92% of Top Email Domains Remain Unprotected Against Phishing

DOVER, DE, UNITED STATES, June 17, 2025 /EINPresswire.com/ -- New research from EasyDMARC reveals that just 7.7% of the world's top 1.8 million email domains are fully protected against phishing and spoofing, having implemented the most stringent DMARC (Domain-based Message Authentication, Reporting, and Conformance) policy. This configuration, known as 'p=reject', actively blocks malicious emails from reaching inboxes.

While DMARC adoption has accelerated since 2023, driven by regulatory pressure and mandates from major email providers, most leading organisations continue to rely on the weakest policy, 'p=none', which passively monitors inboxes for threats without intercepting them.

The findings are part of EasyDMARC's 2025 DMARC Adoption Report, which analyses email security practices across the highest-traffic websites globally, as well as Fortune 500 and Inc. 5000 organisations. The report reveals a significant gap between DMARC implementation and effective enforcement, with more than half (52.2%) of the domains still lacking even a basic DMARC record. Among those that have implemented DMARC, most fail to apply the enforcement policies or reporting mechanisms needed to make the protocol truly effective.

The report comes at a time of escalating phishing threats and increasing pressure from both regulators and mailbox providers. Mandates from Google, Yahoo, and Microsoft, along with frameworks like PCI DSS v4.0.1, have spurred a rush to adopt DMARC. But in many cases, that adoption stops at a passive monitoring setting known as 'p=none', which doesn't block fraudulent emails or provide full visibility into authentication failures.

"There's a growing perception that simply publishing a DMARC record is enough," said EasyDMARC CEO Gerasim Hovhannisyan. "But adoption without enforcement creates a dangerous illusion of security. In reality, most organisations are leaving the door wide open to

attacks targeting customers, partners, or even employees."

Countries with strict DMARC mandates, such as the United States, the UK, and the Czech Republic, saw the biggest reductions in phishing emails reaching inboxes. In the US, for example, the percentage of phishing emails accepted dropped from 68.8% in 2023 to just 14.2% in 2025. In contrast, countries with voluntary or no guidance, like the Netherlands and Qatar, showed little to no improvement.

Compounding the problem is the lack of visibility. Even among domains with DMARC records, over 40% fail to include reporting mechanisms, such as RUA tags, that allow organisations to see who's sending email on their behalf and whether it's failing authentication checks.

Hovhannisyan added: "Misconfigurations, missing reporting, and passive DMARC policies are like installing a security system without ever turning it on. Phishing remains one of the oldest and most effective forms of cyberattack, and without proper enforcement, organisations are effectively handing attackers the keys to their business. As threats grow more sophisticated and compliance pressures mount, stopping halfway with DMARC enforcement is no longer an option."

For more information, view the full report here.

END

Notes to the editor

What is DMARC?
DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email security protocol that helps protect your domain's reputation, prevent email spoofing, and increase email deliverability. It builds upon existing authentication standards like SPF and DKIM to verify the authenticity of emails sent from your domain. DMARC allows domain owners to specify how receiving mail servers should handle emails that fail SPF or DKIM authentication checks.

Research Methodology
The EasyDMARC May 2025 DMARC Adoption Report is based on an analysis of the world's top 1.8 million email domains, ranked by global web traffic. It examines the scale of DMARC adoption worldwide and assesses how effectively organisations are enforcing and monitoring the protocol. The report includes dedicated insights into the world's top 1.8M domains, Fortune 500 and Inc. 5000 companies, offering a comparative view of email security maturity across different organisational sizes. It also incorporates findings from a survey of 980 IT professionals across the United States, United Kingdom, Canada, and the Netherlands, providing regional perspectives on phishing trends, adoption challenges, and the influence of evolving regulatory mandates.

In addition to public DNS data, the report also draws on proprietary data collected through EasyDMARC's platform, including anonymised aggregate DMARC reports received from major mailbox providers (MBPs).

About EasyDMARC
EasyDMARC is a cloud-native B2B SaaS that solves email security and deliverability challenges in just a few clicks. With advanced tools, including its AI-powered DMARC Report Analyser, DMARC, SPF, DKIM cloud management solutions, and email source reputation monitoring, EasyDMARC helps customers protect their domains, increase their email deliverability, and maintain strong email health.

Anush Yolyan
EasyDMARC Inc.
+1 8885635277
email us here
Visit us on social media:
LinkedIn
Facebook