International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-4, Issue-3, May-2017
DOI: 10.21276/ijirem.2017.4.3.3

Emerging Online Frauds: Detection and Their Possible Controlling Strategies in E-Business

Dr. Prabhat Kumar Vishwakarma
Life Member of Indian Society for Technical Education

ABSTRACT
Information Technology boom specially as E-business or online business has given the remarkable business trend among the public which can be observed easily by the frequent usages of Paytm, Debit Card, Credit Cards, Internet Banking, Mobile Banking etc. that is all business deals are just one click or one touch away . As in any business financial transactions are always and will always be the important activity therefore the key role of banking sectors with the handshaking with Information Technology along with Cyber Laws shall always be of prime importance. If the businesses are fully web enabled then basis of brand building may be customer online review about the product which is one of the informal way of certifications about the quality of product or services which could have been possible due to the emergence of E-Commerce and subsequently its effective practices. But still cyber frauds cannot be overlooked. This paper focuses on the current unethical E-Business practices and the role of Cyber laws to overcome it.

Keywords: Cybercrime, Digital Marketing, Forced Targeted Traffic, Internet of Things, Spear- Phishing

1. INTRODUCTION
The emergence of World Wide Web (WWW) has now given the business a new real trend and shape coined as E-Commerce. Surfing on web portal through catalogues to order goods, subscribing on line services and to pay through smart cards for that is now the very common day to day activity. The E-business has the reach to the customers of the whole world connected via Internet. Therefore the E-Commerce enabled business provides its customer the borderless marketplace rather than physical marketplace. Because of the pull type processing E-Commerce provides customized product services to fulfill the customer requirement. Now the E-business is free from time, place and person. Customers involved in E-Commerce have the choice of shopping around the world and also they can go easily for price comparison either by surfing the individual web portal or through the web portal acting as an intermediary and providing comparison lists of similar kind of products offered through different companies. For example if a customer is intended to purchase an insurance policy, he or she can go on the website policybazaar.com and purchase a policy after a proper comparison of similar policy offered by different insurance companies on a same web place. Due to less initial investment the opportunities for new competitors are easy in cyber market, resulting competitive advantage to the web enabled customers. No any technology always has the benefits but also has some limitations. Sometimes biggest advantage becomes the major disadvantage like competitive advantage to customer may be the big loss to company due to price war. The threat of continuous technology update and regular eye watch needed about the product or services offered by the company due to the fear of always the possibility of entry of new competitors with better similar products or services to affect the business. The biggest challenge which still lies with E-Commerce is security of the communication channels due to emergence of plenty of adware's, malwares, spywares, intruders, hackers and the risk of being blackmailed for sensitive information from Network security providers due to leniency in cyber laws. In the root of any business activity the role of authentic, secure and confidential communication cannot be overlooked. Lack of confidence in financial transactions and in privacy is some of major hurdles to electronic commerce. At any stage of online business vulnerability in data communication and authentication, may lead it toward cyber scam. If someone got an offer for any task which needs to be carried away online for that the concerned will be paid , initially it seems its very good deal , and if payments are received timely as per the terms and condition said primarily then it is a symptom of good online business and later on if it is asked for to attach more persons in this , then online earning person will certainly try to attach more persons with whom he will have good contacts and this is continued up to certain level but meanwhile if the company operated online, stops payment for the desired task and not giving the justified reason of this then business relation with the company will certainly adversely be affected and in general it will be termed as ONLINE FRAUD.

2.OBJECTIVE
The main objective of the paper is to diagnose the security threats commonly observed in online business in today's scenario especially in branding and promotional practices through digital marketing by critically reviewing some online fraud cases in Indian context. And also to identify key factors to be considered while getting involved into the online business for avoiding financial losses.

3. LITERATURE REVIEW
Social networking has totally changed the way of interaction with friends and associates. Now social networks such as Whatsapp, Facebook, Twitter, YouTube, LinkedIn and Google+ have a significant role in communication in today's life style, and also are on high risk for security threats. On one side it is the tool for being in regular touch with families and friends on the other hand these are becoming the way of possible reason of security breaches and providing the route to scammers so that they can execute their unethical intention such as phishing ,under the cover of social networks by attractive fake offers and promotions

which may later on become the reason of mental exploitation and online financial frauds.

3.1 E-Crime and Cyber Security

To commit illegal, unauthorized, malicious activity using the information and communication technologies is referred as E-crime. With the change of time the scope of E-crime has been changed .it now includes potential illegal activities conducted online such as cyber bullying, stealing of intellectual properties etc. E-Crime uses social engineering as basis and is performed either by web-based activities, by downloading activity or by the means of e-mail similar to spam-campaign. Through malicious distributed networks, E-crimes are executed in a grouped way. One group compromises on security and subsequently other groups involved in other malicious activities such as administering and renting the compromised online resources. For securing the web resources tools such as firewalls, encryption techniques are some useful techniques. Privacy policies and procedures should be clearly explained to customers. Although respecting consumer privacy rights is a legal requirement, it also represents good business practice. If customers trust a site and business then they are more likely to trade with it.

3.2 Data Breaches

Data breach is the unauthorized practice by outside cyber attackers to penetrate the online defense of organization and exposing the data which were not expected to see or share. Data leakages may have the adverse impact of online business. It may damage the reputation of organization which may become the reason of losing the trust of company among customers. It can also form the basis to file a legal case against the breached firm by the customers. The consumers are the ultimate victims of data breaches, such cybercrimes may impose serious risks to the consumers for example the personal information stolen may be used to gain access to the account of consumer under attacker's control which may be the reason of big money loss by misusing debit/credit cards. The insiders prevailing the privileged access to customer personal and confidential information may also indulge in unethical practice for undue monetary advantage. Personal digital privacy and protection from spyware and malware are the major threats and without proper protection from these risks proper controlling and promoting online business will be a big challenge. With reference to www.statistica.com,data breaches in famous sites are shown in figure 1

Table 1: Most Popular Data Breaches

Web Sites	Data Breaches(in Millions)
Yahoo 2013,revealed Dec16	1000
Yahoo 2014,revealed Dec16	500
MySpace May 16	427
Adobe Sep 13	152
E Bay March 14	145
Linkedln revealed Jan16	117
AOL Dec 14	92

4. DISCUSSION ABOUT EMERGING ISSUES

The majorly observed issues have been discussed under this section

4.1 Spear Phishing

Spear-phishing attack exploits social engineering approach for improving the chance of success in the personal information stealing. In this approach the emails are tailored by the attacker to guess the interest of the targeted user and using those clues tries to execute the financial scams. Suppose a user works in financial sector then possible approach may be to send the spear-phishing mail that looks as the new financial rules and regulations for stealing the personal information from the targeted users. Prior to such attack, it is thoroughly being analyzed the pattern, trends, profile and workforce of the targeted organization by the spear-phishing attacker.

4.2 Banking Trojans and Heists

Banking Trojans are the key areas for attackers to do malicious activities such as modifying banking online sessions and injectionof extra fields for hacking the session or for stealing the sensitive details. The most common form of attack continues to be financial Trojans which perform a Man-In-The- Browser (MITB) attack on the client's computer during an online banking session.

4.3 Social Trade: One Of The Biggest Indian Cyber Frauds

A firm registered under the name Ablaze Info Solutions Pvt. Ltd in Noida which is an ISO: 2008 certified company is accused that under the scheme named Social Trade it has cheated approx. seven lakhs investors. This was operational through web portal socialtrade.biz. This cyber fraud is of worth Rs 3,700 crores. The web portal was launched in august 2015 with different offers to investors for earning. Social Trade is based on Digital Marketing which works on Social Exchange Plan which helps to Earn by Working Online. Social Trade Biz gives services which include likes on Facebook pages, buying products through them, clicking on Ads etc. This help to promote the brand by giving them "Forced Targeted Traffic". That means, people are paid on visit some sites, liking a Facebook page or buying a product. Social Trade part time work had become famous in a very short duration of time. The site had become so famous that it started getting a monthly traffic of about 90 lacks more than popular news sites.

4.4 Security Issues in IoT

The Internet of Things describes an idea that everything on and around if linked by specific way known as low-power lossy networks with the feature of energy conservation and automation then it will be very much helpful to end-user for the purpose of security and privacy .Internet of Things is a term which describes how devices are interconnected via the internet, Security issues in IoT will be to protect the devices connected on Internet. Without compromising the communication speed if several devices will be connected then definitely the devices with sensors will be prominent. And in such case user sensitive information (for example health monitoring) may be stored and communicated, But in such case it will be very important to ensure the security and privacy of the user connected on

it.Adevice, if part of IoT , shall have several stages which comprises of different security and privacy concern and most of things will have manufacturing, installation and operational cycle phase. The probable threats during these three phases are shown as in Figure 1[9]

	Manufacturing	Installation/ Commissioning	Operation
Transport Layer		Eavesdropping & Man-in-the-middle	Eavesdropping & Man-in-the-middle
Network Layer			DoS attack Routing attacks
Physical Layer	Device Cloning	Substitution	DoS attack Privacy threat Extraction of security parameters

Figure 1: Threats throughout life cycle

4.5 Legal Issues in E-Business

It is essential that legal rules are set and applied appropriately to ensure that digital technology does not undermine the basic doctrine of copyright and related rightsIn India, Information Technology Act 2000 is the legislation that deals with the issues related with Internet. It has amended by, Information Technology Act 2008.Identity theft, violation of privacy, sending offensive messages through communication service, breach of confidentiality and privacy, misinterpretation are all covered under Information Technology Act.

5. KEY OBSERVATIONS & SIMPLE PREVENTIVE STEPS

Global companies have the responsibility to deal with some of the legal issues such as how to form contracts, abide by consumer protection laws, create privacy policies and protect databases. "As of now, there is no comprehensive set of laws or regulations that exist for international electronic commerce," says David D. Barr [5]. He added that it is difficult to establish uniform worldwide laws forE-commerce, but some building block legislation within individual countries is necessary. By applying laws and sketching boundaries around the borderless Internet do we negate the term "freedom of information"? How willlegal structure affect international transactions on the Internet? Will it restrict the potential growth of the Internet prematurely? Rapid changes in technology do not allow enforcement of specific laws in cyberspace. For now many organizations are promoting global coordination of legal structures [5]. Some other observations are-

- Need of imposing high ethical values and belongingness among employees so that data breach by internal attack may be minimized.
- The suspicious part in social trade scam is that all the legal documents available on website are on the name of Ablaze and not on Social Trade Biz.
- Social Trade issue is now in court for legal explanation and subsequentaction.
- Forced LIKES on the social media is not the ethical way of product promotion through Digital Marketing
- It seems that the gaps in cyber laws are being exploited in Online Business intelligently.
- One should try link scanner such as URLVoid or MyWOT For suspicious links.
- Shortened links should surely be verified for security.
- One should hover the links prior to click so that full length of URL may be checked whether it is known or unknown to the user.
- More Post more vulnerable to external attacks, so only relevant posting on the net.

6. CONCLUSION

There is a need of reviewing CSR in the context of Online Business practices because earning online is good but not in a suspicious or in illegal way. The level of transparency, disclosure of relevant information should be the prime concern for the organizations involved in online business otherwise the risk of conversion of any online business along with its maturity due to violation of any legal issue knowingly or unknowingly into cyber fraud will be very high within no time. The social media as global platform is free from all the national and international boundaries in terms of communication but not in terms of international business policies in online business context which is also a big barrier in the growth of online business. Therefore through continuous evaluation research and with proper liasioning of these researchers with corporate world into the light of cyber laws, these issues may be properly monitored and regulated. There is a need of cohesive and comprehensive approach in tackling cyber-crimes issues. And it is also the need of empowering the relevant stakeholders with relevant awareness for ensuring the successful convictions of cyber-criminals.

REFERENCES

[1]https://www.statistica.com/statistics/290525/cybercrimebiggesonlinedatabreachesworldwide

[2] Internet Security Threat Report 2014: Volume 19

[3]http://www.abplive.in/indianews/socialtradescamallyouneedtoknowaboutonlinefraudofrs3700cr488405

[4]http://timesofindia.indiatimes.com/city/noida/multiagencyprobeinnoidaponziscamedraidsin3cities/articleshow/56992039.cms

[5] Barr, David D. "The Need of a Broad Standard in Global Ecommerce" *The Internet Law Journal*, Dec. 26, 2000

[6]https://www.scmagazineuk.com/top10issuesinitsecurityfor2014/article/ 545904/

[7]"Law, Ethics and Cyber Crime" Prentice Hall 2003

[8] Garcia-Morchon, O., Kumar, S. Security Considerations in the IP-based Internet of Things , Sept. 11., 2013. http://tools.ietf.org/html/draft-garcia-core-security-06

[9] Chris Lu, Prof. Raj Jain, Security and Privacy issues in Internet of Things, 2014 http://www.cse.wustl.edu/~jain/cse57414/ftp/security/index.html

