Cyber security: it's info & cyber ethics

RANPRIYA TIRTH S.[1]
Computer Engineering Department, V.V.P. Engineering College, Rajkot, Gujrat, India.
Email: 22ce128.tirth.ranpariya@vvpedulink.ac.in
RATHOD UDAY J.[2]
Computer Engineering Department, V.V.P. Engineering College, Rajkot, Gujrat, India.
Email: 22ce025.uday.rathod@vvpedulink.ac.in
RATHOD UMANG R.[3]
Computer Engineering Department, V.V.P. Engineering College, Rajkot, Gujrat, India.
Email: 22ce011.umang.rathod@vvpedulink.ac.in

ABSTRACT: This paper discusses the various aspects of ethics in cybercrime, highlighting the emergence of cybercrime as a serious threat and the global response to address it and make it important. It mentions the establishment of ethics centres and programs focusing on different type or parts such as business ethics, legal ethics, bioethics, medical ethics, engineering ethics, and computer ethics. These super aims to see the impact of moral principles and practices on human activity. The paper also mentions the work taken by governments, police departments, and intelligence units worldwide to combat cyber threats, including the establishment of special cyber cells in all over the world. It provides a glimpse of the current scenario of cybercrime in India, based on reports from news media and news portals. we can strive towards a more responsible and trustworthy cyber security community.

Keywords: Cyber security, Cyber-ethics, cyber bully, cyber space, cyber stalking, back door.

INTRODUCTION: Ethics can divide in two ways: normative and prescriptive. Normative ethics sets out rules for what is right and wrong, telling us what we should do in terms of rights, duties and benefits to society, well fairness and virtues. For instance, ethical standards tell us not to do crimes such as rape, theft, murder, assault, slander, or fraud. They also give as knowledge such as honesty, compassion, and loyalty. Ethical standards also include rights, like the right to live your life as you want, freedom from harm, choice, privacy, and freedom of speech with some limitation. These standards are considered valid because they have logical and well-founded reasons. Ethics is important for study and development of personal ethical standards, as well as those of the community from the belongs to. Therefore, it's important to evaluate again and again with time our standards to make sure they are logical and well-founded. Ethics also entails continuously examining our own moral beliefs and behaviours, and working to ensure that we, our community, and the institutions we influence adhere to standards that are reasonable and based on solid principles for human advancement.

"Ethics are moral standards that help guide behaviour, actions, and choices."

Ethics are based on the responsibility and accountability. Individuals, organizations, and societies are behind this their actions and should be held completely responsible for the consequences. Laws in societies codify important ethical standards and provide a way to hold people, organizations, and governments accountable. The Internet has become a crucial part of modern life, offering new possibilities that were never see or thought before. It's now a tool for

communication and provides huge benefits. However, it also gives us opportunities for crime using sophisticated technology. Email and websites are now common means of communication, and organizations provide Internet access to their staff, enabling instant exchange of data and information. Cybercrime, including hacking, viruses, and internet-based crimes, is on the rise, as reported in the media also it is head line of the newspaper in last some years. This makes challenges for legal systems and law enforcement as they try to address new forms of criminal activity.[1]

Now let's see some sub topic or related topic with it

1. **CYBER SPACE-CYBER CRIME:** Cyberspace means to say online environments created by the Internet. Crime is any punishable work or thing against morality or law. In simple words crime is act which is agents of society. Cybercrime involves using computers or networks for illegal activities, including hacking and fraud also many time cases like cyber bully. It makes a big threat to individuals, businesses, and governments worldwide. Cybercriminals exploit technology to commit crimes such as identity theft and data breaches. Preventing and combating cybercrime requires international cooperation and advanced security measures also some boundary for learning and practice hacking.

2. **TRADITIONAL CRIME – CYBER CRIME:** Computer crime specially includes crime like unauthorized access, data alteration, destruction, and intellectual property theft. In terms of national security, cybercrime can know for activism, espionage, and information warfare. It's a global issue and a major source of revenue for organized crime with **value of almost $8 trillion USD a Year in 2023 which is more than India GDP also may be $10.5 Trillion annually by 2025**[2]. This has shown to a significant rise in malware risks. Unlike traditional crimes, cybercrime directly targets the Information Technology infrastructure itself. Examples of crimes using computers include pornography, identity theft, and phishing, while crimes against computers include viruses, hacking, cyber bully, and cyber staking and software piracy. Cybercrime has two sides: the assassin and the victims, and the number of crimes should ideally match the number of victimizations but some time it is more than that number. There won't always be a direct match between the number of crimes and victimizations, as one crime can affect multiple victims, and multiple crimes can impact a single victim. Some crimes may not lead to measurable or identifiable victimizations. Cybercrime's impact on businesses is primarily seen in the changing threat landscape. Initially, attackers aimed for fame, but now the motive is mainly criminal due to the lucrative nature of cybercrime.

3. **CYBER CRIME VARIANTS:** There are some types of cybercrimes, and while a few are discussed here, this topic does not cover all of them.

    - **Cyber stalking:** Cyber stalking mean to say using the Internet or electronic methods to stalk or harass someone, which is also known as online harassment or abuse. Stalking typically involves repeatedly harassing or threatening behaviours, such as following someone, showing up at their home or workplace, making harassing calls, leaving messages or objects, or damaging their property. Example like in India if you can arrest in cyber staking then Under Section 67 of the Act, when a stalker sends or posts any obscene content to the victim via electronic media then they will be liable

to punish with 5 years of jail and Rs. 1 Lakhs fine [3].this thing is mainly happened on girls but they ignore it but some time it is very serious issue. They must come out and talk about parents about this.

- **Hacking:** "Hacking" is a criminal act that involves breaking into computer systems to access data without permission. This year, hacking has seen a 37 present increase.

- **Phishing:** Phishing is a type of internet fraud where scammers try to trick people into giving away their money using many type of scam like money win and other wining things. They send fake emails to bank customers, asking them to enter their personal information on a fake website and this is most common and famous type of phishing. When people click on the links in the email and enter their information, the scammers can access their bank accounts. A report by F-Secure Corporation found that the banking industry in India was a common target for phishing scams with very huge number of Number of frauds in banking **sector rose in FY23, amount involved halved to Rs 30,252 crore .**[4]

- **XSS:** Cross-site scripting (XSS) is a security flaw often seen in web applications. It lets malicious users inject code like HTML or scripts into web pages viewed by others. Attackers can use this vulnerability to bypass access controls. xss is mostly use type .[5]

- **Cyber Squatting:** Cybersquatting involves registering a well-known domain name with the intention of selling it at a high price. This practice is not addressed in the IT Act of 2000. Specific for India there is not any kind of law for IT sector but for general file there is law of Trademarks Act 1999.[6]

- **backdoor:** Backdoor is a type of cybercrime where criminals secretly control computers by tricking users into downloading malicious software, often disguised as email attachments using website like usemydisk. Once infected, these computers can be used to carry out coordinated attacks, giving criminals access to significant computing power. Criminals use these networks to scan for weaknesses in other systems and carry out attacks. The malicious software, known as a Trojan horse, provides a hidden way for criminals to access the computers. This poses challenges for organizations as criminals can quickly update the software, making it difficult to defend against. This type of scam may happen using some friend's email id but in real it is similar named email id not real email id. But if you don't have idea then you may install or click on attachments which come to hack your system.[7]

4. **Reasons behind the Cyber Crime:** Cybercriminals commit acts for recognition, money, or causes. Global online reach offers low-cost operations, but law enforcement struggles to catch them effectively. Lack of regulation, reporting standards, and identification methods limits media coverage. Corporate cybercrimes are often collective efforts, not individual actions.[8]

Conclusion: In conclusion, cybercrime is a significant challenge in today's digital age, encompassing various illegal activities that exploit vulnerabilities in online systems and networks. It is crucial for individuals, organizations, and governments to prioritize cyber security measures to protect against cyber threats effectively. Additionally, cyber ethics play a vital role in guiding ethical behaviour online, emphasizing the importance of responsible and respectful use of technology. Adhering to ethical principles such as respecting privacy, avoiding plagiarism, and promoting digital literacy can help create a safer and more secure online environment for all users. Also country like India which are in developing stage and famous for future IT hub must add the cyber ethics in the education curriculum so student first learn about what to do and what not to do. India government must make some boundary for practice the ethical hacking and also make some serious acts & rules for develops a well cyber society.

REFERENCES:

[1] Mohit Goyal ON ETHICS AND CYBER CRIME IN INDIA AT International Journal of Engineering and Management Research, Vol. 2, Issue-1, Jan 2012 ISSN No.: 2250-0758 Pages: 1-3

[2] Special Report: Cyber warfare In The C-Suite .Steve Morgan, Editor-in-Chief. Sausalito, Calif. – Nov. 13, 2020

[3] stay safe India Cyber Stalking government website option cyber stalking.

[4] RBI Annual Report 2022-23

[5] A Survey of Voice Over Internet Protocol (VOIP) Technology. POURGHASEM1, S. KARIMI1 AND S. A. EDALATPANAH2, 3 IJCMSA: Vol. 6, No. 3-4, July-December 2012, pp. 53– 62

[6] Cybersquatting in the Age of Digital Era **Riya Gupta**
O. P. Jindal Global University - Jindal Global Law School/ Divita Vashisht O. P. Jindal Global University - Jindal Global Law School .Date Written: June 15, 2023.

[7] *[Submitted on 17 Jul 2020 (v1), last revised 16 Feb 2022 (this version, v5)]* Backdoor Learning: A Survey . Yiming Li, Yong Jiang, Zhifeng Li, Shu-Tao Xia.

[8] © 2021 IJCRT | Volume 9, Issue 9 September 2021 | ISSN: 2320-2882 Issues and Challenges of Cyber Crime in India: An Ethical Perspective Gobinda Bhattacharjee Lecturer, Dept. of Philosophy, Rabindranath Thakur Mahavidyalaya, Bishalgarh, Tripura, INDIA

[9] Cyber Crime Today & Tomorrow, Thiru Dayanithi Maran, http://w w w. d. m aran.nic.in/speechdisplay.ph,p?jd=i?

[10] Police make headway, The Hindu