The impact of cybercrimes threats on social media usage in Tanzania

Hamisi R. Zahoro[1]
Veneranda Rutainurwa[2]

[1]hamisizahoro1@gmail.com
[2]vennyrich@gmail.com

[1,2]Department of Accountancy and Marketing, College of Business Education, Mbeya, Tanzania

https://doi.org/10.51867/ajernet.7.3.24

ABSTRACT

This paper examined the impact of cybercrime threats on social media usage in Tanzania. Protection Motivation Theory (PMT) and Social Cognitive Theory (SCT) guided this paper. Descriptive survey design was employed utilizing mixed research methods to collect quantitative and qualitative data. The target population comprises the social media users from Dar es Salaam region, from which a sample of 340 was drawn using two stage cluster sampling technique. Data was collected through questionnaire and semi-structured interview. Seemingly Unrelated Regression (SURE) was employed to test postulated relationships between phishing attacks, cyberbullying and harassment, data breaches and social media usage factors such as engagement, trust and platform preferences. The findings revealed that phishing, cyberbullying and data breaches significantly undermine social media usage. Furthermore, phishing attacks lowered trust and engagement, cyberbullying deterred engagement particularly from women and youth while data breach had the most significant negative impact by lowering user confidence in privacy and security. The study concludes that cybercrime threats have a crucial impact on user behavior and lower substantial engagement on social media platforms in Tanzania. The research proposes to enhance digital literacy campaign, enforcement of cyber laws and platform level safety features to restore trust and promote safe interaction.

Keywords: Cybercrime, Cyberbullying, Data Breaches, Phishing, Social Media Usage, Tanzania

I. INTRODUCTION

Global adoption of internet technologies and emergence of social media networks, such as Facebook, Instagram, X (previously Twitter), Tiktok and WhatsApp represent the key aspects of a significant change in the patterns of human social interaction and information exchange. Over 5.17 billion people use these websites actively as of (DataReportal, 2024). Fast growth is connected with the fact that social media became the target of many criminal activities, so the annual cost of global cybercrimes will reach the highest level of USD 10.5 trillion by 2025 (Morgan, 2020; The Citizen, 2023)). It means that the cost of cybercrimes will exceed the profitability of the illegal drug economy and become the biggest transfer of economic value in the history. According to the global risk report of the World Economic Forum (2024), cybercrime occupies one of the first five positions by likelihood. Committing crimes through social media affects people because they need to reconsider their attitude toward privacy issues and patterns of online interaction. There are many types of social media related cybercrimes such as phishing, identity theft, cyberbullying, fraud, and data breach (PhishLabs, 2024). As of Q4 2023, the leading cybersecurity threats of organizations through social media comprise impersonations accounting for 45% of reported attacks followed by fraud (28.23%), hacking (over 21%) and phishing (PhishLabs, 2024).

Emergence of new technologies and innovations brings unprecedented development to the digital sphere in developing countries; however, it is accompanied by the increase in cybersecurity threats. The growth in the number of people using the internet is caused by mobile broadband penetration, affordability of smartphones and increasing levels of digital literacy. GSMA (2024) states that Sub-Saharan Africa acquires millions of mobile internet users annually, while according to the International Police INTERPOL (2025) cybercrimes become widespread in these conditions. Social media represents an attractive place for criminals where they can take advantage of people who have recently accessed the internet. Many researches indicate that cybercrime threats change people's behavior and their attitude toward social media sites making them less willing to use them (Börsting et al., 2024; Niu et al., 2024). Application of the Protection Motivation Theory (PMT) in developing countries shows that threat appraisals and coping beliefs are closely linked to the protection against online attacks (Ho et al., 2023). Despite the existence of abundant world literature on the topic, little is known about the way cybercrime influences individuals in Sub-Saharan countries, particularly in East Africa. There are scarce empirical researches of cybercrimes and their implications for the use of social media in Tanzania.

Nowadays, Tanzania experiences the rapid development of technologies and digital services while being faced with the problem of cybersecurity threats. The number of internet users increased from 29 million in 2020 up to 54.1 million by the end of the 2024/25 fiscal year (Tanzania Communications Regulatory Authority [TCRA], 2025). About 6.75 million people use social media as of January 2025, which is almost a half of the previous year's increase year (DataReportal, 2024; Gurdian (Tanzania), 2024). The penetration rate of mobile phones is over 85%, which makes it one of the leaders in Africa (The Citizen, 2025). The median age in Tanzania equals 17 years (DataReportal, 2024), which means that the majority of people are young and use social media very often. Young and inexperienced internet users represent the high-risk category for cybercrimes. For example, in 2022, the number of cybercrimes increased by 30% compared to 2021 (TCRA, 2024). Among other forms of cybercrimes in social media in Tanzania, there are phishing, which involves the theft of personal information; identity theft through impersonation; cyberbullying and harassment of young and female users; and posting content leading to data breach (Mkoweka, 2023) . Such actions of cybercrime represent danger for people's safety when they use social media websites. Despite many efforts made by the Tanzania government to overcome the problem of cybercrimes, including adoption of the Cybercrimes Act (2015), the National Cybersecurity Strategy 2023-2028 and establishment of the Data Protection Commission, the country suffers from many problems associated with low levels of digital literacy (Nashon et al., 2025; The Citizen, 2025). Continuous efforts to inform citizens about the dangers of cybercrimes remain crucial as well. It is necessary to note that the lack of information regarding the effects of the crime remains the problem to be solved.

Although some literature on cybercrime threats and social media use exists, this topic is not enough covered in the literature, especially when it comes to developing countries. First, most literature on the topic deals with Western countries; therefore, it poses problems with the transfer of findings to another country (Börsting et al., 2024; Chen et al., 2023). Besides, Tanzanian literature is mostly concerned with the description of different forms of cybercrimes; however, it does not pay much attention to any causative variables or mediators associated with social media use and behavior, which may lead to the problem of cybercrimes. However, it is necessary to have empirical findings regarding cybercrimes in terms of social media use in Tanzania in order to help the government achieve 80% internet penetration in the country (The Citizen, 2025).

1.1 Statement of the Problem

With increased social media usage in Tanzania, the digital ecosystem become increasingly vulnerable to cybercrime. Currently, social media plays an important role communication, interactions, education, e-commerce and civic engagement. It is mainly used by the youth population that is considerable as main consumer of online media (DataReportal, 2024; TCRA, 2025). Moreover, cybercrimes including cyberbullying and data breaches are common among the students of higher educational institutions of Dar es Salaam city thus posing a serious threat to their online safety (Mwamba & Mjema, 2024). Social media phishing tricks innocent people into providing their personal data while impersonation helps commit identity fraud (Toukabr, 2024). Privacy invasion because of data breaches makes people think twice before posting their private data on the websites (Chen et al., 2023; Ho et al., 2023).

Despite the fact that empirical studies on the global level indicate that cybercrime threats have a substantial impact on the online behavior of people (Börsting et al., 2024), privacy concerns play an important role in mediating the effect of negative online experiences on social media behaviors (Niu et al., 2024), there is a lack of empirical evidence to verify if the same patterns apply to the case of Tanzania. Available empirical literature on the topic related to the country under discussion is limited to the description of various types of cybercrimes and does not provide any methodologies to establish causation between social media usage and cybercrimes (Mkoweka, 2023; Nashon et al., 2025). Additionally, due to the lack of knowledge about whether policies to deal with cybercrime have been implemented successfully, it is unknown whether there is an effect of these policies on people's behavior concerning cybercrime. Therefore, in order to develop effective solution both government bodies and social media companies face difficulties due to sufficient knowledge about the of cybercrime threats on online behavior and social media usage. Thus, this study aims at analyzing the effect of cybercrime threats on social media usage.

1.2 Research Questions

i. What is the effect of phishing attacks on social media usage?
ii. What is the influence of cyberbullying and online harassment on social media usage?
iii. What is the relationship between data breaches, privacy violation and user's trust in social media usage?

II. LITERATURE REVIEW

2.1 Theoretical Review

2.1.1 Protection Motivation Theory (PMT)

Protection Motivation Theory developed by Rogers (1975) highlights how people become motivated towards adopting protective measures when exposed to threats. As per Maddux and Rogers (1983) two factors play an important

role in motivating people in terms of protection motivation: threat appraisal and coping appraisal. The former consists of perception of severity and vulnerability whereas the latter consists of perceived response efficacy and self-efficacy. Hedayati et al. (2023) indicate that individuals with coping appraisal, especially self-efficacy have lower chances of becoming victims of phishing attacks. In the current study, PMT theory is used to understand user's behavior regarding cyber-risks such as phishing, cyberbullying, and data breach.

2.1.2 Social Cognitive Theory (SCT)

As per Social Cognitive Theory (SCT), introduced by Bandura (2001), social interactions, learning and self-efficacy shape human behavior in the digital environment. SCT suggests that user behavior such as levels of engagement, trust and privacy settings on digital platforms are influenced by observational learning, social and cognitive processes. The empirical findings of Frauenstein et al. (2023) state that habitual use of social media platforms and heuristic (i.e., low-effort) processing makes people more vulnerable to phishing scams. In this study SCT therefore provides insights into how learned experiences, habits and social environment influences individual's responses to cyber threats.

2.2 Empirical Review

Empirically, this study reviews literature that corresponds to the research questions.

2.2.1 Phishing Attacks and Social Media Usage

Empirical studies consistently show that phishing remains a major vector of cybercrime affecting social media users and that exposure to phishing influences users' behavior, trust, and platform engagement. Major monitoring studies have confirmed increases in volume of phishing attacks and also noted the growing trend in delivery of phishing via social media that results in credential and account takeovers and subsequently reduces user confidence in online communication channels (Anti-Phishing Working Group [APWG], 2025). On the context-specific and country-level scale, research found not only economic losses in terms of financial fraud but also behavior changes such as reduction in online activity, cautiousness regarding clicking links, and abandoning of services in some cases. Field research in Tanzania among mobile phone and market vendors has found that phishing incidents create both social and psychological impact on victims in terms of reduced trust, altered social interaction and financial harm (Mwamba & Mjema, 2024). Literature has also revealed demographic differences with younger, less educated, less security-aware and technologically illiterate users being more prone to phishing attacks on social media whereas increased awareness and improvement of security features on platforms reduce users' vulnerability and boost confidence (Toukabr, 2024).

2.2.2 Cyberbullying and Online Harassment Influence on Social Media Usage

The empirical significance of cyberbullying and online harassment has been demonstrated through various studies which link such exposure with serious psychological outcomes. Notably, Young et al. (2024) applying survey and epidemiological data at the national level, demonstrate the emergence of significant withdrawal behavior, characterized by reduced content sharing, activating of restrictive privacy settings, and full-scale platform departure, among frequent social media users exposed to cyberbullying events, mediated by clinical psychological distress symptoms such as sadness, hopelessness, and anxiety. This evidence directly guides the current research by offering behavioral disengagement and emotional distress as relevant outcome variables in relation to the effects of cybercrime threats on social media usage among Tanzanian users, and by supporting the employment of platform withdrawal and decreased usage intensity as dependent indicators within the research design. Other policy-related evidence highlights the impact of the insufficient enforcement of rules on creating a hostile environment, dissuading the involvement in activity especially among vulnerable groups, such as young people, women, and individuals with poor digital skills. Specifically, this aspect provides an important contribution to the current research by allowing an assessment of whether perceptions about the sufficiency of legal protection moderate the influence of cyberbullying threats on social media usage among Tanzanian users, since there are clear examples of inadequate enforcement of the Cybercrimes Act of 2015 in Tanzania (Nashon et al., 2025). Benard et al. (2021), examining the impact of cyberbullying on Sub-Saharan countries, emphasize the importance of cultural norms of silence and social stigma in combination with low levels of organizational infrastructure to provide support to victims as the determinants of the increased negative correlation between online harassment exposure and social media consumption. This particular regional insight is especially crucial in relation to the current study as a reminder that results from Western countries and developed nations should not be generalized to Tanzania, and as a methodological justification of conducting an empirical research based on local evidence in order to understand the interaction between cyberbullying and social media usage among Tanzanian users.

2.2.3 Data Breaches, Privacy Violations, and Users' Trust in Social Media Usage

Literature on privacy violation and data breach risks, as well as the consequences for trust and social media usage, provides several important theoretical references and operationalized variables that will be used in the current research. Neves et al. (2024), analyzing privacy behavior across various national contexts, have identified that higher

levels of concern about privacy translate into greater restrictions in disclosing private data and engaging in interpersonal communication in online environments. Furthermore, Kim et al. (2023) support the argument regarding privacy concerns as important predictors of reduced social media usage and avoidance of any kind of personal information disclosure in order to avoid potential misuse. In particular, a lack of public awareness of digital privacy rights leads to a situation where privacy risk perception increases significantly (Nashon et al., 2025). Moreover, Hedayati et al. (2023) provide another key determinant in form of coping appraisal, which is an important factor behind maintaining safe online activity. This insight is crucial for selecting protection motivation theory (PMT) as the main theoretical foundation of the study. Finally, Fletcher et al. (2024) suggest that inadequate account control and data management on the part of platform providers lead to distrust, irrespective of cybercrime threat experience. These studies are applicable to the current research since there is a relatively poor regulatory infrastructure for protecting users' data in Tanzania

2.3 Research Gap

Notwithstanding the fact that cybercrime threats, such as phishing, cyberbullying, and data breaches, are now widely recognized across the globe, little is known empirically about how these issues influence social media usage in Tanzania. Most of the studies have been conducted in developed countries, which creates a contextual gap in knowing user behavior in developing country settings. The local available studies are fragmented and individually focused on specific groups rather than the general population. Furthermore, the combined effects of these threats on trust, engagement, and platform preference remain underexplored. This calls for this study to fill the gap by examining how cybercrime threats influence social media usage among Tanzanian users.

III. METHODOLOGY

3.1 Research Design

This study employed a descriptive research design with a mixed method approach, combining both quantitative and qualitative techniques. The descriptive design was chosen because it allows systematic collection of information on current conditions, opinion and practice regarding the impact of cybercrime threats on social media usage. The mixed approach enables triangulation of data, improving reliability and validity by capturing both statistical trends and in-depth perspectives.

3.2 Study Area

This study was conducted in Dar es Salaam region where internet penetration and social media usage are highest. Dar es Salaam was selected as the study area due to its highest internet penetration and social media usage in Tanzania (TCRA, 2025b). The city also experiences a higher rate of cybercrime incidents because of its huge online population and also, its social and economic variety offers a suitable sample size that is representative of social media usage (Kayumbe & Gilliard, 2024)..

3.3 Target Population

The target population of this study was social media users, particularly individuals aged 18 years and above who actively use platforms such as Facebook, Instagram, WhatsApp, TikTok and X (formerly Twitter). This group was chosen because they are most likely to experience cybercrime threats such as phishing, cyberbullying and harassment, identity theft and privacy violations.

3.4 Sampling Strategy

This study used two stage cluster sampling strategy to gather respondents as complemented by purposive sampling strategy. In implementing the strategy, the study kept districts within Dar es Salaam region into five clusters representing Ilala, Kinondoni, Ubungo, Kigamboni and Temeke districts. Initially, three municipalities Kinondoni, Ilala and Kigamboni were randomly selected from Dar es Salaam region. The second stage, specific clusters such as universities, markets and public transport hubs were identified within each municipality from which respondents were selected using systematic random sampling. This approach allowed inclusion of diverse social media users across demographic and social economic groups. To complement the quantitative data, purposive sampling was used to select key informants including social media influences, victims of cybercrime and ICT experts for quantitative interviews which enhance the validity and reliability of findings.

3.5 Sample Size

The sample size is calculated using Cochran's formula with 95% CI, 5% margin

$$n_0 = \frac{Z^2 p(1-p)}{e^2} \quad (1)$$

Where:

n_o= required sample size
Z = Z-score for chosen confidence level
p = estimated proportion of attribute in population
e = desired margin of error
Z=1.96, p=0.5, e=0.05.
n_o= 385 Social Media users

The targeted sample size for this study was 385 Social Media users. Nevertheless, out of 385 targeted sample, only 340 successful sample were used as respondents. In that regard, the study final sample size was 340 respondents.

3.6 Data Collection Approach and Methods

The cross-sectional approach was utilized in administering and collection of the mixed data. The study used both quantitative and qualitative methods for comprehensive understanding. Quantitative data were collected through five-point Likert scale questionnaires distributed to social media users, while qualitative data came from semi-structured interviews with ICT experts, influencers, and victims of cybercrime. These methods complemented each other to enhance data validity and reliability.

3.7 Data Analysis

Mixed descriptive analysis approaches were engaged in processing, manipulating, and presenting findings based on the data nature. Moreover, the quantitative data collected through Likert scale questionnaires were analyzed using Seemingly Unrelated Regression (SURE) whereby each independent variable was tested with each dependent variable to establish the existing influence Further, the qualitative data collected through semi-structured interview were manipulated using content analysis to get insight responses for triangulation purpose.
Analysis required separate equations as described below.

Regarding **Phishing Attacks**, the equation reads

$$Y1 = \beta 0 + \beta 1X1 + \beta 2X2 + B3X3 + \varepsilon 1 \quad (2)$$

Where;

Y1= Phishing attacks
X1 = Platform preference
X2 = Engagement level
X3 = Trust and privacy perception
β0 = Intercept
β1, β2, β3 = Coefficients
ε1 = Error

Regarding **Cyberbullying and Online Harassment**, the equation reads;

$$Y2 = \beta 0 + \beta 4X1 + \beta 5X2 + B6X3 + \varepsilon 2 \quad (3)$$

Where;

Y2 = Cyberbullying and Harassment
X1 = Platform preference
X2 = Engagement level
X3 = Trust and privacy perception
β0 = Intercept
β4, β5, β6 = Coefficients
ε2 = Error

Regarding **Data Breaches and Privacy Violation**, the equation reads;

$$Y3 = \beta 0 + \beta 7X1 + \beta 8X2 + B9X3 + \varepsilon 3 \quad (4)$$

Where;

Y3 = Data Breaches and Privacy Violation
X1 = Platform preference
X2 = Engagement level
X3 = Trust and privacy perception
β0 = Intercept
β7, β8, β9= Coefficients
ε3 = Error

3.8 Validity and Reliability

The piloting of the tools was done to enhance data validity and therefore amendments were made correspondingly to remove redundant items and errors whereas reliability was attained using Cronbach Alpha test based on 0.70 -1 score.

3.9 Ethical Consideration

The researcher adhered to research ethics, policy, and code of conduct throughout the study. Moreover, during the data collection processes, respondents were informed that their participation was completely voluntary. The data were triangulated to reflect blended responses. Pseudonyms were utilized to hide the names of respondents for the purposes of confidentiality and privacy.

IV. FINDINGS & DISCUSSION

4.1 Demographic Profile of Respondents

Table 1 shows the demographic profile of total 340 participants involved in the study. The male-female ratio shows a slightly higher number of male, 195 (57.4%) than females, 145 (42.6%). This skewness is consistent with the general trend of greater uptake of social media usage among men than women in Tanzania (DataReportal, 2024; TCRA, 2022). However, the presence female participants is still enough to address the various dimensions of cybercrime vulnerability, especially cyberbullying and online harassment (Benard et al., 2021). In terms of age, the large number of respondents were those aged 18-29 (55%), while 30-39 accounted for 27.9% of respondents and above 40 years for 17.1%. the aforementioned proportions are in line with the general median age of the population in Tanzania that is estimated to be 17 years (DataReportal, 2024). In addition, these proportions support previous studies that revealed the greatest activity in social media use among the youth age group (18-39) which makes this age group most susceptible to cybercrimes. These reasons include poor awareness of digital security, significant involvement in social media activities and tendency to provide personal information online (INTERPOL, 2025; Mkoweka, 2023; Mwamba & Mjema, 2024). With regard to educational qualification, the study sample has considerable variability in terms of qualification level, the largest group was represented by individuals with Bachelor's degrees (n=112, 32.9%), second in size was individuals with secondary education (n=97, 28.5%), followed by individuals with Diploma/ Certificate education (n=62, 18.2%), individual's with primary education (n=46, 13.5%) and individuals with Master's degree and above (n=23, 6.8%). Particularly, 42.1% of respondents had secondary or lower level of education, meaning that different groups have access to social media therefore are potentially exposed to cybercrime (Hedayati et al., 2023).

Table 1

Demographic Profile

Category	Description	Frequency	Percent
Gender	Male	195	57.4%
	Female	145	42.6%
Age	18–23 years	78	22.9%
	24–29 years	109	32.1%
	30–39 years	95	27.9%
	40 and above	58	17.1%
Education	Primary	46	13.5%
	Secondary	97	28.5%
	Diploma/Certificate	62	18.2%
	Bachelor's Degree	112	32.9%
	Master's and above	23	6.8%

Source: Field Data (2025)

4.2 Statistical Test

Reliability, data normality and correlation test were performed. *Reliability Test*: Cronbach's Alpha was computed for major constructs. All values were above the 0.70 threshold, confirming strong internal consistence (Koonce & Kelly, 2014).

Table 2
Reliability Test

Variable	Cronbach's Alpha	No. of Items
Phishing Attacks	0.886	7
Cyberbullying & Harassment	0.803	6
Data Breaches & Privacy Violations	0.771	6
Engagement Level	0.741	4
Trust & Privacy Perception	0.763	4

4.3 Normality Test

Before conducting the regression analysis, it was checked whether all five study variables follow normal distributions through skewness and kurtosis statistics. The outcomes of normality tests are presented in Table 3. According to the results, all five variables can be described by a normal distribution and meet parametric assumptions for SUR estimation. The skewness statistics for five variables varied from −0.019 for Engagement Level to 0.033 for Trust and Privacy Perception, which was not out of ±1.0 range according to Hair et al. (2019), and meant that there is an insignificant asymmetry of the distributions of studied variables. Moreover, kurtosis statistics varied from −0.032 for Phishing Attacks to 0.044 for Cyberbullying and Harassment; however, all kurtosis statistics remained below ±1.0 boundary, and indicated lack of peakedness or flatness in distribution of the examined variables. Only one variable, Engagement Level, showed a negative skewness statistic (−0.019) which means a slight shift of the distribution curve towards the right side, whereas a slightly larger skewness statistic (0.033) was observed for Trust and Privacy Perception. Nevertheless, such deviations are statistically insignificant and have no practical implications. All five variables met the requirements for normality ($p < 0.05$), while the p-value statistics of four out of five variables were equal to zero (Phishing Attacks, Cyberbullying and Harassment, Data Breaches and Privacy, and Trust and Privacy Perception). The only exception was Engagement Level ($p = 0.041$). Therefore, having considered near zero skewness and kurtosis statistics together with significant p-values of all variables, it can be stated that the collected data follow the normal distribution.

Table 3
Normality Test

Variable	Skewness	Kurtosis	p-value
Phishing Attacks	0.021	-0.032	0.000
Cyberbullying & Harassment	0.015	0.044	0.000
Data Breaches & Privacy	0.028	-0.025	0.000
Engagement Level	-0.019	0.037	0.041
Trust & Privacy Perception	0.033	0.002	0.000

4.4 Correlation Test

Table 4 provides the correlation matrix for the five dependent and independent variables included in this study. The output demonstrates a clear pattern of associations in the expected direction, providing a preliminary rationale to advance the proposed hypotheses to multivariate testing. As expected from the study's theoretical underpinnings, the three cybercrime threats (phishing attacks, cyberbullying, and data breaches) present moderate intercorrelations (ranging from 0.367 to 0.412), suggesting that they tend to occur in tandem rather than independently within the social media environment of Tanzania, which is consistent with the regional cybersecurity assessments (INTERPOL, 2025). The observed intercorrelations are not only theoretically meaningful but statistically plausible, remaining moderate in magnitude and falling below the accepted limit for multicollinearity ($r < 0.70$) to allow for the proper discriminant validity of the threat constructs and their independent role as predictors in regression models

All three cybercrime threats were found to be negatively correlated with social media engagement, with cyberbullying presenting the highest negative association ($r = -0.402$), followed by privacy violations caused by data breaches ($r = -0.344$) and phishing ($r = -0.321$). The findings imply that the more likely the exposure to cybercrimes, the less likely the users are to use social media platforms actively. The particularly high suppressive impact of cyberbullying on social media engagement is consistent with Young et al.'s (2024) assertion that harassment-related psychological distress is the main driver behind individuals' decisions to withdraw from social networks. The negative relationship between phishing attacks and social media engagement is attributable to increased risk perception and protective avoidance motivated by the principles of protection motivation theory (Rogers, 1975).

Similar to the observed correlations with social media engagement, all three cybercrime threats showed a negative relationship with trust and privacy perceptions, where the impact of data breaches proved to be the most severe ($r = -0.415$), followed by the impact of cyberbullying ($r = -0.375$) and phishing ($r = -0.298$). The finding that data breaches contribute the most to user dissatisfaction is consistent with the literature, including Neves et al. (2024) and

Fletcher et al. (2024), who argue that the violation of online privacy and the absence of sufficient data security measures serve as antecedents of users' distrust. Notably, there was a very strong and positively correlated association between social media engagement and trust (r = 0.529).

Table 4
Correlation Test

Variables	Phishing	Bullying	Breaches	Engagement	Trust
Phishing Attacks	1	0.412	0.389	-0.321	-0.298
Cyberbullying & Harassment	0.412	1	0.367	-0.402	-0.375
Data Breaches & Privacy	0.389	0.367	1	-0.344	-0.415
Engagement Level	-0.321	-0.402	-0.344	1	0.529
Trust & Privacy Perception	-0.298	-0.375	-0.415	0.529	1

4.5 Model Fits

Seemingly Unrelated Regression (SUR) was used to assess the model fit across all nine hypotheses tested, with results presented in Table 5. Overall, measures of the model fit including RMSE, percentage explained variance (R^2), Chi-square value (χ^2) and corresponding p-values suggest that the tested models have statistically significant but relatively small explanatory power regarding all nine examined relationships. The smallest RMSE was found equal to 0.887 (H1: Phishing → Platform Preference), whereas the largest was equal to 0.934 (H8: Data Breaches → Engagement Level), which suggests that all models have consistent and acceptable prediction capabilities with regards to all nine variables investigated. Explained variance ranges between 0.031 (H1: Phishing → Platform Preference) and 0.071 (H9: Data Breaches → Trust and Privacy Perception). Although explained variance is relatively low, these results should be considered theoretically acceptable as social media behavior and social media security are very complex multidimensional constructs and, thus, should be expected to demonstrate small-to-moderate effect sizes (Cohen, 1988). It is noteworthy that the equations for data breaches are characterized by the highest explanatory power for all three dependent variables investigated (R^2 = 0.048, 0.063, and 0.071 for H7, H8, and H9, respectively), which means that data breaches are the most impactful cybercrime category influencing the choice of platform, level of engagement with the chosen social media platform and overall perception of trust and privacy. On the other hand, equations for phishing attacks display the smallest values of explained variance (0.031 to 0.052). All nine models under investigation demonstrated statistical significance as shown through Chi-square test results, with p-values ranging between p = 0.026 (H1) to p < 0.001 (H8 and H9). Best-fit models were found to be H9 (Data Breaches → Trust and Privacy Perception; χ^2 = 18.75, p < 0.001) and H8 (Data Breaches → Engagement Level; χ^2 = 15.29, p < 0.001), which implies that data breaches have the largest impact on user behavior on social media platforms, as well as on their perceptions of the level of trust and privacy.

Table 5
Model Fit

Hypothesis	Relationship Tested	RMSE	R^2	Chi^2	p-value
H1	Phishing → Platform Preference	0.915	0.031	5.87	0.026
H2	Phishing → Engagement Level	0.902	0.044	9.63	0.003
H3	Phishing → Trust & Privacy Perception	0.933	0.052	11.78	0.001
H4	Cyberbullying → Platform Preference	0.926	0.036	7.54	0.009
H5	Cyberbullying → Engagement Level	0.911	0.049	10.67	0.002
H6	Cyberbullying → Trust & Privacy Perception	0.934	0.041	8.93	0.004
H7	Data Breaches → Platform Preference	0.898	0.048	12.34	0.001
H8	Data Breaches → Engagement Level	0.887	0.063	15.29	0.000
H9	Data Breaches → Trust & Privacy Perception	0.904	0.071	18.75	0.000

4.6 Findings

4.6.1 Effect of Phishing Attacks on Social Media Usage

The seemingly unrelated regression (SUR) findings for hypotheses 1-3 that investigate the effect of phishing attacks on dimensions of social media usage are presented in Table 6. Hypotheses 1-3 are valid, as the independent variable significantly affects platform preference, engagement level, and trust and privacy perception. Hypothesis 1 posited that phishing attacks negatively impact the social media users' preference towards a particular platform. The data proves that the research hypothesis is valid (β = -0.214, SE = 0.082, z = -2.61, p = 0.009, 95% CI [-0.374, -0.054]) by revealing that exposure to phishing attacks leads users to switch or avoid social media platforms viewed as not safe

enough. Similarly, hypothesis 2 posits that phishing attacks negatively affect social media engagement level. The data supports the hypothesis (β = -0.332, SE = 0.095, z = -3.49, p = 0.001, 95% CI [-0.518, -0.146]). Given the greater magnitude of the coefficient in comparison to H1, it can be concluded that phishing attacks have a stronger negative impact on active platform engagement than choosing the social network to use. This result corresponds to the idea of Protection Motivation Theory that states that people react to high threats through behavioral disengagement (Maddux & Rogers, 1983). Finally, hypothesis 3 assumes that phishing attacks negatively affect users' social media trust and privacy perception. The results provide empirical support to this assumption as well, and the coefficient value is the highest compared to other variables (β = -0.401, SE = 0.101, z = -3.97, p < 0.001, 95% CI [-0.599, -0.203]). Therefore, it can be stated that the effect of phishing is especially adverse for users' trust regarding platform security. This statement is consistent with the study by (Toukabr, 2024), which proves that phishing attacks lead to substantial distrust toward the social media environment. All three coefficients demonstrate increasing magnitude when comparing platform preference (β = -0.214), engagement level (β = -0.332), and trust and privacy perception (β = -0.401). Therefore, it can be claimed that phishing attacks adversely impact all aspects of social media usage among Tanzanian individuals, with the most damaging one being trust perception.

The results show that phishing attacks have a strong and adverse impact on participation, trust, and platform choice. Interviews also testified that the majority of users grew suspicious or stepped back following scams. One respondent said:

> "*After losing money through a deceitful WhatsApp link, I began to ignore the unknown messages and made fewer online visits."* (Respondent 14, 26th May 2025)

This is supported by APWG (2025) and Mwamba and Mjema (2024), who argue that phishing deters trust and online participation.

Table 6

Seemingly Unrelated Regression Results (Phishing H1–H3)

Hypothesis	Coef.	Std. Err.	Z	p > z	[95% Conf. Interval]
H1: Phishing → Platform Preference	-0.214	0.082	-2.61	0.009	-0.374 – -0.054
H2: Phishing → Engagement Level	-0.332	0.095	-3.49	0.001	-0.518 – -0.146
H3: Phishing → Trust & Privacy	-0.401	0.101	-3.97	0.000	-0.599 – -0.203

4.6.2 Influence of Cyberbullying and Harassment on Social Media Usage

The findings reported in Table 7 below show that the three hypotheses postulating an influence of cyberbullying and harassment on dimensions of social media usage were all supported significant negative beta coefficients for all three constructs. H4 hypothesized that cyberbullying and harassment would negatively affect the dimension of platform preference and was supported (β = -0.243, SE = 0.089, z = -2.73, p = 0.006, 95% CI [-0.418, -0.068]). This finding supports the view that cyberbullied individuals tend to abandon or cease using platforms where they have had such experiences. Hypothesis H5, which stated that cyberbullying and harassment negatively affect engagement level on social media platforms, yielded the highest coefficient value among the three cyberbullying hypotheses, thus showing a highly significant influence of cyberbullying (β = -0.378, SE = 0.094, z = -4.02, p < 0.001, 95% CI [-0.562, -0.194]). The findings indicate that suppression of engagement is the immediate and the most noticeable behavioral consequence of being exposed to cyberbullying among Tanzanian social media users. The findings are consistent with the empirical evidence of Young et al. (2024) that harassment-induced psychological stress, such as anxiety, hopelessness, and withdrawal, mediates the relationship between cyberbullying and decreased level of active engagement on social platforms. H6 assumed that cyberbullying and harassment would negatively influence the dimension of trust and privacy perception and was supported (β = -0.295, SE = 0.087, z = -3.39, p = 0.001, 95% CI [-0.466, -0.124]).

Upon comparing the strength of the negative influences of cyberbullying on the three dimensions in question (engagement level, trust and privacy perception, platform preference), engagement level (β = -0.378) emerges as the most affected construct, followed by trust and privacy perception (β = -0.295), and platform preference (β = -0.243). This pattern reflects the fact that cyberbullying initially affects active participation and gradually leads to distrust of particular platforms. These findings are consistent with those of Benard et al. (2021) reporting increased likelihood for East African social media users who had been harassed online to stop engaging in particular interactions rather than migrating to different platforms immediately. In comparing cyberbullying beta-coefficients with phishing ones, one can observe that cyberbullying affects engagement more strongly (β = -0.378 vs. β = -0.332), but trust and privacy perception less strongly (β = -0.295 vs. β = -0.401). The results show that cyberbullying lowers social media usage significantly through reduced interaction and confidence. The interviewees confirmed that harassment online leads to withdrawal, especially in women. A victim replied:

> "*When I was bullied on Facebook, I deactivated my account for two months. I didn't feel safe*." (Respondent 7, 26th May 2025)

These findings are consistent with Mataga (2021) and Young et al. (2024),who showed that harassment leads to disengagement and emotional distress.

Table 7

Seemingly Unrelated Regression Results (Bullying H4–H6)

Hypothesis	Coef.	Std. Err.	Z	p > z	[95% Conf. Interval]
H4: Bullying → Platform Preference	-0.243	0.089	-2.73	0.006	-0.418 – -0.068
H5: Bullying → Engagement Level	-0.378	0.094	-4.02	0.000	-0.562 – -0.194
H6: Bullying → Trust & Privacy	-0.295	0.087	-3.39	0.001	-0.466 – -0.124

4.6.3 Impact of Data Breaches and Privacy Violations on Trust

The results regarding hypotheses H7-H9 on the influence of data breaches and privacy violations on social media use are provided in Table 8. In particular, the coefficients and levels of statistical significance were highest for the equation of data breach among all the variables considered for all the types of cybercrime. Specifically, H7 states that data breach has a negative effect on platform preference, and the hypothesis is confirmed (β = -0.271, SE = 0.084, z = -3.23, p = 0.001, 95% CI [-0.436, -0.106]). It can be interpreted that individuals who have been involved in data breach episodes reconsider their preferences about the platforms and choose other alternatives as less exposed to risks. H8 states that data breaches have a negative effect on engagement level and is supported by the results (β = -0.356, SE = 0.092, z = -3.87, p < 0.001, 95% CI [-0.537, -0.175]), which confirms that privacy violation experiences affect users' activity on the social network sites significantly. The findings are consistent with Kim et al. (2023) reporting that online privacy violations inhibit individuals from sharing information online because they fear adverse effects due to lack of regulatory mechanisms. Lastly, H9 claims that data breach negatively influences trust and privacy perceptions, providing the largest coefficient and the highest significance level of all the hypotheses examined in this research (β = -0.447, SE = 0.098, z = -4.56, p < 0.001, 95% CI [-0.639, -0.255]). Namely, it means that trust erosion becomes the most damaging consequence experienced by individuals who face the exposure to data breaches, as stated by Neves et al. (2024) and Fletcher et al. (2024). As follows from the analysis of the hypotheses concerning data breaches and privacy violations, the coefficients decrease from trust and privacy perception (β = -0.447), to engagement level (β = -0.356), to platform preference (β = -0.271). In other words, data breach influences the level of confidence in platform security first and then leads to decreased engagement levels and changes in preferences. Data breaches have the strongest negative effect, especially on privacy perception and trust. Many respondents expressed reluctance to post personal data on the Internet. One respondent reported that

> "*Upon hearing news of leaked accounts, I do not keep my personal information in apps anymore*." (Respondent 2, 26th May 2025)

This aligns with Kim et al. (2023), Neves et al. (2024) and Fletcher et al. (2024) who assert privacy issues reduce engagement and trust.

Table 8

Seemingly Unrelated Regression Results (Data Breaches H7–H9)

Hypothesis	Coef.	Std. Err.	Z	p > z	[95% Conf. Interval]
H7: Breaches → Platform Preference	-0.271	0.084	-3.23	0.001	-0.436 – -0.106
H8: Breaches → Engagement Level	-0.356	0.092	-3.87	0.000	-0.537 – -0.175
H9: Breaches → Trust & Privacy	-0.447	0.098	-4.56	0.000	-0.639 – -0.255

4.7 Discussion

The empirical evidence supports the theory that cybercrime risks significantly influence social media usage among Tanzanian users regarding the dimension of platform preference, engagement, and trust and privacy perceptions based on PMT-SCT framework.

Firstly, phishing had significant negative influence on all three dimensions – preference (β=-0.214, p=0.009), engagement (β=-0.332, p=0.001), and trust and privacy perceptions (β=-0.401, p<0.001). As the coefficients increased progressively, one can say that phishing affects first of all the confidence and security in using platforms before influencing behavior directly, according to PMT. In this case, the perception of both severity and vulnerability prompts an avoidance coping response that leads to platform disengagement. Moreover, it can be interpreted within the SCT framework by taking into account that users acquire a vicarious experience through their peers' suffering that creates both trust and privacy issues and influences the usage even without actual experience (Bandura, 1986). Thus, these findings can be explained by Anti-Phishing Working Group (2025) and Mwamba and Mjema (2024)who state that phishing causes long-lasting psychological injuries to the online community's trust, not just financial ones, especially in developing countries characterized by poor cybersecurity education.

Secondly, cyberbullying and harassment had the most pronounced negative impact on the engagement level (β=-0.378, p<0.001) among the threats studied but relatively weak on trust (β=-0.295, p=0.001) and preference (β=-0.243, p=0.006). Thus, it can be stated that harassment influences the usage through behavioral dimension rather than the cognitive one similarly to phishing. While cyberbullying is aimed at causing emotional distress and therefore leading to depression and hopelessness, which results in platform disengagement, phishing is more cognitive in terms of eroding users' trust in platforms(Young et al., 2024). Moreover, the same disengagement strategies were reported among Tanzanian victims by Mataga (2021) who opted out for account deletion and selective silence rather than for reporting the offense. According to PMT, users experiencing harassment will prefer avoiding this risk by reducing the level of engagement and thus not implementing any preventive measures (Hedayati et al., 2023). Moreover, SCT shows that witnessing cyberbullying leads to emotional responses, which suppress participants' behavior (Bandura, 2001).

Finally, data breaches and privacy violations caused the most significant negative impacts in all three areas: preference (β=-0.271, p=0.001), engagement level (β=-0.356, p<0.001) but above all, trust and privacy perception (β=-0.447, p<0.001). Hence, privacy violation appears to be the most destructive cybercrime threat to social media usage. The reason for this impact lies in the theory as data breaches involve not only a personal risk but also vulnerability on a platform's side; thus, a platform is also involved in creating a threat. It was proved by Neves et al. (2024), Fletcher et al. (2024) who found insufficient platform-level data management as the most significant threat to building trust between users and platforms. Besides, Kim et al. (2023) found that privacy threat perception acts as a systematic deterrent from sharing personal information online, especially in countries lacking effective regulations like Tanzania (Nashon et al., 2025). Hence, according to PMT, people perceive the threats associated with data breaches much greater than their ability to cope with them, which leads to avoidance coping, and SCT explains how media communication about such cases and discussion by peers spread privacy risks among users (INTERPOL, 2025).

Thus, the hierarchy of cybercrimes in terms of their negative impacts is as follows: data breaches cause structural harm, cyberbullying leads to engagement disengagement, and phishing causes an erosion of trust in platforms. Therefore, one can identify corresponding implications. Firstly, it should be noted that the implementation of the Personal Data Protection Act of 2022 by Tanzania's authorities and strengthening the enforcement powers of the Data Protection Commission should be done immediately. Secondly, platform-based moderation strategies should be implemented together with culturally appropriate reporting systems since social stigma prevents victims from asking for help (Benard et al., 2021). Finally, digital literacy programs can significantly mitigate phishing risk among the young vulnerable population of Tanzania (Mkoweka, 2023).

V. CONCLUSION & RECOMMENDATION

5.1 Conclusion

The aim of this study was to assess the effect of cyberbullying threats on social media usage in Tanzania. The focus was put on such types of crimes as phishing, cyberbullying and harassment, and data breach. The findings suggest that these threats impact users by deterring their activity, creating mistrust, and influencing social media preference. More specifically, phishing discourages users from active social media usage while harassment makes users withdraw from online space as it causes emotional distress. Finally, data breaches create the largest effect by decreasing trust towards data privacy and security. Although these findings agree with similar international studies, they seem to be more intense due to the poor cybercrime enforcement, cultural prohibitions, and poor level of digital literacy. Therefore, it can be stated that cyber threats affect not only individual users but also prevent people from actively using social media as a medium for communication and doing business in Tanzania.

5.2 Recommendation

Considering the findings of the current study, it can be concluded that several measures should be taken to reduce cybercrime risks. Firstly, there is a need for conducting massive digital literacy programs that would provide individuals with an understanding of how to identify and deal with threats. Secondly, there is a need to improve the enforcement of existing legislation as well as develop new laws regarding new types of cybercrime. Moreover, social media companies operating in Tanzania are obliged to introduce safety features and user management tools for fostering trust. Finally, adequate assistance programs are essential for the victims of cyber threats so that people can actively participate in social media without fear of intimidation. The strength of the current study lies in its mixed-methods design that allowed obtaining quantitative and qualitative data thus ensuring better validity of the results. Besides, Seemingly Unrelated Regression used in the quantitative study made it possible to analyze several variables at once. At the same time, the limitations of the study are connected with its restriction to the area of one region in Tanzania, i.e. Dar es Salaam.

Declaration of Interest

The authors declare that they do not have any known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

REFERENCES

Anti-Phishing Working Group. (2025). *Phishing activity trends report: 4th quarter 2024*. https://docs.apwg.org/reports/apwg_trends_report_q4_2024.pdf

Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual Review of Psychology, 52*, 1–26. https://doi.org/10.1146/annurev.psych.52.1.1

Benard, M. C., Mwadudu, C. M., Charo, J., & Mgala, M. (2021). Cyber-crimes issues on social media usage among higher learning institutions students in Dar es Salaam Region, Tanzania. *International Journal of Scientific Research in Science, Engineering and Technology*, 8(4), 138–148. https://doi.org/10.32628/IJSRSET218418

Börsting, J., Frener, R., & Trepte, S. (2024). Privacy and political online microtargeting during the German Federal Election 2021. *Behaviour & Information Technology, 44*(12), 3097–3114. https://doi.org/10.1080/0144929X.2024.2431052

Chen, S., Gu, C., Wei, J., & Lv, M. (2023). Research on the influence mechanism of privacy invasion experiences with privacy protection intentions in social media contexts: Regulatory focus as the moderator. *Frontiers in Psychology, 13*, Article 1031592. https://doi.org/10.3389/fpsyg.2022.1031592

DataReportal. (2024). *Digital 2024: Tanzania*. Kepios, We Are Social, & Meltwater. https://datareportal.com/reports/digital-2024-tanzania

Fletcher, R., Robertson, C. T., Arguedas, A. R., & Nielsen, R. K. (2024). *Reuters Institute digital news report 2024*. Reuters Institute for the Study of Journalism. https://doi.org/10.60625/risj-vy6n-4v57

Frauenstein, E. D., Flowerday, S., Mishi, S., & Warkentin, M. (2023). Unraveling the behavioral influence of social media on phishing susceptibility: A personality–habit–information processing model. *Information & Management, 60*(7), Article 103858. https://doi.org/10.1016/j.im.2023.103858

GSMA. (2024). *The mobile economy: Sub-Saharan Africa 2024*. https://event-assets.gsma.com/pdf/GSMA_ME_SSA_2024_Web.pdf

The Guardian (Tanzania). (2024, April 22). *State of digital in Tanzania 2024/25*. IPP Media. https://www.ippmedia.com/the-guardian/business

Hedayati, S., Damghanian, H., Farhadinejad, M., & Rastgar, A. A. (2023). Meta-analysis on application of Protection Motivation Theory in preventive behaviors against COVID-19. *International Journal of Disaster Risk Reduction*, Article 103758. https://doi.org/10.1016/j.ijdrr.2023.103758

Ho, F. N., Ho-Dac, N., & Huang, J. S. (2023). The effects of privacy and data breaches on consumers' online self-disclosure, protection behavior, and message valence. *SAGE Open, 13*(3), 1–14. https://doi.org/10.1177/21582440231181395

INTERPOL. (2025). *Africa cyberthreat assessment report 2025*. https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa

Kayumbe, E., & Gilliard, E. (2024). Cybersecurity in Tanzania: Opportunities and challenges. *International Journal for Multidisciplinary Research, 6*(1), 1–13.

Kim, Y., Kim, S. H., Peterson, R. A., & Choi, J. (2023). Privacy concern and its consequences: A meta-analysis. *Technological Forecasting and Social Change, 196*, Article 122789. https://doi.org/10.1016/j.techfore.2023.122789

Koonce, G. L., & Kelly, M. D. (2014). Analysis of the reliability and validity of a mentor's assessment for principal internships. *NCPEA Education Leadership Review, 15*(2), 33–48.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Mataga, V. T. (2022). *Factors influencing university female students' response to cyberbullying and effects on academic performance* (Master's thesis, University of Cape Town). http://hdl.handle.net/11427/37621

Mkoweka, W. M. (2023). Assessment of public awareness on cyber complexity when using social media platforms in Tanzania: A case of Kigamboni Municipality. *European Journal of Theoretical and Applied Sciences, 1*(4), 774–781. https://doi.org/10.59324/ejtas.2023.1(4).70

Morgan, S. (2020, November 13). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybersecurity Ventures. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Mwamba, F., & Mjema, E. A. (2024). The effects of phishing attacks on mobile phone users in Tanzania: A case of Kariakoo Market, Dar es Salaam. *African Journal of Empirical Research, 5*(4), 665–674. https://doi.org/10.51867/ajernet.5.4.54

Nashon, S. (2025). Assessing the implementation of the Cybercrimes Act in combating cybercrimes. *International Journal of Current Science, 15*(4), 439–455. https://rjpn.org/ijcspub/papers/IJCSP25D1051.pdf

Neves, J., Turel, O., & Oliveira, T. (2024). Privacy concerns in social media use: A fear appeal intervention. *International Journal of Information Management Data Insights, 4*(2), Article 100260. https://doi.org/10.1016/j.jjimei.2024.100260

Niu, J., Mazhar, B., Haq, I. U., & Maqsood, F. (2024). Protecting privacy on social media: Mitigating cyberbullying and data heist through regulated use and detox, with a mediating role of privacy safety motivations. *Social Media + Society, 10*(4), 1-6. https://doi.org/10.1177/20563051241306331

PhishLabs. (2024). *Leading cybersecurity threats targeting organizations on social media worldwide as of the fourth quarter of 2023*. Statista. https://www.statista.com/statistics/1499087

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Tanzania Communications Regulatory Authority. (2022). *Communications statistics report: Quarter ending December 2022*. https://www.tcra.go.tz/uploads/text-editor/files/Quarter%202%20Communications%20Statistics%20-%20Revised%20Final%20(1)_1677145396.pdf

Tanzania Communications Regulatory Authority. (2024). *Communications statistics: Quarter ending September 2024.* Tanzania Communications Regulatory Authority.

Tanzania Communications Regulatory Authority. (2025). *Communications statistics report: Quarter ending December 2025.* Tanzania Communications Regulatory Authority.

The Citizen. (2023). *Kyela cocoa boom: Farmers urged to go commercial as prices rise*. https://www.thecitizen.co.tz/tanzania/business/kyela-cocoa-boom-farmers-urged-to-go-commercial-as-prices-rise-4471128

The Citizen. (2025). *Experts back Tanzania's cyber-security push amid growing digital threats*. https://www.thecitizen.co.tz

Toukabri, O. (2024). *Analysis of social media and phishing awareness among diverse higher education students: A Health Belief Model* (Master's thesis). Örebro University.

World Economic Forum. (2024). *The global risks report 2024*. https://www.weforum.org/reports/global-risks-report-2024

Young, E., McCain, J. L., Mercado, M. C., Ballesteros, M. F., Moore, S., Licitis, L., Stinson, J., Everett Jones, S., & Wilkins, N. J. (2024). Frequent social media use and experiences with bullying victimization, persistent feelings of sadness or hopelessness, and suicide risk among high school students—Youth Risk Behavior Survey, United States, 2023. *MMWR Supplements, 73*(4), 23–30. https://doi.org/10.15585/mmwr.su7304a3