Healthcare Companies' Customers at Risk for Email Scams

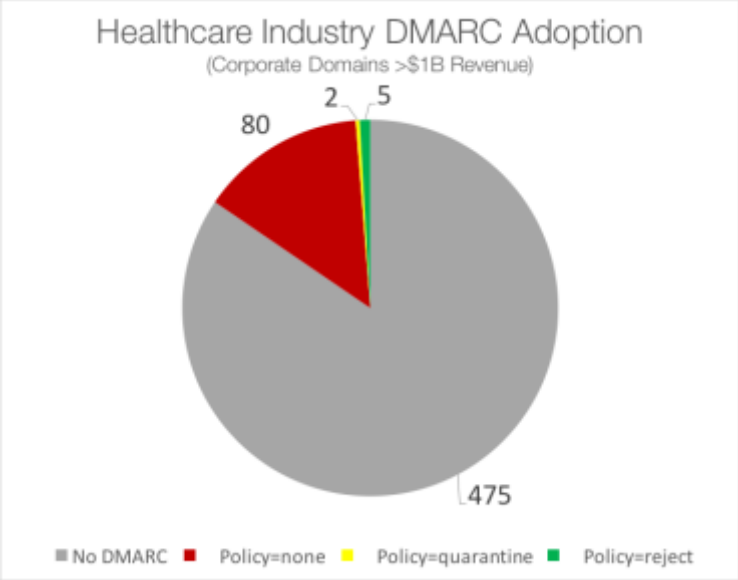
Customers Unprotected Against Phishing Attacks

A recent study conducted by Agari found that out of 562 companies with revenues above $1B in the healthcare and pharmaceuticals sectors, roughly 1% had protections in place to keep their customers from receiving inauthentic and/or fraudulent emails.

Email was designed without safeguards to ensure messages claiming to be from a sender are actually *from* that sender. A standard called DMARC was created some years ago to solve this problem. A DMARC record, which is published alongside your domain's DNS records, ensures that only authorized senders can send email on behalf of your organization or domain. However very few companies have implemented DMARC adequately enough to protect their customers.

The Data

Agari found that most healthcare companies had no DMARC record at all. Of those that did have a record in place, most had no policy implemented to take action against fraudulent emails. Only seven of them had a policy in place to take specific action—either to quarantine or delete the fraudulent emails—and of those, five (less than one percent) actually reached the state of a "reject" policy. Achieving reject is important because only then are mailbox providers instructed to refuse any malicious emails purporting to be from their brand.



The Risk of No DMARC Implementation

Having an inadequate (or no) DMARC policy in place causes significant risk of:

- Customers being phished
- Corporate brand erosion from unauthorized emails
- Reduction of customer trust
- Reduced ROI from email campaigns and digital engagement

To learn more about whether your customers are protected from receiving fraudulent emails visit our site and enter your domain into Agari's DMARC Tool.

To begin protecting your customers from phishing and other fraudulent email scams using your company's brand, start your free trial of Agari Customer Protect.