EINPRESSWIRE

South Africa Market Research by EasyDMARC

South Africa Market Research by EasyDMARC

MIDDLETOWN, DELAWARE, USA, September 9, 2022 /EINPresswire.com/ -- The South African financial sector, especially banks, loan companies, and insurance companies, have experienced a stark uptick in cybercrimes lately. The COVID-19 pandemic has also contributed to this as many people diverted to malicious activities to make quick money.

Phishing, scamming, and spoofing are common ways used by threat actors to attack. They use tactics to send emails on behalf of financial companies, requesting customers to share sensitive details. The information is then exploited for stealing money.

www.easydmarc.com

However, organizations using email protection protocols like SPF, DKIM, and DMARC are far more protected against them. Email authentication isn't a luxury anymore; it's rather a necessity to maintain your financial institution's reputation and customer trust.

What is DMARC?
DMARC or Domain-Based Message Authentication, Reporting, and Conformance is an email authentication protocol that uses SPF and DKIM to evaluate the genuineness of emails sent from your domain. It helps ISPs or Internet Service Providers identify and block fraud and spam emails. A DMARC record is published using a DNS record to let recipients' mailbox understand how to deal with each email.

It has three policies:

None Policy (p=none): It enables the receiver’s mailbox to do nothing with unqualified emails.

However, they're added to the DMARC record for any infractions.
Quarantine Policy (p=quarintine): It sends unsolicited emails to the spam folder.
Reject Policy (p=reject): Reject policy tells the receiver's mailbox to welcome only 100% verified emails and denies the entry of all unqualified ones.

Banks in South Africa

As of 2020, South African banks have accumulated assets of 448.4b USD, making it one of the most sought-after sectors by bad actors. They perform spoofing attacks to get sensitive customer details to pinch their identity. Customers receive fraudulent emails asking them to click on a link that directs them to a genuine-looking website where they're asked to submit credentials, credit card numbers, CVVs, social security numbers, etc.

DMARC Adoption in South African Banks

Well, one of the most efficient solutions to email phishing and spoofing is DMARC policy adoption. As per research conducted by the research team of EasyDMARC, a DMARC deployment service provider, out of 49 banks in South Africa, 38 use DMARC policy. This means their email systems are more secure than the 11 banks not deploying it. However, not all of them use the Reject policy, which means they’re still prone to phishing, spamming and spoofing attacks.

Out of the 38 banks using the DMARC protocol, 9 use the None policy, 8 use the Quarantine policy, and 18 use the Reject policy. The 9 banks who’ve set p=none for months still have both legitimate and illegitimate sending sources. Without this prolonged and patient monitoring, your DMARC policy might block genuine senders too.

EasyDMARC’s research results show that 94% of banks use SPF or Sender Policy Framework policy, which lets domain owners specify genuine email servers. SPF is the first step toward email protection, and companies must pair it with DMARC to avoid cybercrime.

Insurance Companies in South Africa

Like many industries, insurance companies in South Africa, are also under the radar of phishers and spoofers. The digital shift has opened many doors for the customers; however, they're also more exposed to email-based attacks.

Imagine a threat actor using your business email domain to send malicious links to your customers! How detrimental it would be for your reputation!

Liberty Insurance became a victim of a ransomware attack when hackers capsized a database containing crucial details related to the company and customers. Its customers even received fraudulent emails, but fortunately, nobody witnessed a financial loss as the insurance company quickly responded to the attack and regained control.
In situations like this, DMARC policy either lets you know about fraudulent senders (p=none) or blocks illegitimate emails from reaching your customers’ mailbox (p=reject).

DMARC Adoption in South African Insurance Companies
Out of 35 South African insurance companies, only 18 have a DMARC policy deployed for email authentication. This means only 51.42% of insurance companies are prepared against phishing, spoofing, and spamming attacks attempted in their name. The percentage of them using none, quarantine, and reject protocol is 38.88%, 11.11% and 50%, respectively.

EasyDMARC officials are concerned about these statistics as the South African insurance sector isn't fully shielded by DMARC protocol. They've come across several insurance companies who've set the None policy for years and believe their domain is protected. This isn't true as the None policy is meant for the preliminary stage only.

However, 94% of them have already deployed SPF protocol, which means their DMARC deployment journey will be a bit easier and quicker.

DMARC Adoption in South African Loan Companies
As per the data collected by EasyDMARC's market research team, there're 29 loan companies in South Africa, out of which only 8 have deployed DMARC policy. The number of them using none, quarantine, and reject protocol is 4,3 and 1, respectively. The rest 21 loan companies are highly prone to email-related cyberattacks. Also, 82% of companies use the SPF protocol, which is lesser than banks and insurance companies.
One of the biggest DMARC enforcement mistakes is forgetting about subdomains. If you haven't set a subdomain policy of sp=none, attackers can spoof you. Say, if phishing emails sent from abc@xyz.com won't pass through, but abc@mail.xyz.com will.

Summary
Hackers target financial institutions like banks, loan companies, and insurance companies to attempt email-related cyberattacks and fool their customers. They try phishing, spamming, and spoofing using your email domain to make recipients believe that emails are coming from a legitimate source.

Thus all South African banks, loan companies, and insurance companies must deploy SPF, DKIM, and DMARC authentication protocols. A DMARC record is a DNS TXT record that's added to the domain to tell the recipient's server how to deal with legitimate and illegitimate emails.

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

try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.