Global Political Review (GPR)
Vol. III, **No.** II (Fall 2018) | **Pages:** 84 – 97
URL: http://dx.doi.org/10.31703/gpr.2018(III-II).09

GLOBAL Political REVIEW

DOI: 10.31703/gpr.2018(III-II).09

Social Media and Cyber Crimes in Pakistan: Facts, Propaganda, Awareness, and Legislation

Asad Munir* Ghulam Shabir†

- **p- ISSN:** 2520-0348
- **e-ISSN:** 2707-4587
- **ISSN-L:** 2520-0348

Headings

Abstract *Cybercrime is a criminal act committed using computing devices and the Internet. It ranges from downloading pirated movies to destabilizing national economies. Non-financial crimes range from phishing to top-notch crimes such as cyber terrorism. Comprehensive detail of such crimes has been revealed through this empirical study. It investigates the level of awareness, crime sophistication, the extent of the vulnerability, and legislation in Pakistan. Important aspects of cyber laws in Pakistan have been put forth. The survey-based study was carried out on university students. Data reveals that the graduate and postgraduate students being the huge consumers of SNS are at a higher risk of being prey to cybercriminals. Students although they have some information on cybercrimes they have very little knowledge on how to stay safe on the internet. Knowledge of cyber laws such as PECO is desirable to be made a part of the syllabi.*

Key Words: Cybercrimes, Technological crimes, Social Media and cybercrimes, Digital Crimes, New Media Crimes

Introduction

Cyber Crime

"Any activity commissioned via computer, digital devices, and networks used in the cyber realm, and is facilitated through the internet medium. It can include the distant theft of information belonging to an individual, government, or corporate sector through criminal tress-passing into unauthorized remote systems around the world. It includes from stealing millions of rupees from online bank to harassing and stalking cyber users" (NR3C, 2017).

Types of Cybercrimes

Panda Security (2018) divided two categories of cybercrimes i.e. Crimes that target devices and networks and crimes that use different devices to take part in criminal activities. Major types of cybercrimes are:

Drugs Trafficking

Drug traffickers are rigorously using the internet and new media technologies to sell unlawful things through email that are encoded. Some of the drug smugglers or traffickers put the stuff on bargaining at web shopping portals, use chatting messengers and web services to sell illegal medicines, and sell or buy formulas through access to the visit rooms or chat rooms. The increment in Internet drug sales or exchanges might also be ascribed without any close or personal type of exchange of words. Such businesses do not exist in routine markets.

* PhD Scholar, Islamia University of Bahawalpur, Bahawalpur, Punjab, Pakistan. Email: asad.munir@aiou.edu.pk
† Former Chairman, Department of Media Studies, The Islamia University of Bahawalpur, Bahawalpur, Punjab, Pakistan.

Hostile Content and Harassment: The data in websites and other digital means of communications may not be acceptable, foul, or against the assortment of different motives. Once in a while, such correspondences are also needed to be considered illegal. The amount of those illegal interchanges shifts heavily within the center of international locations, and even inside nations.

Electronic Money-Laundering: Electronic money exchange has started to increment aggressively so it has the potential threat that e-exchanges may be captured or interfered with. Credit card numbers are quite simply captured electronically, and physically, the computerized knowledge helped in a phenomenon that a card can be re-developed.

Dispersion of Abusive Materials: There is a huge content of cyber media that might be considered objectionable. It varies in nature such as it can be sexually abusive or explicit material, racism based, political propaganda, ethnic or religious extremist views, and much more. There are several cases in which the people post the personal pictures of their ex-boyfriends or girlfriends to create troubles in their future lives.

Digital tormenting and Cyber Stalking: Digital tormenting is taken as the usage of the Internet and other innovative gadgets to hurt others, in intentional and hostile ways. Digital tormenting may also be explained as "when internet and other electronic gadgets are utilized to disseminate the content or pictorial data to cause damage or to insult someone". Digital tormenting can be of any basic nature such as sending texts or emails to someone who doesn't want to receive your texts or messages however it can involve threats, dangers, physical or sexual assertions, harsh remarks, and publishing falsified explanations as truth.

Stealing Telecommunication: The phone pastors of the last three decades set a perspective for what has transformed into a significant crime industry of this age. Through getting to an organization's telephone switchboard, individual criminals or criminal affiliations can procure access to phone calling circuits and a while later can make their calls or offer call time to outcasts.

Piracy against Copy Rights: This type of robbery has brought on extensive worry to proprietors of the copyrighted material. "The Software Publishers Association" states that programs of billions of dollars have been stolen or pirated through the internet. Similarly, a pirated copy of the latest James Bond Film "The World is insufficient" was available free on the internet before even it was released.

Electronic Extortion and Vandalism: In no time, a western society based on industrialized colonies is connected upon complex data connection and data exchange structures. Any damage to or impedance with any of these systems can incite perilous results. Whether Different individuals and groups have hacked the site pages of various managerial and business firms. Regulatory bodies around the world are widely placing assets into information battling strategy for interfering with the information advancement and establishment of gatekeeper structures.

Digital Terrorism and Warfare: Computerized extortion is a kind of advanced terrorism in which a website, PC network, or email server is subjected by dismissing the routine administrative actions or strikes by insidious software engineers, who demand money to guarantee to stop the ambushes.

While hoping such strikes might transform into the routine in future battling among nations, the thought of the web usage influences and will be balanced by fighting military heads later out of the zone.

Major Techniques of Cybercrimes

- Botnets
- Cyber Stalking

- Malicious Software
- Child soliciting and Abuse
- Ransomware
- Theft
- Identity Theft
- Hacking
- Social Engineering
- DDoS attacks
- Spamming
- Publishing Derogatory Materials
- E-Money Laundering and Taxation

Seven Types of Cyber Criminals

There are seven major types of cybercriminals as mentioned by Batke (2011) described below:

- Script kiddies
- Phishers
- Scammers
- Political/religious/commercial groups
- Insiders
- Hacker groups
- Advanced Persistent Threat Agents

Cyber laws in Pakistan

- "The Telegraph Act, 1885",
- "The Wireless Telegraph Act, 1933",
- "The Electronic Transaction (Re-organization) Act, 1996",
- "Electronic Transaction Ordinance 2002",
- "The Payment Systems and Electronic Fund Transfers Act, 2007",
- "Prevention of Electronic Crimes Ordinance, Pakistan 2007",
- "Prevention of Electronic Crimes Ordinance, Pakistan 2008"

Government's Proposed and Modified "Cybercrime Bill 2015"

There are five major points of Cybercrime Bill 2015:

1. It will be a criminal offense to send messages or photos to anyone's email or mobile phone without the consent of the recipient.
2. The FIA or Police or any other agency will not require a warrant to search, hold, or arrests anyone.
3. Political remarks and expressing political views within in shape of commentary, cartoons, blogs, memes, and caricatures will be considered a crime. It is the Authorities who will decide what is harmful and what is harmless.
4. If the government finds any website of blog inappropriate in any sense, she will block it.
5. ISPs, food places, shops, restaurants or hotels, offices, bus stations, airports, and wherever the internet facility is provided, they will be bound to preserve the usage information for three months.

Crimes and Penalties

As per Chapter I of the new bill, the following deeds are referred to be the cybercrimes and their punishments are given along them:

Sr#	Crimes	Penalties
1	Illegal access to IT networks or data	6 months imprisonment or fine of Rs.100,000 or both
2	Unauthorized copy or transmission of data	Up to six months imprisonment or fine up to Rs.100,000 or with both
3	Criminal Interference with information systems	Up to 02 years imprisonment or fine up to Rs. 500,000 or both
4	Criminally Interfering with sensitive infrastructure information system	Up to 07 years imprisonment or fine up to Rs. 50,00,000 or with both
5	Accessing sensitive information	Up to 03 years imprisonment and a fine up to Rs. 10,00,000 or both
6	Making, providing, or acquiring devices for use in crime	Up to 6 months imprisonment or fine up to Rs.50,000 or with both
7	Illegal issuance of SIM cards	Up to 03 years imprisonment or fine up to Rs. 500,000 or both
8	Identity crime	03 months imprisonment or fine up to Rs. 50,000, or both
9	Electronic forgery	Up to 2 years imprisonment, or fine up to Rs.250000 or both
10	Electronic fraud	02 years imprisonment or fine up to Rs.10,000,000, or both
11	Cyber terrorism	Up to 14 years imprisonment or fine up to Rs. 5,00,000,000 or both
12	Tempering. of communication tools	Up to 03 years imprisonment or fine up to Rs. 10,00,000 rupees or both
13	Offense against the dignity of a natural person	Up to 01-year imprisonment or fine up to Rs. 10,00,000 rupees or both
14	Spamming	Fine up to Rs. 50,000 for the first time
15	Unauthorized interception	Up to 02 years imprisonment or fine up to Rs. 500,000 or both
16	Cyberstalking	Up to 02 years imprisonment or fine up to Rs.10,00,000, or both
17	Spoofing	Up to 03 years imprisonment, or fine up to Rs.5,00,000 or both

"Pakistan Penal Code 1860" will apply to the extent not inconsistent with anything provided in this Act.

Aim of the Study and Statement of the Problem

The study is aimed at providing insight into some comprehensive details of cybercrimes. It further puts lights on the level of awareness on different types of cybercrimes in youth, highlights the sophistication used for such crimes and the ways how people are targeted. Providing general awareness on cyber laws with special reference to Pakistan was the prime motive of the study.

Literature Review

Cybercrimes can be committed in a variety of ways such as a denial of service, stealing information, data diddling, email bombs, illegally getting access to computers or networks, virus attacks, stealing internet time, website hacking, Trojan attacks, pornography of children, violation of privacy, stealing intellectual property, spamming, phishing, terrorism through cyber media, piracy, cheating, fraud, drug trafficking or selling

banned items and hacking, etc. Such crimes are committed for greed, fame, revenge, adventure, power, negative mindsets, etc. (Al-Hamami & Al-Sadoon, 2014).

When we plan how to make legislation for cybercrimes, evaluation of conformance of laws with the CoE Convention is necessary. A global commitment is desirable to make new cyber laws. Just like the WWII, genocide, hunger, nuclear threat, terrorism, cybercrimes seek an equal amount of attention globally to develop a legal framework (Alkaabi, Mohay, McCullagh, & Chantier, 2010).

Most of the anti-phishing software is not user friendly. Anti-phishing software has been capable to find fake websites without any negative motives, however, the usability problems are the reason that customers still fall victim to fraud (Nirmala & Kumar, 2010). People have although got control over the crimes with the help of IT. Globalization has increased the values and showed new ways for information-rich criminals in controlling the information-poor. Access to information sources and SNS may create more threats (Wall, 2007).

Modification of data, network attacks, IP spoofing, denial of service, sniffing, and attacks on network traffic is the increasing crimes especially against the IT industry (EC-Council, 2009).

It has been observed that kids are more vulnerable as they might be exploited by online predators. Educating them on new media technologies and possible threats is necessary while taking preventive measures by their parents, therapists, and law enforcers. The proactive role of ISPs will also play its part in controlling the situation (Bhakare, 2013).

Innocent and curious youngsters are being exploited by cybercriminals intensively. Most of the youngsters who were surveyed responded that they do have online profiles they share their personal information and pictures there. By uploading information of personal nature and talking to people unknown people, they might fall prey or get involved in bad activities such as harassment. On the preventive side, the parents, guardians, and the mentors should maintain open relationship with the youngsters and keep a consistent watch over the cyber activities (Bansal, Sofat, Harsha, & Saluja, 2011).

It is not only the software and websites that are developing, hate crimes are also on the rise. In most of the cases, it is difficult to act against such criminals as their identity is unknown. Legal reforms are required to cope with the law deficiencies. SNS is facilitating some digital mobs who are completely anonymous. It is resulting in extremism (Citron, 2014).

Cybercrimes are the biggest hindrance to diffuse e-commerce and e-government in developing economies globally. Here the governments can play their part in developing control mechanisms and making laws to minimize cybercrimes. It will increase the speed of internet diffusion (Shalhoub & Al-Qasimi, 2010).

Internet criminals can easily guess your passwords today because people are sharing their personal information over social networking websites and it can cause significant financial problems especially our banking system is online today. Things can worsen even and result in physical harm. Interaction over the internet is no substitute for a warm handshake (Trout, 2007). The Internet, if properly exploited, is the modern business tool and financial management resource. In case of a cyber-attack, there will be no one today who will stay safe. The slow law enforcement is the actual problem that needs attention (Vazquez, 2006).

If the new media technologies keep growing, the threat to security information will sustain however the corporations or organizations can institute a system of information security governance to keep safe and secure. Individual users need to keep anti-viruses updated; also should install antispyware malware detection software, do secure online transactions, and keep a consistent look over their activities on the internet (Opala & Rahman, 2013).

Most of the hackers are teen-agers, rivals of businesses, ex-boyfriends or girlfriends, political activists, or professional hackers, etc. Bullets are replaced by bytes. Internet is providing an opportunity for to criminals in making black money or harming people for mala fide objectives. India is the fifth-largest county that faces the greatest number of cybercrimes. Even the IT Act does not help investigate the cybercrimes.

One of the reasons is that cyber forensic facilities are not available. The forensic system is direly required to cope with digital crimes (Kumar, Jha, & Ray, 2012).

Technology plays the main role in a cyber-attack. Cyber-attacks are resembled a missile loaded with a warhead, targeting a system, network, or organization. Illegal access, easiness in exploitation, low complexity, little opportunity, and remote access are the areas where cybercrimes initiate and propagate. Lawyers who are not versed with the understandings of IT cannot comprehend and file the cases accordingly (Villiers, 2011).

A study indicated that 65% of adult internet consumers consider that they have fallen a victim to cybercrimes out of which 75% responded that they are the reason for that. It is a tendency that people mostly do not report to the Police and just inform their banks in case of online monetary fraud. The majority of cyber-attacks are virus attacks or malware attacks that are not targeted to someone specifically, and common people have fewer chances of being a victim to them. Almost 51% of internet users had faced a virus or Trojan attack at some stage. The targeted attacks for example social hacking, bank scams phishing, online frauds, and sexual crimes were faced by very few internet consumers. Most victims feel annoyed and worried, up to 35% felt frightened too (Maniscalchi, 2010).

It is essential to provide the prosecutors and police with the resources, training, and technology to cope with the challenges of cybercrimes as it has emerged as new warfare. Investigative skills should be combined with technical expertise as a unified team. Global cooperation is required to meet up the challenges and act against cybercriminals across the globe. The application of sophisticated investigative methods is the need of the hour and it needs to be adjoined with the expertise of IT professionals. A protracted-term commitment of resources is desirable which assists every single individual user (USAID, 2015).

Pakistanis do not pay much attention to cyber issues such are cybercrimes. They are mostly busy with their routine lives. They are generally not aware of the tools of cybercrimes. Pakistan's role in cybersecurity is almost nothing at all. FIA and other bodies are although trying their best to cope with the situations, but things are getting worse. At least a few features of social networking should not be allowed in Pakistan. It can help reduce the victimization of cybercrimes a great deal (Ahmed & Khan, 2015).

Theoretical Framework

- Social Responsibility Theory
- Social Learning Theory

Social Responsibility Theory

In the middle of the twentieth century, many of the third world and underdeveloped countries used this concept of the press that was associated with "the commission of the liberty of Press" in the U.S. in 1949.

Social Responsibility theory believes in the free flow of information without any censorship on it but at the same time the contents of the media must be mentioned in the public panel and the media organizations or personnel should feel their responsibility towards the society they are living in and should filter their content according to the acceptance level and requirements of the society. It does not believe in external control over media contents but emphasizes that there should be a system of internal accountability. The ownership thence stands exclusive. The concept of social accountability passes the easy "goal" of information reporting to investigative reporting. The speculation helps develop professionalism within the media organizations with the help of establishing a higher standard of professionalism, accuracy, and knowledge. The theory enables:

- Every individual to claim something or express his/her opinion regarding the media.
- Group opinion, customer motion, and work ethics.
- Serious invasion of critical social interests.

- Personal ownership of media can ensure better public service besides of government's take over.
- Media ought to feel the social responsibility and if they do not, the government or other organizations will do.

The theory of social responsibility was associated partially to this study to the extent that social media demands social responsibility from both the regulators as well as the users.

The study engages different implications and aspects of Social Responsibility Theory and emphasizes intensive knowledge of possible consequences and vulnerability while using the internet especially social media. It further highlights the role of public institutions in setting the guidelines and making policies for better, healthier, and safer use of the internet.

Social Learning Theory

Bandura (1977) presented the Social Learning Theory after a series of studies proposing that people can learn from each other. They learn through observation and imitation. They also learn through modeling certain models. This learning is also based on their attention, the amount of memory engaged, and motivational factors behind that. He further suggests that human behavior is a product of different influences that include:

- Cognitive influences
- Behavioral influences and
- Environmental influences

The theory further highlights some characteristics that help achieve effective modeling. These are:

- Attention
- Retention
- Production and
- Motivation

Different aspects of Social Learning Theory relate to the current study such as learning from the society, learning from others, learning about different kinds of cybercrimes from friends, family, social circle, and the internet itself. Awareness and learning are some important components of the current study and social learning theory fits it to a good extent.

Awareness of common cybercrimes such as spoofing, hacking, phishing, tormenting, and cyber terrorism is indispensable.

Research Methodology

Research Design

A survey questionnaire was designed for the respondents. Students were surveyed through a questionnaire.

Population and Sampling Technique

Students of different universities across Pakistan who are users of social media websites and have social accounts were taken as the universe of the study. A randomization technique was used. After randomly selecting four different universities, one from each province, two main strata were defined: Male and Female students. From each university, four different departments were chosen randomly. Undergraduate and postgraduate students in equal numbers (25 each) were selected by at this stage purposely the users of social media. So, a total number of 200 students from each university were selected. It was made sure that there is a minimum of 800 returned questionnaires at least. A total 800 (400 male and 400 female students) had been considered the sample out of the sampling frame.

Variables

- Level of Education (Graduate and Postgraduate)
- Gender (Male and Female)

Research Questions

This study was scrutinized to fetch the answer to the following queries:

RQ1: Is there any significant level of awareness among light and heavy social media consumers about cybercrimes and cyber laws in Pakistan?
RQ2: Are heavy users of social media are more aware of cybercrimes and cyber laws?
RQ3: To what extent are social media users aware of their rights against cybercrimes?
RQ4: To what extent are social media users satisfied with cyber-laws and procedures in Pakistan?

Hypothesis

Individuals, who spend more time on social media, will be significantly more aware of cybercrimes.

Data Analysis

A comprehensive sample of 800 students of HEC recognized universities across Pakistan was drawn from the population. The sample truly represented the population it was withdrawn from, because of the complex methodology used that addressed both randomization and purpose. Students of postgraduate studies and undergraduate studies were given equal representation, as well as based on gender. So, the chances of sampling error were minimized. The sample consists of the university students across Pakistan who belonged to different vicinities, different cultures, and different psychographic backgrounds.

Education Level * Gender * How much the users know about cybercrimes Crosstabulation

How much the users know about cyber crimes				Gender		
				Male	Female	Male
Very greatly	Education Level	Graduate	Count	47	72	119
			% of Total	19.7%	30.1%	49.8%
		Postgraduate	Count	24	96	120
			% of Total	10.0%	40.2%	50.2%
		Total	Count	71	168	239
			% of Total	29.7%	70.3%	100.0%
greatly	Education Level	Graduate	Count	40	40	80
			% of Total	21.7%	21.7%	43.5%
		Postgraduate	Count	64	40	104
			% of Total	34.8%	21.7%	56.5%
		Total	Count	104	80	184
			% of Total	56.5%	43.5%	100.0%
Sometimes	Education Level	Graduate	Count	88	72	160
			% of Total	27.5%	22.5%	50.0%
		Postgraduate	Count	104	56	160
			% of Total	32.5%	17.5%	50.0%
		Total	Count	192	128	320
			% of Total	60.0%	40.0%	100.0%
Never	Education Level	Graduate	Count	24	16	40
			% of Total	42.9%	28.6%	71.4%
		Postgraduate	Count	8	8	16

			% of Total	14.3%	14.3%	28.6%
		Total	Count	32	24	56
			% of Total	57.1%	42.9%	100.0%

The extent of Awareness about Cyber Crimes

As per the data, there are 239 respondents (47 male and 72 female graduates, 24 male and 96 female postgraduates) who are very greatly aware of the cybercrimes while there were 184 students (40 male and 40 female graduates, 64 male 40 female graduates) who answered the question in "greatly". Similarly, there were 320 students (88 male and 72 female graduates, 104 male and 56 female postgraduates) who answered that they are somewhat aware of cybercrimes; while there were 56 respondents (24 male and 16 female graduates and 8 males and 8 female postgraduates) who said they are not aware at all.

Education Level * Gender * How much the users are aware of their legal rights Crosstabulation

How much the users are aware of their legal rights				Gender		
				Male	Female	Total
Very greatly	Education Level	Graduate	Count	16	8	24
			% of Total	13.3%	6.7%	20.0%
		Postgraduate	Count	24	72	96
			% of Total	20.0%	60.0%	80.0%
		Total	Count	40	80	120
			% of Total	33.3%	66.7%	100.0%
greatly	Education Level	Graduate	Count	40	24	64
			% of Total	38.5%	23.1%	61.5%
		Postgraduate	Count	24	16	40
			% of Total	23.1%	15.4%	38.5%
		Total	Count	64	40	104
			% of Total	61.5%	38.5%	100.0%
Sometimes	Education Level	Graduate	Count	79	64	143
			% of Total	27.5%	22.3%	49.8%
		Postgraduate	Count	80	64	144
			% of Total	27.9%	22.3%	50.2%
		Total	Count	159	128	287
			% of Total	55.4%	44.6%	100.0%
Never	Education Level	Graduate	Count	64	104	168
			% of Total	22.2%	36.1%	58.3%
		Postgraduate	Count	72	48	120
			% of Total	25.0%	16.7%	41.7%
		Total	Count	136	152	288
			% of Total	47.2%	52.8%	100.0%

Awareness of legal rights

As per the data, there are 120 students (16 male and 8 female graduates, 24 male and 72 female postgraduates) who are very greatly aware of their legal rights while using the internet and social media whereas there were 104 students (40male and 24 female graduates, 24 male 16 female graduates) who answered the question in "greatly". Similarly, there were 287 students (79 male and 64 female graduates, 80 male and 64 female postgraduates) who answered that they are somewhat aware of their legal rights; while there were 288 respondents (64 male and 104 female graduates and 72 males and 48 female postgraduates) who said they are not aware at all.

Education Level * Gender * Level of satisfaction with the cyber laws and legal procedures in Pakistan Crosstabulation

How much the users are aware of their legal rights				Gender		
				Male	Female	Total
Very greatly	Education Level	Graduate	Count	39	64	103
			% of Total	18.1%	29.8%	47.9%
		Postgraduate	Count	24	88	112
			% of Total	11.2%	40.9%	52.1%
		Total	Count	63	152	215
			% of Total	29.3%	70.7%	100.0%
greatly	Education Level	Graduate	Count	48	40	88
			% of Total	24.0%	20.0%	44.0%
		Postgraduate	Count	64	48	112
			% of Total	32.0%	24.0%	56.0%
		Total	Count	112	88	200
			% of Total	56.0%	44.0%	100.0%
Sometimes	Education Level	Graduate	Count	80	80	160
			% of Total	25.6%	25.6%	51.3%
		Postgraduate	Count	96	56	152
			% of Total	30.8%	17.9%	48.7%
		Total	Count	176	136	312
			% of Total	56.4%	43.6%	100.0%
Never	Education Level	Graduate	Count	32	16	48
			% of Total	44.4%	22.2%	66.7%
		Postgraduate	Count	16	8	24
			% of Total	22.2%	11.1%	33.3%
		Total	Count	48	24	72
			% of Total	66.7%	33.3%	100.0%

Level of Satisfaction with Cyber Laws in Pakistan

The statistics reveal that there were 215 students (39 male and 64 female graduates, 24 male and 88 female postgraduates) who very greatly are satisfied with the cyber laws in Pakistan whereas there were 200 respondents (48 male and 40 female graduates, 64 male 48 female graduates) who greatly are satisfied. Similarly, there were 312 students (80 male and 80 female graduates, 96 male and 56 female postgraduates) who opted for the option "somewhat" while there were 72 respondents (32 male and 16 female graduates and 16 males and 08 female postgraduates) who are not satisfied at all.

Testing Hypothesis with Regression Analysis

$H0_1$: There is no correlation between the time spent on cyber media and awareness of cybercrimes.

R	R Square	Coefficient B	Beta	P
0.649	0.421	0.741	0.649	0.000

It was revealed that 64% of the variance can be predicted from the independent variable. The level of significance (0.05) predicts the value of probability. In this case, the value of P (Probability) was 0.000 that indicates that the null hypothesis is rejected. Beta is the predicted value of relationships between independent and dependent variables. Greater the "Beta" values, greater will be "t-values". If the value of P is less than 0.05, it is indicated as Sig.=0.000 which means that this value is significant enough to approve the alternative hypothesis and reject the null hypothesis with a 95% confidence level.

Thus based on statistical procedures, the research may conclude that there is a positive correlation between the extent of internet consumption and level of awareness on cybercrimes. The value of "R^2 and Beta" is fairly close to "1 (with a reference value of -1 to +1)" indicating a strongly positive relation. The results can the whole population.

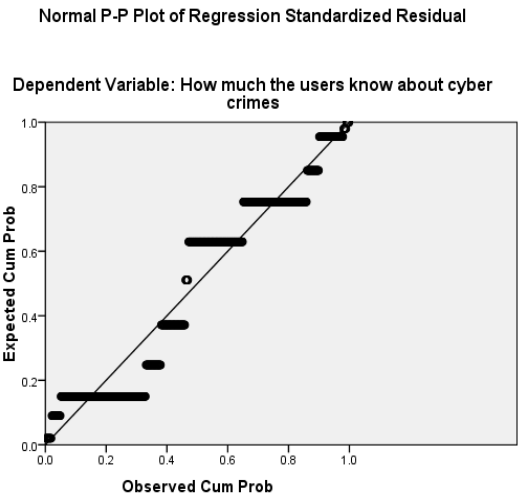

Figure 1: P-P Plot for H1

The scatter-plot is drawn to indicate that the Independent variable is placed on the "X-axis" and the dependent variable on the "Y-axis" whereas a linear representation predicts which way the values of Y are moving if the values of X are manipulated. Overall, the image reflects a strong positive correlation between independent and dependent variables.

Discussion

The findings endorsed that the concept of learning from social institutions in the informal settings as described by Bandura (1977) is validated.

The need of the hour is to engage the key concepts of social responsibility with the new communication patterns as the youth is highly inclined towards the digitized communication; also because the social relations, definitions of society and culture and reliance patterns on social institutions are intensively changing. it is not the same way as Siebert, Peterson, and Schramm (1949) once defined. Overall, the comprehension of the following result may further be correlated to the theories and a new theoretical framework needs to be developed in the coming times. Most of the respondents said that they are aware of cybercrimes vary greatly or greatly while there were very few of them who seemed not aware at all. Many respondents seemed somewhat aware of cyber media crimes. Most of the aware respondents belong to the women. Comparatively, the greatest number of respondents seemed somewhat aware of the cyber laws whereas there was a hopeful number of those who were very greatly or greatly aware too. Males seemed to be more aware of comparatively. Those who said they are not aware at all were 232 in number. There was very low awareness about prominent cybercrimes like Phishing and ID Theft. Most respondents did not know about them at all. Only 311 students said that they know a little bit about these crimes. Slightly over fifty percent of the respondents seemed satisfied greatly or very greatly with the cyber laws of the country while 72 respondents did not seem satisfied at all.

Cyber laws are facing so many issues in implementing them and most important of all is the problem of fixing the legal jurisdiction. Business Crimes in Cyber-age are seriously deteriorating the economies worldwide. Lawyers and investigators need to understand IT and new media technologies to probe the modern-day crimes and they have now such resources available readily as mentioned by USAID (2015). Ethical hacking also needs to be flourished to cope with sophisticated crimes alongside taking cybersecurity measures. Social Responsibility Theory stresses the social role of the media users and media organizations to disseminate and consume the communication channels following their social norms, values, and global acceptance standards.

Conclusion

Both graduate and postgraduate students who are heavy users of social media are more aware of cybercrimes but they lack the knowledge of different techniques that cybercriminals use to target them. Youth, especially university and college students are on relying heavily on social media for information and connectivity and criminals can target them. The level of satisfaction on cyber legislation is not up to the mark and it indicates that there is room for improvement for both enhancing the cyber laws and educating the youth.

References

Ahmed, A., & Khan, D. S. (2015). Cyber Security Issues and Ethical Hacking in Pakistan. *Department of Computer Science Karachi University*.

Al-Hamami, A. H., & Al-Sadoon, G. M. (2014). *Handbook of Research on Threat Detection and Coutermeasures in Network Security: Advances in Information Security, Privacy and Ethics.* Hersley: IGI Global.

Alkaabi, A., Mohay, G., McCullagh, A., & Chantier, N. (2010). Dealing with the Problem of Cybercrime. *Digital Forensics and Cyber Crime: Second International ICST Conference* (pp. 14-15). Abu Dhabi: Springer Science & Business Media.

Bandura, A. (1977). *Social Learning Theory.* Eaglewood Cliffs, NJ: Prentice Hall.

Bansal, D., Sofat, S., Harsha, S., & Saluja, S. (2011, June). Current Trends in Internet Usage and Cyber Crimes against Youth. *International Journal of Cyber Society and Education, IV*(1), 55-62.

Batke, K. (2011, December 21). *7 types of cyber crimes and criminals*. Retrieved March 17, 2015, from Faronics: https://www.faronics.com/news/blog/7-types-of-cyber-criminals

Bhakare, J. (2013). Sexual exploitation of children over the Internet - International perspectives. *SASCV 2013 Proceedings* (pp. 396-399). K. Jaishankar.

Citron, D. K. (2014). *Hate Crimes in Cyberspace.* Cambridge, Massachuetts, London: Harvard University Press.

EC-Council. (2009). *Computer Forensics: Investigating Network Intrusions and Cyber Crime.* Cengage Learning.

Kumar, T., Jha, R. k., & Ray, S. M. (2012, October). Cyber Crime And Thier Solution. *International Journal Of Engineering And Computer Science, I*(1), 48-52.

liao, x. (2006). central asia and china,s energy security. *china and eurasian quarterly*, 62.

Maniscalchi, J. (2010, October 4). *The Human Impact of Cyber Crime*. Retrieved 12 14, 2015, from Digital Threat: http://www.digitalthreat.net/2010/10/the-human-impact-of-cyber-crime/

Nirmala, M., & Kumar, K. N. (2010, September-October). A Survey on Methodologies and Techniques for Detection and Prevention of Phishing. *International Journal of Advanced Research in Computer Science, I*(3).

NR3C. (2015). *Cyber Crime*. Retrieved March 17, 2015, from National Response Centre for Cyber Crimes: http://www.nr3c.gov.pk/cybercrime.html

Opala, O. J., & Rahman, S. M. (2013, September). Corporate Role in Protecting Consumers from the Rist of Identity Theft. *International Journal of Computer Networks & Communications, V*(5), 19-33.

Panda Security. (2018, August 20). *Types of Cybercrimes*. Retrieved from Panda Security: https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/

Shalhoub, Z. K., & Al-Qasimi, S. L. (2010). *Cyber Law and Cyber Security in Developing and Emerging Economies.* Edward Elgar Publishing.

Trout, B. J. (2007). *Cyber Law: A legal arsenal for online businesses.* World Audience Inc. .

USAID. (2015). *Cyber Crime: Its impact on Government, Society an the Prosecutor*. Retrieved December 16, 2015, from USAID: http://pdf.usaid.gov/pdf_docs/Pnada641.pdf

Vazquez, C. I. (2006). Cyber crime, the internet and its impact on the business enterprise and the role of the technology manager. *Capstone Project, University of Denver*.

Villiers, M. d. (2011). Enabling Technologies of Cyber Crime: Why Lawyers Need to Understatand IT. *Pittsburgh Journal of Technology Law and Policy*, 01-53.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age Crime and society series.* Cambridge: Polity Press.