Inspira-Journal of Commerce, Economics & Computer Science (JCECS)
ISSN : 2395-7069, Impact Factor: 4.964, Volume 06, No. 03, July-September, 2020, pp. 151-157

EMERGING TRENDS IN CYBERCRIME: A COMPREHENSIVE ANALYSIS

Tikam Chand Malakar*

ABSTRACT

Technology that is used for commercial and e-commerce reasons, including the cloud, the online, mobile devices, and social media environments. Given that the majority of financial transactions are carried out online, cyber security is of the utmost importance. Both in terms of their methods and their effect, cyberattacks on various kinds of organisations are distinct from one another. This research investigates a number of different methods that may be used to thwart such cybercrimes. The severity, aggressiveness, and extension of these crimes, all of which constitute a threat to the economy as a whole, are brought into sharper focus by this. Education of consumers is the most important factor in preventing these crimes, in addition to the development of systems and devices that are impossible to get into. Cybercrime insurance is one of the methods that may be taken to limit the harm that either the customer or the bank would experience.

***KEYWORDS**: Cloud Technology, e-Commerce, Cybercrime, Cyber Security.*

Introduction

The fast growth and development of technology has resulted in the emergence of new possibilities and sources of productive resources for organisations of all types. The nature of cybercrime is always evolving to accommodate new dangers, and the internet is a significant contributor to the progression of technology. It is possible that if you are aware of the indicators of cybercrime, you will be able to protect your data and avoid being attacked. Social networking sites on the internet are becoming an increasingly popular target for cybercriminals. At this point in time, it is possible to send and receive digital media such as email, music, and video with only the touch of a button. The Internet is one of the social infrastructures that is increasing at the fastest rate, and the most cutting-edge technical innovations are responsible for the transformation of humanity. Nevertheless, the advent of new technology has made it difficult for us to protect our personal information, which has led to an increase in the number of cybercrimes. Furthermore, the fact that more than sixty percent of all commercial transactions are now conducted online makes the need for stringent security measures even more pressing. From the protection of data in the information technology industry to the protection of data in other areas, such as cyberspace, cybersecurity involves a broad variety of operations. It is necessary to implement strict security measures This is because these technologies hold information that may be used to identify individuals. The capacity of a nation to strengthen its cybersecurity and protect its information is a critical factor in determining its level of prosperity and security. The urgent need for a more secure Internet is acknowledged by both the policies of the government and the development of new services. To effectively address cybercrime, a plan that is both broad and secure is essential. Considering that technology protections are not capable of eliminating cybercrime on their own, it is essential that the appropriate authorities have the capacity to investigate and punish violations of this kind. Several nations and governments throughout the world are now enforcing stringent regulations in an attempt to prevent the loss occurring. Each and every worker is required to get training on cybersecurity. Technology has had an effect on a variety of spheres, including international trade and economy, travel and communication, and even governments and market economies. It is true that the world of the internet has both good and harmful characteristics. In a study that included thirty nations, it was found that people in the United Kingdom, the United States of America, and Australia spent the most time online (8.5 hours per day) using desktop computers, mobile phones, and tablets. Thailand is now in first position, with Brazil coming in second place after eight hours and forty-nine minutes of competition. Many individuals

* Principal, Darbar Government Senior Secondary School, Sambhar Lake, Jaipur, Rajasthan, India.

are increasing the amount of time they spend online as a direct result of social media. Individuals make use of social networking websites such as Facebook, Instagram, WhatsApp, YouTube, and Twitter, as well as instant messaging applications. Internet crime is the one that reigns supreme when it comes to cybercrime. The three most prevalent types of criminal activity that may be committed online are cyberstalking, identity theft, and online fraud.

Common forms of cybercrime include:

- Scam emails designed to steal sensitive information (also known as "phishing");
- Theft of personal information
- Hacking into computer systems or websites
- Spreading hate speech and terrorist propaganda
- Child pornography
- Grooming
- Copyright infringement
- Illegal product sales
- Child pornography requests and production

There are certain crimes that have been committed over the internet that have been brought to light, but there are also other crimes that continue to remain a mystery. Individuals have made an effort to solve the problem of viruses by installing virus protection software on their computers in order to secure them. This will hopefully prevent viruses from spreading further. The crux of the problem is that those who break into one's computer while using the internet are seldom caught. It is essential that individuals who use the internet make use of passwords that are unique to them and make use of software that protects against viruses and spyware. Pornography, which is regarded to be an act of obscenity and is susceptible to legal penalties, has grown more popular as a result of the proliferation of the internet. In addition to the fact that there is no straightforward solution to this problem, the fact that criminal activities performed against kids over the internet are a matter for concern. However, despite the fact that the internet is a fantastic tool that has become an indispensable part of our lives, there are a great deal of things that can be found on the internet that have the potential to cause big problems.

Cybercrime

In the context of criminal activity, the term "cybercrime" refers to any unlawful activity that incorporates the use of computers or computer networks as a tool in order to carry out prohibited activities. This expression is used to describe the illegal behaviour that is being committed. There has been a rise in the quantity of illegal behaviour that takes place online as a direct result of the expanding significance of personal computers in the fields of business, government, and entertainment. Computer crime may be broken down into its most fundamental components, which include unauthorised access to computer systems, the modification of information, the destruction of information, and the theft of technology that is secured. Theft of identity, attempts to steal bank accounts, and theft of data from multinational corporations are all instances of actions that fall under the category of cybercrime. Fraud done via email and the internet is another example. The term "cybercrime" refers to a collection of illegal behaviours that are carried out with the intention of obtaining financial advantage. In order to carry out cyberattacks, cybercriminals make use of a wide number of various channels, and they are always searching for new techniques and capabilities that they can employ without the risk of being detained or prosecuted. It is possible to infect systems and networks with malicious software in order to cause damage to the programme or data that is stored on the system. One way to do this is to access the system. An additional objective of cybercriminals is to initiate attacks against websites with the intention of modifying or removing content, as well as gaining unauthorised access to databases or manipulating them. There are many different sorts of cybercrime, some of the most common of which include illegal gambling, the sale of illegal things including weapons, drugs, and manufacture, as well as the possession or distribution of child pornography. It is possible that it involves the theft of corporate secrets or information that belongs to the government via the use of distant networks that are situated in different parts of the globe in order to participate in illegal endeavours. As an additional point of interest, the term "cybercrime" embraces a broad variety of acts, such as the downloading of illegal recordings and the theft of money from online bank accounts.

Objectives

- To study on the Brief Study of Cybercrime on an Internet.
- To study on the Emerging Trends in Cybercrime: A Comprehensive Analysis"

Cyberattacks

Our investigation is based on the prior research work (Table 1) that was carried out by practitioners, researchers, and industry experts. This work serves as the basis for our study. The study that Arief and his colleagues have done in the past has looked at cybercrime from two different perspectives: Part 1 from the perspective of the attacker [4], and Part 2 from the perspective of the defenders and victims [5]. In their study, Chawki and colleagues [6] focused their emphasis on cybercrime and the management issues that it offers. Cardwell and his colleagues conducted investigations into a variety of areas, distinct groups based on the sorts of crimes that they performed while using information technology.

Authors	Insight about their taxonomy
Arief, Adzmi and Gross (2015)	Stakeholder participation taxonomy: attackers, defenders, and victims
Chawki, Darwish, Khan and Tyagi (2015)	They looked at the principles of cybercrime, computer systems as tools and targets, offences involving content, and cyberspace anonymity, which includes privacy, security, and criminal control.
Cardwell et al. (2007)	consists of the three Ts: incidental material related to the crime, victim targets, and tools for committing crimes.
	They used both external and inner assaults to categorise cybercrime.
Britz (2013)	Early hackers, component theft, neotraditional cybercrime, identity theft/fraud, cyberterrorism and its connections to organised crime were among the typologies.
McQuade, III (2006)	Negligent users, conventional criminals, fraudsters, hackers, malevolent code authors, media pirates, harassers, cybersex offenders, academic cheaters, freelance spies, and cyberterrorists are some of the categories of IT abusers and cybercriminals.

The foundation of our taxonomy is comprised of the following elements: human mistake, technical constraints, risks, vulnerabilities, the hacker subculture, and the current condition of cyberattacks and cybercrime. Keeping these principles in mind, we need to make it our primary emphasis to safeguard the cybersecurity trinity, which consists of confidentiality, integrity, and availability. At this point in time, hackers may conduct assaults that are simple, complicated, or multi-attacks in order to exploit vulnerabilities in security. Even though we will be discussing the more complex techniques of attack (TTPs) for hacking systems.

(APT) stands for "threats with a long-term impact" and The term "Advanced Persistent Threat" was coined by a security professional working for the United States Air Force in the year 2005. An adversary must possess the knowledge, capacity, and means to execute coordinated assaults across a range of domains and platforms in order to be considered an advanced persistent threat (APT), according to the definition provided by the National Institute of Standards and Technology (NIST) in the United States. It is able to successfully pursue its objectives for an extended length of time because it is able to adapt to the efforts of the defenders and maintain a suitable level of engagement overall. Steps like as picking targets, doing research on them, penetrating them, interacting with command and control, finding new targets, exfiltrating data, distributing intelligence, and exploiting information are all included in attack cycles.

It is possible for attackers to remotely install malware in order to take complete or partial control of a system via the execution of arbitrary code.

Accidental exposure to radioactive substances: When it comes to determining the actual MAC address of a system, Address Resolution Protocol poisoning might cause interconnected devices to be misled. ARP is a communication protocol that only supports two types of communication: ARP requests and ARP answers. The ARP cache on any network system is susceptible to being poisoned by attackers who generate reply packets by utilising fabricated MAC addresses of their own. Using VLAN segmentation provides protection against attacks of this kind.

Bluejacking is the act of sending text messages using a private Bluetooth device without the consent of the owner of the device for which the text messages are intended. When it comes to Bluetooth gadgets, some are just capable of sending text messages, while others can also play music. For the highest level of security, the device should always be used in stealth mode.

Bluesnarfing is the act of stealing data from a Bluetooth connection or taking control of a Bluetooth device without the owner's permission. The device is susceptible to this attack for as long as it is operating in the discovery mode and functioning properly. Linux users that make use of the hcitool and ObexFTP software have the potential to launch this sort of assault without their knowledge.

The occurrence of a buffer overflow takes place when a software receives more data than it is able to handle. The situation ultimately results in a memory leak inside the system, which opens the door for the possibility of malicious code being exploited in the future. The first phase in a typical sequence attack is the overflow of the buffer, which is then followed by the insertion of malicious code, a long NOOP (No Operation) instruction, and an execution trigger.

It is possible for a client-side attack to be carried out by a software that is executing on a client system in an attempt to obtain access to a server or database that is being targeted. Because the appropriate input validation and storage processes have been established, this will not take place. Forest trust connections are the backbone of client-side attacks, and transitive trust access makes it possible to establish forest trust connections in all Active Directory domains.

In addition to the cookies that accompany the documents: It is possible that cookies that store sensitive information, such as login passwords, session IDs, and internet browsing histories, might make it easier for further attacks to be carried out, such as session hijacking. In addition to viruses, worms, and Trojan horses, other types of malicious software may be triggered by attachments that contain dangerous code.

The term "cross-site request forgery" (XSRF) refers to activities in which cybercriminals manipulate HTML URLs in order to deceive others into engaging in hazardous activities. Putting an end to automatic log-on and establishing expiration dates for cookies is a safeguard that should be taken.

A Taxonomy of Cybercrime

ITU [10] and ENISA [11] have conducted research in the past that has resulted in the classification of cybercrime into a wide variety of categories. With the advent of the cyber era, we provide a comprehensive taxonomy (Figure 1) that classifies many types of cybercrime.

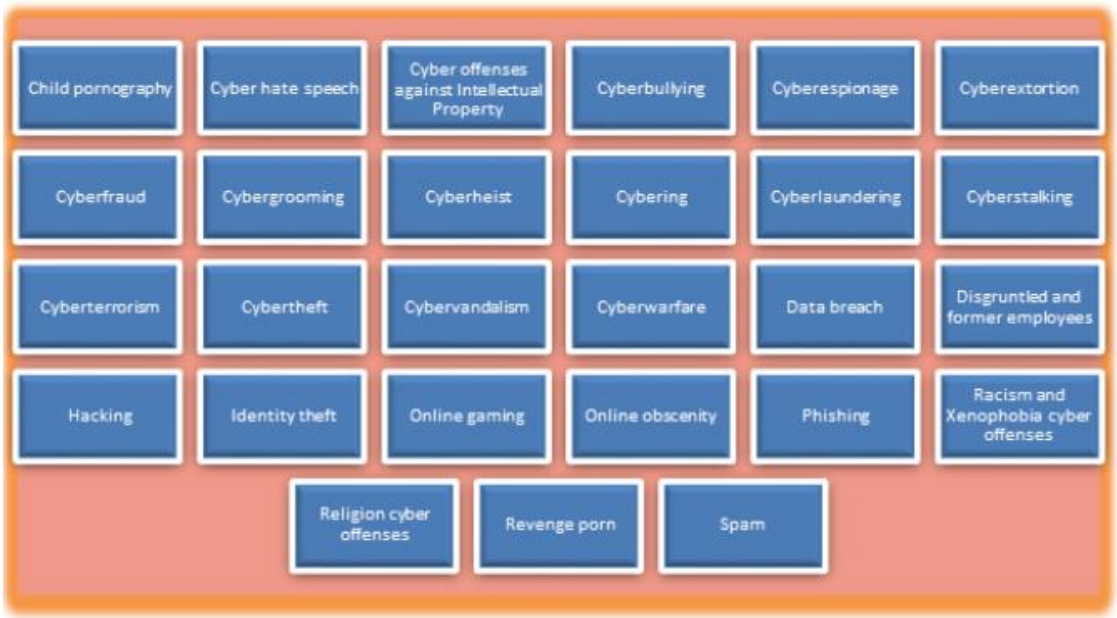

Fig. 1: A Cybercrime Taxonomy

It is referred to as child pornography when children are used as subjects in material that contains explicit sexual content. There are many other types of unlawful activities that may be found on the internet, including but not limited to: and more. The practice of combining photographs of youngsters using computer software is referred to as morphing. Pornographers use this technique. One of the initiatives that Terres de Hommes Netherlands [12] launched to combat the sexual exploitation of minors was the creation of Sweetie, a virtual girl who was ten years old. This was followed by the identification and surrender to Interpol of one thousand predators who originated from seventy-one different countries through the utilisation of nineteen different chat rooms. Twenty thousand seven hundred and seventeen potential predators came close to Sweetie. There is a continued presence of Sweetie 2.0 in the continuing conflict with WCST.

The term "cyber hate speech" refers to any expression of prejudice that takes place in cyberspace and has an effect on the civil and political rights of individuals. Online hatred may be directed at a wide variety of groups, including but not limited to: racism, religion, nationality, ethnicity, countries, migrants, transgender individuals, people with disabilities, political parties, sports teams, sexual orientation, age, gender, youth, and even children and animals. There have been some countries that have established laws in reaction to cyberhate, and there are worldwide groups who are striving to increase awareness.

There is a term known as "cyber torts" that refers to crimes that are committed online and that breach copyrights, patents, trade secrets, or trademarks. In light of the fact that they are more directly associated with computer networks and security, software, databases, digital content, algorithms, and raw data will be included to the list.

Cyberbullying is the act of tormenting another individual via the use of electronic methods of communication. The name "cyberbullying" refers to this activity. The majority of victims of cyberbullying are children and teenagers; nevertheless, adults are not immune to the phenomenon. The act of impersonating victims, sending threatening messages, humiliating images, and extortion are just some of the numerous aspects of cyberbullying. It is important for parents to preserve records of any incidences of cyberbullying so that they may report it to the appropriate authorities.

It is possible to engage in cyberespionage using a variety of methods, including data exfiltration, unauthorised access, interception, and acquisition. Freelance spies have access to a wide variety of technologies, including spyware, keyloggers, surveillance tactics, recording events, intercepting data flow, and monitoring conversations.

When perpetrators of cyberextortion threaten victims with harm unless they pay a ransom, this is known as cyberextortion. In order to avoid the risks associated with computers, fraudsters would demand money in order to get financial advantage. One of the most popular types of ransomware attacks is one that demands payment from the victim in the form of Bitcoin.

The term "cybergrooming" refers to the measures that a paedophile may take in order to gradually participate in sexual molestation by creating a connection with a victim via the use of online contacts. The attacker will begin sending increasingly sexually explicit messages and phone calls to the victim as soon as he has gained the victim's trust.

The Deep Web

The Deep Web, which is unavailable to the majority of browsers and search engines, is the centre of criminal activities on the dark web. To provide just a few examples, the Dark Web includes the Invisible Internet Project (I2P), Freenet, and Tor and other similar services. As a result of the fact that the majority of site owners on the Dark Web want to conceal their material, accessing it requires quite sophisticated tools. In order to visit the Deep Web without revealing your identity, you may utilise the Tor browser, which is an acronym that stands for "The Onion Router." Your IP address will be concealed, and traffic will be redirected to a different location. On the Dark Web, hackers may find whatever they want, including malware, ransomware, crimeware, illegal drugs, guns, stolen accounts, passports, identification cards, credit cards, and cyber-laundering, in addition to a great deal of other things.

There has been an increase in the number of cyberattacks, cybercriminals, and cybervictims as a result of the proliferation of mobile devices, Wi-Fi networks, and the ease with which an individual may access the Internet. The issue of cybercrime is one that is both complex and widespread. Individuals should be the starting point for efforts to combat cybercrime, and then those efforts should be expanded to include corporations, governments, military organisations, and international organisations. By using

many layers of cybersecurity protection, it is possible to lessen, halt, and slow down the progression of cyberattacks. In order to effectively tackle cybercrime, it is required to combine technology solutions an increase in the amount of research conducted by academic institutions; and a more engaged cybersecurity sector.

Conclusion

To add insult to injury, those with lower levels of education need to be instructed in the use of computers, the internet, as well as credit and debit cards. Being cautious and diligent is the simplest way to defend yourself from hackers, while it may be difficult to capture them because they often operate from other countries. Being vigilant and diligent is the easiest way to protect yourself. Due to the fact that computers are used for a variety of purposes, including but not limited to government operations, emergency services, banking, transportation, energy, and telecommunications, the Internet is indirectly tied to the issue of national security. Data may be put to a variety of beneficial ends, but it also presents the possibility of being used in an unlawful manner. In order to prevent cybercrime, it is vital to implement security measures that protect data as well as the privacy of users. The problems are being addressed, but it is very unlikely that they will be remedied in a timely manner, even if they should be resolved in the near future. Through demonstrating its usefulness in a number of different ways, the Internet has prevented itself from becoming a safe haven for criminals. Businesses who produce software as a commodity and people who have the potential to eliminate criminal behaviour need to be the ones accountable for the prevention of criminal conduct. It is imperative that the legal system evolve in response to the ever-shifting technology world in order to forestall the misuse of new technologies. In order to support public awareness efforts, free advertisements, and preventive seminars, funds from the government and non-governmental groups will be used. At the grassroots level, the process of recognising cyber world crimes and cyber illiteracy should be initiated by institutions, computer centres, schools, and individuals alike. It is imperative that quick attention be paid to the rising worry about the emergence of crimes that are based on technology. Every kind of criminal activity should be met with complete and utter indifference. The well-being and financial security of the people who live there have to be safeguarded. It should be possible for everyone to have a sense of security regardless of where they are or what they do online. According to the findings of the research, the simultaneous effect that cybercrime would have on millions of internet users would make it far more serious than conventional crime.

References

⇒ Norton. 11 ways to help protect yourself against cybercrime [Online]. Available from https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-fromcybercrime.html

⇒ Kaspersky. Tips on how to protect yourself against cybercrime [Online]. Available from https:// www.kaspersky.com/resource-center/threats/what-is-cybercrime

⇒ HemrajSaini, Yerra Shankar Rao, et al. Cyber-Crimes and their Impacts: A Review. International Journal of Engineering Research and Applications (IJERA). 2012;2(2):202-209.

⇒ Helpline Law Legal Solutions Worldwide. Cyber Crimes in India-What is, Types, Web Hijacking, Cyber Stalking [Online]. Available from https://www.helplinelaw.com/employment-criminal-andlabour/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html

⇒ V.Karamchand Gandhi. An Overview Study on Cyber crimes in Internet. Journal of Information Engineering and Applications. 2012;2(1):1-6. 8. Search Security (2020, 22 Dec). Cybercrime [Online]. Available from https://searchsecurity. techtarget.com/definition/cybercrime?amp=1.

⇒ DM Chudasama, LK Sharma, et al. A Comparative Study of Information Systems Auditing in Indian Context. Information Systems Audits for eCommerce. 2019;7(4):020-028.

⇒ DM Chudasama, L.K. Sharma, et al. Refine Framework of Information Systems Audits in Indian Context. International Journal of Computer Sciences and Engineering. 2019;7(5):331-345.

⇒ DM Chudasama, Kathan Patel, et al. Awareness of Data Privacy Breach in Society. International Journal of All Research Education and Scientific Methods (IJARESM). 2020;8(10):303-307.

⇒ DM Chudasama, Darsh Patel, et al. Research on Cybercrime and its Policing. American Journal of Computer Science and Engineering Survey. 2020;8(10):14

⇒ Soham Shah, MA Lokhandwala, et al.Decoding Farm Laws. International Journal of Scientific Research and Engineering Development. 2021;4(2):590-595.

⇒ Ajeet Singh Poonia Et al., Cyber Crime: Practices and Policies for Its Prevention

⇒ Bowker, Art (2012). The Cybercrime Handbook for Community Corrections: Managing Risk in the 21st Century. Springfield: Thomas. ISBN 9780398087289

⇒ Gaines. L. K, Miller. R. L. (2008). Criminal justice in action: The Core (p. 7).USA: Cengage Learning

⇒ Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. ITU Telecommunication Development Bureau.

⇒ Luis Garicano, University of Chicago and CEPR Paul Heaton University of Chicago December 4, 2006 Computing Crime: Information Technology, Police Effectiveness, and the Organization of Policing

⇒ Millar Carroll. J. (1996). Computer security (p. 38). USA: Butterworth-Heinemann

⇒ Moon. B, McCluskey. J. D, McCluskey. C. P. (2010). A general theory of crime and computer crime: An empirical test Journal of Criminal Justice.

⇒ Richet, Jean-Loup (2012). "How to Become a Black Hat Hacker? An Exploratory Study of Barriers to Entry Into Cybercrime.". 17th AIM Symposium.

⇒ Shackelford 2014 Managing Cyber Attacks in International Law, Business, and Relations, Cambridge University Press

⇒ Smith, G. R. (2013). Investigating Cybercrime: Barriers and Solutions.

❑❑❑