Project Title:WEB PHISHING DETECTION

Project Design Phase-I-Solution Fit Template

Team ID : PNT2022TMID12128

Define CS, fit into CC

1. CUSTOMER SEGMENT(S) — CS

Who is your customer?
i.e. working parents of 0-5 y.o. kids

1. The main customer focus is on people who use the internet for e-transactions and banking organizations where safeguarding customers data is important and vital.
2. Government agencies and industries are another customer base where they require phishing detection systems to safeguard confidential information or any sensitive business data.

6. CUSTOMER CONSTRAINTS — CC

What constraints prevent your customers from taking action or limit their choices of solutions? i.e. spending power, budget, no cash, network connection, available devices.

1. Lacking basic knowledge in verifying the correct URL of the webpage.
2. Insufficient backup processes, lack of user testing by organization as they require more resources and money. They are always in a rush which makes them prone to errors.
3. Malwares have become more complex than what a layman can understand.

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? i.e. pen and paper is an alternative to digital notetaking

1. Using a good Antivirus software or an Anti-Phishing toolbar which are available as extensions in browsers. Verifying the websites privacy policy and ensuring the websites are SSL certified.
2. Double checking the domain name.
3. Anti-Spam software and Blacklisting.

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.

1. The phishing websites must be detected prior and should be blacklisted.
2. Building a phishing URL detecting website where the user can copy paste the URL and find if the URL is legitimate.
3. Companies trust is broken if private data of customers are leaked.

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?
i.e. customers have to do it because of the change in regulations.

1. Lack of basic awareness among the common folk and leniency in the adaption of new security measures
2. Low-cost phishing and ransomware tools are easy to get hold of.
3. The financial incentive is high which makes more people to launch phishing attacks despite of the consequences.

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 (i.e. Greenpeace)

1. Customers should take a “trust no one” approach when opening an email and should always verify the “From” address of the email.
2. 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.
3. Avoid clicking links or attachments in emails from unfamiliar sources and change your passwords regularly.

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

Identify strong TR & EM

3. TRIGGERS — TR

What triggers customers to act? i.e. seeing their neighbor installingsolar panels, reading about a more efficient solution in the news.

1. To prevent data including login credentials and credit card numbers from getting stolen.
2. Seeing others lose Money due to phishing and their reputation getting damaged. This increases the awareness of the person.

4. EMOTIONS: BEFORE / AFTER — EM

How do customers feel when they face a problem or a job and afterwards?
i.e. lost, insecure > confident, in control - use it in your communication strategy & design.

BEFORE:

1. They feel threatened and insecure using the internet.
2. Anxiety and stress are also other emotions. Experienced.

AFTER:

1. Stress free and a sense of security knowing that their personal data is protected..

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 inthe canvas and come up with a solution that fits within customer limitations, solves a problem and matches customer behavior .

1. A deep learning-based framework by implementing it as a browser plug-in capable of determining whether there is a phishing risk in real-time when the user visits a webpage and gives a warning message.
2. The real-time prediction includes whitelist filtering, blacklist interception, and ML prediction. To deal with phishing attacks and distinguishing the phishing webpages automatically, Blacklist based detection technique keeps a list of websites' URLs that are categorized as phishing sites.
4. Machine Learning based approaches rely on classification algorithms such SVM and DT to train a model that can later automatically classify the fraudulent websites at run-time without any human intervention.

8. CHANNELS of BEHAVIOUR — CH

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

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

Online:

1. By using appropriate firewalls and not clicking random pop ups in browsers and in email links.
2. Using a secure wifi network for online transactions and always double checking the URL twice beforehand.

Offline:

1. Not sharing confidential information in spam phone calls or in random messages.
2. Raising awareness by conducting small camps in your locality among the elderly and people who have less computer knowledge.

Identify strong TR & EM