CYBER PROTECTION ISSUES IN INDIA

[1]Inderjit Singh Blaggan, [2]Lokendra Singh Songara

[1]M. Tech. Scholar, [2]Assistant Professor
Cyber Security
Dr. A.P.J. Abdul Kalam University, Indore (M.P)

***Abstract*: In the present generation, the social life of everyone has become associated with the online social networks. These sites have made a drastic change in the way we pursue our social life. Making friends and keeping in contact with them and their updates has become easier. But with their rapid growth, many problems like fake profiles, online impersonation have also grown. There is no feasible solution exist to control these problems. In this project, we came up with a framework with which automatic detection of fake profiles is possible and is efficient. This framework uses classification techniques like Support Vector Machine, Nave Bayes, and Decision trees to classify the profiles into fake or genuine classes. As, this is an automatic detection method, it can be applied easily by online social networks which has millions of profiles whose profiles cannot be examined manually.**

I. Introduction

Throughout the long term, Information Technology has changed the worldwide economy and associated individuals and markets in manners past creative mind. With the Information Technology acquiring the middle stage, countries across the world are exploring different avenues regarding creative thoughts for financial turn events and comprehensive development. An expanding extent of the total populace is moving to the internet to convey, appreciate, learn, and direct business.

It has likewise set out new weaknesses and open doors for disturbance. The digital protection dangers exude from a wide assortment of sources and show themselves in problematic exercises that target people, organizations, public foundation, and Governments the same. Their belongings convey huge danger for public wellbeing, security of country and the soundness of the all around the world connected economy overall. The beginning of a disturbance, the personality of the culprit or the inspiration for it very well may be hard to learn and the demonstration can occur from essentially anyplace. These credits work with the utilization of Information Technology for troublesome exercises. In that capacity, digital protection dangers present one of the most genuine financial and public safety challenges.

The internet is such a term, which isn't yet totally characterized and furthermore has no topographical constraint. It is a term related with use of the Internet around the world. It is additionally called as a virtual space as actual presence of the internet isn't recognizable in any way. The internet is "the all-out interconnectedness of people through PCs and media transmission regardless of
actual topography."

The ascent in the Internet populace has implied that while the dangers and weaknesses inborn to the Internet and the internet may have stayed pretty much as old as, the likelihood of disturbance has developed apace with the ascent in the quantity of clients. While such interruptions are yet to cause super durable or shocking harm around the world, they fill in as a reminder to the specialists worried to start measures to work on the security and solidness of the internet as far as their own security. State run administrations are compelled in their reactions by pressures applied by politico-military-public safety entertainers toward one side and financial common society entertainers at the other.

Types of Cyber Threats

As we grow more dependent on the Internet for our daily activities, we also become more vulnerable to any disruptions caused in and through cyberspace. The rapidity with which this sector has grown has meant that governments and private companies are still trying to figure out both the scope and meaning of security in cyberspace and apportioning responsibility. Cyber threats can be disaggregated, based on the perpetrators and their motives, into four baskets:

1. Cyber Espionage,
2. Cyber Crime
3. Cyber Terrorism
4. Cyber Warfare

Cyber Espionage

Cyber espionage, is "the act or practice of obtaining secret information without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware." Simply said, Cyber espionage is "The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization."

Types of Security Threats

Cybercrimes consist of specific crimes dealing with computers and networks, such as hacking, phishing and the facilitation of traditional crime using computers (child pornography, hate crimes, telemarketing/internet fraud). A brief introduction to some common cyber related violations, or cybercrimes as they are more commonly referred to are discussed below:

Hacking

Hacking in simple terms means an illegal intrusion into a computer system and/or network. There is an equivalent term to hacking i.e. cracking, but from Indian legal perspective there is no difference between the term hacking and cracking. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer.

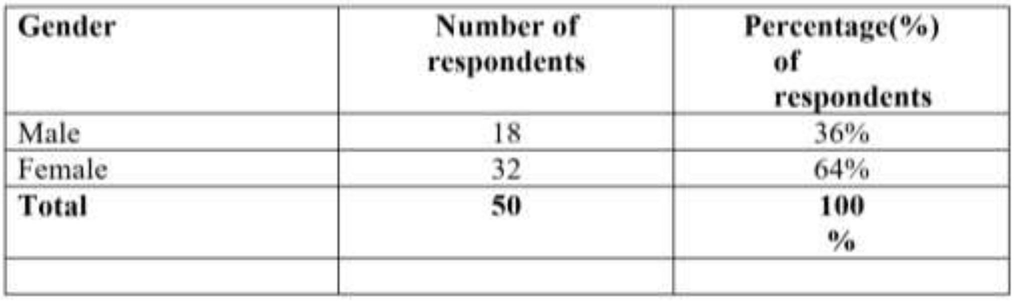
Child Pornography

The Internet is extensively used for sexual abuse of children. As more homes have access to internet, more children are accessing it and this enhances their vulnerability of falling victims to the aggression of paedophiles. Paedophiles (a person who is sexually attracted to children) lure the children by distributing pornographic material and then pursue them for sexual exploitation. Sometimes paedophiles contact children in chat rooms posing as teenagers or children of similar age; they win the confidence of these children, and then induce them into sexually provocative discussions. Then begins the actual exploitation of children.

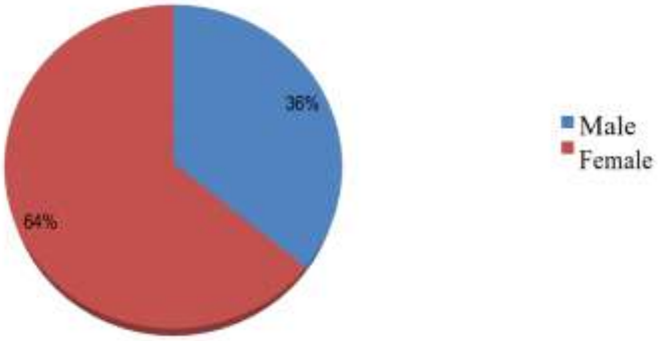
Data Analysis and Interpretation

Questionnaires are administered to respondents selected randomly within twin cities of Hyderabad and Secunderabad. 50/50 respondents have responded. The data so collected is tabulated, analyzed, interpreted and presented in the following tables and charts:

Gender – respondents

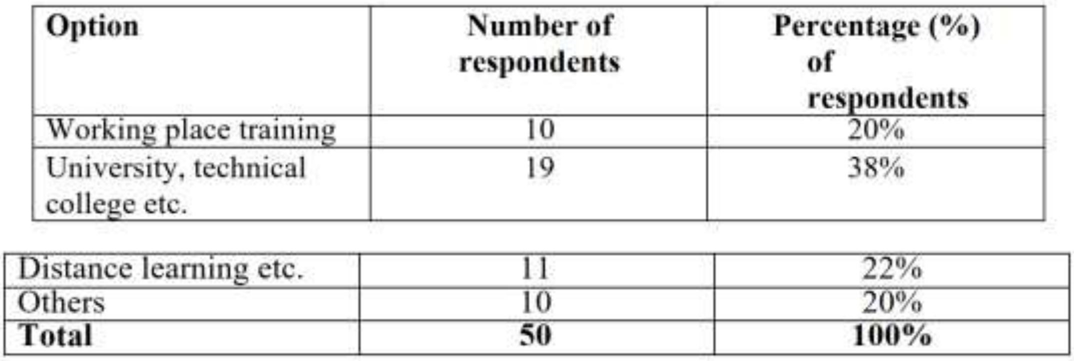


Gender	Number of respondents	Percentage(%) of respondents
Male	18	36%
Female	32	64%
Total	**50**	**100 %**

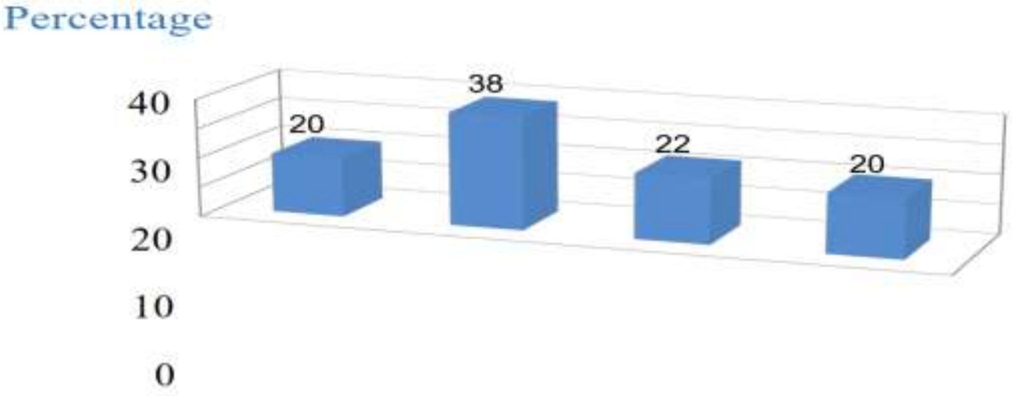


From the above chart it is observed the 36% of respondents (18/50) are male. 64% of respondents (32/50) are female.

Table



Option	Number of respondents	Percentage (%) of respondents
Working place training	10	20%
University, technical college etc.	19	38%
Distance learning etc.	11	22%
Others	10	20%
Total	**50**	**100%**



From the above chart it is observed that 20% of respondents are learning Information Security from the source of Working place training. 38% of respondents (19/50) are learning Information Security from the source of university, technical college etc. 22% of respondents (11/50) are learning Information Security from the source of Distance learning etc. 20% of respondents (10/50) are learning Information Security from the source of others.

Conclusion

Community in cyberspace is based on the interaction between people. Cyberspace has an important social aspect to it that must not be overlooked. Cyberspace can be treated as a channel touching portion of real space at key points. Ideas are passed through the channel, and business is transacted through this channel. The cyberspace communities are members of the global community interacting on a different plane than in real space. With the huge growth in the number of Internet users all over the world, the security of data and its proper management plays a vital role for future prosperity and potentiality. It is concerned with people trying to access remote service is that they are not authorized to use.

Rules for compulsory wearing of helmet for bikers by government authorities, has no benefit for them, it is for our own safety and life. Same we should understand our responsibilities for our own cyberspace and should at least take care of safety for our personal devices. These steps include installation of antivirus software and keeping it updated, installing personal firewalls, and keeping rules updated. We should monitor and archive all security logs. We should have backup of important data. Our devices should be protected by passwords and there should be restricted access to sensitive data on our devices. And above all, we should aspire for more computer literacy to understand the safety issues related to our cyberspace. At the same time we need to utilize the specialization of private sector in the field of cyber security and government should promote more PPP projects for the national cyberspace.