Cyber Crimes, Their Impacts on the Users of Facebook And Prevention from them in the Light of Quran And Hadith

Sheikh Adnan Ahmed Usmani

Lecturer – Computer Science, Sheikh Zayed Islamic Centre, University of Karachi

Dr. Muhammad Shahzad

Assistant Professor Department of Media Studies, Islamia University of Bahawalpur

Abstract:

The internet is a source of mass communication all over the world. Cyber-crime is the most complicated and latest problem in the cyber world. The purpose of this paper is to determine the percentage of how many people exactly know what cyber-crime is, how many people get involved in cyber-crime without knowing that it is a crime, how many users have been victim on Face book because of account hacking. Moreso it aims to evaluate the impact on the users. In this paper after a brief introduction of information technology, cyber crimes, methods, categories of cyber criminals and prevention through government laws and policies, personal efforts in the perspective of Quran and Hadith and impact of cyber crimes on the users of the Face book. Quantitative methodology is adopted to determine the purpose of the paper for primary data. Qualitative methodology is adopted for the prevention for secondary data. 100 Face book users were selected randomly for Questionnaire and an online survey was done to collect data. Pie charts and percentages are used to display the results. The findings disclose that majority of respondents don't know the correct definition of cyber crime and they are not even aware about the laws and punishments for cyber criminals set by the government. Results also indicates that majority of respondents care about the religious values and they don't misuse others' private information. Government laws and punishments are discussed and offered some suggestions by the authors.

Keywords: *Cyber crimes, impact, face book users, prevention, government laws and punishments, Quran and Sunnah*

Literature Review:

Information Technlogy is impeccable. In this world of Information Technology, cyber crime can be considered as one of the evil things which is destroying our society slowly. Information Technology can be and should be used for the enhancement of humankind and society **[1]** and on the other hand the use of the computer for unlawful acts, financial crimes; online fraud and cheating are called cybercrimes. This article sheds light on reasons, modes, and manners of cybercrimes along with the categories of cyber criminals and protection from them. This article is an effort to provide a cursory review of cybercrime in society. This article is based on various reports from news media and news portal.

The present time of fast computing brings a new world known as a cyber world that is an online world where users are doing their personal activities easily and freely.**[2]** Due to the growth of information technology in our daily routine, the entire paper world is completely changed to electronic world. At present criminals have also changed their methods and have started using the latest and modern technology known as cybercrime.

Also with the growth of information technology reading and learning of Holy Quran through electronic mode is increasing day by day. The electronic use of Quran is common nowadays which also involves threats and vulnerabilities of E-Quran and also several forms of cybercrime that are connected to piracy and fraud.[3] There are existing laws related to piracy and forgery and particularly the cyber laws of many countries UAE, Oman and Saudi Arabia but any of the laws of these three countries do not have any clear law to protect E-Quran. Some suggestions are given to have a stronger law for the security of E-Quran. In the end, some case studies related to this research are discussed.

Another example of Cyber crime is breach of privacy and data, In November 2018 due to a cyber-attack 624 customers of different 22 banks lost their money which is 11.7 million in Pakistan. A legal report from the FIA reports that the data of 19,865 ATM cards were sold on a dark web.[4]

According to Islamic Perspective one of the cyber crimes is to consider the ethics in Information and Communication Technology. In an ICT system developer should keep in mind Islamic ethics with ICT ethics while doing their work for the benefits of their work financially and spiritually that the Holy verses or Hadith should be quoted correctly and with references.[5]

Cyber-crime is a worldwide problem that costs billions of dollars and through different ways.An example of Cyber-crime in Nigeria is urbanization, unemployment, the large gap between poor and rich, weak implementation of cybercrime laws and negative role models. So, there is a need for Cyber-crime menace to be minimized if not completely eradicated through government policies which should be strictly implemented on cyber-crime and individual should ensure antivirus protection on their computer system. [6]. Also one of the reasons of Cyber Crimes is the lust for Media which includes social media.[7] The social media is re shaping tool in many ways, by repetition, by broad casting things repeatedly the minds of an individual can be changed which can also lead to cyber crimes as well as cyber terrorism.[8]

Objectives of this Research

The main purpose of this research is to discover the answer of following questions and fulfill some other motives.

- A short introduction of information technology, cyber crime, methods of cyber crime and cyber criminals.
- How many users know exactly what cyber-crime is?
- How many users are being or have been victim by cyber-crime on Face book?
- How many people are doing cyber-crime unknowingly that it is a crime?
- What are the impacts being tabulated on the victims?
- The most important part of the research is to spread awareness about cyber laws and punishments in Pakistan
- To make people aware of its prevention in the light of Quran and Sunnah.

Information Technology:

Information Technology (IT) is the use of computers and other physical devices to save, retrieve, explore, communicate, and operate data, or information, often in the context of a business or other enterprises. IT is considered as a subset of information and communications technology (ICT). IT is playing an energetic role in our daily life. [9]We are depending on IT and we need it at every step of our life. No one can escape from the absolute requirement of technology in our daily routine. The use of technology has made our life easy, fast, and comfortable. At present computer and internet has become very common and crucial for everyone. As compared to 1990, less than 1, 00,000 people were able to access Internet worldwide. According to statistics (Figure 1), 3896 million people

are using Internet. This statistic gives information on the total number of internet users worldwide from 2005 to 2018. As of the most recent reported period, the number of internet users worldwide was 3.9 billion, up from 3.65 billion in the previous year.

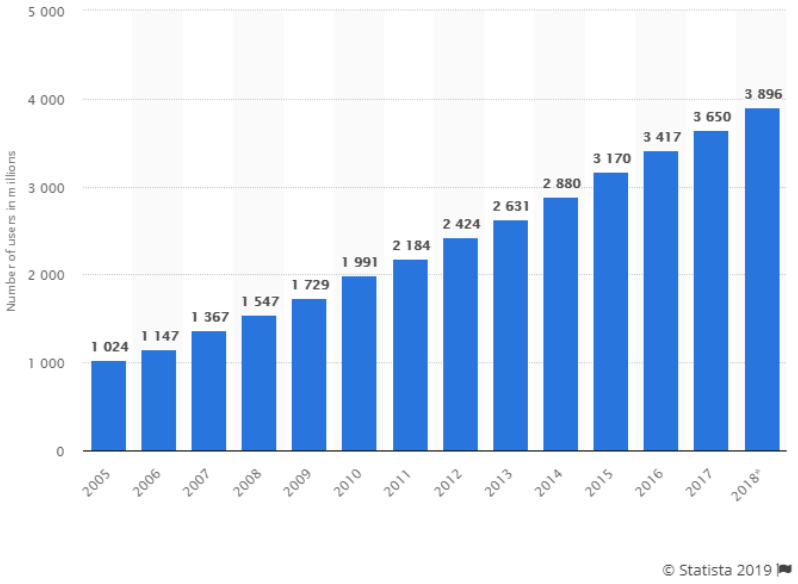

Figure 1

Cybercrime:

There have been several arguments on the definition of Cyber Crime as there is no universal definition for it. [10]As the use of the internet is increasing with the passage of time, criminals have also changed their method of crime and they are using the latest technology known as cybercrime. A crime conducted in which a computer was directly or significantly instrumental. Cybercrime, or computer oriented crime, is a crime that involves a computer and a network. we can define it as "ill-legal act that is committed against individuals or groups with a criminal thinking to intentionally hurt the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly,

using latest telecommunication devices and networks such as the Internet and mobile phones that may lead to a punishment".

There are also problems of privacy when confidential information is interrupted or revealed, lawfully or otherwise. Cybercrime involves illegal activities committed through the internet. Those target the security of computer systems and the data processed by them. It includes fraud, identity theft, hacking, phishing, spoofing, malware, software piracy, pornography, password sniffing, email bombing, salami attack ,data diddling, forgery, cyber terrorism, unauthorized access, bank frauds, online gambling, sale of illegal articles, copyright infringement, intellectual property crime, cyber defamation, logic bomb, Trojan attacks, physically damaging the computer system and cyber stalking etc.[11][12] Sometimes, these crimes cross the borders of countries and involve the actions of other nation states are also named cyber warfare.

Categories of Cyber Criminals

Cyber criminals have various categories and groups. [13] The way of their attacks depends on the objectives that they have in their minds.

Following are some categories of cyber criminals.

- Hunger for Recognition
- Hobby Hackers
- IT professional
- Politically Motivated Hackers
- Terrorist organizations
- Psychological prevent
- Financially motivated hackers
- State sponsored hacking

- Organized criminals
- Former employers seeking revenge competing companies using employees to gain
- economic advantage through damage and theft.

Laws For Prevention Of Cyber Crime In Pakistan

Cyber-law is a connection between technology and law. Pakistan has the largest internet users in Karachi, Lahore and Islamabad; it is no surprise that Pakistan is not free from cyber –crime and some individuals misuse the technology due to their specific purposes. Pakistan's lower house, the National Assembly passed the cyber-crime law called the Prevention of Electronic Act on 11 August 2016. [14]

Laws and Punishments:

There are following punishments according to Pakistani Laws.

1. Three year imprisonment or up to one million rupees in fine or both for spreading the false information publicly or harms the reputation or privacy of the person.

2. Five year imprisonment or up to five million rupees in fine or both for spreading /making the sexually explicit images or videos of a person publicly like to make Photoshop nude images , make video for blackmailing etc.

3. Seven years imprisonment or up to five million rupees in fine or both for making / spreading explicit images or videos of minor publicly for harming the reputation or to blackmail or to create hatred or to take revenge like Photoshop an image of kid , sexually explicit video or images of minor etc.

4. Seven year imprisonment or up to five million rupees in fine or both for produceing or who makes , distributes or sends through the information of a minor (child pornography).

5. Three years imprisonment or up to one million rupees in fine or both for doing cyber stalking like trying to get related with someone online through any communication tool like you are doing something in a manner that other party is harassed out of your actions.

6. Three years imprisonment or up to one million rupees in fine or both for hacking email/ phone for stalking like someone hacking a person for monitoring through electronic communication.

7. Three years imprisonment or up to one million rupees in fine or both for making videos / picture and distributing without consent like take someone's picture or video and post it (without her/his consent) to damage the other party.

8. Five years imprisonment or up to ten million rupees in fine or both for doing cyber stalking with a minor like spying on minors , taking photographs and distributing them without consent, blackmailing etc.

9. Seven years imprisonment or with fine or with both for preparing or distributing the hate speech like write a virus , code which destruct a hard drive , develop a mobile app to spy someone or spread virus etc.

10. Three month imprisonment or up to fifty thousand rupees in fine or both on unauthorized access to information system or data like access to information or data for infringing any security.

11. Six month imprisonment or up to one lac rupees in fine or with both for on unauthorized copying or transmission of data like copies data of flash drive, copy a cell

number, forward someone's SMS to unintended people, hack a website and copy its data etc.

12. Two year imprisonment or up to five lac rupees in fine or with both for interfering or damaging the information system like hacking a website, destroying the content of the server , access of Face book account and delete it , access of email and sending an email from his account etc.

13. Three year imprisonment or up to Rupess one million fine or with both for unauthorized access to critical infrastructure information system or data like hack NADRA's database , intercept a fiber optic cable , hack government of Pakistan website , hack and access to Pakistan stock exchange etc.

14. Three months imprisonment or up to five million rupees in fine or with both for sending spam emails like sending harmful fraudulent emails which may be misleading or illegal.

15. Implementations of three year imprisonment or up to fifty thousand rupees in fine or with both for the commits of spoofing.

16. Two year imprisonment or up to one million rupeesin fine or with both to write , offer , make , distribute or transmit malicious code with intent to harm information system like write a virus, destruct a hard drive , develop mobile app ot to spread virus etc.

17. Seven year imprisonment or up to ten million in fine or with both for spreading information to glorify an offence (relating to terrorism) like post on Face book about Taliban and say that they are good people, they will go to heaven , preachin suicide bombing, supporting terrorists etc.

18. Fourteen years imprisonment or up to fifty million rupees in fine or with both of doing cyber terrorism (copies, accesses or destroys any critical information) to create a panic, fear or insecurity like gain access to back-end system of a mobile company or TV channel and start broadcasting a message that may create panic or fear.

19. Seven year imprisonment or with fine or with both for online recruitment, motivate and invites to fund or plan for terrorism like run a Face book group or WhatsApp group and plan a terror attack or encourage people to fund TTP.

20. Three year imprisonment or up to two hundred and fifty thousand rupees in fine or with both of doing electronic forgery like changing a contract /voice/agreement with intent to gain legal benefits.

21. Implementations of Seven years imprisonment or up to five million rupees in fine or with both of doing electronic forgery of critical infrastructure like electronically changing a contract that may give loss to company.

22. Two years imprisonment or up to ten million rupees in fine or both on making electronic fraud like getting in a relationship with intent to cause financial damage.

23. Six months imprisonment or up to fifty thousand rupees in fine or with both for making, supplying and obtaining device for use in offence like making a software for hacking, writing code for stealing the data , manufacture a phone for planning an attack.

24. Three years imprisonment or up to five billion rupees in fine or with both of unauthorized use of identity information like use someone's email address or call someone and claim a person that you are not .

25. Three years imprisonment or up to five hundred thousand rupees in fine or with both of unauthorized use of SIM cards like selling or offering a SIM card without verifying data.

26. Three years imprisonment or up to one million rupees in fine or with both for tampering of communication equipment like install a spy app that can record calls, SMS or is able to send this data through email to you or someone else.

27. Implementations of two years imprisonment or up to five hundred thousand rupees in fine or with both of unauthorized interception like electromagnetic emissions or transmission.

Prevention of Cybercrimes in the Light of Quran and Sunnah:

Islam is described as "a complete code of life" and it includes ethical conduct, belief, and worship. The corpus of Islamic teachings and laws is called Shari'ah, which provides the ethical foundation of conduct for either the individual or community.**[15]**

Islamic teachings are the light for everyone and should be followed in every aspect of human life. As a Muslim we should act according to Islamic teaching, thoughts and believes in any condition and circumstances. In this era of Modern Technology, IT has been used in Islamic Education as well as with Western Education. Students should be given education about Cyber Crimes and its effects on the lives of an individual as well as on the society.**[16]**

Nowadays we are passing the modern Era that depends on Information technology and it is completely involved in our life. The Web and networks has provided a suitable international background for people to store and send information, work, socialize, communicate, learn, buy, and sell etc that has also opened a door for criminals to access

un authentically to other person's data and information. Islam recommends that all sources of information should be in written form to save them for others or time when required.**[17]**

Islam respects every one's information and privacy and does not allow anyone to spy about other's information or documents, cheat, and control others properties in any form. In this regard Islamic teachings and punishments are very strict and clear for a person who interrupts or steals other properties like information, security, documents, and privacy.

Allah says in Quran:

"Whoever does a wrong will be recompensed for it, and he will not find besides Allah a protector or a helper." Quran 4:123

Information and documentations are viewed in Islam as very significant and valuable assets to gain knowledge and to achieve a successful Islamic society. Islam is very concerned with an effective communications. It reveals that only when a communication is free from any obstacles, the information will be safely conveyed and understood and thus directed to the truth.

Allah says in Quran:

"O you: who believe! Fear Allah and speak a word right." Quran 33:70

The Prophet Muhammad PBUH used to communicate and convey his message effectively with wisdom. He taught his followers to speak nicely and softly. The Prophet had been reported as saying that

" *He who believes in Allah and the Last Day should either utter good words or better keep silence."*

In order to respect the privacy of each Muslim society or community Allah Says in Quran:

"O you: who believe! Avoid much suspicion; indeed some suspicion is sin. And spy not, neither backbite one another." Quran 49:12

Allah again says in Quran:

"And do not consume one another's wealth unjustly or send it [in bribery] to the rulers in order that [they might aid] you [to] consume a portion of the wealth of the people in sin, while you know [it is unlawful]." Quran 02:188

This verse provided the general meaning of fraud where Allah has prohibited Muslims to consume other's wealth unjustly. Therefore, any activities that lead to such action are considered as fraud. Islam forbids all types of fraud and all actions of deceiving, whether the fraud in buying and selling or in any other matter between people. All Muslim are urged to be honest and truthful in all situations in everything they do.

The Prophet had been reported as saying that It is not permissible to sell an article without making everything (about it) clear, nor is it permissible for anyone who knows (about its defects) to refrain from mentioning them. A dishonest act is equivalent to fraud. Dishonesty is one of the worst forms of fraud. A dishonest person is always prone to defraud others whenever and wherever possible. Among the dishonest act or fraudulent activities are embezzlement, misappropriation, misapplication, destruction, removal, or concealment of property, alteration or falsification of paper or electronic documents, including the inappropriate destruction of paper or electronic documents, false claims and/or misrepresentation of facts, theft of an asset, trade secrets or intellectual property, inappropriate use of computer systems including hacking and software piracy, bribery, kickbacks, or rebates, conflict of interest or commitment. Islamic law, being a complete

legal system, seeks to repair the evils and enjoin the order in society in all aspects, including those dealing with protecting goods and security.

Government can set up computer crime laws based on Islam which addresses the individual before the crime is committed and therefore is more of prevention than a cure.

Research Methodology:

There are multiple researches, used in this paper for achieving the perfect conclusion, Quantitative methodology is adopted because it`s a survey based Research, descriptive research is used in this paper because it`s a statistical based research. Casual research is used for evaluating impacts and causes of the cyber-crime. Applied research is used for developing the cyber-crime laws. Qualitative methodology is adopted for the prevention of the cyber-crime.

Sampling:

The population of this study will be one group which consists of hundred persons who use internet and have a Face book account. The researchers were asked twenty questions through Google form they would be randomly selected among Face book users; their ages were less than 30 years old, this procedure made it possible to elicit reliable responses.

Findings

100 face book users participated randomly in this survey those belonged to computer fields and other different fields. Twenty questions were mentioned in the questionnaire in which first three questions were about demography of the respondents like age, gender and profession. The result is displayed with the help of pie charts showing percentages

of respondents in each question.

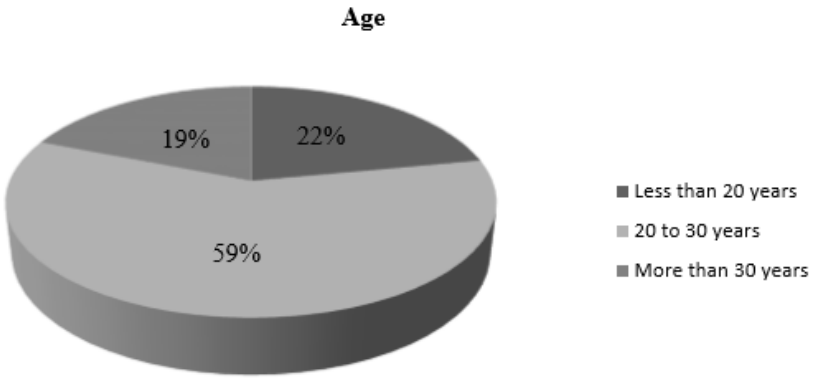

Figure 1

Figure 1 shows that 22% of respondents were less than 20 years while 59% were 20 to 30 years and 19% of them were more than 30 years.

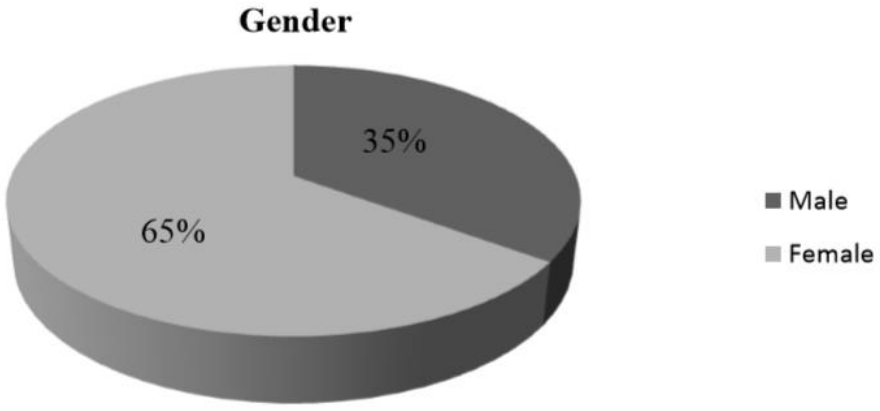

Figure 2

Figure 2 shows that 35% of respondents were male while 65% of them were female.

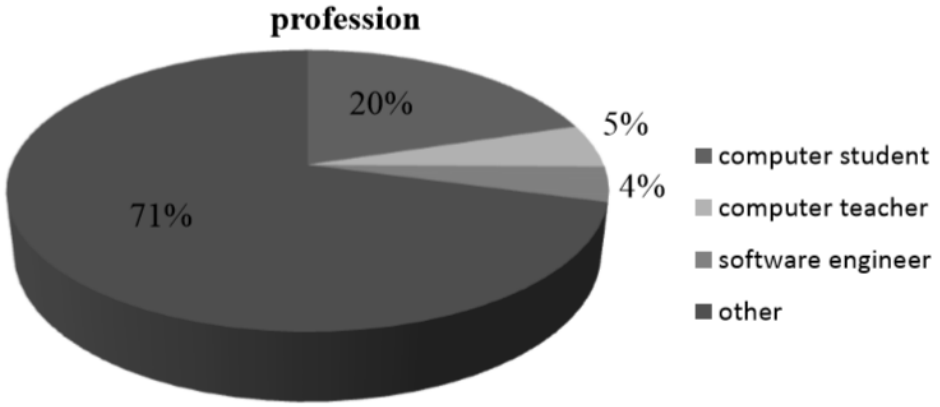

Figure 3

Figure 3 indicates that 29% belongs to computer field either computer teachers or students and software engineer while other 71% belongs to other fields.

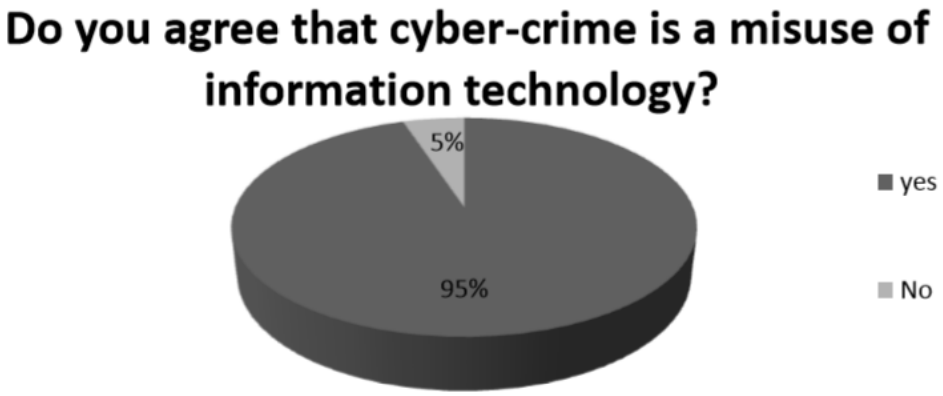

Figure 4

Figure 4 displays that 95% of respondents agreed that cyber crime is a misuse of information technology while other 5% disagreed that shows that they are not well aware about cyber crimes.

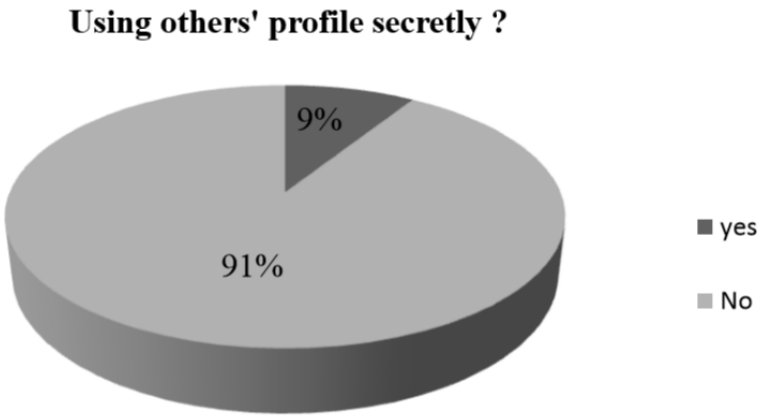

Figure 5

In figure 5, 9% of respondents confessed that they use others 'profile secretly while 91% denied.

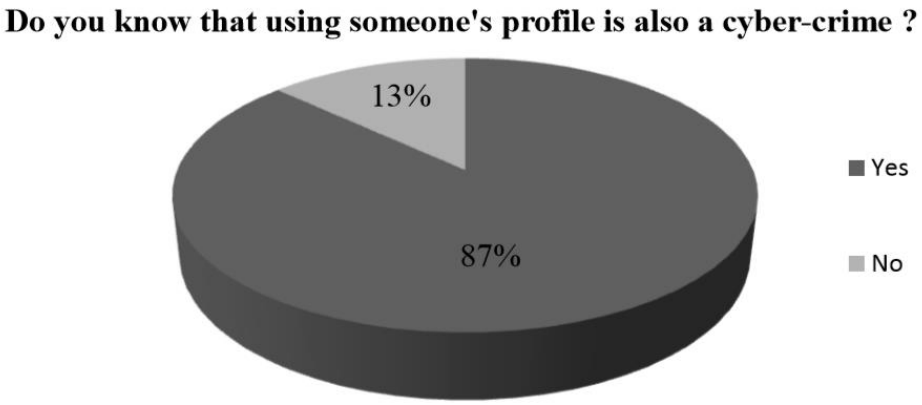

Figure 6

Figure 6 exhibits that 87% of respondents know that using others' profile secretly is also a cyber crime while other 13% of them are not aware about it.

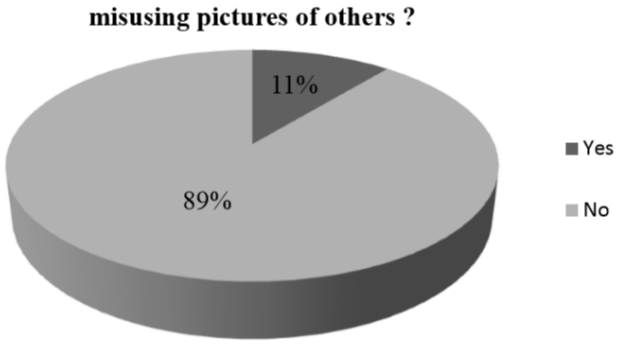

Figure 7

Figure 7 points out that 11% of respondents are involved in misusing pictures of others while other 89% are not involved in this activity.

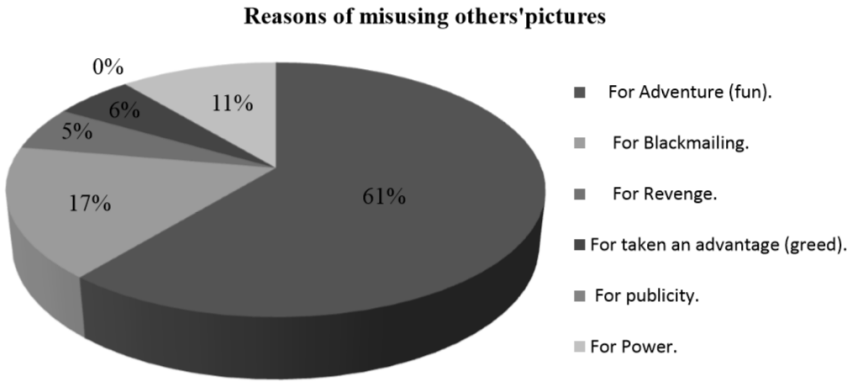

Figure 8

Figure 8 tells us that 61% of respondents just misuse others' pictures for fun while 17% use them for blackmailing.11% use them for power while 6% for taking some advantage.5% use them to take revenge while no one use them for publicity. The findings show that majority of people misuse pictures of others for adventure or fun.

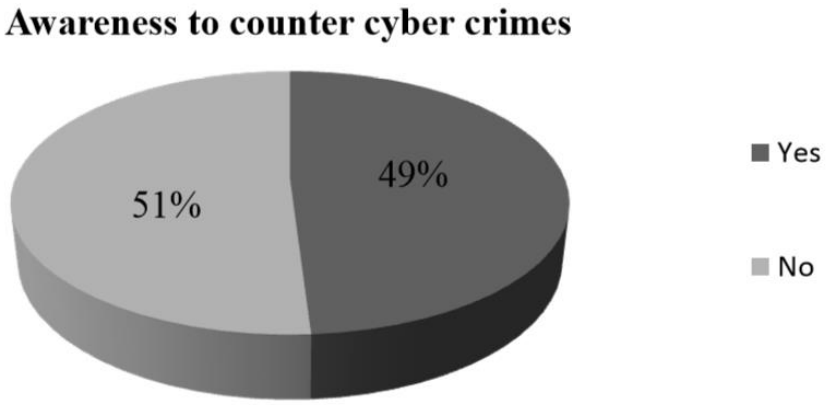

Figure 9

From figure 9 we can know that 49% of respondents know that how to counter cyber crimes while 51% of them are not aware about it.

Figure 10

Figure 10 shows that only 33% of respondents know the laws and punishments of cyber crimes while majority of respondents like 67% don't have knowledge about it.

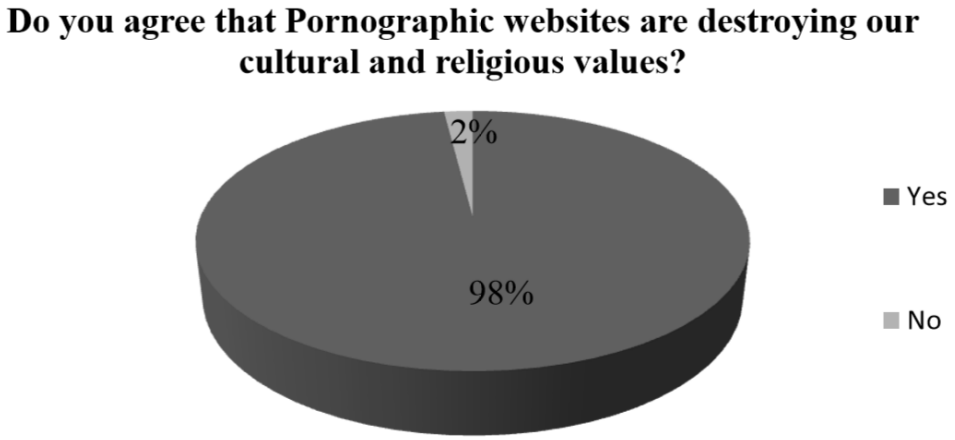

Figure 11

Figure 11 shows that 98% of respondents agreed that pornographic websites are spreading vulgarity among people.

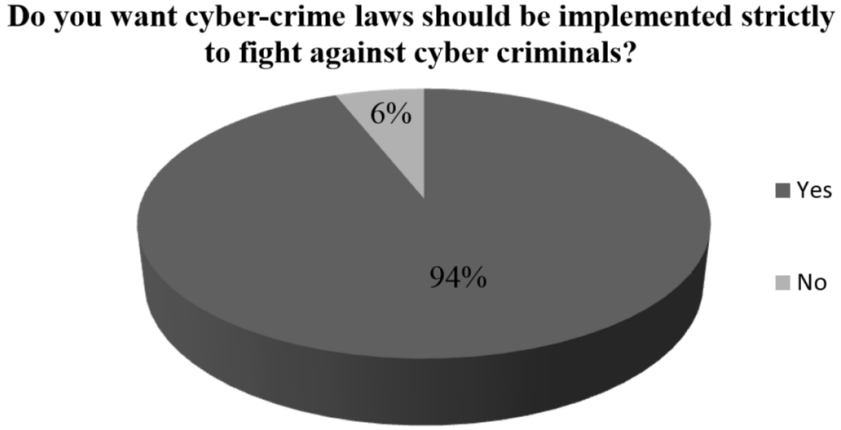

Figure 12

Figure 12 discovers that majority of respondents like 94% want implementations of laws and punishments strictly against cyber criminals.

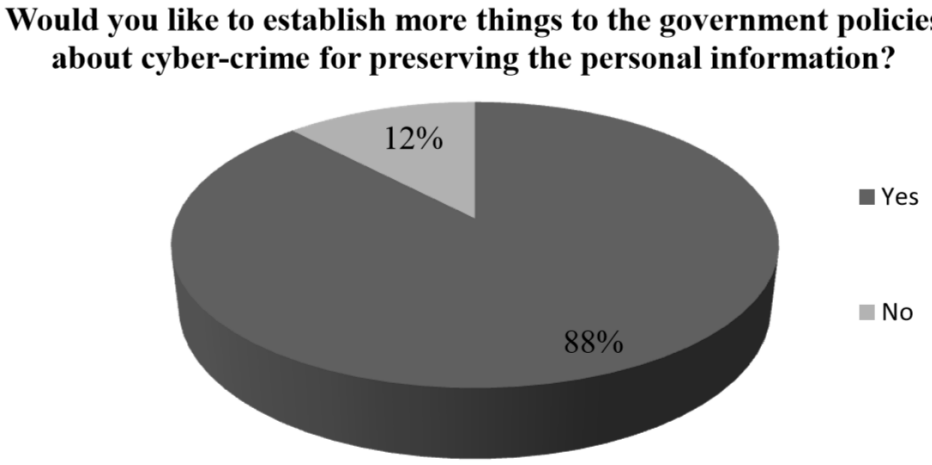

Figure 13

Figure 13 discloses that majority of respondents want more additions in government policies.

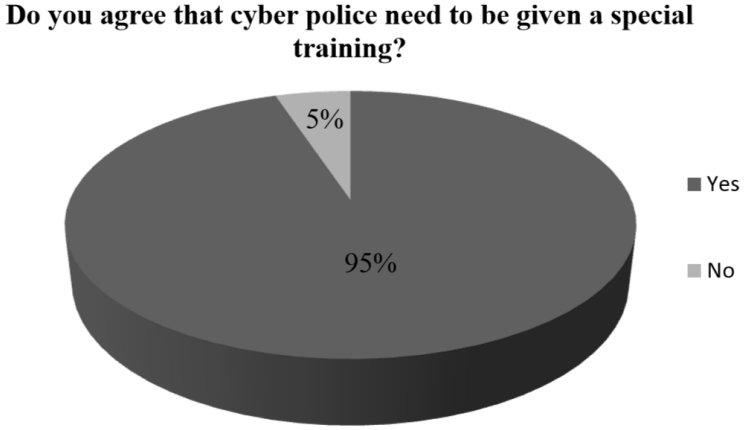

Figure 14

Figure 14 informs us majority of respondents like 95% desire that cyber police need to be given special training.

Figure 15

From figure 15 we get that 36% of respondents faced fraud or cheating in online shopping while other 64% did not face this kind of trouble.

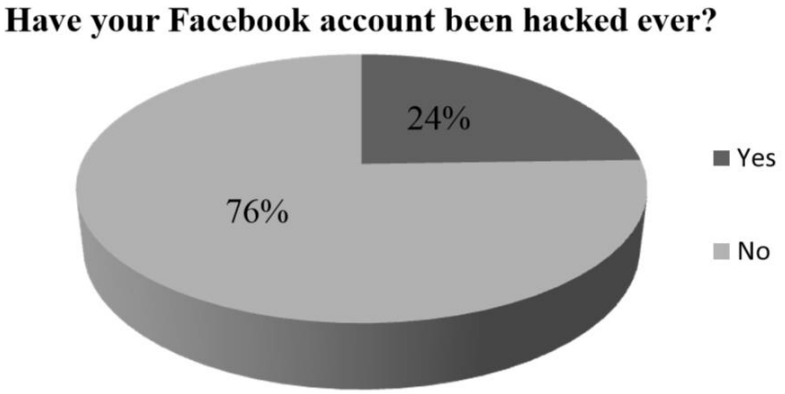

Figure 16

Figure 16 shows that 76% of respondents are not a victim of account hacking while other 24% said that they faced account hacking.

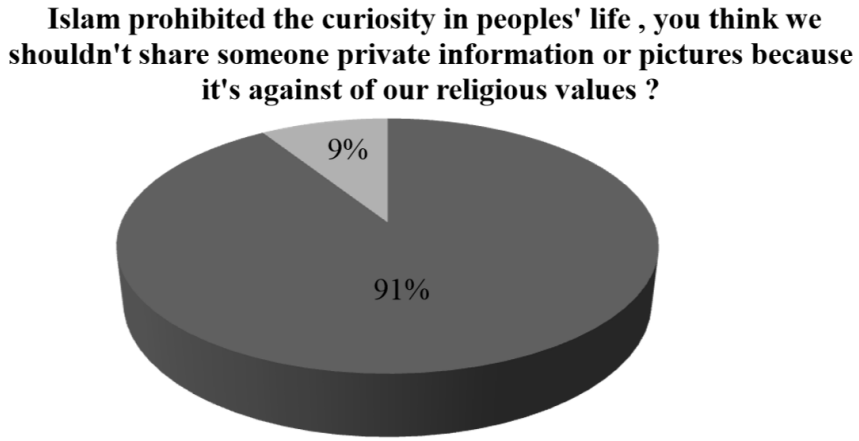

Figure 17

In figure 17 majority of respondents like 91% replied that we shouldn't share someone private information or pictures because it's against of our religious values that indicates that people care about religion and religious values strongly.

When researchers asked the questions from respondents that how would they define cybercrime? Their common answers were it's a computer crime ,hacking, negative use of social sites , misuse of an internet or technology, illegal use of a computer, not different from other crimes, crime by networking, criminal activities through computer via internet and their different answers are severe offence, uncontrollable, , unethical, dangerous, computer is an object of a crime, , cyber bullying , harassment , fraud , fake Face book Id ,invading privacy , technology attack, security lapse of the system designed, to put information at risk , crime which effect human culture of state, use any data without permission , search and misuse other's profile, target and spread computer viruses to other machines. Only 48% people replied and 52% did not reply to this question. Only few respondents identified or define cyber-crime correctly while other did not reply

because they don't know the cyber-crime's definition and other respondents answered wrong.

When researchers asked the question to the respondents that what loss have you faced due to hacking of a Face book account? Their common answers are; the respondents didn't face any loss, they lost personal pictures, lost all contacts, important documents and personal data. The different answers were hacker uploaded pornography, leaked information, leaked pictures, remove all friends' contacts, misuse of messenger, unwanted friend request and did phone calls through Face book, lost password, hacker did bad comments in different pages or pictures and uploaded bad pictures. Only 30% respondents' account has been hacked and they faced a lot of problem due to hacking and the rest of the 70% respondents didn't answer to this question because their account have not been hacked. When researchers asked the question to the respondents that what impacts are being tabulated in the society because of hacking / or any cyber-crime activity? Their common answers were negative impacts are being tabulated such as it affected self-confidence, destroying our youth, culture and society because of misuse of a personal information and blackmailing and trust is being eliminated in the society because of evil activity. The different answers to it were that it had both positive and negative impact. Through positive hacking lots of crime can be stopped by antihackers, stressful environment, youth destroy their education while using computer in wrong activities through spreading and using personal information, feeling unsafe, torture, depression, less self-confidence, non-trust issues, people are scared of making social websites, dangerous impacts because of losing data and misusing pictures by Photoshop, society becomes more destructive because of misuse of a data, death rate is being high because of blackmailing, people facing a lot of troubles and taking tension, bring low confidence , hesitation or person cannot be able to face public, demoralization of personal

lives, cyber criminals take full advantages of the anonymity, secrecy, and the interconnectedness provided by the internet. The impacts are harsh able, stress, violence, money stealing, personal life disruptions, abuse of young generation because of blackmailing, kidnapping etc. Only 43 % respondents answered and 57% respondents did not answer to this question.

Discussion

The primary oal of this article is to identify and prevenet cyber crimes with respect to use of Facebok and other social media platforms in the light of Quran and Sunnah. As per statistics a number of people didnt knew about cyber crime or cyber laws though they had suffered from it. It should be noted that these syber crimes are creating a negative impact on our youth, culture and society. These impacts are stress, violence, robberies, demoralization of personal lives, breach of privacy etc which as a part or whole destroying our society. Cyber laws should be revised and awareness programs should be organized for general public. Specially students from schools, colleges and universities should be made aware of cyber crimes, its causes and prevention.

Suggestions:

- The Pakistani government punishment laws of cyber-crime should be implemented strictly.
- The guide book of cyber-crime should be available for the common users for the awareness purpose.
- Updated latest antivirus software should be used for the protection of the virus attack.
- While chatting on Face book avoid giving personal information or pictures to the strangers, as it could be misused.

- Also avoid adding strangers in face book account and use the privacy settings for securing account.
- Through government policies the self-confidence of the victims of the cyber-crime should be built and maintained the trust of the public must be maintained.
- Facebook administration should create or develop some policies to protect accounts from hackers and misusing.
- Seminars and Workshops should be conducted for students and common people to prevent misuse of their privacy
- Public billboards should be used to spread awareness of cyber crimes.

Conclusion:

Information technology is being used in various fields every day. Criminals found different ways to misuse it and taking illegal advantages from it, that is called cyber crimes. Cyber crimes are computer oriented crimes where computer is used as a target or as a tool for destroying others properties in the form of information or others. There are different methods used for cyber crime by different cyber criminals.

Face book is a great platform to connect people from all around the world where users connect with other people for friendship, chatting, sharing pictures, updating status and doing other activities. Criminals also try to hack face book accounts to misuse and blackmailing that causes stress and violence in society. In order to spread awareness about cyber crimes and their punishments, this study was done that shed light on information technology, cyber crime and criminal, their methods and protection from it by government policies and Quran and Sunnah.

It well defines the impact of cyber crime on the users of face book and their experiences about it. The results disclose that the victims of cyber crimes face a lot of stress and lost

their confidence. The study also confirms that majority of people care about the religious values and they are not involved in these types of illegal activities. These crimes are also like other crimes. Those are not permissible by the governments and in Islam. Governments and Islam both formed some laws for prevention from these crimes. These laws are needed to be implemented immediately to get rid of cyber crimes and teach a lesson to cyber criminals.

References:

1. Doshara, K. 2011. Cyber Crime in the Society: Problems and Preventions. Journal of Alternative Perspectives in the Social Sciences 3(1), 240-259.Retrieved 10 May 2018 from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.452.5880&rep=rep1&type=pdf
2. Kandpal, V., & Singh, R. K. (2013). Latest face of cybercrime and its prevention in india. International Journal of Basic and Applied Sciences, 2(4), 150-156.
3. Khan, N. K. Cyber laws encompassing the Security of E-Quran in Saudi Arabia.
4. https://www.dawn.com/news/1443970
5. Asadullah, A., Yerima, B., & Aliyu, A.Y. (2014). The Ethics of Information and Communication Technology : An Islamic Overview.
6. Hassan, A. B., Lass, F. D., & Makinde, J. (2012). Cybercrime in Nigeria: causes, effects and the way out. ARPN Journal of Science and Technology, 2(7), 626-631.
7. Usmani, S. A. A., & Akmal, Z. (2018). Social Media and Its Impact on Secularism in Society. The Islamic Culture" As-Saqafat-ul Islamia" الثقافة الإسلامية, (39).
8. Furnell, S. M., & Warren, M. J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium?. Computers & Security, 18(1), 28-34.Nurse, J. R. (2018). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. arXiv preprint arXiv:1811.06624.
9. Leidner, D. E., & Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. MIS quarterly, 30(2), 357-399.

10. Mariam Nouh, Jason R.C. Nurse, and Michael Goldsmith. Towards Designing a Multipurpose Cybercrime Intelligence Framework. IntelligenceandSecurityInformaticsConference(EISIC),2016European, pages 60–67. IEEE, 2016.
11. Muhammad Shoukat Malik, Urooj Islam, (2019) "Cybercrime: an emerging threat to the banking sector of Pakistan", Journal of Financial Crime, Vol. 26 Issue: 1, pp.50-60, https://doi.org/10.1108/JFC-11-2017-0118
12. Stabek, A., Watters, P., & Layton, R. (2010, July). The seven scam types: mapping the terrain of cybercrime. In 2010 Second Cybercrime and Trustworthy Computing Workshop (pp. 41-51). IEEE.
13. Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime. An Analysis of the Nature of Groups engaged in Cyber Crime, International Journal of Cyber Criminology, 8(1), 1-20.D
14. Haq, Q. A. U. (2019). Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan. International Journal of Computer Network and Information Security, 11(1), 62.
15. Johnson, T., & Vriens, L. (2014). Islam: governing under Sharia. Council on Foreign Relations, 25.
16. Usmani, S. A. A., & Tabassum, H. (2018). Islamic Education with the help of Information Technology: Advantages and Disadvantages. The Islamic Culture" As-Saqafat-ul Islamia" الثقافة الإسلامية, (40).
17. Zulhuda, S. (2010, December). Information security in the Islamic perspective: The principles and practices. In Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010 (pp. H-33). IEEE.