phishrod.co

PhishRod
Fortify First Line of Defence

Case Study

Automating Cyber Security Awareness and Phishing Readiness

One of the largest hospitals in Kingdom of Saudi Arabia automates its cyber security awareness program using PhishRod.

The Phishing Landscape

Phishing is a significant threat to organizations of all sectors and sizes. Healthcare and financial sectors are on the radar because they possess sensitive information. Many significant security incidents originate with a successful phishing attempt. Inboxes are no longer clogged with "junk mails", but rather with phishing emails designed to elicit sensitive information or deploy malware to steal confidential data. Malicious actors know that phishing is a highly effective means to penetrate an organization.

Rise of Phishing Attacks in Healthcare Industry

The healthcare industry is expected to be the biggest target because of the valuable data contained in the form of electronic health records. Such data can be used by adversaries to commit several types of fraudulent activities, such as identity theft. In fact, the IT systems and medical records of many hospitals are being targeted by adversaries who try to gain access to the patient's data, launch ransomware attacks to demand money, or make the electronic health records (EHRs) of clinics inaccessible, thereby compromising patient care. WannaCry is one of the biggest examples of a healthcare data breach.

About the Customer

The customer is one of the largest hospitals in the Kingdom of Saudi Arabia. With over 17,000 employees, they have branches across 4 major cities in Kingdom. PhishRod was selected by the customer to automate the security awareness program, and policy compliance and empower its end users against phishing attacks.

The Key Challenges

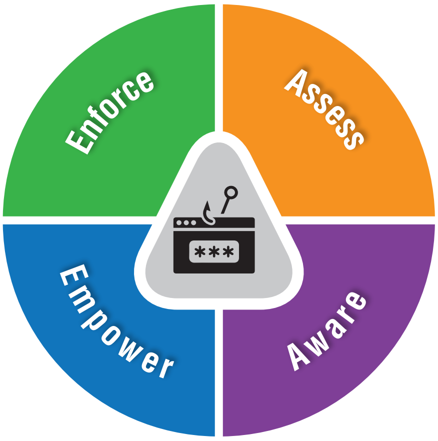
Being one of the largest hospitals in the region with employees from diverse cultural backgrounds, conventional security awareness never produced the desired results. There was no analytics data available to gauge the readiness of the end-users against phishing attacks and no formal mechanism for communicating the IT & IT Security policies.

PhishRod: Fortify the first line of defense

PhishRod was selected by the hospital after a competitive bidding process and product due diligence. PhishRod offered a complete suite that included Phishing Simulator, Security Awareness Manager, Policy Compliance Manager & Automated Phishing Incident Response Management.

PhishRod's existing phishing simulation templates were modified as per the customer's requirements. Once the customized templates were ready, the first phishing campaign was sent that yielded an 84.8% click ratio, indicating a higher risk of falling for phishing attacks. More such simulated phishing tests were conducted to determine the Phishing Index on organizational, departmental & individual user levels.

Once the baseline Phishing Index was determined, the objective was to design and automate the security awareness program. This aim was achieved with the Security-focused LMS called the Security Awareness Manager. It has 300+ computer-based training modules, posters, banners, and awareness tips in multiple languages primarily focusing on English & Arabic.



Using the automated scheduler, the awareness calendar for 3 months was developed and approved. The SCORM compliant security awareness modules on the topics of Phishing, Social Engineering & Ransomware were assigned to the end-users. The dashboard provided complete visibility on the completion of modules by end-users. Security Awareness Index was calculated on an organizational, departmental, and individual user level.
With an objective to empower end-users, PhishRod Reporter Plug-In was provided to all end users to report suspicious emails. Once an end-user reported a suspicious email.

The hospital had over 25 corporate policies related to IT & IT Security and over 100 plus supported processes. The existing process of uploading the policies on a corporate portal was not working, as the end-users never visited the portal. Using the integrated workflow for policy compliance, all corporate policies were assigned to end-users using the PhishRod Policy Compliance Manager. The end-users had to go through the salient content of the policy which is followed by a quiz. This ensured that all of the end-users read the policy, passed a quiz related to it, and provided their concurrence to adhere to the policy. Policy Compliance Index on organizational, departmental & individual user the level was mapped on a dashboard.

Products

1. Phishing Simulator
2. Security Awareness Manager
3. Policy Compliance Manager
4. PhishScout

Services

- Baseline Assessment
- Content Review
- Security Awareness Framework Development

To learn more about PhishRod and how we help organizations to fortify their first line of defense, please visit the following link:

www.phishrod.co