A growing problem of cyber crime

Law

Crime is a common word that we hear in this era of globalization. Crimes refer to any violation of law or the commission of an act forbidden by law. A nation with high index of crime cases cannot grow or develop well. This is because crime is the direct opposite of development. It can contribute to the negative impact in term of social and economic development. Cyber crime is a new type of crime that occurs in this age of Science and Technology. There are multiple definitions for cyber crime. I will only give the most generic one, which will cover all the aspects. Cyber crime refers to all activities done with criminal intent in cyberspace. A Computer can be considered as a tool in cyber crime when the individual is the main target of cyber crime. In addition, cyber crime also includes traditional crimes that have been conducted with the access of the Internet, for example hate crimes, telemarketing Internet fraud, identity theft, and credit card account thefts. In a simple word, cybercrime can be defined as any criminal action that can be conducted by using a computer or other devices with access to the Internet. The Internet is a system of law and regulation. Cyberspace is governed by a system of law called Cyber Law.

According to Kumar and Pandey, there are 3 basic categories of cyber crime: cyber crime against persons, cyber crime against property and cyber crime against the government. The first type includes material that is used to damage any personal effect, like transmission of child pornography. These are the tactics used by the hackers to damage any person. This type of cyber crime also uses harassment of different kinds like race, sexual and religious harassment. Kumar and Pandey make their point by giving us this example. “ The email id of top Indian squash player Saurav Ghoshal was hacked, this

hacking has created confusion in squash and media fraternity. The hacked sent a mail to the leading news paper, claimed that the squash star and his family were mugged in Spain and requested monetary help for settling the hotel bill". (Kumar, and Pandey). This example explains that the target of cyber crime can be high profile person and cyber criminals can work towards their disgrace by spreading some viral information about victim.

Later, Kumar and Pandey states that after cyber crime against persons, the other category of cyber crime is against forms of property. This type includes transmission of harmful programs from someone's computer to victim's computer and then stealing all of the important information. They say that one of the important cyber crime included in this category is that cyber criminals can steal the contents of a bank account and they can transfer money from victim's account to any unauthorized account. Whenever someone receives an email from an anonymous person saying some attractive offer, as soon as you will open that email, it will leave a virus in your computer without your notice and it will start transmitting important personal information to the hacker's computer. They claim that in some cases, they steal your credit card information and then they would sell that information over the Internet. These crimes also include computer defacement, transmission of harmful programs, Internet time theft, trespassing, and Intellectual Property crimes. According to Kumar and Pandey, Identity time theft is a technique for Identity theft when someone pays other persons to work on computer and then steal their victim's personal information for Identity theft. (Kumar, and Pandey).

In addition to these categories, cyber crime against governments constitutes a third level of cyber crime. Kumar and Pandey later argue that, one distinct crime is this category is known as cyber terrorism. Cyber terrorism is used to threaten international governments and also to terrorize the citizens of those countries. Kumar and Pandey claims that the most important example of hacking against government is web jacking. By this tactic, hackers can gain control over the government's websites especially military websites and they can change the important and sensitive information without even notifying the actual authority. According to them, some terrorist groups use this type of cyber crime to monitor a government's activities and they also use this cybercrime to transfer funds from a government's bank accounts to their accounts in order to promote their activities. (Kumar, and Pandey)

Lets discuss some examples of cyber crime. One of the important examples of cyber crime is identity theft. Identity theft means that someone has stolen victim's personal information like social security number, driver's license number and home address. After stealing all this key information, hacker can pose as victim and then he can access all victim's credit cards and bank accounts. Identity theft basically includes three types of frauds, unauthorized use of an existing account, unauthorized use of personal information to open new accounts, and misuse of personal information for fraudulent purposes. Here are some statistics of identity theft cases from 2012.

About 7% of individuals aged 16 or older were victims of identity theft in 2012. The majority of identity theft incidents (85%) involved the fraudulent use of existing account information, such as credit card or bank account information. Victims who had personal information used to open a new

account or for other fraudulent purposes were more likely than victims of existing account fraud to experience financial, credit, and relationship problems and severe emotional distress. Over half of identity theft victims who were able to resolve any associated problems did so in a day or less; among the victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems. (Harrell, Langton).

This example gives some statistics based on the yearly analysis of the cyber crime.

According to Dashora, there are certain factors that are working towards the increase of cyber crime. The first reason for cyber crime is that nowadays, by using computers we can store a lot of information in small devices. Many of us don’t like to write the information on the paper and we are storing all of the information on one device. Dashora claims that this makes it easy for a cyber criminal to access all of victim’s information at one place and he doesn’t need to look for the sensitive information at any other place. We can minimize this factor by securing all-important information in a secure place other than a computer, or by having different key information at different places. (Dashora)

In addition to above-mentioned reason, there is another reason for cyber crime that the computers are very easy to access. Dashora states that even though many of us have some antivirus software installed on the computers, there are some tools through which hackers can breach the firewall and easily access the data. The computers use operating systems, which are

very complex and hard to understand. There is human error at every stage of programming. According to Dashora, hackers take advantage of this lapse and use it to beach the operating system. Negligence plays an important role in cyber crime to grow up. Sometimes victims are so negligent that they don’t care if their computer is turned on for the whole night. Hackers take advantage of this inactivity over a long period of time and they breach in to victim’s personal data. (Dashora)

There are some preventive measures that we can take in order to avoid becoming the victim for cyber crime. A strong password is the very first layer of defense against anyone trying to hack your account. According to Microsoft, a strong password should have at least eight characters, that at least include three of these, upper case, lower case, numerals, punctuation marks, and symbols. Cybercriminals use sophisticated tools to rapidly crack passwords, but we can foil their attempts. Do not use, personal information that can be easily discoverable like your name, pet name, address etc. Sequences like 1122 or aabbcc are not recommended.

After the first layer of strong password, storing the password is termed as the second layer of defense. Do not store your password in common places such as your worktable. According to the research from Microsoft, 55% people use same passwords for everything. That makes it easy for Hacker to hack all information including bank accounts or may be email accounts. There is another extra security feature that you can add to improve your security defense. It’s called two-factor authentication, by using this feature you can register your trusted device with your device maker like apple. After that, device maker will send you a 4-digit code to your cellphone and then

you will enter that code in order to access your account. So, even if someone knows your username and password, they can’t access your account without that verification code.

In addition to the two-factor authentication, there is third layer that is to keep your sensitive information like birthdate; street address and your social security number off the social network websites like Facebook or twitter. In addition to this preventive measure, don’t use public Wi-Fi so frequently. According to a survey from Microsoft, about 95% of the people use public Wi-Fi. Whenever you are using a public network, make sure you have your antivirus updated and working properly. Never update your software on a public network. If possible, save you financial transactions for a secured home network. Passwords, credit card information and financial information are less secure on a public network.

Through this paper, I showed that cyber crime is growing and we need to take steps to stop it. I mentioned some types of cyber crime and how we can avoid becoming its victim. At the end of this paper, I listed some preventive measures to avoid becoming victim of cyber crime.