Web Phishing Detection **Team ID :PNT2022TMID28334**

Problem-Solution fit canvas 2.0

Purpose / Vision

Define CS, fit into CC

1. CUSTOMER SEGMENT(S) — CS

Who is your customer?

- Protect yourself and your family against malicious websites with the platform for free.
- With the platform, protecting your staff, data, brand, and your customer from malicious websites has never been easier.
- Proactively protect multiple customers against malicious websites at once with all-in-one platform.
- The platform can be used for government embeds to provide 100% security and privacy.

6. CUSTOMER CONSTRAINTS — CC

What constraints prevent your customers from taking action or limit their choices of solutions?

- The limitations of the web phishing detection approaches are explored by means of detection time, detection rate, and storage complexity to verify the level of robustness against the phishing attack.
- Thus most of the recent web phishing detection approaches lag in feature selection mechanism as they use handcrafted features to detect the attack.

5. AVAILABLE SOLUTIONS — AS

Which solutions are available to the customers when they face the problem or need to get the job done? What have they tried in the past? What pros & cons do these solutions have?

- Legitimate websites prevent web scraping by several techniques in respect to obfuscation using CSS sprites to display important data, replacing text with images.
- Spam filtering techniques are used to identify unsolicited emails before the user reads or clicks the link.
- When users visit a phishing web page that looks like a legitimate website, many people do not remember the legitimate website's domain name, particularly for some start-ups or unknown companies, so users cannot recognise the phishing website based on the URL. Some web browsers integrate a security component to detect phishing or malware sites, such as Chrome, which will display warning messages when one visits an unsafe web page.
- When the website detects that the IP address and device information of the user who is logging in does not match the commonly used information, it is necessary to verify the authenticity of the user

Explore AS, differentiate

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

2. JOBS-TO-BE-DONE / PROBLEMS — J&P

Which jobs-to-be-done (or problems) do you address for your customers? There could be more than one; explore different sides.

- The objective of phishing website URLs is to purloin the personal information like user name, passwords and online banking transactions.
- Phishers use the websites which are visually and semantically similar to those real websites.
- As technology continues to grow, phishing techniques started to progress rapidly and this needs to be prevented by using anti-phishing mechanisms to detect phishing.

9. PROBLEM ROOT CAUSE — RC

What is the real reason that this problem exists?
What is the back story behind the need to do this job?

- A phishing attack is a type of cybersecurity threat that targets users directly through email, text or direct messages. During one of these scams, a cybercriminal will pose as a trusted contact to steal data from an unsuspecting user such as login information, account numbers and credit card information.
- While there are several types of phishing, the main purpose behind all of them is it to steal sensitive information or transfer malware.

7. BEHAVIOUR — BE

What does your customer do to address the problem and get the job done?
I.e. directly related: find the right solar panel installer, calculate usage and benefits; indirectly associated: customers spend free time on volunteering work

- Customers should take a "trust no one" approach when opening email.
- Check and verify the "From" address of the email.
- By carefully reading the email copy, users can typically spot something that seems "off" including:
- An email with an "urgent" request or An email offering the user something that's "too good to be true".
- Check grammar and spelling. Poor grammar and misspelled words in an email can be red flags.
- Be wary of generic salutations in an email. Legitimate companies, especially those with which you have accounts or have done business typically will address you by name versus by a generic greeting.
- Encourage your clients to look for any unusual or odd requests in their emails. Most fraudulent emails contain a request to respond to the email or click a link in it.
- Avoid clicking links or attachments in emails from unfamiliar sources.

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

Identify strong TR & EM

3. TRIGGERS — TR

What triggers customers to act?

- Your users lack security awareness .
- Criminals are (unsurprisingly) following the money .
- You're not performing sufficient due diligence .
- Low-cost phishing and ransomware tools are easy to get hold of .
- Malware is becoming more sophisticated .

4. EMOTIONS: BEFORE / AFTER — EM

How do customers feel when they face a problem or a job and afterwards?

- Greed- Clicking on fake successful messages.
- Urgency-Hackers use fake security alerts with exclamation marks.
- Helpfulness-Hackers and cyber criminals use major tragedies to appeal for help but they are only helping themselves.
- Fear- Emails that spread fear and phishing links go hand in hand.

10. YOUR SOLUTION — SL

If you are working on an existing business, write down your current solution first, fill in the canvas, and check how much it fits reality.
If you are working on a new business proposition, then keep it blank until you fill in the canvas and come up with a solution that fits within customer limitations.
solves a problem and matches customer behaviour.

- We would create an interactive and responsive website that will be used to detect whether a website is legitimate or phishing.
- This website is made using different web designing languages which include HTML, CSS, JavaScript and Python.
- This website is more useful to the user and it is user friendly also.

8. CHANNELS of BEHAVIOUR — CH

8.1 ONLINE
What kind of actions do customers take online? Extract online channels from #7

- Nothing teaches like experience. When employees click on a link or an attachment in a simulated phishing email, it's important to communicate to them that they have potentially put both themselves and the organisation at risk.

8.2 OFFLINE
What kind of actions do customers take offline? Extract offline channels from #7 and use them for customer development.

- Phishing awareness training starts with educating your employees on why phishing is harmful, and empowering them to detect and report phishing attempts.
- Simulated phishing campaigns reinforce employee training, and to understand risk and improve workforce resiliency as these can take many forms, such as mass phishing, spear phishing, and whaling.

Extract online & offline CH of BE