EINPRESSWIRE

Just 3% of New Zealand Email Domains Fully Protected Against Phishing as Government Mandates Strict Authentication

DOVER, DE, UNITED STATES, June 13, 2025 /EINPresswire.com/ -- Just 3% of email domains registered in New Zealand are fully protected against phishing attacks. That's the finding from new research by EasyDMARC, which reveals a wide gap between the nation's cybersecurity readiness and the New Zealand government's newly mandated email authentication requirements.

Under the Secure Government Email Framework, all public sector domains must enforce DMARC at its strictest level—p=reject—by October 2025. DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email authentication protocol that verifies whether a message is genuinely from the domain it claims to be. At its highest setting, p=reject, DMARC actively blocks phishing and spoofed emails from ever reaching the inbox.

Despite the looming deadline, EasyDMARC's analysis of 141,242 domains registered in New Zealand paints a concerning picture:

- Only 24.5% (34,566 domains) have valid DMARC records
- 72.4% of those with DMARC are set to p=none, the weakest policy that merely monitors for threats without taking action
- Just 3.1% (4,327 domains) enforce p=reject, the only setting that truly protects against phishing

While the mandate currently applies to government domains, its implications are far-reaching.

Organisations across the public and private sectors—including vendors, universities, NGOs, and local councils—risk both deliverability issues and increased susceptibility to impersonation if they don't follow suit.

"Most organisations set up DMARC but don't enforce it," said Gerasim Hovhannisyan, CEO of EasyDMARC. "By mandating DMARC at its strictest level, p=reject, New Zealand is leading by example and showing that email security only works when enforcement is taken seriously."

He continued: "Too many organisations stop at 'p=none', which creates a false sense of security. Our research shows that only 9.5% of the top 1.8 million global domains have adopted p=reject. That gap between implementation and enforcement is exactly why email remains the #1 attack vector."

With over 90% of cyberattacks starting via phishing, the urgency is clear—especially as phishing emails grow more sophisticated with the help of AI. "They're no longer clumsy scams," Hovhannisyan said. "They're flawless, targeted, and nearly impossible to detect. The only real defense is blocking them at the source. Email is how governments issue updates, how businesses close deals, and how people reset passwords. If we can't trust our inboxes, the entire system breaks down. New Zealand's email security mandate sets a powerful precedent—and puts pressure on the rest of the world to stop treating partial implementation as progress."

EasyDMARC's full report offers a detailed snapshot of New Zealand's current email authentication status and highlights the urgent need for accelerated adoption ahead of the government's 2025 enforcement deadline.

About EasyDMARC
EasyDMARC is a cloud-native B2B SaaS to solve email security and deliverability problems in just a few clicks. With advanced tools, such as its AI-powered DMARC Report Analyser, DMARC, SPF, DKIM cloud management solutions, and email source reputation monitoring, EasyDMARC's platform helps customers stay safe and maintain the health of their domains without risk.

For Managed Service Providers (MSPs) seeking to increase their revenue, EasyDMARC presents an ideal solution. The email authentication platform streamlines domain management, providing capabilities such as organizational control, domain grouping, and access management. Additionally, EasyDMARC offers a comprehensive sales and marketing enablement program designed to elevate DMARC sales. All of these features are available for MSPs on a scalable platform with a flexible pay-as-you-go pricing model.

Anush Yolyan
EasyDMARC Inc.
+1 888-563-5277
email us here