iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.53073

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Trends in Cyber Crime in India

Kashish Dahiya
Amity University, Noida

***Abstract:** This research paper explores the trends in Cyber Crime in India, considering the country's rapidly growing digital landscape and the associated risks. The introduction provides an overview of the digital transformation in India and its dual impact, highlighting the alarming increase in Cyber Crime. One prominent trend discussed is the rise of phishing attacks, where cyber criminals employ deceptive tactics to trick individuals into revealing sensitive information. Another concerning trend is the proliferation of Ransomware attacks that target various sectors, causing significant financial losses and operational disruptions. Additionally, cyber fraud targeting financial transactions and digital payment systems has become prevalent. The paper also highlights the risks associated with social media platforms and online marketplaces, including identity theft and the sale of illegal goods and services. To address these escalating cyber threats, the paper emphasises the importance of prioritising cybersecurity measures, raising awareness about safe online practices, and establishing robust legal frameworks. The findings underscore the urgent need for individuals, organisations, and the government in India to work together to combat Cyber Crime effectively and secure the nation's digital future.*

I. INTRODUCTION TO TRENDS IN CYBER CRIMES IN INDIA

The rapid advancement of technology and the widespread adoption of the internet have brought about numerous benefits and opportunities for individuals and businesses in India. However, this digital transformation has also given rise to a dark side: an alarming increase in cyber-crime. India, with its large population and expanding digital footprint, has become a fertile ground for cyber criminals to carry out their illicit activities. From financial frauds and data breaches to online scams and identity theft, the trends in cyber-crime within the country have taken on a disturbing trajectory. One prominent trend is the rise of phishing attacks, where cyber criminals use deceptive tactics to trick individuals into revealing sensitive information such as passwords, credit card details, or personal identification.

These attacks often employ highly convincing emails, messages, or websites that appear legitimate, making it challenging for users to distinguish them from genuine sources. Another concerning trend is the proliferation of ransomware attacks, which involve malicious software that encrypts a victim's data and demands a ransom payment for its release. These attacks have targeted various sectors, including government organisations, healthcare institutions, and businesses, causing significant financial losses and operational disruptions.

Furthermore, India has witnessed an increase in cyber frauds targeting financial transactions, online banking, and digital payment systems. Fraudsters employ sophisticated techniques to exploit vulnerabilities in these systems, resulting in substantial monetary losses for individuals and businesses alike.

Additionally, social media platforms and online marketplaces have become breeding grounds for cyber criminals, who engage in identity theft, online harassment, and the sale of illegal goods and services. To address these escalating cyber threats, it is imperative for individuals, organisations, and the government to prioritise cybersecurity measures, raise awareness about safe online practices, and establish robust legal frameworks to combat cyber crime effectively. Only through concerted efforts can India mitigate the risks posed by cyber criminals and secure its digital future.

II. WHAT IS CYBER CRIME

Cyber crime refers to illegal activities that are committed using computer networks or digital devices, typically over the internet. It involves the use of technology, such as computers, networks, and the internet, to commit criminal acts or exploit vulnerabilities for illicit purposes.

Cyber crime can take various forms, including financial fraud, cyber attacks, online harassment, data breaches, cyber terrorism, intellectual property theft, cyber extortion, social media crimes, and online gambling, among others. It poses significant challenges in terms of detection, investigation, and prosecution, and requires collaborative efforts from various stakeholders to combat and mitigate the risks associated with cyber crime.

A. Cyber Crime Can Be Broadly Categorised Into Several Types, Including

Cybercrimes can be classified based on the targets they affect, including individuals, property, organisations, and society as a whole. Here's a classification of cybercrimes according to these categories:

1) Crimes against Individuals

Cybercrimes against individuals refer to illegal activities conducted through computers, computer networks, or the internet that directly target and impact individuals. These crimes exploit technological vulnerabilities to cause harm, steal personal information, or violate the privacy and security of individuals. Here are some examples of cybercrimes against individuals:

a) Email spoofing is a technique used in cyber attacks where the attacker sends an email that appears to be from a legitimate source, but in reality, the sender's identity is falsified or forged. By manipulating the email headers, the attacker deceives the recipient into believing that the email originated from a trusted individual or organisation. This form of deception is often used for various malicious purposes, such as phishing scams, distributing malware, or tricking recipients into revealing sensitive information. Email spoofing can be particularly effective when combined with social engineering techniques to manipulate the recipient's trust and encourage them to take actions that benefit the attacker. To combat email spoofing, organisations and individuals can implement email authentication protocols, such as SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail), which help verify the authenticity of email sources. Additionally, user education and awareness about email security best practices, such as verifying email addresses, being cautious of suspicious requests, and refraining from clicking on suspicious links or downloading attachments, are crucial in mitigating the risks associated with email spoofing attacks.

b) Email spamming refers to the practice of sending unsolicited and unwanted bulk emails to a large number of recipients. These emails are typically commercial in nature and often contain advertisements, promotional offers, or fraudulent schemes. Email spammers often obtain email addresses through various means, including purchasing mailing lists, scraping websites, or using automated software to generate random email addresses. The purpose of email spamming is to reach as many recipients as possible in the hopes of generating responses or driving traffic to specific websites. However, spam emails can be a significant nuisance, clogging up inboxes, wasting valuable time, and potentially spreading malware or phishing attempts. To combat email spam, organisations and individuals utilise spam filters and email security systems that detect and block known spam messages. Additionally, users should exercise caution when sharing their email addresses online, avoid responding to or clicking on suspicious emails, and report spam emails to their email service providers. Ongoing advancements in spam detection technology and increased awareness about email security help to mitigate the impact of email spamming on individuals and organisations.

c) Cyber defamation, also known as online defamation or internet defamation, refers to the act of making false and damaging statements about an individual, business, or organisation through digital channels such as social media, websites, or online forums. It involves the publication of defamatory content that harms the reputation, character, or credibility of the target. Cyber defamation can take various forms, including false accusations, spreading rumours, posting misleading information, or creating fake profiles with the intent to tarnish someone's image or reputation. The widespread reach and accessibility of the internet make cyber defamation particularly potent, as defamatory statements can quickly spread and have long-lasting effects. Victims of cyber defamation may suffer significant emotional distress, reputational harm, and even financial losses. Laws and regulations regarding defamation vary across jurisdictions, but individuals and organisations can take legal action against perpetrators of cyber defamation. To protect against cyber defamation, individuals should be cautious about their online activities, think critically before sharing or reposting information, and consider privacy settings and security measures to safeguard their personal and professional reputations.

d) Cyber stalking is a form of harassment and intimidation that occurs through digital means, such as the internet, social media, or electronic communication channels. It involves a persistent and unwanted pursuit of an individual, causing them fear, distress, or emotional harm. Cyber stalkers use various tactics to monitor, track, and invade the privacy of their victims, such as sending threatening or abusive messages, spreading false information, or engaging in online surveillance. They may also engage in identity theft, impersonation, or the creation of fake profiles to further harass their victims. Cyber stalking can have severe psychological and emotional consequences for the targeted individuals, including anxiety, depression, and a loss of personal safety. Victims of cyberstalking should document the evidence, block or report the harasser, and seek support from law enforcement and support organisations specialising in cybercrime.

To protect against cyber stalking, individuals should exercise caution when sharing personal information online, regularly review and adjust privacy settings, and be mindful of their online connections and interactions.

2) Crime against Property

Cybercrimes against property are illegal activities carried out through computers, computer networks, or the internet that target and impact property, assets, or digital infrastructure. These crimes exploit technological vulnerabilities to gain unauthorised access, cause damage, or steal valuable information. Here are some examples of cybercrimes against property:

a) Credit card fraud: It is a prevalent form of cybercrime against property that poses significant risks to individuals, businesses, and financial institutions. It involves the unauthorised use of credit card information to make fraudulent transactions or obtain financial gain. Cybercriminals employ various techniques to carry out credit card fraud, including skimming, phishing, carding, card-not-present fraud, account takeover, identity theft, and exploiting malware and data breaches. These criminals aim to obtain sensitive credit card details, such as card numbers, expiration dates, and security codes, either through physical devices or online methods. Once they have this information, they can make unauthorised purchases, engage in identity theft, or sell the stolen data on the dark web. Credit card fraud not only leads to financial losses for individuals but also impacts businesses and financial institutions, which bear the burden of chargebacks and compromised customer trust. To combat credit card fraud, individuals must safeguard their credit card information, be vigilant for phishing attempts, and regularly monitor their statements for suspicious transactions. Financial institutions employ fraud detection systems to identify and prevent fraudulent activities, while collaboration between businesses, law enforcement agencies, and payment processors is essential for sharing information and coordinating efforts to combat credit card fraud. By implementing robust security measures, raising awareness, and enhancing fraud prevention technologies, we can reduce the occurrence of credit card fraud and protect both individuals and businesses from financial harm.

b) Intellectual property (IP) crime: which involves the unauthorised use, reproduction, distribution, or theft of copyrighted material, trade secrets, or proprietary information. Intellectual property crime in the cyber realm poses significant threats to individuals, businesses, and industries. Cybercriminals engage in activities such as copyright infringement, software piracy, trade secret theft, counterfeit products, online brand abuse, digital content theft, online streaming piracy, reverse engineering, and patent infringement. These activities undermine the rights and economic interests of creators, innovators, and businesses. By unlawfully reproducing or distributing copyrighted material, cybercriminals deprive content creators of rightful earnings. Trade secret theft compromises the competitive advantage and investment made by businesses. Counterfeit products harm both consumers and legitimate brands. Infringing on patents hinders innovation and discourages research and development efforts. To combat intellectual property crime, efforts are made to strengthen copyright laws, enforce intellectual property rights, collaborate with international agencies, and raise awareness about the importance of respecting intellectual property. Businesses employ security measures, such as digital rights management systems and trademark monitoring, to protect their intellectual property online. Education and public awareness campaigns play a crucial role in promoting respect for intellectual property rights and encouraging responsible consumption of digital content. By addressing intellectual property crime, we can foster an environment that fosters innovation, creativity, fair competition, and respect for intellectual property rights.

c) Internet time theft: which involves the unauthorised use or misuse of internet or computer resources, leading to financial losses or exploitation of services. Internet time theft can occur in various forms, targeting both individuals and organisations. It involves activities such as unauthorised use of internet services, identity theft and account takeover, phone phreaking, toll fraud, manipulation of internet advertising, resource misuse, and stealing paid services. Cybercriminals exploit vulnerabilities in networks and systems to gain unauthorised access, bypass payment mechanisms, or manipulate services for their benefit. These activities result in financial losses for service providers, individuals, or organisations that bear the costs of unauthorised usage. To combat internet time theft, individuals and organisations should employ measures such as securing Wi-Fi networks, enabling two-factor authentication, monitoring account activities, establishing internet usage policies, implementing network monitoring and auditing, and staying informed about emerging threats. Collaboration between individuals, organisations, and law enforcement agencies is crucial in investigating and prosecuting those involved in internet time theft, as well as implementing preventive measures to safeguard internet resources and mitigate financial losses. Cybercrimes against property can result in financial loss, reputational damage, disruption of services, compromised intellectual property, and erosion of customer trust.

It is crucial for individuals and organisations to implement robust cybersecurity measures, including firewalls, encryption, regular system updates, and employee training to prevent and mitigate these threats.

Collaboration between law enforcement agencies, cybersecurity experts, and affected organisations is essential in investigating these crimes, bringing perpetrators to justice, and developing proactive strategies to combat cyber threats.

3) Crime against Organisations

Crimes against organisations encompass a range of illegal activities specifically targeted at businesses and institutions. These crimes include data breaches, insider threats, financial fraud, corporate espionage, sabotage, and more. They can result in financial losses, reputational damage, disruption of operations, and compromised data security. Perpetrators may seek to steal sensitive information, gain unauthorised access, manipulate financial records, or sabotage infrastructure. To mitigate these risks, organisations must implement robust cybersecurity measures, conduct regular risk assessments, educate employees on security best practices, and establish incident response plans. Collaboration with law enforcement agencies and staying updated on emerging threats are also crucial in combating crimes against organisations.

a) Unauthorised Access refers to the act of gaining entry to a computer system, network, or digital resource without proper authorization or permission. It is a serious cybercrime that can lead to significant harm, including data breaches, privacy violations, financial losses, and disruption of operations. Cybercriminals exploit vulnerabilities in security systems or employ various techniques such as password cracking, social engineering, or exploiting weak authentication mechanisms to gain unauthorised access. Once inside, they may steal sensitive information, install malware, alter or delete data, or use the compromised system as a launching pad for further attacks. To prevent unauthorised access, organisations and individuals must implement strong access controls, utilise multi factor authentication, regularly update and patch systems, monitor network activities, and educate users about the importance of strong passwords and vigilant cybersecurity practices.

b) Denial of Service (DoS) attack is a cyberattack that aims to disrupt the availability of a computer system, network, or website, rendering it inaccessible to legitimate users. In a DoS attack, the attacker overwhelms the targeted system with a flood of malicious traffic or resource-intensive requests, exhausting its computing resources or network bandwidth. This overload leads to a severe degradation in performance or a complete shutdown of the targeted service, denying access to genuine users. DoS attacks can be executed using various methods, including botnets, network congestion attacks, or exploiting vulnerabilities in network protocols. The impacts of a DoS attack can be detrimental, resulting in financial losses, reputational damage, and disruption of critical services. To mitigate DoS attacks, organisations employ strategies such as traffic filtering, load balancing, intrusion detection systems, and the use of content delivery networks (CDNs) to distribute and handle traffic effectively. Additionally, robust incident response plans and collaboration with internet service providers (ISPs) and cybersecurity experts are crucial to minimise the impact and quickly restore affected services.

c) Virus attack is a malicious act in which a computer system or network is infected by a self-replicating program that can spread and cause harm. Viruses are typically designed to disrupt system functionality, corrupt or delete data, steal sensitive information, or gain unauthorised access. Once a virus infects a host system, it can propagate to other connected devices, spreading rapidly and potentially causing widespread damage. Virus attacks often occur through infected email attachments, compromised websites, or downloads from untrusted sources. They can result in system crashes, data loss, privacy breaches, and financial losses. To protect against virus attacks, individuals and organisations should use up-to-date antivirus software, regularly apply security patches, exercise caution when opening email attachments or clicking on suspicious links, and maintain secure backups of critical data. Additionally, user awareness, strong cybersecurity practices, and prompt response to any detected infections are vital in mitigating the risks associated with virus attacks.

d) Email bombing is also known as email flooding or email bombing attack, is a form of cyber attack in which an individual or a group overwhelms a target's email account with an excessive amount of emails, causing disruption and inconvenience. The attacker typically sends a large volume of emails to the target's email address, flooding their inbox and consuming their available storage space. This can lead to the target's email service becoming unresponsive, difficulty in accessing legitimate emails, or even complete email service outage. Email bombing attacks can be initiated for various reasons, including harassment, revenge, or as a form of protest. To mitigate email bombing attacks, email service providers and individuals can implement spam filters, rate limiting mechanisms, and email authentication protocols to identify and block excessive incoming emails. Additionally, users should be cautious when sharing their email addresses and report any suspicious or abusive email activity to the appropriate authorities or email service providers.

e) Salami attack, also known as salami slicing or penny shaving attack, is a type of cybercrime where small, unnoticed fraudulent transactions or activities are carried out over a period of time to accumulate significant gains.

The attacker manipulates financial systems or processes to syphon off tiny amounts of money or assets, which individually go unnoticed, but collectively result in substantial illicit profits. This technique is often used in financial sectors, such as banking or investment accounts, where the attacker can exploit vulnerabilities in automated systems or take advantage of rounding errors or decimal truncation. The term "salami attack" comes from the idea of slicing off small pieces, like slices of salami,

without raising suspicion. To prevent salami attacks, organisations need to implement robust fraud detection mechanisms, conduct regular audits, monitor transactional patterns, and educate customers on security measures. Additionally, strong security controls, system monitoring, and anomaly detection can help identify and prevent such fraudulent activities from occurring.

f) Logic bomb is a malicious piece of code or software program that is intentionally inserted into a system with the purpose of triggering a harmful action or event at a specific time or under certain conditions. Unlike other types of malware, a logic bomb remains dormant until the predetermined trigger condition is met, such as a specific date, a specific action, or the absence of a particular event. Once activated, the logic bomb can carry out a range of malicious activities, including deleting files, disrupting system functionality, or spreading other types of malware. Logic bombs are often covertly inserted by insiders or disgruntled employees who have access to the system or application. These hidden threats can be challenging to detect as they do not exhibit any suspicious behaviour until the trigger condition is met. To mitigate the risk of logic bomb attacks, organisations should implement robust security measures, regularly monitor and audit systems for suspicious activities, restrict access privileges, and conduct thorough background checks on employees with system or code access. Additionally, maintaining up-to-date antivirus software and employing intrusion detection systems can help identify and neutralise potential logic bomb threats.

g) Trojan horse, or simply Trojan, is a type of malicious software that disguises itself as a legitimate program or file, deceiving users into unknowingly installing or executing it on their systems. Similar to the ancient Greek story of the Trojan horse, these programs appear harmless or useful but contain hidden malicious code that can cause significant harm once activated. Trojans can take various forms, such as fake software updates, games, or even email attachments. Once inside a system, Trojans can perform a wide range of malicious activities, including stealing sensitive information, granting unauthorised access to the attacker, creating backdoors for remote control, or facilitating the installation of additional malware. Unlike viruses or worms, Trojans do not self-replicate but rely on user actions to spread. To protect against Trojan attacks, users should exercise caution when downloading files or opening email attachments from unknown or suspicious sources, regularly update their operating systems and security software, and employ firewalls and comprehensive malware detection tools to identify and prevent the infiltration of Trojan horses.

h) Data Diddling is a form of cyber attack where an individual or a malicious insider manipulates or alters data before or during its entry into a computer system, with the intention of misleading or deceiving users or gaining unauthorised benefits. This manipulation of data can occur at various stages, including during data input, transmission, or storage, and is often done without detection. Data diddling attacks can have serious consequences, such as financial fraud, identity theft, or the compromise of sensitive information. Attackers may modify transaction amounts, change account details, manipulate inventory records, or tamper with critical data to create discrepancies or cause chaos within systems. To mitigate the risks associated with data diddling attacks, organisations should implement strict access controls, regularly monitor and audit data integrity, enforce segregation of duties, employ encryption and secure transmission protocols, and educate employees on data security best practices. Additionally, implementing data validation mechanisms, utilising backup and recovery procedures, and conducting regular security assessments can help detect and prevent data diddling attacks.

4) Crime against Society

a) Forgery is a type of crime against society that involves the creation, alteration, or use of fraudulent documents, signatures, or other forms of written or printed material with the intention to deceive or defraud others. It is a serious offence that undermines the trust and integrity of legal, financial, and administrative systems. Forgery can take various forms, including counterfeit currency, forged identification documents, fake contracts, falsified academic credentials, or manipulated official records. The consequences of forgery can be significant, leading to financial losses, reputational damage, legal disputes, and compromised public safety. To combat forgery, governments, financial institutions, and regulatory bodies implement security features in documents, employ verification methods, and establish stringent penalties for offenders.

Advanced technologies such as watermarking, holograms, and digital signatures are utilised to enhance document authenticity and deter forgery attempts. Education and awareness campaigns are also essential in educating the public about the signs of forgery and promoting vigilance to protect against such fraudulent activities.

b) Cyber Terrorism refers to the use of cyber attacks and computer technology by individuals or groups with the intent to inflict harm, create fear, or disrupt critical infrastructure for political, ideological, or ideological reasons. It involves the exploitation of digital systems, networks, and information to carry out acts of terrorism in the virtual realm.

Cyber terrorists target a wide range of entities, including government institutions, military organisations, public utilities, financial systems, and private companies, with the aim of causing significant damage, chaos, or disruption. The attacks can take various forms, such as distributed denial-of-service (DDoS) attacks, hacking, data breaches, spreading malware, or even cyber espionage. The consequences of cyber terrorism can be severe, leading to economic losses, compromise of national security, loss of public trust, and potential risks to human lives. Governments and international organisations work together to develop robust cybersecurity measures, enhance information sharing and cooperation, and enact legislation to combat cyber terrorism. It requires a comprehensive approach involving proactive defence strategies, intelligence gathering, early detection, and swift response to mitigate the risks posed by cyber terrorists.

c) Web Jacking, also known as website hijacking, is a cyber attack where an attacker gains unauthorised control over a website or web server. In a web jacking incident, the attacker exploits vulnerabilities in the website's security, such as weak passwords, outdated software, or unprotected administrative interfaces. Once access is gained, the attacker can modify the website's content, deface the pages, steal sensitive information, or redirect visitors to malicious websites. Web jacking can have serious consequences, including reputational damage, loss of customer trust, and financial losses for businesses. To prevent web jacking, website owners and administrators should regularly update their software, use strong and unique passwords, employ security measures such as firewalls and intrusion detection systems, and conduct regular security audits. Additionally, monitoring web traffic and implementing strong access controls can help detect and mitigate potential web jacking attacks. Rapid response and restoring the website's integrity are crucial in minimising the impact of web jacking incidents.

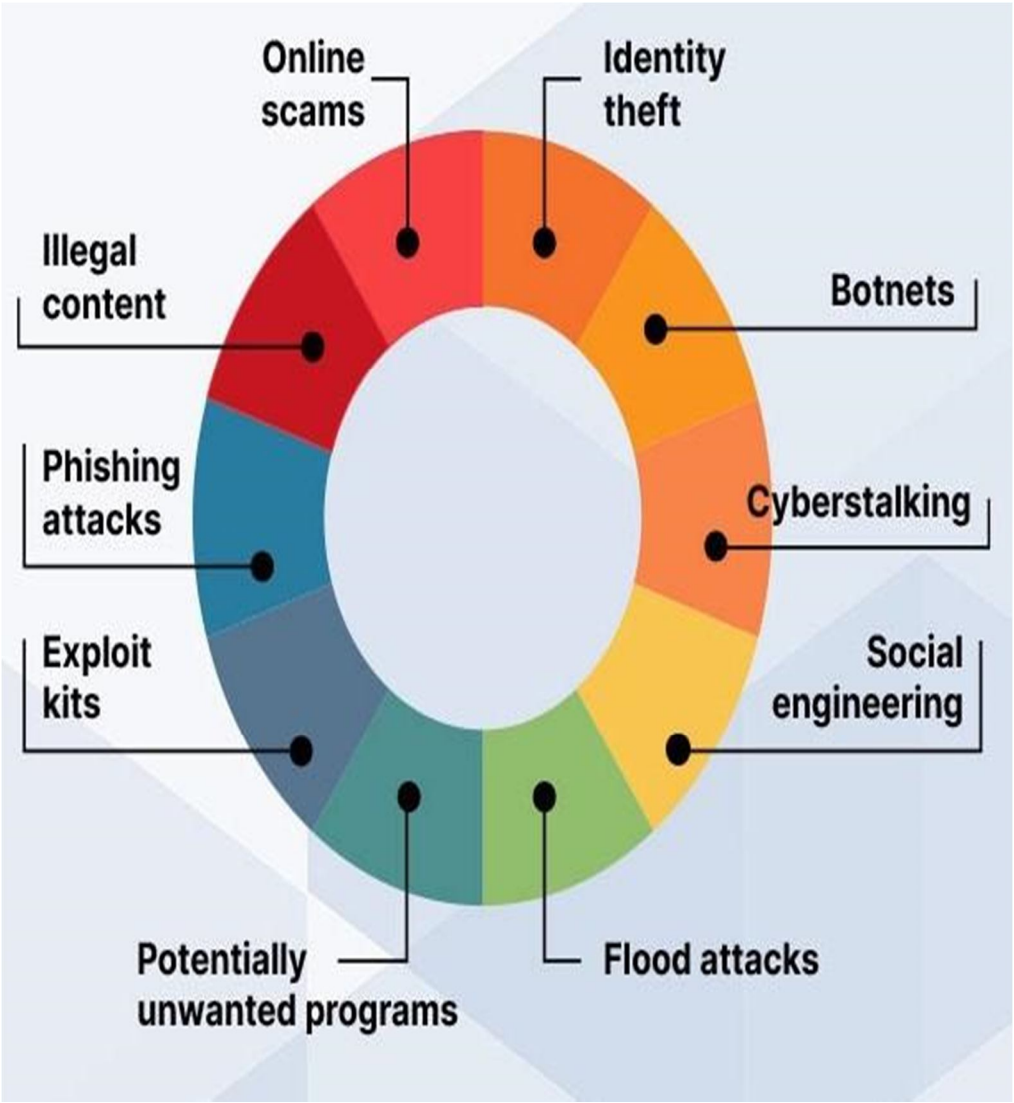


Figure No.1: Types of cyber crimes

III. WHAT CYBER CRIME ENCOMPASSES

Cyber crime includes a wide range of illegal activities that are committed using computer networks or digital devices. Some common categories of cyber crime include:

1) Financial cyber crime: This includes online banking fraud, credit card fraud, investment scams, money laundering, and other forms of illegal financial activities conducted online.
2) Cyber attacks: This involves unauthorised access or disruption of computer systems, networks, or websites, such as hacking, virus/malware attacks, denial of service (DoS) attacks, and ransomware attacks.
3) Cyber fraud: This includes various types of online scams, such as phishing, email scams, lottery scams, online auction fraud, and other fraudulent activities conducted online.
4) Online harassment and stalking: This involves the use of technology to harass, intimidate, or stalk individuals online, such as cyberbullying, threats, and defamation.
5) Data breaches and information theft: This includes stealing, leaking, or misusing personal information, financial data, intellectual property, or other sensitive information.
6) Cyber terrorism: This involves the use of technology to disrupt critical infrastructure, promote political or ideological agendas, or cause fear and panic among the public.
7) Cyber pornography: This includes the creation, distribution, or possession of sexually explicit content involving minors or non-consenting individuals.
8) Intellectual property theft: This includes copyright infringement, trademark infringement, patent infringement, or other unauthorised use of intellectual property online.
9) Cyber extortion: This involves using technology to blackmail individuals or organisations, such as ransomware attacks or other forms of extortion conducted online.
10) Social media and online platform-related crimes: This includes spreading fake news and misinformation, engaging in hate speech, defamation, or identity theft on social media platforms or other online platforms.
11) Online gambling and betting: This includes illegal online gambling, betting, lottery activities, or other forms of online gambling conducted without proper authorization.
12) Phishing: This involves attempts to deceive individuals or organisations into revealing sensitive information, such as passwords, credit card numbers, or bank account details, by posing as a trustworthy entity.
13) Identity theft: This involves stealing someone's personal information, such as name, date of birth, social security number, or financial details, to impersonate them or commit fraudulent activities.
14) Sextortion: This involves using technology to coerce individuals into performing sexual acts or providing explicit content, often for the purpose of blackmail.
15) Child exploitation: This includes the production, distribution, or possession of child pornography, online grooming, and other forms of exploitation involving minors.

These are just some examples of the wide range of activities that fall under the umbrella of cyber crime. It's important to note that cyber crime is a dynamic field, and new types of cyber crimes may emerge as technology evolves and criminals adapt their tactics.

IV. WHAT ARE COMPUTER CRIMES

Computer crimes, also known as cybercrimes, are illicit activities carried out using computers or computer networks. These offences exploit technological vulnerabilities to target individuals, organisations, or even entire nations. They encompass a wide range of illegal actions, each with its own distinct characteristics and potential consequences. Hacking, one prevalent form of computer crime, involves unauthorised access to computer systems or networks to steal sensitive information, disrupt operations, or modify data.

Malware, another significant type of computer crime, entails the creation, distribution, or deployment of malicious software such as viruses, worms, Trojans, or ransomware.

These tools are used to gain unauthorised access, cause damage, or extort money from victims. Phishing, a deceptive technique employed by cybercriminals, leverages fraudulent emails or websites to trick individuals into revealing personal information such as passwords, credit card numbers, or social security numbers.

Identity theft, a widespread cybercrime, involves the unauthorised use of someone's personal information to commit fraud or other criminal activities.

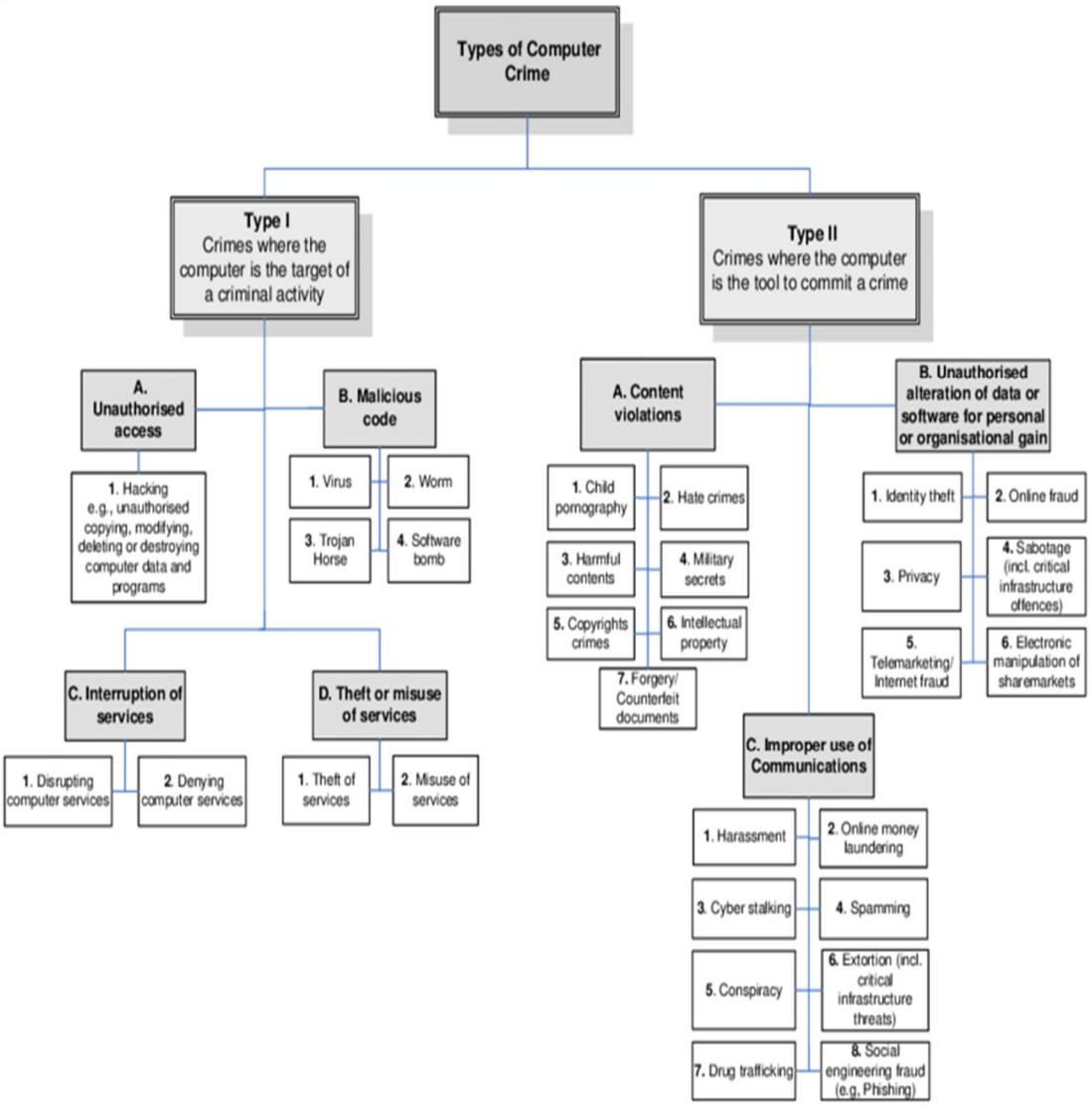


Figure No. 2: types of Computer crime Classification

Computer crimes also encompass activities such as denial-of-service (DoS) attacks, cyberstalking, intellectual property theft, data breaches, cyberterrorism, and money laundering. DoS attacks overload computer systems or networks with excessive requests, rendering them unable to handle legitimate users and disrupting services. Cyberstalking refers to harassment, intimidation, or surveillance of individuals using electronic communication channels, leading to emotional distress or fear. Intellectual property theft involves the unauthorised copying, distribution, or use of copyrighted material, including software, movies, music, or trade secrets. Data breaches occur when sensitive information is accessed or disclosed without authorization, often resulting in identity theft or financial loss for individuals or organisations. Cyberterrorism refers to the use of computer networks to carry out acts of terrorism, including attacks on critical infrastructure, government systems, or public utilities. Money laundering utilises digital platforms to hide the origin or destination of illegally obtained funds, making them appear legitimate.

The consequences of computer crimes can be severe. They include financial loss, reputational damage, privacy violations, and legal repercussions. Individuals and organisations must implement robust cybersecurity measures to protect themselves against these threats. Governments and law enforcement agencies also play a crucial role in combating computer crimes by enacting and enforcing legislation, as well as fostering international cooperation to address these offences effectively. As technology continues to advance, the prevalence and sophistication of computer crimes are likely to increase, highlighting the ongoing need for vigilance and proactive measures to safeguard against cyber threats.

V. COMPUTER CRIME VS CYBER CRIME

	Computer Crime	Cyber Crime
Definition	Illegal activities carried out using computers or networks.	Illegal activities carried out using computers or networks.
Scope	Primarily focused on crimes involving computers.	Encompassess crimes involving computers and the internet.
Physical Component	May involve physical access to the computer system.	Can be committed remotely, without physical access.
Examples	Hacking, malware, phishing, data breaches.	Hacking, malware, phishing, identity theft, cyberstalking.
Targets	Computers, computer systems, networks.	Computers, computer systems, networks, online platforms.
Motive	Financial gain, Information theft, Disruption.	Financial gain, information theft, political motive.
Global Reach	Can be limited to local systems or networks.	Can have a global impact due to the internet.
Legality and Jurisdiction	Government by national laws and regulations.	Require international cooperation due to cross-border nature.
Legal Challenges	May face challenges in applying traditional laws to cyberspace.	Requires specialised cyber laws and enforcement strategies.
Counter Measures	Firewalls, antivirus software, access controls.	Firewalls, intrusion detection system, encryption.

VI. IT ACT 2000

The Information Technology Act, 2000, popularly known as the IT Act 2000, is a comprehensive legislation in India that encompasses various sections addressing electronic communication, transactions, and cyber crime. This Act includes several important sections, each serving a specific purpose and carrying specific punishments for offences committed in the digital realm. One significant section of the IT Act is Section 43, which deals with unauthorised access to computer systems. It states that any person who gains unauthorised access to a computer system or causes damage to computer resources can be held liable for punishment, which may include imprisonment for a term of up to three years or a fine of up to five lakh rupees, or both. Another critical section is Section 66, which covers offences such as hacking, computer-related fraud, and cyber theft. It specifies that any person who commits such offences can be penalised with imprisonment for a term that may extend up to three years, along with a fine that may extend up to two lakh rupees. Section 66B deals with the punishment for dishonestly receiving stolen computer resources or communication devices, which may lead to imprisonment for a term that can extend up to three years or a fine of up to one lakh rupees, or both. Additionally, Section 66C focuses on the punishment for identity theft, stating that anyone who fraudulently uses another person's identity for wrongful gain can be imprisoned for a term that may extend up to three years or fined up to one lakh rupees, or both. The Act also includes Section 66D, which addresses punishment for cheating by impersonation using a computer resource, and Section 66E, which deals with the punishment for violation of privacy through capturing, publishing, or transmitting sexually explicit images or videos.

Moreover, Section 67 of the IT Act addresses the punishment for publishing or transmitting obscene material in electronic form, and Section 72 deals with the penalty for breach of confidentiality and privacy. These sections, along with various other provisions, serve to deter cyber criminals and protect individuals and organisations from cyber offences. The IT Act 2000's inclusion of specific sections and their corresponding punishments reflects the seriousness with which cyber crimes are treated in India and emphasises the need for a robust legal framework to combat such offences effectively.

VII. EFFECTIVE STRATEGIES FOR CYBER CRIME PREVENTION

There are several best practices that individuals, organisations, and governments can adopt to help prevent cyber crimes:

1) Keep software and devices up-to-date: Regularly update all software, applications, and devices with the latest security patches and updates to address known vulnerabilities and reduce the risk of exploitation by cyber criminals.
2) Use strong, unique passwords: Use complex, unique passwords for all online accounts and change them periodically. Avoid using easily guessable passwords such as "123456" or "password", and consider using a password manager to securely store and generate strong passwords.
3) Enable two-factor authentication (2FA): Enable 2FA wherever possible for added security. This adds an additional layer of protection by requiring a second form of authentication, such as a fingerprint, smart card, or SMS code, in addition to a password.
4) Be cautious with emails and attachments: Be cautious with emails and attachments from unknown sources, as they may contain malware or phishing attempts. Avoid clicking on suspicious links or downloading attachments from unknown sources, and be wary of emails that ask for personal or financial information.
5) Be mindful of social media usage: Be cautious about sharing personal information, photos, and other sensitive data on social media platforms. Adjust privacy settings to limit the visibility of personal information, and be wary of friend requests or messages from unknown individuals.
6) Backup important data: Regularly backup important data and files to a secure location to protect against data loss due to ransomware or other cyber attacks.
7) Be cautious with online transactions: Only use reputable and secure websites for online transactions, and avoid sharing financial information, such as credit card numbers, over unsecured or suspicious websites.
8) Educate yourself and others: Stay informed about the latest types of cyber crimes, scams, and security best practices, and educate yourself and others, including family members, employees, or colleagues, about how to recognize and prevent cyber crimes.
9) Use security software: Install and regularly update reputable antivirus software, firewalls, and other security tools on all devices, including computers, smartphones, and tablets, to provide an additional layer of protection against cyber threats.
10) Follow organisational security policies: Organisations should have comprehensive cybersecurity policies in place and ensure that employees are trained and follow them diligently. This includes regular security awareness training, access control measures, and incident reporting protocols.
11) Report cyber crimes: If you become a victim of a cyber crime, report it to the relevant authorities, such as law enforcement agencies or cyber crime cells, to help prevent further incidents and hold the perpetrators accountable.
12) By adopting these best practices and staying vigilant, individuals, organisations, and governments can take proactive steps to prevent cyber crimes and protect against potential cyber threats.

VIII. DIGITAL CRIMINALS AND THEIR GOAL

Virtual/computer CRIMINALS: each length has its miscreants. The vintage West had crooks, educated looters and pony criminals. Privateers and privateers have been far and huge in the instances of sail. The automated length has its very own solid set of malicious characters, and maintaining in thoughts that they may not have a privateer's strut or a teach looter's scramble, they definitely represent a test to individuals who would possibly want to keep the virtual world a covered spot for diversion, facts and business. So who're this era's most notorious hombres? Right here is our "wished list":

1) Malware Authors: Malware is short for malignant programming, is any product used to disturb laptop process, gather fragile statistics, or advantage passage to personal laptop frameworks. It can very well seek within the kind of executable code, scripts, dynamic substance, and different programming. Malware is a regular term used to intend a ramification of some kind of threatening or nosy programming. The term barware is also at times utilised for each malware and routinely unfavourable programming.

Malware incorporates laptop infections, worms, Trojan ponies, ransomware, adware, adware, scareware, and different malevolent initiatives. Starting round 2011 the maximum dynamic malware risks were worms or Trojans as opposed to infections. In regulation, malware is from time to time referred to as a laptop foreign substance. Malware Authors are the ones who document and spread infections, worms, Trojan ponies and exceptional pieces of automated dreadfulness. They pressure humans and businesses to devote loads of coins to enemy malware improvements that take the framework of their energy and execution. Malware writers are the maximum quiet lawbreakers who unfold their snares amongst common oldsters and create tough troubles.

2) Phisher: Phishing is the painting to get sensitive facts, for example, usernames, passwords, and fee card subtleties (and at times, in a roundabout manner, coins) by means of taking up the advent of a solid object in an electronic correspondence. Correspondences professing to be from vast social web sites, closeout destinations, banks, online instalment workstations or IT chiefs are typically used to bait clueless public. Phishing messages might involve connections to web sites that are tainted with malware. Phishing is distinctively finished by way of electronic mail caricaturing or texting and it regularly directs directors to come especially at a manufactured website whose appearance and experience are practically indistinguishable from the genuine one. Phishing is an event of social designing approaches used to lie to clients, and misuses the unfortunate comfort of current net security improvements. Endeavours to manage the growing quantity of discovered phishing occasions include law, client work out, public mindfulness, and specialised security features. Your economic stability is going to lapse and also you should directly refresh your statistics. Not actually: it's most effective for every other miscreant phisher attempting to take your singular information and, most viable, your independence, by directing you to a fake internet site. The AntiPhishing running group, a relationship of retailers and monetary businesses zeroed in on putting off such electronic trickery, says it views as round 20,000 to 30,000 sole phishing net destinations each month.

3) Hoaxster: got any messages from Nigeria as of overdue? What about an "earnest message" from a British blue-blood? A strange bid for employment, perhaps? In those situations, you have presumably pitched some kind of assets to circulate a good deal. Anyhow, as various humans have simply recognised, the main cash that is at any point moved in those plans is from the casualty to the hoaxster.

4) Tricksters: Your email inbox is perhaps loaded up with con artists' pastime, concerning hints for diminishing capsules, time-stocks, well being food sources, gadgets and such. Send those human beings your mastercard quantity or, greater regrettable yet, coins and all you will purpose issues.

5) Online loan Sharks: A six-figure credit without a guarantee or pay test, Will you like a few whipped cream and a cherry what is more, as properly? On no account like con artists, on-line increase regulation breakers guarantee you that they may send you coins. Deplorably, the digital crook will request a direct front instalment to "method the utility," and this is the primary coin to be able to at any factor alternate arms.

6) Spammers: Spammers are crook's inside the manner that they take some time. Not at all like phisher, Hoaxster and other email victimizers that count on to isolate you out of your confidential facts as well as cash, spammers flood your email inbox with promotions (for each true and unwell-conceived items), political denunciations, jokes, important admonitions of possibly coming near near policies and other nonsense. Spammers may not be the most volatile cybercriminals, yet they may be truly some of the most annoying. Spammers likewise force a in reality monetary price through asking for community facts switch potential and driving help providers, ventures and several singular customers to introduce high-priced and often faulty enemy of unsolicited mail improvements.

7) Closeout Fraudsters: You were excited while you gained that Louis XVI gold clock on eBay. The rapture reduced, but, when the clock showed up. The clock scarcely appeared like its web-primarily based picture, seeming to be an article that might effortless the promenade at Coney Island than the Palace of Versailles. Besides, essentially you acquire something, that is past what several survivors of sale fraudsters can assure.

8) False Prize Promoters: you may get male like "Congrats, you've scored the Fredonia national Sweepstakes." All you've virtually received, glaringly, is a suggestion to be hung up and swindled because the "lottery authorities" encompass you in a complex plan containing direct front prices and sham assessments.

9) Media Pirates: Who needs iTunes when you may clearly swipe a melody or video off of Lime twine or every other P2P (dispensed) document sharing help? No one gets injured, correct? Certainly, no person except for individuals who had tried to make the media. Your soul should get destroyed, as well.

10) Social Parasites: Social-systems administration locales, texting networks, web based mingling workplaces and net classifieds are loaded with them: those who pretend to be someone else.

In particular those characters target credulous and weak individuals to cheat them out of their cash. Specific parasites personate individuals, for example, geniuses, in a depressing work to defame their notoriety or clutch a bit of high-quality. Regardless, social parasites are a virus of net society.

IX. CLASS OF VIRTUAL CROOKS

The virtual crooks contain specific gatherings/lessons. This division is probably legitimate based on the object that they've to them. Developing subsequent are the category of virtual crooks

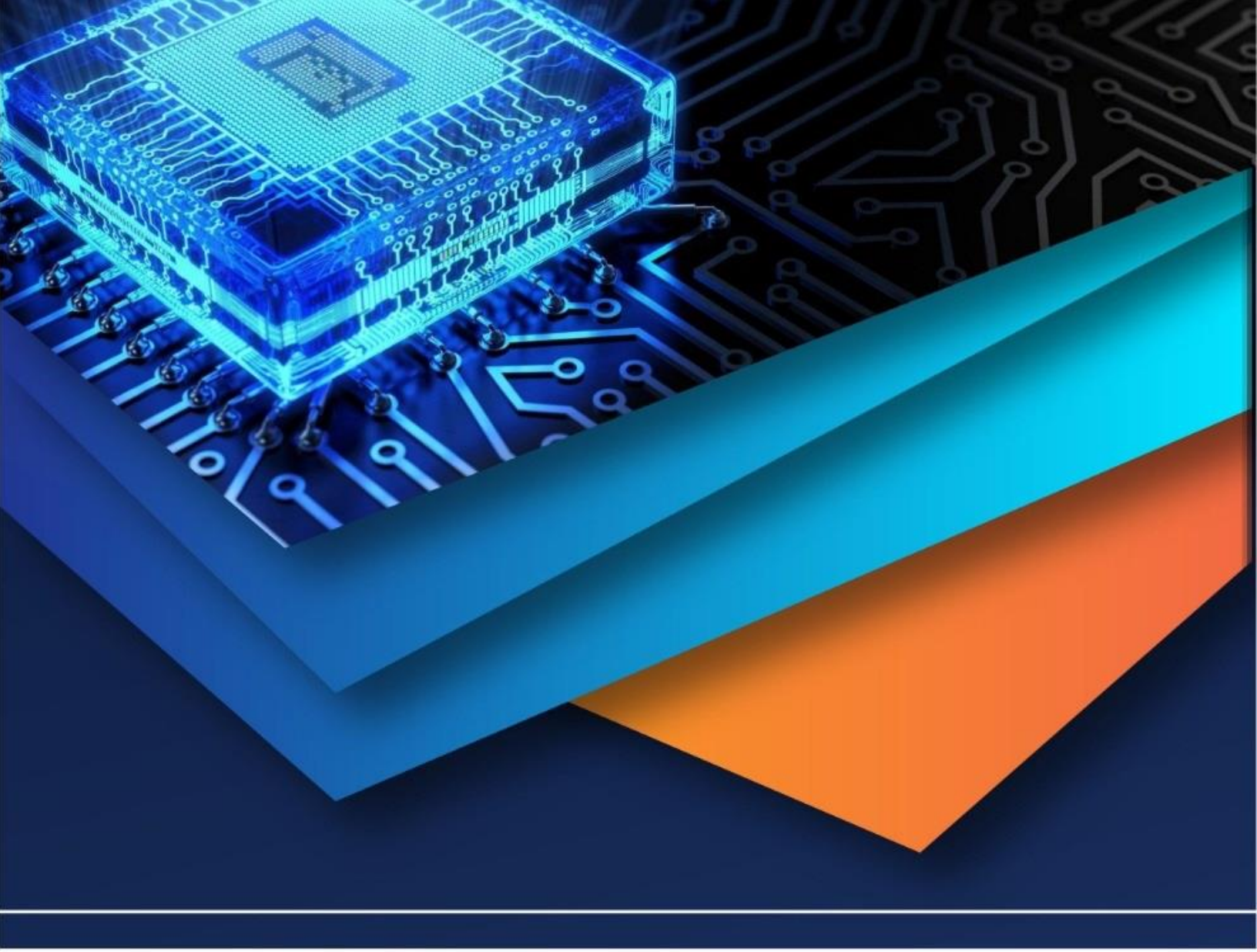
1) Youngsters and youths between the age gathering of 6 to 18 years: The truthful justification behind this type of antisocial way of behaving in children is seen usually because of the interest to be aware and look at among special children in their gathering. In addition the motives might be provocation of the antisocial by means of his companions.
2) Coordinated programmers: these kinds of programmers are for the maximum element coordinated collectively to meet unique goals. The explanation might be to satisfy their political predisposition, fundamentalism, and so forth. The Pakistanis are alleged to be quite the pleasant first-class programmer on earth. They broadly speaking focus on the Indian government locales with the cause to satisfy their political desires. In addition the NASA in addition to the Microsoft locations are generally enduring an onslaught through the programmers.
3) Gifted programmers/saltines: Their work is inspired through the coloration of cash. These forms of programmers are commonly applied to hack the website of the adversaries and get sound, reliable and massive statistics. In addition they're applied to interrupt the arrangement of the business fundamentally as a movement to make it extra relaxed with the aid of distinguishing the provisos.
4) Malcontented employees: This collection includes the ones individuals who've been both sacked by using their boss or are upset with their manager. To vindicate them in the main hack the association in their people. They're for the maximum element disillusioned representatives, ex-employees, and impermanent representatives regularly capitulate to the goddess of the rapid greenback. Moreover, careless and profoundly obliging employees additionally contribute intensely toward laptop violations. They will just be 20% of the threat, but they produce eighty% of the damage. These aggressors are viewed as the maximum noteworthy gamble.

X. GOAL

Corporate houses, banks, economic foundations, ventures, government divisions, army and knowledge institutions and even exploration and scholarly establishments might be the targets for executing laptop violations. Their rivals, looking for proprietary innovations, might also focus on the corporate homes, even though the expert centre class lawbreakers would possibly be aware of the banks and the other economic establishments for financial income. The business, contemporary or changing businesses is probably the objective in their own representatives because of sadness and sick will. The mental militants may be conscious of any management affiliation or management industry for their incendiary physical activities. The experts of a threatening country may be secret agents upon the navy and perception associations. The faculties and the logical examination establishment is probably the objective of the understudies, cutting-edge or enterprise homes and different enemies of social additives to take licences/research work. Apart from this goal of 'programmers' or 'wafers', who revel in such sporting events for scholarly test, vengeance, advantage or in any event, for entertainment simplest. Causes in the back of digital wrongdoings: capacity to store information in addition to little space: The pc has the exceptional trait of placing away information in a tiny space. This bears to dispose of or determine statistics both via bodily or virtual mediums and make it lots greater sincere. Easy to get to: the difficulty that runs over in looking at a laptop framework from an unapproved front is that there's opportunity of infringement now not because of individual blunder yet due to the complicated innovation. Via furtively constant purpose bombs.

REFERENCES

[1] Arya, Nidhi. “Cyber Crime Scenario in India and Judicial Response.” International Journal of Trend in Scientific Research and Development, vol. Volume-3, no. Issue-4, 30 June 2019, pp. 1108–1112, https://doi.org/10.31142/ijtsrd24025. Accessed 3 Feb. 2020.
[2] Baiden, John E. “Cyber Crimes.” SSRN Electronic Journal, vol. 2, no. 1, 2011, https://doi.org/10.2139/ssrn.1873271.
[3] Douglas, John, et al. Crime Classification Manual. John Wiley & Sons, 26 Mar. 2013.
[4] K Jaishankar. Cyber Criminology : Exploring Internet Crimes and Criminal Behavior. Boca Raton, Fl, Crc Press, 2011.
[5] Pandey, Kritarth. “Laws Relating to Cyber Crimes in India.” SSRN Electronic Journal, vol. 3, no. 1, 2014, https://doi.org/10.2139/ssrn.2412469. Accessed 4 Oct. 2019.
[6] Renu, Dr. “Impact of Cyber Crime: Issues and Challenges.” International Journal of Trend in Scientific Research and Development, vol. Volume-3, no. Issue-3, 30 Apr. 2019, pp. 1569–1572, https://doi.org/10.31142/ijtsrd23456. Accessed 21 Nov. 2019.
[7] Sabyasachi Pramanik. Cyber Security and Digital Forensics : Challenges and Future Trends. Hoboken, New Jersey, John Wiley & Sons, Inc, 2022.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY