A Study of Emerging Internet Advertising Frauds and Subsequent Cyber Laws in India

Dr Hitesh Keserwani
Assistant professor
Amity Business School, Amity University, Lucknow , India

Abstract: ***Today, internet marketing fraud schemes operate from, and increasingly seek to target victims in, numerous countries on multiple continents. Internet marketing fraud has become a substantial concern for law enforcement in several regions of the world. The term Internet Marketing describes both a particular business model used to sell fraudulent products and services online, and the community or subculture that embraces it. It operates out in the open with poorly designed websites, tacky infomercials, and outrageous claims designed to scare off the wary and draw in the curious, desperate, and naive. At present, there are no comprehensive and authoritative statistical data regarding the scope of internet-marketing fraud on a global level. Furthermore, many victims who lose money due to internet-advertising fraud do not contact authorities or reporting centers. While it is impossible to know how many victims fail to report fraud, the number is likely substantial. Customers buy online because they expect choice, transparency about inventory levels and the ability to research prices, customer reviews and promotional offers but if an online retailer does not provide adequate information about privacy, terms and conditions of use, dispute resolution or contact details it might lead to scams which are not only a financial loss but also affects consumer psyche. The purpose of this study is therefore to map out internet marketing frauds in terms of its distinctive qualities and to outline the emerging challenges that have taken place over time with the help of recent case lets. The study also discusses the prevalence of new internet marketing frauds and some of the issues arising for criminal justice systems and cyber laws.***

Keywords: Internet advertising, Online Scams, Privacy, Cyber Laws

---

Introduction

An Internet fraud (online scam) is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them; for example, by stealing personal information, which can even lead to identity theft. A very common form of Internet fraud is the distribution of rogue security software. Internet services can be used to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme. To mitigate and control internet frauds various cyber laws have been made over the years which also ensures the criminal justice system i.e. practices and institutions of governments directed at upholding social control, deterring and mitigating crime, or sanctioning those who violate laws with criminal penalties and rehabilitation efforts. Recently, several class action lawsuits against large online advertising publishers appear. Google paid 90 million dollars to settle a class action lawsuit about click fraud in March 2006. In June 2006, Yahoo settled a similar lawsuit by paying 4.95 million dollars to plaintiffs' counsel, and allowing credit refund to advertisers who claim click fraud back through January 2004.

Methodology

The methodology adopted for the research would be CASE STUDY METHOD. The researcher would study three cases to Study the Emerging Internet Advertising Frauds and Various Issues. Case study research is conducted to gain in-depth understanding of a case set in real word context. The case study method may be defined as follows:

"An empirical inquiry about a contemporary phenomenon (e.g., a "case"), set within its real-world context—especially when the boundaries between phenomenon and context are not clearly evident (Yin, 2009a, p. 18)". Case studies are pertinent when a research is either descriptive or explanatory. The research is said to be explanatory when it aims to explain a phenomenon and attempts to find why or how a thing happened.

Advertising on the Internet

Online advertising is a form of marketing that relies on the Internet to deliver marketing messages to the targeted users. Internet advertisement typically comprises a short text, an image, or an animation embedded into a Web page. The purpose of an ad is generally to capture a user's attention and persuade him to purchase or to consume a particular product or a service and, consequently, to increase the revenue of the advertiser. Advertisers pay for their ads to appear online, thus online advertising has become the major business model for monetizing online content. In contrast to other types of media (e.g., television or radio), online advertisements are not limited to an audience at a given time or a geographic location. An additional benefit is that online advertising allows for the customization of advertisements, thus increasing the probability that a user is interested in the advertised products and services. Hence, many advertisers, realizing the opportunities of online advertising, invest significant budgets into this form of advertising. Consequently, for many of the websites that users visit, a number of advertisements appear together with the content of a Web page.

Ad Fraud

An online advertising system can be abused in many ways. This paper focuses on the ad fraud attacks that have been the most prevalent in practice and that yield monetary benefits for the adversary. The paper also addresses possible countermeasures to these attacks.

Cyber Law of India-

As businesses increasingly depend on electronic data and computer networks to conduct their daily operations, growing pools of personal and financial information are being transferred and stored online. This can leave individuals exposed to privacy violations and financial institutions and other businesses exposed to potentially enormous liability, if and when a breach in data security occurs. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

Cyber crimes can be categorized in two ways-

- The Computer as a Target :-using a computer to attack other computers.

Example: Hacking, Virus/Worm attacks, DOS attack etc.

- The computer as a weapon :-using a computer to commit real world crimes.

Example: Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds,etc.

Common Cyber Crimes Committed-

- On Facebook and other Social Media- Uploading/spreading of objectionable or communal sensitive multimedia content or message.
- Defaming someone, invading someone's privacy or harassing.
- Piracy – Distributing copyright software or movie or anything without permission.
- Hacking and Spoofing.
- Spam

Cyber Laws existing in India-

IT Act 2000- The Information Technology act , 2000 received the assent of president of India on 9 June 2000 and came into force from 17 October in that same year .The act was enacted to provide legal recognition for transaction carried out by means of electronic data interchange and other means of electronic communication , commonly referred to as "Electronic Commerce" , to facilitate electronic filling of documents with governments agencies which involve the use of alternative to paper based method of communication and storage information This law applies to any kind of information in the form of data message used in the context of commercial activities.

•Amendment act 2008- The notable features of this act are-

- Focusing on data privacy
- Focusing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognizing the role of Indian Computer Emergency Response Team

OFFENCES, COMPENSATION AND PENALTIES

1. Penalty and compensation for damage computer, computer system etc: If any person, without permission of the owner or any other person who is in charge of a computer, computer system or computer network-

- Accesses or secures access to such 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 information data held or stored in any removable storage medium.
- Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.
- Damages or cause to be damage to any computer , computer system or computer network , data, computer database or any other programmers residing in such computer , computer system or computer network .
- Disrupts or cause of disruption of any computer, computer system or computer network.

2. Compensation for failure to protect data[Sec. 43-A] : where a body corporate , possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns , control or operates , is negligent in implementing and maintaining reasonable security practices and produces and thereby causes wrongful loss and wrongful gain to any person , such body corporate shall be liable to pay damage s by way of compensation to the person so affected.

3. Penalty to failure to furnish information, return etc.[Sec. 44] :If any person is required to:

- Furnish any document, return or report to the controller or the Certifying Authority, fails to furnish the same, he shall be liable to penalty not exceeding rupees one lakh and fifty thousand for each such failure.
- Maintain books of account or records, fails to maintain the same, he shall be a liable to a penalty not exceeding rupees ten thousand for every day during which the failure continues.
- Penalty for securing access to a protected system[Sec 70]: The appropriate government may declare that any computer resource which directly or indirectly affects the facility of critical Information Infrastructure to be protected system and may , by in order in writing , authorize the person who are to access protected notified system. Any person who secure access or attempts to secure to such a protected system by unauthorized manner shall be punished with imprisonment of a term which may extend to 10 years and shall also be liable to fine. The central Government has prescribed the Information Technology (Security Procedure) Rules, 2004.

- Tampering with computer source documents [sec.65] :Whoever knowingly or intentionally conceal , destroy or alters any computer source code used for computer , computer programmed, computer system is required to be maintained by law, shall be punishable with imprisonment up to three years or with fine which may extend up to rupees two lakhs or with both .

Case 1: People experiencing mental health issues targeted by fraudsters

The National Fraud Intelligence Bureau's (NFIB) Proactive Intelligence Team have identified an increasing trend whereby people experiencing mental health issues are actively being recruited by fraudsters from within local communities to unknowingly become money mules.

A money mule is a term used to describe someone who is recruited by fraudsters needing to launder funds they have obtained illegally. Even if the money mule is not involved in the fraud to generate the money, they are still committing a crime.

In most cases criminals carrying out this type of fraud are located abroad and usually try to recruit people by cold calling, sending emails or by posting fake job adverts. The NFIB team have found that fraudsters are now targeting vulnerable individuals on a personal level in order to carry out this crime.

How someone with depression and dyslexia was targeted

In one case a male with severe depression and dyslexia was targeted and befriended over a period of time until the fraudster asked the male if he could use his bank accounts to take receipt of a series of money transfers for a new IT business. The male agreed to let the fraudsters use his accounts and was subsequently arrested and sentenced to three years in prison for money laundering.

The NFIB Proactive Intelligence Team interviewed a convicted money mule who said: "When you are so depressed and thinking about taking your life, you just need someone to talk to. I tried to look for help but I am useless with computers and suffer from dyslexia, so I always found it hard to find support. I was an outcast in my local community and even people in my church wouldn't talk to me. I don't think people understand mental health and we are easy targets for people wanting to take advantage of our need to talk and to feel accepted".

"These fraudsters welcomed me. They talked to me and socialised with me. They listened to me and understood what I was going through. When they eventually started to talk to me about their IT business, I struggled to understand because of my dyslexia". "They told me that by using my bank accounts, I could be part of their business.

Case 2: Online Sales Fraud Cases Shooting up

KOCHI: When Suresh Kumar (name changed), of Aluva, launched an online search for a used car, he never thought that he would be duped soon after making a call to the mobile number published on the classified web portal which advertised a 'Toyota Innova car for sale'. Seeing the advertisement, he called the mobile phone number and the 'sellers' asked him to reach Nedumbassery Airport to see the vehicle. When he reached there, Suresh was asked to pay an advance of Rs 3.5 lakh, in order to prove that he was a genuine customer, to a bank account number provided by the sellers. However, when he called the sellers after paying the money, the mobile phone was switched off. He came to knew that he was cheated after repeated efforts to get the sellers over phone proved futile.

Officers attached to the Kochi City Police say cases of fraud on sales via classified websites are showing a rising trend. The police have registered as many as 10 online fraud cases during the past three months, in which the seller posts photos of products in online classified websites and seeks advance payment from gullible customers for facilitating the trade.

The online websites which offer classified services are unable to prevent the fraudsters as there is no mechanism to monitor the merits of the products being displayed in their sites. It is up to the customers to be on guard while engaging in the online trade.

"Police book these kinds of cases with sections for cheating under IPC, various sections of Consumer Protection Act and IT Act as per the circumstances,"

In order to create awareness among the public, the Kochi City Police have posted a message warning them to be cautious of classified portals offering high profits. As there is the possibility to get electronic goods, mobile phones, cameras, laptops and automobiles at prices lower than the open market, many prefer online trade now. Hence, the frauds in this medium also escalated, according to Cyber Cell officers. Moreover, it is difficult for the police to keep track of the IP address of each case from overseas service providers in many cases though majority of the fraudsters are operating from within the country. The online websites which offer classified services are unable to prevent the fraudsters as there is no mechanism to monitor the merits of the products being displayed in their sites. After paying the amount, the customer comes to know that there is no such party or goods

Case 3: Digital Money India

Several new websites have emerged in the last few months that claim to offer "Work from Home" opportunities for Indians. This case is about the websites which operate under the name of Digital Money India and Digital Cash Course. How they Bait you ?

Over the last few months there are few Facebook Advertisements that claim to give an opportunity to work from home. When you click on these ads they take you to a website where you need to fill in your contact information. Once you have provided them your contact details, you will receive a call usually within the next few days, where a representative of the company will claim that this is an exclusive work from home opportunity and you will need to pass a round of interviews before they deem you eligible to become a part of this program. They will then proceed to the Interview, during which they will ask you trivial and frivolous questions such as:

- How much Time Do you Spend on the Internet?
- Do you make Payments Online?
- Do you know how to build a website?
- Have you worked online before?
- Do you have a Debit Card?

After conducting the interview for 5 minutes, they will announce that you are now eligible to become a part of the program and must pay an amount ranging from Rs 3500 to Rs 4400 to get a kit, which will be delivered at your home.

The Digital Money India kit will consist of some CD's with videos and tutorials along with some printed material on how to build a website and earn money online through advertisements. The Two Websites through which the company is currently operating are:-

http://www.digitalmoneyindia.com/
http://www.digitalcashcourse.com/
It is a scam. As all the information they provide in the CD's and Books is available online for free. The questions asked in the Interview are aimed at gauging your awareness of the Internet, if they realize you know a lot about the Internet then they immediately hang up. But if you are a novice, then they try to defraud you with their fake training program about building websites. They have borrowed the name of a scheme that was re-launched some months ago by the Government of India to connect all the villages and small towns to the Internet via a fiber network. The scheme called Digital India is expected to be completed over the next 2 years. To confuse users they are using the Digital India brand name.

Conclusion

E-commerce fraud costs merchants billions of dollars in lost products and services, but its prevention also remains a significant ongoing cost for retailers. Fraud can hit a retailer's reputation and cause huge customer churn, which can take years to regain. Though retailers have historically neglected fraud management, amid growing online business volumes, the industry is now investing in better tools and processes to make fraud management more robust and proactive. However, it is important to understand that fraud management is also an art -- a balancing act between risk acceptance and customer experience. Undue focus on one of these aspects will adversely affect the other. There has to be a level of fraud risk that a retailer is willing to accept in order to minimize interference with the shopping experience of its loyal customers. Apart from implementing sophisticated tools and automating fraud detection, retailers need to establish internal processes to make fraud management an enterprise-wide responsibility and a key component of strategic initiatives.

References-

[1] V. Anupam, A. Mayer, K. Nissim, B. Pinkas, and M. K. Reiter. On the security of pay-per-click and other web advertising schemes. Comput. Netw., 31(11-16):1091–1100, 1999.

[2] B. Krishnamurthy, D. Malandrino, and C. E. Wills. Measuring privacy loss and the impact of privacy protection in Web browsing. page 52. ACM Press, 2007.

[3] C. Larsen. Exploiting Trust in Advertising Networks. http://rocket.bluecoat.com/blog/exploiting-trustadvertising-networks, 2010.

[4] Daswani, N., Mysen, C., Rao, V., Weis, S., Gharachorloo, K., Ghosemajumder, S.: Online Advertising Fraud. In: Crimeware: Understanding New Attacks and Defenses. Addison-Wesley Professional, Reading (2008).

[5] eMarketer. Online ad spending to total $19.5 billion in 2007. http://www.emarketer.com/Article.aspx?1004635, Feb. 2007.

[6] Google, 2008. "Content Network." https://adwords.google.com/select/afc.html?sourceid=awo&subid=en-us-et-awhp_related

[7] How fictitious clicks occur in third-party click fraud audit reports. http://www.google.com/adwords/ReportonThirdPartyClickFraudAuditing.pdf, August 2006.

[8] M. K. Reiter, V. Anupam, and A. Mayer. Detecting hit shaving in click-through payment schemes. In Proceedings of the 3rd USENIX Workshop on Electronic Commerce, 1998.

[9] M. Gandhi, M. Jakobsson, and J. Ratkiewicz. Badvertisements: Stealthy click-fraud with unwitting accessories. Journal of Digital Forensics Practice, 1(2), 2006.

[10] P. Ipeirotis. Uncovering an advertising fraud scheme. http://behind-theenemy-lines.blogspot.com/2011/03/uncovering-advertising-fraud-scheme.html, 2011.

[11] http://www.newindianexpress.com/cities/kochi/Online-Sales-Fraud-Cases-Shooting-up/2016/02/25/article3294835.ece

[12] http://indiamicrofinance.com/digital-money-india-review-scam.html