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

# A COMPREHENSIVE REVIEW STUDY OF CYBER SECURITY

**[1] Jaswant Narendra Saxena, [2] Ananya Nagraj, [3] Dr. Kommerla Siva Kumar**
[1] Post Graduate Student
Yale University
Advanced Management- Management Information System
[2] Post Graduate Student
Stevens Institute of Technology
Master of Science (MS) in Management Information Systems
[3] Dr. Kommerla Siva Kumar
Associate Professor, Department of CSE
R.V.R & J.C College of Engineering
Guntur, Andhra Pradesh, India.

***Abstract:*** Data and information can now move more easily between networks thanks to the Internet, a global network of loosely connected networks. The movement of data and information between networks at different places has made security issues a key concern in recent years. A small number of people have also exploited the internet for illegal purposes, such as frauds and illegal access to other people's networks. Cybercrimes are the illegal actions connected to the internet. We hear the term "online banking" and "online shopping" a lot in the news these days due to the growing popularity of these activities. Thus, "Cyber Law" was developed in order to apprehend and punish the cybercriminals. Cyber law, sometimes known as the law of the web, is a subset of law that deals with matters pertaining to the Internet, cyberspace, and other related legal concerns such as online privacy and security. In order to give a brief overview of what constitutes cybercrime, the perpetrators—hackers and crackers—the many kinds of cybercrimes, and the development of cyber laws in India, this chapter has been organized into sections with the aforementioned objectives in mind. The chapter goes on to explain how these laws operate as well as the different preventative steps that can be taken to stop this "hi-tech" crime in India.

*Index Terms -*
**Cybercrime, Cyber-Security, Hacking, Trojans, Worms, Botnets, Phishing, Keylogger attacks, Brute-force attacks.**

## I. INTRODUCTION


Cyberattacks happen frequently; as we speak, the security of some large and small organisations is being jeopardised. For instance, all current cyberattacks can be viewed by visiting the "threat cloud" website. It provides us with an idea of the scope of real-world cyberattacks that occur on a regular basis. These days, we use the internet for a variety of daily tasks. But we must continue to be aware of the system and the notifications we get. The ways in which cybercriminals carry out their crimes are evolving daily in tandem with the progress of information technology.
Online Crime: Unauthorized access to computer systems is a felony known as cybercrime or computer crime. It's an illicit activity carried out online.

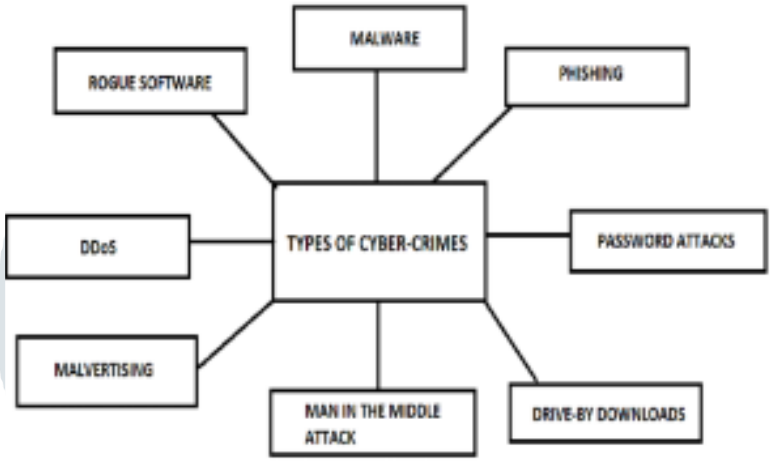
The term "cyber" is colloquial for anything having to do with virtual reality, information technology, and computers. Consequently, it stands to reason those offences pertaining to computers, information technology, the internet, and virtual reality constitute "cybercrime". Cybercrime is any crime where the perpetrator uses a computer and the internet to steal information and data. Some of the examples are: 1. Theft of credit card details. 2. Intrusion onto the official website 3. Fraud using email and the internet. 4. Theft of identity. 5. Theft and sales of company information. 6. ransomware assaults. 7. Cyberextortion: the practice of obtaining money to stop a threatening attack. 8. Cyberespionage, in which hackers obtain data from businesses or the government. 9. Crypto jacking: this is the practice of hackers mining cryptocurrency on resources they do not possess.

## II. LITERATURE SURVEY:

It is impossible to pinpoint the precise moment when a crime was committed over a computer network, or the beginning of cybercrime. The first instance of computer theft occurred in 1973 when a teller at a nearby bank in New York stole more than $2 million using a computer. In 1978, the first email containing spam was sent. Spam emailing is considered a cybercrime. Sending spam emails can land us in jail in some countries. MNC Database (IDM and Pentagon) was breached in the 1980s. In 1982, the first virus was loaded onto an Apple computer.

Ian Murphy, also referred to as Captain Zap, was the first person to be found guilty of cybercrime in 1981. He altered the internal clock of the AT&T network through hacking, charging peak hours for off-peak rates. 2.5 years of probation and 1,000 hours of community service were imposed upon him. Microsoft's NT operating system and the national crackdown on criminals in 1990 were both breached. This is the point at which hacking gained popularity. Hacking was mostly restricted to organizations prior to this. Cybercriminals attacked a number of websites in 2001, including eBay, Yahoo, CNN.com, Amazon, and others. 2007 saw the largest hacking attack ever on a bank. The Swedish bank Nordea reported that 250 accounts had about $1 million stolen from them in just three months. Adobe experienced 2.9 million hacked accounts in 2013, with the usernames and passwords of those users made public on the internet. One of the top antivirus companies in the world, Kaspersky, reported 758 million harmful attacks in 2016.

## III. TYPES OF CYBERCRIME: -




### MALWARE ATTACKS: -

It is an attack in which malware, such as computer viruses, infects a computer system or network. The term encompasses a wide range of cyberattacks, including those caused by trojan viruses. It is described as harmful code that usually steals information or corrupts computer hardware. The well-known WannaCry ransomware assault, a global cybercrime carried out in May 2017, is an illustration of a malware attack. In 150 countries, 230,000 systems were impacted by the WannaCry ransomware outbreak. Users received a message requesting payment of a Bitcoin ransom to unlock their encrypted data. Computer viruses are frequently used by cybercriminals to obtain unauthorized access to systems and steal data. Malicious software, or malware, is installed on a computer without the user's knowledge and is referred to as a computer virus.

**Viruses: -**

As implied by their name, viruses cling to clean files, infect other clean files, and propagate uncontrollably, erasing or corrupting files as well as harming a system's essential operations. Usually, you can find them as an executable file that you downloaded from the internet.

**Trojans: -**

This type of malware poses as trustworthy software or is a component of trustworthy software that is susceptible to manipulation. It often behaves covertly, opening backdoors in our security to allow further malware to infiltrate our system.

**Worms: -**

Through the use of network interfaces, worms can infect vast networks of devices locally or globally. Every infected system after that is used by it to infect more.

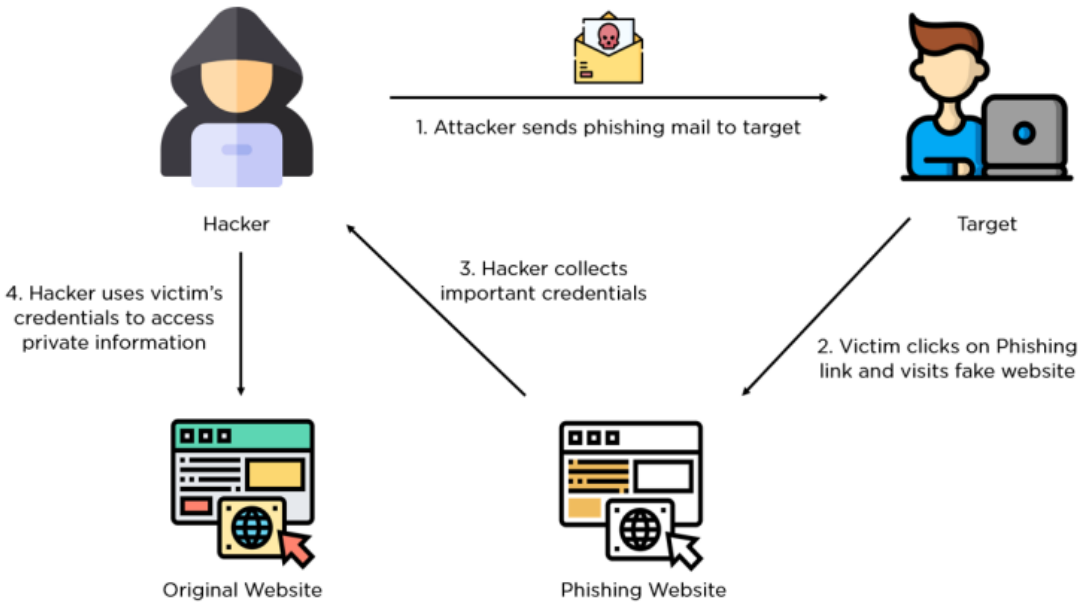
**Botnets: -**

Botnets are collections of compromised computers designed to cooperate under the direction of an attacker. Malware may inadvertently enter our system through open vulnerabilities, genuine software we download from the internet, or infected email attachments.

**PHISHING: -**

It's a cybercrime in which fraudsters pretending to be representatives of reputable organizations contact victims via phone, email, or messaging. Phishing campaigns involve sending spam emails or other types of correspondence with the intention of deceiving the recipients into taking actions that compromise their personal security or the security of the company they work for. These fraudsters first gather passwords and bank account information, then they take money. Phishing emails pretend to be real and ask for victims' personal information.

**Phishing working: -**




The attacker must choose which company to target and figure out how to obtain the clients' email addresses. After determining which company to impersonate and who their targets are, attackers proceed to the setup stage. During this time, they develop strategies for sending messages and gathering data, and finally, they carry out the attack. The attacker then logs the data the victims enter into the webpage or pop-up windows. In the final stage, identity theft and fraud, the attacker use the data they have collected to conduct fraudulent transactions or make unlawful purchases.

**PASSWORD ATTACK: -**


It's an attempt to get the password of a user and use it illegally by decrypting it. Hackers can employ password sniffers, dictionary assaults, and cracking software in their password attacks. The only real defense against password attacks is to have a password policy that mandates frequent changes, minimum length requirements, and unidentifiable wording. There are a number of reasons why this assault could be carried out, but the most nefarious one is to obtain unapproved access to a computer without the owner's knowledge or consent; this leads to criminality such password theft for bank information. There are three standard techniques for getting past a password-protected system.

**Brute-force attack:** In this technique, a hacker attempts to log in using a variety of password combinations, usually starting with the most straightforward one. They accomplish this by using a computer programme or script.

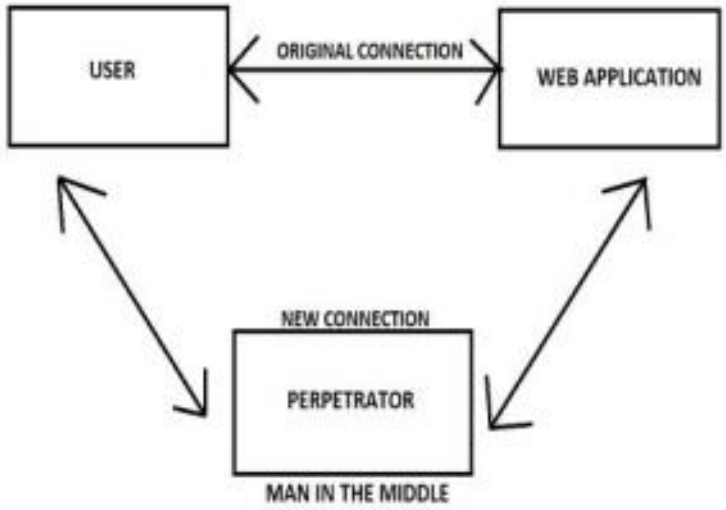
**Dictionary attacks:** In these, a hacker cycles through word combinations in an attempt to log in using a programme or script. This approach only attempts the options that have the highest chance of success; these are usually selected from a list of words, such as a dictionary. People frequently select simple passwords like their names, birthdates, or other personal information, making these attacks more successful.

**Keylogger intrusions:** In order to record everything, the user types, including login IDs and passwords, the hacker employs a programme to track all of the user's keystrokes in this instance.

**DISTRIBUTED DoS ATTACK: -**

Cybercriminals utilize distributed denial-of-service (DDoS) assaults as one kind of cybercrime attack to take down a system or network. DDoS assaults are occasionally launched via linked Internet of Things devices. In this scenario, the attacker floods the network with a lot of data until it is overloaded and unable to continue operating.

**MAN IN THE MIDDLE ATTACK: -**




The end-user and the entity with whom they are interacting can both provide information to this attack. For instance, when you conduct online banking, the man in the middle would pretend to be your bank and converse with you and your bank. All information sent between the two parties would end up in the hands of the man in the middle, including potentially sensitive information like bank account numbers and personal details.

**IMMIGRATION PREVENTION**

1. Make use of encrypted wireless access points (WAPs)
2. Verify your connection's security at all times. (HSTS, or HTTP/S)
3. Purchase a VPN.

DRIVE-through Download. This attack happens when computers that aren't too secure are compromised only by browsing a webpage. This attack has emerged as the most significant web security danger to be concerned about, according to findings from the most recent Microsoft Security Intelligence Report.

**MAGICAL SOFTWARE: -**

Another name for this is rogue security. Its purpose is to harm or interfere with a computer system. In this instance, the malware will attempt to deceive you into using your credit card for a purchase in addition to interfering with your system.

Here are some more techniques to con people:

1. Hacking: One type of cybercrime involves breaking into a person's system in order to attempt to use information, interfere with network operations, or disrupt other systems.
2. Credit card fraud: Credit card fraud is the most frequent type of cybercrime and can be committed via a variety of channels, including the internet and call centers.
3. Virus dissemination: One of the more prevalent forms of cybercrime is installing and disseminating viruses over the network, emails, texts, etc.
4. Computer vandalism: This is a modern issue that is involving a lot of people.
5. Software piracy: Software piracy is the illegal use, distribution, or duplication of software. Cybercriminals profit from the distribution of software that has been pirated. One of the largest marketplaces for software piracy is thought to be Southeast Asia.
6. Identity theft: Identity theft is a type of cybercrime in which thieves take personal information such as bank account information or passwords.
7. Cyberbullying: Cyberbullying is a type of online harassment directed at those who use computers or smartphones. It is sometimes referred to as online bullying or cyberharassment. Social media and gaming platforms are the usual venues for cyberbullying. It entails disseminating false information about someone and making hateful posts.

## CYBERCRIME AND INFORMATION SECURITY: -

Information and other communication systems can be safeguarded against unauthorized use, alteration, exploitation, and even theft through the potential activity of information security. The following are some precautions we can take to prevent falling victim to cybercrimes:

1. Keep operating systems and software updated: By keeping these components current, you can take advantage of the most recent security fixes to keep your computer safe.
2. Control the social media settings: Don't share any personal or sensitive information. With just a few pieces of information, social engineering cybercriminals can frequently obtain your personal information. For example, posting the name of your pet could reveal the answers to frequently asked security questions.
3. Make use of and maintain up-to-date antivirus software. This is the prudent approach to defend your system against intrusions.
4. Use secure passwords: Make careful to create secure passwords that are difficult for others to figure out and to keep them secret. Alternately, create strong passwords with a trustworthy password manager.
5. Avoid clicking on links from dubious websites or spam emails.

Clicking on links in unsolicited emails or other correspondence, or on unknown websites, is another way that people fall victim to cybercrime.

6. Pay attention to the URLs of the websites you visit.

Be mindful of the URLs you are selecting. Refrain from clicking on links that appear spammy or unexpected. Steer clear of public wifi networks.

1). Avoid the use of public wi-fi networks.
2. Refrain from conducting financial transactions on public computers.
3. Never divulge your passwords to outside parties.
4. Refrain from installing unidentified apps on your computer.

## SOME KEY POINTS OF THE INFORMATION TECHNOLOGY (IT) ACT, 2000 ARE AS FOLLOWS: -

Email is currently regarded as a legitimate and authorized method of correspondence. The Act grants legal legitimacy to digital signatures. The Act created new business entities that are now the Certifying Authorities and are able to issue digital certificates. Through e-governance, this Act enables the government to post notices online. The internet is now a means of communication for businesses as well as for businesses and the government. The primary purpose of this Act is to address the security issue. It presented the idea of digital signatures, which are used to confirm a person's identity online. The Act offers the corporation financial compensation as a remedy in the event that criminals cause it any loss or harm.

In addition to the Sections under the IPC and ITAA, 2008 that have been listed above, the Indian government has implemented the following measures to deter cybercrimes: States and U.T.s have established cybercrime units to report and look into cybercrime incidents. In order to raise awareness and provide training against cybercrimes, the government has also established Cyber Forensics and Training Labs in the states of Kerala, Assam, Mumbai, Mizoram, Manipur, Nagaland, Arunachal Pradesh, etc. under the IT Act of 2000. For the purpose of raising awareness and providing training, NASSCOM, Cyber Forensic Labs, and the Data Security Council of India (DSCI) have established locations in Mumbai, Bengaluru, Pune, and Kolkata.

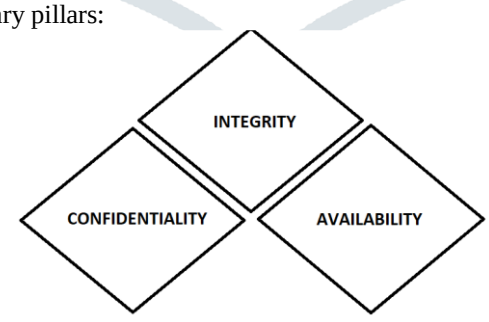
## CYBERSECURITY: -

It is the procedure and technology intended to shield devices and networks from harm, attack, or unauthorized access.

**Benefits:** 1. Safeguarding our company. 2. A rise in productivity 3. Encourages trust from customers. 4. Prevents the website from collapsing. 5. Safeguarding your clients or customers.

**WHY IS CYBERSECURITY ESSENTIAL?**

Cybersecurity is supported by three primary pillars:




1. Confidentiality: According to the principle of confidentiality, only parties with permission can access information and functions. Therefore, data should be kept private. 2. Integrity: The principles of integrity state that only authorized individuals and methods may add, change, or remove data and functions (data integrity should remain intact). 3. Availability: Systems, functions, and data must be available on demand in accordance with predetermined criteria based on service levels, according to the principles of availability.

## MOTIVES BEHIND CYBERCRIME: -

1. Interrupting the continuity of business. 2. Data manipulation and information theft. 3. Disrupting vital infrastructure in order to incite chaos and terror. 4. Amount of money lost by the target. 5. Fulfilling the military goals of the state. 6. Making a ransom demand. 7. Demanding the target's reputation.

**DOMAINS IN CYBER SECURITY: -**

1. Safety of Assets. 2. Engineering and Architecture for Security. 3. Network security and communication. 4. Management of identity and access. 5. Security management. 6. Evaluation and testing of security. 7. Software engineering and safety. 8. Risk and security management.

**CONCLUSION: -**

The modern era of technology is pushing everyone onto the internet. Additionally, using the internet is essential to our daily lives. However, there is a great need for us to employ cyber security in our daily lives and to be aware of it in order to safeguard and secure our information.

**REFERENCES: -**


1. Anderson, T. M. & Gardener, T.J. (2015). Criminal Law: Twelfth Edition. Stanford, CT: Cengage Learning.
2. Bar Association of India (2015). Anti-Bullying Laws in India. Retrieved from
3. https://www.indianbarassociation.org/wp-content/uploads/2015/11/Anti-bullying-laws-in-india.pdf
4. Brenner, W. Susan (2010). Cybercrime: Criminal threats from cyber space. Green Wood Publishing Group, Westport.
5. .https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.
6. Jaswant Narendra Saxena, Ananya Nagraj, Dr. Kommerla Siva Kumar, "Leaf of A Plant: Deep Learning for Feature Extraction", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.10, Issue 3, Page No pp.481-489, September 2023,
   DOI : http://doi.one/10.1729/Journal.36357.
7. Jaswant Narendra Saxena and Ananya Nagraj, " An Optimized Technique for Plant Identification Through Deep Residual Networks" , IJFMR Volume 5, Issue 4, July-August 2023. DOI: https://doi.org/10.36948/ijfmr.2023.v05i04.5807.
8. Jaswant Narendra Saxena and Ananya Nagraj, " An Efficient Real-Time Object Recognition Model Using Deep Learning Approach", International Journal of Multidisciplinary Educational Research ISSN:2277-7881; Volume:12, Issue:7(1), July- 2023.
   DOI : http://ijmer.in.doi./2023/12.07.08 .
9. Jaswant Narendra Saxena and Ananya Nagraj, " Hybrid System for Detection and Classification of Plant Disease Using Qualitative Texture Features Analysis", International Journal of All Research Education and Scientific Methods (IJARESM), ISSN: 2455-6211, Volume 11, Issue 7, July-2023.
   DOI: https://doi.org/10.56025/IJARESM.2023.117232299.
10. Jaswant Narendra Saxena and Ananya Nagraj, " An Optimized Technique for Image Classification Using Deep Learning", IRJCS: International Research Journal of Computer Science ISSN: 2393-9842 Volume 10, Issue 04, May-2023.
    DOI : https://doi.org/10.26562/irjcs.2023.v1004.11 .