Survey: 50% of US banks have no email security

MIDDLETOWN, DELAWARE, USA, December 14, 2022 / EINPresswire.com/ -- The banking sector has always been on hackers' radars, and the situation has worsened in the digitalization era. Now that every banking procedure has shifted to the web, customers are more likely to get attacked. Moreover, the COVID-19 pandemic has contributed to the soaring statistics of banking fraud.

Malicious actors attempt phishing, scamming, and spoofing attacks in the name of reputed banks to gain the recipients' trust. The emails request customers to share sensitive financial details, which hackers exploit to transfer money to their accounts or make expensive purchases. This causes a loss to the customers and tarnishes the bank's reputation.

Fortunately, using email authentication protocols (SPF, DKIM, and DMARC) can prevent this company name abuse. EasyDMARC's research team acquired data on DMARC adoption in the US banking sector. This article reveals the crucial findings and other facts related to DMARC adoption in the US banking sector.

What is DMARC?

DMARC is short for Domain-Based Message Authentication, Reporting, and Conformance. It's an email authentication protocol that builds on SPF and DKIM to check if the emails sent from your domain are authentic. It lets email service providers (like Gmail, Yahoo, Outlook, etc.) detect and block illegitimate emails. DMARC policy uses a customized DMARC record published in the DNS record to help recipients' mailboxes know how to treat emails coming from your domain. You can set one of the three policies.

None policy (p=none): It tells the receiver's server to take no action against emails that fail DMARC verification.

Quarantine policy (p=quarantine): If you've set your DMARC policy to quarantine, the recipient's server sends unsolicited emails to the spam folder.
Reject policy (p=reject): Per this policy, the receiver's mailbox will completely reject the entry of failed emails.

DMARC Implementation in the US Banking Sector

It's scary to know the cost of cyberattacks in the banking industry has touched $18.3 million annually. As of 2021, there are 4,236 FDIC-insured commercial banks in the United States. The EasyDMARC's research team reviewed 2646 .bank domains, out of which only 1338 (approximately 50%) companies have DMARC. This means that less than half of the USA's banking sector protects its customers against spoofing and phishing attacks.

Out of the 1338 banks implementing the DMARC protocol, 89 (6.65%) have set the none policy, 56 have set the quarantine policy (4.18%), and 1193 (89.1%) have established the reject policy. However, out of 1193 companies who've set the DMARC policy to reject, 406 (34.03%) don't use the "rua" tag, which means they don't monitor and collect DMARC reports. These reports show you which messages sent from your domain pass SPF and DKIM and let you filter potential spammers, acting on their attempts before things get out of hand.

These findings by EasyDMARC show that cybercriminals know how sensitive and vulnerable is the whole structure of online banking in today's time. The ever-expanding data bucket and the increasing number of malicious activities demand better security protocols, and DMARC is indeed helpful.

Why is DMARC Implementation Important for the Banking Sector?

DMARC was introduced to safeguard outbound emails. It also protects you from receiving fraudulent impersonated emails by allowing only legitimate senders to land in the inbox. This decreases the chances of BEC or Business Email Compromise fraud – one of the most financially damaging cybercrimes.

Hackers use the official bank domain to email customers and prospects on their behalf. The recipients think they received it from the bank authorities and proceed with the requests. These emails generally ask for sensitive details like social security numbers, CVVs, OTPs, credit/ debit card details, and other financial information. They may even ask you to participate in a lucky draw contest, start a fixed deposit, acquire a pre-approved loan, etc., by paying a small amount in the name of a procedural fee.

All this can be averted because DMARC allows only authorized IP addresses to send emails using the bank domains. The banks can define rules for the receiving server on how to treat potentially spoofed emails, and in return, they receive reports having details about the emails' origin and SPF and DKIM results.

EasyDMARC offers a free DMARC Record Generator Service that guides you through each step.

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