An Interactive Model for Creating Awareness and Consequences of Cyber-crime in People with Limited Technology Skills

Sheeraz Akram, Muhammad Ramzan, Muhammad Haneef and Muhammad Ishtiaq

Abstract Technology is being used every day by the people irrespective of their technology skills. People with limited technology skills are not aware of what actions are legal and what actions are illegal according to the laws. In this paper, an interactive model for creating awareness and consequences of cyber-crime in people with the limited technology skills is proposed.

Keywords Regulator · Media · Technology skills · Cyber-companies · Social websites

1 Introduction

The 21st century is the era of information technology. In past people have different mechanism to share the information which were very slow, expensive, and unreliable and not enough to fulfill needs of all users. The people use to sit physically in their social circles for the social activities. For education purposed, they physically gathered at some location like schools and colleges. They use to have different games and it was necessary for all the participants to be present at one location for playing the game. The messages were sent by writing them on the

S. Akram(✉) · M. Haneef · M. Ishtiaq
Foundation University Rawalpindi Campus, Foundation University Islamabad, Islamabad, Pakistan
e-mail: {sheeraz,muhammadhaneef,ishtiaq}@fui.edu.pk

M. Ramzan
College of Computing and Information Technology,
Saudi Electronic University, Riyadh, Saudi Arabia
e-mail: m.ramzan@seu.edu.sa

S. Latifi (ed.), *Information Technology New Generations*,
Advances in Intelligent Systems and Computing 448,
DOI: 10.1007/978-3-319-32467-8_14

pages and later sent through different means like postman; to be a carrier. The money was kept in the form currency notes at the homes and banks.

Currently, the internet is medium to pass any kind of information from one location to another location. The social websites are available for people to create their social circles and friendships. The messages are sent from one place to another place by emails and different chat applications. Now people can play games by sitting on different locations and can compete with each other. The money is transferred online from one location to another location. All this is achieved by internet which is the backbone of current technology.

The world of internet is known as cyberspace. This world has its methods of communication, financial transaction, sports and developing social circles. In the cyber space, some actions are legal and some actions are not legal. The illegal actions in the cyberspace are known as cybercrime. There are people who are aware of what they are doing in the cyberspace, so they are well aware of the status of their actions whether legal or illegal. But there are great number of people who are illiterate with reference to the usage and working of cyberspace and they do illegal actions unknowingly. There is need to create awareness about cybercrime and it consequences especially for the people with limited literacy and knowledge regarding rules and working in cyber world. The related work is given below.

In [1], the current status of cybercrime related to financial based crime, non-financial matters, the threat to public and business are given and strategies again mentioned crimes are discussed. The conventional crimes, cyber-crimes, different models of committing cyber-crimes and cyber-crime prevention strategies are given in [2]. The basic measures required to curb the cybercrimes and spamming activities in Kenya are discussed in [3]. In [4], the current concepts and strategies of cybercrime and cybersecurity, possible elements of cybercrime policies and strategies are discussed. The motivations behind the cybercrimes, analysis of behavior of cybercrimes and the impact of cybercrime on the society are discussed in [5]. In [6], the phenomenon of cybercrime, topology of cybercrime, challenges of fighting cybercrime and anti-cybercrime strategies are discussed. The awareness level about cybercrimes and cyber law in Bangladesh is given in [7]. In [8], the impact of cybercrime on business and losses due to these crimes are presented. The cybercrime and what should do when you become victim of cybercrime is described in [9]. In [10], the cybercrime measurements, legislation and framework to handle cybercrime, investigation of cybercrime and electronic evidence required for handling cybercrime are discussed. In [11], the components of malicious activities are briefly described. The cybercrime related to identity theft, the nature and type of cybercrime and consequences of cybercrime in tertiary institution are discussed in [12]. The cybercrime in banks, the actors involved in cybercrime and its impact on banking finance is described in [13]. In [14], the existence of law against cybercrime and impact of cybercrime on the society in Nigeria is presented.

There is very less work related to creating awareness about cybercrime and consequences of cybercrime for the people who are not familiar with the technology.

So in this paper, an interactive model for creating and increasing awareness about cyber-crimes and its consequences for people with limited technology skills and literacy is proposed.

2 Proposed Model

The proposed model is to create awareness of cyber-crime and its consequences in the common public especially with low skills in technology. The components of proposed model are Government, Regulators, Media, Cyber Companies and User with Limited Technology skills. All the components collaborate with each other and focus is on User with Limited Technology Skills as given in Fig. 1. The purpose is to create awareness about cyber-crime and it consequences for the user having limited technology skills.

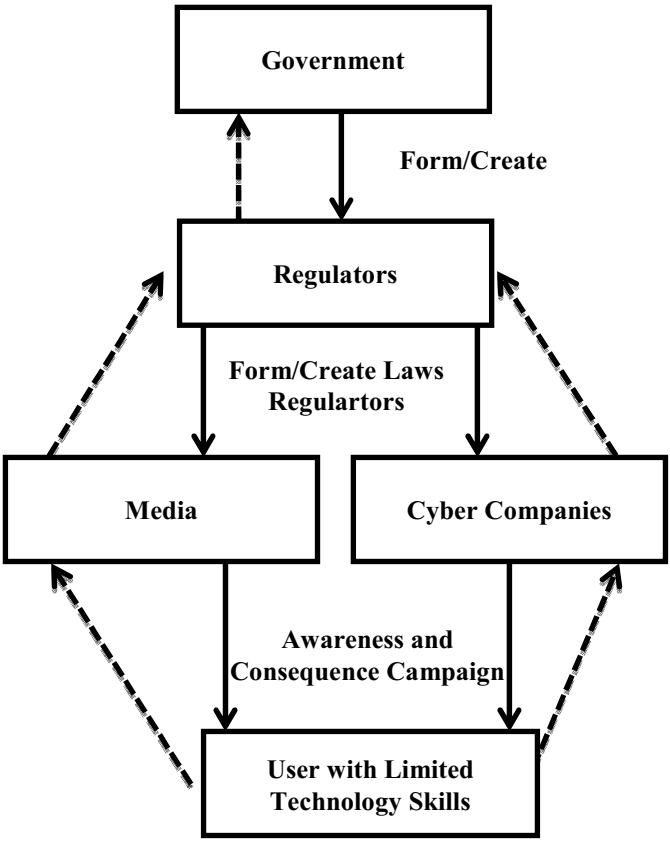

Fig. 1 Proposed Interactive Model

3 Roles of Components of Proposed Model

The components in the proposed models interact with each other. Each component provides feedback to the top component.

3.1 Government

The government is most important component of this model. The policy of the government depict about the rules and regulation for usage of any technology. Government is not a technical entity which is expert about everything; rather the role of government is produce/form certain institutions to look after different matters. The government work under set of rules and same rules allow government to form different agencies/regulators for the support of government. The agencies role is to help and make sure the proper implementation of orders given by the government. The Regulators are which takes response from the government as well as user too, so the regulator hold important place in proposed model. The Regulator provides feedback to the Government. The policies are modified according to feedback provided by the Regulators.

3.2 Regulator

The regulator is formed by the government using power, inherits at the time of formation. The regulator works according to policy given by the government. In our model, the component Regulator is working to control Media (Electronic & Print) and another Regulator control Cyber companies, for example the internet services provider, social websites etc as given in Fig. 2. The Regulator works on policy given by Government and makes rules for Media and Cyber companies. The Regulator advises them to prepare and launch campaign for creating and increasing awareness of cyber-crimes and its consequences in the people with limited technology skills.

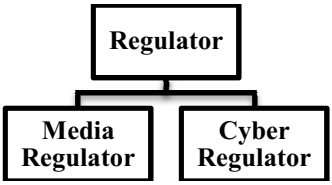

Fig. 2 Types of Regulator

The Regulator also takes the feedback from the Media and Cyber companies and presents it to the Government. The Government modifies the policy for user with limited technology skills based on feedback it receives from the Regulators. There is separate Regulator for Media and Cyber companies. The print media exist since long but electronic media got fame in last two to three decades.

At the same time the Cyber companies are more complicated and provide greater facilities and functionalities. So, the Regulator for the Cyber companies must be equipped with more power and vision.

3.3 Media

The Media is an important component in our proposed model. The types of media are given in Fig. 3. The print media is working since years in the form of newspaper, magazine etc. This is basic mean to convey any news and information to user who can read little despite having limited access to the technology. The print media produce and print such advertisements in the newspaper and magazine which guide the reader regarding the usage of technology. In the proposed model, the role of print media is very important as the impact of print media is long lasting. In case of any miss-use of the technology, where the user has to contact, should also be mentioned clearly in those advertisements. In proposed model, the news of cyber-crime is reported in way which mention that the person who has done crime is a technology skilled person or non-skilled. Also the crime should be reported in way which could be understood by person with limited technology skills.

The electronic media works through Television. The electronic media use the audio for any news along with visual aid. In the proposed model, the electronic media is instructed to show such programs which make people comfortable in using technology, especially people with limited technology skills. The cyber-crime news must be reported in way that the audio is understandable to the person with limited technology skill. The consequences of cyber-crime must be reported with examples so that the person can understand about cyber-crime and its consequences.

The media receives the feedback of the news and advertisements regarding increasing awareness of cyber-crime and its consequences and pass it to Regulators. The Regulator changes the rules for Media and also passes the feedback to the Government in order to make appropriate changes in the policy.

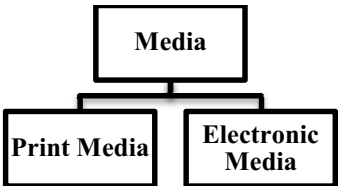

Fig. 3 Media Types

3.4 Cyber Companies

In the proposed model, the Cyber Companies are referring to internet service providers and other websites like email service providers and social websites. The internet service providers keep the track of each internet user through IP address.

In proposed model, the cyber companies must have separate groups of IP address for the technology skilled people and limited technology skilled people. The material must be sent to limited technology skills people in a language that is easily understandable for them. The illegal action from IP address in group of limited technology skill must be given immediate warning and provided guidance toward proper usage of the technology.

The email service providers allow user to send message electronically from one place to another place. In the proposed model, the email service providers collect the data at the time of account creation regarding the level of technology skills and later different ads appears along with emails to increase awareness of cyber-crimes and its consequences.

The social websites are very common now days. The people are using social websites for maintaining their social circle. The user uploaded different kind of material in the form of text, images and video. This material can be offensive to any single person or a community. In the proposed model, only that social website should be accessible which follow the instructions to display material for guiding user about cyber-crime and its consequences.

3.5 User with Limited Technology Skills

The User with Limited Technology Skills is most important component of our proposed model as all the components in model works for the awareness of this component. In the proposed model, the user with limited technology skills must read the advertisements on the media and ads in the email with care and should act on those instructions.

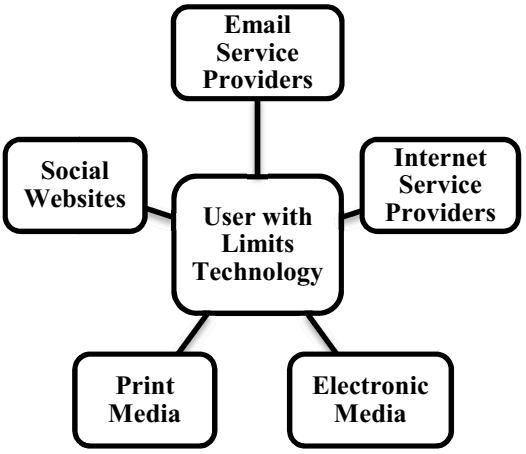

Fig. 4 Interaction of User with Different Components

The user must not perform any action which is not known to him. In the proposed model, the use must provide proper feedback to the Media and Cyber-companies so that they can convey to the Regulators to modify the policies. The limited Technology skilled people keep on learning with proper feedback mechanism in our proposed model. The user held responsible for committing a cyber-crime faces the consequences. The proposed model also suggests the design of consequences which should be developed in way that the user can become more skilled about the technology in the future.

4 Conclusion

The technology is vital in the current time. The people use the technology in their daily activities. The people do actions which are not suitable for the others and sometimes they cross the legal boundaries. This paper proposed an interactive model which shows the interaction between different components of the proposed model. The proposed model focuses on creating the awareness and consequences of cyber-crime in the people with the limited technology skills.

References

1. Department, S.o.S.f.H.: Cyber Crime Strategy. Surrey (2010)
2. Dashora, K.: Cyber crime in the society: problems and preventions. Journal of Alternative Perspectives in the Social Sciences **3**(1), 240–259 (2011)
3. Magutu, P.O., Ondimu, G.M., Ipu, C.J.: Effects of cybercrime on state security: types, impact and mitigations with the fiber optic deployment in Kenya. Journal of Information Assurance & Cybersecurity **2011**(1), 1–20 (2011)
4. Crime, G.P.o.C.: Cyber Crime Strategies (2011)
5. Saini, H., Rao, Y.S., Panda, T.C.: Cyber-crimes and their impact: a review. International Journal of Engineering Research and Applications (IJERA) **2**(2), 202–209 (2012)
6. Sector, T.D.: Understanding CyberCrime: Phenomena. Challenges and Legal Response (2012)
7. Khan, K.A.: Awareness towards cybercrime & cyber law. Insight Bangladesh Foundation (2013)
8. Study of the impact of cyber crime on business in canada. International Cyber Security Alliance (2013)
9. Cruz, A.: Cyber Crime and how it effect you. Cyber Security Tips **7**(1), 2 (2013)
10. Crime, U.N.O.o.D.a.: Comprehensive Study on cybercrime (2013)
11. The economic impact of cybercrime and cyber espionage. Centre for strategic and international studies (2013)
12. Okeshola, F.B., Adeta, A.K.: The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state, Nigeria. American International Journal of Contemporary Research **3**(9), 98–114 (2013)
13. Raghavan, A.R., Parthiban, L.: The effect of cybercrime on a bank's finances. International Journal of Current Research and Academic Review **2**(2), 173–178 (2014)
14. Olayemi, O.J.: A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology **6**(3), 116–125 (2014)