International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 07 | July 2024 www.irjet.net p-ISSN: 2395-0072

Unveiling Cyber Crimes: A Comprehensive Overview of Cybersecurity Laws and Practices

Dr Roopali Sood[1], Rudraksh Gupta[2]

[1]HOD, Department of Computer Science and Applications, Apeejay College of Fine Arts, Jalandhar, India
[2]BCA, Department of Computer Science and Applications, Apeejay College of Fine Arts, Jalandhar, India
Guru Nanak Dev University, Amritsar, Punjab, India

Abstract - *The internet connects linked networks worldwide. It eases data and information flow between different networks. Security issues have grown in importance as networks exchange data across distant locations. Some individuals exploit the internet for illegal acts like network breaches and fraud. These internet-related crimes go by the name "Cyber Crimes." We hear this term often in news reports due to the rising popularity of online banking and shopping. To combat and penalize cyber criminals, authorities created "Cyber Law." This law governs the web. It forms part of legal frameworks addressing the Internet, cyberspace, and related issues such as online security and privacy. This research conducted by Guru Nanak Dev University student splits into sections to achieve its goals. It presents a quick look at cybercrime's nature, its actors - hackers and crackers, and its various forms. The text also tracks how cyber laws evolved in India. It sheds light on these laws' workings and suggests ways to fight this high-tech crime in India. The chapter aims to give readers a clear picture of the cybercrime landscape and India's response to it.*

Key Words: Cybercrime, Cyber-Security, Hacking, Trojans, Worms, Botnets, Phishing, Keylogger attacks, Brute-force attacks.

1. INTRODUCTION

Our growing need for the internet has changed how we live and work, making things easier but also more involved. It's as if we've stepped into a huge digital space where we can do so much with just a few clicks or taps. Yet, with this ease comes new problems. Think of it as walking down a crowded street in a big town—you're surrounded by chances and people, but you also have to keep an eye out for thieves, cons, and other dangers. In the digital world, risks come as fake emails that try to trick you into giving away your personal info, malware that locks your data until you pay, or hackers getting into systems to steal important information.

So, just like in the real world, we need to be careful online. It means knowing the dangers and acting first to keep our info safe. Using strong passwords, updating software, or being careful about which links we click - these small steps can help a lot in keeping us safe in our digital lives.

2. DEFINITION

CYBERCRIME:
It is the use of computers, communication devices, or networks to facilitate illegal acts.

When we say “cyber”, it is used informally for anything concerning computers, IT and virtual realities. This implies that “cybercrime” are offenses related to computers, IT, the Internet and virtual realities. A cybercrime is a crime in which data and information are stolen using a computer and the internet.

3. EXAMPLES

There are various examples which owes it’s happening as Cybercrime such as-:

- Breaking into the government website.
- Identity Fraud.
- Stealing Credit Card Information.
- Ransomware Attacks.
- Theft and sale of corporate data.
- Cyberextortion (demanding money to prevent a threatened attack).
- Cyberspying (unauthorized access of government or company data by hackers).

- Cryptojacking (where hackers mine cryptocurrency using the resources they do not own).

4. HISTORY

We can't know exactly when cybercrime started or the very first time someone committed a crime over a computer network. The first computer theft was in 1973, a teller at a New-York bank used a computer to embezzle over 2 million dollars.

The first spam email was in 1978. Sending spam emails is a cybercrime. In some countries we can go to jail if we send spam emails. In 1980's MNC Database (pentagon and IDM) was hacked. The first virus was installed on Apple computers was in 1982.

In 1981, Ian Murphy, known as Captain Zap was the first person convicted of cybercrime. He hacked into the AT&T network and changed the internal clock to charge off-hours rates at peak times. He got 1,000 hours of community service and 2.5 years of probation.

In 1990's National crackdown on criminals and Microsoft's NT operating system was pierced. This is where hacking started to become main stream. Before this hacking was very limited to organization.

In 2001, Cybercriminals attacked eBay, Yahoo, CNN.com, amazon and others. In 2007, Bank was hit by biggest ever hack. Swedish bank, Nordea recorded nearly $1 Million has been stolen in three months from 250 accounts.

In 2013, Adobe had 2.9million accounts compromised and their usernames and passwords were released on the open internet. In 2016, Kaspersky: one of the leading antivirus providers to the world reported around 758 million malicious attacks that occurred.

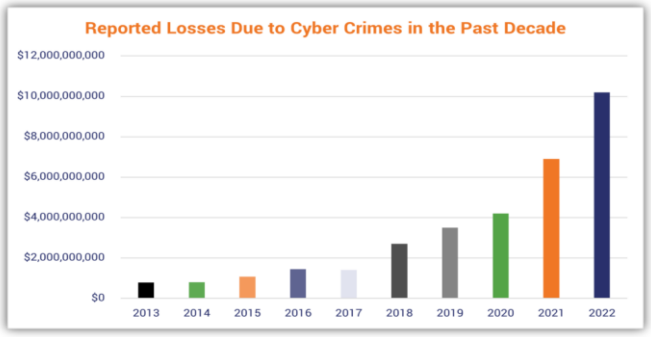

Fig 1: Losses by Cyber Crimes over the years

5. FORMS OF CYBERCRIME

Fig 2: Various Types of cybercrime

5.1 MALWARE ATTACKS

Malware is an attack where a computer system or network gets infected with a virus or malware. It's a broad term for all types of cyber-attacks including trojans. It's defined as code with malicious intent that steals data or destroys something on the computer.

A famous example of a malware attack is the WannaCry ransomware attack in May 2017.

When WannaCry ransomware hit, 230,000 computers were affected in 150 countries. Users were locked out of their files and a message was sent demanding they pay a Bitcoin ransom to get access back.

Many cyber criminals use computer viruses to gain unauthorized access to systems and steal data. A computer virus is a malware (malicious software program) loaded into a computer without the user's knowledge.

5.1.1 Trojans: -

Trojan is a kind of malware disguises itself as legitimate software or is included in legitimate software that can be modified. It acts stealthily and creates backdoors in our security to let other malware enter our system.

5.1.2 Viruses: -

Owing to its name, viruses attach themselves to clean files and infect other clean files and can spread uncontrollably

damaging the system's core and deleting or corrupting files. They appear as an executable file that you might have downloaded from the internet.

5.1.3 Botnets: -

Botnets are collections of compromised computers. Designed to cooperate under direction of an attacker.

5.1.4 Worms: -

In this, Whole device networks being infected by worms. Local networks or network interfaces used over the internet can help spread it. It makes use of every subsequent compromised system. It spreads more easily and silently.

Malware may infiltrate our system. If we have open security holes. If we download reputable software from website or if we have corrupted email attachments.

5.2 PHISHING

It is type of cybercrime. Perpetrators 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. Intention is deceiving the receivers into taking actions that compromise their own security or security of the company they work for. These fraudsters first gather passwords and bank account information.
Then they take money. Phishing messages appear genuine. They try to trick victims into disclosing personal information.

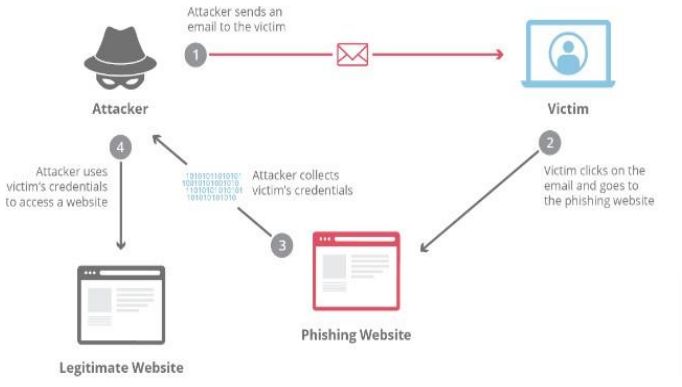

Fig 3: Process of Phishing attack

The attacker must choose which company to target. They must figure out how to obtain email addresses of those companies' clients. After determining which company to impersonate and who their targets are the attackers go through a setup phase. During this time, they develop strategies for sending the messages. They gather data. Finally, they carry out attack. Subsequently, the assailant logs data that victims input into popup windows. Lastly the attacker utilizes the information they have obtained to commit fraudulent. They commit identity theft transactions.

5.3 DISTRIBBUTED DOS ATTACK

Cybercriminals utilize distributed denial-of-service (DDoS) assaults as one kind of cybercrime to incapacitate system or network. IoT devices with connections are used occasionally. The attacker employs the network send large amounts of data. This overwhelming influx of data results in network experiencing overloading. It is no longer able to operate effectively.

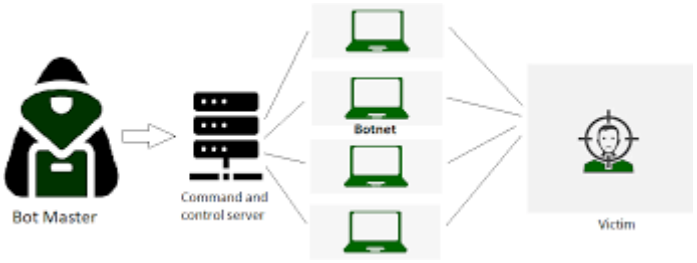

Fig 4: DDOS Attack

5.4 PASSWORD ATTACK

It is an attempt to obtain the password of a user for the purpose of using it in a malicious manner or decode it. Password attacks used by hackers can include the use of password sniffers, dictionary attacks and cracking software. The only protection from Password attacks is to have a policy for passwords which include weekly updates, selection of random words, and length.

Fig 5: Common Types of Password Attacks

This assault can be done for many reasons, but the most malicious is to get unauthorized access to a computer

without the consent of the owner of the computer to perform unlawful act such password stealing for bank details. There are Three widely used methods used to hack a password protected system.

1) **Brute-Force Attack-:** In this case, the hacker logs in using a computer program or script y guessing the password on several attempts and the first one is often the most common.
2) **Dictionary Attacks**-: In this, hacker tries overset of common word sequences with a program or a script in an effort to log in. It only tries the attempts that are most likely to be successful in the first place; these are normally taken from a list comprising terms such as dictionaries. The human factor that plays a role in these attacks is that individuals choose easy passwords such as their names, birthdates or other easily guessed passwords
3) **Keylogger Attacks-:** In this, hacker tries to capture all actions that the user has entered, including login ID and password, the hacker uses a program to follow all keystrokes.

5.5 MAN IN THE MIDDLE ATTACK

This attack is supported by the end-user and the specific entity with which the end-user is interacting.

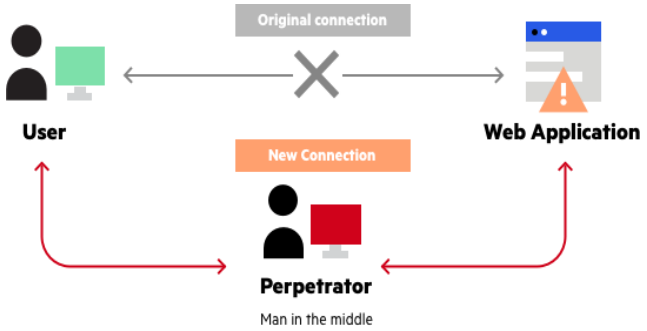

Fig 6: Man-in-the-middle Attack

For example, if we are doing banking through the internet, the man in the middle will be doing the following two things; He will be interfacing with you in as much as he will also be communicating with your bank

.

Every message that was exchanged between the two parties would instead go to the middle man, and this would in fact mean that such important details as bank account numbers and passwords or any other private information being passed around would reach the man in the middle.

5.5.1 Man in the middle Prevention

Using following steps can help to prevent these type of crime-:

1) Employ encrypted wireless access points (WAPs).
2) It is important always to check whether the connection is secure (HTTPS or HSTS) before proceeding with connection.
3) Spend on high secured VPN

DRIVE-BY Download: This attack targets vulnerable machines when they connect to a webpage containing this assault.
This kind of attack has been identified as the leading web security threat in the current world, based on the recent Microsoft Security Intelligence Report.

5.6 ROGUE SOFTWARE

Rogue software is also known as frauds security or scam security. Its goal is to have an adverse impact or modify computer settings in an adverse manner. In this instance, it will convince you to spend some money using your credit card besides effecting changes in the system.

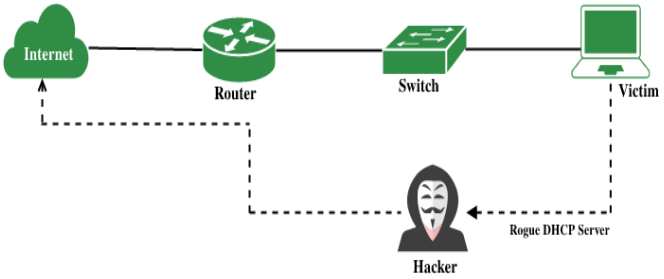

Fig 7: Rogue DHCP Server Attack

Different ways of tricking and scamming people are-:

1) **Hacking: -** It is the act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal or organizational data.
2) **Identity Theft: -** It is referred to as a type of cybercrime in which criminals steal unauthorized and important personal information like passcodes and bank-account details.
3) **Software Piracy: -** Software piracy is the unauthorized use, copying or distribution of copyrighted software. It may take many forms, including: Unauthorized copying of software programs purchased legitimately, sometimes known as "end-user" piracy. Gaining illegal access to protected software, also known as "cracking"
4) **Credit-Card Fraud:** - It is the form of fraud that involves an unauthorized taking of another's

credit card information for the purpose of charging purchases to the account or removing funds from it.

6. CYBERCRIME AND INFORMATION SECURITY

Information Security is an activity, which could be possibly performed by, to keep and protect Information and other related communications from stealing and misuse, tampering, and malicious act.

6.1 The following are some precautions which we can take to prevent cybercrime actions:

1) **Ensure Software and operating systems are updated:** - When these components are updated, it ensures you have the latest security update to protect your computer.
2) **Controlling the Social Media settings:** - Protect oneself from personal and private information. Social engineering hackers can most of the time, get our personal details with even little details. For instance, you might get in the habit of posting the name of your pet, thus revealing the answers to common security questions.
3) **Using Updated Anti-Virus software:** - Updated antivirus software can help and secure our computer to various trojans and malware that affect out data and information.
4) **Use secure passwords:** - Be particular while coming up with password to ensure they are hard for other people to guess and ensure you do not disclose them. To ease this, you can also use a reliable password generator from a password manager and create these passwords at random.
5) **Do not click on links in unsolicited emails or websites:** - Opening links in emails or other messages that people receive or links found on the internet in general is another way people are caught with cybercrime.
6) **Pay attention to the URL's one is visiting:** - Ensure that the URLs you are choosing are well-captured. Do not click on links that seem to be spam or you did not expect to see them.
    - Using of public networks should be avoided
    - Utilizing public computers for financial transactions should be refrained by user.
    - Never divulge your passwords to outside parties.
    - Refrain from installing unidentified apps on your PC.

7. INFORMATION TECHNOLOGY (IT) ACT, 2000

- Email is now regarded as a legitimate and authorized means of exchange of ideas.
- The Act grants legal legitimacy to digital signatures.
- The Act established new corporate entities known as the Certifying Authorities, who are now 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 between them and the government.
- The internet is now a means of communication for businesses as well as between them and the government.
- 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, the Indian government has implemented the following measures to deter cybercrimes:

- States and U.T.s have established cybercrime units to record and look into cybercrime incidents.
- In addition, the government has established Cyber Forensics and Training Labs in the states of Kerala, Assam, Mumbai, Mizoram, Manipur, Nagaland, Arunachal Pradesh, etc. under the IT Act, 2000, with the purpose of raising awareness and providing training against
- For the purpose of raising awareness and providing training, NASSCOM, Cyber Forensic Labs, and the Data Security Council of India (DSCI) have established Cyber Forensic Labs in Mumbai, Bengaluru, Pune, and Kolkata.

8. CYBERSECURITY

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

USAGE:
1. Safeguarding the company.
2. Enhanced output
3. Encourages trust from customers.
4. Prevents the website from collapsing.
5. Safeguarding the clients or customers.

8.1 NEED OF CYBERSECURITY

- Cybersecurity is needed today as people store, transmit, and process their personal and financial information, business secrets, and crucial infrastructure's data in the cyberspace. Malicious attacks are dangerous and can lead to monetary loss, tarnishing of companies' images, and in some cases, loss of life.
- cyber security remains crucial in any organization irrespective of the nature and size of the organization. The increase in technology and in turn the increase in software in the governmental, educational and hospital sectors lead to information going digital through wireless communication networks.
- The significance of cyber security is to protect the information of different organizations such as e-mail, yahoo and many more, that have such confidential data which if leaking, can result to losses to both parties and tainted reputations. Evil doers focus on the small and big firms and acquire the papers that are of importance.
- Security as a whole has greatly become an important aspect especially in the contemporary society with the internet and other related technologies. Due to the increased storage and transmission of data, the cases of cybercriminal attacks in organizations have also continued to rise. Cyber security is a way of safeguarding computers as well as their networks, hardware, software, data and digital information and assets.

8.2 TECHNIQUES USED IN CYBERSECURITY

Cybersecurity techniques are used by all in day-to-day life such as-:

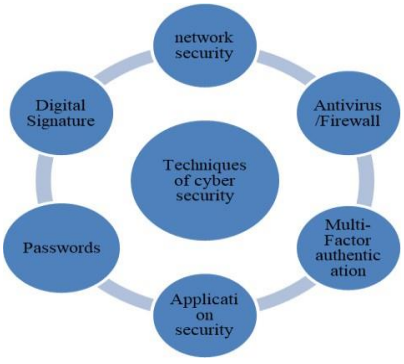

Fig 8: Cybersecurity techniques

- **Firewalls:** It act as a barrier between a trusted internal network and untrusted external networks. They filter incoming and outgoing traffic based on predetermined security rules. Firewalls can be hardware-based, software-based, or a combination of both.
- **Multi-Factor Authentication (MFA):** MFA requires users to provide two or more verification factors to gain access to a resource. This might include something they know (password), something they have (security token), and something they are (biometric verification).
- **Application Security**: Application security encompasses measures to improve the security of an application often by finding, fixing, and preventing security vulnerabilities.
- **Passwords:** Passwords are the most common form of authentication, requiring a user to provide a secret string of characters to gain access to a system. Enforcing strong password policies (complexity, length), regular password changes, using password managers, and avoiding the reuse of passwords across different platforms.
- **Digital Signature**: A digital signature is a mathematical scheme for verifying the authenticity and integrity of digital messages or documents. Utilizing public key infrastructure (PKI) to create and verify signatures, ensuring non-repudiation and authenticity of documents and communications.
- **Network Security:** Network security involves measures taken to protect the integrity, confidentiality, and availability of computer networks and data using both software and hardware technologies. Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Virtual Private Networks (VPNs), and secure network protocols.

8.3 DOMAINS IN CYBERSECURITY

Cybersecurity involves broad range of domains such as:

- Asset Security.
- Security Architecture and Engineering.
- Communication and Network Security.
- Identity and access management.
- Security operations.
- Security assessment and Testing.
- Software development and Security.
- Security and risk management

10. CONCLUSION

Indeed, the internet is widely used in the present day and age to the extent of being a formidable tool that dictates how lives are lived, tasks are accomplished, and people relate. With that said, we continue to engage in this environment, and now the protection of one's data has never been more vital. The best thing that can be implemented today is the ability to live a secure life online by adhering to cybersecurity concepts. By understanding and applying these principles, we can navigate the digital world with confidence and peace of mind.

11. REFERENCES

1) Brenner, W. Susan (2010). Cybercrime: Criminal threats from cyber space. Green Wood Publishing Group, Westport
2) https://www.indiacode.nic.in/bitstream/12345 6789/1 3116/1/it_act_2000_updated.pdf
3) Bar Association of India (2015). Anti-Bullying Laws in India. Retrieved from
4) Anderson, T. M. & Gardener, T.J. (2015). Criminal Law: Twelfth Edition. Stanford, CT: Cengage Learning.
5) Ugander G J Reddy, Nikhita Reddy Gade (2014). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies
6) https://www.cisco.com/c/en_in/products/securi ty/what-is-cybersecurity.html
7) https://www.geeksforgeeks.org/cyber-security-types-and-importance/