

## Ideation Phase

### Problem Statements and Ideation Phase

Team ID	PNT2022TMID50410
Project Name	WEB PHISHING DETECTION

#### Customer Problem Statement:

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:

### Brainstorm & idea prioritization

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

1. Welcome to ideate
2. Team is selected
3. 3-5 people are involved

#### 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.

1. Welcome
2. Team is selected
3. 3-5 people are involved

#### Define your problem statement

What problem are you trying to solve? Frame your problem as a how might this statement. This will be the focus of your brainstorm.

How might we (your problem statement)?

As online transactions grow in popularity, cybercriminals also grow quickly. Because of the anonymity offered by the internet, hackers try to find ways to steal sensitive data (credit card, ID, medical, business, etc.) and use it for their own gain. Phishing is used to be the most widespread of all of these tactics.

#### Brainstorm

After the session you'll have a lot of ideas. Don't worry, you'll have a chance to refine them later.

1. Welcome
2. Team is selected
3. 3-5 people are involved

#### Saadhana, G(Team Leader)

Difficult to track "redocking pages" as these URLs can be disguised.

To know more of all potential phishing techniques, you can design a security gateway.

Analyze comparison of bandwidth and "redocking" endpoints.

#### Seelashree, G(Team member 1)

Anti-phishing detection with advanced technology.

Monitoring web phishing reports with a team monitoring.

Remember of network history. Know its identity. Network history. Remember to check and make sure that their functionality.

#### Arya Priya, V(Team member 2)

Like phishing and being traced after detection of phishing.

By understanding it with real-time phishing tactics, a network security can be identified.

To make the network more secure and prevent loss, stopping phishing attacks (phishing) is the best way to prevent.

#### Venkatesh, V(Team member 3)

Indirectly worked endpoints and add website changes.

Requesting confirmation of a website's authenticity.

Verify secure web protocols (like "https") properly.