

CYBER PHISHING - A THREAT FOR E-COMMERCE AND CONSUMER PROTECTION IN E-COMMERCE

Rajeshwari Suryakanth Nagamarpalli

Alliance University

Bangalore, India

E-mail : rajeshwarinagamarpalli@gmail.com

ABSTRACT

The prevalence of smoothness of technology innovation has seen to have a skyrocket of cyberattacks. Ensuring the protection of personal information is significant about various data privacy laws. Emerging market trends have led to an increase in this field where everything from food to clothes to entertainment is being preferred online. So, this leads to the sharing of one's information online and hence paves way for such frauds.

Keywords: *Cyber-Crime; Cyber Phishing; Identity Theft; Financial Fraud; E-Commerce; Online Banking; Commercial Transactions; Consumer Protection; Emails; Cards; Deceptive Actions.*

INTRODUCTION

E-commerce has brought a big difference all over the entire world. On the contrary, the E-commerce sector in India has had spectacular growth over the past recent years but the E-commerce sector is still facing real and serious challenges. The meaning of E-commerce is the buying and selling of goods and services through an electronic medium by the consumers. The OECD¹ states that E-commerce is a better approach for directing business, qualifying it as business happening over networks that uses non-proprietary conventions that are established through an open standard-setting process, for example, the Internet.

The reason behind the increasing popularity and acceptance of E-commerce all over the world is due to

1. The organization for Economic Cooperation and Development.

a great deal of convenience in commercial transactions with the support of the internet where the seller or merchant of the product can sell his products or offer his services directly to the consumer and the payment for the goods or services offered can be made electronically through various ways, for example, payment through Debit or credit card or net banking. It is because of these conveniences and ease in doing business, the E-Commerce market holds a great deal of value and has increased demand as well as it is expanding very fast and replacing most NonE-commerce transactions in various sectors. E-commerce has already expanded in almost all areas of business and customer services².

With the rapid increase in usage of information and communication technology (ICT), various new branches of law have emerged, which are: Cyberlaw, Cyber Space Law or Information Technology law or Internet law to ensure law and order in cyberspace. A model law on E-commerce (MLEC) was adopted by the United Nations Commission on International Trade and Law (UNCITRAL) in 1996 and the main focus of the Model law on E-commerce (MLEC) was to bring forward a

consistent law relating to E-commerce at a global level to bring Electronic transactions at a standard level with paper-based transactions discovering the rights and liabilities of the executing parties like those of paper-based transactions.

India enacted the Information Technology Act, 2000³ as India was a signatory to the Model Law which was adopted in 1996. Likewise, to give effect the UNCITRAL law on E-Signature (MLES), 2001⁴ India enacted the Information Technology (Amendment) Act, 2008⁵.

It is just the beginning of the E-Commerce revolution in India and will envelop a lot more extensive scope of goods and services on a pan India basis in over a few years from now. E-commerce is generating lakhs of entrepreneurs each year, and that number can add upto lakhs and lakhs annually with a period of a year or two.

• INFORMATION TECHNOLOGY ACT, 2000

Information Technology Act, 2000 was the first law to be enacted by the GOI on E-commerce and the purpose of enactment of the IT Act, 2000 was to put into practice the UNCITRAL Model

2. "The Future of E-Commerce in India: Challenges and opportunities" 1 (12) IJAR 646 (2015) by Rajendra Madhukar Sarode
3. INFORMATION TECHNOLOGY ACT, 2000; Law Dealing With Electronic Commerce And Cybercrime.
4. UNICTRAL, The Model Law On Electronic Signatures (2001)
5. INFORMATION TECHNOLOGY AMENDMENT ACT (2008), further development of IT laws.

Law on E-commerce, 1996. It was then embraced by the General Assembly of the United Nations on 30th January 1997 recognizing the Model Law on Electronic Commerce for a good consideration by the Member States as a Model Law when they order or overhaul their laws, taking into account the requirement for consistency of the law relevant to options to paper based techniques for communication and capacity of information.⁶

The only focus of the IT Act was to furnish a legal recognition to the transactions that were carried out by the mode of E-data interchanges and through some other mode of electronic communication, which is also called E-commerce. The IT Act, 2000 paves a smooth way for E-commerce and E-governance in India. The IT Act holds provisions for legal recognition of E-records and E-signatures, rules for attribution for the E-record, for mode and way of affirmation, for deciding time and spot of dispatch and receipt of electronic records. The Act additionally builds up a regulatory framework and sets down discipline systems for various cybercrimes and offences. Offences such as hacking, breach of confidentiality and privacy and fraud concerning digital signatures were made punishable under the Act. Furthermore, the act provides for civil

liability i.e. for Cyber and criminal violations.

The IPC 1860, The Indian Evidence Act, 1872, and Reserve Bank of India, Act 1934 were also amended to take over the issues related to E-Commerce and crimes related E-commerce⁷.

• INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

To give effect to The UNCITRAL Model Law on E-signatures 2001, India enacted the IT (Amendment) Act, 2008. The act has many known changes including the introduction of the concept of E signatures.

The act also gave specific powers to the state to control websites for protecting privacy and also to keep track of misuse leading to tax evasions. The IT Act also gave legal validation to E-signatures and E-records for the very first time in India and also emphasized securing E-signatures and E-records. These kindsof significant changes were brought forward to decrease electronic frauds.⁸

CHALLENGES AND LEGAL ISSUES FACED IN E-COMMERCE LAW

It is very normal to see disputes between parties when it comes to

6. Supra Note, 7

7. "Law Relating to E-commerce: International and National Scenario with Special Reference to India" 1(2) IJSSEI 7 (2015) by Dr Jyoti Rattan.

8. Supra note 9

commercial relations. Problems or disputes may arise based on the contractual terms and negotiations. Disputes can arise in and out of the contractual terms which may be contractual or non-contractual. Copyright issues and data protection issues are some of the examples of these kinds of disputes. Disputes in the B2C⁹ segment which may be small in monetary terms, still involve problems such as problems in trans-border litigation and choice of law which are not at all convenient for consumers. Some of the legal issue and challenges are discussed hereafter:

ISSUES REGARDING VALIDITY OF THE E-CONTRACTS

The Indian Contract Act, 1887 governs all the E-contracts which are entered online. The acceptance of the terms & conditions before any purchase made online automatically implies a contract between the merchant and the consumer. These kinds of implied contracts are known as “Click-wrap” contracts. Click Wrap contracts mean that any contract is created by clicking on the ‘I accept’ tab. Another form of the well recognized implied contract includes the ‘Browse-Wrap’ Contract which is automatically created by browsing a certain website¹⁰.

As a result, all the provisions under the Contract Act, 1887 would automatically

apply to an E-Commerce Transaction. All the necessary conditions of a valid contract are to be fulfilled as provided under the Contract Act. The necessary conditions which are to be fulfilled to consider a contract valid include free consent of the parties involved, the intention to enter into a legal contract and the capacity of the parties. These conditions can easily be defeated in E-commerce contracts very easily. The terms & conditions in a website have to be in adherence to the Indian Contract Act, 1887 regardless of the agreements such as ‘Click-Wrap or Shrink-wrap’ to enter into a contract recognized by the IT Act¹¹. All these aspects mentioned above are effective only in case of a dispute. Some of the problems that arise out of the E-commerce contracts make a contract void which renders the contract not acceptable i.e. inadmissible as evidence in the court.

Moreover, the E-contracts may be held unreasonable in itself or giving no alternative of negotiation. Then the question that arises here is whether such standard form of contracts is to be considered unreasonable and whether it should be struck down by the court. Such contracts have been opposed by the U.S. courts and have been treated as unreasonable and have been struck down considering the facts and situations of the cases. There are no well-developed laws in India for

9. Business to Consumer

10 “E-commerce Laws In India: Foreign Investment And Retail Trade” 2-3 by Jayanth Pattanshetti Associates.

11. “Evolution of E Commerce in India: Challenges Ahead (Part 2)” 3 by M.M.K. Sardana.

considering the issue of whether online agreements are immoral. On the other hand, there are some legal provisions under the Indian Contract Act which discuss unreasonable contracts like when the object of the contract is averse to public policy. Therefore, The Indian Contract Act does not offer much direction towards these kinds of serious problems.

PROBLEMS OF JURISDICTION IN DISPUTES:

The main constituents of E-commerce are taking orders, managing delivery of the product or service and collect E-payments. When such issues come up in such E-transactions, the complication can be irreparable and should be handled practically. The settlement of disputes in the B2C segment can be quite challenging. The disputes arising in E-commerce are mainly resolved with the physical territory where one or both the parties to the dispute are located. In these types of cases, different kinds of principles are applied when it comes to different national jurisdiction.

The courts have laid down the guidelines to determine the jurisdiction based on the level of interactivity and the commercial nature of the exchange of information that takes place in a distinct jurisdiction. The activities are categorized into three areas:

- a) Completely interactive websites where their consumers buy goods and services, swap details or files or enter into agreements;

- b) Completely passive websites where facts and figures are available as information for consumers to view.
- c) Websites with limited interaction.

In the case of completely interactive websites, the courts mostly take jurisdiction over the out of state entrepreneur except in cases where the entrepreneur has forbidden E-transactions in the state. In the case of completely passive websites, they are not likely to be subject to jurisdiction as they operate from outside the state¹².

Section 3 of the Indian Penal Code, 1896 states that any person who is liable under any Indian law who is going to be tried under any crime committed outside India should be handled in accordance with the provisions of the Indian Penal Code for any crime committed outside India in the same manner as if the crime has been committed inside India.

Therefore, when it comes to cases of E-commerce, there is no proper regulation in India to resolve the issue of jurisdiction.

• ISSUES CONCERNING PRIVACY

While completing any E-commerce transaction, it is almost very difficult to complete the E-transaction without gathering any personal data of the consumer such as the information about the consumer's identity and their financial information. E-Commerce

12. Supra Note 3.

platforms tend to collect a variety of indirect but valuable information such as the preference of the consumers and search patterns along with the collection of primary data from the consumers.

The concept of violation of privacy is dealt with in a very restricted sense under the Information Technology Act. The Act provides that the privacy of a person is said to be violated when images or pictures of their intimate body areas are captured or recorded and published or shared with the permission of the person where the person would have a sensible expectation of privacy. The prescribed punishment for such crimes is imprisonment of up to 3 years or a fine amounting up to INR 2 lakhs¹³.

But under the Information Technology Act, a notification has been issued under Section 43A which states that the Act contains a framework for data protection in relation to personal and sensitive data. The identity of a person is regarded as personal data and the information relating to bank accounts, or data related to payment instrument details often come under sensitive personal information. Due to the notification, obligations were cast for data protection in regard to personal data and sensitive personal data on punishment as given under the IT Act besides making the person liable for monetary reparations. Thus it is asked of the E-commerce platforms to have reliable instruments and arrangements in place so that they can be the legally correct position.

The E-commerce platforms have to protect their systems both internally and externally from any unauthorized intrusion¹⁴.

• ISSUES RELATED TO INTELLECTUAL PROPERTY RIGHTS

One of the prime concerns for any company entering into the E-commerce business is Intellectual Property. The internet is a place with no limited access and a very minimum regulation, so therefore the biggest challenge in the E-business is the protection of Intellectual Property Rights. India has well-established framework for the protection of Intellectual Property Rights in the physical world, but on the other, the effectiveness of these laws and regulations to protect the rights of E-commerce transactions is not that simple.

Another burning issue is the disputes for domain names on which the Indian Law falls silent. A company that starts their business in E-commerce transactions would have to register for their domain name. A domain name in a very basic sense is an address on the internet. In more scientific terms, domain name is an easily distinguishable and significant name to the Internet Protocol Resource. The Domain names generally fall under Trademark law. Two identical domain names can never be registered in the domain name registry but it is possible that it quite possible that similar domain names can be

13. Section 66-E of the Information Technology Act.

14. "E commerce in India, Legal, Tax and Regulatory Analysis, Nishith Desai Associates

recorded. There is no particular law in India on Domain names excluding the judicial pronouncements which state that domain names are subject to trademark protection and are extremely valuable¹⁵.

MAJOR ATTACKS THAT OCCURRED AND RESPECTIVE GRAPHS SHOWING HOW THEY PREVAILED AND LEAD TO DATA BREACH

PAYPAL ATTACK:

- 2019 was a major year for PayPal for all the bad purposes. PayPal phishing shot up exponentially in 2019 after a drop in phishing URLs in Q4 2018, rising 167.8 per cent in Q1 and consistently outpacing its peers for a total of 61,226 phishing URLs found by Vade Secure in 2019.¹⁶
- Everything which happens to exist online comes with a flaw of suspicion from suspicious emails to suspicious websites to suspicious SMS. There is nothing that can be relied on aptly or something which you can trust.
- Phishing on PAYPAL mostly takes place on the weekend as the customers are free then and

tend to shop or use their cards more frequently out for dinner or online ordering of food, etc, which makes it easier for the data breach.

- Now PAYPAL to ensure consumer satisfaction and safety provides for anti-fraud protection, end-to-end payment offerings.

MICROSOFT ATTACK:

- The corporate Office 365 user base of Microsoft makes it a great match for phishing on weekdays when users are in the office and most engaged in email. However, PayPal users include millions of non-business customers who are using the PayPal app. The essence of the business of PayPal means that, unlike business users who can completely neglect email, customers will pay attention to account updates on weekends.¹⁷
- Microsoft Protector for Office 365 also offers simulations to help you recognise and correct phishing threats in your enterprise.¹⁸
- The fraudsters use techniques like social engineering and timely subject lines to attract victims to click the emails and register their

15. "E-Commerce Laws In The Indian Perspective, Sumanjeet

16. PayPal Phishing Hits an All-Time High by Adrien Gendre, 2019.

17. Zoom-Themed Phishing Campaign Targets Office 365 Credentials, <https://www.databreachtoday.com/zoom-themed-phishing-campaign-targets-office-365-credentials-a-14600?>

18. Terranova Security, pedagogical approach to cybersecurity, including gamification and interactive sessions designed to engage users' interests. The simulations are localized for employees around the world and follow the highest web content accessibility guidelines (WCAG).

credentials, which are then captured.¹⁹

- On weekdays, Microsoft primarily faces crimes, as the office operates from Monday to Friday and then valuable details can be collected.

Nevertheless, the study also found that many of these teams lack adequate requirement structures that are a key component of the intelligence process and underpin proper intelligence output.

For policy-makers on cyber-security, the study offers authoritative guidance on:

Top 10 brands - 2019

	Mon	Tue	Wed	Thu	Fri	Sat	Sun	
Overall	2,626	2,542	2,457	2,433	2,371	1,628	1,574	
Microsoft	213	244	244	239	191	59	40	Top 2
PayPal	188	137	144	157	205	165	175	
Netflix	129	117	118	123	112	106	121	Middle 3
Facebook	104	115	130	113	124	119	104	
Bank of America	51	61	53	55	62	54	43	Bottom 2
Apple	33	37	34	36	34	31	28	
CIBC	23	22	25	23	25	23	25	
Chase	20	21	17	32	21	14	11	
DHL	24	25	25	24	21	8	8	
Amazon	11	19	18	16	24	16	19	

AVERAGE OF PHISHING ATTACKS ON ORGANISATIONS ON WEEKENDS AND WEEKDAYS.²⁰

2020 SANS CYBER THREAT REPORT²¹ Shows Need for Better CTI Metrics

The number of organisations that fund full Cyber Threat Intelligence (CTI) programmes show tremendous growth in a recent study from the SANS Institute.

- Optimizing the combination of individuals, processes and resources to produce, ingest and act on information about threats.
- Comprehension and transcending inhibitors that hold back the CTI software.
- Identifying how to access the data

19. Phishing Campaigns Target Senior Executives via Office 365, <https://www.databreachtoday.com/phishing-campaigns-target-senior-executives-via-office-365-a-14214?>

20. Vade Secure for Cyber Security, March 26 2020.

21. 2020 SANS CYBER THREAT REPORT, National Technology Security Centre - Cyber Threat Intelligence Survey.

that will help respond to the most critical cyber threat

Furthermore, it can help save threat analysts considerable time by using automated tools to collect context on threat indicators for faster threat investigation.

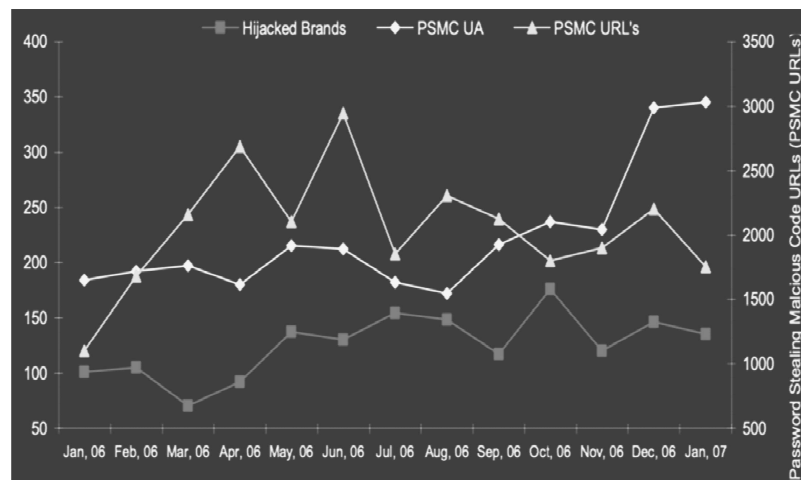
Some phishing attacks have made a magnificent difference:

- In 2016, when hackers managed to get Hillary Clinton campaign chair John Podesta to cough up his Gmail address, maybe one of

outcome of a number of active data breaches.

- Employees at the University of Kansas replied to a phishing email in 2016 and handed over access to their paycheck deposit records, causing them to lose pay.

From January 2006 to January 2007, the statistic shows the percentage of hijacked brands, the number of unique passwords which steal malicious code applications and the number of passwords which steal malicious URLs. While hijacked brands remained



HIJACKED BRANDS, PASSWORD STEALING MALICIOUS CODE APPLICATIONS AND URLs²²

the most consequential phishing attacks in history occurred.

- The “fappening” attack, in which intimate images were made public to several celebrities, was originally assumed to be a result of vulnerability on the iCloud servers of Apple but was the

relatively stable throughout these months, numerous non-traditional websites were hijacked, such as social networking portals and gambling sites. As reported by APWG in the form of malicious code applications and URLs, the above diagram also shows several phishing-based Trojans. In the form of

22. Anti-Phishing Working Group (APWG), KOREAN ENTERPRISE.

malicious code applications and URLs that detect specific identity theft activity, as documented by APWG.

MALWARE DOWNLOAD (soft-targeted emails attack).

These kinds of phishing emails try to get the victim to infect their own machine with malware, like a lot of spam. The messages are also “soft targeted”; for example, they may be sent to an

HR employee with an attachment that purports to be the resume of a job seeker. These attachments are sometimes .zip files or malicious embedded code from Microsoft Office documents. Ransomware, the most common type of malicious code, is 93% of phishing emails are estimated to contain ransomware attachments.

In many distinct ways, phishing emails can be targeted. They are often not targeted at all as we noted; emails are sent to millions of possible victims to try to trick them into logging in to fake versions of very famous websites. The most famous brands hackers use in their phishing attempts have been counted by Iron Scales.

These were the top brand’s attackers used from the 50,000-plus fake login pages the company monitored:

PayPal: Twenty-two per cent

Microsoft: Nineteen per cent

Facebook: Fifteen per cent

eBay: six per cent

Amazon: three per cent

Other times, attackers can send “soft targeted emails to someone who plays a specific role in an organisation, even though they don’t personally know anything about them. Some phishing attacks are aimed at extracting login information from or infecting specific individuals’ computers. Attackers devote even more resources to deceiving the victims, who were chosen because the possible rewards are very high.

CONSUMER PROTECTION IN E-COMMERCE

A report written by the Internet and Mobile Association of India disclosed that E-commerce market in India has almost reached USD 20 billion. Almost all the industries in India have been impacted by the E-commerce Industry, mainly the travel industry and online trading industry. The government of India has encouraged E-commerce platforms on a broad level which turns out to be a promotion of E-commerce activities.

Efforts have been made for the protection of E-commerce as it is global as well as domestic in nature. The relationship between the consumers and the merchants who provide the good or services is governed by the Consumer Protection Act, 1986²³. It is noteworthy

23. Consumer Protection in E-Commerce, 2010, Subhalanga Choudhary

that currently there is no specific act that regulates online transactions. The act has been carefully drafted to build up the confidence of the consumers in law and liability under the act arises only when there is a lack of services or in the case when the goods are defective in nature or in case of unfair trade practices. Any service that is free of charge or cost is outside the scope of the Consumer Protection Act. Liability is triggered depending upon the actual seller who is selling off the goods. The distribution of goods comes under the Ambit of the act. Some of the various defences under the act are enlisted below:

- The defects in the goods will be removed.
- The goods will be replaced if defective.
- The amount spent on the purchased item will be returned in case of any discrepancy.
- Will discontinue any form of restrictive trade practices.

It is prohibited under the Consumer Protection Rules for E-commerce entities as well as merchants selling their products or offering their services from getting into any unfair trading practices while conducting their business. The act in itself provides for an extensive explanation as to what constitutes unfair trade practice. Following are the duties and liabilities under the act to address unfair trade practices:

- ***Prohibition to fake false review and ratings:***

Various market survey's conducted on e-commerce platforms have indicated that consumer reviews and ratings play a very important role when it comes to the customer's decision-making process. Fake reviews and ratings tend to distort the views of the consumers which against the consumer's right to make an informed choice. Therefore the act prohibits any merchant or E-commerce based entity from falsely representing itself as a consumer and rating and reviewing their own products to gain customers.

- ***Authenticity of the product:***

The Consumer Protection Rules direct all E-commerce based entities and all the merchants selling their goods on all e-commerce platforms to make sure that their advertisements promoting their goods and services are uniform with the actual quality of the product.

- ***Prohibition on manipulating the price of goods and services:***

The Consumer Protection Rules restrict any merchant or E-commerce based entities from procuring any unconscionable amount of profit by selling their product at a very high price. It is called engaging in the manipulation of prices of goods and services.

- ***Prohibition to discriminate:***

The Consumer Protection rules also state that no merchant or E-commerce

based entities will discriminate between their customers on the basis of sex, caste or creed. According to the rules, discrimination creates the arbitrary distinction between the customers which directly affects consumer rights.

DUTIES OF E-COMMERCE ENTITIES

- a. All the E-commerce entities will have to provide the given necessary information to its consumers in a very clear and accessible manner:
 - Legal name of the entity
 - Address/location of its headquarters
 - Address/ Location of other branches
 - Name & details of the entity's website
 - Contact information of the entity such as email ID, phone number etc²⁴.
- b. All E-commerce entities are prohibited from getting into any kind of unfair trade practices.
- c. All the E-commerce entities are directed to set up a grievance redressal mechanism and appoint a grievance officer.
- d. All E-commerce entities will have to make sure that the grievance

officer takes up all the consumer complaints within 48 hours and redress it within a month.

- e. If any of the E-commerce entities offer imported goods to its consumers, the entity has to mention the name and relevant information of the importer from whom the goods they're importing.
- f. No E-commerce entity is allowed to charge a cancellation fee on their customers when the consumer has cancelled the goods after purchasing.

CONCLUSION

The fast and increasing growth of the E-commerce business has created a need for a functional regulatory framework that would ensure the success of the E-commerce industry in India. It has always been pointed out that the cyber laws in India are not up to the mark and as there is no proper E-commerce regulatory framework available, there are so many challenges that are being faced by the Indian consumers as well as the e-commerce industries in order to enjoy a consumer-friendly E-commerce environment.

Other than the Information Technology Act, India has no other regulatory framework which governs the E-commerce business in India. Therefore the Government should come up with a

24. Consumer protection E-Commerce Rules, 2020, S.S. Rana & Co. Advocates (2020)

legal framework for E-commerce business in order for the business to grow successfully globally as well as nationally. For the E-commerce business to flourish, the basic rights of the consumers such as the right to privacy, prevention of fraud, intellectual property are to be taken care of. Also, it is an exclusive necessity for a specialized regulation to govern and regulate certain aspects of E-commerce business.

The Consumer Protection Rules a remarkable step towards better digital governance. But the execution of these rules would surge the operational costs of the E-commerce entities including small sellers. Therefore, the implementation of the rules will protect consumers and their interests from unfair trade practices.

RECOMMENDATIONS

- i. When it comes to consumer protection, the areas defining return and exchange, information relating to the product and details about the seller should be specifically mentioned.
- ii. As far as corporations and businesses are concerned they need to have software's which immediately detect cyber-attacks or when their information is being transferred to some other device or website.
- iii. The current use of artificial intelligence can be used as one

of the efficient tools to detect identity theft and the deceptive actions of criminals where a notification can be sent to the user when such activity takes places.

- iv. Cyber cells and authorities need to be more proactive in order to combat this issue.
- v. Stringent laws and punishments for these criminals must be given to deter them.
- vi. 'Sandboxing' of emails can be helped to prevent suspicious/spam attacks.

REFERENCES AND BIBLIOGRAPHY

BOOKS:

- [1] Ammu Charles, E-Commerce laws – Law and Practice, Eastern Book Company, 1st Edition.
- [2] Avatar Singh, Law of Contract & Specific Relief, Eastern Book Company, 12th Edition.
- [3] Paul Todd, E-commerce Law, Routledge-Cavendish; 1st Edition.
- [4] Kamath Nandan, Law Relating to Computers Internet & E-commerce - A Guide to Cyber laws & the Information Technology Act, Rules, Regulations and Notifications along with Latest Case Laws,

- 2012 (Reprint), Universal Law Publishing - An imprint of LexisNexis; Fifth Edition.
- [5] Toshiyuki Kono, *Selected Legal Issues of E-Commerce: 16 (Law & Electronic Commerce)*, Kluwer Law International; 1st Edition.
- [6] Vakul Sharma, *Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce*, Universal Law Publishing - An imprint of Lexis Nexis; Fifth Edition.
- [7] Arpana Vishwanathan, *Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E-Commerce, Cloud Computing And Cyber Crimes*, Lexis Nexis; First Edition.
- ARTICLES:**
- [1] Coteanu Cristina (2005), *Cyber Consumer Law and Unfair Trading Practices*, Ashgate Publishing Company, United States of America.
- [2] Dash, Dipak K and Sarkar, John (2017) Complaints against E-commerce Companies Top List at National Consumer Helpline, *The Times of India*, available at <https://timesofindia.indiatimes.com/india/complaints-against-e-commerce-companies-top-list-at-national-consumer-helpline/articleshow/58781723.cms>
- [3] Hill, Jonathan (2008), *Cross-border Consumer Contracts*, Oxford, Oxford University Press.
- [4] Reich, Norbert (2000) *Consumerism and Citizenship in the Information Society in Consumer Law in the Information Society*, Thomas Wilhelmsson, Salla Tuominen and Heil Tuomola (ed.), The Hague/London/Boston: Kluwer Law International.
- [5] Dalla, H. S., & Geeta. (2013). *Cyber Crime – A Threat to Persons, Property, Government and Societies*. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(5), 997-1002.
- [6] Desk, T. (2015, Aug 19). Ashley Madison hacked: Here's why the website for 'cheating spouses' got targeted. from <http://indianexpress.com/>: <http://indianexpress.com/article/technology/social/ashley-madison-data-breach-why-the-website-for-cheating-spouses-got-hacked/>
- [7] Dhanoa, R. (n.d.). *Cyber Crime Awareness*. *International Journal in Multidisciplinary and Academic Research (SSIJMAR)*, 2(2), 1-7.
- [8] Michael Totty (2002), "E-Commerce (A Special Report)",

- The Wall Street Journal, July, 2002.
- [9] S. D. Vashistha (2005), "Ecommerce in Indian Perspective", The Business Review. March, 2005.
- [10] Holz, Thurston (2005), "On the Economics of Botnets" available online at <http://honeyblog.org/archives/54-On-the-Economics-of-Botnets-Part-2.html>
- [11] Biever, Celeste, (2004), "How Zombie Networks Fuel Cybercrime" New Scientist, November available at <http://www.newscientist.com/article.ns?id=dn6616>.
- [12] Trend Micro, (2006), "Botnet threats and solutions", November, 2006 available online at <http://www.trendmicro.com>.
- [13] Microsoft, (2005), "Spear Phishing: Highly Targeted Scams", Microsoft, Corporation December, 2005.
- [14] Lazarus, David, (2006). "Phishing expedition at heart of AT&T hacking", San Francisco Chronicle, September, 2006. available at www.sfgate.com.
- [15] FCAC, (2006), "FCAC Cautions Consumers About New Vishing Scam", Financial Consumer Agency of Canada, July, 2006.
- [16] Schulman, Jay (2006). "Voice-over-IP Scams Set to Grow", VoIP News, July, 2006.
- [17] KrCERT/CC, (2006) "Korea Phishing Activity Trends Report", Korean Internet Security Centre available at http://www.antiphishing.org/reports/200612_Korea_Phishing_Activity_Report_Dec2006.pdf.
- [18] Dan Ferguson (2006), "Phishing warning Beware e-mails asking for personal info, Peace Arch News", Black Press, November, 2006, available at <http://www.peacearchnews.com/portals-code/list.cgi?paper=44&cat=23&id=746625&more=>.
- [19] Stevenson, Robert Louis B (2005), "Plugging the Phishing Hole: Legislation Versus Technology", Duke Law and Technology Review 0006, 2005.
- [20] Symantec Corporation, Internet Security Threat Report (2006), available at http://www.symantec.com/specprog/threatreport/ent-white_paper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf.

