Cyber Crime Attack in Networks - Prevention & Protection

1Dr. Shaju Varughese, 2Dr. kurian M.J
1Associate Professor, 2Associate Professor
B.PC College ,Piravom

Abstract - **The Cyber is the term relating to or characteristic of the culture of computers, information technology, and virtual reality. The Internet is a global network of billions of computers and other electronic devices. A total of 5.07 billion people around the world use the internet today – equivalent to 63.5 percent of the world's total population. Internet users continue to grow too, as of 2022, China had over one billion internet users, more than any other country in the world. India ranked second, as close to 933 million Indians accessed the internet via any device. Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. The slogans used to address data privacy are: "Data privacy belongs to you.". Lock it down, protect it, and block hackers. Our cyberspace, our digital life. This paper concentrate on issues related to hacking, impact of cybercrime , basic cyber laws, security threats and protection which are a warning alarm to internet users.**

keywords - **Cybercrime, hacking , Phishing , Cyberbullying ,Cyber spying, Spyware, Adware, DoS**

I. Introduction

Cybercrime is a global problem which has been dominating the news cycle. It poses a threat to individual security and an even bigger threat to government, banking sector and large international companies. Today's organized cybercrimes far out shadow lone hackers of the past now large organized crime rings function like start-ups and often employ highly-trained developers who are constantly innovating online attacks. With so much data to exploit out there, Cyber security has become essential.

It is very clear that young generation lives on the internet, and we , the general users are almost ignorant as to how those random bits of 1's and 0's reach securely to our computer. It is a golden age of hackers and cyber-attacks are evolving by the day. With so many access points, public IP's and constant traffic and tons of data to exploit, black hat hackers, are having one hell of a time exploiting vulnerabilities and creating malicious software for the same. Hackers are becoming smarter and more creative with their malware and how they bypass virus scans and firewalls still baffles many people. Even though there has to be some sort of protocol that protects us against all these cyber attacks, our data falls into the wrong hands. In this context, world think about cyber security and how to protect ourselves.

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 want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal. Cybercrime can be carried out by individuals or organizations. The increase in cyber-dependent crimes has mainly been experienced by individual victims rather than organizations [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].

II. categories of cyber crime

The three major categories of cybercrimes are as follows:

- Crimes against People. While these crimes occur online, they affect 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 to encompass 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.

- 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 pirated software.

Top Five Motives for committing Cybercrimes in 2021

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

Table 1 – Major crime motives and corresponding crime count

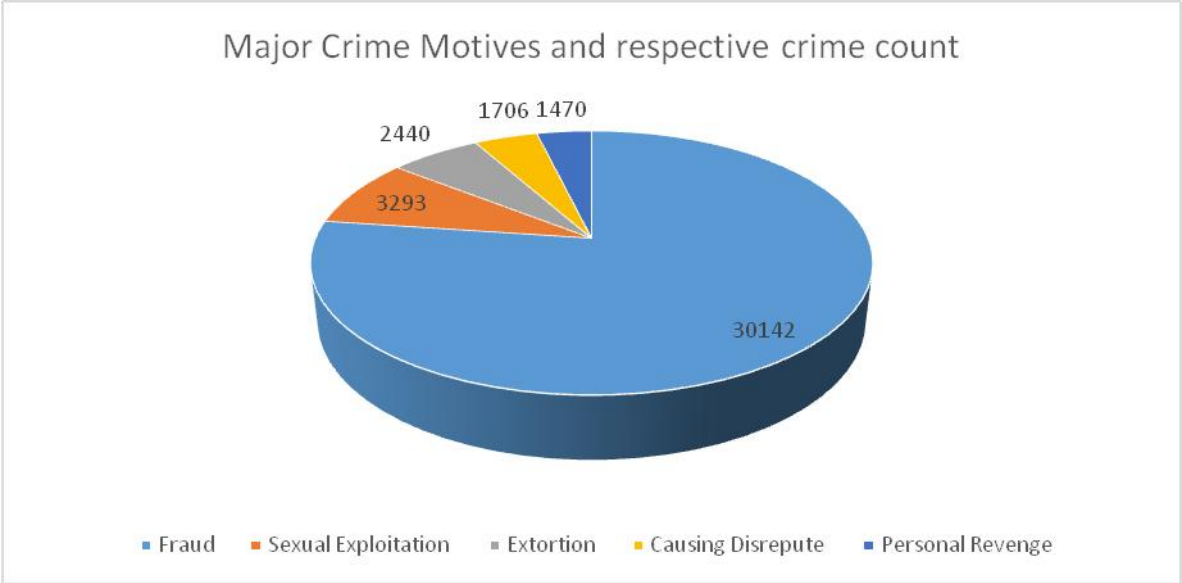

Figure 1 – Major crime motives and corresponding crime count

Indian Cities which have highest number of cybercrimes in 2021

Name of City	Bengaluru	Hydrabad	Mumbai	Lucknow	Ghaziabad
No. of crimes	6423	3303	2883	1067	451

Table 2 – Cities with highest number of cyber crimes

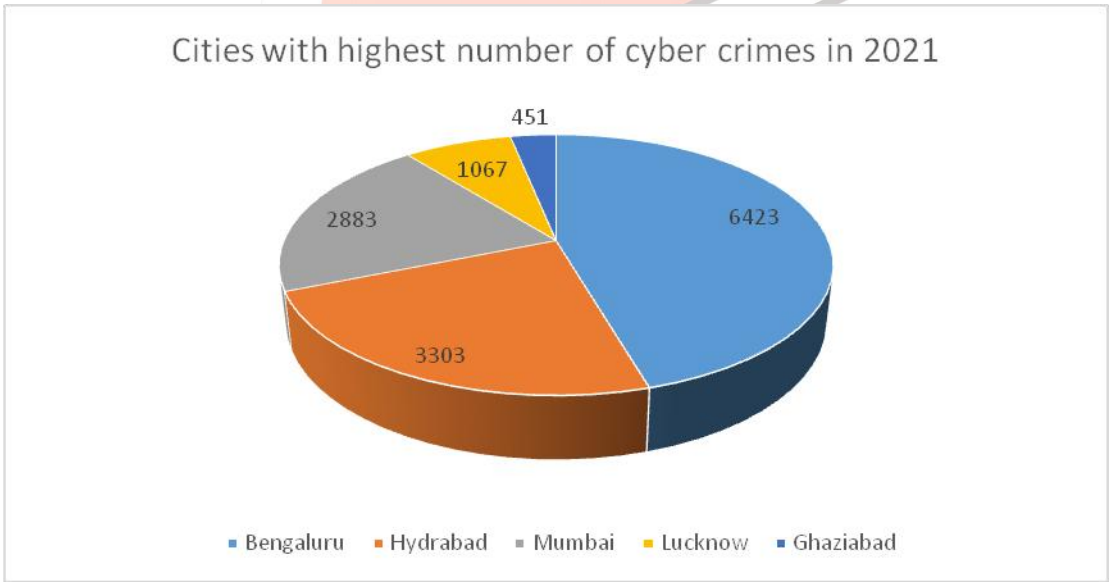

Figure 2 – Cities with highest number of cyber crimes.

III. Cyber crime types

Types of cybercrime include:

- Theft via cyberspace: Cyber theft is a sort of cybercrime that includes an individual infiltrating another person's or company's system in order to steal wealth, private information, financial information, or proprietary information. 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.

- Malware: Malware is a term that refers to any software program that is meant to infiltrate or harm a device. Viruses are a type of software that falls under the malware category. 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.
- Phishing: Phishing happens when fraudsters act as an organization in order to dupe victims into disclosing important information. Scare techniques, such as notifying the victim that their bank account or personal device is under assault, are frequently used by cybercriminals to effectively fulfill their phishing aims. Traditional methods for identifying phishing links rely on blacklists and white lists , but this cannot identify new phishing links [4].
- Extortion via the internet: Cyber extortion is a type of blackmail that takes place through the internet. In these occurrences, cybercriminals target or try to harm the person and demand pay or a reaction in order to halt their threats.
- 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.
- Crypto jacking: When hackers utilize other people's processing resources to mine crypto currency without their permission, this is referred to as crypto jacking. Crypto jacking varies from cybercrimes that utilize malware to enter the device of a victim to steal data whereas the crypto jackers are not interested in stealing a victim's data. Crypto jackers, on the other hand, employ the computing power of their victim's gadget. Despite appearing to be less harmful than other cybercrimes, crypto jacking should not be taken lightly because falling prey to it can drastically delay one's device and render it vulnerable to further cyber assaults.
- Cyber spying: Cyber spying occurs when hackers target a public or private entity's network in order to gain access to classified data, private information, or intellectual property. Cybercriminals may utilize the sensitive information they discover for a variety of purposes, including blackmail, extortion, public humiliation, and monetary 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, web cam, 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 in order to do things online without the user's consent, allowing 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 hoodwinks: Some hackers utilize dating websites, chat rooms, and online dating apps to pose as possible mates and attract people in order to have access to their data.
- 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 important 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.

These hackers get into a company's network in order to uncover existing holes in their clients' systems and provide fixes to 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).
- Crypto jacking (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 that target computers may infect them with malware to damage devices or stop them working. They may also use malware to delete or steal data. Or cybercriminals may stop users from using a website or network or prevent a business providing a software service to its customers, which is called 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 are often doing both at once. They may target computers with viruses first and then use them to spread malware to other machines or throughout a network. Some jurisdictions recognize a third category of cybercrime which is where a computer is used as an accessory to crime.

Country	U S	Japan	Germany	UK	Franc e	Singapor e	Canada	Spain	Ital y	Brazil	Austral ia
Average Cybercrime cost (in Million Dollars)	23.7	13.5	13.1	11.4	9.7	9.3	9.2	8.1	8.0	7.2	6.8
Increase from 2017 (%)	29	30	18	31	23	n/a	n/a	n/a	19	n/a	26

Table 3 – Country wise average cyber cost

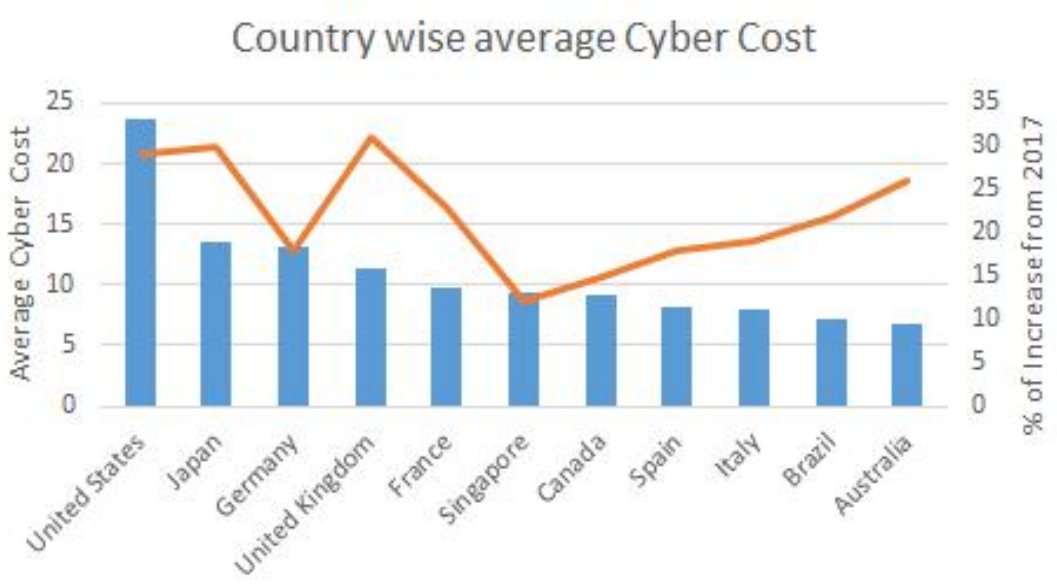

Figure 3 – Country wise average cyber cost..

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 affect individuals too since many of them store sensitive data and personal information from 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 totaled $56 billion.

For both individuals and companies, the impact of cybercrime can be profound – primarily financial damage, but also loss of trust and reputational damage. The growth of potential sales in cyberspace is the reason for increasing attention to cyber crime [5].

V. cyber laws

Most of these types of cybercrimes have been addressed by the IT ACT of 2000 and the IPC. With the intention of regulating criminal activities in the cyber world and protecting the technological advancement system, the Indian parliament approved the law on technological information, 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 Narcotic Drugs and Psychotropic Substances Act, 1985

VI. e-commerce security threats & protection

Ever since the first online businesses entered the world of the internet, financial fraudsters have been giving businesses a headache. Though the E-commerce is using good marketing strategies or attractive web design but still cyber-attacks can ruin the business. So, the awareness regarding various cyber-attacks and cyber security schemes has become mandatory for the successful running of an online business[7].There are various kinds of financial frauds prevalent in the e-commerce industry, but we are going to discuss some of them.

- 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 enable them to get a new credit card.
- Fake Return & Refund Fraud: The bad players perform unauthorized transactions and clear the trail, causing businesses great losses. Some hackers also engage in refund frauds, where they file fake requests for returns.
- Phishing : Several e-commerce shops have received reports of their customers receiving messages or emails from hackers masquerading to be the legitimate store owners. Such fraudsters present fake copies of your website pages or another reputable website to trick the 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 website and overall sales because of DDoS (Distributed Denial of Service) attacks.
- Malware :Hackers may design a malicious software and install on your IT and computer systems without your knowledge. These malicious programs include spyware, viruses, trojan, 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.

Exploitation of Known Vulnerabilities

Attackers are on the lookout for certain vulnerabilities that might be existing in the e-commerce store. Often an e-commerce store is vulnerable to SQL injection (SQLi) and Cross-site Scripting (XSS).

- SQL Injection : It is a malicious technique where a hacker attacks your query submission forms to be able 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 dealt with static and dynamic analysis previously. Both techniques have shortcomings and fail due to frequent variations in XSS payload [9].

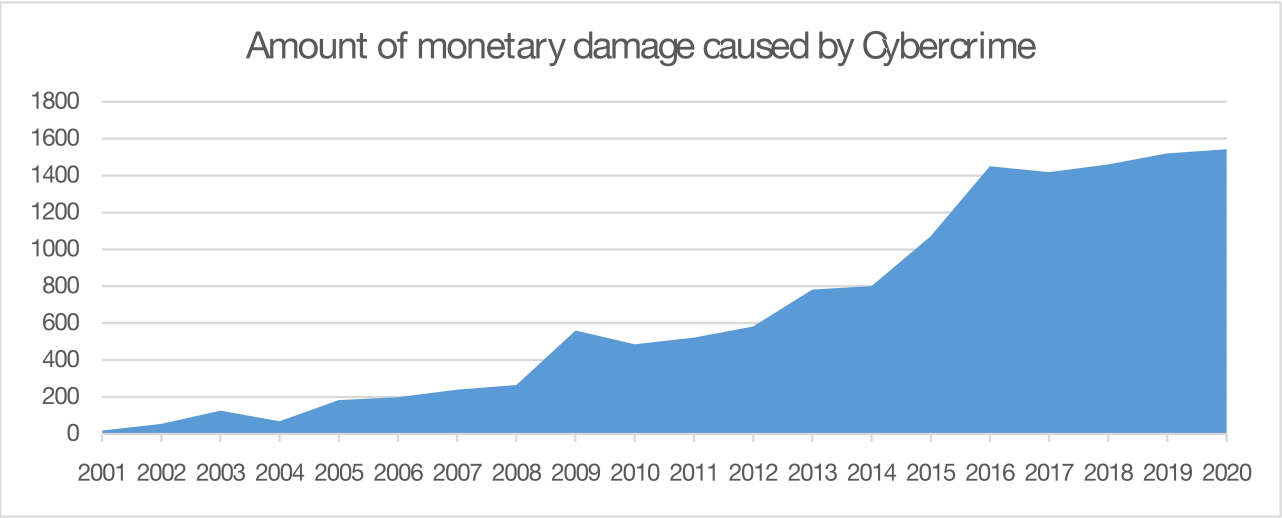

Figure 4 – Amount of monetary damage caused by Cybercrime

Amount of monetary damage caused by reported cybercrime to the IC3 from 2001 to 2020 (in million U.S. dollars)

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

Table 4 – Amount of monetary damage caused by cybercrime..

Protection against Cybercrime

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

- Keep software and operating system updated: Keeping our software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.
- Use anti-virus software and keep it updated: Using anti-virus or a comprehensive internet security solution is a smart way to protect your system from attacks. 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 piece of mind. Keep your antivirus updated to receive the best level of protection.
- Use strong passwords :Be sure to use strong password that people will not guess and do not record them anywhere. Or use a reputable password manager to generate strong passwords randomly to make this 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 unfamiliar websites. Avoid doing this to stay safe online.
- Do not give out personal information unless secure : Never give out personal data over the phone or via email unless you are completely sure the line or email is secure. Make certain that you are speaking to the person you think you are.
- Contact companies directly about suspicious requests :If you are asked for personal information or data from a company who has called you, hang up. Call them back using the number on their official website to ensure you are speaking to them 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 URLs that look like 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 important. Keep an eye on your bank statements and query any unfamiliar transactions with the bank. The bank can investigate whether they are fraudulent.

VII. Conclusion

The most common forms of cybercrime is phishing, using fake email messages to get personal information from internet users and misuse it. Protect our Storage Data: Stealing Data or information is the main cause of any form of hacking. Therefore, it is important that encrypt all data to prevent any and every kind of attack on system or database, as this could prove fatal to privacy. So, cyber security 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 & prevent instead of repair & repent. Best be safe today.

VIII. References

[1] David Buil-Gil, Fernando Miro-Llinares "Cyber crime and shifts in opportunities during covid-19: a preliminary analysis in UK" European societies Vol23,2021.

[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.

[4] Lizhen Tang, Qusay H Mahmoud , "A survey of machine learning-based solution for phishing website detection", Machine Learning & knowledge Extraction August 2021.

[5] Nashrudin Setiawan, Vita Emia Tarigan, " Impact of Cyber crime in E-Business and Trust", International Journal of Civil Engineering and Technology, Vol 9(7) 2018.

[6] Divy Shivpuri, " Cyber crime : Are the law 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 sindhu, "Resolving Cross-site Scripting attack through genetic algorithm and reinforcement learning", Expert System with applications Vlo.168 ,April 2021.

[10] Lie De Kimpe, Miche 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" Behavior & Information TechnologyVol.41(8),2022.