Identity Theft And Cyber Crime: An Interpretation

Dr. Sushama Mishra
Asst. Prof. of English
Govt. Pt. Shyamacharan Shukla Colle Dharsiwa
Dist.Raipur
Email: mishrasushma2301@gmail.com

(Received:10June2021/Revised:20June2021/Accepted:1July2021/Published:6July2021)

Abstract

Cyber crime refers to the act of performing a criminal act using computer or cyber space (the internet network) as the communication vehicle. Millions of people around the world use computers and the internet every day. We all use it in school, work, even at home, computers have made our life easier, it has brought so many benefits to the society, but it has also brought some problems and cyber crime is one of them. Violation of privacy of online citizens is a Cyber crime of a grave nature. No one likes any other person invading the invaluable and extremely touchy area of his or her own privacy which the medium of internet grants to the citizen. There are certain offences which affect the personality of individuals such as harassment via E-mails, cyber-stalking, defamation, hacking, cracking, E-mail spoofing, SMS spoofing, carding, cheating and fraud, assault by threat. Computer crime does have a drastic effect on the world in which we live. In my view point hacking and computer crime will be with us for as long as we have the internet. It is our role to keep the balance between what is a crime and what is done for pure enjoyment. The true nature of what cyber crime will include in the future is unknown. The users of computer system and internet are increasing day be day across the world and it is very easy to communicate within a few second by using internet. Certain precautionary measures should be taken by all of us while using the internet to stop this major threat to communication.

Keywords: Cyber Crime, Hacking, Cyber Fraud, Prevention Of Cyber Crime.

Cyber crime refers to the act of performing a criminal act using computer or cyberspace (the Internet network), as the communication vehicle. Though the there is no technical definition by any statutory body for Cyber crime, it is broadly defined by the Computer Crime Research Center as - " Crimes committed on the internet using the computer either as a tool or a targeted victim" All the types of cyber crimes involve both the computer and the person behind it as victims; it just depends on which of the two is the main target. Cyber crime could include anything as simple as downloading illegal music files to stealing million of dollars from online bank account.

An important form of cyber crime is identity theft, in which criminals use the internet to steal personal information from other users. Various types of social networking sites are used for this purpose to find the identity of interested peoples. There are two ways this is done - phishing and harming, both methods lure users to fake websites, where they are asked to enter personal information. This includes login information, such as usernames and passwords, phone numbers, addresses, credit card numbers, bank account numbers, and other information criminals can use to "steal" another person's identity.

Cyber crimes committed against persons include various crimes like transmission of cyber porn, harassment of a person using computer such as through e-mail. The trafficking. distribution, posting and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important cyber crime known today.

Cyber harassment as a crime also brings us to another related area of violation of privacy of citizens. Violation of privacy of online citizens is a Cyber crime of a grave nature. No one likes any other person invading the invaluable and extremely touchy area of his or her own privacy which the medium of internet grants to the citizen.

People do feel hurt and violated by others words on the web. Their feelings are real and so therefore the crime is real. The internet requires interaction, and without the voluntary interaction of the victim crimes would never happen. If the victims didn't react to the crime but simply logged off, the virtual criminal would most likely receive no satisfaction from committing the crime.

Surrendering your character to a wizard by logging off would seems to be surrendering your entire reputation as well. The worst that could happen through logging of would be the loss of your perhaps well established character; the worst that could happen from witnessing the forced crime upon your virtual character could be life long emotional scars and possible counseling.

To punish someone for their words seems irrational, and it will only set off another from a legal system that often is thought to restrictive as it is in real life. By taking responsibility of our own characters and responsibilities on the web, in the long run we will benefit from the new freedom we waited so long to obtain. By protecting ourselves, we protect our best interests, and that is what freedom is all about.

To fight back individual and businessman should be proactive, not reactive we do not have to remain at the receiving end of crime forever. The fight against cyber crime starts in our very own home. We should not replay any email from unknown persons, we should learn to report spam mails to the email servers. We should not upload our personal information on social networking sites or our account details on other such sites. Also the antivirus softwares can be a great help to fight against viruses and worms. Fighting Cyber crime requires intelligent knowledge and that has to be IT intelligence. IT experts should be recruited in to law enforcement agencies to assist in the fight.

Shailesh Kumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber Crime Cell, advocates the 5P mantra for online security:

1. Precaution
2. Prevention
3. Protection
4. Preservation
5. Perseverance

One should avoid disclosing any personal information to strengers, the person whom they don't know, via e-mail or while chatting or any social networking site. One must avoid sending any photograph to strangers by online as misusing or modification of photograph incidents increasing day by day. An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination. It is always the parents who have to keep a watch on the sites that their children are accessing, to prevent any kind of harassment or depravation in children.

Conclusion

In my view point hacking and computer crime will be with us for as long as we have the internet. It is our role to keep the balance between what is a crime and what is done for pure enjoyment. Since users of computer system and internet are increasing worldwide in large number day by day where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by all of us while using internet which will assist in challenging this major threat Cyber Crime.

References

1. Harrington, James. " Beware of chilling Freedom of Expression". Cyber Reader. Ed.
Victor Vitanza. Arlington, TX: Allyn and Bacon, 1996 157-159.
2. Communications Fraud control association. 2011 global fraud loss survey. Available:

http://www.cfca.org//fraudlosssurvey/,2011.