REVIEW OF RESEARCH
ISSN: 2249-894X
IMPACT FACTOR : 5.7631(UIF)
VOLUME - 13 | ISSUE - 1 | OCTOBER - 2023

CYBER CRIME: A BUDDING ISSUE

Ms. Jyotsna
Assistant Professor, Department of Commerce,
Dyal Singh Evening College, Delhi University, Delhi.

ABSTRACT :

In the face of development, crime is nevertheless elusive and constantly tries to elude detection. Several countries, based on the type and severity of the crime, implemented various ways to combat it. A country with a high rate of crime cannot advance or grow. Crime is the exact opposite of what should be avoided. It has detrimental social and economic repercussions. Cybercrime is characterized as crimes done online using a computer as a tool or a specific target.

KEYWORDS : *detrimental social and economic repercussions , specific target.*

INTRODUCTION :

'Cyber crime' is a misnomer. In no statute or Act passed or adopted by the Indian Parliament is this term defined. The idea of cybercrime is not new. Extremely dissimilar to the idea of traditional crime both include behavior, whether it be an action or an inaction, that violates the law and is punished by the government.

Cybercrime may be broadly defined as "illegal acts in which a computer is either a tool, a target, or both." Financial crimes, the sale of illegal goods, pornography, online gambling, crimes against intellectual property, email spoofing, forgery, cyberdefamation, and cyberstalking are some examples of the types of activities of cyber crimes. However, the computer may be the target of illegal activities in the following scenarios: unauthorised access to computers, computer systems, or computer networks; theft of information stored in electronic form; e-mail bombing; data theft; salami attacks; logic bombs; Trojan attacks; theft of computer systems; and physical damage to computers.

India is on the radar of cyber criminals with increasing cyber attacks. Digital technology and cybercrime are pervasive features of modern life. The increased adoption of digital technology has caused an evolution in criminal behavior, resulting in the increased occurrence of 'cybercrime'.

There are many real and damaging consequences associated with cyber crimes. One of the major effect is loss of revenue. This loss can be caused by an outside party who obtains sensitive financial information, using it to withdraw funds from an organization. Another major effect is the time that is wasted from such crimes. This is in turn also damage the reputation and goodwill of the organization which leads to decreased productivity. Overall trust in the organization is lost in the long run.

LIST OF REFERENCES:-

- Bada M, Nurse JR (2020) The social and psychological impact of cyberattacks. In: *Emerging Cyber Threats and Cognitive Vulnerabilities*. Cambridge: Academic Press, 73–92.
- Bocij P, McFarlane L (2003) Cyberstalking: the technology of hate. *The Police Journal* 76: 204–221.
- Leukfeldt ER, Notté RJ, Malsch M (2020) Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Victims & Offenders* 15(1): 60–77.
- Nodeland B, Morris R (2020) A test of social learning theory and self-control on cyber offending. *Deviant Behavior* 41(1): 41–56.

Ms. Jyotsna
Assistant Professor, Department of Commerce, Dyal Singh Evening College,
Delhi University, Delhi.