Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 6): pp. 6560-6570
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.06.640

An Analytical Study On Cyber Crime In Indian Marketing

Dr. Naresh Mahipal Assistant Professor (Sr. Scale), Faculty of Law, University of Delhi.

Dr. Jyoti Garg Assistant Professor, Department of Law, Dr. C. V. Raman University, Bilaspur (C.G.)]

Abstract

India's meteoric rise in the digital age has been a double-edged sword. While the internet has empowered citizens, fueled economic growth, and established India as a global tech contender, it has also opened a Pandora's Box of cybercrime threats. This paper delves into the complexities of cybercrime in India, exploring its diverse landscape from prevalent financial scams and data breaches to sophisticated cyberattacks targeting critical infrastructure. The analysis extends beyond the technical aspects, examining the multifaceted impact of cybercrime on Indian society. It sheds light on how cybercrime erodes trust online, discourages social interaction, and has the potential to inflict lasting psychological damage on victims. Furthermore, the paper explores the economic consequences of cybercrime, including direct financial losses, investor apprehension, and the stifling of innovation. Real-world examples, like recent e-commerce website malware attacks, social media influencer fraud, and mobile app phishing attempts, illustrate the evolving nature of these threats. The paper acknowledges ongoing government initiatives, such as the National Cyber Security Agency (NSCA) and public awareness campaigns, but underscores the need for a more comprehensive approach. It emphasizes the importance of public-private partnerships, international cooperation, and robust cyber hygiene practices to create a safer digital space for all. Ultimately, this paper serves as a call to action, urging India to build a secure and resilient digital ecosystem that fosters continued progress in the face of the ever-present threat of cybercrime.

Keywords:-

- **Clandestine Operations:** Cybercrime activities.
- **Phishing Expeditions:** Deceptive attempts to steal personal information online.
- **Data Exfiltration:** Unauthorized extraction of sensitive data.
- **Digital Disruption:** Cyberattacks that cripple critical infrastructure.
- **Cyber Espionage:** Clandestine intelligence gathering through cyber means.
- **Crypto jacking:** Covert use of someone else's computer to mine cryptocurrency.
- **E-commerce Fraud:** Deceptive practices within online marketplaces.

- **Social Engineering Maneuvers:** Psychological manipulation tactics used in cybercrime.
- **Blockchain Security Vulnerabilities:** Weaknesses in the security of cryptocurrency systems.
- **Internet of Things (IoT) Attack Vectors:** Entry points for cybercriminals to exploit vulnerabilities in interconnected devices.

Literature Review:-

There have been many research studies on the topic of marketing and some specifically related to cybercrime. A selection of representative studies will be briefly reviewed here.

Marketing through online platform i.e., through E- commerce websites are more vulnerable to various risk, including cybercrime.

Zomori (2001) has done a combined study of risk caused by cyber-crime and money laundering. He stressed on the element of 'trust' in marketing. Loss of trust and the ability to do marketing would not only represent financial loss but a societal loss also.

Smith (2008) has done a review of widespread use of e-commerce in all types of business, including retails stores and other services firms. Smith (2010) examines various marketing strategies often used in digital media.

Oates (2001) stresses the importance of preventing, detecting, investigating, and prosecuting cybercrimes with the goal of reducing their impact on market, business as well as on society. Oates also stresses on the combined efforts in order to stop cybercrimes, of all societal groups, institutions to share the information openly so that they are used to detect and prevent the cybercrimes.

Riem (2001) found that the biggest threat to computer security in marketing business comes from employees, interns, consultants and contractors working within the company, rather than from the outsider hackers.

Yapp (2001) agrees that the greatest threat to security while doing any business or in markets is still from the insiders.

The eminent English Jurist Salmond has rightly observed that law seeks to regulate the conduct of individuals in the society.

Research Questions:-

The research questions addressed by this study include:

(1) What are some ways that cybercrime affects marketing activity? And

(2) What are the combined threats related to cybercrimes in marketing?

Results suggest that there are a number of types of cybercrime that have detrimental effects on marketing activity.

Introduction:-

India's digital revolution has been nothing short of phenomenal. From bustling online marketplaces to a burgeoning tech startup scene, the internet has become an inextricable thread woven into the fabric of Indian society. This digital transformation has empowered citizens, propelled economic growth, and positioned India as a global powerhouse. However, this rapid ascent has cast a long shadow - the ever-present threat of cybercrime. Millions of Indians have embraced the internet, participating in e-commerce, accessing government services online, and connecting with loved ones across the globe. This digital inclusion has fostered financial empowerment, enhanced communication, and broadened educational opportunities. The rise of Indian tech giants and the burgeoning startup ecosystem are testaments to the nation's digital prowess.

Types of Threats:-

- **The Looming Threat:** Yet, this digital dreamland harbors a sinister counterpart the world of cybercrime. India, with its vast user base and nascent cybersecurity infrastructure, has become a prime target for malicious actors. Cybercriminals exploit vulnerabilities, deploy sophisticated scams, and launch relentless attacks, jeopardizing the very foundation of India's digital progress.
- **A Multifaceted Threat:** Cybercrime in India encompasses a diverse spectrum of activities, financial scams that steal hard-earned savings, data breaches exposing personal information, and cyberattacks that disrupt critical infrastructure. These crimes erode trust in online transactions, stifle innovation, and inflict devastating economic damage.
- **Beyond the Numbers:** The impact of cybercrime transcends financial losses. It fosters fear and distrust online, discourages social interaction, and can have detrimental psychological consequences for victims. The erosion of privacy and the potential for social stigma further exacerbate the societal impact of cybercrime.
- **A Call to Action:** India stands at a crossroads. To fully realize the potential of its digital revolution, it must confront the challenge of cybercrime head-on. This paper delves into the complexities of cybercrime in India, analyzing the prevalent types and threats, their multifaceted impact on society and the economy, and explores recent, concerning examples. It also examines the ongoing efforts by the government and the need for public awareness campaigns to combat this growing menace. By fostering a collaborative approach involving government, industry, and citizens, India can build a secure and resilient digital ecosystem, ensuring a brighter future for all stakeholders.
-

Expanding the Impact of Cybercrime on the Economy:-

Cybercrime poses a burgeoning threat in India, impacting millions of individuals and organizations. According to the National Crime Records Bureau (NCRB), cybercrimes in India

in 2020 resulted in a staggering loss of rupees 66.66 crore, with 4850 reported cases. A recent report by the Indian cybercrime coordination Centre (14C) revealed that digital financial frauds accounted for staggering rupees 1.25 lakhs crore over the last three years. According to the National cybercrime Reporting Portal (NCRP), in 2020, at least 10319 crore was reported to be lost by victims of digital financial fraud. Cybercrime in India inflicts significant financial damage, but its impact goes beyond direct losses. It disrupts economic activity, discourages investment, and hinders innovation. Let's delve deeper into these economic consequences:

- **Direct Financial Losses:** This includes stolen funds through online scams, credit card fraud, and ransomware attacks. Businesses lose revenue due to data breaches and disruptions caused by cyberattacks. Individuals suffer financial hardship from identity theft and fraudulent transactions. The cumulative financial losses from cybercrime can be staggering, impacting both individuals and the national economy.
- **Erosion of Investor Confidence:** The prevalence of cybercrime can discourage foreign investors from entering the Indian market. Investors are wary of investing in a country with a weak cybersecurity posture, fearing data breaches, intellectual property theft, and disruptions to critical infrastructure. This lack of investor confidence can hinder economic growth and limit access to vital foreign capital.
- **Disruption of Business Operations:** Cyberattacks can cripple business operations, causing downtime, data loss, and productivity declines. Businesses may incur significant costs for restoration, investigation, and legal fees associated with cyber incidents. Furthermore, disruptions to supply chains due to cyberattacks on logistics or transportation infrastructure can have a ripple effect across the economy.
- **Increased Security Costs:** Businesses are forced to invest heavily in cybersecurity measures to protect their data and infrastructure. This includes costs for security software, hardware upgrades, employee training, and incident response plans. These expenses can strain profit margins and divert resources away from core business activities.
- **Stifling Innovation:** The fear of cybercrime can discourage businesses from adopting innovative technologies and online business models. Companies may be hesitant to invest in cloud computing, e-commerce platforms, or the Internet of Things (IoT) due to cybersecurity concerns. This can stifle innovation and hinder India's digital transformation.
- **Impact on Reputation:** Cyberattacks on major corporations or government institutions can damage India's reputation as a reliable and secure business environment. This negative image can discourage foreign investment, tourism, and international trade.

Case Study:-

6563 | Dr. Naresh Mahipal An Analytical Study On Cyber Crime In Indian Marketing

1. E-commerce Malware Mayhem : A Breach of Trust

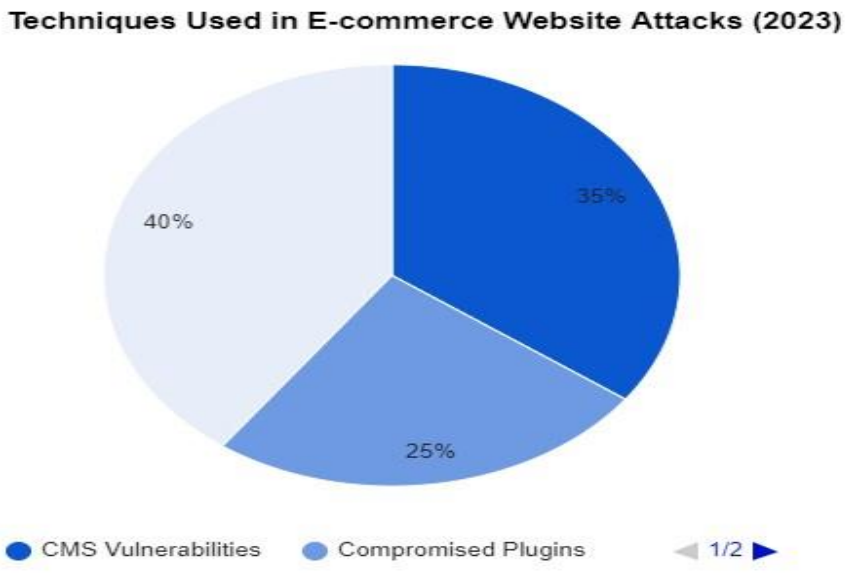
Imagine browsing a trusted e-commerce website, adding items to your cart, and feeling confident about entering your payment details. Suddenly, the news breaks – the website has been infiltrated with malware! This was the harsh reality for many Indian online shoppers. Cybercriminals launched a series of attacks, injecting malicious software into popular e-commerce platforms. These programs lurked unseen, waiting to capture sensitive information like credit card numbers and passwords.

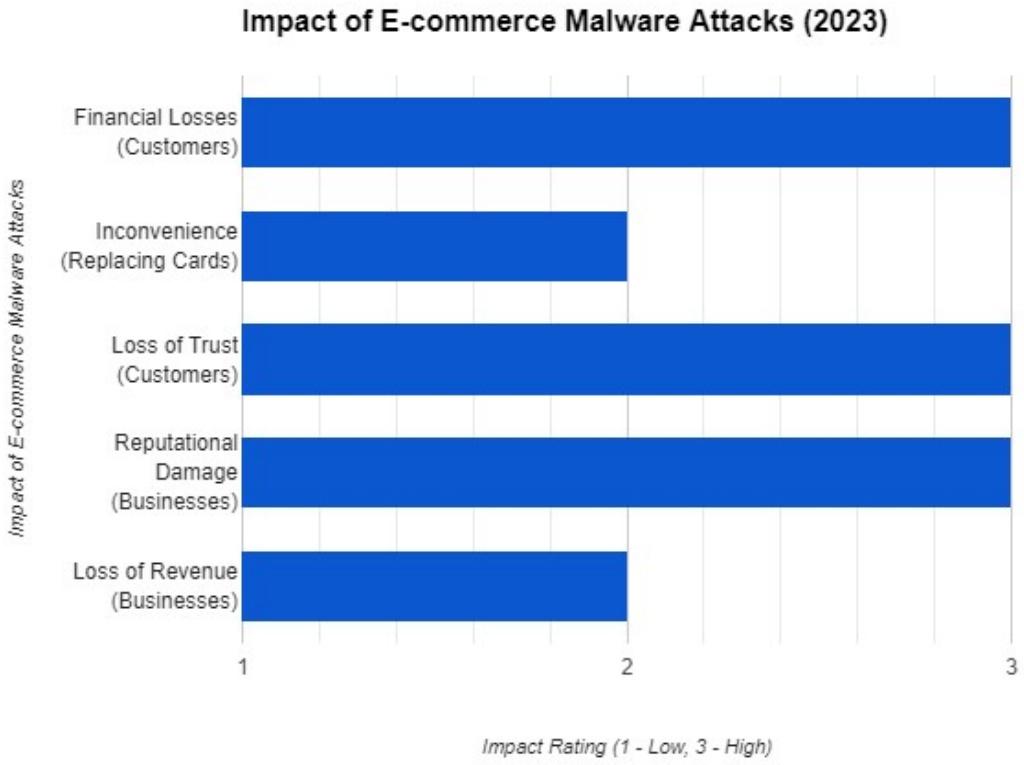
In what ways:

- **Exploiting Weaknesses:** Cybercriminals are adept at finding chinks in the armor. They targeted vulnerabilities in the software used to manage the content of these e-commerce websites (CMS) – the digital tools that power online stores.
- **Compromised Plugins:** Just like apps for your phone, websites can use plugins to add features. Hackers found ways to compromise these plugins, creating backdoors into the websites.
- **Social Engineering Schemes:** Sometimes, the simplest approach works. Cybercriminals may have launched phishing attacks or other social engineering tactics to trick website administrators into handing over their login credentials.

The Aftermath:

The consequences were severe. Customers who had unknowingly entered their payment information became victims of fraud. Financial losses were widespread, and the inconvenience of replacing compromised cards added insult to injury. More importantly, trust in online shopping platforms took a hit. Consumers became wary of entering their financial details online, potentially hindering the growth of e-commerce in India. For the businesses themselves, the reputational damage was significant. Regaining consumer confidence became a top priority.





2. Social Media Influencer (2019-Ongoing): Deception Disguised as Popularity

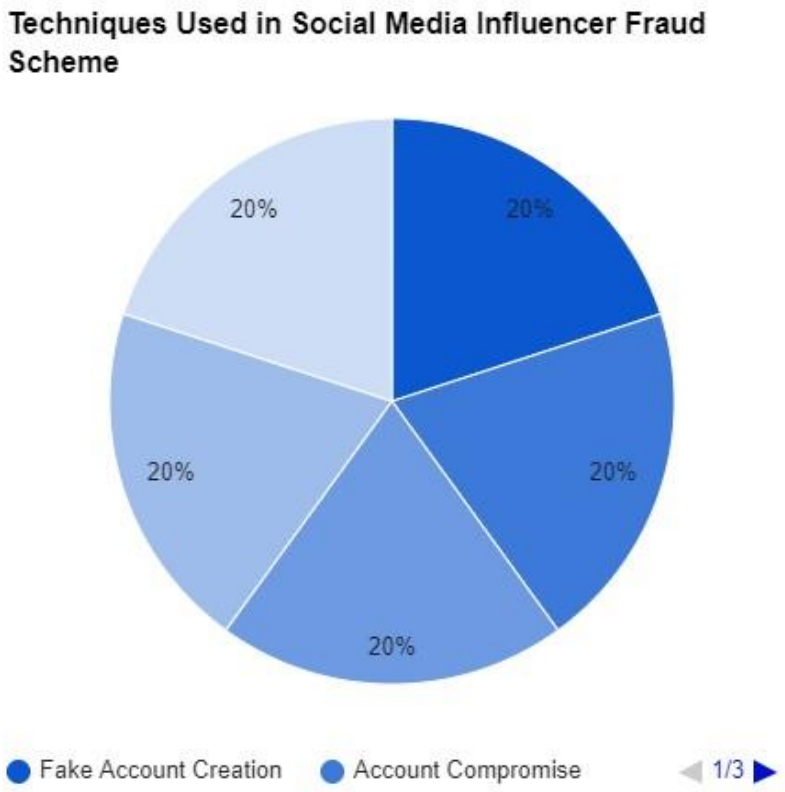
In today's world, social media influencers hold immense power. Their recommendations can sway purchasing decisions and influence investment choices. However, this influence has become a target for cybercriminals, leading to a concerning trend – social media influencer fraud. This ongoing scheme, active since 2019, exploits the trust people have in these online personalities.

The Scheme:

- **Fake Identities:** Cybercriminals may create fake accounts that mimic popular influencers, complete with stolen photos and fabricated biographies. These imposters then promote bogus investment schemes or endorse fake products, tricking unsuspecting followers.
- **Account Takeover:** Alternatively, they may compromise the accounts of genuine influencers. Through hacking or social engineering tactics, they gain access to the influencer's account and use it to spread misinformation or promote scams.
- **Deceptive Marketing:** The tactics used to lure victims are sophisticated. Phony testimonials, fake celebrity endorsements, and promises of high returns with minimal risk paint a picture of legitimacy.

The Damage:

The consequences of social media influencer fraud are multifaceted. Victims who fall prey to these scams can suffer significant financial losses. The emotional toll can also be substantial, with feelings of betrayal and frustration impacting victims. Trust in online advertising plummets as consumers become wary of influencer recommendations. Furthermore, the credibility of genuine influencers is tarnished, making it harder for them to promote legitimate products and services.



3. Mobile App Phishing Frenzy: A Wolf in Sheep's Clothing

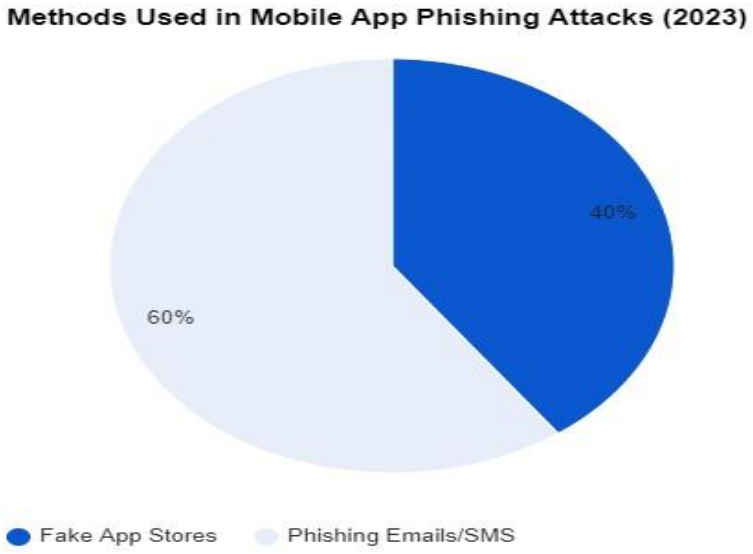
The convenience of mobile apps has revolutionized our lives. However, this convenience comes with a hidden threat - mobile app phishing attacks. In past, India witnessed a surge in these attacks, highlighting the need for vigilance in the mobile app ecosystem.

The Methods:

- **Fake App Stores:** Cybercriminals create fake app stores that appear legitimate, offering a wide range of applications. These stores may host pirated versions of popular apps or distribute malware disguised as legitimate software. Unsuspecting users, lured by the promise of free or discounted apps, download and install them, unknowingly compromising their devices.
- **Phishing Emails and SMS:** Deceptive emails or text messages may arrive, promoting seemingly legitimate apps. These messages may trick users into clicking on malicious links that download malware or redirect them to fake app stores.

The Impact:

The consequences of mobile app phishing attacks can be devastating. Downloaded malware can steal sensitive data like bank account details, passwords, and contact information. This can lead to financial losses, identity theft, and even account hijacking. Victims may also experience frustration and a sense of helplessness as they navigate the process of recovering from a cyberattack.



Government initiative towards the Cybercrime:-

The Indian government recognizes the growing threat of cybercrime and has undertaken several initiatives to combat it:

- **National Cyber Security Agency (NSCA):** Established in 2017, the NSCA serves as the nodal agency for cybersecurity policy formulation, coordination, and implementation. It facilitates information sharing among stakeholders, develops cybersecurity frameworks and guidelines, and promotes capacity building initiatives.
- **Indian Computer Emergency Response Team (CERT-In):** Functioning under the Ministry of Electronics and Information Technology (MeitY), CERT-In is the national agency responsible for cyber security emergencies. It issues advisories and alerts about cyber threats, coordinates cyber security incident response, and manages the national cybercrime reporting portal.
- **Cyber Swachta Kendra (Botnet Cleaning and Malware Analysis Centre):** This government initiative provides free tools and services to detect and remove malware from infected systems. It also analyzes malware to understand the tactics and techniques employed by cybercriminals.
- **National Cyber Crime Reporting Portal:** This online platform allows citizens to report cybercrimes easily and conveniently. The portal facilitates the registration of

complaints, tracking of investigation progress, and provides guidance on online safety measures.

- **Cyber Surakshit Bharat Initiative:** Launched in 2018, this initiative aims to raise awareness about cyber security and create a culture of cyber hygiene. It focuses on capacity building for government officials, critical infrastructure operators, and the general public.
- **Collaboration with Law Enforcement Agencies:** The government works closely with law enforcement agencies to investigate cybercrimes, apprehend cybercriminals, and strengthen legal frameworks to deter cybercrime activities.

Conclusion:-

Cybercrime in India presents a complex and multifaceted challenge. From sophisticated financial scams to disruptive infrastructure attacks, the evolving threats demand a multi-pronged approach. This paper has explored the various types and threats of cybercrime, their wide-ranging societal and economic impacts, and provided real-world examples that illustrate the dangers lurking in the digital landscape.

The ongoing efforts of the Indian government, including the National Cyber Security Agency (NSCA) and public awareness campaigns, are commendable. However, building a truly secure digital ecosystem requires a collaborative effort. Public-private partnerships, fostering international cooperation, and promoting robust cyber hygiene practices are crucial.

Individuals can play a vital role by remaining vigilant, practicing safe online habits, and keeping software updated. Businesses must prioritize cybersecurity investments and implement robust data protection measures.

By acknowledging the gravity of the situation and adopting a proactive approach, India can build a more secure and resilient digital landscape. This will not only safeguard citizens and businesses but also pave the way for continued economic growth and social progress in the digital age. The fight against cybercrime is a marathon, not a sprint. Through constant vigilance, collaboration, and innovation, India can navigate this challenge and ensure a brighter digital future for all its stakeholders.

Suggestions Or Recommendation:-

After the brief study on the topic, I recommend the following suggestions. These are as under:-

1. Combined efforts should be taken by private individual, public sectors and the government to overcome the cybercrime in market.
2. A strong password and security programs must be use so that a strong privacy protection can be made.
3. Government should initiate new programs to reduce the cybercrimes in market.

4. Government should implement new special laws on cybercrime which specifically protect the cybercrime in India.
5. The jurisdiction of Information technology laws should be widened so that it covers all related issues.
6. A separate forensic expert team should be appointed by the government which is specifically deal with the cybercrime.

References:

- News Articles: Major Indian news outlets like The Times of India, The Economic Times, and Hindustan Times frequently cover cybercrime issues in India.
- Government Websites: The websites of the National Cyber Security Agency (NSCA), MeitY (Ministry of Electronics and Information Technology), and CERT-In (Indian Computer Emergency Response Team) provide valuable information about cybercrime trends, government initiatives, and resources for citizens and businesses.
- Industry Reports: Cybersecurity research firms like Gartner, McAfee, and Palo Alto Networks publish periodic reports on the global cybercrime landscape, often with specific insights into India.
- Academic Journals: Scholarly articles published in journals like the Journal of Cyber Policy, Computers & Security, and the International Journal of Cybercrime and Information Warfare delve deeper into the technical and social aspects of cybercrime.
- www.cybercrime.gov/cccases.html.
- Bansal S.K. “Cyber Crimes” (2003) P 276.
- The European Convention cybercrime was held in June, 2001.
- Dr. Amita Verma “Cybercrime and Law” (Central Law Publications) 2009.
- R Nagpal ‘what is Cyber Crime’ (2003).
- Wall, D.S. 2001. “Cybercrimes and the internet.” In crime and the internet, edited by D.S. Wall, 1-17, New York: Routledge.