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 Security Issues and Challenges in India

[1]Mr. Purushottam Kumar, [2]Dr. Prakash Kumar

[1]Assistant Professor, [2]Assistant Professor (HOD)

Department of Computer Science and Cyber Security, Jharkhand Raksha Shakti University, Jharkhand, India

[1] purushottamkumar7086@gmail.com [2] mail.drprakash@gmail.com

ABSTRACT: In today's world, where internet access is widespread, data security has emerged as the biggest concern. One of the largest issues in the modern world is information security. Although the word "cyber security" can be helpful, it is difficult to define precisely. It is occasionally incorrectly combined with other ideas like privacy, information sharing, acquiring intelligence, and monitoring. The effective cyber security is regarded as requiring the control of risk to information systems. The dangers posed by any attack depend on three things: threats (who is attacking), vulnerabilities (how they are attacking), and impacts (what the attack does). The government's responsibility in cyber security includes both defending non-government networks and securing its own systems. This paper will examine how this framing injures both human rights and the security of the online world. By the conclusion, it will aid in learning how threats are most commonly perceived in cyberspace. How to participate in these debates and why this framing may be problematic. This paper also seeks to determine how we can interact with the government and the public to uphold and defend these rights. It also focuses on modern techniques and ethics in changing the face of cyber security.

Keywords: cyber security, cyber-attacks, modern cyber-attacks, cyber threats.

I. INTRODUCTION

The word "cyber" is a derivative of the term "cybernetics," which is derived from the Greek word "Kubernetes," which means "pilot" or "steersman." [1] Norbert Wiener, an American mathematician, is actually credited with popularising it. In the 1940s, he published a book titled Cybernetics. This was his forecast for a day when a self-governing PC framework that had an ongoing feedback loop will rule the world. Actually, it wasn't until the 1980s that the term "cyber" became associated with other terms that meant anything connected to digital. Cyber refers to something that is "related to or characterised by computers, virtual reality, or information technology." The Cyber age, often known as the age of analysts, virtual reality, or information technology, is the era in which we currently live. The cyber cosmos is expanding, just like the real one. For instance, thousands and millions of updates on Facebook, Twitter, and other platforms will have been made in the last 60 seconds. Every day, we spend time reading our emails. According to estimates, more than 70% of such emails are truly spam, hacker spam, or spam containing harmful malware attempting to access your systems and your personal data. In everyday speech, the word "security" is synonymous with "safety," but in technical parlance, it also signifies that something has been secured. Cyber security, which is formed by joining the two words, is concerned with protecting cyberspace from risks, specifically cyber threats. Over the past 50 years, the information and communications technology (ICT) sector has undergone significant development. Security has grown to be a serious worry with the introduction of the internet. ICT equipment and parts are frequently interdependent and susceptible to security breaches. Cyber security is the practise of securing information and communication technology (ICT) systems and associated data.

When hackers attempt to compromise or harm a computer network or system, this is known as a cyber attack. The hypothetical setting in which computer network communication takes place is known as cyber space. The word first made its way into mainstream culture through science fiction. Today, however, a large number of people use it, including technological strategists, business titans, security experts, and the military. We refer to the area of the global technological environment as "cyber space." Technology advancements have rendered man totally dependent on the internet, which has an impact on both us as individuals and as a society. Man may now easily access everything while remaining stationary thanks to this. Everything a man may imagine is possible with the use of the Internet, including social networking, online shopping, data storage, gaming, online classes, and job chances. It's used and consumed in all conceivable ways. The idea of cybercrimes grew together with the development of the web and its attendant benefits. The Internet's original creators had no concept that it could be abused for criminal behaviour when it was originally developed.

Cyber security is a crucial tool for safeguarding data and preventing illegal monitoring. The phrase "cyber security," as it is frequently used, relates to three things:

a. A collection of actions and other measures, both technical and non-technical, designed to safeguard computers, computer networks, related hardware, software, and the data and software they store and transmit, as well as other components of cyberspace, from all dangers, including dangers to the country's security.

b. The level of protection brought about by the use of certain practises and precautions.

c. The related sphere of professional endeavour, which includes study and analysis geared toward putting these activities into practise and raising the calibre of them.

The abuse of the invention has increased to its ideal degree along with the rise of innovation. The amount of cybercrime has significantly increased since the turn of the century. Cybercrimes can endanger an individual's safety, a nation's security, or an organization's financial stability. India is not far behind other countries where the frequency of digital infractions is rising day by day in a similar manner.

II.CYBER CRIME IN INDIA

The physical world is overpowering. A cyber fraudster would have targeted one victim every two seconds. The true amount of cybercrime is significantly larger. Cyber fraud, which was earlier known to be operated from Jamtara in Jharkhand, has become a cottage industry as a result of the Covid pandemic. Certain crimes that are committed using or that primarily target computer systems or internet-connected assets, such as email accounts and internet banking, are included in the cyber-crime sections of laws.

According to the Federal Bureau of Investigation's United States Internet Crime Complaint Centre (IC3) 2019 Internet Crime Report, India is ranked third globally among the top 20 countries where cybercrimes are committed. With 93,796 victims of cybercrime, the United Kingdom tops the list among nations other than the USA, followed by Canada (3,721) and India (2,901). Since 2018, the number of cybercrime cases has steadily increased. India recorded 2,08,456 incidents in 2018, 3,94,499 incidents in 2019, 11,58,208 instances in 2020, 14,02,809 cases in 2021, and 2,12,485 events in the first two months of 2022, according to the most recent data from the National Crime Records Bureau (NCRB).

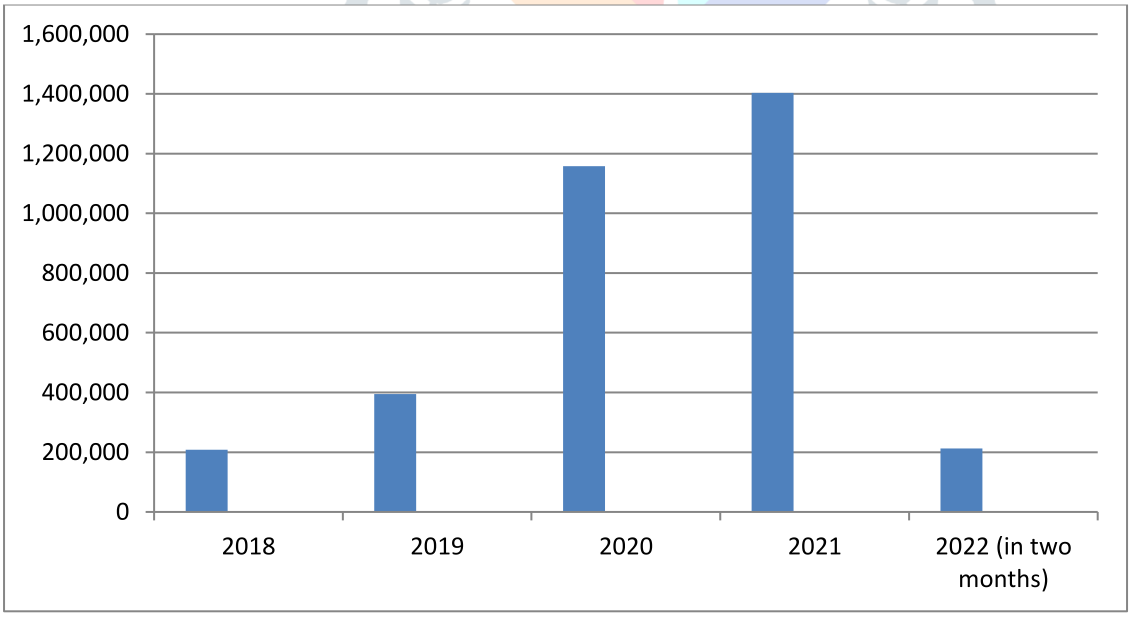


Fig1:- Increase in cyber crime since 2018 (data source: - NRCB)

4,047 cases of internet banking fraud, 2,160 cases of ATM fraud, 1,194 cases of credit/debit card fraud, and 1,093 cases of OTP fraud were reported in 2020. According to NCRB data, there were also 578 instances of fake news on social media and 972 occurrences of cyber bullying and stalking of women and children. Fraud was determined to be the primary motivation, accounting for 30,142 of the 50,035 cases (60.02 per cent). Following these were extortion (4.9%) and sexual exploitation (6.6%). Karnataka has the highest rate of cybercrime (16.2%), followed by Telangana (13.4%) and Assam (10.1 per cent). Around the same time, 1,205 cyber-attack incidences were registered in Telangana. According to Jharkhand police, cyber fraud has extended from Jamtara to the neighbouring city of Deoghar, where around 100 cases have been reported in the previous nine months.

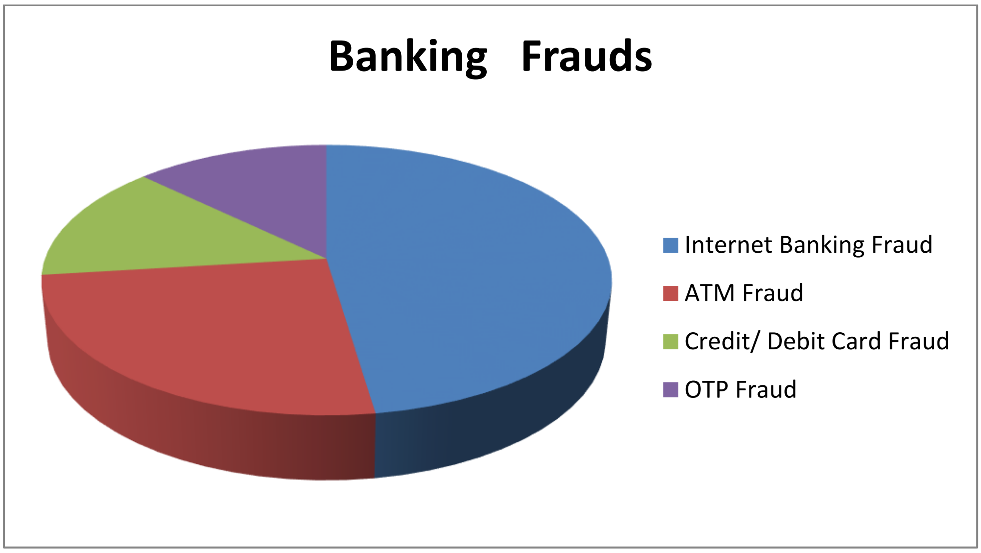
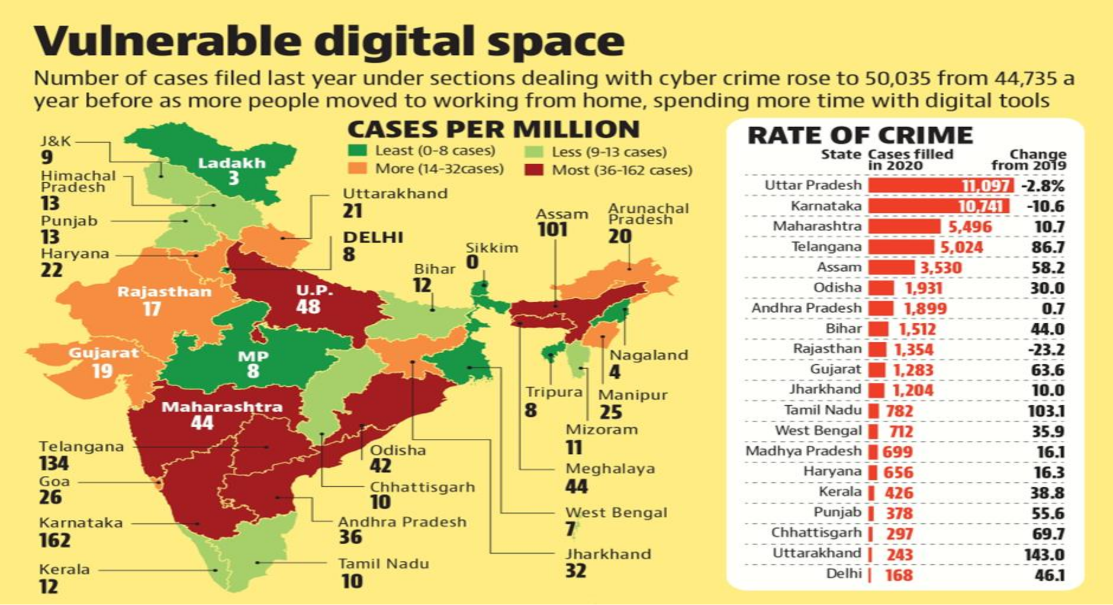


Fig 2:- Most common banking frauds

Several states have recently established specialised units in response to the surge in these crimes. Rajasthan has made the decision to establish a cyber police station in each district, Kerala is creating a new cyber police battalion, Telangana has established a department specifically for investigating cybercrimes, Delhi Police has established a separate wing for cybercrimes and has a unit for spotting cyber-fraud in each district, and Karnataka has made cybercrime detection training mandatory for all police officers in the state.

For reporting cybercrime, the home ministry now has a dedicated website called cybercrime.gov.in. Since the portal's introduction in January 2020, around 200,000 complaints have been submitted. The agency requested that all states file First Instance Reports (FIRs) on complaints received through this site in November 2020. Of the nearly 2,000 000 complaints received through the portal in 2020, 5,000 cases were recorded.


Vulnerable digital space

Number of cases filed last year under sections dealing with cyber crime rose to 50,035 from 44,735 a year before as more people moved to working from home, spending more time with digital tools

RATE OF CRIME

State	Cases filled in 2020	Change from 2019
Uttar Pradesh	11,097	-2.8%
Karnataka	10,741	-10.6
Maharashtra	5,496	10.7
Telangana	5,024	86.7
Assam	3,530	58.2
Odisha	1,931	30.0
Andhra Pradesh	1,899	0.7
Bihar	1,512	44.0
Rajasthan	1,354	-23.2
Gujarat	1,283	63.6
Jharkhand	1,204	10.0
Tamil Nadu	782	103.1
West Bengal	712	35.9
Madhya Pradesh	699	16.1
Haryana	656	16.3
Kerala	426	38.8
Punjab	378	55.6
Chhattisgarh	297	69.7
Uttarakhand	243	143.0
Delhi	168	46.1

Fig 3: - Rise in cyber-crime in different states [12]

III. TOP CYBER ATTACKS AND DATA BREACHES

3.1 Operation Shady RAT: - Dmitri Alperovitch, Vice President of Threat Research at Internet security company McAfee, who also led and identified the Night Dragon Operation and Operation Aurora cyber espionage incursion investigations, reported on Operation Shady RAT, an ongoing series of cyber attacks that began in mid-2006. At least 71 organisations have been affected by the attacks, including the International Olympic Committee, the United Nations, and defence companies. The operation, which Alperovitch named after the abbreviation for remote access tool used frequently in the computer security field, is described by McAfee as "a five-year targeted campaign by one specific actress". The research asserts that a state actor may have been responsible for the hacks after several athletic supervision bodies were targeted around the time of the 2008 Summer Olympics. It is largely believed that the People's Republic of China is that state actor.

3.2World of Hell: -A grey hat computer hacking gang known as World of Hell (or simply WoH) claims responsibility for numerous well-known attacks in 2001. It attracted attention because of its high-profile targets and the humorous messages it posted following its attacks. Since its debut in March 2001, World of Hell has been effective in attacking the websites of numerous significant businesses. It specialises in locating websites with weak security, which it subsequently vandalises with a message offering help. In that time, it has utilised well-known zero-day exploits. World of Hell also participated in "Project-China," a cyber warfare initiative.

3.3Petya cyber attacks:- On June 27, 2017, a wave of potent cyber attacks using the Petya virus flooded the websites of Ukrainian institutions including banks, ministries, media, and utility companies. Similar illnesses have also been recorded in Australia, France, Germany, Italy, Poland, Russia, the United Kingdom, and other countries. It is believed that Stuxnet, a harmful computer worm, has been under development since at least 2005. It was first discovered in 2010. Stuxnet is thought to have significantly harmed Iran's nuclear programme and targets supervisory control and data acquisition (SCADA) systems.

3.4 The Domino's incident in India: - The well-known pizza brand Dominos, India, experienced a significant data leak in the month of May 2021. One million consumers who had placed orders on their portal using either mobile devices or computer systems had all of their information exposed, including names, addresses, delivery locations, cell phone numbers, and email addresses. There were 18 million orders in all.

3.5 Juspay incident: - An Indian payment processor, on a number of websites like Amazon, Swiggy, and others. In 2020, a hack affecting 35 million Juspay user accounts in India went undetected. Masked card data and the cardholders' fingerprints were among the compromised data. Because Telegram App's communications can self-destruct after a set amount of time, the hackers chose it for price negotiation.

3.6Police exam incident: -Hackers stole information from a test in December 2019 to hire police officers in India, and as a result, all 50,000 candidates' private information was exposed. The candidates' biographical information, which included their full names, dates of birth, cell phone numbers, email addresses, FIR records, and criminal histories, was made available for purchase.

3.7 Covid incident: - A database containing the personal data of at least 1500 Indian residents was breached at the start of 2021 as a result of an attack on official websites. Through downloaded PDF files, the hackers had made the data accessible to the general public. Later, it was discovered that the attack was carried out by organisations with a New Delhi basis. A similar issue happened in 2020 when 80,000 COVID-19 patients' personal information was stolen from the Delhi State Health Mission database. The Kerala Cyber Hackers organisation claimed responsibility for the attack and stated that it did so because it was unhappy with how the government was treating medical professionals.

3.8 Unacademy incident: -In May 2020, 22 million customers' data was made available for purchase for USD 2000.

3.9 CAT incident: - 190,000 applicants who took the Common Admission Test, which was administered by the Indian Institutes of Management, had their test scores and personally identifiable information stolen in May 2021 and sold on a cybercrime site.

3.10 Air India incident: - The national airline of India, Air India, had a data breach in February 2021 when an unauthorised user gained access to its Data Management Service Provider, SITA PSS, and stole the information of 4.5 million customers worldwide.

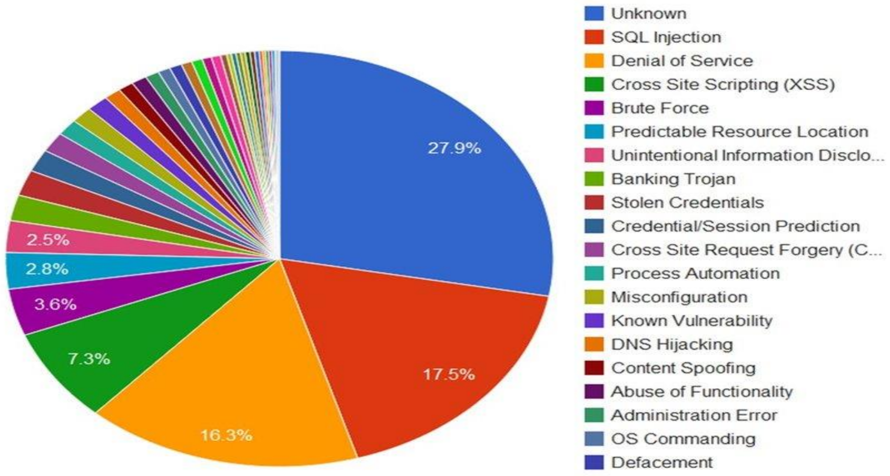


Fig 4: - Most common cyber-attacks [13]

IV. TYPES OF CYBER ATTACKS AND THEIR PREVENTION

4.1 Phishing: - It is the act of sending false messages that appear to be from a trustworthy source, most often by email. This cyber-attack seeks to steal private information like credit card numbers or login credentials, or it may even aim to infect the user's device with malware. A malicious link or attachment will be included in an email that has a trustworthy appearance but is really created by an attacker. Phishers entice victims to click on links and open attachments by appealing to their feelings of urgency, anxiety, and curiosity. Your network may be infiltrated just by clicking on one malicious link, and the phisher may steal your personal information. One of the most prevalent types of cyber-attack is phishing, largely because it's simple to execute and surprisingly successful.

The following are some of the riskiest phishing scenarios:

- Withdrawal of funds from your bank account.
- Unauthorized use of your credit cards.
- Gaining access to your files and media by the phisher.
- The phisher is using your accounts to post bogus updates on social media.
- A friend or family member is put at risk when the phisher pretends to be you in their presence.

Preventions: - Observing hypertext links is one of the greatest ways to spot a phishing attack. Verify that the destination URL link matches the email's contents. Additionally, stay away from clicking on links that include unusual characters or are truncated. Phishing attempts are also guarded against using HTTPS (SSL).

4.2 Distributed Denial-of-Service (DDoS) Attack: - A distributed denial-of-service (DDoS) attack is an intentional attempt to obstruct a server, service, or network's regular traffic by saturating the victim or its surrounding infrastructure with an enormous amount of Internet traffic. By using numerous compromised computer systems as sources of attack traffic, DDoS attacks are made effective. Computers and other networked resources, like as IoT devices, can be exploited machines.

What Distinguishes DoS Attacks from DDoS Attacks?

DoS attacks are system-on-system attacks, whereas DDoS attacks include multiple systems attacking a single system. This is the main distinction between the two types of attacks. However, there are further variations in either their discovery or nature, such as:

a. DoS originate from a single site, making it simpler to identify its source and cut the connection. Ease of detection/mitigation in truth, a capable firewall is capable of doing this. A DDoS attack, on the other hand, conceals its source by coming from numerous distant sites.

b. Attack speed: A DDoS attack can be launched significantly more quickly than a DoS attack that emanates from a single place because it originates from numerous locations.

c.Traffic volume: A DDoS assault uses several remote machines (zombies or bots), which enables it to send significantly bigger volumes of traffic from different locations at once, quickly and covertly overloading a server.

d.Execution method: A DDoS attack orchestrates numerous hosts that have been infected with malware (bots), forming a botnet that is controlled by a command-and-control (C&C) server. A DoS attack, on the other hand, usually employs a script or tool to execute the attack from a single machine.

e. Tracking the source(s): Tracing the real origin of a DDoS assault is far more difficult than tracing the origin of a DoS attack due to the involvement of a botnet.

Types of DDoS attacks: -

a. UDP Flood: -It involves flooding ports with IP packets containing UDP datagrams. As more and more UDP packets are received and responded, the system becomes overloaded and unresponsive.

b. ICMP (Ping) Flood: - ICMP stands for internet control message protocol. In this the attacker overwhelms the victim's computer with pings, causing it to crash (ICMP echo requests). As a result, regular traffic won't be able to access the target.

c. SYN Flood: - It is a DDoS assault that seeks to exhaust all of the server's resources in order to make it unavailable to users. The targeted device either ceases to react to valid traffic altogether or replies slowly.

d. Ping of Death: - An attack where the attacker uses the ping command to deliver oversized or malformed packets in an attempt to overload, crash, destabilise, or freeze a target device or service.

e. HTTP Flood: - It is a methodical attempt to flood a server with HTTP requests.

Preventions: -

i. Make a DDoS response strategy.

ii. Make sure that the network is very secure.

iii. Have redundant servers, be aware of warning signs and constantly watch network traffic.

iv. Utilize the Cloud to Protect against DDoS Attacks and avoid ignoring the DDoS threat.

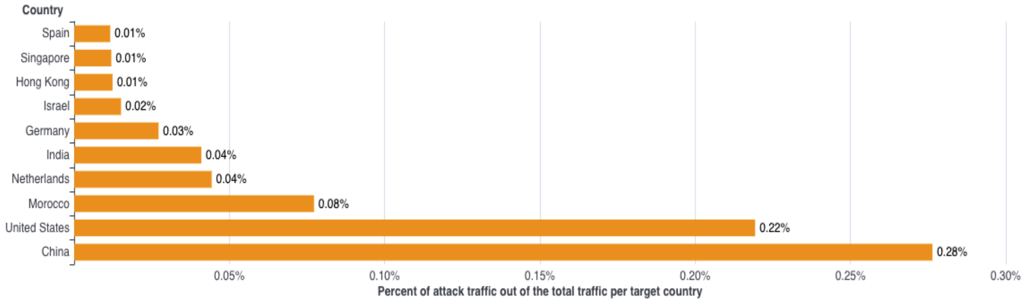


Fig 5: - DDoS attack by target countries. [13]

4.3 Vishing attack: - Voice phishing, sometimes known as "vishing," is the practise of scamming people over the phone by luring them into disclosing personal information. The attacker tries to obtain the victim's data and utilise it for personal gain, usually financial gain.

Difference between vishing and fishing attack are as follows: -

Vishing is done via voice call over the phone. Voice over Internet Protocol (VoIP) systems, cellphone networks, and landlines can all be used for this. On the other hand, email is used to carry out phishing.

Preventions: -

i.Don't answer the phone: - Let a suspicious number go to voicemail if you notice it. You can check your mails to see how important it is.

ii. Register with the National Do Not Call Registry: - The quantity of telemarketing and vishing calls you receive might be decreased by using the National Do Not Call Registry. Companies risk fines if they phone the numbers on the list.

iii. Avoid pressing buttons or answering prompts: - Automated phishing calls rely on the victim's input. The attack can be stopped if you refuse to push any buttons or provide any information.

iv. Look up the Caller's Information: - You can look up the caller's name, business, physical address, and other relevant information online.

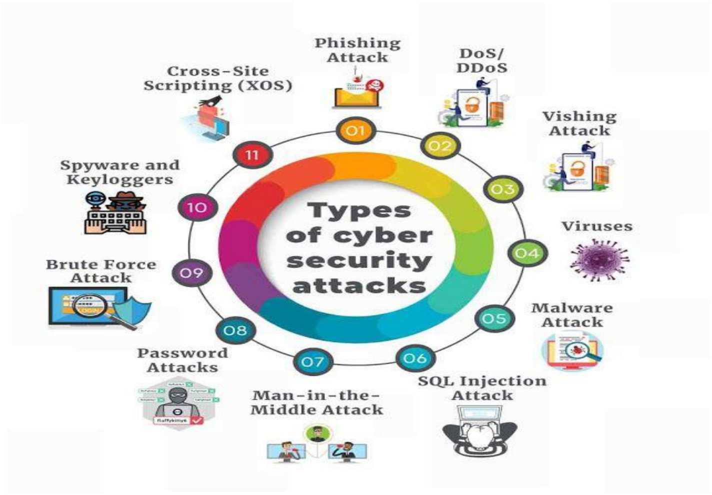


Fig 6: - Different types of cyber security attacks [14]

4.4 Viruses: - A computer virus is a form of malware, or malicious software that travels between computers and corrupts software and data. Viruses are designed to interfere with systems, lead to serious functional problems, and cause data loss and leakage. When a file is opened, viruses often attach to an executable host file, causing their viral programming to run. The associated software or document subsequently spreads the code via networks, discs, file-sharing applications, or corrupted email attachments.

Types of viruses: -

a. Resident Viruses: - It spread them by contaminating host computer software. By infecting apps as they are opened by a user, a resident virus does this. When no programmes are operating, executable files can be infected by a non-resident virus.

b. Multipartite Virus: - A multipartite virus infects and spreads across computers using a variety of strategies. Usually, it stays in the computer's memory until it infects the hard drive, then spreads by changing the application contents to infect further discs. Performance lag and low application memory are the results of this. By not opening attachments from unknown sources and by using reputable antivirus software, multipartite viruses can be prevented. Cleaning the computer's full drive and the boot section can also stop it.

c. Direct Action: - A direct action virus gains access to the main memory of a computer and spreads infection to all applications, files, and directories in the autoexec.bat path before erasing itself. Although this virus usually degrades a system's performance, it is also capable of wiping out all the data on a computer's hard drive and any USB devices that are connected to it. By using antivirus scanners, direct action viruses can be prevented. They are simple to spot, and recovering corrupted files is as simple.

d. Website hijacker: - An application called a "browser hijacker" alters the default settings of online browsers, such as the homepage, new tab page, and default search engine. It cannot infect files, therefore technically it is not a virus, but it can inflict a great deal of harm to computer users.

e. Network virus: - This type of viruses has the ability to entirely disable entire computer networks. They are exceedingly harmful. Since the virus could be concealed within any machine on an infected network, they are frequently challenging to find. By transferring to devices linked to the network via the internet, these viruses can readily proliferate and propagate. The best defence against network infections is the usage of dependable, powerful antivirus programmes and cutting-edge firewalls.

f. Boot Sector Virus: - A computer's master boot record is the target of a boot sector virus (MBR). When a computer resumes, the virus injects its code into the partition table of the hard drive before moving into main memory. Poor system performance, boot-up issues, and the inability to locate the hard disc are signs of the existence of the virus. The majority of contemporary computers are equipped with boot sector protections that limit the possibility of this kind of malware.

4.5 Malware attack: - Ransomware, spyware, viruses, and worms are a few examples of the malicious software that is referred to as malware. A unique vulnerability, typically when a person clicks on a malicious link or email attachment that installs destructive software, is the most frequent route for malware to infiltrate a network. Ransomware is the most prevalent type of malware. A malware known as Ransomware encrypts the victim's files and demands payment in exchange for the decryption key. Spyware, on the other hand, is software that self-installs on your device and covertly tracks your internet activity without your knowledge or consent.

Prevention: - Installing antivirus software is one technique to defend against malware. Your machine will be scanned by antivirus software to find and remove the infection. Additionally, it will give automatic upgrades to enable improved defence against recently developed viruses.

4.6 SQL Injection attack: - SQL injection attack is a technique of introducing random SQL into a database query for a web application. Through backend database modification, the malicious SQL code allows access to confidential information that wasn't intended to be seen**.**

Types of SQL Injection techniques: -

i. In-band SQLi: - The most frequent SQL Injection attack is this one. When a cybercriminal launches the assault and collects the data, this is known as in-band SQL injection.

ii. Inferential SQLi: - This kind of attack involves sending payloads, watching the web application's reaction, and analysing the database server's behaviour to reconstruct the database structure.

iii. Out-of-band SQLi: - Only when specific functionalities on the web application's database server are enabled then the attacker use this type of attack.

Preventions: - Input validation, parameterized queries, stored procedures, and escaping are effective prevention methods for SQL injection attacks.

4.7 Man in the middle attack (MitM): - Man-in-the-middle assaults occur when a perpetrator eavesdrops on a conversation between two individuals. The attacker wants to spy on the victims and take their credentials or personal information. For instance, when a victim connects to an unprotected public Wi-Fi network, an attacker can place oneself in between the victim's device and the network. After gaining access to a device, a hacker can install software to process the victim's data.

Prevention: - To encrypt your web traffic, use a Virtual Private Network (VPN). An encrypted VPN can make it very challenging for an intruder to read or alter web traffic.

4.8 Password attack: - One of the most frequent ways that personal and corporate data is compromised is through password attacks. An attempt to steal your password by a hacker is known as a password attack. In 2020, compromised credentials accounted for 81% of data breaches. Passwords are becoming less secure since they can only have so many letters and numbers. Hackers will continue to utilise password attacks as long as passwords are in use since they are aware that many passwords are improperly constructed.

Preventions: -

i. Using a two-step authentication process: - Users can be authenticated via a personal device (like a mobile phone) or a physical token, ensuring that passwords are not the only access point.

ii. Remote access: - Individual websites are no longer the foundation of user confidence when a clever remote access platform is used. Instead, it verifies the user's identity before allowing them to log in.

iii. Biometrics: - It will be exceedingly challenging to duplicate your fingerprint or facial features. By enabling biometric authentication, you reduce the number of points of trust that a hacker must breach from many to just one.

4.9 Brute force attack: - A brute force attack is like using a battering ram if a password is like using a key to access a door. When a hacker tries 2.18 trillion password/username combinations in 22 seconds, your account could be targeted if your password is weak.

Preventions: -

i. Make your password complex: - A mixed case, mixed character, 10-digit password is very different from an all lowercase, all alphabetic, six-digit password. A successful brute force assault is less likely as your password complexity rises.

ii. Set up and enable remote access: - If your business employs remote access management, inquire with the IT department. The risk of a brute-force attack will be reduced.

iii. Make multi-factor authentication: - A potential hacker can only request access to your account by sending a request to your second factor if multi-factor authentication (MFA) is configured on your account. Hackers are likely to be locked out of your account because they won't have access to your mobile device or thumbprint.

4.10 Keylogger: - Malicious software called keyloggers records each keystroke and sends the information to a hacker. Typically, a user will download the programme thinking it is safe, only for it to secretly install a keylogger.

Preventions: -

i. Verify your physical equipment: - A hardware keylogger can be installed on your workstation by someone who has access to it in order to record your keystrokes. Make sure you are familiar with all of the hardware by performing routine inspections of your computer and the environment around it.

ii. Do a virus check. Regularly scan your PC using a reliable antivirus programme. The most popular malware keyloggers are tracked by antivirus providers, who mark them as potentially harmful.

4.11 Cross-site scripting attack (XOS): - Attacks using cross-site scripting (XSS) are comparable to attacks using SQL injection. However, they are often used to infect users that visit the site rather than the application itself. Depending on the intensity of the attack, Trojan horse programmes may be activated and user accounts may be compromised. The attacker could be able to impersonate legitimate users and utilise their private accounts if session cookies are exposed.

Prevention: Regular code scanning of your website or online application offers the strongest defence against cross-site scripting. Contrary to popular belief, web application firewalls do not actually provide protection against cross-site scripting; rather, they merely make the attack more challenging.

V. Conclusion

India, a nation of 1.3 billion, has the lowest data rates worldwide. The advancement of the network has increased the importance of data and information security. E-commerce is booming, and a large number of e-governance-related tasks are now being completed online. We become more susceptible to any disruptions brought about in and through cyberspace as we become more reliant on the Internet for our daily activities. Despite having big ambitions to increase cyber connectedness.

The existing laws are ineffective in stopping cybercrimes, necessitating their modification in order to put a stop to these actions. International cooperation is required if states are to effectively combat cybercrime. This study makes it quite evident that as cyberspace and technology advance, so will the range of cyber threats. To protect data, one must take precautions such as installing antivirus software, employing firewalls, creating strong passwords, and practising hacker avoidance. To preserve rights and privacy and uphold the rule of law, it is necessary to raise awareness, implement firm reforms, amend criminal law, and implement cyber security policies.

References

[1] "National Cyber Security Policy-2013". Department Of Electronics & Information Technology, Government of India. 1 July 2013.

[2] "Amid spying saga, India unveils cyber security policy". Times of India.

[3] "National Cyber Security Policy 2013: An Assessment". Institute for defence Studies and Analyses.

[4] Dr. Prakash Kumar, International Journal of Creative Research Thoughts, Volume 6, Issue 2 June 2018 | ISSN: 2320-2882, pp. 302-306.

[5] "For a unified cyber and telecom security policy". The Economic Times.

[6] A Survey on Load Balancing In Cloud Computing Mr. Purushottam Kumar, Dr. Prakash Kumar

[7] “Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cyber security". Stanford Journal of International Law, Vol. 50, p. 119, winter 2014 Indiana Legal Studies Research Paper No. 290. 15 July 2014.

[8] "Analysis of National Cyber Security Policy of India 2013 (NCSP-2013) And Indian Cyber Security Infrastructure". Centre of Excellence for Cyber Security Research and Development in India (CECSRDI). 21 November 2014.

[9] A Review on various Security Issues and Challenges in VANET”,” IJCRT, Vol. 6 | Issue 1, Feb 2018, ISSN 2320-2882, pp. 396-40.

[10] Dr. Prakash Kumar, International Journal of Computer Science and Mobile Computing, Vol.6 Issue.12, December- 2017 | ISSN 2320–088X, pp. 157-163.

[11] Dr. Prakash Kumar, International Journal of Creative Research Thoughts, Volume 6, Issue 2 April 2018 | ISSN: 2320-2882, pp. 428-434.

[12]Hindustan Times, New Delhi

[13] Research gate

[14] mobile.twitter.com

[15]https://www.exai.com/blog/types-of-cyber-attacks

[16]https://www.cyberralegalservices.com/detail-casestudies.php

[17]http://www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html

[18]https://alpinesecurity.com/blog

[19]https://blog.cloudflare.com/ddos-attack-trends-for-2021-q1