Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand (Gujarat State, India)

Dr. Archana Chanuvai Narahari[1] & Vrajesh Shah[2]

[1]Dr. Archana Chanuvai Narahari, MCJ, Ph.D., UGC-NET, Asst. Professor, Dept. of Journalism and Mass Communication, Institute of Language Studies and Applied Social Sciences (ILSASS), Affiliated S.P. University, V.V.Nagar, Anand, Gujarat, India.
[2]Vrajesh Shah is currently pursuing Third Year BA in Journalism and Mass Communication from ILSASS, V.V.Nagar Anand, Gujarat, India.

ABSTRACT

With the increasing internet penetration in India and its convergence with digitally supported platforms and gadgets, safeguarding the netizens from the cybercrimes is becoming a challenging task. In addition to, the pinching reality is that the internet users are not getting updated on the vulnerable cyber threats and security issues, at the pace they are getting updated with the usage of internet enabled tools and apps. Thus the current research paper focuses in finding out the answers to alarming questions – "Is the netizen really aware that he/she is vulnerable to various cyber crimes?"; "If netizen is aware, to what extent?", "If not aware of cybercrimes, what measures can be adopted to make the nitzens more aware and updated. The paper suggested a conceptual model explaining how to uphold and implement the awareness programmes among internet users regarding cybercrimes.

Keyword: *Cyber Crime, Internet, Awareness, Netizens, IT Act, Ethical Hacking*

1. INTRODUCTION

Usage of Internet has become a daily routine for majority of people for day-to-day transactions. By end of 2016, there are going to be 462,124,989 internet users in India with a penetration of 34.8% sharing around 13.5% share of World Internet Users (www.internetlivestats.com, 2016). With the increasing internet penetration, safeguarding the netizens from the growing cyber threats is the challenging task that a system should take care of. In India, cybercrimes grew 20% in 2015 over preceding year, while logging an increase of 2,400% over the last decade (The Times of India, 2016). The latest report of the National Crime Records Bureau (NCRB) showed that the number of cyber crime cases increased from 9,622 in 2014 to 11,592 last year with nearly one-third of the crimes committed for financial gain. And there is prevailing criticism that Indian cyber laws are yet to be geared up and updated while comparing with other country laws (Jamil and Khan, 2011).

It is not just the technology of Internet that is luring the users, but the convergence of Internet with various digitally supported platforms and services that make the users hook to it like never before. The recent statistical information on mobile phone internet penetration in India shows that in 2016, 24.33 percent of the population accessed the internet from their mobile phone. This figure is expected to grow to 37.36 percent in 2021 (www.statista.com, 2016).

On a positive note, this unique convergence of digital gadgets like smart phones and internet helps us to communicate with others, family and friends instantly and frequently from anywhere in the world. We abundantly depend on internet provided information quite often either for office chores, e-commerce, banking, weather forecasts, business deals, fitness tips, share markets, entertainment, fun, satisfying psychological urges and emotions, and pass-time activity etc. Upload, share, download, Google it, Apps etc., are treated to be quite common jargons these days that are functioned at finger tips. Hence, it is no exaggeration to say that smart phones and other internet enabled personal electronic gadgets has entered every realm of life and opened gates for cybercrimes to flood in. Lack of awareness on such issues would end up in a severe damage on financial, emotional, moral, or ethical grounds.

Under such dire scenario, besides tackling the cybercrimes, another issue that needs to be focused on higher priority is – creating awareness on "cybercrimes and security" among the internet users. Thus the current study focuses in finding out the answers to alarming questions – "Is the netizen really aware that he/she is vulnerable to various cyber crimes?"; "If netizen is aware, to what extent?", "If not aware of cybercrimes, what measures can be adopted to make the nitzen more aware and updated.

1.1. Understanding the Cybercrime

According to Dhawesh Pahuja (2011) Cyber crimes actually means – It could be hackers vandalizing your site, viewing confidential information, stealing trade secrets or intellectual property with the use of internet. It can also include 'denial of services' and viruses attacks preventing regular traffic from reaching your site. The crimes such as frauds, forgery are traditional and are handled by the separate statutes such as Indian Penal Code or State Level Legislatures (SLL). However the abuse of computer and the related electronic media has given birth to a set of new types of crimes which has some peculiar features. A simple yet sturdy definition of these crimes would be "***unlawful acts wherein the equipment transforming the information be it a computer or a mobile is either a tool or a target or*** both" (Joshi, 2016).

In India the information Technology (IT) Act deals with the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers and Internet. Cyber Crimes in India are registered under three broad heads, the IT Act, the Indian Penal Code (IPC) and other State Level Legislations (SLL). Currently, the Ministry of Home Affairs has issued an Advisory to the State Governments and Union Territory Administrations on Cyber Crime. The State Governments have been advised to put up adequate technical capacity in handling cyber crime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of cyber crimes (Dubbudu, 2016). Several Cyber Cells have been put up pan India to handle exclusively the cases registered under cyber crimes.

1.2. Categories of Cybercrimes

The cybercrimes are not fixed to, or limited to few types that are quite being heard by the netizens, but they are ever evolving with new strategies, thus throwing new challenges to crack down. Given below is the compiled list, updated from various studies (Aggarwal, 2015; Pahuja, 2011).

Crimes against Individuals are done to harm particular individuals. These crimes care like – harassment via emails, cyber-stalking, cyber bullying, dissemination of obscene material, defamation, hacking, cracking, email spoofing, SMS spoofing, carding, cheating and fraud, child pornography, assault by threat, denial of service attack, forgery, and phishing.

Similarly, there are ***cybercrimes done to harm the property of an Individual or Organizations.*** They can be classified as – Intellectual property crimes, cyber squatting, cyber vandalism, hacking computer system, computer forgery, transmitting viruses & malicious software to damage information, Trojan horses, cyber trespass, Internet time thefts, robbery or stealing money while money transfers etc.

Cybercrimes against government are like – cyber terrorism, cyber warfare, distribution of pirated software, possession of unauthorized information etc. ***Cybercrimes that are highly threatening issues at societal level*** are child pornography, cyber trafficking, online gambling and financial crimes.

1.3. What is User Awareness?

User's awareness in this particular context can be referred to the level of attention and knowledge that enables the internet users (netizens) to understand what an Internet is; how it works; its environment and functionalities; do's and don'ts of internet; uses, misuses, its consequences; transactions through internet; vulnerable threats and remedial functions; including other users and governance factors such as laws and regulations. These parameters would enable to predict the levels of awareness and understanding towards cybercrimes and security. The study also made an attempt to analyze how the netizens perceive the overall issue of cybercrime and what exactly it is for them.

2. REVIEW OF LITERATURE

Criminals are taking advantage of the fast internet speed and convenience provided by the internet to perform large and different criminal activities, says Agarwal (2015). In her paper, she insisted that it becomes the duty of all the internet users to be aware of the cyber crime and the cyber law made to deal with cyber crimes. She has also discussed the types of cyber crime, which can help people to identify the crime that they have been victim of.

Parmar and Patel (2016) concluded from their survey that most of the netizens, irrespective of being related to IT field were not able to actively keep themselves updated with the latest information related to cyberlaw and computer security. They felt that the situation could be ever worse among the netizens who are not associated with IT field. They recommended inculcating basis ethics among netizens, while creating awareness on cyber laws in India. A similar kind of result was evidently visible among B.Ed students of Perambalur district, tamilnadu (Singaravelu & Pillai, 2014). Singaravelu and Pillai (2014) felt that this condition should not help them to be successful teachers without knowledge and awareness on cybercrimes.

A similar kind of research is conducted by Mehta & Singh (2013) to study the awareness about cyber laws in Indian society and found that there is a significant difference between the awareness level of male and female users of internet services and it was established that male netizens are more aware of cyber laws compare to women users. In contrary to the above result, a study by Hasan *et al.,* (2015) on ‘cybercrime awareness in Malaysia’ found that female students are more aware at cybercrime and perceived the issue of risk differently compared to male students.

Aparna and Chauhan (2012), analysis on cybercrime awareness in Tricity has revealed that giving more importance to cybercrime awareness can be an efficient tool to decrease or prevent the cybercrimes. It remains the responsibility of the net users as well as the government to ensure a safe, secure, and trustworthy computing environment (Aparna & Chauhan, 2012; Avais, M. Abdullah *et. al.,* 2014).

3. OBJECTIVES OF THE STUDY

- To find out the levels of awareness among internet users regarding cyber crimes.
- To design a framework to uphold the awareness programmes among internet users to curb the cyber crimes and cyber security.

4. METHODOLOGY

The current study is based on both qualitative and quantitative research analysis. To understand the nature and types of cyber crimes prevalent in society and how they are being addressed, the researcher felt it necessary to conduct in-depth interviews with the professional hackers. In the first stage, In-depth Interviews are conducted with two ethical hackers. Researcher adopted ‘Purposive sampling method’ to select the hackers, based on the availability and feasibility of the hackers. For interviewing them the researcher adopted structured open ended schedules. Few of the suggestions provided by them are used in designing the questionnaire for survey.

In the second stage, a survey is conducted on 100 young internet users on the awareness of cyber crimes in the “Anand”, District Headquarters of Anand (Dist), Gujarat. The age of the respondents falls between 17 to 35 years. Simple random sampling method was adopted to select the respondents for the survey. The opinions regarding level agreement are gathered on Likert scale and analysed using percentages.

5. RESULTS AND DISCUSSIONS OF THE RESEARCH STUDY

5.1. Outcome of In-depth Interviews with Ethical Hackers

The experts opined that internet users still lack knowledge and awareness on cybercrimes, pan India. The challenges that cybercriminals throw are becoming tougher day by day and the government has to keep a vigilant eye on the happenings. ‘Unfortunately, there is a huge dearth of cyber experts to handle the issues when compared to number of cases that are being filed in India”, said the expert 1.

“The general assumption prevailing among the common people is that the cyber criminals target only organizations and big shots and why would they bother me. But that is not the ground reality. A common man who uses internet, mobile or have any scope to share their personal transactional details by any means (either by email or by orally) can easily become prey” said expert 2.

Both the experts felt that the security measures taken by banking and companies are not much impactful. “Honestly nothing on internet is safe. Banking verifications and sessions inquiry has been processing but when it is linked with other online website, it can be hacked very easily” opines expert 1. As mentioned earlier, irrespective of safety measures, if an individual is not aware of how to deal with personal information that he/she share in internet or public domains, there is a chance of getting cheated.

The experts delineated on the new trending concept called ‘Ethical Hacking’, which has a great scope to address the concerns related to cybercrimes and to have a secured cyber world. The ethical hackers, on behalf of owners or organizations attempts to penetrate a computer system or networks to counter attack the hackers, to find out security vulnerabilities which can be exploited by the hackers. Thus, the experts in the interview insisted on the role of government in initiate proper mechanisms to train and produce more and more ethical hackers for a holistic approach of cyber security.

5.2. Findings on Internet Usage

- 83% respondents use internet on smart phones quite regularly. 15% people sometimes use internet on smart phones and 2% occasionally.
- A majority of respondents (83%) have their own laptop or PC. 17% people don’t have laptop or computer.
- A majority of respondents (75%) have replied that more than one person uses Internet at home, mostly the siblings. 45% opined that their parents know how to use Internet.
- 95% people use internet daily basis and 2.5 % people use internet in weekly twice and 2.5% people use internet rarely like once in a month.
- 43% people spend their 3 to 5 hours on internet. 37 % people spend 1 to 2 hours of time on internet. 8 % people spend their 6 to 8 hours and 12 % people spend 9 hours or above.
- Most popular activities done on Internet are random web browsing/ casual surfing (95%), instant messaging (80%), e-mail exchanging (93%), watch YouTube videos (87%), play music (75%), social networking sites like facebook (98%)etc.
- A quite good majority (60%) also download games, music and movies from Internet.
- 3% people opined that they don’t have enough knowledge about computer usage. 53% people are moderate in computer usage knowledge and 32% people have high knowledge about computer usage and 12% netizens have claimed that they are experts in using computers.

5.3. Awareness on Cybercrime & Security

- 11% people are not familiar with the term “Cybercrime” and 47% people are somewhat familiar with term ‘cybercrime’, 36% people opined that they are very familiar.
- 75% of people think that cybercrime is political motivated attacks on computer systems of major infrastructures such as airports, power plants etc., to create damage or disruptions.
- Only 15% of respondents understood the technical meaning of cybercrime i.e., **“*cybercrime is a criminal activity or a crime that involves the internet, a computer system or a computer technology*”** and 10% of people though that it is offense involving a computer as the object of crime.

- 43% agreed that Government organizations are more vulnerable to cybercrimes.
- 63% felt financial institutions, like Banks, finance companies etc. Are more vulnerable for cybercrimes.
- 50% said Private sectors are the victims and 10% opted for Educational institutions
- 65% thought there is threat to Law enforcement agencies like police, CBI, courts etc.
- 32 % felt any individual can be victim of cybercrime.
- Regarding awareness on various types of cybercrimes 64.4% people know about *Hacking*. Awareness on other kinds like cyber stalking, Phishing, Identity theft, Cyber Bullying, Tor and deep web crime, mobile hacking, Child soliciting and abuse etc is absolutely less. ***The awareness levels did not cross 9% for any of these serious issues.***
- 79% of respondents know that downloading from illegal torrents and blocked URL is a crime.
- 21% of respondents don't know that downloading from illegal torrents and blocked URL is a crime.
- 56% of people know that accessing block torrents ends you up in jail for 3 years and fine of 3 lakhs of rupees.
- 12% of respondents have heard about cybercrimes from the known people / people of proximity who have personally experienced it.
- ***68% of respondents have not heard about 'Cyber Cells" and literally don't know whom to contact for reporting the cybercrime, other than approaching police.***
- ***Only 15% have referred to IT Act. 43% are aware that IT act deals with cybercrimes, but never referred it or read it. 24% agreed they heard about IT Act, but not sure that cybercrimes are covered under it. Remaining 18% have no idea about IT Act at all (Refer to Figure 1).***

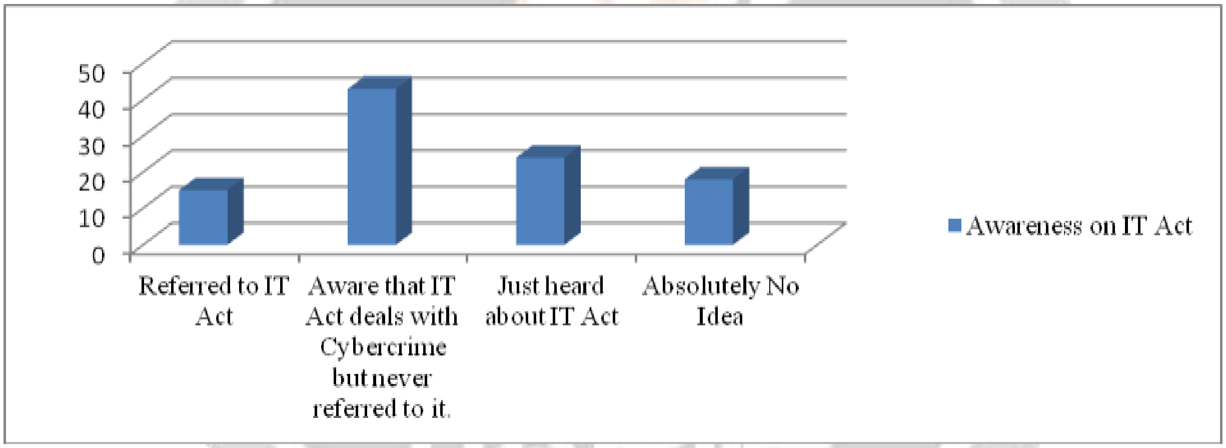


Figure-1: Awareness on IT Act Among Internet Users

5.4. Awareness on Safety while using Personal Computers & Internet

- 55% of respondents have agreed that their PCs are often been damaged by the viruses and other components like data sharing devices and 45% people felt they are safe by installing anti-viruses from time to time.
- 9% of respondents have said their identity has been stolen and 91% of net users said NO.
- 44% of internet users have struggled with spam emails and 56% of people agreed that they can manage with such mails.
- 48% of respondents share their personal details with other persons even they don't know them closely, whereas, 52% agreed they are careful in case of sharing personal information.
- 42% of respondents think that sharing photographs on social networking sties is not a risky activity and 58% felt it's risky.
- 23% of respondents agreed that their social media accounts have been hacked at least once, till date.
- 67% of people often receive phishing emails asking for their sensitive information like mobile no., bank Ac., address etc.
- 51% of people have received phishing phone calls.

- 74% of people restrict from sharing their PC/ Laptop/ Smart phone with others, other than family members.
- Only 14% of people change their password regularly, 51% of people change their password occasionally and 35% of people rarely change their password.
- 17% of respondents strongly agreed they are well protected from various cybercrimes. 35% felt they are protected to some extent. Whereas, 13% of people felt they are not well protected and 35% of people are not sure about protection from cybercrimes (Refer to Figure 2).

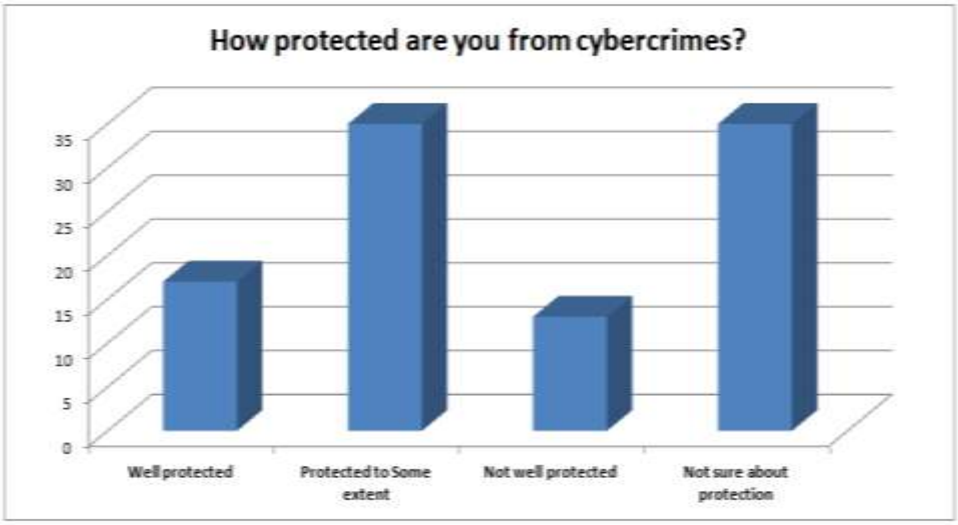


Figure-2: Self evaluation by netizens on how protected they are from cybercrimes

6. CONCLUSION

The study proves that internet users in Anand are not thoroughly aware of cybercrimes and cyber security that are prevailing. A growing net addiction is visible in towns like Anand. The convergence of smart phones and internet are on stride and quite popular. This means, there is more scope for cybercrimes. Though many internet users claim to be aware of such crimes, still majority consider the cybercrime as hi-fi politically motivated attacks on big organizations. They fail to understand that it can affect any internet user. Other than hacking, a quiet majority of users are not aware of crimes like cyber stalking, mobile hacking, TOR and Deep web crimes, copyright violation, cyber bullying, phishing, child soliciting and abuse, sharing disturbing content of pornography, identify theft etc. A significant amount of internet users are not even aware whom to contact or report for any grievances regarding cybercrimes.

The lack of awareness is also observed drastically in case of protection towards their personal PCs and laptops also, as half of the respondents are still the victims of various virus, not been updating their passwords from time to time, and have the tendency of sharing their personal information with others. Regarding the illegal downloads, though the internet users are aware of consequences, still they take this activity for granted and been downloading movies, games and music easily from various torrents. Ignorance on this issue can grow further if the government fails to take serious attempts in implementing the rules and regulations in this regard.

7. SUGGESTIONS

Based on the overall conclusions of the study, and the analysis of the inputs given by experts in cybercrime, few suggestions are observed that can help all the potential victims to safeguard from cybercrimes.

1. Every internet user has a right to be aware of the consequences of its threats and misuses. Hence educating them is on high priority on the issues like:-
   a. Uses and misuses of Internet
   b. Importance of Internet security
   c. Awareness about cyber law and regulations
   d. Impact of technology on crime
   e. Hardware and software requirements to protect the data from exploitation and pilfering.
   f. Knowledge on internet policies at the organizations.

    g. Right to protect the personal data from sharing with others

2. Now a days, Internet users are as young as 8 years old. Hence educating them right from the school has to be accorded importance. Workshops can be conducted in schools for both kids and parents for better understanding on ‘Safe Surfing’ of Internet.
3. The same strategy can be adopted even in colleges. Colleges should take special initiative to incorporate a course work or a paper on “Cyber Crimes and Security” for a professional outlook and can allot credits for clearing the same.
4. Workshops and orientation form experts and ethical hackers are to be encouraged.
5. Web site owners should have a through watch on traffic and check for any irregularities are on the site to avoid the scope of malfunctions.
6. Web site owners should be made aware of their minimum responsibilities in order to adopt some policy for preventing cybercrimes as number of internet users are growing day by day.
7. Web servers running public sites must be physically separately protected from internal corporate network. In order to safeguard the information and data on sites, the corporate authorities can use sophisticated security programmes.
8. Government should bring out more awareness campaigns in various places where the potential net users are high.
9. Mainstream media like television, newspapers, radio and New media platforms like facebook can be utilized to the fullest to make all the netizens aware of various kinds of cybercrimes.
10. Government can collaborate with Ethical hackers to bring out more practical solutions for the prevailing problems.
11. Rules and regulations that deal with cybercrimes should be implemented strictly to make sure that no one is taking the security issues for granted. Strict governance is required so that no one is inculcating the habit of indulging in illegal download and data theft.
12. Number of cyber cells can be increased even in small towns. Every organization should be made aware of the procedure to reach these cyber cells, their roles and responsibilities.
13. Justice to the victims of cybercrimes should be rendered within in specified period with assurance and further guidance on how to tackle such issues.
14. The punishments and penalties to the offenders should be strictly implemented.
15. As cross border cyber crimes are on stride, transparency and coordination between the governments of various countries at international level is highly recommended so that the required actions can be implemented meticulously.

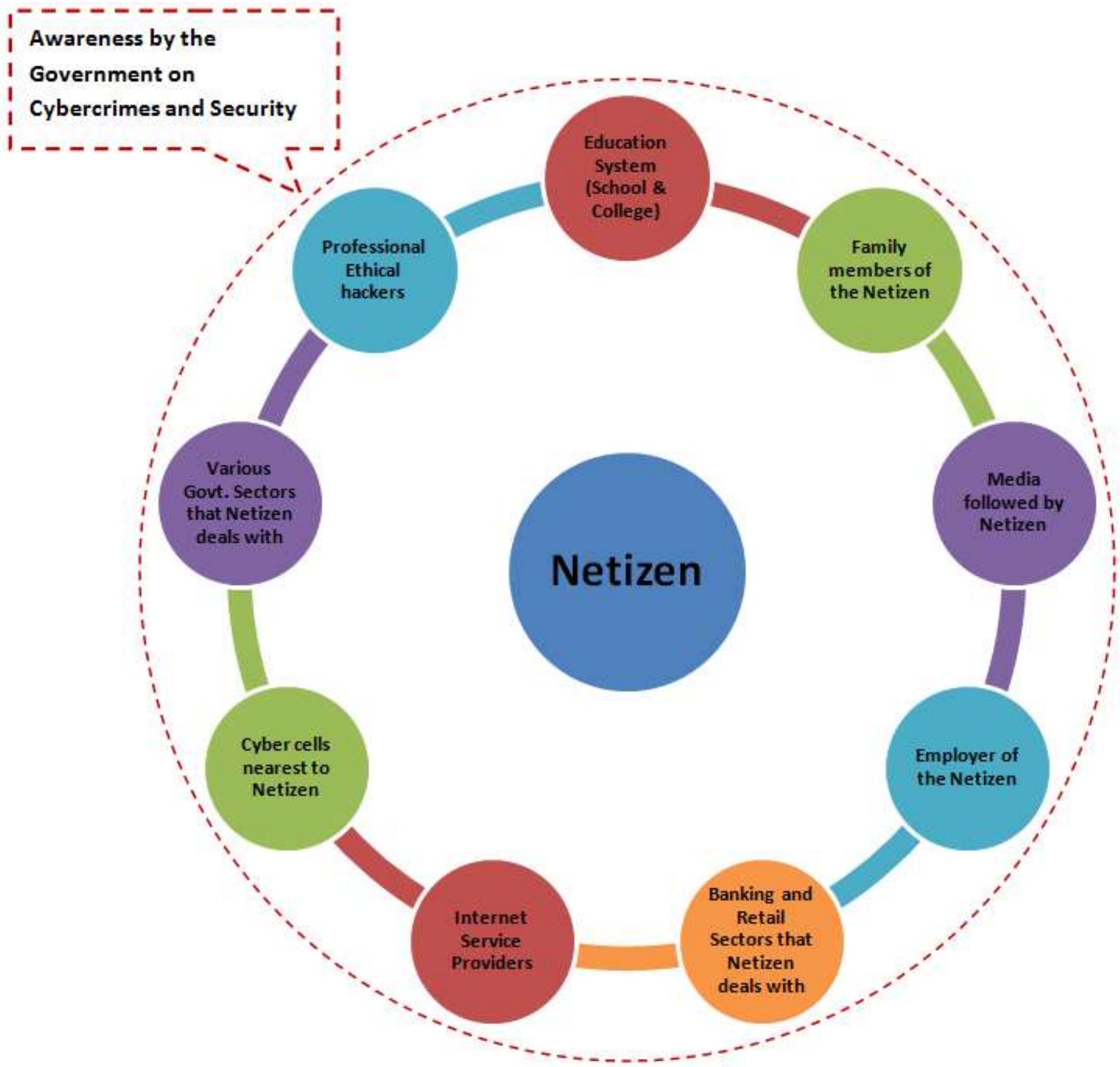
8. A “CONCEPTUAL MODEL” FOR CREATING AWARENESS ON CYBER CRIMES AND SECURITY AMONG NETIZENS

A strong coordination and transparency on issues related to cybercrimes and security should be encouraged between Government, Netizen, and his primary groups and various stakeholders that he deals with. The given below model explains how a normal individual who uses internet (Netizen) is connected with various stakeholders for various transactions and dealings on day to day basis. These stakeholders can be Schools / colleges that he belongs to; family members who use internet at home; Media that he follows; heads of the various govt. and private organizations that he comes across / depends on; banking sectors, retailer outlets and various shopping centres where netizen deals with money transactions; various website owners; Internet service providers; Fellow Internet users etc.

As the dotted red line indicates, the Government can take initiative of creating awareness among netizens and stakeholders at various levels, with multiple approaches, like

- Inform and educate all the stakeholders on cybercrimes and security measures as they deal with general public on a larger scale through internet.
- Informing, educating and altering the netizens through those stakeholders that he deals with by using Internet for various transactions. For instance, the bank can take the responsibility to alert the customer through personal counselling or by providing information when ever required.
- Encouraging cross-flow of knowledge and information between media, cyber cells, ethical hackers and education sectors to reach the netizen in easiest and appropriate way.
- On the whole, the surveillance of the Government should be vigilant on all the stakeholders, and the netizens to make sure that -- the required and updated information and awareness is happening; the rules, regulations and being followed within the crux of cyber laws and provisions; and the netizens is acting safe and secure with proper measures.

Conceptual Model for Creating Awareness on Cybercrimes


Awareness by the Government on Cybercrimes and Security
Education System (School & College)
Family members of the Netizen
Media followed by Netizen
Employer of the Netizen
Banking and Retail Sectors that Netizen deals with
Internet Service Providers
Cyber cells nearest to Netizen
Various Govt. Sectors that Netizen deals with
Professional Ethical hackers
Netizen

9. REFERENCES

1. Aggarwal, Gifty (2015), General Awareness on Cyber Crime. *International Journal of Advanced Research in Computer Science and Software Engineering*, August Vol 5, Issue 8. [https://www.ijarcsse.com/docs/papers/Volume_5/8_August2015/V5I8-0156.pdf]
2. Aparna & Chauhan, Meenal (2012), Preventing Cyber Crime: A Study Regarding Awareness of Cyber Crime in Tricity. *International Journal of Enterprise Computing and Business Systems*, January, Vol 2, Issue 1. [http://www.ijecbs.com/January2012/35.pdf]
3. Avais, M. Abdullah *et.al.*,(2014), *Awareness regarding cyber victimization among students of University of Sindh, Jamsharo*. International Journal of Asian Social Science, Vol. 4(5): 632-641 [http://www.aessweb.com/pdf-files/ijass-2014-4(5)-632-641.pdf]
4. Dubbudu, Rakesh (2016), *Most number of Cyber Crimes reported in Maharashtra & Uttar Pradesh*. Article published on Sep 2, 2016 in -- https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/

5. Hasan *et al*.,(2015), Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. Journal of Social Sciences, Vol. 11 (4): 395.404
6. Jamil D. and Khan M.N.A. (2011), Data Protection Act in India with Compared To the European Union Countries. *International Journal of Electrical & Computer Sciences*, Vol: 11 No: 06.
7. Joshi, S. Mayur (2016), *Full Guide on Cyber Crimes in India*. Article published in “Cyber Fraud Resources”. Journal of Frauds, India Forensic Consultancy Services. [http://indiaforensic.com/compcrime.htm]
8. Mehta, Saroj & Singh,Vikram (2013), A Study of Awareness About Cyberlaws in the Indian Society. *International Journal of Computing and Business Research*, January, Vol.4, Issue. 1.
9. Pahuja, Dhawesh (2011), *Cyber Crimes and the Law*. Article published in LegalIndial.com on July 17, 2011. [http://www.legalindia.com/cyber-crimes-and-the-law/]
10. Parmar, Aniruddhsinh & Patel Kuntal (2016), *Critical Study and Analysis of Cyber Law Awareness Among Netizens.* Conference: International Conference on ICT for Sustainable Development, At http://link.springer.com/chapter/10.1007%2F978-981-10-0135-2_32, Volume: 409
11. Singaravelu, S & Pillai, K. Perumal (2014), B.Ed. Students Awareness on Cybercrime in Perambalur District. *International Journal of Teacher Educational Research (IJTER)* Vol.3 No.3 March.
12. The Times of India (August 31, 2016), *Cyber crimes in India grew 20% in 2015 over preceding year.* [http://timesofindia.indiatimes.com/india/Cyber-crimes-in-India-grew-20-in-2015-over-preceding-year/articleshowprint/53951437.cms?null]
13. www.internetlivestats.com, 2016
14. www.statista.com, 2016