

Ideation Phase

Problem Statements and Ideation Phase

Date	14 November 2022
Team Id	PNT2022TMID46893
Project Name	Project – WEB PHISHING DETECTION
Maximum Marks	2 Marks

Customer Problem Statement Template:

As online transactions grew in popularity, cybercrimes also grew quickly. Because of the anonymity offered by the internet, hackers try to trick users by using techniques like phishing, SQL injection, malware, man-in-the-middle attacks, domain name system tunnelling, ransomware, web trojans, and other forms of attack. Phishing is said to be the most misleading of all of these tactics.

Problem - 1



Problem - 2



Problem - 3



Problem - 4



Problem Statement (PS)	I am (Customer)	I'm trying to	But	Because	Which makes me feel
PS-1	Student	Opens an compromised link and enters the credentials	Gets Hacked	It was a Fake website	Insecure
PS-2	Shopkeeper	Opens a link from a bank and enters the account details	His bank account details and his credit card details gets hacked	The link was fake and the hacker aims for the money from the account.	untrustworthy
PS-3	Homemaker	make transactions for the purchased items from checkouts	Ended up as she purchases from an fake website	The website had an advertisement for discounts.	disappointed
PS-4	Employer	complete the tasks by the end of the day	Found an file through mail and opens it, and his company details gets hacked	the file seemed to be phishing and fake one	annoyed & disturbed

Brainstorming Ideation Phase:

Template



Brainstorm & idea prioritization

Use this template in your own brainstorming sessions so your team can unleash their imagination and start shaping concepts even if you're not sitting in the same room.

10 minutes to prepare
1 hour to collaborate
2-8 people recommended

Share template feedback

01

Before you collaborate

A little bit of preparation goes a long way with this session. Here's what you need to do to get going.

10 minutes

- Team gathering**
Define who should participate in the session and send an invite. Share relevant information or pre-work ahead.
- Set the goal**
Think about the problems you'll be focusing on solving in the brainstorming session.
- Learn how to use the facilitation tool**
Use the Facilitation Superpowers to run a happy and productive session.

Open article

02

Define your problem statement

What problem are you trying to solve? Frame your problem as a How Might We statement. This will be the focus of your brainstorm.

5 minutes



As online transactions grew in popularity, cybercrimes also grew quickly. Because of the anonymity offered by the internet, hackers try to trick users by using techniques like phishing, SQL Injection, malware, man-in-the-middle attacks, domain name system tunnelling, ransomware, web trojans, and other forms of attack. Phishing is said to be the most misleading of all of these tactics.

03

Brainstorm

Write down any ideas that come to mind that address your problem statement.

10 minutes

Tip
You can select a sticky note, and let the virtual camera be ready to move the note around!

Akash.S (Team Leader)

Difficult to block "redirecting pages," as these URLs can be disguised

To keep track of all potential phishing techniques, use an intelligent online security gateway.

Analytical comparison of trustworthy and fraudulent websites

Ramki.V (Team member 1)

Web phishing detection with advanced deployment

Maintaining web phishing records with a spam repository

Observation of resource loading times to identify fraudulent websites' tendencies to display just costs rather than their functionality

Guhan.v, Vishwa.K (Team member 2, Team member 3)

Link pathways are being traced after detection of tampering

By contrasting it with real online domain names, homograph spoofing can be identified.

To check for extended links and prevent link shortening, because most fraudulent websites use the "bit.ly" extension

Ashok.D, Anandharajan.S (Team member , Team member 4)

Incorrectly worded keywords and odd website changes

Requesting confirmation of unrelated qualifications

Verify secure web protocols like "https" visually