ThreatCop

Phishing Simulation Report For

birlasoft

Prepared By

KRATIKAL
SECURE FOR SURE

DOCUMENT:	Birlasoft Phishing Simulation Report
PREPARED BY:	Kratikal Tech Pvt Ltd.
FOR:	Birlasoft
REPORT CONTENT:	Detailed Phishing Simulation Report
CLASSIFICATION:	Confidential
STATUS:	Confidential
DATE:	08-11-2022

DISCLAIMER

This report was generated by Kratikal Tech Pvt Ltd. and contains confidential data that might be sensitive in nature. This report shall not be copied or disclosed, in whole or in parts, without the prior written consent of Kratikal Tech Pvt Ltd. The report has been submitted on the condition that you shall not quote our name or reproduce our logo in any form or medium without our prior written consent.

The absolute accuracy, correctness, competency, or completeness of this report is based on the information provided to us and hence, no amount of guarantee can be taken for the findings, estimates and forecasts in the report since we believe that the advice, statement of opinion and recommendation is true.

You can disclose the information present in this report on your own discretion to your legal and other professional advisors for the purpose of seeking advice in relation to the report.

To the fullest extent permitted by law, we accept no liability or responsibility to them in connection with this report.

TABLE OF CONTENTS

PURPOSE

The purpose of this report is to provide a detailed analysis of the employees' susceptibility to phishing attack.

Today, most of the organizations have become largely dependent on network and technology. Data available digitally is extremely vulnerable since attackers have the required expertise to access the data using several attack-vectors.

This report will help you analyse the attack susceptibility of your employees against phishing, which is the most prominent cyber-attack as of now, since approximately 91% of the cyber-attacks are occurring due to the negligence of the employees by not paying attention to the email and clicking on fake links thereby submitting sensitive data.

APPROACH

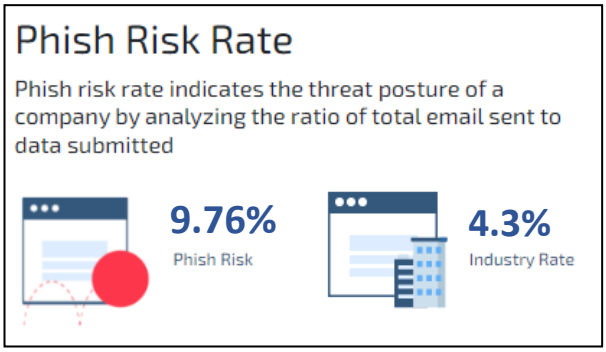
Campaigns are run on either one or more groups. A group consists of employees that can be selected either department wise or as per the requirement.

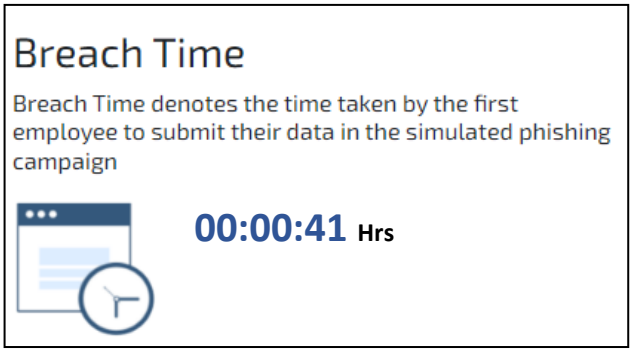
CAMPAIGN DETAILS

Executive Summary of Phishing Simulation

(Email Template: Myntra Voucher)

Phish Risk Rate and Breach Time:





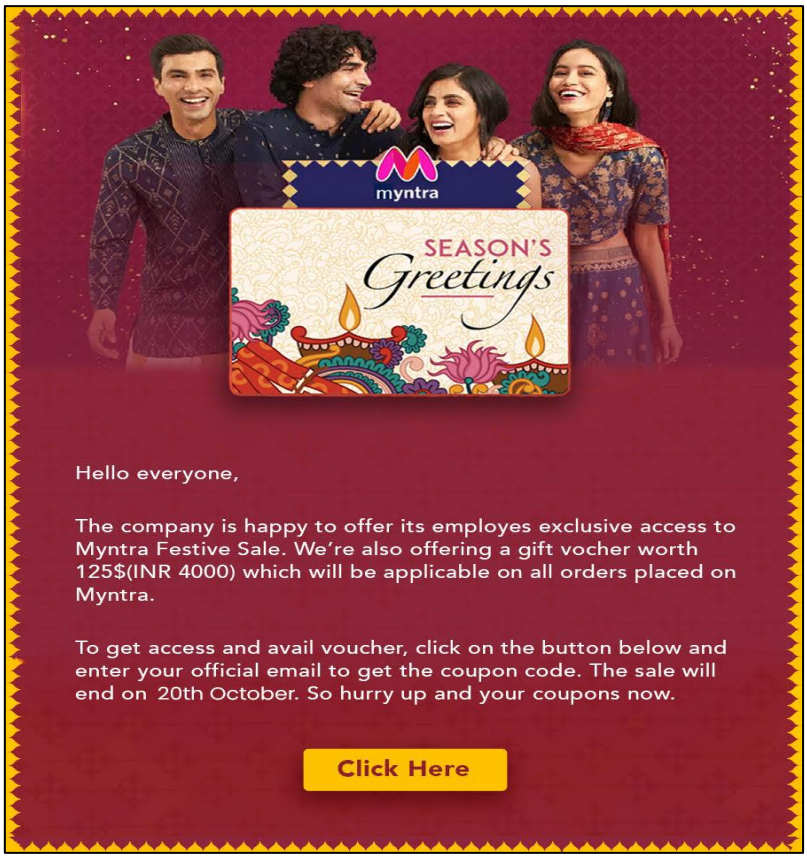
Phish Risk Rate and Breach Time for the above campaign was found to be **9.75%** and **41** Secs respectively.

First 5 Hacked Employees:

Bhaskar Kulshrestha ICTS HBU bhaskar.kulshrestha@birlasoft.com	41 Sec
Nilesh Namdeo Sawant Digital HBU nilesh.sawant@birlasoft.com	51 Sec
Prathyusha Peguda Digital HBU prathyusha.peguda@birlasoft.com	52 Sec
Naresh Mohanlal Jata IES HBU naresh.mohanlaljata@birlasoft.com	53 Sec
SRINIVAS KULKARNI IES HBU srinivas.kulkarni@birlasoft.com	53 Sec

Here is a list of first few users who became the victim of the simulated attack. It took only **41 secs** for the first employee to submit the data

PHISHING EMAIL TEMPLATE



The above shown email template was used in the **simulation** and sent to the user group involved in the campaign. Below are the red flags that an employee should have paid attention to:

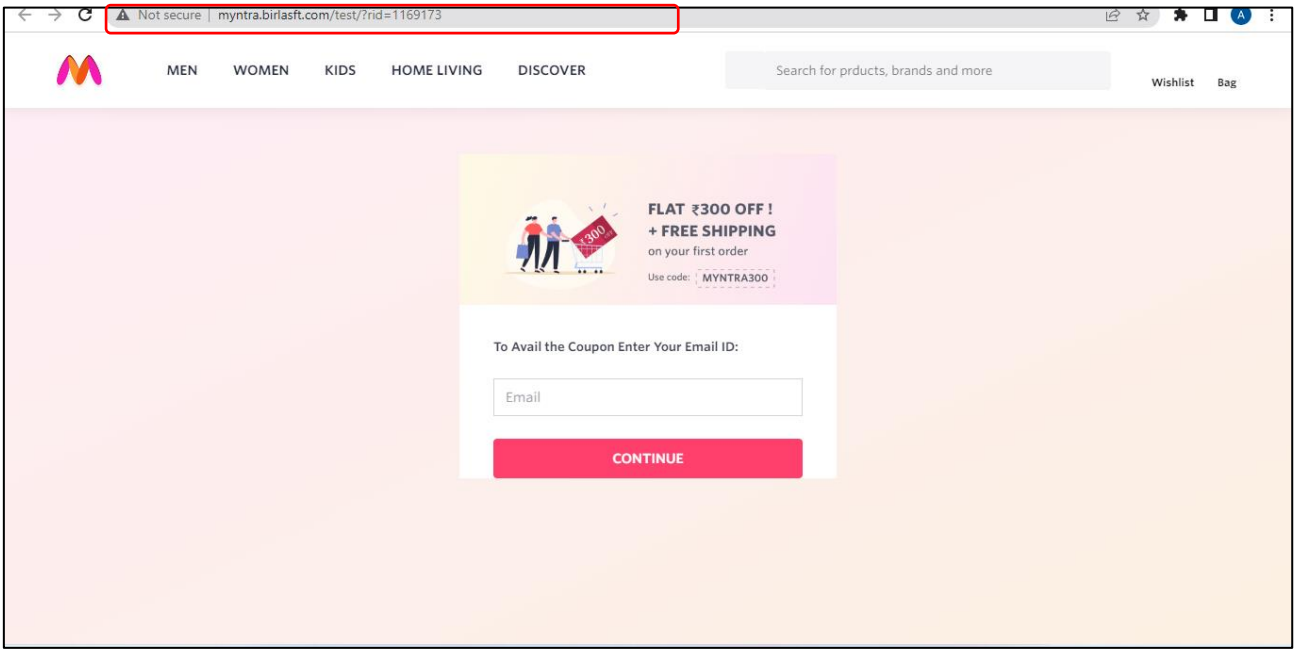
Sender id: This is a forged email address. While going through the email, you will notice that the sender ID is '<hr@birlasft.com>'. Here in **'Birlasoft'**, the letter ***'o'*** is missing to create a spoofed domain. The original domain name of '**Birlasoft is** '***@birlasoft.com'**.

What should be done?

1. When you hover on the linked text (which is Click Here in this case); within the template; you can see the actual URL to which you will be redirected.

2. In case you open the mail, read the email content carefully and look for certain spelling errors or any kind of urgency triggered amongst the users. Only then click on any links to proceed.

LANDING PAGE



Once the employee clicks on the link provided within the email, he/she will be redirected to a **Landing Page**. This page is a fake landing page meant for tricking employees into filling their credentials unknowingly.

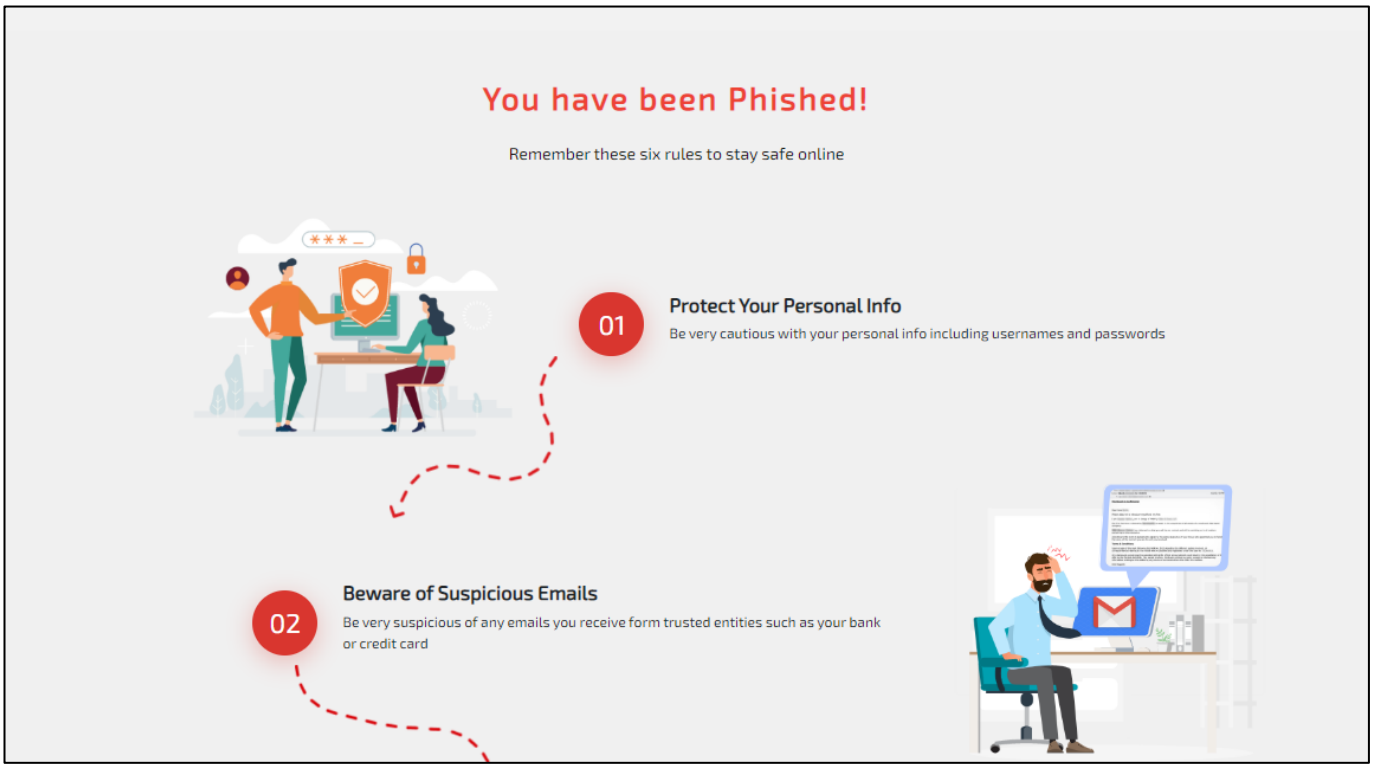
There are a few red flags that are present in the landing page:

1. **Insecure URL:** The URL of the above shown landing page is not secure since it is not over '***HTTPS'***.
2. **Incorrect URL:** The original URL for **Myntra** is "https://www.myntra.com" whereas the one used in this phishing campaign is 'http://myntra.birlasft.com'

What should be done?

- *Do not react but respond.* Once you are directed to a login page, take out some time to look at the URL. Check whether the URL is insecure or has an incorrect TLD (Top level domain)
- Try clicking on the hyperlinked sections within the landing page since most of the hyperlinks do not work on phished webpages.

AWARENESS PAGE



Once the employee clicks on the **'Continue'** button; an awareness page appears on the screen displaying the message **"You Have been Phished"** and an infographic on how to identify a phishing email.

CONCLUSION

It can be safely concluded from the above data that out of the total **12808** emails sent, **3377** employees opened the email. Out of those **2440** employees clicked the links and **1250** employees even submitted their data. These numbers are indicative of the fact that still there exists some room for improvement among employees while dealing with the phishing emails. It is clearly reflected in the percentage of people who became the victim of the attack, which is **9.75%**.

As per the industry standards, if the percentage of the vulnerable employees in an organization is more than **4.3** %, then the organization is susceptible to cyber-attacks. In our case, this percentage stands at **9.75%** and such low-scale attack can easily put the organization at risk.

RED FLAGS IN EMAIL TEMPLATE

- The sender id is 'hr@birlasft.com' instead of '*@birlasoft.com'.
- The URL of the above shown landing page is not secure since it is not over 'https'.
- The URL was changed from "https://www.myntra.com" to "http://myntra.birlasft.com".

|| Thank You ||