Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 07 Issue 02
2024

Research Article
https://doi.org/10.56979/702/2024

A Comprehensive Review on Challenges and Prevention of Cybercrimes in Social Media

Rana Adeel[1*], Syed Asad Ali Naqvi[1], and Gohar Mumtaz[1]

[1]Faculty of Computer Science and Information Technology, Superior University, Lahore, 54000, Pakistan.
[*]Corresponding Author: Rana Adeel. Email: ranaad071@gmail.com

Received: April 12, 2024 **Accepted:** August 21, 2024 **Published:** September 01, 2024

Abstract: Social media is no doubt a great source of communication in today's modern world but it has various advantages and disadvantages. Because of its widespread usage cyber-attacks on social media becoming the major risk for data security. Attackers use new technologies such as AI and other tools for performing attacks on social media leading to more cybercrimes on social media. Therefore, the understanding of cybercrimes and their counter techniques are very important to address this challenge. The goal of this paper is to analyze the causes of cybercrimes, and their preventive techniques, and propose new countermeasures. The paper also discusses the major reasons and challenges of these cybercrimes on social media including the lack of information, malicious users, and weak privacy measures. This paper also explores major cybercrime types including targeted, modern, and usual attacks, and also evaluates how the prevention techniques are suitable and effective in combating cyber-attacks, and proposes new preventive measures such as authentication, and privacy settings considered important against attacks. For effective prevention of attacks, there is need to develop more effective strategies to minimize the increasing number of cybercrimes on social media,a nd awareness of users are necessary factors.

Keywords: Cybercrimes; Social Media; Prevention Measures.

1. Introduction

Cybercrime is a major and increasingly important challenge. Social media platforms cause users to become vulnerable to various attacks [1]. The main reason for these attacks is that anyone can use social media so it is difficult to determine who is accessing social media with authorization. Data security is the main factor in social media. Hackers enter into the digital world through different types of attacks. Cybercrimes have negative effects on the lives of people. Most are unaware of these attacks. Different methods are used to stop attacks including authentication, face recognition, password two-factor security, and voice matching but these methods are not too good for information security. These methods have weaknesses. Recent developments have shown that there is a need for improvement in security and countermeasures. If users write passwords on paper it can also be stolen so users are not safe from attackers. Now security methods are firewalls and anti-viruses which are also not much safer attackers can bypass them and become a threat to confidential information [2]. In this paper, this study builds on cyber-crime methods on social media and contributes to their counters.

Most studies on this issue have been carried out to overcome this problem and in the past many solutions have been proposed for their mitigation [3] but cannot be successful to much extent now also the demanding increase of social media breaks all records. A study also revealed that a user goes to 6 social media sites in a month and each person consumes 2.5 hours in a day on social media people around the world spend 10 billion hours on social media sites [4]. Similarly According to the report [5] the no of users in March 2019 no of users reached 4,168,46,1500 which represents half 50 % of the world's population. Between 2019 and 2020 the no increases to 5.8%. Facebook has the largest no of users in 2023 is 2023.7 million which is more than in 2020,2021, and 2022.

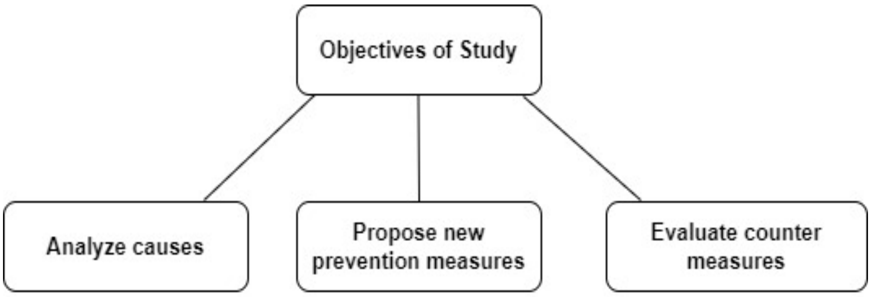

Figure 1. Objectives of Study

Figure 1 describes about objectives of this study. In this study, analyzing the causes of cybercrimes on social media is necessary for proposing effective strategies. This study also evaluates the currently being used countermeasures there are weaknesses in the current countermeasures that are also the major reason for increasing the cybercrimes. After analyzing the causes and countermeasures this study proposes new preventive strategies.

The current challenges are the security and privacy of data on which there is no compromise there are a lot of attackers on social media ready to steal confidential information this is our main challenge how to protect data from attackers on social media and one main factor is user knowledge of attacks and countermeasures. The study also discusses the crimes on social media. Our main problem is the prevention of cybercrimes in social media. Research has been conducted on this topic and determined solutions for prevention from cyber-attacks. Now discuss about architecture model of research.

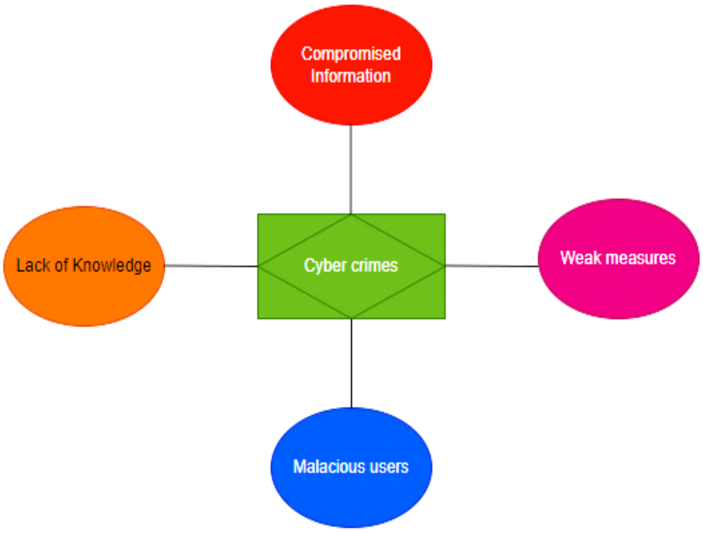

Figure 2. Reasons and challenges

Figure 2 describes about reasons and challenges for cyber-crimes. The major reasons for cyber-crimes are lack of knowledge about attacks, weak security measures, and malicious users in the form of attackers and compromised information.

New developments in this area of cyber security have also led to increasing interest in countermeasures of cyber-crimes. The preventive measures include face recognition, voice recognition, two-step authentication, scanning links, block malicious users. Discussing cybercrimes and prevention the current methods and strategies are safe to some extent but they don't provide enough information security. The main reason is the world is growing digitally faster and faster so attackers also use modern ways to attack social media sites. Regarding to this there are flaws in current technologies. Awareness is not properly given to users so users are not cautious about the security of data and attackers have more chance to attack. Secondly, social media sites need to improve their security features like improving their CAPTCHA functions when the user enters into site. Similarly, checking the security of user's connection so they can securely enter into website. Antivirus software companies use modern technologies to improve the secure scanning feature of users' computers because attacker uses some viruses that hide in files and change into the same file.

1.1. Research Goals and Questions

To fill the gap of previous research this survey paper's goal is to provide all types of attacks of cybercrimes in this paper with their prevention and countermeasures. The scope of this paper focuses on the following research questions:
RQ1: What are the methods of cybercrimes on social media used by attackers?
RQ2: What are countermeasures to prevent these attacks?
RQ3: How counter countermeasures developed more efficiently?

2. Literature Review

There are many studies done in this field. No doubt social sites are a great way of sharing data but with more users, cybercrimes are increasing day by day. The main question of research is determining ways of cybercrimes on social media and their counter. So now take a review of previous studies which validate our question.

The investigation done in the [6] discussed the methods for stopping cyber threats. The authors highlighted cybercrimes like Phishing, Scams, identity theft, Malware, Cyber casing, cyberbullying, etc. along with their countermeasures. This investigation showed that most frauds occurred due to users using social media sites and sharing more information so attackers get a benefit to attack on them. The second is Phishing where the attacker sends emails having cloned links of organizations to get user's data, not respond to emails. The prevention is not sending data over insecure websites. The third is malware where attackers send emails containing malware, prevention is installing antivirus, focusing on the URL of websites. The fourth is cyberstalking is harassing a person by sending messages and videos, prevention is separate emails for work and home and not sharing online locations, not using the actual name. The other is identity theft to hack someone's account for personal use prevention is destroying old documents, not keeping documents in the system. Besides this, the authors also discussed other crimes like cybercasting. The authors explored the fraud is increasing day by day. Law organizations control the crimes but they face many problems. It is concluded by the authors that users must be focused on social media about their data, emails, and their accounts.

The researchers in [7] emphasized that social media is a great communication site. In this study, the authors also discussed the dangers when sharing some sensitive information or data on social sites and their preventive techniques. They combine numerous threats and their resolutions in OSNs. They conducted a survey focused on threats that are harmful to the security and privacy of data. Furthermore, they discussed the risks when sharing confidential information on social sites. In methodology, authors proposed recent criteria developed on behalf of these criteria a search technique was developed to remove biases and finalized research queries and this includes three criteria evaluation methods 1. Prepare 2. Conduct 3. Review the study. In this research, authors explained crimes like Phishing, scams, Identity duplicates, and many other crimes. The authors also emphasized that users use safer privacy like encryption, marking on data, authorization, and different fraud-determining techniques. There is a need for programs to aware users of these crimes. It is concluded by the authors that these counter methods are not very safe there is a need for a model or system that detects all frauds and first user accounts go through these systems to verify.

The authors in [8] explored how the problematic use of social media is related to cyber fraud, in their research, they use the factors of LET and RAT to find the relation between PSMU and cyber victimization. They used a data collection approach in Finland in 2017. Firstly, the authors focused on the relation between problematic use and victimization. In this approach, they targeted Finland's population aged from 18-74. Secondly, focused on effects by examining if the increase in problematic usage increases victimization. The other studies showed that the three are positive and negative effects of social sites. The researchers stated that previous studies were only based on Youngers. The study by the authors showed two concepts 1). More use of social media is equal to becoming targeted 2). the association between more uses of social media and targeted users is based on three factors 1). Relation with attackers 2). Risk factor 3). Target attracters. The dependent variable is whether the users become victims of cybercrime or not. Five questions are used for that 1. Targeted by threat 2. Accused online 3. Target with accused material online. 4. Account steals. The independent variables were PSMU and increased use of social sites determined based on a scale named compulsive scale (CIUS). The results of the First stage are cybercrime increases as PSMU increases. Their results revealed that more use of social media allowed more people to become targeted and using every day has the probability of 40 % for becoming target.

The authors in [9] stated that social media crimes increased nowadays. Cyber harassment is discussed in this article and its counter methods. The investigation done by the author showed cyberbullying is much more on social media so they built an intrusion detection system. The system can log in, like posts, and comments, and share data. In the methodology, author used the techniques like picture detection, posting detection, and emotions related to posts. The emotion technique analysis used in this algorithm was applied to posts based on text. The system discussed was developed in Django framework and Convolution neural networks are used in this system. This system alerts the persons when they submit bad comments on posts if it has happened then their account will be sealed. This system also does not allow users to post bad images on social media. The author argued the system is based on sign-based ID's which determine only familiar threats. Results revealed that this system bans users from using the system if their unethical or illegal posts, comments, and pictures increase the limits.

Table 1. Comparison with existing papers.

Different Threats	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	This Paper
Spam	✓	✓	✕	✕	✓	✓	✓	✓	✓	✓	✓
Phishing	✓	✓	✕	✕	✓	✓	✓	✓	✓	✓	✓
Cross-site	✕	✓	✕	✕	✕	✕	✕	✕	✕	✓	✓
Bulgary	✕	✕	✕	✓	✕	✕	✕	✕	✕	✕	✓
Malware	✓	✓	✕	✕	✓	✕	✕	✕	✕	✓	✓
Identity theft	✓	✓	✕	✕	✓	✓	✓	✓	✕	✓	✓
Clickjacking	✕	✓	✕	✕	✕	✓	✕	✓	✓	✓	✓
Fake profile	✕	✕	✕	✕	✕	✕	✕	✕	✕	✕	✓
Inference	✕	✕	✕	✕	✕	✓	✕	✕	✕	✓	✓
Cyber stalking	✓	✕	✕	✕	✓	✕	✕	✕	✕	✓	✓
Cyber grooming	✕	✕	✕	✓	✕	✕	✕	✕	✕	✓	✓

The authors in [10] discussed cyber safety, attacks, and education about threats. The author used the methodology of literature review. The author's main goal is to find Cyber threats, Factors damaging security How much user has the education of threats, How users behave on threats on social media, and Counter methods. The author used the methodology of having 4 4-step flow diagram. They found only 2500 relevant articles but only 339 were supposed to screen and 170 articles were evicted from the list due to abstracts not related to the specific criteria of authors, 160 articles were searched and 126 were extracted due to excluding criteria, 69 articles were found most relevant. The study conducted by authors showed that there are numerous attacks like harassment, profile stolen, scams, Duplicate data, attacks through malicious data, etc. The study explored that users are not too much protected by a higher rate of attacks. The author focused on that users are responsive to attacks because they have the power to control them. They discussed factors that affect the knowledge level of attacks the user's age, their qualifications do not matter or matter.

The authors in [11] explored how the privacy of data is compromised, its effects on users' communities, and how to stop such crimes, various techniques discussed in his paper. The authors argued social sites are a great way of communication among people. If users show negligence on social sites then they become vulnerable to the dangers of cybercrimes. The authors discussed some of the cybercrimes which are phishing (Use of emails and websites from organizations to get sensitive data) and identity thefts (Getting other's social security numbers, and cell numbers without his/her authorization). Profile matching crime (creating a copy of someone's profile to fool his/her friends and family members). Clickjacking attack (Users click on a website another page opens like that page and the attacker gets data). They also discussed about prevention of these attacks. Data leaking is the most common crime so awareness in businesses is important to stop these attacks. To make the application safe run the application through a scanner for checking SQL injection attacks. Attackers use spyware to get data of users so they must be aware of spyware and not follow unsecure links. Users must not connect to unsecured networks like WIFI is a common way to steal a person's data. It is concluded by the authors that users must be aware of attacks, the author emphasizes the harms of attacks on the community, and user data needs to be safe.

The research conducted by the authors in [12] argued the cyber-attacks on social sites and discussed the prevention against these threats in this paper. The authors highlighted most users visit different sites to communicate with others to share data, photographs, and other stuff. The authors explored the main threats and prevention methods. Internet no doubt provides greater ease but also gives criminals a great way to conduct social crimes. Social sites have positive and negative effects on users spending most of their time on social sites which results affects their personal lives, employment activities, and students their study. The author explored how cyber-attacks can be divided into two types privacy privacy-related threats which include people's sensitive data on sites that attacker uses for their advantage. Second is a traditional network threat which has two security problems one is the safety of user and second is the safety of their data in the systems they are using. Some preventive measures are discussed as developing awareness among users, empowering awareness, using stronger authentication, using antivirus methods and the security of networks need to be stronger. It is concluded by the authors that increasing social site usage gives attackers more ways to attacks like phishing, and Trojan horses.

The author in [13] highlighted the threats of social sites, Anti-threat methods, and prevention techniques. They emphasized social media sites are a medium for sharing data, communicating with each other, and used for many other purposes. No of users increasing every day so they are unaware of risks and threats on social sites. The authors discussed some social sites some as Facebook which is more popular on which users share their profiles, data, and other stuff. Twitter is also the most famous site where people share tweets, news, and other information. Threats related to network sites are phishing main purpose of phishing is to duplicate the login of other users and use it for their benefit. Key logger attacks in which the attacker records the keystrokes of a person's computer and then analyzes them to find passwords. Clickjacking is an attack in which the attacker sends some photos, and videos so person clicks on it some malicious actions occur. The study conducted by the authors was based on online searching methods and most of the cyber-attacks occur due to users' unawareness. In findings author explored that Facebook has 61 % of danger. Facebook users share data, photos, location, and access to some apps or software so their privacy is compromised. In terms of ratio adults aged 18-29 are at risk of threats majority of them lose their sensitive data and people between the ages of 30-39 lose their bank details, and 23 % become harassed. Strategies There must be awareness programs about attacks and their prevention to users. The authors concluded Government agencies must take strict actions and monitor the events on social sites. Must implement strong security steps, anti-virus, and use strong safety tools.

Authors [14] highlighted the social network effects on people, discussing social issues related to privacy in this paper. They emphasized Social media no doubt is everywhere people are using different sites and sharing information. The no of users increased a few years ago and increasing day by day. The research conducted by authors revealed that Web 2.0 and the internet made social media a big invention. They revealed that big change in social media after 2001 when an experiment on broadband was conducted in Britain where for the first time network sends data ten times higher. The authors highlighted that the issue of social privacy and threats is related to the identifiability and connection of information available in a social environment. The authors explored threats has two types one is conventional in which users face threats since using social sites and the second is modern in which attackers use modern techniques for attacks. The authors discussed threats like scams, and hacking which are everywhere users receive links dangerous sent by attackers and they click on them. They discussed the example of the company VEVO where employees become victims of data breaches and LinkedIn Phishing scams. Moreover, they also discussed physiological attacks in which the attacker poses a real person's identity and uses this for attacking. The authors emphasized that for prevention use strong privacy settings across accounts, carefully select data for public access, use two-step authentication, avoid opening unfamiliar links, and install data from official resources. It is concluded by the authors that social media is an important source of information but increasing users on social media are unaware of threats so mainly protection of information is the responsibility of users.

The research conducted by authors in [15] discussed the social platforms, online social networks (OSN) threats, privacy data issues, guidelines and prevention methods of various threats, and existing solutions in this paper. The authors revealed that social media is a great platform to share ideas, and information with each other. Information on social networks spreads very fast but more information leads to privacy issues, attackers try to attack and steal data from users. With increasing cyber threats they proposed some solutions which are Phishi ARI for phishing detection, spam detection, and GARS a technique used to prevent cyber grooming. The benefits of OSNs are social connections and professional relations. They also discussed the negative effects of OSNs which include the selling of private information, isolation means a person's real life is affected, and addiction. The threats are divided into three categories modern, conventional, and targeted. Traditional threats are spam, malware, and phishing, modern threats are cross-site scripting attacks where a user's browser is attacked by an attacker and sent the malicious script to a server, profile cloning attack to clone the profile of the user, and hijacking to take control of user account for fraudulent activities. The authors also emphasized using prevention methods involving the use of strong passwords, minimizing location sharing, be careful with friend's requests. It is concluded by author's that user's lack of awareness causes cyber threats so we must monitor events on social networks and improve security measures with the latest technologies.

3. Concepts and Characteristics of Cybercrimes & Social Media

3.1. Social Media

Social media is a platform where people can communicate with each other, and share data like videos, photos, text, etc. Users can communicate with each other eliminating barriers of geographic locations, and distances. The popular social media sites on the internet are Gmail, yahoo mail; Microsoft-related sites, software and Hotmail, Skype, WhatsApp, Instagram and Facebook, etc. There were 4.3 billion users in 2021 who are using social media which is more than 55 % of the population. The growth increased from 13.7 percent from 2020 to April 2021 [2].

3.2. Cybercrimes

Cybercrimes are tasks performed by attackers to perform various attacks on social media sites for their malicious purposes to obtain users' sensitive information. Attackers use different types of attacks like phishing, malware, scams, and other types of crimes [16].

3.3. Types of Cybercrimes

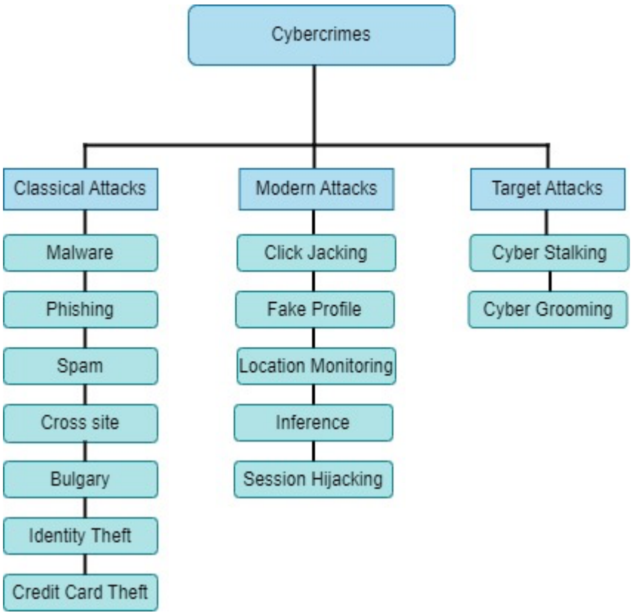

Figure 3. Classification of Attacks

3.3.1. Classical Attacks

Malware: Social media despite its benefits also provide harmful effects to users attackers hide viruses in their links, and attachment files and send them to users when users open these links, files then their computers become infected with a virus called malware. According to Sophos developer of antivirus, 40% of users are infected with malware. Microsoft also observed that 19 million PCswere infected with rogue viruses. Sophos surveyed 500 million companies and 70 % percent of companies were anxious about their security issues [6]."In 2019, based on the Symantec ISTR, a substantial reduction can be seen in newly developed malware variants during the 2018 period, but Emoted a form of banking Trojan malware aggressively showed a great increase in its market share from 4 percent in 2017 to 16 percent in 2018" [5].

Phishing: The most common attack in the world. It involves sending links to users containing some attractive content so the user becomes attractive and opens the link so the virus enters into his/her computer and is trapped. The attacker asks for confidential information. The main goal is to obtain information from users and use it for its purposes. The phishing attack consists of five stages which include planning, setting up, execution, fraud, and post-attack stages [7]. It was the most common attack in 2020 and became double in the next year [4].

Spam: The most common crime every day is when malicious users send messages email to targeted users. Email is the most common method of spreading spam messages. Information about victimized users can be obtained from companies and other sites. So it becomes easy to send spam messages to those users. Spam is known as conventional fraud [15]. Nowadays attackers also send ad messages to users to attack their confidential information [5].

Cross-site scripting attack: It is also the most common attack on web browser pages. Many web pages are malicious but users cannot predict whether it is secure or not. In this attack, attackers inject harmful code into web pages when users visit that web page on their browsers the harmful code executes into user browsers the code is injected in the form of JavaScript [7]. The user goal is to obtain user login credentials, browser history, and user's sensitive information.

Identity theft: This is also the most common crime in which attackers steal the identity of users like their driving licenses, social media accounts, credit cards, and mail identity thefts that are common. Attackers use this information to obtain benefits against targeted users. Identity theft is on top of complaints in 2020 [4]. Attackers attack the applications that are used by users and when an application requires access attackers have access to their contacts, gallery, and many other permissions so in this way attackers steal their sensitive information and use them for their benefit.

Bulgary via social media: Users post their day-to-day activities on social media so attackers find their targets and they get time to burgle the property of victims. According to a report by BBC robbery of 10 million USD cost jewelry from Kim Kardashian last year is the most familiar example of this type of crime. She was robbed in Paris at gunpoint before returning to New York [6].

Credit card theft: Credit card theft is also common nowadays. Attackers try to steal information, credit card pins, passwords, and other confidential details and then steal all money. Attackers create fake/clone stores online and advertise on different sites users become victims of these stores and give their information so attackers get information related to credit card details and other sensitive information misuse this [6].

3.3.2. Modern Attacks

Clickjacking: It is the most common modern attack. The attacker uses some techniques to create a virtual or duplicate page and upload it onto the original website page this virtual page is just a layer of user interface that contains login and password and some other links when the user clicks on the page fill in the login details the page takes the user to attackers legitimate website in this way user becomes stole in attackers website. The attacker uses the information to their advantage. In this attack, the attacker shares photos, videos, and files when the user clicks on it some actions occur [12].

Fake profile: In this attack, the attacker creates many fake profiles of the user, harming the user. This attack was used to start the Sybil attack. Users or attackers have various cloned friends in a fake identity profile; so the likings can be increased and increases familiarity on social media. In this type of attack, an attacker sends messages to targeted users, collects sensitive information spreads information as spam. If the user has many friends and anyone accepts the attacker's request then all other friends will be affected. This attack can reduce the value or reputation of users and spread false information [7].

Location monitoring attack: In today's era, everyone is using social media but users share their location on social media to update others about their current activities. There is a drawback in that users set the privacy setting but attackers still compromise the accounts.

Inference attack: Users also share some statistical data on social media including either company's data or their data. Some sensitive information users do not want to share but attacker uses data-extracting methods on the network layer to obtain sensitive information and gain insights into user or company businesses [11].

Session hijacking attack: This attack occurs when a user enters his name and password into the system for using the system called session. So the request goes to the server and the user logged into the system session starts so the attacker authorizes the session by different methods to show that it is that user. The attacker can do anything after accessing the session [17]..

3.3.3. Targeted/Victimized threats

Cyberstalking/bullying: Cyberstalking/bullying means torturing someone on social media by sharing his/her images, and disturbing messages so the victim becomes emotionally harassed. Due to this the users feel stressed, anxious, and physically disturbed. January has been considered National Stalking Awareness Month since 2004 which leads to determining the effects of stalking and helping victims to get comfort from depression, stress, and fear of cyberstalking [4]. A survey conducted revealed that 6 to 7.5 million people become stalked in the USA. The people aged 18-24 are highly stalked [4]. The difference between these two is cyber stalking means malicious users keep monitoring social media user accounts attack user accounts and send him/her messages through social sites to disturb the target [15].

Cyber grooming: Cyber grooming is an attack less discussed in previous papers. In this attack, the criminal-minded attackers made contact with children on the internet and built emotional connections with the child's future intentions to obtain sensitive information. Attackers take fake identities of children and get in contact with other children they are unaware threat attackers use them[18].

4. Counter and Preventive measures

This section discussed prevention and countermeasures that users must take while using social media because the majority of attacks are done due to user negligence. So in this case we discussed various preventive and counter techniques as discussed below:

4.1. Authentication mechanism

Authentication techniques are considered to be most effective in previous research. Empowering this mechanism decreases the risk of social media attacks [12]. In WhatsApp, there is a verification code, in Facebook accounts there is also a verification code. Similarly in other social media sites, the same kinds of authentication mechanisms are working. There are three authentication-based techniques as discussed in [7]. These are

- Hashing: It is used for devices with low cost, and limited resources and requires less computational power.
- Proxy-based techniques: It is used for communication between users and uses asymmetric encryption.
- Certificate mechanism: Making sure about the nonrepudiation of digital signatures.

4.2. Privacy settings

The protection of data and information from unauthorized access, attacks, and users on social media or internet-related technologies is called prevention or prevention. It is necessary to take preventive measures otherwise social media becomes a place for criminals. The measures are important for cyber-crime prevention. First of all, messages, and data. Use antivirus, and firewalls activated and updated. Use strong passwords. To prevent Cyber bullying/stalking minimize the amount of data on profiles. To prevent Phishing attacks using additional security and more popular technique is using one one-time password where the user gets a one-time password and CAPTCHAS [4]. To prevent malware use antivirus software. To prevent identity theft use passwords of long length, monitor the account regularly, and use three-factor authentication, algorithms for that is logistic regression [4]. Updating antivirus, and firewalls [19]. Use a random session ID to make it difficult for the attacker to guess the session ID [20].

5. Discussions and Insights

RQ1: What are the methods of cybercrimes on social media used by attackers?

Cybercrimes are becoming a major issue not only in social media but also affecting other fields including IoT, cloud computing, etc. Various types of attacks including targeted, classical, and modern threats are evolving at a fast rate and affecting users everywhere on the internet. User awareness is one of the major issues leading to cybercrimes. So there is a need to give knowledge to users about these various types of attacks to prevent them from the attacks.

RQ2: What are countermeasures to prevent these attacks?

There are many countermeasures to prevent attacks but these measures are not suitable or sufficient to prevent attacks. As the technology is increasing, and evolving at a fast pace attackers also use AI to do attacks these attacks avoid the common security measures and do some damage to data. With the advent of AI, the attacker uses AI to perform some attacks and generate some malicious codes so this type of attack is not detected by common security measures including firewalls, antiviruses, passwords, CAPTCHAS, signatures, etc. So there is a need for strong preventive measures.

RQ3: How counter countermeasures developed more efficiently?

The recent countermeasures based on studies are not providing much safety to user's data. Due to evolving technologies such as AI, these measures need to be developed more effectively to prevent attacks. One of the major reasons is awareness among users most of which are unaware of attacks. So, there is a need for training sessions, to promote secure practices among users. Moreover, developing effective measures also uses AI technologies to improve security against attacks.

6. Conclusion

Social media is becoming the major platform for communication, information sharing, and for other businesses. Despite its benefits, cybercrimes on social media are also increasing day by day. This study highlights the important cybercrimes on social media and their defensive mechanisms and techniques to eradicate them. Cybercrimes are evolving in nature attackers use new techniques such as AI and tools for targeting users on social media. The objectives discussed in the study are to determine the causes of these cybercrimes, and their prevention techniques, and propose new counter-measures. Moreover, the study also discussed the reasons and challenges for these cybercrimes that impact cybersecurity behavior the major challenges discussed are malicious users on social media, weak privacy measures, and compromised information. The countermeasures are also discussed in this paper including authentication mechanisms and privacy settings. For effective prevention against the attacks, there is a need to develop more effective countermeasures to minimize the ratio of attacks.

References

1. G. Kaur et al., "Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime," Engineering Proceedings, vol. 62, no. 1, Art. no. 1, 2024, doi: 10.3390/engproc2024062006.
2. E. Etuh, F. S. Bakpo, and E. A.H, "Social Media Network Attacks and their Preventive Mechanisms: A Review," in Computing Advances & Trends, Academy and Industry Research Collaboration Center (AIRCC), Dec. 2021, pp. 59–74. doi: 10.5121/csit.2021.112405.
3. M. Ismailov, M. Tsikerdekis, and S. Zeadally, "Vulnerabilities to Online Social Network Identity Deception Detection Research and Recommendations for Mitigation," Future Internet, vol. 12, no. 9, p. 148, Aug. 2020, doi: 10.3390/fi12090148.
4. A. Anudini, H. Dissanayake, and G. Uwanthika, "Impact of Social Media-Related Cybercrimes and Preventive Precautions," 2021.
5. L. Almadhoor and E. Al, "Social Media and Cybercrimes," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 10, Art. no. 10, Apr. 2021, doi: 10.17762/turcomat.v12i10.4947.
6. T. R. Soomro and M. Hussain, "Social Media-Related Cybercrimes and Techniques for Their Prevention," Applied Computer Systems, vol. 24, no. 1, pp. 9–17, May 2019, doi: 10.2478/acss-2019-0002.
7. N. A. Nawaz et al., "A comprehensive review of security threats and solutions for the online social networks industry," PeerJ Computer Science, vol. 9, p. e1143, Jan. 2023, doi: 10.7717/peerj-cs.1143.
8. E. Marttila, A. Koivula, and P. Räsänen, "Cybercrime Victimization and Problematic Social Media Use: Findings from a Nationally Representative Panel Study," Am J Crim Just, vol. 46, no. 6, pp. 862–881, Dec. 2021, doi: 10.1007/s12103-021-09665-2.
9. B. K. Shah, N. Sharma, S. Bandgar, and S. Patil, "Cybercrime Prevention on Social Media," International Journal of Engineering Research & Technology (IJERT), vol. 10, no. 03, 2021.
10. T. B. G. Herath, P. Khanna, and M. Ahmed, "Cybersecurity Practices for Social Media Users: A Systematic Literature Review," JCP, vol. 2, no. 1, pp. 1–18, Jan. 2022, doi: 10.3390/jcp2010001.
11. B. Vivekanandam and Midhunchakkaravarthy, "Preventive Measures for the Impacts of Social Media Networks in Security and Privacy - A Review," JISMAC, vol. 3, no. 4, pp. 291–300, Apr. 2022, doi: 10.36548/jismac.2021.4.001.
12. S. Kumar and V. Somani, "Social media security risks, cyber threats and risks prevention and mitigation techniques," International Journal of Advance Research in Computer Science and Management, vol. 4, no. 4, pp. 125–129, 2018.
13. S. Shoro, M. S. Hyder, and S. N. H. Kazmi, "Social Media Security Risks and Cyber Threats," International Journal of Computer Science & Emerging Technologies, vol. 2, no. 1, pp. 33–37, 2018.
14. A. Shabani and I. Gashi, "Social and privacy threats in social networks, challenges and the most critical issues," ijhs, pp. 5578–5586, Oct. 2022, doi: 10.53730/ijhs.v6nS8.13545.
15. A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," Complex Intell. Syst., vol. 7, no. 5, pp. 2157–2177, Oct. 2021, doi: 10.1007/s40747-021-00409-7.
16. G. Sunil, S. Aluvala, S. Reddy, R. Dadi, and R. Varun, "VARIOUS FORMS OF CYBERCRIME AND ROLE OF SOCIAL MEDIA IN CYBER SECURITY," pp. 2709–2715, Jan. 2020.
17. I. O. Ogundele, A. O. Akinade, and H. O. Alakiri, "Detection and Prevention of Session Hijacking in Web Application Management," International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, no. 7, pp. 1–10, Jul. 2020, doi: 10.17148/IJARCCE.2020.9601.
18. "Cyber Grooming," ChildSafeNet. Accessed: Feb. 02, 2024. [Online]. Available: https://www.childsafenet.org/new-page-15.
19. M. Singh, C. Verma, and P. Juneja, "Social media security threats investigation and mitigation methods: A preliminary review," J. Phys.: Conf. Ser., vol. 1706, no. 1, p. 012142, Dec. 2020, doi: 10.1088/1742-6596/1706/1/012142.
20. A. Baitha and S. Vinod, "Session Hijacking and Prevention Technique," International Journal of Engineering & Technology, vol. 7, p. 193, Mar. 2018, doi: 10.14419/ijet.v7i2.6.10566.