International Interdisciplinary Virtual Conference on
'Recent Advancements in Computer Science, Management and Information Technology'
International Journal of Scientific Research in Computer Science,
Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

# Cyber Crime and Cyber Security: An Overview

**H. J. Kharat**
Department of Physics, Shankarlal Khandelwal Arts, Science and Commerce College, Akola, Maharashtra, India

## ABSTRACT
In the present age of Information technology, internet has become an integral part of everyone's life. It is the global system of interconnected computer networks, which links the devices worldwide. It carries an extensive range of information resources and services. However, some of the peoples use the internet to harm the individuals who becomes victims and affects the national security. Such cyber-Crimes and online criminal activities have increased in multiples after COVID-19 pandemic. So, this is a serious challenge to the society to increase the Cyber security and aware the people from the techniques of the criminals. In the present study, various types of cybercrimes such as Phishing, Scams, Online harassment, Identity Theft, Financial Theft, Malware, Ransomware, Spyware, Virus, Worm, Trojan programs in the cyber word have been described. Various domains of cyber security and Preventive measures against the cybercrime have been presented for national security.
**Keywords:** Internet, Cybercrime, Cyber security, Preventive measures, National security

## I. INTRODUCTION

Information technology has changed the modern way of living life. The internet provides us with many benefits and touches almost all aspects of our lives. It can be used for communication, real time updates and recent news, financial transductions, online booking, shopping, blogging, job searching, finding life partner, business, social networking, entertainment, education and research [1]. However, it also makes us vulnerable to a wide range of threats. A minor negligence in managing our digital lives can open the door to cyber criminals due to which new and powerful cyber-attacks are striking the internet and disturbing the life [2]. Cyber crimes can perform by many ways. It has been increased from COVID-19 pandemic and increasing day by day in multiples [3].So there is a need to reduce the risk of cyber threats and criminal activities, Cyber security is most important [4]. Cyber security is also called as Computer security or IT security. It includes the protection of personal data and computer systems from the theft or damage to the hardware, software or disruption of the services. [5]

### 1.1. CYBER CRIME

Online or virtual criminal activities carried out through internet using computer, or networking devices are known as Cybercrimes. Cybercrimes have wide range of activities. Cyber crimes are committed by

cybercriminals for financial benefits or for accessing intentionally unauthorised personal or institutional data. Cyber criminals are usually skilled computer programmers, find the weaknesses of the users and perform the crime with number of ways. Some of the common cyber crimes are described in brief in this presented work [6-8].

### 1.1.1. Hacking

Hacking is identifying the negligence in computer systems and/or networks and exploiting it for gaining the unauthorised access of the system passing the login algorithm.

### 1.1.2. Identity theft

It is the act of wrongfully obtaining someone's identity proof without his or her permission. This may include their name, phone number, address, bank account number, Aadhaar number or credit/debit card number etc.

#### 1.1.2.1. Gaining access to social media accounts

The Cyber criminal gains access to the social media accounts and can then harm the victim by misusing their personal information and photographs. He can also post offensive content on victim's profile.

#### 1.1.2.2. Misuse of photo copies of identity proofs

The attacker misuses the photo copies of identity proofs of the victim. These can be PAN Card, Aadhaar Card or any other identity proof of the victim. The attacker can use these photo copies to steal money or cause harm to the victim.

#### 1.1.2.3. Skimming of debit or credit cards

Skimmer is used to duplicate the Debit or Credit card, which can be used to withdraw the money from the ATM. The Debit or Credit card is swiped through a skimmer and captures all the details.

### 1.1.3. Psychological tricks

Hacker used psychological tricks by offering profit making schemes and traps the user. Once trapped, he can exploit the victim by either stealing money or stealing sensitive personal data. Recently Lottery scam (Congratulations! You just got Rich!), Nigerian Scam (Help me move Money and I will dip you in Cash!), Astrology Scam (..I can See your Future!), Work from Home Scam (Hello, I make you Rich!), Job Related Frauds (offering a job with an attractive salary!) /Debit Card Frauds (your card has been blocked!), WhatsApp Calling Invitation Scam, Snapchat Nude Photos Leak , –eBay, iCloud Leaks, can be done using psychological tricks.

#### 1.1.3.1. Phishing

Hacker sends fake emails to many peoples to impersonate real systems with the goal of capturing sensitive data. E mail might come from a bank or other well known institution with the need to verify your login information. Some greedy people will reply and trapped.

#### 1.1.3.2. Vishing

Phishing by phone is also called Vishing. Recently, Fraudsters have started phishing using the telephone as their new pawn. Victim will receive a phone call from a person posing as an employee of a bank or any other known organization. The caller instructs the victim to call another number. The attendant will ask the caller for their bank account details.

#### 1.1.3.3. Smishing

It is the SMS equivalent of phishing. Text messages will be sent and asks the recipient to visit a websites or weblinks or call a phone number. The victim is then tricked into providing sensitive personal information.

### 1.1.4. Social media related attacks

No any mobile user can think without Social Media as it is the new and easy way of communication. We share our day to day information, photographs and live locations on social media. One can understand the entire history of an individual through their social media profile and it becomes easy for cyber criminal to access the important data. So there is a need to protect the social media accounts and use it in an appropriate manner.

#### 1.1.4.1. Sympathy fraud

With frequent interactions, the criminal becomes friends with the user on social media. After getting sympathy extracts money and harms the user.

#### 1.1.4.2. Honey trap

After gaining the victim's affection through social media, the criminals makes fake video calls and records them and exploits the victim physically or financially or emotionally.

#### 1.1.4.3. Cyber stalking

Cyber Criminal continuously follows the activities of targeted users through electronic communications and harasses a victim sending SMS, E-mails, messages posted on a website.

#### 1.1.4.4. Cyber bullying

Cyber bullying can occur through sending negative, harmful SMS, posting or sharing, false content about someone else on social media,

#### 1.1.4.5. Photo morphing

Personal photos of the user posted on the social media can be edited smoothly from one image to another by small gradual steps using computer animation techniques. Using these photos fraudsters can blackmail or harass the person.

### 1.1.5. Attacks through mobile applications

Use of smartphones increases the use of android applications. These applications are widely used not only for entertainment but also for the convenience to perform day-to-day tasks such as bill payments, bank accounts management, service delivery etc. Cyber criminals infect the applications with malicious software, called

Trojan. Trojan can get access to your messages, OTP, camera, contacts, e-mails, photos etc. for malicious activities and extract data and money.

### 1.1.6. Online banking frauds

Online banking services such as account statement request, funds transfer, cheque book request, preparing demand draft etc. can be done sitting at home. Due to these online services, cyber frauds related to banking are also increasing. Hence, protection of bank accounts with strong passwords becomes highly essential.

#### 1.1.6.1. Hacking of bank account due to weak password

Criminal used a program to guess commonly used passwords and hacks the victim's account and perform an illegal transaction by stealing the money.

#### 1.1.6.2. Digital payments applications related attacks

Digital payments have become very common in today's life. However, they do pose a threat if the account is hacked.

#### 1.1.6.3. Hacking of multiple accounts due to same password

If same password is used for multiple accounts, then hacking of one account may also lead to hacking of other accounts.

### 1.1.7. Malware attacks on personal computer

We used to store important information in the personal computers or laptops. Protection of data is highly essential. A virus is a program that replicates to erase or damage the data.

#### 1.1.7.1. Malware attack through external devices

A virus can enter the computer through external devices like pen drive or hard disk etc. This virus can spread across all the computer files.

#### 1.1.7.2. Attack by downloading files from un-trusted websites

When we download the files from un-trusted websites, virus can enter the computer and spread across all the computer files. The virus can be hidden in the form of music files, video files or any attractive advertisement.

#### 1.1.7.3. Malware attack by installation of malicious software

The virus can enter into the computer by installing malicious software from un-trusted sources. The virus can be an additional software hidden inside unknown game files or any unknown software. This virus can spread across all the computer files.

### 1.1.8. Worm and Trojan horse attack.

Worm and Trojan horse are also used to harm the computer without 'run' manually. Worms spread automatically in whole network. Trojan is used for gaining admin access of target.

## 1.2. CYBER SECURITY

India stands fifth in worldwide ranking of countries affected by cybercrime. Cyber Security plays an important role in reducing the crime and developing information technology as well as internet services. Cyber-security can be described as a combination of technologies and methods, to protect the privacy, and integrity of computer systems, networks and data from unauthorized access [9-11].

Cyber security usually refers to three characteristics of information systems, 1. Confidentiality (privacy of information), 2. Integrity (computing processes have not been destroyed), 3. Availability (assurance of service availability when needed). These characteristics needs protection.

Continuous development of new security initiatives and strategies to keep pace with criminals is necessary. It is essential to enhance the cyber illiteracy and aware the people about its security and current developments in the Cyber Security domain. Sub domains of Cyber security have been studied as follows [12-13]

### 1.2.1. Network security

Effective network security includes hardware and software systems to protect networks and infrastructure from unauthorized access, disruption, and misuse.

### 1.2.2. Mobile security

Mobile security means protecting the data stored on mobile devices such as cell phones, laptops, tablets, etc. from various threats.

### 1.2.3. Cloud security

Cloud Security is concerned with the security of data stored by service providers such as AWS, Google, Azure, Rackspace, etc.

### 1.2.4. Data security

Data security involves the implementation of a robust information collection system that ensures the security of the data at rest and in transition.

### 1.2.5. Application security

The implementation of various techniques against a variety of threats to all software's and services used in an organization is application security. The techniques used are secure code writing, robust data input authentication, threat modelling, etc. These can minimize the possibility of any unauthorized access or alteration of resources in the application.

## 1.3. SECURITY MEASURES

There are many simple and effective online securities available in the market. The available technological security measures such as Firewalls, antivirus software, and other technological solutions for safeguarding personal data and computer networks are essential to ensure the security. Some of the major cyber security measures are described as follows [14-22].

### 1.3.1. Think before you click

Hacker sends the password recovery links either by email or on social media or by websites. Clicking these links, hacker gains access to personal data and account details. So do not click unknown links.

### 1.3.2. Use strong and varied passwords

It is easy to use and remember the same password for all accounts but it makes account more insecure. So use distinct and strong passwords for all different accounts. Use passwords with more than 8 characters with at least one uppercase letter, one lowercase letter, one number, and a few symbols other than &, #, @, etc. Change password often and reset it.

### 1.3.3. Use password manager tool

The password manager is a software application that is used to store and organize the passwords encrypted. User can create a strong master password for accessing the entire password database.

C.4.Set up two-factor or multi-factor authentication

Two-step verification enables extra security layers to online verification. In this MFA method, we have to authenticate twice and required to enter more than two credentials such as password, code, fingerprint, OTP etc. while logging in. This keeps the account more secure by making it more difficult for hackers to access your data.

### 1.3.4. Keep your systems updated

At workplace, user must keep all browsers, software, and operating systems up-to-date. Updating will prevent attackers from exploiting them for enough time until new updates.

### 1.3.5. Use firewalls and anti-viruses

Hacker can gain access of the systems and networks through different attacks such as, malware, viruses, trojans, spyware, phishing attacks, etc., Antivirus software and firewalls detects and eliminates the viruses and protects the system from being infected or hacked. We have to scan external devices before use and run virus scans on your computer frequently. Use licensed antivirus and keep it updated, avoid using torrent sites.

### 1.3.6. Don’t use public Wi-Fi without VPN

We should not use public Wi-Fi unless it will not be urgently needed. Whenever we have to use it, use Virtual Private Network (VPN) along with it. VPN allows your device to be secure as it encrypts the traffic between the server and your device. This increases the difficulty of hackers when they try to access your personal data. Turn off Wi-Fi, Location Services and Bluetooth when not in use.

### 1.3.7. Take data backup regularly

Cyber attacks may lead to data loss and file damage in the system or network. Backups are nothing but a copy of the files or network’s data for the purpose of restoration in case of damage or loss. So users always take a backup of important data.

### 1.3.8. Avoid useless downloads

Cyber attackers use the tricks of downloads to access the systems or networks. So user should avoid downloading of unnecessary software and browser extensions. For safe downloading, choose the process of custom installation and follow the steps carefully. During installation process, Pop-ups for any extensions or add-ons, must be declined.

### 1.3.9. Stay careful on social media

Every user is trying to reconnect or remained in touch with friends and family through various social media platforms over the internet, Hackers can access easily a lot of information from your social media pages and profiles. However, there is need to be careful about online sharing of the data. Avoid making your personal information public on social media.

### 1.3.10. Avoid online use of debit cards

For online purchasing and online transactions, instead of debit cards for paying the bills, use applications which will provide more protection to your bank accounts. Avoid saving your credit/debit card information on websites and web browsers.

### 1.3.11. Know about phishing attacks

In order to avoid phishing attack, do not open emails with malicious links from unknown people or sources. Check the mails carefully and links for any type of grammatical errors and the ID of the sender. Such links may be malicious and unsafe. This sigle click may lead cyber attack. Educate your friends and family about such types of errors so that they avoid opening such emails or forward them to you without any knowledge

### 1.3.12. Avoid unfamiliar websites

If any one of your friends sends new sites, be cautious of visiting them because some of them may contain drive-by download attacks, Such attacks does not required to click on anything in order to get the computer infected. It attacks your system by injecting malicious code as soon as you click on the link of the website. So, try to avoid such websites and visit only well known, well-established and familiar websites. Avoid checking 'Keep me logged in' or 'Remember me' options on websites.

### 1.3.13. Watch frequently and online transactions

Keep a check continuously on your bank statements: Keep an eye on your bank statements and query any unfamiliar transactions with the bank.

### 1.3.14. Safety tips for camera:

Avoid geographical tagging, disable location sharing, upload pics of resolution 72 or watermark them, check changing room / trial room, avoid sharing personal pics.

### 1.3.15. Secure Your Data

We must have awareness about Cyber Security so that we would be capable of securing personal data and systems safe from any type of cyber attacks from external threats.

### 1.3.16. Cyber Security Measures in brief

- Permanently delete all documents downloaded on computers in cybercafé.
- Never provide details or copy of identity proofs to unknown person/ organization.
- Be careful while using identity proofs at suspicious places.
- Do not share sensitive personal information and photos on public platforms.
- Do not give your card to swipe to any one and leave your credit, debit or ATM card receipts behind, in places such as a bank/ATM or a store; never throw them away in public.
- Do not share your PIN, CVV, OTP with anybody. Bank will never ask for.
- Do not respond to suspicious e-mails or click on links. Beware of the fake calls.
- Do not transfer money to any un-trusted unknown account.
- Always verify the domain names of websites. Govt. websites have ".gov.in" or ".nic.in" as part of their web address.
- Proper spam filters must be enabled in your e-mail account.
- Be careful while accepting friend request from strangers on social media. Always inform to family members about social media friends and your internet practices.
- Restrict access to your profile.
- Avoid sharing your location on Social media.
- Always install mobile applications from official application stores or trusted sources. Free applications may be malicious.
- Scrutinize all permission requests for application to be downloaded.
- Register personal phone number and e-mail with bank and subscribe to notifications, which will alert after transaction quickly.
- Always check "https" appears in the website's address bar before making an online transaction. The "s" stands for "secure" and indicates that the communication with the webpage is encrypted.
- Never download or install free and pirated software's. Always read the terms and conditions before installation.
- Always use virtual keyboard to access net-banking facility from public computers and logout from banking portal/website after completion of online transaction. Also ensure to delete browsing history from web browser after completion of online banking activity.
- Cell phone has IMEI code keep it noted in a safe place. The operator can blacklist/ block/trace a phone using the IMEI code, in case the cell phone is stolen.
- Try for optimal use of internet. Always follow cyber safety tips and be aware about cyber crimes and security. Spread the awareness in the society. Your single effort can help for national security.
- Do not involve in the cyber crime and avoid the punishment as per cyber law against the crime.
- If online account has been hacked, immediately log in and change the password to a strong, unique password.
- Unfortunately, if any incident of cyber crime will happened, report to nearest cyber police station and lodge the complaint on National cyber crime reporting portal: https://cybercrime.gov.in

## II. CONCLUSION

In the present study, we have described the various methods of cyber crime and cyber attacks which helps to overcome the several loopholes in the computer operating systems and networks. The study has been started with the aim 'Prevention is always better than cure'. The main objective of this study was to explore the cyber safety and security measures while operating the internet. Author believes that this study must support to enhance the cyber security awareness and to reduce the risk of cyber crimes in the country.

## III.REFERENCES

[1]. Barry M. Leiner at. al., "A Brief History of the Internet," ACM SIGCOMM Computer Communication Review, Volume 39, Number 5, October 2009

[2]. V.Karamchand Gandhi. An Overview Study on Cyber crimes in Internet. Journal of Information Engineering and Applications. 2012;2(1):1-6.

[3]. C.M. Williams, R. Chaturvedi and K. Chakravarthy, "Cybersecurity Risks in a Pandemic", Journal of Medical Internet Res., vol. 22, no. 9, pp. 23692, 2020

[4]. Asif Perwej "The Impact of Pandemic Covid-19 On The Indian Banking System", International Journal Of Recent Scientific Research (IJRSR), ISSN 0976 –3031, Volume. 11, Issue 10 (B), Pages 39873-39883, 28th October, 2020

[5]. S. Aftergood, "Cybersecurity. The Cold war online", Nature, vol. 547, no. 7661, pp. 30, 2017

[6]. Soham Shah, MA Lokhandwala, et al.Decoding Farm Laws. International Journal of Scientific Research and Engineering Development. 2021;4(2):590-595.

[7]. Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 IJSER © 2012

[8]. Abraham D. Sofaer, David Clark, Whitfield Diffie ,Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/catalog/12997.htmlCyber Security and International Agreements ,Internet Corporation for Assigned Names and Numbers pg185-205

[9]. Thilla Rajaretnam, University of Western Sydney, The Society of Digital Information and Wireless Communications (SDIWC),International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 232-240 2012 (ISSN: 2305-0012)

[10]. Thomas H. Karas and Lori K. Parrott , Judy H. Moore , Metaphors for Cyber Security ,Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0839

[11]. Bina Kotiyal, R H Goudar, A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India PritiSaxena, IACSIT International Journal of Information and Education Technology, Vol. 2, No. 2, April 2012

[12]. S. Bistarelli, F. Fioravanti, P. Peretti, Using CP-nets as a guide for countermeasure selection, Proceedings of the 2007 ACM Symposium on Applied Computing (Seoul, Korea, 2007), 2007, pp. 300–304.

[13]. Admiral Dennis C. Blair, Annual Threat Assessment, House Permanent Select Committee on Intelligence, 111th Congress, 1st sess., 2009.

[14]. Mike McConnell, —Mike McConnell on How to Win the Cyber-war We're Losing,‖ February 28, 2010,
[15]. D. J. Bodeau, R. Graubart, and J. Fabius-Greene, —Improving cyber security and mission assurance via cyber preparedness (Cyber Prep) Levels,‖ September 9, 2010.
[16]. Anju P Rajan Mathew1, A. Ajilaylwin2 & Shaileshwari M, Cyber Security Solutions For Dlms Meters Using Gsm/Gprs Technology ,U3 1&2 Department Of Cse, The Oxford College Of Engineering, Bangalore3engineering Officer Grade 2, Central Power Research Institute, Bangalore, India
[17]. Ajith Abraham1, Crina Grosan2, Yuehui Chen3, Cyber Security and the Evolution of Intrusion Detection Systems, School of Computer Science and Engineering, Chung-Ang University, Korea 2 Department of Computer Science Babes-Bolyai University, Cluj-Napoca, 3400, Romania 3School of Information Science and Engineering Jinan University, Jinan 250022, P.R.China.
[18]. Hemraj Saini, Yerra Shankar Rao, T.C.Panda, Cyber-Crimes and their Impacts: A Review, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209 202.
[19]. Divyashree Mahesh , Divyashree S K , Dr. Madhusudhan S, A Review Paper on Study of Cybersecurity on Cybercrime, International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) Volume 2, Issue 2, March 2022 Copyright to IJARSCT DOI: 10.48175/IJARSCT-2858 261 www.ijarsct.co.in
[20]. Dr.Yusuf Perwej, Prof. (Dr.) Syed Qamar Abbas, Jai Pratap Dixit, Dr. Nikhat Akhtar, Anurag Kumar Jaiswal, A Systematic Literature Review on the Cyber Security, International Journal of Scientific Research and Management (IJSRM),Volume 09, Issue 12, Pages, EC-2021-669-710, 2021, Website: www.ijsrm.in ISSN (e): 2321-3418 DOI: 10.18535/ijsrm/v9i12.ec04.
[21]. T. Rid and B. Buchanan, "Attributing cyber-attacks", Journal of Strate St., vol. 38, no. 1-2, pp. 4-37, 2015.
[22]. Z. Trabelsi, K. Hayawi, A. Braiki and S. Mathew, Network Attacks and Defenses: A Hands-on Approach, Boca Raton, Florida:CRC Press, 2013