

Study On Fraud By Fake Advertisement By Ads Engines On Their Social Media Platform

Awanish Kumar¹ *, Dr. Shalini Srivastav², Dr. Santosh Kumar³

¹Management, Amity University, UP, India

²Management, Amity University, UP, India

³Marketing & Analytics, Sharda University, Greater Noida

awanish.kumar@s.amity.edu, ssrivastav@gn.amity.edu, santosh.kumar6@sharda.ac.in

* Corresponding Author

How to cite this article: Awanish Kumar , Shalini Srivastav, Santosh Kumar (2024) Study On Fraud By Fake Advertisement By Ads Engines On Their Social Media Platform. *Library Progress International*, 44(3), 22110-22123.

ABSTRACT

Over time, social media have become a big platform of advertisement for new products and services. A very intelligent “Ads Engine” works in background to give ads on social media based on user’s recent history or interest. Fake e-commerce portal is not new but when the fake ads comes via Ads engine on reputed social media, it has big impact [1]. Any advertisement on big tech platform is considered authentic by users. There is surge in fraudulent activities by giving fake advertisement on social media and targeting approx. 450 million people in India [2]. The big platform companies have not developed proper mechanism to validate ads [3] and there is no accountability. Approx. 30% Indian are using social media every day, multiple fraudulent online portals came-up offering trendy products at huge discount. In few days, there will be no trace of these fake e-commerce portal.

Keywords: ads on social media, fake ads by ads engine, fake ads by ads manager, no delivery of products, fake e-commerce.

1. Introduction

Now a days, for any type of advertisement, social media platforms have become first choice. Online platform like Facebook, YouTube, Google search etc are very popular in India. Whenever you open your smart phone, these advertisements will come in some way. People easily believe these website as they come as an advertisement on big social media platform. The reach of social media is very large and cover all section of societies approx. 30% [2]. The advertisement cost is very less compared to main stream media. The fake portal offers very common items like cloths, electronic items, bicycle etc. Customers ended up paying partially or full in advance but never gets delivery.

Fake e-commerce portal is not new, but has increased in recent time, particularly after covid-19. The Covid-19 has forced people to go online both in urban and rural areas. Big E-commerce giant like Amazon, FlipKart, Blinkit, PayTm, IRCTC etc. have created an environment in India for online shopping and also created faith in people’s mind that online shopping is easy and reliable way to buy and sell products. India has 450+ millions smartphone users by the end of year 2022, in other words 40% users have smart phones [4]. There are more than 19,000+ e-commerce companies in India.

India is going through a “Startup age”, every day we see or hear new startup news. In e-commerce space, it’s very common that you see some advertisement of new e-commerce portal in social media. Google ads and Facebook ads Manager are leaders in market for advertisement and using these by fraudsters to spread fake advertisement has high chances that people will response. Fake online portals are mushrooming and new way of frauds are being invented to cheat people sometime by delivering either fake product or not delivering product at all.

1.1 Example of a fake online shopping portal recommended by ads engine:

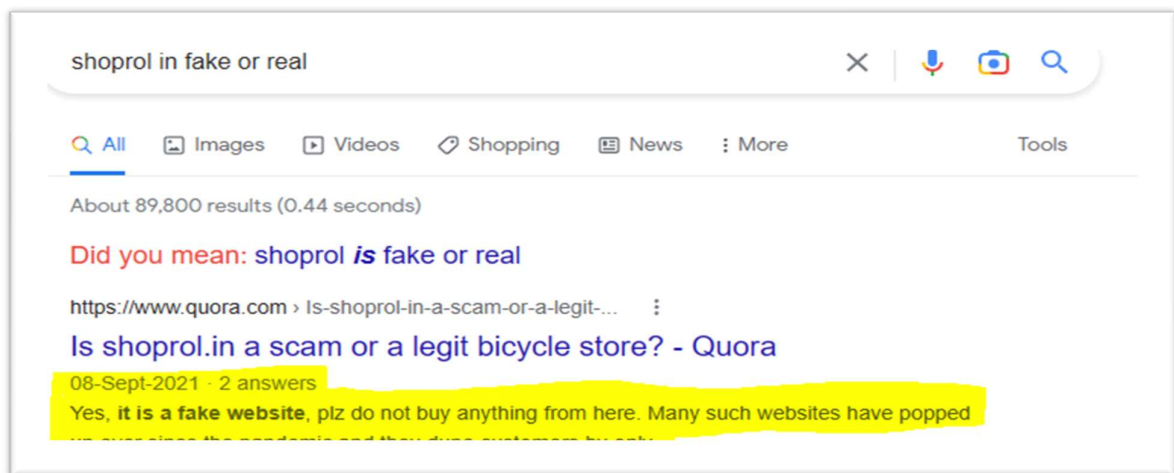
The Google ads gave advertisement on YouTube App. The one of the examples of fake portal that I have seen on *YouTube is Shoprol.in*. This fake e-commerce portal was selling bicycles of high quality at heavy discount. During Covid-19, it was only offering pre-payment mode and after sometime this portal got disappeared. For detail of this website and screen shot, see Annexure – 1.

1.2 Scope of study:

For this study, researcher have considered YouTube and Facebook ads managers. These are most used social media platform in India.

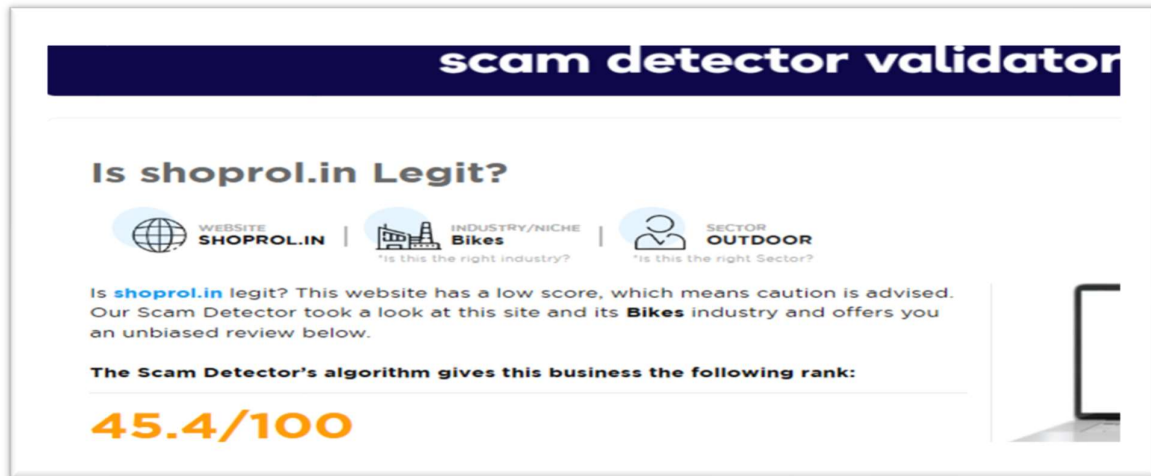
1.3 Fraud e-commerce experience

- a) Current status of SHOPOROL as per google

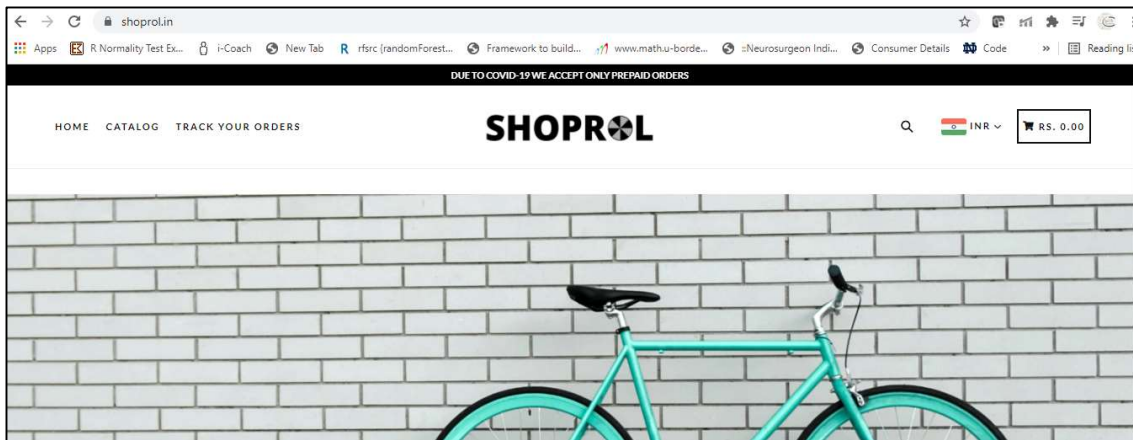


Picture-1: Fake website portal snapshot

- b) Few websites offer fake website score “Scam detector validator”. It gives safe score to a website and which helps to detect where a given website is suspicious. Lower score means suspicious.



Picture-2: Fake website scam score



Picture-3: Fake website homepage snapshot Shoprol.in

2 Fraud experience:

One fraud incident happened with people in Noida city: During Covid-19 lock down, most of people started "work from home". Since people were not travelling and road was very empty, people started buying Bicycle. I searched bicycle in google to get idea of price and variety. I started getting ads on YouTube for new portal which is selling bicycle. The bicycle was available on heavy discount. But there is one condition, "DUE TO COVID-19 ACCEPT ONLY PREPAID ORDERS". I paid rupee 1000/- and message came that it will be delivered in next 15 days. But it never got delivered and after a month time, there is no trace of this website.

1. 2. Background:

Now E-commerce or online shopping has reached to the remotest part of country. The expansion of 4G mobile network (5G in progress) with fast internet throughout the country have played a major role in expansion of smart phones. Online shopping apps have made shopping very convenient and accessible to large people. Below are the factors which has helped e-commerce expansion in India.

Government policy: Government of India policy like 100% FDI is allowed in B2B e-commerce. 100% FDI user automatic route is permitted in marketplace of model of e-commerce.

Smart Phones & internet: Now approx. 800 plus millions of customers have smart phone which have become potential customers of online shopping.

Online shopping mobile App: The shopping apps available in smart phone changed the entire dynamics of online shopping. These apps are so user friendly that even a new user who is not very tech can also use it. Apps are available in all the Indian languages.

Trust in Online shopping: The pioneer companies like Amazon and FlipKart have established trust in customer mind for online shopping. This has opened a new door to new players in market. The delivery network is now PAN (Presence Across Nation) India. So even in rural part of country can do online shopping.

Digital Payment in India: Payment was one of the major bottlenecks. Digital payment is new way of banking in country. Most households have bank accounts, which is very easy to link for mobile and online payment. Digital payment played a big role in e-commerce acceptance by people.

Wide product offering online: For daily use purpose, almost all products and services are available online. You name it and you will get some online portal which is offering these product or services. Few product categories are like electronics, garments, groceries, books, plants, haircut, electric items services and finally online classes.

2.1 Aggregator vs individual online portal:

The big e-commerce company like Amazon and FlipKart play a role of aggregator, which means their state-of-the-art portal allow any seller to register and sell their products, any buyer to register and buy products.

Similarly, for buyer it becomes a one stop shop to buy any product. Aggregator also provides complete delivery network of product from seller to buyer like logistic support, where-house, home delivery, billing and taxation. To provide these services, aggregator charge some percentage of revenue. [5]

Individual online portal: any individual business entity creates their own web page or app to facilitate customers the online shopping directly from his store. The seller has to manage delivery of products. Individual sellers generally provide services limited to few places.

Each has their positive and negative points, but both co-exist in every market place. This research paper is focused on two prominent players: Google Ads and Facebook Ads Manager.

“Google Ads is an online advertising platform developed by Google, where advertisers bid to display brief advertisements, service offerings, product listings, or videos to web users. It can place ads both in the results of search engines like Google Search and on non-search websites, mobile apps, and videos.” [Wikipedia](#)

“Ads Manager is your starting point for running ads on Facebook, Instagram, Messenger or Audience Network. It's an all-in-one tool for creating ads, managing when and where they'll run, and tracking how well your campaigns are performing towards your marketing goals.

With the Ads Manager app for iOS and Android, you can keep an eye on your campaign while you're on the go. Wherever you are, you'll have the power to create and edit ads, track their performance and manage ad budgets and schedules.” [6]

General opinion is that Google and Facebook (now Meta) must have verified the vendors before allowing advertisement on their platform. Another understanding is, since it is paid advertisement so only serious sellers will be giving product promotion. So, advertisements are believed authentic by people. [“Meta website”](#)

Here come fraudsters, in name of offering some very common things searched by many people with heavy discount.

2.2 How does Ads manager work?

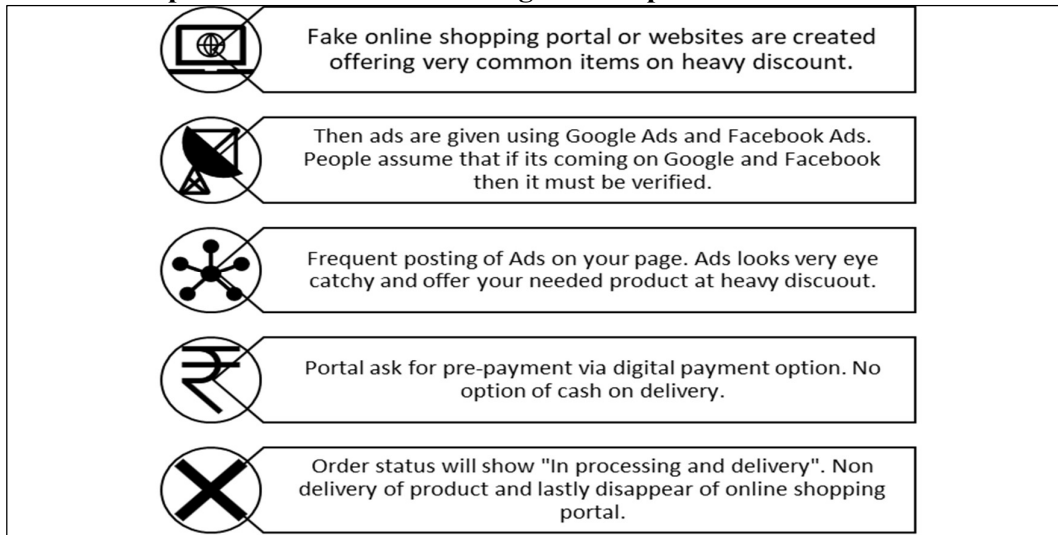
When any user register to Google or Facebook, he or she automatically gives consent to these companies to send advertisement using their Ads engine. Ads engine keeps tracking

your behavior to know your area of interest, your current requirement and then place matching advertisement when you are using their services.

A recommendation engine is working in background which keep tracking your recent activities and recommend you matching ads. The social media offer free services to all users, but in reality, they earn money by giving ads whenever a user access their services. The ads annual revenue aggregate to billion \$.

* recommendation engine – Recommendation engine is a machine learning based system which find similarity between users and items. Then recommend the similar items to similar users.

2.3 Modus Operandi of fraudsters to target smart phone users



Picture-4: shows the modus operandi followed by fraudster in cheating money by fake ecommerce portal.

**Ads engine means Google ads, Facebook ads manager or other similar product.

2.4 How does people reach to fake online shopping portal?

On smart phone, when you search for any keywords, the smart phone stores your browsing activities in cookies. Similarly, when you click on any ads, then your smart stores details. Ads engine start giving advertisement matching your previous search activities. Going forward, whenever you open your phone, you will observe that more and more content similar to your previous likes will start coming on your social media page. Sometime one to one message or even call on your phone will come.

Similarly, users give rating of items which they have used like rating on scale of 1 to 5 for LED TV you purchased, rating of Movie, rating of web series, rating of book you read etc. Ads engine powered by machine learning (ML) recommendation system, run algorithm and recommend similar users' similar advertisements.

Fraudsters use the same ads engine to give advertisement of fake products or portals. Fraudsters watch which items are getting more views and likes. Then they will create fake portal offering similar items and start giving ads on Google and Facebook. But in reality, these are fake and their intension is to run away with money. Even they manage with fake rating of their portal. It is happening on daily basis and people gets cheated.

Big tech companies like Google and Facebook (now Meta) have trust of people. Any advertisement pushed by Ads engine are easily believed by users. Contents on social media are created by people so you may or may not belief it but ads are shown by Ads engine of Google and Facebook. So, it has high chances that people believe on these. After few days, you will not see this advertisement and if you try to open their website, it will not open.

Another pull factor is heavy discount, which can range up to 90%. It attracts people to go and see the products, and sometime they login and order product on these fake portals. Seeing the very low price, people take chance to order on these portals. The amount involve in most of cases is between one to two thousand and people are not really bothered about this. Few people order product as a trail.

2.5 What is offered?

The fraudsters are very smart and they offer common durable items. They can offer any items which is in trend or fashion and people are enquiring about that.

- Crypto currencies.
- Bi-Cycle for adult and kids
- Readymade cloths like Jacket, trousers
- Shoes and other appeal items.
- electronic items
- cosmetic products
- office chairs etc

Now a days, when a person thinks of purchasing any items, they search it on laptop or mobile to know about product features, product price, discount offers and many more. Based on your search history, ads engine starts placing similar product advertisement in your phone during surfing. Seeing required product advertisement along with heavy discount, people tends to click and check the detail. These fake portals ask for advance payment but no option of cash on delivery.

Some people get doubt that it's not possible to have this price but they go for it as it's just the matter of one or two thousand rupee. Only few people file any formal complaint.

2.6 Why people buy product on these new e-commerce websites?

- New e-commerce portal is a normal thing.
- Offer better deals and heavy discount on product.
- Attractive advertisement.
- Customer requirement.
- Small amount involved.
- Home delivery

2.7 Non-payment non-delivery fraud

As e-commerce is growing in India, so is online fraud. One of the most common fraud is non-delivery fraud. Everyday some new online portal comes with new offering, in which most are genuine but some are fraud. They look very similar to any other normal online website, but they have intension of cheating people and getting disappeared.

2.2.8 Online purchase fraud

It is defined as in online purchase where scammers use online technology to offer attractive deals, take the payment before delivering products and no product or service is delivered. There are 3 different way this fraud is being done:

- a. Creating of identical website of any big brand.
- b. Creating new online website to take payment and not delivering product.
- c. Online website delivering fake product.

3. 2.9 Learning for future:

The fraudsters are always one step ahead. This type of fraud is going to stay in future also. Below is the list of learning to minimize the fraud.

- Be watchful, don't carry away by seeing heavy discount.

- Keep in mind the modus operandi of fake online portal.
- Check the authenticity of new website online.
- Must report complain to portal and other authority, so that other can be saved.
- Big Technology companies like Google, Facebook etc have play vigilant role in future while placing ads on their platform.
- Pro-active approach by cyber cell and bank to deal this time of fraud.
- Post any fraudulent transaction, bank can pro-actively create similar identical Virtual IDs and apply check these ids. If any transaction and these IDs in Debit of Credit detail then deny the transaction and raise an alert to customer.

4. 2.10 Does it look suspicious seeing the price of product?

The answer is yes. These are multiple points which raise doubts:

- a) Let say bicycle, which price start at approx. 7000 /- is available at 1000/-. This is unbelievable. It raises a very pertinent question as how could a product be sold at this price?
- b) This online portal is new and not known to anyone including your friends and family.
- c) Asking 100% payment before delivery stating the reason of Covid-19. No option of cash on delivery.
- d) Free shipping in addition to such an unbelievable low-price all-over India.
- e) Asking complete detail while making payment, not getting any acknowledgement on either mobile and mail.
- f) No change in delivery status of product even after a week time.

2.11 Beneficiary of this fraud:

- Direct: Fraudsters who create the fake advertisement and fake business to cheat the people. These fraudsters are direct beneficiary of this fraud.
- In-direct: Platform owner companies which allow this advertisement on social media page of different users without doing proper due diligence. At the end of the day, they are making money from ads but a normal user is losing money.

5. 3. Literature review:

In literature, *"Fake ads; real problems: how easy is it to post scam adverts on Facebook and Google?"*, the author says that its really easy to put fake ads and information on Google and Facebook which could misled into buying something doubtful or unsafe product, and can become a victim to a financial scam. Author says that Facebook or Google don't have a stringent vetting process and barely any checking. The author launched a fake brand of bottled water and successfully placed in Ads using Facebook and Google [3]. It did not check whether there is any proof that our business actually existed and within an hour for our fake advertisement applications got approved by Google. Same with Facebook ads. These big company are driven by ad money nothing else. The platform providers should be putting more resources into preventing fraudsters from abusing their platforms. The law should be made to set responsibility of fake ads and content on these platforms and they should compensate the users.

Another literature *"What you need to know about fraudulent ads on Facebook and Google"*, the report state that fraudulent advertisement increasing at alarming rate and Google alone has blocked at least 3.1 billion of them to date [1]. "A study from the U.K. consumer group Which? found that a substantial number of the fraudulent ads reported to Google (34%) and Facebook (26%) were not removed.". The inaction of platforms to control fake ads and users' casual approach to not report complain after fraud has made this a serious problem. The

author suggests platform providers need to have more proactive approach.

The fraudulent ads have one common characteristic of delivering inferior products if they get anything at all [1]. Second form of scam of false ads, promote some super trendy thing like cryptocurrency with false information. The article is saying that tech-platform is taking few steps like, filing legal case in court against fraudsters, tightening of rules and regulation.

In literature, *"FAKE SHOPPING WEBSITE FRAUDS"*, it highlights how the fraudster creates a very matching website like the original website of known brand like Mi. The article on Delhi Cyber Cell [7] educate people with four different type of fake online shopping. 1) Fraudster create very identical website of known brands like mobile brand I-Phone, MI etc. Customer fail to realise the fake website and make payment. Product never get delivered and they lose money. 2) Fraudster create online shopping website/portal/mobile app and offer huge discount. Customer make buy product because of discount, make payment and product never get delivered. 3) In this way, when a customer buys expensive product, a gift is offered before actual delivery of product. Later on, in name of processing charge, handling charge and GST, fraudster ask to pay some money, which latter on turn to be fake. 4) The fourth way is the, fake website delivers fake or duplicate product / refurbished product and never return the money. The Cyber-crime also suggest ways save from these websites. [7]

In literature, "Interpol has warning and tips on non-delivery scams", Interpol is alerting people of non-delivery fraud. Here shopping portal take the payment of product but never deliver these to the customers. The cases are increasing and also involve cross boarder product delivery [8]. These fraudsters are very well planned and offer wide range of products. They also take use of social media to divert people to these fake websites. Fraudster are very expert, the website, contact and other detail looks very genuine. Interpol suggest customers to be causes and look for website name carefully, read review and be more caution if payment is going abroad [8].

In literature, "5 reasons non-delivery scams work", the Interpol website suggest modus operandi of new type of fraud where an online shopping party take money and never deliver the money. Interpol suggested that is very sophisticated modus operandi and involve multiple parties like "sophisticated modus operandi involving websites, salespeople, intermediaries and of course, bank accounts" [9].

In literature, *"Caught in online money scam? Cybercrime expert tells you what to do next"*, Internet has become a place of crime and fraud and its increasing day by day. This article talked about OLX scam, which is a platform for second hand product buy and sell. The fraudsters pretend to be either buyer or seller and present themselves has defence personal. [10] They start the conversation and when payment time come, they take the money and run away. Sometime they play a trick by sending receive money request instead of paying money. Sometime they repeat the same trick twice to same customer saying this is to revert the money they taken at first place. [10]

The article *"Online purchase fraud"*, define the online purchase fraud where payment is received and product never delivered [11]. This also suggest different reason how fraudsters target customers. The author suggest that low price is the main reason why people become pray to fraudsters and lose money [11]. The article also suggesting ways to avoid these types of fraud. But it does not suggest if portal is new and not getting users comments. What if fake online link is coming in google ad and YouTube advertisement.

In literature, *"Consumers alert! Fake ecommerce websites con shoppers amid festive season boom"*, highlights fake ecommerce website mostly in festival time to cheat people. This article highlights the that link of fake websites comes on social media Facebook [12]. This gives an impression that social media company must have verified this. The article states an example of "wellbuymaill.com" where many people lost their money [12]. After taking payment, this Chinese does not deliver product and URL become inaccessible. It is more

common in Indian festival time.

In literature, “*PREVENTIVE MEASURE FOR PREPAYMENT & NON-DELIVERY FRAUD ON ONLINE SHOPPING PAGES PUBLISHED IN THE SOCIAL MEDIA ACCOUNT*”, it states that biggest fraud in online shopping is Non-delivery in which seller takes payment in advance but never deliver the product [13]. The seller gives fake transaction id and later on, block customer number. As per report 23% complains are of non – delivery of product in year 2018. The author proposed they own third party payment solution which will keep the payment till the time product is delivered. But problem how and who will regulate this new third-party app. Till this time nothing like this has come in market. There is absence of regulator.

4. Scope of study

- Fraud using fake advertisement on Google ads and Facebook ads manager etc
- Fake e-commerce online shopping portal.
- Use of trusted social media platform to advertise fake portals and spread dubious link.
- Focused on two prominent players: Google Ads and Facebook Ads Manager.
- Limited to fake ads, no study on fraud happening because of spyware, trojan horse.

5. Objective of study

- To study the extent of fraud, people have experience using fake advertisement via Google ads, Facebook Ads Manager etc.
- To understand the non-payment non-delivery fraud across India (urban and rural India).
- Fraud pattern by fake advertisement within educated and un-educated.
- Fraud using non-delivering product or delivering fake product.
- Study on loss because of fake ads on social media.
- Study on complain filled on tech portal and to police.

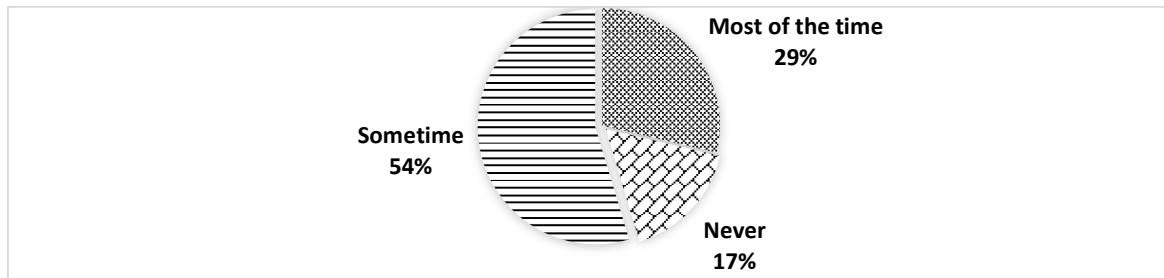
6. Research Methodology

The study is aimed to know how fake products or e-com portal advertisement on social media is used to cheat people. This research has used primary data from approx. 108 respondents to evaluate in NCR region of Delhi. Sample data are collected with structured questionnaire and schedule. These questionnaires are sent to random people to know their feedback to people who are using social media and have experienced fake ads on YouTube or Facebook.

6.7. Data Analysis and Findings

- Responded number – 108
- Statistic Tool – Python
- Data Collection – Questionnaires, Schedule

Finding-1: 4 out of 5 people have noticed *fake advertisement* which is more than 80% at some point of time. Secondly, approx. 1/3 of people have experienced *frequent fake advertisement* on social media. Picture 5 shows the percentage of social media users noticed fake advertisement on social media platforms.



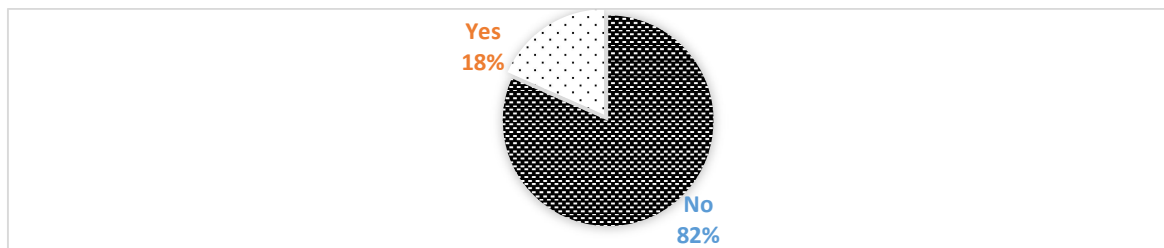
Picture-5 percentage of social media users noticed fake advertisement

Finding-2: Approx. one fifth of the people has purchased from fake advertisement link, sometime as a trial. This is really high number because even if a fraction of them loose money, the actual loss amount will be very big. Below Table-1, show percentage of people did not used fake e-com portal = 73% approx. and approx. 25% people have used fake e-com someway.

Table-1

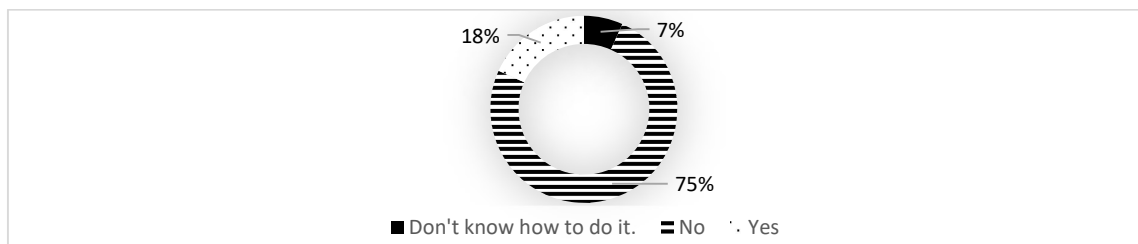
Users used fake e-com website	Percentage of people
Yes, as trail	27 %
No	73%

Finding-3: Approx. 18%, means 1 in 5 people have lost money because of purchased from fake advertisement. This a really high percentage, as India have 800 Million social media uses. Most the uses have used it as trail considering the low amount involved. In majority of cases the fraud amount is less than 2k. Picture -6, the pie chart shows the percentage people lost money because of fake e-com ads.



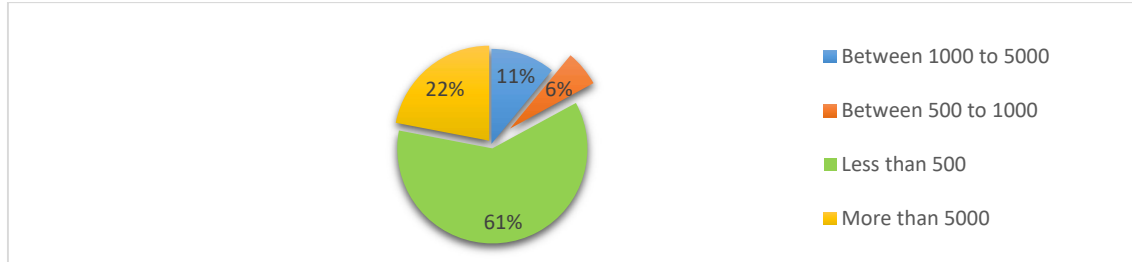
Picture-6 percentage people lost money because of fake e-com ads

Finding-4: Users are more comfortable in filling complain to Social media platform Google and Facebook. Approx. 18% users have filled complains to platform they use. At the same time, more than half of the users, 75%, don't know how to report complain. This may be because majority of users are not very educated. Picture-7, shows percentage people who has filled complained on social media portal from where they show ads.



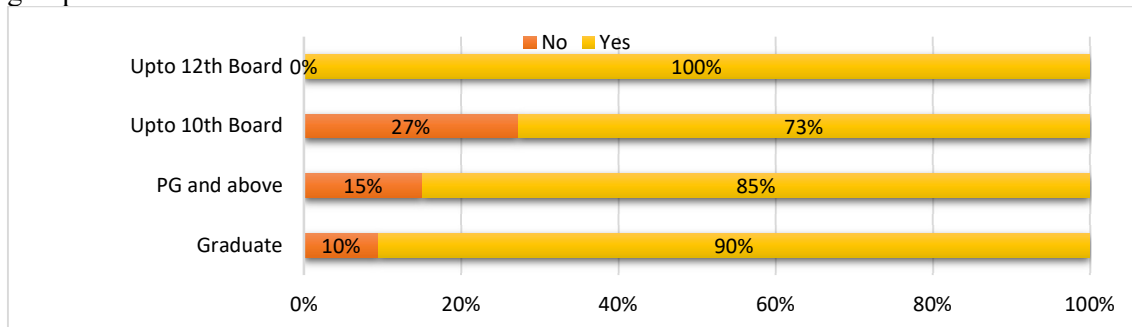
Picture-7 percentage people who has filled complained

Finding-5: It is a surprising fact that no users filled complain to cyber police. This could be because in more than 67% cases the fraud amount is less than Rs 1000/-. The other surprising finding is that even educated users have not filled police complain or even when loss amount is more than 5000/-. Picture-8 is pie chart of actual amount lost in fraud. Four buckets are created, the chart show what is the % people falling in each bucket.



Picture-8 chart of actual amount lost in fraud by customer

Finding-6: Is there any relationship between education level of users and awareness? Education level has direct relation with awareness of advertisement given by Google ads and Facebook ads on social media. Higher educated users are more informed about advertisement on social media. Picture-9 shows the Sack chart of awareness of ads in different education group.



Picture-9 awareness of ads

Null Hypothesis (H0) = There is no relationship between user education and awareness about fake advertisement.

Chi-Square p value is 0.439, it means null hypothesis is rejected and it means education level of users have impact on awareness about advertisement being push to platform. It can be said that educated people are more aware of ads being pushed on social media like Google and Facebook.

Table-2: Shows the awareness of sponsored ads on social media among different education group.

Education level	Awareness of advertisement pushed by Google ads and Facebook ads?	
	No	Yes
Graduate	4	38
PG and above	8	45
Up to 10th Board	3	8
Up to 12th Board	0	2

Finding 7: Higher educated users more aware and able to notice fake advertisement on Google or Facebook? Table-3, sample distribution of awareness of fake ads in different education

group.

H₀ = There is no relationship between user education and have you noticed any fake advertisement on Google or Facebook?

Table-3

	Have you noticed any fake advertisement on Google or Facebook?		
Row Labels	Most of the time	Never	Sometime
Graduate	12	9	21
PG and above	18	4	31
Up to 10th Board	0	5	6
Up to 12th Board	1	0	1

Null Hypothesis (H₀) = There is no relationship between User education and Have you noticed any fake advertisement on Google or Facebook?

Chi-Square p value is 0.04, it means no evidence against null hypothesis, so null hypothesis gets accepted. That means education level of users have no impact on capability of users to identify fake ads on Google and Facebook. All section of users is equally vulnerable.

Finding 8: Higher educated users are less vulnerable in losing money in fraud done via fake ads on social media. Table-4, shows loss of money in fraud in different education group social media users.

Table-4

	Did you lose money?	
Row Labels	No	Yes
Graduate	28	4
PG and above	27	9
Up to 10th Board	6	0
Up to 12th Board	1	1

Null Hypothesis (H₀) = There is no relationship between user education and users losing money on fake ads on social media.

Chi-Square p value is 0.215, it means Null hypothesis (H₀) holds true (rejected H₀) and means education level of users have impact on losing money in fake ads on social media. It means educated people are more aware of fake ads less chances of losing money on social media like Google and Facebook. But here it looks like educated people have used these ads as trial and lost money.

7. 8. Conclusion & Suggestion:

Fake advertisement on social platforms are not new and it has been raised by multiple users and researchers time to time. But still fake ads are very common things visible on social media. In India, smart phone user base has touched 800 million and all pockets of country has fast and cheap internet availability. People from all section of societies are using smart phone and social media apps. Majority of users are not tech savvy and not very educated. People from rural part are less aware of these things and become easy target of these fraud. In urban area, people are going on these ads as a trial with less than one thousand rupee. In any way, users are losing money.

8. 9. Recommendation

1. Tech companies who own these platforms should be made accountable to fake ads coming on their portal.

2. The tech giant platform owners have biggest responsibility to do the proper due diligence of any new ads request. It should be thoroughly verified by physical visit and document submission before putting ads on platform.
3. Users should be aware of these fake ads. Don't fall pray of heavy discount advertisement of product on social media.
4. Users must file complain to platform and also to cyber security. So that more people came to know about this and these can be minimised.
5. The tech giant platform compensates the loss if happens to users because of fake ads.
6. The tech giant platform owner should follow the best practice present all over the world.

9.10. Declarations

Conflicts of interest statements:

Awanish Kumar, the corresponding author declare that I have no relevant financial or non-financial interests to disclose.

Data Availability Statement:

The data that support the findings of this study are available from the corresponding author, Awanish Kumar, upon reasonable request.

10. References

- [1] T. Bunker, "What you need to know about fraudulent ads on Facebook and Google," July 2021. [Online]. Available: <https://www.theladders.com/press>.
- [2] "DIGITAL 2023: INDIA," Feb 2023. [Online]. Available: <https://datareportal.com/reports/digital-2023-india>.
- [3] A. Laughlin, "Fake ads; real problems: how easy is it to post scam adverts on Facebook and Google?," *www.which.co.uk*, July 2020.
- [4] "India to have 1 billion smartphone users by 2026: Deloitte report," 02 2022. [Online]. Available: https://www.business-standard.com/article/current-affairs/india-to-have-1-billion-smartphone-users-by-2026-deloitte-report-122022200996_1.html#:~:text=India%20had%201.2%20billion%20mobile,in%20the%20next%20five%20years..
- [5] O. Demidenko, "ECOMMERCE AGGREGATOR: WHAT IS IT AND HOW TO DEVELOP IT?," [Online]. Available: <https://geomotiv.com/blog/how-to-develop-ecommerce-aggregators/>.
- [6] "Facebook ads," [Online]. Available: <https://www.facebook.com/business/tools/ads-manager/>.
- [7] C. c. D. Police, "Cyber crime Delhi Police," [Online].
- [8] TIMESOFINDIA.COM, "Interpol has warning and tips on non-delivery scams," [Online]. Available: TIMESOFINDIA.COM.

- [9] "5 reasons non-delivery scams work," [Online]. Available: <https://www.interpol.int/en/News-and-Events/News/2020/5-reasons-non-delivery-scams-work>.
- [10 I. T. T. Desk, "Caught in online money scam? Cybercrime expert tells you what to do next,"
] [Online]. Available: <https://www.indiatvnews.com/technology/news-caught-in-online-money-scam-cybercrime-expert-tells-you-what-to-do-next-679882>.
- [11 L. eFraud Prevention™, "Online purchase fraud," [Online]. Available:
] <https://efraudprevention.net/home/templates/?a=174>.
- [12 "Consumers alert! Fake ecommerce websites con shoppers amid festive season boom," 06 10
] 2021. [Online]. Available: <https://www.deccanherald.com/national/rahul-gandhi-en-route-lakhimpur-after-brief-row-at-lucknow-airport-1037906.html>.
- [13 A. M. M. K. Dr. Manish Kumar, "PREVENTIVE MEASURE FOR PREPAYMENT & NON-DELIVERY
] FRAUD ON ONLINE SHOPPING PAGES PUBLISHED IN THE SOCIAL MEDIA ACCOUNT," *European Journal of Molecular & Clinical Medicine*, 2020.