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 mean to penetrate into 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 phishers 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 phishers who try to gain access to the patient's data, launch ransomware attacks for demanding money, or make the electronic health records (EHRs) of clinics inaccessible, thereby compromising the patient's care. WannaCry is one of the biggest example of the 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, policy compliance and empower its end users against phishing attacks.

The Key Challenges

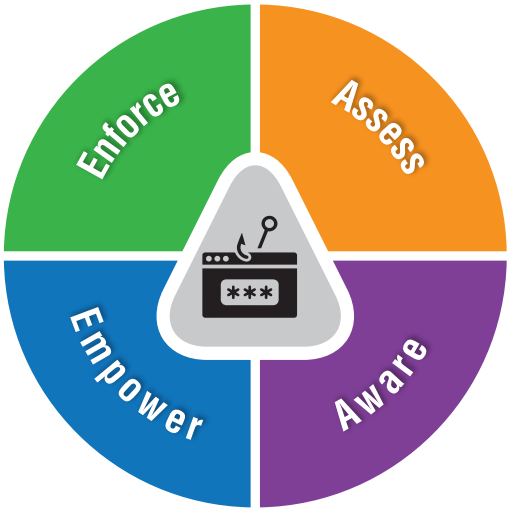
Being one of the largest hospitals in the region with employees from diverse cultural backgrounds, the conventional security awareness never produced the desired results. There were no analytics available to gauge the readiness of the end users against phishing attacks. There was no formal mechanism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

PhishRod®
Fortify First Line of Defence

PhishRod: Fortify the first line of defence

PhishRod was selected by the hospital after a competitive bidding process and product due diligence. PhishRod offered a complete suite which included Phishing Simulator, Security Awareness Manager, Policy Compliance Manager & Threat Advisory Manager.

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 84.8% click ratio, indicating a higher risk to fall for phishing attacks. More such simulated phishing tests were conducted to determine the Phishing Index on organizational, departmental & individual user level.

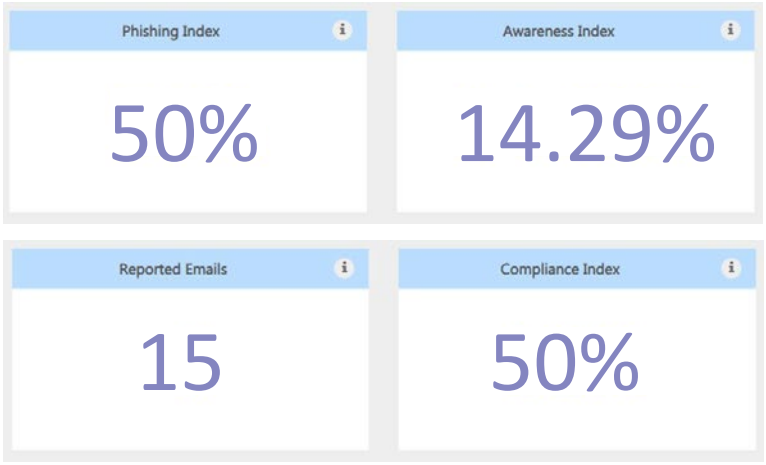


Once the baseline Phishing Index was determined, the objective was to design and automate the security awareness program. This aim was achieved with the Security Awareness Manager. It had 30+ modules in English as well as in Arabic. Using the automated scheduler, the awareness calendar for 3 months was 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 a complete visibility on the completion of modules by end users. Security Awareness Index was calculated on 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 PhishRod administrator in the hospital would receive a notification (with body, header and other relevant details) regarding the reported email. The security administrator could also verify the reported suspicious email from 3rd party as well, as PhishRod integrates with Virus Total, Google Safe Browsing API & PhishTank.

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

level was mapped on a dashboard.



"PhishRod Suite helped us to completely automate the security awareness program. The analytics from the Phishing Simulator helped us to focus on most vulnerable end users and departments, while the awareness manager provided complete visibility for management on the state of the awareness program being run. Though it took a bit of time for the end users to report suspicious emails, but the integration with 3rd Party tools, such as PhishTank helped us to identify the false positives. PhishRod's team also developed the customized content for us and helped us transform into a cyber aware organization". CISO, The largest specialize hospital in the Kingdom of Saudi Arabia.

PhishRod®

Fortify First Line of Defence

Products

1. Phishing Simulator
2. Security Awareness Manager
3. Policy Compliance Manager
4. Threat Advisory Manager
5. PhishRod Reporter

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 defence, please visit the following link:

www.phishrod.co

info@phishrod.co