JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CYBER CRIME IN INDIA A CRITICAL STUDY IN MODERN PERSPECTIVE

Thamidela Mythri Devi

LLM Scholar

School of Law, Gitam University

ABSTRACT

The advantages of computer technology are not without disadvantages. Even though computers make life easier and faster, they are also under threat from the deadliest sort of criminality known as "Cybercrime." Without computers, entire businesses and government functions would nearly cease to exist. The widespread availability of inexpensive, powerful, and user-friendly computers has enabled an increasing number of people to use and, more significantly, rely on computers as part of their everyday lives. Criminals are becoming more reliant on them as corporations, government institutions, and individuals become more reliant on them. Cybercrime prevention requires a thorough examination of their behavior and an awareness of their ramifications at many levels of society. As a result, the current article explains a systematic understanding of cybercrimes and their repercussions on many areas such as socio-economic, political, consumer trust, teenagers, and future trends in cybercrimes.

KEYWORDS: **Cyber, Crime, Technology.**

Introduction

Cybercrime is a broad word that encompasses everything from electronic cracking to denial of service attacks in which computers or computer networks are utilized as a tool, a target, or a location for illegal conduct.

It can also refer to classic crimes using computers or networks to facilitate criminal activity[1]. Cybercrime can halt any railway where it is, misdirect planes on their flight by sending out incorrect signals, cause any sensitive military data to slip into the hands of foreign countries, block e-media, and bring down any system in a matter of seconds.

The purpose of this research is to look at some of the elements, effects, and prospects of cyber technology, with a focus on the threat that cybercrime poses to India. Efforts have been undertaken to examine the legal structure in India that can be used to manage it. To begin with, it is required to define the dimensions of the term "crime." Thus, there is little doubt that 'crime' is a relative phenomenon that is universal and that it has been present in virtually all communities from ancient to current times[2]. Each culture has developed its definition of criminal behavior and conduct that is punishable by the express desire of the political community reigning over the society, which is always influenced by the religious-social-political-economic values that exist in that society. As a result, the behavior that attracts 'penal responsibility' has been affected and characterized by the total outcome of these norms since time immemorial[3].

Interestingly, just as the definition of crime has evolved as a result of the advancement of information technology, so have the types of criminals who commit such crimes. In terms of Indian society, the definition of crime has been influenced by religious interpretation, particularly during ancient times. Religion was utterly dominant throughout this period. All political and social actions, including 'crime,' are thought to have occurred due to the presence of supernatural force. This period gave birth to the Demonological Theory of Crime Causation.

There were renaissance and restoration phases during the Middle Ages, which gave 'crime' a new and refreshing look. This time gave birth to utilitarianism, a positive attitude, analytical thinking, principles of natural justice, lessie fairy's thoughts, hedonistic philosophy, and pain and pleasure theory, all of which contributed to opening new frontiers in the study of crime. The later time paved the stage for the scientific and industrial revolutions, and rational thinking predominated[4].

[1] Sumanjit Das and Tapaswini Nayak, IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES, 6 IJESET, 142-153, (2013),https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf.

[2] Shivesh Shrivastava, A study of Emerging Issues of Cyber Law, CALR, (Jan. 8, 2022, 12:13 PM), https://calr.in/a-study-of-emerging-issues-of-cyber-law/.

[3] Rita Dewanjee and Dr. R. Vyas, Cyber Crime: Critical View, vol.5 Issue. 1, International Journal of Science and Research, 85-87, (2016), https://www.ijsr.net/get_abstract.php?paper_id=NOV152579.

[4] Rita Dewanjee and Dr. R. Vyas, Cyber Crime: Critical View, vol.5 Issue. 1, International Journal of Science and Research, 85-87, (2016), https://www.ijsr.net/get_abstract.php?paper_id=NOV152579.

CATEGORIES OF CYBER CRIME

Data Crime

Data Interception

In order to obtain information, an attacker monitors data flow to or from a target. This attack could be carried out to gather data in preparation for a future episode, or the data acquired could be the attack's end purpose. This attack typically entails sniffing network traffic, but it could also entail watching other data streams, such as radio. The attacker is usually passive and merely manages regular communication. Still, in some forms, the attacker may try to start the construction of a data stream or affect the type of data conveyed[5]. The attacker is not the intended recipient of the data stream in all forms of this attack, which distinguishes it from other data gathering methods. Unlike some other data leakage attacks, the attacker is watching and accessing explicit data channels (such as network traffic). This contrasts with assaults that gather more qualitative data, such as communication volume, which is not communicated via a data stream.

Data Modification

Communications must be kept private to ensure that data cannot be edited or viewed while in transit. In a distributed environment, a malevolent third party may commit a computer crime by interfering with data as it travels between sites. An unauthorized entity on the network intercepts data in transit and modifies sections before retransmitting it in a data modification attack. Changing the dollar amount of a financial transaction from $100 to $10,000 is an example of this. A whole set of valid data is repeatedly introduced onto the network in a replay attack. A legitimate $100 bank account transfer transaction, for example, could be repeated 1,000 times[6].

Data Theft

This term is used when information is illegally stolen or obtained from a corporation or another individual. User information is commonly used, such as passwords, social security numbers, credit card numbers, other personal information, or other private company information. Because this information was gained unlawfully, it is likely that the person who stole it will be prosecuted to the greatest extent of the law when apprehended[7].

[5] Akash Kori, Critical Analysis of Cyber Laws in India, iPleaders, (Jan. 8, 2022, 11:05 AM), https://blog.ipleaders.in/cyber-laws-in-india/.

[6] Vumetric Cyber Portal, https://cyber.vumetric.com/vulns/CVE-2021-44480/missing-encryption-of-sensitive-data-vulnerability-in-wokkalokka-wokka-watch-q50-firmware/ (last visited on Jan. 7, 2022).

[7] Singh, Pushpinder, and Kirandeep Kaur., Role of Social Networking Sites as a Component in Modern Social Structure: A Study on College Students, vol.10 no.4 , International Journal of Education and Management Studies, Indian Association of Health, Research and Welfare, p.447., Dec. 2020.

Network Crime

Network Interferences

Network Inputting, transmitting, destroying, deleting, degrading, changing, or concealing Network data to disrupt the operation of a computer network.

Network Sabotage

'Network Sabotage,' or inept managers, are attempting to perform the duties of those they are ordinarily in charge of. It could be one or more of the factors mentioned above. If, on the other hand, Verizon is exploiting the help the children line to obstruct first responders, they may be using network issues as a pretext to persuade the federal government to act in the name of public safety. Of then, what good are unions and strikes if the federal government pushes these folks back to work[8]

Access Crime

Unauthorized Access

"Unauthorized Access" looks into the computer cracker underworld from the inside. Filming took place in several locations around the United States, Holland, and Germany. "Unauthorized Access" examines the people behind the screens of computers, attempting to divorce the media's portrayal of the "outlaw hacker" from reality[9].

Virus Dissemination

Malicious software that integrates with other programs. (Viruses, worms, Trojan Horses, Time bombs, Logic Bombs, Rabbit, and Bacterium are examples of malicious software that damages a victim's system.)[10].

TYPES OF CYBERCRIME

Theft of Telecommunications Services

Three decades ago, the "phone phreakers" established a precedent for what has since evolved into a massive criminal enterprise. Individuals or criminal organizations can acquire access to dial-in/dial-out circuits and make their calls or sell call time to third parties by gaining access to an organization's telephone switchboard (PBX) (Gold 1999). Impersonating a technician, fraudulently obtaining an employee's access code, or using

[8] Help Net Security, https://www.helpnetsecurity.com/2010/09/08/the-emotional-impact-of-cybercrime/ , (last visited on Jan. 7, 2022).

[9] Akash Kori, Critical Analysis of Cyber Laws in India, iPleaders, (Jan. 8, 2022, 11:05 AM), https://blog.ipleaders.in/cyber-laws-in-india/.

[10] Akash Kori, Critical Analysis of Cyber Laws in India, iPleaders, (Jan. 8, 2022, 11:05 AM), ihttps://blog.ipleaders.in/cyber-laws-in-inda/.

software available on the Internet are all options for gaining access to the switchboard. To avoid detection, some adept criminals create a loop between PBX systems. Capturing "calling card" details and on-selling calls charged to the calling card account, as well as counterfeiting or illicit reprogramming of stored value telephone cards, are all examples of service theft[11].

Communications in furtherance of criminal

On spiracies

In the same way that legitimate organizations in the business and governmental sectors rely on information systems for communications and record-keeping, criminal organizations' activities are aided by technology. Telecommunications equipment enables organized drug trafficking, gambling, prostitution, money laundering, child pornography, and weapons trafficking (in those jurisdictions where such activities are illegal). Criminal communications may be beyond the grasp of law enforcement if encryption technology is used. The use of computer networks to create and transmit child pornography has gotten a lot of press lately. These materials can now be imported at the speed of light across national borders (Grant, David, and Grabosky 1997). The more overt expressions of internet child pornography require a minor level of organization, as required by IRC and WWW infrastructure. Still, the activity appears to be confined mainly to people[12].

Telecommunications Piracy

Thanks to digital technology, print, graphics, music, and multimedia combinations can now be easily reproduced and disseminated. Many people have succumbed to the temptation to copyrighted material for personal use, for sale at a lower price, or even for free dissemination. Owners of copyrighted material have expressed substantial anxiety as a result of this. Each year, the industry is expected to lose between $15 and $17 billion due to copyright infringement (the United States, Information Infrastructure Task Force 1995, 131). In addition to financial loss, when authors of works in any media cannot profit from their contributions, there can be a chilling impact on creative activity in general[13].

[11] Singh, Pushpinder, and Kirandeep Kaur., Role of Social Networking Sites as a Component in Modern Social Structure: A Study on College Students, vol.10 no.4 , International Journal of Education and Management Studies, Indian Association of Health, Research and Welfare, p.447., Dec. 2020.

[12] Vumetric Cyber Portal, https://cyber.vumetric.com/vulns/CVE-2021-44480/missing-encryption-of-sensitive-data-vulnerability-in-wokkalokka-wokka-watch-q50-firmware/ (last visited on Jan. 7, 2022).

[13] Ryan Paul, Cybercrime more profitable than illicit drug sales?, ars technica,(Jan. 8, 2022, 10:45 AM), https://arstechnica.com/uncategorized/2005/11/5648-2/.

Dissemination of Offensive Materials

In online, there is a lot of content that some people find disagreeable. Sexually explicit literature, racist propaganda, and directions for creating incendiary and explosive devices are just a few examples. From the typical obscene telephone call to its contemporary form in "cyber-stalking," in which persistent messages are transmitted to an unwilling receiver, telecommunications networks can be exploited for harassing, threatening, or intrusive communications.

Electronic Money Laundering and Tax Evasion

For a long time, computerized funds transfers have aided in the concealment and movement of criminal proceeds. Emerging technology will make it easier to hide the source of ill-gotten money. Income acquired legally may also be more easily hidden from tax authorities. Large Financial institutions will no longer be the only ones capable of sending electronic funds transfers across many jurisdictions at light speed. The growth of informal financial institutions and parallel banking networks may allow for the bypassing of central bank oversight. Still, it may also make it easier to avoid cash transaction reporting requirements in countries with them. Through telecoms, traditional underground banks, which have thrived in Asian countries for generations, will have even more capacity[14].

Electronic Vandalism, Terrorism and Extortion

Western industrial society is now more than ever reliant on complicated data processing and telecommunications networks. Any of these damaged or interfered with systems can have disastrous repercussions. Electronic invaders, whether motivated by curiosity or vindictiveness, cause, at best, inconvenience and have the ability to cause massive harm (Hundley and Anderson 1995, Schwartau 1994)[15].

Illegal Interception of Telecommunications

Telecommunications advancements have opened up new avenues for electronic eavesdropping. Telecommunications interception has a growing number of uses, ranging from the traditional surveillance of an unfaithful spouse to the most cutting-edge kinds of political and economic espionage. New vulnerabilities are created as a result of technological advancements yet again. The electromagnetic signals that a computer emits

[14] Rita Dewanjee and Dr. R. Vyas, Cyber Crime: Critical View, vol.5 Issue. 1, International Journal of Science and Research, 85-87, (2016), https://www.ijsr.net/get_abstract.php?paper_id=NOV152579.

[15] Shivesh Shrivastava, A study of Emerging Issues of Cyber Law, CALR, (Jan. 8, 2022, 12:13 PM), https://calr.in/a-study-of-emerging-issues-of-cyber-law/.

can be intercepted as well. Broadcast antennas could be made out of cables. The remote monitoring of computer radiation is not prohibited by law[16].

Electronic Funds Transfer Fraud

As the use of electronic payments transfer methods has grown, so has the possibility of such transactions being intercepted and redirected. Valid credit card numbers can be blocked both electronically and physically, and the digital data stored on a card can be forged. Just as an armed thief may steal a car to make a quick getaway, a criminal could steal telecommunications services and use them for vandalism, fraud, or promote a criminal conspiracy. Compound computer crime is when two or more generic kinds listed above are combined.

IMPACT OF CYBER CRIME

Crime as an Evil Factor of Society

Even though a crime-free society is a myth, crime is an omnipresent, inextricable aspect of social existence. The question, "Why is there so much ado about crime?" may irritate some people. No one can deny that crime is a social phenomenon; it is everywhere, and it is nothing new; it is one of the defining characteristics of all civilizations that have ever existed, civilised or uncivilised, and it is one of the most basic inclinations of all human activity! However, it is essential to remember that high crime rates are a source of societal worry not because of their character but because of the potential for social disruption. Furthermore, some people are victims of crime more severely. Victims of crime may lose everything they own. Safety, peace, money, and property are perhaps fundamental values because they help fulfill various desires[17].

Impact of Cyber Crime over Teenager

These days, the worst fear in teenagers' Cyberbullying is bullying through the Internet. According to the investigation, it has become more widespread in the last five years, and children under eighteen are more prone to and fearful of cyberbullying. In our culture, it is becoming an alarming movement. According to research, the most common target of cybercrime is female teenagers. Cyberbullying is a worry that arises when a person receives threats or unfavorable feedback comments, or negative pictures or comments from another person.

This is accomplished mainly through the use of the above-mentioned essential technologies, which are accessed primarily through the Internet. Chatting, instant messaging, and other forms of cyberbullying can be

[16] Sumanjit Das and Tapaswini Nayak, IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES, 6 IJESET, 142-153, (2013),https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf.

[17] Pushparaj Pal, Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India, ResearchGate (Jan. 8, 2022, 12:43 PM), https://www.researchgate.net/publication/337818340_Cyber_Crime_An_Analytical_Study_of_Cyber_Crime_Cases_at_the_Most_Vulnerable_States_and_Cities_in_India.

used. Users of social networking sites such as Facebook, Orkut, and Twitter are more vulnerable to cyberbullying. Generally dreaded people, in my opinion, can reach a point of melancholy, humiliation, and threats. We may conclude from this data that if a person gets Bullied online, they may be depressed to the point of self-harm[18].

Impact of Cyber Crime over Consumer Behavior

The information revolution and the strategic use of the Internet have made a lot of generally open societies vulnerable to cybercriminal and cyber-terrorist attacks, particularly in commercial business operations. This dark commercial side has been known as cybercrime, and it has taken on numerous forms that alter our impressions of how we shop online, thanks to the rise of e-commerce. Corporations should recognize that these dangers to their online enterprises have strategic consequences for their long-term success. They should take appropriate steps to eliminate or considerably decrease these threats to maintain consumer confidence on the Internet as a shopping alternative. These countermeasures, dubbed "cyber security," were created to protect consumer privacy and information while allowing for a worry-free shopping experience. There is a need to develop models that will enable businesses to evaluate the effects of cybercrime on online consumer confidence and respond by utilizing the benefits of recent cyber security advancements. With these two aspects of e-commerce impacting the online consumer, businesses must ensure that the security measures in place will ultimately win out, ensuring that customers will continue to use the Internet to meet their buying demands[19].

Emotional Impact of Cyber Crime

The study, which is the first to look into the emotional impact of cybercrime, finds that victims are most likely to feel angry (58 percent), annoyed (51 percent), and deceived (40 percent) and that they often blame themselves for the attack. Only 3% do not believe it will happen to them, and over 80% do not think, so cybercriminals will be prosecuted, leading to an ironic reluctance to act and a sense of impotence. "We accept cybercrime because of a 'learned helplessness,'" said Loyola Marymount University associate professor of psychology Joseph LaBrie, Ph.D. "It's like getting ripped off at a garage — you don't dispute with the mechanic if you don't know anything about vehicles." People simply accept a situation, even if it is unsatisfactory." People aren't changing their behavior despite the emotional toll, the universal threat, and cybercrime incidences, with barely half (51%) of adults indicating they would change their conduct if they were a victim. A victim of cybercrime, "I was emotionally and financially unprepared since I never anticipated I would be a victim of such

[18] Kaite O'Connor, Record Number of Anti-Trans Bills Filed in States This Year, Psychiatry Online, (Jan. 8, 2022, 10:30 AM), https://psychnews.psychiatryonline.org/doi/10.1176/appi.pn.2021.6.10.

[19] Ryan Paul, Cybercrime more profitable than illicit drug sales?, ars technica,(Jan. 8, 2022, 10:45 AM), https://arstechnica.com/uncategorized/2005/11/5648-2/.

a crime," Todd Vinson of Chicago remarked[20]. I felt violated as if someone had entered my home to obtain this information and as if my entire family had been subjected to this heinous crime. Now I can't help but wonder if other data has been obtained unlawfully and is simply sitting in the hands of the wrong people, waiting to be exploited." The report's "human effect" section digs deeper into the minor crimes or white lies that customers commit against friends, family, loved ones, and enterprises. Nearly half of those polled believe it is permissible to download a single song, album, or movie without paying for it. Twenty-four percent say that surreptitiously viewing someone else's e-mails or browsing history is permissible or acceptable. Some of these habits, like downloading data, expose consumers to additional security risks[21].

Impact of Cyber Crime over Youth

Society's newest mode of interaction is cyber communication. Users can contact with people all around the world through social networking websites, text messages, and emails. Teenagers, in particular, spend a significant amount of time online each day, either on computers or on portable electronic devices.

Friendships

According to Family-rescource.com, 48% of teenagers believe the Internet helps their friendships. With the rise in popularity of social networking sites, young people can keep in touch with both real and virtual pals. Some teenagers believe that having cyber connections gives them the confidence to be themselves. Instant messaging apps, which are used by an estimated 13 million teenagers, allow them to have real-time interactions with their pals. Friendships with other teens from all over the world can be formed via online communication technologies[22].

Writing

According to Family-rescource.com, 48% of teenagers believe the Internet helps their friendships. With the rise in popularity of social networking sites, young people can keep in touch with both real and virtual pals. Some teenagers believe that having cyber connections gives them the confidence to be themselves. Instant messaging apps, which are used by an estimated 13 million teenagers, allow them to have real-time interactions

[20] Akash Kori, Critical Analysis of Cyber Laws in India, iPleaders, (Jan. 8, 2022, 11:05 AM), https://blog.ipleaders.in/cyber-laws-in-india/.

[21] Shivesh Shrivastava, A study of Emerging Issues of Cyber Law, CALR, (Jan. 8, 2022, 12:13 PM), https://calr.in/a-study-of-emerging-issues-of-cyber-law/.

[22] Pushparaj Pal, Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India, ResearchGate (Jan. 8, 2022, 12:43 PM), https://www.researchgate.net/publication/337818340_Cyber_Crime_An_Analytical_Study_of_Cyber_Crime_Cases_at_the_Most_Vulnerable_States_and_Cities_in_India.

with their pals. Friendships with other teens from all over the world can be formed via online communication technologies[23].

Cyber Bullying

Cyberbullying is a detrimental side effect of teenage contact online. Victims of cyberbullying are frequently subjected to rumours and misinformation posted on social media sites. Bullies may upload images of their victims that are improper or embarrassing. Another facet of cyberbullying is the use of harassing text texts. According to the National Crime Prevention Council, cyberbullying affects over half of all American teenagers. Teens have taken their own lives as a result of internet bullying in certain extreme circumstances[24].

Sexual Solicitation

For kids who use forms of cyber communication, sexual solicitation is becoming a significant concern. It could happen in chat rooms or on social media platforms. When an adult or a peer attempts to engage in a sexual connection over the internet, this is known as sexual solicitation. A teen can be urged to reveal personal information, watch pornography, or talk about something sexual over the internet. Girls account for over 70% of those who are sexually solicited online. Teens should exercise caution while sharing suggestive photos on the internet or conversing with strangers in chat rooms[25].

FUTURE TRENDS IN CYBER CRIME

One of the most concerning aspects is the rapid growth of cybercrime. "Last year was the first year when proceeds from cybercrime were bigger than proceeds from the sale of illegal drugs, and that was, I believe, over $105 billion," said Valerie McNiven, a US Treasury Advisor." She also stated that ""Cybercrime is moving at such a fast pace that law enforcement is unable to keep up." iii It appears that the problem will only worsen in the coming years, now that professionals have recognised the potential windfalls if correctly exploited.

There has been a lot of talk recently about how organised crime and cybercrime are intertwined. Such a combination does definitely portend a bad omen in the near future. With the majority of criminal organisations based in Eastern Europe, Russia, and Asia, where laws and enforcement are lacking, traditional techniques of controlling and neutralising the danger appear to be futile[26]. Phil Williams, a CERT visiting scientist, summed up the situation concisely. Both are available on the Internet channels and are targets for criminals, allowing them to

[23] Sumanjit Das and Tapaswini Nayak, IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES, 6 IJESET, 142-153, (2013),https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf.

[24] Rita Dewanjee and Dr. R. Vyas, Cyber Crime: Critical View, vol.5 Issue. 1, International Journal of Science and Research, 85-87, (2016), https://www.ijsr.net/get_abstract.php?paper_id=NOV152579.

[25] Help Net Security, https://www.helpnetsecurity.com/2010/09/08/the-emotional-impact-of-cybercrime/ , (last visited on Jan. 7, 2022).

[26] Rita Dewanjee and Dr. R. Vyas, Cyber Crime: Critical View, vol.5 Issue. 1, International Journal of Science and Research, 85-87, (2016), https://www.ijsr.net/get_abstract.php?paper_id=NOV152579.

be exploited for large sums of money with minimal risk. It's tough to ask for more in the world of organised crime."

The upshot will very certainly be an increase in sophisticated phishing assaults and other two-pronged methods of identity theft. For example, using contact centres to alert "customers" of a problem ahead of time, and then following up with emails requesting personal information. Personal data aggregation in many third-party data centres will prove to be lucrative targets for infiltration. It's not difficult to picture criminals employing data mining techniques to identify the most trusting customers, or personalising phishing emails to specific individuals based on their medical, financial, or personal information. Theft detection will become more automatic as well. Botnets, for example, will be used not only for denial-of-service assaults and spam, but also as massive search engines for locating sensitive information such as credit cards and social security numbers[27]. The botnet's controllers will then be paid to conduct queries on its "database."

As a result, the entry hurdle to the sector is so low that practically anyone may try their hand at it and join the growing ranks of cybercriminals. With such a minimal learning curve, it should spark debate on the need for a new paradigm of thought in how to prevent and deal with criminals that isn't bound by old ways. To sneak into a house, for example, a burglar must not only arrange the right time, but also be knowledgeable about lock picking, security system evasion, and have the courage to overcome moral barriers. In contrast, the simplicity of cybercrime appears to be inversely proportionate to the profits it generates, and these tendencies continue[28].

CONCLUSION

The future of the Internet is still up for grabs between criminals and everyday users. Fears of a cyber apocalypse abound, and the breadth of damage that large-scale fraud may cause is virtually endless. These anxieties should be properly tempered by the knowledge that the problems are being handled, albeit slowly. The Internet's benefit has been shown in a variety of ways, which should be enough to keep it from becoming a hub of criminal activity and a shelter for the evil. Although the government has an important role to play, private software providers and those with the ability to detect and prevent fraud must do the majority of the work.Others must be protected automatically by non-stressing processes that require significant participation. Security must be simple and effective if it is to succeed. In some ways, it's impossible to determine whether cybercrime will still be a relevant issue in ten years, but if the Internet is to continue to grow, cybercrime must be solved to the point where it's on par with, if not better than, real-world crimes.

[27] Sumanjit Das and Tapaswini Nayak, IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES, 6 IJESET, 142-153, (2013),https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf.

[28] Pushparaj Pal, Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India, ResearchGate (Jan. 8, 2022, 12:43 PM), https://www.researchgate.net/publication/337818340_Cyber_Crime_An_Analytical_Study_of_Cyber_Crime_Cases_at_the_Most_Vulnerable_States_and_Cities_in_India.

BIBLIOGRAPHY

ONLINE RESOURCES

1. Pushparaj Pal, Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India, ResearchGate (Jan. 8, 2022, 12:43 PM), https://www.researchgate.net/publication/337818340_Cyber_Crime_An_Analytical_Study_of_Cyber_Crime_Cases_at_the_Most_Vulnerable_States_and_Cities_in_India
2. Shivesh Shrivastava, A study of Emerging Issues of Cyber Law, CALR, (Jan. 8, 2022, 12:13 PM), https://calr.in/a-study-of-emerging-issues-of-cyber-law/
3. Sumanjit Das and Tapaswini Nayak, IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES, 6 IJESET, 142-153, (2013),https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf
4. Rita Dewanjee and Dr. R. Vyas, Cyber Crime: Critical View, vol.5 Issue. 1, International Journal of Science and Research, 85-87, (2016), https://www.ijsr.net/get_abstract.php?paper_id=NOV152579.
5. Singh, Pushpinder, and Kirandeep Kaur., Role of Social Networking Sites as a Component in Modern Social Structure: A Study on College Students, vol.10 no.4 , International Journal of Education and Management Studies, Indian Association of Health, Research and Welfare, p.447., Dec. 2020.
6. Vumetric Cyber Portal, https://cyber.vumetric.com/vulns/CVE-2021-44480/missing-encryption-of-sensitive-data-vulnerability-in-wokkalokka-wokka-watch-q50-firmware/ (last visited on Jan. 7, 2022).
7. Tiana Amo, How to Sell a Car to a Private party Through an Installment Plan, The Nest, (Jan. 7, 2022, 1:30 PM), https://budgeting.thenest.com/sell-car-private-party-through-installment-plan-24980.html .
8. My First Property, https://www.myfirstproperty.co.uk/firsthome/sticking-budget-at-auction , (last visited on Jan. 7, 2022).
9. Ryan Paul, Cybercrime more profitable than illicit drug sales?, ars technica,(Jan. 8, 2022, 10:45 AM), https://arstechnica.com/uncategorized/2005/11/5648-2/
10. Akash Kori, Critical Analysis of Cyber Laws in India, iPleaders, (Jan. 8, 2022, 11:05 AM), https://blog.ipleaders.in/cyber-laws-in-india/.
11. Rita Dewanjee and Dr. R. Vyas, Cyber Crime: Critical View, vol.5 Issue. 1, International Journal of Science and Research, 85-87, (2016), https://www.ijsr.net/get_abstract.php?paper_id=NOV152579.
12. Sumanjit Das and Tapaswini Nayak, IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES, 6 IJESET, 142-153, (2013),https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf.