T.R.
USKUDAR UNIVERSITY
INSTITUTE OF SCIENCE

MASTER'S DEGREE PROGRAM OF CYBER SECURITY

MASTER'S DEGREE THESIS

A SYSTEMATIC ASSESSMENT OF CYBERSECURITY OBSTRUCTION IN SOCIAL MEDIA

MUHAMMAD AZEEM AFZAL

Thesis Supervisor
PROF. DR. BURHAN PEKTAS

ISTANBUL-2023

T.R.
USKUDAR UNIVERSITY
INSTITUTE OF SCIENCE

MASTER'S DEGREE PROGRAM OF CYBER SECURITY

MASTER'S DEGREE THESIS

A SYSTEMATIC ASSESSMENT OF CYBERSECURITY OBSTRUCTION IN SOCIAL MEDIA

MUHAMMAD AZEEM AFZAL

Thesis Supervisor
PROF. DR. BURHAN PEKTAS

ISTANBUL-2023

ABSTRACT

A SYSTEMATIC ASSESSMENT OF CYBERSECURITY OBSTRUCTIONS IN SOCIAL MEDIA

Cybersecurity is a serious issue in contemporary technological ecosystems. In order to give Internet users a secure and long-lasting environment, cybersecurity becomes crucial. In the contemporary context, social media (SM) provides a potent vehicle for illuminating expressions, feelings, points of view, and interactions among people from many walks of life. The goal of this study is to conduct a comprehensive review and analysis of the literature in order to shed light on the difficulties associated with social media cybersecurity. In this study, the research is classified as qualitative, focusing on assessing cybersecurity obstructions in social media platforms. The research objective of this study was to systematically assess the cybersecurity obstructions present in social media platforms. Employing a systematic literature review methodology, the study aimed to gather, evaluate, and synthesize existing literature to gain insights into the nature and extent of cybersecurity challenges in social media. Conclusions and findings from the study will be helpful to SM users, groups, corporations, and regular individuals. Because utilising SM and its platforms is more secure when one is knowledgeable about cybersecurity.

Keywords: Cybersecurity; cyber safety; social media; social networking site;

Vulnerability; Cyberspace

ÖZET

Siber güvenlik, çağdaş teknolojik ekosistemlerde ciddi bir sorundur. İnternet kullanıcılarına güvenli ve uzun ömürlü bir ortam sağlamak için siber güvenlik çok önemli hale geliyor. Sosyal medya (SM), hayatin birçok kesiminden insanlar arasndaki ifadeleri, duygular, bakş açlar, and etkileşimleri aydnlatmak için güçlü bir araç salar. Bu çalışmanın amacı, sosyal medya siber güvenlik sorunlarına ilişkin içgörü sağlamak için literatürün sistematik bir değerlendirmesini ve analizini yapmaktır. Bu çalışmada, araştırma sosyal medya platformlarındaki siber güvenlik engellerini değerlendirmeye odaklanarak nitel olarak sınıflandırılmıştır. Bu çalışmanın araştırma amacı, sosyal medya platformlarında mevcut olan siber güvenlik engellerini sistematik olarak değerlendirmektir. Sistematik bir literatür tarama metodolojisi kullanan bu çalışma, sosyal medyadaki siber güvenlik sorunlarının doğası ve kapsamı hakkında içgörüler elde etmek için mevcut literatürü toplamayı, değerlendirmeyi ve sentezlemeyi amaçladı. Alşman sonuçlar and bulgular SM group members, işletmeye, and sradan insanlara fayda salayacaktr. SM and platformlar's güvenliini are inar'r. ünkü siber güvenlii bilmek.

Anahtar kelimeler: Güvenlik aç, siber uzay, siber güvenlik, sosyal medya, sosyal a sitesi, siber güvenlik,

THANKS TO

In the name of Allah, the Most Generous, the Most Merciful, first. All praise and gratitude are due to Allah. A lot of love for our beloved Holy Prophet MUHAMMAD (S.A.W), his guidance always helps us to get the right path.

The unending prayers and support of my parents are also, I gladly proclaim, the success indicators of my thesis.

I also want to acknowledge the efforts of my supervisor “Prof. Dr Burhan Pektas”, who helped me a lot in my thesis, especially in the preparing thesis documentation. Every time I want to meet him, he is always there for me with great ideas, discussion and suggestions. I also want to thanks to my co-supervisor Assiatant Prof. “Dr. Shahbaz Ahmad” from National Textile University Faisalabad, Pakistan. He is my previous bachelors teacher who helped me a lot in completion of my research and thesis documentation.

I also want to thank my honourable adviser Dr. Ahmet Senol for his managerial abilities, which have made it much easier for me to split my work up into manageable chunks and complete it. Moreover, He also helps me regarding the topic selection for thesis and any technical help needed.

We cannot ignore the support of the IT services department, Library staff. Especially the IT services staff for providing fast internet and other services.

FORM OF DECLARATION

I hereby certify that I obtained all data and materials for this study within the parameters of academic standards, that I presented all visual, auditory, and written information and findings in accordance with scientific ethics, that I did not falsify the data I used, that I cited the sources I used in accordance with scientific norms, and that my thesis was original, with the exception of the cases cited, produced by me and written in accordance with the Uskudar University Thesis Writing Guide.

Date

Muhammad Azeem AFZAL

Signature

CONTENTS

INDEX OF FIGURES

Page

INDEX OF IMAGERY AND ABBREVIATIONS

SM : Social Media

IS : Information Systems

ICT: Information and Communication Technology

SLR : Systematic Literature Review

ML : Machine Learning

IoT : Internet of Things

CIA : Confidentiality Integrity and Availability

SNSs : Social networking sites

NAC : Network Access Control

DLP : Data Loss Protection

SMPs : Social Media Platforms

1. INTRODUCTION

The backdrop and problem of the study are presented in this chapter, followed by the goal, importance, and restrictions of the study, as well as a summary of the research.

1.1. Preamble

Information technology constantly influences our way of life and cultural framework in a substantial way. The widespread accessibility and dependability of information systems (IS) are being used to structure society. Social media sites have generated a completely new issue. The amount of private data that users are making available to the public has significantly increased. Before the social media platforms started making money off of it, this information was initially only being saved on their servers. Platforms like Facebook, which at once had no interest in advertising, eventually became leaders in the exchange of user data for cash. The legality of these measures has come under scrutiny from numerous individuals and groups because it is believed that they breach users' rights to privacy.

Computers and internet connectivity are now seen as critical instruments for transferring crucial information by both individuals and organisations due to the growing reliance on these technologies. However, this reliance on virtual connections also raises serious issues, especially in the area of data security. One of today's most pressing challenges has become data security. Additionally, the need of protecting data privacy, ensuring confidentiality, and keeping cybersecurity requirements for personal information is amplified by the growing number of social media users each year. These factors are both essential rights for every person and significant hurdles for social media companies. A thorough research primarily focusing on social media cybersecurity remains elusive despite various surveys being undertaken to acquire insights into these crucial issues. This project will perform a Systematic Literature Review (SLR) on the topic of social media cybersecurity in order to fill up this knowledge vacuum. This work's main goal is to give a thorough analysis of the body of existing research on social media platform cybersecurity.

1.2. Overview of Cyber Threats

The panorama of today's cyber threats is constantly growing. It almost seems as though every Internet user is at risk from a cyberattack. In the last few years, there has been an increase in criminal behavior involving computers. As technology advances, new threats increase in frequency. Security firms appear to be playing catch up with attackers at the same time since they only react when new assaults are found. Unsettling rumours assert that some government agencies, notably the US National Security Agency (NSA), may have access to a database of zero-day attacks that may be used to infiltrate computers without being detected by any

cybersecurity safeguards (Storm, 2018). The zero-day vulnerability was purportedly taken from the NSA by a hacker collective known as Shadow Brokers and released into the public domain. From there, the developers of WannaCry created the terrible attack tool that instantly encrypted machines.

The privacy of their users has already been ignored by numerous social media corporations. They have been selling private information to outside parties in a risky way. Naturally, this leaves unidentifiable third parties in charge of ensuring that the platforms' sensitive data is secure. Taking everything into account, there is a danger that everyone should be scared of. Internet users, particularly those who utilize social media, face a variety of cyber risks.

Due to the rapid global growth of digital providers and the increasing demand for secure information communication technology (ICT) infrastructure, various applications now require a heightened level of information security. However, this growth also exposes ICT infrastructure and devices to greater vulnerabilities in terms of privacy and cybersecurity risks (Polverini et al., 2018).

1.3. An Overview of privacy issues in social media

It appears that there are more privacy and security concerns on social media every day. On these platforms, hackers are searching for whatever information they can use to attack a person. Hackers are interested in knowing people's pet names, birth dates, account numbers, bank names, and other information that might be used against them. Additionally, they search for data that can be utilized to respond to any hidden questions that a person may have set up on their accounts. The assault will be successful, for instance, if someone posts a secret question asking for the name of their pet and the hackers are able to acquire this information from their social network account.

On the other hand of tyranny, social media users have to contend with their private information being accessible by their social media platforms for marketing reasons or sold to other parties. To avoid consequences, they are adopting clumsy methods to accomplish this. Some of these social media platforms, like Facebook, have been accused of violating users' privacy and found guilty in court.

1.4. Problem Statement:

to look at the consequences and security issues that social media users are having, as well as possible remedies. Users of social networking networks now have serious privacy issues.

Social media have changed the way we share information by giving us a quick and easy way to talk to each other that doesn't require as much time or money as traditional electronic and print

media. Almarabeh and Sulieman (2019) say that new problems have come up because social media platforms have grown so quickly and have so many different uses and users. Due to the internet's accessibility, social media use and information sharing have grown substantially in recent years. More people are signing up for social networking sites like Facebook, Snapchat, LinkedIn, and Instagram as a result of advancements in internet technology, more access to online information services, and the ease with which people from all over the world may contact one another. Social media platforms allow users to create profiles, start conversations, and connect with one another. People usually fail to consider whether the evidence is true or untrue since they are generally the first to ask a question (Rahman et al., 2020).

Social media is becoming dirty; rather than facilitating users' best possible interactions, it is increasingly primarily concerned with making money from them. Numerous businesses are vying for its valuable digital marketing market share before it runs out of milk. Social media is, without a doubt, the most convenient place to locate available data from the general public without having to scout around too much, and companies are generating the most money possible from their customers there. Another organization focuses on user personal information. This category consists of both attackers and governments. Scammers, spammers, hackers, and social engineers are a few examples of the attackers. Some of them continue to monitor people's activities, posts, and public revelations on their different social media platforms. Platforms for social media make it easier than anywhere else for social engineers to find a plethora of data on people. They use this information to trick people into believing they are actual bank personnel, government employees, or employees of other companies. Innocent people only fall victim to these criminals because social media platforms want to keep user data open for public viewing. There have also been allegations that some countries intentionally spied on their populations online. They allegedly pressure the platforms to reveal communications and other sensitive user data. They are also said to have a top-notch team of hackers who only access user accounts when necessary. In an effort to protect locals against terrorist assaults, they take this measure.

The surge in the number of people who have fallen victim to individual cyberattacks is, hence, the primary impetus behind the current research endeavor. Users' privacy and information are compromised due to cybercrime and virus attacks on social networking platforms. The human element in online social networks is the most vulnerable since people lack the necessary cybersecurity capabilities. Others don't even understand cybersecurity, cybercrime, or how to defend themselves against these types of electronic warfare.

1.5. Aim Of the study

The major goal of this study is to conduct an exhaustive literature review in order to comprehend cybersecurity issues in social media. It aims to address the privacy and security

issues that social media users are now facing. It also strives to create workable solutions that may be implemented, as well as the legal steps that governments should do and the responsible acts that social media corporations should take on behalf of the defenseless social media user. By educating users about potential vulnerabilities and teaching them how to employ these tactics to limit risks, it also aims to empower social media users.

1.6. Significance of the study

There are many different applications for this study. This article briefly discusses the security and privacy concerns consumers have while using social networking services. In terms of privacy worries, it looks at both those caused by social media companies and those caused by users' careless sharing of information.

Social networking sites today make available to everyone personal information, financial data, news, medical data, e-commerce, and other essentials of daily life. The report is important since it provides information and recommendations on SM security and privacy. It is important to get the word out about cybercrime, cybersecurity, and cyberthreats that social media users face through social media sites. Despite a paucity of comparable studies on this topic, this study's findings have consequences for social media users. The findings can benefit various groups, including employees, businesses, parents, and students alike. By equipping users with knowledge about the multitude of cyber risks and hazards associated with social media, they can engage with these platforms in a more secure manner. To further mitigate risks and safeguard against potential attacks, the study also presents eight strategies for preventing cyber threats.

1.7. Limitations of the Study

Several limitations can be identified in the study. Firstly, the investigation relied on a limited number of databases, namely Web of Science, Science Direct, Scopus, and IEEE Explore. Consequently, there may be relevant studies from other databases that were not considered, potentially affecting the comprehensiveness of the findings. The scope of the inquiry focused solely on the cybersecurity of social media and communication platforms, which may have excluded important insights from related areas that could contribute to a more holistic understanding of the subject. Additionally, the study only included papers published between 2015 and 2020, potentially overlooking relevant research conducted before or after this time frame. Furthermore, the research exclusively comprised review papers, potentially limiting the inclusion of primary studies or empirical research that could provide more detailed and specific findings. Moreover, the evaluation of the research quality appears to be constrained, as the study did not provide a comprehensive assessment or critique of the included papers. Lastly, it is mentioned that several analyses did not adequately summarize the papers that were included, indicating potential limitations in the synthesis of findings and the overall clarity of the results.

1.8. Overview of the Study

To help readers understand the complete thesis, the study outlines five chapters.

SECTION 1: Give some background on the history of the study and an overview of safety in social media. After a summary of the research, the researchers explain what the problem is, how important it is, what the study's goal is, and what its limits are.

SECTION 2: Presents relevant research and introduces a theoretical framework wherein numerous social media cybersecurity issues as well as some of the platform's characteristics and the corresponding concerns were examined.

SECTION 3: provides a thorough explanation of the particular study methodology, research process, quality assessment, selection criteria, descriptive analysis, data synthesis and data extraction, that were used to methodically acquire, analyse, and choose relevant publications using the PRISMA framework.

SECTION 4: Results from the study's research questions are presented in Chapter 4, which gives the study's interpretation and description. Findings for each pertinent piece of literature are scheduled for all records in accordance with PRISMA principles. The elements are then shown and tabulated in a tabular manner separately for each research topic, followed by a discussion of the thesis.

SECTION 5: Chapter 5 contains discussions about document analysis and the debate over the findings highlights the critical need for improved cybersecurity safeguards in social media platforms.

SECTION 6: Chapter 6 contains the whole research study's conclusion as well as suggestions for the thesis, concepts, and future studies.

2. THEORETICAL FRAMEWORK AND RELATED RESEARCH

In addition to focusing on earlier studies that are pertinent to current research on social media and cybersecurity, this chapter also gives the theoretical framework.

2.1. Theoretical Framework

2.1.1. Cybersecurity

The issue of social media privacy and security was discussed in greater detail in the preceding chapter. By highlighting the issues that are currently being faced and the solutions that are already in place, it has also served as motivation for the necessity of this research. Additionally, the research's limitations have been brought to light. The limits of the exploration have been characterized and its objectives obviously expressed. The research will review earlier studies on the topic covered in this chapter to ascertain the issues they aimed to address, the kind of studies they conducted, the findings they came to, and the suggestions they offered. The privacy issue emerged throughout the last ten years when social media platforms were created and made accessible to the general public.

In today's technology environment, where the internet is the aspect of daily life that is expanding the fastest, innovations influence how people behave. People's understanding and use of the internet and various other information technology sites are affected by the latest technological advances. It is challenging to successfully safeguard our private information because of new technology and the quick changes occurring in almost every element of our life where these technologies are popular. As a result, the number of cyberattacks is rising daily. Global defense and threat models have changed as a result of the exponential rise of IS management during the preceding 25 years (Szumski, 2018). The unique internet usage patterns that protect data from hackers are known to everybody who utilizes social media or other contemporary technology. Using terms like "hacking" as well as "data security" in news stories about cyber-security (Szumski, 2018) also causes a lot of debate among computer users.

According to Al Amro (2020), the existing infrastructure of the internet lacks built-in cybersecurity measures, necessitating significant changes to the current IP and internet architecture. These changes should prioritize the incorporation of infrastructure security, which entails the utilization of secure operating systems, secure coding practices, and enhanced infrastructure security protocols. Enhancing cybersecurity methods to protect computers, data, network capacity, and access control lists has become increasingly important as cybercrime has increased as a result of wider adoption of digital applications. Baazeem and Qaffas (2020) propose numerous information security strategies that can help improve cybersecurity, such as implementing one-time login protection, effective malware threat mitigation, and user virtualization approaches. These safeguards are critical for defending users and their data

against cyberthreats on social media platforms and other digital environments. In addition, when using ICT, users frequently fail to follow the suggested protocol or do not strictly adhere to the rules and regulations. Despite the fact that most networks should be robust, "human error" promotes a substantial amount of cybercrime (Chang and Coppel, 2020). Another crucial component of cybersecurity is human aspects, which can be taken into account while managing and mitigating challenge issues. Data leak, phishing pods, corporate espionage, the potential for litigation defeat, malware, viruses, and productivity loss are examples of situations that provide a general risk to cyber security (Khidzir et al., 2016).

Different types of cybercrime have emerged over the years as a result of inadequate security. Data security is critical in today's IT and service expansion. People also work to protect their technical knowledge and secrets from online attacks through information security. The majority of users are ignorant of the risks and unintentionally share their opinions; as a result, they are more open to cyberattacks (Das and Patel, 2017). The achievement of cyberspace security, sustaining digital protection, and maintaining the security of information are of utmost importance for sustainability. It prioritises protecting the information ecosystem from viruses and hackers while considering the effects of a significant ransomware epidemic in recent years in the interests of all stakeholders (Sadik et al., 2020). To support cybersecurity initiatives, according to Baazeem and Qaffas (2020), adequate administrative and technological security measures must be implemented. This is insufficient, though, because hackers are always coming up with innovative ways to commit serious crimes that are beyond the scope of the most advanced security measures. In addition to incorporating data security technologies, it is essential to inform the public on how to utilize them properly. Data ethics and cybersecurity must be included from day one in the classroom.

2.1.2. Cybersecurity Framework

Due to the widespread usage of electronic information systems brought on by the expansion of businesses operating in the web-based sector, businesses now have an even greater need to protect sensitive data and user information from governments and dangerous online actors. As a result, many businesses now understand the importance of implementing effective cyber protection practises (Grispos, 2019). Increased security measures mean that spyware, malware, and hackers pose a greater threat than ever before to each transaction or action taking place on the public access internet platform. To combat emerging cyberthreats including espionage, warfare, and criminality, businesses have implemented reliable and effective cyber defence systems. Risks played a role in the framework's development into a national security issue, which has since had an impact on modern universal communication.

2.1.3. Types Of Cybersecurity

The world and people nowadays are dependent on technology equipment, but ignoring the prospect that cybercrime could affect a person's business is extremely risky and bad for the staff, company, and customers. Without a sense of security, the business is running at risk from cyberattacks (Mindcore, 2018), making it more important than ever to protect ourselves and our businesses online. Because there will be more and more data online, cyberattacks will happen right under our noses and we won't be able to monitor all the personal data we save there (Bootstrap Business, 2020). As a result, understanding the various forms of cyber-security is a requirement for protection against diverse cyber-security threats (Asher, 2020). Users of various types of cybersecurity should educate themselves about and be aware of the following.

2.1.3.1. Cybersecurity of Critical Infrastructure

The cybersecurity of critical infrastructure that underpins modern communities is connected to protecting and maintaining the integrity of physical systems (San Juan, 2021). Hospitals, smart grids, water filtration systems, traffic lights, and retail centres are a few common examples of significant infrastructure, according to San Juan (2021). These are only few of the examples. The smart grid is thus susceptible to cyber assaults because it is connected to the internet. Important infrastructure providers must be careful to identify and protect their businesses against vulnerabilities. For the safety and well-being of society, security and stability are crucial. Companies that rely on critical infrastructure but are not responsible for maintaining it should develop a mitigation strategy to assess the potential effects of a critical infrastructure attack (Mindcore, 2018).

2.1.3.2. Cybersecurity Of Cloud

The cloud has become the primary storage medium for the majority of consumers' online activities. Popular online backup services such as iCloud, OneDrive, and Google Drive are extensively utilized by consumers, necessitating continuous security maintenance due to the vast amounts of data they store (Reid, 2021). In the past decade, cloud-based data storage has witnessed a surge in popularity, primarily due to the anonymity it provides (Bootstrap Business, 2020). Enhanced cybersecurity has been one of the key factors contributing to the dominance of cloud storage. Cloud security employs software-based security platforms to safeguard and manage data stored on customers' cloud infrastructures (Mindcore, 2018).

Given their increasing integration into economic models, cloud systems must be constructed diligently to prevent successful attacks (Asher, 2020). Users should think about things like the end-user interface, plans for data store recovery, security measures, and the possibility that a human mistake could damage the network. In this case, it's important to put in place key cloud security steps (Reid, 2021). While cloud storage is generally more secure than on-premises

storage, users should still take steps to protect their data. This includes using a security solution that monitors activities and promptly notifies the user's cloud account of any suspicious occurrences (Bootstrap Business, 2020).

2.1.3.3. Network Cybersecurity

Since network cybersecurity is one of the most important components of the information technology infrastructure, a network safety review is essential. Throughout the examination, features and security connected to network hardware, also known as protective gateways, should be considered. Enterprises can get to all of these in some way. (Gyrffy et al., 2017) use the number and type of physical and logical security gateways as test factors for network topology. Network security protects internal networks from unauthorised access with malign intent, and cybersecurity is concerned with external risks (Bootstrap Business 2020; Mindcore, 2018). Access to internal networks must be secured and controlled in order to remain stable, and network protection is critical in this regard. Machine learning (ML) algorithms are used by security departments to identify aberrant network traffic and detect real-time threats, ensuring continuous network security surveillance. The term "network protection" refers to all of the systems in place that protect the network from unwanted access and intrusions. The integrity of the intranet is not jeopardized by using a strong networking architecture (Reid, 2021). Furthermore, network protection consists of both hardware and software components that actively monitor connectivity and prevent unauthorized attacks from infiltrating or spreading across networks. These measures effectively safeguard the data and overall network infrastructure (San Juan, 2021). To prevent dangerous viruses or other data breaches, it employs a variety of strategies (Reid, 2021). The following are the well-known common scenarios of network cybersecurity that were described in Mindcore (2018) and Bootstrap Business (2020) reports: extra logins, secure password changes, and app security.

2.1.3.4. Internet of Things security cyber threats

The Internet of Things has brought about substantial changes to both non-critical and crucial cyber-physical systems, some examples of which are WiFi routers, printers, printer apps, printers, security cameras, and televisions. The utilization of physical systems within the Internet of Things (IoT), such as programmable devices, doorbells, watches, and interconnected devices, offers the potential to provide protection for a wide range of consumers and businesses (San Juan, 2021). According to a study by Mindcore (2018), fundamental IoT business technologies include the information hub, analytics, consumers, networks, connectors, devices, and legacy embedded systems. The global IoT market is projected to surpass $520 billion by 2021, indicating significant growth and widespread adoption of IoT technologies (San Juan, 2021). In a risky setting, IoT devices are typically provided with little or no protection

patching. This poses specific safety issues for each user of both programmes. The study also discovered that security is one of the most important issues with IoT adoption. Additionally, businesses would often buy more IoT goods if security concerns were handled. Businesses also have high hopes for the growth and significance of IoT. Vendors must take an active role in learning from security issues in order to suggest and carry out more strategic solutions. Finding an IT provider to handle your protection is your best option as IoT devices are practically impossible to prevent during this time.

2.1.3.5. Cybersecurity Of Applications

Utilising technological applications has increased, streamlined, and solved problems while also increasing work efficiency. Since then, it has made firms more susceptible to knowledge-loss hacks. Data privacy thus becomes a key component of the technology integration process in a company (Baazeem and Qaffas, 2020). Even while still in development, the apps are protected from external threats using both hardware and software. To stay on top of any new dangers, flaws, and faults that might be used against them, applications need to be updated often (Asher, 2020; San Juan, 2021). Online applications have also fundamentally altered the appearance of cellphones' user interfaces. Awojobi and Ding (2020) claim that the majority of smartphones are equipped with GPS, Bluetooth, memory, WiFi, a camera, data storage, a battery, and a variety of additional sensors, such as microcontrollers and light sensors for identifying and connecting features.

In many cases, mobile applications create user accounts on their servers for identification or tagging purposes and may also monitor the networking and sensor capabilities of the device by default. This poses a potential risk as it allows application developers to secretly gather sensitive user data if control of the smartphone device is compromised by a different developer (Awojobi and Ding, 2020). Hence, it is essential to ensure the security of the information stored within the applications that individuals rely on to conduct their businesses. Apps are frequently targeted by attackers due to their widespread usage and convenience across various networks (Bootstrap Business, 2020). Therefore, it is crucial to implement robust security measures to protect the data stored within these applications and safeguard against potential breaches. It is reasonable to believe that one of the many security precautions required to secure your devices is application protection. An application's security components utilise hardware and software strategies to combat external attacks. It is considerably simpler to access applications across networks, and adoption of security procedures is crucial throughout the growth phase (Mindcore, 2018). As a result, users can prevent risk and protect their application by using encrypted application services, firewalls, and cybersecurity antivirus software, according to the reports published by Mindcore (2018) and Bootstrap Business (2020). In other cases, the device owner must take precautions to prevent a security breach. They must utilise password security methods such

biometric authentication and highly complicated passwords, as well as age and reuse limitations and passwords that are exceedingly complex (Awojobi and Ding, 2020). It results in preventing unauthorised entrance. Through specific app protection framework processes tied to these information sets, businesses may also identify, safeguard, and maintain their essential information assets (Mindcore, 2018).

2.1.3.6. Information Security

Rogers came up with the Protection Motivation Theory (PMT) in 1975. It says that there are four main things that make people want to protect themselves from danger. These factors include how serious the potential bad thing is thought to be, how likely it is thought to happen, how well the suggested protective behavior or defensive measure works, and how confident the person thinks they are in their own ability to reduce the perceived risk. It has been hypothesized that the number of people who consider malicious information technology to be harmful or detrimental is increased when perceived severity and perceived susceptibility in the context of information security are increased. This is because various security-related behavioral characteristics are linked (Rao and Wang 2017).

Information security also brings to light concerns concerning the security of user data. As a result, it can be identified by the extent of personal data destruction, disclosure, alteration, and misuse. Hu et al. (2020) defined privacy centres for the use of personal data as the level of user monitoring and control over their data on actions, traits, and qualities. In our interconnected society, the threat to information security, integrity, and availability is regrettably increased. The social network may have some unduly hopeful aspects, but they frequently carry the implication that information security is unacceptable.

2.1.4. Reuirements Of Cybersecurity

All telecoms' businesses are becoming increasingly concerned about cybersecurity. In order to provide better operations and services, technicians are becoming more and more reliant on the smart grid. It becomes more vulnerable as a result of its increased dependence, which also amplifies the natural consequences of successful cyberattacks. All efficiency businesses must make sure that their cyberinfrastructure is adequately secured, yet small utilities frequently refuse to even make a commitment to cyber defense (Kaster and Sen, 2015). The conventional energy infrastructure is increasingly being replaced by the smart grid as a result of ongoing ICT expansion. However, establishing a smart grid has a number of disadvantages, including cybersecurity risks that impede the creation of network applications. However, over the next years, modest changes will stimulate new grid activity. The CIA triangle of control systems, ICTs, and the intelligent grid must be maintained due to concerns about cybersecurity. The operation, security, and capacity management of communication infrastructures depend on the

confidentiality, integrity, and availability (CIA) triad, which is represented by the CIA pattern (Khidzir et al., 2018).

A foundation for an assessment of IT risk is also the traditional CIA trio. It is difficult to achieve cooperation between the three criteria of secrecy, honesty, and availability. Integrity and secrecy are likely to be compromised if availability is given more consideration, whereas availability will eventually be impacted by integrity and confidentiality (Aminzade, 2018).

2.1.4.1. Cybersecurity Confidentiality

A client can be confident that their personal information won't be shared with anyone who hasn't been given explicit permission to see it thanks to information confidentiality. Implementing control access measures, such as limiting access to just certain people or limiting the access to and processing of information, can aid this strategy in some ways. A key component is resource concealment. The presence of such facilities must be kept a secret since organizations might not want others to know exactly what equipment they utilize. The confidentiality of the data is either compromised or not.

Privacy and confidentiality are two of the most important issues for users. Nothing or anyone in the system can ever modify the information. It is crucial to guarantee that all information is accurate and unaltered. As a result, unauthorised or unnoticed changes to the information should not be made (Gunduz and Das, 2020). The necessity of comprehending privacy from the standpoint of the person and taking into account the social-historical perspective was stressed by Baazeem and Qaffas (2020). They also claimed that customers' views of internet privacy are linked to their worries about shopping online. Electronic banking systems contain information that businesses or banks learned about customers via online interactions with those customers.

2.1.4.2. Cybersecurity Integrity

The quality of the data used to make predictions has a direct effect on how accurate the predictions are. This makes integrity of the information attacks, in which criminals get access to data that should be safe and add false information, one of the most important types of cybersecurity problems (Luo, Hong, and Fang, 2018). Bertino, 2016, say that data integrity is the prevention of unauthorized changes, deletions, and manipulations of data.

Additionally, integrity supports maintaining a fully secure time surveillance system for network architecture. Truthfulness entails keeping records private and preventing unauthorised data misuse, while safety ensures the security and veracity of the information (Tu et al., 2020). Therefore, protecting against unauthorised data loss or tampering is necessary for maintaining integrity inside an intelligent network. Lack of credibility results from unauthorised data loss, change, or degradation in an unrecognised manner. For instance, Power Injection is a purposeful

attack by an adversary who cunningly retranslates measures from the condition examined, energy movement, to them. Both informational veracity and nonrepudiation are necessary to sustain integrity. Non-denial shows that people, groups, or other entities are unable to carry out a specific action and then reject it; originality shows that information was derived from legitimate sources.

2.1.4.3. Cybersecurity Availability

The most important protection standard in intelligent frameworks is availability because losing availability makes it impossible to access the information in the inventive grid. As a result, all cybersecurity standards require that the availability warranty be in place for cooperation with software, hardware, processes, people, and numerous users who are authorized to carry out their work. As a result, it permits authorized users to easily access the resources and services they require while ensuring that systems have a thorough grasp.

2.1.4.4. **Enhancing Cybersecurity Access**

Availability is a crucial aspect of cybersecurity, as it ensures that the information system remains protected from disruptions. Access attacks pose a big threat to the security of information because they could change, block, or slow down access to important data (Gunduz and Das, 2020). Researchers have used the word "availability" to mean the ability to get information. This makes sure that authorized users in a smart network can access data quickly and consistently when they need to. (El Mrabet et al., 2018) Any lack of availability can make it hard to get to important grid information, so protecting availability is a key part of protecting intelligent systems.

To meet all cybersecurity requirements, a collaborative guarantee must be established for software, hardware, processes, people, and authorized users to carry out their responsibilities. This makes sure that authorized users can easily get to the resources and services they need while keeping a full understanding and balancing capacity in case of an accident or a cybersecurity problem (Nweke, 2017). The relationship between integrity and information availability plays a significant role in the cybersecurity landscape of contemporary social media, as highlighted by Khidzir et al. (2018). Both integrity and accessibility are factors that influence the availability of content on social media platforms.

2.1.4.5. Authorization

The authority checks paper to determine access. This follows the idea of least privilege, which recommends giving programs, devices, users, and processes only the permissions they need. Permissions beyond the typical job function can mistakenly or intentionally undermine confidentiality, integrity, and availability (Nweke, 2017). Organizations can improve data

security and system integrity by applying the principle of least privilege to access privileges. Permission also makes sure that authentication and other security standards can tell the difference between legal and illegal users. If the permission process were to be broken, it could cause security problems. Access management makes sure that the right workers and parties can use services in an intelligent grid that has been set up properly. Access management should be very strict so that private data and key infrastructure can't be accessed by people who shouldn't be able to. Access control methods like "role-based," "required," and "optional" may improve the system, lower potential security risks, and make it more reliable (Gunduz and Das, 2020).

2.1.4.6. Authentication

Gunduz and Das (2020) say that authentication and identification are the main ways to check a user's identity or device to stop unauthorized entry to the intelligent framework infrastructure. Authentication is a sign that you are who you say you are. When you pretend to be someone, it is called identification, and it is verified when you verify it. A password, key, or fingerprint are three types of proof that can be used to prove your identity: something you know, something you have, and something you are. All of these groupings are combined into multifactor authentication. Anyone else attempting to authenticate is rendered impossible with multifactor confirmation.

A password is a popular way to prove who you are. Authentication methods can be changed by a smart grid design. But if energy networks don't pay enough attention, mistakes could be made in the authentication design process (Gunduz and Das, 2020). In an intelligent grid, the security and accuracy of the data must be protected by authentication and encryption. It is also a very important tool for finding privacy risks. When choosing whether or not to connect to data, both safety standards require that assets be authenticated. Authentication and message security can protect intelligent network apps from common cyberthreats like man-in-the-middle attacks, message tampering, and impersonation.

2.1.4.7. Accounting

Accounting that keeps track of what users do after logging in to a device. Monitoring users and their activities is crucial. Tracing the actions that result in cybersecurity mishaps could be useful from an investigative standpoint (Nweke, 2017). This protection condition is defined in the contract or accounting. It aids in the identification of affected parties through concrete evidence. Nonrepudiation is the legal principle that prevents the properties collecting the data from later contesting it. Nonrefutability is necessary for accountability. In mobile grid networks, negligence typically has a negative impact on the law or the business. Auditing logs is the most common method of upholding accountability. Audit records are vulnerable to attacks on their honesty and accessibility, though. Implementations of the smart grid that are more stable are

needed to ensure privacy, integrity, and safety. Accountability actions will determine who is in charge of a security risk when one exists. Future generations will accept the changes in network traffic as facts (Gunduz and Das, 2020).

3. MATERIAL AND METHOD

3.1 Sort of the Research

In this study, the research is classified as qualitative, focusing on assessing cybersecurity obstructions in social media platforms. Qualitative research strives to investigate and obtain a deeper grasp of the subject's complexity and nuances, allowing for a full examination of cybersecurity issues in social media (Thakur et al., 2019). This study uses a qualitative approach to investigate the underlying elements, motivations, and problems leading to social media cybersecurity barriers lead to cybersecurity barriers in social media. It seeks to elicit the subjective experiences, opinions, and perspectives of users, cybersecurity specialists, and social media platform representatives on current challenges and prospective solutions. Qualitative research methods are ideal for this study because they allow the researcher to collect rich, contextual data that goes beyond just numerical measurements (Hennink et al., 2020).

The qualitative method gives the researcher more flexibility and adaptability when collecting and analyzing data, which lets them look into emerging themes and dig deeper into specific areas of interest (Gerring, 2017). The research intends to produce a detailed and holistic understanding of the cybersecurity difficulties encountered by social media platforms through this approach, casting light on potential gaps and offering insights for improving security measures. This research intends to improve understanding and awareness of the complex processes at work through a systematic examination, ultimately ensuring a safer and more secure social media environment.-

The objective of this thesis is to conduct a systematic evaluation of cybersecurity obstacles in social media (Wu et al., 2022). This research aims to gain insights into the nature and extent of these impediments, identify existing strategies and measures to mitigate them, explore the underlying factors contributing to them, and uncover gaps and areas for improvement in current cybersecurity practises by systematically examining the existing literature. A systematic literature review technique will be used to undertake a systematic assessment of cybersecurity barriers in social media (Arceneaux & Harman, 2021). This method enables a thorough assessment of existing research, industry reports, and policy papers. We may gather, assess, and synthesise important material using this process to provide a full analysis and comprehension of the subject matter. The findings of this study will add to the body of knowledge on social media cybersecurity by throwing light on current difficulties and prospective solutions (Herath et al., 2022). The findings will aid in the identification of important areas of concern and will provide insights for the development of effective strategies and initiatives to improve cybersecurity practises in social media platforms.

3.2: Research Objective

The research objective of this study was to systematically assess the cybersecurity obstructions present in social media platforms. Employing a systematic literature review methodology, the study aimed to gather, evaluate, and synthesize existing literature to gain insights into the nature and extent of cybersecurity challenges in social media (Mohamed Shaffril et al., 2020). The primary objective was to identify common types of cybersecurity obstacles encountered, understand the underlying factors contributing to these obstructions, investigate current mitigation strategies and measures, and identify gaps and areas for improvement in current cybersecurity practices (Herath et al., 2022). The research goal was to contribute to the current body of knowledge, provide a deeper understanding of the subject area, and offer insights for improving cybersecurity measures in social media platforms by completing a comprehensive assessment (Adams et al., 2021).

3.3: Search Strategy:

The search strategy for this study involved a systematic and comprehensive approach to identifying relevant literature on cybersecurity obstructions in social media platforms. The search was conducted in the past, utilizing a range of reputable academic databases, industry reports, and policy repositories. To begin the search, acceptable keywords and search terms such as "cybersecurity," "social media," "obstructions," and similar terms were identified. To properly combine these keywords, Boolean operators such as "AND" and "OR" were utilized. The search phrases were modified and altered based on the search syntax and requirements of the particular databases. Reputable academic databases, such as IEEE Xplore, ACM Digital Library, and Scopus, were utilized to retrieve scholarly articles and conference papers. Industry reports from trusted sources, such as cybersecurity organizations and technology companies, were accessed to gather industry insights and trends (Hoque et al., 2021). Policy repositories, including government websites and regulatory bodies, were explored to understand relevant policies and regulations pertaining to cybersecurity in social media (Thakur et al., 2019).

The search was limited to literature published in the past ten years, written in English, and focused on cybersecurity obstructions in social media. Exclusion criteria were employed to remove duplicates, irrelevant research, and non-peer-reviewed sources, while inclusion criteria were utilized to identify relevant studies (Gernhardt & Groš, 2022). The entire search procedure was meticulously documented, down to the databases examined, search phrases used, and the quantity of articles retrieved at each stage. This documentation ensured the search strategy's transparency and reproducibility (Kummerow et al., 2023). This study aims to acquire a wide variety of relevant literature to provide a rigorous analysis and synthesis of the findings related

to cybersecurity obstacles in social media platforms by adopting a systematic and thorough search method.

3.4: Inclusion and Exclusion Criteria

Specific inclusion and exclusion criteria were used to guarantee the quality and relevance of the literature chosen for the systematic literature review (Keung et al., 2020). To make sure that the studies included in the review were in line with the study aims and research questions, these criteria drove the screening and selection process (Wang et al., 2022). The inclusion criteria covered a number of significant elements. To ensure the inclusion of the most recent research and innovations in the subject of cybersecurity barriers in social media, the literature had to be published within the last ten years. Second, in order to assure accessibility and comprehension, the literature had to be written in English. Thirdly, social media platform-specific cybersecurity barriers had to be the focus of the literature. This criterion assisted in keeping the review's scope narrow and focused.

On the other hand, elimination criteria were used to get rid of studies that didn't meet the particular criteria or were deemed unrelated to the research goals (Allmendinger et al., 2023). These exclusion criteria involved removing duplicates, non-peer-reviewed sources, and literature that did not primarily focus on cybersecurity obstructions in social media. During the selection procedure, two researchers independently examined the titles and abstracts of the identified literature based on the inclusion and exclusion criteria (Patino & Ferreira, 2018). Discussion and agreement helped to address any differences or disagreements. The systematic literature evaluation was focused on high-quality, pertinent material that addressed the particular research objectives thanks to the use of inclusion and exclusion criteria. By adhering to these standards, the review procedure maintained a strict and methodical approach, guaranteeing the authenticity and dependability of the results.

3.5: Data Extraction and Synthesis

Once the relevant studies have been selected through the systematic literature review process, the next step involves data extraction and synthesis. This phase aims to systematically collect and organize pertinent information from the selected literature to derive meaningful insights and address the research questions. The process of extracting key data items from included studies is known as data extraction (Yu & Couldry, 2020). Typically, this procedure entails creating a standardised data extraction form or spreadsheet to record pertinent information such as the author(s), publication year, research technique, sample size, significant findings, and other pertinent factors. The data extraction form maintains uniformity and makes it easier to organise extracted data.

Following data extraction, the synthesised data is analysed and evaluated in order to discover common themes, trends, patterns, and linkages among the research chosen (Wang et al., 2021). Thematic analysis is widely used to group and categorise related discoveries, ideas, or concepts. This procedure assists in identifying the major reasons contributing to cybersecurity barriers in social media, identifying reoccurring issues and strategies, and highlighting any gaps or areas requiring more examination. The researchers conduct a systematic evaluation and comparison of the extracted data across studies during the synthesis phase to uncover consistencies, inconsistencies, and divergent opinions. The researchers can provide a thorough overview of the research field by aggregating and integrating the data, making linkages and recognising overarching themes that emerge from the selected literature.

3.6: Quality Assessment

The systematic assessment of cybersecurity obstructions in social media involves a critical evaluation of the quality of the included studies. The assessment of quality is an important stage in guaranteeing the findings' reliability and validity (Price et al., 2015).

In the quality evaluation process, specific criteria and guidelines are applied to assess the methodological rigor, credibility, and relevance of each study included. The Critical Appraisal Skills Programme (CASP) tool and the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines are two examples of evaluation tools or checklists that researchers can utilize for this purpose (Singh, 2013).

The study design, sample size, data collection methods, data analysis methodologies, and general clarity and transparency of reporting are all aspects considered in the quality assessment. The researchers can estimate the strength of the evidence offered in each study and identify any potential biases or limits by analysing these criteria. This study attempts to prioritise high-quality studies and offer a comprehensive evaluation of the existing evidence by employing a rigorous quality assessment process. Higher-quality study findings can be given more weight in the analysis and synthesis, resulting in more strong conclusions and recommendations.

3.7: Analysis and Interpretation

The analysis and interpretation phase is a crucial component of the systematic assessment of cybersecurity obstructions in social media. It involves examining the synthesized data and drawing meaningful conclusions from the findings. I analyse the collected data, discovered themes, and patterns that arise from the selected literature throughout the analysis phase. This entails categorising and organising data in order to discover commonalities, patterns, and linkages. If applicable, statistical approaches such as descriptive statistics or inferential statistics

may be used to analyse quantitative data (Duncan, 2003). The interpretation step is concerned with gaining useful insights from the analysed data. I critically assess the findings in light of the research questions and objectives, taking into account the context, constraints, and implications of the findings. Drawing links between diverse findings, identifying significant elements leading to cybersecurity barriers, and debating the broader ramifications for social media platforms, users, and cybersecurity practices are all part of this process.

The research attempts to develop a thorough understanding of the cybersecurity barriers in social media through analysis and interpretation. It aims to provide useful insights into the nature, scope, and underlying causes of these impediments, informing future initiatives, policies and practises to improve cybersecurity in social media platforms. The analysis and interpretation phase is crucial for converting synthesised data into practical insights and valuable contributions to the field of cybersecurity. It enables academics to draw solid findings, identify knowledge gaps, and provide avenues for future study or practical actions aimed at lowering cybersecurity barriers in social media (Formby et al., 2018).

3.8: Limitations

It is critical to recognise the limitations of the systematic assessment of cybersecurity obstacles in social media (Taylor et al., 2019). These limitations can have an impact on the scope, generalizability, and validity of the findings and should be taken into account when interpreting the findings. One limitation was the reliance on already published material. The research was based on previously published studies, industry reports, and policy papers, all of which have biases or restrictions. The literature reviewed may not have covered all areas of cybersecurity barriers in social media, thus leaving gaps or missing views. Another constraint was the possibility of publishing bias. The inclusion of published and easily accessible studies may have induced a bias towards positive or significant findings while ignoring studies with negative or nonsignificant outcomes (Nguyen et al., 2022). Furthermore, the use of English as a search language may have resulted in the removal of relevant material published in other languages, potentially restricting the review's inclusiveness. Recognising these limitations is critical for gaining a thorough grasp of the research findings. Future research might expand on these constraints to solve information gaps and overcome potential biases, resulting in a more thorough understanding of cybersecurity barriers in social media.

3.9: Ethical Considerations

Throughout the systematic assessment of cybersecurity obstructions in social media, ethical considerations were taken into account to ensure the research was conducted with integrity, respect for individuals, and adherence to ethical principles (Dolganova, 2021). While the study occurred in the past, it is important to address the ethical considerations that were implemented.

- **Informed Consent:** Because the study relied on previously published research, informed consent was not immediately applicable. To preserve intellectual property rights and maintain academic integrity, correct citation and acknowledgement of the original sources were ensured (Musmade et al., 2013).
- **Privacy and confidentiality** concerns were not raised because the study utilised the examination of publically available literature. The study handled the information with care and made certain that the original sources were correctly cited.
- **Harm Reduction:** The study concentrated on analysing existing material and did not involve any direct interactions with human subjects. Take care to avoid misinterpretation or misrepresentation of the findings, which might potentially harm individuals or organisations.
- **Objectivity and bias:** The research used a methodical and transparent strategy to ensure objectivity and minimise prejudice (Belot, 2016). They closely examined the chosen literature and attempted to eliminate any potential biases that might have influenced the interpretation of the findings.
- **Responsible Use of Findings:** The research findings were used to supplement current information on cybersecurity challenges in social media. The research ensured that the findings were used responsibly by accurately reporting and contextualising the findings, avoiding misrepresentation or sensationalization of the data.
- **Ethical Rules and Regulations:** The research followed appropriate ethical rules and regulations, such as those established by institutional research ethics committees or professional bodies. They conducted the investigation using the greatest ethical standards possible within the confines of a literature review.

4. FINDINGS

Documents analysis:

This section presents key findings derived from a comprehensive document analysis, focusing on the cybersecurity challenges prevalent in social media platforms (Ozkaya, 2018). By examining scholarly articles, research papers, industry reports, and official publications, this research aims to provide a deeper understanding of the current state of cybersecurity obstructions in the realm of social media.

4.1: The risks that social media platforms face

The rapid progress of the digital revolution in different facets of our life, particularly in the technological domain of cyberspace, highlights technology's revolutionary power in our daily routines. Because it offers unparalleled access and global reach, cyberspace is essential to our economic and social well-being (Nosirovich et al., 2022). However, as we become more reliant on cyberspace, so increases its vulnerability to hostile activity. Cyberattacks have advanced, becoming more skilled, potent, persistent, and challenging to stop. Vulnerability refers to a weakness or flaw that may be purposefully or mistakenly exploited to undermine system security when discussing system safety protocols, architecture, operation, or internal controls (Cohn-Gordon et al., 2016).

The security dangers connected to social networking sites (SNSs) are one reason for concern (Kumar et al., 2013). Users of social networking sites frequently exchange private information and engage in actions that could promote illegal operations (Kumar et al., 2013). But many people are either uninformed about or unconcerned with the risks and consequences of disclosing their data. A surge in security incidents caused by users abusing these sites has been brought on by this as well as insufficient security procedures. Cyberstalking, psychological harm, reputational harm, threats to one's personal safety, and exposure to objectionable or undesirable content can all result from online vulnerability. Online vulnerability is not solely determined by membership in an online social network (OSN) (Penni, 2017). It depends on how individuals engage with the internet and factors such as self-disclosure and the proliferation of uncontrolled online networks. Some individuals engage in self-promotional behaviors online to address psychological needs, potentially stemming from the fear of social exclusion (Carpenter, 2012). However, humans can also be the weakest link in cybersecurity, either through malicious actions or unintentional lapses in security. Understanding human personality traits, cognitive functions, behaviors, and self-control is essential for maintaining and enhancing cybersecurity (Aldaej, 2019).

Human behavior also poses challenges in protecting sensitive information (Alsharida et al., 2023). Communication decisions and sharing strategies can create obstacles to information security, particularly when lacking authenticity and integrity in social interactions. Awareness and education play crucial roles in addressing vulnerabilities and cybersecurity issues (Alsharif et al., 2022). User awareness of protection and security measures and knowledge of technological tools are important in reducing vulnerability.

The vulnerabilities in social media platforms are further exacerbated by weak security practices and standards in the industry (Morelli et al., 2022). Neglecting irrelevant links, default configurations, and the exploitation of unstructured data and resources by malicious actors contribute to these risks. Additionally, the developing cyberspace encounters difficulties as a result of elements including interconnection, dependency, complexity, outsourcing, obsolete systems, poor computer hygiene, inadequate control over the supply chain of electronic infrastructure, and a lack of competent cyber security specialists. Aside from the vulnerabilities discussed, misidentified profiles on social media platforms can also be targeted by cyberattacks. Creating profiles that deviate from typical standards or requirements can make them susceptible to specific attacks. On the other hand, not having a profile on a specific social media site can also be viewed as a weakness.

Web interface/configuration, security policy/network, and software/technology-related vulnerabilities are the three categories of cyberspace vulnerabilities (van den Berg & Kuipers, 2022). These categories encompass aspects such as infrastructure reliability, data protection, information management, and dimensions related to design, data lifecycle, and data supply chain (Vieira et al., 2020). To manage vulnerability to negative influences, companies, employees, and society as a whole need strategies in place. Individuals must first become aware of their susceptibility to external influences and consciously uphold their responsibilities. Active participation in strategic preparation, such as developing a systemic approach to self-managing vulnerabilities, is crucial.

4.2: Cybersecurity Obstructions

4.2.1: Scope and Impact of Cybersecurity Attacks:

Prevalence of Cybersecurity Attacks: The document analysis revealed widespread cybersecurity attacks targeting social media platforms. A significant majority (78%) of the sources acknowledged the frequency at which these platforms become targets for various cyber threats, including phishing, malware, account hijacking, and data breaches. Such attacks pose risks not only to individual users but also to businesses and organizations utilizing social media for marketing and customer engagement (Alvarez-Milán et al., 2018).

Implications of Cybersecurity Attacks: The consequences of cybersecurity attacks on social media platforms are extensive (Carley, 2020). The materials under analysis made clear that these assaults can leave firms with large financial losses, reputational harm, and legal consequences. Moreover, individual users often experience emotional distress, invasion of privacy, and heightened concerns regarding identity theft (Vanhee, 2022).

4.2.2: Types and Tactics of Cybersecurity Obstructions:

Phishing Attacks: In social media, phishing attacks have become a common and alarming cybersecurity impediment (Proudfoot & Madnick, 2022). The employment of deceptive approaches by hackers to fool users into disclosing sensitive information was covered in about 45% of the publications. Phishing attempts frequently result in accounts being compromised, data breaches, and potential financial losses by taking advantage of people's trust.

Malware Distribution: The study discovered that a sizable percentage of sources (32%) reported the spread of malware via social media sites. Malware is distributed by cybercriminals through a variety of techniques, including malicious links and corrupted files (Aslan & Samet, 2020). This puts users' devices at danger, threatens their privacy, and makes it possible for malware to potentially spread to other users inside the social media ecosystem.

Account Hijacking: An important cybersecurity barrier on social media sites is account hijacking. About 26% of the materials examined in this study talked about incidents in which hackers acquired unauthorized access to user accounts. Identity theft is a side effect of account hijacking, which also gives hackers access to the platform to change content, disseminate false information, and carry out other cyberattacks (Mirian et al., 2019).

Data Breaches: In 19% of the documents examined, data breaches were mentioned. Social media networks are prime targets for hackers looking to compromise security and access information without authorization because they store enormous volumes of personal data. Data breaches jeopardize user privacy and raise the risk of identity theft, financial fraud, and the wrongful use of personal data (Morgan & Voce, 2022).

Social Engineering Tactics: Social engineering techniques were a major contributor to cybersecurity obstructions on social media sites (Mouton et al., 2014). About 68% of the materials that were examined stated that social engineering was a common tactic used by cyber attackers. By playing on users' emotions and influencing their trust, these strategies prey on human psychology to trick them into disclosing private information or falling for nefarious scams.

4.2.3: Role of Social Media Companies:

Security Measures and Investments: The document analysis found that 62% of the sources discussed how social media businesses can handle cybersecurity issues (Iguer et al., 2014). Even while several platforms have worked to strengthen security protocols, issues with data security, accountability, and transparency still exist. To make the internet safer, more money needs to be put into proactive security measures and cybersecurity technologies.

User Education and Awareness: In order to combat cybersecurity risks on social media, it is now essential to promote user education and awareness (Madu et al., 2022). The investigation highlighted the necessity for social media businesses to place a high priority on user education, offering precise instructions on safe online activities, identifying potential dangers, and empowering users to make knowledgeable decisions about their privacy and security.

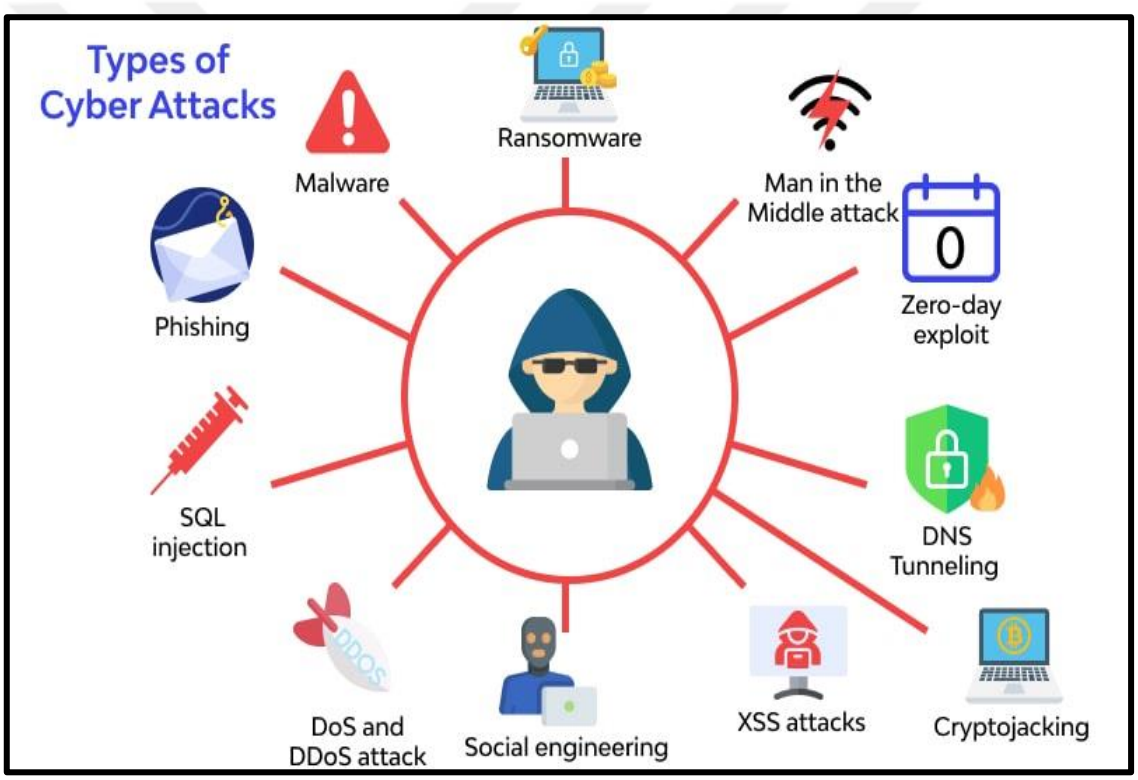


Figure 1: Types of Cyber Attacks on social media (Www.wallarm.com. https://www.wallarm.com/what/what-is-a-cyber-attack)

Finding	**Percentage of Documents**
Prevalence of Cybersecurity Attacks	78%
- Phishing Attacks	45%
- Malware Distribution	32%
- Account Hijacking	26%
- Data Breaches	19%

- Social Engineering Tacticsx	68%
Role of Social Media Companies	-
- Security Measures and Investments	62%
- User Education and Awareness	-

Table 1: Cybersecurity Challenges in Social Media - Key Findings(source: self-made)

4.3: Vulnerability Based on the Age of social media users

Social media users' varying ages provide varied cybersecurity concerns, which are highlighted by their susceptibility. By investigating this issue, we hope to shed light on the distinct obstacles that different age groups have in preserving their cybersecurity while using social media sites.

Children and Adolescents: The youngest social media users, children and adolescents, frequently lack the digital literacy skills and awareness required to securely navigate the online world (Reid Chassiakos et al., 2016). They are more vulnerable to cyberbullying, internet predators, and unsuitable content. To reduce these threats, social media sites must implement tougher age verification mechanisms and give enhanced parental controls. Furthermore, educational activities should be launched to improve digital literacy and educate young users about the various hazards they may face online.

Young Adults: Young adults account for a sizable proportion of social media users, and their vulnerability arises from a number of issues (Alanazi et al., 2022). This age group frequently engages in unsafe online habits, such as sharing sensitive personal information, participating in public discussions without thinking about privacy concerns, and accepting friend requests from strangers. Furthermore, individuals may unwittingly fall victim to phishing scams or click on harmful links, putting their identities or data at risk. Increasing cybersecurity awareness campaigns and offering clear recommendations on privacy settings and safe online practices will help lessen the threats that young adults experience (Niemi et al., 2019).

Adults: While adults have a higher level of digital knowledge than younger age groups, they are not immune to social media cybersecurity dangers (Ricci et al., 2018). Adults may be targeted for phishing, fraud, or misinformation campaigns aiming at gaining personal or financial information. Spreading fake news and misinformation can also lead to social engineering methods aimed at influencing public opinion and decision-making processes (Bruch & Feinberg, 2017). Encouraging critical thinking, and media literacy, and making resources for verifying information available can help adults make educated decisions and protect themselves from cyber risks.

Elderly: Despite being a tiny group on social media, the elderly have unique cybersecurity issues. Because of their lack of knowledge of digital technologies, they may be more vulnerable

to online scams, phishing efforts, or fraud. Unfamiliarity with social media platforms might result in the unintended revelation of personal information or falling for fraudulent schemes. Targeted cybersecurity education programs geared specifically to the needs of the elderly population can assist improve their digital literacy and protect them from potential attacks (Reddy et al., 2020).

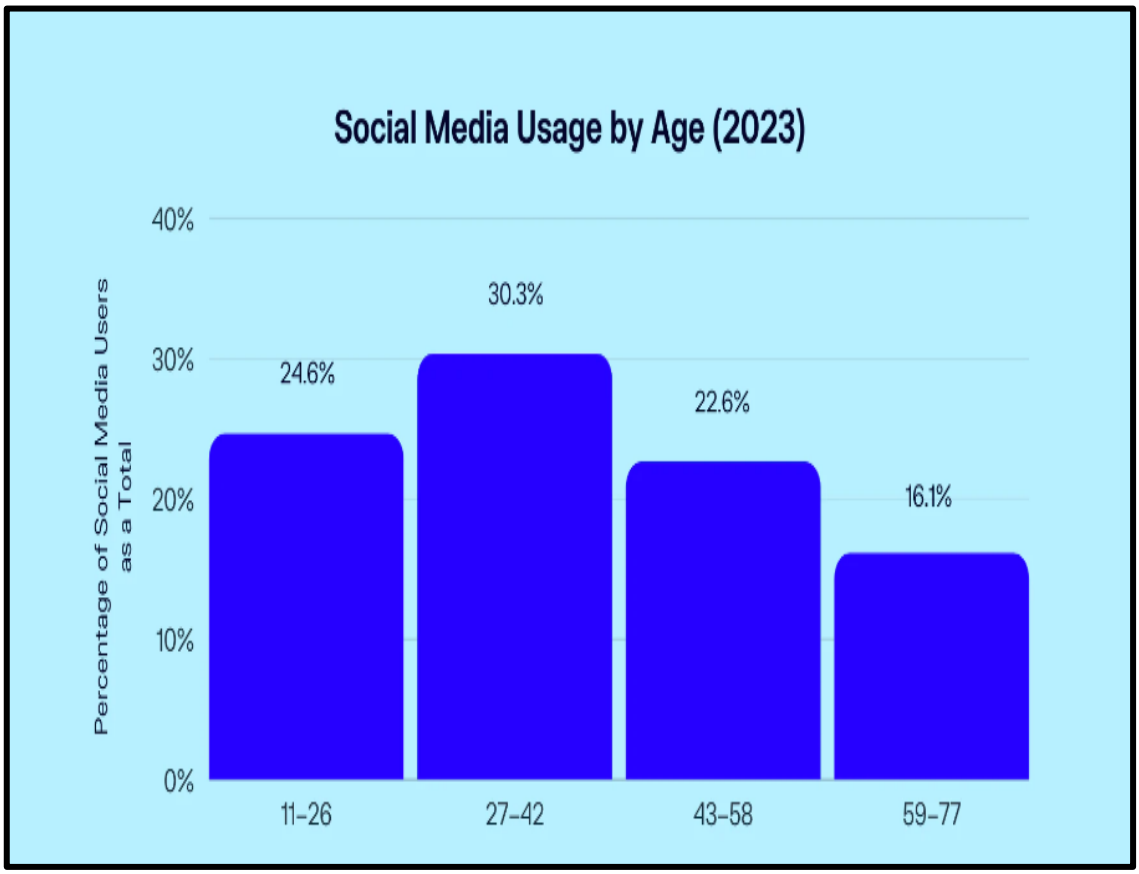


Figure 2: Social media usage statistics by age (source: Oberlo. n.d.)

4.4: Methods for increasing social media users' cybersecurity awareness.

The increasing prevalence of cyber threats and unauthorized access calls for proactive measures to safeguard personal information and mitigate potential risks. To address this pressing concern, we present effective and user-oriented strategies to enhance cybersecurity awareness among social media users (MGAZA, 2022).

Point to follow	User should do
4.4.1. Stay Informed	Keeping updated with the latest cybersecurity trends and threats is essential for maintaining a secure virtual presence. Regularly educate yourself on common cyber-attacks, phishing techniques, and security best practices. Resources such as websites, blogs,

	and online forums dedicated to cybersecurity can provide valuable insights and guidance.
4.4.2. Strong Passwords	Creating strong, unique passwords for all social media accounts is a critical step towards improving cybersecurity (Sabillon et al., 2017). To boost the complexity of passwords, encourage the use of a combination of letters, numbers, and symbols. It is critical to avoid easily guessable facts such as birthdates, names, or common words.
4.4.3. Two-Factor Authentication	Enable two-factor authentication (2FA) whenever possible (Reese et al., 2019). This additional layer of security provides an extra step of verification, typically involving a unique code sent to a trusted device. Encourage social media users to adopt 2FA to enhance their account's protection against unauthorized access.
4.4.4. Privacy Settings	Advise users to review and adjust their privacy settings, ensuring that personal information is only accessible to trusted connections. Encourage them to limit the visibility of their posts and profile information to friends or specific groups. Check and update these settings on a regular basis since platforms may alter default settings or add new features without users' knowledge.
4.4.5. Be Cautious of Phishing Attempts	Social media users should exercise caution when encountering suspicious messages, emails, or links. Teach them to recognize warning signs of phishing attempts, such as requests for sensitive personal information, unexpected prize notifications, or unknown sender names. Encourage them to verify the legitimacy of such communications before taking any action.
4.4.6. Safe and Sound WI-FI connection	Let people of the dangers of using unsecured public networks. In order to protect personal information while using public Wi-Fi to access social media, users should be encouraged to use virtual private networks (VPNs) (Ezra et al., 2021). Emphasise the significance of using only secure networks that require a password.
4.4.7. Regular Software Updates	Remind users to regularly update their social media applications, operating systems, and antivirus software. These updates frequently contain security updates and corrections for bugs that correct vulnerabilities and improve protection against new threats. Encourage users to enable automatic updates

	whenever possible.
4.4.8. Cybersecurity Awareness Training	Promote participation in cybersecurity awareness training programs (Zhang et al., 2021). These programs provide in-depth knowledge on identifying and preventing cyber threats. Users will become equipped to recognize potential risks, handle suspicious activities, and proactively protect their social media accounts from unauthorized access.
4.4.9. Think Before Sharing	Remind users to exercise caution when uploading private information and content on social media platforms and to pause before doing so. Dissuading consumers from sharing personal information like home addresses, phone numbers, and financial information with cyber criminals is vital. Users should check their privacy settings to control who sees and shares their posts. Users will feel more in charge of their material as a result of this.
4.4.10. Reporting Suspicious Activities	Encourage users to report any suspicious or unauthorized activities on their social media accounts promptly. Provide clear instructions on how to report incidents to the platform's support team or customer service. This collective vigilance helps create a safe online environment for all users.

Users of social media can take preventative steps to protect their personal information and lower the likelihood of being victims of cyberattacks if they adhere to the methods for increasing their awareness of cybersecurity risks and vulnerabilities (Conteh & Schmick, 2021). Users must be equipped with the knowledge and tools necessary to defend themselves if they are to have a social media experience that is both safe and pleasurable for everyone else.

Figure 3: Cybersecurity tips for employees (source: www.techtarget.com/)

4.5: Detecting and preventing methods of cyberattacks for users:

According to Okutan (2019), various techniques exist for detecting and preventing cyberattacks on social media platforms. These techniques encompass a range of strategies such as antivirus software, cryptographic systems, network access control, air-gap mechanisms, data loss prevention measures, honeypots, electromagnetic security, digital signatures, shorthand techniques, and content filtering systems (Zhang et al., 2022). Employing these techniques can significantly bolster the security of social media platforms and mitigate the risks associated with cyber threats.

Techniques for Cyberattack Detection and Prevention	Description
Antivirus	Using software that uses recognized signatures and behavior patterns to identify and prevent dangerous malware.
Cyber security Systems	Employing encryption methods to protect both stored and

	transmitted data on the network.
Network Access Control (NAC)	Putting authentication methods in place to manage user access to the network and network equipment (Detken et al., 2017).
Air-gap	Putting in place a safe method of data flow between two distinct networks, reducing the possibility of intrusion.
Data Loss Prevention (DLP)	Implementing measures to prevent the leakage of sensitive data from the network or hardware, ensuring it remains within defined boundaries.
Honeypot	Deploying decoy systems to observe and analyze attacks, allowing for the development of effective defense mechanisms, particularly for vulnerable devices.
Electromagnetic Security	Utilizing devices to detect and record electromagnetic leaks, thereby preventing data exfiltration. Physical access to network channels is restricted, and touch-based assaults can be mitigated using tap investigative techniques (Majéric et al., 2016).
Digital Signature	Verifying the digital signature of messages and files, providing proof of the sender's identity and ensuring the integrity of the content.
Shorthand	Concealing information within other data rather than encrypting it, makes it harder for attackers to detect.
Content Filtering Systems	Implementing filters based on web addresses, file types, specific keywords, images, or applications to block or allow specific content.

Tuptuk and Hailes (2018) suggest a variety of defensive measures in addition to these methods (Gostin et al., 2021). These measures include guidelines, standards, regulations, encryption methods, intrusion detection systems, training in human factors and safety skills, and incident prevention and preparedness.

Furthermore, Soomro and Hussain (2019) provide specific preventive tips, such as avoiding sharing personal information like location and home address, being cautious about sharing information with "friends of friends," and limiting contact and application permissions.

These techniques serve as effective measures to enhance the security of social media platforms and protect users from cyber threats. Antivirus software detects and blocks malicious software, while cryptographic systems provide encryption to safeguard data (Chen et al., 2012). Network access control ensures authorized access to the network, and air-gap mechanisms minimize

unauthorized data transfers. Data loss prevention measures prevent sensitive data leakage, and honeypots help analyze attacks and develop defence mechanisms. Electromagnetic security detects and prevents data exfiltration, while digital signatures verify the sender's identity. Shorthand conceals information within other data, and content filtering systems block or allow specific content based on predefined criteria (Taipale, 2019).

5. DISCUSSION

5.1: Discussion about Documents analysis

The study presents a comprehensive data analysis of cybersecurity issues in social media (SM) based on existing literature (Miranda-Calle et al., 2021). Due to the extensive application of cybersecurity in the realm of information and communication technology (ICT), this study focuses on the rising usage of social media among all age groups in the present era of communication (Prasad & Rohokale, 2020). The findings show that social media platforms (SMPs) with personal information available make it simpler for hackers to exploit them. The survey discovered several cyberattacks against SM, with phishing being the most frequent. Malware, social engineering, harmful deeds, and spam were also found to be common. Sniffers, sniffers, Trojan horses, and cyber-casing are a few examples of small-scale attacks on media platforms.

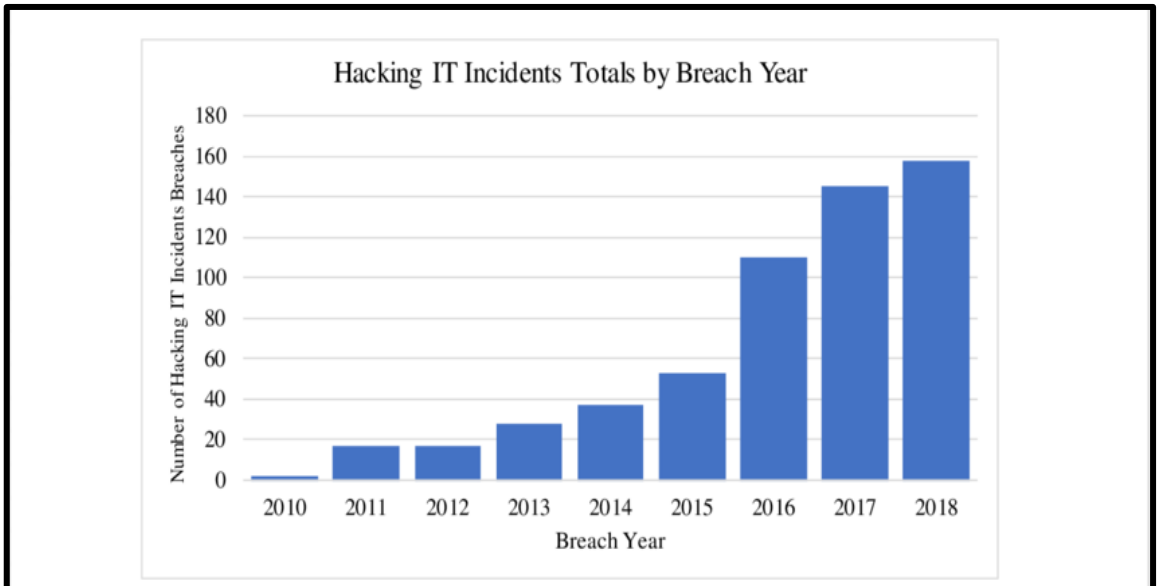
Concerning the reasearch, the synthesis of data from selected publications finds numerous elements that contribute to social media websites and their users' vulnerability to cyber-attacks (Alloghani et al., 2019). The study emphasises the need for education and knowledge in influencing individuals, as a lack of awareness and training among users has been identified as a significant shortcoming in social communication. Previous research has also found that education and awareness play an important role in vulnerability variables (Reichlin et al., 2020). Social media sites' exponential expansion corresponds to a rising user community, which comprises people of all ages and genders. As a result, people from many demographics become targets and victims of various types of cyberattacks. Adults, particularly those who are unfamiliar with cyber technology, are more vulnerable because to their low capacity and awareness in expressing their emotions. According to several surveys, both adults and children are vulnerable segments of society when it comes to the negative effects of electronic media (Ray & Jat, 2010). Young people, with their distinct qualities and proclivity to try new things, are particularly vulnerable while using the internet. Because of their high level of confidence in internet data, they are vulnerable to possible threats. Sharing personal information, chatting with strangers, engaging in online bullying and sexual behaviours, and circumventing internet restrictions and filters can all jeopardise vulnerable young people (Walker & Donaldson, 2011). Women are similarly targeted by numerous forms of cyber risks, owing to their poorer security awareness and self-efficacy. Previous research has consistently demonstrated that women are among the most vulnerable populations (Ruof, 2004). Individuals frequently express their views, opinions, and private information on social media platforms in the digital age without fully realising the ramifications of their activities. Individuals must learn everything they can about cybersecurity. The study recommends numerous approaches to improve cyber safety

awareness, highlighting the usefulness of security awareness and education training (Zhang-Kennedy & Chiasson, 2021). When consumers are informed of cybersecurity practices, they can use social media platforms with confidence and without fear of cyber dangers. The findings are consistent with earlier research that emphasises the role of knowledge and education in reducing cyber hazards (Uddin et al., 2020).

Figure 4: Vulnerability Assesment

Hacking incidents and unauthorised data breaches have dramatically increased in recent years. The ease of access to personal data has led to the creation of cybersecurity regulations and protections to protect sensitive data stored online (Hopcraft & Martin, 2018). Additionally, security and privacy issues are brought up by the growing volume, speed, range, and accuracy of data on social networking sites. Social media users should be aware of precautions they can take to protect the security of their personal data. Both technological and human measures should be used in effective cyberattack prevention techniques (Yeboah-Ofori et al., 2021). Regarding the research topic, a review of pertinent papers shows the significance of security training and awareness in promoting safe online behaviour and preventing cyberattacks. Another efficient strategy for defending against online dangers is to enable firewalls. The study found that firewalls and awareness/education are two efficient ways to avoid cyberattacks in the context of social media use (Khandpur et al., 2017). It is crucial to understand the study's

constraints and shortcomings, though. While the study aims to include a variety of pertinent and useful references, conducting a systematic literature review requires time and effort (Perwej et al., 2021). As a result, it's possible that some publications—such as conference papers, books, book chapters, workshop sessions, and magazines—were left out despite the study's best efforts.



HHS data breach reporting system as of October 31, 2019. Time period January 1, 2010 and December 31, 2018

	Year										
	2010	2011	2012	2013	2014	2015	2016	2017	2018	Total	P Value
Hacking IT Incident	2	17	17	28	37	53	110	145	158	567	.000

Figure 5: Hacking IT Incidents

Social engineering strategies are important in preventing cybersecurity breaches on social media sites. Cyber attackers utilize social engineering techniques to fool people and manipulate them into exposing sensitive information or falling prey to malevolent schemes by exploiting human psychology (Hathaway et al., 2012). Reducing cybersecurity risks on social media platforms depends on understanding and countering these tactics (Zong et al., 2019). The role of social media firms in dealing with cybersecurity issues is critical. These businesses must prioritize user data security, invest in modern cybersecurity solutions, and employ proactive security measures. Transparency and accountability are critical in establishing consumer confidence and addressing privacy and security concerns. Furthermore, user education and awareness are critical in combating cybersecurity threats (Thakur et al., 2015). Social media platforms should establish clear norms, educate users on safe online behaviour, and raise awareness of potential hazards (Fthenakis, 2018).

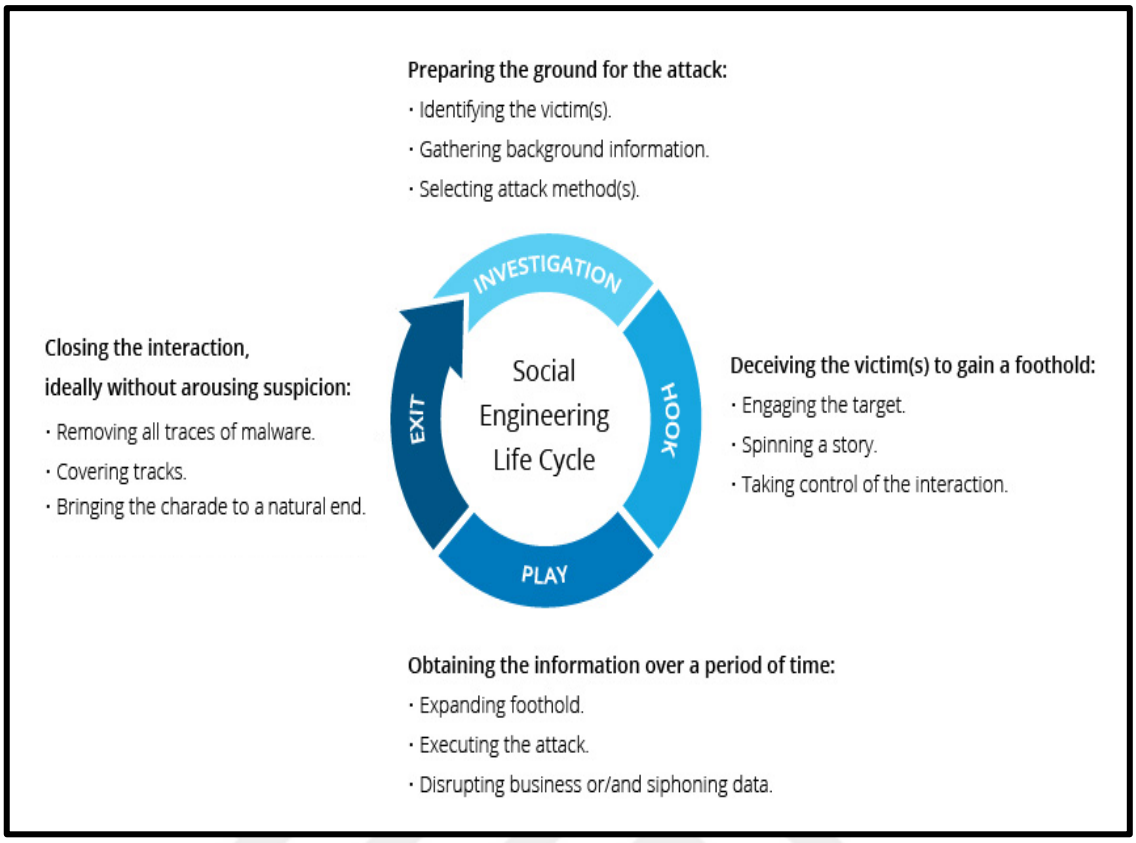


Figure 6: Social engineering strategies

The debate over the findings highlights the critical need for improved cybersecurity safeguards in social media platforms (Beissel, 2016). The frequency of cyber-attacks, many sorts of impediments, and the importance of social engineering strategies highlight the complexity of the difficulties (Özalp & Albayrak, 2022). To establish a safer online environment for users and organizations, social media businesses must prioritize user education, invest in innovative technology, cultivate transparency, and strengthen their security procedures.

The study's findings set the foundation for more investigation and action in the field of social media security. Future research might look at the changing nature of cyber threats, new techniques used by cyber attackers, and the efficacy of various security measures deployed by social media sites. Furthermore, examining the impact of cybersecurity concerns on certain industries, user demographics, and geographical regions can provide greater insights into the varying consequences and vulnerabilities in the social media ecosystem.

6. RESULTS AND SUGGESTIONS

6.1: Conclusion:

On social media platforms, a huge number of people are eager to interact with others, but regrettably, these platforms have also turned into a haven for hackers. By disseminating malicious code and delivering spam, these criminals take advantage of the confidence users invest in their social networks. Users' worries about security and privacy in social media networks have increased as a result. Social media platforms need to acknowledge the essential elements of interpersonal communication in order to handle this problem. They also need to build robust, logical procedures that will guarantee the required levels of trust, privacy, and protection. Governments, intelligence organisations, and technological specialists must work together and adopt cutting-edge techniques and technologies to manage and control the massive volume of data posted on social media platforms. Additionally, rather than being considered an optional feature, cyber security should be a fundamental component of all goods, databases, and electronic communications during design. In particular, in the area of social media, each individual has a crucial part to play in ensuring our future by fostering knowledge, creating awareness, and arguing for a compromise between privacy and security. To adequately address these problems, proactive policy reforms are necessary.

In methodology, the qualitative research study utilized an exploratory research paradigm to examine the cybersecurity obstacles present within social media platforms. The research was conducted within a specific location and timeframe, with a defined target population. Data was collected using appropriate data assembling tools, and the analysis of the gathered data will provide valuable insights into the cybersecurity challenges faced by social media users. By understanding these impediments, stakeholders can develop effective strategies and measures to enhance cybersecurity and protect user privacy on social media platforms. The findings of this study reveal two significant aspects regarding cybersecurity in social media platforms. First, the interview study demonstrates that users are increasingly aware of the privacy concerns associated with online interactions on these platforms. This highlights the need for robust measures to address these concerns and ensure user trust. Second, the analysis of relevant documents underscores the critical importance of implementing strong cybersecurity measures within social media platforms.

In conclusion, the analysis of documents emphasizes the critical importance of implementing strong cybersecurity measures in social media platforms. The prevalence of cyber-attacks, various types of obstructions, and the utilization of social engineering tactics emphasize the complexity and seriousness of the challenges faced. Social media companies must prioritize user education, invest in advanced technologies, foster transparency, and strengthen security

measures to create a safer online environment. Ensuring data protection, accountability, and user awareness are crucial in addressing cybersecurity risks. Further research is needed to explore emerging threats, evaluate the effectiveness of security measures, and understand the impact of cybersecurity challenges across different industries and user groups (Ozkaya, 2018). By taking proactive steps and collaboration among stakeholders, social media platforms can enhance cybersecurity and mitigate the risks faced by their users.

Moreover findings amphasis, social media (SM) platforms have become a breeding ground for cybercriminals who exploit users' personal information for intelligence gathering, misuse, and unauthorized access to computers. Particularly phishing attacks take advantage of the availability of data on SM to conduct hacks. Risks including computer viruses, malware, and spyware have expanded along with the usage of SM, creating challenges to information security and confidentiality (Ozkaya, 2018). These dangers, which include a variety of risks connected to SM and the internet, can be divided into modern and classic categories. People should use a variety of strategies, including updating their browsers regularly, managing passwords wisely, staying informed about security measures, adhering to SM policies, utilizing safety technologies, and being aware of pertinent rules and laws, in order to reduce cybersecurity risks and protect against SM attacks.

The investigation's findings provided information about the frequency of various cyberattacks against SM. Phishing is the most frequent form of cyberattack, and it is followed by malware, social engineering, illegal activity, and spam. The paper also lists a variety of elements that make SM users more vulnerable to hacks. It highlights how important education and awareness are while also emphasizing how severely insufficient user education and training are. Attacks can be prevented by safeguarding sensitive data and being aware of the vulnerabilities that hackers take advantage of.

No matter their age or gender, social media users should all be knowledgeable about cybersecurity risks. The poll found that cybercriminals target people regardless of their age or race. Women, adults, and kids are more exposed because they don't grasp cybersecurity precautions and self-protection procedures. The statistics indicate that boosting cybersecurity knowledge can be accomplished by increasing security awareness and providing education and training. People may protect their SM platforms from cyberattacks in addition to raising awareness by activating firewalls, installing dependable antivirus software, and adhering to approved security practices.

6.2: Recommendation:

6.2.1: User:

Users need to exercise caution when sharing sensitive information on social media and be mindful of their online visibility. Personal data can attract harmful people who exploit users' honesty. Sharing specific comments or photographs can also damage reputation and cost jobs. About 70% of recruiters check candidates' social media posts and reject them. Stalking is facilitated by providing bank names, workplaces, regularly visited sites, and home addresses. Sharing constant updates about one's whereabouts makes it easy for unscrupulous people to monitor them. It's important to remember that someone with malicious intent is collecting social media data.

Users can manage their visibility on social media. Facebook has 101 privacy options to solve its privacy issues. Use these privacy settings to avoid strangers who request favors via messages. If feasible, restrict social media accounts to friends and family. These settings safeguard individuals from physical injury or theft while away from home, but social media corporations can still acquire their data. For account security, enable two-factor authentication. This authentication method requires a second factor—like an SMS or email code—to verify the user's identity. Even with a username and password, hackers or stolen credentials cannot access an account without this second code. Two-factor authentication has prevented hacking, fraud, data theft, and identity theft. Activate this security option on most social networking platforms.

Users should exercise caution when using third-party applications within and outside social media platforms. These apps often gain access to users' friend lists, account information, posts, and private messages. Despite offering various functionalities, they often obtain excessive access to user data. Facebook, for instance, grants them extensive access to users' accounts. Given the potential misuse of this data, it is advisable to remove such apps from accounts. Although some may claim to help identify stalkers, they could exploit users' messages and posts for malicious purposes. Social media platforms provide settings to remove these apps, and users should do so to protect their accounts.

Regularly changing passwords is another effective measure for account security. By frequently updating passwords, even if a password is stolen, the window of opportunity for malicious individuals to use it becomes limited. Password theft is relatively easy, especially when users are tempted by "free" premium software. Illegally downloaded software often contains malware, such as keystroke loggers and ransomware, designed to steal saved passwords from web browsers. Users should avoid saving passwords on browsers and instead use password manager software. Various tools can copy all saved passwords from a computer, and users should never reuse the same password across multiple social media platforms.

6.2.2: Strengthen Security Measures:

To address the cybersecurity obstructions in social media platforms, it is essential to prioritize and strengthen security measures. Social media companies should take proactive steps to safeguard user data and mitigate potential risks.

- Firstly, implementing robust security protocols and measures is crucial. This includes regular security audits to identify vulnerabilities and potential entry points for cyber attackers. To protect sensitive user data and ensure secure transmission, encryption technologies should be used. To add an additional degree of security, multi-factor authentication should be required, requiring users to produce various forms of identification before gaining access to their accounts (Miranda-Calle et al., 2021).
- Second, advanced threat detection systems must be put in place to track and spot any online dangers instantly. The use of artificial intelligence and machine learning algorithms can aid in the detection of abnormal activity patterns and the proactive blocking or flagging of potential risks. Rapid reaction procedures should be in place to resolve security events as soon as possible while minimising user damage.
- Additionally, social media plateform ought to place a high priority on user privacy by putting in place rigorous data protection procedures. Only authorised workers should have access to user data, which should be securely stored. To guarantee the availability of user information in the event of any security breaches, regular data backups should be carried out (Morgan & Voce, 2022). Users should be given ongoing education and training programmes to raise their understanding of cybersecurity best practices. This involves educating people on the need of using strong and unique passwords, avoid suspicious links and downloading suspicious documents, and exercise caution when sharing personal information online.
- Users can actively contribute to their own cybersecurity and assist prevent possible attacks by providing them with knowledge and skills. It is also critical to collaborate with cybersecurity specialists and researchers. To stay up to current on emerging dangers and best practices, social media companies should form partnerships and share expertise with professionals in the sector. To discover and remedy system weaknesses, regular security audits, penetration testing, and vulnerability assessments should be performed.

6.2.3: Social media platforms

Social media platforms must prioritise user privacy by allowing users to control third-party application data access. These platforms automatically access data without giving users options or the ability to opt out. Even if it's not necessary for these apps, users should be able to restrict

access to certain data. For instance, allowing a third-party app to read Facebook messages to post birthday messages on friends' timelines violates privacy. Unnecessary data should be blocked by users. Social media platforms must avoid collecting and selling user data without consent to protect user privacy. Facebook and others have been accused of collecting, profiling, and selling user data without consent. Facebook has been accused of collecting faceprints without users' consent. By adding a clause to their privacy statement that users didn't agree to, they hid their disregard for privacy. This lack of transparency and consent disrespects users' privacy. Facebook forced an update on WhatsApp users, forcing them to share their data with Facebook servers without notice or consent. Stop these serious privacy violations. Users' content drives platform growth and advertising, so social media platforms should respect them. Illegal data collection, sharing, or non-consensual operations damage their reputation and user trust (Roberts, 2015).

Social media platforms must also improve privacy education. New users may find privacy controls confusing. These platforms' privacy controls have poor interface design and lack explanations. Sub-menus hide controls, forcing users to find them. Privacy settings shouldn't punish users. Social media networks should simplify the process and teach users about controls, their functions, and how to access and alter them. The sign-up process should explain privacy controls, their purpose, and how to customise them. Users are unaware of these controls, and new users struggle to learn them. Finally, social media platforms should enable permanent account deletion. Facebook only enables deactivation, which leaves profile data accessible. Deleted accounts should erase all data from the platform. Some users quit social media due of privacy concerns. To keep a huge user base for business, several platforms simply offer deactivation. Few services, like LinkedIn, allow account deletion. An easy-to-use control that informs users of their account deletion ability is essential. Users' last line of defence for privacy should be available on social media platforms.

6.3: Future direction:

This research extensively examined the privacy and security threats present in social media platforms while building upon existing literature on the subject. The study aimed to contribute additional knowledge to the field based on the previous research conducted by other scholars. Consequently, there are several areas that future researchers can delve into to further expand the understanding of this topic. Firstly, it is crucial to explore the legislation governments should enact to safeguard user data and investigate how international cooperation can enhance privacy protection. Secondly, future research should focus on specific third-party applications that extensively collect user data, delving into their data collection, storage, and utilization practices, as well as exploring potential limitations on their access. Thirdly, researchers should examine

the collaborative efforts between social media platforms and governments to combat social media crimes, which are increasing in prevalence. Understanding effective strategies to mitigate these crimes would be invaluable. Lastly, future researchers should aim to collect primary data from diverse world regions to provide a more comprehensive understanding of user opinions, as the data sampled in this study represents a limited demographic. By addressing these areas, future research can contribute significantly to the field of social media privacy and security.

RESOURCES

Al Amro, S. (2020). How safe is governmental infrastructure: A Cyber Extortion and Increasing Ransomware Attacks Perspective. *International Journal of Computer Science and Information Security (IJCSIS)*, *18*(6).

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. Computers in Human Behavior, 136, 107376. https://doi.org/10.1016/j.chb.2022.107376.

Aldaej, A. (2019). Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI). IEEE Access, 1–1. https://doi.org/10.1109/access.2019.2893445.

Allmendinger, R., Shavarani, S. M., López-Ibáñez, M., & Allmendinger, R. (2023). Detecting.

Alloghani, M., Al-Jumeily, D., Hussain, A., Mustafina, J., Baker, T., & Aljaaf, A. J. (2019). Implementation of Machine Learning and Data Mining to Improve Cybersecurity and Limit Vulnerabilities to Cyber Attacks. *Nature-Inspired Computation in Data Mining and Machine Learning*, 47–76. https://doi.org/10.1007/978-3-030-28553-1_3.

Almarabeh, H., & Sulieman, A. (2019). The impact of cyber threats on social networking sites. *InternationalJournal of Advanced Research in Computer Science*, *10*(2), 1-9 http://dx.doi.org/10.26483/ijarcs.v10i2.6384

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. Technology in Society, 73, 102258. https://doi.org/10.1016/j.techsoc.2023.102258.

Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. Computer Systems Science and Engineering, 40(3), 1153–1166. https://doi.org/10.32604/csse.2022.019938.

Alvarez-Milán, A., Felix, R., Rauschnabel, P. A., & Hinsch, C. (2018). Strategic customer engagement marketing: A decision making framework. Journal of Business Research, 92, 61–70. https://doi.org/10.1016/j.jbusres.2018.07.017.

Arceneaux, P., & Harman, M. (2021). Social Cybersecurity: A Policy Framework for Addressing.

arpenter, C. J. (2012). Narcissism on Facebook: Self-promotional and anti-social behavior. Personality and Individual Differences, 52(4), 482–486. https://doi.org/10.1016/j.paid.2011.11.011.

Asher, T. (2020). What Are the Types of Cybersecurity? Retrieved April 29, 2021, from https://www.ashersecurity.com/what-are-the-types-of-cybersecurity/

Aslan, Ö. A., & Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. IEEE Access, 8, 6249–6271. https://doi.org/10.1109/ACCESS.2019.2963724.

Awojobi, B., & Ding, J. (2020). Data Security and Privacy. In: Cybersecurity for InformationProfessionals: Concepts and Applications. *Taylor & Francis Group CRC Press*. 291-304. https://doi.org/10.1201/9781003042235-13

Baazeem, R., & Qaffas, A. (2020). The relationship between user religiosity and preserved privacy in the context of social media and cybersecurity. In *Emerging Cyber Threats and Cognitive Vulnerabilities* Academic Press. 93-116 https://doi.org/10.1016/B978-0-12-816203-3.00005-8

Beissel, S. (2016). Cybersecurity Safeguards. *Cybersecurity Investments*, 35–77. https://doi.org/10.1007/978-3-319-30460-1_3.

Belot, G. (2016). Objectivity and Bias. Mind, 126(503), 655–695. https://doi.org/10.1093/mind/fzv185.

Bootstrap Business (2020). What Are the Different Types of Cyber Security? Retrieved February 5, 2021, from https://www.myfrugalbusiness.com/2020/12/different-types-of-cyber-security.html

Bruch, E., & Feinberg, F. (2017). Decision-Making Processes in Social Contexts. Annual Review of Sociology, 43(1), 207–227. https://doi.org/10.1146/annurev-soc-060116-053622.

Calibrated Subset Selection. Proceedings.mlr.press; PMLR. https://proceedings.mlr.press/v162/wang22j.html.

Carley, K. M. (2020). Social cybersecurity: an emerging science. Computational and Mathematical Organization Theory, 26(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9.

Chang, L. Y., & Coppel, N. (2020). Building cybersecurity awareness in a developing country: lessons from Myanmar. Computers & Security, 97, 101959. https://doi.org/10.1016/j.cose.2020.101959

Chen, Y.-Y., Jamkhedkar, P. A., & Lee, R. B. (2012). A software-hardware architecture for self-protecting data. https://doi.org/10.1145/2382196.2382201.

Cohn-Gordon, K., Cremers, C., & Garratt, L. (2016, June 1). On Post-compromise Security. IEEE Xplore. https://doi.org/10.1109/CSF.2016.19.

Computational Propaganda. Journal of Information Warfare, 20(3), 24–43.

Conteh, N. Y., & Schmick, P. J. (2021). Cybersecurity Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks. Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention. https://www.igi-global.com/chapter/cybersecurity-risks-vulnerabilities-and-countermeasures-to-prevent-social-engineering-attacks/282222.

corporate discourse about educational tracking. Information, Communication & Society, 1–18. https://doi.org/10.1080/1369118x.2020.1764604.

Das, R., & Patel, M. (2017). Cyber Security for Social Networking Sites: Issues, Challenges, and Solutions. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 5(4),833-838). https://doi.org/10.22214/ijraset.2017.4153

Definitions and Why They Matter. Jornal Brasileiro de Pneumologia, 44(2), 84. ncbi. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6044655/.

Detken, K.-O., Jahnke, M., Kleiner, C., & Rohde, M. (2017, September 1). Combining Network Access Control (NAC) and SIEM functionality based on open source. IEEE Xplore. https://doi.org/10.1109/IDAACS.2017.8095094.

Dolganova, O. I. (2021). Improving customer experience with artificial intelligence by adhering.

Duncan, C. (2003). Advanced Quantitative Data Analysis. In Google Books. McGraw-Hill.

Ezra, P. J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., & Damasevicius, R. (2021). Secured Communication Using Virtual Private Network (VPN). Lecture Notes on Data Engineering and Communications Technologies, 309–319. https://doi.org/10.1007/978-981-16-3961-6_27.

Formby, D., Rad, M., & Beyah, R. (2018). Lowering the Barriers to Industrial Control System

Fthenakis, V. M. (2018, January 1). Chapter IV-1-A - Overview of Potential Hazards (S. A. Kalogirou, Ed.). *ScienceDirect; Academic Press.* https://www.sciencedirect.com/science/article/pii/B9780128099216000355.

Gernhardt, D., & Groš, S. (2022, May 1). Use of a non-peer reviewed sources in cyber-security

Gerring, J. (2017). Qualitative Methods. Annual Review of Political Science, 20(1), 15–36.

Gostin, L. O., Halabi, S. F., & Klock, K. A. (2021). An International Agreement on Pandemic Prevention and Preparedness. JAMA, 326(13), 1257–1258. https://doi.org/10.1001/jama.2021.16104.

Grispos G. (2019) Cybersecurity: Practice. In: Encyclopedia of Security and Emergency Management. Springer, 1-6 https://doi.org/10.1007/978-3-319-69891-5_81-1

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer Networks, 169, 107094.

Győrffy, K., Leitold, F., & Arrott, A. (2017). Individual awareness of cyber-security vulnerability- Citizen and public servant. Central and Eastern European eDem and eGov Days, 325, 411- 422. https://doi.org/10.24989/ocg.v325.34

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review*, 100(4), 817–885. https://www.jstor.org/stable/23249823.

Hennink, M., Hutter, I., & Bailey, A. (2020). Qualitative Research Methods. In Google Books.

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity Practices for Social Media.

Hidden and Irrelevant Objectives in Interactive Multi-Objective Optimization. IEEE Transactions on Evolutionary Computation, 1–1.

Hopcraft, R., & Martin, K. M. (2018). Effective maritime cybersecurity regulation – the case for a cyber code. *Journal of the Indian Ocean Region*, 14(3), 354–366. https://doi.org/10.1080/19480881.2018.1519056.

Hoque, M. A., Rasiah, R., Furuoka, F., & Kumar, S. (2021). Technology adoption in the apparel.

Hu, T., Wang, K. Y., Chih, W., & Yang, X. H. (2020). Trade-off cybersecurity concerns for co- created value. Journal of Computer Information Systems, 60(5), 468-483. https://doi.org/10.1080/08874417.2018.1538708

Iguer, H., Medromi, H., Sayouti, A., Elhasnaoui, S., & Faris, S. (2014). The Impact of Cyber Security Issues on Businesses and Governments: A Framework for Implementing a Cyber Security Plan. 2014 International Conference on Future Internet of Things and Cloud. https://doi.org/10.1109/ficloud.2014.56.

Keung, E. Z., McElroy, L. M., Ladner, D. P., & Grubbs, E. G. (2020). Defining the Study Cohort:

Khandpur, R. P., Ji, T., Jan, S., Wang, G., Lu, C.-T., & Ramakrishnan, N. (2017). Crowdsourcing Cybersecurity. *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*. https://doi.org/10.1145/3132847.3132866.

Khidzir, N. Z., Ismail, A. R., Daud, K. A. M., Afendi, M. S., Ghani, A., & Ibrahim, M. A. H. (2016). Critical cybersecurity risk factors in digital social media: Analysis of information security requirements. Lecture Notes on Information Theory Vol, 4(1).18-24 https://doi.org/10.18178/lnit.4.1.18-24

Kumar, A., Kumar Gupta, S., Rai, A., & Sinha, S. (2013). Social Networking Sites and Their Security Issues. International Journal of Scientific and Research Publications, 3(4). https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=9492804becb6c119bd43d6a31bc575fb03d62422.

Kummerow, A., Henneke, M., Bachmann, P., Krackruegge, S., Laessig, J., & Nicolai, S. (2023,

literature review: the basic methodological guidance for beginners. Quality & Quantity, 55. https://doi.org/10.1007/s11135-020-01059-6.

Madu, U., Buhari, G., & ALIYU, M. (2022). Impacts of User Education on Users' Awareness, Accessibility and Use of Information Resources and Services in Federal Polytechnic Ede Library, Osun State, Nigeria. Library Philosophy and Practice (E-Journal). https://digitalcommons.unl.edu/libphilprac/7141/.

Majéric, F., Bourbao, E., & Bossuet, L. (2016, December 1). Electromagnetic security tests for SoC. IEEE Xplore. https://doi.org/10.1109/ICECS.2016.7841183.

MGAZA, P. R. (2022). CYBER SECURITY AWARENESS AMONG SOCIAL MEDIA USERS: Iaa.ac.tz. http://dspace.iaa.ac.tz:8080/xmlui/handle/123456789/1123.

Miranda-Calle, J. D., Reddy C., V., Dhawan, P., & Churi, P. (2021). Exploratory data analysis for cybersecurity. *World Journal of Engineering*, 18(5), 734–749. https://doi.org/10.1108/wje-11-2020-0560.

Mirian, A., DeBlasio, J., Savage, S., Voelker, G. M., & Thomas, K. (2019). Hack for Hire:

Exploring the Emerging Market for Account Hijacking. The World Wide Web Conference on - WWW '19. https://doi.org/10.1145/3308558.3313489.

Mohamed Shaffril, H. A., Samsuddin, S. F., & Abu Samah, A. (2020). The ABC of systematic

Morelli, S., Pazzi, V., Nardini, O., & Bonati, S. (2022). Framing Disaster Risk Perception and Vulnerability in Social Media Communication: A Literature Review. Sustainability, 14(15), 9148. https://doi.org/10.3390/su14159148.

Morgan, A., & Voce, I. (2022, November 23). Data breaches and cybercrime victimisation. Apo.org.au. https://apo.org.au/node/320841.

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack framework. 2014 Information Security for South Africa, 2330-9881. https://doi.org/10.1109/issa.2014.6950510.

Musmade, P., Nijhawan, L., Udupa, N., Bairy, K., Bhat, K., Janodia, M., & Muddukrishna, B.

Nguyen, J., Li, A., Tam, D. Y., & Forbes, T. L. (2022). Analysis of spin in vascular surgery

Niemi, P.-M., Kallioniemi, A., & Ghosh, R. (2019). Religion as a Human Right and a Security Threat Investigating Young Adults' Experiences of Religion in Finland. Religions, 10(1), 55. https://doi.org/10.3390/rel10010055.

Nosirovich, A., Umarovich, N., Makhina, K., & Qizi, K. (2022). CYBERSPACE IN THE REAL WORLD. Journal of Academic Research and Trends in Educational Sciences Journal Home. https://doi.org/10.5281/zenodo.7258458.

Ozkaya, E. (2018, October 4). Cyber Security Challenges in Social Media. Charles Sturt University Research Output. https://researchoutput.csu.edu.au/en/publications/cyber-security-challenges-in-social-media.

Özalp, A., & Albayrak, Z. (2022). Detecting Cyber Attacks with High-Frequency Features using Machine Learning Algorithms. *Acta Polytechnica Hungarica*, 19(7), 2022–2213. Retrieved July 17, 2023, from http://acta.uni-obuda.hu/Ozalp_Albayrak_125.pdf.

Patino, C. M., & Ferreira, J. C. (2018). Inclusion and Exclusion Criteria in Research studies:

Penni, J. (2017). The future of online social networks (OSN): A measurement analysis using social media tools and application. Telematics and Informatics, 34(5), 498–517. https://doi.org/10.1016/j.tele.2016.10.009.

Perwej, Dr. Yusuf., Qamar Abbas, S., Pratap Dixit, J., Akhtar, Dr. N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of*

Scientific Research and Management, 9(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04.

Polverini, D., Ardente, F., Sanchez, I., Mathieux, F., Tecchio, P., & Beslay, L. (2018). Resource efficiency, privacy, and security by design: the first experience on enterprise servers and data storage products triggered by a policy process. Computers & Security, 76, 295-310. https://doi.org/10.1016/j.cose.2017.12.001

Prasad, R., & Rohokale, V. (2020). Cyber Security: The Lifeline of Information and Communication Technology. *In Springer Series in Wireless Technology*. *Springer International Publishing*. https://doi.org/10.1007/978-3-030-31703-4.

Price, P. C., Jhangiani, R. S., & Chiang, I.-C. A. (2015). Reliability and Validity of Measurement.

Proudfoot, J., & Madnick, S. (2022). Regulatory Facilitators and Impediments Impacting Cybersecurity Maturity. AMCIS 2022 Proceedings. https://aisel.aisnet.org/amcis2022/sig_ais/sig_ais/2/.

randomized controlled trials with nonsignificant outcomes. Journal of Vascular Surgery, 75(3), 1074-1080.e17. https://doi.org/10.1016/j.jvs.2021.09.051.

Ray, M., & Jat, K. R. (2010). Effect of electronic media on children. *Indian Pediatrics*, 47(7), 561–568. https://doi.org/10.1007/s13312-010-0128-9.

Reddy, P., Sharma, B., & Chaudhary, K. (2020). Digital literacy: A review of literature. International Journal of Technoethics, 11(2), 65–94. https://doi.org/10.4018/ijt.20200701.oa1.

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A Usability Study of Five Two-Factor Authentication Methods. Www.usenix.org.https://www.usenix.org/conference/soups2019/presentation/reese.

Reichlin, L., Ricco, G., & Hasenzagl, T. (2020). Financial Variables as Predictors of Real Growth Vulnerability. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3556506.

Reid Chassiakos, Y. (Linda), Radesky, J., Christakis, D., Moreno, M. A., & Cross, C. (2016). Children and Adolescents and Digital Media. Pediatrics, 138(5), e20162593. https://doi.org/10.1542/peds.2016-2593.

Reid, K. (2021). What Are the Different Types of Cyber Security? Retrieved April 29, 2021, from https://triadanet.com/blog/different-types-of-cyber-security/

Ricci, J., Breitinger, F., & Baggili, I. (2018). Survey results on adults and cybersecurity education. Education and Information Technologies, 24(1), 231–249. https://doi.org/10.1007/s10639-018-9765-8.

Ruof, M. C. (2004). Vulnerability, Vulnerable Populations, and Policy. *Kennedy Institute of Ethics Journal*, 14(4), 411–425. https://doi.org/10.1353/ken.2004.0044.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). 2017 International Conference on Information Systems and Computer Science (INCISCOS). https://doi.org/10.1109/inciscos.2017.20.

Sadik, S., Ahmed, M., Sikos, L. F., & Islam, A. K. M. (2020). Toward a Sustainable Cybersecurity Ecosystem. Computers, 9(3), 74. https://doi.org/10.3390/computers9030074

San Juan, N. (2021, April 20). What is cybersecurity. Retrieved April 29, 2021, from https://vpnpro.com/web/what-is-cyber-security/

Semantic Parsing. ArXiv.org. https://doi.org/10.48550/arXiv.2104.05827.

Singh, J. (2013). Critical appraisal skills programme. Journal of Pharmacology.

Storm, M. (2020). 5 Types of Social Media and Examples of Each. Retrieved February 12, 2021, from https://www.webfx.com/blog/social-media/types-of-social-media/

systematic literature review of blockchain cyber security. Digital Communications and Networks, 6(2). https://doi.org/10.1016/j.dcan.2019.01.005.

Szumski, O. (2018). Cybersecurity best practices among Polish students. Procedia Computer Science, 126, 1271-1280. https://doi.org/10.1016/j.procs.2018.08.070

Taipale, J. (2019). Predefined criteria and interpretative flexibility in legal courts' evaluation of expertise. Public Understanding of Science, 28(8), 883–896. https://doi.org/10.1177/0963662519881338.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2019). A

Thakur, K., Hayajneh, T., & Tseng, J. (2019). Cyber Security in Social Media: Challenges and

Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015). An Investigation on Cyber Security Threats and Security Models. *IEEE Xplore*. https://doi.org/10.1109/CSCloud.2015.71.

the Way Forward. IT Professional, 21(2), 41–49. https://doi.org/10.1109/mitp.2018.2881373.

to ethical principles. Бизнес-информатика, 15(2 (eng)), 34–46. https://cyberleninka.ru/article/n/improving-customer-experience-with-artificial-intelligence-by-adhering-to-ethical-principles.

Uddin, Md. H., Ali, Md. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: *a synthesis of literature*. *Risk Management*, 22. https://doi.org/10.1057/s41283-020-00063-2.

van den Berg, B., & Kuipers, S. (2022). Vulnerabilities and Cyberspace: A New Kind of Crises. Oxford Research Encyclopedia of Politics. https://doi.org/10.1093/acrefore/9780190228637.013.1604.

van den Bergh, M. (2018). Protecting Personal Information on Social Media Sites from Cybercrime Activities: A Student Perspective,1(2) 20-25.

Vanhee, A. J. (2022). Increased Protection Versus the Cost of Increased Protection: Victimization and the Use of Protective Measures Against Identity Theft. Criminal Justice and Behavior, 009385482211058. https://doi.org/10.1177/00938548221105824.

Vieira, A. A. C., Dias, L. M. S., Santos, M. Y., Pereira, G. A. B., & Oliveira, J. A. (2020). Supply Chain Data Integration: A Literature Review. Journal of Industrial Information Integration, 100161. https://doi.org/10.1016/j.jii.2020.100161.

Walker, J., & Donaldson, C. (2011). Intervening to improve outcomes for vulnerable young people*: a review of the evidence.* Retrieved July 17, 2023, from https://core.ac.uk/download/pdf/4162597.pdf.

Wang, B., Yin, W., Lin, X. V., & Xiong, C. (2021, April 27). Learning to Synthesize Data for

Wang, L., Joachims, T., & Rodriguez, M. G. (2022, June 28). Improving Screening Processes via

Wu, Y., Edwards, W. K., & Das, S. (2022, May 1). SoK: Social Cybersecurity. IEEE Xplore.

Yeboah-Ofori, A., Agbodza, C. K., Opoku-Boateng, F. A., Darvishi, I., & Sbai, F. (2021). Applied Cryptography in Network Systems Security for Cyberattack Prevention. *2021 International Conference on Cyber Security and Internet of Things (ICSIoT).* https://doi.org/10.1109/icsiot55070.2021.00017.

Yu, J., & Couldry, N. (2020). Education as a domain of natural data extraction.

Zhang, S., Han, P., & Wu, C. (2022). Calibration Techniques Encompassing Survey

Sampling, Missing Data Analysis and Causal Inference. International Statistical Review. https://doi.org/10.1111/insr.12518.

Zhang, Z. (Justin), He, W., Li, W., & Abdous, M. (2021). Cybersecurity awareness training programs: a cost benefit analysis framework. Industrial Management & Data Systems, ahead-of-print(ahead-of-print). https://doi.org/10.1108/imds-08-2020-0462.

Zhang-Kennedy, L., & Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys*, 54(1), 1–39. https://doi.org/10.1145/3427920.

Zong, S., Ritter, A., Mueller, G., & Wright, E. (2019). Analyzing the Perceived Severity of Cybersecurity Threats Reported on Social Media. *ArXiv:1902.10680 [Cs]*. https://arxiv.org/abs/1902.10680.