Case Study

Exploring the Phishing Threat Landscape

See how one of the largest banks in Qatar was able to proactively respond to rising Phishing Threats

Organization's Background

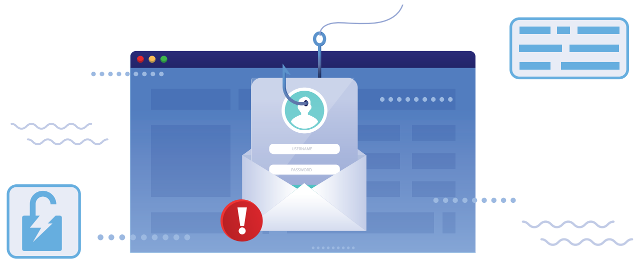
One of the largest banks in Qatar found itself under the impeding threat of cyberattacks. In today's digital age, where the disclosure of sensitive financial information due to cyberattacks is unfortunately common, a new breed of cyber threats has emerged, characterized by their sophistication and rapid evolution. These evolving threats have left every organization vulnerable to potential breaches.

The Common Enemy: Different Types of Phishing Attacks

In the ever-evolving landscape of cybersecurity, understanding the diverse array of cyberattacks is crucial. Phishing, the most common one, comes in various forms, each presenting unique challenges and risks to individuals and organizations.

The increasing frequency of Phishing attacks like Spear-Phishing (Highly Targeted Phishing) and Whaling (CEO-Fraud) in the region not only jeopardizes the confidentiality, availability, and integrity of sensitive data but also poses a significant risk of disrupting an organization's operational infrastructure.

Faced with this mounting challenge, the bank went on a rigorous selection process to identify the best partner to help mitigate risks and evaluate the vulnerability of its workforce.



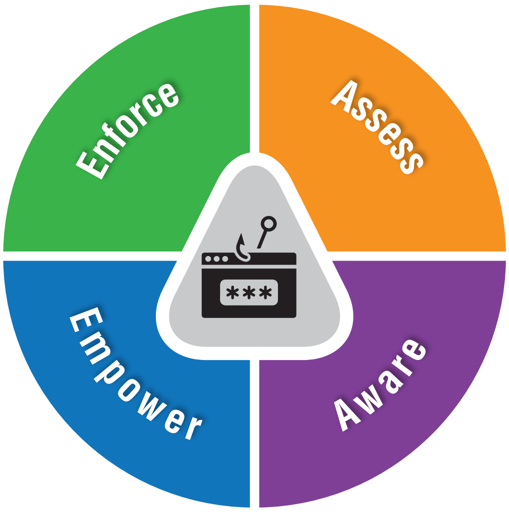
It is widely acknowledged that phishing accounts for 65% of all cyberattacks (AAG), evidencing the need to assess if the bank was able to respond appropriately to these threats. This was reiterated in the bank's CISO's own words, "The objective was to analyze and understand employee's swift responses when confronted with a cybersecurity threat like Phishing. In a world where a single click can make or break an organization's reputation, it was imperative to employ the most effective phishing simulation exercises to gauge employee vulnerability and address the need to raise awareness about the rising tide of cyberattacks with the help of an integrated response platform. This is where PhishRod stepped in to provide us with a solution."

The Challenged Encountered

The bank faced a substantial challenge in categorizing individuals from a vast pool of employees to identify those that were the most susceptible to falling victim to phishing attacks. Without a statistical mechanism to evaluate and analyze employee behavior, they were left with limited options to provide their end-users with an optimized phishing readiness and incident response plan.

The Solution: PhishRod's Phishing Simulator

By delivering its cutting-edge Phishing Simulator, designed to effectively analyze user behavior and provide quantifiable results, PhishRod was able to help the organization substantially. PhishRod embraces an analytics-driven approach, and its simulator perfectly reflects this.



Leveraging the Phishing Simulator, PhishRod conducted multiple simulation exercises for the bank to pinpoint potential breach points. Open communication with the bank's security team was maintained throughout the exercise, allowing them to select their preferred phishing simulation template from PhishRod's extensive library. Once chosen, PhishRod executed the simulation, delivering quantifiable results that enabled the bank to assess their organization's preparedness against security breaches.

Once the "Phishing Index" was established across organizational, departmental, and individual dimensions, it gave us the insight of how this valuable metric enabled all stakeholders involved to evaluate the vulnerability index, serving as the foundation for the strategic implementation of the Bank's security awareness plan.

The Outcomes

PhishRod collaborated closely with the organization's security team to develop and implement a tailored security awareness plan based on the insights gained from the "Phishing Index" assessment, ensuring that it addressed the specific needs and challenges of the various levels within the bank.

In addition to that, PhishRod equipped all users at the bank with an intelligent reporter agent called the Reporter Plug-in, enabling them to promptly report any suspicious emails. Leveraging its extensive library of over 130+ built-in threat intelligence feeds, any reported suspicious emails underwent a comprehensive analysis, followed by their quarantine and subsequent removal from users' inboxes.