Ideation Phase

Empathize & Discover

Date	18 October 2023
Team ID	Team-592613
Project Name	Online Payments Fraud Detection Using ML
Maximum Marks	5 Marks
Team Members	Srajal Agarwal (Leader) Deepesh Dhruv Paras Garg

Empathy Mapping for “Online Payments Fraud Detection Using ML”

An empathy map is a useful tool that may be used by teams as they go on the journey to obtain deeper insights into their users. In the context of our project, "Online Payments Fraud Detection Using ML" this tool is more than simply an asset, it is a vital success factor. The success of our endeavour is dependent on our ability to grasp the genuine challenges that users confront and to obtain a thorough knowledge of the persons navigating the complex environment of online payment systems.

The process of creating an empathy map helps all project contributors to adopt a viewpoint that is consistent with the user's experiences. It pushes us to see things through the user's eyes, effectively stepping into their shoes and understanding their goals, as well as the barriers they face on their trip through the world of online payments. This allows us to have a deeper insight of their requirements, anxieties, motivations, and pain areas.

Empathy Map Link

https://app.mural.co/t/project7000/m/project7000/1697616774598/c2c783ad1c848c3d28bcba53dd5b923124aaeb53?sender=96985ce8-9f51-48d3-9d9d-6ee51eee3f95

Online Payments Fraud Detection Using ML

In today's digital age, the expansion of the internet and e-commerce provides unparalleled ease and potential. This digital economy is driven by online credit/debit card transactions, but its development has also fostered online payment fraud. As card acceptance rises, so does fraud frequency, revealing the limits of old detection approaches. Our project understands the need of proactive, adaptive fraud detection. Transactional deviations may indicate fraud, and our solution, backed by powerful Machine Learning algorithms, revolutionises detection accuracy. We prioritise end-user and corporate issues by incorporating security into the online transaction experience. Our goal is to protect and strengthen confidence in the digital payment ecosystem.

Originally created by Dave Gray at

XPLANE®

Share template feedback

Empathy Map for "Online Payment Fraud Detection Using ML"

This empathy map is designed for our project, "Online Payment Fraud Detection Using ML," which employs Machine Learning Algorithms to identify and prevent fraudulent activities within online payment systems. It provides insight into the key elements of the project by addressing the fundamental 5 W's: who, what, where, when, and why.

WHO are we empathizing with?

Who is the person we want to understand?
What is the situation they are in?
What is their role in the situation?

Customers: They want their payments to be processed quickly and securely. Understanding and addressing customer concerns is essential to maintain their trust.

Merchants: Merchants are concerned about chargebacks and the potential impact on their revenue.

Regulators and Compliance Agencies: Regulations and standards in place to protect customers and businesses. Understanding and complying with these regulations is vital.

Fraudsters: These individuals or groups aim to make unauthorized payments, and their actions need to be identified and stopped.

Machine Learning Engineers and Data Scientists: Responsible for developing the ML algorithms and models. They need a deep understanding of the domain, data, and the nuances of fraud detection.

Data Analysts and Security Teams: They need to understand the technical aspects of how ML can be used to identify fraudulent transactions.

GOAL

What do they need to DO?

What do they need to do differently?
What job(s) do they want or need to get done?
What decision(s) do they need to make?
How will we know they were successful?

Check for SSL Certificates: Before making online payments, check the address bar for "https://" and a padlock symbol to ensure that the website has a valid SSL certificate. Avoid visiting unencrypted websites.

Examine App rights: Review the rights provided to mobile applications on a regular basis and limit their access to personal information to the bare minimum.

Enable Transaction Notifications: To receive real-time alerts for any suspicious activity, enable transaction notifications on your bank and credit card accounts.

Be Aware of Unsolicited reward Offers: Be wary of unsolicited reward offers or emails saying you've won a contest. Check the credibility of such offerings.

Apply Credit Freezes: To prevent unauthorised access, consider establishing a credit freeze on your credit reports.

Use Virtual Credit Cards: For online purchases, use virtual credit card numbers wherever feasible. By separating your actual card data from internet merchants, these throwaway numbers give an added degree of security.

No Unauthorised Access: There has been no unauthorised access to sensitive accounts or personal information, suggesting that efficient security measures are protecting online accounts.

Positive Security Tool Feedback: Positive security tool and system feedback demonstrating effective deployment of security practises and defences.

Stronger legislative Protections: Successful lobbying and implementation of legislative safeguards against online payment fraud, resulting in increased accountability for cybercriminals.

Best Practices:
Users read blogs and articles highlighting best practices for online payment security. They learn about the significance of strong passwords, two-factor authentication, and safe browsing habits.

Transaction History:
Users may review their transaction history to monitor their financial activities and ensure all transactions are legitimate.
This behavior can intensify if they've experienced fraud or false positives in the past.

What do they HEAR?

What are they hearing others say?
What are they hearing from friends?
What are they hearing from colleagues?
What are they hearing second-hand?

Experts and industry professionals: Those in the field of online payments fraud detection would stay updated with the latest industry trends, best practices, and emerging technologies related to ML and fraud detection.

Industry news and reports: Staying informed about recent fraud trends, data breaches, and case studies is crucial. Professionals in this area would follow news and reports related to fraud detection and prevention

Colleagues: Colleagues working in the same field might share knowledge, exchange information about new tools or techniques, and discuss common challenges they face in online payments fraud detection.

Friends: Professionals often discuss their work with friends, and they might share interesting or challenging experiences related to online payments fraud detection.

Regulatory Changes: They hear about changes in regulations and compliance requirements related to online payments and data security from industry associations, government agencies, and legal experts.

Market Analysis: Market analyses and insights on the growth of ecommerce, mobile payments, and digital wallets that impact the online payment landscape

What do they THINK and FEEL?

PAINS

What are their fears, frustrations, and anxieties?

Financial Loss: One of the primary fears associated with online payment fraud is the fear of financial loss.

Trust Issues: Fear of losing trust in online payment systems or service providers is common.

Inconvenience: Dealing with online payment fraud can be incredibly frustrating due to the inconvenience it causes.

Customer Support Challenges: Frustration can arise when individuals encounter challenges in reaching out to customer support or getting timely assistance from their bank or payment service provider.

Uncertainty: Anxiety often stems from the uncertainty of whether one's personal and financial information is secure. The constant threat of online payment fraud can create a pervasive feeling of unease.

Future Vulnerability: Anxiety may also manifest as concerns about future vulnerability.

GAINS

What are their wants, needs, hopes, and dreams?

Security: They expect their financial and personal information to be protected from unauthorized access and fraudulent activities.

Privacy: Users desire privacy in their online financial transactions. Resolution and Redress: Victims of fraud want a quick and effective resolution to their problems.

Education and Awareness: People need education and awareness about the various forms of online payment fraud, how to recognize scams, and how to protect themselves.

Support and Assistance: Victims need support from financial institutions, law enforcement, and relevant agencies to help them navigate the aftermath of fraud.

Seamless, Secure Transactions: The dream is to have a digital world where online payment transactions are not only secure but also convenient and seamless.

A Safer Digital World: The ultimate dream is to create a safer digital environment where the dreams and aspirations of legitimate users are protected from the malicious intentions of fraudsters. This includes a world where cybercriminals are held accountable for their actions and where fraud prevention and detection measures are highly effective.

Online Payments Platforms:
Users encounter a wide range of online payment platforms, each offering different features and levels of security.

What do they SEE?

What do they see in the marketplace?
What do they see in their immediate environment?
What do they see others saying and doing?
What are they watching and reading?

Concerns :
Users express their concerns about the security of online payments, especially when it comes to sharing sensitive financial information.
They may say things like, "I worry about my credit card data being stolen during online transactions" or "Is this platform really secure?"

What do they SAY?

What have we heard them say?
What can we magine them saying?

Frustrations :
Users have often voiced their frustrations about false positives and the inconvenience of legitimate transactions getting blocked.
They say things like, "I hate it when my bank blocks my card for no reason" or "It's so annoying when a legitimate purchase gets flagged as fraud."

Expectations :
Users likely express their expectations for a more secure and seamless online payment experience.
They may say things like, "I hope this system can accurately detect fraudulent transactions" or "I expect a hassle-free and secure payment process."

What other thoughts and feelings might influence their behavior?

Mental illness: In some cases, online payment fraud may be committed by people with mental health problems, such as schizophrenia or bipolar disorder. These individuals may have difficulty distinguishing between right and wrong, or they may have delusions that justify their behavior.

Desire for financial gain: Greed and the desire for easy money are powerful motivators for many fraudsters. They may see online payment fraud as a low-risk opportunity to make a quick profit.

Revenge or spite: Some people may commit online payment fraud as a way to get back at a company or individual they feel has wronged them. For example, they may hack into an ex-partner's online account and make fraudulent purchases.

Boredom or excitement: For some people, online payment fraud may be a way to get a thrill or to relieve boredom. They may enjoy the challenge of outsmarting security systems and getting away with stealing money.

What do they DO?

What do they do today?
What behavior have we observed?
What can we imagine them doing?

Use Strong and Unique Passwords: They create complicated passwords for online accounts and avoid using readily guessable payment information.

Enable Multi-Factor Authentication: To provide an extra degree of protection to their accounts, they enable Multi-Factor Authentication whenever possible.

Regularly Monitor Accounts and Set Account Alerts: They monitor their bank and credit card accounts for unauthorised transactions on a regular basis and set up account alerts to warn them of any strange activity or big transactions.

Shop from trustworthy Merchants: They buy from trustworthy and established internet stores.

Increased Email Caution: Many users have become more wary of unwanted emails and are less inclined to click on links or download attachments.

Limited Use of Public Wi-Fi for Sensitive Transactions: People are avoiding utilising public Wi-Fi networks for critical transactions and financial operations.

Prompt Reporting of Suspect Behaviour: There is an increasing readiness to report any suspect internet behaviour to appropriate authorities and financial institutions as soon as possible.

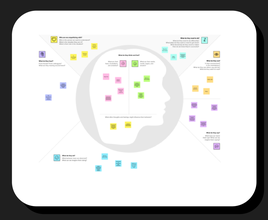
Scam Awareness: Many consumers are now aware of popular internet scams and fraud strategies, making them less likely to fall for such schemes.

Biometric Authentication Advances: Increased use of biometric authentication technologies for secure payment and account access, such as facial recognition and retinal scans.

Secure Communication Channels: Use of end-to-end encryption and secure communication channels for the exchange of sensitive payment information.

Increased Cybersecurity Education: Continued investment in cybersecurity education to ensure that individuals are up to date on the newest risks and protection methods.

Compliance and Evolving legislation: Adherence to evolving legislation and compliance standards aimed at improving the security of online payment systems.



Need some inspiration?

See a finished version of this template to kickstart your work.

Open example