International Journal of Advance Research in Science and Engineering
Volume No. 13, Issue No. 05, May 2024
www.ijarse.com
IJARSE
ISSN 2319 - 8354

AWARENESS OF CYBERCRIME TO USE OF MOBILE COMPUTING AND WIRELESS DEVICES

Isharat Ali[1], Anurag Gupta[2], Dr. Vijay Shukla[3]

[1]Assistant Professor (CSE-AI&DS, Greater Noida Institute of Technology, U.P., India)

[2]Assistant Professor (CSE, ABES Engineering College, U.P., India)

[3]Head of Department (CSE-AI&DS, Greater Noida Institute of Technology, U.P., India)

[1]mirzaishratali@gamil.com, [2]anurag.ideal09@gmail.com, [3]Hodai-ds@gniot.net.in

ABSTRACT

The role of mobile computing and wireless devices is very important in our daily life. Now day by day mobile computing enables connecting portable devices to wireless networks to access data and use services while moving. Mobile communication involves the infrastructure that is used to wirelessly transmit and receive data between devices seamlessly and safely. Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations that target the security of mobile computing and wireless devices and the data processed by them, hence cybercrime can sometimes be called as computer-related crime, computer crime, E-crime, internet crime, high-tech crime.

Keywords: *Spoofing, cybercrime, hacker, malware, ransom, mail boms*

INTRODUCTION

The internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of be it entertainment, business, sports or education. There are two sides to a coin. Internet also has it's own disadvantages is cyber crime- illegal activity committed on the internet.

- Crime committed using a computer and the internet to steal data or information.
- Illegal imports.
- Malicious program.
- Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution
- Any financial dishonesty that takes place in a computer environment.
- Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom.

- All criminal activities done using the medium of computers, the internet, cyberspace and the www.

CATEGORIZATION OF CYBERCRIMINALS

Type 1: Cybercriminals – hungory for recognition

- Hobby hackers
- IT professional (social engineering)
- Politically motivated hackers
- Terrorist organizations

Type 2: Cybercriminals – not interested in recognition

- Psychological perverts
- Financially motivated hackers
- State-sponsored hacking

Type 3: Cybercriminals – the insiders

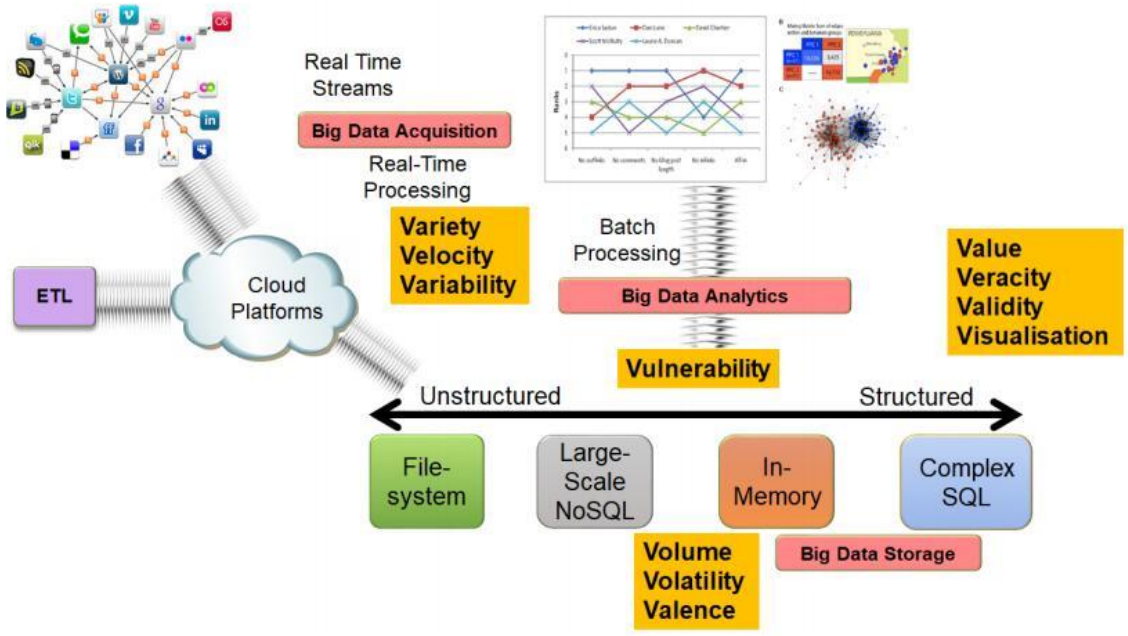
- Disgrunted or former employees seeking revenge

- Competing companies using employees to gain economic advantage through damage and/or theft.
- State-sponsored hacking

International Journal of Advance Research in Science and Engineering
Volume No. 13, Issue No. 05, May 2024
www.ijarse.com
IJARSE
ISSN 2319 - 8354

CHALLENGES FOR SECURING DATA IN BUSINESS PERSPECTIVE

Cybercrime occupy an important space in information security due to their impact. Most organizations don't incorporate the cost of the vast majority of computer security incidents into their accounting. The difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost. Financial loses may not be detected by the victimized organization in case of insider attacks, such as laeking customer data.



CLASSIFICATION OF CYBERCRIMES

1. **Cybercrime against an individual** – Electronic mail spoofing and other online frauds, phishing, spear phishing, spamming, cyberdefamation, cyberstaking and harassement, computer sabotage, pornographicsoffenses, passwordsniffing.
2. **Cybercrime against property**- credit card frauds, intelectual property (IP) crimes, internet time theft.
3. **Cybercrime against organization** – unauthorized accessed of computer, denial-of-service attacks, email bombing/mail boms, data diddling, industrial spying/individual espionage. Computer network intrusions, software piracy.
4. **Cybercrime against society** – forgery, cyberterrorism, web jacking.
5. **Crimes emanating from usenet newsgroup** – usenet group amy carry very offensive, harmful, inaccurate mateial. Postings that have been mislabeled or are deceptive in another way, hence service at your own risk.

International Journal of Advance Research in Science and Engineering
Volume No. 13, Issue No. 05, May 2024
www.ijarse.com
IJARSE
ISSN 2319 - 8354

THERE ARE THREE TYPES OF MODERN HACKERS

- **Black Hats** - criminal hackers, posses desire to destruction, stealing credit card information, transferring money from various bank accounts to their own account, extort money from corporate giant by threatening.
- **White Hats** - ethical hackers, network security specialist.
- **Grey Hats** - deals in both of the above (jack of all trades, master of none).

RESULTS AND DISCUSSION

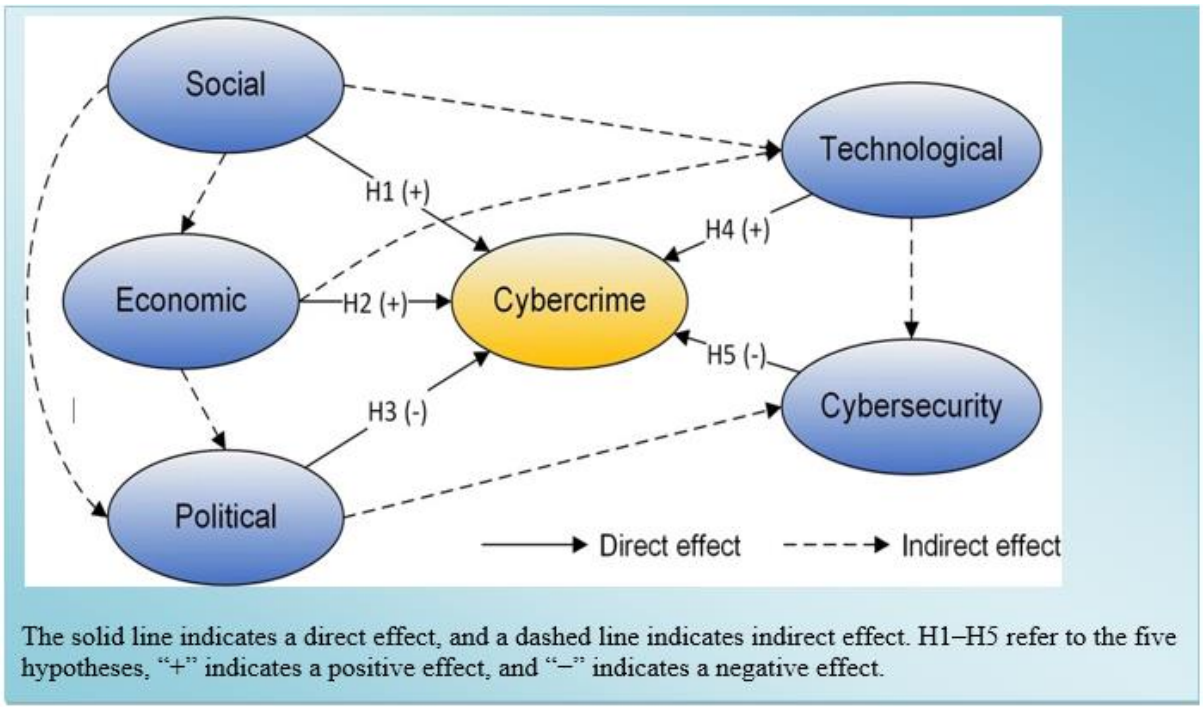
India has the fourth highest number of internet users in the world. 45 million internet users in India. 37% in cybercafés, 57% are between 18 and 35 years. The information technology (IT) Act, 2000, specifies the acts which are punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T.

With 755 cases registered per 100,000 people in 2023, Delhi had the highest number of cybercrime complaints in the country for any state or Union territory, according to the Indian Cyber Crime Coordination.

Global cybercrime damage costs this year are expected to breach US $6 trillion an annum. This is almost one-fourth of the US GDP or twice GDP of India. This is expected to scale up to US $10.5 trillion an annum by 2025. Cyber attackers are disrupting critical supply chains at least 4 times more than in 2019.

Total malware expected to exceed 1.2 billion samples in 2021 and is averaging approx. 18 million new malware samples every month (Source AV-Test). Average ransom payment peaked in Q3 2020 at ~US $234k but decreased to ~US $154k in Q4 2020.

CONCLUSIONS



The solid line indicates a direct effect, and a dashed line indicates indirect effect. H1–H5 refer to the five hypotheses, "+" indicates a positive effect, and "−" indicates a negative effect.

In this paper, learnt what cybercrime is and appreciate the importance of cybercrime as topic. Understand the different type's cybercrime. Understand the difference between cybercrime and cyber fraud. Learnt about different types of cybercriminals and motive behind them. Get an overview of cybercrime scenario in India and global. Understand legal perspective on cybercrimes.

REFERENCES

1. Sunit Belapure and Nina Godbole, "Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives", Wiley India Pvt Ltd, ISBN: 978-81- 265-21791, Publish Date 2013.
2. Basta, Basta, Brown, Kumar, Cyber Security and Cyber Laws, 1st edition , Cengage Learning publication.
3. Dr. Surya PrakashTripathi, RitendraGoyal, Praveen Kumar Shukla, KLSI. "Introduction to information security and cyber laws". Dreamtech Press. ISBN: 9789351194736, 2015.
4. Cyber Security and Date Privacy by Krishan Kumar Goyal , Amit Garg , Saurabh Singhal , HP HAMILTON LIMITED Publication, ISBN-13-978-1913936020
5. Thomas J. Mowbray, "Cybersecurity: Managing Systems, Conducting Testing
6. Investigating Intrusions", Copyright © 2014 by John Wiley & Sons, Inc, ISBN: 978 - 1-118 -84965 -1.
7. James Graham, Ryan Olson, Rick Howard, "Cyber Security Essentials", CRC Press, 15-Dec 2010.

8. Anti- Hacker Tool Kit (Indian Edition) by Mike Shema, McGraw-Hill Publication.
9. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.