POWERDMARC

Case study

Leading Financial Services and Banks in Sultanate of Oman

Solution

Aligning all domains with email relay, SPF, DKIM, MTA-STS TLS-RPT and implementing DMARC.

Challenge

Restoring retail and corporate clients' trust in the bank's email channel. Allowing marketing emails to reach clients and stopping spoofing attacks.

Results

Controlled email flows, better deliverability and spoofing mitigation.

"Today, customers don't stay silent", explained Jamal. "If they've been a victim of a phishing attack, odds are, they will tell their friends over social media. PowerDMARC helped us restore trust into our email delivery channel and combat phishing attacks with absolute ease."

Jamal al Khusaibi - Deputy Head of IT

alizz islamic bank

بنك العز الإسلامي
alizz islamic bank

Situation before PowerDMARC

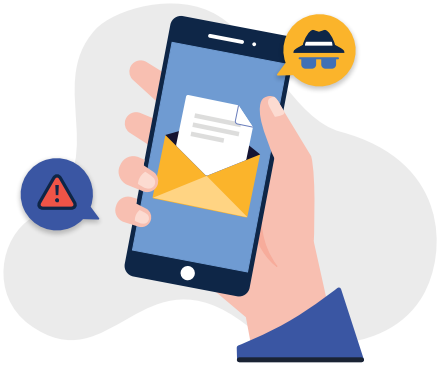
Prior to utilizing PowerDMARC's services, alizz islamic received numerous complaints from their retail and business clients, indicating that their domains were being spoofed and illegitimate emails were sent on their behalf.

Looking to prevent frustration from building up within their diverse customer-base, the team at alizz islamic decided to look into a reliable, long term solution that would effectively combat this issue. This ultimately led them to PowerDMARC.

Identifying the problem

After communicating the initial problem, we narrowed down the main challenges faced by alizz islamic to:

- Difficulty in managing multiple domain names
- Lack of visibility on sending sources
- Spoofing and phishing attacks on retail and corporate online banking users
- Marketing emails delivered to the junk folder
- High volume mails for e-statements



We then explained how these issues can be mitigated via DMARC and outlined the necessary steps needed to achieve full DMARC enforcement, namely:

- Gaining insight into all email channels
- Authenticating all emails with DKIM
- Aligning email deliverability for marketing channels
- Mitigating the effect of phishing, spoofing, business email compromise

This involved working hand in hand with the IT team in alizz islamic to publish and update the necessary SPF, DKIM and DMARC records and gradually working up to a 100% p = reject DMARC policy.

Implementing the solution

1 While the team at alizz islamic was first worried that implementing DMARC would disrupt their normal email flow, this was not the case. Their DMARC records were first published with a p = none policy. This provided them with visibility into their email channels without any enforcement.

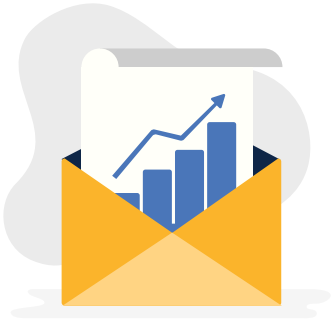
2 Alizz islamic was astonished at the level of detail provided by the PowerDMARC application, they were able to easily filter emails sent on their behalf according to: the sending source, host, reporting organization and authentication results. This allowed them to identify where their legitimate email originated from and update their SPF records accordingly and ensure that all their email forwarding 3rd party services where DKIM signed.

3 Moreover, alizz islamic appreciated the executive reports produced by us as they provided an overview of their DMARC implementation status. Not only that, our comprehensive threat intelligence view coupled with the one click Take down button made it so easy to track and report abusive senders.

Achievements

Alizz Islamic was able to seamlessly transition from p = none to p = reject in record time, allowing them to

- Gain full insight into their email channel
- Authenticate all emails with a DKIM signature
- Protect all of their domains with a DMARC enforcement policy
- Significantly improve their email deliverability
- Protect their customers against phishing and spoofing attacks



Schedule a demo today. **Contact us!**