# Study of Cyber Security

**[1]Prof. Sunita Totade, [2]Vaishnavi S. Kadu, [3]Vishakha S. Payghan, [4]Dhanashree P. Dhote**

[1]HOD, Department of MCA, Vidyabharati Mahavidyalaya, Amravati, India

[2,3,4]Student, Department of MCA, Vidyabharati Mahavidyalaya, Amravati, India

Authors E-mail: [2]vaishnavikadu200@gmail.com, [3]vishakhapay@gmail.com, [4]dhotedhanshri123@gmail.com

***Abstract* - In the modern context, 'cyber attacks' or 'cyber hazards' otherwise referred as 'cyber crimes', is a highly referred term because of its complex and evolving nature in a sphere unseen to the human eye; 'cyber sphere'. The perpetrators and the victims of cybercrimes are reported from all over the world with no particular location, meaning any individual of any part of a region can be subjected to a cyber threat or actively participate in the particular area. As individuals who are living in a highly digitalized society, it is a vital need to be aware of the potential threats that comes with the use of information technology and how to be protected from these threats. Cyber security aims in protecting individuals from this border-less crimes and to ensure their safety while protecting their personal data, when surfing internet/ World Wide Web. The research has been conducted in the context of Socio-legal, analytical and qualitative research formats in order to provide an understanding on the current position of cyber security. Safeguarding the information has become an enormous problem in the current day. The cyber security the main thing that originates in mind is 'cyber crimes' which are aggregate colossally daily. Different governments and organizations are taking numerous measures to keep these cyber wrongdoings. Other than different measures cyber security is as yet a of cyber security discuss in it. The cyber-terrorism could make associations lose billions of dollars in the region of organizations.**

***Keywords:*** Cyber security; cyberspace; cyber terrorism; Information security.

## I. INTRODUCTION

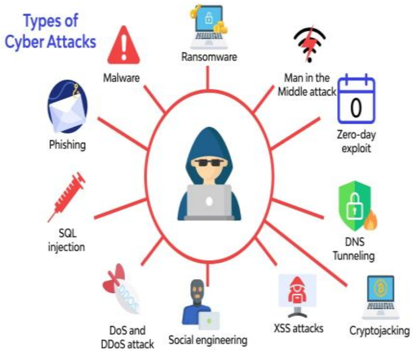
Today Internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cybercrimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc. Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic wellbeing.

### What is Cyber Attacks??

Cyber-attacks have several negative effects. When an attack is carried out, it can lead to data breaches, resulting in data loss or data manipulation. Organizations incur financial losses, customer trust gets hampered, and there is reputational damage.

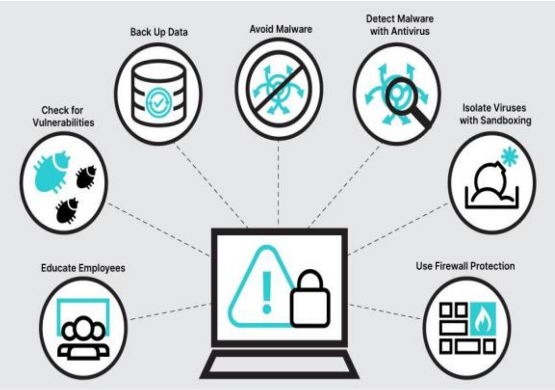
## II. TYPES OF CYBER ATTACKS

There are many varieties of cyber attacks that happen in the world today. If we know the various types of cyber attacks, it becomes easier for us to protect our networks and systems against them.



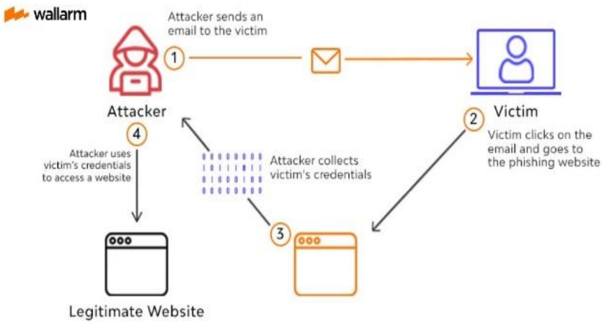
### *1. Malware Attack*

This is one of the most common types of cyberattacks. "Malware" refers to malicious software viruses including worms, spyware, ransomware, adware, and trojans. The trojan virus disguises itself as legitimate software. Ransomware blocks access to the network's key components, whereas Spyware is software that steals all your confidential data without your knowledge. Adware is software that displays advertising content such as banners on a user's screen. Malware breaches a network through vulnerability. When the user clicks a dangerous link, it downloads an email attachment or when an infected pen drive is used.


Back Up Data
Avoid Malware
Detect Malware with Antivirus
Check for Vulnerabilities
Isolate Viruses with Sandboxing
Educate Employees
Use Firewall Protection

### 2. Phishing Attack

Phishing attacks are one of the most prominent widespread types of cyberattacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact and sends the victim fake mails. Unaware of this, the victim opens the mail and clicks on the malicious link or opens the mail's attachment. By doing so, attackers gain access to confidential information and account credentials. They can also install malware through a phishing attack.


wallarm
Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
Legitimate Website

### 3. Password Attack

It is a form of attack wherein a hacker cracks your password with various programs and password cracking tools like Aircrack, Cain, Abel, John the Ripper, Hashcat, etc. There are different types of password attacks like brute force attacks, dictionary attacks, and keylogger attacks.

### 4. Man-in-the-Middle Attack

A Man-in-the-Middle Attack (MITM) is also known as an eavesdropping attack. In this attack, an attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. By doing so, hackers steal and manipulate data. The client-server communication has been cut off, and instead, the communication line goes through the hacker.

**How to prevent cyber attacks??**

1) Change your passwords regularly and use strong alphanumeric passwords which are difficult to crack. Refrain from using too complicated passwords that you would tend to forget. Do not use the same password twice.
2) Update both your operating system and applications regularly. This is a primary prevention method for any cyber attack. This will remove vulnerabilities that hackers tend to exploit. Use trusted and legitimate Anti-virus protection software.
3) Regularly back up your data. According to many security professionals, it is ideal to have three copies of your data on two different media types and another copy in an off-site location (cloud storage). Hence, even in the course of a cyber attack, you can erase your system's data and restore it with a recently performed backup.
4) Safeguard your mobile, as mobiles are also a cyberattack target. Install apps from only legitimate and trusted sources, make sure to keep your device updated.

**Advantages**

1) It will safeguard your company.
2) Please keep your personal information private.
3) Enables users to work in a relaxed environment.
4) It also maintains efficiency.
5) Various jobs are mechanized as a result of this.
6) Organize data and information more effectively.
7) The information and files as recommendations and suggestions are essential for the productivity.

## III. METHODOLOGY

Cyber Security Methodology Reconnaissance refers to gathering information about the target for the ex-Domain name, IP, Target personal information, Email, Sub domains, Job information, etc. Reconnaissance is also known as Foot-Printing.

Hpinh3/2-used for packet crafting for TCP/IP, Netscan pro-it help to truoubleshoot the network, ID serve-for a banner grabbing/OS fingerprinting, Nessus/open VAS/Qualys-for vulnerability scanning. Gaining access that-It refers to the real hacking phase in this phase hacker takes place in the system. The hacker exposed vulnerabilities and information in the first and second phases are now exploited to gain the target computer. Now attacker cracking Password by Dictionary attack-create passwords word list and runs against the user account. Brute force-in this software combines all words it tries every combination. Hash injection attack: it converts normal text into the encrypted form and it is not easy to decrypt the password. Windows Passwords are stored in

ISSN (online): 2581-3048
Volume 6, Issue 10, pp 122-125, October-2022
https://doi.org/10.47001/IRJIET/2022.610022

(SAM) Security Account Manager. In Linux user's passwords are stored in (Shadow) file. In maintaining access phase, hackers inside the target system by exploiting vulnerabilities and password cracking. Now the attacker can easily download and upload anything in the target system and to gain system easily next time attacker installs some software like Trojan horses, Keylogger and Root-kits. Trojan horses are a malicious software user thinks it is legitimate software but it steals all information. Keylogger records the movement of target keyboard keys. Rootkits is software that hides its presence in the target system and its compromised system. Clearing tracks now here is the final phase once a hacker gained into the target system after that hacker covers all their tracks to prevent their presence in the system. Hacker uses Auditpool a tool to remove their presence Auditpool tool stores in the Windows Nt Resource kit for the system by this tool attacker can easily disable their auditing. There are some security measures, and these will give you a basic level security against the most common IT risks, by Use strong passwords, Control access, put up a firewall, use security software, Update programs and systems regularly, Monitor for intrusion. Strong passwords are vital to good online security. Make your password difficult to guess. Make sure that individuals can only access data and services for which they are authorized. Firewalls are effectively gatekeepers between your computer and the internet, and one of the major barriers to prevent the spread of cyber threats such as viruses and malware. You should use security software, such as anti-spyware, anti-malware, and anti-virus programs, to help detect and remove malicious code if it slips into your network. Updates contain vital security upgrades that help protect against known bugs and vulnerabilities. You can use intrusion detectors to monitor system and unusual network activity.

## IV. DATA COLLECTION

In several studies, researchers have identified security concerns and drawn attention to the need to be more thoughtful about securing data collected in developing world contexts. Hussain (2013) gives a broad overview of the potential risks of mobile phone use in global development projects. She describes the sensitive types of data that organizations collect and references the legal code of several countries to argue that it is worth securing. These recommendations are good starting points for organizations employing digital data collection. Our work investigates how organizations already engaged in data collection approach and understand security, as well as the threats they have encountered and considered. Other projects have identified and studied specific security concerns in digital data collection. Mobile devices in digital data collection projects are frequently not owned by the people entering the data. Instead projects will typically provision and distribute phones as part of a deployment. Schwartz et al. (2013) explore how this leads to non-prescribed, personal usage of the devices and how it can impact deployments. Our work reiterates that such usage is a real concern for many deployments. Data collectors can also be a source of inaccurate data. Birnbaum et al. explore methods to detect fabricated survey data using passive analysis (Birnbaum et al., 2013) as well as through measuring surveyor behavior (Birnbaum et al., 2012). Respondents in our study also consider data fabrication a threat, and many collect GPS coordinates or photographs in an effort to manually detect fabricated data.Providing important insight to the context that informs how some data collectors think about data security, many groups performing digital data collection have experience with paper data collection. Parikh (2005) notes that paper can provide a sense of familiarity and security beyond that provided by a borrowed mobile phone. Ghoshetal. (2015) echo these findings, noting that paper passbooks can be kept in a specific location and thus secured. Our work adds depth to comparisons of paper and digital data collection by discussing how intuitions around paper.

## V. RESULT

Throughout the research it was found that the government should recommend more cybersecurity policies and standards, and laws and regulations while facilitating the implementation of such policies in all government institutions and other relevant sectors which posses' confidential information. It is high time to raise awareness among the people, especially the youth who are always prone to cyber threats, by conducting awareness programs, and starting from the school education, where the children will be taught about the cyberspace and how to face the computer related threats, in an advanced manner. Most importantly, this type of education should not be limited only to urban areas of the country. Even the youth in suburbs should be given the opportunity to embrace the technology and to learn how to overcome the threats directed from cyber sphere. Since the young people use internet more than that of adults, and as majority of the youth have access to internet, the government should take measures to create virtual assistants or various safe portals, with the help of the experts in the field. Moreover, in the present context, youth are more biased towards online shopping and online banking. Because of this their personal data which includes the passwords, names, etc, are always threatened. The number of frauds that relate with businesses and online transactions have risen up, which in result have made them to face unbearable situations such as loss of money and confidential data. They should be also taught how to secure their devices from various types of computer viruses such as boot sector viruses, web scripting viruses, browser hijacker, polymorphic viruses and many more, by installing legal software applications that are available in the app stores. Although, a considerable amount of youth is aware on this, there is still a group of individual who are not aware on this situation. Thus, the aforementioned steps should be brought forward in no time.

## VI. CONCLUSION

In the event of a cyber security incident, such as an attack, studies show that the greatest defense is a PC-savvy customer [4]. To consider is by far the most vulnerable, who are identified in this investigation as new employees inside an organization, as specifically, with the adversary seeking for personally identifiable information from people involved. Mental issues that contribute to customer and organization vulnerability are also addressed in this investigation. This study finds that cyber security threats and approaches have a role to play in reducing the impact of digital attacks, risk, and vulnerability, while creativity has a role to play in reducing the influence of digital attacks, threat, and lack of strength. Cyber-attacks can be mitigated, but there does not appear to be an absolute solution for overcoming such network security threats at this time. Later, when the company implements the system security design, the operation of the cyber attack, threat, and vulnerability decreases.

## REFERENCES

[1] A Sophos Article 04.12vl.dNA, eight trends changing network security by James Lyne.

[2] Cyber Security: Understanding Cyber Crimes-Sunit Belapura Nina Godbole.

[3] Computer Security Practices in Non Profit Organisation – A NetAction Report by Audrie Krause.

[4] A look back on Cyber Security 2012 by Luis corrons – Panda Labs.

[5] International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 page nos.68 – 71 ISSN 2229-5518, “Study of Cloud Computing in HealthCare Industry “by G.nikhita Reddy, G.J.Ugander Reddy.

[6] IEEE security and Pravicy Magazine – IEEECS “Safety Critical System – Next Generation “July/Aug 2013.

[7] CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.

[8] K. Thakur, M. Qiu, K. Gai and M. L. Ali, "An Investigation on Cyber Security Threats and Security Models," 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, 2015, pp. 307-311, doi: 10.1109/CSCloud.2015.71.

[9] J. Akram and L. Ping, "How to build a vulnerability benchmark to overcome cyber security attacks," in IET Information Security, vol. 14, no. 1, pp. 60-71, 1 2020, doi: 10.1049/iet-ifs.2018.5647.

[10] Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31. doi:10.1016/S2212-5671(15)01077.

[11] Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. (2018). Cybersecurity: trends, issues, and challenges. EURASIP Journal on Information Security. doi:10.1186/s13635-018-0080-0.

[12] https://www.csis.org/news/cybersecurity-agenda-45th-president13

[13] http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

[14] https://www.cyberbit.com

**Citation of this Article:**

Prof. Sunita Totade, Vaishnavi S. Kadu, Vishakha S. Payghan, Dhanashree P. Dhote, “Study of Cyber Security” Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 6, Issue 10, pp 122-125, October 2022. Article DOI https://doi.org/10.47001/IRJIET/2022.610022

*******