UJEAS

UNIZIK JOURNAL OF ENGINEERING AND APPLIED SCIENCES

UNIZIK Journal of Engineering and Applied Sciences 5(2), June (2025), 2587-2604
Journal homepage: https://journals.unizik.edu.ng/index.php/ujeas
PRINT ISSN: 2992-4383 || ONLINE ISSN: 2992-4391

The impact of social media on cybersecurity awareness

Musab Mubaraq Mburaimoh[1] and *[2]Kile Awuna Samuel
[1]Department of Computer Science, National Open University of Nigeria, Abuja
[2]Department of Computer Science, University of Maiduguri, Maiduguri, Borno State
*Corresponding Author's E-mail: awunkile2@gmail.com

Abstract
The rapid growth of social media in Nigeria has transformed communication and business but also introduced cybersecurity threats like phishing and identity theft, with limited awareness of their impact. This study assessed social media's influence on cybersecurity awareness among Nigerian users, evaluating awareness levels, information dissemination, and behavioral changes. Using a descriptive survey design, 1,000 adult social media users were selected via stratified random sampling. Data was collected through questionnaires on platforms like Facebook and WhatsApp and analyzed using descriptive and inferential statistics (chi-square tests). Findings showed most respondents understood basic cybersecurity concepts, such as malware and multi-factor authentication. Over 65% encountered cybersecurity content on social media, with more than half improving their online practices due to this exposure. Gender significantly influenced awareness, suggesting a need for gender-sensitive strategies, while age, education, and usage frequency showed no significant correlation. Social media effectively promoted awareness but also posed risks like misinformation. The study concludes that social media is a valuable tool for enhancing cybersecurity awareness and safer practices if challenges like trust gaps and content overload are addressed. Recommendations include interactive, gender-sensitive campaigns, ensuring credible information, and fostering collaborations between social media platforms and cybersecurity organizations.

Keywords: Awareness, cybersecurity, digital literacy, online safety, social media and trust.

1. Introduction

Social media's pervasiveness in daily life has significantly influenced how individuals perceive and respond to cybersecurity threats. Research indicates that the widespread use of social media sites like Facebook, LinkedIn, and Twitter presents both opportunities and challenges for enhancing cybersecurity awareness; while these platforms enable rapid dissemination of security information, they also expose users to risks such as phishing, social engineering, and misinformation (Alotaibi et al., 2021; Herath et al., 2022). To understand how individuals process these risks and adopt protective behaviors, this study is guided by the Protection Motivation Theory (PMT). PMT explains how people are motivated to react in protective ways when faced with perceived threats, based on four key factors: perceived severity, perceived vulnerability, response efficacy, and self-efficacy. Applying PMT in the context of social media and cybersecurity helps clarify how users interpret online threats and what drives their decisions to implement secure practices such as multi-factor authentication or cautious information sharing.

Social media platforms have completely changed how people and organizations interact, exchange information, and do business. These platforms have improved communication and the spread of information, but they have also created serious cybersecurity risks and vulnerabilities. Because of its wide audience and high user involvement, social media has emerged as a top target for cybercriminals looking to take advantage of organizational and personal data. By disclosing staff contacts or internal information, social networking platforms can increase a company's

attack surface. Chin (2025) stated that cybercriminals can then use these resources to carry out phishing attacks, credential theft, data theft, and other frauds. Employees' own social media profiles are subject to the same hazards. In the same view, DHS NCSAM (2020) informed that businesses are especially at risk from people who regularly share private information on social networking platforms. By disclosing private information, individuals not only expose themselves to danger, but they also provide hackers access to a database that they may use to launch focused assaults. Malicious content and false information can proliferate through social media. Cheong Hin Hong et al. (2022) opined that these platforms are a double-edged sword in terms of cybersecurity because of their anonymity and wide reach.

According to Herath, Khanna, and Ahmed (2022), when social media sites actively supports awareness efforts, students who regularly used the platform were more informed about cybersecurity measures. According to Alharbi and Tassaddiq (2021), students who are aware of the dangers of social media, including identity theft, are more likely to employ greater security measures, like creating complex passwords and configuring privacy settings. Cybersecurity awareness is another name for cyber awareness. It can be defined as the behaviors, knowledge, and abilities that people and businesses need to adopt in order to protect themselves from cyberthreats. Knowing the fundamentals of phishing scams, malware assaults, and other similar hazards will help one reduce them. Keeping abreast on the most recent developments in cybersecurity is a component of cyber awareness. These include creating strong, one-of-a-kind passwords, updating software and apps on a regular basis, and carefully reviewing any questionable emails or texts. Effective cyber awareness initiatives aim to educate individuals about these threats so they can take preventative measures to safeguard their companies and themselves (Anakha & Sanju, 2024).

Notwithstanding these advantages, there are significant obstacles. According to Alasmari, Chaczko, and McDonald (2021), there is a growing trend of hackers using social media to spread false information and launch targeted phishing schemes, which might cause users to underestimate risks or fall for frauds. The intricacy of striking a balance between privacy concerns and educational advantages is highlighted in a work done by Thakur et al. (2019) on "Cyber Security in Social Media," which also highlights the significance of ongoing research and flexible security training on social media platforms. Additionally, it highlights that social media presents particular privacy protection issues even as it increases cybersecurity awareness by bringing attention to real-time concerns. Thakur et al. (2019) revealed that users frequently grow complacent, which emphasizes how crucial it is to provide continual training on security measures on these platforms.

The purpose of this research is to investigate the effects of social media cybersecurity awareness, looking at both its advantages and disadvantages as a teaching tool. Researchers can more accurately evaluate social media's significance as a tool for thwarting cyberthreats and create more focused plans for raising cybersecurity awareness in the digital era by knowing how it adds to cybersecurity knowledge, as expressed by Buhari and Sulaiman, (2023).

Social media's explosive growth has led to a paradox in cybersecurity awareness, although these platforms can educate users about cyberthreats and best practices, they also put users at greater risk because they have become ingrained in daily life, with billions of users actively using sites like Facebook, Instagram, LinkedIn, and Twitter (Anakha & Sanju, 2024). Cybercriminals utilize social media networks to conduct phishing attacks, social engineering, and identity theft, despite the fact that social media platforms provide many advantages, including improved connectivity and information exchange. Many users are not aware of these dangers. According to studies, people frequently fail to understand the security consequences of their online activity, making both personal and professional data vulnerable to breaches (Alotaibi et al., 2021; Herath et al., 2022). The efficiency of existing cybersecurity education and the function of social media in supporting or impeding safe online practices are both seriously called into question by this knowledge gap. Thus, the purpose of this study is to investigate the aforementioned issues by looking at how social media affects cybersecurity awareness, taking into account both its advantages and disadvantages as a teaching tool. Fundamentally, the aim of this research project is to study the impact of social media on cybersecurity awareness. Specific objectives are:

1. Assess the current level of cybersecurity awareness among social media users

2. Investigate the role of social media in disseminating cybersecurity information
3. Analyze the influence of social media on cybersecurity practices

This study will answer questions like:

1. What is the current level of cybersecurity awareness among social media users?
2. What is the role of social media in disseminating cybersecurity information?
3. What influence does social media has on cybersecurity practices?

Areas with limited access to formal cybersecurity training, social media platforms have emerged as important means for interacting with users and sharing cybersecurity knowledge. Available data as stated by Sasu (2025) shows that 94.7% and 95.3% of Nigerians use Facebook and WhatsApp, respectively, demonstrating the country's high utilization of both platforms. However, Alzahrani & Alqahtani (2020) stated that social media exposes users to online dangers including phishing and identity theft, even as it offers a platform for awareness-raising.

The development of cybercrimes, from simple attacks like spam to more complex ones like phishing and malware, shows how the risks are increasing as technology develops. Users are now more susceptible to these dangers because of social media, particularly because of targeted phishing assaults on sites like Facebook and LinkedIn, where criminals use personal data for social engineering (Trend Micro, 2020). By promoting information exchange, fostering public dialogue, and acting as a platform for interactive education, Khan & Khan (2022) revealed that social media can raise knowledge of cybersecurity. Studies indicate that interactive social media campaigns, such as infographics or quizzes, can successfully boost user engagement and aid users in remembering important security details, a view expressed by Wen et al. (2019).

Zhang and Gupta (2016) highlighted that social media platforms present particular cyberthreats, including phishing, social engineering, and malware; they make it easier for cybercriminals to gather data about users' personal information, which is frequently voluntarily shared online; there are also many fake accounts and malicious activities, such as cyberbullying and impersonation, which increase security risks. Researches by Li et al. (2020) and Verkijika (2019) indicated that phishing awareness is influenced by factors such as gender, age, and experience; demographic-tailored campaigns are effective in lowering vulnerability to phishing.

Privacy issues, content saturation, and the indirect nature of engagement metrics make it difficult to engage consumers with cybersecurity content on social media. Because of privacy concerns, users might refrain from engaging with cybersecurity content, which would reduce the effectiveness of awareness initiatives, according to Belanger and Crossler (2011). Additionally, cybersecurity information frequently finds it difficult to compete with articles that are more exciting, which lowers visibility and engagement. AI is being included more and more into social media cybersecurity plans to help with threat identification and reaction. But as cybercriminals use AI to launch more complex assaults, this trend also brings with it new difficulties. With organizations like the Cybersecurity and Infrastructure Security Agency (CISA) using social media to provide real-time alerts and preventive advice, social media continues to be a key platform for public awareness.

Informed by the reviewed literature and guided by the Protection Motivation Theory, the following hypotheses were developed and put to the test in order to direct the inferential analysis in accordance with the goals and research questions of the study. The purpose of these hypotheses is to assess how demographic factors, social media usage trends, and trust affect the way information on cybersecurity awareness and behavior is shared among Nigerians social media users.

- H_{01}: There is no significant relationship between demographic characteristics (gender, age) and cybersecurity awareness among social media users in Nigeria.
- H_{11}: There is a significant relationship between demographic characteristics (gender, age) and cybersecurity awareness among social media users in Nigeria.
- H_{02}: There is no significant influence of social media usage frequency on cybersecurity practices among social media users.

- H_{12}: There is a significant influence of social media usage frequency on cybersecurity practices among social media users.
- H_{03}: There is no significant relationship between educational qualification and the adoption of cybersecurity practices.
- H_{13}: There is a significant relationship between educational qualification and the adoption of cybersecurity practices.
- H_{04}: There is no significant impact of cybersecurity information disseminated on social media on users' behavioral changes.
- H_{14}: There is a significant impact of cybersecurity information disseminated on social media on users' behavioral changes.

2.0 Materials and methods

This study adopted the quantitative approach to researches. A descriptive survey approach was used for the research in order to examine how social media affects cybersecurity awareness. This method enables a thorough examination of current awareness levels, social media's role in diffusion, and its influence on user cybersecurity habits. The survey approach was appropriate since it makes it possible to gather quantitative information from a sizable sample of respondents, guaranteeing thorough insights.

2.1 Population of the Study

The study population consisted of Nigerian social media users aged 18 and above. A stratified random sampling technique was employed to ensure representation across key demographic segments, particularly age, gender, and social media platform usage (e.g., Facebook, WhatsApp, Twitter/X). The strata were defined using publicly available demographic data from Statista (2024) and national ICT reports. Quotas were established to reflect the approximate distribution of users across these demographics (e.g., higher weighting for users aged 18–35, who dominate social media usage in Nigeria). Within each stratum, participants were randomly selected using online survey distribution and targeted sampling on social platforms. This approach enhanced the generalizability of findings while maintaining proportional representation of the study population.

2.2 Instrument for Data Collection

A structured questionnaire was used as the primary instrument for data collection. The survey will be separated into sections that address each of the study's objectives:

- **Section A**: Demographic Information
- **Section B**: Questions on current cybersecurity awareness level
- **Section C**: Questions on social media as a source of cybersecurity information
- **Section D**: Questions on how social media influences cybersecurity practices

The questionnaire utilized a Likert scale (e.g., 1 = Strongly Disagree to 5 = Strongly Agree) to measure respondents' perceptions and experiences.

2.3 Method of Data Analysis

Both descriptive and inferential statistical techniques were used to code and analyze the information gathered from the structured questionnaire. The demographic traits of the respondents and their answers about cybersecurity awareness, social media use, and cybersecurity behaviors were compiled and presented using descriptive statistics, such as frequencies and percentages. The developed hypotheses were tested, and the relationships between variables were investigated, using inferential statistical techniques. To evaluate the relationships between specific factors including gender, age, educational attainment, and cybersecurity awareness, chi-square tests of independence were employed. Microsoft Excel was used to perform all statistical tests at a 5% level of significance ($\alpha = 0.05$).

3.4 Instrument Validation and Reliability

To ensure the validity and reliability of the research instrument, the structured questionnaire was reviewed by academic experts in cybersecurity and research methodology. Their feedback was used to refine ambiguous items and ensure content relevance.

3.0 Result and Discussion

The data gathered from the study is presented, examined, and interpreted in this section. Social media users in Nigeria were given structured surveys to complete in order to get the data. In keeping with the goals and objectives of the study, the data analysis aims to provide answers to the research questions mentioned in the previous section. The analysis used both descriptive and inferential statistical techniques.

3.1 Descriptive Statistics

3.1.1 Social Media Usage

We asked respondents how often they use social networking sites like LinkedIn, Facebook, Instagram, WhatsApp, and X (Twitter).

Table 4.1: Social Media Usage

Social Media Usage Frequency	Frequency	Percentage
Daily	91	77.8%
Frequently (4–6 times/week)	20	17.1
Occasionally (1–3 times/week)	4	3.4%
Rarely (<1 time/week)	2	1.7%

Source: Field Research

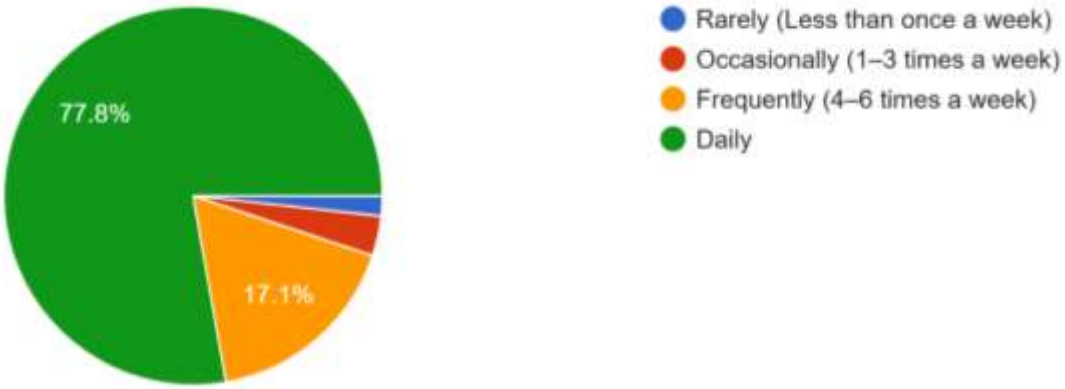


Figure 4.1: Social Media Usage PI Chart

According to Table 4.1, 91 respondents (77.8%) use social media every day, 20 (17.1%) use it regularly (four to six times per week), 4 (3.4%) use it sometimes, and 2 (1.7%) use it rarely. This suggests that the responder uses social media extensively.

Table 4.2: Current Level of Cybersecurity Awareness

How much do you agree with the following statements?	SD	D	N	A	SA	TOTAL
I understand basic cybersecurity concepts (e.g., phishing, malware, data privacy).	22 18.0%	10 9.0%	9 8.0%	33 28.0%	43 37.0%	117 100%
I can recognize phishing emails and social engineering attacks.	17 15.0%	19 16.0%	13 11.0%	35 30.0%	33 28.0%	117 100%
I regularly update my passwords and use strong password policies.	21 18.0%	19 16.0%	22 19.0%	29 25.0%	26 22.0%	117 100%
I am aware of the importance of multi-factor authentication (MFA).	21 18.0%	8 7.0%	11 9.0%	29 25.0%	48 41.0%	117 100%

I avoid sharing sensitive personal information on social media.	25 21.4%	4 3.4%	12 10.2%	16 14.0%	60 51.0%	117 100%
I know how to identify and report suspicious online activities.	19 16.0%	17 15.0%	15 13.0%	36 31.0%	30 25.0%	117 100%

Source: Field Research

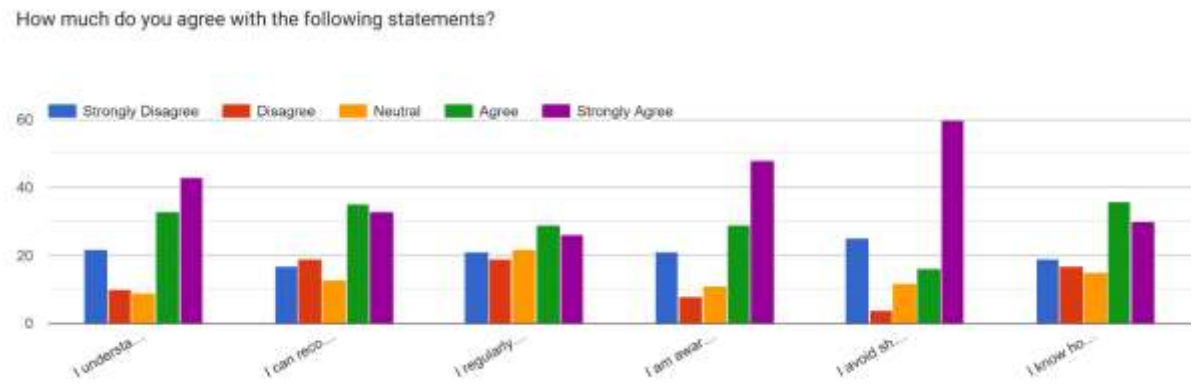


Figure 4.2: Current Level of Cybersecurity Awareness

Table 4.2's first statement aimed to ascertain respondents' comprehension of fundamental cybersecurity ideas such malware, phishing, and data privacy. 37.0% of respondents strongly agreed, and 28.0% agreed, according to the research, meaning that 65.0% of participants think they comprehend these basic ideas. However, 9.0% disagreed and 18.0% strongly disagreed, indicating that roughly 27.0% of the respondents either do not comprehend these concepts or do not have trust in their knowledge. Just 8.0% of the population was neutral.

According to this finding, a sizable minority of respondents still have little knowledge of cybersecurity, even though the majority are aware of its fundamentals. The high degree of agreement suggests that social media might have contributed to the spread of fundamental information about cyberthreats. Nonetheless, the fact that more than 25.0% of participants acknowledged that they lacked fundamental knowledge highlights the necessity of more focused awareness campaigns and educational initiatives, especially for those with less knowledge.

A total of 58.0% of respondents indicated that they were confident in their abilities to distinguish phishing emails and social engineering attacks, with 28.0% strongly agreeing and 30.0% agreeing. Nonetheless, 31.0% of respondents felt they were unable to identify these types of attacks, with 15.0% strongly disagreeing and 16.0% disagreeing. Eleven percent were neutral. This result indicates that respondents had a moderate awareness of social engineering and phishing. Nearly a third of respondents said they were still at risk, despite more than half saying they could spot phishing attempts. This gap highlights a crucial need for more practical and scenario-based cybersecurity training, especially considering the increasing sophistication of phishing and social engineering strategies regularly utilized on social media platforms.

Only 47.0% of respondents frequently change their passwords and utilize strong password rules, according to the statement evaluating their password management behavior, which found that 22.0% strongly agreed and 25.0% agreed. In contrast, 34.0% of respondents acknowledged ignoring these basic practices, with 18% strongly disagreeing and 16% disagreeing. Furthermore, 19.0% were neutral.

This finding shows that even while almost half of the respondents follow suggested password habits, a sizable portion continue to take risks by failing to change their passwords on a regular basis. They are vulnerable to risks like identity theft and illegal access because of their careless password management. It emphasizes how crucial it is to stress password hygiene in cybersecurity awareness programs and how social media sites should encourage and maybe impose more robust authentication methods.

66.0% of respondents acknowledged the significance of multi-factor authentication (MFA) in improving their cybersecurity, with 41.0% strongly agreeing and 25.0% agreeing. However, 25.0% of respondents seemed unsure or unconvinced about the significance of MFA, with 18.0% strongly disagreeing and 7.0% disagreeing. Nine percent of individuals showed a neutral attitude. A somewhat good level of knowledge of MFA and its use in protecting digital accounts is evident from this response. However, the fact that 25.0% of respondents are either unaware of its significance or are unconvinced indicates that more education is required to advance MFA as a vital security tool.

Future cybersecurity efforts should prioritize the adoption of MFA since it is one of the best strategies to stop unwanted access. 65.0% of respondents exercise caution when it comes to their personal information online, with 51.0% strongly agreeing and 14.0% agreeing with the practice of avoiding publishing sensitive personal information on social media. Nonetheless, 24.8% of those who acknowledged disclosing sensitive information disagreed, with 3.4% disagreeing and 21.4% severely disagreeing. 10.2% more were neutral.

The fact that most respondents engage in safe information-sharing activity makes these results encouraging. Nonetheless, the fact that nearly 25.0% of people still post private information on social media points to a persistent weakness. Because of this conduct, they are more likely to become the target of identity theft or social engineering by cybercriminals. Campaigns to raise awareness should highlight the risks associated with excessive social media sharing and encourage privacy-preserving digital hygiene practices.

The last item assessed the respondents' knowledge of how to spot and report questionable online activity. According to the findings, 31.0% agreed and 25.0% strongly agreed, meaning that 56.0% of respondents felt confidence in their capacity to recognize and report dangers. However, 31.0% lacked this crucial ability, with 16.0% strongly disagreeing and 15.0% disagreeing. Furthermore, 13.0% were neutral.

This indicates that respondents have a moderate level of confidence in their ability to spot and report questionable internet activity. Even though more than half are watchful and proactive, the sizeable minority who are not may expose their networks and themselves to online dangers. Simplified social media reporting procedures and more training on spotting possible threats could close this gap and raise public awareness of cybersecurity.

Table 4.3: Social Media as a Source of Cybersecurity Information

How much do you agree with the following statements?	SD	D	N	A	SA	TOTAL
I have come across cybersecurity awareness content on social media.	17 15.0%	9 8.0%	13 11.0%	48 40.0%	30 26.0%	117 100%
Social media platforms (e.g., Twitter, LinkedIn, Facebook) help me stay updated on cybersecurity threats.	15 13.0%	15 13.0%	29 25.0%	33 28.0%	25 21.0%	117 100%
Cybersecurity professionals and organizations effectively share security tips on social media.	17 15.0%	12 10.0%	22 19.0%	47 40.0%	19 16.0%	117 100%
I trust the cybersecurity information I receive from social media.	15 13.0%	20 17.0%	36 31.0%	33 28.0%	13 11.0%	117 100%
I have taken action based on cybersecurity warnings found on social media.	15 13.0%	12 10.0%	23 20.0%	41 35.0%	26 22.0%	117 100%
Social media discussions and awareness campaigns have improved my cybersecurity knowledge.	21 18.0%	8 7.0%	21 18.0%	36 31.0%	31 26.0%	117 100%

Source: Field Research

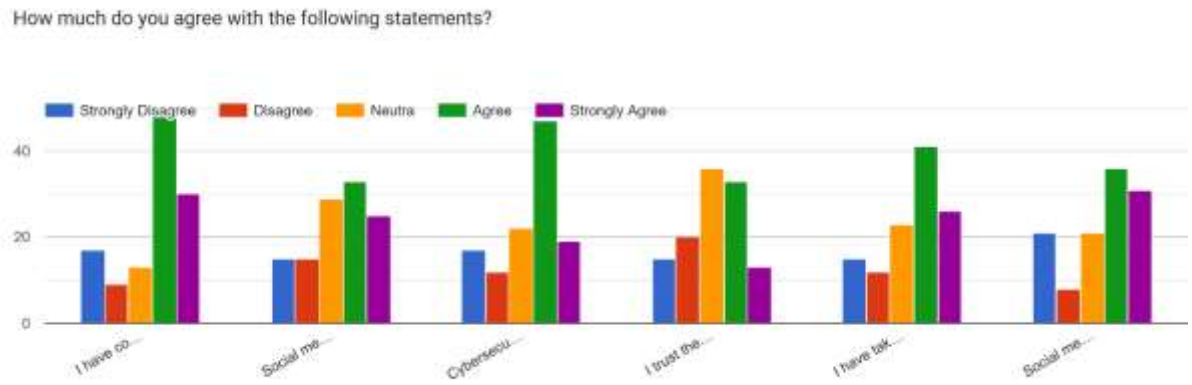


Figure 4.3: Social Media as a Source of Cybersecurity Information

The majority of respondents said they had come across cybersecurity awareness content on social media, according to table 4.3 above. In particular, 66.0% of respondents acknowledged being exposed to posts or campaigns pertaining to cybersecurity, with 40.0% agreeing and 26.0% strongly agreeing. Nonetheless, 23.0% of individuals said they had not come across such content, with 15.0% strongly disagreeing and 8.0% disagreeing. 11.0% had no opinion on the subject. This finding implies that social media is an important medium for sharing content related to cybersecurity awareness. The high agreement rate illustrates how important social media sites like Facebook, LinkedIn, and Twitter are for spreading knowledge about cybersecurity.

The fact that almost 25.0% of respondents said they had not seen such content, however, emphasizes the necessity of more focused and regular awareness initiatives, particularly for groups that might not be reached by conventional means. A total of 49.0% of respondents acknowledged that social media sites assist them in staying informed about cybersecurity concerns, with 28.0% agreeing and 21.0% strongly agreeing. On the other hand, 13.0% disagreed with this remark, 13.0% disagreed, and 25.0% were neutral.

This outcome suggests a perception that is divided. A sizable portion of respondents—especially those who stayed neutral—may not actively seek out or trust material published on social media, even if almost half of them find it helpful for remaining updated about cybersecurity concerns. It highlights a chance for cybersecurity experts and institutions to boost interaction and improve the exposure of reliable, current danger information on social media.

A total of 56.0% of respondents agreed and 16.0% strongly agreed that cybersecurity professionals and organizations effectively disseminate security tips on social media. However, 10.0% disagreed, or 25.0%, and 15.0% strongly disagreed, while 19.0% were neutral. This indicates that the majority of respondents think social media is a good way for companies and experts to exchange useful cybersecurity advice. To improve the legitimacy, scope, and impact of these initiatives, additional work must be done, according to the sizable percentage of respondents who disagree or are unconcerned. To increase the dissemination and retention of knowledge, cybersecurity professionals can think about implementing more captivating formats, including infographics or interactive articles.

Responses to the topic of whether cybersecurity information provided on social media sites can be trusted were not entirely consistent. Just 28.0% of respondents agreed, and 11.0% strongly agreed, meaning that 39.0% of respondents expressed trust. On the other hand, 31.0% took a neutral position, 13.0% strongly disagreed, and 17.0% disagreed, for a total of 30.0%. This suggests both considerable skepticism and a moderate degree of trust in cybersecurity content disseminated on social media. Uncertainty regarding the accuracy of information gleaned from these platforms is indicated by the high proportion of indifferent comments. To solve this, cybersecurity companies can emphasize openness, reference reliable sources, and dispel false information in order to boost confidence and trust in their social media messaging.

57.0% of respondents said they have acted in response to cybersecurity concerns they have seen on social media, with a noteworthy 35.0% agreeing and 22.0% strongly agreeing. On the other hand, 10.0% disagreed, 13.0% strongly disagreed, and 20.0% were neutral.

This is encouraging evidence of social media's capacity to influence behavior. More than 50.0% of participants stated that they updated their passwords or enabled multi-factor authentication as a result of cybersecurity alerts and advisories that were disseminated on social media. This emphasizes how crucial prompt and easily accessible warnings are on social media and how they affect user behavior. Nonetheless, some respondents continue to disregard these warnings, indicating the need for stronger messaging or more obvious calls to action.

31.0% of respondents agreed and 26.0% strongly agreed that social media conversations and awareness initiatives have increased their understanding of cybersecurity, for a total of 57.0% positive answers. However, 7.0% disagreed, 18.0% were neutral, and 18.0% strongly disagreed. This demonstrates that over 50.0% of respondents think that taking part in awareness efforts and social media conversations has improved their comprehension of cybersecurity. This demonstrates how social media platforms may be used to increase cybersecurity knowledge through teaching. The existence of a sizeable group that felt nothing had changed, however, suggests that the campaign's quality, relevance, and reach were lacking. To guarantee a wider impact, campaigns might need to be better adapted to a variety of groups, and instructional materials should be made simpler and more engaging.

Table 4.4: Influence of Social Media on Cybersecurity Practices

How much do you agree with the following statements?	SD	D	N	A	SA	TOTAL
Social media has influenced me to adopt better cybersecurity practices.	19 16.0%	9 8.0%	16 14.0%	52 44.0%	21 18.0%	117 100%
I have changed my online behavior due to cybersecurity awareness on social media.	20 17.0%	10 9.0%	23 20.0%	39 33.0%	25 21.0%	117 100%
Social media helps me identify emerging cybersecurity threats.	20 17.0%	5 4.0%	25 21.0%	42 36.0%	25 22.0%	117 100%
I feel more cautious about my online privacy due to social media discussions.	28 24.0%	8 9.0%	16 14.0%	48 29.0%	28 24.0%	117 100%
I have taken cybersecurity training or awareness programs because of social media influence.	20 17.0%	13 11.0%	29 25.0%	32 27.0%	23 20.0%	117 100%
Social media platforms should do more to promote cybersecurity awareness.	19 16.0%	4 3.0%	13 11.0%	34 29.0%	47 41.0%	117 100%

Source: Field Research

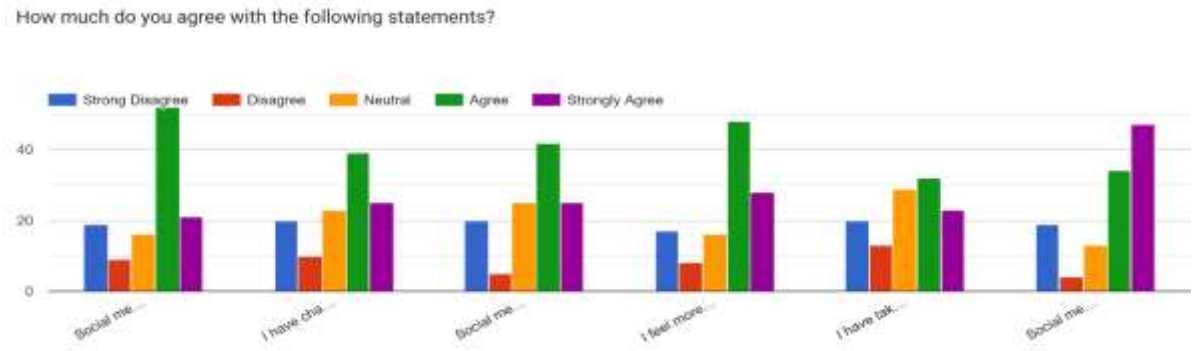


Figure 4.4: Influence of Social Media on Cybersecurity Practices

Based on table 4.4, 62.0% of respondents acknowledged that social media had a beneficial influence on their adoption of better cybersecurity procedures, with 44.0% agreeing and 18.0% strongly agreeing. Yet, 24.0% of

participants said they did not feel influenced by social media in this way, with 16.0% strongly disagreeing and 8.0% disagreeing. An additional 14.0% had no opinion. This research emphasizes how important social networking sites are in motivating users to embrace better cybersecurity practices, such creating stronger passwords or turning on multi-factor authentication. Even though most respondents acknowledge this influence, the 25.0% who say they have no influence suggests that cybersecurity awareness campaigns on social media are not reaching as many people or being as successful. This group of less receptive users may be addressed by making cybersecurity campaigns more appealing and relevant. 54.0% of respondents said they have modified their online behavior as a result of learning more about cybersecurity on social media, with 33.0% agreeing and 21.0% strongly agreeing. In contrast, 26.0% of respondents did not report any change, with 17.0% strongly disagreeing and 9.0% disagreeing. Furthermore, 20.0% of those surveyed expressed no opinion.

This implies that social media significantly influences cybersecurity-related behavioral shifts, including less sharing of private information or more prudence when clicking links. More than 25.0% of responders, however, are unaffected, underscoring the need for more interesting or tailored literature that illustrates the real dangers of subpar cybersecurity procedures and the advantages of taking preventative action.

A total of 58.0% of respondents agreed with the assertion that social media helps users uncover new cybersecurity threats, with 36.0% agreeing and 22.0% strongly agreeing. Conversely, 21.0% of respondents disagreed and 17.0% strongly disagreed, making social media an unreliable source for spotting emerging threats. Of those surveyed, 21.0% had no opinion.

This research demonstrates how social media can be used to disseminate up-to-date information about new cybersecurity risks. Up-to-date threat alerts are frequently shared on social media sites like LinkedIn and Twitter, but the existence of respondents who are doubtful or uninterested points to a lack of trust. While fighting false information that could erode consumers' trust in social media as a reliable source of threat intelligence, cybersecurity firms should keep up their efforts to deliver timely, correct information.

There were differing opinions on the remark regarding heightened awareness of online privacy due to social media conversations. 53.0% of respondents felt that social media had increased their understanding of privacy, with 29.0% agreeing and 24.0% strongly agreeing. Nonetheless, 33.0% of respondents said they were not more cautious, with 24.0% strongly disagreeing and 9.0% disagreeing. 14.0% more respondents said they had no opinion.

These findings imply that although social media conversations have made more than half of the respondents more privacy-conscious, a sizable portion are unaffected. This could suggest a lack of interest in such content or doubt about the applicability of social media privacy issues. By offering relatable examples of privacy breaches and their repercussions, there is an opportunity to increase the efficacy of privacy awareness programs.

47.0% of respondents cited social media as a motivating factor when asked if they had taken part in cybersecurity training or awareness initiatives as a result of social media impact. Of those, 27.0% agreed and 20.0% strongly agreed. However, 11.0% disagreed and 17.0% strongly disagreed, making up 28.0%, while 25.0% were impartial.

This implies that the experiences they had on social media motivated over half of the respondents to pursue proactive cybersecurity education measures. The comparatively large percentage of neutral and negative replies suggests the need for more approachable and persuasive calls to action, even while this shows the beneficial effect of social media in boosting formal cybersecurity education. To promote wider engagement, campaigns could incorporate endorsements from previous participants and direct links to free training or certificates.

A sizable portion of participants think social media sites should do more to raise awareness of cybersecurity. A total of 70.0% of respondents believe that present efforts are insufficient, with 41.0% strongly agreeing and 29.0% agreeing. On the other hand, 11% were neutral, 16.0% strongly opposed, and 3% disagreed, accounting for 19.0%.

This broad consensus shows that there is a strong need for social media businesses to take more proactive steps to raise awareness of cybersecurity. Platforms like Facebook, Instagram, LinkedIn, and Twitter are expected by respondents to offer more meaningful, consistent, and visible awareness content. Dedicated cybersecurity campaigns, privacy settings prompts, or alerts on new dangers and best practices might all be examples of this. Platforms could collaborate with cybersecurity groups to provide authenticated and reliable content.

3.2 Inferential Statistics

To test the hypotheses developed in Section 3.8.1, inferential statistics were used. At the 5.0% significance level ($\alpha = 0.05$), the hypotheses were examined.

3.2.1 Hypotheses Testing and Results

Hypothesis One

H_{01}: There is no significant relationship between gender and cybersecurity awareness.
H_{11}: There is a significant relationship between gender and cybersecurity awareness.

Table 4. 5: Gender vs. Cybersecurity Awareness

Gender	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Female	5	8	4	6	2	25
Male	12	11	9	29	31	92
Total	17	19	13	35	33	117

Source: Extracted from Field Data

Female respondents are less confident in their ability to identify phishing emails, as seen by their higher disagreement rate (13 out of 25 respondents chose Strongly Disagree or Disagree). Although 60 respondents (65%) chose Agree or Strongly Agree, male respondents exhibit better self-reported awareness.

Table 4.6: Result of Chi-Square Test of Independence

Chi-Square Statistic	Degrees of Freedom	p-value
11.17547181	4	0.024661149

Interpretation

The chi-square test ($\chi^2 = 11.17547181$, df = 4, p = 0.024661149) indicates a significant relationship between gender and cybersecurity awareness. This suggests that gender influences how individuals understand and respond to basic cybersecurity concepts such as phishing, malware, and data privacy. Specifically, male respondents reported higher confidence levels compared to female respondents. These findings support previous studies (e.g., McCormac et al., 2017), which observed gender differences in cybersecurity knowledge and behavior. The result highlights the importance of gender-sensitive cybersecurity education and awareness interventions.

Hypothesis Two

H_{02}: There is no significant influence of social media usage frequency on cybersecurity practices.
H_{12}: There is a significant influence of social media usage frequency on cybersecurity practices.

Table 4.7: Social Media Usage Frequency Vs Cybersecurity Practices.

Social Media Usage Frequency	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Daily	16	8	15	37	15	91
Frequently (4–6 times/week)	2	0	1	12	5	20
Occasionally (1–3 times/week)	1	0	0	2	1	4
Rarely (< once a week)	0	1	0	1	0	2

Column Totals	19	9	16	52	21	117

Table 4.8: Result of Chi-Square Test of Independence

Chi-Square Statistic	Degrees of Freedom	p-value
12.73975435	12	0.388236836

Interpretation

The chi-square test (χ^2 = 12.73975435, df = 12, p = 0.388236836) showed no statistically significant relationship between the frequency of social media usage and the adoption of cybersecurity practices. This suggests that how often individuals use social media does not directly influence whether they adopt safer cybersecurity behaviors. This may indicate that exposure alone is insufficient and that the type and quality of information users encounter may play a more critical role than usage frequency.

Hypothesis Three

H_{03}: There is no significant relationship between educational qualification and adoption of cybersecurity practices.
H_{13}: There is a significant relationship between educational qualification and adoption of cybersecurity practices.

Table 4.9: Educational Qualification vs. Understanding Basic Cybersecurity

Highest Educational Qualification	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Bachelor's Degree	13	7	5	17	28	70
Diploma	0	1	1	2	0	4
Higher National Diploma/NCE	3	0	0	3	2	8
Master's Degree or Higher	5	1	2	8	12	28
Secondary School	1	1	1	3	1	7
Column Totals	22	10	9	33	43	117

Table 4.10: Result of Chi-Square Test of Independence

Chi-Square Statistic	Degrees of Freedom	p-value
13.19314	16	0.65858664

Interpretation

There is no statistically significant association between respondents' educational qualifications and their level of cybersecurity awareness. This suggests that higher formal education does not necessarily translate into greater awareness of cybersecurity threats, and that awareness may instead depend on targeted exposure to cybersecurity information, rather than general education.

Hypothesis Four

H_{04}: There is no significant relationship between age group and cybersecurity awareness levels.
H_{14}: There is a significant relationship between age group and cybersecurity awareness levels.

Table 4.11 Age Group Vs Cybersecurity Awareness

Age Group	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
18 – 25	5	2	2	6	5	20
26 – 35	10	6	4	13	16	49
36 – 45	2	0	2	10	13	27
46 and above	5	2	1	4	9	21
Column Totals	22	10	9	33	43	117

Table 4.12: Result of Chi-Square Test of Independence

Chi-Square Statistic	Degrees of Freedom	p-value
9.759858249	12	0.637018932

Interpretation

Table 4.12 also showed no significant association between respondents' age groups and their cybersecurity awareness levels. This finding suggests that cybersecurity awareness may cut across age groups, with both younger and older individuals having similar levels of awareness, potentially due to widespread access to cybersecurity information on social media platforms.

Hypothesis Five

H_{05}: There is no significant impact of cybersecurity information disseminated on social media on users' behavioral changes towards cybersecurity practices.

H_{15}: There is a significant impact of cybersecurity information disseminated on social media on users' behavioral changes towards cybersecurity practices

Table 4.13: Relationship Between Trust in Social Media Cybersecurity Information and Behavioral Change

Trust in Social Media Cybersecurity Information Info	Changed	No Change	Total	% Changed
Strongly Disagree	1	1	2	50
Disagree	5	7	12	41.7
Neutral	0	0	0	0
Agree	30	3	33	90.9
Strongly Agree	23	2	25	92

Note: "Changed" includes respondents who agreed or strongly agreed that they changed their cybersecurity behavior. "No Change" includes those who disagreed, strongly disagreed, or remained neutral.

Table 4.14: Result of Chi-Square Test of Independence

Chi-Square Statistic	Degrees of Freedom	p-value
36.03	16	0.00287

Interpretation

The chi-square test ($\chi^2 = 36.03$, df = 16, p = 0.00287) revealed a strong and statistically significant association between respondents' trust in cybersecurity information shared on social media and their self-reported behavioral changes. Respondents who trusted social media sources were more likely to adopt secure online behaviors, such as using multi-factor authentication, updating passwords, and avoiding risky links. This supports Protection Motivation Theory (PMT), which emphasizes that perceived information credibility and threat appraisal influence protective cybersecurity behaviors.

3.3 Data Analysis (Mathematical)

The data gathered for this study via structured questionnaires were analyzed using both descriptive and inferential statistical techniques. In order to do statistical analysis (chi-square) and test the hypotheses outlined in the first portion of the study, the data were coded and imported into Microsoft Excel for initial organizing and cleaning. The demographic information, social media usage trends, and cybersecurity awareness levels of the respondents were

compiled using descriptive statistics. Tables, charts, percentages, and frequencies were created to visually and textually depict the data.

Chi-square tests were used for inferential statistics to investigate the connections between cybersecurity awareness and demographic factors (gender, age, and educational attainment).

Furthermore, the impact of social media usage frequency and cybersecurity knowledge dissemination on user behavior was examined. These particular steps were taken in the analysis:
(i) Data Cleaning and Coding: To verify consistency and fix entry errors, data was examined.
(ii) Descriptive Analysis: For categorical variables, percentages and frequencies were computed.
(iii) Hypothesis Testing: At a 5% significance level ($\alpha = 0.05$), chi-square tests were performed.
(iv) Results Interpretation: P-values and chi-square statistics were used to analyze the results.

3.4 Findings

The following important conclusions were drawn from the data analysis and hypothesis testing:
1. Social Media Usage and Demographics

(i) Males made up 78.6% of the respondents, and 41.9% of them were between the ages of 26 and 35.
(ii) The majority (77.8%) use social media on a regular basis, with Facebook, Instagram, and WhatsApp being the most popular platforms.

2. Levels of Cybersecurity Awareness

(i) According to 65.0% of respondents, they were aware of fundamental cybersecurity ideas like malware and phishing.

(ii) While 65.0% refrained from disclosing private information on social media, 66.0% recognized the value of multi-factor authentication (MFA).

(iii) In spite of these encouraging numbers, over 27.0% of respondents said they were unconfident in their understanding of cybersecurity.

3. Social Media's Impact on Cybersecurity Knowledge and Practices

(i) 66.0% of those surveyed said they have come across social media posts about cybersecurity awareness.
(ii) 57.0% of respondents acknowledged that social media campaigns and conversations enhanced their understanding of cybersecurity.

(iii) 54.0% of respondents changed their online activity owing to cybersecurity knowledge on social media.

4. Results of Hypothesis Testing

(i) Gender and cybersecurity awareness are significantly correlated ($p = 0.0246$).

(ii) The frequency of social media use and cybersecurity procedures did not significantly correlate ($p = 0.388$).

(iii) There is no discernible correlation ($p = 0.659$) between cybersecurity awareness and educational background.

(iv) Age group and cybersecurity awareness levels did not significantly correlate ($p = 0.637$).

(v) Users' behavioral shifts toward cybersecurity practices are significantly influenced by cybersecurity information shared on social media ($p = 0.00287$).

3.5 Interpretation of Findings

According to the study's conclusions, social media is essential for raising user knowledge of cybersecurity issues and influencing their behavior. In particular,

- The findings show that a majority of users (65.0%) reported understanding basic cybersecurity concepts such as phishing, malware, and data privacy. Additionally, 66.0% indicated awareness of multi-factor authentication (MFA), and 65.0% exercised caution in sharing personal information online. However, up to 27.0% of respondents either disagreed or strongly disagreed with statements testing their understanding, indicating that a substantial portion of users remain unsure or unaware of foundational cybersecurity practices. This suggests that while general awareness is present among the majority, there remains a critical knowledge gap among a significant minority, which increases their vulnerability to online threats.
- Social media emerged as an important platform for cybersecurity awareness. The data revealed that 66.0% of respondents encountered cybersecurity-related content on platforms like Facebook, Twitter, and LinkedIn. Furthermore, 57.0% agreed that such exposure improved their cybersecurity knowledge, while 56.0% acknowledged that organizations and professionals effectively share tips through these channels. However, trust remains a challenge: only 39.0% of respondents expressed trust in cybersecurity information from social media, and 31.0% remained neutral. This lack of confidence may undermine the effectiveness of these platforms as educational tools. Overall, the data supports the assertion that social media serves a dual role as both a source of knowledge and a potential vector for misinformation.
- The survey findings also indicate that 62.0% of users adopted improved cybersecurity behaviors as a result of social media influence, while 54.0% modified their online behavior based on the cybersecurity awareness they gained. Actions included using stronger passwords, enabling MFA, and exercising caution when clicking unknown links. Furthermore, 47.0% of respondents stated that they had taken cybersecurity training or awareness programs prompted by exposure to such content on social platforms. These findings are consistent with Protection Motivation Theory (PMT), which posits that perceived threat and response efficacy drive behavioral change. However, 26.0% of users did not change their behavior, highlighting the need for more engaging and tailored awareness strategies to convert awareness into consistent action.

In summary, the statistics affirm that social media plays a significant role in promoting cybersecurity awareness and influencing protective behaviors. The results align with the study's research questions and demonstrate how cybersecurity knowledge and behavioral change are shaped by users' interaction with content on social platforms. However, the presence of knowledge gaps, varying trust levels, and inconsistent behavioral responses suggest that awareness alone may not be sufficient, and that future strategies should focus on enhancing message credibility, user engagement, and platform accountability.

3.6 Discussion of Findings

The investigation's findings are consistent with those of past research discussed in the literature review. In keeping with Khan & Khan (2022), this study highlighted the role social media plays in influencing user behavior and disseminating cybersecurity knowledge. Respondents' regular usage of social media presents an opportunity for cybersecurity professionals to reach a wide audience. The findings of McCormac et al. (2017), who found gender differences in cybersecurity knowledge and behavior, are in line with the substantial association between gender and cybersecurity awareness. This study suggests that in order to ensure effectiveness and inclusiveness, gender-sensitive awareness campaigns are required. Age, educational attainment, and cybersecurity awareness do not significantly correlate, in contrast to some studies, such as Ogutcu et al. (2016).

According to this study, the prevalence of cybersecurity content on social media may lessen the impact of demographic variables. Campaigns to raise awareness about social media cybersecurity caused a sizable percentage of respondents to indicate behavioral changes. This is in line with Wen et al. (2019), who promoted interactive campaigns that successfully engaged users. However, this study's findings of skepticism and lack of trust in social media information highlight the importance of reliable, open, and verifiable sources. The vast majority of

respondents think social media companies ought to do more to raise awareness of cybersecurity. Belanger and Crossler's (2011) worries that on the efficacy of existing techniques and their potential for improvement are reflected in this.

While the questionnaire underwent expert review to ensure content validity, the study did not include a formal pilot test with the full target population. This may limit the ability to detect potential issues related to item interpretation or measurement consistency across a broader sample. Future research should incorporate pilot testing to strengthen instrument reliability and validity. And note that as multiple hypotheses were tested in this study, the risk of Type I error inflation should be noted. Although no formal adjustment for multiple comparisons (such as Bonferroni correction) was applied due to the exploratory nature of the research and the small number of tests conducted, caution is advised in interpreting marginally significant results. The strongest finding (H_5) remains significant even under conservative corrections.

4.0. Conclusion

According to the study's findings, social media platforms are a useful tool for raising awareness of cybersecurity issues and promoting safe online conduct. These platforms help users learn about potential cyberthreats and safeguards, but they also act as conduits for false information, cyberattacks, and privacy abuses. Given the strong correlation between cybersecurity awareness and gender, tailored awareness programs that consider demographic traits are necessary. Additionally, despite the observed high levels of cybersecurity knowledge, a sizable percentage of users continue to engage in risky activities, highlighting the necessity of ongoing engagement and education. The impact of social media on cybersecurity procedures shows how effective it can be as a tactical instrument in organizational and national cybersecurity plans. However, the efficacy of contemporary awareness campaigns is constrained by problems with trust, skepticism, and content saturation.

5.0 Recommendation

The following suggestions are put out in light of the study's findings and conclusion:

1. Boost Social Media Cybersecurity Campaigns: Social media companies should work with cybersecurity organizations to raise the number and frequency of cybersecurity awareness campaigns. These ads ought to be accessible, dynamic, and interesting, and they ought to be designed to appeal to various demographics.

2. Create Gender-Specific Cybersecurity Training: Awareness campaigns should be tailored to the unique requirements, habits, and risk perceptions of men and women who use social media. Targeted interventions are required to address gender differences in cybersecurity awareness.

3. Foster Cybersecurity Trust Information on Social Media: Organizations and cybersecurity experts should make sure that the information given is reliable, authentic, and sourced from reliable sources. To counter false information and build trust, social media companies might implement verified badges for cybersecurity material.

4. Encourage Cyber Hygiene Practices: Initiatives should aggressively encourage cyber hygiene, which includes frequent software updates, multi-factor authentication, and the use of secure passwords. Users can successfully apply these techniques with the aid of helpful hints and tutorials.

5. Make Use of Peer Networks and Influencers: Peer networks and influencers can be effective allies in promoting cybersecurity messages. Campaigns to raise awareness of cybersecurity should collaborate with well-known personalities who can successfully connect with a range of audiences.

6. Encourage Social Media Platforms to Take Accountability: By providing cybersecurity alerts, privacy reminders, and educational pop-ups, social media platforms should actively contribute to raising awareness of cybersecurity.

References

Alasmari, H., Chaczko, Z., & McDonald, C. (2021). Phishing in social media: Defending social media accounts against phishing attacks. IEEE Xplore Digital Library.

Alharbi, M. & Tassaddiq, M. (2021). Factors influencing cybersecurity awareness among students. *Journal of Cybersecurity Education*, 5(*2*), 23-38.

Alotaibi, M. N., Alharbi, A., & Aldayel, A. (2021). Cybersecurity awareness among social media users: Examining the link between social media use and security practices. *Journal of Cybersecurity and Privacy,* 3(1), 45-60.

Alzahrani, M. A., & Alqahtani, M. A. (2020). The impact of social media on cybersecurity awareness among university students. *Journal of King Saud University - Computer and Information Sciences,* 32(*4*), 482-491.

Anakha, P. & Sanju, R. (2024). The effectiveness of using social media to raise cyber safety awareness among the public. *Journal of the Asiatic Society of Mumbai,* XCVII (02), 1-9.

Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of informationprivacy research in information systems. *MIS Quarterly*, 35(*4*), 1017-1042.

Buhari, A. & Sulaiman, Z.I. (2023). Social media and cyber security: protecting against online threats and attacks. Conference Paper. Online. https://www.researchgate.net/publication/373328868_SOCIAL_MEDIA_AND_CYBER_SECURITY_PROTECTING_AGAINST_ONLINE_THREATS_AND_ATTACKS#fullTextFileContent. Retrieved 10/09/2024.

Cheong, H. H. W., Chi, C., Liu, J., Zhang, Y., Lei, V. N.L., & Xu, X. (2022). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and Information Technologies*, 28, 439-470. Online: https://link.springer.com/article/10.1007/s10639-022-11121-5

Chin, K. (2025). The Impact of Social Media on Cybersecurity. Online. https://www.upguard.com/blog/the-impact-of-social-media-on-cybersecurity. Retrieved 04/02/2025.

DHS NCSAM. (2020). Social media and cybersecurity: Understanding the risks. online https://www.dhs.gov/national-cybersecurity-awareness-month/social-media-and-cybersecurity. Retrieved 12/10/2024.

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: A systematic literature review. *Journal of Cybersecurity and Privacy*, 2(*1*), 1-18.

Khan, S. A., & Khan, F. A. (2022). The impact of social media on cybersecurity awareness: A systematic literature review. *Telemat. Informatics,* 64, 101645.

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. (2020). Experimental investigation of demographic factors related to phishing susceptibility. *Proceedings of the 53rd Hawaii International Conference on System Sciences,* 2240–2249. https:// doi. org/ 10. 24251/ hicss. 2020. 274.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. (2017). Individual differences and information security awareness, *Computers in Human Behavior*, 69, 151-156.

Ogutcu, G.; Testik, O.M.; Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Comput. Secur.* 56, 83–93.

Sasu, D.D. (2025). Most used social media platforms in Nigeria in the 3rd quarter of 2024. Online. https://www.statista.com/statistics/1176101/leading-social-media-platforms-nigeria/. Retrieved 12/01/2025.

Statista. (2024). Social media statistics and facts. Online: https://www.statista.com/topics/1164/social-networks/. Retrieved 17/09/2024

Thakur, K., Hayajneh, T. & Tseng, J. (2019). Cyber security in social media: Challenges and the way forward. *IT Professional,* 21(2): 41-49. DOI: 10.1109/MITP.2018.2881373.

Trend Micro (2020). Everyday cyber threat landscape: 2019 to 2020 trends. Online: https://news.trendmicro.com/2020/01/06/everyday-cyber-threat-landscape-2019-to-2020-trends/. Retrieved 12/12/2024.

Verkijika, S. F. (2019). If you know what to do, will you take action to avoid mobile phishing attacks: Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior,* 101(January), 286– 296. https:// doi. org/ 10. 1016/j. chb. 2019. 07. 034.

Wen, Z.A., Lin, Z., Chen, R., & Andersen, E. (2019). What. hack: engaging anti-phishing training through a role-playing phishing simulation game. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, p. 108. ACM. https://doi.org/10.1145/3290605.3300338

Zhang, Z. & Gupta, B.B (2016). Social media security and trustworthiness: Overview and new direction. *F*uture Generation Computer Systems, 86(*2*). DOI: 10.1016/j.future.2016.10.007.