International Journal of Modern Research in Engineering and Technology (IJMRET)
www.ijmret.org Volume 4 Issue 1 ǁ January 2019.

Awareness level and victimization on Cyber-crime among Mehran University (MUET), Jamshoro, Sindh, Pakistan

Farhan Abbas[1], Tariq Jamil[2], Ali Arsalan[3],Mahaveer Rathi[4]
[1, 2, 3,4]Department of Computer System Engineering Mehran University of Engineering and Technology, Jamshoro

Abstract: To study the scenario of cybercrime victimization at the Mehran University of Engineering and Technology, the details of Jamshoro are ironic. Although cybercrime victimization implies the abuse of fundamental rights and gender based persecution, almost no serious steps have been taken to stop this. Most Internet service providers and social networking sites take into account cyber cultures and cyber rules and regulations that can create opportunities for personal freedoms, especially freedom of expression as well as privacy rights. There is a system of social values at the Mehran University of Engineering and Technology in Jamshoro, which follows the consent of the cybernetic culture, which can lead to several violations of fundamental rights guaranteed by our Constitution. Internet users need to understand that what is offensive in real space should be maintained as offensive in cyberspace. Cyber socialization has opened the door to a global village that can shape its own culture, rules, and ethics, but in no way should it encourage the abuse of personal rights and freedoms. In this work we have studied the cause and effects of implications of cyber security awareness and its governess in practical organization users, specifically the internet using community (i.e. faculty, staff and students) of MUET as test based. Our aim is to check the awareness level of the users under consideration and to investigate the weakness of awareness as well as the deployment of cyber security rules and policies within the organization under observation i.e. MUET finally upon getting results of users experiments. (Which is performed thought the survey, questionaries' and practical use of respondents' recommendations). So our target was to deploy a useful cyber security policy within MUET. Observed, analyzed, tested and recommended the cyber security policies in recent era. The results of this research mimic to convey these rules and regulations.

Keywords: *Cyber Crime, MUET Jamshoro*

I. Introduction

In Pakistan, there is no electoral law adopted for the development of data, unlike other countries. It is worrisome that the level of cybercrime is growing due to ignorance. Cyberbullying is still a type of exploitation that does not occur on the spot. This happens through computer technology. This can happen to intentionally damage the victim's or the assembly's bad reputation. Cybercriminals are comparable to common criminals. The aim of cybercriminals is to acquire cash as quickly and effortlessly as allowed, and the same phenomena are considered for habitual offenders due to the lack of information about laws dealing with illegal digital activities in Pakistan and exploit human rights for the most part People do not show up for strength. Thousands of people are regular Internet users in Pakistan, who are often part of the Internet because of their experts, their individual needs or their training (Nawaz Brohi, 2012).Students who are the future of the nation are also aware of all forms of cybercrime. Simply put, cybercrime is any fraudulent activity in which a computer is used as a tool, goal, or method to perpetuate additional crimes that are subject to cybercrime (Nawaz and Rukshanda, 2012). The last and perhaps the most difficult problem in the cyber world. Cybercrime is more repulsive than ordinary crimes. Cybercrime is very different from ordinary crimes. Any criminal activity that has become a computer as a tool, purpose or means to perpetuate such crimes is part of a cybercrime. To protect themselves from cybercrime, users must constantly know how to reduce the amount of such horrific crimes. Consciousness means knowing or understanding a topic, problem or situation and providing knowledge about changes in this environment. (Gunjan and Etal, 2013).

Many researchers made their suggestion regarding on this issue. (Saravade and Saravade, 2003) suggests need of appropriate training and awareness. (Poonia, Bhardwaj and Dangayach, 2011) suggests a hi-tech technology enabled security system and along with user's awareness. (Cambell, Sherman, Birchmeier, 2001) found men expressed more difficulty and recognition about internet privacy, yet they engage in more unstable behaviors that did females (Govani and Pashley, 2009) learnt awareness of the suggestions of privacy when operating Facebook and found about 40% were restrict in sharing personal information but the rest was sharing confidential information (Connolly,(Maurushat, Vaile, Dijk, 2011) found the awareness of child are mostly influenced on parent's consciousness.

Pakistan is victims of various cybercrimes "online gambling, financial crimes, cyber pornography, illegal articles selling, electronic email spamming, crimes of high-profile equipment, cyber chasing, counterfeiting, unauthorized access PC system networks, virus/ trojan horse attacks, good judgment bombs, trojan attacks, internet time robbery, robbery of facts contained in digital shape, password cracking and buffer overflow". But there are no appropriate measures to solve the problems. Pakistan compares cybercrime with traditional crime and describes the possibilities of cybercrime's style and goals and international culture of cyber-safety (possibly and ultimate 2015). It discusses Pakistan cyber laws and indicates that you. Almost cybercrime should foster international relations to enhance network security and personal development. Some other investigations specialize in cybercrime in Pakistan, which provided wider access to the network in the United States. Approximately 10.6% of the population in 2009 had acquired the right to enter the internet at the time of 2009, which was 0.1 percent. They define cybercrime as any illegal act using computer as a tool or subject of the crime and predict that it will continue to increase in the country as long as network subscribers continue to increase and information remains easily accessible. Therefore, the government responsible for security should pay undue attention to this type of crime. Although current research widely suggests the existence and life of cybercrime in Pakistan, it no longer provides data on these crimes, it is a gap found in most research on the subject (Shabnam et al. 2016).

II. Cybercrime

Pakistan has no selective enactment committed for data engineering contrasted with India. It is worrying that due to lack of information, the level of electronic exploitation is increased. Electronic victimization is the form of exploitation that does not occur in the eyes. This occurs through online computer technology or other electronic or programming devices. This may occur to purposefully hurt the notoriety of victimized person or gathering. Cybercriminals are comparable with customary offenders. The point of Cyber offenders to acquire cash as fast and effortlessly as could be allowed and the same phenomena is considered for customary lawbreakers (Williams, 2015).Due to the lack of information about laws related to illegal digital activities in Pakistan and the exploitation of people's rights, most people do not come to power. Many of people use the Internet frequently in Pakistan, who are often elements of the Internet because of their need for specialists, individuals or training. Similarly, we can expect the Internet with a minimum of specialized instructions and awareness. In Pakistan, a service called the National Cyber Crime Center, which is calibrated by the Federal Investigation Agency, is convenient, but the focus in the latter is a request that can be investigated. (Turanovic et. al, 2016).

III. The aim and objectives of the research

In Pakistan, cybercrime and exploitation in the internet had remained a subject of extraordinary fear, however needs mindfulness. Strange blend of nature of assaults constantly changing patterns of the exploitation, constrained information about immediate laws, which address cybercrimes in Pakistan and privileges of exploited people in instances of digital assaults, help enormously towards shaping an irregular methodology to digital exploitation situation. There are a great many web clients in thought now who are frequenting the internet all the time for expert, business, standardizing and education purposes. In this research, we will choose a case study of MUET, Jamshoro for awareness of cyber-crimes and its prevention for victimization.

a) To identify awareness extent of victimization.

b) To propose a model to minimize cyber victimization at MUET, Jamshoro.

c) To give policy recommendations to the stake holders.

IV. Purpose

Persons, because of their status and position can't perpetrate criminal acts in physical space have propensity to carry out wrongdoing in the internet. Because of absence of discouragement element, adaptability in personality variable, the internet gives the decision to wrongdoer to carry out Cyber Crime.

In Internet, conduct of guilty party is liable to be foreign made to physical space. Discontinuous wanders of guilty parties into the internet and the element spatio-transient nature of the internet give the opportunity to escape. The internet may prompt unite outsiders in physical space to perpetrate unlawful acts. A gathering of individuals having normal reason or enthusiasm toward Physical space might prone to unite to perpetrate unlawful acts in the internet. Persons having a place with shut society are more prone to perpetrate criminal acts than fitting in with open society in the internet. 8. Standards and estimations of digital and physical space may prompt (Cyber-Crime).

V. Design of survey instrument

The choices to various questions were designed in such a manner so as to cover the widest possible responses and ensure complete data capture. The questionnaire was designed in such a manner that the respondents could complete the questionnaire for a time pressed respondent in an average minimum time of 4 minutes. Efforts were taken to limit the number of questions in the questionnaire and the resulting number of questions was 35. There were a total of 35 questions in the survey, of which 1-12 questions were used to obtain socio-demographic profiling, three about modes, frequency of access and typical activity, one about student involvement in Social Networking, one question each about hacking, defamation, cyber bullying, two questions about possible piracy violations, two questions about pornography, and a question in the form of a match the following consisting of 5 questions to observe the awareness of various types of cyber-crimes. All the questions were multiple-choice questions. The questionnaire avoid open responses.

VI. Data analysis

The questionnaires that were returned by the respondents were screened for discrepancies and the data from complete questionnaires was entered into a database. Utmost care was taken to avoid data entry errors. The statistical data obtained from the survey responses are entered into the SPSS 17.0 software for statistical evaluation. It also combines the grouping of records into appropriate groups, identifying family members by variables, noting the patterns and the importance of their appearance.

VII. Limitations of the study

A quandary of this survey is that the researchers do not genuinely recognize if the respondents are completely honest in their solutions. There is also no gender differentiation in this survey. This survey is a convenience survey. It is possible that the responses aren't consultant of larger population of college students, even though the look at does have fee because it offers insights into how aware university students of Mehran University of Engineering and Technology are of cyber-crimes. Another limitation is the non-random pattern strategies used within the selection of the respondents. Destiny studies should use an easy random sampling approach, this can offer room for inferences and generalizations.

VIII. Result and Discussions

(i) Awareness Level

Table1. Level of awareness at MUET, Jamshoro

Awareness Level		
Faculty Members	63	40%
Staff	51	33%
Students	42	27%

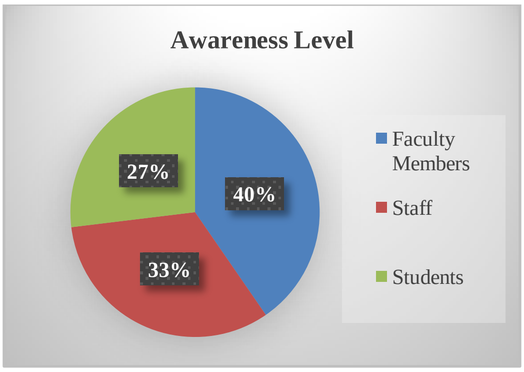


Fig 1. Awareness level

From Figure.1 we can see the awareness level of MUET internet users. Survey was taken from minimum 100 respondents. 40% Faculty members have knowledge about cyber security at MUET, while lower staff have less knowledge as compare to faculty members that is 33%. Students have only 27% knowledge, so we need to aware the students as much as possible through arranging seminars and workshop to increase the awareness level of students.

(ii) Knowledge of cyber security at MUET, Jamshoro.

Table 2. Knowledge of cyber security at MUET, Jamshoro

Knowledge of cyber security at MUET, Jamshoro.	**Yes**	**No**
Are you using internet on MUET domain?	70	30
Do you have mail account on MUET domain?	70	30
Do you read MUET IT policy guidelines from MUET website?	45	55
At MUET campus using campus Wi-Fi	52	48
Are you using IEEE or other research site?	65	35
Do you agree / disagree blocking of Facebook, torrent or other sites	75	25
Do you notice hacking / password store software are installed in labs / libraries computers?	80	20
Are you using your personal laptop?	45	55
Are you satisfy with MUET internet speed?	40	60
Are you satisfy with MUET internet security?	75	25
Do you access digital library, books, notes, videos tutorials or other teaching material at MUET website or domain.	60	40
Are you using proxy server to bypass restriction.	30	70
Are you using proxy server to bypass MUET restriction.	20	80
Posting your photos or videos at social networking sites	72	28
Posting your personal correct information	65	35

at social networking sites.		
Posting you cell no, Skype or other information at social networking sites.	55	45
Do you have any knowledge about internet securities?	50	50
Do you know Prevention of Electronic Crimes Act, 2015?	45	55

Knowledge regarding cyber security, people responded in this manner that only 70% using internet on MUET domain while 30% don’t use internet services of MUET. 52% people using campus WI-FI. 45% people using their own laptop while 55% people using desktop computers in the labs and offices. 72% people sharing their photos and videos at social networking sites. From the survey report 35% people don’t give personal information on the social networking sites. 40% people according to survey report are satisfied from MUET internet speed so information and communication processing center (ICPC) should work on that for speed up the internet services in Mehran UET Jamshoro. Few users using proxy server to bypass the MUET restriction. 75% people are agreed to block the Facebook in the MUET domain.40% peoples don’t take advantage from online digital library, notes and other services. From the above results 65% people using IEEE and other use full research websites. Its very alarming situation that 50% people do not have knowledge about internet security system, people should be aware about that, recently cyber criminals attacked on different banks of Pakistan. Only 45% people know about Prevention of electronic crimes Act-2015.

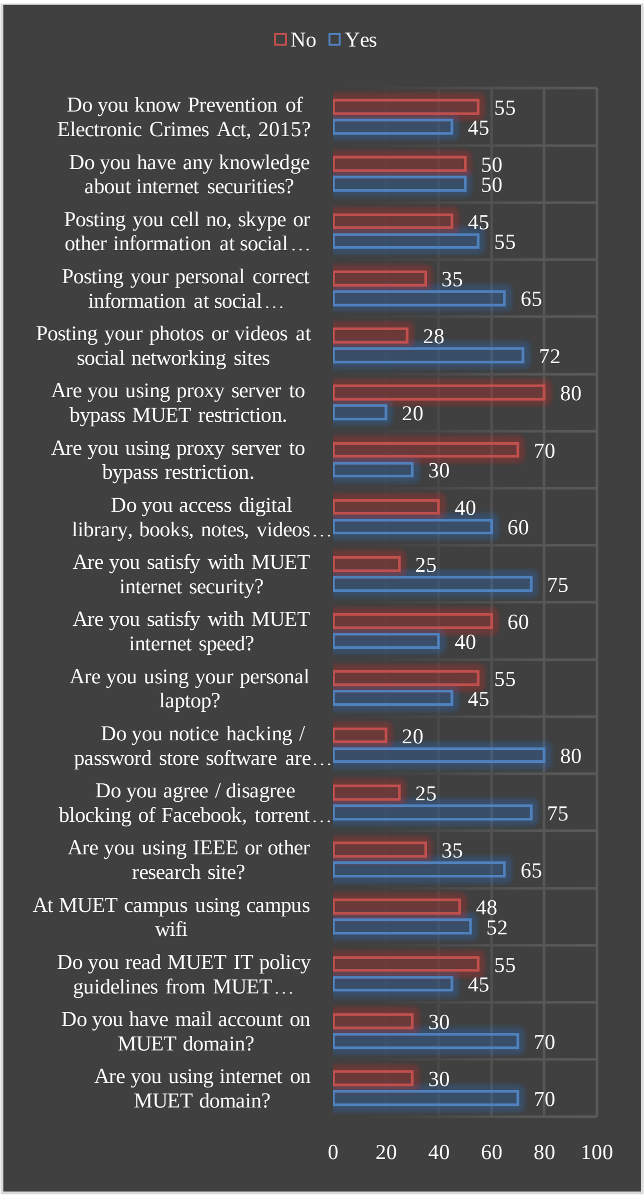


Fig 2. Knowledge of cyber security at Mehran University of engineering and technology

(iii) Knowledge of victimization at MUET, Jamshoro

In this part examine the respondent’s data on victimization and information about it for an advertising tool.

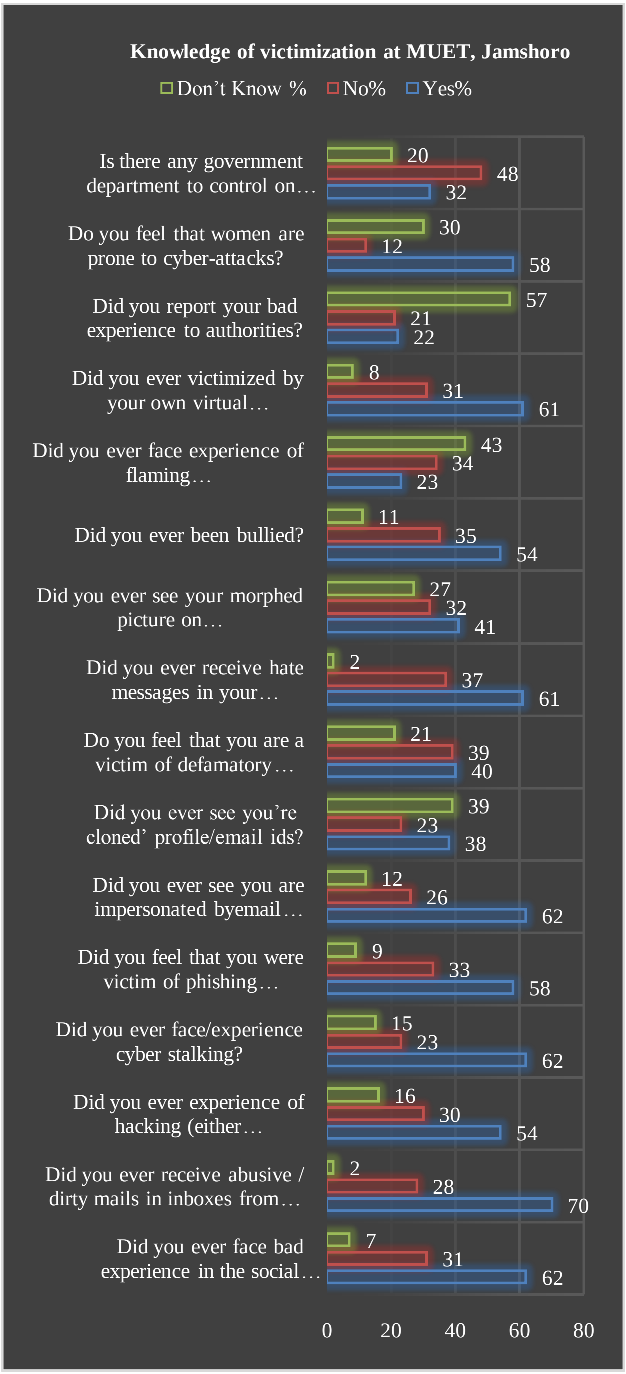
Table 3. Knowledge of victimization at MUET, Jamshoro

Knowledge of victimization at MUET, Jamshoro	**Yes %**	**No %**	**Don’t Know %**
Did you ever confront terrible encounter within the social organizing sites?	62	31	7
Have you ever received harmful / dirty messages from incoming / unknown sources?	70	28	2
Did you ever involvement of hacking (either	54	30	16

directly/indirectly) your ID Did you ever face/experience cyber stalking?			
Did you ever face/experience cyber stalking?	62	23	15
Did you just feel phishing attacks?	58	33	9
Have you ever seen yourself emulate an email account / social profiles / website, etc.?	62	26	12
Have you ever seen profile IDs / email addresses that have been cloned?	38	23	39
Do you think that you are simply the victim of defamatory statements / actions, including yourself in cyberspace?	40	39	21
Have you ever received disgusting messages to your mail	61	37	2
Have you ever seen your image transformed into cyberspace?	41	32	27
Did you ever been bullied?	54	35	11
Have you ever faced meeting the burning words of others?	23	34	43
Have you ever been a victim of your own virtual friends?	61	31	8
Did you report your terrible meeting to the authorities?	22	21	57
Do you feel that women are prone to cyber-attacks?	58	12	30
Is there a government division for the monitor cyber victimization in Pakistan?	32	48	20

Knowledge about victimization in MUET jamshoro, 28% of internet users received harmful and dirty messages from unknown sources. 54% of the people answered that the account has not been pirated. 31% of the people answered that they were not victims of their virtual friends. 41% of internet users responded that their image has been transformed into different social websites. Women were more vitimized than men in cyberspace, which is 58%. Cybercrimes increased recently because people do not report to the interested authorities, only 22% of people report to the authorities involved.

Fig 3. Knowledge of victimization at MUET, Jamshoro



IX. Conclusion

The needs of the Mehran University of Engineering and Technology will be discussed above. The interest will be unexpected because, despite the fact that digital exploitation is fraught with the damage associated with the claim of basic privileges. In addition, sexual harassment, almost no serious steps were taken to confirm this. Internet providers also have a long-term interpersonal environment. We will also see digital societies, in addition to digital principles, rules that can allow promotion and the ability to test these personal freedoms, especially the ability to talk.In MUET, Jamshoro's social value system, the percentage of such digital partnerships could provide growth with a small amount of misuse of claims to substantial privileges guaranteed in accordance with our constitution. The need for digital standardization has uncovered that passage about a world city that can structure its identity or culture, as well as ethical guidelines in any case, which should not affect in the least the privileges of character abuse. The administration, police, social workers, lawyers and non-governmental organizations should welcome educational institutions, universities and schools to conduct social awareness seminars, as well as seminars to discuss the legality of related illegal activities with computer crimes in both genders.

References

[1] Arpana and C. Meenal, 2012. Preventing cybercrime: A study regarding awareness of cybercrime in Tricity. International Journal of Enterprise Computing and Business Systems, 2(1).

[2] Campbell, Sherman, and Birchmeier (2001), InternetPrivacy Awareness and Concerns among College Students.

[3] Govani and Pashley (2005), "Student awareness of the privacyimplications when using facebook.

[4] Hemphill, S. A., Tollit, M., Kotevski, A., & Heerde, J. A. (2015), Predictors of traditional and cyber- bullying victimization: a longitudinal study of Australian secondary School students. Journal of interpersonal violence, 30(15), 2567-2590.

[5] M. Nawaz Brohi, and Rukshanda Kamran."Scientific Awareness about the Computer Forensic to Face the E-Criminal Activities of the E-User", International Journal of Computer Applications (IJCA) 2012, Volume 49

[6] Maurushat , Vaile , Dijk (2011) ,An Overviewof International Cyber-Security Awareness Raising and Educational Initiatives.

[7] Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015), Cybercrime victimization among young people: a multi-nation study. Journal of Scandinavian Studies in Criminology and Crime Prevention, 16(2), 203-210.

[8] Saravade and Saravade (2003),Emerging trends in cyber crime in India.

[9] Poonia,Bhardwaj,Dangayach (2011),Cyber Crime: Practices and Policies for Its Prevention.

[10] Riek, M., Bohme, R., & Moore, T. (2016), Measuring the influence of perceived cybercrime risk on online service avoidance. IEEE Transactions on Dependable and Secure Computing, 13(2), 261-273.

[11] Shabnam, N., Faruk, M. O., & Kamruzzaman, M. (2016), Underlying Causes of Cyber-Criminality & Victimization: An Empirical Study on Students. Social Sciences, 5(1), 1-6.

[12] Turanovic, J. J., Reisig, M. D., & Pratt, T. C. (2015), Risky lifestyles, low self-control, and violent victimization across gendered pathways to crime. Journal of Quantitative Criminology, 31(2), 183-206.

[13] Williams, M. L. (2015), Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. British Journal of Criminology, 56(1), 21- 48.

About Authors

[1] Farhan Abbas Memon (M.E) Student. Institute of Information & Communication Technologies (IICT) MUET, Jamshoro, Sindh, Pakistan.

[2] Tariq Jamil (Professor) Department of Computer System Engineering, MUET, Jamshoro, Sindh, Pakistan.

[3] Ali Arsalan (Assistant Professor) Department of Industrial Engineering, MUET, Jamshoro, Sindh, Pakistan.

[4] Mahaveer Rathi (M.E), Institute of Information & Communication Technologies (IICT) MUET, Jamshoro, Sindh, Pakistan.