2 IDEATION PHASE

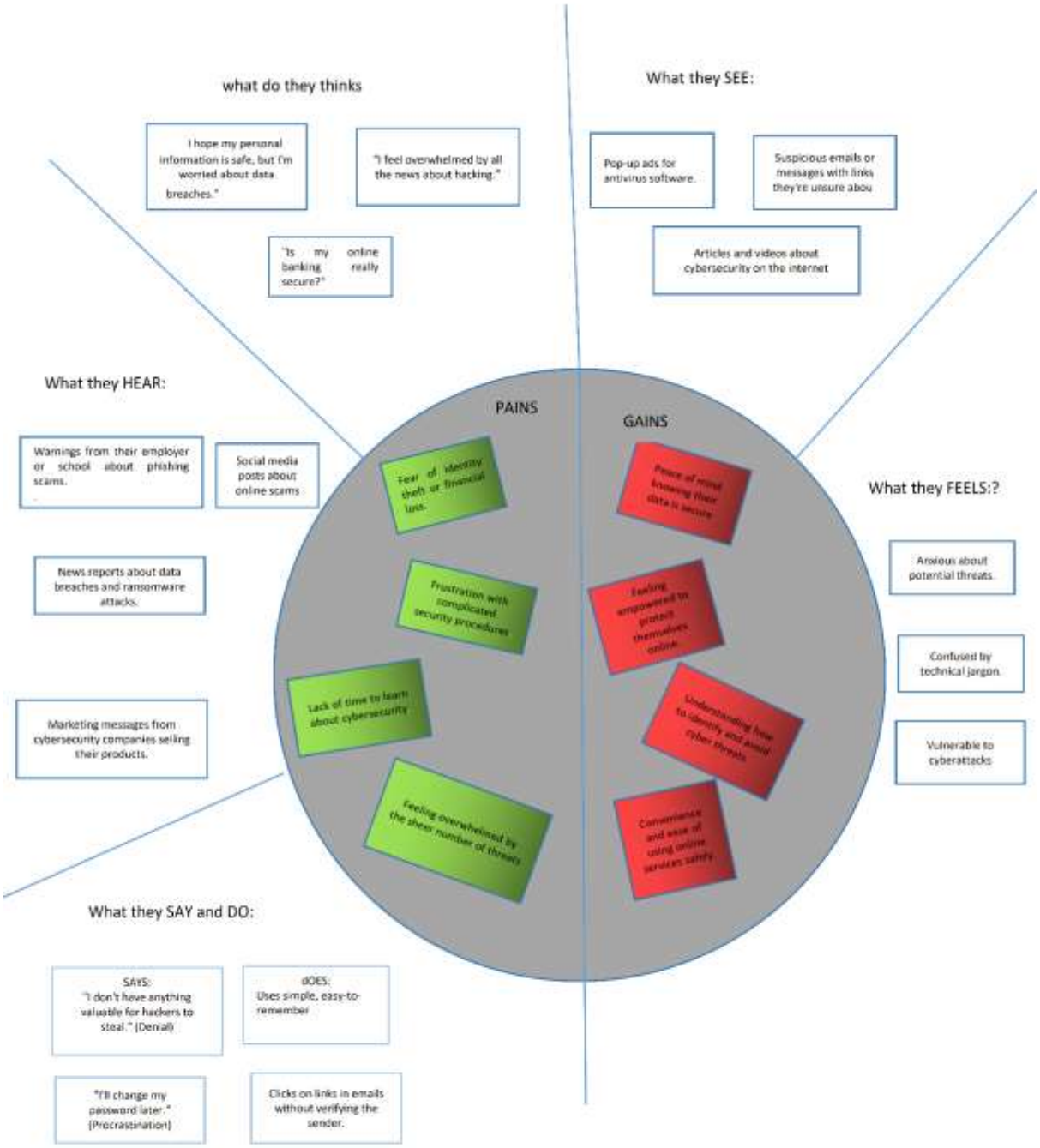
2.1 Problem Statement

Phishing emails are deceptive messages designed to appear as if they are from a trusted source, leading users to provide sensitive information unknowingly. These attacks are difficult to detect because cybercriminals use advanced techniques such as:

- Fake email addresses that resemble real domains.
- Links that redirect users to fraudulent websites.
- Urgent and manipulative messages to trick recipients into taking action.

Traditional spam filters and rule-based security systems **fail to detect advanced phishing attacks** due to their static nature. Therefore, a dynamic, learning-based approach is required to improve detection accuracy.2.2 Empathy Map Canvas

2.2 Empathy Map Canvas


what do they thinks
I hope my personal information is safe, but I'm worried about data breaches."
"I feel overwhelmed by all the news about hacking."
"Is my online banking really secure?"
What they SEE:
Pop-up ads for antivirus software.
Suspicious emails or messages with links they're unsure abou
Articles and videos about cybersecurity on the internet
What they HEAR:
Warnings from their employer or school about phishing scams.
Social media posts about online scams
News reports about data breaches and ransomware attacks.
Marketing messages from cybersecurity companies selling their products.
PAINS
GAINS
Fear of identity theft or financial loss.
Frustration with complicated security procedures
Lack of time to learn about cybersecurity
Feeling overwhelmed by the sheer number of threats
Peace of mind knowing their data is secure
Feeling empowered to protect themselves online
Understanding how to identify and avoid cyber threats
Convenience and ease of using online services safely
What they FEELS:?
Anxious about potential threats
Confused by technical jargon
Vulnerable to cyberattacks
What they SAY and DO:
SAYS:
"I don't have anything valuable for hackers to steal." (Denial)
dOES:
Uses simple, easy-to-remember
"I'll change my password later." (Procrastination)
Clicks on links in emails without verifying the sender.

2.3 Brainstroming

Pratiksha Satavekar

Analyzing the Evoiution of Ransomware

IOT Vulnerabilities

Deepfakes and Social Engineering

Akshaya Chavan

Cloud Security Breaches

Insider Threat

The Threat of AI-Powered cyberattacks

Priyanshi Kalra

AI Driven Threat detection

Zero Trust Security Implementation

Anuja Bodhale

BlockChain for Cyber Security

Security Automation and Orchestration