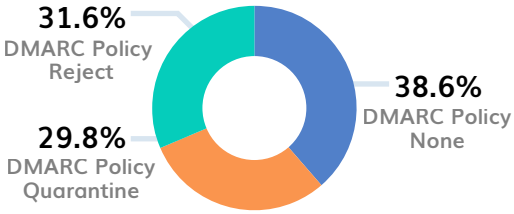
Government Sector

SPF Adoption Analysis: Government Sector



DMARC Adoption Analysis: Government Sector

DMARC Enforcement Rates: Government Sector

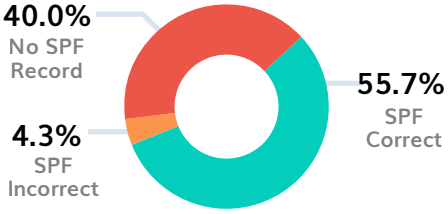


Key Findings:

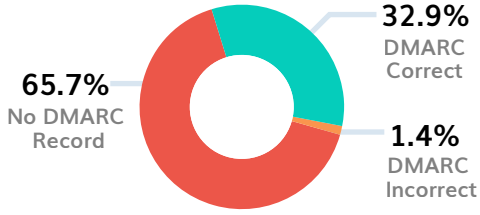
- 26.5% of the domains had no SPF record published in their DNS
- 63.2% of the domains had no DMARC record published in their DNS
- 38.6% of the domains with DMARC implemented were on a “none” policy

Banking Sector

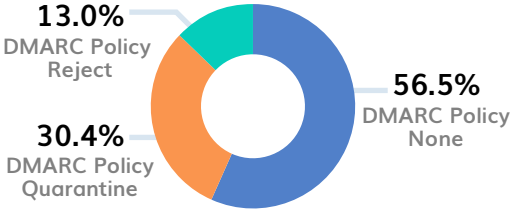
SPF Adoption Analysis: Banking Sector



DMARC Adoption Analysis: Banking Sector



DMARC Enforcement Rates: Banking Sector

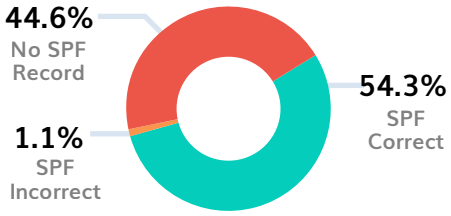


Key Findings:

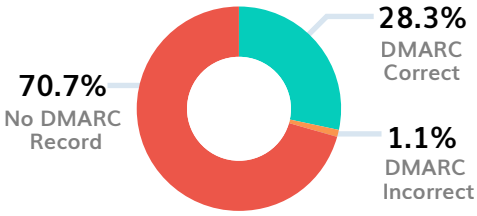
- 40% of the domains had no SPF record published in their DNS
- 65.7% of the domains had no DMARC record published in their DNS
- 56.5% of the domains with DMARC implemented were on a “none” policy

Educational Sector

SPF Adoption Analysis: Education Sector



DMARC Adoption Analysis: Education Sector



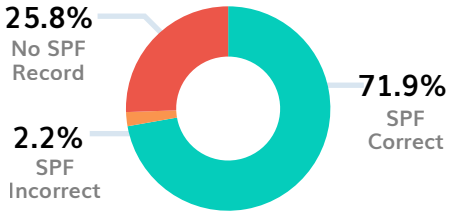
DMARC Enforcement Rates: Education Sector

Key Findings:

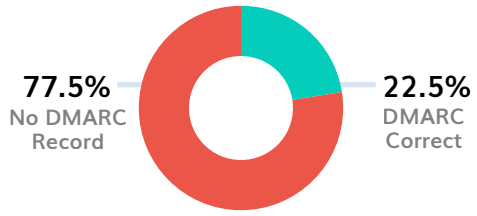
- 44.6% of the domains had no SPF record published in their DNS
- 70.7% of the domains had no DMARC record published in their DNS
- 34.6% of the domains with DMARC implemented were on a “none” policy

Telecom Sector

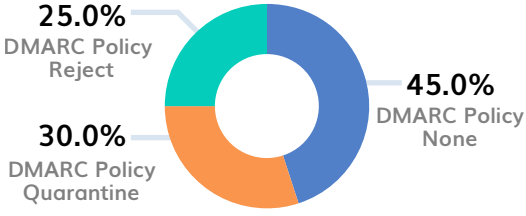
SPF Adoption Analysis: Telecom Sector



DMARC Adoption Analysis: Telecom Sector



DMARC Enforcement Rates: Telecom Sector

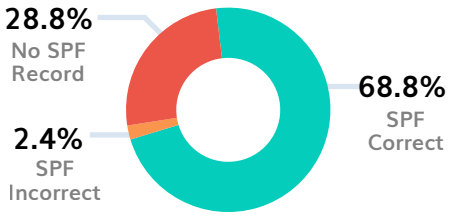


Key Findings:

- 25.8% of the domains had no SPF record published in their DNS
- 77.5% of the domains had no DMARC record published in their DNS
- 45% of the domains with DMARC implemented were on a “none” policy

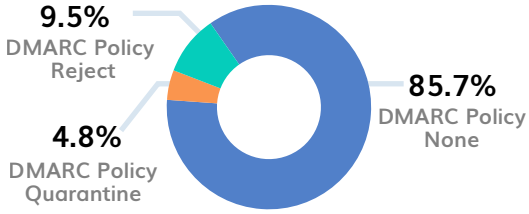
Media & Entertainment Sector

SPF Adoption Analysis: Media and Entertainment Sector



DMARC Adoption Analysis: Media and Entertainment Sector

DMARC Enforcement Rates: Media and Entertainment Sector



Key Findings:

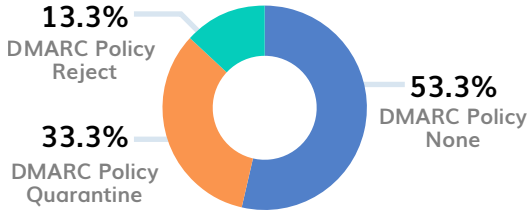
- 28.8% of the domains had no SPF record published in their DNS
- 83.2% of the domains had no DMARC record published in their DNS
- 85.7% of the domains with DMARC implemented were on a “none” policy

Transport Sector

SPF Adoption Analysis: Telecom Sector

DMARC Adoption Analysis: Telecom Sector

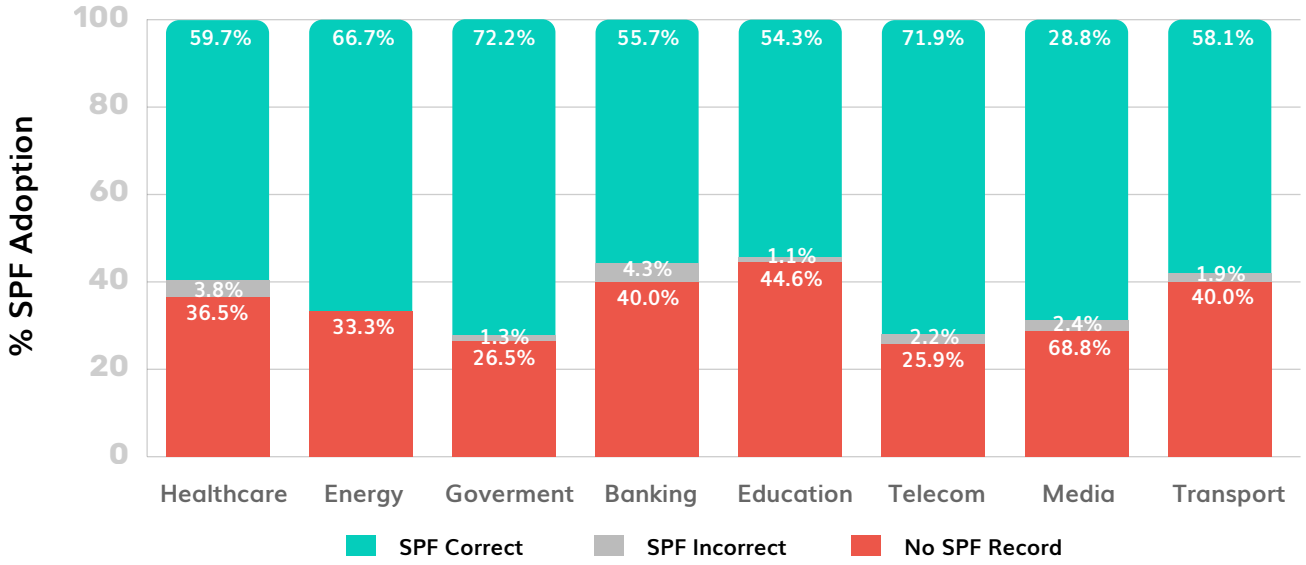
DMARC Enforcement Rates: Transport Sector



Key Findings:

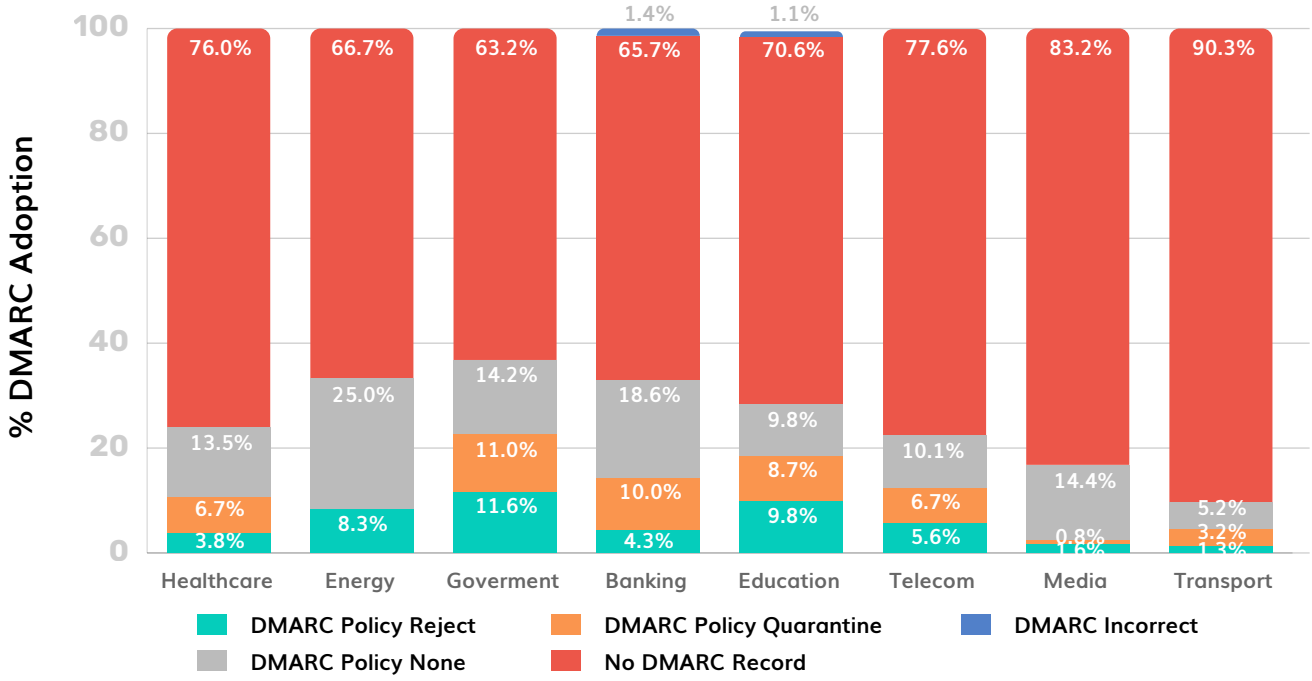
- 40% of the domains had no SPF record published in their DNS
- 90.3% of the domains had no DMARC record published in their DNS
- 53.3% of the domains with DMARC implemented were on a “none” policy

Comparative Analysis of SPF Adoption among Different Sectors in Uzbekistan



The SPF adoption rate was found to be the **lowest** in the Uzbekistan **education sector**, closely followed by the banking and transport sectors. The **highest** rate of SPF adoption was noted in the Uzbekistani **government sector**.

Comparative Analysis of DMARC Adoption among Different Sectors in Uzbekistan



The Uzbekistan **transport sector** noted the **lowest rate** of DMARC adoption. **The highest rate** of DMARC adoption was noted among **energy** and **government** however with considerably low rates of enforcement. A large percentage of organizations in all sectors had their DMARC policies at **monitoring only**

What Errors Are Organizations in Uzbekistan Making?

After examining 826 domains registered in Uzbekistan across different sectors and industries, it becomes apparent that organizations in the country are committing significant mistakes that could pose potential risks to the security of email communications exchanged with their clients or employees.

Erroneous SPF and DMARC Records

If your email server has the wrong SPF or DMARC record syntax, your legitimate emails might end up in the spam folder or get rejected by the recipient's email provider. This can damage your email reputation and make people doubt if your emails are legit.

Alarmingly Low SPF and DMARC Adoption Rates

An alarmingly high percentage of Uzbekistani domains don't use SPF and DMARC, which are like protective shields for your email domain. Without them, hackers can easily fake your emails and trick people into giving away sensitive information.

Multiple SPF Records for the same Domain

You should only have one SPF record for your domain; having more than one can cause problems with email authentication.

Lack of MTA-STS Implementation

MTA-STS helps keep your emails safe during transit, so hackers can't snoop on them or tamper with them. Not having this protection can make your email system vulnerable.

Lack of DMARC Enforcement

When your DMARC policy is not at reject of quarantine, scammers can still send emails that look like they're from your domain which will actually reach your clients without being blocked or flagged as spam, leading to successful phishing attempts.

Too Many DNS Lookups for SPF

RFC specifies the SPF lookup limit to be restricted to 10. If there are too many DNS requests sent that exceed the limit, it can cause issues and make your SPF invalid.

Boosting Email Security in Uzbekistan: Methods and Strategies

- Uzbekistani organizations can take the following steps to improve their overall email security posture:

1. Having visibility on your email senders who are sending emails on your domain's behalf
2. Locking your domains from impersonators by enforcing DMARC policies
3. Staying under the 10 DNS lookup limit for SPF
4. Having error-free SPF and DMARC records
5. Having a single SPF/DMARC record per domain
6. Implementing BIMI, MTA-STS, and TLS-RPT to prevent attacks like Man in the middle and interception
7. Enabling BIMI for more visibility and authentication

How Can PowerDMARC Help You in Your Email Security Journey?

To create a secure email environment, it's crucial to enable email authentication protocols like DMARC, DKIM, SPF, MTA-STS, TLS-RPT, and BIMI on all domains that you operate within your company. This ensures that all communications within the organization adhere to the same set of security standards, preventing accidental or malicious email sources.

PowerDMARC offers a comprehensive suite of email security services and hosted solutions designed to safeguard your brand reputation and protect customers from various email-related threats, without the hassle or technical complexities involved in protocol implementation, management, and monitoring.

Here's what we provide:

- **Configuration:** We assist in setting up and validating your SPF, DKIM, and DMARC records through our hosted services, ensuring they are error-free and effective.
- **Setup:** When you sign up for our DMARC trial, we help you create your DMARC dashboard, providing visibility within just 72 hours.
- **Monitoring:** Our continuous 24/7 monitoring of email traffic detects and manages security incidents, while alerts, reports, and responsive actions keep legitimate sending sources under control.
- **Reporting:** You receive daily Aggregate (RUA) and Forensic (RUF) reports, allowing you to track all emails passing or failing DMARC from your domains. These reports are human-readable and organized into tables and charts with actionable buttons and granular filtering options. Aggregate reports can also be downloaded in PDF/CSV formats.
- **Enforcement:** We assist you in transitioning to DMARC enforcement, implementing "p=reject/quarantine" policies safely and efficiently.
- **PowerSPF:** With our instant and auto SPF flattening service, you always stay within the 10 DNS lookup limit, and we keep you updated in real-time on any changes made by your ESPs (Email Service Providers).
- **Latest Authentication Protocols:** We utilize advanced email authentication techniques, including MTA-STS, TLS-RPT, and BIMI, alongside standard protocols, to effectively address email security challenges.
- **Domain Security Analysis Tools:** PowerDMARC provides you with instant analysis tools that can be used to check your domain's security rating, email headers, and domain health score, along with actionable recommendations to continuously improve and build up your defenses against attacks.
- **Managed Security Services:** Our DMARC MSSP/MSP-ready platform features a dedicated service desk to support your company's DMARC implementation efforts and continuously monitor your domain's email authentication health and user safety along with full white label and multi-tenancy support.

By partnering with PowerDMARC, you can fortify your and your customers' email domains and protect your organization and customers from potential threats, ensuring safer and more reliable email communication

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

Contact us!