International Journal for Multidisciplinary Research (IJFMR)

E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Electronically Advertising Treachery and IT Laws in India

Dr. Monika Rastogi[1], Dr. Vivek Rastogi[2], Mr. Rajiv Kumar Jha[3]

[1]Head, School of Law, Lingaya's Vidyapeeth (Deemed to be University), Faridabad
[2]IMIT Research Organization, Noida
[3]Assistant Professor,School of Law, Lingaya's Vidyapeeth (Deemed to be University), Faridabad

ABSTRACT

Today, online marketing fraud schemes operate in multiple countries and continents, and increasingly aim to target victims in multiple countries. Internet marketing fraud has become a major concern for law enforcement agencies in many parts of the world. The term internet marketing describes both the specific business model used to sell fraudulent products and services online and the community or subculture that embraces it. It works with blatantly poorly designed websites, obfuscating disclosures and outrageous claims designed to scare the wary and appeal to the curious, desperate and naive. There are currently no comprehensive and authoritative statistics on the extent of internet marketing fraud worldwide. In addition, many victims who have lost money due to online ad fraud do not contact the authorities or call centers. Although it is impossible to know how many victims are unreported, the number is likely to be significant. Customers shop online because they expect selection, inventory transparency, and the ability to research prices, customer reviews, and offers, but if an online retailer doesn't provide enough information about privacy, terms of use, dispute resolution, or contact information, they might. lead to frauds, which are not only financial losses, but also affect the psyche of the consumer. Thus, the purpose of this study is to map Internet marketing fraud based on its specific characteristics and outline the emerging challenges that have been revealed over time through recent cases. The study also looks at the spread of new online marketing scams and some issues related to criminal justice systems and cyber laws.

Keywords: internet advertising, online scams, online frauds, privacy, cyber laws

INTRODUCTION

Internet fraud is the use of Internet services or software connected to the Internet to deceive or otherwise exploit victims of fraud; for example, stealing personal information, which can even lead to identity theft. A very common form of Internet fraud is the distribution of fraudulent security software. Online services can be used to make fraudulent offers to potential victims, make fraudulent transactions or transfer the proceeds of fraud to financial institutions or other persons connected to the system. Various cyber laws have been passed over the years to mitigate and control online fraud, which also form the basis of the criminal justice system, viz. governmental practices and institutions aimed at maintaining social control, preventing and mitigating crime, or punishing offenders with criminal sanctions and rehabilitation efforts. Recently, several class action lawsuits have been filed against large online ad publishers. Google paid $90 million to settle a class action lawsuit over click fraud. Yahoo also settled a similar lawsuit, paying $4.95 million to the plaintiffs' lawyers and returning credit to advertisers alleging click fraud.

METHODOLOGY

The research methodology would be CASE Study Method. A researcher examines cases to investigate a new online ad fraud and various issues. A case study is conducted to gain an in-depth understanding of a set of cases in a real world context. The case study method can be defined as Empirical investigation of a contemporary phenomenon placed in its actual context especially when the boundaries between the phenomenon and the context are not clearly evident. Case studies are appropriate when the research is descriptive or explanatory. Research is considered explanatory if its purpose is to explain a phenomenon and try to find out why or how something happened of.

WHAT IS INTERNET FRAUD?

Internet fraud uses online services and software that have access to the Internet to deceive or exploit victims. The term "Internet Fraud" generally includes cybercrime that occurs via the Internet or email, including crimes such as identity theft, phishing, and other hacking activities designed to defraud people of money. Internet fraud targeting victims through online services accounts for millions of dollars in fraud each year. And these numbers continue to grow as internet use increases and cybercrime techniques evolve. Internet fraud crimes are prosecuted under state and federal laws. For example, in federal law, the surveillance warrant is 18 U.S.C. § 1343, which covers general money laundering and is punishable by up to 30 years in prison and a $1 million fine, depending on the severity of the offense. States like California also have laws against phishing, credit card fraud, unauthorized computer access and identity theft. These laws also prohibit obtaining personally identifiable information (PII) over the Internet while posing as a business under the Anti-Phishing Act.

TYPES OF INTERNET FRAUD

Cybercriminals use a variety of attack vectors and strategies to commit Internet fraud. These include malware, email and instant messaging services to distribute malware, phishing sites that steal user information, and sophisticated, large-scale phishing scams. Internet fraud can be divided into several main attacks, including:

1. **Phishing:** Using email and online messaging services to trick victims into sharing personal information, login information, and financial information.
2. **Data Breach:** The theft of confidential, protected or sensitive information from a secure location and its transfer to an untrusted environment. This includes stealing information from users and organizations.
3. **Denial of Service (DoS):** Deny traffic access to a web service, system or network to cause malicious intent.
4. **Malware:** The use of malware to damage or disable users' devices or steal personal and sensitive information.
5. **Ransomware:** A type of malware that prevents users from accessing critical data and then demands payment as a promise to restore access. Ransom ware is usually delivered through phishing attacks.
6. **Business Email Compromise (BEC):** A sophisticated form of attack that often targets businesses making bank payments. It compromises legitimate email accounts using social engineering

techniques to send unauthorized payments. To avoid online fraud attempts by hackers, users should understand the most common examples of online fraud and tactics.

EMAIL PHISHING

Email phishing Scams is one of the most common types of online fraud that continues to pose a serious threat to internet users and businesses. Statistics from Security Boulevard show that in 2020, 22% of all data breaches involved phishing attacks, and 95% of all attacks on corporate networks were phishing. In addition, 97% of users have not detected sophisticated email phishing, 1.5 million new phishing sites have been created every month, and 78% of users understand the danger of hyperlinks in emails, yet click-through email phishing scams are evolving and range from simple attacks to more insidious and sophisticated threats that target specific people. Email phishing scams see cybercriminals masquerading as someone the victim knows or believes to be reputable. The aim of the attack is to encourage people to click on a link to a malicious or fake website designed to look like a legitimate website, or to open an attachment containing malicious content. A hacker first invades a legitimate website or creates a fake website. They then obtain a list of email addresses to target and distribute an email designed to get people to click on a link on that website. When the victim clicks on the link, they are taken to a fraudulent website that either asks for a username and password or automatically downloads malware onto their device that steals data and login credentials. A hacker can use this information to access a user's online accounts, steal additional information such as credit card information, access corporate networks connected to the device, or commit broader identity fraud. Attackers of email phishing scams often express an urgent need for their victims. This includes telling them that their online account or credit card is at risk and they need to log in immediately to resolve the issue.

GREETING CARD SCAMS

Many online fraud attacks focus on popular events to defraud people who celebrate them. This includes birthdays, Christmas and Easter, which are usually celebrated by sharing email greeting cards with friends and family. Hackers typically exploit this by installing malware on an email greeting card that downloads and installs on the recipient's device when the greeting card is opened. The consequences can be devastating. Malware can cause annoying pop-ups that can affect an application and slow down your device. A more alarming consequence would be that the victim's personal and financial information is stolen and their computer is used as a bot in a vast network of compromised computers, also known as a botnet.

CREDIT CARD FRAUD

Credit card fraud usually occurs when hackers fraudulently obtain credit or debit card information to steal money or make purchases. To obtain this information, online scammers often use too-good-to-be-true credit card or bank loan agreements to lure victims. For example, the victim may receive a message from his bank that he is entitled to a special loan agreement or that he has been loaned a huge amount of money. These scams continue to trick people despite widespread awareness that such offers are too good to be true for some reason.

ONLINE DATING SCAMS

Another typical example of Internet scams involves the many online dating apps and websites. Hackers focus on these apps to trick victims into sending money and sharing personal information with new love interests. Fraudsters usually create fake profiles to communicate with users, develop relationships, slowly build their trust, create a fake story and ask the user for financial help.

LOTTERY PAYOUT FRAUD

Another common form of Internet fraud is email scams that tell victims they've won the lottery. These scams inform recipients that they can claim their prize only after paying a small fee. Lottery pay-out scammers usually create emails to look and sound credible, which is why many people fall for the scam. The scam targets people's dreams of winning huge sums of money even though they may never have bought a lottery ticket. Furthermore, no legal lottery system requires a fee from winners to claim their prize.

NIGERIAN PRINCE

A classic Internet scam tactic, the Nigerian Prince scam is still prevalent and thriving despite widespread awareness. The scam is based on a wealthy Nigerian family or individual who wants to share their wealth in exchange for access to their inheritance. It uses a phishing tactic to send emails describing an emotional background and then lures victims with the promise of a large financial reward. The scam usually starts by asking for a small payment to help with legal processes and paperwork, promising a large amount of money later. The fraudster will inevitably charge higher fees to cover the additional administrative tasks and transaction costs supported by legitimate verification documents. However, the promised return on investment never comes.

WHAT IS INTERNET ADVERTISING

Online advertising is a form of marketing that relies on the Internet to deliver marketing messages to target users. An online advertisement usually consists of a short text, image or animation inserted into a web page. The purpose of advertising is usually to capture the attention of the user and make him buy or consume a certain product or service, thus increasing the income of the advertiser. Advertisers pay to have their ads appear online, so online advertising has become the most important business model for monetizing online content. Unlike other forms of media such as television or radio, online advertising is not limited to an audience of a specific time or geographic location. An additional advantage is that online advertising allows the personalization of advertisements, which increases the likelihood that the user will be interested in the advertised products and services. Therefore, many advertisers who understand the potential of online advertising invest significant budgets in this advertising. As a result, multiple advertisements are displayed along with the web page content on multiple websites visited by users.

WHAT IS ADVERTISING FRAUD

The online advertising system can be abused in many ways. In practice, this article focuses on the most common ad fraud attacks that bring financial benefits to the adversary. The article also discusses possible countermeasures against these attacks. Ad fraud is any attempt to defraud digital advertising networks for financial gain. Fraudsters often use bots to commit ad fraud, but not always - fraudsters can use a number of methods to trick advertisers and ad networks into paying them. Ad fraud using bots is usually click fraud. Cybercriminals can commit ad fraud in a number of ways. Some of the methods include:

- **Stealth Ads:** When an ad is displayed in such a way that the user cannot see it. This scam targets ad networks that pay based on impressions (views), not clicks.
- **Click Hijacking:** This occurs when an attacker redirects a click on one ad to a click on another ad and "steals" the click. For a phishing attack to work, the attacker must break into the user's computer, the ad publisher's website, or a proxy server.

CYBER LAW IN INDIAN PERSPECTIVE

As businesses increasingly rely on electronic information and computer networks for their daily operations, more and more personal and financial information is being transferred and stored online. This can expose individuals exposed to data breaches, as well as financial institutions and other businesses, with potentially significant liability if and when a data breach occurs. Cybercrimes can include traditional criminal activities such as theft, fraud, forgery, defamation and vandalism, all of which fall under the Indian Penal Code. Misuse of computers has also given rise to a series of new-age crimes dealt with under the Information Technology Act, 2000. IT Act, 2000 - The Information Technology Act, 2000 received the assent of the President of India on 9 June 2000 and came into force on October 17 of the same year. The law was introduced to allow legal recognition of transactions made through electronic data transmission and other electronic means of communication (commonly known as electronic commerce) to facilitate the electronic filling of documents by government agencies as an alternative to paper-based methods. Communication and retention of data in connection with commercial activities.

Amendment Act 2008- Important features of this Act are-

- To Focus on data protection
- To Focus on data security
- To Concept of cyber café
- To Neutralization of digital signature technology
- Definition of acceptable security practices followed by the company
- Redefining the role of mediators
- Indian Computer Crisis recognition of the role of the working group.

Cyber threats can be classified in two ways –

- Computer-based: – Using a computer to attack other computers. Example: Hacking, virus/worm attacks, DOS attack etc.
- Computer as a weapon: - using a computer to commit crimes in the real world. Example: cyber terrorism, intellectual property violations, credit card fraud, EFT fraud, etc.

GENERAL COMPUTER CRIMES

- On Facebook and other social networks - downloading/disseminating inappropriate or socially sensitive multimedia content or messages.
- Defaming someone, violating someone's privacy or harassing someone.
- Piracy - distribution of copyrighted software, movies or other without permission.
- Hacking, spoofing, Cheating and Spam.

CRIMES, COMPENSATIONS AND PUNISHMENTS

1. **Punishment and compensation for damage to a computer, computer system, etc.:** If someone without the permission of the owner or someone else responsible for the computer, computer system or computer network-

- Uses or provides access to such a computer. Computer system or computer network or computer resource;
- Downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network, including data stored or maintained on any removable medium.
- Introduces or causes any computer contamination or computer virus to enter any computer, computer system or computer network.
- Damages or causes damage to any computer, computer system or computer network, data, database or other programs located on such computer, computer system or computer network.
- Interferes or causes interference with the operation of any computer, computer system or computer network.

2. **Compensation for failure to protect data [Sec. 43-A]:** If an entity that owns, processes or processes sensitive personal data or information contained in a computer resource owned, controlled or used by it, has failed to implement or maintain reasonable security practices and thus creates and causes illegal damage and unauthorized gain to any such entity shall compensate the injured party.
3. **Penalty for non-delivery, return etc. [Sec. 44] : If a person is required to:**

- Deliver any document, return or report to the registrar or certifying authority but fails to do so, he shall be punished with fine which may extend to one lakh and fifty thousand rupees to all such a failure.
- Keep books or records, neglecting to keep the same, he shall pay a fine not exceeding ten thousand rupees for every day during which the contravention continues.

4. **Penalty for providing access to a protected system [Section 70]:** The relevant government can declare that any computer resource that directly or indirectly affects the operation of critical information infrastructure in a protected system and can, by written order, authorize a person using a protected notified system. A person who provides unauthorized access to such a protected system or attempts to access it is punishable by imprisonment for up to 10 years and a fine.
   The Central Government enacted the Information Technology (Security Procedure) Rules, 2004.
5. **Violation of computer source documents [sec.65] :** Whoever knowingly or intentionally hides, destroys or modifies a computer, its source code is used by the computer , a computer system shall be maintained by law, punishable with imprisonment for a term which may extend to three years or with fine which may extend to two lakhs of rupees, or with both of.

CASES RELATED TO CYBER FRAUD

People with mental health problems who are targeted by fraudsters. The National Fraud Intelligence Bureau's (NFIB) proactive intelligence team has identified a growing trend in local communities of fraudsters unwittingly recruiting people with mental health issues as money mules. A money mule is a term used to describe a person recruited by fraudsters to launder ill-gotten money. Even if a moneylender is not engaging in fraud to generate money, they are still committing a crime. In most cases, the criminals behind this type of fraud are based overseas and usually try to recruit people by cold calling, emailing or sending fake job ads. The NFIB team found that fraudsters are now targeting vulnerable individuals on a personal level to carry out this crime. How a person with depression and dyslexia was targeted. In one case, a man with severe depression and dyslexia was targeted and became a friend for a while until the fraudster asked the man if he could use his bank account to obtain receipts for a series of money transfers to a new IT company. The man agreed to let the fraudsters use his accounts, after which he was arrested and sentenced to three years in prison for money laundering. NFIB's Preventive Intelligence Team interviewed a convicted money mogul who said: "When you're so depressed and thinking about taking your own life, you just need someone to talk to. I've tried to get help but I'm useless with computers and dyslexic so it's always been hard to find support. I was an outcast in my local community and even people in my church didn't want to talk to me. I think people don't understand mental health and we are easy targets for people who want to take advantage of our need to talk and feel accepted.―These rascals accepted me. They talked to me and interacted with me. They listened to me and understood what I was going through. When they finally started talking to me about their IT business, I struggled to understand because of my dyslexia‖. - They told me that I could be part of their business using my bank accounts of.

Cases of online sales scams are booming in Kochi. When Suresh Kumar from Aluva resorted to an online search for a used car, he never thought that he would soon be scammed when he called a mobile number posted on a classified internet portal advertising a Toyota Innova for sale. After seeing the ad, he called the mobile number and the sellers asked him to come and see the vehicle at Nedumbassery airport. When he reached there, Suresh was asked to make an advance payment of 3.5 lakhs to the bank account number given by the sellers to prove that he was a genuine customer. However, when he called the sellers after paying the money, the mobile phone was switched off. He realized he had been duped when repeated attempts to reach the sellers by phone proved futile. According to Kochi city police officials, cases of fraud involving sales through confidential websites are on the rise. In the last three months, the police have registered up to 10 cases of online fraud, in which a seller publishes images of products on classified websites online and asks gullible customers to pay in advance to facilitate a sale. Websites offering classified services fail to prevent fraudsters because they have no mechanism to verify the benefits of the product displayed on their websites. Customers should be careful when shopping online. Depending on the circumstances, the police will register in such cases under various sections of SPR, Consumer Protection Act and IT Act. To create awareness among the public, the Kochi city police sent out a message warning them to be wary of confidential portals offering huge profits. As electronics, mobile phones, cameras, laptops and cars are available cheaper in the over the counter market, many today prefer to shop online. Therefore, according to CyberCell officials, frauds in this environment have also increased. In addition, in many cases it is difficult for the police to trace the IP address of each case of foreign service providers, although most fraudsters operate domestically. Websites that offer confidential services cannot prevent fraudsters because they have no mechanism to verify the products displayed on their websites. After paying the amount, the customer knows that there is no such party or object.

In the case of Digital Money India, several new websites have sprung up in recent months that claim to offer work-from-home opportunities for Indians. The case involves websites operating under the names Digital Money India and Digital Cash Course. How do they eat you? Over the past few months, quite a few ads have appeared on Facebook that claim to offer work-from-home opportunities. When you click on these ads, they take you to a website where you have to enter your contact information. After providing your contact information, you will usually receive a call from a company representative within a few days stating that this is an exclusive opportunity to work from home and that you must pass an interview before they will consider you eligible for this program. They then proceed with an interview where they ask you trivial and frivolous questions such as: How much time do you spend online? After a 5 minute interview, they inform you that you are now eligible for the program and you have to pay 3500-4400 rubles to have the package delivered to your home. The Digital Money India package consists of CDs with videos and tutorials and printed materials on creating a website and making money online through ads. This is a scam. Because all information about CDs and books are available online for free. The interview questions are designed to measure your internet awareness. When they realize that you know a lot about the Internet, they immediately stop. However, if you are a beginner, they will try to trick you with their fake website building training. They borrowed the name from the plan restarted by the Indian government a few months ago to connect all villages and small towns to the Internet through an optical network. The system, called Digital India, is expected to be ready in the next two years. They are using the Digital India brand to confuse users.

AROUND 1.1 MILLION FINANCIAL FRAUD CASES REGISTERED IN 2023

A total of 1.13 million financial cyber fraud cases were reported in 2023, according to a Lok Sabha reply dated February 6. A Citizen Financial Cyber Fraud Reporting and Management System has been established under the Cyber Crime Coordination Center of India. The Ministry of the Interior reports financial fraud. "With more than 4.7 million (470,000) complaints, more than 1,200 million rupees have been saved since the introduction of the system. He added that the government has blocked 320,000 SIM cards and 49,000 numbers of International Mobile Equipment Identity (IMEI) reported by the police. The five largest states accounted for half of all financial fraud cases last year. Uttar Pradesh topped the list with about 200,000 cases, the highest among 36 states and the Union. Maharashtra came next, reporting 130,000 complaints, followed by Rajasthan (both 80,000). Lakshadweep was at the bottom with 29 cases. The value of these 1.13 crowns was 7,488.6 crowns. 990.7 million was the highest in Maharashtra. Telangana followed with Rs. 759.1 crore. It was followed by Uttar Pradesh (721.1 billion), Karnataka (662.1 billion) and Tamil Nadu (661.2 million). Lakshadweep's contribution was the lowest at 0.2 crore. In 2023, according to the response, about 300,000 maintenance complaints were processed, amounting to 921.6 billion rupees. Data from India's Computer Emergency Response Team (CERT-IN) shows that 1,391,457 cyber security incidents were reported in 2022, but down from 80,402 in 2021. The trend has been upward in recent years. In 2018, the number was 208,456.

STATISTICAL DATA BY THE NATIONAL CRIME RECORDS BUREAU (NCRB) FOR THE CASES RELATED TO CYBER FRAUDS ON 06 FEB 2024 BY PIB DELHI

The National Crime Records Bureau (NCRB) compiles and publishes crime statistics in its publication Crime in India. The last published report is from 2022. "Police" and "Public Order" are State subjects under the Seventh Schedule of the Constitution of India. States/UTs are primarily responsible for prevention, detection, investigation and prosecution of cyber crimes through their law enforcement agencies. The State Council complements state government initiatives with advice and plans to build the capacity of their law enforcement agencies. In order to strengthen the mechanism to deal with cybercrime in a comprehensive and coordinated manner, the Central Government through the Ministry of Home Affairs has set up the "Indian Cybercrime Coordination Center" (I4C) to deal with all kinds of cybercrime in the country.

The National Cybercrime Reporting Portal (https://cybercrime.gov.in) was launched as part of I4C to enable the public to report all types of cybercrime incidents, especially cybercrime. against women and children. Cybercrime cases reported on this portal, their conversion into FIRs and subsequent actions related to them are dealt with by the law enforcement agencies of the concerned country/UN as per the law. The "Citizen Financial Cyber documents topics of "Citizen Financial Cyber Fraud Management" Citizen Financial Fraud Management System" under the Citizen I4C's "Citizen Financial Cyber Fraud Management System" under I4C has been launched for immediate to report financial fraud and prevent fraudsters from collecting money, it said. Since the establishment of the Citizen's Financial Fraud Reporting and Management System, over Rs. 1200 crore was saved from over 4.7 million complaints. Toll free helpline 1930 has been launched to provide assistance in filing cyber complaints online. State/UN awareness details of the Cyber Financial Cybermanagement system for the period 1/1/2023 to 12/31/2023 are attached. The Indian government has so far blocked more than 3,200 SIM cards and 49 million IMEI codes, according to law enforcement officials.

CERT-In continuously issues alerts and advisories on the latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data. CERT-In through RBI has advised all authorized entities and banks issuing prepaid payment instruments (wallets) in the country to conduct a special audit by CERT-In empaneled auditors, close the anomalies found in the audit report and ensure implementation of best security practices. CERT-In and Reserve Bank of India (RBI) are jointly conducting a cyber security awareness campaign “Watch out and be aware of financial fraud” through the Digital India platform. To spread awareness about cybercrime, the Central Office has introduced measures that include e.g. messaging via SMS, I4C's social media account i.e. X (formerly Twitter) (@Cyberdost), Facebook (CyberDostI4C), Instagram (cyberdostI4C), Telegram (cyberdosti4c), radio campaign, MyGov's commitment to publicity in various media, organizing cyber security and security awareness weeks together with states/UT- s, publication of a youth/student handbook, etc. States/UTs have also been asked to spread the word to create mass awareness.

CONCLUSION

E-commerce fraud costs merchants billions of dollars in lost products and services, but preventing it also comes at a significant cost to retailers. Fraud can affect a retailer's reputation and cause huge customer turnover that can take years to recover from. While retailers have traditionally neglected fraud management as the volume of online business has increased, the industry is now investing in better tools and processes to make fraud management more efficient and proactive. However, it is important to understand that fraud management is also an art – balancing risk acceptance and customer experience. Excessive focus on one of these aspects will negatively affect the other. A retailer must be willing to accept the risk of fraud to minimize disruption to the shopping experience of loyal customers. In addition to implementing advanced tools and automating fraud detection, retailers must create internal processes to make fraud management a central part of enterprise-wide accountability and strategic initiatives.

REFERENCES

1. V. Anupam , A. Mayer, K. Nissim , B. Pinkas and M . K. Reiter. About the security of pay-per-click and other advertising systems. Calculate. Web, 31(11-16): 1091-1100.
2. B. Krishnamurthy, D. Malandrino and CE Wills. Measuring the Impact of Loss of Privacy and Data Protection on Online Browsing.
3. C.Larsen.ExploitingTrust in AdvertisingNetworks. http://rocket.bluecoat.com/blog/exploiting-trustadvertising-network.
4. Daswani, N., Mysen, C., Rao, V., Weis, S., Gharachorloo, K., Ghosemajumder, S.: Internet Advertising Fraud. In: Criminal Malware: Understanding New Attacks and Defenses. Addison-Wesley Professional, Reading (2018).
5. eMarketer. Total online advertising spending in 2021 was $19.5 billion. http://www.emarketer.com/Article.aspx?1004635,2021.
6. Google,2019."ContentNetwork". https://adwords.google.com/select/afc.html?sourceid=awoandsubid=en-us-et-awhp_related
7. How fake clicks show up in third-party audit click fraud reports. http://www.google.com/adwords/ReportonThirdPartyClickFraudAuditing.pdf,2022.
8. M. K. Reiter, V . Anupam and A. Mayer. Detects hit-shaving in pay-per-click systems. Proceedings of the 3rd USENIX Electronic Business Workshop, 2018.
9. M. Gandhi, M. Jakobsson, and J. Ratkiewicz. Bad ads: silent click fraud with unwanted accessories. Journal of Digital Forensics Practice, 1(2), 2021.
10. P. Ipeirotis. Exposing an ad fraud scheme. http://behind-theenemy-lines.blogspot.com/2021/03/uncovering-advertising-fraud-schema.html.
11. http://www.newindianexpress.com/cities/kochi/Online -Sales-Fraud-Cases-Shooting-up/2023/02/25/art133294835.ece
12. http://indiamicrofinance.com/digital-money-india-review-scam.html
13. Approx In 2023, 1.1 million cases of financial fraud were registered, data shows India News - Business Standard (business-standard.com)
14. National Crime Records Bureau (ncrb) Internet Fraud Statistics 6 Feb 2024 pib Delhi52.
15. https://www.fortinet.com/resources