Project Title:Web Phishing Detection **Project Design Phase-I - Proposed Solution Fit** **Team ID PNT2022TMID19033**

Define CS, fit into CC

1. CUSTOMER SEGMENT(S) CS

Customer segmentation is the process of separating customers into groups on the basis of their shared behavior or other attributes. The groups should be homogeneous within themselves and should also be heterogeneous to each other.

The overall aim of this process is to identify high-value customer base i.e.customers that have the highest growth potential or are the most profitable.

6. CUSTOMER CONSTRAINTS CC

An exhaustive systematic search was performed on all the indexing databases. The state-of-the-art research related to the web phishing detections was collected.

The papers were classified based on methodologies. A taxonomy was derived by performing a deep scan on the classified papers. The contributions listed in this survey are exhaustive and lists all the state-of-the-art development in this area.

5. AVAILABLE SOLUTIONS AS

Phishing detection and response tools provide a range of benefits to businesses. In addition to reducing phishing attacks on the organization, phishing detection tools reduce the number of reported false positives that administrators must manage.

They can also automate various routine remediation processes in response to threats, saving admins more time and reducing the time it takes to identify and remediate high-tier vulnerabilities or breaches.

Explore AS, differentiate

Focus on J&P, tap into BE, understand RC

2. JOBS-TO-BE-DONE / PROBLEMS J&P

This article is the first of a series of three related to the challenges that we faced to detect phishing attacks at scale with constraints on accuracy and performance.

In this article, we will describe how—starting mainly from the email stream—we identify suspicious links and then fetch the content from the associated webpages.

In the next article, we will describe how suspicious webpages are analyzed and assessed in real-time, with a focus on Supervised Learning techniques.

9. PROBLEM ROOT CAUSE RC

Nowadays, many people are losing considerable wealth due to online scams. Phishing is one of the means that a scammer can use to deceitfully obtain the victim's personal identification, bank account information, or any other sensitive data.

There are a number of anti-phishing techniques and tools in place, but unfortunately phishing still works.

One of the reasons is that phishers usually use human behaviour to design and then utilise a new phishing technique.

7. BEHAVIOUR BE

Phishing detection systems are principally based on the analysis of data moving from phishers to victims.
.
In this paper we describe a novel approach to detect phishing websites based on analysis of userspsila online behaviours - i.e., the websites users have visited,and the data users have submitted to those websites.

Focus on J&P, tap into BE, understand RC

Identify strong TR & EM

3. TRIGGERS TR

I have found the following four psychological triggers that ecommerce platforms should adopt to increase customer urgency and drive sales:
Utilize the personal touch,Encourage loyalty
Incentivize customers,Capitalize on FOMO.

4. EMOTIONS: BEFORE / AFTER EM

Phishing attacks have always targeted people's emotions.COVID has drastically amplified those emotions,and hackers have not missed the opportunity. During the pandemic, thousands of attacks are taking place every day, preying on people's fears and uncertainty regarding the virus, their jobs and their future.COVID-19-themed phishing attacks now account for 30 percent of all phishing websites.

10. YOUR SOLUTION SL

Paying attention. That's it.

Phishing attacks are an example of social engineering. They rely on the gullibility of the victim rather than technical trickery, and hence have to be stopped by the potential victim being aware and using their brain rather than just clicking on the shiny pictures.

This of course is why confidence tricks never work.

8.CHANNELS of BEHAVIOUR CH

Once a useropens a new webpage, the monitor decides in which mode UBPD should be running.

Then, according to the working mode the monitor chooses appropriate method to collect the data the user submitted to the current webpage, and sends it to the detection engine once the user initiates data submission.

Identify strong TR & EM