IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Cybercrime Evolution: Dark Side of the Web

Ms. Manu Tyagi[1]*
Prof. (Dr) Shyam Lal**

Abstract

In response to the growing threat of cybercrime, governments, businesses, and individuals have had to invest in cyber security measures to protect sensitive data and prevent cyber attacks. These efforts have included the development of stronger encryption, firewalls, anti-virus software, and intrusion detection systems to guard against unauthorized access.

However, the arms race between cybercriminals and cyber security experts is ongoing. As technology continues to advance, so do the tools available to criminals, making it essential for law enforcement and organizations to continually evolve their strategies for combating cybercrime

Introduction:

With the growth of the internet and personal computing came an unexpected consequence: the rise of cybercrime. While the internet brought many benefits, it also opened new doors for criminals to exploit the vulnerabilities in digital systems. The advent of email, e-commerce, and online banking created new opportunities for fraudulent activities, identity theft, data breaches, and a wide range of cybercrimes.

As the internet grew, there was an increasing need to protect the privacy and security of digital transactions and communications. However, just as the internet allowed for unprecedented information exchange, it also became a tool for criminals to engage in activities such as hacking, phishing, spreading malware, and other cybercrimes. Criminals used the anonymity of the internet to commit offenses ranging from financial fraud to cyberbullying and cyber terrorism.

The idea of cybercrime is often tied to the 1980s, when computers began to be used more widely. However, its roots go back even further in history. Some argue that the first recorded instance of cybercrime occurred in 1820, long before the advent of modern computers. This event involves the Jacquard Loom-a device invented by Joseph-Marie Jacquard, a French textile manufacturer, which allowed the automation of weaving patterns.

The introduction of the Jacquard loom caused great fear among the workers, who believed their jobs were at risk. In response, some workers engaged in acts of sabotage to damage the loom and prevent its widespread

[1] ***Research Scholar, Shri Venkateshwara University, Gajraula, UP.**
****Research Supervisor, Shri Venkateshwara University, Gajraula, UP.**

use. While not a cybercrime in the modern sense, this incident can be seen as an early form of technological sabotage or resistance to technological change-a concept that would evolve into cybercrime over time.

The 1980s saw a surge in the use of computers, both in business and personal life. With this surge came new forms of criminal activity, such as hacking, identity theft, and data manipulation. The growing dependence on computers to store and process sensitive information made these systems prime targets for criminals. The personal computer became a tool not only for business and communication but also for criminal exploitation.

As businesses became more reliant on computer networks for data storage and communication, vulnerabilities emerged that allowed criminals to take advantage of the lack of security measures. These vulnerabilities were often exposed by catalyst events-specific high-profile incidents or cases that demonstrated the ease with which systems could be breached and the significant consequences of such breaches.

Criminals began to realize that they could easily encrypt sensitive information, store it securely, and even transmit it across networks with little fear of detection. The increasing complexity and sophistication of computer crimes meant that law enforcement struggled to keep pace. Computers could store vast amounts of data-often evidence of a crime-making it possible for criminals to hide their tracks or destroy evidence without detection.

The challenge was further exacerbated by the global reach of the internet. A computer crime scene could now extend from a victim's personal computer to any location across the globe. This global dimension created jurisdictional challenges and made it difficult for law enforcement to track and apprehend criminals who operated across borders.

LEGAL AND SOCIAL RECOGNITION OF CYBERCRIME:

As computer technology advanced and became more integrated into daily life, the legal and social recognition of cybercrime grew. The criminalization of harmful behaviors took time, often influenced by public outcry or specific "catalyst events" that captured the attention of lawmakers and the public. The early recognition of cybercrime often involved issues like hacking, computer fraud, and unauthorized access to digital systems.

In the early 1990s, cyber laws began to be enacted in various countries to address these emerging threats. In India, the Information Technology Act of 2000 was one of the first pieces of legislation aimed at regulating cybercrimes and electronic commerce. This was followed by increased global cooperation to fight cybercrimes, including the development of international treaties and agreements on cyber security.

CYBERCRIME IN THE 21ST CENTURY:

In the 21st century, cybercrime has become more sophisticated and widespread, fueled by advances in technology. The proliferation of Smartphone, the growth of social media, and the rise of cloud computing have created new opportunities for cybercriminals to exploit.

Some of the most common forms of cybercrime today include:

Hacking: Unauthorized access to computer systems to steal or manipulate data.

Phishing: Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity.

Malware: Malicious software used to damage or gain unauthorized access to a computer system.

Ransomware: A type of malware that locks users out of their systems or files until a ransom is paid.

Identity theft: The stealing of personal information for fraudulent purposes.

Cyberbullying: The use of digital platforms to harass, intimidate, or harm others.

As more people around the world become connected to the internet, cybercrime continues to evolve. With India now having the second-largest number of internet users globally, the need for effective cybersecurity measures and laws is more pressing than ever.

The history of cybercrime reflects the rapid evolution of computer technology, from the early days of room-sized computers to the modern internet-connected world. While technology has brought immense benefits, it has also created new challenges, as criminals adapt and find innovative ways to exploit digital systems. As the world becomes increasingly digital, the fight against cybercrime is more important than ever, requiring continuous legal, technological, and social efforts to ensure a secure online environment for all users.

IMPACT OF TECHNOLOGICAL ADVANCEMENT:

As computer technology progressed through the 1980s and beyond, legislators became increasingly aware of the vulnerabilities it created for criminal activity. Businesses, government agencies, and individuals began to depend more heavily on computerization for their daily operations, leading to a significant shift in how crimes were committed and investigated. This period marked the rise of cybercrime as a serious concern, with criminals exploiting the very technologies that were designed to simplify and enhance life.

ROLE OF COMPUTERS IN CYBERCRIME:

Computer technology altered the landscape of crime in profound ways. In some cases, the computer became the instrument of the crime, such as in hacking or the use of malware to steal personal or financial data. In other cases, the computer became the target of the crime, as seen in denial-of-service (DoS) attacks or cyber terrorism. Ransomware is another example, where the criminal locks the victim's computer system and demands payment to restore access.

Moreover, criminals increasingly used computers to store and protect the evidence of their illegal acts. The rise of digital forensics became a critical tool for law enforcement, but it was a field that was still evolving in the early days of cybercrime. In many instances, criminals relied on their knowledge of computer systems to avoid detection. They would hide evidence in encrypted files or use secure communications to transmit data, often making it incredibly difficult for investigators to trace the origins of the crime.

The technological gap between law enforcement and cyber criminals became a significant challenge. Investigators often lacked the specialized knowledge or skills to effectively handle cases involving computer crimes. As a result, cybercriminals had good reason to believe they could evade detection, especially when traditional law enforcement methods were ill-suited for investigating such crimes.

DOUBLE-EDGED SWORD OF TECHNOLOGICAL PROGRESS:

The rapid advancements in computer technology and the internet during the late 20th and early 21st centuries brought many positive changes to society. The internet made it possible to communicate across vast distances almost instantly, and the ability to gather and organize information became easier than ever before. This technological progress transformed various aspects of everyday life, from education to shopping to entertainment.

Businesses also benefited from the ability to operate more efficiently, utilizing digital tools to streamline workflows, manage resources, and interact with customers. The convenience and speed that computer technology offered brought about significant improvements in the quality of life for many people around the world.

However, this same technology that made life more convenient also opened new doors for criminal exploitation. Cybercriminals began to use the very tools designed to improve our lives for malicious purposes. The rise of cybercrime, such as identity theft, online fraud, phishing, and cyber bullying, highlighted the darker side of technological progress. The anonymity of the internet and the ability to conduct crimes remotely made it easier for criminals to target victims without fear of detection or apprehension.

GROWING COMPLEXITY OF CYBERCRIME:

As we entered the 21st century, the complexity and scope of cybercrime grew exponentially. Malware, including viruses, trojans, and ran somware, became more sophisticated, targeting both individuals and organizations. The rise of social media and mobile computing also created new opportunities for cybercriminals to engage in criminal activity, from data breaches to cyber stalking.

The globalization of the internet meant that a cybercriminal could operate from any part of the world and target victims anywhere else. This created significant challenges for law enforcement agencies, which had to navigate jurisdictional issues and deal with a lack of international cooperation in some cases.

Additionally, as e-commerce grew, so did the opportunities for cybercriminals to exploit online transactions. Online banking fraud, credit card fraud, and identity theft became widespread issues, further complicating efforts to protect consumers and businesses from cyber threats.

CONCLUSION:

The rise of computer technology and the internet has profoundly impacted society, bringing both immense benefits and new challenges. As the world became increasingly digitized, cybercriminals found new opportunities to exploit vulnerabilities in computer systems. The rapid pace of technological change has created an environment where criminals can easily commit crimes with little fear of detection, while law enforcement struggles to keep up with evolving threats. As we continue to advance into the digital age, the fight against cybercrime remains a critical concern for governments, businesses, and individuals alike. The need for robust cyber security measures, international cooperation, and ongoing vigilance has never been greater.

Bibliography:

1) Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (London, UK: Elsevier Inc., Third edition, 2011).
2) Barr, T. (2001), "E-Futures: Towards a better understanding of internet users", Deakin Lectures, www.abc.net.au/rn/deakin/default.html, accessed on September 19, 2019.
3) Slattery, L. (2001), "Snake oil for the ills of modern life". The Australian, 27 June, p.13
4) Starch, R. (1999). "The American Online/ Roper Starch Youth Cyberstudy 1999", Http:// www.corp.aol.com/ press/ study/youthstudy.pdf, accessed on September 19, 2023.
5) Halder D., & K Jaishankar, 'Patterns of Sexual Victimization of Children and Women in the Multipurpose Social Networking Sites.
6) In C. Marcum and G. Higgins (Eds.), Social Networking as a Criminal Enterprise, Boca Raton, FL, USA: CRC Press, Taylor and Francis Group. ISBN, 2014.
7) Interview with Karnika Seth, Cyber Law expert and visiting faculty to National Police Academy and National Judicial Academy, CBI Academy and National Investigation Agency, NOIDA.
8) Press Information Bureau, Government of India, Ministry of Women and Child Development, 3 March 2016. This information was given by the Minister for Women and Child Development, Mrs Maneka Sanjay Gandhi, in reply to a question in the Rajya Sabha.
9) Kothari, Jayna and Aparna Ravi, The Myth of Speedy and Substantive Justice: A Study of the Special Fast Track Courts for Sexual Assault and Child Sexual Abuse in Karnataka, Centre for Law and Policy Research, Bangalore.