Empathy Map Canvas

Designed by: Prasanna D, Thambi Durai P.K

# 1 Who are you empathizing with?

* Who is student you’re trying to understand?

We are Prasanna & Thambidurai and we are trying to detect web phishing.

* What is their situation?

The URL of phishing websites may be very similar to real websites to the human eye, but they are different in IP. **The content-based detection usually refers to the detection of phishing sites through the pages of elements, such as form information, field names, and resource reference**

2

Aim

Web phishing **aims to steal private information, such as usernames, passwords, and credit card details, by way of impersonating a legitimate entity**. It will lead to information disclosure and property damage. We need to detect the before attack and solve all conflicts.

What do they need to do?

* What do they need to do differently?

Software-based phishing detection techniques are preferred for fighting against the phishing attack. Mostly available methods for detecting phishing attacks are **blacklists/whitelists, natural language processing, visual similarity, rules, machine learning techniques.**

* What things do they need to get done?

Current methods for phishing detection include **black and whitelists, heuristics, visual similarity, and machine learning**, among which heuristics and machine learning are more widely used.

* How will we know they were successful at this?

Detection Process. Detecting Phishing Domains is a classification problem, so it means we need labeled data which has samples as phish domains and legitimate domains in the training phase. **The dataset which will be used in the training phase** is a very important point to build successful detection mechanism.

Date: 30.10.2022

# What do they think and feel?

# Phishing is the ultimate social engineering attack, giving a hacker the scale and ability to go after hundreds or even thousands of users all at once. **Phishing scams involve sending out emails or texts disguised as legitimate sources**.

7

6 What do they hear?

* What are they hearing others say? Hacker Attacks.
* What are they hearing from their friends? Someone hacked you and

stealed your information.

* What are they hearing from teachers? Data Breach.
* What are they hearing from their parents? Your personal information

belongs to someone we don’t know.

# 4 What do they say?

It occurs when an attacker, masquerading as a trusted entity, dupes a

victim into opening an email, instant message, or text message.

* What have you heard them say?
* What can you imagine them saying?

# 5 What do they do?

* What behavior have we observed?

Phishing **tricks victims into giving over credentials for all sorts of sensitive accounts**, such as email, corporate intranets and more. Even for cautious users, it's sometimes difficult to detect a phishing attack.

* What can we imagine them doing?

Lack of security awareness among employees is also one of the major reasons for the success of phishing. Organizations should be aware of how the benefits and purpose of security awareness training can secure their employees from falling victim to phishing attacks.

*We acknowledge the original work and source material for empathy maps to be Prasanna and his Teams. ’Web Phishing Detection’ this work with respect and does not claim to have created the original concept.*