Requester Inc

Phishing Engagement Report

July 20, 2023

Submitted by: User

Contents

Document Information

This document contains information retrieved by an independent contractor using the Hackybara platform. It is provided to Requester Inc in accordance with the terms of any agreement between the independent contractor and Requester Inc. Information within this document contains sensitive information related to Requester Inc and should not be released to another vendor, business partner or contractor without written approval from Requester Inc. Furthermore, this document may not be copied, distributed, reproduced, or retained by the independent contractor without approval from Requester Inc.

The contents of this document does not constitute legal advice. The independent contractor using Hackybara's platform offer of services or deliverables that relate to compliance, litigation, or other legal interests is not intended as legal counsel and should not be taken as such.

Contacts

Hackybara Platform Phishing Tester		
Name	**Role**	**Contact Information**
John Jacob	Hackybara Independent Contractor (HIC)	Johnjacob1899@gmail.com

Requester Inc		
Name	**Role**	**Contact Information**
Bob Cyber	Application Coordinator	bobcyber@gmail.com
Alice Cyber	Security Officer	Aliceccyber@gmail.com

Scope

The phishing engagement was targeted against the following email criteria:

Target
Requester Inc Employee Emails

Phishing Statistics

The following information was retrieved during the engagement:

Emails sent	**324**
Emails opened	**240**
Malicious link clicked on within email	**137**
Credentials harvested	**105**

Executive Summary

Requester Inc contacted Hackybara to perform a phishing engagement against its employes. The primary objective of a phishing engagement is to assess the organization's security awareness and determine the effectiveness of its phishing awareness training and cybersecurity measures. The assessment took place between July 1st and July 20th, 2023, and was conducted remotely.

Examine the attached CSV/XML/HTML or Database file that was included with this report for more information and full results.

Conclusions

Overall, the current security awareness within the organization needs to be improved. Further phishing awareness training should be implemented and given to all employees.

Sample of Tools used

- **Mailgun**
- **AWS**
- **GoPhish**