EINPRESSWIRE

New research: 90% of Portuguese domains are vulnerable to phishing and spoofing

ZOETERMEER, NETHERLANDS, June 22, 2023 /EINPresswire.com/ -- New research has discovered that spoofing and phishing protection is lacking in Portugal. Only 9.1% of the researched sample for Portuguese domains had correctly implemented and configured security policies to flag, report, and remove outbound phishing emails.

EasyDMARC, a cloud-native email authentication platform, reviewed 122,398 country code top-level domains in Portugal in an attempt to highlight DMARC adoption rates in the country. The research revealed that only a quarter of the total sample had ever implemented DMARC. The rest of the .pt domains are in the dark on how email authentication can help domain owners protect their businesses and organizations.

Authenticating organization domains with DMARC (Domain-based Message Authentication, Reporting, and Conformance) helps avoid brand impersonation, Business Email Compromise, and ransomware attacks that occur as a result of spoofing and phishing attempts. It protects brand reputation, boosts client trust, and ensures peace of mind for business owners and their teams.

According to EasyDMARC's research, out of the 31,412 domains with DMARC, more than half (54%) were still on the policy 'none.' This means that they only monitor their domain infrastructure without taking any steps to restrict phishing attempts. Out of the domains that have DMARC, 3,222 (10.26%) had set the DMARC policy to 'quarantine,' while 11,140 (35.46%) domains had implemented the 'reject' policy and protected their email environment fully.

Although the percentage of domains with a 'reject' policy was low (9.1%), viewed in the context of the research sample, 35.46% DMARC uptake is a strong performance compared to other countries and industries researched by EasyDMARC.

As for the first and most basic step in email authentication, SPF configuration, 75.4% of the researched domains had implemented the policy. Still, not all the domains that have SPF can boast perfect configuration – with 14.6% having errors.

EasyDMARC also conducted an analysis of Portuguese domains that exist on its platform. The research discovered that the first six months of 2023 have already seen as many phishing attempts on these domains as the year 2022 in its entirety. While the attempts were blocked on

EasyDMARC, these statistics emphasize the persistent, growing threat that phishing emails represent.

Commenting on the research, Gerasim Hovhannisyan, EasyDMARC CEO and co-founder, says:

"While the need for cyber protection is universal, protecting country-specific top-level domains is even more important. A lack of domain authentication in these domains will result in hacks among governmental organizations and local businesses, which will expose them to highly sensitive and potentially costly data breaches. Without DMARC adoption, local companies will continue to see an increase in cyber events and subsequent disruptions and losses."

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.

With offices in the US, Netherlands, and Armenia, the company delivers the most comprehensive platform for anyone who strives to build the best possible defense for their email ecosystem. EasyDMARC ultimately provides peace of mind, enabling clients to focus on achieving their business objectives rather than dealing with the worries and concerns associated with cybersecurity.

Anush Yolyan
EasyDMARC Inc
+1 888-563-5277
email us here
Visit us on social media:
LinkedIn