IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# CYBER CRIME(CC) IS "A THREAT TO SOCIETY(T2S)"

**Mradul Kumar Saxena**

PhD Scholar at Rai University, Ranchi(JH)

**ABSTRACT:**

Cyber security understands protecting data, networks, programs and other important information from unauthorized or unattended access, destruction or change. In today's world, cyber security is very important because of some security threats and cyber-attacks point of view. For data protection, many companies develop software and the software protects the data. Cyber security is important because not only it helps to secure information but also system from virus attack. After the U.S.A. and China, India has the highest number of internet users. India is a developing country and its position is second in terms of population. Population plays a very important role for a country and its systems. Human capital is very important for increasing the power of digital nation. Currently, India's population is 136.64 crores as of 2019, based on the latest United Nations estimates. This population shares 17.7 percent of the world total population. It takes rank number 2nd in the list of countries of dependencies by population. No cyber crime is possible without using social networking platform. A social networking platform is a place where people participate and express themselves through different media sites—such as YouTube, MySpace, Facebook, Whatsapp etc,Social Networking site is a platform where members/participants expose themselves, discuss, reveal, and expound on their personal lives, activities, hopes, dreams, and even fantasies for others to see and marvel upon. Online communities represent a growing class of marketplace communities where participants can provide and exchange information on products, services, or common interests also. While using social networking platform, the user is also exposed to cyber criminals and they can take advantage of personal information shared by any person on social networking platform.

**Key Words: CYBER CRIME (CC), THREAT TO SOCIETY(T2S), Cyber Security, Cyber attack, Cyber Criminals, Digital Nation, Social Networking platform.**

## INTRODUCTION:

The Social networking sites gives a direct way for people to do social activity and have a simple social presence through web. a virtual environment is provided for people to share each and every activity, their interests, and their circle of acquaintance with their family, friends, or even the unknown persons. With so much of data transfer, hackers and thieves can very easily steal/hack personal data and some important information of public at large through these networking sites. That is why a security protocol is needed to safeguard against activities of hackers which form the basis of this research. In this paper, we will discuss some of the privacy and security concerns, cyber-attacks and how they can be prevented and also some of their respective prevention techniques. In this paper an architecture is proposedto avoid any malpractice during request-response exchange of data between two or more users. This architecture helps in improving the customization of profiles. Our research suggests that only a proper knowledge of the hacking strategies will prove the best defense in the war against cyber-attacks[1].

Social networks are useful and important tools of communication these days. They reflect the social image of a person. You can forget the whole physical world around you once you are stick with the social networks. The network of social relations that build up during your everyday life can be simply translated onto your “profile” and made available for the whole of your friends to see. Then there is a concept of “following” that can make you more famous. By sharing your respective data, the world can feel your presence much more. These all things are so adductive that no one can even think of living without it. But sometime we are so comfortable and attached to these social sites, that we share personal details about ourselves without thinking anything. Presently, hundreds of millions of persons, use a wide variety of social networking sites (SNSs) that seem no less than a menu card in a restaurant. For example, Facebook/WhatsApp the world’s leading social networking site, have more users than the population of many of the countries combined. There is absolutely no doubt that social networks have become a part of every internet user these days and the trend is only set to increase.

Even though the use of social network web sites and applications is increasingly day by day but users are not aware of the risks associated with uploading sensitive information. The reason why cyber-conspirators depend on these networks, is because users upload their personal information that commonly include their interests, social relationships, pictures, confidential information and other media content, and share this information to the whole world via SNSs which are very easily accessible. The unemployed youth, housewives, elderly persons are more commonly using the social networking sites without knowing the risk involved. Even, the employees of any company, too, unknowingly share plethora of personal information on SNS thus putting their corporate infrastructure and data at a risk. The volume and ease of accessibility of personal information available on these sites have attracted malicious people who seek to exploit this information. Due to the sensitivity of information stored within social networking sites, intensive research in the area of information security has become an area of paramount importance. Facts reveal that the majority of social media users post risky information online, unaware of the privacy and security concerns. Social networking sites are meant to get as many as users in one place as possible on one platform and for attackers there's a lot of return-on-investment in going after searching them. The values at the core of networking sites – openness, connecting, and sharing with others - unfortunately are the very aspects which allow cyber criminals to use these sites as a weapon for various crimes. Without a careful security policy in place, the entertaining face of social networking could easily compromise on the social stature of an individual. The dramatic rise in cyber attacks in the last year tell us that social networks and their million users have to do a lot more to protect themselves from organized cybercrime, or risk failing to identity theft schemes, scams, and malware attacks.

Understanding these risks and challenges should be addressed to avoid potential loss of private and personal information[2]. Social networking definitely needs to be integrated into the information security policy and user education specially the unemployed youths, housewives and elderly peoples.

**OBJECTIVES:**

The main Cyber Crime's Security Objectives:

01. To create awareness among the users about cyber crime & its Security-aware system design and deployment.
02. To aggregate metrics and events have to be identified the cyber attack detection.
03. To create a tool to enforce a countermeasure towards cyber security.
04. To study & analyze the user behavior and awareness towards cyber crime & it's security
05. To adopt best practices & regulatory requirements for cyber crime & it's security.
06. In-time identify, protect, detect, respond & recover the data as per cyber crime's security is concerned.

**SIGNIFICANCE OF CYBER CRIME & IT'S SECURITY:**

Cyber security's significance is on the rising in nature. The society is more technologically reliant than ever before and there is no sign that this trend will slow. Data leaks that could result in identity theft are now publicly posted on social media accounts. Important secret & sensitive information like social security numbers, credit card PIN information and bank account details are now stored in cloud storage services like Dropbox or Google Drive.

Now days, every individual, small business or large multinational rely on computer systems every day. Pair this with the rise in cloud services, poor cloud service security, smartphones and the Internet of Things (IoT) and there is a myriad of cyber security threats that didn't exist a few decades ago. Governments around the world are bringing more attention to cybercrimes. GDPR is a great example. It has increased the reputational damage of data breaches by forcing all organizations that operate. The major significances are as follows subjected to:

This has driven standards boards like the National Institute of Standards and Technology (NIST) to release frameworks to help organizations understand their security risks, improve cyber security measures and prevent cyber attacks.

- It helps automate various tasks that cannot be done manually.
- It helps organize data and information in a better way and it has much more computing and calculating power than human.
- It may be the storage of important data and files.

**DISADVANTAGES OF CYBER CRIME:**

- The cyber Crime may damage your studies and social life.
- The way it distracts can deviate our thoughts and activities towards unproductive activities.
- It could cause violation of privacy.

**BARRIERS IN CYBER SECURITIES:**

- **Risk towards security**: With increasing use of SNSs, the associated security risks are also increasing tremendously. Some of the security risks are identity theft, phishing, scam, cyber bullying etc. People use to provide their personal data on SNSs like facebook, twitter etc. This data is stored in SNS and due to lack of proper security techniques implemented in SNSs, it is not absolutely secure.
- **Identity-theft**: Some of the attackers attack through the application in which they ask permission for accessing the information provided in the profile of SNS. When a user allows to do so, they get all the information and can misuse that easily without the user knowledge or permissions.

- **Phishing**: Phishing in SNS began in 2007. The purpose of phishing is to harm economically that is the phishers try to retrieve the profile information to know about the banking or the financial information of the users.
- **Profiling Risk**: Profiling risk is the risk associated with profile cloning. The attackers retrieve the personal information of the users and make a clone of the profile [2]. They do so to make their social image bad or for other purposes like knowing about friends of victims. This is the most popular security risk associated with the SNSs because it is very easy to do without the permission of the user. There is nearly no security for profile cloning in SNSs. There is another way of profile cloning that is "cross-site profile cloning". In this the attacker steals information from one social networking site and uses this information to make a profile on another social networking site[3].
- **Fake Product Sale**: the attacker sometime gives offer for selling their products offering high discount to the customer. By clicking on the advertisement, they ask to give the relevant information about themselves. By doing so they can retrieve all the information to misuse of it.

**CYBER HACKING SCENARIOS:**

- **CBIR(Content based Image Retrieval)**:In this scenario, the attacker can know the location of a user by matching the patterns of the images associated with the profile of the user. Thesetypes of attacks are done to know the current location of the user [4].
- **Click jacking**: This is another type of attack scenario in which attacker posts some videos or post to the victim and when victim clicks on the page, some malicious actions are performed [3]. This is common in Facebook with the name like jacking that is when a user likes a page, a picture or a video the user is trapped by the attackers. This type of attacks are done to do malicious attack or to make some page popular.
- **Neighborhood Attack**: The neighborhood attacks are done by the attackers by knowing the victim's neighborhood. [4] It means the attacker knows the friends of the victim. Attacker uses the relationship among these friends and based on this relationship tries to identify the victim.
- **New attack Strategy, Watering Hole:**

**PREVENTIVE MEASURES:**

- **Limit the "amount"** - Limit the amount of personal information you post. Do not disclose information such as your residential address or information about your upcoming schedule or your daily routine. Also be considerate when posting information, including photos, videos and other media content. Internet is always "public" – Always remember that anything that you post on the internet is always available to the public. Thus, it is your responsibility to post information that you are comfortable with anyone seeing. This includes your personal information and photos you post and those in which you are tagged in. Also, once you post information online, you can't delete it. Even if you remove the information from a site, cached versions remain on the world wide web and also on other people's computers that may be later retrieved as well[5].
- **Beware of frauds**- The thing which makes it really easy for people to misrepresent their personal identities and motives in internet. It is always recommended to limit the people who are allowed to contact you on these sites. If you interact with unknown persons, be cautious about the amount of information you reveal or even agreeing to meet them in person. Common sense should prevail and dominate in such situations no matter how alluring it may appear.
- **Always have doubt in doing something**–you should not believe in whatever is written there in online. People make many mistakes and do post false or misleading information about different topics, including their own identity information. This is not necessarily done with a malicious intent since it

could be unintentional, an exaggeration of any topic, or simply a joke that one may misinterpret. Take appropriate precautions, think twice, and make sure, you verify the authenticity of any information before taking any action. As said before, common sense should matter more.

- **Setting management**: One should be always stay updated with the site's privacy settings. The default settings may allow anyone to see your "profile", but there is an option to change your settings to restrict access to only certain people. Sites may change their features periodically, so make sure you review your privacy/security settings regularly to make sure that your choices are still appropriate. Beware of third-party applications - Third-party applications may provide entertainment or functionality, but use caution and common-sense when deciding which applications can access your personal information. Avoid applications that seem suspicious, and make sure to modify your settings to limit the amount of information which the applicants can access.
- **Password protection scheme**: One account should be protected by the strong password which cannot be guessed by others easily. If your password is easy and accessible, someone else may access your account and pretend to be you or can do virtually anything on your behalf, without your knowledge. Combining capital and lowercase letters with numbers and symbols creates a more secure password. We should use different password for different account because Different password for different accounts always confuses the cyber-criminals. Keep software, particularly your web browser, up to date - Install the latest software updates so that attackers cannot take advantage of known problems or vulnerabilities. Almost all operating systems and software offer automatic updates. If this option is available, it is always recommendable to enable it[6].
- **Use an Anti-virus**: Anti-virus software helps protect your computer against known viruses. Since the new virus is continuously created by the attacker, it is important to keep your virus definitions upgraded. Making sure that onehas the latest security software, web browser is the best practice against online threats.
- **Keep an eye on your children**: Children are more commonly and more easily caught to the threats in social networking sites. Although many of these sites have age restrictions, children are smart enough to misrepresent their ages so that they can join. By teaching children about internet usage, being aware of their online habits, and guiding them to proper and safe sites, parents can make sure that the children become responsible and safe internet users.
- **Once posted, it cannot be removed**: one should be aware of his social reputation on these networks. When one post anything online, it stays online even if he is not able to see it. It is always advisable to think twice before posting pictures which wouldn't want the parents or future employers to see. Recent research found that 70% of job recruiters rejected candidates based on information they found online.
- **Create an online reputation**: A recent research conducted by Microsoft also found that recruiters respond positively to a strong, attractive personal brand online. So, show the smartness of one, thoughtfulness and creativeness to create an impression on prospective recruiter.
- **Know and manage your friends:** One should not consider online friend as a real friend unless he has met them personally or have spent some time together. Beware of what one share with these "pseudo-friends". If one is trying to create a public image like blogger or expert, create an open profile or a "fan" page that encourages broad participation and also limits personal information. Use a personal profile to keep your real friends more synched up with your daily life.
- **Be open if you're uncomfortable**: we should make our demand very clear if we are uncomfortable in any situation like If a friend links you to a post and it makes you uncomfortable or you think it is inappropriate, ask them to remove it immediately. Likewise, stay broad-minded and co-operative if a friend asks you to remove something you posted that makes him or her uncomfortable. People have different tolerances and sentimental levels. Respect those differences.

- **We should Know what to do:** If someone is harassing or threatening you, then there are so many ways of dealing with them make sure you use proper measures to remove them from your friends list, block them from the list, or report them to the site administrator using proper channels[7].
- **When in doubt, take the safer path:** Cyber-criminals compromise your computer by sending links in emails, tweets, posts, and online advertising. If it looks suspicious, it's best to delete or if appropriate, mark as spam and reporting to others as well through proper channels and be a responsible internet citizen.
- **Other Ways to Secure an Account**: Typing a username and password into a website isn't the only way to identify yourself on the web services you use. Some authentication uses more than one form of authentication to verify an identity. Some examples are facial recognition, iris recognition, voice ID, and finger scanning. Two-factor authentication uses a username and password and another form of identification, often a security code in the form of a "Captcha", or likewise[8].

**RECOMMENDATIONS**:

The recommendations are given to secure the information of the user:

- ✓ Company should make a policy for mails so that the mails are not confused with any other spam mails or phishing.
- ✓ Antivirus of good quality should be made by the company so that it can filter and block the malicious website.
- ✓ At every level of the website, authentication should be done so that to avoid attackers from access gain of the user's personal information.
- ✓ Cryptography based techniques should be used to ensure the security of the user's information provided on social networking websites. Group key exchange, data mining, encryption are some of the examples which can be used to enhance the security on social media.
- ✓ Training and educational programs should be done by the government to spread the awareness about cyber security. The Government should conduct publicity campaigns and programs which includes seminars, contests, exhibitions about cyber security.
- ✓ Social Networking Sites which have the privacy security setting discusses the tools which are available to make the account more secure.
- ✓ Communicate data breaches among the users
- ✓ Appoint a data-protection officer in the relevant areas
- ✓ Require user consent to process information in details
- ✓ Anonymize data for privacy and secrecy
- ✓ The requirement to notify those affect as soon as possible
- ✓ Let the government know as soon as possible
- ✓ Pay some sort of fine

**CONCLUSION**:

Today due to high internet penetration, cyber security is one of the biggest need of the world as cyber security threats are very dangerous to the country's security. Not only the government but also the citizens should spread awareness among the people to always update your system and network security settings and to the use proper anti-virus so that your system and network security settings stay virus and malware-free. Here is only solution for the privacy of social networking site is to have proper knowledge about the networking site and also adequate knowledge so that no one can fool you. Don't post anything which you would want to hide from a stranger. Be careful who you add as a "friend" since there's simply no way of verifying a user's actual identity online. We have proposed an architecture for secure communication between the users and a secure request-response architecture for exchange of information between the users. Keep your system clean and updated. Keep your senses open while using the internet and never jump to conclusions. Analyze the content thoroughly before doing anything. And remember, there are no free lunches

in this world. And, internet is no different. As growing popularity of the Social Networking Sites, these have become a prime target for cyber-crimes and attacks. Unemployed youth, house wives and elderly peoples who are staying alone in the house are more prone to such cyber criminals. Cyber-crime is becoming a widespread and posing a major threat to the national and economic security. Both public and private institutions in sectors of public health, information, and telecommunication, defense, banking, and finance are at risk. So, the organizations should take proper security measures to be safe from cyber-crime and the users should protect their personal information to avoid and identity theft or misuse. The cyberspace is becoming a significant area for cyber-crimes and terrorist to attack on crucial information. So, there is a need for universal collaboration of nations to work together to reduce the constantly growing cyber threat.

**REFERENCES:**

01. Self study during PhD under guidance of Dr. KHALEDA REHMAN, Assistant Professor & Research Coordinator of JRU, RANCHI(JH)

02. Markus Huber, Martin Mulazzani, Edgar Weippl "Social Networking Sites Security: Quo Vadis" IEEE International Conference on Privacy, Security, Risk and Trust.

03. Michael Lang, Jonathan Devitt, Sean Kelly, Andrew Kinneen, John O'Malley, Darren Prunty"Social Networking and personal Data Security: A Study of Attitudes and Public Awareness in Ireland" 2009 International Conference on Management of e-Commerce and e-Government.

04. EsmaAimeur, SebastienGambas, Ai Ho "Towards a Privacy-enhanced Social Networking Site" 2010 International Conference On Availability, Reliability and Security.

05. Dolvara Gunatilaka "A Survey of Privacy and Security Issues in Social Networks"www.cse.wustl.edu/~jain/cse571-11/ftp/social/index.

06. http://abcnews.go.com/Technology/apple-hacked-similar-attack-facebookdata-breached/story?id=18539110

07. http://pewinternet.org/Commentary/2012/March/Pew-Internet-SocialNetworking-full-detail.aspx

08. http://blog.tweetsmarter.com/social-media/spring-2012-social-media-userstatistics/