International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-12 Issue-3, February 2023

# Thwart and Safeguard of Cyber Crime & Cyber Attack in Computer Networks

**Kurian M.J, Sreekanth D**

***Abstract*: *The term "cyber" is closely related to or characteristic of the culture of computers, computer networks, information technology, and virtual reality. The Internet is a global network of billions of computers and other electronic devices that use standardised communication protocols. A total of 5.07 billion people worldwide use the internet today, equivalent to 63.5% of the world's total population. Internet users continue to grow as well. As of 2022, China had over one billion internet users, more than any other country in the world. India ranked second, with nearly 933 million Indians accessing the internet via any device. Cybercrime is a type of criminal activity that targets or utilises a computer, a computer network, or a networked device. The slogans used to address data privacy are: "Data privacy belongs to you." Secure it, protect it, and block hackers. This paper highlights the issues related to categories and the impact of cybercrime, as well as fundamental cyber laws, security threats, and protection, serving as a warning to internet users.***

***Keywords*: *Adware, Cybercrime, Cyberbullying, Cyber spying, DDOS, DoS, Phishing, Ransomware, Spyware***

## I. INTRODUCTION

Cybercrime is a global problem which has been dominating the news cycle. It poses a threat to individual security and an even greater threat to the government, banking sector, and large international companies—today's organised cybercrimes far outshadow those of lone hackers in the past. Now, large organised crime rings function like start-ups and often employ highly trained developers who are constantly innovating online attacks. With the vast amount of data to be exploited, cybersecurity has become increasingly essential. It is very clear that the young generation lives on the internet, and we, as general users, are often unaware of how those random bits of 1s and 0s reach our computers securely. It is a golden age of hackers, and cyberattacks are evolving by the day. With numerous access points, public IP addresses, and constant traffic, along with a wealth of data to exploit, black hat hackers are having a field day exploiting vulnerabilities and creating malicious software for the same purpose. Hackers are becoming increasingly innovative and creative with their malware, and how they bypass virus scans and firewalls still baffles many people. Even though there must be some sort of protocol to protect us against all these cyberattacks, our data often falls into the wrong hands. In this context, the world considers cybersecurity and how to defend itself. Global use of cryptocurrencies has increased exponentially during the COVID-19 pandemic, including in developing countries," UNCTAD said. **92%** of the world's currency is digital.

**Table I: % of Population Owned Digital Currency in 2021**

| Country | Ukraine | Russia | Venezuela | Singapore | Kenya | US | India |
|---|---|---|---|---|---|---|---|
| % | 12.7 | 11.9 | 10.3 | 9.4 | 8.5 | 8.3 | 7.3 |

India has been the leading market for digital payments since 2019. According to a report by ACI Worldwide in March 2021, India was the leading market for real-time payments transactions with 2,550 crore payments, followed by China (1,570 crore) and South Korea (600 crore). The US ranked 9th with 120 crore transactions.

**Table II: Countries with Digital Payments in 2020**

| Position | Country |
|---|---|
| 1 | India |
| 2 | China |
| 3 | South Korea |
| 4 | Thailand |
| 5 | United Kingdom |
| 6 | Nigeria |
| 7 | Japan |
| 8 | Brazil |
| 9 | USA |
| 10 | Mexico |

PhonePe, with 212 crore transactions, was the leading UPI app in February, followed closely by Google Pay with 152.4 crore transactions, according to NPCI data. India has different reliable apps for digital payment. Digital transactions increased by nearly 90% over the three years from the financial year 2019 to 2021, with 300 billion digital payments made in India in 2021. According to market experts' predictions and statistics, the market is expected to reach $ 1 trillion by 2026. Companies like Paytm and Google Pay have pioneered digital payment in India. Number of cyber crimes related to online banking across India from 2016 to 2021

**Table III: Cybercrime on Online Banking in India (2016-'20)**

| Year | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|---|
| Number of online banking Cyber Cases in India | 1343 | 2095 | 968 | 2093 | 4047 | 4823 |

**Manuscript received on 29 January 2023 | Revised Manuscript received on 04 February 2023 | Manuscript Accepted on 15 February 2023 | Manuscript published on 28 February 2023.**
*Correspondence Author(s)
**Dr. Kurian M.J***, Department of Computer Applications, Baselios Poulose II Catholicos College, Piravom, (Kerala), India. Email: kurianmjbpccollege@gmail.com, ORCID ID: https://orcid.org/0000-0002-0684-7574
**Dr. Sreekanth D**, Head of Research and Solutions, ICT Academy of Kerala (Kerala), India. Email: sreekanth.d@ictkerala.org, ORCID ID: https://orcid.org/0000-0003-3373-0248

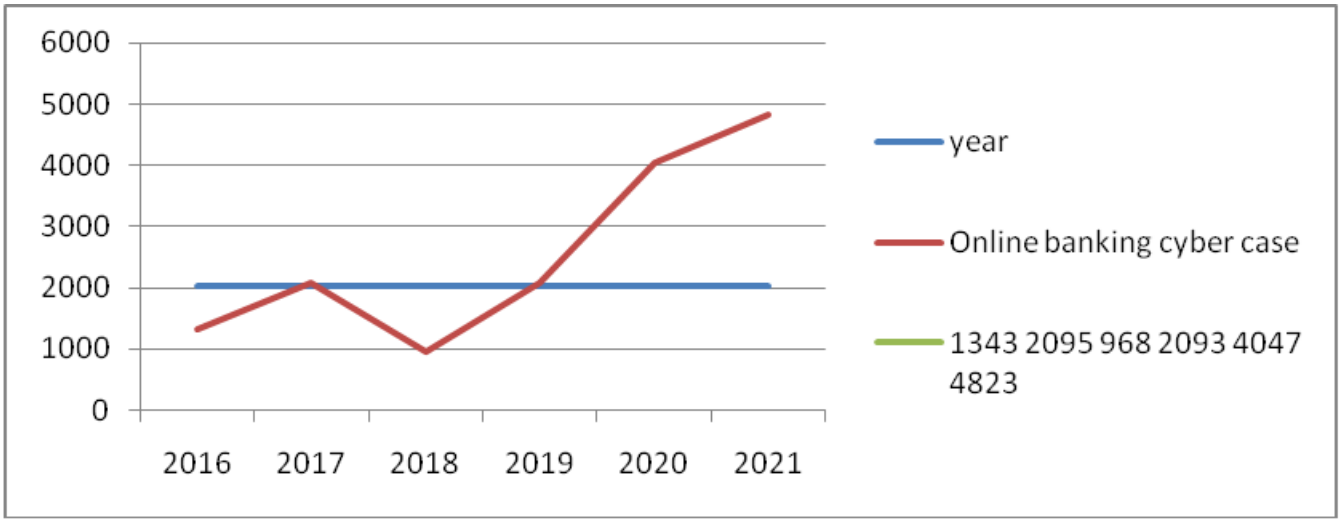


**Fig. 1. Cyber Crime Online Banking in India (2016-2021)**

**Table IV: Cyber Crime Cases in India (2012-2021)**

| Year | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|---|---|---|---|---|
| Number of Cybercrime Cases in India | 3377 | 5693 | 9622 | 11592 | 12317 | 21796 | 27248 | 44546 | 50035 | 52974 |

So, Cybercrime is criminal activity that either targets or uses a computer, a computer network, or a networked device. Most cybercrime is committed by cybercriminals or hackers who seek to profit. However, occasionally, cybercrime aims to damage computers or networks for reasons other than financial gain. These could be political or personal. Individuals or organisations can commit cybercrime. Individual victims, rather than organizations, have mainly experienced the increase in cyber-dependent crimes [1]. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers. A person who enjoys learning the details of computer systems and how to stretch their capabilities, as opposed to most users of computers, who prefer to learn only the minimum amount necessary [2].

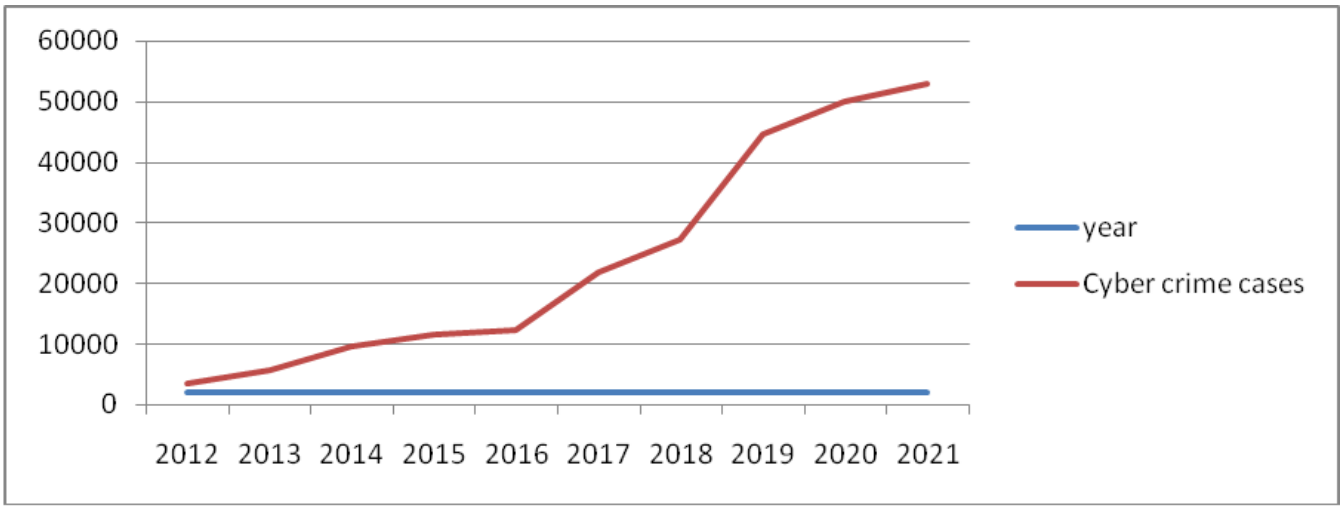


**Fig. 2. Cyber Crime Cases in India (2012-2021)**

## II. CYBERCRIME CATEGORIES

Major categories of cybercrimes are as follows:

- **Crimes against Government.** When a cybercrime is committed against the government, it is considered an attack on that nation's sovereignty and an act of war. Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and the use of pirated software.
- **Crimes against People.** While these crimes occur online, they have a tangible impact on the lives of actual people. Some of these crimes include cyber harassment and stalking, distribution of child pornography, various types of spoofing, credit card fraud, human trafficking, identity theft, and online-related libel or slander. Thus, regardless of its merits or demerits, the term cybercrime generally encompasses all offences against people [3].

- **Crimes against Property.** Some online crimes happen against property, such as a computer or server. These crimes include DDOS attacks, hacking, virus transmission, cyber and typo squatting, computer vandalism, copyright infringement, and IPR violations. A significant increase in cyber crimes in 2021 compared to previous years. During the COVID-19 pandemic, from 2020 to 2021, many individuals were forced to use online services, resulting in approximately 50,000 cyber incidents being reported. The highest share during the period was from Uttar Pradesh and Karnataka.

**Table- V: Cybercrime cases in Kerala, India (2016- 2022 Oct)**

| Year | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 (up to October) |
|---|---|---|---|---|---|---|---|
| Number of Cyber Cases in Kerala | 283 | 320 | 340 | 307 | 426 | 626 | 684 |

From Table V, it is clear that there was a 47% increase in cybercrime during the COVID-19 pandemic period, which shows that cybercriminals utilise the public's ignorance for such activities. This is illustrated in Figure 3.

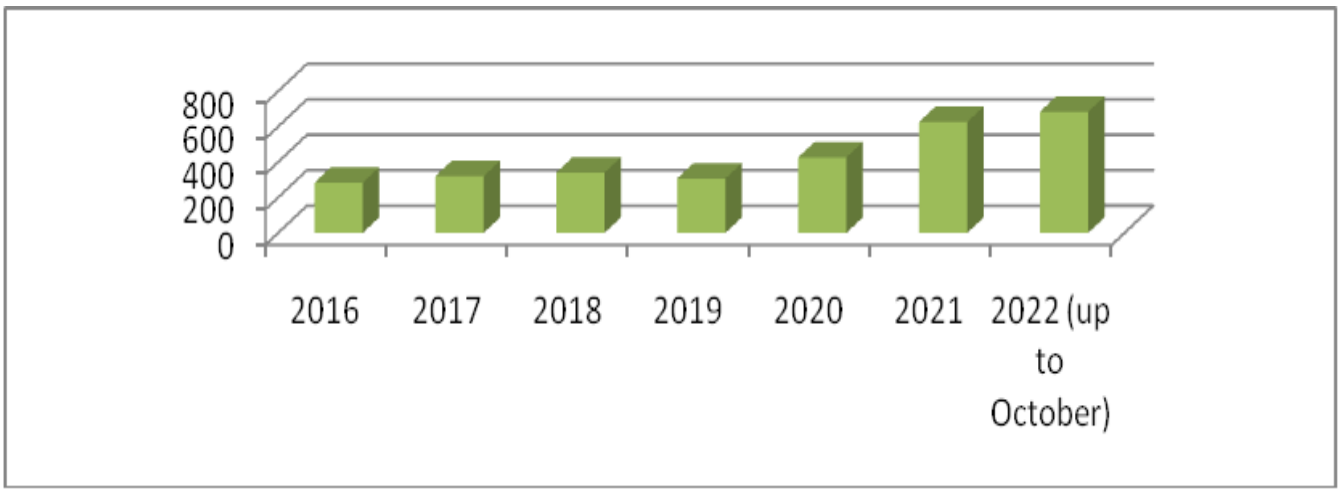


**Fig. 3. Cyber crime cases in Kerala, India (2016-2022 Oct)**

The states that recorded the most cybercrime cases, mostly between 2019 and 2021, are as follows.

**Table- VI: Cyber Crime Cases in India States (2019-2021)**

| States | Telangana | Uttar Pradesh | Karnataka | Maharashtra | Assam |
|---|---|---|---|---|---|
| 2019 | 2691 | 11416 | 12020 | 4967 | 2231 |
| 2020 | 5024 | 11097 | 10741 | 5496 | 3530 |
| 2021 | 10303 | 8829 | 8136 | 5562 | 4846 |

Five Motives for Committing Cybercrimes in 2021.

**Table- VII: Major crimes motives and corresponding crime count.**

| Motives | Personal Revenge | Fraud | Sexual Exploitation | Extortion | Causing Disrepute |
|---|---|---|---|---|---|
| No. of Crimes | 1470 | 30142 | 3293 | 2440 | 1706 |

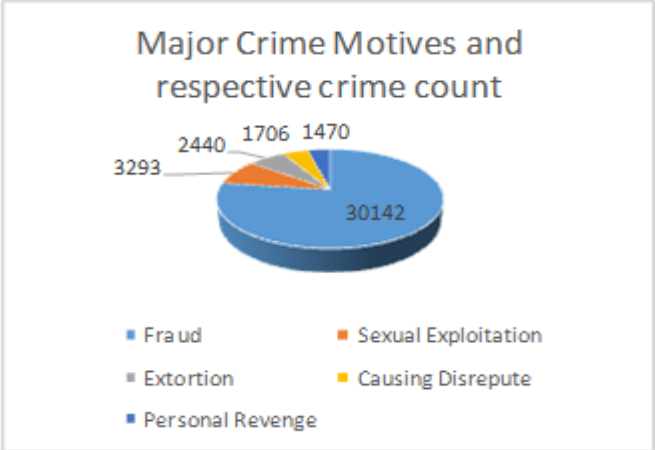


**Fig. 4. Major Crime Motives and Crime Count**

Figure 4 shows that fraud is the most dangerous cybercrime, followed by sexual exploitation, in the COVID pandemic year 2021.

## III. TYPES OF CYBER CRIME

While there are many different ways an attacker can infiltrate an IT system, most cyberattacks rely on similar techniques. Below are some of the most common.

Types of cyber-attacks:

- Malware
- Phishing
- Man-in-the-middle attack (MITM)
- Distributed Denial-of-Service (DDoS) attack
- SQL injection
- Zero-day exploit
- DNS Tunnelling
- Business Email Compromise (BEC)
- Cryptojacking
- Drive-by Attack
- Cross-site scripting (XSS) attacks
- Password Attack
- Eavesdropping attacks
- AI-Powered Attacks
- IoT-Based Attacks

The most common cyber-attacks are malware, phishing, MITM, password, and SQL injection, of which malware, phishing, and MITM are the most frequently occurring. Some of them are explained as follows.

- **Hacking**: Any illegal access to a computer system is generally referred to as hacking. When a hacker gains unauthorized access to a company's or an individual's computers and networks, they can obtain access to crucial corporate information as well as personal and private data. Despite this, not all hackers are crooks. Some "white hat" hackers are employed by software businesses to identify faults and gaps in their surveillance systems
- **Phishing**: Phishing happens when fraudsters act as an organization to dupe victims into disclosing important information. Scare techniques, such as notifying the victim that their bank account or personal device is under attack, are frequently used by cybercriminals to effectively fulfil their phishing aims. Traditional methods for identifying phishing links rely on blacklists and white lists, but this cannot identify new phishing links [4].
- **Malware**: Malware refers to any software program designed to infiltrate or harm a device. Viruses are a type of malware. Viruses may cause a range of problems once they enter a device. They may delete files, record your keystrokes, erase your disk drive, or otherwise corrupt your data.
- **Ransomware**: Ransomware is a sort of cyber extortion that uses malware to achieve its purpose. This software threatens to disclose the victim's data or to block the user from retrieving his/her data unless the cybercriminal gets a predetermined sum of money
- **Theft via cyberspace**: Cyber theft is a type of cybercrime that involves an individual infiltrating another person's or company's system to steal wealth, private information, financial information, or proprietary data. Identity theft and embezzlement are examples of fraudulent crimes that might be classified as cyber theft crimes.
- **Cyberbullying: Bullying an individual online is referred to as cyberbullying**. Cyberbullying includes any threat to a person's safety, coercion of a person to say or do anything, and expressions of hatred or subjectivity against someone. While children are more likely to be victims of cyberbullying, adults are not exempt. According to a survey, 40% of polled teens said they had encountered online harassment, while 24% of adults aged 26–35 said they had experienced cyberbullying.
- **Extortion via the internet**: Cyber extortion is a type of blackmail that takes place through the internet. In these instances, cybercriminals target or attempt to harm the person and demand payment or a response to halt their threats.
- **Cryptojacking: When hackers utilise other people's processing resources to mine cryptocurrency without their permission, this is referred to as cryptojacking**. Cryptojacking differs from cybercrimes that utilise malware to infiltrate a victim's device and steal data, whereas cryptojackers are not interested in stealing a victim's data. Cryptojackers, on the other hand, employ the computing power of their victim's gadget. Although it may appear less harmful than other cybercrimes, cryptojacking should not be taken lightly, as falling prey to it can significantly slow down one's device and render it vulnerable to further cyberattacks.
- **Cyber spying:** Cyber spying occurs when hackers target a public or private entity's network to gain access to classified data, private information, or intellectual property. Cybercriminals may utilise the sensitive information they obtain for various purposes, including blackmail, extortion, public humiliation, and financial gain.
- **Spyware:** Spyware is software that cybercriminals employ to monitor and record their victims' actions and personal information. Often, a victim unintentionally downloads spyware onto their device, giving a cybercriminal unwitting access to their data. Cybercriminals can access a victim's credit card data, passwords, webcam, and microphone, depending on the type of spyware employed.
- **Adware:** Adware is software that you may unintentionally download and install when installing another program. Every time someone views or clicks on an advertisement window, the developers of adware programs profit financially from their actions on people's computers. Although some adware software is lawful and innocuous, others are invasive due to the type and number of ads they display. Many nations consider some adware applications to be unlawful because they contain spyware, malware, and other dangerous software.
- **Botnets**: Botnets are malware-infected computer networks. Malicious hackers infiltrate and gain control of these machines to conduct online activities without the user's consent, enabling them to commit fraudulent crimes while remaining undetected. They may send spam emails and conduct targeted hacks into a company's assets, financial records, data analyses, and other vital information.

- **Dating scams:** Some hackers use dating websites, chat rooms, and online dating apps to pose as potential partners and lure people into sharing their data.

These hackers gain access to a company's network to identify existing vulnerabilities in their clients' systems and provide fixes for such issues.

- Email and internet fraud.
- Identity fraud (where personal information is stolen and used).
- Theft of financial or card payment data.
- Theft and sale of corporate data.
- Cyber extortion (demanding money to prevent a threatened attack).
- Ransomware attacks (a type of cyber extortion).
- Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
- Cyberespionage (where hackers access government or company data).
- Interfering with systems in a way that compromises a network.
- Infringing copyright.
- Illegal gambling.
- Selling illegal items online.
- Soliciting, producing, or possessing child pornography.
- Cybercrime involves one or both of the following:
- Criminal activity *targeting* computers using viruses and other types of malware.
- Criminal activity *using* computers to commit other crimes.

Cybercriminals who target computers may infect them with malware to damage devices or prevent them from functioning correctly. They may also use malware to delete or steal data. Alternatively, cybercriminals may block users from accessing a website or network, or prevent a business from providing a software service to its customers, a type of attack known as a Denial-of-Service (DoS) attack. Cybercrime that *uses* computers to commit other crimes may involve using computers or networks to spread malware, illegal information or illegal images. Cybercriminals often engage in both activities simultaneously. They may target computers with viruses first and then use them to spread malware to other machines or throughout a network. Some jurisdictions recognise a third category of cybercrime, where a computer is used as an accessory to a crime.

**Table VII: Country-Wise Average Cyber Cost**

| Country | U S | Japan | Germany | UK | France | Singapore | Canada | Spain | Italy | Brazil | Australia |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Average Cybercrime cost (in Million Dollars) | 23.7 | 13.5 | 13.1 | 11.4 | 9.7 | 9.3 | 9.2 | 8.1 | 8 | 7.2 | 6.8 |
| Increase from 2017 (%) | 29 | 30 | 18 | 31 | 23 | n/a | n/a | n/a | 19 | n/a | 26 |

From Table VII and Fig. 5, it is clear that the average cyber cost (in million dollars) is highest in the United States of America, followed by Japan.

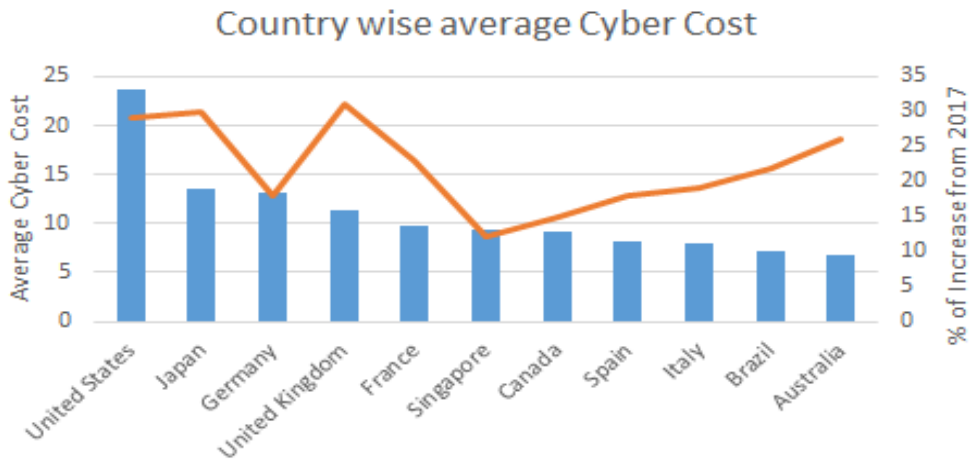


**Fig. 5.Country-Wise Average Cyber Cost**

## IV. IMPACT OF CYBER CRIME

Generally, cybercrime is on the rise. According to Accenture's State of Cyber Security Resilience 2021 report, security attacks increased 31% from 2020 to 2021. The number of attacks per company increased from 206 to 270 year on year. Attacks on companies also affect individuals, as many companies store sensitive data and personal information from their customers. A single attack – whether it's a data breach, malware, ransomware or DDoS attack - costs companies of all sizes an average of $200,000, and many affected companies go out of business within six months of the attack, according to insurance company Hiscox. Javelin Strategy & Research published an Identity Fraud Study in 2021, which found that identity fraud losses for the year totalled $56 billion. For both individuals and companies, the impact of cybercrime can be profound, primarily in terms of financial damage, as well as loss of trust and reputational damage. The growth of potential sales in cyberspace is a key reason for the increasing attention to cybercrime [5].

## V. CYBER LAWS

Most of these types of cybercrimes have been addressed by the IT ACT of 2000 and the IPC. To regulate criminal activities in the cyber world and protect the technological advancement system, the Indian parliament approved the Information Technology Act, 2000. It was the first global law of India to deal with technology in the field of e-commerce, e-governance, electronic banking services, as well as penalties and punishments regarding computer crimes [6].
Cybercrimes under the IT ACT include:

- Sec. 65, Tampering with Computer Source Documents.
- Sec. 66, Hacking Computer Systems and Data Alteration.
- Sec. 67, Publishing Obscene Information.
- Sec. 70, Unauthorized Access of Protected Systems.
- Sec. 72, Breach of Confidentiality and Privacy.
- Sec. 73, Publishing False Digital Signature Certificates.

Special Laws and Cybercrimes under the IPC include:

- Sending Threatening Messages by Email, Indian Penal Code (IPC) Sec. 503.
- Sending Defamatory Messages by Email, Indian Penal Code (IPC) Sec. 499
- Forgery of Electronic Records, Indian Penal Code (IPC) Sec. 463
- Bogus Websites & Cyber Fraud, Indian Penal Code (IPC) Sec. 420
- Email Spoofing, Indian Penal Code (IPC) Sec. 463
- Web-Jacking, Indian Penal Code (IPC) Sec. 383
- Email Abuse, Indian Penal Code (IPC) Sec. 500

There are also cybercrimes under the Special Acts, which include:

- Online Sale of Arms Under Arms Act, 1959
- Online Sale of Drugs Under the Narcotic Drugs and Psychotropic Substances Act, 1985

## VI. E-COMMERCE SECURITY THREATS & PROTECTION

Ever since the first online businesses entered the internet, financial fraudsters have been giving businesses a headache. Although e-commerce is utilising effective marketing strategies and attractive web design, cyber-attacks can still ruin the company. So, the awareness regarding various cyber-attacks and cybersecurity schemes has become mandatory for the successful running of an online business [7]. There are various types of financial fraud prevalent in the e-commerce industry; however, we will discuss some of the most common ones.

- **Credit Card Fraud:** It happens when a cybercriminal uses stolen credit card data to buy products on your e-commerce store. Usually, in such cases, the shipping and billing addresses vary. You can detect and curb such activities on your store by installing an AVS – Address Verification System. Another form of credit card fraud is when the fraudster steals your personal details and identity to obtain a new credit card in your name.
- **Fake Return & Refund Fraud:** Bad actors perform unauthorised transactions and cover their tracks, resulting in significant losses for businesses. Some hackers also engage in refund fraud, where they file fake return requests to obtain refunds.
- **Phishing:** Several e-commerce shops have received reports of their customers receiving messages or emails from hackers masquerading as the legitimate store owners. Such fraudsters present fake copies of your website pages or another reputable website to trick users into believing them
- **Spamming**: Some bad players can send infected links via email or social media inboxes. They can also leave these links in their comments or messages on blog posts and contact forms. Once you click on such links, they will direct you to their spam websites, where you may end up being a victim.
- **DoS & DDoS Attacks**: Many e-commerce websites have incurred losses due to disruptions in their websites and overall sales resulting from DDoS (Distributed Denial of Service) attacks.
- **Malware**: Hackers may design malicious software and install it on your IT and computer systems without your knowledge. These malicious programs include spyware, viruses, trojans, and ransomware.

The systems of our customers, admins, and other users might have Trojan Horses downloaded on them. These programs can easily swipe any sensitive data that might be present on the infected systems and may also infect your website.

### A. Exploitation of Known Vulnerabilities

Attackers are on the lookout for specific vulnerabilities that may exist in the e-commerce store. Often, an e-commerce store is vulnerable to SQL injection (SQLi) and Cross-site Scripting (XSS).

- **SQL Injection:** This is a malicious technique where a hacker attacks your query submission forms to access your backend database. They corrupt your database with an infectious code, collect data, and later wipe out the trail. Structured query injection poses a significant threat to web applications and is one of the most common and widely used information theft mechanisms [8].
- **Cross-Site Scripting (XSS):** The attackers can plant a malicious JavaScript snippet on your e-commerce store to target your online visitors and customers. Such codes can access your customers' cookies and compute. You can implement the Content Security Policy (CSP) to prevent such attacks. Detection of XSS efficiently is still an open issue. Cross-site scripting has been addressed through static and dynamic analysis previously. Both techniques have shortcomings and fail due to frequent variations in the XSS payload [9].

### B. Protection against Cybercrime

Individual internet users are commonly considered the weakest links in the cybersecurity chain because they tend to be overoptimistic regarding their online safety [10]. There are some tips to protect our computer and our personal data from cybercrime:



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- **Keep software and operating system updated:** Keeping our software and operating system up to date ensures that we benefit from the latest security patches to protect our computer.
- **Use anti-virus software and keep it updated:** Utilising anti-virus software or a comprehensive internet security solution is a smart way to protect your system from malware and other online threats. Anti-virus software allows you to scan, detect and remove threats before they become a problem. Having this protection in place helps to protect our computer and our data from cybercrime, giving you peace of mind. Keep your antivirus updated to receive the best level of protection.
- **Use strong passwords:** Ensure you use strong passwords that people cannot easily guess and do not record them anywhere. Alternatively, use a reputable password manager to generate strong passwords randomly, making this process easier.
- **Never open attachments in spam emails:** A classic way that computers get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.
- **Do not click on links in spam emails or untrusted websites:** Another way people become victims of cybercrime is by clicking on links in spam emails or other messages or on unfamiliar websites. To stay safe online, avoid doing this.

**Table VIII: Monetary Damage Caused by Cyber Crime**

| Year | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Total Damage | 17.8 | 54 | 125.6 | 68.1 | 183.1 | 198.4 | 239.4 | 264.6 | 559.7 | 485.25 | 521.40 | 581.44 | 781.84 | 800.49 | 1070.71 | 1450 | 1418 | 1460 | 1520 | 1542 |

- **Do not give out personal information unless secure:** Never give out personal data over the phone or via email unless you are entirely sure the line or email is safe. Ensure that you are speaking to the person you believe you are.
- **Contact companies directly about suspicious requests:** If you are asked for personal information or data from a company that has called you, hang up. Call them back using the number listed on their official website to ensure you are speaking with them directly and not a cybercriminal. Ideally, use a different phone because cybercriminals can hold the line open.
- **Be mindful of which website URLs you visit:** Keep an eye on the URLs you are clicking on. Do they look legitimate? Avoid clicking on links with unfamiliar or suspicious URLs that appear to be spam. If your internet security product includes functionality to secure online transactions, ensure it is enabled before carrying out financial transactions online.
- **Keep an eye on your bank statements:** Spotting that you have become a victim of cybercrime quickly is essential. Keep an eye on your bank statements and query any unfamiliar transactions with the bank. The bank can investigate whether they are fraudulent.

The amount of monetary damage caused by reported cybercrime to the IC3 from 2001 to 2020 (in million U.S. dollars) is described in the table below.

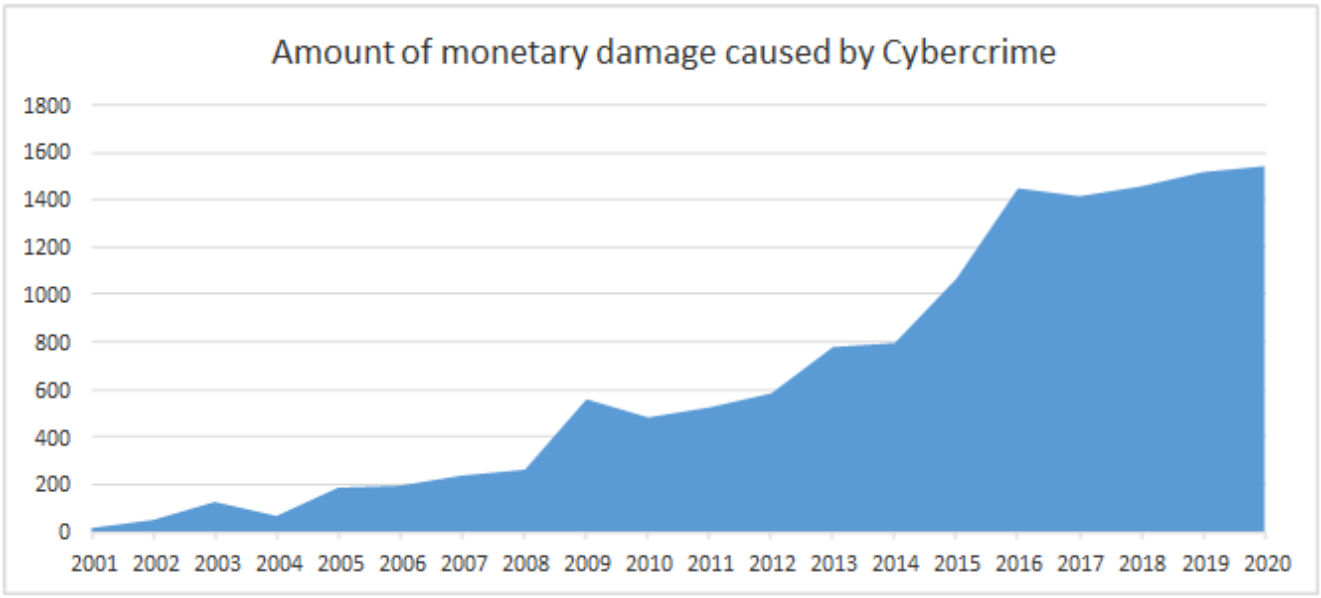


**Fig. 6. Amount of Monetary Damage Caused by Cyber Crime**



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

## VII. RESULT AND DISCUSSION

Cyber attacks are malicious attempts to access or damage a computer or network system. The main consequences of cybercrime are loss of revenue, theft of personal and medical information, the time wasted when IT personnel must dedicate a significant part of their day to handling such incidents, and a damaged reputation of the organisation. Cybersecurity helps protect a company's data, systems, and networks from malicious attacks and cyber threats. Security Awareness Training helps employees understand the importance of cybersecurity and teaches them how to identify potential threats and respond appropriately.

According to Net Set Security Research, malware attacks increased by almost 400% in 2020, mainly due to the COVID-19 pandemic, which led to a decline in cybersecurity awareness. The data mentioned in this paper reveals to the layman that prevention and protection are essential, as in the proverb "prevention is better than cure. "If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees – Kahlil Gibran.

## VIII. CONCLUSION

The most common forms of cybercrime are phishing, which involves using fake email messages to obtain personal information from internet users and misuse it. Protect our Storage Data: Stealing Data or information is the leading cause of any form of hacking. Therefore, it is essential to encrypt all data to prevent any kind of attack on the system or database, as this could compromise privacy. So, cybersecurity is crucial; it safeguards all types of data against theft and loss. Sensitive data, protected health information (PHI), personally identifiable information (PII), intellectual property, personal information, data, and government and business information systems are all included. This paper concludes with a message: prepare and prevent instead of repair and repent. Best be safe today.

## DECLARATION

| | |
|---|---|
| Funding/ Grants/ Financial Support | No, I did not receive. |
| Conflicts of Interest/ Competing Interests | No conflicts of interest to the best of our knowledge. |
| Ethical Approval and Consent to Participate | No, the article does not require ethical approval or consent to participate, as it presents evidence that is not subject to interpretation. |
| Availability of Data and Material/ Data Access Statement | https://www.statista.com/statistics/309435/india-cyber-crime-it-act/ https://keralapolice.gov.in/crime-statistics/cyber-cases |
| Authors Contributions | All authors have equal participation in this article. |

## REFERENCES


1. David Buil-Gil, Fernando Miro-Llinares "Cyber crime and shifts in opportunities during COVID-19: a preliminary analysis in the UK" European Societies Vol. 23, 2021. [CrossRef]
2. Orly Turgeman-Goldschmidt," Meaning that Hackers assign to their being a Hacker", International Journal of Cyber Criminology, vol2 (2) Dec.2008
3. Kristy Phillips, JC Davidson, "Conceptualizing Cybercrime: Definitions, Typologies and taxonomies", Forensic Sciences, April 2022. [CrossRef]
4. Lizhen Tang, Qusay H Mahmoud, "A survey of machine learning-based solutions for phishing website detection", Machine Learning & Knowledge Extraction, August 2021.
5. Nashrudin Setiawan, Vita Emia Tarigan, " Impact of Cybercrime in E-Business and Trust", International Journal of Civil Engineering and Technology, Vol. 9(7) 2018.
6. Divy Shivpuri, " Cyber crime: Are the laws outdated for this type of crime?", International Journal of Research in Engineering Science and Management, Vol. 4, No. 7, 2021.
7. Sumit Badotra, Amit Sundas, "A system review on security of E-Commerce system", International Journal of Applied Science and Engineering, Vol. 18(2), June 2021.
8. Fairoz Q Kareen & Siddeeq Y Ameen, " SQL injection attacks prevention system Technology: Review", Asia Journal of research in computer Science, 10(3),2021.
9. Iram Tariq, Muddassar Azam Sindh, "Resolving Cross-site Scripting attack through genetic algorithm and reinforcement learning", Expert System with applications Vol . 168, April 2021. [CrossRef]
10. Lie De Kimpe, Michiel Walrave, "What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context" Behaviour & Information Technology Vol. 41(8),2022. [CrossRef]


## AUTHORS PROFILE

**Dr. Kurian M. J.** M.Sc. (Maths), M.C.A., M.Phil., Ph.D, Associate Professor & Head of Department of Computer Applications, Baselios Poulose II Catholicos College, Piravom, an aided college affiliated to Mahatma Gandhi University, Kottayam. Twenty-three years of teaching experience. Member of the Board of Studies (2017-2020) and Expert Committee in Integrated Programs Computer Science (2020) of Mahatma Gandhi University. Member of the syllabus and curriculum design of the Integrated M.Sc. Programs in Computer Science (Integrated M.Sc. Computer Science(Artificial Intelligence and Machine Learning), Integrated M.Sc. Computer Science –Data Science, B.C.A, B.Sc. Computer Science and B.Sc.(IT) offered by Mahatma Gandhi University, Kottayam. Serving as Subject Expert in Computer Science. Deputy Chairman of Examinations. Serving as question paper setter for different organizations. Served as a resource person for other conferences. Completed UGC sponsored Minor Research Project –year 2010.

**Dr. Sreekanth D,** an experienced senior professional with a demonstrated history of working in the education and skilling domain. Expertise in Data Science, Machine Learning and Cyber Security with strong capacity to design ICT-enabled solutions. Professional with a Doctor of Philosophy (Ph.D.) degree focused on Machine Learning from Bharathiar University. He has co-authored a book titled "Classical Management Information Systems." Dr. Sreekanth is a member of the pool of examiners at IGNOU and also a member of the Board of Studies at various colleges, including Mar I College, Trivandrum, and Christ College, Thrissur. He has conducted numerous student and faculty development Programs throughout the state and acted as a resource person. He is a winner of the Government of Kerala's e-Government Award 2016-17.