



ThreatCop

Phishing Simulation Report
For



Prepared By



DOCUMENT: Kotak Life Insurance ThreatCop Phishing Simulation Report

PREPARED BY: Kratikal Tech Pvt Ltd.

FOR: Kotak Life Insurance

REPORT CONTENT: Detailed Phishing Simulation Report

CLASSIFICATION: Confidential

STATUS: Confidential

DATE: 02-02-2022

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

1. *Purpose*
2. *Approach*
3. *Campaign Details*
Analysis of the campaign
4. *Template Used*
5. *Landing Page*
6. *Awareness Page*
7. *Conclusion*

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.

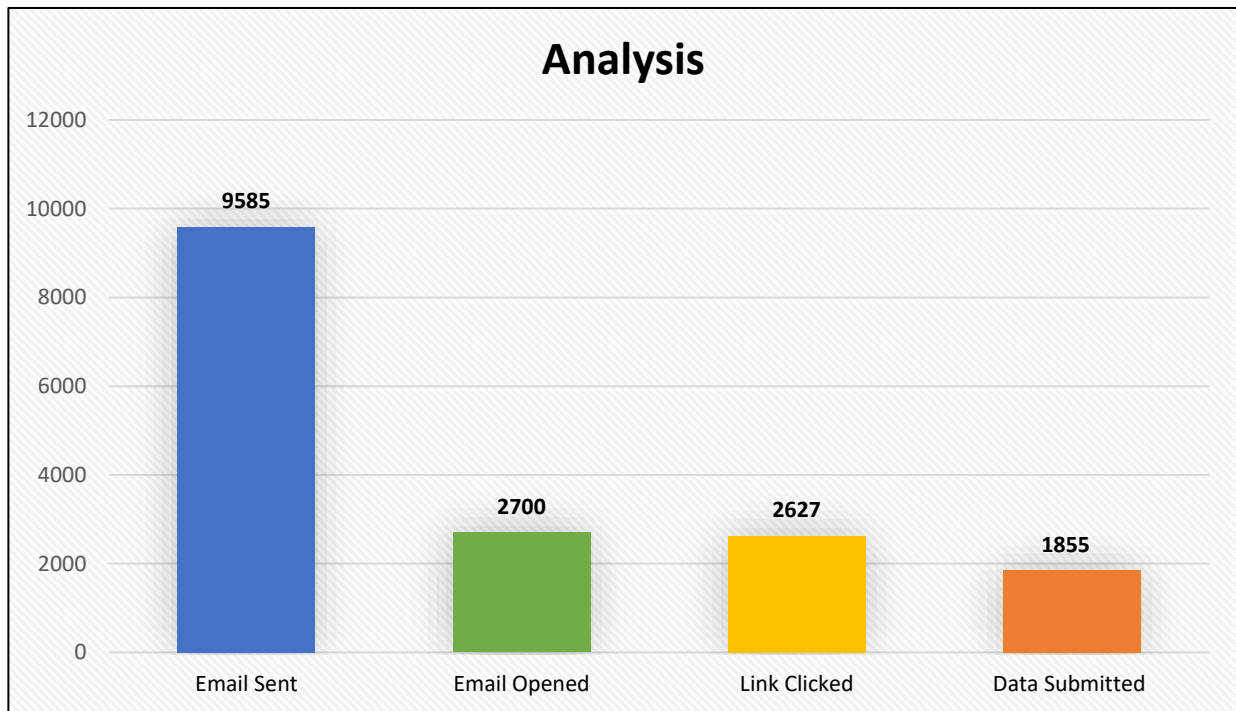
APPROACH

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: EPFO e-nomination for employees)



The above bar graph represents the number of 'email sent', 'email opened', 'link clicked and, 'data submitted' by the employees involved in the campaign.

PHISHING EMAIL TEMPLATE



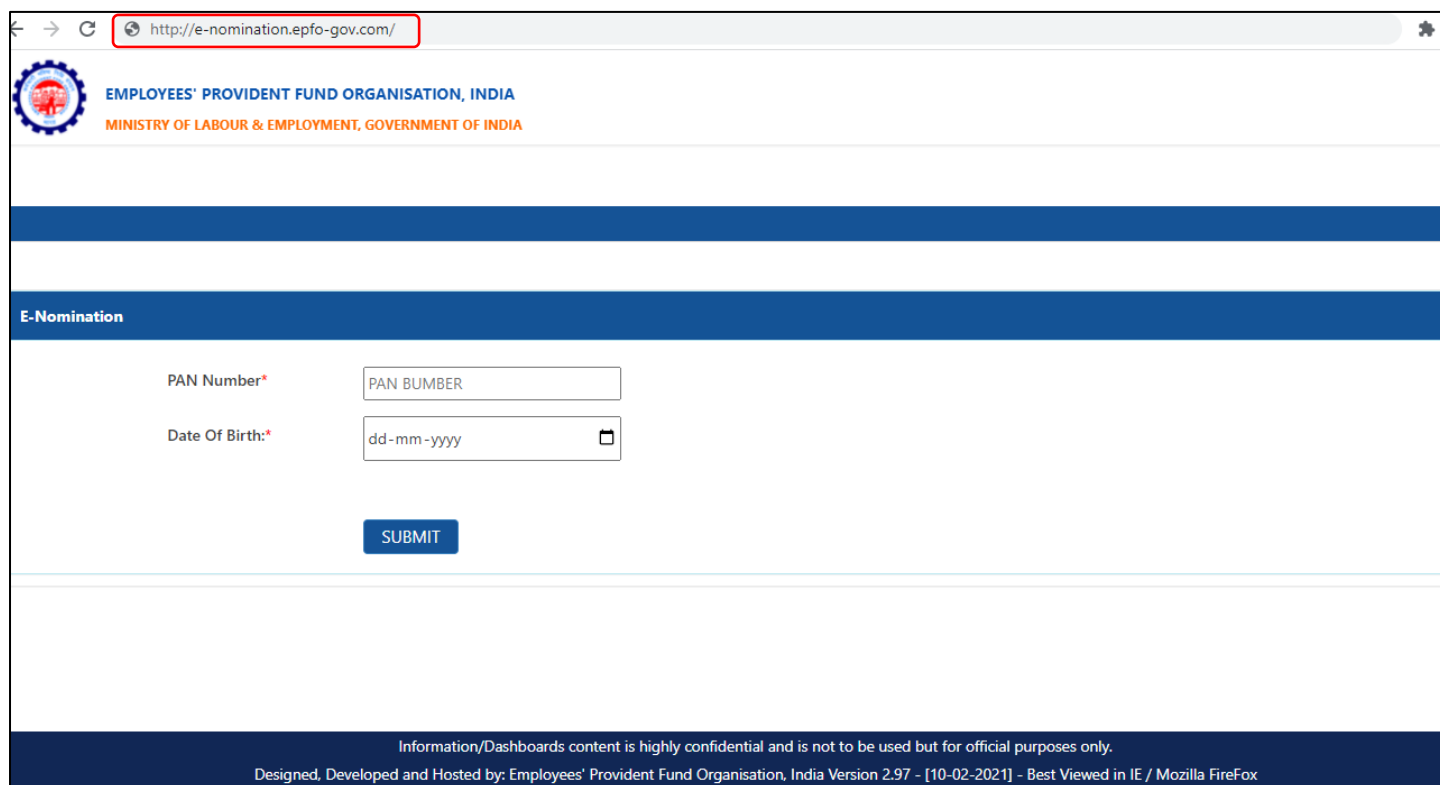
The above shown email template was used in the **simulation** and sent to the user group involved in the campaign. Below are the red flags that an employee should have paid attention to:

Sender id: This is a forged email address. The sender id is (almost) identical to the email address of EPFO India. In this email template, the sender id is '**noreply@epfo-gov.com**', whereas the original domain of EPFO is '***@epfindia.gov.in**'


What should be done?

1. When you hover on the linked text (which is [Update 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



← → ↻ http://e-nomination.epfo-gov.com/

 EMPLOYEES' PROVIDENT FUND ORGANISATION, INDIA
MINISTRY OF LABOUR & EMPLOYMENT, GOVERNMENT OF INDIA

E-Nomination

PAN Number*

Date Of Birth:*

Information/Dashboards content is highly confidential and is not to be used but for official purposes only.
Designed, Developed and Hosted by: Employees' Provident Fund Organisation, India Version 2.97 - [10-02-2021] - Best Viewed in IE / Mozilla FireFox

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 EPFO Bank is "[https:// www.epfindia.gov.in](https://www.epfindia.gov.in)" whereas the one used in this phishing campaign is "<http://e-nomination.epfo-gov.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

You have been Phished!

Remember these six rules to stay safe online

The infographic consists of six numbered rules connected by a red dashed line. Rule 01: 'Protect Your Personal Info' with an illustration of a person at a computer. Rule 02: 'Beware of Suspicious Emails' with an illustration of a person looking at a computer screen. Rule 03: 'Do Not Click Suspicious Links' with an illustration of a person holding a laptop. Rule 04: 'Know Common Phishing Language' with an illustration of a person at a computer. Rule 05: 'False Sense Urgency' with an illustration of a person at a computer. Rule 06: 'Do Not Provide Personal Information' with an illustration of a person at a computer. The infographic also includes illustrations of a person at a computer, a person holding a laptop, and a comparison between a 'Phishing email' (red envelope) and a 'Legitimate email' (green envelope).

- 01 Protect Your Personal Info**
Be very cautious with your personal info including usernames and passwords
- 02 Beware of Suspicious Emails**
Be very suspicious of any emails you receive from trusted entities such as your bank or credit card
- 03 Do Not Click Suspicious Links**
Deceptive links that mimic legitimate URLs addresses are a common tool used in phishing scams
- 04 Know Common Phishing Language**
Legitimate businesses will not send you email to ask for your login information or sensitive personal information
- 05 False Sense Urgency**
Look out for emails that try to convey a sense of urgency and be wary of any email that does not address you directly
- 06 Do Not Provide Personal Information**
Do not provide personal information to anyone who asks for it over the phone or through email

Once the employee clicks on the **'Submit'** button; an awareness page appears on the screen displaying the message "You Have been Phished" and certain steps one can take to prevent phishing attack.

CONCLUSION

It can be safely concluded from the above data that out of the total **9585** emails sent, **2700** employees opened the email. Out of those **2627** employees clicked the links and **1855** employees even submitted their data. This is a threatening situation for the organization since this indicates the lack of awareness in employees. Therefore, the percentage of people who were the victim of the attack comes out to be **19.35%**.

As per the industry standards, if the percentage of the vulnerable employees in an organization is more than 4%, then the organization is susceptible to cyber-attacks. In our case, this figure is concerning at **19.35%** and a low-scale attack can easily put the organization at risk. It is like we are sitting on a landmine and are secure only until a real attack takes place.

The situation is concerning since **1855** employees have a high Employee Vulnerability Score (EVS) which is extremely dangerous since in an actual cyber-attack, **a single employee with high EVS is enough to cripple the entire organization.**

RED FLAGS IN EMAIL TEMPLATE

- The sender id is '**noreply@epfo-gov.com**' instead of '*@epfindia.gov.in'.
- The URL of the above shown landing page is not secure since it is not over 'https'.
- The URL was changed from "**https://www.epfindia.gov.in/** to "**http://e-nomination.epfo-gov.com**".

|| Thank You ||