**A Review Paper on Recent cyberattacks and proactive steps to prevent attacks**

**Abubakar Osman*1***\*, **Zeeshan Malik *2***

1computer Science, Jain Institute of Technology, India

2computer Science, Jain Institute of Technology, India

**Abstract**

  One of the main challenges in the modern world is cyber security. With today's technology, we can communicate any sort of data, whether it be an audio file, a PDF document, or a video, with just a single click. Therefore, protecting information is crucial in the sphere of cyber security. As the globe becomes more and more connected to networks that may be used for conducting digital transactions, cyber security is still a very serious problem since cybercrimes are always destroying data with fresh ideas. Consequently, cyber security is crucial everywhere in the world. Since electronic technology is so prevalent nowadays, safeguarding sensitive data from cyberattacks is a difficult problem. This review paper primarily focuses on current cyberattacks, as well as the most recent cybersecurity tactics, morals, and trends that are reshaping the field.

**Keywords:** Cyber security, cyberattacks, security techniques, digital transactions, global networking.

# INTRODUCTION

The majority of economic, commercial, cultural, social, and political activity currently taking place between nations at all levels, including between people, non-governmental organisations, and governments and governmental institutions, takes place online. Cyber assaults are an issue that many commercial businesses and governmental institutions throughout the world are currently dealing with. The most recent technology, such as net banking, mobile computing, data analysis, and e-commerce, holds crucial data, and security is crucial because the information must be kept private. The fight against cyberattacks also requires a comprehensive strategy that is safer.

Today, the government is enforcing cyber laws, or laws pertaining to cyber security. To protect themselves from cyberattacks, every person needs to be informed about it.

# Cybersecurity statistics

1. One billion emails were exposed due to the vulnerability in just one year, potentially affecting 1 in 5 internet users.
2. In 2022, businesses suffered average losses of $4.35 million as a result of data breaches.
3. The total number of ransomware attacks worldwide during the first half of 2022 was close to 236.1 million.
4. In 2021, accounts of around 50% of interest users in America were compromised.
5. About 1 in 10 US firms did not have cyberattack insurance as of 2022, making them susceptible to intrusions.

**Why are attacks done?**

Although the motivations for cyberattacks might vary, they typically fall into one of three groups: criminal, political, or personal.

Criminally motivated attackers are primarily for monetary gains, which can be obtained in a number of ways, including by stealing money directly from bank accounts, using social engineering to fool others into transferring money, or using data theft to steal identities or sell them on the dark web. Additionally, they may use ransomware, DDoS attacks, or other strategies to hold priceless data or systems hostage until a ransom is paid; according to the X-Force Threat Intelligence Index, about 27% of cyberattacks have an extortion objective.

Attackers who are personally motivated seek retaliation for perceived wrongs; these attackers may be dissatisfied current or former employees. They might steal money, delicate information, or interfere with a business's operations as payback.

Attackers with political motivations are frequently linked to cyberterrorism, cyberwarfare, or "hacktivism." Nation-state actors target key infrastructure or the offices of competing governments in cyberwarfare. For instance, both nations saw a spike in cyberattacks on important institutions during the Russia-Ukraine War. On the other side, hackers who are activist or hacktivists pursue causes or ideas and frequently attract notoriety by making their attacks public rather than seriously harming their targets.

Less frequent reasons for cyberattacks include business espionage, in which hackers steal intellectual property to have an unfair advantage over rivals, and vigilante hacking, in which hackers take advantage of system defects to draw attention to security holes. Additionally, some hackers take part in cyberattacks for the intellectual challenge and pure thrill they provide.

# Cyberattacks

Below are a few recent cyberattacks that had a negative impact on most aspects.

## **Pegasus spyware:**

A spyware called Pegasus was created by the Israeli cyber-intelligence company NSO Group and is easily installed on mobile devices by simply clicking links. The current version also allows for zero-click exploits and network-based attacks. It doesn't leave any obvious traces after being installed on a phone. It can function on the majority of mobile devices running the iOS, Android, BlackBerry, Windows Phone, and Symbian operating systems. Journalists, human rights activists, dissidents, and political figures were the main targets of its use. The spyware can track a user's location, intercept text messages, record phone calls, and gather passwords, pictures, and other information. According to NSO Group, its products are only distributed to government security and law enforcement organisations, and they are only used to support rescue efforts and combat criminals like money launderers, sex and drug traffickers, and terrorists.

Pegasus was discovered in August 2016 after an unsuccessful installation attempt on the iPhone of Arab human rights advocate Ahmmed Mansoor.

According to The New York Times, installing Pegasus on ten phones alone cost about $1.15 million in 2016.

**Technical:**

The spyware can be installed on specific Android devices as well as iOS devices running specific versions of Apple's mobile operating system. Pegasus is not characterised by a single exploit; rather, it includes a wide variety of exploits that take advantage of various system flaws. The Photos app, the Apple Music app, clicking on links, and using iMessage are all examples of potential infection vectors. Pegasus makes use of zero-click exploits, which can run without the target person's involvement. Pegasus can run arbitrary code and extract contacts, call logs, messages, photos, web browsing history, and settings after being installed. It can also gather data from a variety of apps, including iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram, and Skype.

**Attack on the Tallahassee Memorial Healthcare**

Late in January 2023, **TALLAHASSEE MEMORIAL HEALTHCARE** came under cyberattack. It is a non-profit healthcare system that provides care to people in South Georgia and North Florida. The attack forced it to operate under emergency downtime procedures for about two weeks. The hospital lacked sufficient security knowledge, but experts say it was '**RANSOMWARE**'.

The data breach was reported to the **HHS** Office for Civil Rights and affected 20,376 people. The attack's victims first learned about it on March 31, 2023. Names, addresses, dates of birth, Social Security numbers, health insurance numbers, medical record numbers, patient account numbers, and/or limited treatment information are among the data that were compromised. There was no access to the electronic medical record system. The attack is in line with **TMH**. TMH has started sending emails to the approximately 20,000 patients whose data was compromised.

## **T-mobile Attack**

The second data breach of 2023 occurred toward the end of February and led to the hacking of hundreds of customers' personal information. Even though "assailants did not obtain access to personal financial account information and call records of affected individuals," according to T-Mobile, the data that has been obtained is more than enough for the hackers to obtain other important information. The information that was compromised included full names, phone numbers, birth dates, government identification numbers, T-mobile pin codes, and other details.

After learning about the attack, T-Mobile reset the account pins for the impacted customers and gave them two years of free Trans union my True Identity credit monitoring and identity theft detection services.

## **California University Cyber Attack**

The School of Medicine at the University of California, San Francisco, recently experienced a serious ransomware attack. The institution paid the criminal organisation known as Netwalker a significant ransom of $1.14 million in an effort to regain access to important research. BBC News was keeping a close eye on this ransomware bargain after receiving a tip from an unnamed person who was probably connected to the university.

## **Facebook data breach 2019**

In 2019, Facebook experienced a significant security breach that exposed the personal information of over **533 million** users from **106 countries**, including Full Names, Birthdates, Locations, Email Addresses, Bios, and many other details. Hackers stole this information from Facebook for years, and in 2019 it was made freely accessible to the public. Data was sold to criminal organisations after it had been stolen by hackers, who used it for their own purposes and then sold it to them so they could use it. After August 2019, the public was given access to the stolen data. Before it was taken down, the information remained online in a hacker forum for 10 days.

In January 2019, when a user in the same hacking forum advertised an automated bot that could provide phone numbers for hundreds of millions of Facebook users in exchange for a fee, **Alon Gul**, CTO of cyber intelligence firm Hudson Rock, first discovered this data leak. The personal information of Facebook's co-founders Chris Hughas and Dustin Moskovitz, as well as its CEO Mark Zuckerburg, was made public. **Business Insider** received an email from a Facebook representative stating, "This was old data that was previously reported on in 2019. This problem was discovered and resolved in August 2019. At that time, the business fixed a technology flaw that caused the information to leak out. Facebook was afraid that disclosing this data breach would jeopardise its business model of collecting a lot of personal data and using it to market to specific audiences.

Use the "haveibeenpwned" website to find out if your info was compromised or not if you're wondering

# Proactive paths to strengthen cybersecurity

Here, we'll outline several key strategies for reducing the risk of cyber incidents.

## **Instal antivirus software**

Security is improved by antivirus software in the following ways:

* Real-time Threat Detection.
* Malware Removal.
* Regular Updates.
* Web Protection.
* Email Protection.
* Firewall Integration.
* Behaviour Analysis.
* Safe Browsing.
* Vulnerability Scanning.

Along with other tools for preventing cybersecurity attacks, antivirus software is a crucial tool.

## **Strong Password**

Another proactive technique of combating cyberattacks is to maintain a secure password. The password must be a combination of capital and lowercase letters, digits, and special symbols or characters like @, #, \*, &, etc. It must also be at least eight characters long.

## **Enforcing security policies**

Enforcing security policies helps to minimise the possibility of network assaults, helps to protect all networked devices from malware and viruses, and also restricts access to network areas and user rights.

## **Find end points and possible attack vectors**

A sensible strategy is to use many levels of security, which will lessen cyberattacks. Locate the weak places and stop them.

For instance, employing anti-phishing tools to reduce the risk of an email-based attack could be the first layer of defence. This allows us to use various security layers to thwart an attack; the more layers we use, the lower the risk of a cyberattack.

## **Safe links and attachments**

The alternative method of practice involves using safe links and attachments. In this method, a person or defender opens incoming links or attachments in a sandbox to make sure that threats are identified and eliminated. The defender can quickly and cheaply implement these tools by either purchasing new licences or upgrading their current licences.

**Literature survey**

1.In the article, Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies Researchers Nikhitha Reddy Gade and Ugander G J Reddy discussed that, it is impossible to exaggerate the importance of cyber security in the world of information technology. In the modern day, protecting information has become a hard challenge. The first thing that comes to mind when we think of cyber security is the rise in "cybercrimes," which have been constantly increasing. Worldwide, businesses and governments are actively putting various measures in place to counter these cyberthreats. Despite these initiatives, many people still have serious concerns about cyber security. This presentation focuses on the difficulties that the newest technologies present for cyber security. Additionally, it illuminates the cutting-edge methods, moral questions, and developing trends that are altering the field of cyber security.

2. In the article, Cyber Threat Intelligence Mining For Proactive Cyber Security Defence: A Survey and New Perspectives  Researchers  Nan Sun, Ming Ding, Jiaojiao Jiang, Weikang Xu, Xiaoxing Mo, Yonghang Tai, Jun Zhang discussed that , The article presents a clear taxonomy that divides CTI mining studies into groups according to their intended uses, including cybersecurity-related entities and events, cyberattack tactics, hacker profiles, indicators of compromise, vulnerability exploits, malware implementation, and threat hunting.

3.In the article, A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments researchers Yuchong Li and Qinghui Liu discussed that, the vast majority of economic, commercial, cultural, social, and governmental activities in the modern world—involving people, non-governmental groups, and governmental institutions—take place online. But this greater reliance on electronic technology has made private businesses and governmental institutions all over the world more vulnerable to the growing issue of cyberattacks and the dangers of wireless communication technologies. The challenge of defending important data from such attacks has grown.

Cyberattacks can serve a variety of aims, including economic harm to businesses and, occasionally, military or political ones.

4.In the article, A comprehensive review of cyber security vulnerabilities, Threats, Attacks, and Solutions researchers Omer Aslan, Semith Serkant Aktug , Merve Ozkan Okay,Abdullah Asim Yilmaz discussed that, The COVID-19 pandemic has increased the number of daily transactions that people and businesses carry out online as internet usage rises. The expansion of the digital world has, however, also caused a shift in traditional crimes to the online world. The advent of technologies like cloud computing, the Internet of Things (IoT), social media, wireless communication, and cryptocurrency has raised questions regarding cybersecurity. Cybercriminals have responded by automating and enhancing their cyberattacks as a service. These attacks, which can take many different forms including DDoS, phishing, man-in-the-middle, password, remote, privilege escalation, and malware, all exploit flaws in communication, hardware, and software layers.

# Conclusion

Technology progress is dangerously threatened by cyberattacks. Although there is currently no 100% assurance of protection, there are procedures and other measures to minimise significant losses, and it is inevitable that as technology develops, cyberattacks will rise as well. Finally, "PREVENTION IS BETTER THAN CURE" might be used to draw a conclusion.

**Acknowledgement**

I want to recognize and extend my sincere gratitude to Dr. Mohamed Rafi, who made this effort possible. His direction and counsel helped me through every stage of writing my paper. Not least among all of these sources of motivation for me are my parent’s. Therefore, I would like to thank them and send my compliments.

# References:

1.<https://www.ibm.com/topics/cyber-attack#:~:text=ibm.com).-,Why%20do%20cyberattacks%20happen%3F,data%20theft%2C%20or%20business%20disruption.>

2.[**https://www.britannica.com/topic/Pegasus-spyware**](https://www.britannica.com/topic/Pegasus-spyware)

3.[**https://en.wikipedia.org/wiki/Pegasus\_(spyware)**](https://en.wikipedia.org/wiki/Pegasus_(spyware))

4.<https://www.tmh.org/news/2023/notice-to-patients-regarding-it-security-event>

5.<https://www.tmh.org/news/2023/notice-to-patients-regarding-it-security-event>

6.[https://www.bleepingcomputer.com/news/security/t-mobile-discloses-second-data-         breach-since-the-start-of-2023/](https://www.bleepingcomputer.com/news/security/t-mobile-discloses-second-data-breach-since-the-start-of-2023/)

7.<https://www.hutsix.io/university-of-california-ransomware-attack/#:~:text=University%20of%20California%20Ransomware%20Attack,of%20Medicine%20earlier%20this%20month.>

8.<https://www.businessinsider.in/tech/news/533-million-facebook-users-phone-numbers-and-personal-data-have-been-leaked-online/articleshow/81889315.cms>

9.<https://www.eccouncil.org/cybersecurity-exchange/network-security/how-to-prevent-network-security-attacks/>

10..<https://www.cloudservus.com/blog/how-to-shift-from-a-reactive-to-a-proactive-cyber-security-approach>

11.<https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies>

12. <https://ieeexplore.ieee.org/document/10117505/>

13. <https://www.sciencedirect.com/science/article/pii/S2352484721007289>

14.<https://www.researchgate.net/publication/369186216_A_Comprehensive_Review_of_Cyber_Security_Vulnerabilities_Threats_Attacks_and_Solutions>