Phishing Attack Simulation

REPORT

DEMO - PC

CyberSapiens

THE CYBER SECURITY EXPERTS

GABRIEL REGISTRAR
ISO 27001

UNITED ACCREDITATION FOUNDATION
UAF
71808250205

Table of Contents

1. Document Attributes

Report Date	**27 February 2025**
Simulation Date	**27 February 2025**
Reviewed by	**Mohammed Nawaz Sajjad – Senior Security Analyst**
Approved by	**Shahid Ahmed P – Manager -Cyber Security**
Submitted to	**Demo - PC**

2. PhishCare

PhishCare is a simulator to create and run Phishing Campaigns in a very easy and smooth manner. It is designed to test the maturity level of users for identifying a phishing email. The tool automates the results in a report with an easy view of all the analytics of the Phishing activity performed. With the rise in phishing attacks day by day, it has become important to train the users to identify a phishing email and accordingly act towards the same. With more than a thousand of templates on the latest trends, the PhishCare tool makes it convenient to test the user's maturity as per the requirement.

3. Executive Summary

CyberSapiens performed a Phishing Attack Simulation (PAS) on **Demo - PC** using the tool PhishCare. This was a practical exercise intended to analyse and measure the maturity of **Demo - PC** personnel.

The results of this PAS show the susceptibility of **Demo - PC** personnel to social engineering attacks - specifically email phishing attacks, in which the users are tricked into clicking on malicious emails.

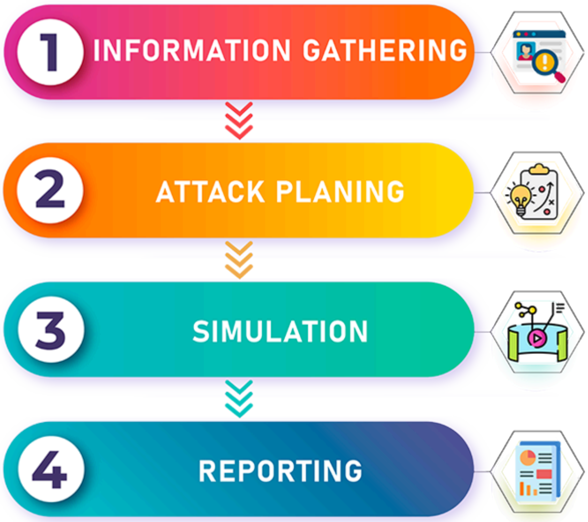
This activity was conducted in a manner that any malicious attacker would engage in real-time with the users. In this activity, CyberSapiens has assessed the provided scope of **Demo - PC** personnel.

4. Scope

The scope of this simulation covered **2** users of **Demo - PC** to test their maturity in identifying the Phishing emails.

5. Methodology

The Phishing Simulation was conducted in accordance with the CyberSapiens Methodology which has been derived from the industry best practices. And as follows below:



6. Simulation Timeframe

The simulation activity was performed from **27 February 2025** to **27 February 2025** as per the agreed schedule and the emails were monitored as per the campaign requirement.

7. Maturity Levels

The maturity level defines how much your users are mature to identify a phishing email, which will help the organization to understand the risks of Phishing Attack that they are exposed to.

Based on the levels and risks, necessary actions need to be taken.

Level	Criteria
Low	If the phished users are more than 75% of the total users.
Medium	If the phished users are more than 50% and less than 75% of the total users.
High	If the phished users are more than 25% and less than 50% of the total users.
Outstanding	If the phished users are less than 25% of the total users.

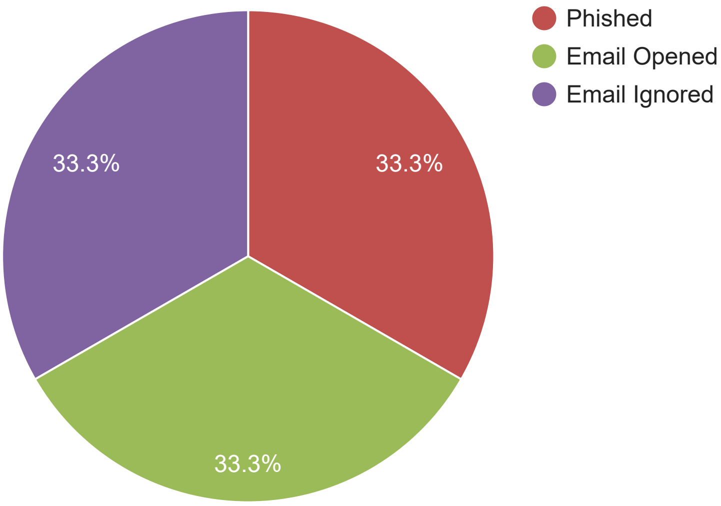
Maturity Level	Risk Level
Low	Critical
Medium	High
High	Medium
Outstanding	Low

∗Lower the Maturity Level, Higher the Risk will be

8. Simulation Summary

A summary of the phishing activity is given below:

Total Email Sent	**2**
Total Email opened (No of users who have accessed/read the email)	**1**
Total Phished (No of users who clicked on the link)	**1**
No of users who clicked and submitted data	**0**
No of users who ignored the Email	**1**



9. Risk Summary

- Based on the attack performed, the User Maturity Level is **Medium**
- Based on the Maturity Level, Demo - PC stands to be at a risk of **High**

10. Conclusion

This is a tool generated report which carries all the necessary information regarding the campaign executed for **Demo - PC** . Further, complete details are available in another report in the xls format which is shared separately.