IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Cybersecurity Practices for Social Media Users

Name :- Dr. Khushbu Khandait
Designation :- Assistant Professor
College :- Ajeenkya D.Y.Patil University

Name :- Shreya Battise
College :- Ajeenkya D.Y .Patil
University Pune , Maharashtra , India

Abstract:

In this paper, we present secondary research on recommended cybersecurity practices for social media users from the user's point of view. Through following a structured methodological approach
of the systematic literature review presented, aspects related to cyber threats, cyber awareness, and cyber behavior in internet and social media use are considered in the study. The study presented finds that there are many cyber threats existing within the social media platform, such as loss of productivity, cyber bullying, cyber stalking, identity theft, social information overload, inconsistent personal branding, personal reputation damage, data breach, malicious software, service interruptions, hacks, and unauthorized access to social media accounts. Among other findings, the study also reveals that demographic factors, for example age, gender, and education level, may not necessarily be influential factors affecting the cyber awareness of the internet users.

Keywords: cybersecurity awareness; cybersecurity behavior; cybercrimes; cyber threats; cybersecurity; recommended cyber practices

Introduction

3. Identify the impact of users' cyber awareness on users' cyber behavior on social media. https://www.mdpi.com/journal/jcp

Citation: Shreya Battise. Cybersecurity Practices for Social Media Users: A Systematic Literature Review. J. Cybersecur. Priv. 2023-11-4.

The internet has become one of the primary communication channels in the modern era and social media possess a large portion of internet usage

([1] Bosse, Renner, and Wilkens, 2020). A total of 3.78 billion users are predicted to have used social media in 2021

([2] Tankovska, 2021 January 28). Most countries have acknowledged that cybersecurity has become one of the most critical issues that has emerged in the past few years with the increased usage of internet and social media

([3] Tosun et al., 2020). This might be due to the fact that high social media usage has become a new trend, reaching a wide range of people within a short time period

([4] Constantinides and Stagno, 2011; as cited by Okyireh and Okyireh, 2016). Additionally, the number of and types of available social media platforms, their less reliable design and construction, the large unstructured content, and more opportunities provided for people to act in malicious ways in those platforms have triggered the vulnerability of high-level cyber threats in social media

([5] Chaffey, 2016; Haimson and Hoffmann, 2016; Assunção et al., 2015; Fire et al., 2014; as cited by van der Walt, Eloff, and Grobler, 2018). Unfortunately, sole technical solution dedicated to overcoming security problems is still unavailable

([6] Scott-Cowley, 2014; as cited by Murire, Flowerday, Strydom, and Fourie, 2021). The above citations suggest that users cannot totally rely on technology to safeguard themselves from cyber threats when using internet or social media. Therefore, users have a responsibility to safeguard themselves from their own point of view. Hence, the main objectives of this article are identified asfollows:

1. Identify cyber threats in internet and social media use.

2. Identify factors affecting users' cyber awareness on social media platforms' securityrelatedfeatures.

3. Identify the impact of users' cyber awareness on users' cyber behavior on social media.https://www.mdpi.com/journal/jcp

. 4. Identify the impact of users' cyber behavior on their vulnerability level on social media. 5. Identify recommended cybersecurity practices for social media users from users' point of view

The structure of this article is organized with several sections. Section 2 of this article discusses the research methodology. Then, the themes and subthemes of the literature related to the article are further discussed in the following order: cyber threats on the internet are discussed in Section 2.1; cyber threats on social media are discussed in Section 2.1.1; cybersecurity on the internet is discussed in Section 2.2; user awareness when using the internet is discussed in Section 2.2.1; user behavior when using the internet is discussed in Section 2.2.2; cybersecurity in social media is discussed in Section 2.3; user awareness when using social media is discussed in Section 2.3.1; user behavior when using social media is discussed in Section 2.3.2. Next, Section 3 discloses the discussion along with the findings of the literature. Then, in Section 4, the limitations of the systematic literature review are discussed. Finally, the article is concluded with Section 5—future development—which illustrates the formation of main and sub research questions for the future research work, followed by Section 6, which provides our conclusion.

2. Methodology

Searching through the literature is a significant component of a systematic review.
The commonly used literature search component is the preferred reporting items for systematic reviews and meta-analyses (PRISMA) statement ([7] Rethlefsen et al., 2021). The PRISMA statement is used in this research article to filter the most relevant literature. The PRISMA statement is a road map that supports authors explaining what was carried out, what was found, and what are they planning to do next([8] Rafael, Ferran, Edoardo, and Craig, 2021). Additionally, the PRISMA checklist is a tool that can be used to guide systematic review reporting([9] Rice, Kloda, Shrier, and Thombs, 2016). The PRISMA statement consists of 4-stage flow diagram and 27 check list items([10] Moher, Liberati, Tetzlaff, and Altman, 2009). The adaptability of this article to the PRISMA statement is depicted in Table 1 and Figure 1, accordingly.

Table 1. The PRISMA checklist.

Section	Page No.
Title	1
Structured summary	1
Rationale	1
Objectives	1–2
Eligibility criteria	3
Information sources	3
Search	3
Study selection	3
Study selection	3
Summary of evidence	7–9
Limitations	9
Conclusions	10

When searching the literature, more than 10,000 probable articles were found usingWintec OneSearch and Google Scholar online databases with the help of relevant keywords and "AND" and "OR" operators. The main keywords used in the search of relevant articles were as follows: cyber threats, cybersecurity, cyber security, social media, user awareness, and user behavior. From that pool, only 2500 articles were revealed to be suitable, after removing duplicates. Then, only 339 of the most relevant articles were screened, and 170 articles were omitted from that pool due to ineligibility of the abstract. Next, 169 relevant articles were filtered from the pool of screened articles, and 126 of them were disregarded due to the exclusion criteria, as listed in Table 2. Finally, 43 articles were serelevant articles were filtered from the pool of screened articles, and 126 of them were and 170 articles wereomitted from that pool due to ineligibility of the abstract. Next,

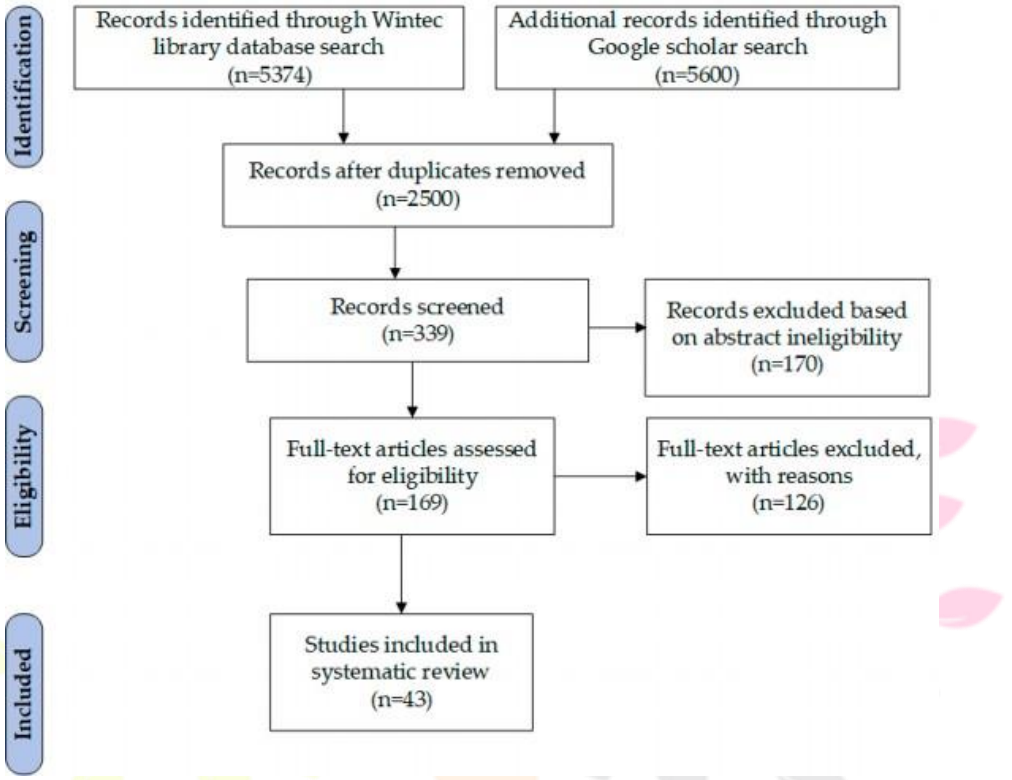

Figure 1. PRISMA flow chart.

Table 2. The PRISMA statement's inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Peer-reviewed articles with full access rights	Articles asking for payments for the access
Published time in between 2015–2021	Published outside the intended time frame
Language: English	Other languages
Full text	Articles with no full-text availability
Include relevant keywords	Not relevant to the literature themes
Original publication	Non-empirical studies

Inclusion Criteria Exclusion Criteria Peer-reviewed articles with full access rights Articles asking for payments for the access Published time in between 2015–2021 Published outside the intended time frame Language: English Other languages Full text Articles with no full-text availability Include relevant keywords Not relevant to the literature themes Original publication Non-empirical studies After filtering relevant literature, the main themes and subthemes were identified as per the concept map, as illustrated in Figure 2. This allowed the readers to refer to each piece of literature easily, as per their preference. All the pieces of literature listed in the concept map are elaborated in detail under the three main subsections within Section 2 and the five subsections within them. The main sections are as follows: Section 2.1. Cyber threats on the Internet; Section 2.2. Cybersecurity on the Internet; Section 2.3. Cybersecurity on Social Media. These main subsections are divided

further into other subsections, as follows: Section 2.1.1. Cyber Threats on Social Media; Section 2.2.1. User Awareness When Using the Internet; Section 2.2.2. User Behavior When Using the Internet; Section 2.3.2. User Awareness When Using Social Media; Section 2.3.2. User Behavior When Using Social Media. The literature depicted in the concept map are further elaborated in the tables listed under Appendix A of the article.

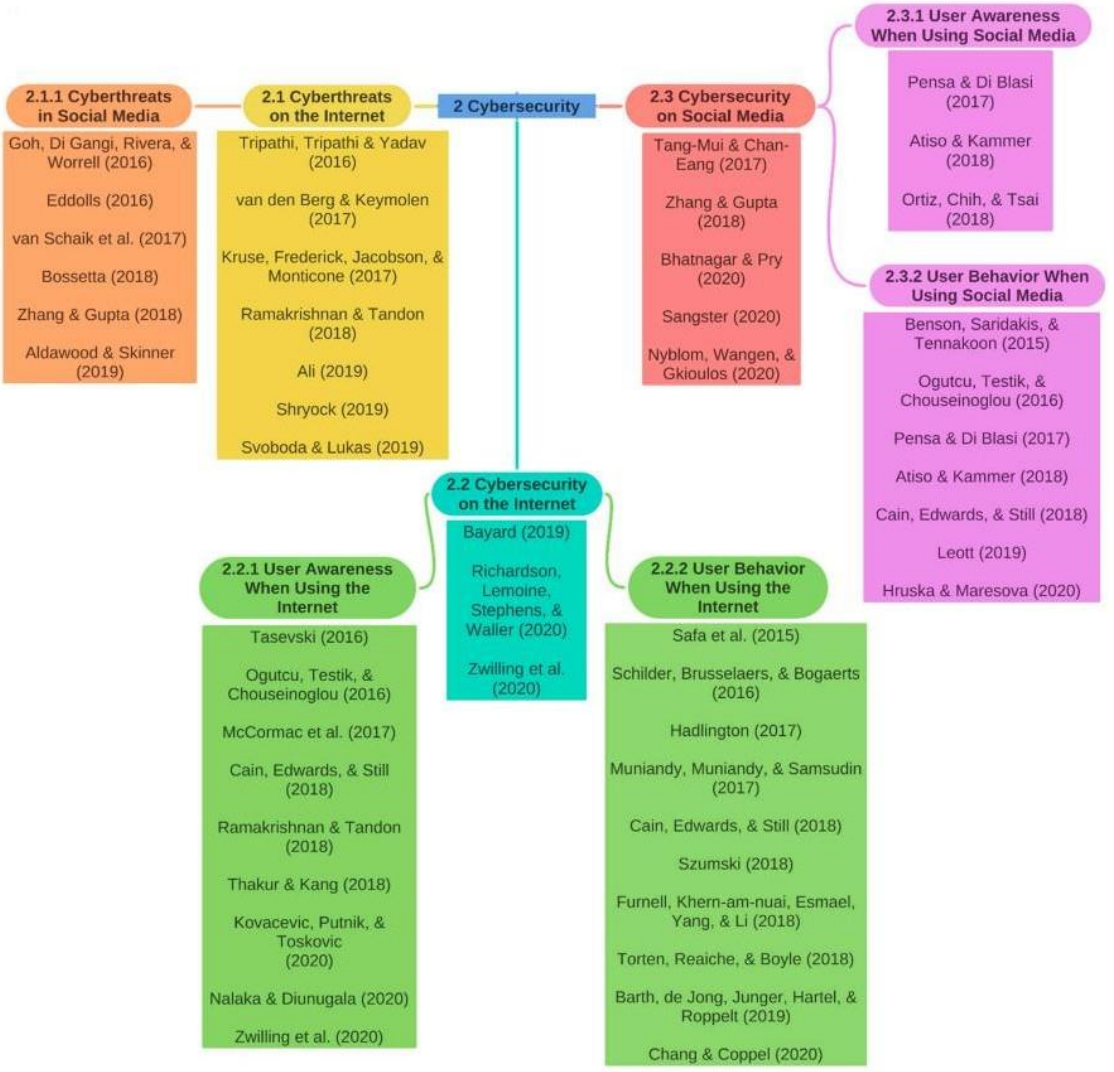

Figure 2. Concept map of the literature related to cyber threats and cybersecurity.

Figure 2. Concept map of the literature related to cyber threats and cybersecurity.

2.1. Cyber Threats on the Internet

The evolution of cybercrimes in the IT industry dates back to late 1970s. It has evolved from just spam at that time to much more advanced forms, such as viruses and malware, in the present day

([11] Jobs, 2016; as cited by Kruse, Frederick, Jacobson, and Monticone, 2017). The word "Cybercrimes" covers a vast range of virtual illegal activities performed by cybercriminals via any source of internet-connected electronic device

([12] Ali, 2019). Experts say that cybercriminals often aim for easy targets with the least resistance, even though they possess many sources, as well as a high level of knowledge on how the technology works and its vulnerabilities. The reason for this is that they can easily commence the hacking with less effort with that kind of user

([13] Shryock, 2019). Gullible users often become targets of hackers and cybercriminals use creative and different ways to collect personal data from them

([14] Ramakrishnan and Tandon, 2018). The internet has become an essential part of society and it has become the core of connecting and sharing information in modern days. This has led the internet to become a target of various cyber threats, ranging from cybercrimes (hacking, identity theft, and other forms of fraud) to cyber espionage, cyber terrorism, and cyber warfare

([15] van den Berg and Keymolen, 2017). Cybercrimes cover various cyber threats, including child pornography, fraud, email abuse, missing children, stalking, copyright, violation, harassment, threats, children abuse hacking, viruses, and many more

([16] Tripathi, Tripathi, and Yadav, 2016). The impact of cyber threats is changing, based on globalization, imposed security environment level, awareness, and the education level of the administrators and users of a given information and communication environment. These cyber threats can range from privacy, personal, confidential, and classified data loss and fund/cryptocurrency loss to harm to the health and/or life of a person ([17] Svoboda and Lukas, 2019).

2.1.1. Cyber Threats on Social Media

There are two major categories of social media risks. One is social risk and the other is technology risk. Social risks further branch into two categories, namely individuallevel risk and professional-level risk. Loss of productivity, cyberbullying, cyberstalking, identity theft, and social information overload belong to individual-level risks, while inconsistent personal branding, personal reputational damage, and data breach belong to professional-level risks. Technology risks mainly include malicious software, service interruptions, hacks, and unauthorized access to social media accounts ([18] van Zyl, 2009; Krasnova et al., 2009; Hogben, 2007; Krasnova et al., 2009; Boyd, 2008;
Argenti and Druckenbiller, 2004; Aula, 2010; Boyd, 2008; Hogben, 2007; Rivera et al., 2015; as cited by Goh, Di Gangi, Rivera, and Worrell, 2016). Cracking a password becomes easy for a hacker who possesses the right software tools and a few personal data, gained from someone's social media ([19] Eddolls, 2016). Fake accounts, cyberbullying, and sexual harassment are some of the major malicious behaviors that can be identified within the social media sphere ([20] van Schaik et al., 2017). Various cyberattacks are present in social media, such as identity theft, spam attacks, malware attacks, Sybil attacks, social phishing, impersonation, hijacking, fake requests, and image retrieval and analysis ([21] Zhang and Gupta, 2018). Additionally, social media has become a major playground for spear phishing attacks ([22] Bossetta, 2018) and social engineering ([23] Wilcox, Bhattacharya, and Islam, 2014; as cited by Aldawood and Skinner, 2019).

2.2. Cybersecurity on the Internet

Cybersecurity is a collection of techniques that have been established to protect individual users' or organizations' cyber environments ([24] Seemma, Nandhini, and Sowmiya, 2018; as cited by Richardson, Lemoine, Stephens, and Waller, 2020). A cybersecurity culture protects information systems, computer networks, user data, and internet users effectively ([25] Patrascu, 2019). Most of the cyber attacks are preventable or at least can be handled carefully; although, there is no perfect defense against them ([26] Kenyon, 2018; as cited by Bayard, 2019). The impact of security breaches cannot be fully eliminated by simply using security tools in computers and infrastructure—this is because human error is the weakest link in the cybersecurity chain ([27] Furnell et al., 2006; Parsons et al., 2014; Schultz, 2005; Anwar et al., 2017; Herath, and Rao, 2009; Schneie, 2004; as cited by Zwilling et al., 2020). 2.2.1. User Awareness When Using the Internet Cybersecurity awareness is the level of understanding achieved by users regarding the significance of information security, their associated responsibilities, and a series of acts to practice an adequate degree of information security control, safeguarding organizational data and networks ([27] Shaw et al., 2009; as cited by Zwilling et al., 2020). The first level of defense with regard to information systems' security and networks is awareness. When it comes to the internet, cybersecurity situational awareness is crucial, since it supports in the prevention of compromise of data, information, knowledge, and wisdom ([28] Tasevski, 2016). In one study, older adults had higher information security awareness (ISA) scores than young adults, and a small significant difference was found in the ISA score related to gender, where females have higher ISA scores, compared with males ([29] McCormac et al., 2017). In contrast to this citation, another research article stated otherwise, indicating that males have more cyber hygiene knowledge than females; however, surprisingly, there was no difference in cyber hygiene knowledge among different age groups ([30] Cain, Edwards, and Still, 2018). In the research, it was found that higher education levels lead to higher information security awareness of the users. It has been found that higher education level or information security training reduces risky user behavior ([31] Ogutcu, Testik, and Chouseinoglou, 2016). In the multinomial regression analysis, it was found that people with higher education, who are not living in their own housing, more often fall into the cybercrime victims category ([32] Oksanen, and Keipi, 2013, as cited by Nalaka and Diunugala, 2020). Internet users should always be updated on cyber threats as new threats are emerging and existing threats are evolving frequently. Unfortunately, most users have failed to achieve an acceptable level of protection, compared with the increasing rate of threats ([14] Ramakrishnan and Tandon, 2018). Human beings are the central figure of cybersecurity, and they should be highly equipped with security awareness to mitigate the risks they face in cyberspace ([33] Kovacevic, Putnik, and Toskovic, 2020). Factors including a lack of awareness of cyber risks and use of third-party apps, information distributed in social media, and web pages direct hackers to easily exploit these vulnerable users ([27] Shaw et al., 2009; as cited by Zwilling et al., 2020). Lack of awareness in cybercrimes can lead to high-level damage to finances, emotions, and the ethical or moral values of users ([34] Thakur and Kang, 2018).

2.2.2. User Behavior When Using the Internet

Online privacy research has found that users are interested in privacy protection, but their actual behavior says otherwise. This inconsistency between expressed privacy concerns and actual, contradictory behavior is known as the privacy paradox ([35] Barth and De Jong, 2017; Joinson et al.,

2010; Tsai et al., 2006; as cited by Barth, de Jong, Junger, Hartel, and Roppelt, 2019). Intentional or unintentional vulnerable user behavior is one of the major issues in the information security sphere ([36] Safa et al., 2015). Research results showed that higher awareness was connected with a lower number of reported online risk behaviors ([37] Schilder, Brusselaers, and Bogaerts, 2016). In the research, it was identified that the cybersecurity behavior of the respondents potentially makes them vulnerable to cyber threats ([38] Muniandy, Muniandy, and Samsudin, 2017). Lack of understanding regarding appropriate cybersecurity actions can lead end users to inappropriate cyber behavior ([30] Debatin et al., 2009; Goodhue, and Straub, 1991; Hu, Hart, and Cooke, 2006; Straub, and Welke, 1998; as cited by Cain et al., 2018). The research findings revealed that user awareness improvements lead to better security behavior ([39] Furnell, Khern-am-nuai, Esmael, Yang, and Li, 2018). Security awareness impacts user behavior when protecting against risks in information security ([40] Herath, and Rao, 2009; Thomson, and Solms, 1998; Puhakainen, and Siponene, 2010; as cited by Torten, Reaiche, and Boyle, 2018). On the other hand, a study conducted by the Global Cybersecurity Capacity Centre at the University of Oxford found that campaigns on cybersecurity awareness were unsuccessful in changing behavior ([41] Bada et al., 2015; as cited by Chang and Coppel, 2020). Addiction to the internet leads to risky cybersecurity behavior ([42] Giffiths, 2010; as cited by Hadlington, 2017). Older users have more secure behavior than younger users ([30] Cain et al., 2018). A proportion of 63% of the Polish students who responded to one study mentioned that they use a "best practices" approach; however, this term is not clear and can be highly subjective— because their main sources of cybersecurity knowledge are the internet, friends, or colleagues ([43] Szumski, 2018). 2.3. Cybersecurity on Social Media Social media is

a collection of electronic communication platforms used by online users to create online communities. They use these platforms to share information, ideas, and personal messages with each other ([44] Bhatnagar and Pry, 2020). Social media networks provide openness to user profiles and the data they share in the profile. However, this openness threatens user profiles with being revealed or hacked ([45] Tang-Mui and Chan-Eang, 2017). Most of the social media users are now addicted to sharing their ideas, sentiments, and experiments with a wide range of friends and friends of friends, via videos and photos ([21] Yan, 2016; as cited by Zhang and Gupta, 2018). People who post information online might not think of security risks associated with it primarily. However, this action can voluntarily reveal more personal information to unknown people than they expected ([46] Nyblom, Wangen, and Gkioulos, 2020). Employees should be more careful about what they share on social media, sincesocial engineering scams are rising gradually in modern days. Those data can be used against them and their company, together with other personal data that the cybercriminals collected through other consumer data breaches ([47] Wikipedia, 2020; as cited by Sangster, 2020).

2.3.1. User Awareness When Using Social Media

Disclosing data that have been perceived as less sensitive in social media platforms by the users can also lead to privacy breaches and user awareness around that sphere is still insufficient. One common example of the above matter is GPS tagging of a place that a user is currently visiting, which may alert thieves to commence a robbery in that user's home or apartment. Another example is that disclosing family relationships on social media may lead to privacy issues, such as stalking, slander, and cyberbullying for that family member(s) ([48] Pensa and Di Blasi, 2017). A stronger information security concern level can be achieved by a high level of privacy awareness ([49] Boyd, and Hargittai, 2010; as cited by Ortiz, Chih, and Tsai, 2018). Most social media users are unaware of the risks and vulnerabilities associated with those platforms unless they have experienced those in their real lives ([50] Atiso and Kammer, 2018). 2.3.2. User Behavior When Using Social Media Awareness of controlling privacy settings in social media is usually limited to the users and thereby limited in actual use as well ([48] Pensa and Di Blasi, 2017). High-level use of social network sites leads to a high level of self-disclosure behavior ([51] Trepte, and Reinecke, 2013; as cited by Benson, Saridakis, and Tennakoon, 2015). High-level usage of social media makes some users more vulnerable. Those vulnerabilities made them face scams and behave online in a fearful and distrusting manner ([50] Kaplan, and Haenlein, 2010; as cited by Atiso and Kammer, 2018).

Attackers always look for vulnerabilities, such as users with poor best practices or more self- disclosure behaviors. Most of the elderly and young participants of a survey study revealed that they have shared too many personal details on social media, including their phone numbers and addresses; the risky side of this behavior is that most of them do not check their privacy settings related to their social media accounts ([30] Cain et al., 2018). Most of the undergraduate participants in another study use social media platforms to connect with family and friends, to initiate and sustain relationships, to pass the time, to gain entertainment, and to express themselves ([52] Park, and Lee, 2014; Sherrel, L. and Lambie, 2016; Kushin, and Yamamoto, 2010; as cited by Leott, 2019). In the research, it was found that the high-risk category includes students from the age range 18–30 years. A possible reason for this is the high usage of the internet, especially social media and social networks ([31] Ogutcu et al., 2016). Social media usage decreases with age and the usage increases when income and education level increase ([53] Hruska and Maresova, 2020). 3. Discussion Based on the aforementioned literature, it was found that there are many cyber threats existing within social media platforms, such as loss of productivity, cyberbullying, cyberstalking, identity theft, social information overload, inconsistent personal branding, Me personal reputational damage, data breach, malicious software, service interruptions, hacks, unauthorized access to social media accounts ([18] van Zyl, 2009; Krasnova et al., 2009; Hogben, 2007; Krasnova et al., 2009; Boyd, 2008;
Argenti and Druckenbiller, 2004; Aula, 2010; Boyd, 2008; Hogben, 2007; Rivera et al., 2015; as cited by Goh et al., 2016), cracking a password ([19] Eddolls, 2016), fake accounts, sexual harassments ([20] van Schaik et al., 2017), spam attacks, malware attacks, Sybil attacks, impersonation, hijacking, fake requests, image retrieval and analysis ([21] Zhang and Gupta, 2018), spear phishing attacks ([22]Bossetta, 2018), and social engineering ([23] Wilcox, Bhattacharya, and Islam, 2014; as cited by Aldawood and Skinner, 2019). All users should have enough current and updated cyber awareness and cyber behavior to safeguard themselves from the aforementioned cyber threats. Tragically, most users have failed to achieve an acceptable level of protection compared with the increasing rate of threats ([14] Ramakrishnan and Tandon, 2018). People who post information online might not think of security risks associated with this behavior. However, this action can voluntarily reveal more personal information to unknown people than they expected ([46] Nyblom et al., 2020). It is also revealed that most social media users are unaware of the risks and vulnerabilities associated with those platforms unless they have experienced those in their real lives ([50] Atiso and Kammer, 2018). Hence, it is always recommended that users take enough precautions to safeguard themselves from cybercrimes from their point of view, since the most powerful user privacy protection strategy in social media platforms falls into users' own hands. Only they can control what they publish,

and to whom, on those platforms ([48] Pensa and Di Blasi, 2017). When it comes to factors affecting cyber awareness, it was discovered that age, gender, and education level may or may not affect the cyber awareness of internet users. Older adults had higher information security awareness (ISA) scores than young adults. A small significant difference was found in the ISA score related to gender, where females had higher ISA scores compared with males ([29] McCormac et al., 2017). In contrast to this citation, another research article stated otherwise, finding that males have more cyber hygiene knowledge than females; however, surprisingly, there was no difference in cyber hygiene knowledge among different age groups ([30] Cain et al., 2018). In the research, it was found that higher education levels lead to higher information security awareness of the users—higher education levels or information security training reduces risky user behavior ([31] Ogutcu et al., 2016). However, in a multinomial regression analysis, it was found that people with higher education and who are not living in their own housing are more likely to fall into the cybercrime victims category ([32] Oksanen, and Keipi, 2013, as cited by Nalaka and Diunugala, 2020). Several items of the literature support the idea that cyber awareness has an impact on cyber behavior. Research results show that higher awareness was connected with a lower number of reported online risky behaviors ([37] Schilder, Brusselaers, and Bogaerts, 2016). Lack of understanding regarding appropriate cybersecurity actions can lead end users to inappropriate cyber behavior ([30] Debatin et al., 2009; Goodhue, and Straub, 1991; Hu, Hart, and Cooke, 2006; Straub, and Welke, 1998; as cited by Cain et al., 2018). The research findings revealed that user awareness improvements lead to better security behavior ([39] Furnell, Khern-am-nuai, Esmael, Yang, and Li, 2018). Security awareness impacts user behavior when protecting against risks in information security ([40] Herath, and Rao, 2009; Thomson, and Solms, 1998; Puhakainen, and Siponene, 2010; as cited by Torten, Reaiche, and Boyle, 2018). On the other hand, a study conducted by the Global Cybersecurity Capacity Centre at the University of Oxford found that campaigns on cybersecurity awareness were unsuccessful in changing behavior ([41] Bada et al., 2015; as cited by Chang and Coppel, 2020); additionally, they found that cyber behavior has an impact on the vulnerability level that users face. In another study, it was identified that the cybersecurity behavior of the respondents potentially makes them vulnerable to cyber According to the research findings, it was identified that the cyber awareness of a user plays a vital role to overcome various cyber threats in cyberspace. Some researchers find a given user's age, gender, and education level have an impact on their cyber awareness; although, some researchers disagree on this. Additionally, some studies suggest that users' cyber awareness has an impact on users' secure cyber behavior, while some studies suggest that this is not the case. The authors were unable to

identify enough literature to analyze the impact of users' secure cyber behavior on their vulnerability level, specifically relevant to social media. Figure 3 summarizes the overall findings of the discussion section.

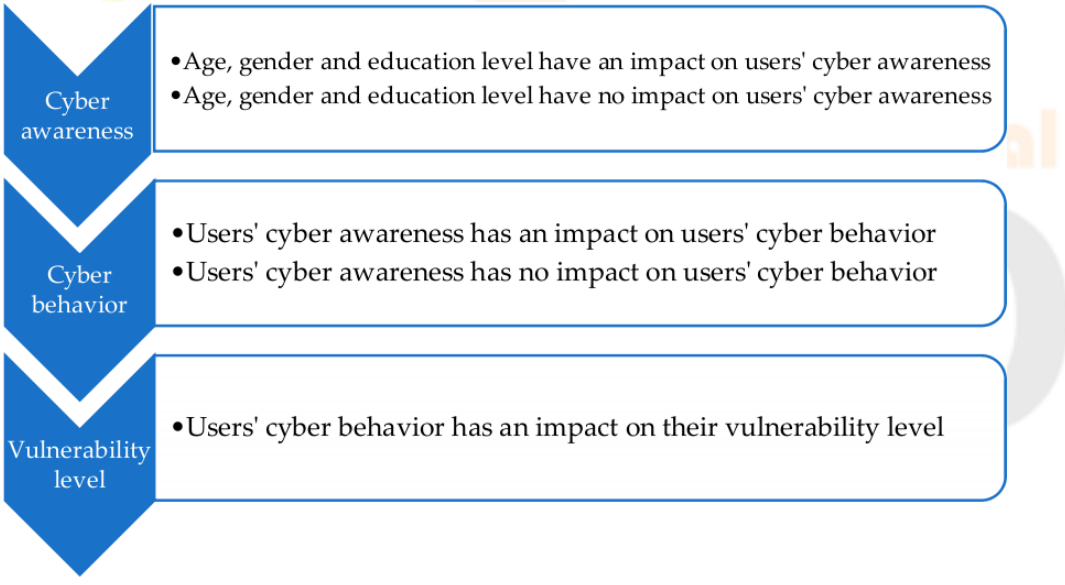

Figure 3. Summary of findings.

Figure 3. Summary of findings.

4. Limitations

Based on the findings in the discussion section of the systematic literature review, some significant limitations have been identified by the authors, as follows:

(1) The authors were unable to identify any studies relevant to recommended cybersecurity practices for social media users from users' points of view, to the best of their knowledge.

(2) The authors were unable to filter any studies discovering the impact of social media users' age, gender, and education level on users' awareness on social media platforms' security-related features, to the best of their knowledge.

(3) The authors were unable to find any studies revealing the impact of social media users' awareness of social media platforms' security-related features on social media users' secure behaviorin it, to the best of their knowledge.

(4) The authors were unable to find enough studies disclosing the impact of social media users' secure behavior on their vulnerability level in the platform, to the best of their knowledge. Weaim to explore the above aspects in our future research to enhance/expand the review presented in this paper.

5. Future Works

The present research was mainly focused on identifying recommended cybersecurity
practices for social media users from users' points of view. Additionally, it intended to identify the factors affecting users' awareness on social media platforms' security-related features and impact of social media users' awareness on their behavior in social media platforms. However, above topics arenot significantly addressed in the past literature, to the best of the authors' knowledge. There were not enough studies found to identify the impact of social media users' secure behavior on their
vulnerability level in the platform. Therefore, it may be worthwhile to carry out further research, considering these variables (including their correlations), to identify recommended cybersecurity practices for social media users from users' points of view. The limitations mentioned earlier are alsoareas worth investigating.

6. Conclusions

Cybersecurity, within the context of social media, is a timely topic to be discussed considering its large user base all around the world. There are many cyberattacks existing in the current social media sphere, according to the literature discussed in this article. Although there is an in-built security framework within the different social media platforms, it may not be enough to protect the social media users from cyber attacks. This is due to human error, where there is the possibility of opening backdoors for commencing cyber attacks. User awareness and user behavior play a major role to reduce the impact of human errors. The impact of factors, such as age, gender, and the education level of the users on their cyber awareness in social media platforms' security features is not clear, based on the current literature found. However, the impact of cyber awarenessover cyber behavior is backed by several studies, discussed in the article. Additionally, there is not
enough evidence to prove the impact of users' secured cyber behavior on their vulnerability level on social media platforms. Hence, further research is crucial to identify the factors affecting user awareness, users' secure behavior, and users' vulnerability level on social media platforms.
Moreover, it is significant to discover recommended cybersecurity practices for social media users, based on the impact of the aforementioned variables.

References

1. Bosse, I.; Renner, G.; Wilkens, L. Social media and Internet use patterns by adolescents with complex communication needs. Lang. Speech Hear. Serv. Sch. 2020, 51, 1024–1036. [CrossRef][PubMed]

2. Tankovska, H. Number of Global Social Network Users 2017–2025. 2021. Available online: https://www.statista.com/statistics/ 278414/number-of-worldwide-social-network-users/ (accessed on 10 January 2021).

3. Tosun, N.; Altinoz, M.; Cay, E.; Cinkilic, T.; Gulseçen, S.; Yildirim, T.; Aydin, M.A.; Metin, B.;Ayvaz Reis, Z.; Unlu, N. A SWOT Analysis to Raise Awareness about Cyber Security and Proper Use of Social Media: Istanbul Sample. Int. J. Curric. Instr. 2020, 12, 271–294.

4. Okyireh, R.O.; Okyireh, M.A.A. Experience of Social Media, Training and Development on Work Proficiency: A Qualitative Study with Security Personnel. J. Educ. Pract. 2016, 7, 122–127.

5. van der Walt, E.; Eloff, J.; Grobler, J. Cyber-security: Identity deception detection on social media platforms. Comput. Secur. 2018, 78, 76–89. [CrossRef]

6. Murire, O.T.; Flowerday, S.; Strydom, K.; Fourie, C.J.S. Narrative review: Social media use by employees and the risk to institutional and personal information security compliance in South Africa. J. Transdiscipl. Res. S. Afr. 2021, 17, e1–e10.

[CrossRef]

7. Rethlefsen, M.L.; Kirtley, S.; Waffenschmidt, S.; Ayala, A.P.; Moher, D.; Page, M.J.; Koffel, J.B. PRISMA-S: An extension to the PRISMA statement for reporting literature searches in systematic reviews. J. Med. Libr. Assoc. 2021, 109, 174–200. [CrossRef]

8. Rafael, S.-O.; Ferrán, C.-L.; Edoardo, A.; Craig, L. How to properly use the PRISMA statement. Syst. Rev. 2021, 10, 1–3. [CrossRef]

9. Rice, D.B.; Kloda, L.A.; Shrier, I.; Thombs, B.D. Reporting completeness and transparency of meta-analyses of depression screening tool accuracy: A comparison of meta-analyses published before and after the PRISMA statement. J. Psychosom. Res. 2016, 87, 57–69. [CrossRef]

10. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. BMJ Br. Med. J. 2009, 339, 332–336. [CrossRef]

11. Kruse, C.S.; Frederick, B.; Jacobson, T.; Monticone, D.K. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol. Health Care 2017, 25, 1–10. [CrossRef] 12. Ali, L. Cyber crimes—A constant threat for the business sector and its growth (A study of the online banking sector in GCC). J. Dev. Areas 2019, 53. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct= true&db=edsbig&AN=edsbig.A554041623&site=eds-live&scope=site (accessed on 12 January 2021). [CrossRef

] 13. Shryock, T. The growing cyber threat: Practices are increasingly coming under attack by cyber criminals. Med. Econ. 2019, 96, 22. Available online:
http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db= edsgac&AN=edsgac.A590952666&site=eds-live&scope=site (accessed on 15 January 2021).

14. Ramakrishnan, U.P.; Tandon, J.K. The evolving lanscape of cyber threats. Vidwat Indian J. Manag. 2018, 11, 31–35. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth &AN=13923579 7&site=eds-live&scope=site (accessed on 18 January 2021).

15. Van den Berg, B.; Keymolen, E. Regulating security on the Internet: Control versus trust. Int. Rev. Law Comput. Technol. 2017, 31, 188–205. [CrossRef]

16. Tripathi, E.; Tripathi, A.; Yadav, M.K.S. Role of information technology in cyber crime and ethical issues in cyber ethics. Int. J. Bus. Eng. Res. 2016, 10, 1–5. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct= true&db=egs&AN=139360194&site=eds-live&scope=site (accessed on 18 January 2021)

17. Svoboda, J.A.N.; Lukas, L. Sources of threats and threats in cyber security. DAAAM Int. Sci. Book 2019, 321–330. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edo &AN=14006292 1&site=eds-live&scope=site (accessed on 18 January 2021).

18. Goh, S.H.; Di Gangi, P.M.; Rivera, J.C.; Worrell, J.L. Graduate student perceptions of personal social media risk: A comparison study. Issues Inf. Syst. 2016, 17, 109–119. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/ login.aspx?direct=true&db=edo&AN=119120441&site=eds-live&scope=site (accessed on 19 January2021).

19. Eddolls, M. Making cybercrime prevention the highest priority. Netw. Secur. 2016, 2016,5–8. [CrossRef]

20. Van Schaik, P.; Jeske, D.; Onibokun, J.; Coventry, L.; Jansen, J.; Kusev, P. Risk perceptions of cyber-security and precautionary behaviour. Comput. Hum. Behav. 2017, 75, 547–559. [CrossRef]
21. Zhang, Z.; Gupta, B.B. Social media security and trustworthiness: Overview and new direction. Futur. Gener. Comput. Syst. 2018, 86, 914–925. [CrossRef] 22. Bossetta, M. The weaponization of social media: Spear phishing and cyber attacks on democracy. J. Int. Aff. 2018, 71, 97–106. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth &AN= 132491875&site=eds-live&scope=site (accessed on 19 January 2021). 23. Aldawood, H.; Skinner, G. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet 2019, 11, 73. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.

aspx?direct=true&db=edb&AN=135682631&site=eds-live&scope=site (accessed on 1 February 2021).[CrossRef]

24. Richardson, M.D.; Lemoine, P.A.; Stephens, W.E.; Waller, R.E. Planning for cyber security in schools: The human factor. Educ. Plan. 2020, 27, 23–39. Available online:
http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=
true&db=eric&AN=EJ1252710&site=eds-live&scope=site (accessed on 2 February 2021).

25. Patrascu, P. Promoting cybersecurity culture through education. eLearning Softw. Educ. 2019, 2, 273–279. [CrossRef] 26. Bayard, E.E. The rise of cybercrime and the need for state cybersecurity regulations. Rutgers Comput. Technol. Law J. 2019, 45, 69–96. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=
egs&AN=144292728&site=eds-live&scope=site (accessed on 2 February 2021). 27. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A Comparative Study. J. Comput. Inf. Syst. 2020, 1–16. [CrossRef] 28. Tasevski, P. IT and cyber security awareness-raising campaigns. Inf. Secur. 2016, 34, 7. [CrossRef] 29. McCormac, A.; Zwaans, T.; Parsons, K.; Calic, D.; Butavicius, M.; Pattinson, M. Individual differences and Information Security Awareness. Comput. Hum. Behav. 2017, 69, 151–156. [CrossRef] 30. Cain, A.A.; Edwards, M.E.; Still, J.D. An exploratory study of cyber hygiene behaviors and knowledge. J. Inf. Secur. Appl. 2018, 42, 36–45. [CrossRef] 31. Ogutcu, G.; Testik, O.M.; Chouseinoglou, O. Analysis of personal information security behavior and awareness. Comput. Secur. 2016, 56, 83–93. [CrossRef] 32. Nalaka, S.; Diunugala, H. Factors associating with social media related crime victimization: Evidence from the undergraduates at a public university in Sri Lanka. Int. J. Cyber Criminol. 2020, 14, 174–184. Available online: http://wintec.idm.oclc.org/ login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edo&AN=143029465&site=ed s- live&scope=site (accessed on 6 February 2021). 33. Kovacevic, A.; Putnik, N.; Toskovic, O. Factors related to cyber security behavior. IEEE Access 2020, 8, 125140–125148. [CrossRef] 34. Thakur, A.; Kang, T.K. Gender and locale differences in cyber crime awareness among adolescents. Indian J. Health Wellbeing 2018, 9, 906–916. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=
edb&AN=134949110&site=eds-live&scope=site (accessed on 7 February 2021). 35. Barth, S.; de Jong, M.D.T.; Junger, M.; Hartel, P.H.; Roppelt, J.C. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. Telemat. Inform. 2019, 41, 55–69. [CrossRef] 36. Safa, N.S.; Sookhak, M.; Von Solms, R.; Furnell, S.; Ghani, N.A.; Herawan, T. Information security conscious care behaviour formation in organizations. Comput. Secur. 2015, 53, 65–78. [CrossRef] 37. Schilder, J.; Brusselaers, M.; Bogaerts,
S. The Effectiveness of an intervention to promote awareness and reduce online risk behavior in early adolescence. J. Youth Adolesc. 2016, 45, 286–300. [CrossRef] 38. Muniandy, L.; Muniandy, B.; Samsudin, Z. Cyber security behaviour among higher education students in Malaysia. J. Inf. Assur. Cyber Secur. 2017, 2017, 1–13. [CrossRef] 39. Furnell, S.; Khern-am-nuai, W.; Esmael, R.; Yang, W.; Li,
N. Enhancing security behaviour by supporting the user. Comput. Secur. 2018, 75, 1–9. [CrossRef] 40.
Torten, R.; Reaiche, C.; Boyle, S. The impact of security awareness on information technology
professionals' behavior. Comput. Secur. 2018, 79, 68–79. [CrossRef] 41. Chang, L.Y.C.; Coppel, N. Building cyber security awareness in a developing country: Lessons from Myanmar. Comput. Secur. 2020, 97, 101959. [CrossRef] 42. Hadlington, L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon 2017, 3, 7. [CrossRef] [PubMed] 43. Szumski, O. Cybersecurity best practices
among Polish students. Procedia Comput. Sci. 2018, 126, 1271–1280. [CrossRef] 44. Bhatnagar, N.; Pry, M. Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. Inf. Syst. Educ. J. 2020, 18, 48–58. Available online:
http://wintec.idm.oclc.org/login?url=http://search.
ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1246231&site=eds-live&scope=site (accessed on 12 February 2021). 45. Tang-Mui, J.; Chan-Eang, T. Impacts of social media (Facebook) on human communication and relationships: A view on behavioral change and social unity. Int. J. Knowl.
Content Dev. Technol. 2017, 7, 27–50. [CrossRef] 46. Nyblom, P.; Wangen, G.; Gkioulos, V. Risk perceptions on social media use in Norway. Future Internet 2020, 12, 211. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb &AN=147738607&site=eds-live&scope=site (accessed on 12 February 2021). [CrossRef] 47. Sangster,
M. When it comes to cyber security, ignorance isn't bliss—It's negligence. Netw. Secur. 2020, 2020, 8–12. [CrossRef] 48. Pensa, R.G.; Di Blasi, G. A privacy self-assessment framework for online social networks. Expert Syst. Appl. 2017, 86, 18–

31. [CrossRef] 49. Ortiz, J.; Chih, W.-H.; Tsai, F.-S. Information privacy, consumer alienation, and lurking behavior in social networking sites. Comput. Hum. Behav. 2018, 80, 143–157. [CrossRef] 50. Atiso, K.; Kammer, J. User beware: Determining vulnerability in social media platforms for users in Ghana. Libr. Philos. Pract. 2018, 1–25. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=
lxh&AN=133873708&site=eds-live&scope=site (accessed on 14 February 2021). 51. Benson, V.; Saridakis, G.; Tennakoon, H. Information disclosure of social media users. Inf. Technol. People 2015, 28, 426–441. [CrossRef] 52. Leott, Y.M. #Screening out: Criminal justice students' awareness of social media usage in policing. Cogent Soc. Sci. 2019, 5. [CrossRef] 53. Hruska, J.; Maresova, P. Use of Social Media Platforms among Adults in the United States—Behavior on Social Media. Societies 2020, 10,
27. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=142616553&site=eds-live&scope=site (accessed on 14 February 2021). [CrossRef].